



IP Design for Mobile Networks

Revolutionizing the architecture and implementation
of mobile networks

IP Design for Mobile Networks

Mark Grayson, Kevin Shatzkamer, Scott Wainner

Copyright © 2009 Cisco Systems, Inc.

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing June 2009

Library of Congress Cataloging-in-Publication Data

Grayson, Mark, 1965-

IP design for mobile networks / Mark Grayson, Kevin Shatzkamer, Scott Wainner.

p. cm.

ISBN-13: 978-1-58705-826-4 (pbk.)

ISBN-10: 1-58705-826-X (pbk.)

1. Wireless LANs. 2. Wireless Internet. 3. Mobile computing. 4. TCP/IP (Computer network protocol) I. Shatzkamer, Kevin, 1978- II. Wainner, Scott. III. Title.

TK5105.78.G73 2009
621.382'12--dc22

2009020541

ISBN-13: 978-1-58705-826-4

ISBN-10: 1-58705-826-X

Warning and Disclaimer

This book is designed to provide information about the evolution of mobile technologies and networks to the All-IP architecture. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the authors and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark. The following copyright block applies to Figure 7-29 through Figure 7-35 of this book:

© European Telecommunications Standards Institute 2000. Further use, modification, redistribution is strictly prohibited. ETSI Standards are available from <http://pda.etsi.org/pda/>

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States, please contact: **International Sales** international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Business Operation Manager, Cisco Press: Anand Sundaram

Manager Global Certification: Erik Ullanderson

Executive Editor: Mary Beth Ray

Managing Editor: Patrick Kanouse

Development Editor: Kimberley Debus

Project Editors: Jennifer Gallant, Seth Kerney

Copy Editor: Water Crest Publishing, Inc.

Technical Editors: Eric Hamel, Kirk McBean, Rajesh Pazhyannur

Editorial Assistant: Vanessa Evans

Book Designer: Louisa Adair

Composition: Bronkella Publishing LLC

Indexer: Ken Johnson

Proofreaders: Jennifer Gallant, Seth Kerney



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks. Changing the Way We Work, Live, Play, and Learn is a service mark, and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

Introduction

The cellular world, for much of its history, has focused on circuit-switched voice and simple text messaging as its two primary applications. Cellular technology is tremendously successful, with over half the world's population being mobile telephony subscribers. At the same time, the Internet revolution has had a profound impact on the diversity of services accessible over IP-enabled networks, with IP now recognized as the fundamental building block for all next-generation communication networks.

The next step in the evolution of the Internet will be to make it available anytime and anywhere. This will require the convergence of the cellular world and the Internet. This convergence is being driven by a host of powerful new mobile devices, high-speed mobile networks, compelling applications, and flat-rate all-you-can-eat billing plans.

IP is now impacting all aspects of the mobile operator's network, from radio bearer support through transmission and service delivery capability. Indeed, the various definitions for the next generation of mobile networks all align around an "all-IP" vision, providing purely packet-switched capabilities and solely supporting IP services.

End-to-end IP provides the flexibility to cost-effectively deliver services and applications that meet users' changing needs.

As today's mobile networks migrate toward "All-IP," with various interim steps along the way, it is important to educate those who are focused on the evolving mobile technologies on proper IP design theory and the fundamental role IP has in their next-generation mobile networks. Tomorrow's RF engineers, mobile network designers, and system architects will be expected to have an understanding of IP fundamentals and how their role in delivering the end-to-end system is crucial for delivering the all-IP vision.

This book seeks to focus on the transition of the mobile network from today's circuit-switched technologies toward a future where IP is the fundamental building block integrated into all aspects of the network. This IP transition begins with function-specific migrations of specific network domains and ends with an end-to-end IP network for radio, transport, and service delivery. This book looks at the transition from both the standards and design theory perspective.

Who Should Read This Book?

This book is not designed to provide an all-inclusive reference for evolving mobile networks to Internet Protocol (IP). This book is intended to increase the reader's understanding of the current and target state of mobile networks, and the technology enablers that assist mobile operators' migration.

This book assumes at least a basic understanding of standard networking technologies, including the Internet Protocol itself. Many concepts are introduced in order to give the reader exposure to the key technology trends and decision points impacting today's mobile operators. The book does not give recommendations on which of these technologies should be deployed, nor does it provide a transition plan for a mobile operator. Each

mobile operator is expected to evaluate the technologies and make decisions based on their own criteria.

This book is written for many levels of technical expertise, from network design engineers and network planning engineers looking to design and implement mobile network migrations toward an all-IP future, networking consultants interested in understanding the technology trends that affect their mobile service provider customers, students preparing for a career in the mobile environment, and Chief Technology Officers (CTOs) seeking further understanding of the value IP technology brings to the mobile network.

How This Book Is Organized

Depending on the level of technical depth required, this book may be read cover-to-cover or be used as a reference manual for IP's role in mobile network evolution. The book is designed to be flexible and enable you to move between chapters and sections of chapters to cover just the material that you need more work with.

The book is divided into three parts.

Part I, "Cellular Networks and Standards," provides an overview of how IP is being integrated into mobile systems, including RF, radio systems, and cellular networks. Part I includes the following chapters:

- **Chapter 1, "Introduction to Radio Systems":** This chapter provides an introduction to various radio technologies, and wireless technologies used to transport IP over radio bearers, an important foundation for expanding into IP design theory for mobile networks.
- **Chapter 2, "Cellular Access Systems":** This chapter provides an overview of legacy mobile radio systems, including GSM, UMTS, and cdma2000, presenting details of how IP services have been overlaid on top of circuit-switched architectures.
- **Chapter 3, "All-IP Access Systems":** This chapter provides an overview of the "All-IP" Access systems and standards. IP as a fundamental technology for future mobile access systems is discussed.

Part II, "IP and Today's Cellular Network," provides an overview of IP, the technologies used for transport and connectivity of today's cellular networks, and how the mobile core is evolving to encompass IP technologies. Part II includes the following chapters:

- **Chapter 4, "An IP Refresher":** This chapter is intended to level set understanding of IP technology and design theories in order to provide a foundation for expanding into IP design theory for mobile networks.
- **Chapter 5, "Connectivity and Transport":** This chapter discusses the technologies involved in connectivity and transport for mobile networks over various media.

- **Chapter 6, “Mobile Core Evolution”:** This chapter provides details on how the mobile core network is evolving, describing how IP connectivity is provided over mobile networks, as well as how IP is being used to transport the circuit-switched core network.
- **Chapter 7, “Offloading Traditional Networks with IP”:** This chapter discusses the evolution of today’s TDM-based technologies to IP through offload scenarios for the mobile backhaul network.

Part III, “The End-to-End Services Network,” provides an overview of the end-to-end services network based on IP, including context awareness and services. Part III includes the following chapters:

- **Chapter 8, “End-to-End Context Awareness”:** This chapter discusses the concept of Intelligent IP Networks to extend core functionality and provide intelligent delivery of traffic to mobile subscribers.
- **Chapter 9, “Content and Services”:** This chapter discusses the evolution of content and services from circuit-switched technologies to IP-based technologies, and the evolution of the service framework from the Intelligent Network (IN) to service delivery platforms and the Intelligent Multimedia Subsystem (IMS).

Offloading Traditional Networks with IP

Traditional mobile networks, such as today's 2G (GSM, CDMA 1x) and 3G (UMTS/HSPA and EVDO) networks, are based on Time Division Multiplexing (TDM) for transmission. These TDM networks comprise the majority of the backhaul networks for transport of voice and data traffic. Figure 7-1 shows backhaul penetration worldwide by technology.¹

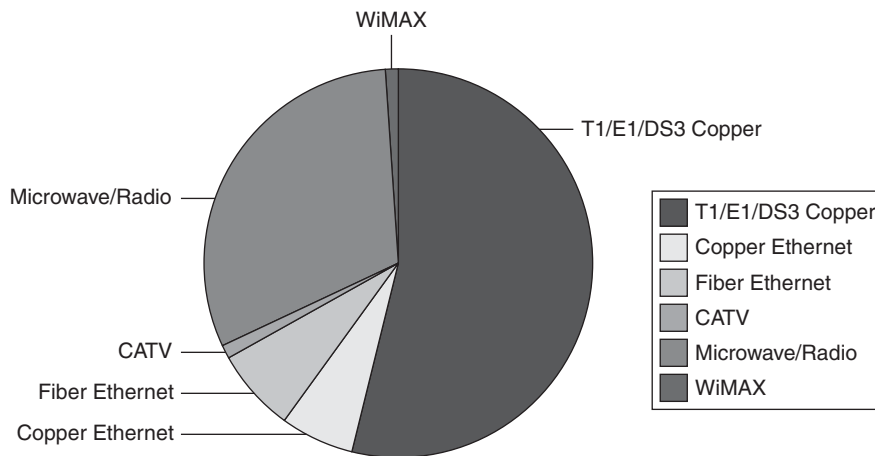


Figure 7-1 *Backhaul Network Penetration*

As mobile network data traffic grows, and user demand and dependency on the mobile operator as a data access provider increases, mobile operators are exploring various offload mechanisms to migrate legacy TDM networks to modern Ethernet and IP. Figure 7-2 demonstrates the increased bandwidth requirements per base station, to support next-generation mobile services.²

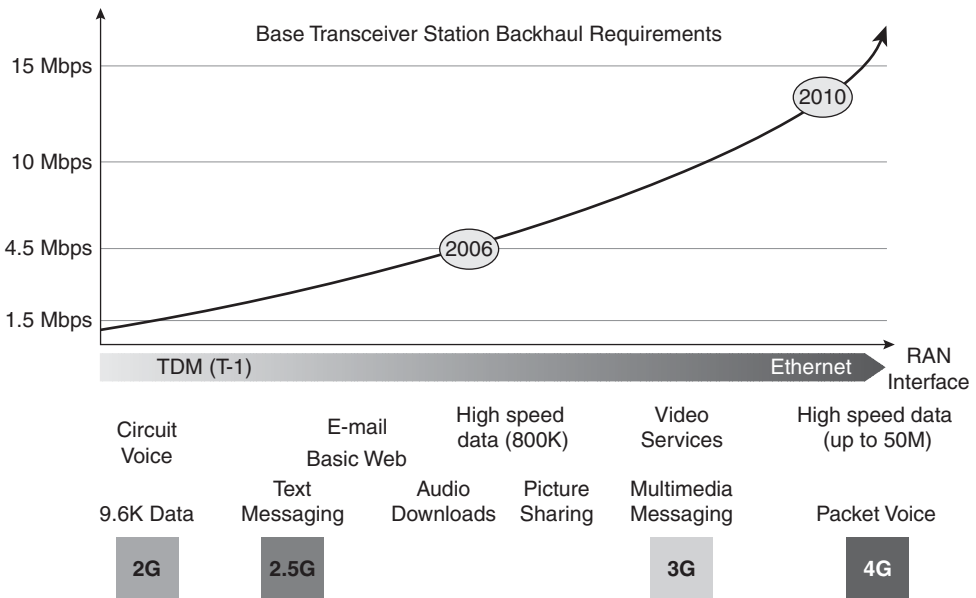


Figure 7-2 Backhaul Bandwidth Requirements

This migration allows a mobile operator to shed excess Operating Expenditures (OPEX) associated with TDM transport. However, during this migration, supporting legacy TDM interfaces and network elements is critical for continuing operations.

Various IP-based offload mechanisms may be employed to allow for this migration without the high Capital Expenditure (CAPEX) outlay for new equipment (BTS, BSC, and MSC infrastructure).

These IP-based offload mechanisms can be largely categorized as follows:

- **Backhaul offload** involves encapsulation of standard TDM protocol communications between the Base Transceiver Station (BTS) and the Base Station Controller (BSC), the BSC and the Mobile Switching Center (MSC), or inter-BSC/MSC, into IP packets.
- **Signaling protocol offload** involves protocol conversion of signaling packets. An example of signaling protocol offload is SS7/SIGTRAN.
- **Bearer protocol offload** involves protocol conversion of bearer packets. Examples of bearer protocol offload include Transcoder-Free Operations (TrFO) mechanisms and IP Soft-Handoff mechanisms.

Backhaul Offload with Pseudowires

Pseudowires allow for the emulation of point-to-point or point-to-multipoint links over a Packet-Switched Network (PSN). Pseudowire technology provides a migration path,

allowing an operator to deploy packet-switched networks without immediately replacing legacy end-user equipment.

Each pseudowire presents a single, unshared “circuit” for carrying “native” services, such as ATM, SONET/SDH, TDM, Ethernet, or Frame Relay, over the PSN. The PSN may either be Layer 2 Tunneling Protocol Version 3 (L2TPv3), MPLS, or generic IP.

Many standards organizations, including the Internet Engineering Task Force (IETF), the Metro Ethernet Forum (MEF), and the International Telecommunications Union Telecommunications Standards Sector (ITU-T), have defined the encapsulation techniques for transport of the relevant protocols in mobile networks today, as follows:

- **IEEE RFC3985:** Pseudowire Emulation Edge-to-Edge (PWE3).
- **IEEE RFC5087 and ITU-T Y.1453:** Time Division Multiplexing over IP (TDMoIP).
- **IEEE RFC4553:** Structure-Agnostic Time Division Multiplexing over IP.
- **IEEE RFC5086:** Circuit Emulation Services over Packet-Switched Networks (CESoPSN).
- **IEEE RFC4717 and ITU-T Y.1411:** ATM Pseudowires.
- **IEEE RFC4842:** Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) Circuit Emulation over Packet (CEP).

Pseudowire Use-Cases

Prior to discussing pseudowire technology itself, the following examples should help to clarify various uses for pseudowire technology in mobile networks. The examples discussed may not be applicable to all mobile operators or all mobile infrastructure vendors, but are representative of some of the many deployment scenarios where pseudowires have been successfully deployed as an offload mechanism. The examples cover four scenarios, as follows:

- TDMoIP Pseudowire for CDMA/EVDO or GSM Backhaul Networks
- CESoPSN Pseudowire for Inter-BSC/MSC Connectivity
- ATM Pseudowires for UMTS R4 Connectivity
- Pseudowires for Multi-RAN Environments

Details of each pseudowire technology and implementation follow.

TDMoIP Pseudowires for EVDO or GSM Backhaul Networks

As discussed in Chapter 4, “An IP Refresher,” the traditional mobile backhaul network for a CDMA or GSM network consists of TDM interfaces on both the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These TDM interfaces connect to a

backhaul provider's T1/E1 circuits for transport. Figure 7-3 illustrates a mobile backhaul network with standard TDM backhaul.

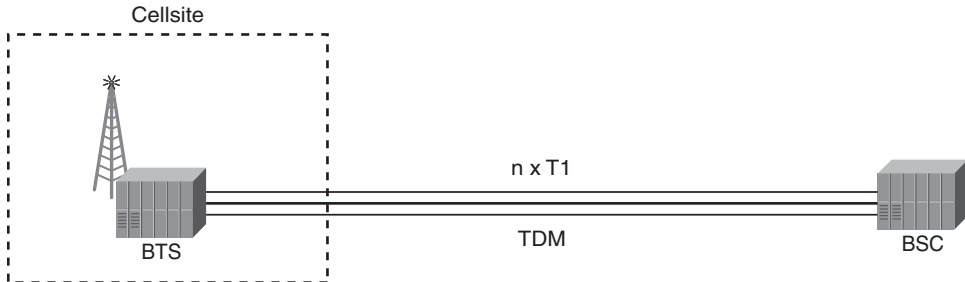


Figure 7-3 *Traditional TDM Mobile Backhaul Network*

TDM pseudowire technology plays a key role in allowing mobile operators to migrate their backhaul networks between the BTS, or cell site, and BSC or MSC location. The pseudowire provides a “transparent wire” between these locations and preserves the integrity of the TDM framing as it is transmitted across the PSN. Figure 7-4 illustrates a mobile backhaul network that uses TDMoIP pseudowires for transport.

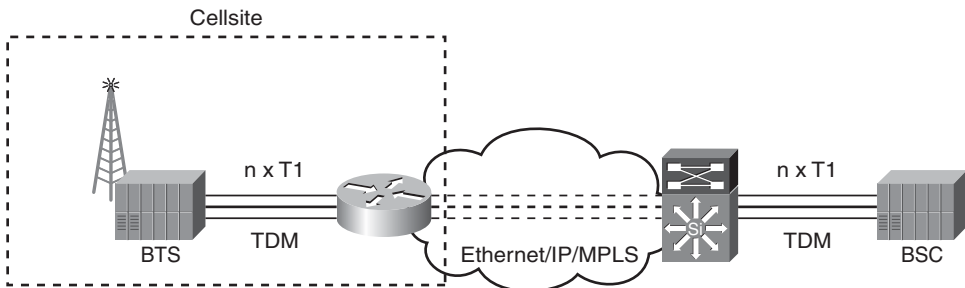


Figure 7-4 *Mobile Backhaul Network with TDM Pseudowires*

CESoPSN Pseudowires for Inter-MSC/BSC Connectivity

As discussed in Chapter 4, the traditional MSC and BSC functionality and connectivity is typically TDM-based. Interconnectivity between all BSCs/MSCs is essential for handling mobility of a voice session in a circuit-switched voice (GSM, CDMA 1x) environment. However, in order to support such an environment, typical mobile deployments rely on a combination of point-to-point TDM circuits between BSC and MSC, and fully-meshed or star configurations of TDM circuits from the MSC toward the core network. Figure 7-5 illustrates one such topology.

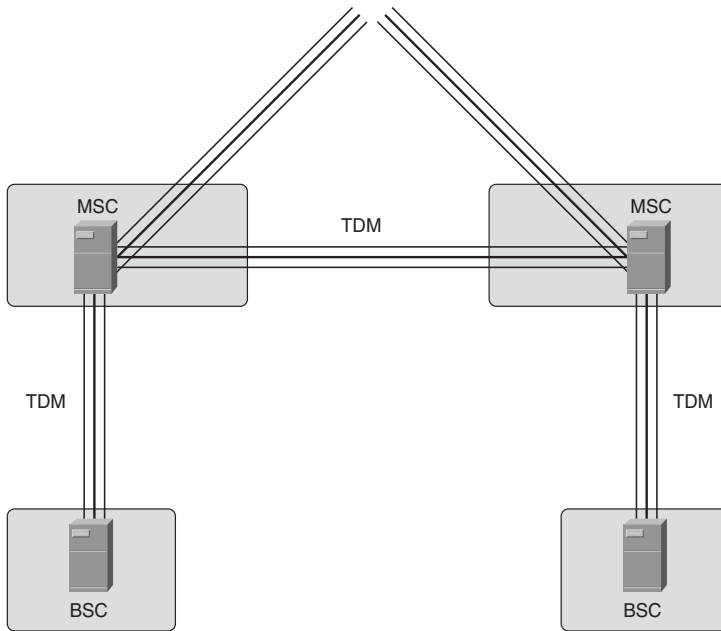


Figure 7-5 *Inter-MSC/BSC Connectivity*

The overall cost of maintaining a fully-meshed, point-to-point TDM architecture is significant from an OPEX perspective. By reducing the number of TDM circuits required from the Local Exchange Carrier (LEC), a mobile operator may immediately see impact to operating margins. One such way to reduce the number of circuits is to leverage CESoPSN pseudowires for interconnecting MSC and BSCs, as illustrated in Figure 7-6.

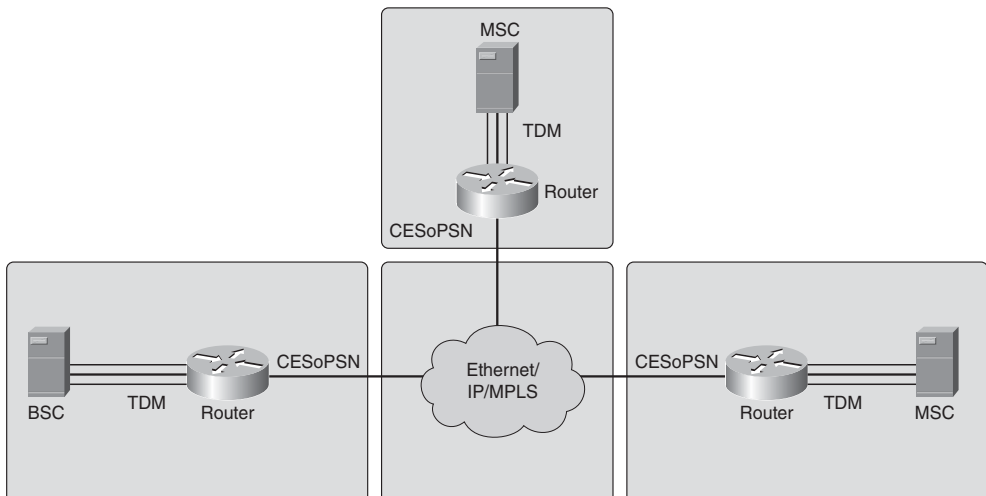


Figure 7-6 *Inter-MSC/BSC Connectivity with CESoPSN Pseudowires*

Inter-MSC/BSC connectivity with CESoPSN pseudowires allows a mobile operator to use existing infrastructure, namely their IP core network, for transport of voice traffic.

ATM Pseudowires for UMTS R4 Backhaul Networks

UMTS Release 4 networks rely heavily on ATM as a transport mechanism for data traffic. Similar to the model previously discussed for transport of TDM backhaul traffic in CDMA and GSM environments, fixed circuits must be deployed to allow for mobility. These fixed ATM circuits, known as Permanent Virtual Circuits (PVCs), are discussed in more detail in Chapter 4. Figure 7-7 depicts a UMTS R4 backhaul network, from Node B to RNC and from RNC to MSC/SGSN.

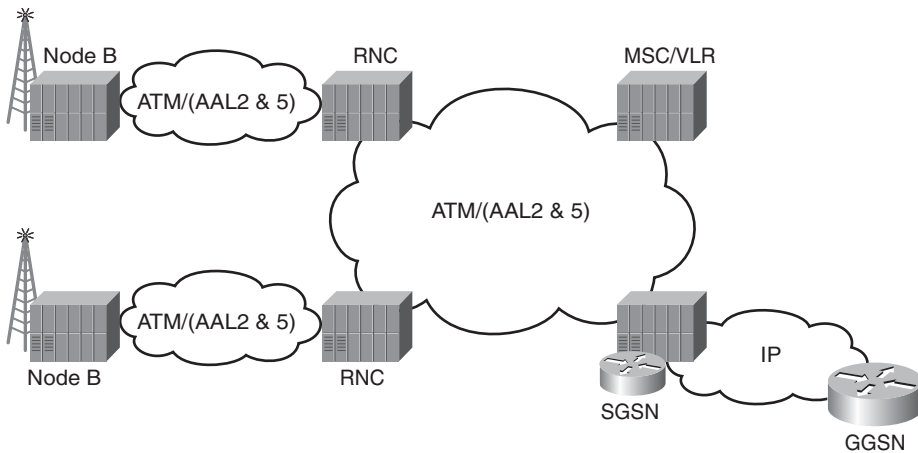


Figure 7-7 UMTS R4 Backhaul with ATM

By migrating to ATM pseudowires and leveraging IP core assets, mobile operators can simplify their architecture, reduce costs, and begin preparing for fourth-generation mobile technology deployment, such as 3GPP Long-Term Evolution (LTE), discussed in Chapter 3, “All-IP Access Systems.” Figure 7-8 illustrates one potential solution with ATM pseudowires.

It is also possible that IP backhaul and IP core networks may converge over a common IP/MPLS network.

