



Packet Backbone Network Solution

Training Programs

Course Descriptions





Table of Content

ACCESS NETWORKS, AN OVERVIEW	4
ATM ESSENTIALS (MBL).....	6
AXERRA AXN INSTALLATION AND MAINTENANCE	7
AXERRA AXN MULTISERVICE OVER IP	10
CORE NETWORKS, AN OVERVIEW.....	13
CUSTOMER CARE PROFESSIONALISM (2DAYS).....	15
DATACOM NETWORKING	17
ERICSSON AXI 520/580 INTERNET ENGINEER	18
ERX CONFIGURATION WORKSHOP	20
IP NETWORKING	22
IP NETWORKING AND INTERNETWORKING.....	25
IP NETWORK APPLICATIONS.....	27
IPV6 ADVANCED FEATURES.....	29
IPV6 AND TRANSITION FROM IPV4 TO IPV6.....	32
IPV6 AND TRANSITION FROM IPV4 TO IPV6, HANDS-ON.....	34
IPV6 ROUTING PROTOCOLS	37



ISP NETWORK MANAGEMENT	40
ISP ROUTING	41
NETWORKING AND ETHERNET STANDARDS	42
NETWORKING BASICS, AN OVERVIEW	44
NRM OPERATION AND CONFIGURATION	46
PACKET BACKBONE NETWORK ADVANCED VPNS	49
PACKET BACKBONE NETWORK ARCHITECTURE	51
PBN M&T-SERIES ROUTER INSTALLATION AND MAINTENANCE	53
PDM CONFIGURATION AND OPERATION	56
SLM CONFIGURATION AND OPERATION	58
THE COMPLETE TEAM LEADER COURSE	60
UNIX SYSTEM ADMINISTRATION LEVEL 1	62
UNIX FUNDAMENTALS.....	65
VPN & IP SECURITY	67

Access Networks, An Overview

LZU 108 5944 R1A

Description

This course provides a comprehensive introduction to the basic concepts and technologies in both fixed and mobile access networks.

Learning objectives

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

- 1 Understand fixed network connections: access networks
 - 1.1 Outline basic concepts, bandwidth and technologies in access networks
 - 1.2 Describe access based on telephone networks (analogue and digital)
 - 1.3 Outline other access network technologies, such as, cable TV, fiber optics and microwave

- 2 Understand the basic concepts of mobile access
 - 2.1 Outline different mobile access (GSM, GPRS and UMTS)
 - 2.2 Explain GSM architecture and outline a basic traffic case
 - 2.3 Explain GPRS architecture and outline a basic traffic case
 - 2.4 Explain UMTS architecture and outline a basic traffic case
 - 2.5 Define mobile IP for IPv4 and IPv6

Target audience

The target audience for this course is anybody wishing to gain a basic understanding of modern access network technologies.

The course focuses on modern standard technologies and does not contain any Ericsson specific product material.

Prerequisites

There are no prerequisites for this course.

Duration

The length of the course is 2 hours 30 mins.



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	Short description of the topics in the course	Estimated time
1	<ul style="list-style-type: none">• Fixed Network Connections: Access Networks	1 hour
1	<ul style="list-style-type: none">• Connecting While Travelling: Mobile Access	1 hour 30 min

ATM Essentials (MBL)

LZU 108 1459

Description

This course introduces the participants to the fundamentals of ATM.

Objectives

After the course, participants will be able to explain the merging of telecom and datacom, including:

- 1 The meaning and use of ATM and B-ISDN concepts
- 2 How ATM, SDH and PDH interact
- 3 The characteristics of ATM
- 4 The applications of ATM and how ATM is used for the services it supports
- 5 How an ATM network functions.

Target Audience

This course is intended for:

- Technical staff who have little or no experience or familiarity with ATM
- Support staff (training and customer care staff) in organizations where ATM products and services are provided
- Customer Care and Marketing Staff working in telecoms
- Management and other non-technical staff who need an appreciation of the fundamentals of ATM technology

Duration

The length of the course is 7 hours.

Learning situation

Multimedia Based Learning

This is interactive CD-ROM based training that has a high multimedia content including graphics, animations and audio.

Axerra AXN Installation and Maintenance

LZU 108 6075 R1A

Description

This course the necessary training for installation and Field personnel to be able to install, commission and fault diagnose the equipment and features supported in release 1.6.

This is achieved through a hands-on lab that will enable the student to become familiar with the hardware, the base configuration required to bring the node(s) online and identify problems internal or external to the system. An understanding of events and alarms, their significance, effects and the steps required to deal with them will be covered.

Learning objectives

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

- 1 Perform the Installation of a new node
 - 1.1 Perform the installation of a node as described in the Installation and commissioning documentation
 - 1.2 Install the chassis, provide power and earthing. Install cards and Power supply modules
 - 1.3 Understand the various cards, connectivity and functions.
 - 1.4 Verify the unit performs a successful power on.

- 2 Perform the Commissioning of a new node
 - 2.1 Perform the commissioning of a node as described in the Installation and commissioning documentation
 - 2.2 Assign cards, and configure interfaces for management
 - 2.3 Set up the node to a stage where it can be configured locally and the cards will all be assigned and ok without outstanding alarm conditions.

- 3 Bring a node Online
 - 3.1 Bring the node to an online state ready for service provisioning.
 - 3.2 Having successfully completed the physical installation, set up the necessary base configuration and confirm the node as ready for service.

- 4 Identify any hardware problems
 - 4.1 Using the the LED indicators on the cards and the alarm/event list identify any internal erroneous conditions.
 - 4.2 Using the the LED indicators on the cards and the alarm/event list identify any external erroneous conditions.
 - 4.3 Monitor the status and statistics of the interfaces and connections.
 - 4.4 Using the CLI, configure the connections and observe the status, and identify any problems.

- 5 Alarms, Fault and Statistics
- 5.1 Identify problems and their causes using the nodal Alarms, statistics and Performance Monitoring features.
- 5.2 Using the card indicators, the alarm/event table and the syslog identify internal or external conditions.
- 5.3 Under a failure condition, accurately qualify the condition, identify the cause and process in the appropriate manner.

Target audience

The target audience for this course is installation and commissioning, support and maintenance personnel involved with AXN devices.

Prerequisites

There are no prerequisites for this course.

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 to provide representative situations as would be encountered in live deployment.

Ericsson AB

Global Services

SE-164 80 Stockholm

Telephone: +46 8 757 0000

Email: global.services@era.ericsson.se

www.ericsson.com

© Ericsson AB 2003



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	<ul style="list-style-type: none">• Perform Nodal installation	2 hr
1	<ul style="list-style-type: none">• Perform Nodal Commissioning	1 hr
1	<ul style="list-style-type: none">• Bring Node Online	0.5 hr
1	<ul style="list-style-type: none">• Understand card indicators	0.5 hr
1	<ul style="list-style-type: none">• Use status information to identify and resolve faults	2 hr

Axerra AXN Multiservice over IP

LZU 108 6076 R1A

Description

This course provides a thorough understanding of the AXN product range and features as supported in release 1.6.

This is achieved through a comprehensive hands-on lab that will enable the student to fully configure and operate AXN nodes, and offer AXN services as would be required in a live deployment. The various exercises cover all the major features supported.

Learning objectives

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

- 1 List the AXN products and their features, the models within the product range and their capacities
 - 1.1 Understand the feature set and explain where the features would be used
 - 1.2 Choose the correct product for a particular application
- 2 Perform the Installation and Commissioning on a new node
 - 2.1 Perform the installation and commissioning of a node as described in the Installation and commissioning documentation
 - 2.2 Set up the node to a stage where it can be configured locally and the cards will all be assigned and ok without outstanding alarm conditions.
- 3 Bring a node Online
 - 3.1 Bring the node to an online state ready for service provisioning.
 - 3.2 Having successfully completed the physical installation, set up the necessary base configuration and confirm the node as ready for service.
- 4 Create Services on AXN nodes
 - 4.1 Define any of the available services
 - 4.2 Configure the physical/logical interfaces and create a service on these interfaces.
 - 4.3 Monitor the status and statistics of the interfaces and connections.
 - 4.4 Using the CLI, configure the connections and observe the status, and identify any problems.
- 5 Alarms, Fault and Statistics
 - 5.1 Identify problems and their causes using the nodal Alarms, statistics and Performance Monitoring features.
 - 5.2 Under a failure condition, accurately qualify the condition, identify the cause and process in the appropriate manner.

