行政院及所屬各機關出國報告
(出國類別：實習)

# 實習「SS7信號網路管理及分析技術」出國報告


服務機關：中華電信研究所
出國人　職　稱：助理研究員 助理研究員
　　姓　名：陳昭禎　蔡志豪

出國地點：美國
出國期間：91年12月1日至92年12月7日
報告日期：92年2月21日

系統識別號:C09200819

# 公 務 出 國 報 告 提 要

頁數: 29　含附件: 否

報告名稱:

實習「SS7信號網路管理及分析技術」

主辦機關:

中華電信研究所

聯絡人／電話:

楊學文／03-4244218

出國人員:

陳昭禎　中華電信研究所　91840專案研究計畫　助理研究員
蔡志豪　中華電信研究所　91840專案研究計畫　助理研究員

出國類別: 實習

出國地區: 美國

出國期間: 民國 91 年 12 月 01 日 -民國 91 年 12 月 07 日

報告日期: 民國 92 年 02 月 21 日

分類號/目: H6／電信　／

關鍵詞: SS7,信號,網路管理,分析技術

內容摘要: 本出國案是中華電信研究所91年度資本支出派員出國計劃第165項「SS7信號網路管理技術」國外實習計劃，爲配合研發SS7網路信號管理系統及其分析技術，學習有關SS7信號對於T1及E1介面技術，及應用在其他通訊的介面技術，同時研習相關SS7網路管理技術，以助各公司擬定SS7信號網路應用規劃、設計與建設策略。藉由此實習能深入了解現有SS7信號網路管理及分析技術，有助於本所建立自主性利基產品之研發技術及加值服務。

本文電子檔已上傳至出國報告資訊網

「赴美國 Radisys 公司實習 SS7 信號網路管理及分析」
出國報告

## 摘要

本出國案是中華電信研究所 91 年度資本支出派員出國計劃第 165 項「SS7 信號網路管理技術」國外實習計劃，爲配合研發 SS7 網路信號管理系統及其分析技術，學習有關 SS7 信號對於 T1 及 E1 介面技術，及應用在其他通訊的介面技術，同時研習相關 SS7 網路管理技術，以助各公司擬定 SS7 信號網路應用規劃、設計與建設策略。藉由此實習能深入了解現有 SS7 信號網路管理及分析技術，有助於本所建立自主性利基產品之研發技術及加值服務。

目錄

1 目的

本出國案是中華電信研究所 91 年度資本支出派員出國計劃第 165 項「SS7 信號網路管理技術」國外實習計劃，爲配合研發 SS7 網路信號管理系統及其分析技術，學習有關 SS7 信號對於 T1 及 E1 介面技術，及應用在其他通訊的介面技術。同時研習相關網路管理及介接技術，以助各分公司擬定應用規劃、設計與建設策略。執行本實習案，不僅能深入了解現有 SS7 信號網路管理及分析技術，並有助於本所建立自主性利基產品之研發技術。

本報告主要分爲 SS7 信號網路監控及管理及 SS7 在 IP 網路之應用兩部分。

2 過程

| 日期 | 地點 | 工作項目 |
|---|---|---|
| 2002/12/1~2002/12/1 | 台北→美國舊金山 | 去程 |
| 2002/12/2~2002/12/5 | Radisys 公司 | 實習 |
| 2002/12/6~2002/12/7 | 美國舊金山→台北 | 回程 |

3 Monitoring and Securing SS7 Links

3.1 SS7 Overview

SS7 is the world's largest data network. It connects SS7 carriers nationally and internationally and callers nationally and internationally. It is used in the PSTN for call setup, call management, call disconnection, returning busy signals and accessing databases. This is a separate network from the voice network and is called the out-of-band network. The SS7 network architecture defines a set of nodes that provide the network entry points, switches for routing, and databases for accessing call information. The SS7 protocol defines a set of independent blocks with each providing a different function. This is the message transport that sends messages between the nodes that provide the call functionality and access to databases.SS7 Network Architecture

3.2 SS7 Network Architecture

The SS7 network is an interconnected set of nodes called signaling points that exchange messages to support the PSTN (figure 1)[3]. There are three kinds of signaling points: Service Switching Point (SSP), Signal Transfer Point (STP), and Service Control Point (SCP). The signaling points are interconnected via signaling links. There are multiple signaling links between signaling points for redundancy. Each signaling point provides a different service. The SSP originates or terminates calls and is

the gateway to the SS7 network. The STP is a switch that routes the SS7 messages to the desired destination. The SCP provides access to databases.

**SS7 Network Architecture**

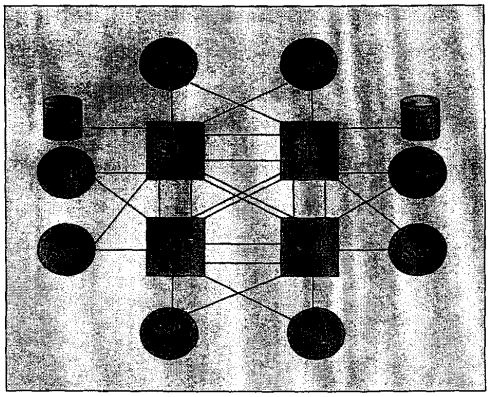


Figure 1

The SSP is the entry signaling point into the SS7 network. The main function of the SSP is to originate, terminate, and determine how to route calls. The SSP connects to voice circuits and converts the signaling from the voice switch to SS7messages. These messages are sent in the SS7 network to originate or terminate a call. The SSP uses the calling party information such as dialed digits to determine how to route a call. If the call is an 800 or 900 number the SSP must send a message to a database to get the proper routing information.

The STP is a switch in the SS7 network. The function of the STP is to route messages to the appropriate destinations. There are multiple signaling links between each STP to provide redundancy when one STP fails. There are three types of STPs: the National STP, International STP, and Gateway STP. The National STP exists within the national network. It can transfer messages that use the same national standard usually in the same country. The international STP is used in the international network. All nodes connecting to the international STP must use the ITU-TS protocol standard. The gateway STP is used to convert messages between a national STP and international STP. It can also be used to interface into another network's database.

The SCP provides an interface to database access. The database stores information such as billing, maintenance, and number translation.

Each SCP is addressed by a point code. Each database is addressed as a subsystem number. The subsystem number allows access to applications within a SCP. Each database can have a different subsystem number.

### 3.2.1 SS7 Protocol Stack

The SS7 protocol stack provides the functionality for the SSP, STP, and SCP. The SS7 protocol is layered protocol (figure 2) with each layer providing a different function. The Message Transfer Part (MTP) levels provide the routing through the network. The Signaling Connection Control Part (SCCP) provides end-to-end routing. The Transactional Capabilities Application Part (TCAP) provides the mechanism to access external databases. ISDN User Part (ISUP) provides the call connect and disconnect services.

