Cellular Networking Perspectives

Editor: David Crowe • Email: David.Crowe@cnp-wireless.com Vol. 10, No. 10 October, 2001

In This Issue...

Next Issue: November 1st, 2001

Terrorist Attacks

To support the families of emergency workers killed in the September 11, 2001 terrorist attacks on the World Trade Center and Pentagon, we have made a donation, via NENA (www.nena9-1-1.org), to the International Association of Fire Firefighters and the New York Fraternal Order of Police. We encourage our readers to make donations to this or other charities that are assisting with families of the victims.

Circumnavigating SS7, Part I: Overview

This month, we are publishing the first in a series describing the various layers of the SS7 protocol, currently the nervous system of modern telecommunications system around the world.

SS7 is a suite of signaling standards – protocols that send control messages between elements of the telecommunications network. Most of the SS7 signaling is for managing circuits and calls, monitoring and managing the network and querying telecommunications databases. SS7 is not optimized for user data transmission, although it is used for sending wireless short messages and other small- to medium-sized packets of user data.

Earlier Signaling Systems

Before SS7, most signaling protocols were in-band, tone-based signaling (e.g. MF, R2), often erroneously referred to as analog signaling. Because these systems transmit tones over the voice facility (in-band), signaling during a call is difficult. And, because each tone is lengthy in duration (about 50-100 milliseconds for MF), they must be followed by a period of silence of about the same duration, and signals often have to be regenerated at intermediate switches. Consequently, signaling throughput is quite low. MF signaling, optimistically, has a throughput of 200 bits/second. Other tone-based signaling protocols, such as R2 used outside North America, are even slower, because they also require acknowledgement signals. SS7, by comparison, is a common-channel protocol (signaling is sent only on dedicated (common) links) and is many times faster than any tone-based signaling system, even considering that one common channel signaling link serves the signaling needs of several trunks.

Data Rates

When SS7 was first developed in the 1980's, it would have been described as a high speed protocol – blindingly fast as compared to older tone-based protocols. But its reliance on 56 or 64kbps (DS0) links now makes it seem like a low-speed protocol. The use of 1.536 Mbps (T1) link speeds has been standardized, but there are significant compatibility hurdles to be overcome before it is actually implemented. Multiple signaling links can be used, but this solution is costly, and is limited to 16 links in a link set to access the network, and 8 links in a link set internally.

Cellular Networking Perspectives (issn 1195-3233) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Crescent NW, Calgary AB, T2N 3W1, Canada. **Phone:** 1-800-633-5514 (+1-403-274-4749) **Fax:** +1-403-289-6658 **Email:** cnpsales@cnp-wireless.com **Web:** www.cnp-wireless.com.
Subscriptions: CDN$350 in Canada (incl. GST), US$350 in the USA and US$400 elsewhere. Payment by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery**: Email or 1st class mail.
Back Issues: Single issues are $40 in the US and Canada and $45 elsewhere, or in bulk at reduced rates.
Discounts: Educational and small businesses: 25% off any order. **Copies**: Each subscriber is licensed to make up to 10 copies of each issue or back issue. Please call for rates to allow more copies.

Packet Size

SS7 is limited to fairly small packets of data – around 250 bytes at most – unless high speed links are used, in which case the limit is about 3,000 bytes.

The exact size of packets that can be transmitted by an application is hard to determine exactly, as it varies with the amount of data in the underlying SS7 protocol layers (MTP and SCCP).

Segmentation of large messages is possible (i.e. splitting one message across multiple packets), but before it can be used with any reliability, newer versions of SS7 must be implemented.

Signaling Mode

SS7 is mainly used in a connectionless mode. A packet can be transmitted between any two points on the network without first establishing a connection (often also known as an association or virtual circuit). This characteristic is most useful on wireless networks, where one network element (e.g. MSC) may have to communicate with hundreds of others (e.g. HLRs for all roamers currently present in a network).

Addressing

The native address for SS7 is the Signaling Point Code (SPC or PC), a binary number (14-24 bits long) that uniquely defines a signaling point on a national signaling network. The same point code may be used in several different countries to identify different points.

Global titles are telephony digit strings, such as International Mobile Subscriber Identities (IMSI), phone numbers (in E.164 or national format) and calling card numbers that identify a network element (such as an HLR) through a numeric prefix. They can be used as secondary addresses (eventually mapping onto a point code). Global titles are often international numbers, and constitute the primary mechanism for addressing messages being transmitted between national networks.

International Signaling

SS7 is, in theory, an international protocol, but in practice, it is a family of similar, but ultimately incompatible, national protocols. This makes direct communications between national SS7 networks impossible. Most importantly, the point code is nationally assigned, making the basic addressing mode inapplicable for international signaling.

