OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM
TECHNICAL
NOTES

MARCH 2001 | *TECHNOLOGY AND PROGRAMS DIVISION* | VOLUME 8, NUMBER 2

Signaling System 7 Internet Protocol Interconnection

by Gabriel Martinez

What Is SS7?

Common Channel Signaling System Number 7 (SS7) is the signaling control system for the public switched network (PSN) in the United States and much of the world. In the PSN, both voice and data traffic are carried on switched circuits. However, SS7 sets up and manages telephone calls, and exchanges data and messages, via a network that is separate from the network that voice and data calls travel over. SS7 data is transferred between network elements using bidirectional channels known as signaling links.

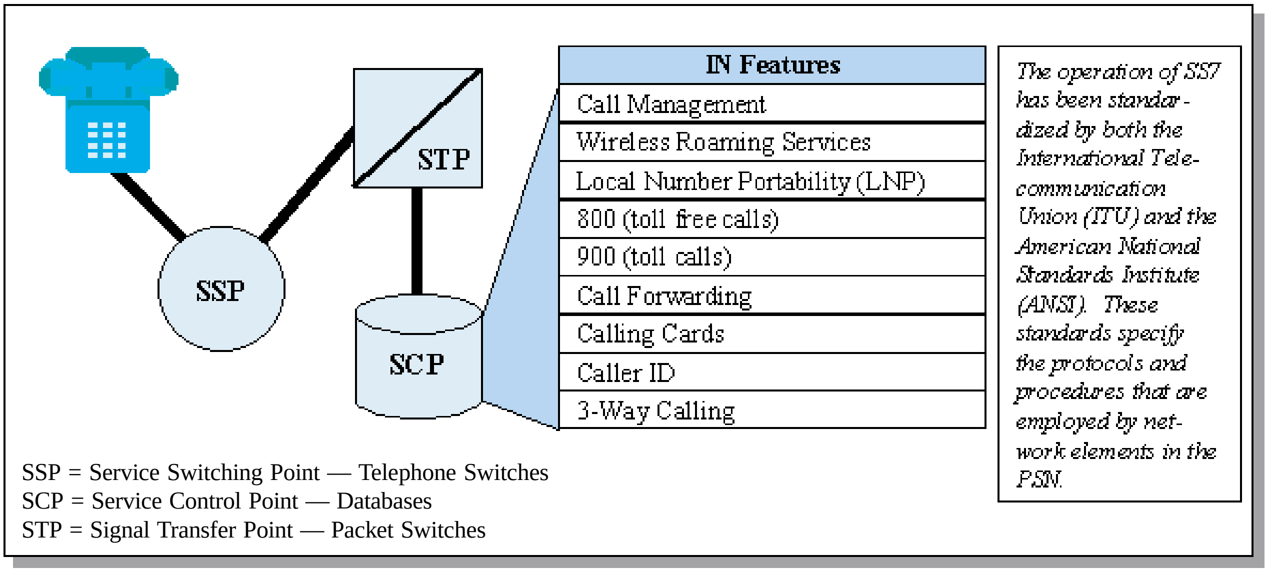
The SS7 architecture consists of a high-speed, packet switched network. This network is connected by three types of signaling links: Service Switching Points (SSP), Signal Transfer Points (STP), and Service Control Points (SCP). These signaling points are also known as SS7 nodes.

Perhaps the most important characteristic of SS7 is that signaling occurs out-of-band on dedicated channels rather than in-band on voice channels, thereby providing an extremely high degree of security and reliability for SS7. In contrast to in-band signaling, out-of-band signaling delivers faster call setups, more efficient utilization of voice circuits, enhanced network fraud controls, and support of Intelligent Network (IN) services.

IN provides many of the services that telephone users encounter daily. IN features, such as setting up and managing call connections, local number portability (LNP), call forwarding, and toll free calls, use SS7 to access the IN databases. Figure 1 illustrates the SS7-IN relationship.