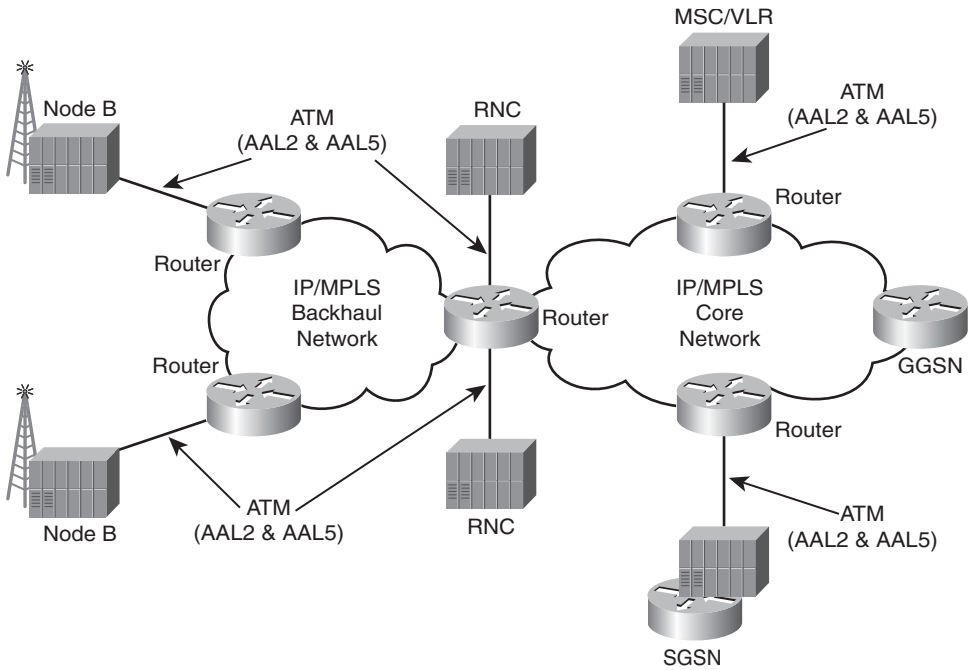


Figure 7-8 UMTS R4 Backhaul with ATM Pseudowire

Converging Multiple RAN Technologies over Common Pseudowire

As mobile operators complete their transition from solely circuit-switched voice networks to voice and data networks, mobile networks begin to become an overlay of multiple radio technologies. With all these multiple overlays requiring unique circuits (TDM or ATM), mobile operators incur large OPEX for maintaining multiple different backhaul networks. For instance, a CDMA operator maintains a CDMA 1x voice network and EVDO data network simultaneously. Even if the radio access cards reside in the same physical element, mobile operators use unique circuits for voice and data traffic in order to facilitate troubleshooting and problem isolation.

Pseudowires present an opportunity for mobile operators to deploy a unified backhaul architecture while still managing each circuit individually.

Example 1, illustrated in Figure 7-9, highlights a converged RAN architecture for a CDMA operator.

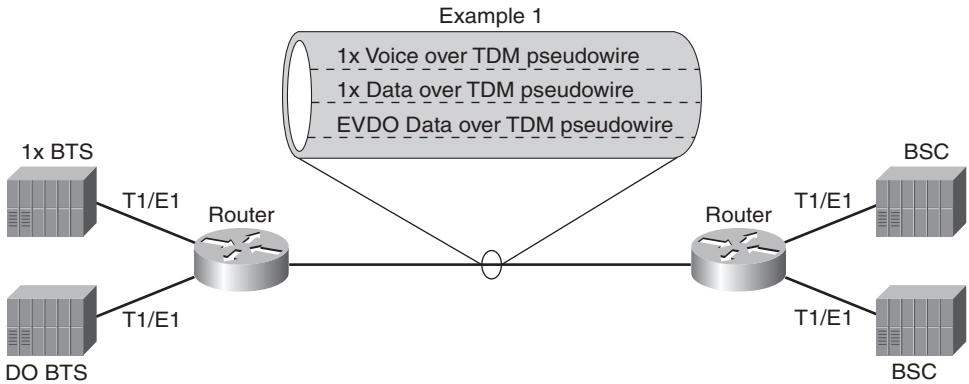


Figure 7-9 Converged RAN Architecture for CDMA

Example 2, illustrated in Figure 7-10, highlights a converged RAN architecture for a GSM/UMTS operator.

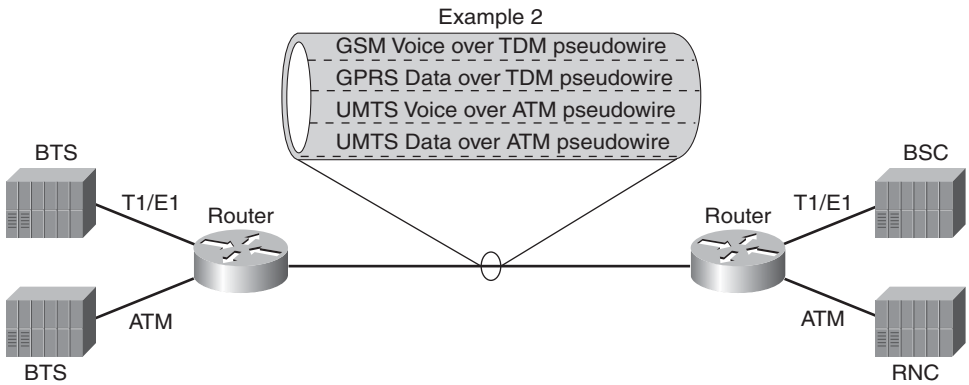


Figure 7-10 Converged RAN Architecture for UMTS

Note With the initial 3G release, there is no differentiation between voice and data traffic on the link between the Node B and the RNC (contrary to what is shown in the figure). The whole traffic is encapsulated in a Frame Protocol and send to/from the RNC. The differentiation is done later. This is changed in later releases of UMTS.

Pseudowire Emulation Edge-to-Edge (PWE3)

Pseudowire Emulation Edge-to-Edge RFC 3985 provides the structure and architecture for emulation of Frame Relay, ATM, Ethernet, TDM, and SONET over packet-switched networks using IP or MPLS.

Pseudowires for Time Division Multiplexing (TDM)

At the most basic level, TDMoIP pseudowires segment T1/E1 frames, encapsulate these frames in Ethernet, and fragment the frames into IP packets for transport across the PSN. At the destination, the IP header is stripped, the Ethernet frame is decapsulated, and the original bit stream is reconstructed, including regeneration of clock information. Figure 7-11 illustrates a high-level view of a TDMoIP pseudowire.

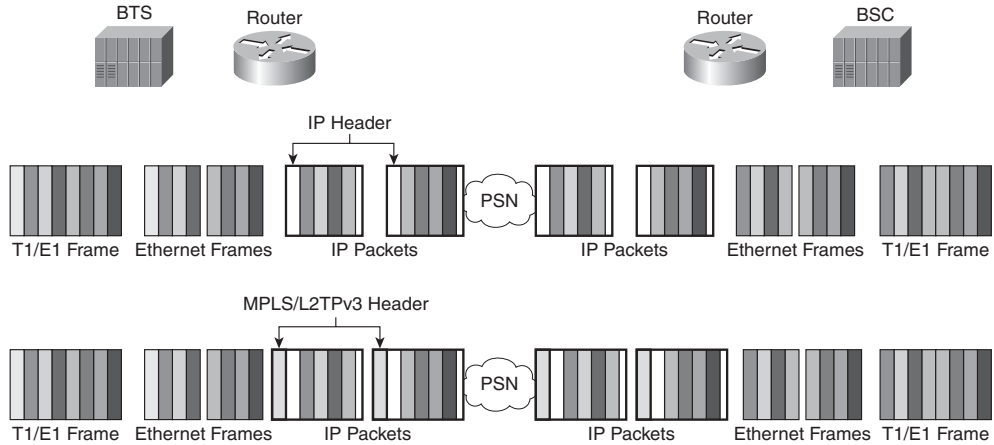


Figure 7-11 *High-Level View of TDMoIP Pseudowire*

Structure-Awareness of TDM Pseudowires

TDM over IP pseudowires can be categorized into two classes, as follows:

- **Structure-Agnostic Transport over Packet (SAToP):** With structure-agnostic transport, the protocol may disregard all structures imposed on TDM signaling or framing. Therefore, this transport method is simply bit-by-bit transport. Structure-agnostic TDM over IP is standardized in RFC4553. The PE devices in SAToP transport network do not participate in TDM signaling and do not interpret the TDM data. This implies that there are no assurances that network degradation does not impact the TDM structure.
- **Structure-Aware Transport over Packet:** With structure-aware transport, such as TDMoIP and CESoPSN, the integrity of the TDM structure is ensured, even in cases of network degradation. Because PE devices have exposure to the TDM signaling, individual channels are exposed, allowing the network to utilize Packet Loss Concealment (PLC) and bandwidth conservation mechanisms on a per-channel basis.

TDM Structures

A frame structure refers to the way a single communications channel is multiplexed in several individual channels. By multiplexing the underlying channel, more than one data stream may be simultaneously transmitted at a time. Because TDM is based on the time domain, a single frame is actually a constant-length time interval. Within this time interval, fixed-length timeslots, each representing a single circuit-switched channel, are transmitted.

A multiplexer is responsible for assigning data, or bytes, from a bitstream to each timeslot, and a demultiplexer is responsible for re-assembling the bitstream. Although every timeslot may not be used, the entire frame is always transmitted in order to ensure that frames remain synchronized.

A T1 frame consists of (24) 8-bit (1-byte) timeslots plus a synchronization bit, allowing for 193 bits. An E1 frame consists of 32 timeslots, each containing 8 bits, or a total of 256 bits per frame, including a synchronization bit. In both cases, frames are transmitted 8,000 times per second. With this framing information, it is easy to calculate the total available bandwidth for both T1 and E1 circuits:

T1 Circuit Bandwidth = (24 timeslots * 8 bits + 1 synch bit) * 8,000 frames per second / 1×10^6 bits/Megabit = 1.544 Megabits per second

E1 Circuit Bandwidth = 32 timeslots * 8 bits * 8,000 frames per second / 1×10^6 bits/Megabit = 2.048 Megabits per second

Multiple channels, each containing 8000 8-bit samples per second, are multiplexed together using TDM framing, as illustrated in Figure 7-12.

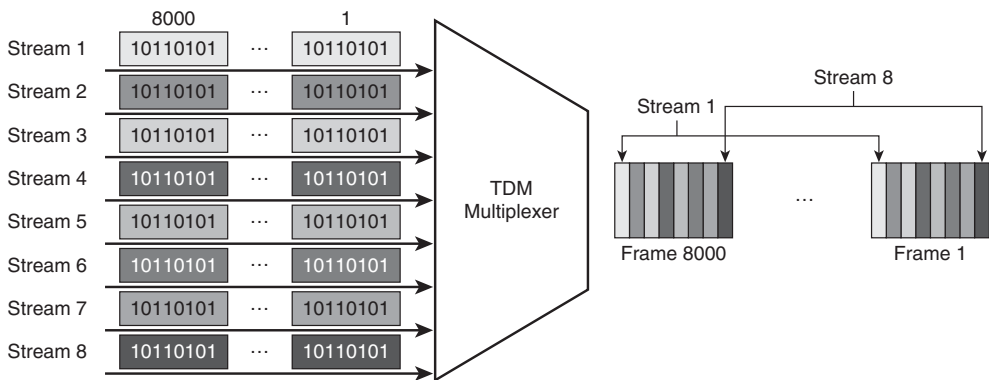


Figure 7-12 TDM Frame Multiplexing

Structure-Aware Transport

Structure-aware emulation assumes that the TDM structure itself, including the framing and control information, are available to the pseudowire edge device. With this information available, pseudowire encapsulation can be done in a more intelligent manner, with the edge device selecting specific channel samples from the TDM bitstream. Structure-aware transport may ensure the integrity of the original TDM structure via three distinct adaptation algorithms, as follows:

- **Structure-Locking:** Structure-locking ensures that each packet on the pseudowire contains an entire TDM structure, or multiple/fragments of TDM structures. The exact number of frames included is locked for all packets, in both directions. The order of the frames in the PSN is the same as those within the TDM frame sequence. When a TDM bitstream arrives, consecutive bits from the bitstream, most significant first, fill each payload octet. Structure-locking is not used in TDMoIP.
- **Structure-Indication:** The structure-indication method is derived from ATM Adaptation Layer 1 (AAL1), described in Chapter 4. Unlike structure locking, structure indication allows for pseudowire packets to contain arbitrary-length fragments of the underlying TDM frames. These fragments are taken from the bitstream in-sequence, from the most-significant bit first. The pseudowire packets also include pointers to indicate where a new structure begins. Because the bitstream sequence is identical to the sequence contained in the PSN, this method is commonly known as “circuit emulation.”
- **Structure-Reassembly:** The structure-reassembly method allows for specific components of the TDM structure to be extracted and reorganized within the pseudowire packet structure by the ingress pseudowire edge, with enough information such that the other edge of the pseudowire may reassemble the original TDM structure. The structure-reassembly method allows for bandwidth conservation by only transporting frames/timeslots that are active. This method is commonly known as “loop emulation.”

TDMoIP uses the structure-indication algorithm for constant-rate, real-time traffic and the structure-reassembly algorithm for variable-rate, real-time traffic. CESoPSN uses the structure-locking algorithm.

Packet Loss Concealment (PLC)

TDM networks are inherently lossless. Because TDM data is always delivered over a dedicated channel at a constant bitrate, TDM bitstreams may arrive with bit errors, but are never out of order and never get lost in transit.

The behavior of a TDM network is not replicable in a cost-efficient manner over an IP network. Implementation of Quality of Service (QoS) and traffic-engineering mechanisms may be used to reduce traffic loss, but there is no guarantee that packets will not arrive out of order, or arrive at all. Packet-Switched Networks are inherently unreliable, and leverage higher-layer protocols to provide for sequencing, retransmission, and reliability.

Because TDM pseudowires carry real-time bitstreams, it is not possible to rely on retransmission mechanisms. Packet Loss Concealment (PLC) masks the impacts of these out-of-order or lost packets. In the case of lost packets, arbitrary packets are inserted into the bitstream to ensure that the timing is preserved. Because a TDM pseudowire packet is considered lost when the next packet arrives, out-of-order packets are not tolerated. TDM pseudowires use different types of arbitrary packets to conceal packet loss, as follows:

- **Zero Insertion:** Insertion of a constant value, or zero, in place of any lost packets. For voice, this may result in some choppiness.
- **Previous Insertion:** Insertion of the previous frame value in place of any lost packets. This method tends to be more beneficial for voice traffic, because voice tends to have a stationarity aspect. This stationarity means that the missing frame should have characteristics similar to the previous frame.
- **Interpolation:** Because a TDM pseudowire is considered lost when the next packet in sequence arrives, the receiver has both the previous and next packets upon which to base the missing frame value. Interpolation algorithms ranging from linear (straight-line interpolation of missing frame value) to more predictive (statistical calculations of missing frame value) may be used; however, there is no standard method for TDM pseudowire frame interpolation.

Time Division Multiplexing over IP (TDMoIP)

TDM over IP was first developed by RAD Data Communications in 1998, and first deployed in 1999 by Utfors, a Swedish broadband communications operator later acquired by Telenor.

Generic Encapsulation

The basic structure of a TDMoIP packet is depicted in Figure 7-13.

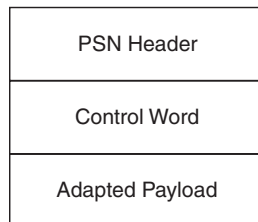


Figure 7-13 *TDMoIP Packet Structure*

TDMoIP packets are composed of three main parts, as follows:

- **PSN Headers:** PSN headers contain IP, MPLS, L2TPv3, or Ethernet information required to send the packet from the pseudowire ingress device toward the destination device, or pseudowire egress device. For example:
 - IP transport requires that the source/destination IP address and port number be included in the header.
 - MPLS transport requires that the MPLS tunnel label be included in the header.
 - L2TPv3 transport requires that the L2TPv3 Session Identifier (pseudowire label) be included in the header.
 - Ethernet transport requires that the Ethernet source/destination MAC address, VLAN header, and Ethertype be included in the header.
- **Control Word:** The Control Word is included in every TDMoIP packet. The Control Word includes information on TDM physical layer failures/defects (local or remote), length of the packet (to indicate if the packet is padded to meet PSN minimum transmission unit size), and sequence number (for detection of lost or misordered packets).
- **Adapted Payload:** The pseudowire ingress device uses either structure-indication or structure-reassembly in order to fill the packet payload.

OAM

Defects in a TDMoIP network may occur in multiple different locations. Depending on the location of the defect, standard TDM OAM mechanisms or TDMoIP mechanisms may be used to alert the TDM peer. Figure 7-14 illustrates the multiple defect locations in a TDMoIP network.

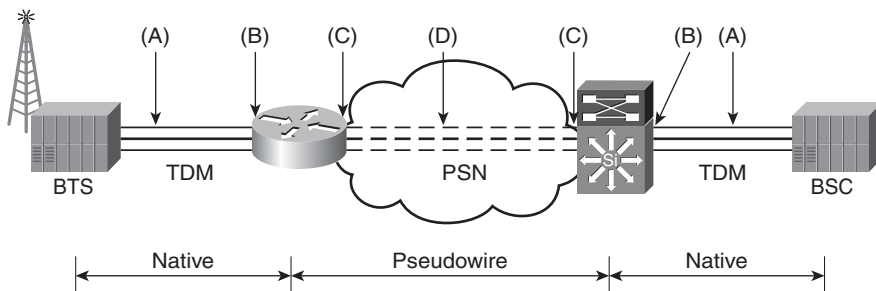


Figure 7-14 TDMoIP Network Defect Locations

Table 7-1 includes information about the reference points illustrated in Figure 7-14 and correlated OAM mechanisms, if available.

Table 7-1 *Reference Points and OAM Mechanisms*

Reference Point	Description	OAM Mechanism
(A)	Defect in the L2 TDM network that impacts any number of circuits terminating on the pseudowire edge devices.	The defect is communicated to the pseudowire edge devices and the remote TDM peer via native TDM OAM mechanisms.
(B)	Defect on the pseudowire edge TDM interface.	
(C)	Defect on the pseudowire edge PSN interface.	
(D)	Defect on the PSN that impacts any number of pseudowires terminating on the pseudowire edge devices.	The defect is communicated to the pseudowire edge devices via PSN or pseudowire OAM mechanisms.

Each pseudowire edge device is responsible for maintaining the state of both forward- and reverse-path traffic. Information on the forwarding paths is communicated to the pseudowire edge devices via Forward- or Reverse-Path indication notifications. Table 7-2 discusses the traffic impacts of the received messages.

Table 7-2 *Indication Notifications*

Indication	Source	Impact
Forward-Path Indication	TDM Peer	Impacts ability of the pseudowire edge device to receive traffic over the TDM circuit from the local TDM device. Note: The pseudowire edge device may be able to detect this directly if the failure occurs in the local port or link.
Forward-Path Indication	PSN Peer	Impacts the ability of the pseudowire edge device to receive traffic from the remote TDM device Note: A Forward-Path indication on the PSN does not necessarily imply that the PSN is working improperly, because the defect may be in the remote TDM circuit.
Reverse-Path Indication	TDM Peer	Impacts the ability of the pseudowire edge device to send traffic to the local TDM device.
Reverse-Path Indication	PSN Peer	Impacts the ability of the pseudowire edge device to send traffic to the remote TDM device. Note: This indication may be indicative of either a PSN fault or a remote TDM fault.

TDMoIP includes its own Operations and Maintenance (OAM) signaling path for reporting of bundle status and performance statistics. OAM signaling provides increased reliability to a protocol stack (TDMoIP pseudowires) that is inherently not reliable. The messages are similar to ICMP messages for the IP network.

Connectivity messages are sent periodically from pseudowire edge to pseudowire edge. A response from the remote pseudowire edge device indicates connectivity. Because forward and receive paths may be different, connectivity messages must be sent in both directions.

Performance messages are sent either periodically or on-demand between pseudowire edge devices. Metrics pertinent to pseudowire performance, such as one-way and round-trip delay, jitter, and packet loss, may be measured.

In addition, standard PSN mechanisms, such as Bidirectional Forwarding Detection (BFD) and MPLS Label Switch Path Ping (LSP-Ping), or other protocol-specific detection mechanisms (L2TP mechanisms described in RFC 3931) may be used over each individual pseudowire, as well as the tunnel itself. These mechanisms may be used continually (proactive notification of defects) or on-demand (reactive notification of diagnostics).

Circuit Emulation Services over Packet-Switched Networks (CESoPSN)

Circuit Emulation Services over Packet-Switched Networks (CESoPSN) is defined in RFC 5086, which was first drafted in January 2004.

Packet Structure

Packet structure of CESoPSN is very similar to that of TDMoIP, except for the inclusion of an optional fixed-length RTP header. This packet structure is illustrated in Figure 7-15.

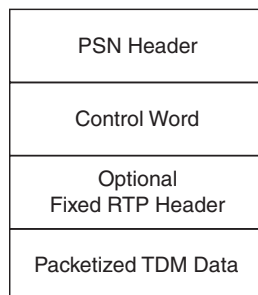


Figure 7-15 CESoPSN Packet Structure

RTP

CESoPSN may use an optional RTP header for the transport of timing information. Timing is further discussed later in the chapter in the section, “Timing.” The RTP header includes specific timestamp information that can be retrieved in the following two manners:

- **Absolute Mode:** In Absolute Mode, the edge pseudowire device recovers the clock information from the incoming TDM circuit. In this mode, the timestamps are closely correlated with sequence numbers.
- **Differential Mode:** In Differential Mode, the edge pseudowire device has access to a high-quality synchronization source. In this mode, timestamps represent the difference between the synchronization source and the TDM circuit.

CESoPSN Versus TDMoIP

Although both CESoPSN and TDMoIP provide for transport of TDM frames over PSNs using pseudowires, there are numerous differences between the two protocols themselves. These differences include the following:

- TDMoIP uses the structure-indication and structure-reassembly mechanisms, whereas CESoPSN uses the structure-locking algorithm. Therefore, CESoPSN transmits consistent, fixed-length packets, whereas TDMoIP has several payload lengths (minimum of 48 bytes) depending on the type of traffic being transmitted.
 - This allows for CESoPSN to have a lower packetization delay in instances where the pseudowire is carrying multiple timeslots.
 - By the same token, using structure-locking creates inefficiencies when transporting unstructured T1 streams. CESoPSN payload is required to begin at a frame boundary. This means that T1 frames must be padded to create the consistent packet size.
- CESoPSN mandates use of RTP.
- By transporting entire frames, CESoPSN simplifies packet loss compensation.
 - CESoPSN does not need to look at individual timeslots. Instead, CESoPSN inserts a packet of all 1's, simulating TDM fault mechanisms.
- TDMoIP must look for structure pointers, jump to the beginning of the next structure, and insert interpolated data.

ATM Pseudowires

An ATM pseudowire uses an MPLS network for the transport of ATM cells.

Note ATM pseudowires follow the PWE-3 architecture, and therefore only ATM-specific information is included in this section.

Defined in RFC 4717, ATM pseudowires provide many of the same benefits as TDMoIP and CESoPSN:

- Simplification of network architecture and reduction of number of core networks supported
- Preserving existing legacy services during migration to next-generation IP services
- Using a common PSN to provide both legacy and next-generation services

The generic architecture of an ATM pseudowire service is illustrated in Figure 7-16.

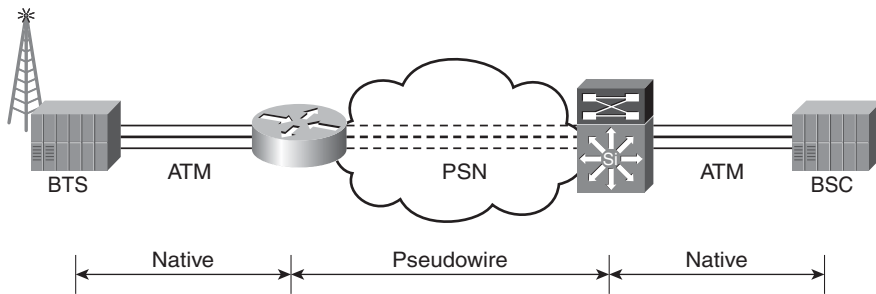


Figure 7-16 *ATM Pseudowire Architecture*

As with all pseudowire services, the intent of an ATM pseudowire is not to perfectly emulate the traditional service, but instead to provide a transport mechanism for the service. This means there are distinct differences between the traditional ATM service and an ATM pseudowire, namely the following:

- ATM cell ordering is optional.
- ATM QoS model can be emulated, but is application-specific in nature.
- ATM flow control mechanisms are not understood by the MPLS network, and therefore cannot reflect the status of the PSN.
- Control plane support for ATM Switched Virtual Circuits (SVCs), Switched Virtual Paths (SVPs), Soft Permanent Virtual Circuits (SPVCs), and Soft Permanent Virtual Paths (SPVPs) are supported only through vendor-proprietary solutions.

Generic Encapsulation

Figure 7-17 illustrates the general encapsulation method for ATM pseudowires.

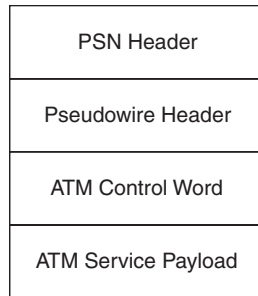


Figure 7-17 *ATM Generic Encapsulation Method*

The PSN Transport header is used to transport the encapsulated ATM information across the network. The structure of this header depends on the type of transport protocol being used.