Some SS7 networks are migrating to a high speed link (HSL) network. There are two modes of running HSL. The first mode is a recent enhancement to the standard SS7 called Q.703 Annex A. This provides enhanced MTP level 2 functions to control SS7 links at T1/E1 rates.

The second mode controls SS7 links at T1/E1 rates over asynchronous transfer mode (ATM). The layers at MTP level 3 and above stay the same. MTP level 2 will be replaced with the ATM high speed link layers.

SS7 Protocol Stacks

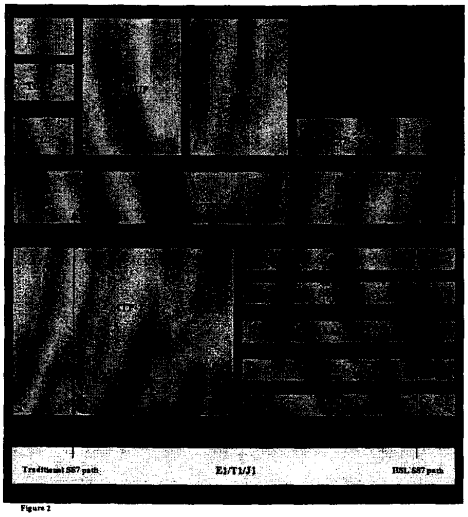



Figure 2

### 3.2.2 Message Transfer Part

MTP level 1 provides the physical layer functionality. It defines the physical and electrical characteristics of the signaling links of the SS7 network. The signaling links have a signaling data rate of 56 kbps or 64 kbps. The links may utilize DS-0 channels on a T1/E1 network or may be over a serial interface such as V.35. With HSL, the signaling rate may run at a rate of up to 2048 Mbps for 1 link.

MTP level 2 provides the data link functionality. It ensures error detection and correction and sequenced delivery of SS7 messages between two signaling points. This level does not have any knowledge of the final destination.

MTP level 3 provides the message routing and link management. Each SS7 node has an address called a destination point code. The message routing function has a routing table that stores destination point codes. When a message arrives, the destination point code is read to determine if the message is for the receiving node or it must be sent to another node. If the message was destined for the receiving node, then the message will be given to a level 4 protocol such as the signaling connection control part (SCCP) or the ISDN user part (ISUP). The message routing function also accepts messages from level 4 and routes them to the proper destination. The link management function verifies the reliability of the link between adjacent nodes. It keeps track of errors and congestion. Status messages are sent to adjacent nodes on link failure or congestion. Notification will be sent on link failure or restored status and messages will be rerouted.

### 3.2.3 HSL (High Speed Signaling Link) SS7 over ATM

HSL replaces traditional SS7 with high speed and band efficient SS7 over ATM. HSL replaces SS7 MTP level-2 of the Message Transfer Part protocol. Its main functionality is to send the SS7 signaling packets in the form of ATM cells over T1/E1/J1 network. It is compromised of five sub-layers (figure 2) with each performing a different function.

Service Specific Coordination Function (SSCF) is used as a mapping function. It maps messages between MTP3 and SSCOP (Service Specific Connection Oriented Protocol). It is responsible of notifying MTP3 in case of link congestion and change in link status.

SSCOP is a connection-oriented protocol. It is responsible for error detection and reporting and maintaining data sequence integrity.

ATM Adaption Layer Common Part Convergence Sub-Layer (AAL5-CPCS) is responsible for providing the cell loss priority and calculating the CRC on the length of the frame. A frame can be 65535 bytes in length.

The AAL5 Segmentation and Re-Assembly ( AAL5-SAR ) sub-layer breaks the AAL5-CPCS frame into 48 byte octets for the send path and re-assembles 48 byte octets into AAL5-CPCS frame on the receive path. These 48 byte octets are added with a 5 byte header to construct the 53 byte octet ATM cell.

The ATM layer multiplexes and de-multiplexes cells based on Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI). The VPI/VCI together helps ATM nodes route the ATM cells to the desired destination. In HSL these ATM cells are carried over T1/E1/J1 interface.

3.2.4 SS7 Level 4 - Protocol and Application Parts

The Signaling Connection Control Part (SCCP) is a level 4 protocol that provides end-to-end routing. SCCP allows routing through the network without the need to know the individual addresses of each of the intermediate nodes. SCCP also provides subsystem addressing. SCCP provides the capability to address applications within a node. MTP uses the point code to access a signaling point, but it is not able to access the applications at the signaling point. Examples of subsystems are 800 call processing, calling-card processing, advanced intelligent network (AIN), and custom local-area signaling services (CLASS) services (e.g., repeat dialing and call return)[1]. The SCCP allows these subsystems to be addressed explicitly.

The Transaction Capabilities Application Part (TCAP) defines the messages and protocol used to communicate between subsystems in nodes. TCAP uses SCCP as its transport protocol so that it can address the subsystems. SCCP also provides fragmentation of messages. TCAP is used for database services such as calling card, 800, and AIN as well as switch-to-switch services including repeat dialing and call return [1]. TCAP is used by an SSP to query a SCP for routing information when the dial digits are 800 or 900 numbers.

ISDN User Part (ISUP) supports basic telephone call setup and disconnect between end offices. ISUP supports ISDN and intelligent networking functions. ISUP is also used to link the cellular network to

the PSTN.

INAP handles the communication between SSP and SCP. INAP uses TCAP to take care of multiplexing and connection management. It is used for 1-800 toll free services and for calling card services

## 3.3 SS7 Link Monitoring

The SS7 network was designed for a closed telecommunications community. The network did not need to provide authentication because it was difficult for any user to access the network directly. This changed when the Telecommunications act of 1996 was passed. The phone companies have to provide connections to the SS7 network for a fee. This created a need for monitoring applications such as network billing, quality of service, and security as telephone calls span more than one network.

### 3.3.1 Network Billing

With the SS7 network fragmented between carriers, billing has become more complex. By monitoring a link a carrier can check for loss of revenue due to errors, verifying the billing of other carriers, monitoring the minutes used for a link, and check the routing used. It is important for a carrier to verify that it is receiving revenue from other carriers using its network and to verify that there are not overcharges by other interconnected carriers. When an ATT customer calls a MCI customer, ATT and MCI would like to verify that the calls are connected and the correct revenue is generated. A monitor can verify that routes are used with the highest probability of a successful connection and that the cheapest route is used across networks increasing the profits for the carrier. By monitoring they can collect statistics on call setup and completion. Figure 3 shows points where a monitor is placed to retrieve the data.

The SSP is the entry point into the SS7 network. Anybody that can access the SSP can attack the SS7 network. If a malicious user can get access to the network through a SSP, they can forge phone numbers or charging related information. This will cause problems for the carriers in billing customers. It would also be possible to insert forged ISUP messages to the network and generate bills for someone else. Monitoring applications can perform real time call tracing or trouble shooting for off line play back. ISUP calls can be traced by calling number or called number when problems like this are detected.

