



IMS Common System (ICS) 4.0

Learning Solutions

Catalog of Descriptions



Catalog of Descriptions

INTRODUCTION.....	4
WHAT'S IN THE ICS 4.0 TRAINING PACKAGE?	4
LEARNING SOLUTIONS.....	5
COMPETENCE GAP ANALYSIS (CGA).....	6
STRUCTURED KNOWLEDGE TRANSFER (SKT).....	6
IMS TRAINING FLOW	7
IMS 4.0 OVERVIEW.....	8
IMS SIGNALING	10
IMS OVERVIEW WEB-BASED LEARNING.....	12
IP NETWORKING	14
IP ADVANCED.....	17
TELECOM SERVER PLATFORM (TSP) 5 OVERVIEW.....	20
TELECOM SERVER PLATFORM (TSP) 5 OPERATION AND MAINTENANCE.....	22
IS OVERVIEW.....	24
IS OPERATION AND CONFIGURATION.....	26



EMA 4.0 OPERATION FOR IMS	ERROR! BOOKMARK NOT DEFINED.
MULTI MEDIATION 5.0 SURVEILLANCE FOR IMS.....	30
MULTI MEDIATION 5.0 PROCESSING AND CONFIGURATION FOR IMS.....	32
MN-OSS SYSTEM ADMINISTRATION FOR IMS	34
OSS RC SYSTEM ADMINISTRATION FOR IMS	36
HSS 4.0 OPERATION & CONFIGURATION	38
CSCF 4.0 OPERATION & CONFIGURATION.....	40
IPWORKS 4.2 OPERATION AND CONFIGURATION FOR IMS	42
OSS FAULT MANAGEMENT TOOLS FOR IMS.....	45
SBG 1.2 OPERATION AND CONFIGURATION FOR IMS	47
IMT 3.0 PSTN GW CONFIGURATION	50
IMS COMMON SYSTEM (ICS) 4.0 NETWORK SURVEILLANCE STRUCTURED KNOWLEDGE TRANSFER (SKT).....	52

Introduction

Ericsson has developed a comprehensive competence development service to satisfy our customers' need for expertise. They require fast access to a range of expertise varying from the skills and knowledge required to operate a network to the expertise required to develop new end-user services.




What's in the ICS 4.0 Training Package?

The ICS 4.0 course flows are focusing on the following job categories:

- Fundamentals
- Operations Centre, Front and Back Office
- IS/IT Support
- Business Management



Service delivery is supported using various delivery methods including:

Icon	Delivery Method
	Instructor Led Training (ILT)
	Web Based Learning (WBL)
	Structured Knowledge Transfer (SKT)

Learning Solutions

Ericsson's Learning Architects can help operators to analyze their competence needs from a business perspective, using Competence Gap Analysis (CGA), and then assist them to deliver a flexible competence development program suited to their needs. The experts can also assist with the evaluation of the training effectiveness against Key Performance Indicators (KPIs), conducting pre-tests before the program begins and post-tests to evaluate progress made during the program.

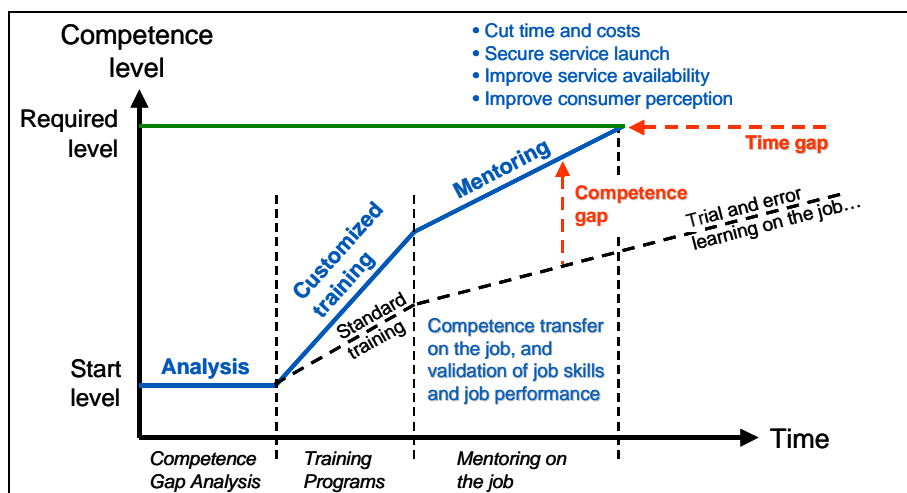


Figure 1. Analysis (CGA), Customization and Mentoring – How to add value relating to your business.

The result is a flexible program which is not only aligned with the business and operational requirements but is also customised to suit the requirements of the group or individuals to which it is directed. Flexibility is ensured; those with expertise spend less time achieving the required standard for task completion, while those at a more basic level get the help and time they need to reach it.

Competence Gap Analysis (CGA)

IMS is a network evolution and requires competence evolution towards the New Multimedia and IP networks.

Ericsson Education can help the operators to further **optimize** the competence evolution, by designing of a **tailor-made training solution** that supports effective learning and **performance** of the employees within the organization

The CGA **assesses the technical competence** of the employees in the relevant departments and **aligns the training plan to the operational needs** throughout the network evolution

Activities:

- Assessment of current competence level for the different job roles;
- Identification of the gaps by Mapping current and required competence levels;
- Identification of the customer specific competence needs/skills to be addressed in the training delivery, based on the customer operations, job roles and IMS technical implementation

Structured Knowledge Transfer (SKT)

The SKT usually takes place at the customer site using the customer's network. The mentor leads each student through tasks that are defined for that employee's job function. Since the SKT is based on the employee daily tasks and customer network, it helps to strengthen the employee's confidence to conduct the tasks on the new network/technology

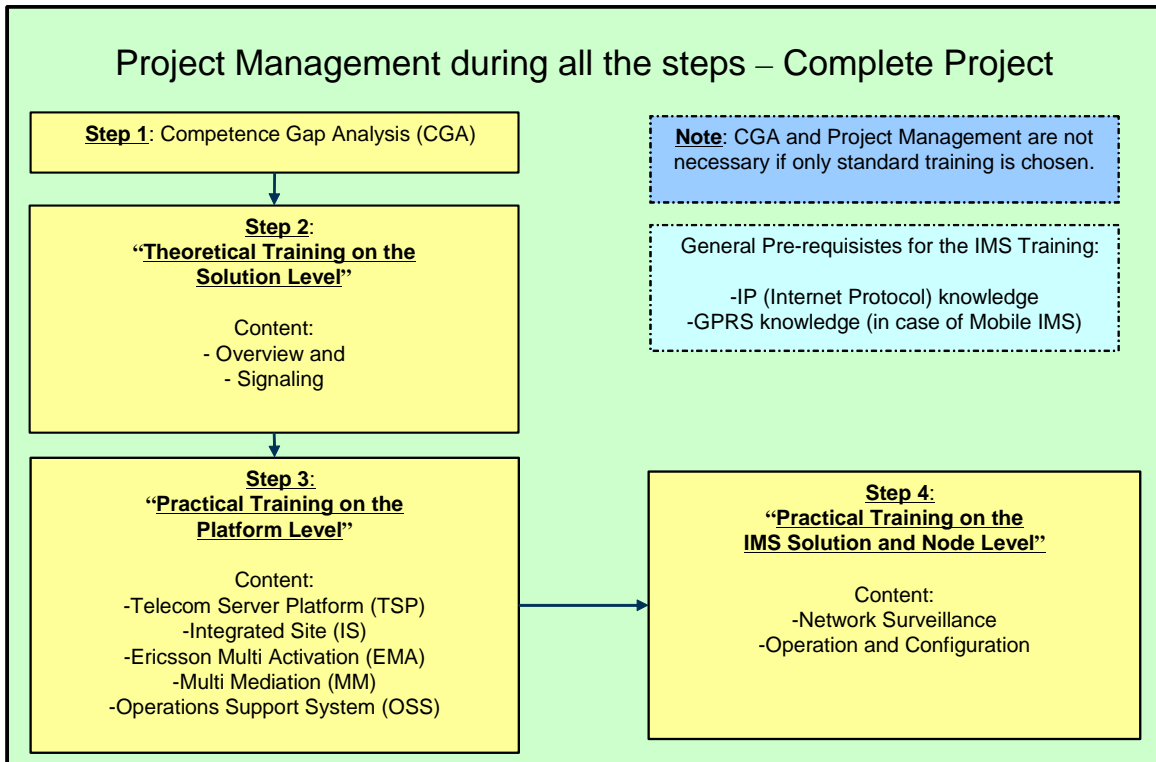
With SKT a mentor works with a small group (max. 4), ensuring that the participants master the content of a job task list drawn up for each identified job role and duty or responsibility, and approved by the customer. The result is accelerated learning tailor-made to the customer's needs and objectives.

As there is no room for error when working on live equipment, the participants have to have completed the prerequisite training courses and lab training before undertaking the SKT. The mentor demonstrates the tasks involved in the job, working with the participants until they successfully perform each duty and task. In effect, while the participants are doing their job, they are learning in their own working environment.