- 6 Resiliency
 - 6.1 Explain the resiliency features
 - 6.2 Decide on the required type and configure using the CLI and check that the resiliency will perform as expected when initiated.

- 7 Handle software and file management
 - 7.1 Explain how upgrades and backups are achieved
 - 7.2 Save configuration files, run scripts and download new releases to and from a FTP server

Target audience

The target audience for this course is system engineers and support and maintenance personnel involved in the installation, commissioning and management of AXN devices.

Prerequisites

It is recommended that the students have successfully completed the following courses:

Introduction to IP Networks, WBL, FAB 102 1313

IP Networking, LZU 102 397

Duration and class size

The length of the course is 2 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 to underpin the example applications.

The training environment replicates a typical Multi-Service over IP network.

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	<ul style="list-style-type: none">• AXN Applications and capacities	1 hr
1	<ul style="list-style-type: none">• Product Range	0.5 hr
1	<ul style="list-style-type: none">• Product Features	2 hr
1	<ul style="list-style-type: none">• AXN Installation and Base Configuration	1.5 hr
1&2	<ul style="list-style-type: none">• AXN Services	3 hr
2	<ul style="list-style-type: none">• AXN Statistics, Alarms and Events	1 hr
2	<ul style="list-style-type: none">• File and Software Management	1 hr
2	<ul style="list-style-type: none">• AXN Resiliency	2 hr

Core Networks, An Overview

LZU 108 5945 R1A

Description

This course provides a comprehensive introduction to the technologies in the core networks, core network architecture and network operation and maintenance.

Learning objectives

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

- 1 Describe the technologies in the core network
 - 1.1 Explain how a physical network is built
 - 1.2 Outline different types of multiplexing (FDM, TDM and WDM)
 - 1.3 Describe transmission technologies such as SDH and SONET
 - 1.4 Describe optical ring architecture and the basics of ATM and MPLS

- 2 Define core network architectures
 - 2.1 Understand traffic trends and outline multiservice backbone requirements
 - 2.2 Explain resource allocation and quality of service
 - 2.3 Understand performance optimization
 - 2.4 Define IPsec and VPN technology

- 3 Understand network operation and maintenance
 - 3.1 Outline steps in network operation
 - 3.2 Understand network traffic and outline some network traffic situations
 - 3.3 Explain monitoring using SNMP and PING
 - 3.4 Define steps and routines for error handling

Target audience

The target audience for this course is anybody wishing to gain a basic understanding of the technologies used in core networks, core network architecture and network operation and maintenance.

The course focuses on modern standard technologies and does not contain any Ericsson specific product material.

Prerequisites

There are no prerequisites for this course.



Duration

The length of the course is 3 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	Short description of the topics in the course	Estimated time
1	<ul style="list-style-type: none">• Technologies in the Core Network	1 hour 15 min
1	<ul style="list-style-type: none">• Core Network Architectures	1 hour
1	<ul style="list-style-type: none">• Network Operation and Maintenance	45 min

Customer Care Professionalism (2days)

LZU 108 3214

Description

This course will help employees in customer care organizations to answer any direct customer inquiry in a correct and professional manner. This course will help our customers to fulfill their goal, regarding “number of inquiries from customers solved at first contact”.

Learning objectives

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

- 1 Answer any direct customer inquiry in a correct and professional manner
- 2 Explain and listen to the customer and assist in the best way possible
- 3 Handle difficult situations - and keep the customer satisfied.

Target audience

The target group has been defined as two different groups:

- Customer Care organizations
- Distributors or Service providers

Prerequisites

There are no prerequisites for this course.

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.



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
	<ul style="list-style-type: none">• Module 1<ul style="list-style-type: none">• Introduction to telecom• Module 2<ul style="list-style-type: none">• Life of a Subscriber• Module 3<ul style="list-style-type: none">• Quality Service and Professionalism• Module 4<ul style="list-style-type: none">• Customer Care Professionalism••••	

Datacom Networking

LZU 102 371

Description

Expert communication knowledge requires a solid foundation in data communications. From standards, physical media and network devices to transmission technologies, protocols, implementation and management this course guides novices effortlessly through modern data communication terminology and technologies and gives a comprehensive overview of underlying networking concepts.

Learning Objectives

General interest in communications technologies and computer literacy is recommended. Having successfully completed this course, students will be able to describe:

- 1 Network Standards
- 2 Physical Media
- 3 LAN and WAN concepts
- 4 Transmission Technologies
- 5 Internet Protocol Suite
- 6 Internetworking

Target Audience

Datacom Networking has been designed for seeking to acquire, refresh or improve knowledge of data technologies. The course is the entry point to Ericsson's datacom classes. This course prepares students for any advanced technology courses and basic product training.

Prerequisites

General interest in communications technologies and computer literacy is recommended.

Duration and class size

The length of the course is 4 days and the maximum number of participants is 16.

Learning situation

This course is based on theoretical instructor-led lessons with study cases given in a classroom environment.

Ericsson AXI 520/580 Internet Engineer

LZU 102 631 R3A

Description

This course will provide the participants with knowledge behind the various routers in the AXI 520/580/590-series. The Ericsson AXI 520/580 Internet Engineer course focuses upon the basic hardware architecture of the series and configuration of JUNOS software version 5.3, including: basic system management, Interior Gateway Protocols, Border Gateway Protocol, routing policy, Multiprotocol Label Switching, firewall filters, and multicast protocols.

Learning objectives

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

- 1 Describe the hardware architecture and installation requirements of the AXI 520/580-series routers
- 2 Describe the JUNOS software architecture and upgrade process
- 3 Describe the JUNOS Command Line Interface and basic configuration
- 4 Configure Interior Gateway Protocols (RIP, OSPF, IS-IS)
- 5 Configure Border Gateway Protocol
- 6 Configure JUNOS Routing Policy
- 7 Configure Multi-protocol Label Switching and RSVP signaling protocol
- 8 Configure JUNOS firewall filters
- 9 Configure JUNOS supported multicast protocols

Target audience

The target audience for this course includes Datacom Engineers, Technicians, and persons responsible for installing, configuring, and maintaining AXI 520/580 routers.

Prerequisites

Successful completion of the following courses/flows:

IP Fundamentals	FAB 101 1314 (or equivalent knowledge)
ISP Routing	LZU 102 325 (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 and tools, which can be accessed remotely. Numerous hands-on configuration exercises reinforce the complex topics presented.