SS7 Network Monitors

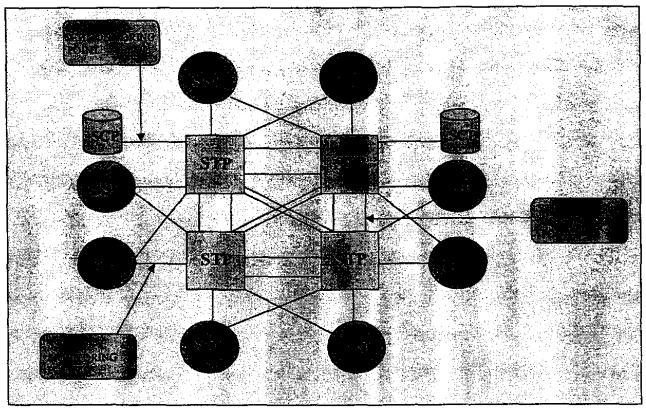



Figure 3

3.3.2 Quality of Service

One of the problems carriers face is a high turnover of customers. It is important that the carrier provide the highest quality of service. A higher call connection rate will result in higher billing minutes. Roaming and international calls generate the highest profits. These calls usually traverse multiple carriers and each carrier wants to ensure the call is not cut off. Calls that are cut off or have poor service will lead customers to switch to another carrier. The carrier can ensure good performance by monitoring the line and correcting problems before seen by the customer. It can also provide alarm generation when the performance hits a preset threshold.

Denial of service is another area of concern. This can happen when a SSP to STP connection is overloaded. Attackers can bring down a network by modifying messages and congesting nodes. A group of attackers can also flood the network by dialing the same 1-800 number. This will overload the connection between the STP and SCP. Monitors can detect when there is a sudden increase in network traffic and generate alarms and disable this number.

3.4 Security

SS7 was not designed for user authentication or for security. The network needs to be protected from fraud and attacks. The number of vulnerabilities in the network has increased as the number of new services

has grown. Attackers want access at the signaling points because this is where they can harm the network.

When attackers get access to an SSP they also have access to STP. One of the services provided in SS7 is called global title digits. These are a sequence of digits provided by the called party address that may be a dialed 1-800/888 number, calling card number, or mobile subscriber identification number. The STP provides global title translation (GTT). The originating signaling points do not need to know the destination point code or subsystem number. The STP maintains a database of destination point codes and subsystem numbers associated with specific services and destinations. The STP translates the global title digits to point codes at the SCCP layer. The point code is the desired SCP. If an attacker is able to get access to the point codes they can access the STP and SCP. With the point codes the attacker can modify the global translation database [2].

Another area of concern is a service provided called local number portability (LNP). LNP is a capability that will allow customers to keep the same telephone number as they change carriers. This requires carriers to pass information back and forth across different SS7 networks. This is a quality of service and a security concern. The call must be tracked across multiple carriers. If a carrier drops the call, it is loss of revenue. If the attacker can access the database, they can modify or erase these numbers.

Some of the databases the SCP has are for billing, toll free numbers, and voice mail. If a user can gain access to these databases they can create massive problems for the carriers. One of the databases at the SCP is the call management service database (CMSDB). The CMSDB processes toll free calls. Toll free calls are mapped to actual numbers. The CMSDB provides the information that routes the call and the billing information. If an attacker can gain access to this database they can avoid billing charges. TCAP messages are used to access and modify SCP databases. An attacker can modify a TCAP message and access a user's password and get access to their voice mail. They can also modify TCAP messages for call forwarding and get free calls [2].

There are vulnerabilities at the SSP, STP and SCP in the SS7 network. Monitoring can be set up at signaling points to try to detect attacks. Detection programs profile activity for the carrier which monitor known attack patterns and monitor abnormal activity. Automated triggering thresholds are used when problems are detected.

## 3.5 Radisys Solution

Monitoring the SS7 network should be non-intrusive. The send and receive path of each link can be monitored. Monitoring each side provides information on what the signaling link is transmitting and receiving. Each layer of the SS7 stack provides different functionality and each layer can be monitored. Figure 4 shows how a monitoring application may be deployed. The send and receive path are brought into a monitoring system. This enables the monitoring system to snoop on what was transmitted and received at a signaling link. This can be used for the applications like billing or security discussed in this paper.

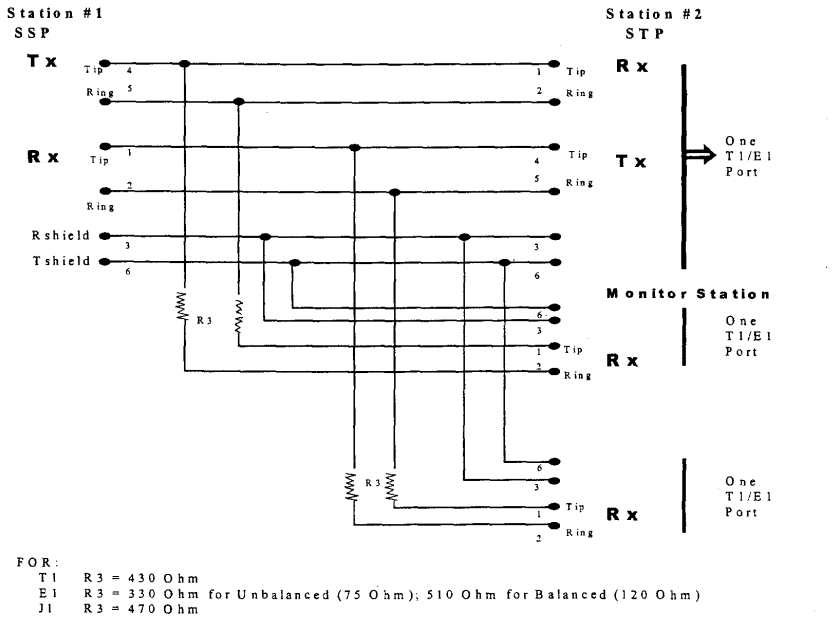



Figure 4

Radisys offers PCI and CompactPCI adapters with T1/E1 and V.35 interfaces that plug into a PCI/CompactPCI chassis under a variety of operating systems. The CompactPCI SS7 adapter is a single-slot, intelligent adapter that provides up to eight ports of 1.544Mbps (T1), 2.048Mbps (E1) or V.35 compatible interfaces perfectly suited for SS7 monitoring. This adapter has the capacity to monitor 128 T1/E1 channels, eight ports of V.35, or four ports of ATM HSL. A PCI SS7 adapter is also available that supports four ports of 1.544Mbps (T1), 2.048Mbps (E1) or V.35. This

adapter has the capacity to monitor 64 channels of T1/E1, four ports of V.35, or two ports of ATM HSL. A PCI Mezzanine Card (PMC) is connected to the adapter which provides the T1/E1 or V.35 interfaces. The T1/E1 PMC also offloads MTP1 and ATM processing. The Host operating system device driver support includes Windows NT 4.0, Windows 2000 and Sun Solaris for SPARC and Intel platforms (figure 5). SS7 monitoring applications will reside on the host.