The pseudowire header maps an ATM service to a particular tunnel. If MPLS is being used, for instance, the pseudowire header would be an MPLS label.

The ATM Control Word contains the length of the ATM service payload, sequence number, and other relevant control bits. There are two types of control words that can be used, as follows:

- **Generic Control Word:** This control word is used for ATM One-to-One cell mode and ATM Adaptation Layer (AAL) 5 Protocol Data Unit (PDU) frame mode.
- **Preferred Control Word:** This control word is used for ATM N-to-One cell mode and AAL5 Service Data Unit (SDU) frame mode.

Cell Mode Modes

There are two methods for encapsulation of ATM cells: N-to-One mode and One-to-One mode.

N-to-One Mode

N-to-One mode is the only required mode for ATM pseudowires. This encapsulation method maps one or more ATM Virtual Circuit Connections (VCCs) or Virtual Path Connection (VPC) to a single pseudowire. The N-to-One mode allows a service provider to offer an ATM PVC- or SVC-based service across a PSN.

With N-to-One mode, the ATM header is unaltered during this encapsulation, so ATM Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) are present. This information is required to be preserved since concatenation of cells from multiple VCCs may occur.

N-to-One mode has the following limitations:

- Explicit Forward Congestion Indication (EFCI) cannot be translated to a PSN congestion mechanism. Conversely, PSN congestion mechanisms cannot be translated to EFCI.
- Cell header detection/correction that exists in ATM cannot be replicated in the PSN.
- Cell encapsulation only functions for point-to-point MPLS Label Switched Paths (LSPs). Point-to-multipoint and multipoint-to-point are not supported.

One-to-One Mode

One-to-One mode is an optional encapsulation method that maps a single VCC/VPC to a single pseudowire. Because only one VPI/VCI is transported on a pseudowire, the pseudowire context (MPLS Label, for example) is used to derive the corresponding VPI/VCI value. The One-to-One mode also allows a service provider to offer an ATM PVC- or SVC-based service across a PSN.

The same limitations as N-to-One mode apply for One-to-One mode.

AAL5 Frame Encapsulation

There are different optional encapsulation methods that exist specifically for AAL5—one for SDUs and one for PDUs.

AAL5 SDU frame encapsulation is more efficient than using either N-to-One or One-to-One for AAL5. Because the pseudowire edge needs to understand the AAL5 SDU in order to transport it, the device must support segmentation and reassembly.

AAL5 PDU frame encapsulation allows for the entire AAL5 PDU to be encapsulated and transported. Because of this, all necessary ATM parameters are transported as part of the payload. This simplifies the fragmentation operation because all fragments occur at cell boundaries, and the Cyclical Redundancy Check (CRC) from the AAL5 PDU can be used to verify cell integrity.

Defect Handling

Figure 7-18 illustrates the four possible locations for defects on the ATM pseudowire service. These four locations are as follows:

- (A): ATM connection from ATM device to pseudowire edge device.
- (B): ATM interface on the pseudowire edge device.
- (C): PSN interface on the pseudowire edge device.
- (D): PSN network.

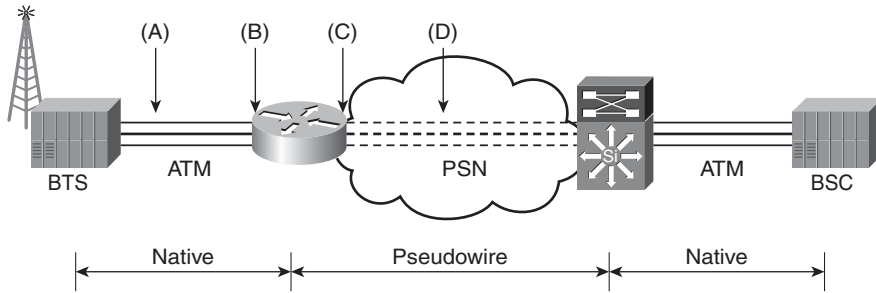


Figure 7-18 *ATM Defect Locations*

In all cases, the pseudowire edge device uses standard ATM signaling methods to notify the receiver of cell loss. This information is transported across the PSN to the receiver.

SONET/SDH Circuit Emulation over Packet

Note SONET/SDH Circuit Emulation over Packet (CEP) follows similar premise and structure to all other PWE3 standards, and therefore only SONET/SDH-specific information is included in this section.

To transport SONET/SDH over packet, the Synchronous Payload Envelope (SPE) or virtual tributary (VT) is fragments, prepended with a pseudowire header, and optionally a RTP header. The basic CEP header is illustrated in Figure 7-19.

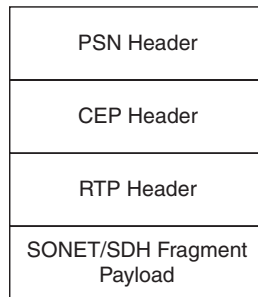


Figure 7-19 *Basic CEP Header*

The CEP header supports both a basic mode, which contains the minimum functionality necessary to perform SONET/SDH CEP, and an extended mode, which contains additional capabilities for some optional SONET/SDH fragment formats. These options fall into two categories, as follows:

- Dynamic Bandwidth Allocation (DBA) is an optional mechanism for SPE transmission suppression on a channel-by-channel basis when one of two trigger conditions are met—that the SONET/SDH path or VT is not transmitting valid end-user data or that the circuit has been de-provisioned, or unequipped.
- Service-Specific Payload Formats are special encapsulations that provide different levels of compression depending on the type and amount of user data traffic. The payload compression options are provided for asynchronous T3/E3 Synchronous Transport Signal 1 (STS-1), fractional VC-4, fractional STS-1, and others.

Fragments

When fragmented, the SONET/SDH fragments must be byte-aligned with the SONET/SDH SPE or VT. That is, the SONET/SDH byte cannot be fragmented, and the first bit in the SONET/SDH must be the most significant bit in the SONET/SDH fragment. In addition, bytes are placed into the fragment in the order in which they are received.

SONET/SDH CEP lies above the physical layer, and assumes that native transport functions, such as physical layer scrambling/unsrambling that SONET/SDH optical interfaces perform as part of their binary coding, occurs as part of the native service. However, CEP does not assume that scrambling has occurred, and fragments are constructed without consideration of this.

Abis/Iub Optimization for GSM Networks

Chapter 2 discusses GSM RAN Abis interface and UMTS RAN Iub interface. GSM RAN Optimization is a method for optimizing and encapsulating structured (NxDSD0) TDM signals between the BTS and BSC into IP packets. The optimization is performed by removing nonessential traffic on the GSM Abis interface. Such nonessential traffic includes idle subrates that have a repeating pattern every 20 msec, idle TRAU frames used to keep subrates in-sync for GPRS, and speech TRAU frames with silence used to provide white noise that lets the other party know that the call has not been dropped. In addition, High-Level Data Link Control (HDLC) signaling data flows, which are part of the GSM Radio Link Protocol (RLP), can be optimized by suppressing inter-frame flags.

Note Chapter 2 describes the GSM Abis interface and UMTS Iub interface, including the protocols, functions, and capabilities of these interfaces.

Optimization is done at the bit level, resulting in no impact to voice quality or data throughput. This bit level optimization makes GSM Optimization radio-vendor independent and radio software version independent. Figure 7-20 illustrates GSM Abis optimization.

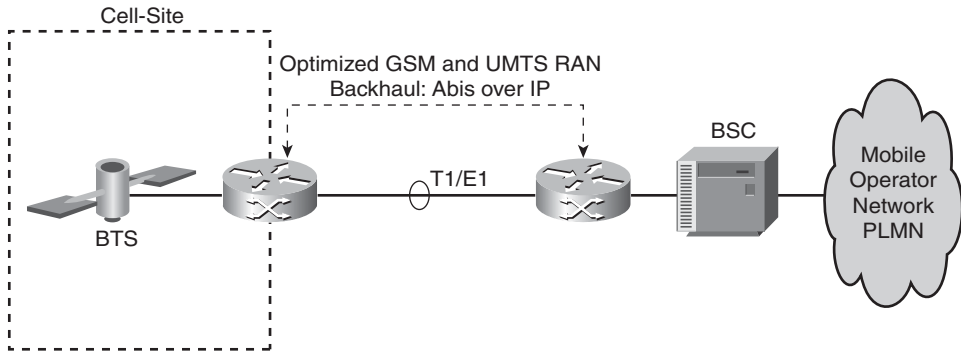


Figure 7-20 *GSM Abis Optimization*

Timing

Today's mobile networks are reliant on accurate timing, or accurate distribution and synchronization of precise clock information, in order to accurately transport voice and data traffic. In existing radio architectures, frequency synchronization is typically achieved through the backhaul network itself. These legacy architectures are based on TDM backhaul. Because TDM carries time inherently, the radio architecture itself was designed with frequency synchronization embedded in the physical layer.

Radio Access Network and Synchronization

The need for synchronization has always been inherent in Radio Access Networks. As discussed in Chapter 1, "Introduction to Radio Systems," radio networks fall into two categories:

- **Frequency Division Duplexing (FDD)**, in which two sets of frequencies are used for transmit/receive. These networks require frequency synchronization in order to accurately send and receive traffic.
- **Time Division Duplexing (TDD)**, in which a single frequency is used for transmit/receive and a demarcation based on timeslots is identified for both transmission and reception. These networks require time synchronization in order to accurately send and receive traffic.

Table 7-3 provides a reference for today's wireless technologies and their synchronization requirements.

Table 7-3 *Wireless Technologies and Synchronization Requirements*

Application	Service
TDM Support	Frequency/Timing
3GPP (GSM, WCDMA FDD)	Frequency
3GPP (LTE, eMBMS)	Time (TDD Mode) Frequency (FDD Mode)
WiMAX (IEEE 802.16d/e)	Frequency Time
DVB-T/DVB-H	Time
TD-SCDMA	Time
3GPP2 CDMA	Frequency

In mobile networks, high-quality frequency and time/phase synchronization are useful and in some cases required. The accuracy of these services differs based on the radio technology and standards organization. The synchronization service accuracy based on application (radio technology) is referenced in Table 7-4.

Table 7-4 *Synchronization Service Requirements*

Synch Service	Application	Expected Quality
Frequency	TDM Support	Primary Reference Source (PRS) Traceable
	3GPP/3GPP2 BS	Frequency assignment shall be less than $\pm 5 \times 10^{-8}$ (± 0.05 parts-per-million [ppm])
	WiMAX (IEEE 802.16)	.16D: Reference frequency accuracy shall be better than $\pm 8 \times 10^{-6}$ ($\pm 2 \times 10^{-6}$) .16e: Reference Frequency Tolerance at BS: $\leq \pm 1 \times 10^{-6}$
	DVB-T/H/SH/T2	Frequency shall provide a traceable Primary Reference Clock (PRC) source for 10MHz signal
Time	802.16D/e TDD	Better than $5 \mu\text{s}$
	DVB-T/H	Within $1 \mu\text{s}$ accuracy
	3GPP LTE	Better than or equal to $3 \mu\text{s}$
	3GPP2 CDMA BS	<i>Should</i> be less than $3 \mu\text{s}$ <i>Shall</i> be less than $10 \mu\text{s}$
	3GPP eMBMS	TBD

Network Synchronization Options

In order to achieve the stringent quality requirements identified in Table 7-4, there are multiple network synchronization options, as follows:

- **Free-running oscillator:** A free-running oscillator is one that has never been synchronized to a reference clock. This oscillator's accuracy is based on the technology within the oscillator. In this model, each network element would either contain or be connected directly to a free-running oscillator and rely on the local clock for all synchronization. Table 7-5 highlights the different oscillator technologies and accuracy.

Table 7-5 *Oscillator Technology and Accuracy*

Technology	Stratum Level	Accuracy
Hydrogen Maser		1×10^{-15}
Cesium	1	1×10^{-11}
Rubidium	2	5×10^{-11}
Crystal	3/4	4.6×10^{-6}

- **Global Positioning System (GPS):** GPS synchronization relies on a GPS satellite to provide the clock source. All GPS satellites contain a Cesium standard clock. Because GPS satellites circle the globe twice per day, any device relying on GPS for synchronization must also calculate geographic location in order to determine from which satellite it can receive signals.
- **Physical layer:** Physical layer synchronization has long been used for transporting clock information. SONET/SDH and T1/E1 are well-known examples of physical layer synchronization. More recently, Synchronous Ethernet (SyncE) uses the Ethernet physical layer interface to pass timing from node to node in much the same way. SyncE is discussed later in this chapter in “Packet-Based Timing.”
- **Higher layer:** Higher-layer synchronization relies on a packet-based protocol to distribute clocking information. IEEE 1588v2 and Network Time Protocol (NTP) are discussed later in this chapter in “Packet-Based Timing.”

Introduction to Timing

This section provides an overview of timing, including definitions, clock hierarchies, and reference clock architectures. These hierarchies and architectures are leveraged repeatedly in many different circuit-switched and packet-switched timing protocols, and understanding these architectures provides the foundation knowledge for the remainder of this chapter.

Understanding Timing Definitions

Before defining architectures, it is important to understand some of the basic definitions that will be used continually throughout the remainder of this chapter. This section provides some of these basic definitions.

Precision, Accuracy, and Stability

Precision, accuracy, and stability are used to measure the reliability of a clock signal.

- **Precision** is defined as the ability of a measurement to be consistently reproduced. When referencing timing, precision refers to the amount of variation of a set of measurements.
- **Accuracy** is defined as the ability of a set of measurements to consistently match the exact value being measured. In the case of timing, the value being measured is a predefined reference time.
- **Stability** is defined as the amount a measurement changes as a function of time or environment (temperature, shock, and so on).

The goal of every clock is to be highly precise, highly accurate, and highly stable. In practice, however, every clock signal has unique characteristics of precision, accuracy, and stability. These clock signals can fall into six broad categories, as follows:

- **Accurate, precise, stable:** This clock source produces a consistent measurement as a function of time and environment that is representative of the predefined reference time. Figure 7-21 illustrates this type of clock source.

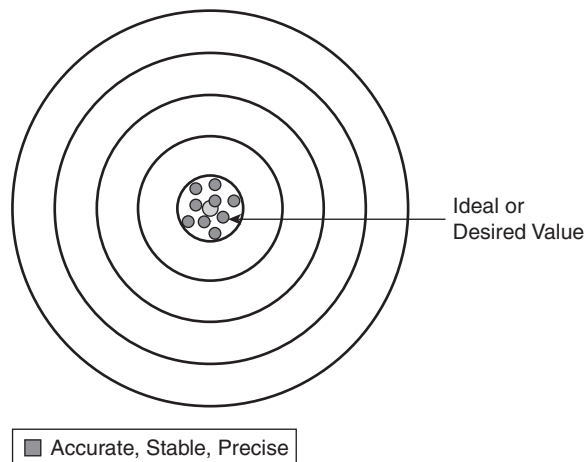


Figure 7-21 *Accurate, Precise, Stable*

- **Accurate, imprecise, stable:** This clock source produces a large variety of measurements, consistent as a function of time and environment, which are representative of the predefined reference time. Figure 7-22 illustrates this type of clock source.

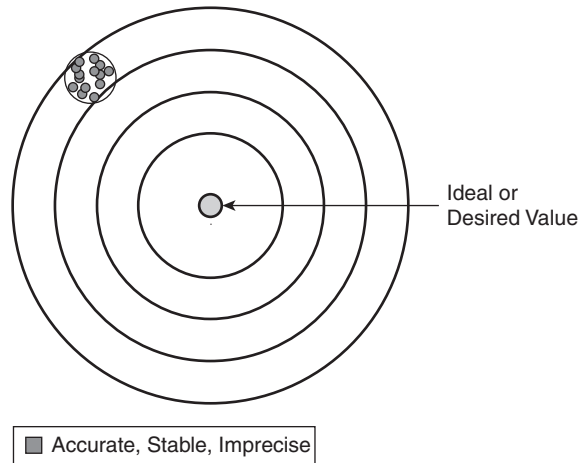


Figure 7-22 *Accurate, Imprecise, Stable*

- **Precise, accurate, unstable:** This clock source produces a small variety of measurement, inconsistent as a function of time and environment, which are representative of the predefined reference time. Figure 7-23 illustrates this type of clock source.

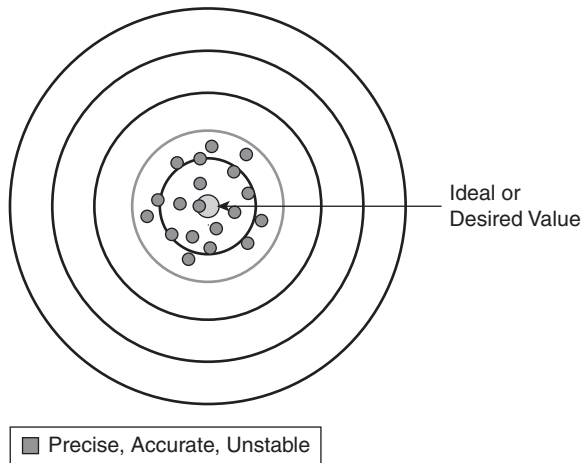


Figure 7-23 *Precise, Accurate, Unstable*

- **Inaccurate, precise, stable:** This clock source produces a small variety of measurements, consistent as a function of time and environment, which are not representative of the predefined reference time. Figure 7-24 illustrates this type of clock source.

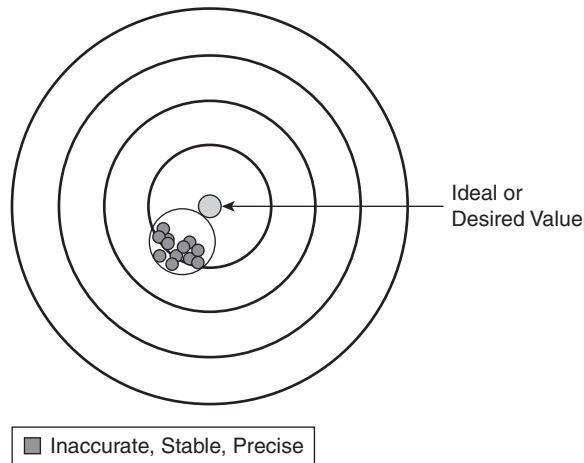


Figure 7-24 *Inaccurate, Precise, Stable*

- **Accurate, imprecise, unstable:** This clock source produces a large variety of measurements, inconsistent as a function of time and environment, which are representative of the predefined reference time. Figure 7-25 illustrates this type of clock source.

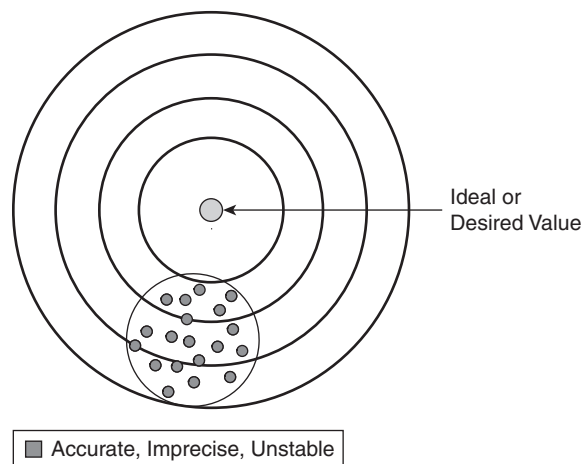


Figure 7-25 *Accurate, Imprecise, Unstable*

- **Inaccurate, imprecise, stable:** This clock source produces a large variety of measurements, consistent as a function of time and environment, which are not representative of the predefined reference time. Figure 7-26 illustrates this type of clock source.

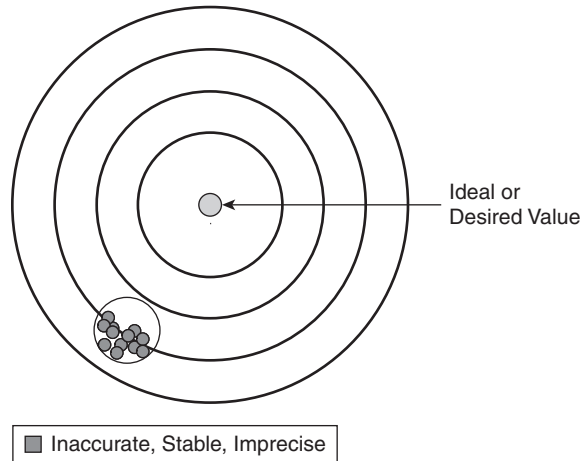


Figure 7-26 *Inaccurate, Imprecise, Stable*

- **Inaccurate, precise, unstable:** This clock source produces a small variety of measurements, inconsistent as a function of time and environment, which are not representative of the predefined reference time. Figure 7-27 illustrates this type of clock source.

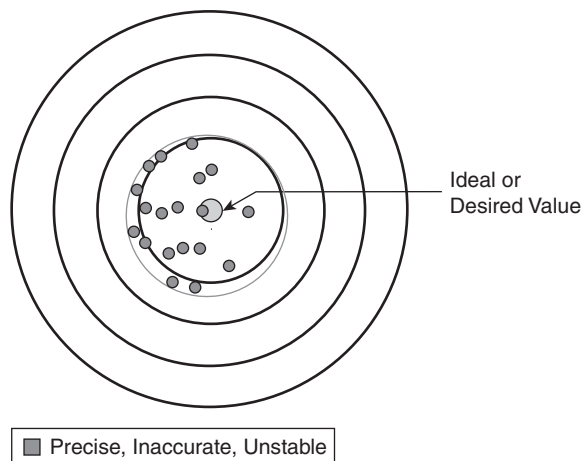


Figure 7-27 *Inaccurate, Precise, Unstable*

- **Inaccurate, imprecise, unstable:** This clock source produces a large variety of measurements, inconsistent as a function of time and environment, which are not representative of the predefined reference time. Figure 7-28 illustrates this type of clock source.

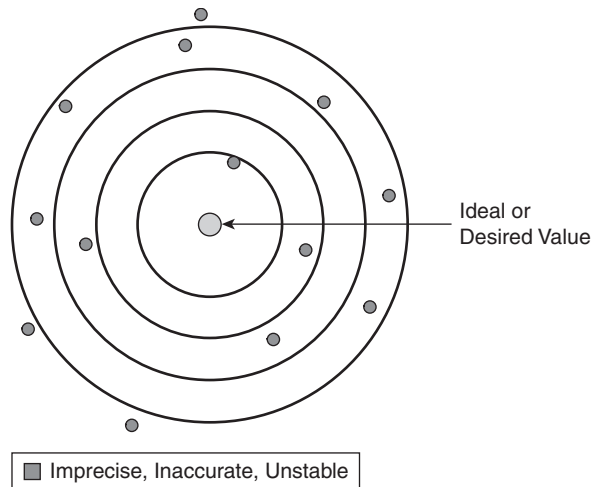


Figure 7-28 *Inaccurate, Imprecise, Instable*

Synchronization

Synchronization refers to timing that requires multiple devices to operate as part of a system at the exact same time. In transporting time-based data traffic, synchronization of all network elements can be achieved in multiple ways. These elements can be synchronized in the following two key ways:

- Frequency synchronization refers to the need for two network elements (transmitter and receiver) to operate at the same rate—that is, both network elements need to operate at the same rate.
- Phase/Time synchronization refers to the need for two network elements to be able to accurately identify the end of a frame or byte. Phase/time synchronization first requires frequency synchronization.

Jitter

Jitter refers to the short-term fluctuations of a timing signal from their ideal positions in time (variations greater than or equal to 10 Hz). Jitter, which is constant over time, makes a clock source unstable. Figure 7-29 illustrates the effects of jitter.

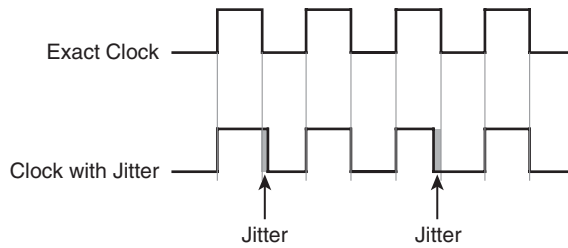


Figure 7-29 *Jitter*

Wander

Wander refers to the long-term fluctuations of a timing signal from their ideal positions in time (variations less than 10 Hz). Unlike jitter, wander is not constant over time, and accumulates in a network. This accumulation leads to either incorrect synchronization or loss of synchronization. Figure 7-30 illustrates the effects of wander. Frequency Drift is a specific type of wander where a constant accumulation occurs.

