

Stamatios Kartalopoulos

Next Generation Intelligent Optical Networks

From Access to Backbone

 Springer

Next Generation Intelligent Optical Networks

Stamatios V. Kartalopoulos

Next Generation Intelligent Optical Networks

From Access to Backbone

Dr. Stamatios V. Kartalopoulos
The University of Oklahoma
Room 4413
Schusterman Center
4502 E. 41st Street, Bldg 4, Room 4413
Tulsa, OK 74135
USA

ISBN: 978-0-387-71755-5 e-ISBN: 978-0-387-71756-2

Library of Congress Control Number: 2007933715

© 2008 Springer Science+Business Media, LLC

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed on acid-free paper.

9 8 7 6 5 4 3 2 1

springer.com

To my wife Anita for her love and support

Preface

Optical networks have been in commercial deployment since the early 1980s as a result of advances in optical, photonic, and material technologies. Although the initial deployment was based on silica fiber with a single wavelength modulated at low data rates, it was quickly demonstrated that fiber can deliver much more bandwidth than any other transmission medium, twisted pair wire, coaxial cable, or wireless. Since then, the optical network evolved to include more exciting technologies, gratings, optical filters, optical multiplexers, and optical amplifiers so that today a single fiber can transport an unprecedented aggregate data rate that exceeds Tbps, and this is not the upper limit yet. Thus, the fiber optic network has been the network of choice, and it is expected to remain so for many generations to come, for both synchronous and asynchronous payloads; voice, data, video, interactive video, games, music, text, and more.

In the last few years, we have also witnessed an increase in network attacks as a result of store and forward computer-based nodes. These attacks have many malicious objectives: harvest someone else's data, impersonate another user, cause denial of service, destroy files, and more. As a result, a new field in communication is becoming important, communication networks and information security. In fact, the network architect and system designer is currently challenged to include enhanced features such as intruder detection, service restoration and countermeasures, intruder avoidance, and so on. In all, the next generation optical network is intelligent and able to detect and outsmart malicious intruders.

This is the first book, to the best of my knowledge, which bridges two disjoint topics, optical networks and network security. It provides a comprehensive treatment of the next generation optical network and a comprehensive treatment of cryptographic algorithms, the quantum optical network, including advanced topics such as teleportation, and how detection and countermeasure strategies may be used. Therefore, we believe that this book differentiates from many others and presents a holistic approach to the treatment of secure optical networks, including fiber to the home (FTTH) and free space optical (FSO).

This book deserves my thanks and appreciation because it came into being after the persistence of Mr. Jason Ward, the expert "literal" eyes of Mrs. Caitlin Womersley, and the many management and production personnel of Springer US anonymous to me.

I hope that the next generation optical network will be intelligent, and when using wireless technologies at the edge, it will enable unlimited and secure communication multi-services with a single and portable device to anyone, anyplace, anytime at low cost.

Stamatis V. Kartalopoulos, Ph.D.

Acknowledgements

To my wife Anita, son Bill, and daughter Stephanie for consistent patience and encouragement. To my publishers and staff for cooperation, enthusiasm, and project management. To the anonymous reviewers for useful comments and constructive criticism. And to all those who worked diligently on the production of this book.

Contents

1	Communication Networks	1
1.1	Analog and Digital Transmission	1
1.2	Breaking the Traffic Barrier	3
1.3	Voice and Data Networks	5
1.3.1	PSTN and the SS7 protocol	5
1.3.2	Data Networks and Protocols	8
1.3.3	Narrowband, Broadband, and Ultraband Services	9
1.3.4	Circuit Switched Versus Store and Forward	10
1.3.5	Traffic and Service Evolution in Optical Networks	12
1.3.6	Reliability of Optical Networks	12
1.3.7	Security in Optical Networks	12
	References	13
2	Digital Networks	15
2.1	Synchronous Optical Networks: SONET/SDH	15
2.1.1	Introduction	15
2.1.2	SONET Frames	17
2.1.3	Virtual Tributaries and Tributary Units	19
2.1.4	STS- <i>N</i> Frames	22
2.1.5	Maintenance	23
2.2	Asynchronous Data/Packet Networks	24
2.2.1	Introduction	24
2.2.2	Synchronization and Timing	25
2.2.3	Data Traffic	25
2.2.4	Packet Networks	26
2.3	Review of Data Networks	28
2.3.1	Asynchronous Transfer Mode	28
2.3.2	Ethernet	32
2.3.3	Gigabit Ethernet	33
2.3.4	10 Gigabit Ethernet	36
2.3.5	FDDI	37
2.3.6	Switched Multi-megabit Data Services	39
2.3.7	Frame Relay	39
2.3.8	The Transmission Control Protocol	39
2.3.9	The User Datagram Protocol	40
2.3.10	The Real-Time Transport Protocol	41
2.3.11	Internet Protocol	41

2.3.12	The Point-to-Point Protocol	43
2.3.13	4B/5B and 8B/10B Block Coding	46
2.3.14	Fiber Channel	47
2.3.15	ESCON protocol	50
2.3.16	FICON Protocol	51
2.4	Resilient Packet Ring	52
	References	53
3	WDM Technology and Networks	55
3.1	Introduction	55
3.2	The Optical Fiber in Communications	55
3.2.1	Propagation of Light in Matter	56
3.2.2	Effects That Affect the Propagation of Light in Fiber	57
3.3	The Optical Communications Spectrum	63
3.4	Types of Fiber	65
3.4.1	Optical Power Limit	66
3.4.2	Fiber Birefringence	67
3.4.3	Fiber Dispersion	67
3.4.4	Non-linear Phenomena Cause Positive and Negative Effects	69
3.5	Optical Amplifiers	69
3.5.1	Raman Amplification	70
3.5.2	EDFA Amplification	71
3.5.3	SOA Amplification	73
3.6	Optical Add-Drop Multiplexers	73
3.7	DWDM Networks	73
3.7.1	DWDM Network Topologies	74
3.7.2	Optical Network Interfaces	75
3.7.3	Network Switching	78
3.7.4	Timing and Synchronization	81
3.7.5	Channel and Link Protection	81
3.7.6	Routing	82
3.8	Access WDM Systems	83
3.8.1	The General PON	84
3.8.2	CWDM-PON	87
3.8.3	TDM-PON	87
3.8.4	TDM-PON Versus WDM-PON	89
3.8.5	Hierarchical CWDM/TDM-PON	89
3.8.6	How Real Is PON?	94
3.8.7	Free Space Optical	95
	References	97
4	Next Generation SONET/SDH	101
4.1	Traffic and Service Convergence	101
4.2	Next Generation SONET/SDH Networks	104
4.2.1	Next Generation Ring Networks	104
4.2.2	Next Generation Mesh Networks	105
4.3	Next Generation Protocols	110
4.3.1	Concatenation	111
4.3.2	Generic Multi-protocol Label Switching	112
4.3.3	The Generic Framing Procedure	114

4.3.4	LCAS	120
4.3.5	LAPS	123
4.4	Concatenation Efficiency	127
	References	128
5	The Optical Transport Network	129
5.1	Introduction	129
5.2	OTN Network Layers	129
5.3	FEC in OTN	131
5.4	OTN Frame Structure	132
5.4.1	OPU-k	132
5.4.2	ODU-k	132
5.4.3	OTU-k	134
5.4.4	The Optical Channel	135
5.4.5	Optical Channel Carrier and Optical Channel Group	136
5.4.6	Nonassociated Overhead	137
5.4.7	Mapping GFP Frames in OPU-k	137
5.5	OTN and DWDM	138
5.6	OTN Management	139
	References	140
6	Network Synchronization	141
6.1	Introduction	141
6.2	Synchronization	141
6.2.1	The Primary Reference Source	142
6.2.2	The Node Timing Unit and the Phase Lock Loop	143
6.2.3	Synchronization Impairments	145
6.3	The Timing Signal	146
6.4	Signal Quality	147
6.4.1	Noise Sources	148
6.4.2	Quantization Noise	149
6.5	Transmission Factors	149
6.5.1	Phase Distortion and Dispersion	150
6.5.2	Frequency Distortion	150
6.5.3	Polarization Distortion	150
6.5.4	Noise due to Nonlinearity of the Medium	150
6.5.5	ASE	150
6.6	Jitter and Wander	150
6.6.1	Intersymbol Interference	153
6.6.2	Data-Dependent Jitter	153
6.6.3	Pulse-Width Distortion Jitter	154
6.6.4	Sinusoidal Jitter	154
6.6.5	Uncorrelated Bounded Jitter	154
6.6.6	Stokes Noise, Chromatic Jitter, and FWM noise	154
6.6.7	Sources of Jitter	155
6.6.8	Jitter Generation, Tolerance, and Transfer	156
6.7	Photodetector Responsivity and Noise Contributors	156
	References	157
7	Network Performance	159
7.1	Introduction	159

7.2	Channel Performance	161
7.3	Carrier to Noise Ratio and Power–Bandwidth Ratio	162
7.4	Shannon’s Limit	163
7.5	Optical Signal to Noise Ratio	163
7.6	Factors That Affect Channel Performance	164
7.7	Analysis of BER and SNR Related to Channel Performance	165
7.8	BER and SNR Statistical Estimation Method	167
7.9	Circuit for In-Service and Real-Time Performance Estimation	170
7.9.1	The Circuit	170
7.9.2	Performance of the Circuit	170
	References	171
8	Traffic Management and Control	173
8.1	Introduction	173
8.2	Client Bandwidth Management	175
8.3	Wavelength Management	175
8.3.1	Paths with ROADM斯	177
8.4	Traffic Management	177
8.5	Congestion Management	178
8.6	Routing Algorithms	178
8.7	Discovery of Optical Network Topology	179
8.8	Node and Network Provisioning	180
8.9	Wavelength Management Strategies	180
	References	181
9	Network Protection and Fault Management	183
9.1	Introduction	183
9.2	Fault Detection and Isolation	184
9.3	Fault and Service Protection	184
9.4	Point-to-Point Networks	186
9.4.1	Medium-Haul and Short-Haul Optical Networks	186
9.5	Mesh Network Protection	187
9.6	Ring-Network Protection	188
9.7	Ring-to-Ring Protection	189
9.8	Multi-ring Shared Protection	190
	References	190
10	Network Security	191
10.1	An Old Concern	191
10.2	Network Security Issues	195
10.3	Definitions	196
10.4	Security Levels	200
10.5	Security Layers in Communication Networks	201
10.5.1	Security on the Information Layer	201
10.5.2	Security on the MAC/Network Layer	202
10.5.3	Security on the Link Layer	203
10.6	Mathematical Foundations for Security Coding	203
10.6.1	Prime Number	203
10.6.2	Modulus Arithmetic	204
10.6.3	Greatest Common Divisor	205
10.6.4	Groups	206

10.6.5	Rings	207
10.6.6	Fields	208
10.7	Ciphers	208
10.7.1	Symmetric Ciphers	208
10.7.2	Shift Cipher	208
10.7.3	The Substitution or Random Shift Cipher	209
10.7.4	The Permutation Cipher	209
10.7.5	The Data Encryption Standard (DES)	209
10.7.6	The Advanced Encryption Standard (AES)	210
10.7.7	The RC4 Algorithm	210
10.7.8	Asymmetric Ciphers	211
10.7.9	The Integer Factorization Problem	212
10.7.10	Elliptic Curve Factoring	212
10.7.11	The RSA Algorithm	212
10.8	Quantum Cryptography	213
10.9	Key Distribution	215
10.9.1	Merkley's Algorithm	215
10.9.2	Shamir's Key Distribution Method	215
10.9.3	Diffie–Hellman Key Exchange	215
10.9.4	Elliptic Curve Cryptography	217
10.9.5	Digital Signature	224
10.9.6	The Trusted Third Party or Key Escrow Encryption System	225
10.10	Quantum Key Distribution	225
10.10.1	Polarization-Based Quantum Key Distribution	226
10.10.2	Entangled States and Quantum Teleportation	229
10.10.3	Quantum Teleportation and Quantum Key Distribution	232
10.10.4	A Trivialized Example	233
10.10.5	Current Issues	233
10.11	Current Vulnerabilities in Quantum Cryptography	234
10.12	Countermeasures in Optical Networks	236
10.12.1	Classification of Security Networks Regarding Countermeasures	236
10.12.2	Discriminating Between Faults and Attacks	236
10.12.3	Estimating the Performance Vector In-Service and in Real Time	238
10.12.4	Detection with Alarm and Countermeasure Intelligence (DACI)	238
10.13	Biometrics and Communication Networks	241
10.14	Security in the Next Generation Optical Networks	242
	References	246
11	Concluding Remarks	253
11.1	Bandwidth Evolution	253
11.2	Convergence	253
11.3	Why Do Not I Have Fiber to My Home?	254
11.4	What About Traditional Services?	254
11.5	How About Security of Information and of the Network?	254
11.6	Number Portability	255
11.7	How Is the Network Managed?	255
11.8	The Bottom Line	255

Appendix: VPI systems - Demonstration Examples	257
Acronyms	261
Short Bio	273
Index	275

Introduction

Optical technology and its applicability in communication networks has intrigued scientists and communications engineers alike. The reason is simple: fiber optic networks are the only ones that can transport at the speed of light a humongous amount of data in the unit of time.

Since the first optical protocol came into being, SONET/SDH has been proven for robustness, bandwidth transport and fast switching to protection. However, the transportable bandwidth and data was soon overrun by an unsaturated bandwidth appetite and new services. Within a decade or so, this led to a new optical network that was based on an optical and photonic technology known as dense wavelength division multiplexing (DWDM). The success of this optical network helped to solve the amount of transportable traffic, although at the same time it created a bottleneck at the network edge or access. Currently, different technologies are under development, and fiber is deployed at the access using an almost passive optical network (PON) technology suitable for fiber to the premises (FTTP). At the same time, new protocols have been developed to allow for a variety of payloads to be transported over the optical network.

As a consequence, the next generation optical network must be backwards compatible with traditional networks and also include nontraditional characteristic features and intelligence. Among these are protocol adaptability, future proofing, bandwidth elasticity, scalability, service protection, and security, both network and information. Security is an emerging topic in optical networks, and highly sophisticated algorithms and methods are under development and also under scrutiny to assure that they will not be outsmarted by sophisticated intruders.

This book provides a comprehensive treatment of the next generation intelligent optical networks, from access to the core where it also provides an insight into new protocols, connectivity management, and network security. Chapter 1 provides an introduction to telecommunications network from which the digital network evolved, which is described in Chapter 2. Chapter 3 describes the modern DWDM network and the technology that makes it possible. Chapters 4 and 5 provide a description of the next generation optical network, NG-SDH and OTN, and the new protocols that enable them to transport all known protocols mapped in a common payload envelope efficiently, reliably, and protectively. Chapter 6 describes the synchronization aspects of modern optical networks, and Chapter 7 describes the current issues with network and link performance, as well as methods for in-service and real-time performance estimation, BER, SNR, Q, and more. Chapter 8 describes the traffic management and control and wavelength management strategies that are needed by the multi-wavelength intelligent optical network of today and tomorrow. Chapter 9 describes network protection and service protection strategies as well as fault management. Network and information security is a growing concern of users, network providers, and government. As a consequence, we have enhanced this book with a thorough description of network security from the application/information layer to MAC and to physical layer. In this chapter, we review cryptographic methods including quantum cryptography and we describe detection methods and countermeasures. Finally, Chapter 11 provides

a discussion on key issues of the next generation intelligent optical network such as protocol and service convergence, portability, security, backward compatibility and retrofitting, and more.

It is my hope that this book will excite and stimulate the interest of the reader in the exciting Next Generation Intelligent Optical Network and it will aid in the development of robust, efficient, and cost-effective systems and networks that will help develop and offer novel services, cost-efficiently and securely.

Stamatis V. Kartalopoulos, Ph.D.

Chapter 1

Communication Networks

1.1 Analog and Digital Transmission

The transmission of analog electrical signals over twisted pair copper cables emulates the acoustic voice signal within a narrowband between 300 and 3,400 Hz within a 4,000 Hz frequency band; the unused spectrum 0–300 and 3,400–4,000 Hz provides a guardband and also a useful sub-band for out-of-band signaling.

As demand for service increases, the analog signal, being subject to attenuation and electromagnetic interference, is difficult to multiplex with other signals reliably and cost-efficiently. However, if the analog signal is converted to digital, then the multiplexing problem is greatly simplified at the small expense of better engineered trunk lines. Based on this, the analog signal is periodically sampled at 8,000 samples per second [1, 2], and each sample is converted to eight bits via a coder-decoder (CODEC) using a nonlinear digital pulse coded modulation (PCM) method, Fig. 1.1. Thus, the signal is converted to a continuous 64 Kbps digital signal, known as digital service level 0 (DS0), Fig. 1.2. Having converted the analog signal to digital PCM, many signals can be multiplexed by upping the bit rate accordingly, based on an established digital hierarchical network [3, 4]. Thus, 24 DS0s are multiplexed to produce a digital service level 1 (DS1) signal at 1.544 Mbps and other higher data rates, Table 1.1.

Up to the 1970s, the established digital hierarchy was sufficient to meet the communication bandwidth demand and service needs, if one also considers regulations that did not allow to mix services such as voice and video despite the fact that video over DS1 lines and the videophone had already been demonstrated. However, this was a decade where personal computers and the Internet were in embryonic phase and phone service in the United States was dominated by the old American Telephone and Telegraph Corporation or AT&T; it was the era when the POTS telephone device was permanently connected on the wall and it was also the property of the phone service provider.

At about the beginning of the 1980s, a need for integrated digital services over the same loop came about, but these services were by far close to the services we have today: the equivalent of two voice channels and a substrate 8 Kbps to a total of 144 Kbps. However, at the time this was a radical loop technology and several experiments were (successfully) demonstrated that eventually led to what is known as ISDN (integrated services digital network) and to DSL (digital subscriber line) [5–11].

* The content of this book is intended to have illustrative and educational value and it should not be regarded as a complete specification of Next Generation Networks or any protocol described herein. The information presented in this book is adapted from standards and from the author's research activities; however, although a serious effort has been made, the author does not warranty that changes have not been made and typographical errors do not exist. The reader is encouraged to consult the most current standards recommendations and manufacturer's data sheets.

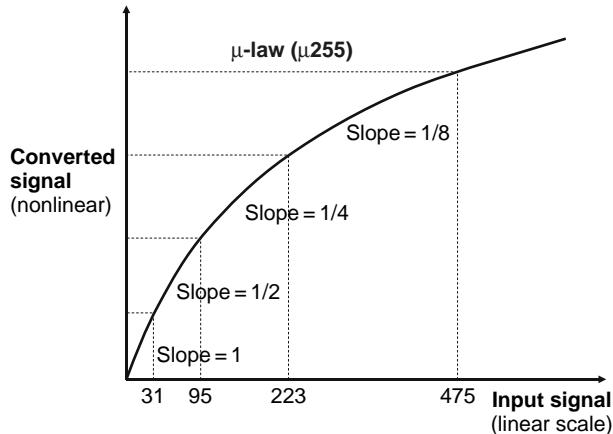


Fig. 1.1 Transfer function for converting linear binary to digital PCM code according to a weighted (nonlinear) curve known as μ -law (in Europe, a similar transfer function is used known as α -law)

Since then, microelectronics have demonstrated an exponential increase in transistor density, antennas have been miniaturized, displays have become ultrathin with very high resolution, novel modulation methods have been deployed, printed circuit technology and packaging have been advanced, and batteries with extended life have been miniaturized. As a consequence, the initial portable or mobile phone that was based on analog signal (AMPS) is slowly being replaced by digital transmission techniques that support voice, data, and low-resolution video.

These incredible advancements over just three decades have opened an appetite for new services and more bandwidth that the traditional communication network was running short in bandwidth capacity. At about the same time, in the 1970s, a new transmission medium became available, the optical fiber based on silica. This medium, being highly purified and with a highly controlled refractive index profile in its core, was able to transport optical signals at unprecedented data rates

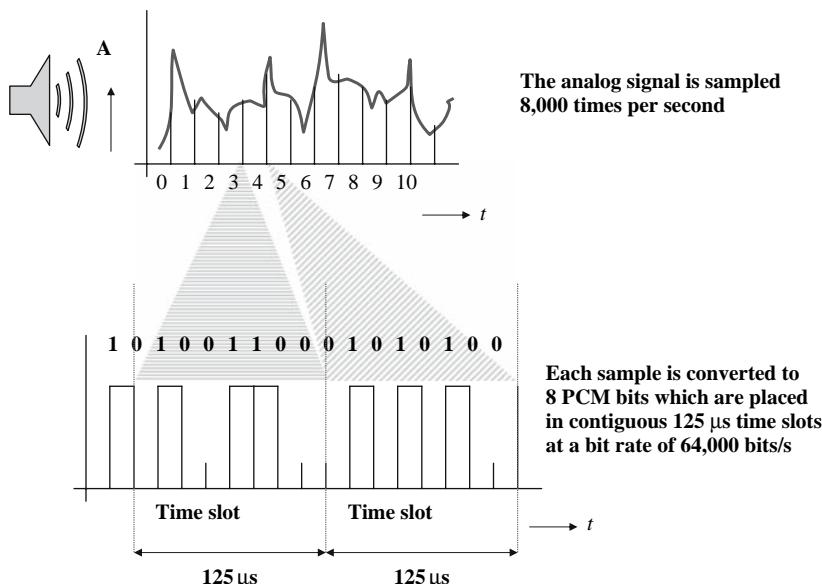


Fig. 1.2 The analog signal is sampled 8,000 times per second, and each sample is converted to eight PCM bits placed in 125 μ s concatenated time slots to generate 64 Kbps (DS0)

Table 1.1 Bit rates in the legacy telecommunications non-optical network

Facility	United States	Europe	Japan
DS0/E0	64 Kbps	64 Kbps	64 Kbps
DS1	1,544 Kbps		1,544 Kbps
E1		2,048 Kbps	
DS1c	3,152 Kbps		3,152 Kbps
DS2	6,312 Kbps		6,312 Kbps
E22		8,448 Kbps	
			32,064 Kbps
E31		34,368 Kbps	
DS3	44,736 Kbps		
DS3c	91,053 Kbps		
			97,728 Kbps
E4		139,264 Kbps	
DS4	274,176 Kbps		
			397.2 Mbps

and distances without amplification. With the first optical transmission demonstration, it was immediately realized that fiber optics is a disruptive technology and the future of telecommunications will be exciting and it will allow for services that could be found in science fiction only. Today, video-phones, teleportation effects, remote surgery, online banking, and many more futuristic services convince us that “the future is here, now”.

The rapidly changing information and communications technologies have summoned World Economic Forums at a high level to negotiate on trade agreements in an effort to set the trade rules in Internet, mobile telephony, video formatting, music formatting, communication technology and networking, security, and other technological developments.

1.2 Breaking the Traffic Barrier

Data traffic has exceeded voice traffic and it is in an explosive path as a result of an abundance of new data services that are offered over the access network. One part that has contributed to this explosive increase in data traffic is emerging wireless, wired, and optical technologies and new techniques that in their own way have increased the accessible bandwidth; digital wireless access technology has enabled Mbps and optical access Gbps allowing for multiplay services, voice, data (IP, Ethernet), and music and video (broadcasting and interactive, streaming, and real time). Another part that contributed to data traffic explosion is new end devices (or gadgets) that have taken advantage of advances in hybrid microelectronics, display technology, RF technology, miniaturized batteries, and advanced packaging; end devices are versatile, pocket size, and affordable. Finally, a third part that has contributed to this explosion is an aggressive pricing model that appeals to very young and to mature customers and a revenue-flow model that satisfies the service providers. One can also add a fourth contributor, an aggressive competitive environment so that every 3 months or so a new gadget becomes available that is smaller, more versatile, more capable, and at lower cost. Thus, the old paradigm of having the same telephone for several years has changed, and telephones have become a perishable commodity so that one may go through few generations in a single year as a result of an appetite for new services and capabilities that cause a bandwidth aggregation which can only be accommodated by high bandwidth access networks.

In addition to high bandwidth demand, many new data services demand quality of service (QoS), reliability, availability and real-time deliverability comparable with that of the legacy public digital synchronous network, as well as bandwidth elasticity, and bandwidth on demand, which only the next generation network can provide.

Thus the question: If the legacy network is characterized by QoS and real time, why don't we improve it instead of needing a next generation network? The legacy synchronous optical network has supported real-time deliverability with reliability and availability. However, when defined in the 1980s, data services were not as pervasive as now, and therefore it is not as cost-efficient for data services as it is for voice. To this, add new technological advancements in wireless and optical technology, and maturing equipment that need replacement, and one finds that it is time for a next generation network with new and advanced technology that is future proofed and cost-efficient to multiplay and anyplay; it is designed with additional intelligence for performance monitoring, control, provisioning, protection, management, security, and more. In particular, the optical backbone network has adopted a relatively new optical technology, the wavelength division multiplexing (WDM) [12, 13], which is capable of transporting many payloads over many optical channels at a bandwidth exceeding Terabits per second per fiber, and thus an enormous aggregate bandwidth capacity.

Another plausible question is: how could such a network with such capacity become cost-efficient for both synchronous voice-type traffic and asynchronous high-capacity data traffic? Again, if one thinks of fibers as "pipes" that transport bandwidth, the answer is found in the supporting protocols, node design and network provisioning and management. And this is where the next generation optical network plays an important role.

To put it in perspective, let us take a look at some interesting data. The data rates of the legacy synchronous networks started from 64 Kbps (DS0) to a rate a little above 44 Mbps (DS3). The synchronous optical network started with a data rate a little below 42 Mbps (OC1) and currently is at 40 Gbps per channel (OC-768) [14], Table 1.2. The initial Ethernet protocol has evolved from a few Mbps to currently 1 Gbps, 10 Gbps and it is still evolving to 20 and 40 Gbps. Thus, in terms of traffic, both TDM-type optical and packet data networks are on a converging path to a common network that satisfies the required cost-efficiency of data networks, and the robustness, real-time delivery, and quality of the synchronous optical network SONET/SDH with high-aggregate data rates that the new WDM technology can support.

Current market indicators show that as more data traffic is transported over the SONET/SDH network, the demand for Ethernet ports on SONET/SDH increases. However, to meet the cost-efficiency of data networks, robustness, and quality requirements of the synchronous network, the SONET/SDH needs to be updated to efficiently transport diverse data protocols, hence "Next Generation SONET/SDH" optical network [15–22].

The initial SONET and SDH standards that were developed in the 1980s and early 1990s recommended methods and specifications for fast and efficient transport of synchronous information. SONET/SDH defines a payload frame of specified fixed capacities that consists of overhead field and a payload field; these frames, regardless of size, would be transmitted within $125\mu\text{s}$ and in a continuous manner one after the other and without gaps (hence *synchronous*). The overhead field specifies alignment, synchronization, maintenance, error control, and other network functions. The

Table 1.2 Bit rates in the synchronous digital optical network (SONET/SDH)

Signal designation		Line rate (Mbps)	
SONET	SDH	Optical	
STS-1	STM-0	OC-1	51.84 (52 M)
STS-3	STM-1	OC-3	155.52 (155 M)
STS-12	STM-4	OC-12	622.08 (622 M)
STS-48	STM-16	OC-48	2,488.32 (2.5 G)
STS-192	STM-64	OC-192	9,953.28 (10 G)
STS-768	STM-256	OC-768	39,813.12 (40 G)

OC-N: Optical carrier-level N

STS-N: Synchronous transport signal-level N

STM-N: Synchronous transport module-level N

payload field transports small data units called *virtual tributaries* (VT) or virtual containers (VC). These data units are also specified in fixed capacities so that they can fill the payload field completely like the pieces of a puzzle. The prespecified capacities are for data transport efficiency reasons since not all digital services are at the same rate or granularity (such as DS1, E1, DS3).

The initial introduction of SONET/SDH was crowned with such success that became a standard network in optical communications. However, with the rapid evolution of data traffic, SONET/SDH did not have the necessary cost-efficiency, simplicity, and traffic granularity in order to compete with the data network. For example, a desirable network that combines both synchronous and asynchronous (data) services should support

- a larger variety of “containers” with selectable bandwidth sizes as needed
- a transporting mechanism that can fit a larger variety of contents and an easily provisioned mix-and-match payload
- quality of service tailored to customer requirements
- a variety of protocols (for both synchronous and asynchronous payloads)
- a more flexible and intelligent routing scheme to support traffic balancing and fault avoidance
- new protocols that can adapt diverse data traffic onto the synchronous payload
- protocols and system architecture that are scalable and future proofed
- reliability
- security
- design simplicity, low power consumption, and small form factor
- bandwidth efficiency, cost-efficiency, and lower equipment cost.

Clearly, the aforementioned requirements present a serious challenge to both network designers and providers. Advanced data services at low cost are not supported by legacy data networks and synchronous optical networks are unprofitable for data services. Thus, there are two choices: make a radical upgrade of the existing data network or make a serious simplification of the optical synchronous network to support quality data services and voice at low cost and at the same time use wavelength division multiplexing (WDM) optical technology. That is, a conceptual fusion of the synchronous (voice-based) network with the asynchronous (packet/data-based) network to an optical intelligent network that combines the cost-efficiency of Ethernet, the reliability, real-time, guaranteed delivery, and QoS of the synchronous optical network, and additionally, the high bandwidth capacity and scalability of WDM technology.

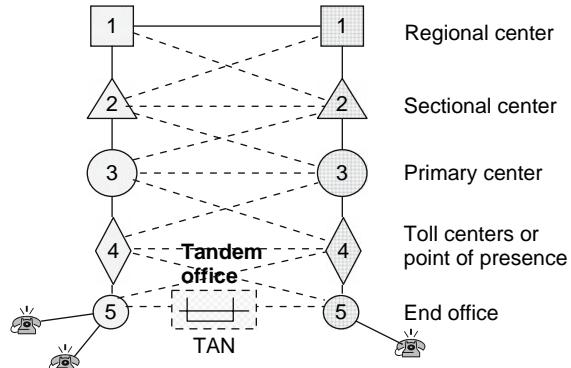
However, to feed a network with converged services and diverse traffic flow at the access points, new access methods and protocols have been developed. Among the access protocols are the wireless LAN (802.11 standard), IP over cable, digital subscriber lines (DSL), computer telephony (CT), and more recently fiber to the home/curb/cabinet/premises/office or x (FTTx). In addition, protocols have been developed such as the generic framing procedure (GFP) to efficiently encapsulate new and old data protocols, IP, IP/PPP, Ethernet, Fiber Channel, FICON, ESCON, ATM as well as TDM and Video and then map them onto the next generation SONET/SDH concatenated frames, which brings us to “The Next Generation intelligent optical network”. As such, the next generation SONET/SDH is an evolution by necessity of a well-known and well-performing transporting vehicle that has been reengineered to meet the current and future communication needs intelligently and cost-efficiently. In Chap. 4, we take a closer look at these protocols and their mapping process.

1.3 Voice and Data Networks

1.3.1 PSTN and the SS7 protocol

The legacy communications network was primarily designed to offer robust voice services, and it consisted of the loop plant at the access side and the trunk plant at the internetworking side. Loops

Fig. 1.3 Traditional communications hierarchy from access to core network



A tandem office provides connectivity between two low-end offices in the same local serving area avoiding toll centers.

consisted of twisted pair (TP) copper and connected the end device, termed as plain old telephone service (POTS), with the nearest switching node (the end office or office level 5) in an hierarchical architecture of switching nodes that makes up the entire communications network, Figs. 1.3, and 1.4. Up to the 1970s, each loop was able to transport low bandwidth bidirectional analog traffic up to 4 kHz, and the trunk was able to transport digital signals level 1, 2, or 3 (DS1 at 1.544 Mbps, DS2 at 6,312 Mbps, and DS3 at 44,736 Mbps); a similar network hierarchy existed in Europe and the rest of the world, although the signals had different bit rates, see Table 1.1.

Because of Ohm's law, the resistance of the loop did not allow the distance of POTS from the end office to exceed 18 Kft with thin copper wires. In the United States, although copper loops up to 18 Kft were able to support POTS service for the majority of urban regions, they could not support POTS service in rural areas and in some suburbia. As a result, the pair-gain system was developed that was able to bring voice services to POTS located many kilometers far from the end office, Fig. 1.5.

Each POTS is associated with a calling number, and this is convenient to residential applications; the well-known Yellow Pages lists residential customers in an alphabetical order within a city serving

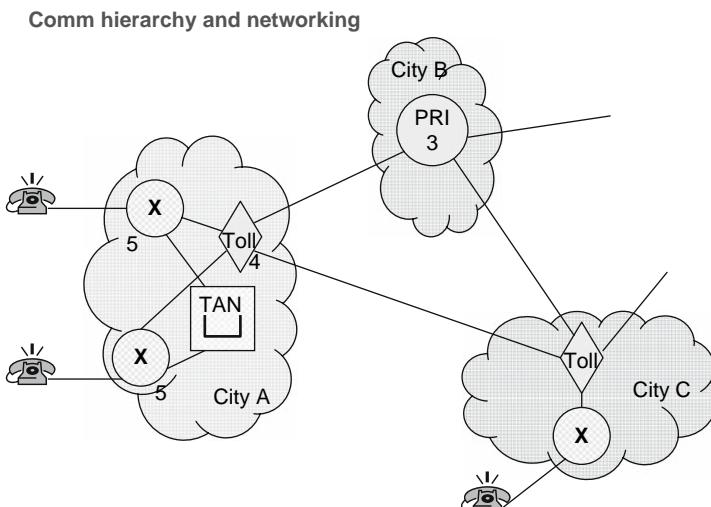


Fig. 1.4 Communications hierarchy and networking; traffic routing through different serving areas (cities)

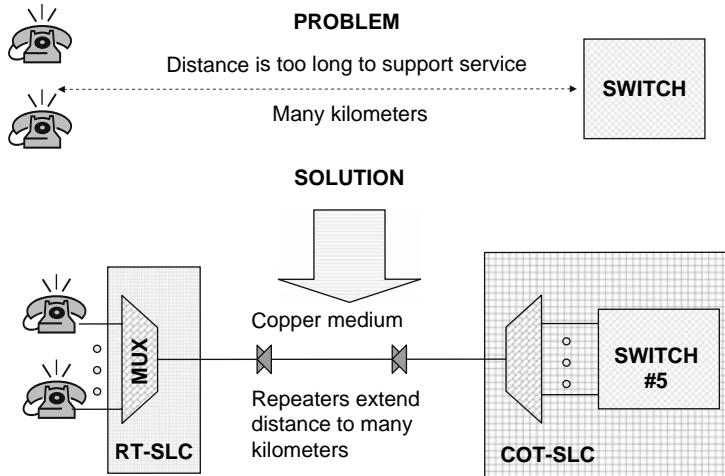


Fig. 1.5 Pair-gain systems also known as Subscriber Loop Carriers (SLC) have been very popular in the rural and suburbia United States, as well as in other countries

as a quick finder. Thus, the old paradigm has been one customer with one or two POTS, one entry in the list. However, imagine a small- or medium-size business with one dozen or more POTS. How convenient is this if all numbers are listed in the Yellow Pages? How easy is it to remember all these numbers? Would it not be better to remember one number only, and then dial an extension? This presented a business opportunity for a communications system that is now known as *public business exchange* (PBX). Thus, the PBX was not more than a low-cost small switching node that connected a small or medium business with the end office over a high-speed link (such as 1.544 Mbps).

For the traditional network to be able to establish connectivity quickly, it consisted of dynamic switching nodes and an operations, administration, and management (OA&M) network layer. These nodes quickly connect inputs with outputs so that a complete end-to-end path is established by running a protocol known as *signaling system 7* (SS7) [23]. The signaling system 7 is a protocol specifically developed to establish connections (or call setup) across the public switch transport network (PSTN) and also terminate (or teardown) connections. SS7 starts from the end office and ends at the remote end office. SS7 uses its own digital network, which consists of three main functional nodes, the *service switching point* (SSP), the *signal transfer point* (STP), and the *service control point* (SCP), Fig. 1.6.