In traditional SS7, Radisys provides extraction of MTP level 2 packets (figure 6). In HSL monitoring, Radisys provides the option of passive extraction of ATM AAL5 CPCS packets or ATM AAL5 SSCOP packets (figure 7). In both cases, APIs are provided so that higher layer applications can be used to scrutinize these packets for probable security breaches. Monitoring can reside at various points in the PTN network; between SSPs, between SSP and STP, between STPs, and between STP and SCP. Radisys provides a solid foundation for monitoring over which robust applications can be developed to make the SS7 network more secure and safe.

Radisys SS7 Monitor Solution

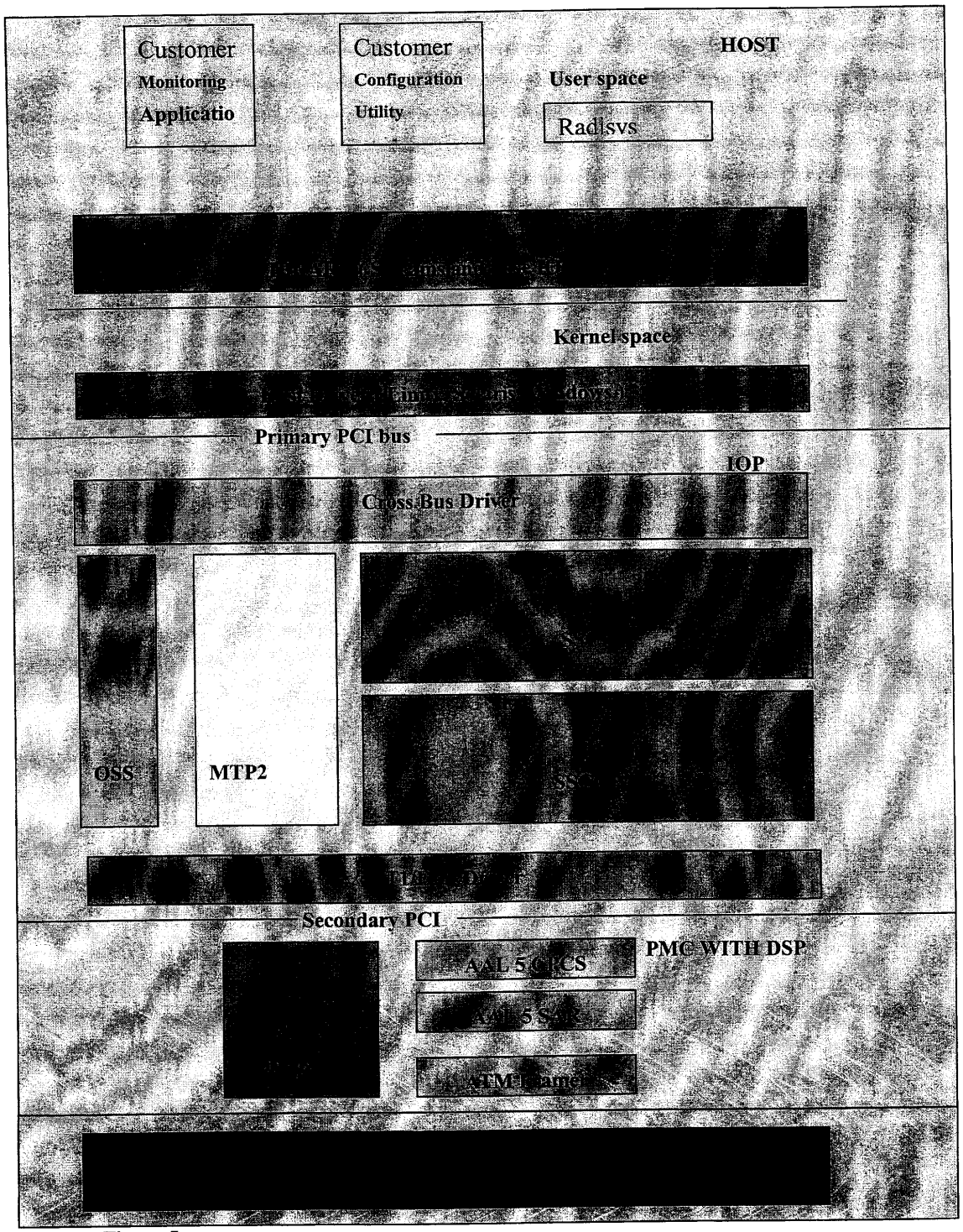



**Figure 5**

Traditional SS7 Monitoring

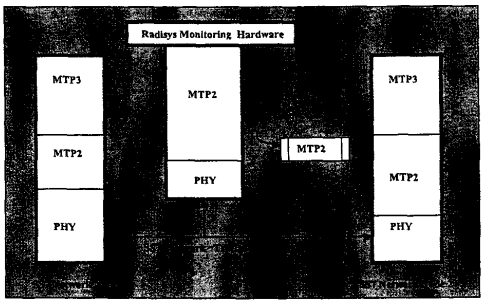



Figure 6

ATM Monitoring

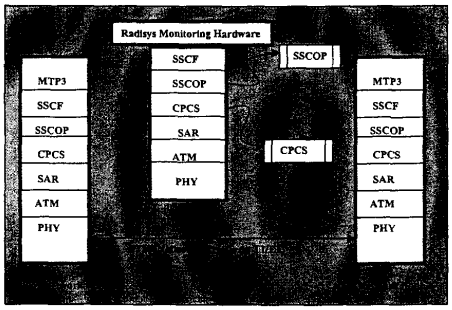



Figure 7

## 3.6 Summary

Every carrier wants to retain customers. They also want to protect their networks from fraud and attacks. By monitoring the network at the signaling points the carriers can detect poor call quality, billing problems, fraud and attacks. Monitoring the network is a non-intrusive method to gather information and protect the network.

# 4 The Role of SS7/IP Signaling Gateways in Today's Wireless Carrier Networks – SS7/IP in Wireless

Innovations in wireless telecommunications applications have been mirrored by correspondingdemands on the wireless telecommunications infrastructure. Nowhere has this impact been moreobvious than in the signaling network.

From early wireless signaling requirements for mobility to more sophisticated features such as Short Messaging Service, wireless networks place new demands on the signaling network. Carriers are faced with the choice of responding to these new demands quickly with new technologies or abandoning next-generation wireless networks altogether and, in the process, abandoning the subscribers and revenue that those networks bring.

This article discusses the role that SS7/IP signaling gateways play in today's wireless carrie networks, and how that differs from the original role conceived by the architects of the decomposed gateway model. It includes a brief overview of signaling gateway evolution and highlights the protocols used for communication between gateway elements. This article also outlines some of the specific SS7 signaling challenges presented by wireless networking and the solutions that signaling gateway technology offers. For example, it considers how the new traffic flows associated with wireless mobility can be supported by leveraging packet transport for SS7 through signaling gateway technology.

