

Signalling System #7 (SS7/C7) to Binary Level Training

OVERVIEW

Signaling System #7 (SS7) (AKA C7 outside N.America) is the predominant signalling system for the **public switched telephone network (PSTN)** and also Public Land Mobile Networks (PLMNs). New packet networks for voice telephony also typically rely on **SS7** for signalling. **SS7** defines the procedures for setting-up, managing and clearing down calls between users, as well as non-circuit related signaling. For example it is used to provide Local Number Portability (LNP) as mandated by the FCC, **Call Management Database Services (CMSDB)** such as 800,900, and 500 services (0500,0800,0898 etc within the UK), and **Line Information Database Services (LIDB)** such as calling card services. The SS7/C7 protocol is also a key component in providing Advanced Intelligent Networks (AINs) as defined by **Bellcore** and **Intelligent Networks** as defined by **ITU-T**.

The first day of the course is a “leveller” - introducing signalling, signalling requirements and associated terminology and concepts. The following three days depict a detailed picture of the architecture and protocol of SS7/C7, down to the binary level. The fifth day is solely hands on and looks at the latest SS7/C7 technological developments, and how SS7/C7 is being used as voice/data converge.

TRAINING METHOD

- # Lectures
- # Exercises
- # Demonstrations
- # Training documentation (~500 pages)
- # Windows® based software for protocol analysis. SS7/C7 log files will be studied that will be distributed in electronic format. It may be beneficial if participants bring notebooks with Windows XP/ Vista/7.

COURSE INFO

- # Duration: **Five days**
- # Language: English
- # Documentation: English
- # Participants: General class size 5-10

WHO SHOULD ATTEND

- # Technical development and support professionals involved in the support and implementation of networks and services
- # Those professionals involved in the design and implementation of **next-generation telecommunication solutions**
- # Planners and developers of packet based carrier grade networks and services, which need to understand the present and future role of SS7/C7

PREREQUISITES

The course has no prerequisites, although a **technical understanding of voice networks and associated technology** would be beneficial.

CONTACT

Lee S Dryburgh

Lead author of **Signalling System No. 7 (SS7/C7): Protocol, Architecture, and Services.**

lee@dryburgh.com

www.ss7.net

LEARNING OUTCOMES

- # Knowledge of public switched telephone networks (PSTNs) and public land mobile networks (PLMNs)
- # Knowledge of signaling systems, associated terminology and concepts
- # Knowledge of the C7/SS7 protocol stack at binary level in the context of both cellular and fixed line systems
- # Insight into how to detect and locate problems
- # Knowledge of what the critical messages and parameters are
- # How to navigate C7/SS7 standards
- # How to analyse the C7/SS7 protocols
- # Understanding of service protocols including INAP and CAMEL
- # How to navigate service protocol standards including INAP, CAMEL and MAP
- # Knowledge of public switched telephone networks (PSTNs) and public land mobile networks (PLMNs)
- # Knowledge of signaling systems, associated terminology and concepts
- # Knowledge of the C7/SS7 protocol stack at binary level in the context of both cellular and fixed line systems
- # Insight into how to detect and locate problems
- # Knowledge of what the critical messages and parameters are
- # How to navigate C7/SS7 standards
- # How to analyse the C7/SS7 protocols
- # Understanding of service protocols including INAP and CAMEL
- # How to navigate service protocol standards including INAP, CAMEL and MAP

PRESENTER DETAILS

The course is delivered by **Lee S Dryburgh**, lead author of **Signalling System No. 7 (SS7/C7): Protocol, Architecture, and Services**.

HIGHLIGHTS FROM HIS CAREER INCLUDE:

- # Graduated in Computer Science then specialised in [signalling](#) for nearly a decade, with the main emphasis on the protocol used in 99% of networks - [Signalling System #7 \(SS7\)](#).
- # Was a [SS7/C7](#) software engineer covering virtually every SS7/C7 layer/applications - [MAP](#), [TCAP](#), [SCCP](#), [INAP](#), [ISUP](#), [MTP](#), [IS-41](#), [BSSAP](#) and standards [ETSI](#), [ANSI](#), [Bellcore](#) and [ITU](#). For example he wrote the software decode for the [Chinese INAP](#). He worked as a software engineer for both the [acceSS7](#) and [HP3900](#) platforms.
 - Was a protocol software engineer responsible for a proprietary [telecommunications protocol system](#) involving communications between transactions terminals out in the field and a central [UNIX](#) host.
 - Played a leading role in achieving [national SS7/C7 certifications](#) for a switch and a softswitch produced by a major Internet equipment manufacturer.
 - Performed switch installations as well as post installation [SS7 testing](#).
 - Performed [SS7/C7](#) testing for many variants including [Swedish ISUP](#), [UK ISUP](#), [NUP/IUP](#) and [Russian ISUP](#) in addition to the more common [ITU](#) and [ANSI](#) protocols.
 - Performed testing against one of the world's most complex [Intelligent Network \(IN\)](#) platforms, certifying the [SCCP](#) and [TCAP](#) SS7/C7 protocols.
 - Has unique knowledge of SS7/C7 Security aspects and provides consulting on signalling security issues largely to parties involved in VoIP and 3G implementations.
- # Since the [initial 3G rollouts](#) in 2001 has provided hands on [2/2.5](#) and [3G](#) support and later service