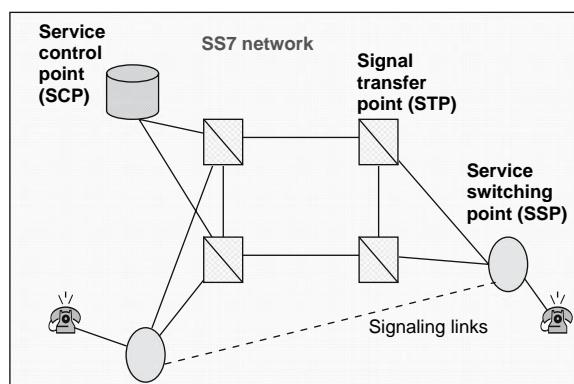


Fig. 1.6 The SS7 Network may be viewed as an network overlay to the communications network. SS7 paths are separate from user paths

- SSP nodes are the end or access offices in a network and they utilize common channel signaling (CCS); that is, a call processing protocol such as TR-303.
- STP nodes are points in the network where SS7 messages are received from a signaling link and are transferred to another link. STPs monitor messages and maintain connectivity (or routing) tables.
- SCPs are computers that maintain databases of the network; such databases are
 - local number portability (LNP)
 - calling name database (CNAM)
 - home locations register (HLR)
 - line information database (LIDB)
 - and more as SS7 has evolved to more advanced version to meet modern communication needs.

There are two STP types, national and gateway. National STPs transfer SS7 messages in the national network. Gateway STPs work with national and international protocols and transfer messages from one to the other. In all, SS7 optimizes the digital network operations, is backward compatible with existing switches and meets future requirements, and it provides a reliable mechanism for data transfer without loss or duplication. Based on this, when connectivity is requested in the PSTN network, all switching nodes that are on the end-to-end path are dynamically provisioned, provided that nodes and bandwidth are available; according to SS7 instructions, a permanent connection is established until one of the end devices hangs up or connectivity termination is requested.

Although trunks that interconnect switching nodes transport DS1 and DS3 signals, these signals are demultiplexed down to the DS0 level when they reach a dynamic switch of the PSTN network. That is, PSTN dynamic switches are DS0 (digital service level 0 or 64 Kbps) and they operate on the time slot level.

In this digital PSTN, another type of switch exists; this is not dynamically provisioned according to SS7 but provisioned according to instructions by craft personnel either over the Ethernet (nodes have an Ethernet connectivity for remote provisioning and testing) or in situ (nodes also have a craft interface terminal (CIT) for provisioning and testing on location). These “static” switches are known as digital cross-connect systems (DACS or DCCS) and provide semipermanent connectivity to enterprise customers and at a higher level than DS0 (such as DS1 and DS3).

Both dynamic and DACS switches pass digital information without delay and buffering. This is an important characteristic of the legacy PSTN (including the more modern optical version) as compared with the current data network.

1.3.2 Data Networks and Protocols

Computer generated data when transmitted through a network require different switching methods than the PSTN supports [24]. Such data is not continuously generated as digital data from voice, and therefore, the notion of DS0 is associated only with the 64 Kbps data rate. Initially, the PSTN network was used to carry data over pre-provisioned paths, such as the frame relay (FR). Another data type but over its own network has been the asynchronous transfer mode (ATM). Since the 1980s, Internet data has been transported over its own network that consists of routers instead of dynamic switches. Routers are computer-based switches that compute according to an algorithm the next best router to transport packetized digital information. However, until the next best router is found, data packets are stored in router memory. Thus, routers have been more inexpensive than dynamic switches of the PSTN network and as a result the Internet usability and services exploded. This in combination with the dramatic cost and price reduction of personal computers with built-in sophisticated wireless communication interfaces and fiber-optic networks that support humongous

transportable bandwidth opened a “never” enough appetite for bandwidth. Over the last two decades, the explosion of data transport created a data networking business and a successful data router industry. Based on specifically defined protocols packet transport any type of data, including digital voice and video from the data source to one or more destinations over the router-based data network.

As already described, routers store data first and then determine the best next router according to a router algorithm. Because of this, if we assume that there is a smart malicious program on it (that found its way in it hidden in one of the packets), then for as long as information data resides on the router, this program may access data, harvest information, and transmit it to an unauthorized destination. A different malicious program may also hide in the computer and execute itself according to a triggering mechanism such as a source address or destination address, a clock, and so on. Thus, the explosion of data networks and the rapid development and deployment of data protocols did not come for free; currently many security issues exist that are associated with software “viruses”, with “Trojan horses” and with many other malicious programs, in addition to a large class of irresponsible hackers who gain unauthorized access into computers, create havoc, and attempt illegal actions and also irresponsible data senders who broadcast all sort of unwanted e-mails, termed “spam”, and use unnecessarily network bandwidth. As a result, in just two decades of data networks existence, a whole new lexicon about such illegal and unauthorized actions has been created contrasted with traditional synchronous communication networks that for over a century had one term only, “eavesdropping”.

A data device generates large groups of bits or files, which are organized in packets to be transported to a destination. Each bit in a packet is represented with one of two symbols, a logical one (1) or a logical zero (0), which in practice correspond to two voltage levels (in electrical transmission), 0 and +V (unipolar), -V and +V (bipolar), or (in optical transmission) presence of light and lack of light.

When packets are generated, they are not generated in a continuous and synchronous manner because files are not generated so. For example, when a “send file” command is issued, a string of packets is formed and transmitted. After that, there are no packets until a next command to send is issued. Thus, contrary to synchronous telephony for which bits are continuously generated and transmitted in a periodic manner, packets are generated sporadically without a predetermined periodicity. To make things more complicated, the generated packets depend on the particular data protocol and they may have a fixed length (such as ATM) or a variable length (such as TCP/IP), Fig. 1.7, and also differently defined overhead bytes because each data protocol is defined to meet specific requirements according to the application they were designed for. Thus, all data networks are not equal and so, there are ATM networks, Internet (IP) networks, frame relay networks, video ok (networks), and the list goes on, as compared with the hierarchical PSTN network, which is one.

1.3.3 Narrowband, Broadband, and Ultraband Services

Transmission engineering is concerned with design issues that impact the timely transport of data at an acceptable quality. This includes a plethora of physical layer media (wireless, wired, and fiber-optic), a plethora of devices such as the transmitter and modulator, the receiver and demodulator, amplifiers (preamplifiers, post-amplifiers, and booster amplifiers), filters, compensators, equalizers, multiplexers/demultiplexers, clock and synchronization circuitry, connectors, and more. A particular subset of these defines the particular characteristics of a link and particularly the transmission data rate (number of bits per second), the link length, and the performance of the link (the number of bits that cannot be correctly recognized at the receiver thus counted as erroneous bit, or the number of

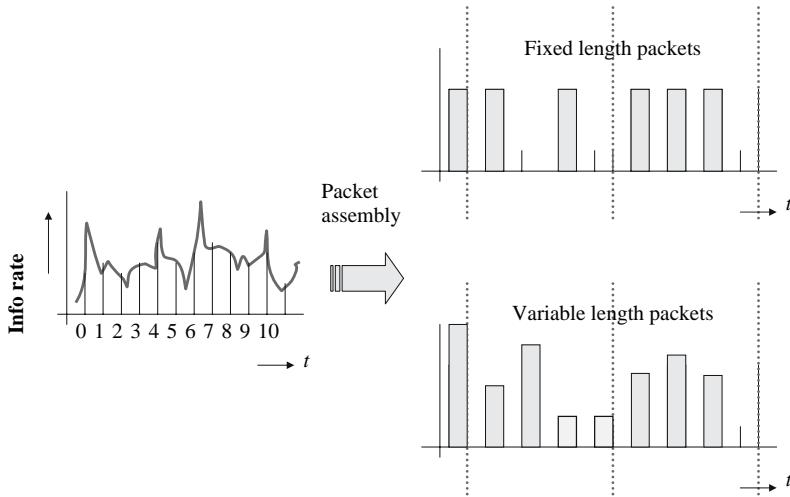


Fig. 1.7 The data protocol determines one of two packetizing scenarios, packets with fixed length and packets with variable length

packets that are not accepted due to excessive noise and jitter and other signal distortions (attenuation, power level, pulse shape, modulation depth, and more).

Accordingly, a link is classified as narrowband, broadband, and ultraband and so are the services that can be offered over such links.

- Narrowband services are those that traditionally are 64 Kbps or less. Such services are voice, low-speed text, and telemetry and are supported by wired and wireless media (millions of voice channels when multiplexed are supported by fiber-optic media).
- Broadband services are typically those that traditionally are at 1.544 or 2.048 Mbps. Such services include multiple voice channels, compressed video, image, and high-speed data, and they are supported by wired, wireless, and fiber-optic media.
- Ultraband services are relatively new and they include high-quality video, interactive real-time video, super-computation, and a mix of many services to support multiplay. The data rate is Gbps and it is typically supported by optical media.

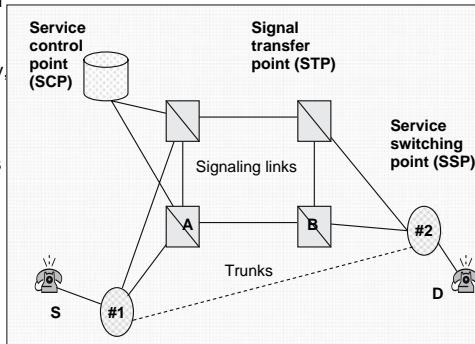
1.3.4 Circuit Switched Versus Store and Forward

The synchronous PSTN network as described in Sect. 1.3.1 dedicates a well-defined path from source to destination, and the flow of information over the defined path is known with precision. That is, the loop number is known (all loops are numbered), the trunk number is known (all trunks are numbered), the input and output port at each circuit switching node is exactly known, and the time slots in multiplexed higher digital services (DS1, DS3, and so on) are exactly known. Each path is allocated during the call process by a number of protocols (such as TR-303) that run at the access nodes and also by SS7 that runs over the SS7 network, Fig. 1.8, as already discussed. One could say that as soon as the path is determined, a “pipe” has been formed that connects source with destination in which information flows end to end.

In contrast to the well-defined path of the PSTN network, the data network does not define the path in detail. Packetized data enters a router node of the data network, packets are stored, and then the router executes an algorithm to define the best next router in the network; this is based

Call setup from S to D via A and B:

1. S dials the number of D.
2. SSP#1 sends to A an *initial address message* (IAM); this checks the database and sends it to #2 via B. IAM contains source and destination addresses.
3. SSP#2 checks D's loop and if not busy, then it sends to A via B an *address complete message* (ACM); ACM contains switch and trunk information.
4. SSP#1 connects S with D using trunks selected for the connectivity.
5. As soon as D picks up, #2 sends an *answer message* (ANM) to B that is addressed to #1. When ANM is received, #1 verifies that S and D are connected in both directions.
6. When S or D goes on-hook, a *release message* (REL) is sent to the corresponding STP addressed to the far end SSP. REL is acknowledged with a *release complete message* (RLC) to STPs.

**Fig. 1.8** Call setup using SS7

on source, destination, priority fields within the overhead of the packet and state of the data network. Thus, the “pipe” of the circuit switching network has no meaning here. Only in specific cases, the notion of “pipe” has meaning for which predefined routes are established for specific end users by provisioning routers on a predefined route. As a consequence, the store and forward network, in general, adds to the delay, and it cannot warranty real-time deliverability as the synchronous network can.

However, the amount of delay introduced by routers and data switches depends on the routing protocol and router technology. For example, the routing protocol may decide which the best next node is after taking into account the traffic and status parameters of all nodes in the network; this would introduce a significant delay due to intense processing. Another protocol may broadcast packets to all neighboring nodes regardless of traffic and status and these nodes to their neighboring, and so on, so that packets will reach their destination expediently; this method would use bandwidth and resources unnecessarily. Another method may precompute the best possible routes to many destinations so that as soon as a packet arrives it relays it to the proper next node according to look-up tables, and so on; this is the fastest method, which depends on robustness and traffic congestion of the on the network.

In conclusion, the synchronous switched network is known for its reliability, real-time deliverability, super-high bandwidth, and security, whereas the traditional data network is known for its low-cost payload deliverability and ease of scalability. Thus, it is plausible that the next generation network should combine the strengths of both and at the same time eliminate or minimize their weaknesses, so that in the next generation network, nodes are

- characterized by real-time payload deliverability
- meet the performance that is commensurate with type of service
- recognize different protocols
- meet the expected quality of service (QoS)
- they restore the signal quality at their outputs
- they are reliable
- they consume low power, and
- they are low cost with small footprint and volumetric capacity minimizing real-estate.

Similarly, the overall network

- meets the expected performance
- meets the expected availability
- transports high and elastic bandwidth
- it is protocol transparent
- it transports payload securely
- it is reliable
- it is fault tolerant, and
- it is cost-efficient.

1.3.5 Traffic and Service Evolution in Optical Networks

The 1980s witnessed the first optical data network and the first optical synchronous network, the Fiber Distributed Data Interface (FDDI) and the Synchronous Optical Network (SONET in the US) or Synchronous Digital Hierarchy (SDH in Europe), respectively. The first was a local area network (LAN) with a dual ring topology and the second a long-haul transport network that supported optical rings with optical add-drop multiplexing nodes topology as well as a point-to-point with optical add-drop multiplexing nodes. Since then, we have witnessed a rapid data network evolution with protagonists the Ethernet protocol and the Internet protocol, and to some extent the ATM, the Frame Relay and other protocols, each developed to meet different needs.

The interesting part in this is that although data networks are more cost-efficient, the optical network supports a humongous bandwidth, and thus even data over very long distances use optical network bandwidth; that is, despite the differences in cost structure, there is a symbiotic existence of both data and synchronous traffic: data needs the optical bandwidth, and optical bandwidth needs data to fill in the unused optical bandwidth. Thus, the next generation optical network, again, is a consequence of the traffic and services evolution.

1.3.6 Reliability of Optical Networks

The deployment of the optical synchronous network (SONET/SDH) has established an unprecedented network reliability, switching protection, availability, unavailability, and performance. A performance at 10^{-12} BER at data rates 2.5 Gbps for link lengths 50–80 km, a network unavailability which is in seconds per year, and a switching protection which is better than 50 ms. However, SONET/SDH was neither based on the WDM dense ITU-T channel grid [25, 26] nor supported data rates at 10 and 40 Gbps, at an aggregate data rate per fiber exceeding Tbps. Therefore, the established metrics should be surpassed or be met in the next generation optical network.

To accomplish this, strong or moderate error correction techniques (such as forward error correction or FEC) should be employed to compensate for performance degradation due to data rate increase, and the performance metrics (BER, SNR, Q-factor, signal power levels) of each channel needs to be monitored in service and in real time by sophisticated methods [27–32] and sophisticated reassignment strategies for channel protection and channel security need to be employed [33–38].

1.3.7 Security in Optical Networks

Security in communication networks is at various levels, user data, link and node, and the network (management and control), each having its own intrusion-resistance and vulnerabilities [39].

End-user data is most vulnerable as bad actors attempt to eavesdrop and harvest personal data. The protection of end-user data is typically the responsibility of the end user who employs encryption algorithms and secret keys to transmit a ciphertext. However, the secret key needs to be distributed to the rightful recipient(s) to decode the ciphertext. Although data ciphering is the responsibility of the end user and it is transparent to network providers, the integrity of the key distribution method is a transmission issue.

Security of the link pertains to security of transmission paths throughout the network. The user trusts the network and expects data and key transported through it to be safe from unauthorized intrusions. Therefore, links should have sensing mechanisms to detect possible intrusions and also employ countermeasures.

Network security is related with security of nodes when they are managed and provisioned; typically, a node is provisioned remotely over the Ethernet or Internet and thus it may fall victim to bad actors. Unauthorized access may alter the provisioning of a node to disable it, flood the network, harvest user information, deflect traffic to other destinations, or inject data and mimic a source. Harvested information may be calling numbers, traffic profiles, and so on. In data networks, harvested information may be credit card numbers, bank accounts, client records and files, connectivity maps, and more. Typically, network security and data delivery assurance is the responsibility of the network provider.

Among the three media currently used in telecommunications, wireless, wired (twisted pair and coax), and fiber optic, the latter has inherently better security features because of the specialized knowledge required to access the medium. Wireless is the most insecure since electromagnetic waves reach both friendly and foe receivers, and thus, its security relies on features built in the authentication protocol and key hardness. The copper medium is easily tapped, but because it requires some effort, its security features may be placed between the wireless and optical; however, eavesdropping is not unusual. Today attackers, hackers, and bad actors are well educated and therefore one cannot assure security by resting on the difficulty of tapping the fiber medium, on the difficulty of breaking the encryption code, or on the hardness of the authentication protocol, as eavesdroppers can harvest critical personal or national security information; they steal IDs, cause denial of service and in general generate havoc [40–43].

In Chap. 10, we examine encryption algorithms and network security in more detail.

References

1. C.E. Shannon, “A Mathematical Theory of Communication”, *Bell System Technical Journal*, 1948, pp. 379–423, 623–656.
2. ITU-T Recommendation G.711, “Pulse Code Modulation (PCM) of Voice Frequencies”, reprinted from the Blue Book, AT&T, Bell Laboratories.
3. ITU-T Recommendation G.704, “Synchronous Frame Structures used at 1544, 6312, 2048, 8488 and 44736 Kbps Hierarchical Levels”, 1995.
4. J.C. Bellamy, *Digital Telephony*, 3rd ed., Wiley, New York, 2000.
5. S.V. Kartalopoulos, “A Time Compression Multiplexing System for a Circuit Switched Digital Capability”, *IEEE Transactions on Communications*, vol. com-30, no.9, September 1982, pp. 2046–2052.
6. S.V. Kartalopoulos, “A Loop Access System for a Circuit Switched Digital Capability”, ISSLS 82, Toronto, Canada, September 20–24, 1982.
7. ITU-T Recommendation G.991.1, “High Bit Rate Digital Subscriber Line (HDSL) Transceivers”, October 1998.
8. ITU-T Recommendation G.991.2, “Single-Pair High-Speed Digital Subscriber Line (SHDSL) Transceivers”, February 2001 and Amendment 1 (11/2001).
9. ITU-T Recommendation G.993.1, “Very High-Speed Digital Subscriber Line Foundation”, November 2001.
10. ITU-T Recommendation G.995.1, “Overview of Digital Subscriber Line (DSL) Recommendations”, February 2001, and Amendment 1 (11/2001).
11. R.E. Matick, *Transmission Lines for Digital and Communication Networks*, IEEE Press, 1995.
12. S.V. Kartalopoulos, *DWDM: Networks, Devices and Technology*, Wiley/IEEE, 2002.
13. S.V. Kartalopoulos, *Introduction to DWDM Technology: Data in a Rainbow*, Wiley/IEEE, 2000.
14. ITU-T Recommendation G.702, “Digital Hierarchy Bit Rates”, 1988.

15. S.V. Kartalopoulos, “*Understanding SONET/SDH and ATM Networks*”, IEEE Press, 1999.
16. ANSI T1.102-1993, *Telecommunications—Digital Hierarchy—Electrical Interfaces*, 1993.
17. ANSI T1.107-1988, *Telecommunications—Digital Hierarchy—Formats Specifications*, 1988.
18. ANSI T1.105.01-1994, *Telecommunications—Synchronous Optical Network (SONET)—Automatic Protection Switching*, 1994.
19. ANSI T1.105.03-1994, *Telecommunications—Synchronous Optical Network (SONET)—Jitter at a Network Interfaces*, 1994.
20. ANSI T1.105.04-1994, *Telecommunications—Synchronous Optical Network (SONET)—Data Communication Channel Protocols and Architectures*, 1994.
21. ANSI T1.105.05-1994, *Telecommunications—Synchronous Optical Network (SONET)—Tandem Connection Maintenance*, 1994.
22. IETF RFC 2823, PPP over Simple Data Link (SDL) using SONET/SDH with ATM-like framing, May 2000.
23. T. Russell, *Signaling System #7*, 4th ed., McGraw Hill, New York, 2002.
24. N.F. Mir, *Computer and Communications Networks*, Prentice Hall, Englewood Cliffs, NJ, 2007.
25. ITU-T Recommendation G.694.1, “Spectral Grids for WDM Applications: DWDM Frequency Grid”, 5/2002.
26. ITU-T Recommendation G.694.2, “Spectral Grids for WDM Applications: CWDM Wavelength Grid”, 6/2002 Draft.
27. S.V. Kartalopoulos, “*Fault Detectability in DWDM: Toward Higher Signal Quality and System Reliability*”, IEEE Press, 2001.
28. S.V. Kartalopoulos, “Real-Time Estimation of BER & SNR in Optical Communications Channels”, *Proceedings of SPIE Noise in Communication Systems*, C.N. Georgiades and L.B. White, eds., vol. 5847, 2005, pp. 1–9. Also, invited paper at SPIE Fluctuation and Noise Symposium, May 24–26, 2005, Austin, TX.
29. S.V. Kartalopoulos, “Channel Error Estimation in Next Generation Optical Networks”, *WSEAS Transactions on Circuits and Systems*, vol. 3, No. 10, December 2004, pp. 2281–2284, ISSN 1109-2734, and ISBN 960-8457-06-8.
30. S.V. Kartalopoulos, “In-line Estimation of Optical BER & SNR”, SPIE Photon East, 10/23–26/05, Boston, MA, Track: “Optical Transmission Systems & Equipment for WDM Networks IV”, session 3, paper no. 6012-8, on CD-ROM: CDS194.
31. S.V. Kartalopoulos, “Circuit for Statistical Estimation of BER and SNR in Telecommunications”, *Proceedings of 2006 IEEE International Symposium on Circuits and Systems (ISCAS 2006)*, May 21–24, 2006, Island of Kos, Greece, paper #A4L-K.2, CD-ROM, ISBN: 0-7803-9390-2, Library of Congress: 80-646530.
32. S.V. Kartalopoulos, “Method and Circuit for Statistical Estimation of Bit Error Rate and Signal to Noise Ratio based on Pulse Sampling for Optical Communications”, US Patent No. 7,149,661, December 2006.
33. S.V. Kartalopoulos, “Channel Protection with Real-Time and In-Service Performance Monitoring for Next Generation Secure WDM Networks”, ICC 2007 Computer and Communications Network Security Symposium, June 24–28, 2007.
34. S.V. Kartalopoulos, “Optical Network Security: Sensing Eavesdropper Intervention”, Globecom 2006, San Francisco, on CD-ROM, NIS03-2, ISBN: 1-4244-0357-X, ISSN: 1930-529X.
35. S.V. Kartalopoulos, “Optical Network Security: Countermeasures in View of Attacks”, SPIE European Symposium on Optics & Photonics in Security & Defense, Stockholm, Sweden, September 11–16, 2006, paper no. 6402-9, on CD-ROM, volumes 6394-6402.
36. S.V. Kartalopoulos, “Optical Network Security: Channel Signature ID”, Unclassified Proceedings of Milcom 2006, October 23–25, 2006, Washington, DC, on CD-ROM, ISBN 1-4244-0618-8, Library of Congress 2006931712, paper no. US-T-G-403.
37. S.V. Kartalopoulos, “Distinguishing Between Network Intrusion and Component Degradations in Optical Systems and Networks”, *WSEAS Transactions on Communications*, vol. 4, No. 9, September 2005, pp. 1154–1161
38. S.V. Kartalopoulos, “Optical Network Security: Countermeasures in View of Channel Attacks”, Unclassified Proceedings of Milcom 2006, October 23–25, 2006, Washington, DC, on CD-ROM, ISBN 1-4244-0618-8, Library of Congress 2006931712, paper no. US-T-G-404.
39. S.V. Kartalopoulos, Di Jin, “Vulnerability Assessment and Security of Scalable and Bandwidth Elastic Next Generation PONs”, Proceedings 11th WSEAS, July 23–28, 2007, Aghios Nikolaos, Crete, Greece, *Advances in Communications*, vol. 3, pp. 33–39.
40. S.V. Kartalopoulos, “Is Optical Quantum Cryptography the ‘Holy Grail’ of Secure Communication?”, SPIE Newsroom Magazine, April 2006, available at <http://newsroom.spie.org/x2260.xml?highlight=x537>.
41. S.V. Kartalopoulos, “Quantum Cryptography for Secure Optical Networks”, ICC 2007 Computer and Communications Network Security Symposium, June 24–28, 2007, on CD-ROM, ISBN 1-4244-0353-7
42. S.V. Kartalopoulos, “Communications Security: Biometrics over Communications Networks”, Globecom 2006, San Francisco, on CD-ROM, NIS03-1, ISBN: 1-4244-0357-X, ISSN: 1930-529X.
43. S.V. Kartalopoulos, “Optical Channel Signature in Secure Optical Networks”, *WSEAS Transactions on Communications*, vol. 4, No. 7, July 2005, pp. 494–504.

Chapter 2

Digital Networks

2.1 Synchronous Optical Networks: SONET/SDH

2.1.1 Introduction

The development of solid-state lasers opened a new realm of possibilities with applications in manufacturing, consumer appliances, medicine, communications, and more. At the same time, optical fiber was developed (initially for medical endoscopes) that constrained light and guided it to travel for many kilometers and not in a straight path (with line of sight) within it. Put a modulated laser and an optical fiber together, and here is a transmission medium able to carry millions or trillions (or many more) of bits per second and over many kilometers. This capability, high data rate over very long distance, is impossible to be supported by any other technology and it was rightfully realized that optical technology offers to communications a tremendous potential to break the old telephony paradigm and support communication services that were and still are unimaginable.

In the 1980s, a new standardized protocol was introduced that defined the specifications of interfaces, architecture and features of a synchronous optical network, which in the United States was called SONET and in Europe and elsewhere synchronous digital hierarchy (SDH); SONET and SDH were defined with enough differences to have two different standards issued as SONET by Telcordia (previously Bellcore) and SDH by ITU [1–16]. Since its introduction, the SONET/SDH network performed beyond expectation; it was quickly adopted by most advanced countries, and it became the de facto standard of optical networks. The reasons for this success were many:

- (glass) fiber as the transmission medium:
 - exhibits high reliability (EMI, RFI, BER, etc.);
 - transports megabits and gigabits per second, which is expandable to terabits;
 - links without repeaters that are many times longer (than twisted copper);
 - uses thinner cable (than twisted copper)/per GHz; and
 - is easy to amplify, retime, and reshape.
- Standardized protocols allow for multi-vendor compatibility and interoperability.
- Technical personnel became well accustomed with the network and with maintenance procedures.
- Although a young technology, it is future proofed and is expected to increase cost-efficiency as it matures. For example, the initial SONET/SDH did not include the OC-768 (40 Gbps) rate, which does now, and currently 100 Gbps is in the evaluating phase.

The set of SONET standard interfaces is the *synchronous transport signal level-N* (STS-*N*), where *N* = 1, 3, 12, 48, 192, and 768. The STS-*N* rate on the optical medium is known as *optical*

Table 2.1 SONET and SDH rates

Signal designation			Line rate (Mbps)
SONET	SDH	Optical	
STS-1	STM-0	OC-1	51.84 (52 M)
STS-3	STM-1	OC-3	155.52 (155 M)
STS-12	STM-4	OC-12	622.08 (622 M)
STS-48	STM-16	OC-48	2,488.32 (2.5 G)
STS-192	STM-64	OC-192	9,953.28 (10 G)
STS-768	STM-256	OC-768	39,813.12 (40 G)

OC- N : optical carrier-level N STS- N : synchronous transport signal-level N STM- N : synchronous transport module-level N

carrier-N (OC- N), Table 2.1; STS- N where $N = 1, 3, 12, 48, 192$, and 768 indicates the bit rate of the electronic signal before the optical transmitter. The topology of the network is typically a protected ring with add-drop multiplexing (ADM) nodes or protected point-to-point with ADMs, Fig. 2.1; network nodes are known as *network elements* (NE).

Similarly, the SDH set of standard interfaces is the *synchronous transport module level-M* (STM- M) where $M = 0, 1, 4, 16, 64$, and 256.

Both SONET and SDH define all layers, from the physical to the application. The physical transmission medium of both SONET and SDH is single-mode fiber (SMF). That, is, the SONET and SDH have many similarities and fewer differences. Some examples are the following:

- SONET and SDH are technically consistent;
- SONET and SDH rates and frame format are the same;
- SDH photonic interface specifies more parameters than SONET; and
- SONET and SDH standards have enough minor differences (technical and terminology) to add enough complexity (and cost) in designing hardware and software.

Both SONET and SDH carry all synchronous broadband rates (DS- n , E- n), asynchronous data (ATM), and well-known protocols (Internet, Ethernet, Frame Relay) encapsulated in ATM first and then mapped in SONET/SDH.

For maintenance, operations, administration, and management, the SONET/SDH defines three network layers: path, line, and section, Fig. 2.2

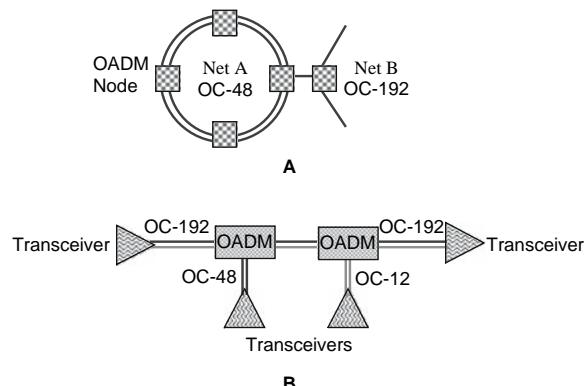


Fig. 2.1 Ring and point-to-point topologies supported by SONET/SDH

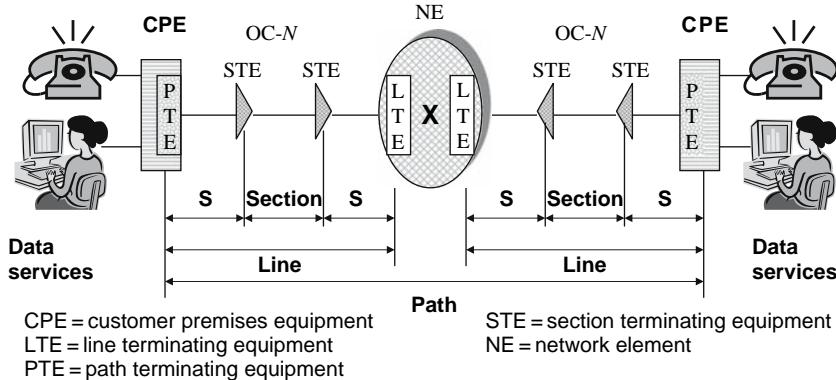


Fig. 2.2 Definition of path, line, and section in SONET/SDH Networks

The *path layer* addresses issues related to transport of “services”, such as DS3, between path terminating network elements (PTE); that is, end to end.

The *line layer* addresses issues related to the reliable transport of path layer payload and its overhead across the physical medium. It provides synchronization and multiplexing for the path layer network based on services provided by the section layer.

The *section layer* addresses issues related to the transport of STS-*N* frames across the physical medium, and it uses the services of the physical layer to form the physical transport. It constructs frames, scrambles payload, monitors errors, and much more.

2.1.2 SONET Frames

SONET/SDH (STS-*N*) frames come in specific sizes. However, regardless of size, a SONET/SDH frame is always transmitted in 125 μ s, and because of this, each STS-*N* signal has a specific bit rate (see Table 2.1).

The smallest frame, STS-1, consists of a matrix of octets or bytes organized in 9 rows and 90 columns. This matrix or 9×90 is partitioned in two distinctive parts: the transport overhead of the first 3 columns and the synchronous payload envelope (SPE) of the remaining 87 columns, Fig. 2.3.

An STS-*N* frame is transmitted row by row, starting with the first octet (row 1, column 1). When the last octet of the first row is transmitted, it continues with the second row (row 2, column 1) and so on until it reaches the very last octet in the frame (in STS-1, this is row 9, column 90).

The SPE of an STS-1 consists of 87 columns; one column for the path overhead, two columns (columns 30 and 59) do not contain customer data, hence called “fixed stuff”, and 84 columns for

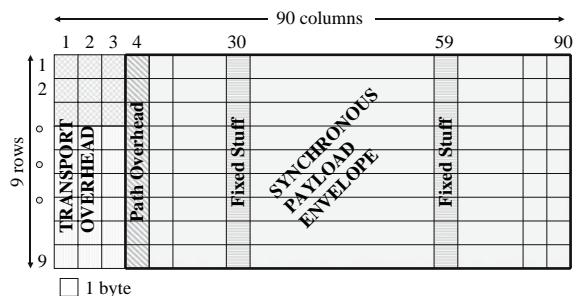


Fig. 2.3 Organization of the SONET STS-1 frame. A SONET frame is transmitted within 125 μ s

Trace	J1	User programmable. Sixty-four repeating bytes for receiving PTE to verify connectivity with transmitting PTE; default value = 0x00
BIP-8	B3	For error control . Calculated over all bits of previous SPE before scrambling
Signal label	C2	Indicates the construction of SPE . For example, asynchronous mapping, ATM, and so on
Path status	G1	Indicates to the originating PTE the status and performance of the terminating PTE
User channel	F2	Allocated for end-user communication purposes
Multi-frame	H4	An end-to-end generalized multi-frame indicator for payloads (a pointer)
User	Z3	Z3 for future ; no defined values
Growth	Z4	Z4 for future ; no defined values
TCM	Z5	Z5 for future ; no defined values

Fig. 2.4 Path overhead in SONET STS-1

customer data. That is, the upper bound efficiency of an STS-1 is 93.33 %. Nevertheless, the actual efficiency is much less (about 60 %) because there is plenty of wasted bandwidth, as it will become evident.

The *path overhead* in an STS-1 frame consists of nine octets, and it is sourced and terminated by the path terminating equipment only. Each octet in it has a specific meaning, Fig. 2.4, although the working of each octet requires several contiguous frames to convey a complete message.

The transport overhead consists of two parts: the section overhead and the line overhead.

The section overhead consists of row 1 to row 4 and column 1 to column 3, Fig. 2.5:

- A1 and A2 = framing pattern for each STS-1. Their hexadecimal value is 0xF628 {1111 0110 0010 1000}. A1, A2 are *not* scrambled.
- C1 = STS-1 ID. It is defined for each STS-1.
- B1 = error monitoring. It is calculated over all bytes of the previous frame *before scrambling* and placed in current frame *before scrambling*.
- E1 = a 64 Kbps voice communication channel; an STS-N that consists of N STS-1s; it is defined for the first (#1) STS-1 only.
- F1 = to be used by section user.
- D1 to D3 = a 192 Kbps communication channel between STEs for alarms, maintenance, control, monitoring, administration, and other needs; in STS-N, it is defined for #1 STS-1 only.

The line overhead consists of row 4 to row 9 and column 1 to column 3, Fig. 2.6.