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	<ul style="list-style-type: none"> AXI 520/580-series Hardware Architecture 	1 hr
1	<ul style="list-style-type: none"> AXI 520/580-series Software Architecture 	1 hr
1	<ul style="list-style-type: none"> JUNOS Command Line Interface 	1 hr 30 mins
1	<ul style="list-style-type: none"> AXI 520/580-series Installation and Initial Configuration 	2 hrs
1	<ul style="list-style-type: none"> AXI 520/580-series Interface Troubleshooting 	30 mins
2	<ul style="list-style-type: none"> JUNOS Protocol Independent Routing properties 	1 hr
2	<ul style="list-style-type: none"> Routing Information Protocol 	2 hrs
2	<ul style="list-style-type: none"> JUNOS Routing Policy configuration 	3 hrs
3	<ul style="list-style-type: none"> OSPF Operation, Configuration, and Troubleshooting 	2 hrs
3	<ul style="list-style-type: none"> IS-IS Operation, Configuration, and Troubleshooting 	2 hrs
3	<ul style="list-style-type: none"> BGP Operation, Configuration, and Troubleshooting 	2 hrs
4	<ul style="list-style-type: none"> Traffic Engineering and MPLS Overview 	1 hr
4	<ul style="list-style-type: none"> Static Label Switched Paths 	1 hr
4	<ul style="list-style-type: none"> Signaled LSPs 	2 hrs
4	<ul style="list-style-type: none"> MPLS and Routing Table Integration 	1 hr
4	<ul style="list-style-type: none"> Named-Path and LSP Constraints 	1 hr
5	<ul style="list-style-type: none"> Firewall Filters 	2 hrs
5	<ul style="list-style-type: none"> Multicast Operational Theory 	2 hrs
5	<ul style="list-style-type: none"> Multicast Configuration and Monitoring 	2 hrs

ERX Configuration Workshop

LZU 108 6182 R1A

Description

This workshop will consist of three days of hands-on configuration scenarios to familiarize the students with deploying Juniper E-series (ERX) routers. The students will perform configuration exercises on ERX 1400 and 1440 routers positioned as edge devices on an active Juniper core network. After attending this course students will be able to configure ERX routers as edge aggregation devices in a production network.

Learning objectives

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

- 1 Build a baseline configuration for an ERX router
 - 1.1 Configure passwords, Telnet, and loopback interfaces as the initial steps of installation and node protection
 - 1.2 Configure timing Sources (pri, sec, ter), VRRP, and system Logging for data stream and node protection
- 2 Configure Interfaces for communication with other network nodes
 - 2.1 Configure IP Interfaces and associated physical and logical properties
 - 2.2 Configure ATM Interfaces and associated physical and logical properties
 - 2.3 Configure IP over ATM (Routed 1483), and PPP over ATM
- 3 Enable Routing Protocols
 - 3.1 Configure static routing, RIP, OSPF, and ISIS protocols
- 4 Configure Virtual Routers for separation of customer traffic
- 5 Configure BRAS Functionality
 - 5.1 Configure Routing Policy, Access Control Lists, and Classifier Lists for control and support of remote access users
 - 5.2 Configure Radius Authentication and Rate Limiting for authentication and control of remote access users
- 6 Configure Other Services for customer traffic security
 - 6.1 Configure IPSec Authentication Header and GRE Tunnel Services

Target audience

The target audience for this course is engineers who will install, configure, and support the Juniper Networks E-Series family of routers and the Ericsson IP Service Engine.

Prerequisites

The participants should be familiar with TCP/ IP and routing. This is a hands-on workshop with minimal time devoted to lecture. As such it requires previous hands-on experience with router equipment. Successful completion of the following courses is recommended:

- Introduction to IP Networks, FAB 102 1313
- IP Networking, LZU 102 397

Duration and class size

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

Learning situation

This is a workshop based on interactive training sessions in a technical environment using equipment and tools. Minimal time will be devoted to instructor lecture. The majority of classroom time will be spent configuring ERX routers as edge aggregation devices in a simulated production network with a live internet feed

Time schedule

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

Day	Short description of the topics in the course	Estimated time
1	<ul style="list-style-type: none"> • Workshop Orientation and Hardware Overview 	1 hrs
1	<ul style="list-style-type: none"> • Baseline Configuration 	1 hrs
1	<ul style="list-style-type: none"> • Ethernet Interface Configuration 	2 hrs
1	<ul style="list-style-type: none"> • ATM Interface Configuration 	2 hrs
2	<ul style="list-style-type: none"> • Routing Protocols 	3 hrs
2	<ul style="list-style-type: none"> • Routing Instances / Virtual Routers 	3 hrs
3	<ul style="list-style-type: none"> • BRAS Configuration 	2 hrs
3	<ul style="list-style-type: none"> • IPSec Encryption 	2 hrs
3	<ul style="list-style-type: none"> • GRE Tunnel Configuration 	2 hrs

IP Networking

LZU 102 397 R1A

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 within the TCP / IP suite such as TCP, UDP, ICMP, HTTP, FTP, SMTP, ARP, DNS and DHCP. 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. Throughout the course hands-on labs and analysers are used to pinpoint important aspects of theory sessions.

- 1 Learning objectives
 - 1.1 On completion of this course the participants will be able to:
 - 1.2 Describe IPv4 and IPv6 protocol, addressing and subnetting / aggregation
- 2 Describe the functions of the different bodies involved in IP standards / RFCs
 - 2.1 Describe IPv4 packet structure, protocol header and features
 - 2.2 Describe and perform exercises on IPv4 addresses, CIDR, subnetting and aggregation
 - 2.3 Describe IPv6 packet structure, protocol header, features and the different types of IPv6 addresses
- 3 Describe the purpose and operation of different protocols such as TCP, UDP, ICMP, SMTP, POP3, IMAP, ARP, DNS and DHCP
 - 3.1 Describe the OSI reference model and how it relates to the TCP / IP stack
 - 3.2 Describe the TCP and UDP protocol structures, headers and functionality
 - 3.3 Describe and perform exercises and analysis on the operation of different protocols / applications (ARP, DHCP, DNS, HTTP, FTP, SMTP, POP3, IMAP, etc.)
- 4 Describe the purpose and operation of different network devices and routing protocols used in IP networking
 - 4.1 Describe the operation of Hubs, Bridges and Switches
 - 4.2 Describe and perform exercises and analysis on the operation of Spanning Tree Protocol (STP)
 - 4.3 Describe and perform exercises and analysis on the operation of Static and Dynamic routing protocols
 - 4.4 Describe and perform exercises and analysis on RIP routing protocol
 - 4.5 Describe and perform exercises and analysis on OSPF routing protocol
 - 4.6 Describe IS-IS and BGP routing protocol.



Target audience

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

Prerequisites

The participants should be familiar with Datacom fundamentals and data transmission principles or successful completion of some of the following courses or equivalent:

Datacom Networking - LZU 102 371 – 4 days ILT

And/or

Introduction to IP Networking, WBL – FAB 102 1313

Duration and class size

The length of the course is 4 days and the maximum number of participants is 12.

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.

PCs with Ethernet analysers, hubs and routers are required for practical exercises in the classroom.

One server providing HTTP, FTP, DHCP, DNS, Email (SMTP, POP3, IMAP) and Telnet access for exercises.

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	• Describe the functions of the different bodies involved in IP standards / RFCs	1.0
	• Describe IPv4 packet structure, protocol header and features	1.0
	• Describe IPv4 addresses, CIDR and subnetting and aggregation	1.5
	• Describe IPv6 packet structure, protocol header, features, different types of IPv6 addresses	1.5
	• Perform exercise on IP addressing and subnetting	1.5
2	• Describe the OSI reference model and how it relates to the TCP / IP stack	0.5
	• Describe the TCP and UDP protocol structures, headers and functionality	1.0
	• Describe the operation of different applications (ARP, DHCP, DNS, HTTP, FTP, SMTP, POP3, IMAP, etc.)	2.0
	• Perform exercise on ARP, DHCP, DNS, HTTP, FTP, TFTP, Telnet, SMTP, POP3, IMAP, etc.	3.0
3	• Describe the operation of Hubs, Bridges, Switches, Collision Domains and Broadcast domains	1.0
	• Describe the operation of Spanning Tree Protocol (STP)	1.0
	• Describe the operation of Static and Dynamic routing protocols	1.0
	• Describe RIP routing protocol	1.5
	• Perform exercises and analysis of protocols on Bridges, STP and Static routing	2.0
4	• Describe OSPF routing protocol	1.5
	• Perform exercises and analysis of RIP protocol	1.5
	• Perform exercises and analysis of OSPF protocol (Areas, aggregation, authentication)	2.0
	• Describe the operation of IS-IS and BGP routing protocols	1.5

IP Networking and Internetworking

LZU 108 5942 R1A

Description

This course provides an introduction to the principles of IP networking and internetworking.