International communications either requires the use of international gateways, which requires the use of global title addressing, or more kludgy solutions such as extending one national SS7 network into another country's network to allow point code routing.

SS7 Network Elements

SCP

Service Control Point. An SP connected only by signaling links and not voice trunks. Examples are HLR, AC and MC.

SP

Signaling Point. An element that generates, receives or routes SS7 network traffic: SCP, SSP or STP.

SSP

Service Switching Point. An SP that provides both switching and signaling functions (e.g. MSC).

STP

Signal Transfer Point. An SP that routes SS7 packets. Configured in redundant 'mated' pairs.

Robustness

Robustness and reliability are some of SS7's greatest strengths. STPs (Signal Transfer Points - packet switches) are redundant, with independent signaling links. This means that any failure of a single link or STP can be counteracted by rerouting messages. It is unlikely that even multiple failures will make it impossible to communicate between two signaling points.

Load Sharing

Signaling data can be re-routed in SS7 not only to avoid link and node failures, but also to share the load between network elements. Traffic can be pseudo-randomly assigned to links to ensure that all signaling points carry a similar load. For example, an HLR could be provisioned in a 2+1 architecture, where three physical devices carry a load engineered for two. The load will normally be shared among the three, but when one device is unavailable due to a failure, software upgrade or other condition, traffic can still be handled by sharing it between the remaining two.

Network Architecture

Nodes that generate, receive or route SS7 traffic are known as Signaling Points (SP) which are classified as SCP, SSP or STP (see sidebar).

SPs are connected by links or link sets (groups of links between the same two SPs). A and E link sets may contain up to 16 links, others only up to 8.
Figure 1 shows how SPs are connected.

Links are classified by their position in the network. The single letter link identifiers, and the somewhat artificial names associated with them, are:

A. Access Links. Used to connect an SSP or SCP (e.g. MSC, HLR) to each of a mated pair of STP's.

B. Bridge Links. Used to connect pairs of STP's within the primary (internal) level of the network. Four links are required to connect a pair of mated pairs of STPs. This is known as a Quad.

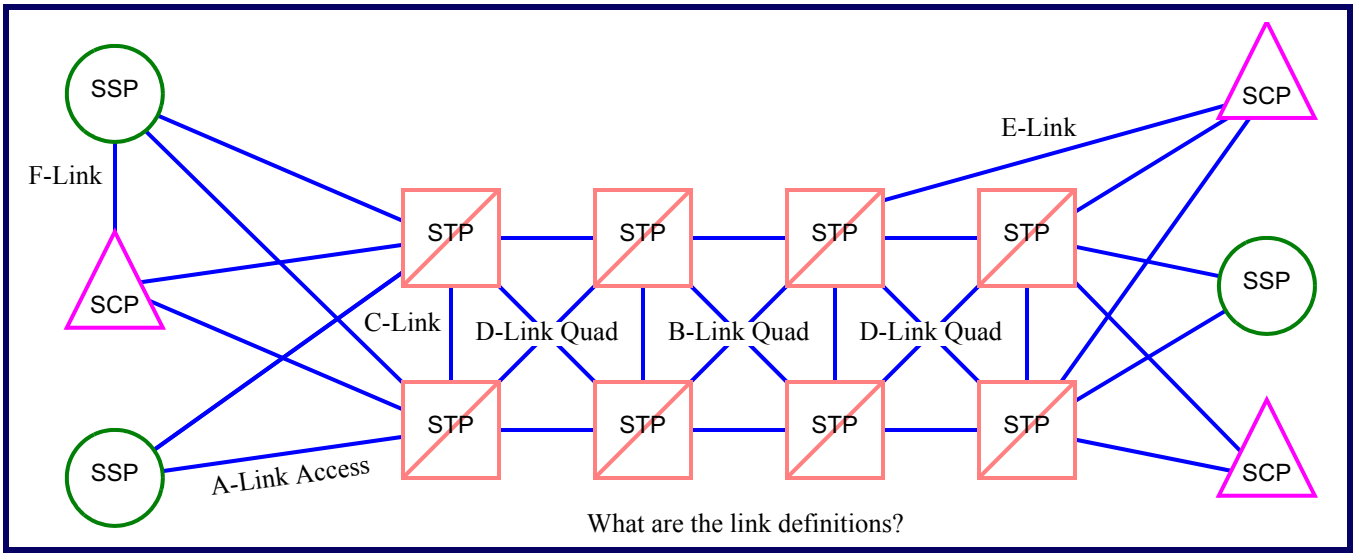
C. Cross Links. Used to connect a mated pair of STP's together. Usually, these will be duplicated for redundancy.