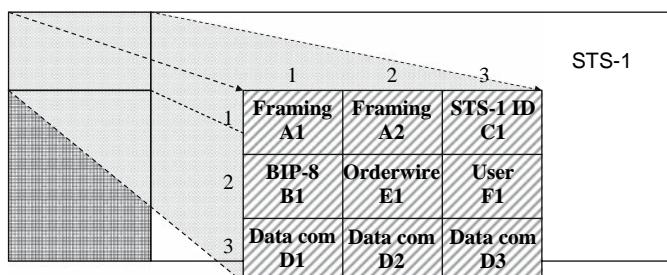


Fig. 2.5 Section overhead in STS-1

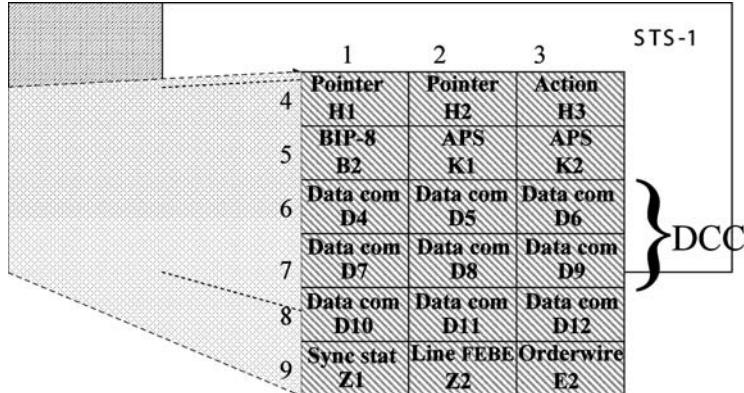


Fig. 2.6 Line overhead in STS-1

- H1, H2 = defines the offset between pointer and first SPE byte.
- H3 = it is called the action byte, and it is used for frequency justification in conjunction with the pointer bytes H1 and H2; if justification is negative, it carries valid payload; if positive or no justification, it is empty.
- BIP-8 = error monitor. It is calculated over a previous STS-1 frame before scrambling, and it is placed in B2 before scrambling of current frame.
- K1 and K2 = automatic protection switching (APS); in STS- N , it is defined for #1 STS-1 only.
- D4 to D12 = this constitutes a 576 Kbps communication channel between LTES for alarms, maintenance, control, monitoring, administration, and other communication needs; in STS- N , it is defined for #1 STS-1 only.
- Z1 and Z2 = not defined; in STS-N #3 STS-1, Z2 is defined as Line FEBE.
- E2 = this is an express 64 Kbps communications channel between LTES; in STS- N , it is defined for #1 STS-1 only.

Since the SONET/SDH frame generated in a network element (NE) may not be in complete synchronism (frequency and phase) with the incoming payload, there is an undetermined phase difference. To minimize latency, SONET/SDH follows the method of dynamic pointer that directly maps the incoming payload within the frame, the offset value (or phase difference from the sync) of which is measured and is incorporated in octets H1, H2, and H3 of the line overhead in every frame, Fig. 2.7.

Because the phase difference does not remain exactly the same over time, the H1 to H3 octets perform a dual function; they indicate the offset and they perform frequency justifications (i.e., corrections of frequency or offset variation). At start-up, the offset is calculated, and if the calculated offset remains the same for three consecutive frames, a “no justification” is indicated. If the frequency slightly varies, then justification is performed, positive or negative; positive when the incoming rate is a little lower than the node clock and negative when the incoming rate is a little higher.

2.1.3 Virtual Tributaries and Tributary Units

Although in synchronous communications DS- ns (and E- ns) are tributaries that carry customer payload, SONET defines virtual tributaries (VT) and SDH defines tributary units (TU) to carry DS- ns or E- ns . The capacity of a VT depends on the number of octets in it, and because the number of rows is always nine, it depends on the number of columns. Thus, if the number of columns is 3, it

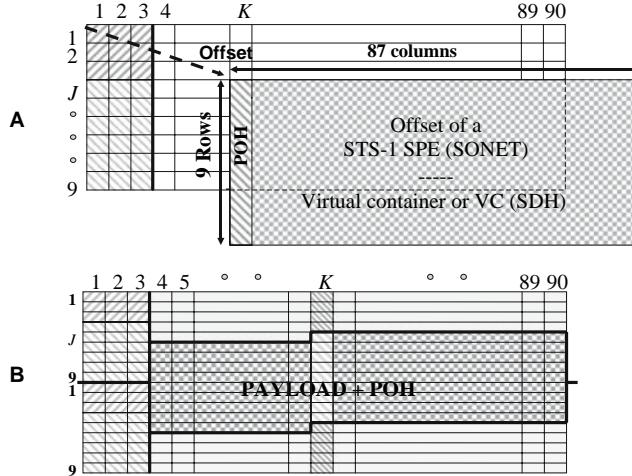


Fig. 2.7 Floating SPE with respect to the STS-1 frame (A). Floating SPE mapped on two consecutive STS-1s (B)

is known as VT1.5, if 4 it is known as VT2, if 6 it is known as VT3, and if 12 it is known as VT6, Fig. 2.8. Each VT contains a client signal not necessarily of the same type and therefore a VT has its own overhead known as VT path layer overhead.

VTs are byte multiplexed to form a group of 12 columns, Fig. 2.9. However, a simple rule applies when forming a group: A group can contain only the same type of VTs. That is, four VT1.5s, or three VT2s, or two VT6s, and so on. Mixing one VT3 and two VT1.5s is *not* allowed in traditional SONET/SDH. Figure 2.10 illustrates the logical multiplexing/demultiplexing hierarchy from/to synchronous TDM to SONET.

Thus, in a SONET STS-1 SPE, only seven groups fit, which are also byte (or column) multiplexed, with the added path overhead and the two fixed stuff columns. Because a SONET frame is transmitted within 125 μ s, so is each octet in a frame, each VT and each group in a frame. Thus, the transportable bandwidth by each VT type is incremental but coarse, Table 2.2.

SDH defines a similar organization and column multiplexing like SONET, Fig. 2.11. However, in SDH, VTs are called tributary units (TU), groups are called tributary unit groups level 2 (TUG-2), and seven TUG-2s are multiplexed in a TUG level 3 (TUG-3), which with the addition of two columns of fixed stuff at the first two columns of the TUG-3 form the SPE. Here, the same rule also applies: a TUG-2 must contain the same type of TUs.

Based on the aforementioned, SONET/SDH does not have the fine granularity to support modern data payloads and thus the bandwidth efficiency of VT or TU structure and groups is low. In particular, the bandwidth capacity of VTs is low for data protocols with thousands of octets in their packets.

VT1.5	VT2	VT3	VT6
1 2 3 4	1 2 3 4 5	1 2 3 4 5 6 7	1 2 3 4 5 6 7 8 9 10 11 12 13
27 bytes 125 μ s 3 cls	36 bytes 125 μ s 4 columns	54 bytes 125 μ s 6 columns	108 bytes 125 μ s 12 columns
9 rows			

Fig. 2.8 Capacity of SONET VTs is determined by the number of columns, 3, 4, 6, and 12

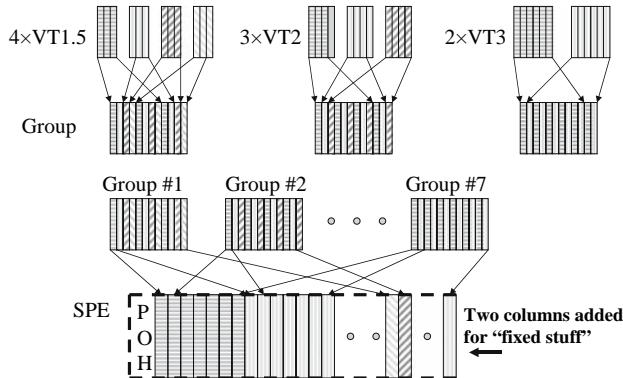


Fig. 2.9 A group is constructed by byte multiplexing VTs of the same type

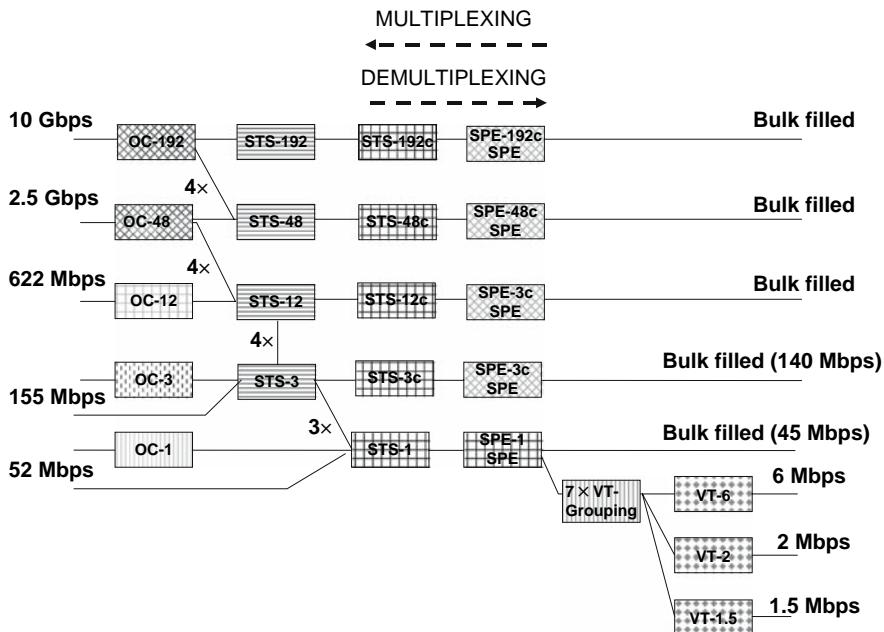


Fig. 2.10 Hierarchical multiplexing/demultiplexing in SONET

Table 2.2 Organization and transportable bandwidth by each VT type

VT Type	Columns/VT	Bytes/VT	VTs/Group	VTs/SPE	VT Payload rate (Mbps)
VT1.5	3	27	4	28	1.728
VT2	4	36	3	21	2.304
VT3	6	54	2	14	3.456
VT6	12	108	1	7	6.912

The latter case was addressed using another protocol, the asynchronous transport mode (ATM), a segmentation or fragmentation method, and a standard that defined how ATM cells are mapped over SONET/SDH. However, as data services and new protocols evolved, more containers and a different mix were needed to support larger variety of payloads, finer granularity, a provisionable mix-and-match payload type, and a variety of quality of services to meet customer requirements. Thus, the

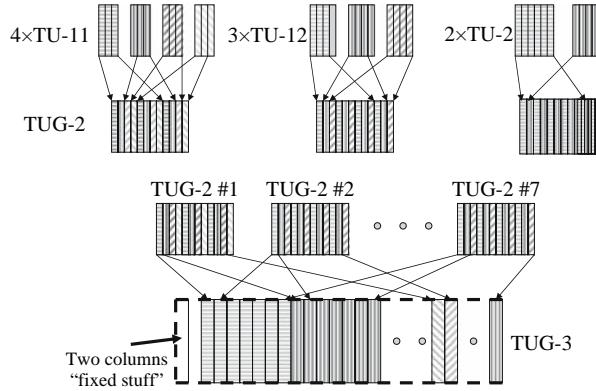


Fig. 2.11 A tributary unit group-2 is constructed by column multiplexing of TUs Within a TUG-2, there is the same TU type. Seven TUG-2 are column multiplexed to form a TUG-3, with the addition of two fixed stuff columns

next-generation intelligent optical network is an inevitable evolution of a proven transporting vehicle but reengineered to support a larger variety of data protocols and new services and requirements with cost-efficiency.

2.1.4 STS-N Frames

SONET and SDH define higher capacity frames. For example, an STS- N has N times the amount of columns of an STS-1 (both overhead and payload) but always nine rows. For example, an STS-3 frame has a total of 270 columns, nine overhead columns, three path overhead and six fix stuff columns. However, if three STS-1s are multiplexed to produce an STS-3, then three overhead pointers must be processed, since each constituent STS-1 may arrive from a different source with different SPE offset, Fig. 2.12.

2.1.4.1 Concatenation

When SONET/SDH was drafted, a need emerged to accommodate super large packet payloads that did not fit in a single STS-1 frame. This was addressed by distributing the large packet over N STS-1s and then multiplexed them in a single STS- N , which is denoted as STS- Nc to indicate ‘concatenation’. Because the STS- Nc payload has the same origin and destination for all STS-1s in it and all STS-1s have the same frequency and phase relationship among them, there are many redundancies. Thus, only one pointer processor is needed, a simplified overhead suffices, one path

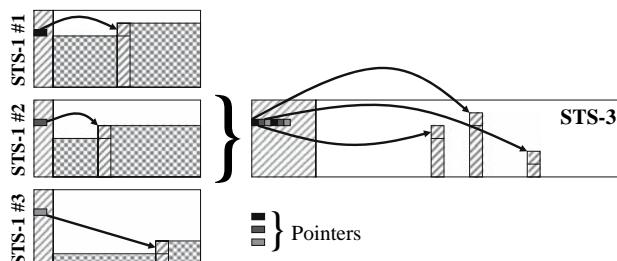


Fig. 2.12 When three STS-1s construct a STS-3, three different pointers are processed, one for each STS-1

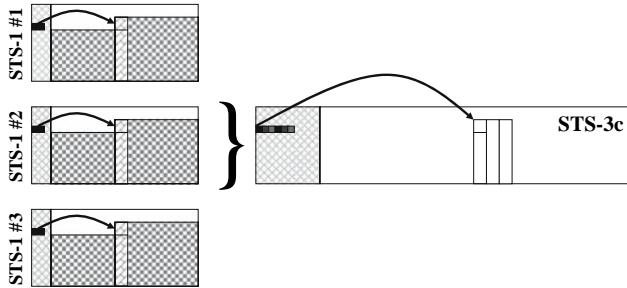


Fig. 2.13 In the STS- Nc case, only a pointer is needed for all STS-1s in it and only one path overhead. Here, the STS-3c case is shown

overhead is needed, and there are fewer fixed stuff columns (the number of columns is calculated by $N/3 - 1$). Moreover, each node or network element treats an STS- Nc as a single entity, and it distinguishes an STS- Nc from a regular STS- N from specific codes written in the unused pointer bytes. Figures 2.13 and 2.14 illustrate the frame and overhead of STS-3c. Notice that an STS-3c has no fixed stuff columns (since $N/3 - 1 = 0$).

2.1.4.2 Scrambling

SONET/SDH defines a scrambling process so that no long strings of zeroes or ones are present. The scrambler is defined by the generating polynomial: $1 + x^6 + x^7$ which generates a random code 127-bits long. The scrambler is set to 11111111 on the MSB of the byte following the # N th STS-1 C1 byte (of a STS- N). Thus, in STS-1, the scrambler starts with the first byte after A1, A2, and C1, and it runs continuously throughout the complete STS- N frame; A1, A2, and C1 are not scrambled because they are used to identify the start of frame.

2.1.5 Maintenance

The SONET and SDH recommendations define all maintenance aspects, criteria, requirements, and procedures to maintain the network element and network operation at an acceptable performance. Requirements include alarm surveillance, performance monitoring (PM), testing, and control features to perform the following tasks:

		A1	A1	A1	A2	A2	A2	J0	Z0	Z0
		B1	X	X	E1	X	X	F1	X	X
		D1	X	X	D2	X	X	D3	X	X
		H1	H1*	H1*	H2	H2*	H3	H3	H3	H3
		B2	B2	B2	K1	X	X	K2	X	X
		D4	X	X	D5	X	X	D6	X	X
		D7	X	X	D8	X	X	D9	X	X
		D10	X	X	D11	X	X	D12	X	X
		S1	Z1	Z1	Z2	Z2	M1	E2	X	X

↑
Section OH
↓
Line OH

Concatenation Indicators:
 H1* = **1001XX11**
 H2* = **11111111**

[X] Undefined OH Bytes (all zeroes)

Fig. 2.14 Not all overhead bytes are used in the STS- Nc . Here, the STS-3c case is shown

Table 2.3 Alarms and impairments at three levels

	Line AIS	STS Path AIS	VT Path AIS
Loss of signal	X	X	X
Loss of frame	X	X	X
Loss of pointer		X*	X*

* No RDI is generated

- trouble monitoring and detection
- trouble or repair verification
- trouble sectionalization
- trouble isolation
- testing, and
- restoration.

The network element alarm surveillance takes place at the termination, such as section (at the STE), line (at the LTE), STS path (at the STS PTE), and VT path (at the VT PTE). A VT PTE contains all the functionality of a STE, LTE, and STS PTE. This is accomplished by monitoring and processing specific overhead bytes in the frame. When a node detects an impairment that occurred in a line, path, or a particular VT path, a corresponding alarm indication signal (AIS) is issued. Thus, AIS can be on any of the three levels, AIS-L for line, AIS-P for path, AIS-V for VT path (see line section and path overhead bytes). AIS is issued when one of the following occurs: loss of signal (LOS), loss of frame (LOF), or loss of pointer (LOP), Table 2.3.

SONET performance monitoring (PM) is based on counting code violations in a second, whereas SDH PM is based on counting errored blocks in a second. In the next generation optical networks, the unit of time “second” is very long and it may be used for metric and comparison purposes since a rate at 10 Gbps or 10,000,000,000 bits per second yields so many bits that are beyond any packet technology; the point is that performance in the next-generation optical network must be monitored much faster than what the original SONET/SDH has defined.

Finally, SONET and SDH have the capability to test the signal at different levels by looping back a complete STS- N or individual VTs.

2.2 Asynchronous Data/Packet Networks

2.2.1 Introduction

Although SONET and SDH transport synchronous and asynchronous payloads with excellent QoS and path protection, with acceptable efficiency and bandwidth elasticity for service diversity, they cannot compete with local area data networks (LAN) that have been specifically designed to provide an inexpensive best-effort transport mechanism of asynchronous and bursty data. As a consequence, packet networks route bursty data and therefore it is doubtful that they can meet the real-time requirements of voice and real-time (interactive) video, without substantial signal delays, unless excess network bandwidth capacity and sophisticated protocols are used.

Typically, there are two types of packet networks; those that form a short fixed-length packet and those that form a variable length packet; packet lengths may vary from 40 to many thousands octets.

Among the most popular data networks to date are the Ethernet and the Internet, although the fiber distributed data interface (FDDI) had been the precursor of optical data networks, the asynchronous transport mode (ATM) is still in use but its popularity is not growing, and other data protocols such as the fiber connectivity (FICON) are for specific data applications.

2.2.2 Synchronization and Timing

Modern networks transmit at bit rates that exceed gigabit per second and therefore receiver synchronization and timing must meet tight performance specifications. Timing affects the bit error rate (BER) signal performance and thus timing circuits must maintain an accuracy, which is specified in parts per million (ppm) pulses, and remain within specified jitter and wander tolerance limits. For example, GR-253-CORE specification, jitter is defined as the “short-term variation” of a signal’s significant instants from their ideal position in time. “Short-term variation” implies some frequency oscillation greater than or equal to a frequency demarcation; in North American hierarchy (DS1-DS3) the demarcation between jitter and wander is 10 Hz. The jitter network element (NE) criteria per interface category are specified as [17, 18]:

- *Jitter transfer*: this is defined as the jitter transfer characteristics of a network element (or node);
- *Jitter tolerance*: this is defined as the point-to-point amplitude of sinusoidal jitter applied on the OC-N (SONET/SDH) input signal that causes a 1 dB power penalty;
- *Jitter generation*: it defines the limits of jitter generated by an NE without jitter or wander at its inputs. In communications systems, payload mapping, bit stuffing, and pointer justifications or adjustments are sources of jitter.

The overall path consists of several nodes, each having its own timing circuitry and accuracy deviation; and because the overall inaccuracy is cumulative, timing accuracy is very important. Therefore, standards have been issued recommendations describing clock accuracy, timing characteristics, and measuring methods [19–21].

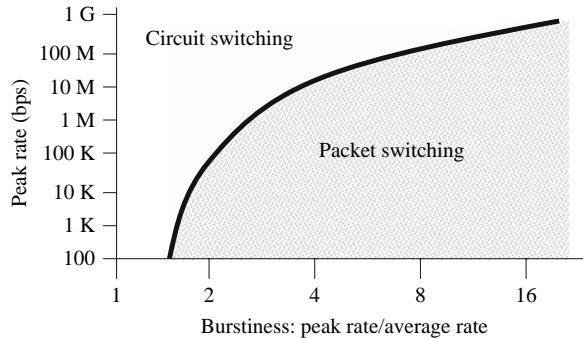
2.2.3 Data Traffic

Data is not generated in a continuous and constant flow, but it fluctuates between a peak rate and a minimum rate establishing an average rate. As packets are formed, one can easily envision two different scenarios. Packets with fixed length (such as ATM) are created at irregular time and packets with variable length may be generated in a more periodic manner, although this can not be warranted. Thus, in addition to packet rate, two more definitions are needed, the distribution of inter-packet interval (or the distribution of time interval between packets with a statistical profile such as Gaussian and Poisson), and also the distribution of packet length over time.

The ratio peak rate to average rate defines the packet burstiness. Clearly, as the difference between maximum and average decreases, the more uniform the packet flow, and as the difference increases, the more bursty. Thus, depending on type of traffic, a curve can be drawn (peak vs. burstiness) that defines a boundary separating the application space in two areas, one which is better suited for synchronous applications and one for asynchronous, Fig. 2.15.

At the transmitting end terminal, a number of client data bytes (or octets) are assembled into a payload block, overhead bytes are attached to it and data and overhead form a packet, the length of which is measured in octets or bytes. At the receiving end terminal, several packets are collected, placed in the correct sequence and they are stripped off their overhead to reconstruct the original data flow. The process at both ends collectively is known as *segmentation and reassembly* (SAR). In addition to delay introduced during packet assembly and disassembly, delays are experienced during buffering and packet switching. Clearly, the more the switching elements on the path the higher the overall latency is. Buffering and delays impact network congestion. In data networks, if the total packet rate exceeds the network capacity, then packets with the lowest priority are the first candidates to be “dropped or stripped” and are not delivered. As a consequence of this, packet flow control is important for congestion avoidance. Different protocols have adopted one of the several

Fig. 2.15 Separating the circuit and packet application space based on peak rate and burstiness



flow control mechanisms, among them are the stop-and-wait, the sliding-window flow control, the leaky bucket, and the double leaky bucket.

- The *stop-and-wait flow control* is a simple link buffer-overflow controlling mechanism. According to this, when the transmitter transmits a packet or frame, it waits for an acknowledgment. If the acknowledgment is not received within a predefined period, the transmitter resends the frame. It is obvious that this mechanism is not very efficient because of the delay involved—(best delay case): the delay: send packet, wait, acknowledgment received; (worst delay case): send packet, wait, resend, acknowledgment received.
- The *sliding-window flow control* transmits a sequential group of packets or frames, all of the same length. The number of frames, say k , in the group fits within a period or a *sliding window* of time. Each frame in the group is sequentially numbered from 1 to k . The number of frames k in the group is known to both transmitter and receiver. In this case, the receiver sends a consolidated acknowledgment back to the transmitter for all packets in a group that were received successfully.

In data networks, the asymmetry of packet flow is also an important parameter. In most data applications, the packet rate in one direction is not the same with that in the other direction; typically, the upstream direction rate is lower than the downstream as is the case in Internet traffic or large data transfers. However, the traffic flow asymmetry also fluctuates. The fluctuation depends on several factors such as the type of service provided, time of the day, day of the year, geographical distribution of subscribers, protocol used, and also to scheduled and unscheduled events; the latter may also cause unpredictable network congestion.

2.2.4 Packet Networks

Packet networks offer integrated multiple service levels at a multiple quality of service, which has been agreed upon between the service provider and the client with a service level agreement (SLA). Packet networks, such as the Internet, are not circuit switched based but they store and forward data to perform packet switching and thus they perform bandwidth management, buffering (queuing), scheduling, routing and dynamic rerouting, policing, and traffic shaping based on buffers at the input or the output or both. Table 2.4 compares features between synchronous services and asynchronous data services.

Bandwidth management consists of functions such as call admission control (CAC), class of service routing, and signaling.

- CAC is performed according to service level.
- Routing is based on algorithms and protocols. In some cases, it requires knowledge of the complete network topology in terms of available bandwidth per service level, and in some others knowledge of the neighboring nodes only. The objective is to estimate the shortest and the

Table 2.4 Comparing TDM and data traffic, a new network with TDM-like and Data-like features is needed, as the trend column indicates

Features	Legacy TDM	Legacy Data (IP)	Trend
Qos	✓	NA	▲
Guaranteed delivery	✓	NA	▲
Real time	✓	NA	▲
Error free (BER)	High	NA	▲
Easy and fast access	✓	Moderate	▲
Architecture	Many/hierarchical	Several/dedicated	TDM-like
Circuitry	Dedicated	Processor based	TDM-simplified
Reconfigurability	Difficult	Easy	Easier
Net protection	✓	Unprotected	TDM-like
Service reliability	✓	Unreliable	TDM-like
Net management	✓	Difficult to manage	TDM-like
Net provisioning	Remote and fast	Mostly manual	TDM-simplified
Net security	Under control	No control	▲
BW aggregation/fiber	Ultrahigh	Moderate-low	▲
Cost per kB-s	High	Low	Low
Revenues	High	Low	▲
BW demand	Slow increase	Fast increase	▲
New services	Slow introduction	Fast introduction	▲

NA: not applicable; ▲: upwards trend

optimum route for which it forms a routing database. Routing also executes scheduling algorithms and simple or complex queuing algorithms per service level agreement (SLA). Dynamic rerouting may also be performed during service.

Policing provides a provisioned mechanism at the entry point that is at an edge node of the data network, in order to verify compliance with traffic parameters that comply with the terms of the subscriber SLA and also to control them.

Traffic shaping is a buffered function that smoothes the packet traffic exiting the node in order to ensure compliance with the agreed SLA and network traffic to avoid congestion situations.

Multiple service levels are supported with parallel *overlay networks*, or with native multiservice technologies such as Asynchronous transfer mode (ATM). The overlay is a purpose-built network to support multiservice.

The supported *classes of service* (CoS) by this network are generally four—guaranteed, predictable, shared, and best effort:

- *Guaranteed*: synchronous, negligible jitter, bounded latency, and low packet loss (such as TDM);
- *Predictable*: isochronous, minimal oversubscribing (or overbooked), bounded jitter, and bounded latency (such as ATM);
- *Shared*: moderate oversubscribing, bandwidth aware, low jitter, some latency (such as frame relay—FR); and
- *Best effort*: highly oversubscribed, high jitter, moderate latency (such as IP).

Multiservices arise from multiple protocol label switching (MPLS) and the differentiated services model (Diffserv).

- *MPLS* is a protocol encapsulation technique, which in addition includes bandwidth aware routing extensions and path signaling specifications. MPLS enables packet networks to apply ATM traffic engineering principles [22–25].

- *Diffserv* provides a model for multiple service levels, utilizing enhanced IP and MPLS protocols to deliver multiservices over an IP backbone network. Based on this model, packets can be classified and dynamically aggregated into provisioned service levels (each with different QoS).

Typically, these service levels are instantiated over separate data networks that are on a different technology platform (TDM, FR, ATM, Ethernet, and IP) which is serviced and maintained by a different service provider, and thus each may be provisioned differently. Thus, guaranteeing a “guaranteed service” over a path that crosses different service providers needs further investigation.

2.3 Review of Data Networks

Standardized data networks come in different types, each depends on protocol, medium, and topology they support. Local area networks (LAN) are standardized (IEEE 802.3 series) nonhierarchical, asynchronous and low-cost multiple access. Switching is accomplished by store and forward and not necessarily in real time. Some LANs have limited geographical coverage, whereas others, such as the asynchronous transfer mode (ATM), have an extended one.

2.3.1 Asynchronous Transfer Mode

Asynchronous transfer mode (ATM) is a data protocol designed to provide quality of service (QoS), service type flexibility, semantic transparency, maintenance, and reliability.

The ATM frame (called *cell*) has a fixed short length of 53 octets, Fig. 2.16; 5 octets for header and 48 octets for data.

The definition of the ATM cell header at the user to network interface (UNI) differs from that at the network to network interface (NNI), Fig. 2.17.

The 4-bit GFC field is defined at the UNI only (at the network access) to assist the control of cell flow, but *not* for traffic flow control. GFG is not carried passed the UNI throughout the network; that is, at the NNI, the GFC field is not defined.

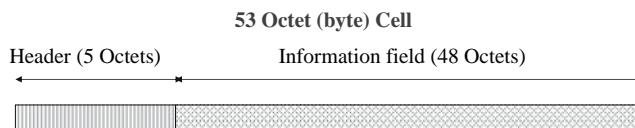


Fig. 2.16 The ATM frame consists of a 5-octet header and 48-octet information field

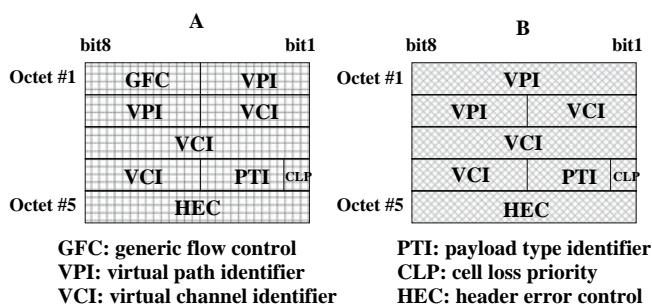


Fig. 2.17 ATM header defined at UNI (A) and at NNI (B)

The VPI/VCI field consists of 24 bits. They are labels identifying a particular virtual path (VP) and virtual channel (VC) on a link. The switching node uses this information and with routing information (tables) that has been established at connection setup, it routes cells to the appropriate output ports. The switching node changes the input value of the VPI/VCI fields to new output values.

The PTI field consists of 3 bits. It identifies the payload type, and it indicates congestion state. The meaning of each PTI code is as follows:

- 000: User data cell; congestion not experienced, SDU = 0
- 001: User data cell; congestion not experienced, SDU = 1
- 010: User data cell; congestion experienced, SDU = 0
- 011: User data cell; congestion experienced, SDU = 1
- 100: OAM F5 segment associated cell
- 101: OAM F5 end-to-end associated cell
- 110: Resource management cell
- 111: Reserved for future

where SDU is a service data unit.

The CLP field consists of 1 bit; 0 = high priority and 1 = low priority. It is set by the user or service provider. Under congestion, the CLP status determines whether cells will be dropped or pass.

The HEC field is used for error detection/correction. This code detects and corrects a single error in the header field or it detects multi-errors. It is based on the $x^8 + x^2 + x + 1$ CRC code.

The HEC is also used for cell delineation. The remainder of the polynomial is EX-ORed with the fixed pattern “01010101”, and this is placed in the HEC field. At the receiving end, the generating polynomial results in a HEC pattern “01010101” which is used to locate the start of the cell.

Some ATM cells carry client data and some are defined for other usages. A list of such cells is

Idle cell:	They are inserted/extracted by the physical layer in order to adapt the cell rate to the available rate of the transmission system;
Valid cell:	It is a cell with no header errors, or with a corrected error;
Invalid cell:	It is a cell with a non-correctable header error;
Assigned cell:	It is a valid cell that provides a service to an application using the ATM-layer service;
Unassigned cell:	This is not an assigned cell;
Metasignaling cell:	It is used for establishing/releasing a VCC. VCs in permanent virtual connections need no meta-signaling.

Client data may consist of long packets (much longer than 53 bytes) or a continuous bit stream. To transport client data over ATM, data is segmented up to 47 or 48 octets, overhead is added and a string of ATM cells is formed. This function is known as *segmentation and reassembly* (SAR), Fig. 2.18.

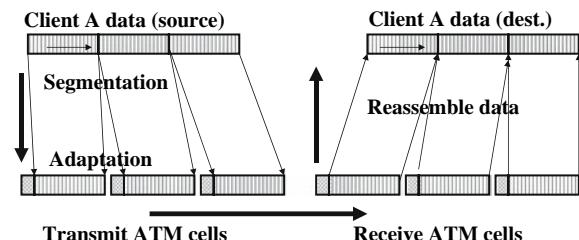


Fig. 2.18 Principles of segmentation, adaptation, and reassembly

Table 2.5 ATM adaptation Layers

	Class A	Class B	Class C	Class D
AAL type	1	2	5, 3/4	5, 3/4
Timing relation between source and destination	Required		Not required	
Bit rate	Constant		Variable	
Connection mode	Connection oriented			Connection-less
Examples:	CBR voice/ video	VBR video/ audio	CBR voice/ video	TCP/IP SMDS PPP

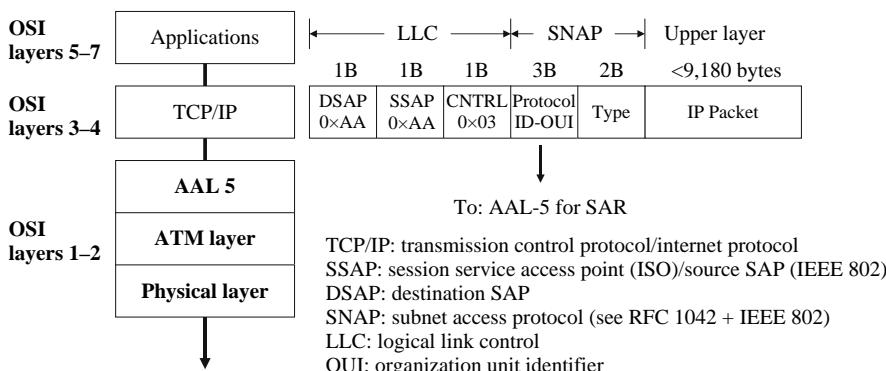
ATM technology defines five adaptation layers (AAL), each suited for different payload type and services such as voice, video, TCP/IP, Ethernet, and so on, Table 2.5. AAL-5 is straightforward and more efficient for point-to-point ATM links. AAL-5 cells are transmitted sequentially and thus there is no mis-sequencing protection, whereas error control is included in the last ATM cell (SAR_PDU). As an example, Fig. 2.19 illustrates the process for TCP/IP packets over ATM and the corresponding OSI layers.

ATM defines extensive traffic parameter requirements and quality of service features. *Quality of service* (QoS) of a connection relates to *cell loss*, *cell delay*, and *cell delay variation* (CDV) for that connection in the ATM network. CDV is a performance metrics pertaining to path speed and is defined as the variability of cell arrival for a given connection.

Traffic shaping (TS) is defined as the function that alters the flow (or rate) of cells in a connection, to comply with the agreed QoS requirements (rate reduction, cell discarding).

The ATM service level agreement (SLA) includes parameters some of which are the following:

- *Peak cell rate* (PCR) is defined as the permitted burst profile of traffic associated at each UNI connection. This is the maximum cell rate in a time interval. In addition, there is
- *Sustainable cell rate* (SCR) is defined as the permitted upper bound on the average rate at each UNI connection.
- *Burst tolerance* (BT) defines the tolerance on additional traffic above the SCR. When this tolerance is exceeded, the ATM traffic is tagged as excessive traffic and it may be lost.
- *Maximum burst size* (MBS) defines the length of bursty cells in a period.

**Fig. 2.19** Process for TCP/IP packets for ATM transport using AAL-5

Semantic transparency determines the capability of a network to transport information from source to destination with an acceptable number of errors and performance metrics. Errors are defined on the bit level as well as on the packet level.

- The bit error rate (BER) is defined as the ratio of erroneous bits over the total number of bits transmitted within a time interval.
- The packet error rate (PER) is defined as the ratio of erroneous packets or cells found over the total number of packets or cells transmitted in a time interval.

In addition, there are errors pertaining to the accuracy of a system such as the following:

- The mis-insertion packet or cell rate (CMR) is defined as the ration of cells or packets mis-inserted over a time interval.

Errors pertaining to the accuracy of the path such as the following:

- The packet or cell loss rate (CLR) is defined as the number of lost cells over the total number of packets or cells sent.

There are performance metrics pertaining to the system speed such as the following:

- The packet or cell transfer delay (CTD) is defined as elapsed time between an exit and an entry measuring point for a cell.