Learning objectives

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

- 1 Describe the basic concepts of IP networking
 - 1.1 Define virtual address and explain how to communicate between networks
 - 1.2 Outline the difference between IPv4 and IPv6 addressing
 - 1.3 Outline how to configure the hosts in LAN (IP address, subnet mask, default gateway)
 - 1.4 Understand Internet domains and how the Domain Name System works
 - 1.5 Describe how to leave the local network using a Router
- 2 Describe the basic concepts of IP internetworking
 - 2.1 Describe the Internet (transit, regional and ISP networks)
 - 2.2 Understand routing domains and usage of two routing protocols (RIP and OSPF)
 - 2.3 Discover networks using two useful utilities PING and Traceroute

Target audience

The target audience for this course is anybody wishing to gain a basic understanding of modern datacom networking technologies.

The course focuses on modern standard technologies and does not contain any Ericsson specific product material.

Prerequisites

There are no prerequisites for this course.

Duration

The length of the course is 3 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	Short description of the topics in the course	Estimated time
1	<ul style="list-style-type: none">• IP Networking	2 hours
1	<ul style="list-style-type: none">• IP Internetworking	1 hour

IP Network Applications

LZU 108 5943 R1A

Description

This course provides an introduction to IP network applications and TCP/IP data communications.

Learning objectives

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

- 1 Describe how to use the network and describe IP network applications
 - 1.1 Explain how Internet applications are addressed in a data packet
 - 1.2 Understand application models (Client/Server and Peer-to-Peer)
 - 1.3 Describe how a Web browser works and how Web pages are constructed using HTML
 - 1.4 Explain Web architecture and connecting to a Web server
 - 1.5 Explain how to send and receive Internet E-mail and outline the protocols used
 - 1.6 Understand IP telephony architecture

- 2 Explain the TCP/IP data communications architecture
 - 2.1 Describe TCP/IP layered approach to networking
 - 2.2 List the layers in the TCP/IP protocol stack
 - 2.3 List the Internet organizations (ISOC, IETF and ICANN)
 - 2.4 Explain IP addressing and routing and some important fields in an IP packet
 - 2.5 Outline how the Transmission Control Protocol (TCP) works

Target audience

The target audience for this course is anybody wishing to gain an understanding of IP network applications and TCP/IP data communications.

The course focuses on modern standard technologies and does not contain any Ericsson specific product material.

Prerequisites

There are no prerequisites for this course.

Duration

The length of the course is 3 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	Short description of the topics in the course	Estimated time
1	<ul style="list-style-type: none">• Using the network - IP Network Applications	2 hours
1	<ul style="list-style-type: none">• The TCP/IP Data Communications Architecture	1 hour

IPv6 Advanced Features

LZU 102 797 R1A

Description

This course is a profound technical presentation of the Internet protocol IPv6, Transitions Mechanisms from IPv4 to IPv6 and of the advanced features related to IPv6: QoS (DiffServ, RSVP / IntServ) and IPsec. IPv6 and these features are essential in a 3G/UMTS cellular network.

These subjects will be discussed and related to examples in real life.

The participants will learn how to configure the advanced features on an IPv6 router. Examples of how to configure a host in an IPv6 network will be presented.

Learning objectives

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

- 1 Describe the protocol IPv6 on an advanced level.
- 2 Describe and configure the Transition Mechanisms between IPv4 and IPv6.
- 3 Understand how QoS (DiffServ, RSVP / IntServ) and IPsec are working.
- 4 Configure these mechanisms and features on a router.
- 5 Configure a host in an IPv6 network.

Target audience

The target audience for this course is anyone who needs technical knowledge within this area, such as Network Designers and Network Engineers.

Prerequisites

Successful completion of the following courses:

The flow

IP Fundamentals, FAB 102 1314,

ending with the course

VPN & IP Security, LZU 102 323

Duration and class size

The length of the course is 4 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.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate. Included in the topics are practical exercises.

Day	Short description of the topics in the course	Estimated time
1	<ul style="list-style-type: none"> • Introduction • Welcome • Presentation • Training Schedule 	1 h
	<ul style="list-style-type: none"> • IPv6 and Mobile Internet • Increased Address Space • Built in Security • Quality of Service (QoS) for Real Time Services • Simple Routing for Scalability 	1 h
	<ul style="list-style-type: none"> • IPv6 • IPv6 Header • Address Architecture • Unicast, Multicast and Anycast • Auto-configuration • Neighbor Discovery • ICMPv6Dual Stack Model DNS • DHCP 	6 h
2	<ul style="list-style-type: none"> • QoS • DiffServ • IntServ (RSVP) • MPLS • Policy • Policing • Traffic Conditioning • Metering • Scheduler • Shaper • Queue Management (RED) 	4 h

- | | |
|---|--|
| 3 | <ul style="list-style-type: none"> • IPSec 4 h • Security Threats • Basic Security Concepts • Security Associations • Crypto Primitives • Authentication Header • Encapsulating Security Payload (ESP) • Internet Key Exchange • Deployment |
| 4 | <ul style="list-style-type: none"> • Tunneling 5 h • Introduction • Connecting IPv6 islands • Configured tunnels • IPv6 to IPv4 (6to 4) • ISATAP • Teredo • Other Tunnel Mechanisms • Automatic Tunnels • Tunnel Broker • IPv6 over IPv4 (6over4) • Routing IPv6 on the internet |
| | <ul style="list-style-type: none"> • Translation 3 h • Introduction • DSTM • Header Translation • NAT-PT • FTP-ALG • DNS-ALG • SIIT • BIS • Socks64 • TCP/UDP Relay |

IPv6 and Transition from IPv4 to IPv6

LZU 102 801 R1A

Description

This course gives a profound technical presentation of the Internet protocol IPv6. The course will also discuss different IPv4-IPv6 transition mechanisms.

After this course it will be clear how IPv6 will function in a network and how IPv6 can co-exist with IPv4.

Learning objectives

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

- 1 Describe the protocol IPv6 on an advanced level.
- 2 Describe some of the important Transition Mechanisms between IPv4 and IPv6.
- 3 Get an overview of how the Transition Mechanisms work when setting up an IPv6 network.

Target audience

The target audience for this course is anyone who needs technical knowledge within this area, such as Technicians and Designers.

Prerequisites

Successful completion of the following courses:

The flow

IP Fundamentals, FAB 102 1314,

ending with the course

VPN & IP Security, LZU 102 323

Duration and class size

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

Learning situation

This course is based on theoretical 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	Short description of the topics in the course	Estimated time
1	<ul style="list-style-type: none"> • Introduction • Welcome • Presentation • Training Schedule • Course outline • IPv6 • IPv6 Header • Address Architecture • Unicast, Multicast and Anycast • Auto-configuration • Neighbor Discovery • ICMPv6 • Making an IPv6 NetworkConnecting IPv6 islandsDual Stack Model DNS • DHCP • Transition Mechanisms • Configured tunnels • IPv6 to IPv4 (6to 4) • ISATAP • Teredo • SIIT NAT-PT • Other Transition Mechanisms 	<p>1 h</p> <p>3 h</p> <p>2 h</p>

IPv6 and Transition from IPv4 to IPv6, Hands-on

LZU 102 798 R1A

Description

This course gives a profound technical presentation of the Internet protocol IPv6 and of IPv4-IPv6 Transition Mechanisms. The change from IPv4 to IPv6 will not happen overnight.

The course gives a clear view of how the Transition Mechanisms function and how they are used to establish IPv6 networks in a world of IPv4 networks and to ensure connectivity between different IPv6 networks and between IPv6 and IPv4 networks.

Different challenges, problems and solutions concerning the transition from IPv4 to IPv6 networks will be discussed. The transition mechanisms will be configured in a network.

Learning objectives

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

- 1 Describe the protocol IPv6 on an advanced level.
- 2 Describe and configure the Transition Mechanisms between IPv4 and IPv6.
- 3 Describe how The Transition Mechanisms work when setting up an IPv6 network.
- 4 Set up an IPv6 network configuring routers and hosts.

Target audience

The target audience for this course is anyone who needs technical knowledge within this area, such as Technicians and Designers.