Tasks and skills are identified during the Competence Gap Analysis (CGA) phase, based on the customer specific job roles and operations.

IMS Training Flow

The following are the recommended steps for a complete and efficient competence development on the IMS technology:



IMS 4.0 Overview



LZU 108 6563 R2A

Description

This Instructor-Led Course provides an overview of the IP Multimedia Subsystem (IMS 4.0) and the IMS Multimedia Telephony (IMT 3.0), IMS Push To Talk (PTT 4.0) and IMS weShare 4.0 solutions. The course describes nodes, features, services and end-user interfaces of IMS.

Learning objectives

On completion of this course the participants will be able to:

1 Describe the IMS system.

1.1 Explain what IMS is.

1.2 Explain what multimedia is.

1.3 Briefly describe the IMS solutions, IMT, PTT, and weShare.

1.4 Explain some operator and end-user benefits of IMS.

1.5 Explain where IMS is positioned within the total telecoms picture.

2 Explain the services provided by IMS.

2.1 List some end-user services for IMT, PTT, and weShare.

2.2 Describe the IMT end-user interface and explain how an IMT session is invoked from a user client.

2.3 Describe the PTT & weShare user interfaces and explain how IMS sessions are invoked from a user client

3 Describe the IMT 3.0 architecture.

3.1 Describe the IMT functional architecture, including IMS common nodes.

3.2 Describe how IMT interworks with the core IP network.

3.3 Explain how IMT interworks with PSTN and other VoIP networks.

3.4 List the signaling and media protocols and describe where they are used.

3.5 List the platforms used in the IMT system and briefly describe some of their functions.

4 Explain how an IMT Multimedia session is established.

4.1 Explain the SIP signaling sequence for Registration.

4.2 Explain the SIP signaling sequence for an IMT to IMT session.

4.3 Explain the SIP signaling sequence for an IMT to PSTN session.

5 Describe the Mobile IMS architecture

5.1 Describe the Mobile IMS functional architecture, including IMS common nodes.

5.2 Describe how IMS interworks with the core IP network.

5.3 Explain how IMS interworks with the mobile access network.

5.4 List the signaling and media protocols and describe where they are used.

5.5 List the platforms used in the Mobile IMS system and briefly describe some of their functions.

5.6 List the platforms used in the IMT and IMS common nodes and briefly describe

6 Explain how PTT & weShare sessions are established.

6.1 Explain the SIP signaling sequence for Registration (SSO).

6.2 Explain the SIP signaling sequences for typical PTT sessions.

6.3 Explain the SIP signaling sequence for a typical weShare session.



7 Explain how O&M and provisioning are implemented in IMS

7.1 Explain the functions of OSS.

7.2 Explain the function of Ericsson MultiActivation (EMA).

Target audience

The target audience for this course is: Fundamentals

Prerequisites

Students should have a good general knowledge of telecommunications.

Duration and class size

The length of the course is 2 days and the maximum number of participants is 16.

Learning situation

This course is based on theoretical instructor-led lessons given in a classroom environment

IMS signaling



LZU 108 6604 R2A

Description

Would you like to know how an IMS session is set up step by step?

This course provides an introduction to signaling in the IMS by presenting the protocols involved and different traffic cases from weShare, Push to Talk (PTT) and the IMT system (IMS Multimedia Telephony).

The SIP protocol and the most important IMS related extensions to SIP and SDP are covered as well as the Diameter Base protocol and its IMS related applications (Cx/Dx, Sh, Rf).

Learning objectives

On completion of this course the participants will be able to:

- 1 List the main logical nodes in the IMS System
- 2 Describe concepts related to mobile access (i.e. 3GPP) for IMS on a high level
- 3 Session Initiation Protocol (SIP)
- 4 Describe the basic functions and capabilities of SIP
- 5 Name major IETF protocols related to SIP, IMS and VoIP
- 6 List at least ten SIP methods and state their function
- 7 Explain the routing and addressing principles of SIP signaling
- 8 Explain the offer / answer model for SDP usage in SIP
- 9 Describe the steps in a generic session establishment
- 10 Describe the basic functions and capabilities of Diameter
- 11 List important Diameter messages (base protocol and application)
- 12 Describe the services provided by the Cx/Dx, Sh and Rf applications for Diameter in IMS
- 13 Describe the weShare architecture
- 14 Explain routing and interworking with CS (for weShare)
- 15 Describe a basic session setup in weShare
- 16 Describe the MSRP encoding
- 17 Describe the PoC architecture
- 18 Explain the routing for different types of PoC sessions
- 19 Explain the relation between the PoC client and the PoC servers (Controlling / Participating)
- 20 Describe a basic 1-1 Ad-Hoc session setup in PoC
- 21 Describe the steps during a registration procedure and in a basic call setup in IMT
- 22 Read and interpret most information in traces of SIP messages

Target audience

The target audience for this course is: Fundamentals

Prerequisites

The students should have attended “IMS Overview” LZU 108 6563, IMT 3.0 Overview LZU 108 2055 or Mobile IMS Overview LZU 108 2254.

Furthermore the students should have a basic understanding of datacom in general and more specifically good knowledge of IP networking and the TCP/IP protocol family.

Duration and class size

The length of the course is 2 days and the maximum number of participants is 16.

Learning situation

Instructor Led Training (ILT). This course is based on theoretical instructor-led lessons and theoretical exercises.

Time schedule

The time required always depends on the knowledge of the participants and the hours stated below can be seen as an estimate.

Day	Topics in the course	Estimated time
1	<ul style="list-style-type: none">• IMS introduction• SIP	6h
2	<ul style="list-style-type: none">• Diameter• weShare• PTT	6h

IMS Overview Web-Based Learning



LZU 108 6488 R1A

Description

If you want to know what IMS is, this course will give you a better understanding of the overall aspects of IMS, its services, solutions and core architecture concepts.

Learning objectives

On completion of this course the participants will be able to:

- 1 Define what IMS stands for and describe the benefits of IMS, product positions and Ericsson's IMS solutions
- 2 Describe the main services and solutions developed for wireline and wireless networks
- 3 Explain what the IMS Common system and application subsystem is
- 4 Describe the IMS node functions and how they are involved in IMS call establishment

Target audience

The target audience for this course is: Service Planning Engineers, Service Design Engineers, Network Design Engineers, Network Deployment Engineers, Service Deployment Engineers, System Technicians, Service Technicians, System Engineers, Service Engineers, Field Technicians, System Administrators, Business Developers.

Prerequisites

There are no prerequisites for this course.

Duration and class size

The length of the course is approximately 2 hours.

Learning situation

This is a web-based interactive training course with multimedia content.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate.



Day	Topics in the course	Estimated time
1	<ul style="list-style-type: none">• Introduction• Services• Architecture• Multimedia Session Establishment	<p>30 mins</p> <p>30 mins</p> <p>30 mins</p> <p>30 mins</p>

IP Networking



LZU 102 397 R3A

Description

This course will give the students an insight and understanding of the TCP / IP protocol stack from the physical layer to the application layer. The students will learn the operation of different protocols and applications within the TCP / IP suite such as ARP, BOOTP, DHCP, DNS, NIS, NTP, NFS, HTTP, FTP, SMTP, Telnet, FTP, TFTP. Students will learn about IP addresses, both classful and classless (CIDR) and how subnetting / aggregation operates. Students will learn about different network devices and will get a detailed understanding of Bridging, LAN Switching, Routing and Routing protocols. The hands-on exercises and analysers are used to facilitate the understanding of theory sessions.

Learning objectives

On completion of each module the participants will be able to:

- 1 List and explain IP Networking Protocols
 - 1.1 List the functions of the different bodies involved in IP standards / RFCs
 - 1.2 Analyze the OSI reference model and how it relates to the TCP / IP stack
 - 1.3 Explain Ethernet as Physical and Data Link Layer: MAC Address, CSMA/CD principles, Fast Ethernet, Gigabit Ethernet and speed negotiation
 - 1.4 Explain the operation of Hubs, Bridges, Switches and Routers
 - 1.5 Explain Wireless LANs
 - 1.6 Explain IP Protocol
 - 1.7 Explain IPv4 packet structure, protocol header and features
 - 1.8 Explain VLSM, CIDR, Subnetting, aggregation, NAT and NAT
 - 1.9 Explain how to use ICPM utilities and traceroute command
 - 1.10 Perform exercises configuring IPv4 addresses, and check connectivity
 - 1.11 Demonstrate IPv6 packet structure, protocol header, features

- 2 List and explain IP Transport and Application Protocols
 - 2.1 Explain TCP, UDP and SCTP protocol structures, headers and functionality
 - 2.3 List and explain the operation of different protocols / applications such as ARP, BOOTP, DHCP, DNS, NIS, NTP, NFS, HTTP, FTP, SMTP, Telnet, FTP, TFTP

- 3 Explain and work with IP Routing
 - 3.1 Explain and perform exercises of VLANs
 - 3.2 Explain the purpose of Spanning Tree Protocol (STP)
 - 3.3 Explain the operation of Static and Dynamic routing protocols
 - 3.4 Perform Static routing exercises
 - 3.5 Explain Interior and Exterior Gateway Protocols
 - 3.6 List the differences between Vector Distance and Link State protocols.
 - 3.7 Explain and perform exercises of RIP routing protocol
 - 3.8 Explain and perform exercises of OSPF routing protocol
 - 3.9 Explain and perform exercises of BGP routing protocol

Target audience

The target audience for this course is personnel who are involved in IP networking or those who require more knowledge on IP addressing, application and routing protocols

- Fundamentals

Prerequisites

There are no pre-requisites

Duration and class size

The length of the course is 5 days and the maximum number of participants is 8.