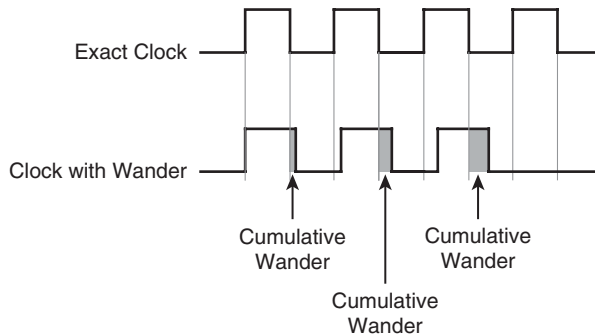


Figure 7-30 *Frequency Drift*

Timing Architectures

Many different timing architectures have been deployed to all accomplish the same end-goal—maximum accuracy, stability, and precision of timing information to all nodes within the network. These timing architectures are dictated by standards-based hierarchies, with each tier of the hierarchy representing a different level of precision. Once the hierarchy is established, operators have varied in their deployment models for distribution and synchronization of this clock information. This section looks at the various clock hierarchy considerations and network architectures that have been deployed.

Clock Hierarchy

Clock standards have a hierarchy defined by the International Telecommunications Union (ITU) Telecommunications Standardization Sector (ITU-T) and the American National Standards Institute (ANSI). For simplicity, ANSI clock hierarchy is used within this chapter. The hierarchy defines the relationship between every clock within a synchronization domain and the model for distribution across the domain. The hierarchy is based on five quality metrics, as follows:

- **Accuracy.**
- **Holdover Stability**, or the ability to continue to preserve accurate time when a clock's reference signal is lost.
- **Pull-In/Hold-In Range**, or the largest offset/differential between the reference frequency and nominal frequency for which the clock can still acquire “lock.”
- **Wander.**
- **Time to First Frame (193 bits) Slip**, or the length of time that the clock can remain accurate.

The ANSI and ITU-T clock standards are summarized in Table 7-6.

Table 7-6 *ANSI/ITU-T Clock Standards*

ANSI Stratum	ITU-T Clock Level	Accuracy	Holdover Stability	Pull-In Range	Wander	Time to First Frame Slip
1	PRC	1×10^{-11}	None	None	None	72 days
2	Type II	± 0.016 ppm	$\pm 1 \times 10^{-10}$ /day	0.016 ppm	0.001 Hz	7 days
-	Type I	Not Defined	$\pm 2.7 \times 10^{-9}$ /day	0.01 ppm	0.003 Hz	
3E	Type III	± 4.6 ppm	$\pm 1.2 \times 10^{-8}$ /day	4.6 ppm	0.001 Hz	3.5 hours
3	Type IV	± 4.6 ppm	$\pm 3.9 \times 10^{-7}$ /day	4.6 ppm	3 Hz	6 minutes
-	Option I	± 4.6 ppm	$\pm 2 \times 10^{-6}$ /day	4.6 ppm	1–10 Hz	
SMC	Option 2	± 20 ppm	$\pm 4.6 \times 10^{-6}$ /day	20 ppm	0.1 Hz	
4	4	± 32 ppm	None	32 ppm	None	

The network is controlled by a Primary Reference Clock (PRC), or Stratum 1 clock, which is accurate to 1×10^{-11} . Synchronization requires the distribution of the reference signal from the PRC to all network elements. The master-slave method is used for this propagation. The synchronization between hierarchies is unidirectional; that is, synchronization is always transferred from a higher layer to a lower layer. The Stratum 1 clock receives information from any number of Stratum 0 clocks. The Stratum 1 clock provides the reference

clock for multiple Stratum 2 clocks, and each Stratum 2 clock provided the reference clock for multiple Stratum 3 clocks. This hierarchy is illustrated in Figure 7-31.

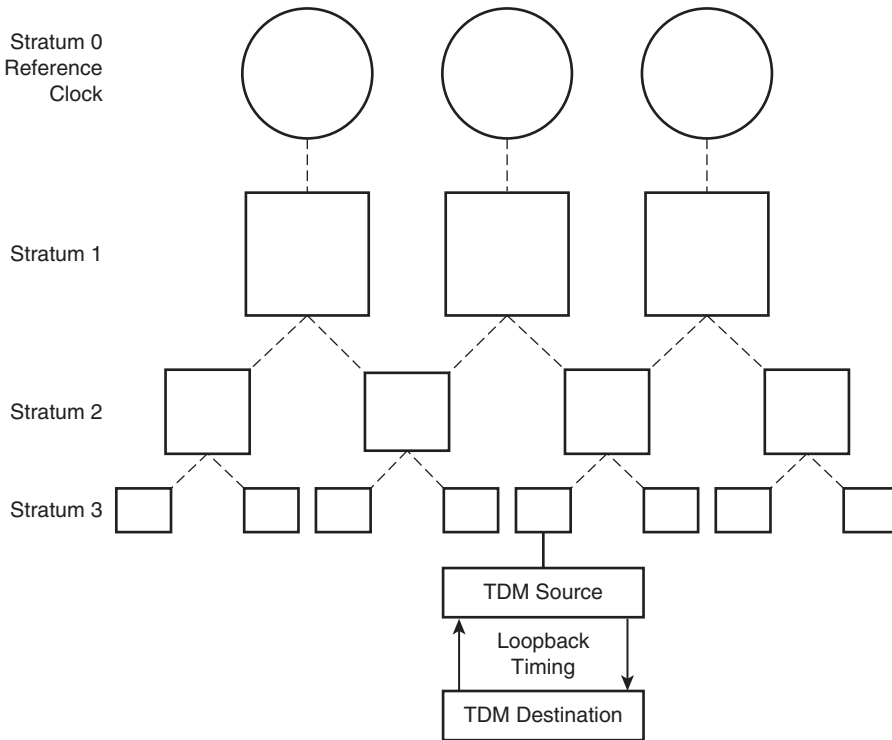


Figure 7-31 *Clock Hierarchy*

PRC Architectures

A PRC is designed to provide highly-accurate time, and therefore tends to rely on more than one Primary Reference Source (PRS). A Cesium-beam tube is always used in the generation of a PRC signal because of their accuracy in ensuring no aging or frequency drift. Three types of PRCs have emerged (and have been identified by The European Telecommunications Standards Institute [ETSI]), as follows:

- Autonomous PRCs with up to three local Cesium tubes incorporated within the PRC and used as the PRS.
- Radio-controlled PRCs, which use remote Cesium tubes in the radio infrastructure (either satellite-based, like GPS, or land-based, like Long Range Aid to Navigation [LORAN]-C) as the PRS.
- PRCs that use a combination of local Cesium tubes and radio-based Cesium tubes.

In the event of a failure of one of the PRS, the PRC can use one of the other PRS as the reference; however, the failover time must be within the Maximum Time Interval Error (MTIE) defined by ITU-T.

Table 7-7 depicts the MTIE defined by ITU-T for each clock level.

Table 7-7 MTIE by Stratum

ANSI Stratum	ITU-T Clock Level	Phase Transient
1	PRC	-
2	Type II	MTIE < 150ns
-	Type I	MTIE < 1μs
3E	Type III	MTIE < 150ns
3	Type IV	MTIE < 1μs
-	Option I	MTIE < 1μs
SMC	Option 2	MTIE < 1μs
4	4	No Requirement

Figure 7-32 illustrates these three types of PRC architectures.

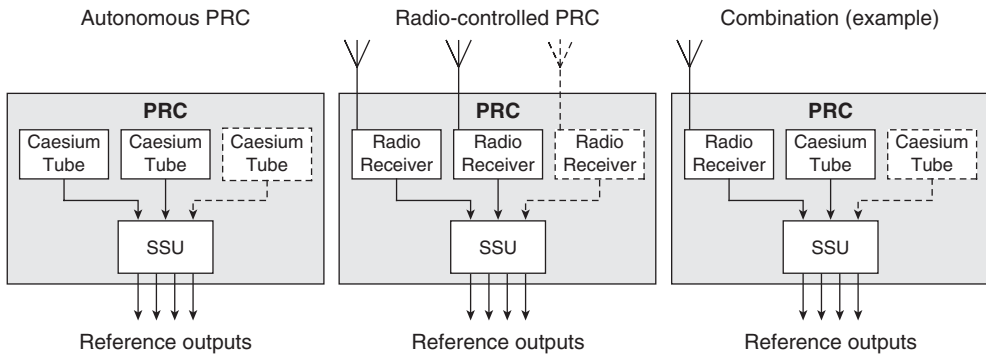


Figure 7-32 PRS/PRC Architectures

PRCs can be deployed in multiple different architectures. These architectures provide different levels of resiliency, complexity, and cost. In general, the following principles are adhered to in all PRC architectures:

- The synchronization distribution is tree-shaped.
- The synchronization network can be decomposed into multiple synchronization chains.

- Several stratum of slave clocks with different properties/roles exist.
- A higher-quality level is never slaved to a reference signal of a lower-quality.
- The SSU provides timing to a portion of the network. If the SSU's reference signal is lost, the SSU supplies timing to the network downstream.
- Radio-controlled PRCs use remote Cesium tubes in the radio infrastructure (either satellite-based, like GPS, or land-based, like Long Range Aid to Navigation [LORAN]-C) as the PRS.
- PRCs use a combination of local Cesium tubes and radio-based Cesium tubes.

Figure 7-33 provides an example of a synchronization network, including the Synchronization Supply Unit (SSU).

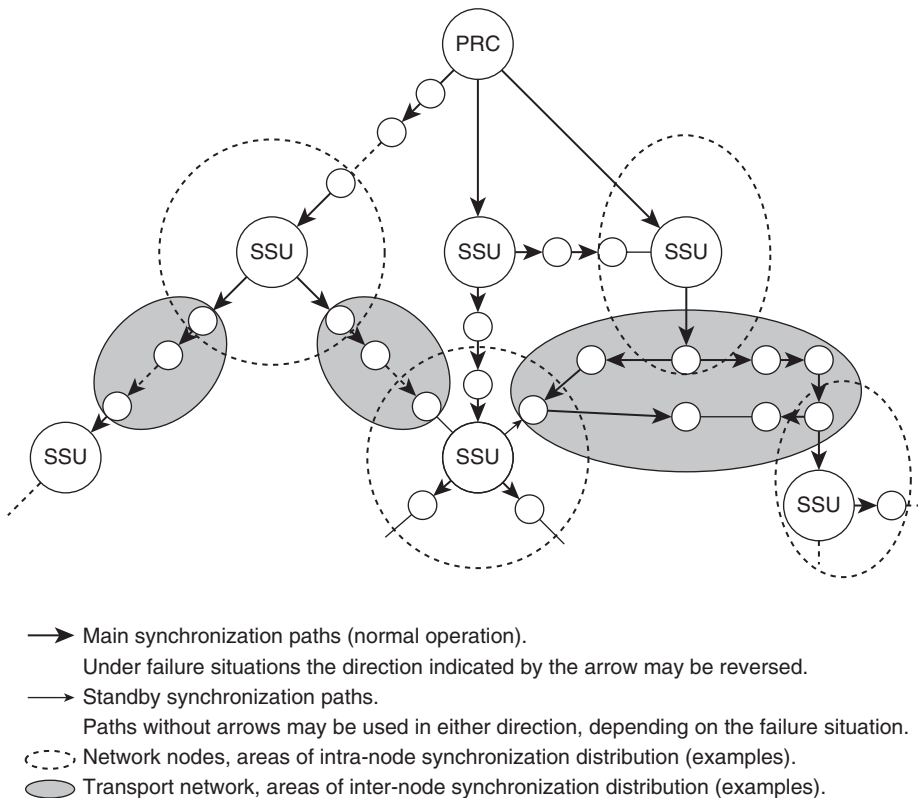


Figure 7-33 Synchronization Network Example

SSUs are used to provide reliable distribution of clock information. SSUs are part of every synchronization domain, including the PRC. SSUs receive clocking information from higher-layer clocks and distribute the clock information to all local equipment. SSUs

also have the ability to provide accurate holdover mode, in the event that their clock source is lost.

The SSU does not belong to the transport network, but only provides the timing for the transport network elements within its synchronization domain.

There are two primary methods for providing clock synchronization, as follows:

- Master-slave synchronization, which has a single PRC from which all other clocks are synchronized. Synchronization in this method is achieved by sending timing signals from one clock to the next, in a hierarchical fashion. Figure 7-34 illustrates this master-slave synchronization network architecture.

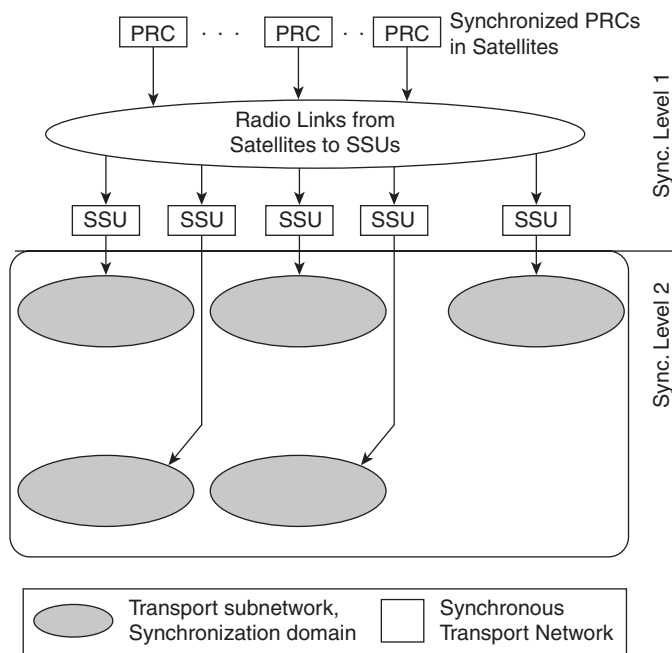


Figure 7-34 *Master-Slave Synchronization Network*

- Mutual synchronization, in which all clocks are interconnected. In this method, there is no unique PRC or hierarchical structure defined. Figure 7-35 illustrates this mutual synchronization network architecture.

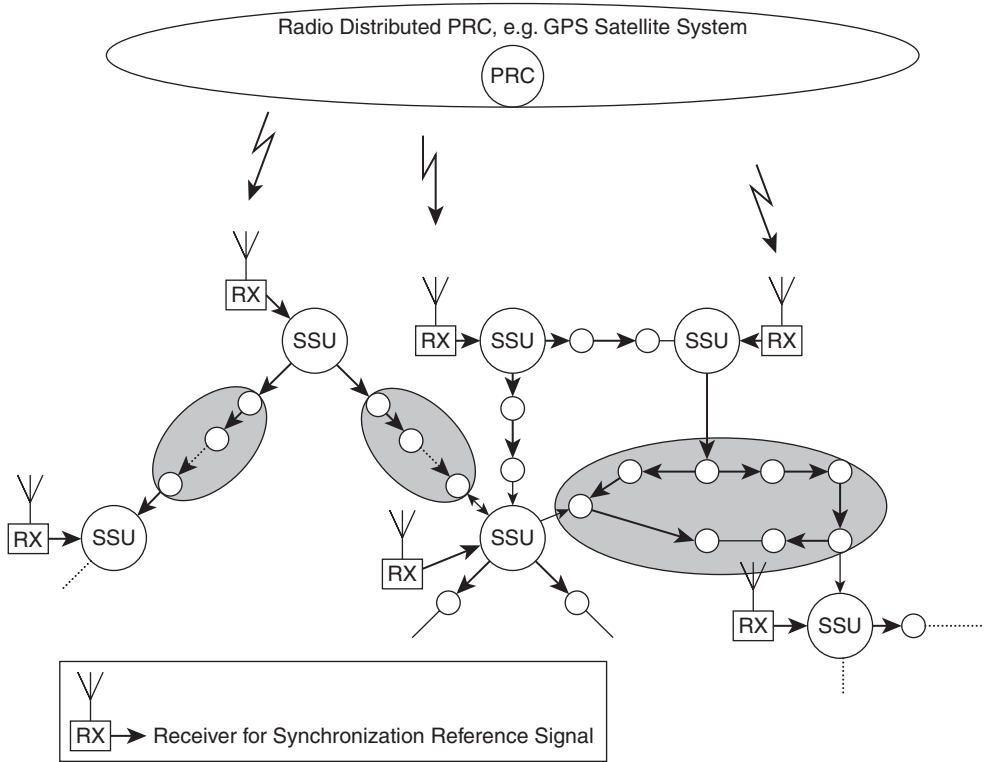


Figure 7-35 *Mutual Synchronization Network*

In practice, master-slave and mutual synchronization methods may be deployed in combination. In this architecture, the main PRC is usually an autonomous or combined PRC (see Figure 7-32). Synchronization from the main PRC is done in standard master-slave hierarchical fashion. At Level 2, the SSU is connected to both the PRC (primary) and an off-air PRC (backup).

Figure 7-36 illustrates this combined network architecture. Priorities for clock source and synchronization are identified in the figure.

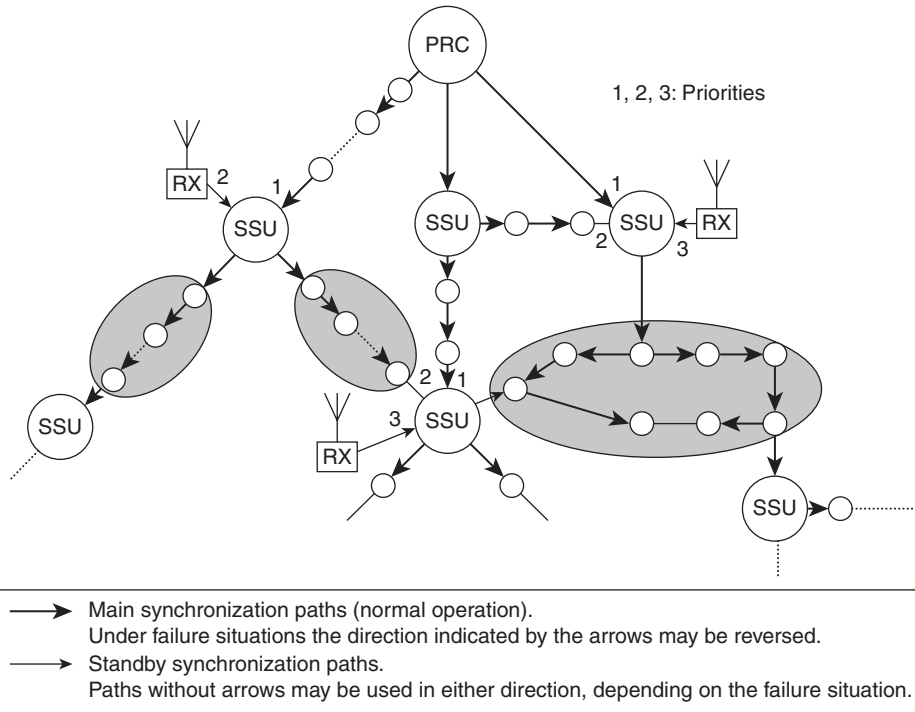


Figure 7-36 Combined Master-Slave and Mutual Synchronization Network

Timing Modes

Timing modes define what a clock is referenced to. Network elements may operate in four different timing modes, as follows:

- External timing, where the reference source signal is received via a local timing interface directly.
- Line timing, where the reference source signal is received from one or more data interfaces that also carries timing information.
- Loop timing, where the reference source signal is received from only one data interface as part of a ring topology.
- Through timing, where the reference source signal is transported transparently across the network element.

These timing modes map to four network architectures—synchronous networks, asynchronous networks, pseudo-synchronous networks, and plesiochronous networks.

Synchronous

A *synchronous network* is one where all clocks within the network have identical long-term accuracy. These networks require synchronization to avoid jitter and wander. Synchronous networks have a single active PRC source signal and rely on line timing to distribute clock information across the network. Figure 7-37 depicts a synchronous network that relies on line timing for clock source.

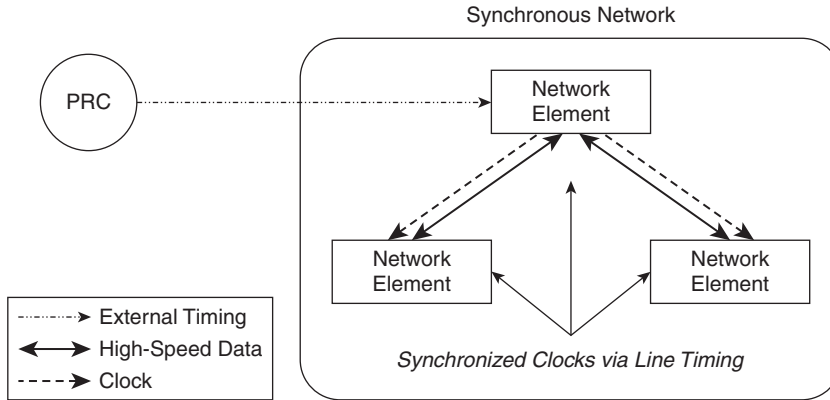


Figure 7-37 *Synchronous Network*

Asynchronous

An *asynchronous network* is one where not all clocks within the network have identical long-term accuracy due to multiple clock sources. In an asynchronous network, clocks are operating in free-running mode. These networks do not require that all clocks be synchronized to operate properly. Figure 7-38 depicts an asynchronous network.

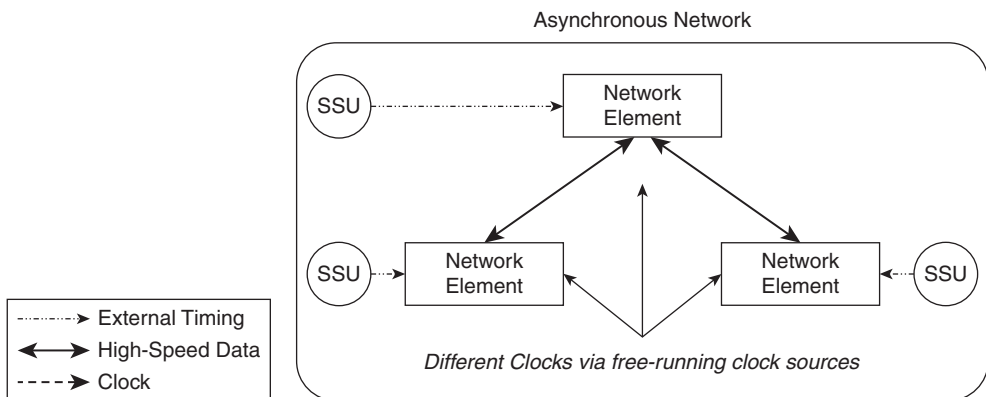


Figure 7-38 *Asynchronous Network*

Pseudo-Synchronous

A *pseudo-synchronous network* is one where not all clocks use the same PRC, but all rely on PRC-level accuracy for their reference source. These networks require synchronization to work properly. Figure 7-39 depicts a pseudo-synchronous network.

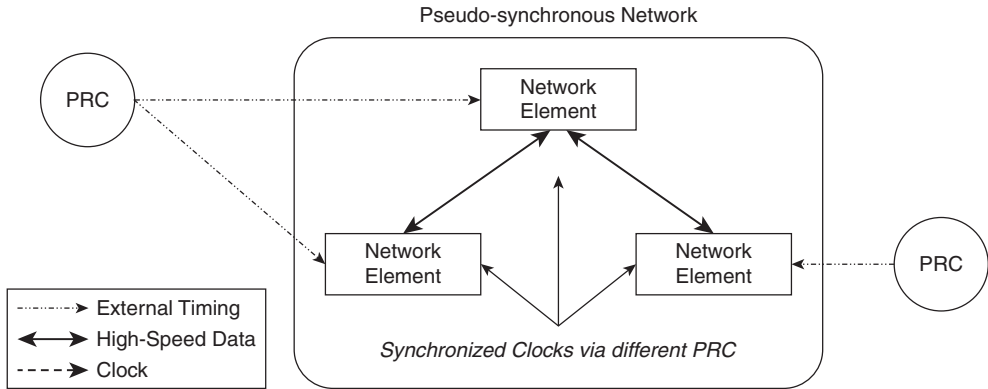


Figure 7-39 *Pseudo-Synchronous Network*

Plesiochronous

A *plesiochronous network* is one where different parts of the network are not perfectly synchronized with each other. Plesiochronous networks operate within a threshold of acceptable asynchronization; that is, two network elements act as if they are synchronized, but must accept and cope with time slips. A plesiochronous network is depicted in Figure 7-40.