D. Diagonal Links. Used to connect pairs of STP's at the secondary (outer) level of the STP's. Similar to B links.

E. Extended Links. Used as a secondary connection from an SSP or SCP to an STP. Similar to an A link.

F. Fully Associated Links. Used to connect pairs of SSPs or SCPs together. These are needed for situations like inter-MSC hand off, where a direct signaling connection is required.

Figure 1: Basic SS7 Network Architecture

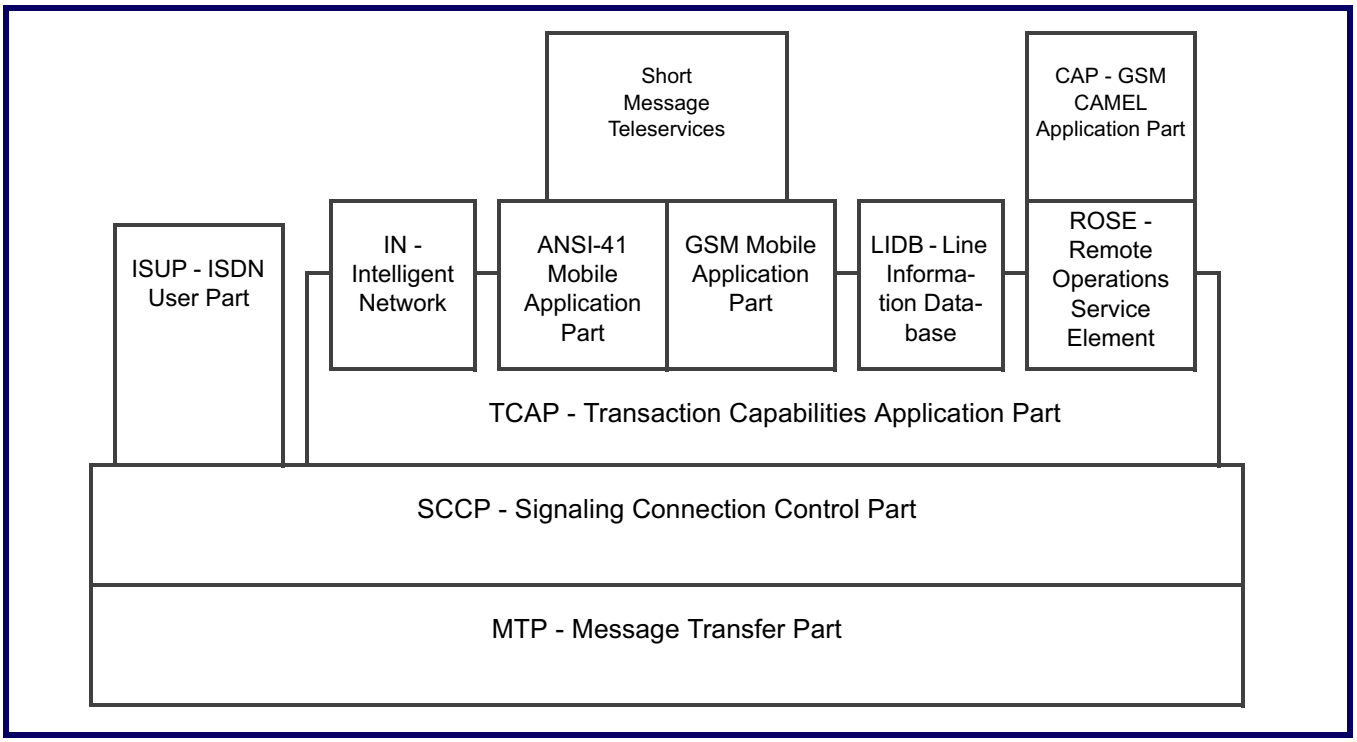


Protocol Layers

Evidence of the success of SS7 is the number of protocols that have been built on top of it. All implementations include MTP to provide the physical and transport layers, and may contain an SCCP layer for supplementary routing services. Above these layers, some protocols are part of the SS7 family (e.g. ISUP and TCAP) and others merely take advantages of the capabilities provided by SS7.

Figure 2 shows the primary SS7 protocol layers (MTP and SCCP) and examples of some application layers:

Figure 2: SS7 Protocol Layers



MTP – Message Transfer Part

The only essential part of SS7, this protocol defines the physical layer, the basic framing of the synchronous protocol and packages for carrying and routing network management messages. To be described in more detail in our December, 2001 issue.