## 4.1 Introduction

At first glance, focusing on the role of SS7/IP signaling gateways in wireless networks may seem odd since SS7 is a core signaling protocol that does not interface with the last-mile connection. One might thus presume that SS7 is effectively unaware of whether a subscriber connects over wireline or wireless technology.

However, the rapid development of wireless-specific applications presents an entirely new set of requirements to the core signaling network. In essence, changes in the nature and scope of the services that providers offer to wireless subscribers today are demanding greater flexibility from the signaling network.

For instance, Short Messaging Service (SMS), an SS7-based application, was originally conceived as a paging equivalent, but SMS now supports applications from chat sessions to e-commerce.

Changes like this are redefining the performance and capacity requirements of the SS7 network and consequently redefining the role of the

SS7/IP signaling gateway in the wireless arena.

A synopsis of signaling gateway evolution helps explain how this technology came into being and offers a framework for summarizing the important functions that the SS7/IP gateway provides in the wireline network as a precursor to its more complex role in the wireless domain.

## 4.2 Evolution of the signaling Gateways

Initially, the SS7/IP gateways grew out of the voice over packet technology, which evolved in three stages. Its first incarnation was a composite gateway that integrated all functions within a single device. This gateway was essentially an enhanced Class 5 switch and suffered from similar limitations.

In this first stage of gateway evolution, a single device performed all functions associated with a traditional Class 5 switch.

The upper half of Figure 1 depicts a traditional end office Class 5 switch receiving signaling information from the SS7 network and voice trunks from the public switched telephone network (PSTN). The switch then sets up calls to users connected to local analog or digital loops. The composite gateway illustrated in the lower half of Figure 1 looks much the same. In this model, the gateway still connects to both the SS7 network and the voice trunks, but the connections to users are replaced by a packet transport, such as IP or ATM. In this configuration, the gateway could just as easily be a mobile switching center—terminating signaling (SS7) and bearer (voice) traffic, performing call control and signaling to wireless handsets, and forwarding packetized voice across the wireless network to users.

One key problem with this design is that the media gateway is burdened with performing all Class 5 switch functions and managing packet voice connections. The industry responded to this problem by separating the signaling and bearer traffic, in essence distributing the gateway into two components. This partially decomposed gateway leverages standards-based protocols for communication among the network devices.

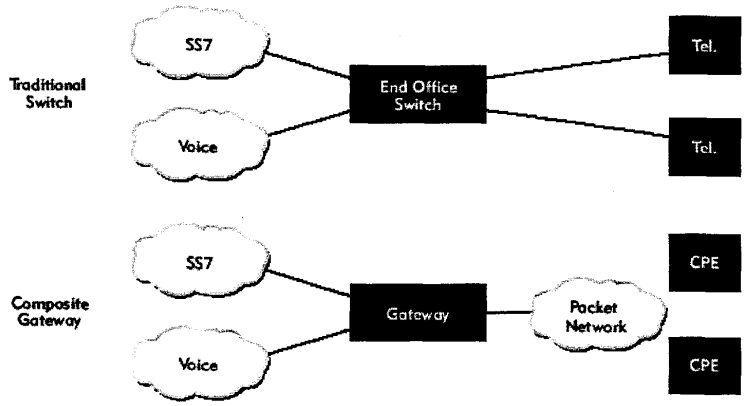



*Figure 1: Traditional switch v. composite gateway*

In the partially decomposed gateway model, the media gateway controller (MGC) handles SS7 traffic, receiving signaling information from the SS7 network and performing call control and supervision across the packet network (see Figure 2). In parallel, the media gateway carries bearer traffic between the circuit- and packet-switched networks, performing compression and decompression of the voice channels.

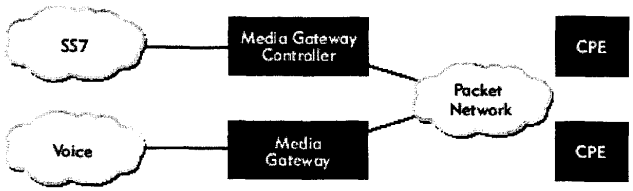



*Figure 2: Partially decomposed gateway model*

This architectural model still requires the MGC to perform two significant tasks: SS7 termination and call control. The complexities of SS7 can consume precious processing and memory resources on the controller, affecting its cost and scalability. As a result, supporting native SS7in the MGC can become problematic.

Thus, the next logical step in signaling gateway evolution involved segregating SS7 and call control processes and distributing them across the network.

In a fully decomposed gateway (see Figure 3), SS7 is uncoupled from the MGC. The MGC still performs call control, supervision and so forth and remains the administrative center of the softswitch architecture. However,

the SS7/IP signaling gateway now terminates lower-layer SS7—the SS7 Message Transfer Parts (MTPs)—and backhauls the upper layers of the SS7 protocol to the MGC over a packet transport.

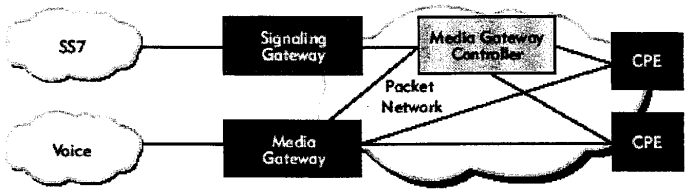



*Figure 3: Fully decomposed gateway model*

Note that Figure 3 oversimplifies the actual network design; the signaling gateway and the MGC aren't necessarily in a one-to-one relationship. In fact, one signaling gateway could interface with multiple MGCs, or multiple signaling gateways could interface with one MGC. The interactions of the signaling gateway with the SS7 network and the MGC depend on the protocol layer at which the signaling gateway performs its interworking functions.

## 4.3 Common Gateway Traffic Protocols

Specific protocols enable communication between the three elements of the decomposed gateway—bearer traffic, control traffic and signaling traffic. The protocols are outlined here primarily to dispel some of the misconceptions that have arisen around the next-generation network architecture, particularly among vendors who propose a single-protocol carrier network. As the next few paragraphs make clear, each protocol targets a specific network element. Thus, carrier networks typically must support multiple protocols throughout the network.

First, consider the bearer traffic protocols. As illustrated in Figure 3, the media gateway in a decomposed gateway model handles the bearer traffic, usually voice. The media gateway receives the voice trunks from the PSTN, then compresses and packetizes the voice and forwards it onto the packet network using one of several protocols. The most common protocols used in IP networks are Real-Time Transport Protocol (RTP) and Resource Reservation Protocol (RSVP). An ATM network is likely to use AAL1 or AAL2 to emulate voice circuits, or AAL5 if the voice traffic is carried over IP within ATM. The protocols common in a wireless network include TDMA, CDMA and GSM.

Regardless of the underlying transport medium, bearer traffic travels over paths that are separate from signaling traffic, and never interfaces directly with the signaling gateway. In other words, even if the signaling traffic and bearer traffic flow over the same physical links—for example, within a Frame Relay network or an ATM carrier backbone—the connections are logically independent. In fact, that independence is a fundamental tenet of the decomposed gateway model.