ATM defines a variety of services. In the service level agreement of ATM, the defined services are the following:

- Constant bit rate (CBR) when ATM bits or cells arrive at a negotiated constant cell rate. It requires low cell loss rate ($<10E-9$) and stringent cell delay variation.
- Variable bit rate (VBR) when ATM bits or cells arrive at a negotiated variable cell rate characterized by a minimum and maximum rate and burstiness. This category is subdivided in
 - Real time variable bit rate (rt-VBR) when ATM bits or cells arrive at a negotiated variable rate characterized by a minimum and maximum rate and burstiness. It requires low cell loss rate ($<10E-9$) and stringent cell delay variation.
 - Non-real time variable bit rate (nrt-VBR) when ATM bits or cells arrive at a negotiated variable rate characterized by a minimum and maximum rate and burstiness. It requires low cell loss rate but has no requirements for cell delay variation.
- Available bit rate (ABR) when ATM cells arrive at a cell rate, determined by the network, based on congestion states and network resources along the path.
- No explicit CLR but ($<10E-5$) is expected. The network guarantees to ABR connections a *minimum cell rate* (MCR).
- Undefined bit rate (UBR) when there are no specific QoS requirements. This service is intended for non-real-time applications, such as file transfer protocol (FTP), electronic mail, and low cost transmission control protocol/Internet protocol (TCP/IP) with non-real-time requirements.

ATM cells are transported over an ATM data network that consists of switching nodes capable of switching ATM cells and of edge nodes that provide the policing function, a function that verifies that the service level agreement is met by both the client and the service provider, and flow control throughout the ATM network that locates traffic congestion areas and provides mechanisms to avoid them or guarantee delivery of high-priority traffic. This is known as pure ATM. During the connection admission control (CAC) process at UNI, the traffic parameters and the requested ATM services are provided by the user to the ATM node.

An end-to-end connection is established with a series of *virtual channel* (VC) links. This is known as *virtual channel connection* (VCC). Each switching node, upon receiving a cell and based on

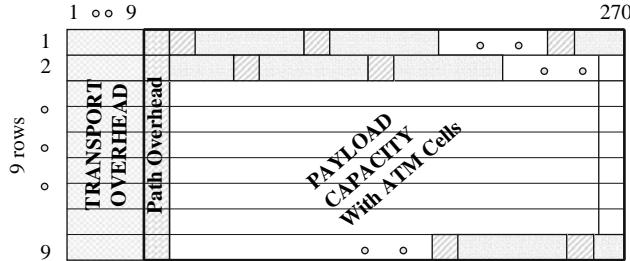


Fig. 2.20 Mapping ATM cells in SONET/SDH SPEs

routing translation tables, translates the incoming VCI in the ATM header cell into an outgoing VCI. Thus, the VCI value is different from node to node. The translation values at each node are determined during the setup of the connection.

An end-to-end connection of a bundle of virtual channel links is established from source to destination, and it is known as *virtual path connection* (VPC). The VPI in the ATM header cell identifies the VPC. Each ATM cell in the bundle has the same VPI. Each switching node, upon receive of a bundle and based on routing translation tables, translates the incoming VPI into an outgoing VPI. Thus, the VPI value is different from node to node. The translation values at each node are determined during the setup of the connection.

VPCs may be permanent or on demand. Permanent connection is established by node provisioning at the subscription phase and thus signaling procedures are not needed. Connections on demand require signaling procedures so that VPCs may be set up and released by the network or by the customer.

Besides pure ATM, ATM may also be transported over SONET/SDH. ATM cells are mapped in concatenated (STS- N_c) payloads. For example, in STS-3c, ATM cells are mapped in the payload capacity by aligning the byte structure of every cell with the STS-3c byte structure. The entire payload capacity (260 columns) is filled with cells, yielding a transfer ATM capacity of 149.760 Mbps, Fig. 2.20. In STS-12c, ATM cells are mapped into the payload capacity by aligning the byte structure of every cell with the STS-12c byte structure. The entire payload capacity (1,040 cols) is filled with cells, yielding a transfer capacity of 599.040 Mbps. If client cells are not available during the filling process, idle ATM cells are used.

2.3.2 Ethernet

Ethernet is a hierarchical local area data network that was designed for high data rate, simplicity, relatively short-distance transport, quick installation, easily maintainable, and low cost [26]. Ethernet was born in the research labs of Xerox Corporation, and it has been around for almost three decades. It has been accepted as an industry standard (IEEE 802.3), and its popularity keeps growing for three reasons: it is a public standard, it is simple, and its cost keeps decreasing because of large production volume. The initial Ethernet was not developed to compete with telephony, and thus error control, network protection and security, real-time data delivery, and quality of service were secondary issues. Nevertheless, new Ethernet versions with data rates of 1, 10, 40 and perhaps 100 Gbps are more service aggressive, and it is inevitable that they will include mechanisms to transport voice, fast data, and video over the gigabit Ethernet (GbE) protocol.

The Ethernet protocol is based on the tree topology. Terminal stations of the Ethernet may initiate a frame transfer. Thus, there is a finite probability that two or more stations may attempt a frame transfer at the same time, in which case a collision may occur. To avoid collisions, all Ethernet

stations use a carrier sense multiple-access/collision detection (CSMA/CD) mechanism that resolves collisions with “equal fairness to all stations”. This mechanism is based on a predefined collision window and on active listening to traffic on the network. If the carrier is absent for at least twice the collision window, a station can start transmitting. If two or more stations start transmitting, they are able to detect the collision from “listening to the traffic” and back off. At a random time thereafter, they start again.

Transmission starts with a preamble signal (a string of zeroes and ones). The purpose of the preamble is to listen and to also stabilize the clock of the receivers. The preamble code is followed by a start-of-frame delimiter, the source ID, the destination ID, and other information, including length of data field, which is followed by data; this is concluded with a frame check sequence.

The Ethernet is based on a tree topology. Ethernet uses CSMA/CD (carrier sense multiple access/collision detect) according to which a node on the tree network always senses or “listens” to the traffic on it. When a node needs to transmit, it will attempt to cease the network only when it is “quite”; that is, there is another node not transmitting. This is the CSMA part of the protocol. If two nodes try to cease the network simultaneously, then they “sense” each other’s attempt (i.e., they detect a collision), they both give way and try again but after a random interval. This is the CD part of the protocol. The frame format of the latter is illustrated in Fig. 2.21.

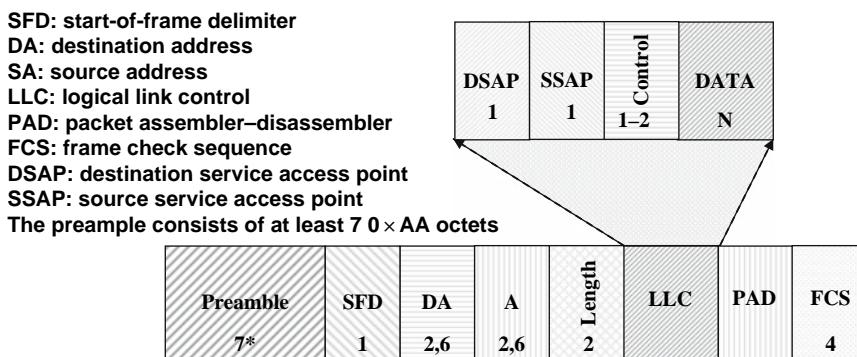
There are several Ethernet variants, among them are the following:

- Ethernet 10BASE-T and 100BASE-T. They are defined for unshielded twisted pair cable (UTP) at 10 and 100 Mbps.
- Ethernet 1000BASE-x is defined for UTP and fiber at 1,000 Mbps; x = T for UTP and F for fiber.
- 10GbE is defined at 10 Gbps over fiber.
- 40GbE is defined at 40 Gbps over fiber.

2.3.3 Gigabit Ethernet

The Gigabit Ethernet (1000BASE-x), or GbE, has evolved from 100BASE-x and 10BASE-T. GbE was initially defined for twisted copper cable, known as 1000BASE-T and subsequently for optical fiber [27–30], it is backward compatible with its predecessor “fast Ethernet” and thus it uses the carrier sense multiple-access/collision detection (CSMA/CD) access method.

Ethernet defines several layers: the media access control (MAC), the physical medium independent interface (PMI), and the physical layer (PHY), which consists of the physical sub-layer and



*Numbers indicate octets

$$0 \times AA = 10101010$$

Fig. 2.21 Ethernet CSMA/CD frame

the medium dependent interface sub-layer (MDI). GbE also defines an intermediate layer between the PMI and PHY known as medium independent interface (MII). The purpose of MII is to provide medium transparency to the layers above it and allow for a variety of media (wired, MMF, and SMF), as already described.

The MAC layer provides network access controllability during frame assembly and disassembly of the client data and during frame transmission to lower layers. It also provides network access compatibility of MACs, end to end and of all intermediate MACs on the path. The MAC layer may optionally provide full- or half-duplex capability; full-duplex means that the MAC supports both transmit and receive. The MAC layer may also request that subsequent peer MACs inhibit further frame transmission for a predetermined period, it may allow for a second logical MAC sub-layer. In the latter case, the basic frame format is maintained but the interpretation of the data fields and the length may differ. It may also support VLAN tagging (per IEEE 802.3ac, 1998) to prioritize packets; however, VLAN tagging requires changes to the frame format.

Four types of media are defined in the GbE standard: 1000Base-SX, 1000Base-LX, 1000Base-CX, and 1000Base-T. The first two (1000Base-SX and 1000Base-LX) consider optical fiber as the physical medium and the fiber channel (FC) technology for connecting workstations, supercomputers, storage devices, and peripherals, the last two (1000Base-CX, and 1000Base-T) consider copper medium.

1000BASE-T is not defined at a serial gigabit bit rate. Instead, it is defined over four unshielded twisted pairs (UTP), category-5, 100Ω copper cables, up to 100 m maximum length conforming to ANSI/TIA/EIA-568-A cabling requirement, at 250 Mbps per pair. Conversely, the 1000BASE-T complies with the same topology rules of 100BASE-T and it supports half- and full-duplex CSMA/CD. It also uses the same auto-negotiation protocol with 100BASE-TX. The four pairs form a parallel cable, each keeping the symbol rate at or below 125 Mbaud, Fig. 2.22.

Because 1000BASE-T is over copper lines, the standard had to address known issues such as echo, near-end cross-talk, far-end cross-talk, noise, attenuation, and EMI. To keep noise, echo, and cross-talk at low levels commensurable with 10^{-10} bit error rate, the following countermeasure design strategies were adopted:

- 4D 8-state trellis forward error correction (FEC) code;
- Signal equalization with digital techniques;
- PAM-5 multilevel encoding where each symbol represents one of five levels, $-2, -1, 0, +1$ and $+2$. The four levels are used for data and the fifth for FEC coding. This results in a reduction of the signal bandwidth by a factor of two;

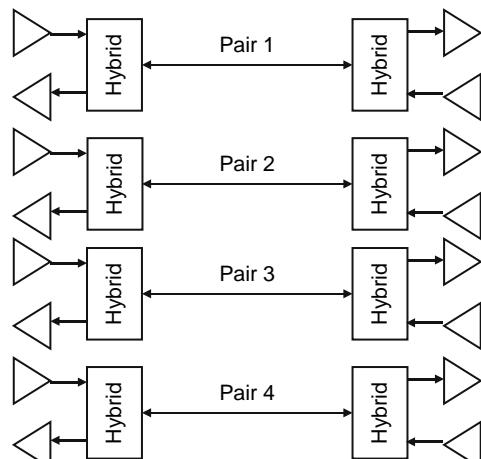


Fig. 2.22 1000BASE-T is on four parallel pairs, each at a symbol rate at or below 125 Mbaud

- Pulse shaping at the transmitter to match the characteristics of the transmission channel and increase the signal to noise ratio;
 - Scrambling to randomize the sequence of transmitted symbols and reduce spectral lines in the transmitted signal.

1000BASE-CX standard defines a gigabit Ethernet for single-pair “twinax” shielded twisted pair (ST) copper cable but for very short lengths (up to 25 m). In addition to UTP cable, the 802.3ab task force has defined standards for fiber cable. These standards are the 1000BASE-SX for short-wavelength fiber (850 nm, MMF) and the 1000BASE-LX for long-wavelength fiber (1,300 nm, SMF).

1000BASE-LX defines a gigabit Ethernet for long haul (up to 3 km) using an optical channel at 1,300 nm over single-mode fiber, or multimode fiber (up to 550 m).

1000BASE-SX defines a gigabit Ethernet for long haul (up to 3 km) using an optical channel at 850 nm over multimode fiber with core diameter 50 μm (up to 550 m) or with core diameter 62.5 μm (up to 300 m).

Because of the four physical media defined in GbE (1000BASE-CX, 1000BASE-SX, 1000BASE-LX, and 1000BASE-T), it was necessary to bring transparency to the media access control (MAC) layer. Thus, a new layer under the MAC was defined, known as the reconciliation sub-layer and the gigabit media independent interface (GMII), Fig. 2.23.

The GMII provides physical layer independence so that the same MAC can be used for any media and it supports 10, 100, and 1,000 Mbps data rates for backward compatibility. It also includes signals such as management data clock and management data input–output and basic and extended (which is optional) registers. The registers are used for auto-negotiations, power down, loop-back, PHY reset, duplex/half-duplex selection, and others.

The Reconciliation sub-layer in the transmit direction maps service primitives or physical layer signalling (PLS) from the MAC to MGII, and vice versa in the receive direction.

The PLS includes signals such as data request, transmit enable, transmit error, transmit clock, collision detect status, data valid, receive error, signal status indicate, carrier status indicate (collision detect, carrier sense, carrier extend), and receive clock.

The GMII is further subdivided into three sub-layers: the *physical coding sub-layer* (PCS), the *physical medium attachment* (PMA), and *physical medium dependent* (PMD).

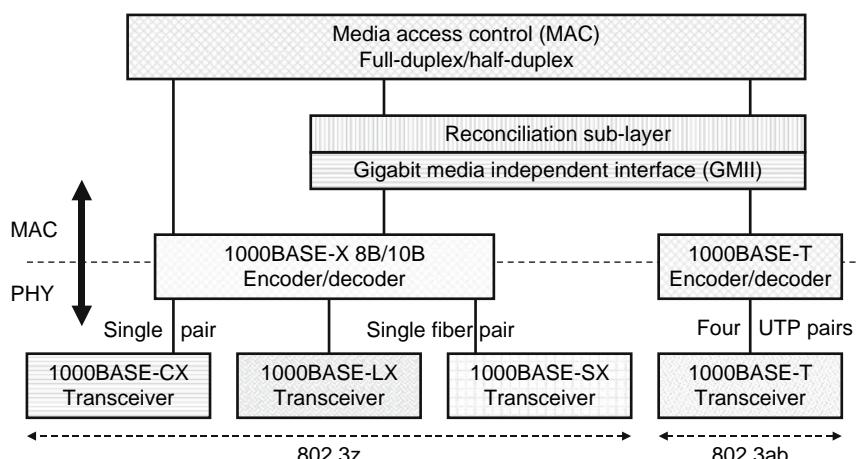


Fig. 2.23 Gigabit Ethernet PHY derivatives

- The PCS sub-layer provides a uniform interface to the Reconciliation layer for all physical media; it uses the 8B/10B coding like the Fiber Channel. In addition, the PCS generates the carrier sense and collision detection indications, and it manages the auto-negotiation process by which the network interface (NIC) communicates with the network to determine the network data speed (10, 100, or 1,000 Mbps) and mode of operation (half-duplex or full-duplex).
- The PMA sub-layer provides a medium-independent means for the PCS to support various serial bit-oriented physical media. This sub-layer serializes code groups for transmission and deserializes bits received from the medium into code groups.
- The PMD sub-layer maps the physical medium to PCS, and it defines the physical layer signaling for the various media it supports. PMD also includes the *medium-dependent interface* (MDI), which is the actual physical layer interface that also defines the actual physical attachment for different media types such as connectors.

The GbE defines two different bit rates. Raw data is formatted at the MAC layer and is passed via the GMII over to the physical layer at 1,000 Mbps. This is known as *instantaneous transmission rate for encoded MAC data*. However, at the physical layer, the 8B/10B coding increases by 25 % the line bit rate to 1.25 Gbps. This is known as the *instantaneous transmission rate*. Thus, the user data transmission rate over the medium is

$$\text{Transmission rate(for user data)} = [n_{\text{data}}/n_{\text{total}}] \times 1,000 \text{ Mbps}$$

2.3.4 10 Gigabit Ethernet

The GbE momentum prompted in 2002 the study of a more advanced Ethernet protocol to match the OC-192 (10 Gbps) bit rate for local area network applications and to support 6–8 million ports, called native 10GbE. The 10GbE supports transmission over fiber-optic physical media, multi-mode fiber (MMF) and single-mode fiber (SMF) and for fiber lengths up to 10 km and in certain cases up to 40 km (IEEE 802.3ae), as well as over copper (IEEE 802.3ak). Thus, the 10GbE enabled previously known Ethernet technology in local area networks (LAN), metropolitan area networks (MAN), wide area networks (WAN), and in storage area network (SAN) applications, employing full-duplex operation only and not CSMA/CD for gaining access to the physical medium. 10GbE compatibility with OC-192 SONET (10 Gbps) is accomplished through the definition of a *WAN interface sub-layer* (WIS). Thus (according to IEEE 802.3ae):

- 10GBASE-LX4 (L stands for long range) supports SMF transmission up to 10 km at 1,300 nm window (O-band: 1,260–1,360 nm) using a coarse wavelength division multiplexing (CWDM) grid. It also supports MMF at 1,310 nm for fiber lengths up to 300 m. (In addition, ITU-T G.694.2 specifies a CWDM grid within the range 1,270–1,610 nm with 20 nm channel spacing using water-free SMF.)
- 10GBASE-EX4 (E stands for extended long range) supports SMF transmission up to 40 km in the 1,550 nm window (C-band).
- 10GBASE-SX4 (S stands for short range) supports MMF transmission and fiber length up to 550 m powered by 850 nm VCSEL lasers. The 10GbE MMF length is specified for the 850 nm channel bandwidth as follows: up to 82 m for 500 MHz km for 50 μm core fiber, 66 m for 400 MHz km for 50 μm core fiber, 33 m for 200 MHz km for 50 μm core fiber, and 26 m for 160 MHz km for 62.5 μm core fiber. In addition, the fiber length may be extended to 300 m (and perhaps up to 1 km) with the 850-nm 50- μm optimized fiber. Currently, 10 Gbps over MMF with 850 nm VCSEL lasers is a cost-effective solution in access networks compared with SMF solutions, which may be twice as costlier.

- 10GBASE-CX4 supports twinax copper cable up to 15 m for datacenter applications.

The actual line rate of 10GbE is higher than 10 Gbps as a result of 8B/10B or 64B/66B coding. Thus, 10GbE-4 transmits at 4×3.125 Gbps (8B/10B) over four optical channels (i.e., 3.125 Gbps/channel), called *lanes*, with a coarse channel spacing of 24.5 nm. The nominal wavelengths defined for each lane are the following:

Lane 0: 1275.7 nm
 Lane 1: 1300.2 nm
 Lane 2: 1324.7 nm
 Lane 3: 1349.2 nm

The reasons for transmitting over four coarsely spaced wavelengths are the following:

- Inexpensive lasers that are directly modulated and without cooling.
- No need for dispersion compensation and equalization for lengths of 10 to 40 km at such low bit rate.
- Polarization effects are negligible.
- Optical devices have lower cost and lower maintenance.

Based on this, the 10GbE MAC layer instead of producing a single serial data stream (like the GbE) maps on four parallel lanes the byte-organized data in a round-robin manner. For example, on the transmit path, the first byte aligns to Lane 0, the second byte to Lane 1, the third byte to Lane 2, the fourth byte to Lane 3, the fifth byte to Lane 0, and so on. In addition, in order to avoid ambiguity of finding the start of the Ethernet frame on a lane and to facilitate frame synchronization, the 10GbE places the start control character of a frame on Lane 0. This is accomplished by adjusting the typical 12-byte idle inter-packet gap (IPG) length either by padding to 15 bytes or by shrinking it to 8–11 idle bytes. A third option uses an averaging method; it includes a deficit idle counter that keeps track of the number of idle bytes added to or subtracted from 12 (ranging from 0 to 3) so that over many frames, the 12-byte average is maintained.

10GbE network adapter cards have been implemented and have been evaluated for high-performance computing applications. Their performance surpassed all previous Ethernet cards (<http://www.guinessworldrecords.com/index.asp?id=58445>, July 7, 2003).

2.3.5 FDDI

Fiber distributed interface (FDDI) is a high data rate local area data network based on a dual fiber-ring topology, Fig. 2.24, and it uses a timed-token protocol (TTP) according to bidding process. Although not widely used, it offers both synchronous and asynchronous services to other stations on the ring by sending priority tokens (i.e., very short messages). If a FDDI station needs to transmit a packet and if there is no traffic on the ring, it sends a token to cease the ring, and if this is successful, then it sends the packet. If two stations attempt to send a token simultaneously, then they stop transmitting and they retry.

FDDI transports data at 100 Mbps, and because it uses a 4B/5B coding, the actual bit rate on the fiber medium is 125 Mbps.

The FDDI frame consists of nine fields:

- Preamble (64 bits)
- Starting delimiter (8 bits)

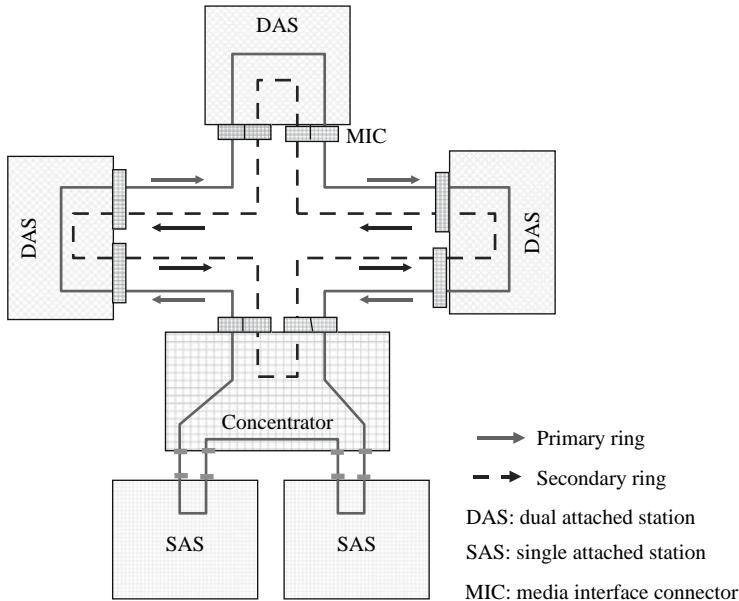


Fig. 2.24 The dual-fiber ring FDDI local area network

- Frame control (8 bits)
- Destination address (16 or 48 bits)
- Source address (16 or 48 bits)
- Information (up to 4,500 octets)
- Frame check sequence (32 bits)
- End delimiter (8 bits), and
- Frame status (at least 12 bits or 3 symbols; each symbol consists of 4 bits).

FDDI was designed with superb protection against link failures; this feature has been adopted by most Metro optical networks. When a link fails, the stations adjacent to failure automatically reconfigure themselves by establishing loops on the physical layer, from the primary to the secondary ring.

The FDDI station standard consists of four sections:

- The physical layer medium dependent (PMD)
- The physical layer protocol (PHY)
- The medium-specific access control (MAC), and
- The station management (SMT).

FDDI networks support links up to 2 km in length. Based on this, a practical FDDI network can have up to 200 km total fiber length (both primary and secondary), and it can accommodate more than 500 stations.

FDDI has inspired the two-connected regular ring-mesh network (RMN) architecture, also known as manhattan street network (MSN) or Manhattan FDDI (M-FDDI). This network utilizes distributed control, packet queuing, adaptive routing, flow control, dead-lock avoidance, and packet re-sequencing and exhibits an increased throughput performance as well as fault and disaster avoidance. As an example, a 64-node RMN network outperforms in throughput a bus network by a factor of 20 to 30, if all things are equal. The factor increases in larger networks. The RMN exhibits a superior routeability or packet deliverability from the standpoint of the number of available routes between two nodes in the network. For unidirectional M-FDDI with $N \times N$ nodes, the total number

of possible routes per channel between source and destination, without visiting the same node twice, is estimated to be $N!(N - 1)$. However, in bidirectional RMNs, this number increases rapidly; for example, a 3×3 has 176 and a 4×4 has 1592.

FDDI, an optical LAN of the 1980s, proved that data fiber rings were an excellent solution for Metro applications that Ethernet could not be easily applied. As a result, many of the topological and protocol features of FDDI were adopted in new fiber data networks, such as the shared rings (from RMN or M-FDDI), two- and four-fiber Metro rings, the Ethernet over Metro (fiber ring), and the new resilient packet ring (RPR).

2.3.6 Switched Multi-megabit Data Services

The Switched multi-megabit data services (SMDS) is a packet technology that

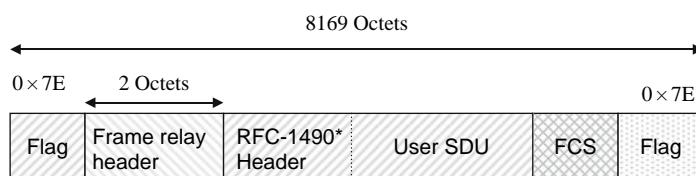
- has large packet size ($\sim 9K$ bytes);
- enables packet transfers to several destinations using grouping addressing;
- enables data transfers across MAN to SMDS in different LANs; and
- is based on the IEEE 802.6 (DQDB) protocol.

2.3.7 Frame Relay

The Frame Relay was an early fixed-size packet technology that was used by a provisioned synchronous network. At the access points, or user to network interface (UNI), the packet traffic is concentrated from a number of users, typically over leased lines (T1/E1), and the concentrated traffic is switched by means of a FR switch and it is put on a common backbone. Several interconnected FR switches form a Frame Relay Network. This network takes advantage of the variability of traffic patterns and by over-subscribing it uses available bandwidth to offer cost effective data service. The frame structure of FR is shown in Fig. 2.25.

2.3.8 The Transmission Control Protocol

The transmission control protocol (TCP) is a connection-oriented protocol; a connection is setup by defining parameters. It is a transport-layer protocol that is built over the Internet protocol and provides congestion control by using the sliding window scheme; *round trip time* (RTT) delay is used as a measure to define the sliding window length.



*RFC 1490 specifies encapsulation of multi-protocol data for transmission over frame relay
FCS: frame check sequence

Fig. 2.25 Frame relay frame

The TCP receives data from the application layer, which it segments and forms packets by adding its own overhead octets. The overhead contains the following fields:

- The *source port* (2 octets) indicates the sending user's port number
- The *destination port* (2 octets) indicates the receiving user's port number
- The *sequence number* (4 octets) able to number $2^{32}-1$ frames
- The *acknowledgment* number (4 octets)
- The *header length* (4 bits) indicates the length of header counted in 32-bit words
- The *reserved* (4 bits)
- The *urgent* (1 bit) indicates whether the urgent-pointer is applicable or not
- The *acknowledgment* (1 bit) verifies the validity of an acknowledgment
- The *push* (1 bit) indicates, when set, that the receiver should forward immediately the frame to the destination application
- The *reset* (1 bit) instructs, when set, the receiver to abort the connection
- The *synchronize* (1 bit) is used to synchronize the sequence numbering
- The *finished* (1 bit) indicates that the sender has finished transmitting data
- Not used (2 bits)
- The *window size* (2 octets) specifies the window size
- The *checksum* (2 octets) checks the validity of the received packet
- The urgent pointer (2 octets) directs the receiver, when set, to add up the value of the pointer field and the value of the sequence number field in order to find the last byte of the data and to deliver urgently to the destination application
- The *options* (up to 4 octets) specifies functions not available in the basic header
- The padding (1 octet) concludes the TCP header. The data field is appended at the padding field.

This comprehensive TCP header is better suited to applications that require reliability but not speed such as e-mail, wide world web, file transfer, remote terminal access, and mobile.

2.3.9 The User Datagram Protocol

The user datagram protocol (UDP) is a transport-layer connectionless protocol. UDP over IP provides the ability to check for the integrity of packet flow. UDP provides error control but not as efficiently as the TCP. Like TCP, so UDP adds a header to a segment of data. The various fields added to a data segment are as follows; notice the absence of any acknowledgment fields in the UDP header, since this is a connectionless protocol:

- The *source port* (2 octets) indicates the sending user's port number.
- The *destination port* (2 octets) indicates the receiving user's port number.
- The *UDP length* (2 octets) specifies the length of he UDP segment.
- The *UDP checksum* (2 octets) contains the computed checksum, and this field concludes the TCP header. The data field is appended at the UDP checksum field.

The UDP protocol was developed with header simplicity, as compared with the TCP header, in order to provide faster and more efficient delivery. Thus, the UDP simplicity, although not as reliable as the TCP is applicable to voice over IP, video over IP, DNS, SNMP network management, and mobile IP.

2.3.10 The Real-Time Transport Protocol

The real-time transport (RTP) protocol provides the basic functions required for real-time applications. RTP segments data into smaller application data units (ADU), to which it adds its own header to form application level frames to run over transport protocols.

RTP is applicable to real-time applications that can tolerate a certain amount of packet loss, such as voice and video. However, RTP includes a mechanism that notifies the source of the received quality of packets so that the source may make some rate adaptation in order to improve transmission and throughput quality or packet delivery quality.

The RTP packet format contains a header (16 octets), the datagram, and the contributing source identifier (4 octets) as a trailer. The added overhead by RTP is as follows:

- The *version* (2 bits) indicates the protocol version.
- The *padding* (1 bit) indicates that there is a padding field at the end of the payload.
- The *extension* (1 bit) indicates the use of an extended header.
- The *contributing source count* (4 bits) indicates the number of contributing source identifiers.
- The *marker* (1 bit) marks a boundary in a data stream. In video applications, this bit is set to denote the end of a video frame.
- The *payload type* (7 bits) specifies the payload in the RTP frame. It also contains information about encryption or compression.
- The *sequence number* (2 octets) identifies the numbered sequence of packets after segmenting the data stream.
- The *timestamp* (4 octets) indicates the time the first byte of data in the payload was generated.
- The *synchronization source identifier* (4 octets) identifies the RTP source in a session.
- The contributing source identifier (4 octets) is an optional field, placed after the datagram, and it indicates the contributing source(s) of the data.

A more comprehensive real-time protocol is the *real-time control protocol* (RTCP) that runs on top of UDP and it supports enhanced performance functions by using multicasting to provide performance feedback. This is supported by defining several types of RTCP packets, such as the *sender reports*, the *receiver reports*, the *source descriptor*, the *goodbye*, and other *application-specific* types.

2.3.11 Internet Protocol

The Internet protocol (IP) and the network based on it is a packet technology defined as *best-effort connectionless* [31]. Thus, IP does not establish a fixed (switched) path dedicated for the duration of a session, but instead, it assembles packets of variable length, and by store-and-forward it delivers each one over one or more routes, taking advantage of the temporal availability of bandwidth resources throughout the network.

At the receiving end, because packets arrive with different latency and perhaps out of sequence, the packets include in their overhead a source and a destination address, a packet sequence number, an error control, and other information. Thus, although the IP network did not measure up in real-time delivery compared with the circuit switched network, it proved to be an economical method for delivering data and it was rapidly deployed. For example, latency exceeded 500 ms, whereas the acceptable round trip delay in synchronous networks is <300 ms (round trip delay is measured from phone-to-phone and back), quality of service (QoS) was limited to best effort whereas the circuit switched network has better than 99 % availability, and privacy was not part of the initial IP strategy.

The IETF Internet Protocol Performance Metrics group (IETF IPPM) and the Cooperative Association for Internet Data Analysis Group (CAIDA) has defined IP performance metrics for evaluating a data network. Among these metrics are

- symmetry or asymmetry characteristics of data flow (geographical, temporal, and protocol related),
- packet length distribution (predominant packet size on the IP network),
- length of packet train or packet flow distribution (i.e., the typical number of packets in a single transaction),
- causes of packet delay,
- causes of network traffic congestion, and
- protocols and their application on the IP network (TCP, http)

The explosion of IP demanded added updates (IPv4, IPv6) to support *voice over IP* and real-time compressed *video over IP* from multiple sources. However, since all sources are not equal, there is a *trust rate* assigned to each. The highest trust rate is assigned to *directly connected interfaces* or *manually entered static routing* and the lowest trust rate to *internal border gateway protocol*. That is, the highest trusted rate sources are similar to traditional synchronous communications networks. As a result, in an effort to offer QoS, service flexibility, granularity, scalability, shared-access, point-to-multipoint, customized bit rates, and easy service migration in optical networks, the Internet protocol is encapsulated in “several forms”, such as “Internet over SONET”, “Internet over ATM over SONET”, and so on.

2.3.11.1 Voice over IP

Voice over IP, also known as IP telephony, must at minimum provide the same (or almost the same) quality of service (QoS) and a publicly acceptable service availability. With traditional routers, it is questionable if IP telephony can match the availability and quality of the traditional wired (circuit switched) telephony. However, this largely depends on future router improvements, and new protocol development based on which VoIP may approach the traditional voice quality and gain popularity mainly due to the low cost of Internet and thus become a direct competitor to traditional telephony, Table 2.6. On the other hand, it is also expected that voice services will be bundled with data services and be offered over the next generation synchronous optical network at very low price, with voice traffic representing a minuscule percent of the total transportable traffic over the multiwavelength fiber-optic network, which using DWDM is several terabits per fiber.

One of the early issues in IP telephony was that it relied largely on non-standard *digital signal processing* (DSP) for coding, in contrast to the α - or μ -law standardized CODECs of traditional telephony. Since then, the ITU-T has defined several recommendations such as the G.723.1 that supports two voice codec rates, 5.3 and 6.4 Kbps, the G.729A supports 8 and 13 Kbps, and others such as G.711, G.728, G.729, G.729B, and recommendations on video (H.261 and H.323). Clearly, for IP telephony to be interoperable, the packet must include in the overhead a code to indicate to the receiving end which coding (compression) algorithm has been used so that the decoder can adapt to this algorithm and decompress the voice packet encapsulated in IP. That is, the IP network must be telephony aware with a technological sophistication by which:

- Overall delay and network latency meet the acceptable level;
- Lost-packets should be compensated and the rate of packet loss should remain below a threshold level commensurable with speech sample loss;
- The network and the path must be reliable under extreme conditions, network, and environmental, complying to the quality of service (QoS);
- The network should be managed complying with standards;

Table 2.6 Protocols for VoIP

Layer	Protocol							
	SIP		H.323 suite of protocols			Security	Signaling	Data
	Media transport	Registration	Media transport	Voice codec	Video codec			
5	H.225.0-RAS	G.711	H.261	H.235	H.225.9-Q.931	T.120		
		G.722	H.323					
		G.723						
		G.728			H.245			
		G.729			H.250			
		H.263						
4	RTP, RTCP		RTP, RTCP			TCP		
	UDP		IP, RSVP, IGMP					
3								

IP: Internet protocol

IGMP: Internet group management protocol

MGCP: media gateway control protocol

RSVP: resource reservation protocol

RTP: real-time transport protocol

RTCP: real-time control protocol

SIP: session initiation protocol

TCP: transmission control protocol

UDP: user datagram protocol

- It meets synchronization, clock, and jitter requirements. Traditional networks operate on a national clock hierarchy defined by standards, whereas routers operate on their own local clock;
- It meets echo cancellation requirements. Echo becomes a significant problem when overall (round trip) echo exceeds 50 ms;
- It addresses talker overlap. This is caused when one-way delay exceeds 250 ms and when one talker steps on the other talker's speech;
- It forms "short" packets with minimal insertion delay;
- Call initiation and termination procedures, emulating call admission control or traditional telephony signaling such as off-hook, on-hook, ringing, busy, and so on.

2.3.12 The Point-to-Point Protocol

2.3.12.1 ISDN

The integrated services digital network (ISDN) is a standardized technology of the 1980s developed to offer digital and integrated services (voice, high-speed data, conferencing, etc.) over the synchronous circuit switched network [32–47]. In ISDN, the POTS end device (the plain telephone) is replaced by the ISDN telephone, which now is more complex as it includes CODEC and other electronic functions in it.