Prerequisites

Successful completion of the following courses:

The flow

IP Fundamentals, FAB 102 1314,

ending with the course

VPN & IP Security, LZU 102 323

Duration and class size

The length of the course is 2 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.

Time schedule

The time required always depends on the knowledge of the attending participants and the hours stated below can be used as estimate. Included in the topics are practical exercises.

Day	Short description of the topics in the course	Estimated time
1	<ul style="list-style-type: none"> • Introduction • Welcome • Presentation • Training Schedule 	1 h
	<ul style="list-style-type: none"> • IPv6 and Mobile Internet • Increased Address Space • Built in Security • Quality of Service (QoS) for Real Time Services • Simple Routing for Scalability 	1 h
	<ul style="list-style-type: none"> • IPv6 • IPv6 Header • Address Architecture • Unicast, Multicast and Anycast • Auto-configuration • Neighbor Discovery • ICMPv6Dual Stack Model DNS • DHCP 	5 h
2	<ul style="list-style-type: none"> • Tunneling • Introduction • Connecting IPv6 islands • Configured tunnels • IPv6 to IPv4 (6to 4) • ISATAP • Teredo • Other Tunnel Mechanisms • Automatic Tunnels • Tunnel Broker • IPv6 over IPv4 (6over4) • Routing IPv6 on the internet 	3 h



- **Translation** 2 h
- Introduction
- DSTM
- Header Translation
- NAT-PT
- FTP-ALG
- DNS-ALG
- SIIT
- BIS
- Socks64
- TCP/UDP Relay

IPv6 Routing Protocols

LZU 102 796 R1A

Description

This course is a profound technical presentation of the routing protocols RIPng, OSPFv3, ISIS and BGP4+. The protocols and their different functions in the Internet will be discussed.

Learning objectives

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

- 1 Know how the Routing Protocols are used in IPv6
- 2 Know how they are working on a router and the hosts of an IPv6 network

Target audience

The target audience for this course is anyone who needs technical knowledge within this area, such as Technicians and Designers.

Prerequisites

Successful completion of the following courses:

The flow

IP Fundamentals, FAB 102 1314,

ending with the course

VPN & IP Security, LZU 102 323

and

IPv6 and Transition from IPv4 to IPv6, Hands-on, LZU 102 798

or

IPv6 and Transition from IPv4 to IPv6, LZU 102 801

Duration and class size

The length of the course is 2 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.

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	<ul style="list-style-type: none"> • Introduction • Welcome • Presentation • Training Schedule 	1 h
	<ul style="list-style-type: none"> • RIPng • The RIPng Header • Distance Vector Algorithm • Hop Counts • Flooding • Counting to Infinity • Reverse Poisoning • Split Horizon 	3 h
	<ul style="list-style-type: none"> • OSPFv3 • The OSPFng Header • Link State Advertisements (LSAs) • The Link-State Database • Hello Packets • Database Synchronization • Flooding • Routing Calculations • SPF Algorithm • External Routing Information • OSPF Areas • OSPF Range • Stub Areas • History • Support on data link layer • Hello packets • Link State packets • Sequence number packets • Options • Level 1 and Level 2 routers • Designated router election • Area reconfiguration • Overload state • Comparison with OSPFv3 	5 h



2

- **ISIS** 1 h
 - History
 - Support on data link layer
 - Hello packets
 - Link State packets
 - Sequence number packets
 - Options
 - Level 1 and Level 2 routers
 - Designated router election
 - Area reconfiguration
 - Overload state
 - Comparison with OSPFv3

- **BGP4+** 2 h
 - The BGP Header
 - BGP Sessions
 - Attributes
 - Keep-Alive Features
 - Internal-External BGP
 - Best Path Calculation
 - Synchronizing with OSPFng
 - Policy Routing – Multi-homing
 - Explosion of routing tables

ISP Network Management

LZU 102 322

Description

This course gives participants a general understanding of Network Management. It discusses the challenges faced by ISPs in converging network technologies. Hands-on network labs using SNMP- based management tools help participants further develop their practical skills.

Learning Objectives

After completing this course, the participant will be able to understand and describe in detail the following technologies and trends:

- 1 Basic Network Management Concepts
- 2 Impact of converging technologies
- 3 SNMP
- 4 MIB
- 5 Integration Reference Points
- 6 ASN.1
- 7 RMON and RMON2
- 8 CMIP
- 9 DEN - Directory Enabled Networks
- 10 CIM
- 11 COPS
- 12 Next generation Network Management

Target Audience

Anyone seeking to refresh or improve the network management knowledge.

Prerequisites

Successful completion of the following courses:

- IP Fundamentals, FAB 102 1314

Duration and class size

The length of the course is 4 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.

ISP Routing

LZU 102 325

Description

This course provides a theoretic background in IS-IS and BGP routing. In extensive hands-on exercises, participants will learn to configure large IP-networks.

Learning Objectives

After completing this course, participants will be able to:

- 1 Understand IS-IS routing and the concepts of the Border Gateway Protocol 4 (BGP4)
- 2 Design IP networks based on IS-IS and BGP 4
- 3 Configure IS-IS and BGP4 routes
- 4 Understand the difference between IS-IS BGP 4, EGP and OSP

Target Audience

This course is primarily designed for network engineers who have to perform IS-IS configuration in IP core networks (AXI 520).

Prerequisites

Successful completion of the following courses:

- IP Fundamentals, FAB 102 1314

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.

Networking and Ethernet Standards

LZU 108 5941 R1A

Description

This course provides a basic introduction to modern LAN and WAN technologies and concepts.

Learning objectives

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

- 1 Describe Local Area Networks (LAN) and the Ethernet Standard
 - 1.1 Define the building blocks in a LAN
 - 1.2 Outline the different types of Ethernet standard
 - 1.3 Explain data transmission in an Ethernet LAN – Ethernet frame
 - 1.4 Understand Ethernet basics (CSMA/CD)
 - 1.5 Outline the difference between a Hub and a Switch
 - 1.6 Describe how to connect communication devices and design a LAN
- 2 Describe Wireless Local Area Networks (WLAN)
 - 2.1 Describe two basic types of Wireless LAN (Ad Hoc and Infrastructure mode)
 - 2.2 Outline the IEEE 802.11 standard and its applications
 - 2.3 Outline the HIPERLAN/2 standard and its applications and compare to IEEE 802.11
 - 2.4 Outline the properties of Home RF
 - 2.5 Understand Bluetooth drivers and communication models

Target audience

The target audience for this course is anybody wishing to gain a basic understanding of modern datacom networking technologies.

The course focuses on modern standard technologies and does not contain any Ericsson specific product material.

Prerequisites

There are no prerequisites for this course.

Duration

The length of the course is 2.5 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	Short description of the topics in the course	Estimated time
1	<ul style="list-style-type: none">• Local Area Networks and the Ethernet Standard	1 hour 15 mins
1	<ul style="list-style-type: none">• Wireless Local Area Networks, WLAN	1 hour 15 mins

Networking Basics, An Overview

LZU 108 5940 R1A

Description

This course provides information on basic networking principles and describes how a PC communicates with other devices and networks.

Learning objectives

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

- 1 Explain the basics of networking
 - 1.1 Outline the input and output devices of a PC and how they are connected
 - 1.2 Describe the communication parameters necessary to understand connections
 - 1.3 Describe physical and logical network topologies
- 2 Describe how to connect a PC to a datacom network
 - 2.1 Identify and describe communication devices in a LAN (Hub, Switch and Router)
 - 2.2 Understand the different types of cables (UTP,STP and Fiber Optical)
 - 2.3 Explain how to connect computers to a LAN
 - 2.4 Explain the difference between Internet and Intranet
 - 2.5 Outline how to implement a Structured Cabling System (independent cabling system)

Target audience

The target audience for this course is anybody wishing to gain a basic understanding of modern datacom networking technologies.

The course focuses on modern standard technologies and does not contain any Ericsson specific product material.