Dedicated Circuits

The switched circuits of the PSN are dedicated connections for the end users. This connection ensures that a dedicated amount of bandwidth is available to end users for the duration of a call. As call requests increase, users are more likely to receive a busy signal. However, in most cases this will be extremely rare, because the availability of dial tone is engineered to 99 percent during the busy hour. In addition, once users are connected, they will receive consistently high performance levels.



SSP = Service Switching Point — Telephone Switches
SCP = Service Control Point — Databases
STP = Signal Transfer Point — Packet Switches

The operation of SS7 has been standardized by both the International Telecommunication Union (ITU) and the American National Standards Institute (ANSI). These standards specify the protocols and procedures that are employed by network elements in the PSN.

Figure 1. Simplified SS7-IN Relationship

In contrast, other networks such as cable networks, local area networks (LAN), or Internet Protocol (IP) networks allow an unlimited number of users (theoretically) to access the bandwidth, but each additional user means a decreasing amount of bandwidth per user.

Why Interconnect to SS7?

The use of data networks to transfer real time voice calls using techniques such as Voice over IP (VoIP), is leading to increased demand for access to IN services. While that means interconnecting SS7 with the Internet today, it will likely lead to interconnecting SS7 with other data networks in the future. Until now, security concerns have limited access to SS7. However, some of these concerns appear to be abating. IN features have already been extended to wireless networks. Now, competitive local exchange carriers (CLEC) and Internet service providers (ISP) are requesting similar access to SS7 based on the provisions of the Telecommunications Act of 1996. Some Internet telephony providers may seek to offer IN services such as LNP and toll free calling on VoIP calls.

SS7 offers high levels of stability and reliability but lacks ease of connectivity. Data networks offer easy connectivity but may lack stability. Interconnectivity may benefit both — giving increased access to SS7 and greater reliability to data networks — or it may introduce new stability issues into SS7 and put tighter restrictions on the interconnectivity of data networks.

A PSN-Internet interconnect will require interoperability between SS7 and IP. Before this can happen, agreement must be reached among the various PSN and Internet participants on how best to interconnect the networks in an efficient and secure manner. To this end, several forums are investigating the issue of network connections, protocols, and security, including: International Telecommunication Union (ITU), Internet Engineering Task Force (IETF), and Network Interconnection Interoperability Forum (NIIF).

SS7-IP Protocols

To connect or bridge IP-based networks to the PSN infrastructure, at least four standards have emerged: H.323, SIP, MGCP, and Megaco.

H.323* is a standard developed by the Telecommunication Standardization Sector of the ITU (ITU-T). The ITU is an international organization within which governments and the private sector coordinate global telecom networks and services. H.323 is also known as the ITU-T Standard for *Packet-Based Multimedia Communication Systems*. H.323 began as a set of standards for broadband voice and video services. It defines a multimedia communications system over packet-switched networks.

Session Initiation Protocol, or SIP, is a standard developed by IETF. IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. SIP is a signaling protocol for Internet conferencing, telephony, presence, events notification, and instant messaging. SIP was developed within the IETF MMUSIC (Multiparty Multimedia Session Control) working group, with work proceeding since September 1999 in the SIP working group. SIP is favored by companies developing IP-based phones. This application layer control protocol has a more flexible platform than H.323. However, SIP and H.323 support many of the same functions.

MGCP, also developed by the IETF, enables external control and management of data communications equipment at media gateways (MG). It is expected to eventually complement existing protocols. Megaco, developed jointly by the ITU-T and the IETF, was recently adopted by the ITU-T as H.248 and by the IETF as the Megaco protocol. In Megaco, media gateway controllers (MGC) will control MGs using H.248, however MGCs will communicate with each other via H.323 and SIP. Therefore, it is considered by proponents as complementary to H.323 and SIP.

Each protocol has advantages and disadvantages. Carriers and vendors will likely choose the protocol that is most advantageous to their needs. Because it is unlikely that a consensus will be made on a single protocol, H.323, SIP, MGCP, and Megaco are all expected to exist simultaneously in the IP network. Figure 2 (page 4) illustrates the SS7-IP relationship.