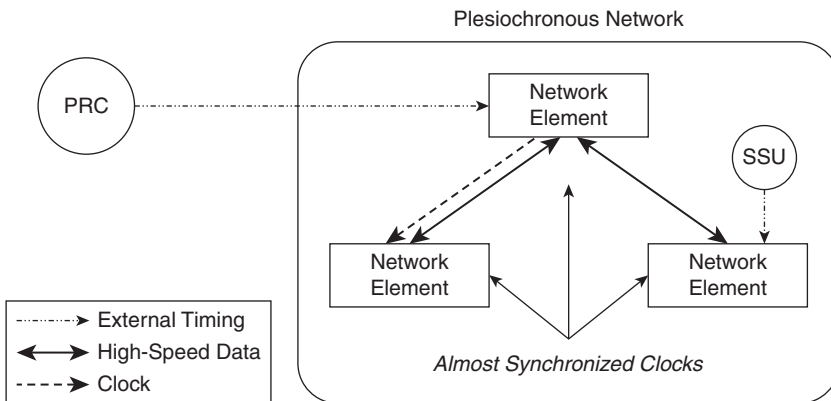


Figure 7-40 *Plesiochronous Network*

Packet-Based Timing

TDM networks are inherently synchronous. All network components must be synchronized with each other to ensure that data is not lost. In a native TDM network, clock synchronization is performed at the physical layer, and clocking information is carried along with data traffic. Clock slips occur when the receiver and transmitter have clocks that either run faster or slower than the other. These clock slips result in frames being either added or lost from the data stream.

IP networks, by nature, are asynchronous, and therefore cannot provide a constant bitrate. Packets reach their destination with random delay, known as jitter or Packet Delay Variation (PDV), already inserted. It is possible to remove random delay with a “jitter buffer,” which temporarily stores all incoming packets and then forwards them at evenly spaced intervals; however, the original reference time is not available to determine what those evenly spaced intervals should be. Due to this, it is not possible to use the physical layer clock synchronization information from the native TDM frame for accurate clocking over pseudowires.

Although pseudowire endpoints do not need the clock synchronization information directly to implement the packet-switching functions, the constant bitrate applications that leverage the pseudowire transport must receive accurate timing information. This requires that the packet-switched network—that is, the pseudowire itself—provide this information to the applications. In such architecture, the reference clock may be connected directly to the synchronous network elements on each side of the pseudowire (see Figure 7-41) or to the pseudowire interworking function (see Figure 7-42).

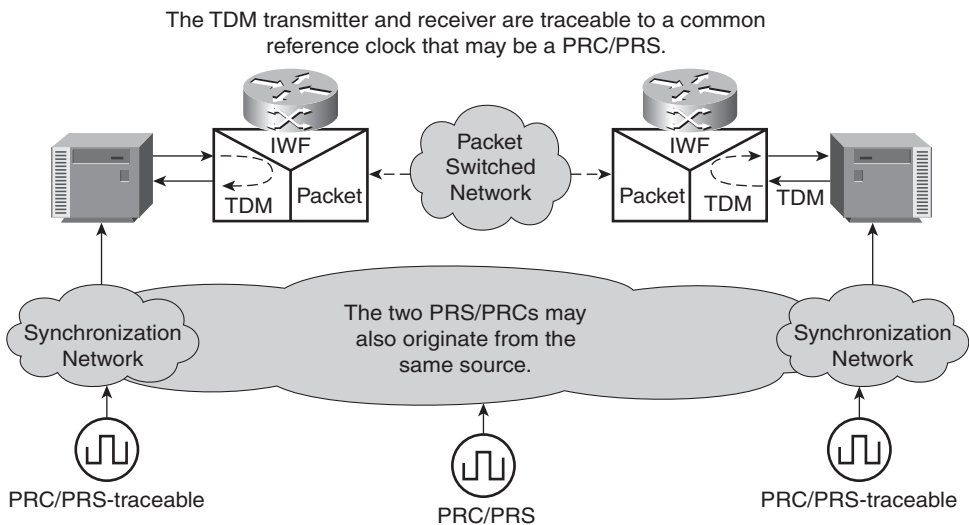


Figure 7-41 *Pseudowire Network Synchronization—Reference Clock Connected to Sync Network Elements*

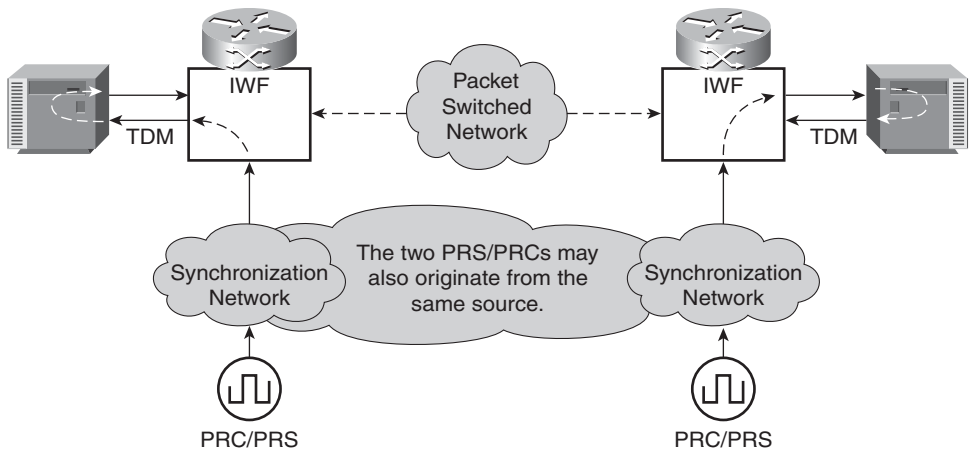


Figure 7-42 *Pseudowire Network Synchronization—Reference Clock Connected to Pseudowire IWF*

Although there are a large number of solutions for providing synchronization information, the same models presented previously in the “Timing Modes” section apply to packet-based networks, namely external timing, line timing, and loop timing.

Clock Recovery over Packet

Clock recovery is an important consideration when providing circuit emulation services over a PSN. The receiving Interworking Functions (IWF) must accurately recover the clock source from the sending IWF. There are two methods to provide clock recovery over packet, as follows:

- **Differential Clock Recovery** involves having a reference clock available at both sides of the pseudowire. Only the difference between the reference clock and the IWF service clock is transmitted across the pseudowire. Although this solution provides accurate frequency information and is tolerant to network delay, delay variation (jitter), and packet loss, the differential clock recovery solutions are expensive because they require multiple reference clocks. CESoPSN optionally may use differential clock recovery. Figure 7-43 illustrates differential clock recovery.
- **Adaptive Clock Recovery** involves having a reference clock available only at one side of the pseudowire. A timestamp is applied to all outbound packets by the sending IWF. The receiving IWF uses the information in the timestamp to recover the original reference clock information. Although this solution is less expensive (only a single reference clock is required), adaptive clock recovery is more susceptible to delay variation. TDMoIP uses adaptive clock recovery. Figure 7-44 illustrates adaptive clock recovery.

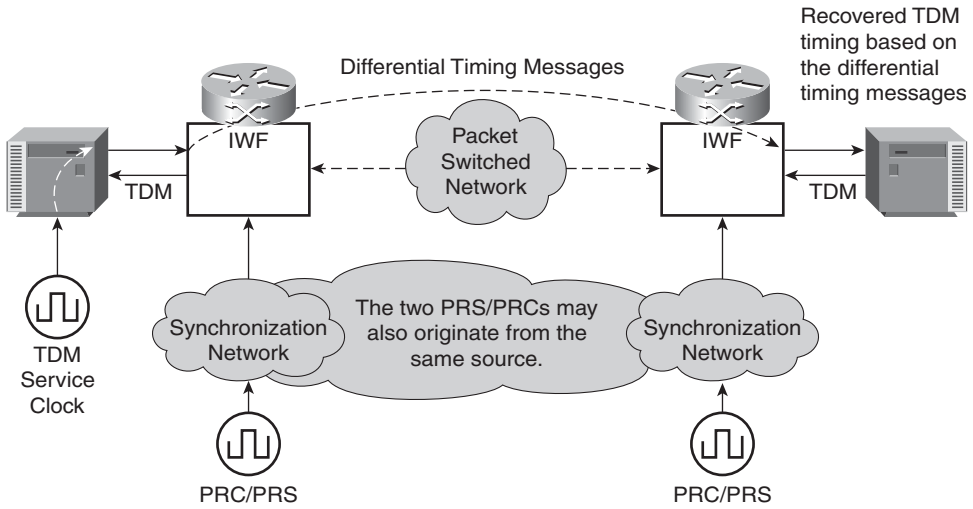


Figure 7-43 *Differential Clock Recovery*

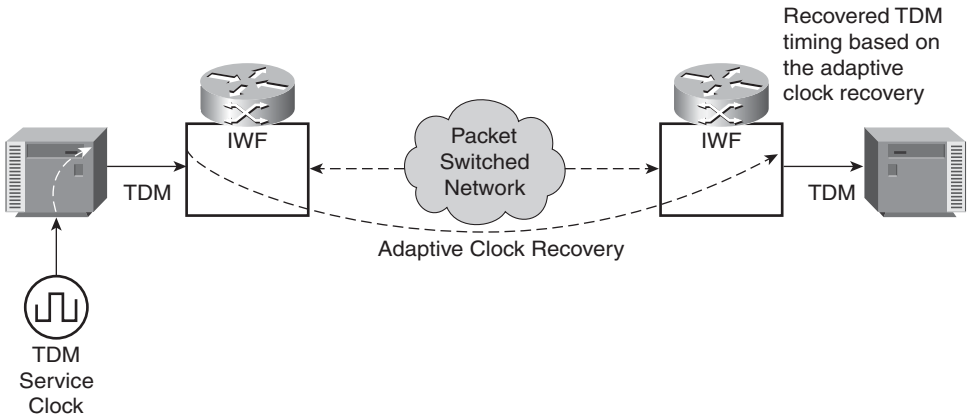


Figure 7-44 *Adaptive Clock Recovery*

Timing over Packet Solutions

There are four technologies for addressing synchronization over a packet network: Synchronous Ethernet (SyncE), Precision Time Protocol (PTP), Network Time Protocol (NTP), and Timing over IP Connection and Transfer of Clock BOF (TICTOC).

Any timing protocol should operate over the generic Internet with little or no intervention or management. Due to the unpredictable nature of the Internet, however, the accuracy of the protocol is greatly diminished. The accuracy of the frequency and time distribution is improved when operated over a managed network.

SyncE

Synchronous Ethernet (SyncE) is a line-timing method for transporting timing information over the Ethernet physical layer. Built on a Layer 1 model similar to SONET/SDH, SyncE provides accurate frequency synchronization, but does not provide time/phase synchronization.

SyncE specifications and requirements rely on four primary standards, as follows:

- **ITU-T G.8261:** Timing and synchronization aspects in packet network
- **ITU-T G.8262:** Timing characteristics of Synchronous Ethernet equipment slave clock
- **ITU-T G.8264:** Distribution of timing through packet networks
- **ITU-T G.781:** Synchronization layer functions

SyncE standards provide additional functionality to the 802.3 Ethernet standards while maintaining interworking between existing asynchronous Ethernet nodes and synchronous Ethernet nodes.

SyncE uses Synchronization Status Messages (SSMs) to transport timing information. Downstream clocks use the SSM for troubleshooting purposes, as the SSM will communicate if the clock source is a synchronized signal or derived from a free-running oscillator. These SSMs are transmitted using the Ethernet OAM protocol (ITU-T Y.1731 standard).

PTP

IEEE 1588v2, Precision Time Protocol, defined a protocol for precise, real-time, network-wide synchronization accuracy in the sub-millisecond range.

Each PTP domain consists of a number of clocks that synchronize with one another using the PTP protocol. Clocks within a PTP domain may not necessarily be synchronized with clocks within a different PTP domain.

Four types of clocks are defined within PTP, as follows:

- **An Ordinary Clock (OC)** has a single interface in a single PTP domain. The OC may be a master or slave, and may be responsible for providing time to an end node or application.
- **A Boundary Clock (BC)** has multiple interfaces in a single PTP domain. These interfaces may consist of multiple master interfaces, but only a single slave interface. The BC transfers all timing on the slave interface to the master interfaces. The BC can only be responsible for providing time to an application, not an end node.
- **A Transparent Clock (TC)** provides information on the time taken for a PTP message to transit the device and provides this information to all clocks receiving the PTP message. There are two types of transparent clocks:

- A Peer-to-Peer Transparent Clock (P2P TC) also provides corrections for any propagation delay on the link connected to the port receiving PTP messages.
- An End-to-End Transparent Clock (E2E TC) provides only the time taken for a PTP message to transit the device.

The PTP establishes a communications path across the network between all OCs and BCs. TCs may lie within the communications path, but, in general, P2P TCs and E2E TCs cannot be mixed in the same path.

Prior to synchronization, the clocks are organized into a master-slave hierarchy through a series of PTP Announce messages. The hierarchy contains a grandmaster, or PRC, multiple masters, and multiple slaves. This selection process is the Best Master Clock Algorithm (BMCA), which includes a clock class, based on where the clock has synchronized its timing from; clock accuracy, based on maximum accuracy threshold; and time source, based on the type of clock from which the advertising clock has received its timing (Atomic, GPS, Terrestrial Radio, PTP, Internal oscillator, and so on).

Synchronization in PTP

Once the hierarchy is established, each slave then synchronizes with its master using either a Delay Request-Response mechanism or a Peer Delay mechanism. These mechanisms cannot be mixed over the same communications path.

Delay Request-Response Mechanism The Delay Request-Response mechanism consists of four messages: Sync, Follow_Up (optional), Delay_Req, and Delay_Resp. Sync and Follow_Up messages are typically multicast, but may be unicast. Delay_Req and Delay_Resp are typically unicast messages between master and specific slave. Figure 7-45 illustrates this Request-Response mechanism.

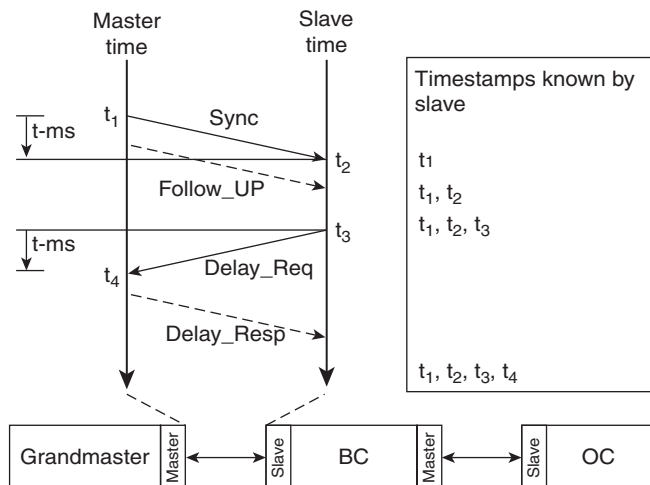


Figure 7-45 PTP Delay Request-Response Mechanism

Propagation time, or transit time, and an *offset*, or processing time, are calculated during this process.

Assuming a symmetrical link:

- The propagation time is $[(t_2 - t_1) + (t_4 - t_3)] / 2$.
- The offset is $t_2 - t_1 - (\text{propagation time})$.

Assuming an asymmetrical link:

- The propagation time is the average of the slave-to-master and master-to-slave propagation times.
- The offset is the difference between the actual master-to-slave time and the average propagation times.

Peer Delay Mechanism The Peer Delay mechanism is limited to point-to-point communications paths between two OC, BC, or P2P TC. The Peer Delay mechanism is also symmetric; that is, it operates separately in both directions.

The Peer Delay mechanism consists of five messages: Sync, Follow_Up (optional), Pdelay_Req, Pdelay_Resp, and Pdelay_Resp_Follow_Up (optional). Figure 7-46 illustrates this Request-Response mechanism.

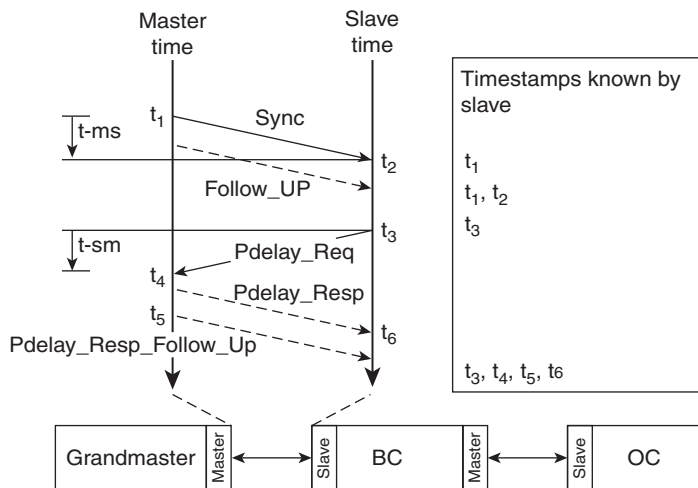


Figure 7-46 PTP Peer Delay Mechanism

A propagation time, or the transit time, and an offset, or the processing time, are calculated during this process.

Assuming a symmetrical link:

- The propagation time is $[(t_4-t_3)+(t_6-t_5)]/2$.
- The offset is $t_2-t_1-(\text{propagation time})$.

Assuming an asymmetrical link:

- The propagation time is the average of the slave-to-master and master-to-slave propagation times.
- The offset is the difference between the actual master-to-slave time and the average propagation times.

When using an E2E TC in the network, the E2E TC is not synchronized at all. Instead, the E2E TC timestamps the Sync message or Follow_Up message on both ingress and egress, and computes the time taken for the message to traverse the node from these timestamps. This time is the residence time, and is included in the message as a Correction field, such that OC and BC may account for this processing time. Each E2E TC in the chain adds its own residence time to the value already contained in the Correction field.

PTP Profiles and Conformance

PTP supports extensible profiles that allow for transport of optional features and attribute values, including interworking and desired performance levels required for a particular application. These profiles are created by numerous third parties, such as standards or industry organizations and vendors.

Network nodes are required to conform to the normative sections of the IEEE 1588 standards and at least one PTP profile. IEEE 1588 defines two default profiles: Delay Request-Response Default PTP Profile and Peer-to-Peer Default PTP Profile. In addition, a network node may comply with certain optional sections of the standards but must implement the optional section in its entirety.

NTP

The Network Transport Protocol (NTP) is the most predominant method of synchronizing clocks on the Internet. The National Institute of Standards and Technology (NIST) estimates over 10 million NTP servers and clients deployed in the Internet.

The most recent version, NTPv4, extends upon previous versions (NTPv3–RFC 1305) by introducing accuracy to the tens of microseconds (with a precision time source, such as a Cesium oscillator or GPS receiver), dynamic discovery of servers, and includes an extensibility mechanism via options.

A NTP node operates as either a Primary (Stratum 1) server, a Secondary (Stratum 2) server, or a client. Primary servers synchronize to national time standards via radio (terrestrial or satellite). A client synchronizes to one or more upstream servers, but does not

provide any synchronization services to downstream nodes. A Secondary server synchronizes to one or more Primary servers and also provides synchronization services to one or more downstream servers or clients.

NTP Protocol Modes

There are three NTP protocol modes: client/server, symmetric, and broadcast.

In client/server mode, clients and servers send unicast packets to each other. Servers provide synchronization services to the clients, but do not accept synchronization from them. In client/server mode, clients are responsible for pulling synchronization from the server.

In symmetric mode, a peer functions as both a client and server. Peers provide synchronization services and accept synchronization from other peers. In symmetric mode, peers push and pull synchronization from each other.

In broadcast mode, a server sends periodic broadcast messages to multiple clients simultaneously. On instantiation of communication, unicast messages are sent between client and server such that the client can accurately calculate propagation delay. Following this unicast exchange, the client listens for broadcast messages generated by the server. In broadcast mode, the broadcast server pushes synchronization to clients.

Offset

The basic operation of NTP synchronization involves determining the offset in clock from one network node to another. This works as follows:

1. The NTP client sends a packet to a specified NTP server. In this packet, it stores the time the packet left as defined by its clock (t_1).
2. The NTP server receives the packet and notes the time it received the packet, according to its clock (t_2), and the time the client sent the packet (t_1).
3. The NTP server sends a packet back to the client and includes what time it was sent according to its clock (t_3). The packet sent back contains three timestamps: t_1 , t_2 , and t_3 .
4. The client receives the packet from the server and notes what time it receives the packet according to its clock (t_4).

Figure 7-47 illustrates this synchronization flow.

Assuming a symmetrical link:

- The propagation delay is $(t_4 - t_1) - (t_3 - t_2)$.
- The clock offset is $[(t_2 - t_1) + (t_4 - t_3)] / 2$.

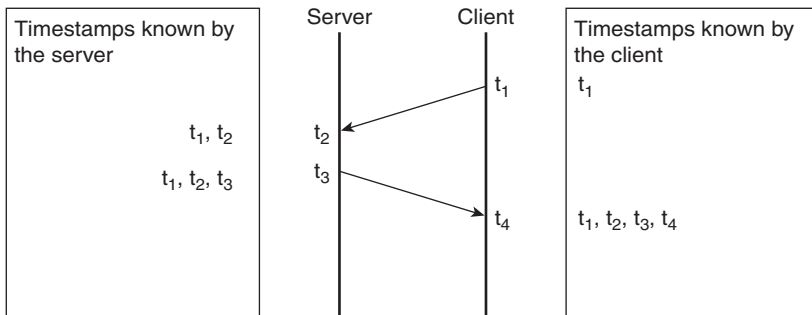


Figure 7-47 NTP Offset Calculation

Although the basic algorithm seems simple, the NTP architecture is more complex than expected. Once a server sends information to a client, the client uses a combination of clock/data filter, selection, clustering, and combining algorithms to determine its local offset. Figure 7-48 depicts a typical NTP architecture.

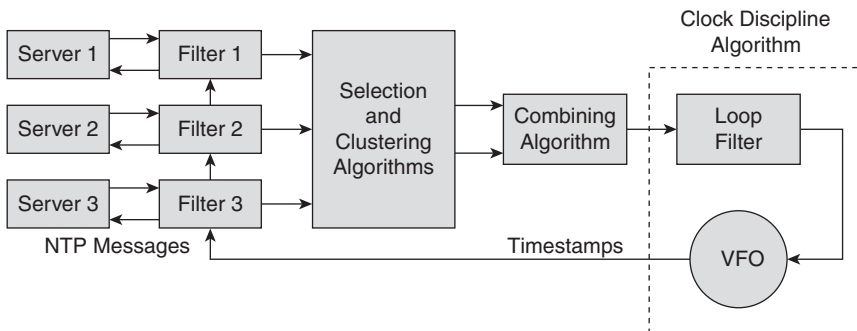


Figure 7-48 NTP Architecture

NTP Clock Filter Algorithm

The NTP clock filter algorithm analyzes the stream of NTP data received to determine which samples are most likely to represent accurate time. The algorithm produces the offset, delay, dispersion (maximum error in measurement), jitter, and time of arrival information that is used to calculate the final offset for the system clock. These values are also used to determine if the server is functioning properly and whether it can be used as a reference source. The NTP clock filter algorithm actually consists of four other algorithms, as follows:

- The NTP selection algorithm scans the stream of NTP data and discards samples that are clearly incorrect, known as *false-tickers*, and keeps only those that appear to be accurate, known as *true-chimers*. False-tickers may be caused by the long-tail effect of Packet-Delay Variation (PDV) or network degradations, such as congestion and reroutes caused by node failures.

- The NTP cluster algorithm then discards those samples that are statistically furthest from the mean until a minimum number of samples remain.
- The NTP combine algorithm produces the final values based on a weighted average calculation from the samples remaining.
- The NTP clock discipline algorithm takes the final values output from the combine algorithm and uses these to discipline the local clock.

NTP Poll Interval

The NTP poll interval is the term used to define how often a new calculation of offset should be made. The poll interval is determined dynamically by the clock discipline algorithm based on the observed clock offset measurements. The poll interval will increase if the internal oscillator frequency stays constant. If the oscillator frequency changes, the poll interval will decrease in order to track these changes.

NTP Security Considerations

Because NTP broadcast clients are vulnerable to broadcast storms from spoofed or misbehaving NTP broadcast servers, NTP includes an optional authentication field. This optional authentication field supports MD5 encryption. This encryption can be negotiated between a broadcast client and server during instantiation.

TICTOC

The Timing over IP Connection and Transfer of Clock BOF (TICTOC) draft standard was written to provide a robust IP/MPLS-based time and frequency distribution architecture. TICTOC, like other protocols, can be decomposed into two layers corresponding to time and frequency. Implementations may vary depending on the exact need of the application. For example, if an application or network node only needs time synchronization and not frequency synchronization, only the time layer may be present.