Learning situation

This course is based on theoretical and practical instructor-led lessons given in both classroom and in a technical environment using equipment or simulation tools.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate.

Day	Short description of the topics in the course	Estimated time
1	• List the functions of the different Standard Bodies involved in IP / RFCs	0.5
	• Analyze the OSI Reference Model and how it relates to the TCP / IP stack	1
	• Explain Ethernet, Fast Ethernet, and Gigabit Ethernet	1
	• Explain the operation of Hubs, Bridges, Switches, Routers, Collision Domains and Broadcast Domains	1
	• Explain Wireless LANs	1.5
	• Explain IP Protocol	1.0
2	• Explain IPv4 (packet format, addressing and features)	1.0
	• Explain VLSM, CIDR, Subnetting, aggregation, NAT and NAPT	1.5
	• Explain ICMP protocol and traceroute	0.5
	• Perform exercises configuring IPv4 addresses, and check connectivity	2.5
	• Demonstrate IPv6 (packet format, addressing and features)	0.5
3	• Explain TCP, UDP and SCTP protocol structures, headers and functionality	2



	• List and explain the operation of different applications (ARP, BOOTP, DHCP, DNS, NIS, NTP, NFS, HTTP, FTP, SMTP, Telnet, FTP, TFTP)	3.0
	• List the purpose and operation of VLANs	1
4	• Explain and perform exercises of Spanning Tree Protocol (STP)	2.0
	• Explain the operation of Static and Dynamic routing protocols	1
	• Explain Autonomous System	
	• Explain Interior and Exterior Gateway Protocols	
	• List the differences between Vector Distance and Link State protocols.	
	• Perform Static routing exercises	1.0
	• Explain and perform exercises of RIP routing protocol	2
5	• Explain and perform exercises of OSPF routing protocol	3
	• Explain and perform exercises of BGP routing protocol	3

IP Advanced



LZU 108 6748 R1A

Description

This course will give the students an insight and understanding of QoS, security issues and management of IP networks. The students will learn the operation of QoS supporting IP Protocols, VoIP protocols, Security topics such as authentication, confidentiality, and integrity and Simple Network Management Protocol. The hands-on exercises are used to facilitate the understanding of theory sessions.

Learning objectives

On completion of each module the participants will be able to:

1 Quality of Service (QoS)

- 1.1 Analyze the enhancement of the IP networks to support transmission of Real Time data
- 1.2 Describe QoS Basic Concepts
- 1.3 Describe QoS Architectures
- 1.4 Describe QoS Mechanisms
- 1.5 Explain Resource Reservation Protocol (RSVP) – RFC 2205
- 1.6 Explain Multi Protocol Label Switching (MPLS) – RFC 3031
- 1.7 Explain Label Distribution Systems (LDP, RSVP-TE, BGP)
- 1.8 Perform practical exercises covering Class Based Marking (CBM) using IP Precedence, DSCP and MPLS

2 Voice over IP (VoIP)

- 2.1 Comment some VoIP Protocols: H.323, Media Gateway Control Protocol (MGCP) – RFC 2705
- 2.2 Explain H.248 (MEGACO)
- 2.3 Explain Session Initiation Protocol (SIP) – RFC 3261
- 2.4 Explain Real-Time Transport Protocol (RTP) and RTP Control Protocol (RTCP) – RFC 3550 and RFC 3611
- 2.5 Perform practical exercises covering SIP messages

3 IP Security (IP Sec)

- 3.1 Analyze the existing security threats types
- 3.2 Explain Access control lists (ACL)
- 3.3 Explain the purpose and use of Firewalls
- 3.4 Explain Data Integrity, Authenticity and Confidentiality
- 3.5 Identify different Security Services (SSL, TLS, SSH, etc) – RFC 4366
- 3.6 Explain how virtual Private Networks (VPN) operate
- 3.7 Explain IP Security (IPSec) – RFC 4301
- 3.8 Explain Authentication Header (AH) – RFC 4302
- 3.9 Explain Encapsulating Security Payload (ESP) – RFC 4303
- 3.10 Explain Internet Key Exchange (IKE) – RFC 2409 v1/RFC 4306 v2
- 3.11 Perform practical exercises covering the configuration of an IPSec VPN tunnel (Phase I and Phase II negotiation)

4 IP Network Management

- 4.1 Explain ISO management areas (FM, CM, AM, PM and SM)
- 4.2 Describe the architecture of the SNMP
- 4.3 Describe functionalities available on SNMPv1, SNMPv2 and SNMPv3
- 4.4 Explain Manager-Agent communication
- 4.5 Explain SNMP operations (Get Request, GetNextRequest, GetResponse, SetRequest, Trap)
- 4.6 Perform practical exercises covering analysis of SNMP messages exchanged between Manager and Agent

Target audience

The target audience for this course is staffs involved in IP networking and require more knowledge on IP networks to guarantee quality of service, security, and management of real-time traffic.

Prerequisites

IP Networking or equivalent knowledge.

Duration and class size

The length of the course is 5 days and the maximum number of participants is 8.

Learning situation

This course is based on theoretical and practical instructor-led lessons given in both classroom and in a technical environment using equipment or simulation tools.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate.

Day	Short description of the topics in the course	Estimated time
1	• Analyze the enhance of the internet to support transmission of real time data	0.5
	• Describe QoS Basic Concepts	0.5
	• Describe QoS Architectures	0.5
	• Describe QoS Mechanisms	0.5
	• Explain Resource Reservation Protocol (RSVP)	1.5
	• Explain Multi Protocol Label Switching (MPLS)	1.0
	• Explain Label Distribution Systems (LDP, RSVP-TE, BGP)	0.5

	<ul style="list-style-type: none"> • Perform practical exercises covering Class Based Marking (CBM) using IP Precedence, DSCP and MPLS 1.0 	1.0
2	<ul style="list-style-type: none"> • Comment some VoIP Protocols: H.323 and Media Gateway Control Protocol (MGCP) 1.0 • Explain H.248 (MEGACO) 1.5 • Explain Session Initiation Protocol (SIP) 1.5 • Explain Real-Time Transport Protocol (RTP) and RTP Control Protocol (RTCP) – RFC 3550 1.0 • Perform practical exercises covering SIP messages 1.0 	
3	<ul style="list-style-type: none"> • Analyze existing security threats types 1.5 • Explain Access control lists (ACL) 0.5 • Explain the purpose and use of Firewalls 1.0 • Explain Data Integrity, Authenticity and Confidentiality 2.0 • Identify different Security Services (SSL, TLS, SSH, etc) 1.0 	
4	<ul style="list-style-type: none"> • Explain how virtual Private Networks (VPN) operate 1.0 • Explain IP Security (IPSec) 1.0 • Explain Authentication Header (AH) 1.0 • Explain Encapsulating Security Payload (ESP) 1.0 • Explain Internet Key Exchange (IKE) 1.0 • Perform practical exercises covering the configuration of an IPSec VPN tunnel (Phase I and Phase II negotiation) 1.0 	
5	<ul style="list-style-type: none"> • Explain ISO management areas (FM, CM, AM, PM and SM) 0.5 • Describe the architecture of the SNMP 1.0 • Describe functionalities available on SNMPv1, SNMPv2 and SNMPv3 1.5 • Explain Manager-Agent communication 1.0 • Explain SNMP operations (Get Request, GetNextRequest, GetResponse, SetRequest, Trap) 1.0 • Perform practical exercises covering analysis of SNMP messages exchanged between Manager and Agent 1.0 	

Telecom Server Platform (TSP) 5 Overview



LZU 108 6441 R2A

Description

This course serves as a general introduction to Ericsson Telecom Server Platform (TSP) and its applications.