Two ISDN rates were defined; the basic rate (BRI) at 144 Kbps and the primary rate (PRI) at 1.544 Mbps. The BRI consists of two *B channels*, each at 64 Kbps, and of one *D channel* at 16 Kbps. The B channels transport data and/or voice. The D channel transports maintenance and control messages and it supports user defined mix payload. Briefly, the D channel is used for:

- Signaling
- Calling number ID
- Far-end supervision

Table 2.7 Utilization of PRI

Designation	N	B	D	Payload
$N \times B + D$	1–23	Y	Y	128 Kbps–1.536 Mbps
$N \times B$	1–24	Y	N	64 Kbps–1.536 Mbps
$N \times H_0$	4	N	N	384 Kbps
$N \times H_0 + D$	3	N	Y	384 Kbps
H1	–	N	N	1.536 Mbps
H10	–	N	N	1.536 Mbps

- User-to-user message transfer
- Telemetry for fire alarms, security, meter reading, and so on
- Access to packet switching network
- Support new network services; multiple directory numbers sharing, and so on.

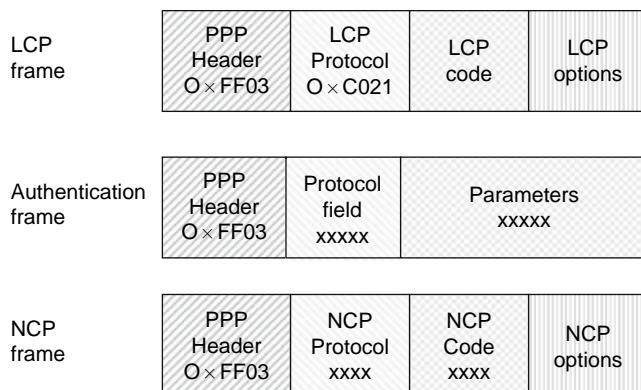
In contrast, the ISDN PRI uses the DS1 facility at 1.544 Mbps (24 time slots or channels each at 64 Kbps + the same ESF framing bit) to transport a combination of voice/data digital channels, Table 2.7.

2.3.12.2 PPP

The point-to-point protocol (PPP) defines the encapsulation of LAN IP over the B channel of ISDN [48]. One encapsulation requires bandwidth greater than 64 Kbps and the other bandwidth lower than 64 Kbps. Prior to transporting LAN IP over PPP, a step-by-step negotiation takes place using specifically defined PPP frames, Fig. 2.26. The main negotiation steps are

- the *link control protocol* (LCP),
- the *authentication protocol* (AP), which consists of
 - the *password authentication protocol* (PAP) and
 - the *challenge handshake authentication protocol* (CHAP), and
- the *network control protocol* (NCP).

The LCP frame consists of the PPP header (0xFF03), the LCP protocol field (0xC021), the LCP code field, and the LCP options field. The LCP code conveys the following messages:

**Fig. 2.26** PPP: LCP, authentication, and NCP frames

- configuration request
- configuration acknowledge
- configuration non-acknowledge
- configuration rejected
- echo request (to check quality of service)
- echo reply.

The LCP negotiated options are

- security option,
- authentication mode, and
- multilink option.

The authentication protocol (AP) frame consists of the PPP header (O×FF03), the protocol field, and the parameters field. The protocol field indicates the type of authentication:

- password authentication protocol (PAP)
- challenge handshake authentication protocol (CHAP).

The network control protocol (NCP) consists of the PPP header (0×FF03), the NCP protocol field, the NCP code field, and the NCP options field. The NCP protocol field conveys the following:

- IP control protocol (IPCP) with hex code O×8021,
- Novell IP extended control protocol (IPXCP) with hex code O×802B
- Bandwidth allocation control protocol (BACP) with code O×C02D.

The NCP code field conveys the following:

- configuration request (the configuration parameters are network number, IPX node, router alias)
- configuration acknowledge
- configuration non-acknowledge
- configuration rejected
- termination request; used to interrupt PPP traffic before B channel is disconnected
- termination acknowledge.

After the negotiation, the IP is encapsulated in PPP frames and is routed; however, there are two cases, Fig. 2.27:

- If the data rate is ≤ 64 Kbps, the encapsulated IP packet is routed over one B channel. In this case, the PPP frame consists of the PPP header (0×FF03), the protocol code field (0×0021), and the IP packet field.
- If the data rate is between 64 and ≤ 128 Kbps, then the IP packet is fragmented into two pieces that are routed over both B channels (B1 and B2). This is called PPP/multi-link protocol (PPP/MLP).

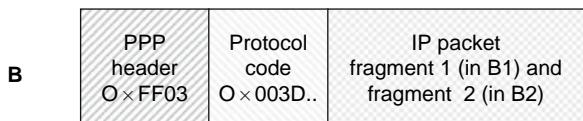
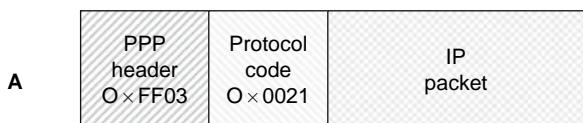


Fig. 2.27 PPP frames for IP packets requiring ≤ 64 Kbps (A) and >64 Kbps (B)

In this case, the frame consists of the PPP header ($0\times FF31$), the protocol code ($0\times 003D$), and the IP fragment field (fragment #1 in B1, and fragment #2 in B2).

2.3.13 4B/5B and 8B/10B Block Coding

We have described that certain protocols (such as Ethernet and FDDI) use a code conversion at the physical layer, the 4B/5B and 8B/10B. That is, 4-bit codes are converted to 5-bit and 8-bit to 10-bit according to a specific algorithm or table code conversion.

Because data is transmitted serially, there is no assurance that there will be no long sequence of zeroes and of ones; typically, it is desirable to have a balanced number of zeroes and ones so that a DC average value is maintained to keep the receiving clock running within the expected accuracy and jitter tolerance. To remove the zero–one imbalance, one successful method is to regard the 4-bit or 8-bit octet as a block and convert it to a 5-bit or 10-bit block.

For example, a 4-bit block provides 2^4 or 16 combinations of binary values, among which the high imbalanced codes 0000, 0001, 1000, 1111 and others are. However, the 5-bit block yields 2^5 or 32 combinations of binary values from which 16 can be selected with a good zero–one balance, whereas the remaining 16 codes are either not used or are used occasionally as specific control codes. To further illustrate how this works, the following describes the 3B/4B simpler code.

2.3.13.1 Example: 3B/4B Block Coding

In this case, 3-bit codes yield the eight combinations: 000, 001, 010, 011, 100, 101, 110, and 111. Similarly, 4-bit codes provide 16 combinations from which a one-to-one association is made between eight 3-bit codes and eight selected 4-bit codes, following an algorithm for uniqueness as follows:

Count the number of ones in the 3-bit code.

If odd, then add a “1” to the right of the least significant bit (LSB)

If 1111 then convert to 1101, else go to the next step.

If even, then add a “0” to the right of the LSB

If 0000 then convert to 0010, else go to the next step.

According to this simple algorithm, a 010 becomes 0101, and so on, Table 2.8.

2.3.13.2 Example: 8B/10B Block Coding

The initial 8-bit octets represent 2^8 binary combinations, many of which have very few ones or zeros. For example, consider the possible string

1000 0000 | 0000 0000 | 0000 0000 | 0000 0001 | ...

Table 2.8 3B/4B conversion

3-bit codes	4-bit codes	4-bit codes improved
000	\Rightarrow 0000	\Rightarrow 0010
001	\Rightarrow 0011	\Rightarrow 0011
010	\Rightarrow 0101	\Rightarrow 0101
011	\Rightarrow 0110	\Rightarrow 0110
100	\Rightarrow 1001	\Rightarrow 1001
101	\Rightarrow 1010	\Rightarrow 1010
110	\Rightarrow 1100	\Rightarrow 1100
111	\Rightarrow 1111	\Rightarrow 1101

which has too many zeroes. Such 8-bit binary codes would appear in delimiters, in control characters, and in data creating ambiguity at the receiver.

Considering 10-bit characters, there are 2^{10} (1024) binary combinations, from which a subset of only 2^8 (256) is selected according to a prescribed algorithm so that the constructed string of 10-bit character codes maintains the desired density of ones. Moreover, some of the remaining 10-bit codes can be used as delimiters and special control characters so that they will never appear in the overhead or data field of a packet (unless there are errored bits). However, this conversion implies that 25 % more bits are introduced; the bit rate on the transmission medium is accordingly increased representing 25 % bandwidth overhead.

For compatibility and interoperability purposes, the 8B/10B conversion process is defined by standards. Eight-bit codes spanning from 0×00 to $0 \times FF$ (a total of 256) are coded as D0.0 to D31.7. For example, binary codes from 0×00 to $0 \times 1F$ are coded as D0.0 to D31.0, from 0×20 to $0 \times 3F$ are coded as D0.1 to D31.1, and so on. However, the conversion of each 8-bit binary code to a specific 10-bit code (known as **abcdei fghj**) depends on the number of ones in the **abcdei** and **fghj** subblocks of the previous states, and it is determined according to complex rules. Based on block-coding theory, according to which these rules are generated, there are 12 special code-groups from which only six are employed in gigabit- Ethernet (GbE). A full description of 8B/10B conversion is beyond the purpose of this and the interested reader may consult appropriate standards.

2.3.14 Fiber Channel

A channel is a well-defined, direct, and structured mechanism to transport information data between a source and a destination, and in some cases, to several destinations. Most of the decision making takes place before and during setting up a channel. When a channel is set up, then very little decision is required and made. In the data space, a channel is set up to connect peripheral devices from a workstation to a peripheral device such as a printer.

Channels are specified by common channel protocols and for a limited distance between source-destination, typically few feet or meters. However, in large systems connected with large capacity peripherals at long distances, few meters is not sufficient, and this is the application target of the *fiber channel* (FC) protocol [49–61].

The *fiber channel* (FC) protocol was developed for high-performance devices that communicate with processors and for intercommunication between many processors. The FC physical interface defines a system that consists of a set of a general purpose processors, servers, or subsystems; a FC node may contain one or more ports called *node_port*, a function that connects the FC node with another FC node or with the FC switching fabric.

FC is specified to support several transmission media, coaxial, shielded twisted copper pair with a DB-9 connector, optical fiber (multimode with 62.5 and 50 μm core, and single-mode fiber with 9 μm core). LED or lasers light sources may be used at wavelengths 780 and 1,300 nm. The maximum link length varies from 500 m to 10 km for optical transmission and from 10 to 100 m for electrical transmission.

FC is specified to support several bit rates. The most common rate is 1,063 Mbaud, also termed “full speed”; this is derived from 100 Mbytes/s ($10 \times$) and adding 63 Mbit/s overhead: $100 \times 10 + 63$ Mbit/s = 1,063 Mbit/s. There are also multiple rates ($2 \times$ at 2,126 Mbit/s and $4 \times$ at 4,252 Mbit/s) and sub-rates ($1/2 \times$, $1/4 \times$, and $1/8 \times$, at 50, 25, and 12.25 Mbytes/s, respectively).

FC defines five layers, FC-0 to FC-4:

- FC-0 specifies the physical interface: media, receiver, transmitter, signaling, medium and data rate. For example, at 100 Mbytes/s, the I/O port may support 1,300 nm laser over SMF, or 780 nm

laser over 50 μm MMF, or electrical over coaxial. In contrast, at 12.5 Mbytes/s may support 1,300 nm LED over 62.5 μm MMF, or electrical over coaxial or shielded twisted pair.

- FC-1 is the transmission protocol that specifies the link maintenance aspects and EBCDIC 8B/10B encoding/decoding.
- FC-2 is the signaling protocol that specifies the frame format, segmentation and reassembly, flow control, classes of services, exchange and sequence management, topologies, and login/logout procedures.
- FC-3 specifies the common services for multiple ports on one mode.
- FC-4 specifies the upper layer protocol (ULP), and it is responsible for mapping traditional higher layer protocols, such as
 - Internet protocol (IP)
 - Asynchronous transfer mode (ATM) using adaptation layer 5 (AAL-5)
 - Small computer system interface (SCSI)
 - High-performance parallel interface (HIPPI)
 - Intelligent peripherals interface-3 (IPI-3)
 - Single byte command code sets (SBCCS)
 - Fiber connectivity (FICON)
 - Enterprise system connection (ESCON)
 - Video/audio multimedia, and networks

The FC frame is preceded and concluded by idle frames to provide margin between frames, Fig. 2.28.

FC is suited to two key topologies: the point-to-point and the arbitrated loop, Fig. 2.29, and it defines a port that consists of a transmitter with outbound traffic and a receiver with inbound traffic.

The point-to-point topology requires a two-fiber link, one for transmit and the other for the receive direction. It also requires a simple link initialization before communication begins.

The arbitrated loop can connect up to 127 ports in a single network and the media is shared among many devices; these devices support the *arbitrated loop initialization protocol*.

In addition, FC supports a fabric switch topology and a fabric switch with arbitrated loops topology capable of interconnecting 224 devices and allowing simultaneous communication, Fig. 2.30; the fabric switch is non-blocking and the I/O ports of the FC fabric are known as F_Ports. When FC ports login the fabric, the fabric assigns native address identifiers to them. Thus, the fabric may be a broadcast server, a directory server, a multicast server, an alias server, and so on.

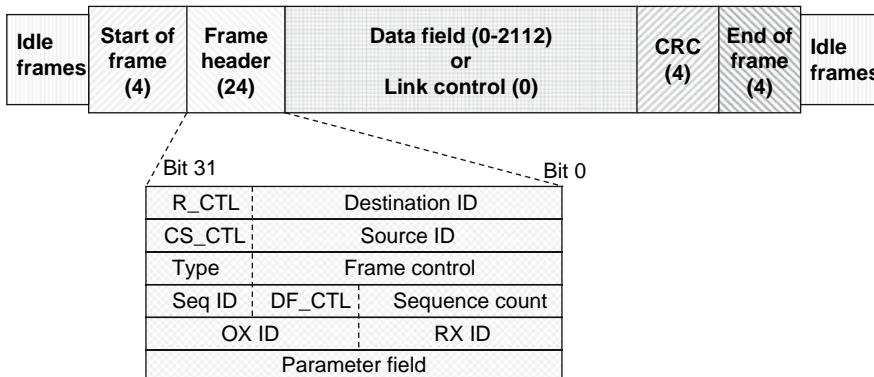
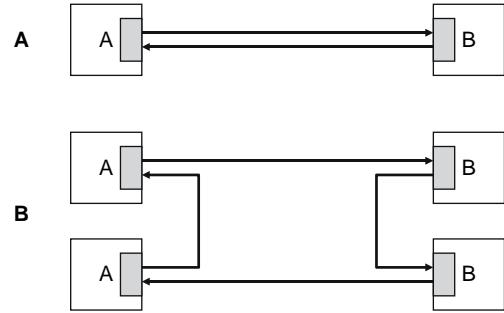


Fig. 2.28 FC frame structure (number in parenthesis indicate octets). However, after 8B/10B encoding, octets become 10-bit long

Fig. 2.29 FC supports the point-to-point topology (A) and the arbitrated loop topology (B)



During the *loop initialization process* (LIP), each port is assigned dynamically an 8-bit *arbitrated loop physical address* (AL_PA).

- The initialization process begins with transmitting a LIP *Primitive Sequence* upon power on or when a loop failure is detected. As the port starts transmitting a LIP, it triggers other ports on the loop to transmit a LIP.
- During this phase, a master port is selected, either the one with the lowest numerical port name or one that is at a fabric switch.
- The next step is to allow a port to select an AL_PA. The loop master transmits a 127-bit bitmap of a frame around the loop and each port seizes a bit. There are four priorities:
 - The highest is known as *loop initialization fabric assigned* (LIFA) and goes to the fabric switch.
 - The other three are *loop initialization previously assigned* (LIPA), *loop initialization hard assigned* (LIHA), and *loop initialization soft assigned* (LISA). Thus, by the time the bitmap frame has returned to the master, all ports on the loop have been assigned an AL_PA.
- Finally, the master transmits a primitive signal to indicate that the initialization process is complete.

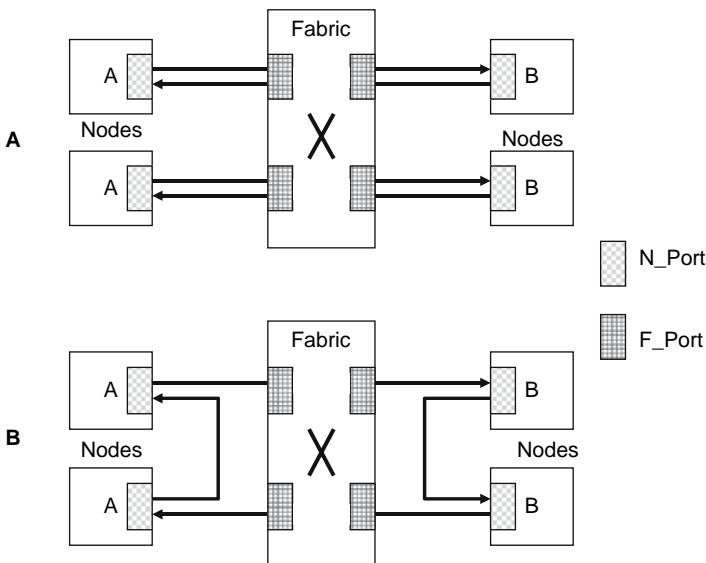


Fig. 2.30 The FC switch supports the point-to-point connectivity (A) and the fabric switch with arbitrated loops topology (B)

For congestion control, FC uses a credit-based flow control scheme. Each transmitting node according to buffer size is given a number of credit tokens. When transmission of frames begins, these credits are decremented. Frame transmission is halted if there are no credits left. Upon receiving acknowledgment, the credits are replenished and transmission may start again. This credit scheme is predictable, equitable and it guarantees that no frames are lost due to buffer overflow.

2.3.15 ESCON protocol

The *enterprise systems connection* (ESCON) is an I/O switch point-to-point technology that provides bidirectional serial bit transmission over two unidirectional optical MMF or SMF fiber cables [62, 63]. It supports distances as far as 9 km between control units and processors over fiber. The optical signal is about 10–50 mW at 850 nm for MMF (or 1300 nm for SMF). The fiber mode (MMF or SMF) is determined according to the distance and bit rate using either LEDs or inexpensive laser sources. Over MMF (62.5/125 or 50/125), a bandwidth/length of 500 Mbps-km is defined; that is, 500 Mbps transmitted over 1 km or 1,000 Mbps over 0.5 km, but at a maximum distance of 3 km. Similarly, over SMF, a bandwidth/length of 100 Gbps-km is used.

ESCON also defines devices known as signal “repeaters/converters”. These monitor the usage of the fiber link and they collect error statistics. In addition, an “ESCON manager” manages a multiple ESCON system configuration.

The ESCON communications protocol is implemented through sequences of special characters and through formatted frames of characters. Sequences consist of a predefined set of characters that signal either specific states or transitions to states. Frames have a variable length and transport data. Switching functionality is implemented with devices called “directors; directors are non-blocking and can dynamically or statically switch traffic”.

Information transmitted over ESCON links is EBCDIC 8B/10B encoded. From the $2^{10}-2^8$ remaining codes several are used as special characters in specific ESCON functions. The 8B/10B coding is transparent to channel units. Thus, if the signal rate is 200 Mbps, the effective information data rate is not 20 MB/s but lower, calculated by $n/(OH+n) \times 20$, where n is the quantity of data, OH is the overhead (header + trailer).

ESCON frames, Fig. 2.31, begin with a 2-character “start-of-frame” (SOF) delimiter and end with a 3-character “end-of-frame” (EOF) delimiter. Following the SOF is a destination field (3 characters), a source field (3 characters), and a link control field (1 character). Then, a variable information field (up to 1,028 characters), and a link trailer (5 characters), which includes the EOF. For synchronization purposes, the SOF is preceded by a string of “idle” characters that are unique (they cannot occur within the frame).

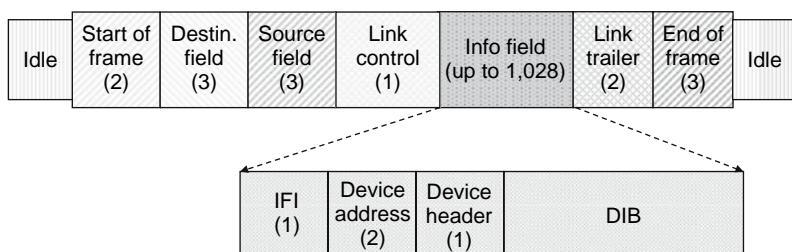


Fig. 2.31 Definition of the ESCON frame

- The ESCON SOF and EOF characters, unlike other protocols, have multiple meaning. SOF characters denote either “connect” (establish a connection) or “passive” (connection has been established). The EOF characters denote either “disconnect” (tear down a connection) or “passive” (connection has been established). Again, these characters are unique and they cannot be found in other fields, a benefit of the 8B/10B encoding.
- The information field consists of the “device header” and the “device information block” (DIB).
 - The “device header” consists of the “information field identifier” (IFI) (1 character), the “device address” (2 characters), and the “device-header flag” (1 character).
 - The DIB field may contain data, control, status, or commands.

2.3.16 FICON Protocol

The *fiber connection* (FICON) protocol is the next generation ESCON developed by IBM Corp. to support connectivity between mainframes and storage devices located at distances requiring longer fiber links and higher bit rates. To accomplish this, the FICON protocol supports

- Link bandwidth of 100 MB/s and 2 GB/s for FICON express (compared with 20 MB/s for ESCON).
- Connections of up to 20 km and up to 100 km lengths (compared with 9 km for ESCON).
- MMF (62.5/125, 50/125) at 850 nm and SMF (9/125) at 1,300 nm.
- Full-duplex data transfer. In storage devices, full-duplex means that data can be read and can be written simultaneously over the same link.
- An address space of 16,384 devices (as compared with 1,024 for ESCON).

FICON has adopted the mapping layer of FC (FC-4) and thus it is capable of multiplexing small and large packets on the same link. Thus, small packets do not have to wait for the large ones (with higher priority) to be transferred over FC links; FC Links are terminated at the FICON switch with a FC adapter card, Fig. 2.32.

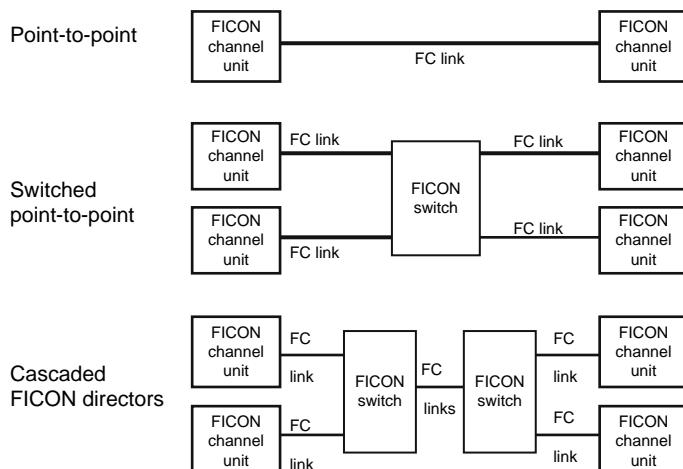


Fig. 2.32 FICON has adopted the FC-4 layer. FC links are terminated at the FICON switch with a FC adapter card

2.4 Resilient Packet Ring

Two known issues with SONET/SDH are resource utilization and cost. Two known issues with Ethernet are latency and jitter. An attempt to minimize these issues is the Metro ring topology that combines the virtues of SONET and Ethernet, it is supported by a protocol known as *resilient packet ring* (RPR), and it is considered by some the rival to next generation SONET/SDH.

SONET and Ethernet are considered layer-1 protocols. RPR is a layer-2 MAC protocol (worked by the 802.17 RPR Working Group), and it supports traditional carrier-class features on dual bidirectional rings such as QoS, restoration, protection, resiliency, access, bandwidth fairness to customers, simplified provisioning, and new services (broadcast and multicast). Additionally, RPR is supported by both SONET and by GbE on the physical layer.

A RPR packet consists of the header, the information payload and the trailing end fields.

- The header contains a destination address (DA), a source address (SA), a payload type (Type), and a cyclic redundancy code (CRC) error control code for error detection and correction in the DA, SA, and Type fields.
- The payload field contains the information payload which can be up to 1,500 bytes, and the payload FCS to detect and correct errors in the payload.
- The trailing end field contains a time to live (TTL) field, a class of service (CoS) field, and an in/out profile indicator (IOP). The IOP advertises the drop eligibility of the packet.

Based on TTL, DA, and IOP values, the RPR MAC determines if a packet should be

- dropped or it should be expressly switched to minimize buffering, jitter, and latency;
- passed in transit to the next node on the ring avoiding the switching function and reducing buffering and latency;
- stripped if the packet is corrupted; and
- copied and pass the copies in transit for multicasting.

In particular, the RPR MAC offers four services: reserved, high priority medium priority, and low priority.

- *Reserved* is a service similar to TDM, and idle bandwidth is not available to other services.
- *High priority* is for jitter and latency sensitive traffic.
- *Medium priority* allows for services that require provisioned bandwidth.
- *Low priority* allows for bandwidth negotiations, via bandwidth-notification messages, between the stations (or nodes) on the ring.

RPR uses two counter-rotating rings to propagate packets, a notion that was first deployed in FDDI and in SONET/SDH. Each station on the ring is designed such that packets not addressed to it pass in transit without being switched. RPR can be synchronized with a stratum-1 8 kHz clock thus supporting SONET ring applications; RPR can be mapped in one or more OC-3s of an OC-12 or OC-192 allowing for TDM payloads to be mapped in the remaining payload envelop capacity. Thus, RPR supports real-time traffic as well.

The RPR ring serves as a shared medium. Both rings transport traffic with different priority; during failures, the lowest priority traffic is dropped first to avoid congestion. Each node on the ring has visibility on ring capacity and it shares bandwidth according to a fairness algorithm, which is built in the RPR protocol.

RPR requires 50 ms protection switching, which is compatible with SONET/SDH. Protection is accomplished with steering all traffic to the other ring, or wrapping traffic (also known as looping back) at the nodes which are adjacent to the failed link. The network architecture of a RPR ring is shown in Fig. 2.33.

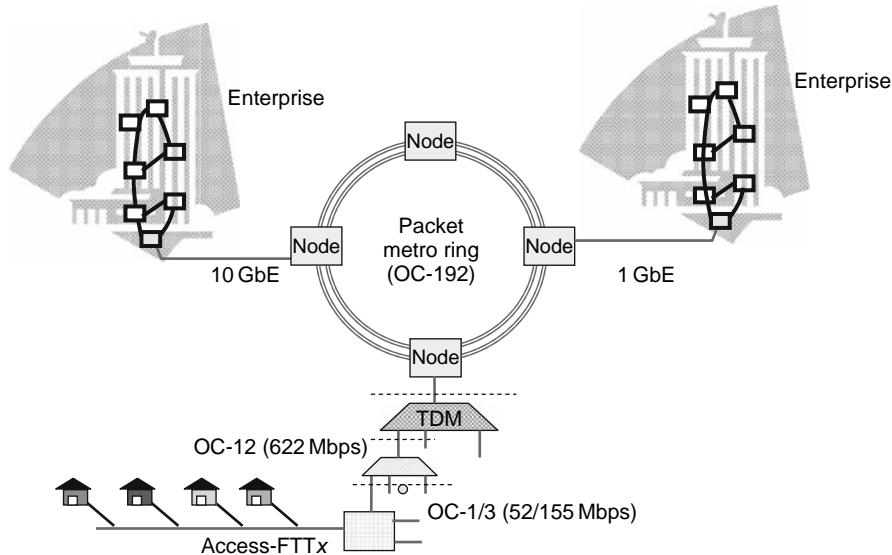


Fig. 2.33 A resilient packet ring network architecture. Nodes on the ring are capable of passing through transit traffic that is destined to another node

References

1. S.V. Kartalopoulos, *Understanding SONET/SDH and ATM*, IEEE-Press/Wiley, Piscataway, NJ, 1999 (Section II contains an extensive bibliography on SONET and SDH).
2. Telcordia (previously Bellcore), GR-253-CORE, Issue 2, “Synchronous Optical Network (SONET) Transport Systems, Common Generic Criteria”, 1992.
3. American National Standard for Telecommunications—Synchronous Optical Network (SONET): Physical Interface Specifications”, ANSI T1.106.06, 2000.
4. ANSI T1.102-1993, *Telecommunications—Digital Hierarchy—Electrical Interfaces*, 1993.
5. ANSI T1.107-1988, *Telecommunications—Digital Hierarchy—Formats Specifications*, 1988.
6. ANSI T1.105.01-1994, *Telecommunications—Synchronous Optical Network (SONET) — Automatic Protection Switching*, 1994.
7. ANSI T1.105.03-1994, *Telecommunications—Synchronous Optical Network (SONET)—Jitter at Network Interfaces*, 1994.
8. ANSI T1.105.04-1994, *Telecommunications—Synchronous optical network (SONET)—Data Communication Channel Protocols and Architectures*, 1994.
9. ANSI T1.105.05-1994, *Telecommunications—Synchronous optical network (SONET)—Tandem Connection Maintenance*, 1994.
10. IETF RFC 2823, PPP over Simple Data Link (SDL) using SONET/SDH with ATM-like framing, May 2000.
11. ITU-T Recommendation G.707/Y1322, “Network Node Interface for the Synchronous Digital Hierarchy (SDH)”, October 2000.
12. ITU-T Recommendation G.783, “Characteristics of Synchronous Digital Hierarchy (SDH) Equipment Functional Blocks”, February 2001.
13. ITU-T Recommendation G.784, “Synchronous Digital Hierarchy (SDH) Management”, 1998.
14. ETSI European Standard EN 300 417-9-1 (currently ITU-T), “Transmission and Multiplexing: Generic Requirements of Transport Functionality of Equipment; Part 9: Synchronous Digital Hierarchy (SDH) Concatenated Path Layer Functions; Sub-part 1: Requirements”.
15. ITU-T Recommendation G.828, “Error Performance Parameters and Objectives for International, Constant Bit Rate Synchronous Digital Paths”, February 2000.
16. Telcordia (previously Bellcore), TA-NWT-1042, “Ring Information Model”, 1992.
17. Bellcore (currently Telcordia) GR-499-CORE, *Transport Systems Generic Requirements (TSGR): Common Requirements*, Issue 2, December 1998.
18. ITU-T Recommendation ITU-T G.823, “The Control of Jitter and Wander Within Digital Networks Which are Based on the 2048 kbit/s Hierarchy”, February 2000.

19. ITU-T Recommendation G.823, *The Control of Jitter and Wander Within Digital Networks Which are Based on the 2048 kbit/s Hierarchy*, March 2000.
20. ITU-T Recommendation G.828, *Error Performance Parameters and Objectives for International, Constant Bit Rate Synchronous Digital Paths*, March 2000.
21. ITU-T Recommendation G.828, *Error Performance Parameters and Objectives for International, Constant Bit Rate Synchronous Digital Paths*, Corrigendum 1, July 2001.
22. E. Rosen et al., *Multiprotocol Label Switching Architecture*, IETF RFC 3031, January 2001.
23. L. Berger et al., “Generalized MPLS—RSVP-TE Extensions”, IETF RFC 3473, January 2002.
24. P. Ashwood-Smith et al., “Generalized MPLS—CR-LDP Extensions”, IETF RFC 3472, January 2003.
25. L. Anderson et al., *LDP Specification*, IETF RFC 3036, January 2001.
26. J. van Bogaert, “E-MAN: Ethernet-Based Metropolitan Access Networks”, *Alcatel Telecommunications Reviews*, 1st Quarter, 2002, pp. 31–34.
27. IEEE 802.3ab, standard on 1000BaseT.
28. D.G. Cunningham and W.G. Lane, “*Gigabit Ethernet Networking*”, MacMillan Technical Publishing, 1999.
29. W. St. Arnaud, “1310 nm vs 1550 nm Window for 10GbE”, IEEE 10G Study Group, May 6, 1999 (http://www.grouper.ieee.org/groups/802/3/10G_study/email/msg00022.html).
30. R. Keenan, “Ethernet-over-SONET Gains Metro Ground”, Communications Design, June 7, 2002, (<http://www.commsdesign.com/story/OEG20020607S0051>).
31. IETF RFC 791, Internet protocol.
32. Telcordia (previously Bellcore), GR-1112-CORE, “Broadband ISDN UNI and NNI Physical Criteria Generic Criteria”, 1994.
33. Telcordia (previously Bellcore), GR-1110-CORE, “Broadband Switching System (BSS) Generic Requirements”, 1995.
34. Telcordia (previously Bellcore), GR-1111-CORE, “Broadband Access Signaling (BAS) Generic Requirements”, 1995.
35. R. Handel and M.N. Huber, “*Integrated Broadband Network*”, Addison Wesley, 1991.
36. N. Dagdeviren et al., “Global Networking with ISDN”, IEEE Communication Magazine, June 1994, pp. 26–32.
37. ITU-T Recommendation I.211, “*B-ISDN Service Aspects*”.
38. ITU-T Recommendation I.311, “*B-ISDN General Network Aspects*”.
39. ITU-T Recommendation I.321, “*B-ISDN Protocol Reference Model and its Application*”.
40. ITU-T Recommendation I.327, “*B-ISDN Network Functional Requirements*”.
41. ITU-T Recommendation I.371, “*Traffic Control and Congestion Control in B-ISDN*”.
42. ITU-T Recommendation I.413, “*B-ISDN User-Network Interface*”.
43. ITU-T Recommendation I.432, “*B-ISDN User-Network Interface—Physical Layer Specification*”.
44. ITU-T Recommendation I.580, “*General Arrangements for Interworking between B-ISDN and 64 kb/s based ISDN*”, December 1994.
45. ITU-T Recommendation I.610, “*OAM Principles of B-ISDN Access*”.
46. ITU-T Recommendation Q.931, “*ISDN UNI Layer 3 Specification for Basic Call Control*”, 1993.
47. ITU-T Recommendation I.432.1, “*Series I: Integrated Services Digital Network. ISDN User-Network Interfaces—Layer 1 Recommendations*”, 1999.
48. IETF RFC 2823, *PPP over Simple Data Link (SDL) using SONET/SDH with ATM-like framing*, May 2000.
49. M.W. Sachs, “Fibre Channel” in *High-Performance Networks: Technology and Protocols*, A.N. Tantawy, ed. Kluwer, Boston, 1994, pp. 109–129.
50. A.F. Benner, *Fibre Channel*, McGraw-Hill, New York, 1996.
51. FC-PH ANSI X3.230-1994, “Fibre Channel—Physical and Signaling Interface”.
52. FC-PH-2 ANSI X3.297-1997, “Fibre Channel—Physical and Signaling Interface-2”.
53. FC-PH-3 Project 1119-D, “Fibre Channel—Physical and Signaling Interface-3”.
54. FC-AL ANSI X3.272-1996, “Fibre Channel—Arbitrated Loop”.
55. FC-LE ANSI X3.287-1996, “Fibre Channel—Link Encapsulation”.
56. FC-FP ANSI X3.254-1994, “Fibre Channel—Mapping to HIPPI-FC”.
57. FC-SB ANSI X3.271-1996, “Fibre Channel Single Byte Command Code Sets (SBCCS) Mapping Protocol”.
58. FC-GS ANSI X3.288-1996, “Fibre Channel—Generic Services”.
59. FC-FG ANSI X3.289-1996, “Fibre Channel—Fabric Generic Requirements”.
60. IBM International Technical Support Org., “*FICON Native Implementation and Reference Guide*”, October 2002.
61. A.X. Widmer and P.A. Franaszek, “A DC-Balanced Partitioned-Block, 8B/10B Transmission Code”, *IBM Journal Research and Development*, vol. 27, no. 5, September 1983, pp. 440–451.
62. J.C. Elliot and M.W. Sachs, “The IBM Enterprise Systems Connection (ESCON) Architecture”, *IBM Journal Research and Development*, vol. 36, no. 4, September 1992, pp. 577–591.
63. IBM International Technical Support Org., “*Enterprise System Connection (ESCON) Implementation Guide*”, July 1996.