Figure 7-49 illustrates the TICTOC layers.

TICTOC Clients

TICTOC clients are comprised of up to four modules (illustrated in Figure 7-50)—the frequency acquisition module, the frequency presentation module, the time acquisition module, and the time presentation module.

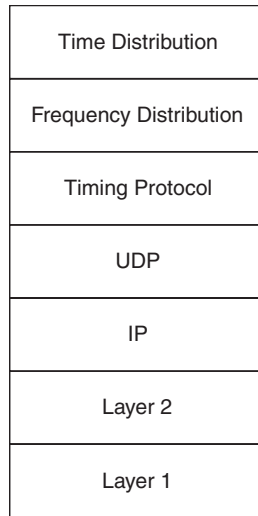


Figure 7-49 *TICTOC Layers*

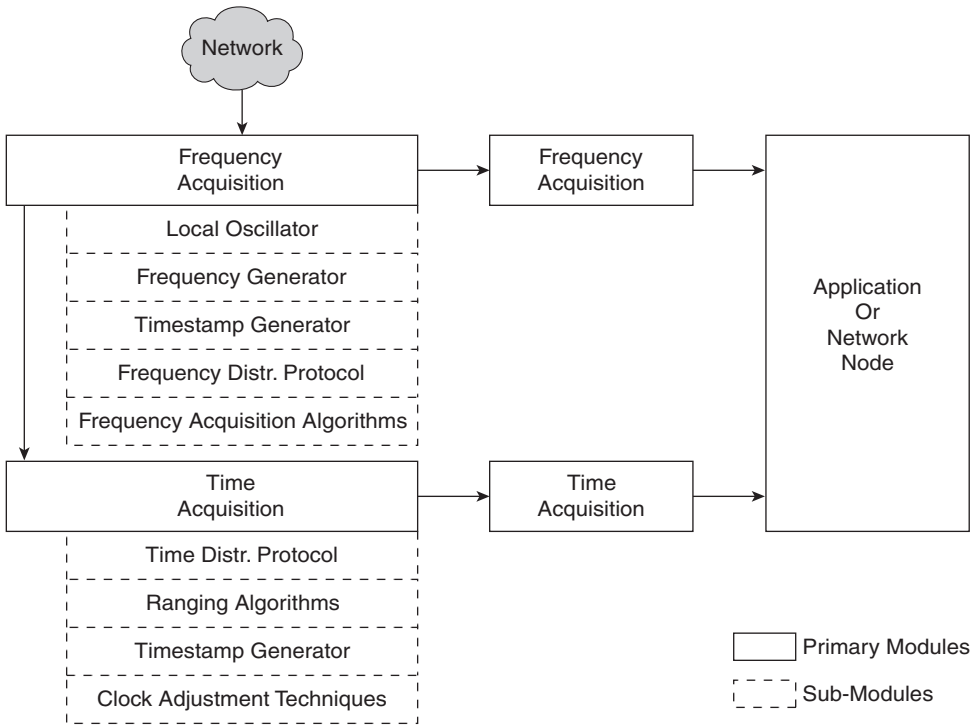


Figure 7-50 *TICTOC Client Modules*

Frequency Acquisition Module

The *frequency acquisition module* retrieves the frequency information distributed over the network. The frequency acquisition module may be divided into the following sub-modules. These sub-modules may not all be present depending on requirements and implementation:

- **Local oscillator.** Both master and clients in the TICTOC architecture need a local oscillator. The master uses a Cesium clock, whereas the clients may use a lower-accuracy oscillator, such as quartz crystal. The client's local oscillator must be adjusted to match the master's oscillator to ensure synchronization. Disciplining the local oscillator is based on arrival time and information received in packets from the frequency distribution protocol.
- **Frequency generator.**
- **Timestamp generator.**
- **Frequency distribution protocol.** The frequency distribution protocol is used to distribute frequency across the network. This protocol may be the same or different than the protocol used to distribute time. Frequency distribution protocols in TIC-TOC are one-way, and may be unicast, multicast, or broadcast. Although multicast distribution is supported, there is the inherent risk that a multicast replication operation may add variable delay.
- **The frequency acquisition algorithms are used to re-acquire the source time from the received packets.** As with all packets in a PSN, the packet distribution protocol packets are subject to Packet Delay Variation (PDV). The frequency acquisition algorithms are used to filter out the PDV through a two-step process, as follows:
 - **Packet Selection and Discard Algorithms:** These algorithms are similar to those used in NTP to eliminate those packets that would lead to accuracy degradation of the recovered frequency. This packet selection algorithm works by selecting a series of packets that are all similar in result, as long as the sample still represents a relatively high percentage of packets.
 - **Filtering and control servos:** With linear averaging, the time to calculate and eliminate frequency drift effects would be so high that the frequency difference calculated would no longer be relevant. "Control loops" are used to accurately model the frequency drift effects on sampled packets in a non-linear manner.

Frequency Presentation Module

If the frequency is needed by the application, the *frequency presentation module* formats this information into the application-specific requirements. Presentation methods may include graphical display, clock discipline, and so on.

Time Acquisition Module

The *time acquisition module* requires a stable frequency reference. Even if frequency is not needed, the time acquisition module may rely on the frequency acquisition module to retrieve information. The time acquisition module may also retrieve information from an external source, such as a GPS receiver. This module allows multiple TICTOC clients to share a common offset. The time acquisition module may be divided into the following sub-modules. These sub-modules may not all be present depending on requirements and implementation:

- **Time distribution protocol:** The time distribution protocol is used to accurately synchronize a clock based on measured offset between client and master oscillators. Ranging algorithms are used to estimate this offset. Time distribution protocol, unlike frequency distribution protocol, is typically bi-directional, requiring both client and master to send and receive packets.
- **Ranging algorithms:** Ranging is the estimation of propagation delay within a network. This is done in a manner similar to PTP, where a packet is sent from the master with a timestamp, followed by a second packet with a timestamp. These timestamps on the packets indicate the time that the master injected the packet into the network. The client then has sufficient timestamp information to calculate the propagation delay.
- Clock adjustment techniques
- Timestamp generator

Time Presentation Module

The *time presentation module* formats information from the time acquisition module into a format that is relevant to the application requiring synchronization.

Generic Modules

TICTOC supports various generic modules that may be applied to frequency distribution, time distribution, or both. These modules include enhanced security (certificate-based), auto-discovery of masters, master clock selection algorithms, OAM, performance monitoring, and network management.

Combining Protocols

SyncE, PTP, NTP, and TICTOC need not be mutually exclusive within a network. A combination of these protocols, along with external means of synchronization, may be leveraged. For instance, because SyncE provides a highly accurate frequency source and TICTOC provides a highly accurate time source, a network may use the SyncE's physical layer frequency synchronization as the source for TICTOC's IP layer time synchronization input.

Summary

This chapter discussed one of the predominant IP migration methods for today's mobile networks. Whether driven by technological or financial decisions, backhaul network evolution to IP-based mechanisms is a clear operator strategy, and pseudowire transport mechanisms provide a bridge between the legacy TDM systems presented in Chapter 2 and the All IP systems presented in Chapter 3. Although not without their share of complexity, including time and frequency synchronization, IP backhaul networks are an obvious value to mobile operators. With such a large number of solutions for both pseudowire transport and synchronization, mobile operators need to understand the technologies themselves and determine which best meets their requirements.

Endnotes

¹Source: ABI Research

²Source: ABI Research

Index

Numbers

3G femtocell. *See* HNB
3GPP, 480

- A3/A8 algorithms, 417
- charging rules, 408
- edge policy admission control, 407
- mobility protocols, 229
 - GSM A interface reference*, 230
 - GSM Abis interface reference*, 232
 - GSM Gb interface reference*, 230
 - GSM Gi interface reference*, 234
 - GSM Gn interface reference*, 232-233
- OCS, 405
- OFCS, 405
- PCC model, 404-406
- PCEF, 405, 408
- PCRF, 405
- QoS control, 407
- quota grants, 408
- SPR, 405

3GPP2

- charging rules, 411
- mobility protocols
 - CDMA*, 241-251
 - summary of*, 251
- QoS grants, 411
- SBBC, 409-410

802.16e (IEEE 802.16-2005), 93, 100

A

A-GPS (Assisted GPS), 439
A/IP interface, 288
A-Links (Access links), SS7, 462
A11-Registration Request messages, 314
A3/A8 algorithms, RAN authentication/encryption

- authentication of subscriber identities, 417
- confidentiality of subscriber identities, 417
- confidentiality of subscriber voice/data traffic, 418-419

- AAA (Authentication/Authorization/Accounting), WiMAX Policy Framework, 413
- AAA Servers, cdma2000 PS CN, 313
- AAL5 frame encapsulation, 351
- AAS (Adaptive Antenna Systems), 105-106
- Abis IP-enabled transport, 247
- Abis optimization, 353
- Absolute Mode (RTP headers), 348
- accounting, WiMAX Policy Framework, 413
- accuracy (timing), 357-359
- ACM (Address Complete Messages), ISUP and, 467
- adaptive clock recovery, 373
- Advertising Decision Manager, 446
- Advertising Insertion Engines, 449
- AES (Advanced Encryption Standard), 107
- AF (Application Function), 413
- agent discovery phase (Mobile IP), 295
- aggregation, 118
- airlinks, 399
- AKA (Authentication and Key Agreement) algorithms, 422
- all IP access systems
 - EUTRAN
 - architecture of*, 108-109
 - MAC layer*, 112-113
 - PDCP layer*, 112-113
 - physical layer*, 110-112
 - requirements of*, 108
 - RLC layer*, 112-113
 - security*, 110
 - sharing*, 113-114
 - IEEE 802.11-2007, 93
 - IEEE 802.16-2005 (802.16e), 93, 100
 - IMT-Advanced systems, 93, 114-115
 - ITU-R systems, 93, 114-115
 - LTE, 93
 - EUTRAN*, 108-114
 - S1-flex technology*, 113-114
 - LTE-Advanced, 114
 - WiMAX, 99
 - 802.16e (IEEE 802.16-2005)*, 100
 - AAS*, 105-106
 - evolution of*, 107
 - frame structure of*, 103
 - interfaces of*, 100
 - MAC layer*, 106-107
 - physical layer*, 102-105
 - profiles of*, 100
 - protocol architecture of*, 101
 - RLC layer*, 106-107
 - security*, 107
 - service flows*, 106-107
 - WLAN
 - GAN, 94, 97-99
 - I-WLAN, 94-97
- AMC (Adaptive Modulation and Coding), 29
- EDGE, 54
- WiMAX, 103
- analytics, Data Integration layer (SDP), 446
- anchor points, IP addressing, 119
- ANM (Answer Messages), ISUP and, 467
- antenna diversity, 35
- anycast IP addresses, 128
- APN (access point names), 307
- application policies, 402
- application servers
 - external servers, accessing via core networks, 214
 - multihomed application servers, DC access, 219-220

proxy servers
accessing via core networks, 215
DC access, 222
 single-homed application servers, DC access, 220-221

ARQ (Automatic Repeat Requests), 34

ASN (Access Service Networks), 260

ASN-GW
 ASN-GW to ASN-GW handover via R4 protocol, 264
 R3 protocol for ASN-GW to HA, 266
 R6 protocol for BS to ASN-GW, 262

asynchronous networks, 370

asynchronous wire-line transport mode, 198-199

asynchronous wireless transport mode, 200

ATM (Asynchronous Transfer Mode), 154
 BTS, 244
 hierarchical ATM switching, 249
 pseudowires, 348
AAL5 frame encapsulation, 351
architecture of, 349
backhaul offload of UMTS R4 backhaul networks, 338
Control Words, 350
generic encapsulation, 349
N-to-One cell encapsulation mode, 350
One-to-One cell encapsulation mode, 351
troubleshooting, 351

authentication
 Authentication Server, 429
 cdma2000 access systems, 85
 Diameter, 434-437
 EAP, 107, 429-431
 I-WLAN, 95

Mobility Management sub-layer (Circuit-Switched Core Networks), 273-274

RADIUS, 425-428, 434
 subscriber-specific policies, 394
 WiMAX Policy Framework, 413

authorization
 I-WLAN, 95
 RAN, 416
A3/A8 algorithms, 417-419
AKA algorithm, 422
CAVE algorithm, 420-424
 WiMAX Policy Framework, 413

autonomous PRC (Primary Reference Clocks), 364

availability, connectionless switching methods, 172

AWGN (Additive White Gaussian Noise), 15-17

B

B-Links (Bridge links), SS7, 463

backhaul networks, 400

backhaul offload via pseudowires
 ATM pseudowires, 348
AAL5 frame encapsulation, 351
architecture of, 349
Control Words, 350
generic encapsulation, 349
N-to-One cell encapsulation mode, 350
One-to-One cell encapsulation mode, 351
troubleshooting, 351

CESoPSN
for Inter-MSC/BSC connectivity, 336
packet structure, 347
 RTP, 348
TDMoIP versus, 348

- converging multiple RAN technologies, 339-340
 - encapsulation techniques, 335
 - GSM Abis/Iub optimization, 353
 - PWE3, 340
 - SONET/SDH CEP, 352-353
 - TDM pseudowires
 - interpolation packets*, 344
 - PLC*, 343-344
 - previous insertion packets*, 344
 - SAToP class*, 341
 - structure-aware transport*, 343
 - Structure-Aware Transport over Packet class*, 341
 - zero insertion packets*, 344
 - TDMoIP pseudowires
 - adapted payloads*, 345
 - CESoPSN versus*, 348
 - Control Words*, 345
 - for EVDO/GSM networks*, 335-336
 - generic encapsulation*, 344-345
 - OAM*, 345-347
 - PSN headers*, 345
 - for UMTS R4 backhaul networks*, 338
 - bandwidth**
 - connection-oriented switching methods, allocation for, 156
 - connectionless switching methods, allocation for
 - QoS, 167-172
 - queue management*, 172-175
 - DBA, 353
 - BC (Boundary Clocks), 375
 - BE (Best Effort) services, WiMAX QoS grants, 415
 - BER (Bit Error Rates), 15-17
 - BGP (Border Gateway Protocol), 139
 - BICC (Bearer Independent Call Control) protocol, ISUP and, 467
 - binary trees, IP address assignments, 121
 - binding Mobile IP, 295
 - blacklisting, 497
 - BPL (Building Penetration Loss), 11-12
 - BPSK (Binary Phase Shift Keying), modulation and, 12
 - broadcast IP addresses, 123
 - broadcast mode (NTP), 379
 - BS
 - BS to BS handover via R8 protocol, 264
 - R6 protocol for BS to ASN-GW, 262
 - BSC (Base Station Controllers)
 - BSC to BSC protocol transport, 248
 - BTS, transporting between, 244
 - GM access systems, 42
 - Inter-MSC connectivity via CESoPSN pseudowires, 336
 - MSC, transporting between, 245
 - PDSN, transporting between, 245
 - BTS (Base Transceiver Stations)
 - BSC, transporting between, 244
 - GSM access systems, 42
 - transport aggregation via ATM, 244
 - bundling**
 - Charging layer (SDP), 447
 - SCTP, 473
 - BYE method (SIP), 481
-
- C**
- C-Links (Cross links), SS7, 464
 - CAC (Call Admission Control), 402
 - Call Agents, 459
 - Capability and Preference Exposure layer (SDP), 444-446

- capacity constrained deployments, 8
- CAVE (Cellular Authentication and Voice Encryption) algorithms, 420-421
- CBC-MAC, CCMP, 424
- CCAF (Call Control Agent Function), 454
- CCF (Call Control Function), 454
- CCMP (Cipher Block Chaining Message Authentication Code Protocol)
 - CBC-MAC, 424
 - Counter mode, 423
 - RAN authentication/encryption, 423-424
- CCoA (Collocated CoA), 295
 - Mobile IP, 296
 - tunneling, 297
- CDMA (Code Division Multiple Access), 18, 23, 26
 - architecture of, 241
 - IP transport of CDMA 3G interfaces
 - Abis IP-enabled transport*, 247
 - signaling transport*, 248
 - user transport*, 249-251
 - transport between, 245
- CDMA/CA (Carrier Detection Multiple Access/Collision Avoidance) method, 199
- cdma2000 access system
 - architecture of, 80
 - packet data operation*, 86
 - physical layer*, 83-84
 - signaling LAC*, 85
 - signaling MAC*, 85
 - authentication in, 85
 - Core Networks, 283
 - evolution data
 - EV-DO Rev. 0*, 87-88
 - EV-DO Rev. A*, 88-89
 - EV-DO Rev. B*, 89
 - Packet-Switched Core Networks
 - session mobility*, 316
 - simple IP sessions*, 314-316
 - SMV voice model, 84
- cellular access systems, 41
 - cdma2000 access system. *See* cdma2000 access system
 - GSM access systems
 - BSC, 42
 - BTS, 42
 - CS data, 47
 - EDGE, 53-54
 - GERAN, 54
 - GPRS, 48-54
 - HSCSD, 48
 - physical layer*, 43
 - protocol architecture of*, 43-48
 - signaling*, 45
 - SMS, 46
 - voice transport*, 46
 - UTRAN, 55
 - architecture of*, 56
 - broadcast support*, 66
 - Core Network Control Plane*, 58
 - eHSPA*, 77-78
 - HNB*, 78-79
 - HSDPA*, 67-73
 - HSUPA*, 74-76
 - Iur interface*, 57
 - MAC layer*, 60-61
 - MBMS*, 66-67
 - multicast support*, 66
 - packet-switched services*, 64-65
 - PDCP*, 62
 - RLC layer*, 60-61
 - transport network*, 62-63
 - UMTS physical layer*, 58-59
 - user plane protocols*, 56
- Cesium tubes, PRC and, 364

CESoPSN (Circuit Emulation Services over Packet-Switched Networks)

Inter-MSC/BSC connectivity, 336

packet structure, 347

RTP, 348

TDMoIP versus, 348

channel equalization, 29**Charging layer (SDP), 446-447****Chase Combining, H-ARQ and, 34****CIDR (Classless Internet Domain Routing), IP addressing and, 125****Circuit-Switched Core Networks, 271**

A/IP interface, 288

bearer independent CS architectures, 285-287

cdma2000 Core Networks, 283

GSM handovers, 279-280

HLR, 272

Iu-CS interfaces, 288

Mobility Management sub-layer

*authentication, 273-274**device identity requests, 274**identity management, 273**key exchanges, 273**location management, 273, 276*

MSC, 271

MT calls, 276-277

SM-SC, 272

SMS, 272, 281

TrFO, 287

VLR, 272

WCDMA Core Networks, 283-285

class queuing, 174-175**Client Mobile IP, WiMAX and, 266****client/server mode (NTP), 379****clock filter algorithm (NTP), 380****clocking, 198****clocks (timing)**

ANSI/ITU-T standards, 363

asynchronous networks, 370

BC (PTP), 375

E2E TC (PTP), 376

external timing mode, 369

hierarchy of, 363

line timing mode, 369

OC (PTP), 375

P2P TC (PTP), 376

plesiochronous networks, 371

PRC, 363

*architecture of, 364-366**autonomous PRC, 364**Cesium tubes, 364**MTIE, 365**radio-controlled PRC, 364**synchronization and, 365-368*

pseudo-synchronous networks, 371

recovery over packet, 373

synchronous networks, 370

TC (PTP), 375

CM ALERTING messages, 279**CM CALL CONFIRMED messages, 278****CM CONNECT messages, 279****CM SETUP messages, 278****CMIP (Client Mobile IP), 320****co-located CoA, 188****CoA (care-of-address), 294**

CCoA, 295

*Mobile IP registration, 296**tunneling, 297*

co-located CoA, 188

FA CoA, 295

foreign agent CoA, 189

Commit Phase (QoS), 411

communication planes (core networks)

data bearer plane

external application server access, 214

IP application flow state, 212

proxy application server access, 215

stateful transition of, 213

stateless transition of, 213

subscriber IP routing, 210

subscriber session management, 208

traffic profile analysis, 215

management plane, 217

messaging plane, 204

signaling plane, 204

voice bearer plane

transcoded voice transport, 206

TrFO voice bearer transport, 208

tunneling-encoded voice bearers, 207

voice bearer switching on mobile wireless architectures, 205

VoIP packet transport, 205

congestion avoidance, 402**connection-oriented switching methods, 152**

ATM, 154

bandwidth allocation

QoS, 156

queue management, 156

Frame Relay switching, 154

TDM, 153

connectionless switching methods

bandwidth allocation

QoS, 167-172

queue management, 172-175

Ethernet packet switching, 157-159

MPLS, 160

L2VPM, 163-164

L3VPM, 166

constellation diagrams (QAM), 13

content transformation engines, 448

Control Words

ATM pseudowires, 350

TDMoIP pseudowires, 345

converged core networks, 218

core networks, 201

bifurcated transports, 202

combined transports, 203

converged core networks, 218

data bearer plane

external application server access, 214

IP application flow state, 212

proxy application server access, 215

stateful transition of, 213

stateless transition of, 213

subscriber IP routing, 210

subscriber session management, 208

traffic profile analysis, 215

DC access, 218, 223

application proxy servers, 222

multihomed application servers, 219-220

single-homed application servers, 220-221

management plane, 217

messaging plane, 204

partitioning, 218

signaling plane, 204

structured TDM trunks, 201-202

TFO, 206

transport requirements, summary of, 229

TrFO, 207
 voice bearer plane
 transcoded voice transport, 206
 TrFO voice bearer transport, 208
 tunneling-encoded voice bearers, 207
 voice bearer switching on mobile wireless architectures, 205
 VoIP packet transport, 205
 correlation functions (PDP), 387
 Counter mode (CCMP), 423
 coverage limited deployments, 7
 CRF (Charging Rules Function), 409
 CS (Circuit-Switched) data
 GSM access systems, 47
 HSCSD, 48
 CSCF (Call State Control Functions), 486

D

D-Links (Diagonal links), SS7, 463
 data bearer plane (core networks)
 application servers
 external server access, 214
 proxy server access, 215
 IP application flow state, 212
 stateful transition of, 213
 stateless transition of, 213
 subscriber IP routing, 210
 subscriber session management, 208
 traffic profile analysis, 215
 data fragmentation (SCTP), 473
 Data Integration layer (SDP), 446
 data mining, 446
 DBA (Dynamic Bandwidth Allocation), 353
 DC (Data Center), accessing core networks via, 218, 223
 application proxy servers, 222
 multihomed application servers, 219-220
 single-homed application servers, 220-221
 DCCA (Diameter Credit Control Application), 437
 decades, 6
 decision functions (PDP), 388
 Delay Request-Response mechanism (PTP), 376
 delays
 Delay Request-Response mechanism (PTP), 376
 propagation delays, 168
 queuing delays, 168
 serialization, 168
 switching, 168
 deploying
 capacity constrained deployments, 8
 coverage limited deployments, 7
 device capabilities databases, 445
 device identity requests, 274
 DFP (distributed functional plane), IN, 454
 Diameter
 BASE specification, 435
 DCCA, 437
 EAP, 437
 IMS, 437
 IP authentication/authorization, 434-437
 MIPv4, 437
 NASREQ, 437
 Transport profile, 435-437
 differential clock recovery, 373
 Differential Mode (RTP headers), 348
 Diffserv, 402

distance-vector routing algorithms,
132

diversity combining, 35

DVB-H, 494

DVMRP (Distance Vector Multicast
Routing Protocol), 146

E

E-Links (Extended links), SS7, 464

E2E TC (End-to-End Transparent
Clocks), 376

EAP (Extensible Authentication
Protocol)

Authentication Server, 429

Diameter, 437

EAP Authenticator, 429

EAP Peer, 429

EAP-AKA, 431

EAP-SIM, 430

EAP-TLS, 432

EAP-TTLS, 433

IP authentication/authorization,
429-431

RADIUS support, 429

WiMAX, 107

EDGE (Enhanced Data Rates for GSM
Evolution)