These protocols vary in levels of security. Some security enhancements have been offered, such as Transport Layer Protocol (TLP), Internet Protocol Security (IPSEC), and encryption; however, no definitive rules or standards are in place for service providers to follow. The Office of the Manager, National Communications System (OMNCS), is working with the Laboratory for Telecommunications Sciences to fully understand these issues.

NIIF

The NIIF was established as a voluntary open forum (it is sponsored by the Alliance for Telecommunications Industry Solutions [ATIS]). The NIIF encourages the discussion and resolution of industrywide issues associated with telecommunications network interconnection and interoperability that involve: network architecture; network management; and testing and operations. The NIIF is designed to facilitate the sharing of data concerning these topics.

Among the topics that the NIIF has investigated is the issue of abnormal SS7 network operations resulting from the interconnection of external networks with an SS7 gateway. The NIIF believed that the existing ANSI gateway specifications were insufficient. Furthermore, the NIIF wanted to ensure that

The “H” indicates that the standard is within the Audiovisual and Multimedia Systems Series of Recommendations, the “323” indicates that this is the 323rd standard considered under the H Series.

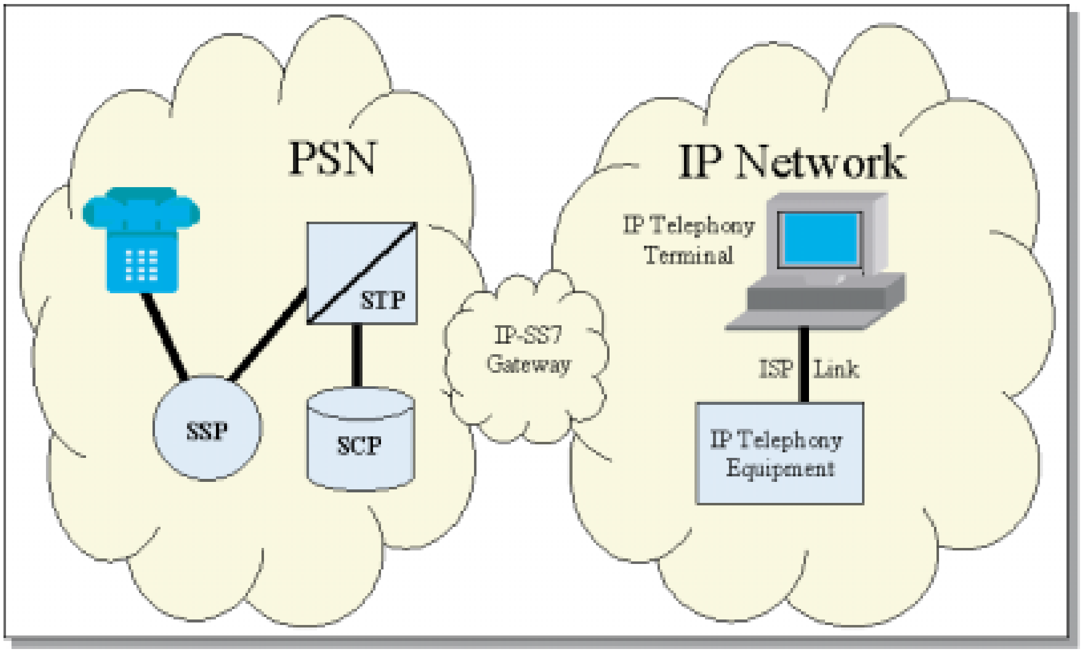


Figure 2. Simplified SS7-IP Relationship

service provider networks would be protected from internetwork propagation of bad SS7 messages, sabotage, and / or congestion whenever possible. The NIIF requested that telecommunications equipment vendors and ISPs provide recommendations for verifying SS7 gateway screening functionality. Based on this input, the NIIF enhanced its existing Reference Document (Part III, Section 9) to include a new section on SS7 interconnectivity reliability and security (see Box 1, page 5). The intention was to help resolve the issue of verifying intercarrier security beyond the ANSI specifications.