Prerequisites

There are no prerequisites for this course.

Duration

The length of the course is 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	Short description of the topics in the course	Estimated time
1	<ul style="list-style-type: none">• Networking Basics	1 hour
1	<ul style="list-style-type: none">• Your PC and the Datacom Network	1 hour

NRM Operation and Configuration

LZU 102 558 R2A

Description

This course is intended to provide the necessary skills for network operators to use NRM to create, maintain and troubleshoot network element configurations in an IP network.

The course is also intended to give NRM administration skills for system administrators starting to work with NRM.

Learning objectives

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

- 1 Describe the structure of the NRM application
 - 1.1 Describe the NRM architecture and NE requirements
 - 1.2 Describe NRM basic functions and operation
 - 1.3 Describe configuration spaces, configuration generation and rollback options
 - 1.4 Describe the Direct Network Access functions
 - 1.5 Describe the validation function
- 2 Work with configuration management
 - 2.1 Import and edit NE configurations
 - 2.2 Validate NE configurations
 - 2.3 Export NE configurations
 - 2.4 Perform Network Rollback
- 3 Work with the Topology Viewer
 - 3.1 View current and planned network topology
 - 3.2 View node properties
 - 3.3 Use filters to select NE
 - 3.4 Customize views
- 4 Automate network element configuration using NRM wizards
 - 4.1 Describe the wizards that exist in NRM
 - 4.2 Describe NE requirements for NRM wizards
 - 4.3 Configure and use wizards to perform network modifications
- 5 Perform network troubleshooting
 - 5.1 Find and correct configuration errors in the network
- 6 Handle NRM administration
 - 6.1 Describe security options
 - 6.2 Define NRM user types
 - 6.3 Edit the NRM configuration file
 - 6.4 Edit the NE configuration file

- 6.5 Configure authentication
- 6.6 Handle NRM processes
- 6.7 Configure automatic import and validation
- 6.8 Perform troubleshooting

Target audience

The target audience for this course are customers or Ericsson technical personnel who are interested in learning about the core operation of NRM. Emphasis is on hands-on operations.

Prerequisites

Successful completion of the following courses or equivalent knowledge:

IP Networking	LZU 102 397
VPN & IP Security	LZU 102 397
ISP Network Management	LZU 102 322
Packet Backbone Network Architectures	LZU 108 5965

Duration and class size

The length of the course is 2 days and the maximum number of participants is 8. The number of participants is determined by the number of routers available, since each group of two students need access to one router.

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.



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	• Introduction	1 h
	• NRM structure	2 h
	• Configuration Management	3 h
2	• Topology Viewer	2 h
	• Wizards	1 h
	• Troubleshooting	1 h
	• NRM administration	2 h

Packet Backbone Network Advanced VPNs

LZU 108 5986 R2A

Description

This course will provide the participants with in-depth knowledge behind the various Virtual Private Network (VPN) technologies in use within the Packet Backbone Network (PBN) AXI 520/580/590-series routers. The PBN Advanced VPN course focuses upon the configuration of JUNOS software version 5.3, including: draft Kompella and Martini-based Layer 2 VPNs, RFC 2547bis MPLS/BGP Layer 3 VPNs, and advanced Carrier of Carrier and Inter-Provider VPNs.

Learning objectives

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

- 1 Describe the various VPN technologies within the PBN supported by JUNOS software.
 - 1.1 List the software features supporting VPN.
 - 1.2 Explain the use of Multiprotocol BGP
 - 1.3 Explain Routing Information Exchanges
- 2 Describe and configure Layer 2 VPNs supported by JUNOS software
 - 2.1 Explain JUNOS software features supporting Layer 2 VPNs
 - 2.2 Using JUNOS software, configure Layer 2 Circuit VPNs
 - 2.3 Using JUNOS software, configure Layer 2 MPLS/BGP VPNs
- 3 Describe and configure RFC 2547bis MPLS/BGP Layer 3 VPNs
 - 3.1 Explain routing information exchanges
 - 3.2 Using JUNOS software, configure full-mesh Layer 3 MPLS/BGP VPNs
 - 3.3 Using JUNOS software, configure hub-and-spoke Layer 3 MPLS/BGP VPNs
 - 3.4 Using JUNOS software, configure Layer 3 MPLS/BGP VPNs with Internet access
- 4 Describe and configure advanced RFC 2547bis MPLS/BGP Layer 3 VPNs
 - 4.1 Explain routing information in Carrier of Carrier and Inter-Provider topologies
 - 4.2 Using JUNOS software, configure Carrier of Carrier MPLS/BGP Layer 3 VPNs
 - 4.3 Using JUNOS software, configure Inter-Provider MPLS/BGP Layer 3 VPNs
- 5 Identify Tunneled VPNs supported by the AXI 520/580
 - 5.1 Using JUNOS software, configure non-encrypted tunnel VPNs
 - 5.2 Using JUNOS software, configure IPsec encrypted tunnel VPNs

Target audience

The target audience for this course includes Datacom Engineers, Technicians, and persons responsible for installing, implementing, and maintaining Virtual Private Network solutions.

Perequisites

Successful completion of the following flow:

AXI 520/580 Network Configuration (FAY 113 75)

Duration and class size

The length of the course is three days and the maximum number of participants is 10.

Learning situation

This product is an instructor-led course that consists of lectures, group and individual discussions, and numerous hands-on configuration exercises to reinforce the complex topics presented.

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	<ul style="list-style-type: none"> JUNOS VPN features 	1 hr
1	<ul style="list-style-type: none"> JUNOS Layer 2 VPN features 	1 hr
1	<ul style="list-style-type: none"> Layer 2 Circuit Theory and Configuration 	4 hrs
2	<ul style="list-style-type: none"> MPLS/BGP Layer 2 VPN Theory and Configuration 	2 hrs
2	<ul style="list-style-type: none"> MPLS/BGP theory and configuration 	3 hrs
2	<ul style="list-style-type: none"> BGP/MPLS VPNs with Internet Access 	1 hr
3	<ul style="list-style-type: none"> Carrier of Carrier VPN Theory and Configuration 	2 hrs
3	<ul style="list-style-type: none"> Inter-Provider VPN Theory and Configuration 	3 hrs
3	<ul style="list-style-type: none"> Tunneled VPN theory and configuration 	1 hr

Ericsson AB

Global Services
 SE-164 80 Stockholm
 Telephone: +46 8 757 0000
 Email: global.services@era.ericsson.se
www.ericsson.com
 © Ericsson AB 2003

Packet Backbone Network Architecture

LZU 108 5965 R2A

Description

The course PBN Architecture is designed to provide an introduction to the Ericsson solution for Packet Backbone Networks. The solution is based on Ericsson's vision on a horizontal network model with different Network layers for Access & Backbone networking as well as Server layers for control & Service Management.

This course is intended to be a solid foundation for further product specific training relating to the PBN solution.

Learning objectives

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

- 1 Briefly describe the Ericsson PBN solution
 - 1.1 Describe common features of Packet Backbone Networks
 - 1.2 Identify the enhancements the Ericsson PBN 2.3 Solution provides to the standard features.
- 2 Identify the components of the PBN 2.3 solution
 - 2.1 Identify the primary features of the components
 - 2.2 Explain the logical placement of the components
- 3 Describe the management tools implemented within the PBN solution.
 - 3.1 Explain the purpose of NRM, SLM and PDM
- 4 Describe the implementation and future of Packet Backbone Networks

Target audience

The main target audience for this course is:

- Engineers
- Support staff

The course is also intended for:

- Managers
- Sales and marketing staff

Prerequisites

Students should have a basic understanding of the telecommunications and datacommunications industry, including conceptual knowledge of switching, routing, and network management. Examples of a courseflow that would provide these prerequisites are:

- IP Fundamentals, FAB 102 1314

Duration and class size

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

Learning situation

This course is based on theoretical 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	Short description of the topics in the course	Estimated time
1	Course Introduction	30 mins
1	Packet Backbone Networks and the PBN Solution	1 hr
1	PBN Component Nodes	2 hrs
1	PBN Management Tools	1 hr
1	The Future of PBN	1,5 hr

PBN M&T-Series Router Installation and Maintenance

LZU 108 6069 R1A

Description

This course will provide the participants with the knowledge necessary to install M and T-series hardware and create an initial software configuration for the various routers in the M and T-series. The course focuses upon the basic hardware architecture of the series and installation requirements. Basic CLI techniques and interface configuration is also covered.