AMC, 54

GPRS, 53-54

edge policy admission control (3GPP),
407

eHSPA (evolved High-Speed Packet
Access), UTRAN and, 77-78

ELF (Extremely Low Frequency), 2

encryption

AES, 107

Diameter, 434-437

EAP, 429-431

RADIUS, 425-428, 434

RAN, 416

A3/A8 algorithms, 417-419

AKA algorithm, 422

CAVE algorithm, 420-421

CCMP, 423-424

EPC (Evolved Packet Core). Packet-
Switched Core Networks, 324-325

E2E QoS, 327

EPC macro-mobility, 327

non-3GPP access, 325

equalization (channel), 29

ErtVR (Extended Real-Time Variable
Rates), 414

ETH-CS (Ethernet-Convergence Sub-
Layer), 262

Ethernet

asynchronous wire-line transport
mode, 199

ETH-CS, 262

hierarchical switching, 179

packet switching, 157-159

partial mesh topologies, 179

switching methods, 176

redundancy, 177-179

VLAN switching, 180-181

SyncE, 375

EUTRAN (Evolved UMTS Terrestrial
Radio Access Networks)

architecture of, 108-109

MAC layer, 112-113

PDCP layer, 112-113

physical layer, 110-112

requirements of, 108

RLC layer, 112-113

security, 110

sharing, 113-114

EV-DO Rev. 0, 87-88

EV-DO Rev. A, 88-89

EV-DO Rev. B, 89

EVDO, backhaul offload via TDMoIP pseudowires, 335-336
 external application servers, 214
 external timing mode, 369

F

F-Links (Full Associated links), SS7, 465
 FA (Foreign Agent), Mobile IP, 294-296
 fast fading (radio propagation), 9
 FCH (Frame Control Headers), 104
 FDD (Frequency Division Duplexing), 354
 FDMA (Frequency Division Multiple Access), 18, 21-23
 Feature Servers, 459
 FEC (Forward Error-Correcting) codes, 28-30
 FISU (Fill-In Signaling Units), SS7 SU, 469
 foreign agent CoA, 189
 fragmentation (data), 473
 Frame Rate scheduling, 156
 Frame Relay switching, 154
 free-running oscillators, 356
 frequency acquisition modules (TICTOC), 383
 Frequency Drift, 362
 frequency presentation modules (TICTOC), 383
 frequency selective fading (radio propagation), 9
 frequency selective transmissions, 30

G

GA-CSR (Generic Access Circuit Switched Resource Control) protocol, 97
 GA-PSR (Generic Access Packet Switched Resource Control) protocol, 97
 GA-RC (Generic Access Resource Control) protocol, 97
 GAN (Generic Access Networks), 94, 97-99
 GA-CSR protocol, 97
 GA-PSR protocol, 97
 GA-RC protocol, 97
 GANC, 97-98
 UMA/GAN, 99
 Gb interface (GPRS), 52
 GERAN (GSM/Edge Radio Access Networks), 54, 229
 GGSN, 233
 global functional plane (IN), 454
 global policies, 392
 global routing exchange peering, path vector routing and, 143
 GPRS (General Packet Radio Systems), 48
 access QoS, 52-53
 EDGE, 53-54
 FEC coding schemes, 49
 Gb interface, 52
 LLC layer, 51
 MAC layer, 50
 NACC, 53
 RLC layer, 50
 RTT, 52
 SNDCCP, 52
 GPS (Global Positioning Systems), 356
 A-GPS, 439

ground reflection, propagation and, 6
GSM (Global System for Mobilization)

Abis optimization, 353
 backhaul offload via TDMoIP
 pseudowires, 335-336
 BSC, 42
 BTS, 42
 CS data, 47
 EDGE, 53-54
 GERAN, 54, 229
 GPRS, 48
 access QoS, 52-53
 EDGE, 53-54
 FEC coding schemes, 49
 Gb interface, 52
 LLC layer, 51
 MAC layer, 50
 NACC, 53
 RLC layer, 50
 RTT, 52
 SNDCP, 52
 handovers, 279-280
 HSCSD, 48
 Iub optimization, 353
 Mobility Management sublayer
 (Circuit-Switched Core Networks)
 authentication, 273-274
 device identity requests, 274
 identity management, 273
 key exchanges, 273
 location management, 273, 276
 mobility protocols, 229
 A interface reference, 230
 Abis interface reference, 232
 Gb interface reference, 230
 Gi interface reference, 234
 Gn interface reference, 232-233
 MT calls, 276-277
 physical layer, 43

protocol architecture of, 43-48
 signaling, 45
 SMS, 46
 voice transport, 46

**GTP (GPRS Tunneling Protocol),
 190-191, 290**

EPC PS CN, 327
 fields of, 291
 header fields, 291
 MBMS-GTP tunnels, 293
 QoS support, 292
 UTRAN PS CN, 311

GTT (Global Title Translation), 466

H

**H-ARQ (Hybrid Automatic Repeat
 Requests), 34**

HA (Home Agent)

Mobile IP, 294
 cdma2000 PS CN, 313
 registration, 296
 PDSN, transporting between, 245
 R3 protocol for ASN-GW to HA, 266

header fields (GTP), 291

**hierarchical mobility of Packet-
 Switched Core Networks, 288**

higher-layer synchronization, 356

HLR (Home Location Registers), 272

HNB (Home Node B), 78-79

**HSCSD (High-Speed Circuit-Switched
 Data), 48**

**HSDPA (High-Speed Download Packet
 Access)**

AMC and, 29
 architecture of, 68-69
 performance of, 69-72
 transport networks, 72-73
 UTRAN and, 67-73

HSUPA (High-Speed Uplink Packet Access)

- architecture of, 74
- performance of, 75-76
- UTRAN and, 74-76

HTTP (Hyper-Text Transfer Protocol), 186**I-CSCF (Interrogating Call State Control Functions), IMS, 486****I-WLAN (Interworking WLAN), 94-97**

- authentication, 95
- authorization, 95
- Packet-Switched Core Networks, 318

IAM (Initial Address Messages), ISUP and, 467**identity management, 273****identity requests (devices), 274****IEEE 802.11-2007, 93****IEEE 802.16-2005 (802.16e), 93, 100****IGMP (Internet Group Management Protocol), 150****IM-SSF (IMS Service Switching Function), 487****IMPI (IMS Private Identities), 489****IMPU (IMS Public Identities), 489****IMS (IP Multimedia Subsystems), 486**

- components of, 487
- CSCF, 486
- Diameter, 437
- framework of, 488-489
- identity model, 489
- IM-SSF, 487
- IMPI, 489
- IMPU, 489
- MRF, 488
- subscriber model, 489-490

IMT (International Mobile Telecommunications)

- IMT-Advanced systems, 93, 114-115
- Radio Frequency Spectrum, 3

IN (Intelligent Networks)

- architecture of, 453
- history of, 452

INCM

- DFP, 454*

- global functional plane, 454*

- physical plane, 455-457*

- services plane, 453*

LNP, 458**MNP, 458****mobile IN, 457-458****Incremental Redundancy, 34****INFO method, 485****Integrated IS-IS (Intermediate System to Intermediate System)**

- applicability to mobile providers, 139
- network architecture, 138

Inter-MSC, 336**interleaving, 30****interpolation packets, 344****INVITE method (SIP), 481****IP (Intelligent Peripherals), 456****IP addressing**

- aggregation in, 118
- anchor points in, 119
- IPv4

- address classes, 120*

- binary tree address assignments, 121*

- broadcast IP addresses, 123*

- interoperability of, 129*

- multicast IP addresses, 123-124*

- private IP addresses, 122*

- unicast IP addresses, 122*

- IPv6 (RFC-4291)
 - anycast IP addresses, 128*
 - CIDR and, 125*
 - header format, 125*
 - interoperability of, 129*
 - multicast IP addresses, 126*
 - unicast IP addresses, 126*
- IP authorization/authentication**
 - Diameter, 434-437
 - EAP, 429-431
 - RADIUS, 425-428, 434
- IP Core, 402**
- IP transport protocols**
 - HTTP, 186
 - RTP, 185
 - SIP, 186
 - IP protocol, 182
 - SCTP, 184*
 - TCP, 183*
 - UDP, 184*
 - tunneling protocols
 - GTP, 190-191*
 - IPSec ESP, 191*
 - MOBIKE protocol, 192*
 - Mobile IP, 187-189*
 - transporting Layer 2 frames via, 193-195*
- IP-CS (IP-Convergence Sub-Layer), 263**
- IPSec ESP (IP Security Encapsulating Security Payload), 191**
- IS-IS (Intermediate System to Intermediate System), Integrated**
 - applicability to mobile providers, 139
 - network architecture, 138
- ISUP (ISDN Signaling User Part), SS7**
 - protocol stack, 467

- ITU (International Telecommunications Union)**
 - ITU-R systems, 93, 114-115
 - Radio Frequency Spectrum, 3-4
- Iu-cs interfaces, 288**
- Iub optimization, 353**
- Iur (inter-RNC) interface, 57**

J-K

- jitter, 169**
 - defining, 361
 - packet loss and, 171
- key exchanges, 273**

L

- L2TPv3 (Layer 2 Tunnel Protocol version 3), 193**
- Layer 2 frames**
 - transporting via mobile provider networks, 195
 - transporting via tunneling protocols
 - L2TPv3, 193*
 - T-LDP, 194*
- line timing mode, 369**
- link-state routing algorithms, 133**
 - Integrated IS-IS
 - applicability to mobile providers, 139*
 - network architecture, 138*
 - OSPF protocol
 - applicability to mobile providers, 135*
 - network architecture, 134*
- LLC (Logical Link Control) layer, 51**
- LNP (Local Number Portability), IN, 458**

location awareness, 451
 defining, 437
 device-based mechanisms, 437
 hybrid mechanisms, 439
 network-based mechanisms, 438
 sector localization, 438
 triangulation, 438
 trilateration, 438
location management, 273, 276
location servers, 479
Location Update Request messages, 274
log-normal fading, 11
loop timing mode, 369
loss (packet), 170-171
LSMS (Local Service Management Systems), 458
LSSU (Link Status Signal Units), SS7 SU, 469
LTE (Long Term Evolution), 93
 EUTRAN
 architecture of, 108-109
 MAC layer, 112-113
 PDPC layer, 112-113
 physical layer, 110-112
 requirements, 108
 RLC layer, 112-113
 security, 110
 sharing, 113-114
 LTE-Advanced, 114
 LTE/SAE (Long-Term Evolution/System Architecture Evolution), 251
 architecture of, 251
 eNodeB, 253-254
 LTE RAN transport infrastructure, 257
 MME, 254-255
 PDN-GW S5 and S8 interfaces, 255
 S1-flex technology, 113-114

LTE/SAE (Long-Term Evolution/System Architecture Evolution)
 architecture of, 251
 eNodeB
 S1 transport interfaces, 253
 S1-MME RAN transport interfaces, 253
 X2 transport interfaces, 254
 LTE RAN transport infrastructure, 257
 MME, 254-255
 PDN-GW S5 and S8 interfaces, 255

M

M2PA, SIGTRAN, 473
M3UA, SIGTRAN, 475
MAC (Media Access Control), 130-131
 cdma2000 access system, 85
 EUTRAN, 112-113
 GPRS, 50
 UTRAN, 60-61
 WiMAX, 106-107
management plane (core networks), 217
MAP (Mobile Application Parts), 275, 467
master-slave synchronization, PRC and, 367-368
mated pairs (SS7), 462
MBMS (Multimedia Broadcast and Multicast Service)
 MBMS-GTP tunnels, 293
 UTRAN, 66-67
MediaFLO, 495-496
MESSAGE method (SIP), 480
messaging plane (core networks), 204
MGW (Media Gateways), 460

migrating traditional networks

backhaul offload via pseudowires

ATM pseudowires, 338,
348-351*CESoPSN*, 336, 347-348*converging multiple RAN tech-*
nologies, 339-340*encapsulation techniques*, 335*GSM Abis/Iub optimization*,
353*PWE3*, 340*SONET/SDH CEP*, 352-353*TDM pseudowires*, 341-344*TDMoIP pseudowires*, 335-336,
344-348

timing, 356

accuracy in, 357-359*asynchronous networks*, 370*clock hierarchy*, 363*clock recovery over packet*, 373*combining protocols*, 384*external timing mode*, 369*Frequency Drift in*, 362*jitter in*, 361*line timing mode*, 369*loop timing mode*, 369*NTP*, 378-381*packet-based timing*, 372*plesiochronous networks*, 371*PRC*, 363-366*precision in*, 357-359*pseudo-synchronous networks*,
371*PTP*, 375-378*stability in*, 357-359*SyncE*, 375*synchronization in*, 361,
365-368*synchronous networks*, 370*through timing mode*, 369*TICTOC*, 381-384*wander in*, 362**MIMO (Multiple-Input Multiple-**
Output), 35-36

mining data, 446

MIP Encapsulation, 296**MIPv4 (Mobile IP version 4)**,
Diameter, 437**MLD (Multicast Listener Discovery)**,
151**MME (Mobility Management Entity)**
EPC PS CN, 324S10, S11, S3 and S4 transport inter-
faces, 254-255**MN (Mobile Node)**, **Mobile IP**, 294

registration, 295

tunneling, 297

MNP (Mobile Number Portability), **IN**,
458**MOBIKE (Mobile Internet Key**
Exchange) protocol, 192**mobile IN (Intelligent Networks)**,
457-458**Mobile IP**

agent discovery phase, 295

binding updates, 295

Client Mobile IP, WiMAX and, 266
FA, 294-296

HA, 294

cdma2000 PS CN, 313*registration*, 296

MN, 294

registration, 295*tunneling*, 297

optimal routing, 298

Proxy Mobile IP, WiMAX and, 266

proxy Mobile IPv6, 301-302

IPv4 support, 303*overlapping IP address support*,
304

- registration, 295
- security, 300-301
- tunneling, 187-189, 296
- mobile networks**
 - end-to-end reference model, 397
 - independence of, 397-404
 - location awareness, 438
 - maintaining state in, 415-416
 - reference points
 - airlinks*, 399
 - backhaul networks*, 400
 - IP Core*, 402
 - mobile stations*, 398-399
 - Mobile Transport and Application layer*, 402
 - RAN Core*, 401
 - RAN to Gateway communications protocols*, 400
- mobile stations**, 398-399
- Mobile Transport and Application layer**, 402
- mobile video delivery**, 490
 - multicast video delivery, 492-493
 - overlay broadcast video delivery, 493
 - DVB-H*, 494
 - MediaFLO*, 495-496
 - unicast video delivery, 491-492
- mobility (hierarchical)**, 288
- Mobility Management sub-layer (Circuit-Switched Core Networks)**
 - authentication, 273-274
 - device identity requests, 274
 - identity management, 273
 - key exchanges, 273
 - location management, 273, 276
- mobility network transport architecture**
 - 3GPP mobility protocols
 - GSM*, 229
 - GSM A interface reference*, 230
 - GSM Abis interface reference*, 232
 - GSM Gb interface reference*, 230
 - GSM Gi interface reference*, 234
 - GSM Gn interface reference*, 232-233
- UMTS**
 - architecture of*, 235
 - Control Plane transport*, 237
 - lub interface*, 236
 - luCS interface*, 239-241
 - luPS interface*, 239
 - lur interface*, 236-238
 - NodeB Traffic aggregation into RNC*, 237
 - User Plane transport*, 237
- modulation**
- modulation (radio frequency signals)**
 - AMC, 29, 54
 - BER, 15-17
 - BPSK, 12
 - EV-DO Rev. 0, 87
 - QAM, 13-16
 - QPSK, 13
 - SNR, 15
- MPLS (Multi-Protocol Label Switching)**, 160
 - L2VPN, 163-164
 - L3VPN, 166
- MPLS-TE (MPLS Traffic Engineering)**, 402
- MPoP (Multiple Points of Presence)**, 449
- MRF (Media Resource Function)**, IMS, 488
- MSC (Mobile Switching Centers)**, 271
 - BSC, transporting between, 245
 - Inter-MSC, 336

MSDP (Multicast Source Discovery Protocol), 152
MSRN (Mobile Station Roaming Numbers), 277
MSU (Message Signaling Units), SS7 SU, 468
MT (Mobile-Terminated) calls, 276-277
MTIE (Maximum Time Interval Errors), PRC and, 365
MTP (Message Transfer Part), SS7 protocol stack, 466
MUD (Multi-User Diversity) gains, 103
multicast
 multicast distribution trees, 124
 multicast IP addresses, 124
 IPv4, 123
 IPv6 (RFC-4291), 126
 multicast routing, 145
 DVMRP, 146
 IGMP, 150
 MLD, 151
 PIM routing, 146-149
 multicast video delivery, 492-493
 unicast tunneling of
 MSDP, 152
 PIM-Register, 152
multihomed application servers, 219-220
multihoming, TCP support, 471
multipath effects, 29-31
multipath propagation, 9
multiple access technologies (radio systems)
 CDMA, 18, 23, 26
 combining, 19
 FDMA, 18, 21-23
 SDMA, 19, 27-28
 TDMA, 18-20

multiuser diversity, smart scheduling and, 32
mutual synchronization, PRC and, 367-368

N

N-to-One cell encapsulation mode, 350
NACC (Network Assisted Cell Changes), 53
NAP (Network Access Points), 455
NASREQ (Network Access Server Application), 437
NAT (Network Address Translation)
 NAT-PT, 128-130
 private addresses, 128
NE (Network Elements), 388-389
network capabilities databases, 445
Network layer (SDP), 447-448
network policies
 3GPP
 A3/A8 algorithms, 417
 charging rules, 408
 edge policy admission control, 407
 OCS, 405
 OFCS, 405
 PCC model architecture, 404-406
 PCEF, 405, 408
 PCRF, 405
 QoS control, 407
 quota grants, 408
 SPR, 405
 3GPP2
 charging rules, 411
 QoS grants, 411
 SBBC, 409-410
 application policies, 402

- defining, 387
- examples of, 396
- global policies, 392
- IP authentication/authorization
 - Diameter*, 434-437
 - EAP*, 429-431
 - RADIUS*, 425-428, 434
- NE interactions, 388-389
- PDP, 387-388
- PEP, 388
- PIP, 388
- proactive policy control, 390-392
- RAN authorization/encryption, 416
 - A3/A8 algorithms*, 417-419
 - AKA algorithm*, 422
 - CAVE algorithm*, 420-421
 - CCMP*, 423-424
- reactive policy control, 391-392
- subscriber-specific policies, 392-395
- WiMAX
 - QoS grants*, 414-415
 - service-flow management*, 412
- networks**
 - end-to-end reference model, 397
 - independence of, 397-404
 - location awareness, 438
 - maintaining state in, 415-416
 - policies. *See* network policies
 - reference points
 - airlinks*, 399
 - backhaul networks*, 400
 - IP Core*, 402
 - mobile stations*, 398-399
 - Mobile Transport and Application layer*, 402
 - RAN Core*, 401
 - RAN to Gateway communications protocols*, 400
- NOTIFY method (SIP)**, 480

- NPAC (Number Portability Administration Center)**, 458
- nrtVR (Non-Real-Time Variable Rates)**, 415
- NTP (Network Transport Protocol)**, 378
 - broadcast mode, 379
 - client/server mode, 379
 - clock filter algorithm, 380
 - offset calculation in, 379
 - poll intervals, 381
 - security, 381
 - symmetric mode, 379

O

- OAM (Operations and Maintenance)**, 345-347
- OC (Ordinary Clocks)**, 375
- OCS (Online Charging System)**, 405
- OFCS (Offline Charging System)**, 405
- OFDMA systems**, 30
- offloading traditional networks**
 - backhaul offload via pseudowires
 - ATM pseudowires*, 338, 348-351
 - CESoPSN*, 336, 347-348
 - converging multiple RAN technologies*, 339-340
 - encapsulation techniques*, 335
 - GSM Abis/Iub optimization*, 353
 - PWE3*, 340
 - SONET/SDH CEP*, 352-353
 - TDM pseudowires*, 341-344
 - TDMoIP pseudowires*, 335-336, 344-348
 - timing, 356
 - accuracy in*, 357, 359
 - asynchronous networks*, 370

clock hierarchy, 363
clock recovery over packet, 373
combining protocols, 384
external timing mode, 369
Frequency Drift in, 362
jitter in, 361
line timing mode, 369
loop timing mode, 369
 NTP, 378-381
packet-based timing, 372
plesiochronous networks, 371
 PRC, 363-366
precision in, 357-359
pseudo-synchronous networks, 371
 PTP, 375-378
stability in, 357-359
 SyncE, 375
synchronization in, 361, 365-368
synchronous networks, 370
through timing mode, 369
 TICTOC, 381-384
wander in, 362
OMAP (Transaction Capabilities Application Parts), SS7 protocol stack, 467
One-to-One cell encapsulation mode, 351
optimal routing, 298
OSPF (Open Shortest Path First) protocol
 applicability to mobile providers, 135
 network architecture, 134
overlay broadcast video delivery, 493
 DVB-H, 494
 MediaFLO, 495-496
Overlay services (SDP), 449-451

P

P-CSCF (Proxy Call State Control Functions), IMS, 486
P2P TC (Peer-to-Peer Transparent Clocks), 376
packet loss, 170-171
packet switching protocols
 connection-oriented switching methods, 152
 ATM, 154
 bandwidth allocation, 156
 Frame Relay switching, 154
 TDM, 153
 connectionless switching methods
 bandwidth allocation, 167-175
 Ethernet packet switching, 157-159
 MPLS, 160, 163-166
 Ethernet switching methods, 157-159, 176
 redundancy, 177-179
 VLAN switching, 180-181
packet validation, 473
Packet-Switched Core Networks, 271
 cdma2000 PS CN, 313
 session mobility, 316
 simple IP sessions, 314-316
 EPC PS CN, 324-325
 E2E QoS, 327
 EPC macro-mobility, 327
 non-3GPP access, 325
 GTP, 290
 fields of, 291
 header fields, 291
 MBMS-GTP tunnels, 293
 QoS support, 292
 hierarchical mobility and, 288
 I-WLAN PS CN, 318

- IP policy enforcement per subscriber, 289
- Mobile IP
 - agent discovery phase*, 295
 - binding updates*, 295
 - FA*, 294-296
 - HA*, 294-296
 - MN*, 294-297
 - optimal routing*, 298
 - proxy Mobile IPv6*, 301-304
 - registration*, 295
 - security*, 300-301
 - tunneling*, 296
- MIP Encapsulation, 296
- mobility support
 - Layer 3-based IP mobility*, 289
 - network-based local mobility*, 289
 - protocol definition table*, 290
- QoS, 288
- roaming, 288
- UTRAN PS CN, 304-305
 - APN*, 307
 - attaching to*, 306-307
 - direct tunnels*, 311
 - PDP context activation*, 307-309
 - PDP context transfers*, 310-311
 - PDP paging*, 309-310
 - PDP preservation*, 309-310
- WiMAX PS CN
 - CMIP*, 320
 - PMIP*, 321-323
 - QoS*, 324
 - session establishment*, 321
 - session mobility*, 322
- parallel tone modem systems, 30
- partitioning core networks, 218
- path loss, 6
- path vector routing**, 139
 - global routing exchange peering, 143
 - mobile provider Internet access, 141-142
- PCC (Policy and Charging Control) model (3GPP)**, 404-406
- PCEF (Policy and Charging Enforcement Points)**, 405, 408
- PCF (Packet Control Function)**, 313
- PCRF (Policy Control and Charging Rules Function)**, 405
- PDCP (Packet Data Convergence Protocol)**, 62
- PDCP layer (EUTRAN)**, 112-113
- PDF (Policy Decision Function)**
 - 3GPP2 SBBC, 409
 - Data Integration layer (SDP), 446
- PDN GW (Packet Data Network Gateway)**
 - EPC PS CN, 325
 - S5 and S8 interfaces, 255
- PDP (Policy Decision Points), UTRAN PS CN**, 387-388
 - context activation, 307-309
 - context transfers in, 310-311
 - paging in, 309-310
 - preservation in, 309-310
- PDSN**
 - BSC, transporting between, 245
 - HA, transporting between, 245
- Peer Delay mechanism (PTP)**, 377-378
- PEP (Policy Enforcement Points)**, 388, 409
- PF (Policy Function)**, 413
- physical layer synchronization, 356
- physical plane (IN), 455-457
- PIM (Protocol Independent Multicast)**
 - routing, 146, 149
 - PIM-Register, 152
 - PIM-SM, 146
 - PIM-SSM, 148