Internetworking Issues

To facilitate call setup and call handling between the PSN and the Internet, SS7-IP gateways are used. Two concerns exist with these new connections. The first concern is that the race to bring SS7-IP gateways to market leaves little time to thoroughly test equipment. The testing process for SS7 equipment is estimated to require at least 6 months. However, some vendors are selling SS7 gateways after only 4 to 6 months of development and testing. Without rigorous testing, systems connected with these gateways face increased risks from network interoperability issues and system failures as a result of overloads. However, many companies are willing to face these risks in order to be first to market with new equipment and services.

The second concern with implementing SS7-IP gateways stems from allowing an open IP network (such as the Internet) to have access to SS7. Previously, SS7 was a closed network protected by physical barriers. However, with the introduction of new gateways, SS7 could become more vulnerable via Internet access. This vulnerability raises potentially serious security problems. If intruders were to gain access to the SS7 network, they could adversely affect the operation of switches across multiple networks. An intruder could also attempt to disrupt the various network elements required to process a call. Other risks include injecting false messages or initiating a network attack. Note also that many of these problems could be introduced accidentally via bad coding or other unintended actions. Carriers are greatly concerned

> *SS7 network providers are responsible for ensuring the reliability and security of their own SS7 networks with respect to defending against the propagation of abnormal SS7 signaling messages when interconnected with other networks. This responsibility should ensure protection against unexpected SS7 messages, SS7 messages with protocol errors, attempts at sabotage, or any other harmful conditions that may be propagated across interconnected SS7 networks.*
>
> *Note that SS7 network intermediate nodes generally examine those parts of incoming messages with respect to message routing. The SS7 destination node examines additional information for proper message processing, and this effort may include additional security considerations. Examination of the content of every message is not done routinely, and may not be practical. Various methods of protocol analyzation that further examine message content are available to detect and resolve troubles, but those methods are used only on an exception basis.*
>
> *A variety of processes and responsibilities intended to ensure reliability, network security, and risk minimization associated with SS7 network interconnection are outlined elsewhere in this document (i.e., NIIF Reference Document).*

Box 1. Modified Part III, Section 9,
NIIF Reference Document

with these threats to their infrastructure. To address these issues, carriers are expected to use high levels of IP security to protect their portions of the SS7 network.

Future Interconnections

What does the future hold for the internetworking of SS7 with other networks? Using the interconnection of SS7 and IP as a baseline demonstrates the need for concerted efforts to guide future interconnections. Developing secure, uniform protocols for network interconnection and convincing developers, vendors, carriers, and ISPs to use them is key.

Conclusions

Because of a rush to market and the short product cycles for new interconnection products, security for SS7 interconnected networks is not well understood and will rely heavily on security measures implemented by carriers. The OMNCS continues to work with carriers and standards bodies to enhance the security of the SS7 interconnected network through participation in and review of the standards development process.

References

1. “Internet/PN Interconnectivity and Vulnerability Report,” Booz·Allen & Hamilton, January 1999.

2. “Issue #0094: Gateway Screening for Reliability,” NIIF, April 28, 1999.

3. Sean Buckley, “IP Telephony: An Insider’s War,” *Telecommunications*, July 2000, p. 33.

4. “Next Generation, Voice Over Packet, and Hybrid Networks Security Issues,” Telcordia Technologies, July 2000.

5. Gary Ragsdale, Gerard Lynch, and Michael Raschke, “The Convergence of Signaling System 7 and Voice-over-IP,” Southwest Research Institute, September 2000.

6. NIFF Reference Document, Version 2.3, ATIS, February 2000.

For further information about SS7 Interconnection, please contact:

Gabriel Martinez
National Communications System
Technology and Programs Division (N2)
701 South Court House Road
Arlington, VA 22204-2198
(703) 607-6200