Learning objectives

On completion of this course the participants will be able to:

- 1 Explain when TSP is a good platform choice and why
 - 1.1 List the principles of layered networks
 - 1.2 Identify the main characteristics of TSP and how they are achieved
 - 1.3 Interpret the terms scalability, high system availability and reliability, Telecom Grade software and hardware network redundancy

- 2 Identify the applications available on TSP
 - 2.1 IMS Applications
 - 2.2 IN Applications
 - 2.3 User Databases and Authentication Entities
 - 2.4 Charging Applications

- 3 Explain the hardware architecture
 - 3.1 Discuss GEM
 - 3.2 Explain the different types of processor modules
 - 3.3 Outline the different hardware types (NSP 4.0, NSP 4.1, NSP 5.0)
 - 3.4 Recognize the standard configurations (Pico, Micro, Mini, Midi, Opti, Macro)

- 4 Recognize the software architecture
 - 4.1 Explain TSP cluster types and DBN
 - 4.2 Describe processes and process types
 - 4.3 Identify database objects, POTs, DUs
 - 4.4 Explain distribution principles
 - 4.5 Explain replication principles
 - 4.6 Discuss data security

- 5 Describe how high availability is achieved:
 - 5.1 Discuss how system upgrades are performed

- 6 Explain what external interfaces are supported by TSP:
 - 6.1 VIP
 - 6.2 Diameter
 - 6.3 SS7
 - 6.4 CORBA

- 7 Examine on a basic level how node management is performed



Target audience

The target audience for this course is: Service Planning Engineers, Service Design Engineers, Network Design Engineers, Network Deployment Engineers, Service Deployment Engineers, System Technicians, Service Technicians, System Engineers, Service Engineers, Field Technicians, System Administrators, Application Developers, Business Developers.

Prerequisites

The participants should be familiar with basic knowledge about telecommunications and data communications.

Duration and class size

The length of the course is 1day and the maximum number of participants is 16.

Learning situation

Instructor Led Training, theoretical course.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate.

Day	Topics in the course	Estimated time
1	• Introduction	1.0 hours
	• Applications on TSP	1.0 hour
	• TSP Hardware	1.0 hour
	• Software architecture	2.0 hours
	• Interfaces and Protocols	0.5 hour
	• Node Management	0.5 hour

Telecom Server Platform (TSP) 5 Operation and Maintenance



LZU 108 6443 R2B/1

Description

This course provides participants with the skills and knowledge to configure and manage the TSP5 platform. It explores the elements involved in the operation, administration and maintenance of the TSP5 platform. These include the areas of fault management, configuration management, performance and security management on the TSP5 platform. Each operation and maintenance task is complemented by practical exercises on a real TSP5 node. User interfaces for O&M purposes are also covered. Participants will complete practical configuration and management exercises using on-line documentation, TelORB Manager and the TSP Node Management (NM) Toolbox.

Learning objectives

On completion of this course the participants will be able to:

- 1 Describe the TSP operation and maintenance architecture
 - 1.1 Outline the operational and maintenance functional areas
 - 1.2 Navigate the embedded Element Managers – TSP Node Management Toolbox and TelORB Manager
 - 1.3 Use the on-line documentation
- 2 Perform fault management
 - 2.1 Use the user interface for receiving alarms and notifications
 - 2.2 Find the relevant alarm information in the on-line documentation
 - 2.3 Review the error logs in the system
- 3 Describe the principles of backup and restoration of the TSP platform, DBN Backup, Disk DBMS backup, IO backup, FS backup, Scheduled Centralized Archive Backup
 - 3.1 Create a Backup and restore the TelORB database
 - 3.2 Create a Backup and restore an IO
- 4 Describe various types of system upgrade that can be performed on the TSP platform
 - 4.1 Perform a system upgrade on the TSP-based node
 - 4.2 Describe the product inventory feature
- 5 Describe the Virtual IP function on the TSP platform
 - 5.1 Explain the distributed IP stack on the TSP platform
 - 5.2 Perform management functions of Virtual IP on the TSP platform via the Node Management interface
 - 5.3 Perform the router configuration
- 6 Outline the different secure elements within TSP
 - 6.1 Describe provisioning principles
 - 6.2 Outline the concept of the JAMBALA Information Manager
 - 6.3 Describe the usage of LDAP protocol for the directory access
 - 6.4 Add administrators, using CM Browser

- 7 Describe the function of performance management on the TSP platform
 - 7.1 Explain the Performance Management Framework (PMF)
 - 7.2 Configure and analyze performance management data via xml files and CM browser

- 8 Manage the TSP hardware
 - 8.1 Describe the procedures required to add, remove or replace traffic processors.
 - 8.2 Replace faulty boards and cables

- 9 Describe the concept of the File Transfer Utility
 - 9.1 Explain how the FTU works
 - 9.2 Use FTU GUI to perform file transfer

- 10 Discuss the Diameter protocol
 - 10.1 Describe the main purpose of the Diameter protocol
 - 10.2 Describe the Diameter protocol layered architecture.
 - 10.3 Explain basic Diameter concepts

Target audience

The target audience for this course is: Network Deployment Engineers, Service Deployment Engineers, System Technicians, Service Technicians, System Engineers, Service Engineers, Field Technicians, System Administrators.

Prerequisites

Successful completion of the following courses:

- TSP 5 System Overview (LZU 108 6441)
- UNIX Basics (LZU 108 206)
- UNIX Fundamentals (LZUBB 108 170)
- Signaling in the Core Network GSM (LZU 108 897/2)

The participant should be familiar with Linux, TCP/IP and SS7.

Duration and class size

The length of the course is 3 days and the maximum number of participants is 8.

Learning situation

The course is based on instructor-led lessons and practical exercises on the TSP nodes. Remote access to this equipment is available to both the Ericsson and the operator's organizations.

IS Overview



LZU 108 6364

Description

This course gives an introduction to the Integrated Site (IS). It answers the questions: What is IS and why IS. The drivers for IS, the scope and the benefits are highlighted together with some examples of IS application blade systems. In addition to the general principles, some technical details are presented to provide a bridge for further studies of the Integrated Site concept.

Learning objectives

On completion of this course the participants will be able to:

- 1 Understand the IS concept
 - 1.1 Describe the background for the IS concept (why IS?)
 - 1.2 Explain the IS basic concept and give examples of possible site solutions (what is IS?)
 - 1.3 Explain basic terminology related to the IS (blade, blade system etc.)
 - 1.4 Understand the benefits and drivers associated with the IS
 - 1.5 Understand the consequences of introducing the IS
 - 1.6 Explain the consequences of the IS concept and list areas that will be affected by the IS concept
 - 1.7 Describe the IS's approach to standardization
 - 1.8 Describe the Equipment Practice employed in the IS (E-GEM) and name related standards
 - 1.9 Give examples of possible solutions for IS based nodes

- 2 Have basic understanding of the IS Architecture, framework and Infrastructure
 - 2.1 Have a basic knowledge about the technical solutions for the Integrated Site in terms of network configuration, hardware, software, site management and security
 - 2.2 Give an introduction to HW and SW management
 - 2.3 Describe the purpose and function of the ISCO, BSOM and the internal O&M subnets
 - 2.4 Explain the purpose and function of the IS common parameters
 - 2.5 Explain the function and purpose of the IS Management System (ISM), the Common Management Framework and related user interfaces
 - 2.6 Describe the Multiple Subrack domain solution
 - 2.7 Have a basic knowledge about the layer 2 switching and layer 3 routing (IPv4 and IPv6) implementation in the IS
 - 2.8 Describe Quality of Service and Class of Service treatment in the IS
 - 2.9 Describe the IS PMON, VLAN and ISP and improvements realized in IS 1.2
 - 2.10 Describe the mechanisms for maintaining robustness of ISP in the IS
 - 2.11 Explain the use of link aggregation in the IS
 - 2.12 Have basic understanding of traffic differentiation handling and the IP Security solutions in the IS

Target audience

The target audience for this course is: Network Design Engineers, Network Deployment Engineers, System Technicians, System Engineers, Field Technicians, System Administrators, Application Developers, Business Developers, Customer Care Administrators.

This is the fundamental course for IS training. It forms the basis for all other courses related to the Integrated Site and is intended for anyone who needs an introduction to the Integrated Site concept.

Prerequisites

The students should have a basic understanding of the network architecture for the fixed and mobile core networks. Furthermore knowledge of datacom in general and more specifically in TCP/IP is desirable.

Duration and class size

The length of the course is 1 day and the maximum number of participants is 16.

Learning situation

Instructor Led Training (ILT). This course is based on theoretical instructor-led lessons.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate.

Day	Topics in the course	Estimated time
1	<ul style="list-style-type: none">• Introduction	80 min
	<ul style="list-style-type: none">• IS Solution Scenarios	30 min
	<ul style="list-style-type: none">• IS Equipment View	70 min
	<ul style="list-style-type: none">• IS System View	30 min
	<ul style="list-style-type: none">• IS Management View	30 min
	<ul style="list-style-type: none">• IS Network View	60 min
	<ul style="list-style-type: none">• IS Security View	10 min
	<ul style="list-style-type: none">• Conclusion	10 min

IS Operation and Configuration



LZU 108 6832

Description

This course provides participants with the skills and knowledge needed for managing an IS domain by exploring the elements involved in operation and maintenance and network configuration. This includes fault management, network management, hardware and software management of the IS infrastructure. Each task is complemented by practical exercises on a real IS. Participants will complete practical site management exercises using on-line documentation and the IS Management Interfaces. During the network configuration part of the training, the participants will work hands-on with configuration of the EXB, ISER and L3X blade systems.