SCCP – Signaling Connection Control Part

Provides additional routing services, most notably global title addressing and segmentation.

SCCP will be described in more detail in our January, 2002 issue.

ISUP – ISDN User Part

The basic call processing protocol for SS7. Used by wireless systems to interface more efficiently with the PSTN and other landline switching networks.

TCAP – Transaction Capabilities Application Part

A protocol for packaging messages for transaction oriented applications (e.g. command/response), especially those that contain many optional or variable length parameters. Commonly used for database query and wireless applications. This protocol will be described in more detail in our November, 2001 issue.

IN – Intelligent Network

A landline protocol that allows switching systems to offload complex applications (such as 1-800 databases) through the use of triggers (essentially command/response message pairs generated when a trigger point is detected in call processing). Defined by ATIS T1.667, the ITU-T Q.12XX series and as the 'Advanced' Intelligent Network in FR-15 from Telcordia.

ANSI-41 MAP

The protocol that supports roaming services for AMPS, N-AMPS, D-AMPS (TDMA) and CDMA (cdmaOne and cdma2000) radio interface.
Defined by TIA/EIA-41.

GSM MAP

The protocol that supports roaming services for the GSM radio interface. Originally standardized by ETSI, but now standardized by 3GPP (www.3gpp.org) in TR 29.002.

Short Message Teleservices

Short message service protocols contain 'bearer' data that is transparent to most of the wireless network, being transmitted from an SMS message center (MC/SMSC) to a mobile. These protocols are used to provide not only traditional short messaging, but also over-the-air mobile provisioning and GPS-based location services. The contents of the teleservices are defined by the individual digital radio interfaces.

LIDB – Line Information Database

The LIDB database and protocol is used to provide enhanced landline services, such as verification of collect and third party calling and access to calling party names. Because the database is accessible, via SS7, to all landline carriers (and potentially, in future, to wireless carriers) it is possible to, for example, make a collect call from a payphone in Canada to a home phone served by a US carrier.

This protocol is not formally a standard, being a proprietary specification of Telcordia defined in GR-1149 and GR-1158.

ROSE – Remote Operations Service Element

A CCITT/ITU protocol providing enhanced transaction-oriented application communications beyond that provided by TCAP. It is defined by ITU-T X.881 and X.882.

CAP – CAMEL (Customised Applications for Mobile network Enhanced Logic) Application Part

A protocol that enhances GSM by providing intelligent network-like services, such as prepaid calling and special translations, such as access to office extensions through 3, 4 or 5 digit dialing. In concept, it is very similar to ANSI-41 WIN.

CAP is defined in 3GPP specifications 22.078, 23.078 and 29.078 (formerly ETSI GSM specifications 22.078, 23.078 and 29.078).

SS7 Standards

One of the most widely used national SS7 protocols is known as ANSI SS7, standardized for use in North America by ATIS (www.atis.org) standards committee T1S1 (www.t1.org).

Table 1: ANSI SS7 Standards

Standard	Protocol
T1.110	Overview
T1.111	MTP
T1.112	SCCP
T1.113	ISUP
T1.114	TCAP

ANSI SS7 standards are updated approximately every four years. The 1988 version is the basis for most networks. Major enhancements in 1992 and 1996 have not all been implemented, because of compatibility issues that would necessitate a network-wide coordinated approach to an upgrade.

ITU SS7 standards (often known as 'C7') are the basis for most countries outside North America, although usually with national adaptations affecting network fundamentals such as the number of bits in a point code.

Table 2: ITU SS7 Standards

Standard	Protocol
Q.700	General
Q.701-710	MTP
Q.711-719	SCCP
Q.720-729	TUP (forerunner to ISUP)
Q.730-739	ISDN Supplementary Services
Q.740-749	Data User Part (DUP)
Q.750-759	Management
Q.760-769	ISUP
Q.770-779	TCAP
Q.780-789	Test Specification

ITU SS7 standards are also produced on a four year cycle.

In our future discussions of TCAP, MTP and SCCP, we will refer mainly to ANSI SS7 while providing comparisons with ITU SS7 where appropriate.

TIA TR-45.4/3GPP2 TSG-A Radio to Switching Technology ("A" Interface) Standards

Cellular Networking Perspectives

Editor: David Crowe • Phone +1-403-289-6609 • Email David.Crowe@cnp-wireless.com *Last published April, 2001*

Note: 1. IS- Interim Standard, TSB- Telecommunications Systems Bulletin, PN- Project Number, SP- ANSI Standards Proposal, A.Pxxxx - TSG-A project, A.Rxxxx - TSG-A report, A.Sxxxx - TSG-A specification.
2. Bold Type indicates a modification since the previous publication of this information.
3. Published TIA standards can be obtained from TIA at www.tiaonline.org/standards/search_n_order.cfm.