Chapter 3

WDM Technology and Networks

3.1 Introduction

The optical components that were initially used for scientific and commercial purposes were based on naturally found transparent crystals, and artificially made from them lens and mirrors. Ancient mathematicians, geometers, and astronomers like Apollonios of Perga (third century BCE), Diocles of Carystos (third century BCE), Eudoxos of Cnidos (fifth to fourth century BCE), Hipparchos of Nicaea (second century BCE), Zenodoros of Athens (third to second century BCE) studied the propagation and reflectivity of light and developed the theory of spherics: conics, parabolas, and hyperbolas; they discovered the focusing imperfection of spherical mirrors and corrected them with transmission media based on glass.

Glass-based fiber has been so fantastic, as compared with copper and electromagnetic waves, that currently it is the only medium considered for ultrafast and ultrahigh bandwidth [1, 2]. Optical components that have been deployed in wavelength divisions multiplexing (WDM) optical communications systems are based on artificially and highly sophisticated components that provide well-known functionality [3, 4]. Among such functionality is optical multiplexing and demultiplexing, sourcing (lasers), receiving (photodetectors), filtering, modulation, optical amplification (EDFA, Raman), dispersion compensation, equalization, add-drop multiplexing, cross-connecting, coupling, and so on [5], Fig. 3.1. The working optical frequencies used in DWDM communications are in the spectral range of $0.8\text{--}1.6 \mu\text{m}$. Thus, optical communication components are transparent to these frequencies, with the lowest attenuation and with negligible non-linear undesirable effects. Additionally, optical communication components need to be at optimal cost-efficiency and performance and have small volumetric dimensions, many of which are already in the *micrometer* or smaller. Among the critical components in optical communications is the transmission medium, the glassy fiber.

3.2 The Optical Fiber in Communications

The propagations of light in transparent dielectric material have been studied for centuries. However, it is in the last few decades that propagation of light in a glassy fiber thinner than the human hair has found a widespread applicability in communications as well as in the medical field. In particular, it is optical communications that has driven fiber technology to a supreme state that in the last decade or so, fiber has wrapped the world many times over connecting each continent and each country under water and over land. Without this fiber-optic optical network, the communication services offered today and those that will be offered tomorrow will not be possible.

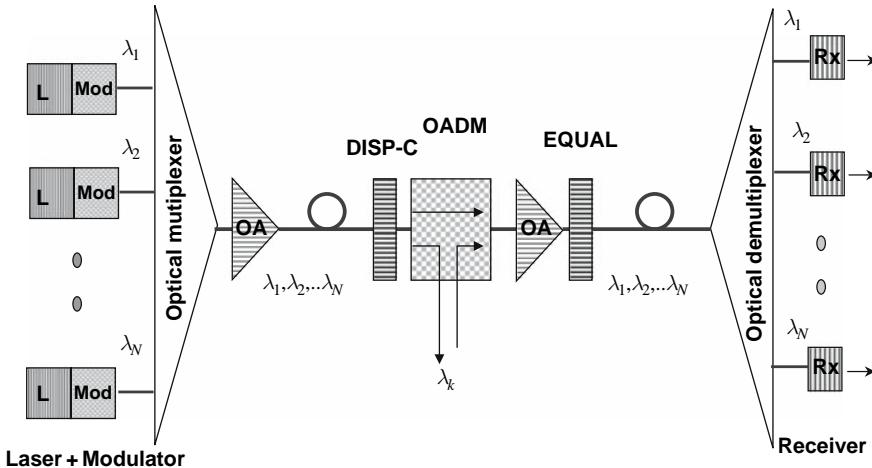


Fig. 3.1 A broad range of optical components has made possible DWDM networks to transport several terabits per second

It is known that light travels in a straight path when in free space. However, when it travels in fiber, it follows its curves and loops for many kilometers, therefore, it is of interest to examine the glassy medium and how light travels in it.

3.2.1 Propagation of Light in Matter

When light travels within a dielectric transparent matter, it travels at a velocity that depends on the dielectric constant of matter and its wavelength. In general, the propagation of a monochromatic plane wave within a dielectric matter in the direction z is described by

$$E(t, z) = A e^{[j(\omega t - \beta z)]},$$

where A is the amplitude of the field, $\omega = 2\pi f$, and β is the *propagation constant*.

Phase velocity, v_ϕ , is defined as the velocity of an observer that maintains constant phase with the traveling field, that is, $\omega t - \beta x = \text{constant}$. Replacing the traveled distance x within time t , $x = v_\phi t$, then the phase velocity of the monochromatic light in the medium is $v_\phi = \omega/\beta$. In reality, the dielectric constant of matter is a function of frequency. Consequently, within dielectric matter, different optical frequencies propagate at different velocities. This is important because in optical communications, the actual optical signal is not purely monochromatic but it consists of a band of frequencies. Thus, each frequency in the band travels at a slightly different velocity and different phase. In this case, *group velocity*, $v_g = c/n_g$, is defined as the velocity of an observer that maintains constant phase with the group-traveling envelope of the frequencies in the band, that is, $\omega t - (\Delta\beta)x = \text{constant}$, from which $v_g = \omega/\Delta\beta = \partial\omega/\partial\beta = 1/\beta'$, where β is the propagation constant and β' is the first partial derivative with respect to ω (because the optical signal is not purely monochromatic, the derivative with respect to ω is not zero). The dependency of dielectric constant, and thus refractive index, of optically dielectric matter causes some interesting effects, many of which are to the detriment of photon propagation in matter. Optical fiber consists of dielectric matter.

Additionally, matter is not pure, but it includes impurities that scatter or absorb photons. Both absorption and scattering have a net effect of optical power loss, which along with other effects put a limit to the link length between the transmitter-receiver; the amount of light that reaches the

photodetector must match the photodetector sensitivity in order to be detected reliably [3–6]. However, absorption may also be advantageous in optical amplification, erbium-doped fiber amplifiers (EDFA), and Raman-type amplifiers. Photon scattering centers within matter is known as *Rayleigh scattering*.

Other influences that affect the propagation of light in fiber and contribute to optical loss are *temperature* variations along the fiber, mechanical *stress*, and material *non-linearity*. To counterbalance these effects, geometry, fiber consistency, and strength of fiber cable play a critical role, and this is one of the main reasons for having different types of fibers.

3.2.2 Effects That Affect the Propagation of Light in Fiber

Two relations describe the propagation of electromagnetic waves in nonconducting media:

$$E(r, t) = \varepsilon_1 E_0 e^{-j(\omega t - k \cdot r)} \text{ and} \\ H(r, t) = \varepsilon_2 H_0 e^{-j(\omega t - k \cdot r)},$$

where ε_1 and ε_2 are two constant unit vectors that define the direction of each field, \mathbf{k} is the unit vector in the direction of propagation \mathbf{r} , and E_0 and H_0 are complex amplitudes, which are constant in space and time.

Electromagnetic waves that propagate in dielectric medium without charges have a zero field gradient, that is, $(\text{del})\mathbf{E} = 0$ and $(\text{del})\mathbf{H} = 0$. Based on this, the product of unit vectors is $\varepsilon_1 \cdot \mathbf{k} = 0$ and $\varepsilon_2 \cdot \mathbf{k} = 0$. That is, the electric (\mathbf{E}) and the magnetic (\mathbf{H}) fields are perpendicular to the direction of propagation \mathbf{k} . Such a wave is called a *transverse wave*.

3.2.2.1 Attenuation or Power Loss

When an electromagnetic wave propagates in dielectric matter, an interaction between the fields of the wave and the distributed fields in matter takes place. From this interaction, some energy exchange takes place, which in most cases is at the expense of the propagating wave. In addition, matter is not perfectly organized, but there are centers of discontinuity due to nonhomogeneity, as well as foreign atoms in it that absorb or scatter the wave. Metals, rare earth elements, and compounds absorb specific frequencies. For example, OH – radicals absorb light about $1.4 \mu\text{m}$, and erbium atoms absorb 980 and 1,480 nm.

The net result is that when light propagates in dielectric such as fiber, it suffers power loss or *attenuation*. Because the probability of being attenuated is commensurate with the distance traveled within the dielectric, an *attenuation constant* is defined, which for fiber is expressed in decibel per kilometer. ITU-T G.652 recommends a loss below 0.5 dB/km in the region 1,310 nm, and below 0.4 dB/km in the region 1,500 nm.

In optical communications, the term *fiber loss* is often used indistinguishably with power attenuation. Fiber loss, for a given optical power, $P(0)$, launched into fiber affects the total power arrived at the receiver, P_r . Based on this, fiber loss limits the fiber span, L_{\max} , without amplification, and/or determines the required amplification gain.

However, the attenuation constant or fiber loss is not the same for all frequencies. For an attenuation constant $\alpha(\lambda)$, the optical power attenuation at a length L is expressed as

$$P(L) = P(0)10^{-\alpha(\lambda)L/10}.$$

If we replace $P(L)$ with the minimum acceptable power at the receiver, P_r , then the (ideal) maximum fiber length is determined by

$$L_{\max} = [10/\alpha(\lambda)] \log_{10}[P(0)/P_r].$$

In general, the optical power attenuation constant, $\alpha(\lambda)$ is non-linear:

$$\alpha(\lambda) = C_1/(\lambda)^4 + C_2 + A(\lambda),$$

where C_1 is a constant (due to Rayleigh scattering), C_2 is a constant due to fiber imperfections, and $A(\lambda)$ is a function that describes fiber-impurity absorption as a function of wavelength.

The optical power attenuation constant of silica fiber (measured in dB/km) is typically plotted as a function of the wavelength, Fig. 3.2.

Standard single-mode fiber has two low attenuation ranges, one at about 1.3 μm and another at about 1.55 μm. Between these two ranges, and at about 1.4 nm, there is a high attenuation range (1,350–1450 nm), due to the OH – radical with a peak at 1,385 nm.

3.2.2.2 Insertion Loss

Insertion loss (IL) is related to the optical power lost when an optical signal passes through a component, and it is expressed by the ratio power-in to power-out and it is measured in decibel, $IL = -10 \log(P_{in}/P_{out})$, where the signal power is in milliwatts. As the signal passes through several components, IL of each component is additive.

3.2.2.3 Component Isolation

Component isolation is the degree of transmitted power through a component in one direction compared with the power returned in the opposite direction. The desirable value of isolation is near infinity (or zero power returned through the component).

3.2.2.4 Channel Isolation

In dense wavelength division multiplexing, optical channels are spectrally, closely located. To minimize cross-talk due to frequency drifting, channels are required to be spectrally separated. This is known as *channel isolation* or *channel separation*.

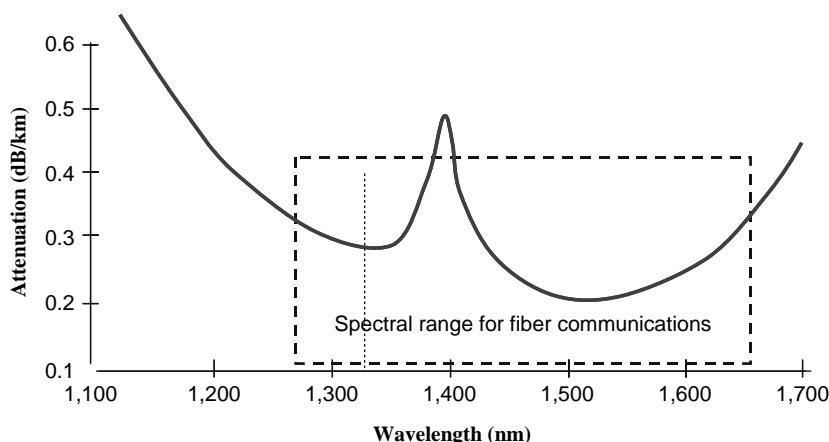


Fig. 3.2 Attenuation of silica fiber over the communications spectrum

3.2.2.5 Polarization of Matter

The electrical state of matter on a microscopic level consists of charges, the distribution of which depends on the presence or absence of external fields. If for every positive charge there is a negative charge, then the positive-negative pairs constitute electric dipoles. For a distribution of electric dipoles, *the electric dipole moment per unit volume is defined as the polarization vector \mathbf{P}* . The dielectric constant and refractive index of matter depend on the polarization vector. In fact, some materials (such as crystals) have different refractive index in different directions that coincide with the crystallographic axes of the material [3–7].

3.2.2.6 Polarization of Light

As light propagates through a medium, it enters the fields of dipoles, and field interaction takes place. Interaction in certain directions affects the strength of field of light differently so that the end result may be a complex field with an elliptical or a linear field distribution as seen on a plane perpendicular to the direction of propagation. Thus, the electric field \mathbf{E} becomes the linear combination of the components in the x and y Cartesian coordinates, \mathbf{E}_{ox} and \mathbf{E}_{oy} , so that,

$$\mathbf{E}(r, t) = (\epsilon_x \mathbf{E}_{ox} + \epsilon_y \mathbf{E}_{oy}) e^{-j(\omega t - \mathbf{k} \cdot \mathbf{r})}.$$

The latter relationship implies that the two components, E_{ox} and E_{oy} , vary sinusoidally; they are perpendicular to each other, and there is a phase between them, ϕ . In this case, the dielectric quantity ϵ is described by a tensor that, in general, has different values in the three axes x , y , and z :

$$\boldsymbol{\epsilon} = \begin{vmatrix} \epsilon_x & 0 & 0 \\ 0 & \epsilon_y & 0 \\ 0 & 0 & \epsilon_z \end{vmatrix} = \epsilon_o \begin{vmatrix} n_x^2 & 0 & 0 \\ 0 & n_y^2 & 0 \\ 0 & 0 & n_z^2 \end{vmatrix}$$

Now, from $(\text{del})^2 \mathbf{E} = (1/v^2)(\partial^2 E / \partial t^2)$ and $\mathbf{E}(r, t) = \boldsymbol{\epsilon} \mathbf{E}_o e^{-j(\omega t - \mathbf{k} \cdot \mathbf{r})}$, the following is obtained

$$\mathbf{k} \times (\mathbf{k} \times \mathbf{E}_o) + \mu_0 \boldsymbol{\epsilon} \omega^2 \mathbf{E}_o^2 = 0 \text{ or : } [\mathbf{k} \times (\mathbf{k} \times \mathbf{I}) + \mu_0 \boldsymbol{\epsilon} \omega^2] [\mathbf{E}_o] = 0,$$

where \mathbf{I} is the identity matrix. The latter is a vector equation equivalent to a set of three homogeneous linear equations with unknown components of \mathbf{E}_o , \mathbf{E}_{ox} , \mathbf{E}_{oy} , and \mathbf{E}_{oz} . In a typical case, the component \mathbf{E}_{oz} along the axis of propagation is equal to zero. This vector equation determines the relationship between the vector \mathbf{k} (k_x , k_y , k_z), the angular frequency ω , and the dielectric constant $\boldsymbol{\epsilon}$ (ϵ_x , ϵ_y , ϵ_z), as well as the polarization state of the plane wave.

The term $[\mathbf{k} \times (\mathbf{k} \times \mathbf{I}) + \mu_0 \boldsymbol{\epsilon} \omega^2]$ describes a three-dimensional surface of the field. As the electric field is separated into its constituent components, each component may propagate in the medium at a different phase. The phase relationship as well as the magnitude of each vector defines the *mode of polarization*:

- If \mathbf{E}_{ox} and \mathbf{E}_{oy} have the same magnitude and are in phase, then the wave is called *linearly polarized*.
- If \mathbf{E}_{ox} and \mathbf{E}_{oy} have a phase difference (other than 90°), then the wave is called *elliptically polarized*.
- If \mathbf{E}_{ox} and \mathbf{E}_{oy} have the same magnitude, but differ in phase by 90° , then the wave is called *circularly polarized*.

Example: The wave equation of circularly polarized is $E(r, t) = E_o(\varepsilon_x \pm j\varepsilon_y)e^{-j(\omega t - \mathbf{k} \cdot \mathbf{r})}$. Then, the two real components in the x and in the y direction are

$$E_x(r, t) = E_o \cos(\mathbf{k} \cdot \mathbf{r} - \omega t) \text{ and } E_y(r, t) = \pm E_o \cos(\mathbf{k} \cdot \mathbf{r} - \omega t).$$

These equations indicate that at a fixed point in space the fields are such that the electric vector is constant in magnitude and it rotates in a circular motion at a frequency ω . The term $\varepsilon_x + j\varepsilon_y$ denotes counterclockwise rotation (facing the oncoming wave), and the wave is called *left circularly polarized* or with *positive helicity*. Similarly, the term $\varepsilon_x - j\varepsilon_y$ denotes clockwise rotation and the wave is called *right circularly polarized* or with *negative helicity*. Thus, $E(r, t) = (\varepsilon_+ \mathbf{E}_+ + \varepsilon_- \mathbf{E}_-)e^{-j(\omega t - \mathbf{k} \cdot \mathbf{r})}$, where \mathbf{E}_+ and \mathbf{E}_- are complex amplitudes denoting the direction of rotation, positive and negative, respectively.

- If \mathbf{E}_+ and \mathbf{E}_- are in-phase but have different amplitudes, the last relationship represents an *elliptically polarized* wave with principal axes of the ellipse in the directions ε_x and ε_y . Then, the ratio semimajor-to-semiminor axis is $(1+r)/(1-r)$, where $\mathbf{E}_-/\mathbf{E}_+ = r$.
- If the amplitudes \mathbf{E}_+ and \mathbf{E}_- have a difference between them, $\mathbf{E}_-/\mathbf{E}_+ = re^{j\alpha}$, then the ellipse traced out by the vector \mathbf{E} has its axes rotated by an angle $\phi/2$.
- If $\mathbf{E}_-/\mathbf{E}_+ = r = +/-1$, then the wave is *linearly polarized*.

Thus, the electric and the magnetic fields of monochromatic light are in quadrature and in time phase. When created light propagates in free space, the two fields change sinusoidally and each one lies on one of two planes perpendicular to each other. When light enters matter, then depending on the displacement vector distribution in matter (and hence the dielectric and the refractive index), the electric and/or magnetic field of light interacts with it in different ways. In addition, light becomes polarized when it is reflected, refracted, or scattered. In polarization by reflection, the degree of polarization depends on the angle of incidence and on the refractive index of the material, given by the *Brewster's Law* $\tan(I_P) = n$, where n is the refractive index and I_P the polarizing angle.

3.2.2.7 Polarization-Dependent Loss (PDL)

As the optical signal travels through optically transparent matter, due to spatial polarization interaction it suffers selective power reduction or optical power loss in specific directions; this power loss due to local polarization influences is wavelength dependent and is known as *polarization-dependent loss* (PDL) and is measured in decibels (dB). At bit rates below 10 Gbps, PDL is a minor contributor to the total power loss. At 10 Gbps and above, PDL becomes equally important and its contribution may be 0.5 dB or more. This value does not change with respect to the center wavelength of the received signal. However, asymmetric spectral polarization loss causes asymmetric amplitude signal distortions and the signal may appear with shifted center wavelength.

3.2.2.8 Extinction Ratio (ER)

In general, when polarized light is traveling through a polarizer, the maximum transmittance, T_1 , is termed *major principal transmittance*, and the minimum, T_2 , is termed *minor principal transmittance*. The ratio major to minor is known as *principal transmittance*. The inverse, minimum to maximum is known as *extinction ratio*. Consider two polarizers in tandem, one behind the other with parallel surfaces. Then, if their polarization axes are parallel, the transmittance is $T_1^2/2$. If their axes are crossed (perpendicular), the transmittance is $2T_2/T_1$. This is also (but erroneously) termed as *extinction ratio*.

In optical communications, the term extinction ratio is defined slightly differently. It describes the modulation efficiency in the optical medium, considering that the source (laser) is always continuous

and it is externally ON–OFF modulated. In this case, the extinction ratio is defined as the ratio of the transmitted optical power of a logic 1 (ON), P_1 , over the transmitted optical power of a logic 0, P_0 , and it is measured in decibels.

$$ER = 10 \times \log(P_1/P_0)(dB) \text{ or } ER = (P_1/P_0) \times 100(\%)$$

3.2.2.9 Phase Shift

When a wave propagates in optically transparent matter or in space with dielectric constant ε_0 and it enters an optically transparent matter with dielectric constant ε_1 (and refractive index n_1), its velocity slows down (if $\varepsilon_1 > \varepsilon_0$) or speeds up (if $\varepsilon_1 < \varepsilon_0$). As a result of this, a phase difference is created between the original wave in matter with ε_0 and that in matter ε_1 . The amount of phase shift $\Delta\phi$ depends on the wavelength λ , the dielectric constant difference, $\Delta\varepsilon$, and the optical path (thickness) of material with ε_1 .

3.2.2.10 Birefringence

Anisotropic material has different refractive index in specific directions. Thus, when a beam of monochromatic unpolarized light enters the material in a specific angle and travels through it, it is refracted differently in the directions of different indices; materials with two dominant refractive indices, one called *ordinary index*, n_0 , and the other *extraordinary index*, n_e , are known as *birefringent*. Thus, when unpolarized ray enters birefringent material, it is separated into two rays, each with different polarization, different direction, and different propagation constant—one called *ordinary* (O) and the other *extraordinary* (E). The property of such crystals is known as *birefringence*. Birefringence in fiber alters the polarization state of the propagating optical signal and it is undesirable. In general, all optically transparent crystals have some degree of birefringence (some more than others), unless they belong to the cubic system or they are amorphous.

Some birefringent crystals are the following:

- Calcite (CaCO_3) has $n_e = 1.477$ and $n_0 = 1.644$ at 1,500 nm. Calcite has a spectral transmission range of 0.2–3.2 μm .
- Quartz (SiO_2) has $n_e = 1.537$ and $n_0 = 1.529$ at 1,500 nm. Quartz is used. Quartz has a spectral transmission range of 0.2–2.6 μm .
- Titanium dioxide (rutile) has an index of birefringence $n_0 - n_e = 0.27$. The spectral transmission is in the range of 0.45–6.2 μm .

Several steps can be made to minimize fiber birefringence:

- minimize geometry imperfections;
- minimize variations in the refractive index;
- minimize residual birefringence;
- “immunize” the system from fiber polarization variations, using *polarization spreading* (polarization scrambling, data-induced polarization), or *polarization diversity*;
- careful handling as mechanical stress, compression, or twist induces birefringence.

3.2.2.11 Dispersion

The refractive index of matter is related to the dielectric coefficient and to the characteristic resonance frequency of its dipoles. Thus, the closer to their resonance frequency the stronger the photon interaction and absorption is. Consequently, the refractive index $n(\omega)$ depends on the optical frequency, ω . This dependency is termed *chromatic dispersion*.

Silica, a key dielectric ingredient of optical fiber cable, has a refractive index that varies with optical frequency, and therefore, dispersion is a serious issue in optical communications and therefore is treated in more detail in a subsequent section.

3.2.2.12 Electro-optic Effect

Electro-optic effect refers to the variation of material optical properties when an electric field is applied to it. When matter is within an electric field, the latter influences its electron distribution in atoms or molecules, it influences the crystal structure and thus the refractive index distribution and optical properties. For example, the application of an electric field may cause an isotropic crystal (e.g., GaAs) to become non-isotropic (birefringent). In general, the refractive index n^* (after a field is applied) is a function of the applied electric field and it may be expanded in a series, $n^* = n + a_1 E^1 + [a_2 E^2 + \dots]$.

There are two types of electro-optic effects: the Pockel's effect and the Kerr effect.

The Pockel is applicable to matter for which $\Delta n = n^* - n = a_1 E$. However, the coefficient a_1 is not nonzero for all materials. It is zero ($a_1 = 0$) for all liquids and non-crystals, as well as for all crystals with a symmetric structure; glass and NaCl have no Pockel's effect but GaAs, LiNbO₃, and KDP (KH₂PO₄–potassium dihydrogen phosphate) have.

The Kerr is applicable to matter for which $\Delta n = n^* - n = a_2 E^2 = (\lambda K) E^2$, where K is the Kerr coefficient, measured in m/V^2 , and it depends on wavelength. In contrast to Pockel's effect, the Kerr effect is applicable to all materials (all have $a_2 \neq 0$) including glass. However, the Kerr effect is a second-order phenomenon and therefore it requires a strong applied field. Because certain crystals exhibit a Kerr effect with a response time in the order of picoseconds or less, the Kerr effect is suitable for ultrafast modulation at bit rates exceeding 10 Gbps.

3.2.2.13 Four-Wave Mixing

Four-wave mixing (FWM) is the product of interaction and energy exchange between several closely spaced optical frequencies and the nonlinearity of dielectric matter [8–10]. The product of this interaction is a new frequency (or wavelength). Typically, three wavelengths will interact with the nonlinear dielectric to produce a fourth wavelength, and hence *four-wave mixing* (FWM), Fig. 3.3.

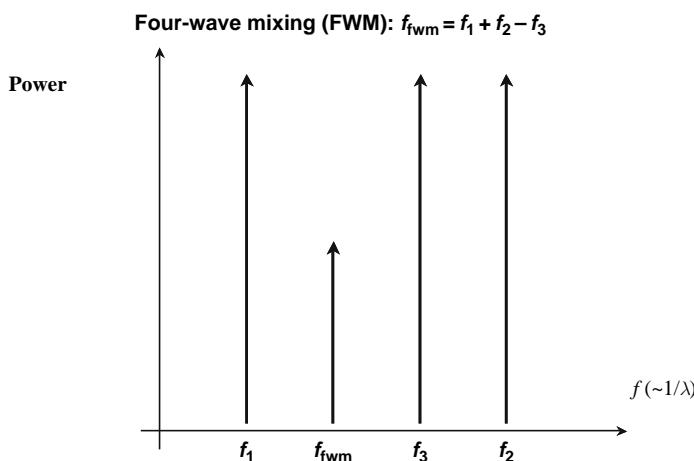


Fig. 3.3 Principles of four-wave mixing

In optical communications, FWM has been used advantageously, although in optical propagation, FWM adds to the noise content of optical channels.

Example 1: We want to convert a modulated wavelength λ_1 to another wavelength, λ_2 . Then λ_1 and two continuous (unmodulated) wavelengths are selected at a power that produces maximum FWM. All three are injected in a highly nonlinear dielectric device. The product of FWM is the fourth wavelength, λ_2 , which is modulated as the λ_1 . A passband filter rejects all but the newly created wavelength, λ_2 .

Example 2: In DWDM, three modulated wavelengths (optical channels) interact with the nonlinearity of fiber and produce a fourth wavelength. However, data on the three modulated wavelengths is not correlated and thus the fourth wavelength represents noise which is superimposed on an optical channel with the same wavelength.

3.3 The Optical Communications Spectrum

The electromagnetic spectrum that is used in fiber-optic communications has two bands. One band is in the 800–900 nm range and the other in the 1,280–1,640 nm range.

The first band has been applied in short-haul applications, local area networks, and Metro networks that have used multimode fiber (see next section for fiber types) because it is these frequencies that originally VCSEL (vertical cavity surface emitting lasers) laser sources generated [11]; VCSELs are much more inexpensive light sources than laser sources (DFB, Fabry–Perrot) that are used in long haul. However, recently VCSELs have been made to operate in the 1,550 nm range.

The range 1,280–1,640 nm is more attractive to optical networks with either single-mode or multimode silica fiber. Silica fiber today is the fiber of choice, and there are several contributing factors that favor this spectral range for silica fiber:

- Silica is a ubiquitous material with which fiber can be inexpensively manufactured, if we consider cost per bit transferred.
- Silica fiber meets optical and mechanical characteristics required by optical networks.
- This range has the lowest attenuation of silica fiber, Fig. 3.2.
- This range is suitable for optical fiber amplifiers, Fig. 3.4.
- This range is suitable for Raman amplification.
- This range has least dispersion.

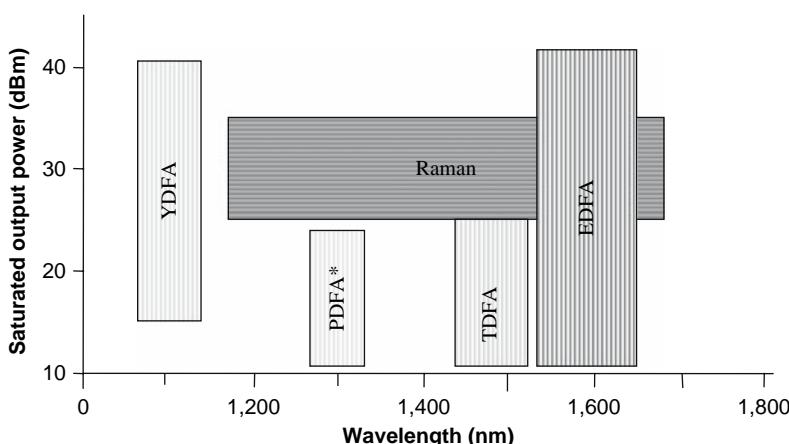


Fig. 3.4 Amplifier technologies over the optical communications spectrum

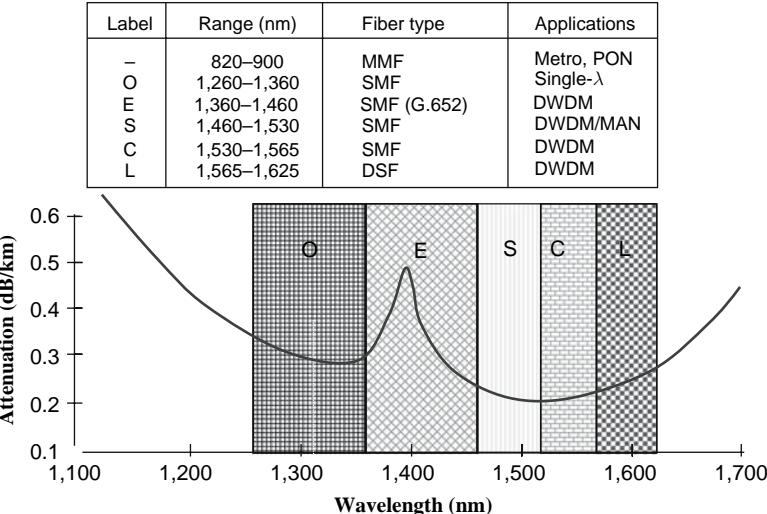


Fig. 3.5 DWDM bands over the optical communications spectrum

This spectral range is subdivided in bands, Fig. 3.5. The C band and the L band are mostly used in long-haul optical networks and the specific frequencies to be used, known as the channel grid, Fig. 3.6. Currently, there are two prevalent standards: the dense wavelength division multiplexing (DWDM) and the coarse wavelength division multiplexing (CWDM).

DWDM is defined over a grid of frequencies with 25, 50, 100, and 200 Ghz channel separation [12]. The reference frequency point is 196.10 Thz (or 1,528.77 nm) to which $n \times 50$ Ghz ($n = 1, 2, \dots$) are added or subtracted to generate the grid. Currently, the C and L bands are used with as many as 320 optical channels but theoretically the complete spectrum can be used to as many as 1,000 channels. DWDM is defined for applications where high performance, high data rate, and long distances are important, such as Metro, backbones, long-haul point-to-point, undersea connectivity, and so on.

CWDM is defined over a grid of 18 frequencies, from 1,280 to 1,640 nm with 20 nm separation, Fig. 3.7 [13]. CWDM is defined for applications where low cost and shorter distances are important, such as optical LANs and fiber to the home.

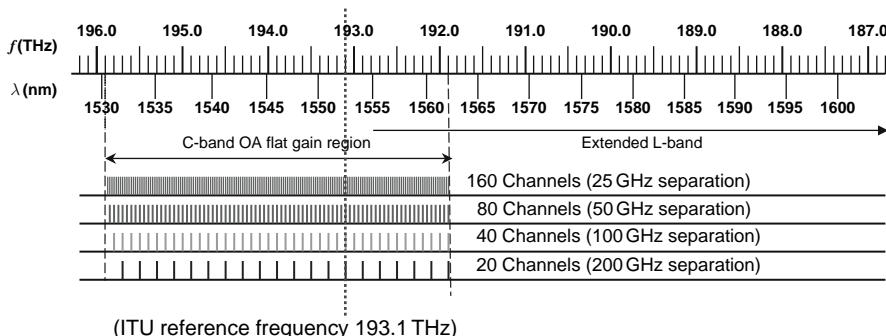


Fig. 3.6 The DWDM grid over the C-band

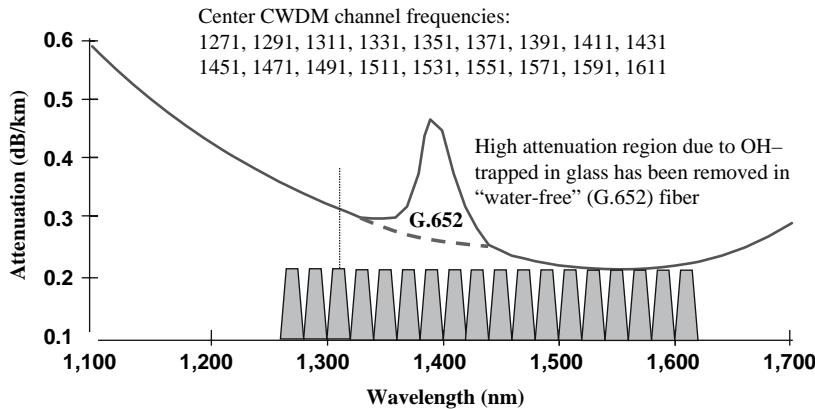


Fig. 3.7 CWDM grid over the optical communications spectrum

3.4 Types of Fiber

A fiber-strand consists of ultrapure silica glass SiO_2 (70–95 wt %) mixed with specific elements, known as *dopants*, such as germanium, fluorine, phosphorus, and boron. Dopants are added to adjust the refractive index of fiber and the propagation characteristics. Glass fiber is so pure that it attenuates light as little as 0.35 dB per km at 1,310 nm, or 0.25 dB at 1,550 nm.

The typical transmission fiber consists of two concentric layers, the core and the surrounding cladding, both made of silica but with different dopants and thus different refractive index. The refractive index of the cladding is always less than the core; it is the core in which optical information flows. Light escaping into the cladding layer is typically lost. However, when photons are coupled correctly onto the core, the cladding will reflect back into the core all photons that reach the core-cladding interface.

Cladding is surrounded by other materials (plastic, coloring, etc.) for added strength, protection, and type identification.

There are two core configurations: a core of diameter 50 μm (also a 62.5 μm is in use) and 9 μm diameter. In either case, the added cladding increases the diameter to a total of 125 μm , Fig. 3.8. The 50 μm core supports many modes of transmission as optical rays may be reflected by the core-cladding interface at different angles, hence *multimode fiber* (MMF). Conversely, the 9 μm core supports one mode of transmission, along the axis of the fiber, hence *single-mode fiber* (SMF) [14].

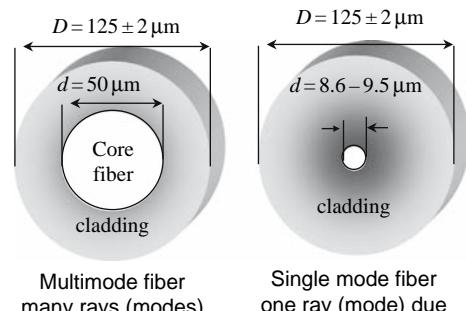


Fig. 3.8 Cross-section of multimode and single-mode fiber

Multimode fiber
many rays (modes)
may propagate

Single mode fiber
one ray (mode) due
to small d propagates

The fiber as a dielectric guided medium puts a limit on the number of modes, M . The number of modes a fiber supports depends on fiber geometry (core diameter), the refractive index of core and cladding, and the wavelength of the optical signal. These parameters are combined in a normalized parameter known as the M number, expressed by $M = 1/2\{(4\pi/\lambda)d\sqrt{(n_{\text{clad}}^2 - n_{\text{core}}^2)}\}^2$, where λ is the wavelength and d is the core diameter. Notice that a fiber supports fewer modes at shorter frequencies and more modes at higher frequencies. The square root factor is known as the *numerical aperture* of the step index fiber, $\text{NA} = \sqrt{(n_{\text{clad}}^2 - n_{\text{core}}^2)}$.