Learning objectives

On completion of this course the participants will be able to:

- 1 Connect and handle the recommended infrastructure management interfaces
 - 1.1 Describe the IS management user interfaces (CLI, ISM-GUI and CMF-UI)
 - 1.2 Connect to SIS (ISM) to execute O&M tasks
 - 1.3 Connect to ISER, EXB and L3X to execute O&M tasks

- 2 Manage Users and Accounts
 - 2.1 Handle user accounts, access permissions and password settings in the ISM
 - 2.2 Handle access permissions and password settings in the ISER

- 3 Network management
 - 3.1 Verify the configuration of SIS, MXB, EXB, ISER and L3X
 - 3.2 Verify defined IS and BS Logical Networks, Subnets, Subnet Segments and VLANs
 - 3.2 Check the state of virtual routers
 - 3.2 Check the routing table in Virtual Routers (VR)
 - 3.2 Find destination availability using trace command
 - 3.2 Verify the state of logical and physical IP interfaces in the ISER
 - 3.2 Verify the VR redundancy
 - 3.2 Check the routing table in the L3X
 - 3.2 Verify the state of logical and physical IP interfaces in the L3X

- 4 Manage blade system log files
 - 4.1 View and Transfer BS log files

- 5 Software Management
 - 5.1 Understand the difference between a software group (swg) and a software delivery package, blade swg and BS swg
 - 5.2 Download and install new software
 - 5.3 Upgrade software
 - 5.4 Create and restore a blade system backup and site backup
 - 5.5 Keep track of installed software (software version control)

6 Hardware Management

- 6.1 Lock and unlock blades and blade systems
- 6.2 View installed hardware in the ISM-GUI (sub-racks, blade systems and blades)
- 6.3 Check valid blade types in the ISM-GUI
- 6.4 Transfer a copy of the Hardware Inventory to a remote location
- 6.5 Create new blade systems and add/delete blades to/from a blade system
- 6.6 Replace a faulty blade
- 6.7 Be familiar with visual indicators on the boards
- 6.8 Manage multi-sub rack connections

7 Detect faults and act on them

- 7.1 Monitor the IS in terms of alarm and event notifications
- 7.2 Find relevant information on how alarms are ceased
- 7.3 Understand how alarms are ceased
- 7.4 Transfer Alarm and Event logs
- 7.5 Create user defined Alarm and Event logs

8 Network configuration

- 8.1 Map blade system network requirements to common Integrated Site resources
- 8.2 Describe the purpose of the IS common parameters and BS parameters
- 8.3 Understand how BS parameters are mapped to the IS parameters
- 8.4 Understand the model for interacting entities in the IS
- 8.5 Explain L2 Switching and the use of link aggregation in the IS
- 8.6 Explain the mapping between layer 2 and layer 3
- 8.7 Configure the Northbound interface (SNMP Agent)
- 8.8 Describe the role of Netconf in the IS CMF
- 8.9 Setup CLI and Netconf access to IS
- 8.10 Define logical networks, subnets, subnet segments and VLANs.
- 8.11 Configure L2 switching and LAG
- 8.12 View link aggregation info for the MXB and configure link aggregation for the EXB (create LAGs for the EXB front ports)
- 8.13 Setup port mirroring
- 8.14 Define Virtual Routers and setup routing protocols for virtual routers (including VRRP)
- 8.15 Configure an interface to ISER
- 8.16 Configure static routing in the L3X and ISER
- 8.17 Describe the IPv6 and IPv4 routing implementation in IS
- 8.18 Configure IPSec/IKE for the ISER
- 8.19 Define traffic classes for IS common resources
- 8.20 Configure tunnels and VPN's in the ISER
- 8.21 Handle Diffserv (Differentiated services)
- 8.22 Configure firewall and filtering
- 8.23 Performance management configuration (housekeeping etc.)
- 8.24 Setup multi-sub rack connections
- 8.25 Understand how scripts can be used to simplify site management

Target audience

The target audience for this course is:
System Technicians, System Engineers, Field Technicians.

This course is intended both for internal students and external customers.

Prerequisites

Successful completion of the following courses:

LZU 108 6364 IS Overview

Duration and class size

The length of the course is 4 days and the maximum number of participants is 8.

Learning situation

Instructor Led Training (ILT). This course is based on theoretical instructor-led lessons and practical / hands-on exercises on IS systems.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate.

Day	Topics in the course	Estimated time
1	Theory <ul style="list-style-type: none"> • Introduction • Management Interfaces • Security Management 	2h
1	Exercises <ul style="list-style-type: none"> • Connecting to the SIS (ISM), EXB, ISER and L3X via recommended management interfaces • Using the on-line help documentation • Managing ISM Users and Accounts 	4h
2	Theory <ul style="list-style-type: none"> • Introduction to IS Network Management • Blade System Log Files • Software Management 	2h
2	Exercises <ul style="list-style-type: none"> • Checking the state of virtual routers • ISER log tracing • Viewing and transferring blade system log files • Software installation and upgrade • Creating and restoring backups 	4h
3	Theory <ul style="list-style-type: none"> • Hardware Management • Fault Management 	2h



3	Exercises	4h
	<ul style="list-style-type: none">• Replacing a faulty blade• Creating Blade Systems and Blades• Hardware control (transferring a HW inventory)• Manage alarm and event logs• Locate the cause of the error using available documentation and tools (event and alarm lists)	
4	Theory	2h
	<ul style="list-style-type: none">• Network Configuration	
4	Exercises	4h
	<ul style="list-style-type: none">• Defining logical networks, subnets, subnet segments and VLANs• Creating and configuring virtual routers with OSPF, BGP• Creating and configure tunnels and VPN's in the ISER• Configuring static routing in the L3X and ISER• Defining virtual routers and setting up routing protocols for virtual routers (including VRRP)• Defining link aggregation for the EXB• Defining traffic classes for IS common resources• Setting up multi-sub rack connections• Activating Nothbound SNMP conection• Configuring IPSec and Stateless filtering	

Multi Mediation 5.0 Surveillance for IMS



LZU 1086826 R1A

Description

The IP Multimedia Subsystem gives operators the ability to rapidly add new services to their existing portfolios. Innovative Services require Innovative Infrastructure to support them. Ericsson's Multimediation 5.0 offering simplifies the integration of any application into an existing charging network, while at the same time making it easier to monitor and perform administration on the Front and Business end Interfaces.

Multimediation Surveillance for IMS introduces the participants to the Multimediation System and its component parts. Integration with different IMS nodes and administration of existing IMS configurations are also discussed for both the Online and File and Event Mediation applications.

Learning objectives

On completion of this course the participants will be able to:

- 1 Discuss the role of Multimediation in the IMS Network
 - 1.1 List interfaces between the IMS core and Multimediation
 - 1.2 List interfaces from the Multimediation node to Business systems/Post-Processing Systems

- 2 Differentiate between the roles of Online and File and Event Mediation in an IMS based configuration
 - 2.1 Understand the difference between File and Event Collection activities and Online Front End Interfaces
 - 2.2 Understand the difference between File and Event Distribution and Online back end Interfaces
 - 2.3 Show where Intercom activities between Online and File and Event configurations might be implemented in an IMS configuration

- 3 Supervise the Dataflow through both Online and File and Event Configurations

- 4 Be able to perform basic maintenance on Online and File and Event Systems

- 5 Be able to View Alarms raised by the Multimediation System

Target audience

The target audience for this course is: Service Planning Engineers, Service Design Engineers, Network Design Engineers, Network Deployment Engineers, Service Deployment Engineers, System Technicians, Application Developers.

Prerequisites

The participants should be familiar with Basic Telecoms, Basic UNIX, IMS fundamentals and Charging protocols.



Duration and class size

The length of the course is 2 days and the maximum number of participants is 8.

Learning situation

Multimediation for IMS is a classroom based ILT course with theoretical exercises. The practical material is limited to demonstrations by the instructor.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate.

Day	Topics in the course	Estimated time
1	• Introduction to Multimediation	1 hr 30 mins
	• IMS Fundamentals	1 hr 30 mins
	• Charging in IMS	1 hr 30 mins
	• Multimediation Interfaces to IMS	1 hr 30 mins
2	• Processing Activities in Multimediation	1 hr 30 mins
	• Dataflow Supervision	1 hr 30 mins
	• Alarm Handling	1 hr 30 mins
	• Summary	1 hr 30 mins

Multi Mediation 5.0 Processing and Configuration for IMS



LZU 108 6827 R1A

Description

The IP Multimedia Subsystem has given operators with the ability to deliver a myriad of new services to their subscribers. In this new environment it has become more important than ever to be able to quickly integrate new features into the existing portfolio of offered applications, while allowing customers to maintain accurate spending control.

Ericsson's Multimediation platform provides a method of quickly integrating these new applications into an existing charging system, using real time, event driven or DR based configurations. The Multimediation 5.0 Processing and Configuration for IMS course provides the participants with the skills necessary to create configurations and supervise processing operations with confidence.