A second set of protocols relate to the media gateway controller. Note that this article distinguishes between the *control* protocols used by the MGC to control the media gateway and the customer premises equipment (CPE), and the *signaling* protocols used for SS7 interworking. Control protocols connect the MGC with the bearer traffic network, whereas signaling protocols connect the MGC to the SS7 network.

The most common control protocols in carrier networks today are ITU H.323 and the Media Gateway Control Protocol (MGCP) defined by the IETF. MGCP is the precursor to the ITU H.248/IETF Megaco specification, and it is more widely deployed than its successor at present, but carriers are migrating in increasing numbers to standards-based solutions. Thus, Megaco is gaining considerable traction and may eventually become an industry de facto standard. In recent years, Session Initiation Protocol (SIP) has also grown in popularity. The choice of control protocol is up to the carrier, significantly influenced by the specific protocols supported by the MGC, the media gateway and the customer premises equipment.

The third type of gateway traffic protocols—signaling protocols—are the most relevant to the focus of this article. As shown in Figure 3, native circuit-switched SS7 traffic is terminated by the signaling gateway, which then converts it to IP and sends the modified signaling traffic on to the MGC. This modified signaling stream is usually transported via Stream Control Transmission Protocol (SCTP), a peer protocol to TCP and UDP.

The upper-layer SS7 protocols, such as ISUP and TCAP, are usually passed through the signaling gateway without modification. With that in mind, consider the interworking function that the signaling gateway plays in a wireless network. Because of its mobility requirements, wireless technology has fostered the creation of a new suite of protocols, including ANSI-41 and GSM MAP. These mobility-specific protocols rely on the underlying ISUP and TCAP SS7 protocols that, in turn, rely on the SS7 Message Transfer Parts. Because the signaling gateway interworks the MTP layers, the wireless applications above remain essentially unaware of the

underlying transport, the gateway and which SS7 layer the gateway is interworking.

## 4.4 SS7/IP Interworking Protocols

Figure 4 compares two common SS7/IP interworking models, one operating at Layer 2 of the OSI seven-layer stack and the other operating at OSI Layer 3.

The arrows in the diagram indicate the location of SS7 Point Codes—essentially, the network addresses in the SS7 network. The specific type of SS7 signaling end points in the network is irrelevant to this discussion. More significant is the fact that the signaling devices at the right of the graphic are connected to IP, whereas those at the left are connected to a native SS7 circuit.

Before signaling gateways emerged, devices at either end of this connection linked directly to SS7 circuits, mandating separate SS7 interfaces on both devices for every SS7 link. In this model, however, the IP device converges multiple logical signaling links into one physical interface, for example, a 10/100Mbps Ethernet connection.

In both of the Figure 4 configurations, the signaling gateway interworks traditional, circuitswitched SS7 with packet-switched signaling. However, the two interworking models differ significantly. In the upper configuration, the Layer 2 signaling gateway translates between SS7 MTP2 at one end and M2UA over IP at the other. In this model, the higher-layer SS7 MTP3 messages are forwarded across the gateway between the two end points without modification. In fact, the signaling gateway is effectively invisible to the end points. Moreover, because the signaling gateway doesn't communicate at Layer 3, it doesn't present an SS7 Point Code and thus requires no reconfiguration within the SS7 signaling points on either side of the link. This plug-and-play simplicity makes Layer 2 interworking especially attractive.

The lower configuration, by contrast, shows a Layer 3 signaling gateway terminating MTP3 messages from the SS7 network and forwarding higher-layer protocols, such as ISUP, to the IP device. This Layer 3 configuration offers the advantage of offloading SS7 processing from the IP device, potentially enhancing performance. This approach also provides a single SS7 Point Code front-end to the IP device, enabling multiple IP elements to be "hidden" behind one Point Code.

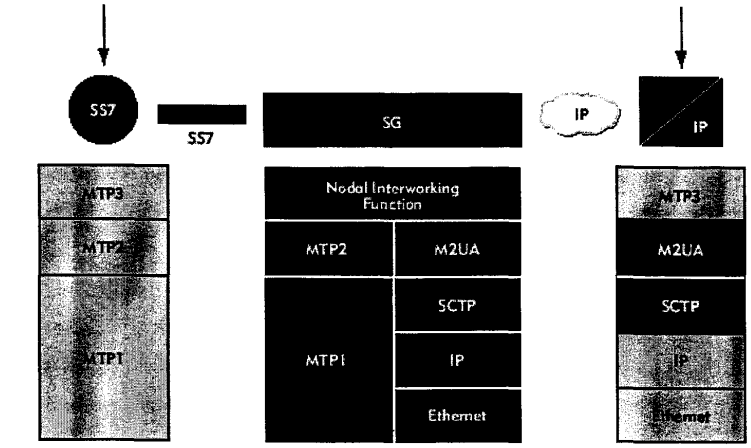
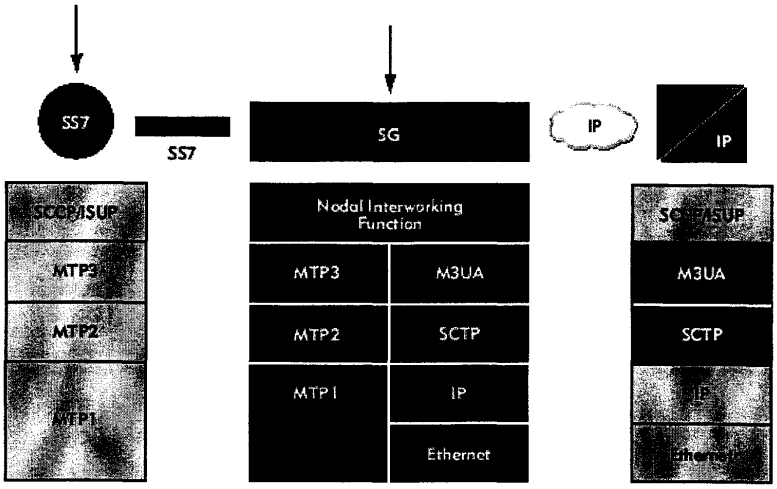



*Figure 4: Two SS7/IP interworking models*




This design conserves precious Point Codes and does away with repeated SS7 recertifications as devices evolve. At the same time, this design fundamentally alters the network topology by moving the Point Code onto the signaling gateway, resulting in a more obtrusive approach than a Layer 2 configuration.

Clearly, both approaches offer immediate benefits, and carriers can choose different solutions based on their particular needs.

Another interworking option is an innovative technology called SS7/IP

Tunneling. Unlike earlier examples, in which only one signaling device was attached to the SS7 circuit network, Figure 5 depicts a network in which both SS7 signaling end points connect to the SS7 network. This is one way that traditional, legacy SS7 signaling points can connect across the next-generation packet-switched network without modification to the SS7 interfaces. It offers a compelling migration path by allowing carriers to install and validate IP transport for SS7 without wholesale equipment changes.