Learning objectives

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

- 1 Describe the Hardware Architecture of the various routers within the M and T-series routers
 - 1.1 List and Explain major architecture features of M and T-series routers
 - 1.2 Describe the common hardware components of the M and T-series routers
 - 1.3 Explain packet flow through various routers in the M and T-series routers
- 2 List installation requirements for the M and T-series routers
 - 2.1 Identify the location of components on the M and T-series routers
 - 2.2 Describe the environmental and space requirements of the M and T-series routers
 - 2.3 Identify the Power Specifications for various M and T-series routers
- 3 Install the M and T-series router
 - 3.1 Identify tools necessary to install M and T-series routers
 - 3.2 Identify safety guidelines for installing M and T-series routers
 - 3.3 Identify proper installation procedures for installing M and T-series routers
 - 3.4 Identify the boot process and indicators of a proper router boot
 - 3.5 Shutdown the router using the proper procedures
- 4 Describe the JUNOS software architecture
 - 4.1 Identify the operational modes of the CLI
 - 4.2 Navigate within the CLI
 - 4.3 Create an initial configuration for the M-series or T-series router
- 5 Configure and troubleshoot interfaces
 - 5.1 Describe the naming conventions for interfaces on the M and T-series routers
 - 5.2 Configure basic physical parameters on interfaces
 - 5.3 Configure basic logical addressing on interfaces
 - 5.4 Use operational commands to troubleshoot interfaces
- 6 Monitor and maintain the M&T-series routers
 - 6.1 Monitor the router chassis environment using operational commands
 - 6.2 Identify removal operations for various components of the M and T-series routers

- 6.3 Remove and replace various parts of the M and T-series routers
- 7 Upgrade JUNOS software
- 8 Recover lost passwords on the M and T-series router

Target audience

The course is intended for personnel who are in charge of installation and maintenance of the Ericsson M and T-series router. The course also addresses to everyone who needs a basic understanding of the concept and the architecture of the M and T-Series routers.

Prerequisites

The participants should be familiar with basic installation and electrical safety requirements for telecommunication and datacom equipment. In addition it is recommended that the participants have basic knowledge of IP, which could be obtained from Introduction to IP Networks, WBL (FAB 102 1313).

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 lessons and practical exercise that include hands-on demonstration of equipment, if available, and configuration of routes in a remote lab environment. The course is designed to be most effective when held with some equipment to be installed available. If instruction is to be held without equipment available on site, the theory of equipment installation is taught. The course utilizes remote labs for completion of all configuration and CLI-based troubleshooting exercises.

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	<ul style="list-style-type: none"> Course Introduction 	15 minutes
1	<ul style="list-style-type: none"> PBN M and T-series Router Hardware Architecture 	1 hour 45 minutes
1	<ul style="list-style-type: none"> Pre-installation Requirements 	1 hour
1	<ul style="list-style-type: none"> Installation and Start-up Procedures, installation of hardware – including hands-on demonstration and lab practice, if equipment is available 	2 hour
1	<ul style="list-style-type: none"> JUNOS Software Architecture and CLI 	1 hour
2	<ul style="list-style-type: none"> CLI Introduction and Basic Configuration Lab 	45 minutes
2	<ul style="list-style-type: none"> Configuring and Troubleshooting M and T-series Interfaces 	1 hour 30 minutes
2	<ul style="list-style-type: none"> Interface Configuration Lab 	30 minutes
2	<ul style="list-style-type: none"> Monitoring and Maintaining Router 	1 hour 30 minutes
2	<ul style="list-style-type: none"> CLI Monitoring and Maintenance Tasks 	1 hour 30 minutes

PDM Configuration and Operation

LZU 102 561 R2A

Description

This course is intended for operators and network administrators who are going to use PDM to provide VPN and QoS policies. The course will also cover basic system administrator tasks.

Learning objectives

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

- 1 Understand requirements on the network where PDM is used
 - 1.1 List supported router types
 - 1.2 Describe requirements on routing protocols in the network and CE, PE and P router relationships

- 2 Describe key functions in PDM
 - 2.1 Handle PE Router Discovery
 - 2.2 Handle Customer Management

- 3 Handle VPN provisioning using PDM
 - 3.1 Understand the VPN concept
 - 3.2 List requirements for VPN deployment using PDM
 - 3.3 Create, validate and activate L3 VPN policies
 - 3.4 Create, validate and activate L2 VPN policies
 - 3.5 Understand how PDM can be used to support the creation of APN between a GPRS network and an ISP domain

- 4 Handle QoS provisioning using PDM
 - 4.1 Describe QoS parameters and goals
 - 4.2 Define Meter Services using PDM
 - 4.3 Define Traffic Descriptors using PDM
 - 4.4 Configure and activate QoS policies using PDM

- 5 Handle System Administration for PDM
 - 5.1 Describe the components and architecture in PDM
 - 5.2 Create and modify PDM users
 - 5.3 Handle security and user access
 - 5.4 Monitor server applications and processes
 - 5.5 Perform backup and restore of file systems and databases

Target audience

The target audience for this course is Customer or Ericsson personnel who are interested in learning about the core operation and administration of PDM. Emphasis is on hands-on operations.

Prerequisites

Successful completion of the following courses/flow:

ISP Network Surveillance FAB 101 1368 (or equivalent knowledge)

Packet Backbone Network Architectures LZU 108 5965 (or equivalent knowledge)

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 Task Oriented and will

This is a task-oriented learning course based on tasks in the work process given in a technical environment using equipment and tools such as access to PDM servers and a network environment based on AXI-type routers.

The course focuses on the tasks that need to be performed by the three different user types that work with PDM.

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	• Introduction	1 h
	• User administration	1 h
	• Network requirements	1 h
	• VPN provisioning	4 h
2	• QoS provisioning	2 h
	• System administration	3 h

SLM Configuration and Operation

LZU 102 559 R2A

Description

This course is intended for operators and administrators who want to learn about core operation and administration of SLM. The focus is on alarm handling and the configuration needed to customize the alarm lists. The course will familiarize the student with SLM features, requirements on the network elements that are monitored from SLM and the basic system administrator tasks such as user administration and process management.

Learning objectives

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

- 1 Describe the structure of the SLM application
 - 1.1 Describe the Netcool/OMNIBus architecture
 - 1.2 Describe the function of: Probes, ObjectServer, Gateways, Event Lists, Views, filters, automations, De-duplication and Event correlation

- 2 Use Event Lists, Views and Filters to handle events and alarms from network elements
 - 2.1 Handle alarms in the event lists
 - 2.2 Customize views
 - 2.3 Customize filters

- 3 Handle basic SLM configuration and administration
 - 3.1 Handle user administration
 - 3.2 Handle SLM processes
 - 3.3 Understand event parsing
 - 3.4 Configure event processing in SLM and on the NE

- 4 Handle automations
 - 4.1 Describe the function of automations
 - 4.2 Describe triggers and actions
 - 4.3 Describe popular event fields used in automations
 - 4.4 Recognize ObjectServer SQL statements

- 5 Handle Objective Views – Maps
 - 5.1 Be able to navigate an Objective View
 - 5.2 Be able to create a new map with Objective View Editor
 - 5.3 Be able to trigger event lists, additional pages or external executables

- 6 Handle Gateways
 - 6.1 Describe gateway options and functions
 - 6.2 Install a bi-directional gateway
 - 6.3 Configure gateway components and licenses

Target audience

The course is designed for Customers who are interested in learning about the core operation and administration of SLM. Emphasis is on hands-on operations.