Learning objectives

On completion of this course the participants will be able to:

- 1 Understand the relationship between the IMS Core, Multimediation and Post Processing Systems.
 - 1.1 List IMS core components and the charging/billing information that they may produce
 - 1.2 Be able to configure File and Event collector activities to receive information from IMS nodes
 - 1.3 Be able to configure Online front end interfaces to collect charging data from any serving applications in the IMS network
 - 1.4 Use back end interfaces, Intercom activities and distribution activities to send information from the mediator to any post processing systems.

- 2 Be able to distinguish between charging protocols used in IMS
 - 2.1 Interpret and Edit existing and new data structures used in IMS activities
 - 2.2 Implement formatting activities to modify data structures in DUP
 - 2.3 Make further changes to formatting activities to add and remove charging information from data events in the system using XML or Java
 - 2.4 Create Value Router activities in configurations using DUP, XML and Java based on specifications

- 3 Create external connections from the mediation system for alarm handling
- 4 Examine and Act on Alarms that have been raised by events or the environment.

Target audience

The target audience for this course is: Service Planning Engineers, Service Design Engineers, Network Design Engineers, Network Deployment Engineers, Service Deployment Engineers, System Technicians, Application Developers.

This audience is responsible for configuration & administration of existing or new Multimediation Systems, Charging System or the IMS core.

Prerequisites

The participants should be familiar with Telecoms Principals, IMS Core Activities, Provisioning in IMS, Charging Data Handling, Charging and IMS Protocols, UNIX, Oracle.

Duration and class size

The length of the course is 3 days and the maximum number of participants is 8.

Learning situation

The course is a classroom based ILT course. There is a large practical component undertaken by the students. Access to File & Event and Online mediation systems is required.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate. (This paragraph is mandatory).

Day	Topics in the course	Estimated time
1	• Multimediation and IMS overview	1 hr 20 mins
	• Multimediation Interfaces	1 hr 10 mins
	• Implementing Intercom Activities	1 hr 10 mins
	• Data Structures	1 hr 10 mins
	• Charging Protocols	1 hr 10 mins
2	• F & E Overview	1 hr 30 mins
	• Formatters	1 hr 30 mins
	• Value Routers	1 hr 30 mins
	• Optional Features	1 hr 30 mins
3	• Online Overview	1 hr 30 mins
	• Processing Nodes	1 hr 30 mins
	• Supervision of the Data Flow	1 hr 30 mins
	• Maintenance of the Server	1 hr 30 mins

MN-OSS System Administration for IMS



LZU 108 6829

Description

This course will give the student knowledge about administration of the MN-OSS system used in IMS networks.

After the course the students will be able to handle the standard maintenance of an up-and-running system.

The focus in the course is on the MN-OSS UNIX platform and the student will gain thorough knowledge about how to handle processes, errors and authority in the MN-OSS system. The course also covers fault management and network element connections.

Learning objectives

- 1 Describe the overall structure of an MN-OSS system.
 - 1.1 Describe the role that MN-OSS plays in supporting an IMS network
 - 1.2 Describe the MN-OSS architecture
 - 1.3 Describe how the MN-OSS is located in the IMS network
 - 1.4 Use the online documentation to find out how to perform system administrator tasks

- 2 Handle Authority Administration in the MN-OSS system
 - 2.1 Add new users to the MN-OSS system
 - 2.2 Describe the structure of the Administrative Model
 - 2.3 Use TSS Authority Administration GUI and CLI to administer users, targets and activities
 - 2.4 Use TSS Password Administration CLI
 - 2.5 Use BASE Security

- 3 Manage the MN-OSS processes and error logs
 - 3.1 Describe the structure of CIF and the services it provides
 - 3.2 Describe the Managed Component (MC) Concept
 - 3.3 Use the CIF Management Console to manage MCs
 - 3.4 View CIF error log messages
 - 3.5 Use CIF's command line interface

- 4 Use and describe the main components in the fault management system
 - 4.1 Describe the flow of alarms from network elements to the alarm viewer applications
 - 4.2 Configure the alarm viewer applications

- 5.1 Manage Network Element Connections
 - 5.2 Add Network Element:
 - 5.3 Use Add Remove Network Element (ARNE)
 - 5.4 Describe the parts of the system modified by changes in ARNE
 - 5.5 Establish connection to an IMS network



- 6 Perform standard maintenance in the MN-OSS system
- 6.1 Perform platform maintenance
- 6.2 Handle the scripts scheduled in the crontab
- 6.3 Understand MN-OSS backup and restore procedures
- 6.4 Know the location of all vital log files

Target audience

The target audience for this course is: System Engineer.
This audience is performs standard and corrective maintenance in the system.

Prerequisites

The participant would benefit from equivalent knowledge to the following external courses:

Sybase: Fast track to Adaptive Server Enterprise

Sun: Solaris System Administration I and II

The participants would also benefit from being familiar with Veritas Volume Management and have general knowledge of TCP/IP and SNMP.

Duration and class size

The length of the course is 5 days and the maximum number of participants is 8

Learning situation

The course consists practical sessions (task-oriented) but there will also be theoretical parts. The students will solve the tasks on a training system, using the on-line documentation. The tasks are always concluded by an instructor lead discussion.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate.

Day	Topics in the course
1	<ul style="list-style-type: none">• System administration introduction
1-2	<ul style="list-style-type: none">• User Administration
2-3	<ul style="list-style-type: none">• Process management
3-4	<ul style="list-style-type: none">• Handling Network Element
5	<ul style="list-style-type: none">• Regular Maintenance & Backup and Restore



OSS RC System Administration for IMS



LZU 108 6828

Description

This course will give the student knowledge about administration of the OSS RC system used in IMS networks.

After the course the students will be able to handle the standard maintenance of an up-and-running system.

The focus in the course is on the OSS RC UNIX platform and the student will gain thorough knowledge about how to handle processes, errors and authority in the OSS RC system. The course also covers fault management and network element connections.

Learning objectives

On completion of this course the participants will be able to:

- 1 Describe the overall structure of an OSS RC system.
 - 1.1 Describe the role that OSS RC plays in supporting an IMS network
 - 1.2 Describe the OSS RC architecture
 - 1.3 Describe how the OSS RC is located in the IMS network
 - 1.4 Use the online documentation to find out how to perform system administrator tasks

- 2 Handle Authority Administration in the OSS RC system
 - 2.1 Add new users to the OSS RC system
 - 2.2 Describe the structure of the Administrative Model
 - 2.3 Use TSS Authority Administration GUI and CLI to administer users, targets and activities
 - 2.4 Use TSS Password Administration CLI
 - 2.5 Use BASE Security

- 3 Manage the OSS RC processes and error logs
 - 3.1 Describe the structure of CIF and the services it provides
 - 3.2 Describe the Managed Component (MC) Concept
 - 3.3 Use the CIF Management Console to manage MCs
 - 3.4 View CIF error log messages
 - 3.5 Use CIF's command line interface

- 4 Use and describe the main components in the fault management system
 - 4.1 Describe the flow of alarms from network elements to the alarm viewer applications
 - 4.2 Configure the alarm viewer applications

- 5 Manage Network Element Connections
 - 5.1 Add Network Element:
 - 5.2 Use Add Remove Network Element (ARNE)
 - 5.3 Describe the parts of the system modified by changes in ARNE
 - 5.4 Establish connection to an IMS network



- 6 Perform standard maintenance in the OSS RC system
- 6.1 Perform platform maintenance
- 6.2 Handle the scripts scheduled in the crontab
- 6.3 Understand OSS RC backup and restore procedures
- 6.4 Know the location of all vital log files

Target audience

The target audience for this course is: System Engineer.
This audience is performs standard and corrective maintenance in the system.

Prerequisites

The participant would benefit from equivalent knowledge to the following external courses:

Sybase: Fast track to Adaptive Server Enterprise

Sun: Solaris System Administration I and II

The participants would also benefit from being familiar with Veritas Volume Management and have general knowledge of TCP/IP and SNMP.

Duration and class size

The length of the course is 5 days and the maximum number of participants is 8

Learning situation

The course consists practical sessions (task-oriented) but there will also be theoretical parts. The students will solve the tasks on a training system, using the on-line documentation. The tasks are always concluded by an instructor lead discussion.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate.

Day	Topics in the course
1	<ul style="list-style-type: none">• System administration introduction
1-2	<ul style="list-style-type: none">• User Administration
2-3	<ul style="list-style-type: none">• Process management
3-4	<ul style="list-style-type: none">• Handling Network Element
5	<ul style="list-style-type: none">• Regular Maintenance & Backup and Restore

HSS 4.0 Operation & Configuration



LZU 108 2082

Description

This course will provide the participants with the knowledge to perform Surveillance, Operation and Configuration activities on the HSS Node.

It will provide practice using the procedures necessary to keep the node functioning and to be able to perform Network expansions.