In an SS7/IP Tunneling configuration, a pair of signaling gateways forms a virtual tunnel for carrying SS7 traffic across an intervening packet network. Because the gateways don't represent a Point Code, they can provide transparent transport of MTP3 messages between the two SS7 signaling end points. The end points are unaware of the gateways, and the network operator makes no changes to them when the gateways are added. This approach offers some important advantages in wireless networks, which will be outlined later in this article.

4.5 Wireless Signaling challenges

The SS7/IP signaling gateway that has evolved in the wireline network also has implications for carriers operating in the wireless arena. To understand how various SS7/IP interworking options might spell solutions, consider three of the most significant key wireless signaling challenges that carriers face today.

One important challenge involves migrating the latest next-generation wireless systems to packet signaling networks while maintaining connectivity to the PSTN. Economic pressures, coupled with rapid technological evolution in the wireless arena, have fostered widespread interest in packet-switched signaling. However, wireless carriers must continue to provide access to PSTN legacy systems to ensure market share.

Another serious wireless challenge involves network performance, particularly in the areas of scalability and reliability. Wireless carriers are encountering rapidly increasing call volumes, more sophisticated TCAP transactions and call hand-offs, as well as greater fluctuations in call volumes as users move between systems and switching centers. Packet technology provides an ideal method for supporting these call volumes economically.

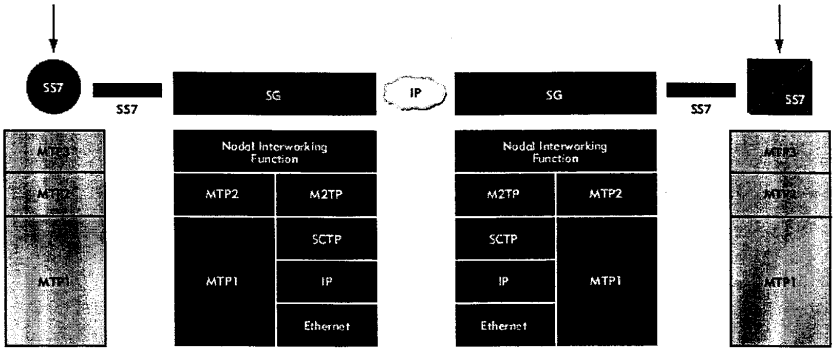



*Figure 5: SS7/IP Tunneling configuration*

Wireless carriers also face the problem of SMS transactions causing congestion in the signaling network. Of particular concern is the impact that SMS traffic volumes have on high revenuegenerating, time-sensitive voice call signaling. Wireless providers who offer SMS services must ensure the continued performance of voice networks, even as they add new services and protocols.

The following sections explain how SS7/IP gateways can address these wireless signaling challenges.

## 4.6 Resolving SS7-to-IP Interworking in Wireless Environments

SS7/IP signaling gateways can enhance wireless carrier networks by providing SS7-to-IP interworking, thus enabling wireless carriers to capitalize on the latest signaling platforms with native packet interfaces. Wireless applications and platforms are evolving far more quickly than their wireline counterparts and, with less legacy infrastructure to support, interest is mounting in providing native packet interfaces to the signaling equipment. SS7/IP gateways facilitate the deployment of these next-generation network platforms and new wireless services.

At the same time, the carrier network often includes some wireline signaling equipment or at least connectivity to SS7 in the PSTN. SS7/IP gateways are specifically designed to connect legacy circuit-switched SS7 and packet-switched signaling. Thus, they enable wireless carriers to migrate SS7-connected equipment to IP connectivity incrementally, all the while maintaining PSTN connectivity.

Figure 6 depicts a wireless carrier with mobile switching centers (MSCs), a home location register (HLR) and a visitor location register (VLR) connected to circuit-switched SS7. This carrier is also beginning to

deploy next-generation application servers on the packet network, and is simultaneously migrating existing Service Control Points (SCPs) to the packet network. SS7/IP gateway technology provides the needed connectivity between elements on the packet network, the internal SS7 circuit network and the PSTN.

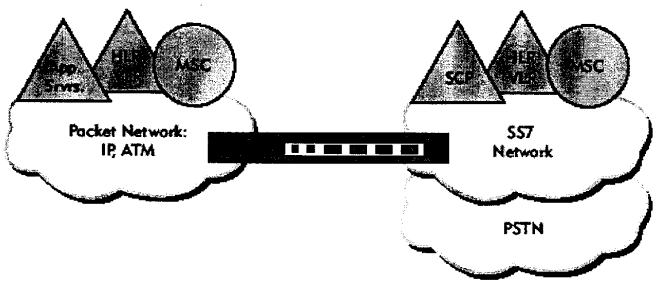



*Figure 6: SS7/IP gateway technology connects diverse network elements*

Moreover, migrating wireless signaling points from SS7 to the packet network enables multiple signaling elements to share a single SS7 Point Code, a model that facilitates growth and evolution of the network infrastructure by making repeated SS7 recertification and Point Code assignments unnecessary. This Point Code advantage, originally conceived for the wireline network, can potentially deliver even greater benefits in the rapidly-evolving wireless arena.

## 4.7 Addressing Wireless Carrier Performance Issues

Signaling gateways can also solve the problem of wireless carrier performance, particularly in the area of network scalability. The rapid growth that wireless carriers are seeing today—in both the number of subscribers and the depth of features they demand—is generating dramatic increases in the quantity of SS7 traffic that the network must support. Moreover, wireless mobility translates into dramatic swings in subscriber utilization, making over-subscription predictions more challenging.

As an example, the circuit-switched SS7 network at the left of Figure 7 suffers from limitations associated with fixed bandwidth circuits. The mesh network opposite it, by contrast, provides a statistical multiplexing of all the traffic across a single packet-switched core. This model takes advantage of the SS7/IP Tunneling technology mentioned earlier, in which native SS7 devices connect to an SS7/IP gateway that transparently tunnels the SS7

traffic across the packet core. This approach leverages the cost and performance benefits of meshed, packet-switched, nextgeneration signaling.

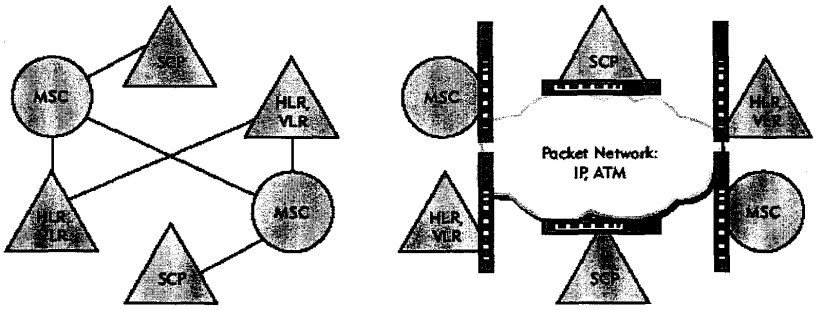



*Figure 7: Replacing a circuit network with a packet-switched core enhances performance*

Many carriers achieve the same result by simply IP-enabling the SS7 signaling end points in the network. However, wireless networks today are growing far more rapidly than IP signaling technologies can evolve. SS7/IP Tunneling offers carriers an appealing migration tactic, allowing them to take advantage of a packet transport while phasing in native IP signaling connectivity. Moreover, the advantages of such a packet-switched approach rise dramatically as the network grows and the number of SS7 signaling end points increases.