In addition to fibers been classified in MMF and SMF, single-mode fibers are further classified according to dispersion characteristics, such as dispersion shifted fiber (DSF), nonzero dispersion shifted fiber (NZDSF), and others that are known by a commercial name [15]. Among them, is a fiber type that is free from OH – and thus it exhibits flat and low loss at about 1,400 nm. This fiber is known as *water-free fiber* and it has been specifically made for CWDM applications so that the total optical communications range can be used by the CWDM grid.

The refractive index of the core of the single-mode fiber is complex; it is manipulated during the manufacturing process to optimize the light propagation characteristics. This is accomplished by controlling the chemical deposition of dopants in a specific radial distribution in the core. Table 3.1 lists some refractive indices for illustrative purposes.

3.4.1 Optical Power Limit

The *maximum acceptable optical power density* is the amount of optical power that a fiber can support without being damaged. *Power density* is the ratio of laser beam power over the cross-sectional area of the laser beam. Because the cross-sectional area is very small, low laser power may result in large density. For example, a 10 mW power beam lunched onto a 9 μm diameter core (assuming uniformity) produces a power density (P/A):

$$P/A = 10 \times 10^{-3}/\pi(4.5 \times 10^{-4})^2 \text{ W/cm}^2 = 10 \times 10^{-3}/63.58 \times 10^{-8} = 15.7 \text{ kW/cm}^2$$

In optical communications, the signal is modulated in pulses and thus the optical power is not continuous. A pulse has duration (in ps or ns) and energy per pulse measured in millijoules. In this case, to calculate the power density of the pulse, the energy over time is first converted in power and then in power density. Thus, a pulse of 1 mJ for 1 ns is equivalent to $P = 1 \times 10^{-3}/10^{-9} \text{ J/s} = 1 \text{ mW}$.

Table 3.1 Refractive index of certain materials

Material	Refractive index
Ge	4.02
Si	3.43
GaAs	3.31
CdTe	2.70
SiO_2 (0.8 wt.% F)	1.65
CaF_2	1.56
KBr	1.53
BaF_2	1.47
GeO_2 (at 2 mol%)	1.46
P_2O_5 (at 2 mol%)	1.46
B_2O_3 (at 8 mol%)	1.46
Fused silica	1.41
MgF_2	1.37

3.4.2 Fiber Birefringence

The ideal single-mode fiber is supposed not to exhibit birefringence. However, pragmatic fibers have a small amount of birefringence which is provided by the manufacturer. Thus, if n_x and n_y are the indices for the dielectric fiber in the x - and y -axis (z is the axis of propagation), then the *degree of fiber birefringence* is defined by

$$B = |n_x - n_y|$$

Fiber birefringence causes power exchange between the two polarization states in an evolutionary manner. In optical communications, where optical coherency or the state of polarization needs to be conserved, then birefringence may be of concern. Similarly, at data rates greater than 10 Gbps, polarization-dependent loss (PDL) due to birefringence also becomes an issue.

Birefringence is difficult to combat; depending on application, a *polarization-preserving fiber* (PPF) may be used; this is a specialty fiber that exhibits very strong birefringence ($B \sim 10^{-4}$). Thus, when a signal enters the PPF, the birefringence induced by the fiber is so strong that it “overshadows” other sources of birefringence, which by comparison is negligible.

3.4.3 Fiber Dispersion

The propagation fiber in optical communication networks consists of dielectric material, exhibits birefringence, and has a defined long cylindrical shape. All three, dielectric, birefringence, and shape contribute in their own way to signal dispersion. The net effect is that a narrow pulse becomes wider. In ultrahigh data rates with sub-nanosecond bit periods, *pulse widening* degrades the signal quality and channel performance.

3.4.3.1 Modal Dispersion

For simplicity, consider a purely monochromatic optical signal as a bundle of rays. The bundle of rays is launched onto a fiber within a small cone. Thus, if the fiber core is wide enough, then each ray in the cone will propagate along the fiber in a different zigzag path or different *mode*, some arriving at the end of the fiber later than others, and some never arriving as they have been refracted in the cladding. Because rays travel different distances, they arrive at the end of the fiber at different times and the net result is a wider pulse. This is known as *modal dispersion*; modal dispersion is particularly important in multimode fibers. Single-mode fibers support one mode, rays traveling along its axis, and hence single-mode fiber.

3.4.3.2 Chromatic Dispersion

In reality, the optical signal is not purely monochromatic, but it consists of a bundle of frequencies (or wavelengths). Because the dielectric constant (and hence the refractive index) are functions of optical frequency, each wavelength in the bundle does not propagate at the same speed. Thus, a short pulse (that consists of a bundle of frequencies) that travels along the fiber will be wider at the end of the fiber because each constituent wavelength in the bundle arrives at different times. This *pulse spread* is termed *chromatic dispersion*. Chromatic dispersion is measured in picoseconds per nanometer. Because chromatic dispersion is an evolutionary phenomenon, a *chromatic dispersion coefficient* (D) is defined which is measured in picoseconds per nanometer-kilometer (i.e., delay per wavelength variation and per fiber length). In terms of the coefficient D , chromatic dispersion is expressed as $\Delta\tau = |D|L\Delta\lambda$, where $\Delta\lambda$ is the optical spectral width of the signal (in nm units).

Because dispersion is not a linear phenomenon and because it depends on optical frequency, there is a certain frequency (or wavelength) for which dispersion becomes zero, and thus this is known as the *zero-dispersion wavelength*. Above this wavelength, dispersion is positive and below is negative. Thus, a conventional single-mode fiber with a core diameter of about 8.3 μm and an index of refraction variation of about 0.37% has a zero-dispersion wavelength at about 1.3 μm . A fiber with the zero-dispersion point shifted to 1,550 nm (1.55 μm) is called *dispersion-shifted fiber* (DSF). These fibers are compatible with optical amplifiers that perform best at around 1,550 nm and thus they are suitable in DWDM applications. A fiber with near-zero dispersion in the range from 1.3 to 1.55 μm is called *dispersion-flattened fiber* (DFF). To meet specific optical transmission requirements, a variety of specialty fibers have been engineered, such as the *dispersion-compensated fiber* (DCF), the *dispersion-flattened compensated fiber* (DFCF), the *dispersion-slope compensated fiber* (DSCF), the *dispersion-shift compensated fiber* (DSCF), the *non-zero-dispersion-shifted fiber* (NZDSF), and many others.

Chromatic dispersion is a serious concern in optical communications for all data rates. ITU-T Recommendations G.652 and G.653 [16, 17] elaborate on the characteristics and the *chromatic dispersion coefficient* (CDC), $D(\lambda)$. In general, negative dispersion causes shorter wavelengths to travel slower than longer wavelengths. To counterbalance chromatic dispersion, *dispersion compensation* entails alternating fiber having negative dispersion with fiber having positive dispersion.

3.4.3.3 Polarization Mode Dispersion

Fiber birefringence and core noncircularity cause optical signals to be separated in two orthogonally polarized signals, each traveling at different speed and phase. When the two polarized signals recombine, because of the variation in time of arrival, a pulse spreading occurs. This phenomenon is particularly noticeable in single-mode fiber at ultrahigh bit rates (above 2.5 Gbps), and it is known as *polarization mode dispersion* (PMD). PMD is measured in picoseconds [18].

The *polarization mode dispersion coefficient* is defined as the delay induced by polarization mode dispersion (in ps) divided by the square root of fiber length (ps/ $\sqrt{\text{km}}$) in which light travels. Typical polarization mode dispersion coefficient for single-mode fiber is less than 0.5 ps/ $\sqrt{\text{km}}$.

All three dispersion mechanisms (modal, chromatic, and PMD) contribute to a net effect of pulse widening in optical propagation, which puts a limit on link length. That is, the higher the bit rate, the shorter the distance an optical signal can travel in single-mode fiber in order to meet the expected performance. For example, assuming 0.1 ps PMD, the fiber distance at the expected performance for 2.5 Gbps can be 100 km, for 10 Gbps and for the same performance is 10 km, and for 40 Gbps, it is shorter than 1 km. Thus, in general dispersion, PMD plays a significant role in fiber-optic communications, and each mechanism is combated differently; among them, PMD by far is the most difficult and costly to combat.

3.4.3.4 Stokes Noise and Chromatic Jitter

In practice, neither the fiber core is perfect (the core cross-section varies nonuniformly along the z -axis between circular and elliptical) nor the optical channel is purely monochromatic. Therefore, as an optical channel propagates in the fiber, PMD is the unavoidable result of fiber core birefringence and channel non-monochromaticity. As the two orthogonal polarization states propagate, they experience polarization variability due to nonuniform fluctuation known as *Stokes noise* and due to optical channel wavelength content known as *chromatic jitter*. In this case, the contribution of the two effects is the sum of squares of each noise component (the Stokes-related and the jitter-related):

$$[d(\Delta\tau)/\Delta\tau]^2 = [d(\Delta S)/\Delta S]^2 + [d(\Delta\omega)/\Delta\omega]^2$$

where $\Delta\omega$ is the frequency variation, d is the differential operator, and ΔS is the polarization state variation at the output of the fiber. The inverse of the latter is also known as the “bandwidth efficiency factor” $\alpha = 1/d(\Delta S)$. The bandwidth efficiency factor is related to maximum signal to noise ratio (SNR) of the optical signal as $\text{SNR} \leq \alpha \Delta\tau \Delta\omega$. That is, given α , and measuring $\Delta\tau$ and $\Delta\omega$, the maximum possible SNR is calculated.

3.4.3.5 Fiber Polarization-Dependent Loss

Optically fiber, like all dielectric matter, exhibits polarization sensitivity. That is, certain polarized states as they travel in fiber are attenuated very little while others are attenuated more. This is known as fiber *polarization-dependent loss* (PDL), and it represents the peak-to-peak optical power variation measured in decibels (dB). Some linear polarizers have strong PDL (e.g., >30 dB), whereas SMF very little (<0.02 dB).

In DWDM, PDL becomes critical when the bit rate is greater than 10 Gbps, and the number of optical grid is dense, with a narrow linewidth, at or less than 0.05 nm at fullwidth half maximum (FWHM); such narrow linewidth becomes highly polarized. PDL degrades the signal quality and system link performance.

3.4.4 Non-linear Phenomena Cause Positive and Negative Effects

When light enters dielectric matter, photons interact with atoms. The response of any dielectric (such as glass fiber) to optical power is nonlinear; the behavior of dielectric to optical power is like a dipole. It is the dipole nature of dielectric that interacts harmonically with electromagnetic waves such as light. When the optical power is low, the oscillations are small and the photon-fiber system behavior is linear. However, when the optical power is large, then oscillations are strong and the photon-fiber system’s behavior is nonlinear.

Under certain circumstances, photons are absorbed and excite atoms to higher energy levels. Atoms in an excited state become metastable, that is, they remain at that level for a very short time, in the range of nanoseconds to microseconds. However, while in the excited state, certain photons may stimulate them to come down to their initial lower energy level by releasing energy, *photons* and/or *phonons* (acoustic quantum energy).

In addition, there are also photon–atom–photon interactions that result in some complex phenomena that are best described by quantum theory, and thus, we only provide a quantitative description. They are distinguished in *forward scattering* and in *backward scattering* (Raman and Brillouin scattering) as well as in *four-wave (or four-photon) mixing*. The direction (forward and backward) is with respect to the direction of the excited light with respect to the direction of the stimulated light. Backward scattering is mostly due to reflected light at the end face (or other discontinuities) of the fiber.

Nonlinear phenomena are viewed as both advantageous and as degrading.

- *Advantageous* because lasers, optical amplifiers, modulators, dispersion compensation, frequency doublers, and wavelength converters are based on them.
- *Degrading* because signal loss, noise, jitter, cross-talk, and pulse broadening are caused by them.

3.5 Optical Amplifiers

Photon absorption may advantageously be used to overcome signal attenuation by direct photonic amplification. Consider a short-wavelength intense source (source A) and a long-wavelength (by about 80 nm) weak source (source B) propagating within the same medium. The short-wavelength

high-energy (~ 500 mW) source A (known as *pump*) excites atoms to a high-energy level. Then, as photons of the weak signal travel, they stimulate the excited atoms which emit photons having the same wavelength; thus, amplification takes place. However, this simplistic description is not the same for all materials and under the same conditions [19–21]. We describe three amplifier types: the Raman amplifier, the erbium doped fiber amplifiers (EDFA), and the semiconductor optical amplifier (SOA).

Because of the quantum mechanical aspects of optical amplification and because of the statistical spontaneous photon emission and also the stimulation emission, optical amplification produces optical noise, which is known as amplifier spontaneous emission (ASE). The contribution of ASE noise depends on the dielectric material, material purity, travel distance of light in matter, wavelength, optical power, polarization states of pump and signal, and other parameters.

The key common characteristics of optical amplifiers are the following:

- *Gain* is the ratio of output power to input power (dB).
- *Gain efficiency* is the gain as a function of input power (dB/mW).
- *Bandwidth* is a function of frequency.
- *Gain bandwidth* is the range of frequencies over which the amplifier is effective.
- *Gain saturation* is the maximum output power of the amplifier beyond which it cannot increase, despite the input power increase.
- *Noise* (ASE) is an inherent characteristic of optical amplifiers. In optical amplifiers, it is due to spontaneous light emission of excited ions.
- *Polarization sensitivity* is the gain dependence of optical amplifiers on the polarization of the signal.
- *Output saturation power* is defined as the output power level for which the amplifier gain has dropped by 3 dB.

3.5.1 Raman Amplification

Consider a moderate power continuous wave (CW) laser source, the *pump*, coupled onto a common single-mode fiber. Because of nonlinearity in the fiber medium, atoms will be excited. Now, if the excited atoms are not stimulated, then after a short time they will spontaneously “drop” to an intermediate energy level releasing light energy at a wavelength longer than the pump source. Eventually, all atoms at the intermediate level will “drop” to their initially low (or ground) energy level by releasing the remaining energy in the form of phonons. This is known as *stimulated Raman scattering* (SRS). Raman scattering occurs in either direction of the fiber (forward or backwards) with respect to the direction of the pump.

Now, if the excited atoms are stimulated by photons of a weak optical signal that is at a wavelength offset by 70–100 nm from the pump wavelength, then the excited atoms are stimulated and emit photons of the same wavelength with the stimulating source. Thus, the weak signal is amplified; this is known as *Raman amplification*, Fig. 3.9. In theory, Raman lines also known as *Stokes lines* are generated according to the relationship $f - n\Delta f$, where f is the pump frequency and for single-mode fiber Δf is 70 nm at 1,310 nm and 102 nm at 1,550 nm and n is an integer.

Raman amplification uses common (non-doped) single-mode fiber, and it takes advantage of the fiber nonlinearity in the presence of high pump power; thus, Raman is a nonresonant process. Because of this, Raman is useful in the complete useful spectrum 1.3–1.6 μm ; this is known as *Raman super-continuum*.

In DWDM, there are many wavelengths within a band to be amplified. One implication of Raman amplification is that the gain is not uniform for all optical channels but it is a function of the wavelength difference between pump and signal, as shown in Fig. 3.9. As a consequence, each channel

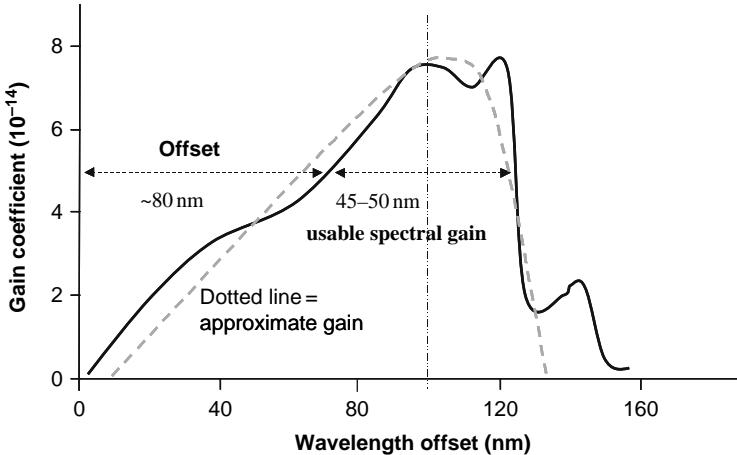


Fig. 3.9 Raman amplification characteristic

in the amplification range is not amplified with the same gain. Another implication is that the usable gain bandwidth is narrow, in the range of 20–40 nm. Therefore, if a broader band of weak signals require “Raman” amplification, then more than one pump is needed, each offset by 30–40 nm, so that both together can effectively cover the broad spectral band [22–27].

The Raman gain is an evolutionary process and the gain also depends on distance from the pump, z . The closer to the pump the more the excited atoms that contribute to power gain, which is exponentially decreasing with distance from the pump. If the initial signal power is $P_s(0)$, then the signal power at point z , $P_s(z)$, as a result of Raman gain is described by the exponential relationship:

$$P_s(z) = P_s(0) \exp \{G_R P_p(z) L_{\text{eff}} - \alpha_z\}$$

where $G_R = g_R / A_{\text{eff}} K$ is the Raman gain efficiency, g_R is the Raman gain, A_{eff} is the effective core area of the pump (between 40 and $80 \mu\text{m}^2$), K is a polarization factor that describes how close the polarization state of the pump is with the signal, ranging from orthogonal to parallel, $P_p(z)$ is the pump power, α is the fiber attenuation coefficient, and L_{eff} is the effective fiber length.

There are three methods for Raman amplification:

- The Raman pump is placed at the receiver in an opposite direction to the optical signal toward the source; this is termed *counter-propagating* Raman.
- The Raman pump is placed at the source in the same direction with the optical signal; this is termed *co-propagating* Raman.
- Two Raman pumps, one is placed at the receiver and opposite to the signal and the other is placed at the source along with the signal; we call this *bidirectional* Raman.

3.5.2 EDFA Amplification

Optical fiber amplifiers (OFA) are heavily doped with one or more rare-earth elements. Dopants absorb optical energy in one spectral range and emit optical energy (or fluoresce) in another. However, each element has its own absorption–emission characteristics. Some of the rare-earth elements useful in DWDM amplification are those whose spectral gain matches the spectrum of minimum fiber loss; these are Nd^{3+} and Er^{3+} that emit in the ranges 1.3 and 1.5 μm , respectively. Other

rare-earth elements suitable for optical amplification are Ho, Te, Th, Tm, Yb, and Pr, or in combination (e.g., Er/Yb), each operating in various spectral bands [28–33], Fig. 3.4.

The most popular OFA is the *erbium-doped fiber amplifier* (EDFA); erbium is excited by several optical frequencies, 514, 532, 667, 800, 980, and 1,480 nm and produce stimulated emission in the range 1,530–1,565 nm; that is, over the DWDM C band used. The shortest wavelengths excite erbium ions to high energy levels from where excited atoms drop to one of four intermediate metastable levels, radiating phonons (the acoustical quantum equivalent of photon). From the lowest metastable level, they finally drop to the initial (ground) level emitting photons of a wavelength about, 1,550 nm. The longest wavelength, 1,480 nm, excites atoms directly to the lowest metastable level; from this level, stimulated erbium atoms drop to the ground energy level, emitting photons. The two most convenient excitation wavelengths for EDFA are 980 and 1,480 nm.

Some of the important parameters in the EDFA gain process are

- concentration of dopants
- effective area of EDFA fiber
- length of EDFA fiber
- absorption coefficient
- emission coefficient
- power of pump
- power of signal
- relative population of upper states
- lifetime at the upper states
- direction of signal propagation with respect to pump.

EDFAs are applicable to DWDM long-haul transport systems. Single-mode fiber of hundreds of kilometers long consists of fiber segments (tens of kilometers each) where at the interconnecting points, EDFAs are placed to restore the attenuated optical signal. However, because of nonuniform amplification and cumulative ASE, the total fiber span cannot include many EDFAs (the typical maximum is 8). In addition, the total gain of the EDFA is shared by the number of optical channels in the C band; the more the channels the less the gain per channel. Thus, to determine the proper power level, many parameters must be taken into account:

- fiber length between amplifiers (in km)
- fiber attenuation coefficient
- number of amplifiers in the optical path
- amplifier parameters (gain, noise, bandwidth)
- number of channels
- channel width and channel spacing
- receiver specifications
- transmitter specifications
- dispersion
- polarization
- nonlinearity
- fiber type
- optical component losses and noise (connectors, other devices)
- expected signal performance
- signal modulation method and bit rate
- and many other design parameters.

3.5.3 SOA Amplification

Semiconductor optical amplifiers (SOA) are based on conventional solid-state laser principles; that is, an active waveguide region sandwiched between a p- and n-region. When a bias voltage is applied to it, it excites ions in the region and creates electron–hole pairs. Then, as light of a specific wavelength is coupled in the active waveguide, stimulation takes place and causes the electron–hole pairs to recombine and generate photons (of the same wavelength with the optical signal).

The excitation and recombination of electron–holes process is described by rate equations; the rate of electron–hole generation and the rate of recombination must be balanced for sustained amplification. This largely depends on the material of the active region, the bias, and the density and lifetime of carriers.

The SOA's salient characteristics are

- high gain (25–30 dB)
- output saturation power in the range of 5 to +13 dBm
- nonlinear distortions
- wide bandwidth
- spectral response in the wavelength regions 0.8, 1.3, and 1.5 μm
- SOAs are made with InGaAsP and thus they are small, compact semiconductors easily integrable with other semiconductor and optical components
- SOAs may be integrated into arrays
- polarization dependency; thus, they require a polarization-maintaining fiber (polarization sensitivity 0.5–1 dB)
- Higher noise figure than EDFA (higher than 6 dB over 50 nm)
- higher cross-talk level than EDFA due to nonlinear phenomena (four-wave mixing).

SOAs are compact solid-state devices, which may also be used in wavelength conversion, regeneration, time demultiplexing, clock recovery, and optical signal processing applications.

3.6 Optical Add-Drop Multiplexers

Add-drop multiplexing (ADM) is a well-known function in conventional transport systems with electronic methods. In optical communications, the ADM is accomplished with all-optical demultiplexers, multiplexers, optical amplifiers, and so on, hence *optical add-drop multiplexer* (OADM). In DWDM networks, the main function of an OADM is to selectively remove one or more optical channels from the fiber, pass the remaining channels through the OADM, and add the same channel(s), Fig. 3.10. OADMs may be of *fixed* wavelength or *dynamically* selectable wavelength.

3.7 DWDM Networks

DWDM systems use optical channels, the wavelength of which is according to ITU-T defined grids. The many wavelengths in a single fiber, like many colored threads in a single string, support protocol versatility (SDH/SONET, ATM, IP, Ethernet, high-speed data, video, etc.), a variety of services (established and new to come), and an unprecedented bandwidth (exceeding Tbps), all transported at the speed of light. In terms of these attributes alone, there is no other communication technology that can cost-efficiently compete with optical technology. As a result, within the last two decades, fiber has been deployed across continents and oceans, connecting cities and countries and recently penetrating the neighborhood with fiber to the premises (FTTP). In fact, there were so many fiber

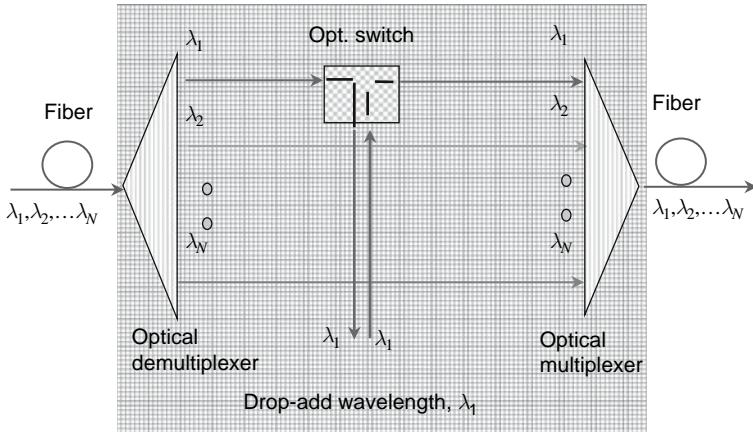


Fig. 3.10 Principles of OADM constructed with a mux/demux

cables installed, in which there are hundreds of fiber strands, that it was not feasible to use all fibers so the term *dark fiber* was coined to denote installed but not used or lit fiber. Imagine a cable with 200 strands, each with 160 channels, each channel at 10 Gbps; a potential $200 \times 160 \times 10 = 32,000$ Gbps or 32 Tbps per cable. What does this mean in communications? More than 0.5 billion clear-channel simultaneous conversations, or more than 20 million compressed video channels, or a mix of millions of voice channels + millions of video channels + millions of high-speed data, all in one cable!

3.7.1 DWDM Network Topologies

A fiber link establishes a point-to-point technology, a laser source or transmitter, and a photodetector or receiver. However, other subsystems such as optical regenerators, OADMs may be included in the link, as already illustrated. Thus, network nodes may be designed so that an optical network, in addition to point-to-point it supports ring topologies, star, and mesh, Fig. 3.11. Each topology has its own complexities and issues to address in terms of network management, protection (channel, link, and path), synchronization, performance, scalability, service support, traffic capacity, security, and cost. The simplest is the point-to-point and the most complex is the mesh topology.

The point-to-point topology connects two distant geographical locations (20–4,000 km). Short haul (up to 40 km) interconnects a central office with a town or neighborhood, whereas very long haul interconnect continents. Short haul is simple, needs no amplification, and supports relatively few optical channels, each at data rates up to 10 Gbps. Long haul, particularly the transoceanic, requires extensive optical amplification strategies as well as link and channel protection strategies because the installed fiber is neither easily nor inexpensively retrieved for repairs. Moreover, the fiber cable has been manufactured with a steel core for added strength so that the cable can withstand its own weight plus the weight of the intermittent optical amplifiers positioned along its length.

The ring topology is most suitable in local or metropolitan area networks. It can be as small and simple as a *single-fiber* ring (1-F) that interconnects few OADMs, transports few channels at 2.5 Gbps each, and covers an area of few square kilometers. It can also be a more complex *four-fiber* ring (4-F) (for path protection) that interconnects more OADMs, transports many channels at 10 Gbps each, and covers a large city or large campus, hence known as *large Metro*. In fact, the original SDH/SONET optical network was designed based on the ring topology. The *two-fiber* ring (2-F)

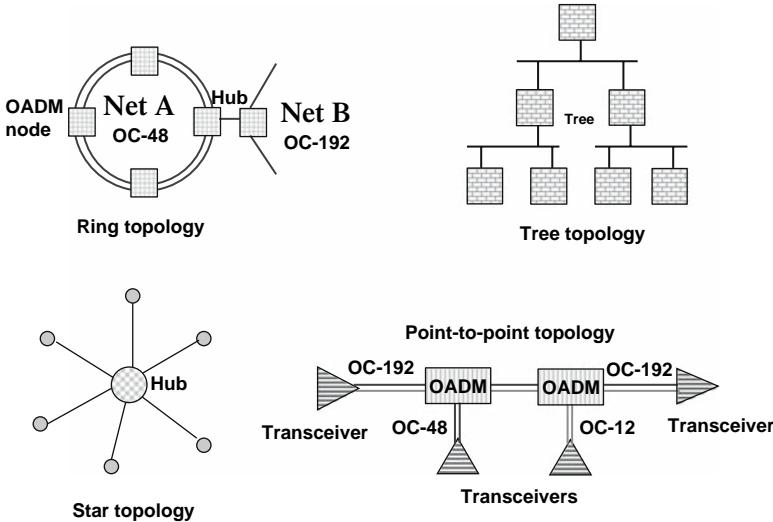


Fig. 3.11 Network topologies supported by optical technology

supports intermediate ring size and traffic. The number of dropped channels per OADM also varies accordingly, from the 1-F to the 4-F ring.

The star topology is used in few but important fiber applications, such as fiber to the premises (FTTP). In this case, the WDM signal is demultiplexed and each wavelength is coupled onto its own fiber; thus from one fiber to many. Similarly, one or more wavelengths over a single fiber are power split (with a power splitter) and each power segment is coupled onto its own fiber, thus from one fiber to many establishing a star topology.

The mesh is the most versatile, scalable, and service-protected topology because it offers many alternate paths or routes for protection and also traffic balancing and congestion-avoidance strategies. It also offers better *network scalability* (adding/removing nodes in the network), *bandwidth elasticity* (offering services that require bandwidth in small increments) and is the network topology of choice for backbone applications. However, the mesh topology requires more extensive protocols for traffic management and network management, and adherence to node-to-node and network-to-network interface standards. Furthermore, the optical technology in an all-optical mesh topology is more complex as it includes large optical switching fabrics (such as MEMS), wavelength converters, optical channel equalizers and compensators, and much more [5].

3.7.2 Optical Network Interfaces

The definition of interfaces and their standardization by international standards entities is primarily for interoperability purposes, so that products from different manufacturers (hardware and software) are compatible and work together; interoperability and compatibility is a serious and costly issue in communication networks [34–40].

An interface between two points in the network defines the physical interconnectivity, protocol, and responsibilities. There are different types of interfaces. For example,

- The physical interface between the user-terminating equipment and the network is the user-to-network interface (UNI). Depending on the protocol and network type, this interface defines the user-network physical aspects, data rate, power level, payload type, service level agreements, call initiation and termination, terminal verification and user authentication, UNI link security, and

much more. It also defines the demarcation point from which the user responsibility starts and the network responsibility ends.

- The interface between a node and another node in the same network is known as node-to-node interface (NNI). Depending on the protocol and network type, this interface defines the node-to-node physical aspects, data rate, power level, payload type, channel and traffic management, routing management and protocol, congestion avoidance strategies, service and link protection, fault management, service restoration, service availability, NNI link security, node verification and authentication, and much more.
- The interface between a network and another network is known as the inter-network interface (INI). This is similar to NNI, but because one network may be operated by one network provider and the other network may be operated by another, it also includes additional network aspects that depend on the responsibility agreement between the two network providers such as path protection, quality of service, path restoration, INI fault management, INI link security, billing, and more.

We have used the terms (UNI, NNI, and INI) as generic and logical; in reality, this terminology may differ among protocols and network technologies. For example, SDH/SONET defines section, line and path, whereas the integrated service digital network (ISDN) defines S and the T interfaces, and so on.

In addition to these interfaces, data communication networks define interfaces and responsibilities between layers as data moves from the application layer to the physical layer (the transceiver). These interfaces were initially defined by the seven-layer open system interconnect (OSI) model, Fig. 3.12. Each layer defines a set of functions and responsibilities in a node, and the boundaries (interfaces) between the layers define the protocol and interface compatibility format. Notice that the OSI model is a logical partitioning of all functions from the application to the physical layer and vice versa, and also a logical sequence of function execution within a layer.

For example, the optical physical layer defines optical power, data rate, modulation methods, wavelength grid, receiver sensitivity commensurate to performance objectives, and so on, the next layer up defines scrambling algorithms, and so on. The application layer defines the format in which the user data will be sent over the network and how received data will be presented or used. Thus, between layers there are also different communication protocols and traffic handling responsibilities that become clearer in the management section of this book. It is worth mentioning however that the OSI partitioning of functions in seven-layer is not followed by all communications technologies; for example, ATM has adopted a five-layer model whereas the TCP/IP a three layer model to provide

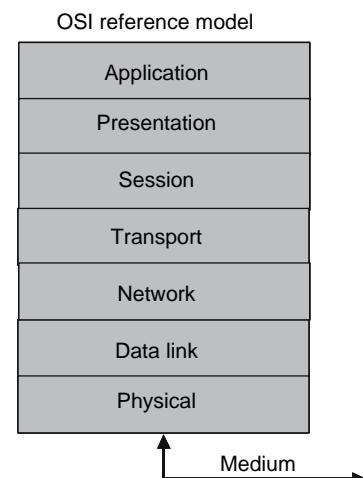


Fig. 3.12 The OSI model partitions functionality and responsibilities at each layer

simplicity, increased performance, cost efficiency, and reduce interlayer handling and thus buffering and delay.

The next generation optical network [41], although a synchronous network, is defined to transport both asynchronous payloads and protocols (packetized data, TCP/IP, ATM, Ethernet, etc.) and synchronous payloads and protocols (voice, real-time video). Thus, although synchronous protocols (SONET/SDH, DS1/DS3, etc.) do not abide to the OSI model, data protocols (IP, ATM, Ethernet) do. The transport of both synchronous and asynchronous protocols by the next generation optical network is accomplished by the generic framing procedure (GFP) and its routing flexibility by the (LCAS) [42, 43] over the optical network and particularly the WDM.

In addition to interfaces that are client data related, network management also has its own set of interfaces. In synchronous networks, the network management model is hierarchical and it consolidates functionality related to network resource management, monitoring, and controlling, and it assures the consistent performance of network and services; it is known as the telecommunications management network (TMN) five-layer structure, Fig. 3.13. The TMN five layers are the following:

1. Interconnected network elements (NE) comprise networks that may be managed by different providers; the sum of NEs constitutes the NE layer.
2. NE layers are managed by element management system (EMS); this is known as the EMS layer. The communication protocol between NEs in the multi-vendor network and its corresponding EMS varies. It may be proprietary or standard, such as the transport language 1 (TL1), the signaling network management protocol (SNMP), the common management information service element (CMISE), and so on.
3. On the northbound interface, EMSs communicate via an open, standard, to a higher level network management system (NMS). This is known as the *network management layer*. NMSs manage the network and nodes for capacity, congestion, diversity, and so on [44, 45].
4. Above the NMS is the *service management layer* (SML) that is responsible for service quality, cost, and so on.
5. Above the NML is the *business management layer* (BML), which is responsible for market share, and so on.

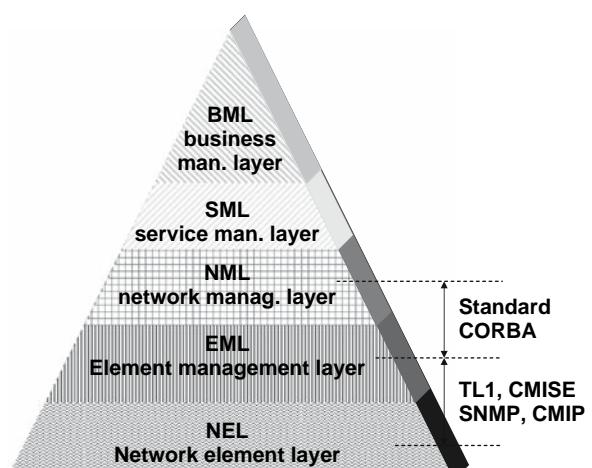


Fig. 3.13 The TMN five-layer architecture

3.7.3 Network Switching

The routing performance in optical networks depends on several factors. Among them are

- network topology,
- number of nodes in the network,
- switching capacity of each node,
- method of switching,
- speed of switching,
- through switch delay, and
- the non-blocking capability of the switching fabric.