additions as well as 3GPP lead architecture changes. Such support has included [SS7](#), [SIP](#), [H.323](#), [CODECs/transcoding](#) and [softswitch](#) management.

- # Has been working in [Next-Generation Network \(NGN\)](#) environments since first rollouts in 2004.
 - Wrote and performed [SS7 to SIP interworking](#) tests.
 - Dealt with signalling issues such as [SIP/H.323/SS7 interworking](#) for PSTN calls.
 - Tested [3G services](#) such as video calling and location based services which require such [signalling interworking](#).
 - Managed [softswitches](#) and [media gateways](#) since 2004.
 - Played a leading role in [BICC/ISUP/SIP interworking](#) verification for a [softswitch](#) produced by a major telecoms equipment vendor.
 - He is currently authoring another book on [next generation](#) signalling systems including [NGN protocol interworking with SS7/C7](#).
- # Has spent 7+ years delivering signalling related training on an international basis. He currently provides training in [SS7](#), [C7](#), [INAP](#), [CAMEL](#), [MAP](#) ([GSM](#) and [ANSI-41](#)), [SIGTRAN](#) ([M3UA](#), [M2UA](#), [SUA](#), [M2PA](#)), [H.323](#), [SIP](#), [P2P SIP](#), [NGNs](#) as well as issues related to the future of telephony.
- # He is working on an Engineering Doctorate in conjunction with the University College of London (UCL) mapping out the [future of telephony](#) and trying to [foresee killer applications and required protocols](#).
- # He is a member of The Institution of British Telecommunications Engineers (IBTE), The Professional Contractors Group (PCG), The Federation of Telecommunications Engineers of the European Community (FITCE), The British Computer Society (BCS), The Institution of Electrical Engineers (IEE) and The Institute of Electronic and Electrical Engineers (IEEE).

COURSE CONTENTS

SIGNALLING INTRODUCTION
SUBSCRIBER SIGNALLING PROTOCOLS
NETWORK SIGNALLING PROTOCOLS
THE HISTORY OF SIGNALLING
SIGNALLING STANDARDS
SIGNALLING CONCEPTS AND TERMINOLOGY
PSTN OVERVIEW
SS7/C7 OVERVIEW
SS7/C7 NETWORK ELEMENTS
MESSAGE TRANSFER PART 1 (MTP 1)
MESSAGE TRANSFER PART 2 (MTP 2)
MESSAGE TRANSFER PART 3 (MTP 3)
SIGNALLING CONNECTION CONTROL PART (SSCP)
TELEPHONY USER PART (TUP)
NATIONAL USER PARTS (NUPS)
NARROWBAND ISDN USER PART (N-ISUP)
TRANSACTION CAPABILITIES APPLICATION PART (TCAP)
INTELLIGENT NETWORK APPLICATION PROTOCOL (INAP) AND CUSTOMISABLE APPLICATIONS FOR MOBILE ENHANCED LOGIC (CAMEL)
MOBILE APPLICATION PART (MAP)
SS7/C7 SECURITY, TESTING AND MONITORING
FUTURE DEVELOPMENTS AND TOMORROW'S SIGNALLING

SIGNALLING INTRODUCTION

What is Signaling?