Learning objectives

On completion of this course the participants will be able to:

- 1 Perform surveillance tasks on the HSS
 - 1.1 Explain the HSS Node interworking and protocols.
 - 1.2 Explain the alarms connected to the HSS
 - 1.3 Navigate the Element Manager and use APIs, in order to perform basic status checks of the nodes and interfaces
 - 1.4 Fetch and understand relevant logs for the HSS
 - 1.5 Perform node backup of the HSS

- 2 Explain how to configure the HSS in a secure and redundant way.
 - 2.1 Explain how node hardening is achieved for the HSS
 - 2.2 Explain parameters in the HSS that are important for security

- 3 Configure and verify the HSS Interworking interfaces and parameters
 - 3.1 Configure and verify the Cx interface between CSCF & HSS
 - 3.2 Configure and verify Service Profiles containing triggers in HSS
 - 3.3 Configure Charging Profiles in HSS

- 4 Perform root cause analysis of faults in the HSS
 - 4.1 Relate IMS end-to-end session faults to faulty parameter settings in the HSS
 - 4.2 Resolve alarms related to HSS faults
 - 4.3 Use signal traces in order to localize HSS end-to-end faults
 - 4.4 Find and solve faults in HSS related to subscriber provisioning

- 5 Handle Performance management for the HSS
 - 5.1 Explain how to monitor the performance of the HSS
 - 5.2 Configure and verify HSS measurements



Target audience

Customer System Engineers and Ericsson Personnel working with operation and configuration of the HSS 4.0 for IMS 4.0

Prerequisites

LZU 108 6563 R2A IMS 4.0 Overview

LZU 108 6443 R2B/1 TSP 5 Operation and Maintenance

LZU 108 2078 IMT 3.0 End to End Session Establishment or LZU 108 2088 Mobile IMS 4.0 End to End Session Establishment

LZU 108 2079 IMT 3.0 Provisioning or LZU 108 2089 Mobile IMS 4.0 Provisioning

Duration and class size

The length of the course is 3 days and the maximum number of participants is 6.

Learning situation

The course is based on theoretical and practical instructor-led lessons given in a classroom environment

CSCF 4.0 Operation & Configuration



LZU 108 2083

Description

This course will provide the participants with the knowledge to perform Surveillance, Operation and Configuration activities on the CSCF Node.

It will provide practice using the procedures necessary to keep the node functioning and to be able to perform Network expansions.

Learning objectives

On completion of this course the participants will be able to:

- 1 Perform surveillance tasks on the CSCF
 - 1.1 Explain the CSCF Node interworking and protocols.
 - 1.2 Explain the alarms connected to the CSCF
 - 1.3 Navigate the Element Manager and use CPIs, in order to perform basic status checks of the nodes and interfaces
 - 1.4 Fetch and understand relevant logs for CSCF
 - 1.5 Perform node backup of the CSCF

- 2 Explain how to configure CSCF in a secure and redundant way.
 - 2.1 Explain how TSP network redundancy is used for CSCF
 - 2.2 Explain how CSCF makes use of the DNS/ENUM Active Select function
 - 2.3 Explain how node hardening is achieved for CSCF
 - 2.4 Explain parameters in CSCF that are important for security

- 3 Configure and verify the CSCF Interworking interfaces and parameters
 - 3.1 Configure and verify the Cx interface between CSCF & HSS
 - 3.2 Configure and verify the Rf interface between CSCF and Multi Mediation
 - 3.3 Configure and verify the interface between CSCF and the DNS/ENUM
 - 3.4 Configure and verify the ISC interface between CSCF and the Application Servers
 - 3.5 Configure and verify the Number Normalization tables in CSCF
 - 3.6 Configure and verify the External Network Selection Tables in CSCF

- 4 Perform root cause analysis of faults in the CSCF
 - 4.1 Relate IMS end-to-end session faults to faulty parameter settings in the CSCF
 - 4.2 Resolve alarms related to CSCF faults
 - 4.3 Use signal traces in order to localize CSCF end-to-end faults

- 5 Handle Performance management for CSCF
 - 5.1 Explain how to monitor the performance of the CSCF
 - 5.2 Configure and verify CSCF measurements



Target audience

Customer System Engineers and Ericsson Personnel working with operation and configuration of the CSCF 4.0 for IMS 4.0

Prerequisites

LZU 108 6563 R2A IMS 4.0 Overview

LZU 108 6443 R2B/1 TSP 5 Operation and Maintenance

LZU 108 2078 IMT 3.0 End to End Session Establishment or LZU 108 2088 Mobile IMS 4.0 End to End Session Establishment

LZU 108 2079 IMT 3.0 Provisioning or LZU 108 2089 Mobile IMS 4.0 Provisioning

Duration and class size

The length of the course is 3 days and the maximum number of participants is 6.

Learning situation

The course is based on theoretical and practical instructor-led lessons given in a classroom environment.



IPWorks 4.2 Operation and Configuration for IMS



LZU 108 2084 R1A

Description

Have you decided to implement the IMT 3.0 or Mobile IMS 4.0 solution? Do you require training to know how to supervise IPWorks in your network?

With the help of IPWorks overview training and the guidance of the instructors, the attendees can achieve a thorough understanding of the terminology of DNS services. The course is targeted to those with minimal DNS experience. In the course the attendees will learn how to work with the IPWorks interfaces. The course will also give the participants an understanding of the requirements for DNS in an IMS environment. The course will also provide the attendees with knowledge of fault, node and performance management. Attendees will learn the skills necessary to deploy, configure and manage DNS service using IPWorks. An emphasis is made on developing and understanding of IPWorks as a management tool so students can develop their own procedures for supporting and using IPWorks. The course will also discuss the security aspects for IPWorks. Attendees will learn the skills necessary to handle faults in IPWorks.

Learning objectives

On completion of this course the participants will be able to:

- 1 Describe the purpose of IPWorks
 - 1.1 Introduce and explain Domain Name System (DNS)
 - 1.2 Describe a simple SIP session and the involvement of IPWorks
 - 1.3 List some of the basic records used by IPWorks on IMS
 - 1.4 Present the purpose of IPWorks in IMS

- 2 Describe the architecture of IPWorks
 - 2.1 List and describe the components of the IPWorks 4.2 architecture

- 3 Work with IPWorks interfaces:
 - 3.1 Control Panel
 - 3.2 Graphical User Interface
 - 3.3 Command Line Interface
 - 3.4 Look at alarms and make log settings
 - 3.5 Make backups and restore
 - 3.6 Dump and view statistics

- 4 Perform Configuration Management
 - 4.1 Add, modify and delete records
 - 4.2 Configure and verify the node interfaces

- 5 Handle IPWorks Security aspects

- 6 Troubleshoot and locate common problems for IPWorks



Target audience

The target audience for this course is: Service Planning Engineers, Service Design Engineers, Network Design Engineers, Network Deployment Engineers, Service Deployment Engineers, System Technicians, Service Technicians, System Engineers, Service Engineers, Field Technicians, System Administrators.

This audience is responsible for configuration of IPWorks.

Prerequisites

The participants should be familiar with IMS or Successful completion of the following courses:

IMT 3.0 Overview LZU1082055

Mobile IMS 4.0 Overview LZU1082054

Duration and class size

The length of the course is 2 days and the maximum number of participants is 8.

Learning situation

The course is based on instructor-led theory and practical instructor-led task oriented lessons given in the classroom using equipment.



Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate. (This paragraph is mandatory).

Day	Topics in the course	Estimated time
1	• Describe the purpose of IPWorks	1
	• Describe the architecture of IPWorks	1
	• Work with IPWorks interfaces:	1
	• Exercises	1
	• Look at alarms and make log settings	0,5
	• Exercises	0,5
	• Make backups and restore	0,5
	• Exercises	0,5
	• Dump and view statistics	0,5
	• Exercises	0,5
	2	• Perform Configuration Management
• Exercises		2
• Handle IPWorks Security aspects		0,5
• Exercises		1
• Trouble shoot and locate common problems for IPWorks		0,5
• Exercises		2



OSS Fault Management Tools for IMS



LZU 108 2081 R1A

Description

Are you implementing IMS in your network? Are you facing the challenges of understanding how to operate it?

This course will provide the participants with the knowledge to perform alarm handling activities on the IMS system. It will provide practice using the procedures in the Operation Support System (OSS).

Learning objectives

- 1 Use MN-OSS Fault Management tools.
- 2 Briefly describe OSS.
- 3 Perform Customer Product Information (CPI) searches.
- 4 Use Alarm Status Matrix (ASM) to monitor the status of all connected network elements.
- 5 Alarm List Viewer (ALV) to display and manage alarms from individual network elements.
- 6 Use the Alarm Log Browser (ALB) to search the Alarm Log for specific alarms and to gather alarm statistics.

Target audience

The target audience for this course is: System Engineers and Service Engineers.
This audience is responsible for Back Office or 2nd line support.

Prerequisites

Successful completion of the following courses:

IMS Overview LZU 108 2055

Duration and class size

The length of the course is 1 day and the maximum number of participants is 8.



Learning situation

This course is based on theoretical and practical instructor-led lessons given in both classroom and in a technical environment using equipment and tools, which could be accessed remotely.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate.