- PIP (Policy Information Points), 388**
- PLC (Packet Loss Concealment), 343-344**
- pleisochronous networks, 371**
- PMIP (Proxy Mobile IP)**
 - EPC PS CN, 327
 - WiMAX PS CN, 321-323
- PoD (Packet of Disconnect), RADIUS, 428**
- policies**
 - 3GPP**
 - A3/A8 algorithms, 417*
 - charging rules, 408*
 - edge policy admission control, 407*
 - OCS, 405*
 - OFCS, 405*
 - PCC model architecture, 404-406*
 - PCEF, 405, 408*
 - PCRF, 405*
 - QoS control, 407*
 - quota grants, 408*
 - SPR, 405*
 - 3GPP2**
 - charging rules, 411*
 - QoS grants, 411*
 - SBBC, 409-410*
 - application policies, 402
 - defining, 387
 - examples of, 396
 - global policies, 392
 - IP authentication/authorization
 - Diameter, 434-437*
 - EAP, 429, 431*
 - RADIUS, 425-428, 434*
 - NE interactions, 388-389
 - PDP, 387-388
 - PEP, 388
 - PIP, 388
 - proactive policy control, 390-392
 - RAN authorization/encryption, 416
 - A3/A8 algorithms, 417-419*
 - AKA algorithm, 422*
 - CAVE algorithm, 420-421*
 - CCMP, 423-424*
 - reactive policy control, 391-392
 - subscriber-specific policies, 392-395
 - WiMAX
 - QoS grants, 414-415*
 - service-flow management, 412*
- policing connectionless switching methods, 175**
- policy enforcement (IP), Packet-Switched Core Networks, 289**
- poll intervals (NTP), 381**
- port translation, NAT-PT, 128-130**
- port-based VLAN (Virtual Local Area Networks), 181**
- portals (SDP), 447**
- PRC (Primary Reference Clocks), 363**
 - architecture of, 364-366
 - autonomous PRC, 364
 - Cesium tubes, 364
 - MTIE, 365
 - radio-controlled PRC, 364
 - synchronization and, 365-368
- precision (timing), 357-359**
- presence servers (SIP), 479**
- presence technology**
 - location awareness, 451
 - mobile UC, 450
 - MPoP, 449
 - SDP Overlay services, 449
- previous insertion packets, 344**
- private IP addresses, 122**
- proactive policy control, 390-392**

propagation (radio frequency signals), 5

- BPL, 11-12
- decades, 6
- defining, 6
- fast fading, 9
- frequency selective fading, 9
- frequency-dependent losses, 7-8
- ground reflection and, 6
- indoor coverage, 11-12
- log-normal fading, 11
- multipath propagation, 9
- outdoor coverage, 6-7
- path loss, 6
- Rayleigh fading, 9, 17
- shadowing, 11

propagation delays, 168

proxy application servers, 215

Proxy Mobile IP, WiMAX and, 266

proxy Mobile IPv6, 301-302

- IPv4 support, 303
- overlapping IP address support, 304

proxy servers (SIP), 479

PSDN (Packet Data Serving Node), 313

pseudo-synchronous networks, 371

pseudowires, backhaul offload via, 195

- ATM pseudowires, 348
 - AAL5 frame encapsulation, 351*
 - architecture of, 349*
 - Control Words, 350*
 - EVDO/GSM networks, 338*
 - generic encapsulation, 349*
 - N-to-One cell encapsulation mode, 350*
 - One-to-One cell encapsulation mode, 351*
 - troubleshooting, 351*

CESoPSN

- Inter-MSC/BSC connectivity, 336*
- packet structure, 347*
- RTP, 348*
- TDMoIP versus, 348*

converging multiple RAN technologies, 339-340

encapsulation techniques, 335

GSM Abis/Iub optimization, 353

PWE3, 340

SONET/SDH CEP, 352-353

TDM pseudowires

- interpolation packets, 344*
- PLC, 343-344*
- previous insertion packets, 344*
- SAToP class, 341*
- structure-aware transport, 343*
- Structure-Aware Transport over Packet class, 341*
- zero insertion packets, 344*

TDMoIP pseudowires

- adapted payloads, 345*
- CESoPSN versus, 348*
- Control Words, 345*
- EVDO/GSM networks, 335-336*
- generic encapsulation, 344-345*
- OAM, 345-347*
- PSN headers, 345*

PSN

converged PSN RAN, 257

RAN, 227

TDMoIP pseudowires, 345

PTP (Precision Time Protocol)

BC, 375

conformance in, 378

Delay Request-Response mechanism, 376

E2E TC, 376
 OC, 375
 P2P TC, 376
 Peer Delay mechanism, 377-378
 profiles in, 378
 synchronization in, 376-378
 TC, 375
**PUSC (Partial Usage of Subcarriers),
 WiMAX, 103-104**
**PWE3 (Pseudowire Emulation Edge-
 to-Edge), 340**

Q

**QAM (Quadrature Amplitude
 Modulation), 13-16**
QoS (Quality of Service)
 3GPP, 407
 3GPP2, 411
 connection-oriented switching meth-
 ods, bandwidth allocation, 156
 connectionless switching methods,
 bandwidth allocation, 167
availability, 172
delays, 168
jitter, 169
loss, 170-171
 EPC PS CN, 327
 GPRS access, 52-53
 Packet-Switched Core Networks, 288
 WiMAX, 414
BE services, 415
ErtVR, 414
nrtVR, 415
rtVR, 414
UGS, 414
WiMAX PS CN, 324
**QPSK (Quaternary Phase Shift
 Keying), modulation and, 13**

quads (STP), 462
queue management
 class queuing, connectionless switch-
 ing methods, 174-175
 connection-oriented switching meth-
 ods, bandwidth allocation, 156
 connectionless switching methods,
 bandwidth allocation, 172
 queuing delays, 168
quota grants, 3GPP, 408

R

**radio-controlled PRC (Primary
 Reference Clocks), 364**
Radio Frequency Spectrum, 2
 ELF, 2
 IMT operation, 3
 ITU and, 3-4
 UHF, 3
radio systems
 FDD, 354
 modulation
AMC, 29
BER, 15-17
BPSK, 12
QAM, 13-16
QPSK, 13
SNR, 15
 multiple access technologies
CDMA, 18, 23, 26
combining, 19
FDMA, 18, 21-23
SDMA, 19, 27-28
TDMA, 18-20
 propagation, 5
BPL, 11-12
decades, 6
defining, 6

- fast fading*, 9
- frequency selective fading*, 9
- frequency-dependent losses*, 7-8
- ground reflection and*, 6
- indoor coverage*, 11-12
- log-normal fading*, 11
- multipath propagation*, 9
- outdoor coverage*, 6-7
- path loss*, 6
- Rayleigh fading*, 9, 17
- shadowing*, 11
- Radio Frequency Spectrum
 - ELF*, 2
 - IMT operation*, 3
 - ITU and*, 3-4
 - UHF*, 3
- synchronization, 354-355
- TDD, 354
- troubleshooting
 - ARQ*, 34
 - diversity combining*, 35
 - FEC codes*, 28-30
 - multipath effects*, 29-31
 - smart scheduling*, 31-32
 - spatial multiplexing*, 35-36
- RADIUS**
 - EAP support, 429
 - IP authentication/authorization, 425-428, 434
 - PoD, 428
- RAN (Radio Access Networks)**, 223
 - authorization/encryption, 416
 - A3/A8 algorithms*, 417-419
 - AKA algorithm*, 422
 - CAVE algorithm*, 420-421
 - CCMP*, 423-424
 - converged PSN aggregation, 227
 - converged PSN RAN, 257
 - converged RAN technologies,
 - pseudowire and, 339-340
 - converged TDM aggregation, 223
 - divergent aggregation, 225
 - LTE RAN transport infrastructure, 257
 - RAN Core, 401
 - RAN to Gateway communications protocols, 400
 - transport requirements, summary of, 229
- rating engines, Charging layer (SDP), 447
- Rayleigh fading (radio propagation)**, 9, 17
- reactive policy control, 391-392
- receivers, multicast IP addresses, 123
- redirect servers (SIP), 479
- redundancy**
 - Ethernet switching methods
 - dual-homed Ethernet attached end-systems*, 178
 - partial mesh Ethernet topologies*, 179
 - single-homed Ethernet attached end-systems*, 177
 - Incremental Redundancy, 34
- REFER method (SIP)**, 480
- reflection (ground), propagation and**, 6
- registrars (SIP)**, 479
- registration**
 - All-Registration Request messages, 314
 - Mobile IP, 295
- REL (Release Messages), ISUP and**, 468
- Reserve Phase (QoS)**, 411
- Return Routability exchanges, Mobile IP**, 299

RLC (Radio Link Control) layer
 GPRS, 50
 UTRAN, 60-61

RLC (Release Complete Messages)
 EUTRAN, 112-113
 ISUP and, 468
 WiMAX, 106-107

RNC, NodeB Traffic aggregation into RNC, 237

roaming, Packet-Switched Core Networks, 288

ROHC (Robust Header Compression), 485

routing protocols, 117
 IP addressing, 118
 aggregation, 118
 anchor points in, 119
 IPv4, 120-124, 129
 IPv6 (RFC-4291), 125-129

MAC, 130-131
 Mobile IP, 298
 multicast routing, 145
 DVMRP, 146
 IGMP, 150
 MLD, 151
 PIM routing, 146-149

NAT
 NAT-PT, 128-130
 private addresses, 128

unicast routing, 132
 distance-vector routing algorithms, 132
 link-state routing algorithms, 133-135, 138-139
 path vector routing, 139-143
 static routing, 132
 summary of, 144

unicast tunneling of multicast, 152

RTP, 185
 Absolute Mode, 348
 CESoPSN, 348
 Differential Mode, 348
 TCP, 471
 VoIP bearer, 485

RTT (Round Trip Times), 52

rtVR (Real-Time Variable Rates), 414

S

S-CSCF (Serving Call State Control Functions), IMS, 486

S1-flex technology, 113-114

SAToP (Structure-Agnostic Transport over Packet) class (TDM pseudowires), 341

SBBC (Service-Based Bearer Control), 409-410

SCCP (Signaling Connection Control Part), SS7 protocol stack, 466

SCEF (Service Creation Environment Function), 454

SCEP (Service Creation Environment Points), 456

SCF (Service Control Function), 454

SCP (Service Control Points), 455

SCTP (Stream Control Transmission Protocol), SIGTRAN, 184, 471-473

SDF (Service Data Function), 454

SDMA (Space Division Multiple Access), 19, 27-28

SDP (Service Delivery Platforms), 443
 Capability and Preference Exposure layer, 444-446
 Charging layer, 446-447
 Data Integration layer, 446
 Network layer, 447-448
 Overlay services, 449-451

- physical plane (IN), 455
- portals, 447
- sector localization, 438**
- security**
 - authentication
 - I-WLAN, 95*
 - subscriber-specific policies, 394*
 - WiMAX, 107*
 - authorization, I-WLAN, 95
 - blacklisting, 497
 - encryption, WiMAX, 107
 - EUTRAN, 110
 - I-WLAN, 95
 - LTE, EUTRAN, 110
 - Mobile IP, 300-301
 - NTP, 381
 - spam-filtering (SMS), 497
 - TCP, 471
 - WiMAX, 107
- sequence numbering, 485**
- serialization delays, 168**
- Service Delivery Platforms. See SDP, 443**
- Service-Specific Payload Formats, 353**
- services plane (IN), 453
- SFA (Service Flow Agent), 413
- SFM (Service Flow Manager), 412
- SGSN, 233
- SGW (Serving Gateway), 324
- shadowing, radio propagation, 11
- shaping, connectionless switching methods, 176
- SIB (Service Information Blocks), 454**
- signaling**
 - GSM access systems, 45
 - signaling LAC (Link Access Control), 85
 - signaling plane (core networks), 204
 - signaling transport, 248
- SIGTRAN (Signaling Transport), 470**
 - M2PA, 473
 - M3UA, 475
 - SCTP, 471-473
 - SUA, 476
- single-homed application servers, 220-221**
- SINR (signal-to-Interference-and-Noise Ratio)**
 - Space Time Coding, 37
 - spatial multiplexing, 36-37
- SIP (Session Initiation Protocol), 186, 478**
 - addressing, 480
 - bridging, 482
 - location servers, 479
 - methods of, 480-481
 - presence servers, 479
 - proxy servers, 479
 - redirect servers, 479
 - registrars, 479
 - SIP User Agent, 479
 - SIP-I, 286, 485
 - SIP-T, 482-484
- SM-SC (Short Message Service Centers), 272**
- SMAF (Service Management Access Function)**
 - DFP (IN), 454
 - physical plane (IN), 456
- smart scheduling**
 - multiuser diversity, 32
 - radio systems, troubleshooting in, 31-32
- SMF (Service Management Function), 454**
- SMP (Service Management Points), 456**

- SMS (Short Message Services), 272, 469**
 - Circuit-Switched Core Networks, 281
 - GSM access systems, 46
 - SMS Spam-filtering, 497
- SMSC (Short Message Service Center), 469**
- SNDCP (Sub-Network Dependent Convergence Protocol), 52**
- SNR (Signal-to-Noise Ratios), modulation and, 15**
- SOA (Service Order Administration), 458**
- softswitches**
 - Call Agents, 459
 - Feature Services, 459
 - MGW, 460
- SONET/SDH CEP (Circuit Emulation over Packet), 352**
 - DBA, 353
 - fragments, 353
 - Service-Specific Payload Formats, 353
- Space Time Coding, 37**
- spam-filtering (SMS), 497**
- spatial multiplexing**
 - MIMO, 35-36
 - radio systems, troubleshooting in, 35-36
 - SINR, 36-37
- Spectrum (Radio Frequency)**
 - ELF, 2
 - IMT operation, 3
 - ITU and, 3-4
 - UHF, 3
- SPR (Subscription Policy Repository), 405**
- spread spectrum systems, 29**
- SRF (Specialized Resource Function), 454**
- SS7 (Signaling System #7), 461**
 - A-Links, 462
 - architecture of, 462
 - B-Links, 463
 - C-Links, 464
 - D-Links, 463
 - E-Links, 464
 - F-Links, 465
 - mated pairs, 462
 - protocol stack, 465, 470
 - ISUP*, 467
 - MAP*, 467
 - MTP*, 466
 - OMAP*, 467
 - SCCP*, 466
 - TCAP*, 466
 - quads, 462
 - SU, 468
- SSF (Service Switching Function), 454**
- SSP (Service Switching Points), 455**
- stability (timing), 357-359**
- static routing, 132**
- stations (mobile), 398-399**
- STP (Signaling Transfer Points), 462**
- structure-aware transport (TDM pseudowires), 343**
- Structure-Aware Transport over Packet class (TDM pseudowires), 341**
- SU (Signaling Units), 468**
- SUA (SCCP User Adaptation), SIGTRAN, 476**
- SUBSCRIBE method (SIP), 480**
- subscriber profiles, 444**
- subscriber self-care databases, 445**
- subscriber-specific policies, 392-395**
- switching delays, 168**
- symmetric mode (NTP), 379**

synchronization

- combining protocols, 384
- defining, 361
- free-running oscillators, 356
- GPS, 356
- higher-layer synchronization, 356
- NTP, 378-381
- physical layer synchronization, 356
- PRC and, 365-368
- PTP, 375-378
 - BC*, 375
 - conformance in*, 378
 - Delay Request-Response mechanism*, 376
 - E2E TC*, 376
 - OC*, 375
 - P2P TC*, 376
 - Peer Delay mechanism*, 377-378
 - profiles in*, 378
 - TC*, 375
- radio systems, 354-355
- service requirements, 355
- SyncE, 375
- synchronous networks, 370
- TICTOC, 381-384
- wireless technology requirements, 354-355
- synchronous wire-line transport mode, 197-198
- synchronous wireless transport mode, 199

T

-
- T-LDP (Targeted Label Distribution Protocol), 194
 - tagging, VLAN, 180
 - TC (Transparent Clocks), 375

- TCAP (Transaction Capabilities Application Parts), SS7 protocol stack, 275, 466
- TCP (Transmission Control Protocol), 183, 471
- TDD (Time Division Duplexing), 354
- TDM (Time Division Multiplexing), 153
 - RAN, converged TDM aggregation, 223
 - structured TDM trunks, core networks and, 201-202
 - TDM pseudowires
 - interpolation packets*, 344
 - PLC*, 343-344
 - previous insertion packets*, 344
 - SAToP class*, 341
 - structure-aware transport*, 343
 - Structure-Aware Transport over Packet class*, 341
 - zero insertion packets*, 344
 - TDMoIP pseudowires
 - adapted payloads*, 345
 - CESoPSN versus*, 348
 - Control Words*, 345
 - generic encapsulation*, 344-345
 - OAM*, 345-347
 - PSN headers*, 345
- TDMA (Time Division Multiple Access), 18-20
- TDMoIP pseudowires, backhaul offload of EVDO/GSM networks, 335-336
- TFO (tandem-free operations), 206
- through timing mode, 369
- TICTOC (Timing over IP Connection and Transfer of Clock BOF), 381-384
 - clients of, 381
 - frequency acquisition modules, 383
 - frequency presentation modules, 383

- generic modules, 384
- time acquisition modules, 384
- time presentation modules, 384
- time acquisition modules (TICTOC), 384**
- time presentation modules (TICTOC), 384**
- timestamping, 485**
- timing, 356**
 - asynchronous networks, 370-371
 - clock hierarchy, 363
 - clock recovery over packet, 373
 - combining protocols, 384
 - external timing mode, 369
 - Frequency Drift in, 362
 - jitter in, 361
 - line timing mode, 369
 - loop timing mode, 369
 - NTP, 378-381
 - broadcast mode, 379*
 - client/server mode, 379*
 - clock filter algorithm, 380*
 - offset calculation in, 379*
 - poll intervals, 381*
 - security, 381*
 - symmetric mode, 379*
 - packet-based timing, 372
 - plesiochronous networks, 371
 - PRC, 363
 - architecture of, 364-366*
 - autonomous PRC, 364*
 - Cesium tubes, 364*
 - MTIE, 365*
 - radio-controlled PRC, 364*
 - synchronization and, 365-368*
 - precision defining, 357-359
 - PTP
 - BC, 375*
 - conformance in, 378*
 - Delay Request-Response mechanism, 376*
 - E2E TC, 376*
 - OC, 375*
 - P2P TC, 376*
 - Peer Delay mechanism, 377-378*
 - profiles in, 378*
 - synchronization in, 376-378*
 - TC, 375*
 - SyncE, 375
 - synchronization in, 361, 365-368
 - synchronous networks, 370
 - through timing mode, 369
- TICTOC**
 - clients of, 381*
 - frequency acquisition modules, 383*
 - frequency presentation modules, 383*
 - generic modules, 384*
 - time acquisition modules, 384*
 - time presentation modules, 384*
- wander in, 362
- TLDP (Targeted LDP), 164**
- TPF (Traffic Plane Function), 409**
- traffic classification, 172**
- transcoded voice transport, voice bearer plane (core networks), 206**
- transmission systems**
 - asynchronous wire-line transport mode, 198-199
 - asynchronous wireless transport mode, 200
 - synchronous wire-line transport mode, 197-198
 - synchronous wireless transport mode, 199
- transport infrastructures, evolution of, 268**

transport modes

- asynchronous wire-line transport mode, 198-199
- asynchronous wireless transport mode, 200
- synchronous wire-line transport mode, 197-198
- synchronous wireless transport mode, 199
- TRAU (Transcoding and Rate Adaptation Units), 46
- TrFO (Transcoder Free Operations), 207-208, 287
- triangulation, 438
- trilateration, 438
- troubleshooting
 - ATM pseudowires, 351
 - radio systems
 - ARQ, 34
 - diversity combining*, 35
 - FEC codes*, 28-30
 - multipath effects*, 29-31
 - smart scheduling*, 31-32
 - spatial multiplexing*, 35-36
- trunking, VLAN switching, 180
- tunneling, 187
 - GTP, 190-191
 - IPSec ESP, 191
 - Layer 2 frames, transporting
 - L2TPv3, 193
 - T-LDP, 194
 - transitioning mobile provider networks via pseudowires*, 195
 - MOBIKE protocol, 192
 - Mobile IP, 187-189, 296
 - multicast distribution trees, 125

- tunneling-encoded voice bearers, 207
- unicast tunneling of multicast, 152

U

-
- UC (Unified Communications), 450
 - UDP (User Datagram Protocol), 184
 - UGS (Unsolicited Grant Service), 414
 - UHF (Ultra High Frequency), 3
 - UMA/GAM, 99
 - UMTS (Universal Mobile Telecommunications Systems). *See* UTRAN (UMTS Terrestrial Access Networks)
 - unicast IP addresses
 - IPv4, 122
 - IPv6 (RFC-4291), 126
 - unicast routing
 - distance-vector routing algorithms, 132
 - link-state routing algorithms, 133
 - Integrated IS-IS*, 138-139
 - OSPF protocol*, 134-135
 - path vector routing, 139
 - global routing exchange peering*, 143
 - mobile provider Internet access*, 141-142
 - static routing, 132
 - summary of, 144
 - unicast tunneling of multicast
 - MSDP, 152
 - PIM-Register, 152
 - unicast video delivery, 491-492
 - UPDATE method (SIP), 480
 - updates, binding updates, 295
 - user plane protocols, 56
 - user transport, 249-251

UTRAN

Circuit-Switched Core Networks, 284

Packet-Switched Core Networks,
304-305

APN, 307

attaching to, 306-307

direct tunnels, 311

*PDP context activation,
307-309*

PDP context transfers, 310-311

PDP paging, 309-310

PDP preservation, 309-310

UTRAN (UMTS Terrestrial Access Networks), 55

architecture of, 56, 235

broadcast support, 66

Control Plane transport, 237

Core Network Control Plane, 58

eHSPA, 77-78

HNB, 78-79

HSDPA, 67-73

HSUPA, 74-76

Iur interface, 57

Iub interface, 236

IuCS interface, 239-241

IuPS interface, 239

Iur interface, 236-238

MAC layer, 60-61

MBMS, 66-67

multicast support, 66

NodeB Traffic aggregation into RNC,
237

packet-switched services, 64-65

PDCP, 62

RLC layer, 60-61

transport network, 62-63

UMTS R4 networks, backhaul
offload via ATM pseudowires,
338

UMTS physical layer, 58-59

user plane protocols, 56

User Plane transport, 237

V**video delivery, 490**

multicast video delivery, 492-493

overlay broadcast video delivery, 493

DVB-H, 494

MediaFLO, 495-496

unicast video delivery, 491-492

VLAN (Virtual Local Area Networks)

switching

link segmentation, 180-181

multiple VLAN interfaces, 181

network segmentation, 181

port-based VLAN, 181

trunking, 180

tagging, 180

VLR (Visitor Location Registers), 272**voice bearer plane (core networks)**

transcoded voice transport, 206

TrFO voice bearer transport, 208

tunneling-encoded voice bearers, 207

voice bearer switching on mobile
wireless architectures, 205

VoIP packet transport, 205

voice signaling

SIGTRAN, 470-476

SIP, 478-484

SMS, 469

SS7, 461

A-Links, 462

architecture of, 462

B-Links, 463

C-Links, 464

D-Links, 463

E-Links, 464

- F-Links*, 465
- mated pairs*, 462
- protocol stack*, 465-467, 470
- quads*, 462
- SU*, 468
- voice transport, GSM access systems, 46
- VoIP (Voice over IP), 460
 - packet transport, voice bearer plane (core networks), 205
 - voice signaling
 - SIGTRAN*, 470-476
 - SIP*, 478-484
 - SMS*, 469
 - SS7*, 461-470
 - VoIP bearer, 485

W-X-Y-Z

- wander
 - defining, 362
 - Frequency Drift, 362
- WCDMA Core Networks, 283-285
- WiMAX, 99
 - 802.16e (IEEE 802.16-2005), 100
 - AAS, 105-106
 - architecture of, 259
 - ASN reference interfaces, 260
 - Client Mobile IP, 266
 - ETH-CS, 262
 - evolution of, 107
 - frame structure of, 103
 - interfaces of, 100
 - IP connectivity models, 262
 - IP-CS, 263
 - MAC layer, 106-107

- mobility handover on R4 and R8 interfaces, 263
 - R4 protocol for ASN-GW to ASN-GW handover*, 264
 - R8 protocol for BS to BS handover*, 264
 - transport for R4 and R8 reference interfaces*, 265
- Packet-Switched Core Networks
 - CMIP*, 320
 - PMIP*, 321-323
 - QoS*, 324
 - session establishment*, 321
 - session mobility*, 322
- physical layer, 102-103
 - AMC*, 103
 - data rates*, 104-105
 - FCH*, 104
 - PUSC*, 103-104
- Policy Framework, 412
- profiles of, 100
- protocol architecture of, 101
- Proxy Mobile IP, 266
- QoS grants
 - BE services*, 415
 - ErtVR*, 414
 - nrtVR*, 415
 - rtVR*, 414
 - UGS*, 414
- R3 protocol for ASN-GW o HA, 266
- R6 protocol for BS to ASN-GW, 262
- RLC layer, 106-107
- security, 107
- service flows, 106-107
- transport architecture, 267-268
- wireless policies
 - 3GPP
 - A3/A8 algorithms*, 417
 - charging rules*, 408