- # The Purpose of Signaling Explained
- # The History of Signaling Detailed
- # Subscriber VS Network Signaling
- # Why Signaling is a "Hot" Subject Detailed

SUBSCRIBER SIGNALLING PROTOCOLS

- # Analog Access Signaling Technologies Introduced (Pulse, DTMF)
- # Digital Access Signaling Technologies Introduced (DSS1, DSS2)

NETWORK SIGNALLING PROTOCOLS

- # Analog Network Signalling Technologies Introduced (MF)
- # Digital Network Signalling Technologies Introduced (SS6, SS7)

THE HISTORY OF SIGNALLING

The History of Signalling Explained

SIGNALLING STANDARDS

The Purpose of Signaling Standards

- # History of Signaling Standards
- # Standard's Bodies
- # World-wide SS7/C7 Standards
- # Regional SS7/C7 Standards
- # National SS7/C7 Standards

SIGNALLING CONCEPTS AND TERMINOLOGY

- # Channel Associated Signaling (CAS)
- # CAS Examples
- # Common Channel Signaling (CCS)
- # CCS Examples
- # CCS and CAS Contrasted

- # CCS Signaling Modes Explained
- # Associated Mode
- # Quasi-Associated Mode
- # Non-Associated Mode

PSTN OVERVIEW

- # Basic PSTN Components
- # Signaling Between the Components
- # Network Hierarchy Explained
- # UK Network Examined
- # US Network Examined

SS7/C7 OVERVIEW

- # The SS7/C7 Protocol Stack against the OSI Model
- # SS7/C7 Functionality Overview
- # SS7/C7 Based Services - CNAM, LNP, CLASS, LIDB, SMS, EMS, PVN, E911, Do-Not-Call, and Supplementary Services
- # SS7/C7 as Thread of Convergence

SS7/C7 NETWORK ELEMENTS

- # Service Switching Point (SSP)
- # Signal Transfer Point (STP)
- # Service Control Point (SCP)
- # N.American SS7 Network Architecture
- # European and Asian C7 Network Architecture
- # Link Types and Usage
- # Links and Linksets Explained
- # Routes and Routesets Explained

MESSAGE TRANSFER PART 1 (MTP 1)

- # Functions of MTP 1 Described
- # North American T1 Carrier Explained
- # European PRI E1 Carrier Explained
- # The Digital TDM Hierarchy for N.America Shown
- # The Digital TDM Hierarchy for Europe and Asia Shown

MESSAGE TRANSFER PART 2 (MTP 2)

- # Functions of MTP 2 Described
- # MTP 2 Overhead Shown
- # Signal Units Introduced
- # Message Signal Unit (MSU) Detailed
- # Link Status Signal Unit (LSSU) Detailed
- # Fill in Signal Unit (FISU) Detailed
- # SU Layers of Operation Explained
- # SU Delimitation Explained
- # SU Alignment Explained
- # SU Error Detection/Correction Explained
- # Basic Error Correction Method Shown
- # Preventive Cyclic Retransmission Shown
- # Methods used for Link Error Monitoring
- # Link Management Detailed
- # Link Transmission Priorities Shown
- # Link Initial Alignment Shown

MESSAGE TRANSFER PART 3 (MTP 3)

- # Functions of MTP 3 Described
- # MTP 3 Overhead and Message Format Shown
- # Service Information Octet (SIO) Contents Explained
- # SubService Field (SSF) Explained
- # Service Indicator (SI) Explained
- # ITU Routing Label Shown
- # ITU Point Code Format Explained
- # ANSI Routing Label Shown
- # ANSI Point Code Format Explained
- # Assignment of the ANSI Point Code Explained
- # UK Routing Label Shown
- # UK Point Code Format Explained
- # Assignment of UK, US and International Point Codes Explained
- # International and National SS7/C7 Network Hierarchy Explained
- # Point Codes and Interconnect Explained
- # Relationship between L1, L2 and L3 Shown
- # Signaling Message Handling (SMH) Overviewed
- # SMH - Routing in More Detail (SLS and CIC Fields)
- # SMH - Heading Code (H0 / H1) Fields

- # Signaling Network Management (SNM) Overviewed
- # Signaling Traffic Management (STM) Overviewed
- # STM - Changeover/Changeback Examples
- # STM - Forced and Controlled Re-Routing Examples
- # STM - MTP Restart Example
- # STM - Management Inhibiting Example
- # STM - Flow Control & Traffic Reconfiguration Example
- # Signaling Link Management (SLM) Overviewed
- # SLM - Link Activation Demonstrated
- # SLM - Restoration Demonstrated
- # SLM - De-Activation Demonstrated
- # Signaling Link Test Explained
- # Processor Outage Explained
- # Signaling Route Management (Overviewed)
- # SRM - Transfer Prohibited Example
- # SRM - Transfer Allowed Example
- # SRM - Route Set Test Example
- # MTP3b (Broadband) Described

SIGNALLING CONNECTION CONTROL PART (SCCP)