Day	Topics in the course	Estimated time
1	<ul style="list-style-type: none">Use the OSS fault management tools	6 hours



SBG 1.2 Operation and Configuration for IMS



LZU 108 2085 R1A

Description

Concerned about security of your IMS network? Wanted to know what SBG can offer? Without SBG, your IMS network is vulnerable to attack from both internally and externally. This course will help you to understand the importance of SBG in IMS network. It will also cover operational aspect and configuration so that you can operate and configure SBG in your network.

Learning objectives

On completion of this course the participants will be able to:

- 1 Describe the Node interworking and protocols
 - 1.1 Understand the position of SBG in IMS network
 - 1.2 Describe basic features and functions of SBG
 - 1.3 Know the different of A-SBG and N-SBG

- 2 Describe the alarms connected to the node
 - 2.1 Understand how the alarms are generated in SBG

- 3 Navigate the element manager and use APIs, in order to perform basic status checks of nodes and interfaces
 - 3.1 Check the status of SBG

- 4 Perform Node backup and Restore
 - 4.1 Perform SBG backup
 - 4.2 Understand SBG restore process

- 5 Be able to fetch and understand relevant logs for the node
 - 5.1 Understand logging mechanism in SBG
 - 5.2 Retrieve and transfer SBG logs

- 6 Monitor the performance of the node
 - 6.1 Retrieve various statistics related to SBG

- 7 Configure and verify the SBG Interworking interfaces
 - 7.1 Configure SBG towards IMS core
 - 7.2 Configure SBG towards Access/Other Network

- 8 Perform root cause analysis of fault by examining alarms and events in the SBG
 - 8.1 Identify, Analyze and Solve SBG related problem

- 9 Set up and analyze measurement for SBG
 - 9.1 Activate related SBG measurement and analyze the result

- 10 Understand how to configure a secure and redundant SBG
- 11 Look at measures taken to perform SBG node hardening



Target audience

The target audience for this course is: Service Planning Engineers, Service Design Engineers, Network Design Engineers, Network Deployment Engineers, Service Deployment Engineers, System Engineers, Service Engineers and System Administrators.

This audience is responsible for operation and configuration of the SBG.

Prerequisites

Successful completion of the following courses:

- IMS Overview LZU 108 6563
- IMS Signaling LZU 108 6604
- Integrated Site Overview LZU 108 6364
- Intergrated Site Operationd and Configuration LZU 108 6832

Duration and class size

The length of the course is 3 days and the maximum number of participants is 6.

Learning situation

The course is based on the theoretical and practical instructor-led lessons given in a classroom environment.



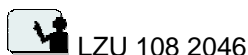
Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate.

Day	Topics in the course	Estimated time
1	• Introduction	½ hr
	• Architecture	1 ½ hr
	• User Interface	1 hr
	• Node Management	1 hr
	• Fault Management	1 hr
	• SBG Logs	½ hr
	• Performance Management	½ hr
2	• SBG Configuration	1 day
3	• Alarms and Events analysis	2 hr
	• SBG measurement analysis	2 hr
	• SBG Node Hardening	2 hr



IMT 3.0 PSTN GW Configuration



Description

This course provides Ericsson customers with the competence needed to perform the configuration of the IMT 3.0 PSTN Gateway.

The course consists of theory and case based exercises on how to configure the IMT 3.0 PSTN Gateway on the Media Gateway Controller (MGC) and Media Gateway (AXD 301) platforms. The traffic and signaling interfaces in IMT 3.0 PSTN Gateway will be covered.

Learning objectives

On completion of this course the participants will be able to:

- 1 Explain how the PSTN GW is used in the IMT 3.0 Network.
- 2 Outline the main components used in the IMT 3.0 PSTN Gateway Network
- 3 Outline the signaling interfaces of IMT 3.0 PSTN Gateway
- 4 Understand the different concepts and terms used in IMT 3.0 PSTN Gateway
- 5 Explain the HW needed to implement the IMT 3.0 PSTN GW.
- 5.1 Understand the HW required for the MGC and the MGW when implementing IMT 3.0 PSTN GW
- 6 Describe High Availability in MGC (HA-MGC)
- 7 Outline the Element Managers for MGC and MGW
- 8 Configure and verify the MGW IP interface used for traffic towards the IP core NW.
- 9 Configure the IP interface in the MGW
- 10 Configure SCTP interface in the MGW
- 11 Create Static Routes in the MGW
- 12 Configure and verify the MGW function in both AXD 301 and MGC.
- 13 Configure a new MGW in the Network
- 14 Configure and verify H.248 Signaling Links
- 15 Configure interface-related MGW IP address
- 16 Configure and Verify the SS7 Network.
- 17 Configure the SS7 network in MGC
- 18 Verify the State of the SS7 Network in MGC
- 19 Configure and verify an ISUP access connected towards the IMT 3.0 PSTN GW
- 20 Configure and verify an ISUP access towards a MGW
- 21 B-Number Analysis
- 22 Verify the B-Number Analysis Configuration in MGC
- 23 Verify SIP Configuration in MGC
- 24 Call Path Tracing and Alarms.
- 25 Perform call path tracing in the MGW
- 26 Verify the main alarms in the PSTN GW Network (MGC and MGW)

Target audience

The target audience for this course is: System Engineer, Network Deployment Engineer.

This audience is working with implementation, installation, testing, integration, operation and support tasks on the IMT 3.0 network.



Prerequisites

Successful completion of the following courses:

IMS Overview (LZU 108 6563) (or equivalent knowledge).

AXD 301/305 7.1 Maintenance (LZU 108 6130) (or equivalent knowledge)

Duration and class size

The length of the course is 3 days and the maximum number of participants is 8

Learning situation

This course is based on theoretical and practical instructor-led lessons given in both classroom and in a technical environment using equipment and tools, which could be accessed remotely.



IMS Common System (ICS) 4.0 Network Surveillance Structured Knowledge Transfer (SKT)



LZP 101 032

Description

IMS is a complex and competence-demanding area. Most IMS implementations are unique and highly customized. **Training should therefore be tailored to the operator's special needs.**

The Delivery of a SKT program follows four phases: Competence Gap Analysis (CGA), Build, Deliver and Evaluate

In the Competence Gap Analysis (CGA), skills and competence gap analysis will be performed in order to outline an SKT program. Gaps for each group and/or individual will be identified. A suggested training solution is then outlined.

The IMS Common System (ICS) 4.0 Network Surveillance SKT is designed to accelerate learning and deliver competence to participants in a short time. Technicians gain a thorough understanding of their roles and responsibilities while operating and maintaining their Mobile IMS network.

Learning objectives

On completion of the IMS Common System (ICS) 4.0 Network Surveillance SKT, the participants will be able to:

Main objectives

- 1 Explain the network topology and corresponding functionalities of the nodes including HSS, CSCF, SBG, DNS/ENUM (IPWorks), EMA, MultiMediation (MM), OSS, MGC and MGW
- 2 Examine and acknowledge alarms and events, handle alarm and event logs and escalate alarms and events according to customer procedures including HSS, CSCF, SBG, DNS/ENUM (IPWorks), EMA, MultiMediation (MM), OSS, MGC and MGW
- 3 Perform preventive maintenance including HSS, CSCF, SBG, DNS/ENUM (IPWorks), EMA, MultiMediation (MM), OSS, MGC and MGW
 - o system backup and restore,
 - o basic status checks of hardware, software and traffic interfaces,
 - o monitor traffic load levels
- 4 Collect and export statistics
- 5 Provision subscribers including assigning of services

Detailed Learning objectives

The main objectives will be broken down to detailed tasks during the CGA phase.



Target audience

The target audience for this training is Technicians responsible for IMS network first line operation and maintenance.

Prerequisites

The pre-requisites are included in the CGA report. Prerequisites would typically be:

- 6 IMS Overview Training Flow
- 7 IP Fundamentals Training Flow
- 8 Ericsson IMS Platform Training Flows
- 9 GPRS Knowledge (in case of Mobile-IMS)

Duration and group size

The length of the training is typically 5 days.

Adjustments can be done according to the findings from the CGA.

For SKT deliveries the minimum number of participants is two (2), and the maximum number of participants is four (4).

Learning situation

- Structured Knowledge Transfer (SKT) is a process to build customer-employee competence by using Ericsson Mentors to discuss, perform, practice and confirm successful employee performance. The training is mentor-led using the customer's network. The mentor presents, demonstrates, and oversees participants performing the tasks agreed.



Time schedule

The time required depends on the outcome of the CGA and the hours stated below can be used as estimate.

Day	Short description of the topics in the course	Estimated time
1	<ul style="list-style-type: none">• Includes introduction to the training and administration of a possible training Pre-assessment	3 hours
1-5	<ul style="list-style-type: none">• Mentor demonstration and participant hands-on performance of tasks identified in the CGA.	6 hours/day
6	<ul style="list-style-type: none">• Mentor administers the possible training Post-assessments. The participants can then view their Pre- and Post-assessments.• Mentor and each participant agree on a development plan possibly based on the result of the Post-assessment.• Participants complete the Final Evaluation form.	6 hours