SS7/IP signaling gateways also provide a corollary performance benefit in the area of network reliability. Although subscribers seem remarkably forgiving about dropped calls and lack of service in certain geographic locations, carriers are unforgiving when it comes to signaling network performance. Carriers demand reliability equivalent to that of the PSTN—insisting on at least 99.999 percent reliability.

As illustrated at the left of Figure 8, the public SS7 network relies on sophisticated processing within the SS7 stacks in the end points to reconverge around network failures. This was an ideal approach years ago when there were no data networks to leverage and circuit reliability was poor. Today, however, many carriers enjoy high-quality fiber-optic connections coupled with high-bandwidth long-haul data connections that parallel the reliability features inherent in SS7. Consequently, carriers hope to capitalize on the latest packet-switching reconvergence technologies to provide equivalent functionality in the next-generation network.

In Figure 8, the model on the right is based on an existing meshed, packet-switched data network that enables multiple parallel paths through the network. This significantly increases aggregate end-to-end bandwidth

by statistically multiplexing traffic over multiple parallel connections dynamically in response to network resource utilization. Moreover, IP routing provides inherent fail-over capabilities through protocols such as OSPF and HSRP. In addition, any mis-sequencing or packet loss in signaling traffic is corrected by SCTP. This results in a highly reliable system for signaling message delivery in the packet network.

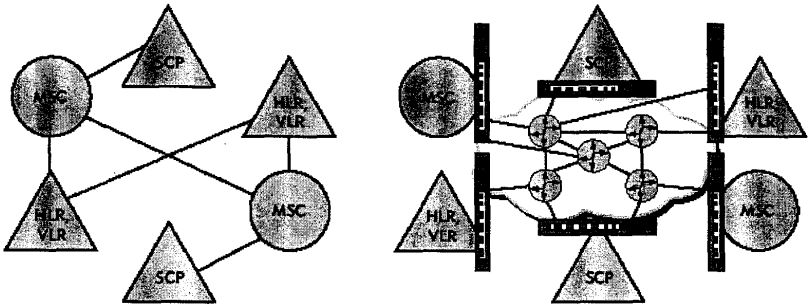



*Figure 8: SS7 technology provides reliability for circuit switching; IP technology provides reliability for packet switching*

One drawback of this approach is the potential for increased and unpredictable latency often associated with packet switching. Thus, this solution is predicated on good packet network design, including the number of network paths available, the number of hops in each path, the router protocols in use and the bandwidth at each hop.

## 4.8 Using SS7/IP Signaling Gateways to Divert SMS Traffic

SMS was initially designed to provide simple notifications to wireless handsets for voice mail or short text messages. However, SMS has evolved into a virtual data transfer service, supporting everything from on-line ticket purchases to gambling, chat sessions, gaming and stop-smoking messages. The result is that SS7 circuits are becoming clogged with traffic that does not require the stringent performance targets of the public SS7 network. Carriers, driven by market forces to support SMS, are looking to SS7/IP signaling gateways to divert these high volumes of SMS traffic onto packet networks.

Figure 9 depicts a possible implementation of the SMS offload concept. In this scenario, two signaling gateways detect SMS traffic from the wireless devices (indicated by the yellow triangles) and divert it away from the SS7 network onto a separate packet-switched network. As an alternate migration strategy, one could even direct SMS traffic onto a separate digital

circuit.

Although this design resembles other SS7/IP gateway solutions, it relies on the segregation ofSMS from other SS7 services, transparently or through reconfiguration of the switching systems. However, in this network configuration, some SS7 traffic is forwarded to the SS7 network while the SMS traffic is sent to another network. Thus, unlike SS7/IP Tunneling, this SMS offload design provides for at least three logical interfaces on the gateway: one for the wireless network connection where the SMS devices are located, one for the public SS7 network and one for the packet-switched offload network.

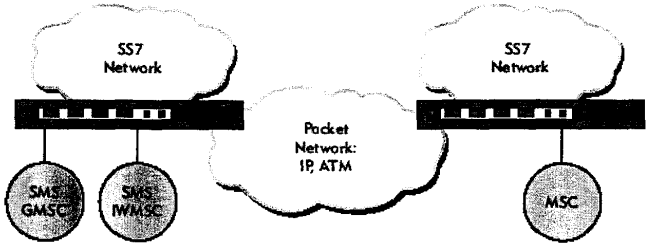



*Figure 9: SS7/IP gateways relieve the SS7 network of heavy SMS traffic loads*

## 4.9 Conclusion

Although SS7/IP interworking was originally designed for wireline networks, this technology also facilitates the evolution of today's emerging wireless applications. As wireless carriers deploy infrastructure to support next-generation applications, they can take advantage of SS7/IP signaling gateway technology in several ways, from simple access between the wireless network and the PSTN, to long-haul circuit replacement, to sophisticated SMS off-load.

New applications for gateway technology will continue to emerge; however, all are founded upon the core function of connecting existing circuit-switched SS7 signaling to packet-switched signaling with minimal effort and optimal performance.

Signaling gateway vendors such as RadiSys offer a variety of technologies that can deliver this functionality, from traditional SS7/IP protocol and signaling termination to SS7/IP Tunneling with SMS offload. These and other solutions enable wireless carriers to deliver services more quickly and affordably than is possible with legacy signaling architectures.

## 5 心得

本次赴美國 Radisys 公司實習 SS7 信號網路管理及監控，得到以下心得：

1. 以目前 SS7 信號網路發展的走向，由於 IP 網路普及，SS7 信號網路逐漸由原來的使用交換機實體線路連結，改爲經由 IP 網路彼此連結，而 IP 網路的安全性是必須要納入考慮。
2. 第三代通信網路勢必繼續沿用 SS7 信號網路作爲通信架構，附加的額外服務也會不斷增加，對於中華電信龐大的通信網路來說，維護 SS7 信號網路的完整性也就相對的重要，故應該對於 SS7 提供的服務及規約，應做詳細了解，以建立自主性的技術分析。
3. 針對有的 SS7 信號網路，應針對不同系統介接的技術部分多加研究，以因應未來多元化的通信設備及加值服務。

## 6 Reference

[1]IEC : Signaling System 7.
<http://www.iec.org/online/tutorials/ss7/topic09.html>

[2] G. Lorenz, et al. Securing SS7 Telecommunications Networks, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June 2001.

[3] T. Russell, Signaling System #7, McGraw-Hill, New York, 1995.