Prerequisites

Successful completion of the following courses/flow:

ISP Network Surveillance FAB 102 1368 (or equivalent knowledge)
 Packet Backbone Network Architectures LZU 108 5965 (or equivalent knowledge)

Duration and class size

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

Learning situation

This is a task-oriented learning course based on tasks in the work process given in a technical environment using equipment and tools such as access to an SLM server and a JUNOS based network element (AXI 520) for each group of two students.

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	• Introduction	1 h
	• SLM Overview	1 h
	• SLM Tour	2 h
	• SLM administration	2 h
2	• Event lists, filters and views	2 h
	• Automations	1 h
	• Object Views	1 h
	• Gateways	2 h

The Complete Team Leader Course

LZU 108 2049

Description

The main idea with the Ericsson Customer Care Training Package is to provide the team leader with useful tools for handling his/her role as a team leader being aware of such as group dynamics, group processes, conflicts, the importance of coaching etc. Specific cases will be studied so that the participants interactively will be able to discuss how to handle eventual complications linking theory with practice.

Learning objectives

This course will help a team leader at a call-center or another type of Customer Care Organization to handle his/her role as a team leader being aware of what influence a team, its well being and effectiveness. To achieve this objective the participant will learn about leadership styles, team development, team roles, communication skills, tools for handling conflicts, guidelines for coaching, measuring quality etc. This course also intends to upgrade the importance of the team leader and his/hers collaborators as being the ones facing the customer and therefore delivering Excellent Customer Service.

Target audience

Team leaders and potential team leaders working at:

- GSM/ 3 G/ Fixed Operators' Customer Care organizations.
- Distributors or Service Providers

Prerequisites

There are no prerequisites for this course.

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.



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
	<ul style="list-style-type: none">• Module 1<ul style="list-style-type: none">• The leaders´ role, leadership styles.• Module 2<ul style="list-style-type: none">• Team development• Module 3<ul style="list-style-type: none">• Team roles• Module 4<ul style="list-style-type: none">• Assessment• Module 5<ul style="list-style-type: none">• Coaching- Points to consider• Module 6<ul style="list-style-type: none">• Feedback- Why & how• Module 7<ul style="list-style-type: none">• Communication and handling conflicts• Module 8<ul style="list-style-type: none">• Motivation• Module 9<ul style="list-style-type: none">• To delegate• Module 10<ul style="list-style-type: none">• Action plan	

UNIX System Administration Level 1

LZUBB 108 356 R1A

Description

This course Unix System Administration Level 1 is a practical course, which will enable the students to perform the basic system administration tasks for a Solaris based Unix platform which include installation, file system management, backup procedures, process control, user administration and device management.

Learning objectives

On completion of this course the participants will be able to

- 1 Describe the role of a UNIX System Administrator
- 2 Access system documentation and reference sources for performing administration tasks and troubleshooting
- 3 Perform an installation of the UNIX Operating System
- 4 Add and remove software packages
- 5 Add and configure new devices
- 6 Perform booting and shutdown procedures
- 7 Manage User and Group accounts
- 8 Manage the File System and Disk devices
- 9 Monitor system performance (Memory, File System, Processes, CPU)
- 10 Understand how to implement UNIX security features
- 11 Perform backup and restore
- 12 Implement System Administrator Tools and Utilities

Target audience

The target audience for this course primarily personnel new to UNIX administration and who will be involved in supporting UNIX based nodes and applications.

Perequisites

Successful completion of the following courses:

- UNIX Fundamentals (LZU 108 170)
- UNIX Basics (LZU 108 5134)

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.



UNIX Fundamentals

LZUBB 108 170 R1A

Description

This course provides an overview of the fundamentals of the UNIX operating system. The course provides an introduction to the structure and operation of UNIX using the wide range of fundamental commands and utility programs. Tutorials on the 3 shells (Bourne, Korn and C) are given, allowing to the students to experiment with useful shell scripts. Students are encouraged to use the fundamental commands and utility programs throughout the duration of the course.

Learning objectives

On completion of this course the participants will be able to

- 1 Describe the history of UNIX
- 2 Describe the UNIX operating system
- 3 Describe the UNIX file system
- 4 Use fundamental UNIX commands
- 5 Overview of the vi editor
- 6 Work within a shell environment
- 7 Use network utility programs
- 8 Write basic shell scripts
- 9 Use the on-line documentation
- 10 Set up file permissions
- 11 Describe the role of the System Administrator
- 12 Describe the role of a UNIX System Administrator

Target audience

The target audience for this course primarily personnel working with UNIX administration and needing to get familiar with UNIX and shell scripting.

Perequisites

Successful completion of the following courses:

- UNIX Basics (LZU 108 5134)

Duration and class size

The length of the course is 2 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.

VPN & IP Security

LZU 102 323 R1A

Description

This course will give the students an insight and understanding of the security issues in IP networks. The students will learn about the threats and weaknesses in the TCP / IP suite and how to enable security within an IP network. The course covers such topics as encryption, cryptography, digital signatures and certificates. The course will also give the students an understanding of different VPN technologies and how different VPNs are implemented within the IP network. Throughout the course hands-on labs and analysers are used to pinpoint important aspects of theory sessions.

Learning objectives

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

- 1 Describe the threats and security issues in the IP networks
 - 1.1 Describe the different security threats and weaknesses in TCP / IP suite
 - 1.2 Describe how to develop a security policy, how to respond to incidents and the different bodies involved in IP security
- 2 Describe the devices and services in building a secure network
 - 2.1 Describe and perform exercises and analysis on the operation of NAT and router filters / access lists, and how they are implemented
 - 2.2 Describe firewall solutions, and how to implement firewall security in a network
 - 2.3 Describe the operation of secure DNS, HTTPS, S/MIME and SSH
- 3 Describe Encryption technologies, security services and certificates
 - 3.1 Describe encryption, cryptography, and symmetric and asymmetric algorithms
 - 3.2 Describe the operation of message digest and digital signatures
 - 3.3 Describe operation of Certificate Authorities and how certificate are exchanged
 - 3.4 Describe the operation of other security devices such as Smart Cards
- 4 Describe the purpose and operation of IPSec VPNs
 - 4.1 Describe and perform exercises and analysis on the operation of L2TP
 - 4.2 Describe and perform exercises and analysis on the operation of IPSec Authentication tunnels
 - 4.3 Describe and perform exercises and analysis on the operation of IPSec ESP tunnels

Target audience

The target audience for this course are Ericsson customers who are involved in IP networking and who need to know how to implement security in IP networks.

Prerequisites

The participants should be familiar with IP networking, IP routing and different IP services and applications or successful completion of the following courses:

IP Networking - LZU 102 397 – 4 day ILT course

Duration and class size

The length of the course is 2 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.

Ericsson AB

Global Services
SE-164 80 Stockholm
Telephone: +46 8 757 0000
Email: global.services@era.ericsson.se
www.ericsson.com
© Ericsson AB 2003

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	• Describe the different security threats and weaknesses in TCP / IP suite	1.0
	• Describe how to develop a security policy, how to respond to incidents and the different bodies involved in IP security	1.0
	• Describe and perform exercises and analysis on the operation of NAT and router filters / access lists, and how they are implemented	2.0
	• Describe firewall solutions, and how to implement firewall security in a network	1.0
	• Describe the operation of secure DNS, HTTPS, S/MIME and SSH	0.5
	• Describe encryption, cryptography, and symmetric and asymmetric algorithms	1.0
	2	• Describe the operation of message digest and digital signatures
• Describe the operation of Certificate Authorities and how certificate are exchanged		1.0
• Describe the operation of other security devices such as Smart Cards		0.5
• Describe and perform exercises and analysis on the operation of L2TP and how it is implemented		1.0
• Describe and perform exercises and analysis on the operation of IPSec Authentication tunnels		1.0
• Describe and perform exercises and analysis on the operation of IPSec ESP tunnels		2.0