- # Functions of SCCP Described
- # Signaling Information Field (SIF) for SCCP MSU Shown
- # SCCP Message Structure Detailed
- # Connectionless Services Explained
- # Connection-Orientated Services Explained
- # SCCP Management Procedures Overviewed
- # Traffic Information Management Detailed
- # Signaling Point Management Detailed
- # SCCP Routing Overviewed
- # Point Code Routing Explained
- # Subsystems and Subsystem Routing Explained
- # ITU, ANSI and 3GPP Subsystem Numbers Shown
- # Global Title Translation (GTT) Explained
- # GTT Examples
- # GTT Outcomes
- # CgPA/CdPA Fields Detailed
- # CgPA/CdPA Cellular and Fixed Line Examples
- # Address Indicator Explained

- # Global Title Indicator (GTI) Field Explained
- # Translation Type Field Explained
- # Encoding Scheme Field Explained
- # Numbering Plan Field Explained
- # Nature of Address Indicator Explained
- # Intra-PLMN Routing Example
- # Inter-PLMN Routing Example
- # ISUP Routing Example

TELEPHONY USER PART (TUP)

- # User Parts Described
- # User Part Overhead Shown
- # TUP/TUP+/TUP-E Explained and Overviewed
- # Signaling Information Field (SIF) for TUP MSU Shown
- # Two TUP Call Sequences Shown

NATIONAL USER PARTS (NUPS)

- # Signaling Information Field (SIF) for NUP MSU Shown
- # NUP History
- # British Telecom NUP Example
- # Interconnection User Part (IUP) Example
- # Five IUP Call Sequences Shown

NARROWBAND ISDN USER PART (N-ISUP)

- # N-ISDN User Part (N-ISUP) Overviewed
- # Signaling Information Field (SIF) for N-ISUP MSU Shown
- # N-ISUP Evolution Detailed
- # N-ISUP Variants Discussed
- # N-ISUP Message Groups Shown
- # En Bloc Signaling Explained
- # Overlap Signaling Explained
- # N-ISUP Message Format Explained
- # Common Messages Detailed
- # Five Call Sequences Shown
- # Common Parameters Detailed
- # Supplementary Services Overviewed
- # Three Supplementary Services Explained
- # International ISUP Detailed

- # ISUP Nationalisation Described
- # Broadband ISDN User Part (B-ISUP) Introduced

TRANSACTION CAPABILITIES APPLICATION PART (TCAP)

- # Transaction Capabilities Application Part (TCAP) Overviewed
- # Signaling Information Field (SIF) for TCAP within SCCP MSU Shown
- # Transactions Detailed
- # Transaction Sequences Shown
- # Components Detailed
- # Dialogue Portion Detailed
- # Error Handling Described
- # ANSI Message Contents
- # ITU Message Contents

INTELLIGENT NETWORK APPLICATION PROTOCOL (INAP) AND CUSTOMISABLE APPLICATIONS FOR MOBILE ENHANCED LOGIC (CAMEL)

- # Intelligent Networks (INs) Described
- # IN Standards Explained
- # Intelligent Network Conceptual Model (INCM)
- # Intelligent Network Call Modelling Concepts
- # General Structure of the Capability Sets
- # INAP Overviewed
- # CAMEL Standards
- # CAMEL Overviewed

MOBILE APPLICATION PART (MAP)

- # GSM Network Components
- # GSM Network Identifiers
- # MAP operations on 'A' Interface
- # MAP operations on 'B' Interface
- # MAP operations on 'C' Interface
- # MAP operations on 'D' Interface
- # MAP operations on 'E' Interface
- # MAP operations on 'F' Interface
- # MAP operations on 'G' Interface

SS7/C7 SECURITY, TESTING AND MONITORING

- # Tools for Protocol Measurement
- # Overview of the Protocol Analyser
- # Validation and Compatibility Testing Explained
- # The ITU-T Test Specifications Introduced
- # Test Specification Creation
- # MTP2 Test Examples
- # MTP3 Test Examples
- # ISUP Test Examples
- # Supplementary Service Test Examples
- # SCCP Test Examples
- # TCAP Test Examples
- # SS7/C7 Network Vulnerabilities
- # SS7/C7 Security Measures

FUTURE DEVELOPMENTS AND TOMORROW'S SIGNALLING

- # Convergence of PSTN, Internet and Cellular
- # Media Gateways (MGs) and Controllers (MGCs) Described
- # Softswitches Described
- # Remote Access Servers (RASs) Described
- # Internet Offload Solutions Outlined
- # Session Initiation Protocol (SIP) Described
- # SIP/SS7 Interworking Described
- # MEGACO Described
- # MGCP/SCGP Described
- # SS7 Over IP (SIGTRAN) Discussed
- # Bearer Independent Protocol (BICC) Discussed
- # Evolution of SS7/C7 Beyond Circuit Switched Voice Calls Discussed