Thanks to Steve Jones (MALR, Chair of TR-45.4) for his assistance compiling the information in this table.

Published Standards

Standard	Project	Description	Status
TIA/EIA-634-B	SP-4277	"A" interface supporting analog, CDMA, SMS, data services, frame relay and 1800MHz PCS	Published 04/99
TIA/EIA-828-A	**SP-4604-A**	**BTS-BSC (A bis) interface for cdma2000 systems**	**Published 07/01**
TIA/EIA-829	PN-4683	Tandem free operation (eliminates intermediate vocoders in mobile-to-mobile calls with compatible vocoders)	Published 06/00
IS-634-0		MSC-BS "A" Interface Standard	Published 12/95
IS-634-A	PN-3539	MSC-BS Interface, including support for IS-95-A, EIA/TIA-553-A, IS-41-C, SMS, data and frame relay	Published 10/98
IS-878	**PN-3-0009**	**1xEV-DO interoperability specification (IOS) for cdma2000 "A" interface**	**In press**
IS-2001	**PN-4545**	**cdma2000 Access Network Interface ("A" Interface) based on 3GPP2 TSG-A IOS V4.1**	**Published 12/00**
IS-2001-1	**PN-4545-AD1**	**Addendum 1 for IS-2001**	**Published**
IS-2001-A	**PN-4545-RV1**	**cdma2000 Access Network Interface based on IOS v4.2**	**Published 08/01**
TSB-80		IS-634-0 Addendum (corrections, SMS, subrate voice frame format)	Published 11/96
TSB-104		PCS Service Description (now IS-104 in committee TR-46)	Published 06/94

Completed Internal Documents

Project	Description	Status
PN-3142	Cellular Microcell/Microsystems Requirements Document	Internal project
PN-3296	MSC-BS Interface (A-Interface) Requirements for Public 800 MHz	Internal project

Active TIA TR-45.4 Projects

Standard	Project	Description	Status
TIA/EIA-634-C	SP-4377	Revision of BS-MSC "A" interface	Project cancelled
TIA/EIA-658-A	**PN-3473-RV1**	**Data services interworking function for cdma2000 (L-interface)**	**Development**

TIA/EIA-895	**SP-3-0030**	**Tandem free operation (elimination of voice coders in mobile-to-mobile calls)**	**Ballot**
TIA/EIA-2001	**PN-4546**	**cdma2000 Access Network Interface (ANSI version)**	**Development**
IS-828	PN-4604	BTS-BSC (A bis) interface for cdma2000 systems	Ballot failed
IS-2001-B	**SP-4545-RV2**	**cdma2000 Access Network Interface based on IOS v4.3**	**Development**
	PN-3964	Use of A-Interface standards in Wireless Local Loop	Project cancelled
	PN-4276	Fixed Wireless Access (Stage I Description)	On hold pending review by CDG
	PN-4376	**Addendum to TIA/EIA-634-B to Address 3G Extensions**	**Replaced by PN-4545**
	PN-4378	Addendum to TIA/EIA-634-B for TIA/EIA-136-B (TDMA)	Project cancelled
	PN-4379	Addendum to TIA/EIA-634-B for TIA/EIA-95-B (CDMA)	Replaced by PN-4545

Active 3GPP2 TSG-A Projects

Standard	Project	Description	Status
A.P0006	PN-3-0007	IP-based Radio Access Network "A" interface between base station and MSC	Development
A.P0007	PN-3-xxxx	Support for 1xEV-DO (CDMA) between RAN and elements and to the Core Network	Development
A.R0003		**Abis interface technical report for cdma2000 systems**	**Published 12/99**
A.S0001-A	**PN-4545**	**Same as IS-2001**	**Published 01/01**
A.S0001-B	**PN-4545-RV1**	**Same as IS-2001-A**	**Published 08/01**
A.S0003	**PN-4604-A**	**BTS-BSC (A bis) interface for cdma2000 systems (same as IS-828)**	**Published 03/00**
A.S0004		**Tandem free operation (eliminates intermediate vocoders in mobile-to-mobile calls with compatible**	**Published 12/99**
A.S0004-0.1		**Addendum to tandem free operations**	**Published 01/01**
A.S0004-A	**SP-3-0030**	**Revision A of Tandem Free Operations**	**Published 07/01**
A.S0007-0	**PN-3-0009**	**1xEV-DO interoperability specification (IOS) for cdma2000 "A" interface (see IS-878)**	**Published 07/01**