If we limit ourselves to purely WDM (all-optical) mesh networks, Fig. 3.14, then it is clear that there are two prevalent switching methods: *wavelength switching* and *optical packet switching* [46, 47]

Wavelength switching is simple in the sense that a single (or the same) wavelength connects two points across the network. This method is also known as “wavelength assignment” (WA). When the network is pre-provisioned to provide connectivity with the same wavelength for a long period, then this is termed static WA. This method provides a better wavelength efficiency but the efficiency depends on the number of wavelengths per fiber and also on the number of fibers in and out each node. Node provisioning is relatively easy and it can be achieved with centralized control (or management) or with distributed control. Conversely, a path may be determined and the same wavelength may be assigned on a per call basis; this is known as *dynamic WA*. Static and dynamic wavelength assignment cannot warranty that there will always be the same wavelength available across the network. However, the wavelength assignment is greatly improved if wavelength converters are used in each node. In this case, a route is established by using different available wavelengths. In this case, the wavelength assignment with wavelength conversion has the highest efficiency. However, what is more important is the efficiency of traffic deliverability, which depends on the traffic utilization of each wavelength. For example, if the data rate on each wavelength is 10 Gbps, the question is, what is the effective data rate each wavelength transports? It is clear that a route may be established to transport end-user data, which is a fraction of 10 Gbps. This problem is not much different than the flow in a pipe. A pipe may connect two points but it does not warranty that it will always be full; think that a pipe is a wavelength.

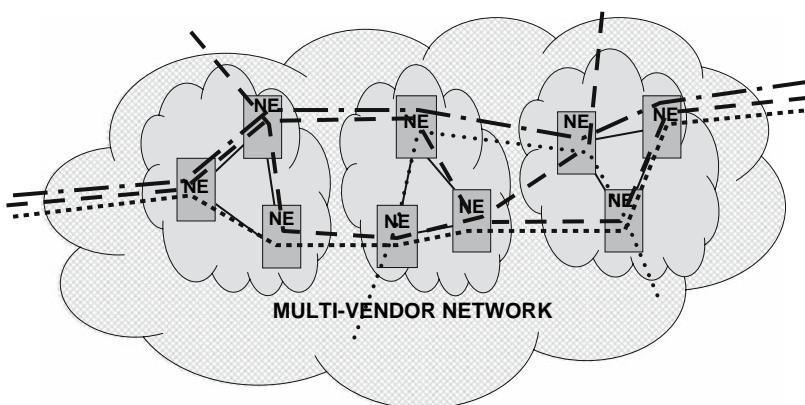


Fig. 3.14 The overall WDM mesh network may consist of several subnetworks that must be interoperable, provide comparable service quality and have common interfaces at the boundaries. Different wavelengths establish connectivity across the overall network

Optical packet switching operates on a different concept. Different packets may flow over the same wavelength but when they arrive at a node, the node recognizes how each packet should be switched, Fig. 3.15.

Optical packet switching increases packet route-ability but it is not without its own challenges. For example, when optical packets arrive at the all-optical switching node, the destination information must be read in the optical domain at the speed of the packet and the packet must be switched at the same speed; at 10 Gbps, the bit period is 100 ps and a packet of 1,000-bits long must be switched within 1,000 ns. That is, execution time must be at almost supercomputer speed, which for a single packet may be feasible but not for thousands or millions of packets per second at a large optical node. Moreover, optical delays and buffers are currently a research tool but not commercially available and thus in a practical network, optical packet switching, as described, is not an easy problem to solve. However, if the node would have *a priori* control information of packet arrival and packet routing information, then optical packet switching would be closer to being feasible. In this case, the *a priori* control information for each data packet arrives in small control packets over a separate supervisory channel, Fig. 3.16.

When the control information arrives in time for data packet switching, it is termed *just-in-time* (JIT) switching. If it arrives with enough latency for data packet switching, it is termed *just-enough-time* (JET) switching. In either case, synchronization of control packets, optical data packets, and optical switching function are critical. Additionally, synchronization implies extremely short optical switch acquisition time and switching speed. Another issue with optical packet switching is that the time offset between control and data packet may not remain within the expected value. This is the result of the two packets traveling over separate paths, and also the result of terminating the control packet at one node (where the switching is done) and being regenerated and sent to the next switch, and so on. Thus, although optical packet switching is an attractive method, it still is a technological challenge.

The ring topology is more deterministic in that respect. Medium- and small-ring networks have fixed wavelengths at the optical add-drop multiplexing (OADM) node. Large-ring networks with DWDM channels may have reconfigurable yet static OADMs, where the number of wavelengths

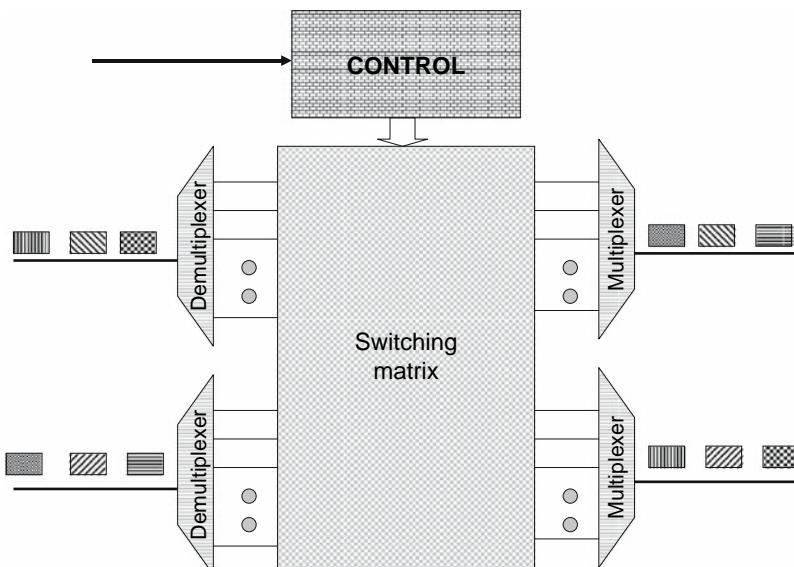


Fig. 3.15 Principles of packet switching

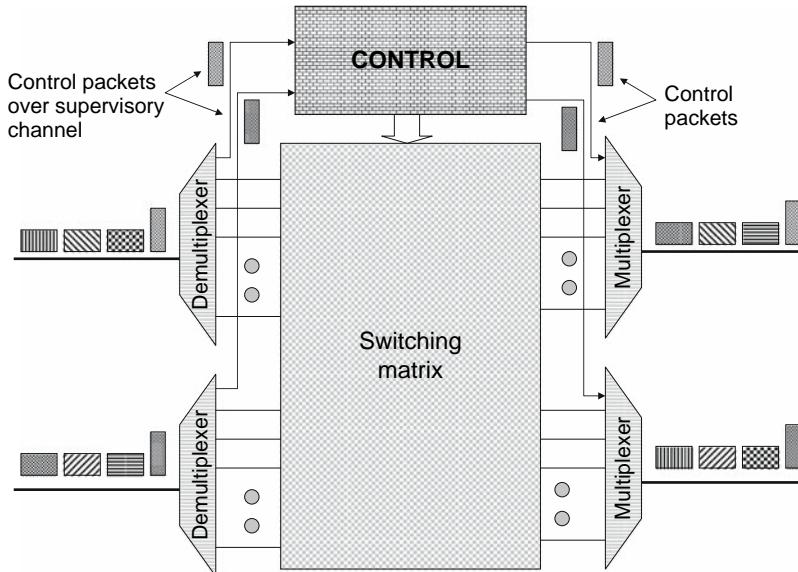


Fig. 3.16 Packet switching with supervisory channel

to be dropped/added may be variable to meet OADM capacity needs over time. However, channel variability is within specific ranges and it is not dynamic because in Metro applications, the network is configured according to a business and traffic capacity model that does not change dynamically.

Optical rings may also support optical packet switching. In this case, packets may be *addressable*, whereby the control information is mapped in the overhead of a packet addressing an OADM node on the ring. Each node reads the destination address in each incoming packet. The node that is addressed terminates it and it sources a new packet which is added on to the ring. Nodes that are not addressed multiplex the packets back onto the main WDM stream heading to the next node. Alternatively, packet addressing may arrive at the OADM node with small control packets over a supervisory channel.

In general, in addition to switching or addressing information, supervisory channels carry performance, control, provisioning, maintenance, and administration data to and from each node. There are four supervisory channel cases: *addressable*, *shared*, *channelized*, and *hybrid*.

- In the *addressable* case, each packet includes the destination address as the term implies.
- In the *shared packet* case, the packet has been partitioned in sections and each section corresponds to a node only. Thus, each node terminates its own section, it buffers the others unaltered, it rewrites its own section, and it re-sources the complete packet to the next node. Thus, all nodes may be addressed at once with the same packet minimizing latency.
- In the *channelized* case, each node has its own dedicated supervisory channel (wavelength); the wavelength is dropped, terminated, re-sourced and multiplexed in the main DWDM stream. This is the fastest method to communicate with a node, but it uses spectral resources (wavelength) for each node. However, it may be applicable in high-performance systems where real-time supervisory data at high rate is critical.
- In the *hybrid* case, it may be any two of the above methods combined. For instance, it may be addressable and shared, addressable and channelized, or shared and channelized.

3.7.4 Timing and Synchronization

In digital communications, timing implies the following functions:

- Transmit the signal at the data rate, clock accuracy, modulation method and power level complying to the adopted physical layer protocol standard;
- At the receiver, extract clock from the incoming signal;
- At the receiver, remove jitter or wander by passing the serial signal through an elastic store;
- At the node output (transmitter) retime and transmit the signal with a clock accuracy according to standards (a typical accuracy is ± 20 ppm (parts per million)).

In optical nodes, the aforementioned functionality is not easily achieved. Extracting clock from the incoming optical signal implies splitting-off some optical power from an already attenuated signal; therefore, right in front of the photodetector an optical post-amplifier is placed. Moreover, optical elastic stores and optical jitter removers are on the experimenter's bench and not a commercial reality yet. As such, in a large mesh network, because timing impairment is cumulative (jitter is transferred from optical node to node), an opaque node is needed to "clean up" and restore the optical signal. Opaque nodes convert the incoming optical signal to electrical and then back into optical; while in the electrical state, the signal is retimed, reshaped, and reconstituted (known as 3R regeneration). Despite this, 3R in DWDM communications is costly, and a substantial amount of research is going on to define all optical 3R regenerators; currently, optical amplification and pulse reshaping (dispersion compensation and channel equalization) fulfill the 2Rs that are commercially available [48–50].

Timing accuracy is defined by standards. In the United States, the primary timing reference source (PRS) is an atomic clock of the highest accuracy; it can miss one tick in 10^{11} , or it can slip 2.523 ticks in a year. This clock is referred to as stratum 1, and it is distributed to many geographic areas via satellite and other wireless means. From stratum 1, strata with lesser accuracy are derived, and depending on network layer, networks must comply with the accuracy of one of the strata, Table 3.2.

3.7.5 Channel and Link Protection

DWDM networks have the great advantage that within a fiber, there are many (hundreds of) optical channels or wavelengths. Each wavelength is generated by individual laser sources, and each channel is detected by individual photodetectors. However, on the link, there are other optical components such as filters, amplifiers, multiplexers, and demultiplexers that may affect groups of channels within a fiber. Moreover, there may be failures that may affect all channels in the fiber. That is, unlike conventional networks, DWDM systems and networks may experience single channel failure, multiple channel failures, and total failure over a link (a typical total link failure is a fiber cut or a contaminated fiber connector). Consequently, there should be protection mechanisms for all three cases: single channel, group channel, and link.

Consider that the total number of channels in a DWDM system consists of 320 wavelengths in the C and L bands (we assume an arbitrary number, yet as recommended by ITU). In this case, consider

Table 3.2 Timing strata

Stratum	Min. accuracy	Slip rate	System example
1	10^{-11}	2.523/yr	Primary ref. source (PRS)
2	1.6^{-8}	11.06/day	5ESS or equivalent
3	4.6^{-6}	132.48/h	5ESS/DCS or equivalent
4	3.2^{-5}	15.36/min	COT/digital PBX

that all channels in a fiber are partitioned in logical groups that depend on filter technology used in the system. Consider P groups with N channels in each group.

Channel protection: Channel protection may be accomplished using standard methods such as 1 + 1 (1 committed protection channel for each service channel), 1:1 (1 protection channel that also passes low priority traffic for each service channel with high-priority traffic), or 1:($N - 1$) (1 protection channel for each ($N - 1$) service channels).

Group protection: When a group of channels fails, the reasonable solution is to have a group reserved and implement 1:($P - 1$) protection method (1 protection group for ($P - 1$) service groups).

Link protection: In this case, the 1 + 1 (1 protection fiber for each service fiber), 1:1, or 1: n (1 protection fiber for n service fibers) may be implemented, as already done in optical networks.

3.7.6 Routing

A DWDM all-optical mesh network consists of many nodes, and each physical optical link between nodes carries many wavelengths or optical channels.

In DWDM all-optical networks, a lightpath connects a source with a destination. Thus, DWDM all-optical nodes either terminate or pass through lightpaths. However, connectivity on the wavelength level is more complex than non-DWDM single wavelength optical networks. In DWDM, it is not sufficient to establish connectivity over a transporting frame such as SONET/SDH but also to find the right wavelength end-to-end over the complete path. This is a routing issue known as the *wavelength assignment problem*.

There are two routing types in DWDM optical networks. One uses the same wavelength over the complete end-to-end path, known as *continuous wavelength* (CW), and the other uses wavelength converters (or λ -converters) at intermediate nodes when a lightpath cannot be established with a single wavelength but it needs to be changed from link to link; this is known as *wavelength concatenation* (WC). A parenthesis needs to be made here to clarify some possible terminology issues.

- A *wavelength* is an optical channel based on the ITU-T grid.
- A *lightpath* is an optical path between a source and a destination; it may consist of the same wavelength over the complete path or of many wavelengths “stitched” together with wavelength converters.

The end-to-end connectivity of DWDM all-optical networks, also known as *lightwave establishment*, with or without λ -converters depends on the availability of a single wavelength either over each link or over the complete path. If wavelengths are not available, then blocking of service may occur. In this respect, the selection or assignment of wavelength(s) algorithm over a path is made based on statistical demand expectations of connectivity, knowledge of network topology, network parameters, and network capacity.

In general, the wavelength assignment may be static, dynamic, or adaptive. Each method has its own requirements. The static case is applicable to networks for which all nodes over the path are pre-provisioned and the path remains established for a prolonged time, typically for weeks or months. The dynamic case is applicable to networks for which nodes can establish a path when a request to connect or to disconnect is made; that is, the path is established for a very short time, hence dynamic. Adaptive is also a dynamic case applicable when connectivity is re-provisioned dynamically in an effort to optimize the network traffic efficiency, minimize blocking, and react to network changes such as avoid faulty and congestion conditions.

There are two primary adaptive routing algorithms: the *alternate path routing* and the *unconstrained path routing*.

- The *alternate path routing* requires that each node stores the *first k shortest paths* to each possible destination. To accomplish this, the status of global and local node and link information is required, including g congestion. Congestion is determined in part by the number of wavelengths available per path/link.
- The *unconstrained path routing* considers all paths, including the first *k* shortest paths. This is based on the knowledge of a cost function for each link in the network based on which the optimal end-to-end path is determined.

A synopsis of wavelength assignment algorithms is given.

- *Random*: This algorithm selects randomly a wavelength when the new request comes from an available list of wavelengths without regard to optimization and no attempt is made to proactively reduce the blocking probability.
- *First Fit*: This algorithm indexes all wavelengths by assigning a number. Lower numbered wavelengths have higher priority. While searching for available wavelengths, the lowered indexed wavelengths are selected first.
- *Longest First*: This algorithm assigns the wavelength to the longest path first; longest path is determined by the number of hops (or links) between the source and the destination. This algorithm assumes wavelength converters in the network.
- *Least Used*: This algorithm selects the least used wavelength in the network. That is, it gives priority to the wavelength that is not used in most links over a path. This algorithm assumes wavelength converters in the network.
- *Most Used*: This algorithm selects the most used wavelength in the network. This algorithm assumes wavelength converters in the network.

The quest to identify the most efficient algorithm has not been exhausted, and research continues to find the best routing algorithm [51–53]. However, network efficiency does not depend only on wavelength routing but also on the percent of utilization of each wavelength or lightpath. For instance, assuming that the wavelength assignment algorithm is performing with the most satisfactory efficiency, then if the lightpath carries 10 Gbps SDH/SONET or OTN frames, the question is how much client traffic (or the percent of utilization) does it transport in such frames all the time? Similarly, if the lightpath carries packetized data, what is the percent of time it carries client packets? That is, not only what the capacity of each lightpath is but also what the true efficiency of the transporting mechanism is?

3.8 Access WDM Systems

WDM technology employed in point-to-point, ring, and mesh networks has proved that WDM networks can address current and future data rate needs, they are scalable and reliable, and paths can be well protected, but they are costly and as such it was not initially deployed in the access network. This created a traffic bottleneck at the access part of the optical network (ON); the ON was able to pass terabits per fiber but at the “last/first mile” of its access only few hundred kilobits, Fig. 3.17. Nevertheless, cost is relative and it is technology dependent. Thus, it may be measured by the bandwidth a technology delivers, by the number of end customers it serves, and by the distance it transports it cost-efficiently. Thus, if for simplicity we consider a cost unit per 100 Kbps/km and if passive optical technology delivers an aggregate of many gigabits over many kilometers to a large number of end users, then it becomes attractive to access optical networks. Additionally, one must consider other factors that the access technology supports, such as future-proofing, security, consolidation of equipment, network management, maintenance, and types of services, for which fiber-optic technology has proved to be superior to other technologies. Thus, as early as end of the

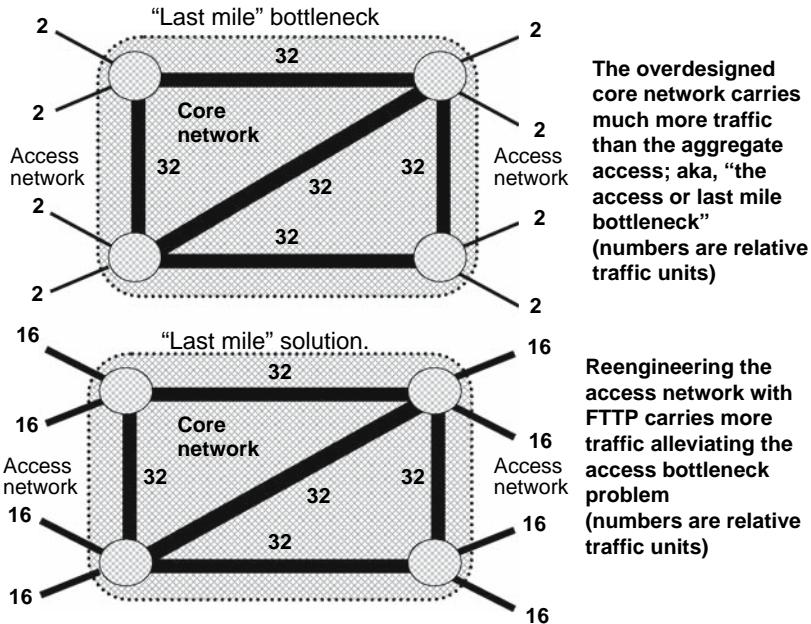


Fig. 3.17 The “last mile bottleneck” is readily solved by increasing traffic at the access; a solution that FTTP offers

1980s, various companies initiated studies for the most cost-efficient passive optical technology to be deployed in the access network so that fiber replaces the loop plant, and it was termed *fiber-in-the-loop* (FITL), *passive optical network* (PON), and also *fiber-to-the-home* (FTTH) [54]. Since then, the acronym PON has prevailed and several variant PONs were proposed and a prefix to PON was included to denote the standard protocol in use. Thus, E-PON means Ethernet PON, G-PON means gigabit PON [55], A-PON means ATM PON, and so on (generically, it is denoted xPON) [56]. PONs are also termed as *access optical networks* (AON), which may be a better representative term.

Because PONs are fiber based and because access links (also known as loops) connect end users (at the premise, home, neighborhood, office, etc.) with the public network, these optical access networks are also known as *fiber to the premise* (FTTP), or FTTx, where x is the home (FTTH), the curb (FTTC), the cabinet (FTTCab), the business (FTTB), and so on. Herein, we will use the terms PON or FTTP interchangeably [57–59], and we will avoid the confusing alphabet soup for the access optical network.

Since its initial study in the 1990s, FTTP has enjoyed an exponential growth; we identify three key drivers for this growth: advances in optical technology and standards, increased bandwidth demand to the home (voice, high-speed data, and high-definition TV) and to the enterprise (voice, high-speed data, and interactive real-time video), and certain deregulations that allow network providers to provide triple-play services over the optical communications networks. However, although FTTP is perhaps the only access technology that can offer all these services and future services not yet identified, nevertheless, the momentum has not been the same in all countries, although this is changing rapidly.

In subsequent sections, we examine the general PON topology and three PON technologies, CWDM-PON, TDM-PON, and CWDM/TDM-PON.

3.8.1 The General PON

The general PON topology is illustrated in Fig. 3.18. Depending on passive technology used, it is a point-to-point or a point-to-multipoint architecture. The access network is defined between two

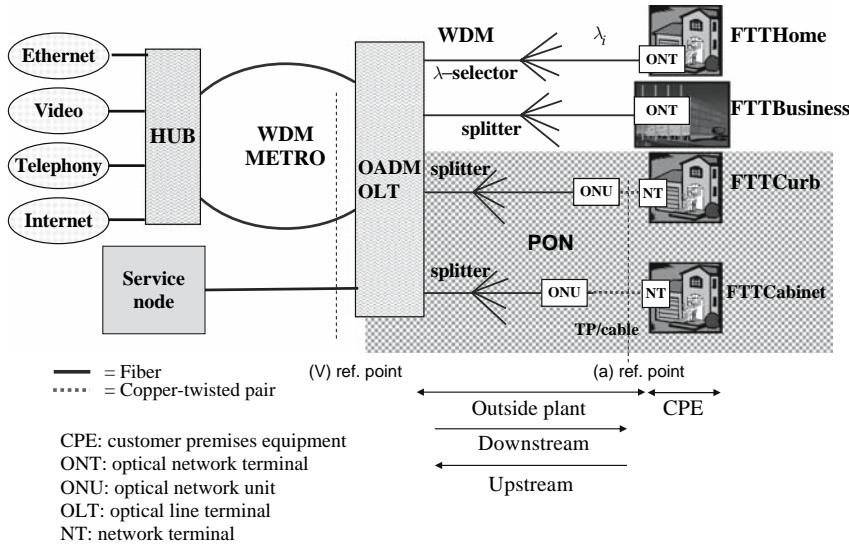


Fig. 3.18 PON architecture including reference points (adapted from [5])

interfaces: the service node interface (SNI) at the network side and the user-to-network interface (UNI) at the home network side. It is between these two interfaces that the fiber transports traffic to/from the network from/to the end user. Thus, in the optical domain, the fiber at the network side is terminated by the *optical line termination* (OLT), and at the user side, it is terminated by the *optical network unit* (ONU). Between the OLT and the ONU, there may be an optical distribution unit known ODN; an ODN may be as simple as an optical power splitter, which also provides *wavelength transparency*.

When the ONU is at the home, it is known as *optical network termination* (ONT); ONT may be placed at the premises, indoor, or outdoor and be protected from atmospheric conditions. However, the ONU may be interfacing fiber on the network side and copper (or loop) on the premises side; in such case, the ONU is located outdoors yet in a protected cabinet located, whereas copper twisted pairs are terminated by *network termination* (NT) units located at the premises.

For administration purposes and maintenance responsibilities, several reference points are defined between the network and the NT:

- the point between the OLT and the service node in the network is the (V) reference point,
- the point between the ONU and the NT is the (a) reference point.

In the downstream direction: The point after the output of the OLT is the S reference point, and the point before the input of the ONU is the R reference point.

In the upstream direction: The point right after the output of the ONU is the S reference point, and right before the input to the OLT is the R reference point. The R/S reference points are also termed *PON interface* (IF_{PON}).

According to this architecture, bidirectional traffic over the fiber link between OLT and ONU may be transported using one of the three methods, *diplex* (or di-plex), *duplex*, and *dual-fiber*.

Diplex uses different wavelengths in each direction of a single fiber. According to this, one wavelength is transmitted in the downstream direction and another in the upstream; typical wavelengths are 1,310 and 1,550 nm. The separation of the two wavelengths is accomplished with a simple rotator at each end of the fiber link.

Duplex uses the same wavelength in both directions of the single fiber (typically 1,310 or 1,550 nm); separating each direction is accomplished with a simple rotator at each end of the fiber link.

The *dual-fiber* may be in one of the three modes:

- one fiber for the downstream traffic and the other for the upstream;
- each fiber is in diplex mode carrying the same traffic, where the second fiber is for protection; and
- each fiber is in duplex mode carrying the same traffic, where the second fiber is for protection.

The direction from the network side to the user side is termed *downstream* whereas the opposite direction *upstream*.

The maximum fiber length between OLT and ONU is estimated from the link parameters such as laser optical power, fiber attenuation, component insertion loss, dispersion, other nonlinear effects, possible gain (if optical amplification is used) photodetector sensitivity, margin and expected signal performance following *link power budget* calculations; using decibel units, this is a mere additive process. However, independent of optical budget, the maximum achievable fiber length for a particular transmission system is termed *logical reach*.

3.8.1.1 Protection Strategies for the General PON

The fiber link protection strategy may range from no protection to full protection. Full protection is achieved in the dual-fiber mode, two bidirectional fibers in diplex or duplex mode, or one fiber for normal traffic (working fiber) and the other for protection; that is, a 1+1 protection strategy.

3.8.1.2 Traffic Symmetry in the General PON

With new emerging services delivered to the premises over PON networks, the amount of traffic over the link may be the same or not in each direction. In one case, the traffic in the downstream direction is much higher than that in the upstream direction; this traffic is termed *asymmetric*. Asymmetric traffic is encountered when one-way broadcast services (such as video, Internet, etc.) are offered. In the other case, traffic is expected to be the same in both directions; this is termed *symmetric traffic* (such as voice, etc.).

If packetized data technology over the FTTP is used, depending on FTTP technology, it is possible that packet collision may take place. To avoid this from happening, the OLT may take control of the packet flow by granting each ONU to send packets in the upstream direction. To synchronize the *grant process*, the ONU measures the round trip delay around the access link OLT–ONU by dividing the sum of travel time in each direction by two; this round trip delay is termed *mean signal transfer delay*.

3.8.1.3 ONU Authentication in the General PON

The FTTP network is expected to be scalable and expanding. Thus, the network expects that new ONUs may be added. This expansion however provides an opportunity to bad actors to add ONUs illegally. To combat this, the network must have the capability to authenticate the ONUs (existing and newly added) on the FTTP network.

3.8.1.4 PON Installation Methods

Fiber for PON is installed using different methods:

- aerial cable: fiber cable is installed on utility posts;
- micro-duct: fiber cable passes through inground and surface plastic ducts;
- conventional duct cable: fiber cable passes through ducts buried inground;

- underground: fiber cable runs through large utility underground ducts; and
- combined method: fiber cable may be aerial for some length, through underground for some other length and through microduct, and so on to reach its destination.

Each method depends on geography, topology, and customer density, and it has different installation and distribution issues and also cost structure.

The projected power budget over the OLT–home path is from 22 to 25 dB (assuming an additional 3 dB margin). In the premises, passed the network termination, the traffic distribution will be via standard connectors such as RJ-11 for POTS, RJ-45 for Ethernet, and Coax RG-59 for video.

3.8.2 CWDM-PON

When the PON carries many wavelengths over the fiber link, it is known as WDM PON. In fact, the notion of many wavelengths or frequency channels in a medium is not far from what is already known as frequency division multiplexing (FDM). Because a PON is expected to be a low cost optical technology, ITU-T (G.694.2) has defined a coarse grid of 18 optical channels over the full spectrum for communications 1,261–1,621 nm; this is termed coarse WDM (CWDM); PONs based on the CWDM grid are termed CWDM-PONs. The CWDM grid defines a channel spacing of 20 nm allowing a laser drift due to temperature variation of $\pm 6\text{--}7$ nm, which enables the usage of uncooled lasers (and thus low cost) and wide passband filters.

In such case, the full CWDM grid becomes useful if single-mode water-free fiber [60] is used over the OLT–ONU link. PONs may also be based on the coarse DWDM C and L band grid (channel separation of 200 nm) to increase the number of channels from 18 (CWDM) to 20 (C band only) or 40 (C+L band); this is termed DWDM-PON. Clearly, because of the tight specifications of DWDM components, DWDM-PONs do not provide a cost advantage over the CWDM (CWDM costs less), but it takes advantage of EDFA optical amplification and the large variety of optical DWDM components.

In CWDM-PONs, each optical network unit (ONU) operates on a different wavelength. In the upstream direction, signals from several ONUs are wavelength division multiplexed (WDM) and coupled onto the single-mode fiber, Fig. 3.19. In the downstream direction, at the OLT, several wavelength division multiplexed signals are coupled onto the fiber link. At the distribution network, the WDM signal is demultiplexed, and each wavelength is sent to its corresponding ONU. Transmission over the link may be in one of the methods discussed earlier, diplex, duplex, or dual-fiber, but in this case, there is not a single wavelength but a group of wavelengths.

3.8.3 TDM-PON

The TDM-PON takes advantage of the well-known method of time division multiplexing (TDM), which is in use since the development of digital transmission and synchronous optical multiplexing (in DS1, DS3, etc.). In principle, the TDM-PON uses a single wavelength in diplex, duplex, or dual-fiber mode.

The OLT transmits TDM traffic in the downstream direction, and it manages the upstream traffic. In the downstream direction, TDM traffic from the OLT (typically using the wavelength 1,490 nm) reaches over fiber a 1 to N optical splitter. That is, all N outputs of the power splitter carry the same TDM traffic. However, a time slot is associated with a particular ONU, and thus each ONU finds its own time slot and extracts the data from it, which then passes onto the NT and from there to the end user, Fig. 3.20.

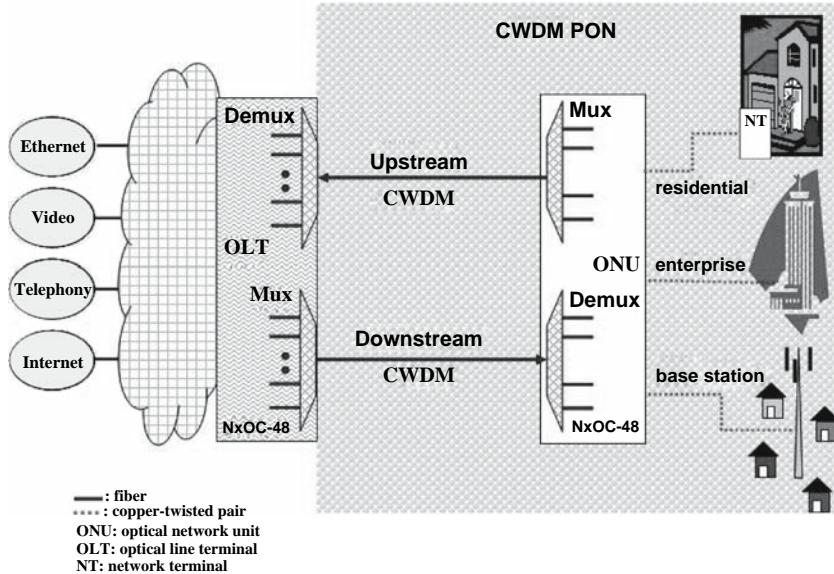


Fig. 3.19 CWDM-PON

In the upstream direction (typically using the wavelength 1,310 nm), end-user data arrives at the associated ONU which places it in its corresponding time slot and sends it toward the OLT via a combiner, which is collocated with the splitter. At the combiner, time slots from all ONU arrive, and they are time division multiplexed onto a single TDM stream coupled onto the single-mode fiber. It is evident that time slots arriving at the combiner must be well synchronized, else they will collide in the time domain. This clearly is not as easy to accomplish in the optical domain because the distance between ONUs and combiner is not the same as the propagation delay between ONUs-combiner is not. Synchronization may be achieved if each ONU either is capable of measuring the propagation

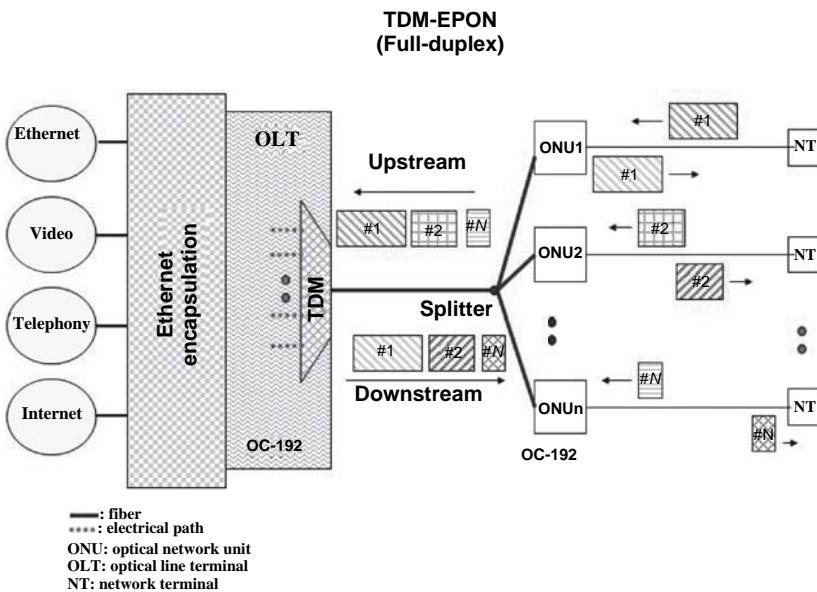


Fig. 3.20 TDM-PON

delay ONU-combiner, which is not as simple, or is provisioned to generate the proper delay, which makes the ONU costly.

3.8.4 TDM-PON Versus WDM-PON

The TDM-PON split the optical power via the 1 to N splitter, for which N is relatively small and so is the number of subscribers and also the deliverable data rate to each end user. Conversely, the CWDM-PON with relatively few channels delivers traffic to as many ONUs as the channels but at high data rate to each one [61].

Because the medium is shared by all end users, the available bandwidth and the network resources are better used in TDM-PON than in WDM-PON, hence the TDM-PON is more efficient.

The TDM-PON is based on a fixed number of well-synchronized time slots. Thus, the TDM-PON is not easily scalable. Conversely, the WDM-PON is only limited by the number of wavelengths available in the grid, which however may be increased by migrating to DWDM or by defining a denser CWDM grid 36 channels and 10 nm channel separation. Although the latter requires standards approval, it is not unreasonable; the DWDM was initially defined with 50 Ghz separated 80 channels, which now has been redefined to 160 channels 25 Ghz separated.

The TDM-PON requires a complex time arbitration mechanism to avoid time slot collision in the upstream direction. WDM-PONs do not require such arbitration.

The TDM-PON, because of its broadcast nature, allows bad actors to “listen” to time slots that belong to other ONUs. Thus the TDM-PON is less secure. The WDM-PON does not broadcast data and thus in that respect it is better than the TDM-PON. However, an eavesdropper may also extract data from an individual ONU by unauthorized access of the ONU or by tapping the input or output of the ONU. In all, security is an issue which needs to be examined seriously by encrypting data and by securing the fiber link. Security is discussed in detail in Chap. 10.

In conclusion, the TDM-PON and the WDM-PON have advantages and disadvantages in a complimentary way. The advantages of the former are disadvantages of the latter and vice versa.

In the following section, we describe a hierarchical WDM/TDM-PON which combines the advantages of both.

3.8.5 Hierarchical CWDM/TDM-PON

This is a proposed topology that combines CWDM in a point-to-point topology between OLT and ONU, an optical tree topology at the ONU, and an optical TDM in a point-to-multipoint topology between ONU and NTs. Because of this, we call this network “hierarchical CWDM/TDM-PON” or hCT-PON [62].

At the OLT, 16 CWDM optical channels for data and 2 channels for supervision and control are multiplexed and send to the optical network demultiplexing unit (ONU-d), Fig. 3.21; in this scenario, the ONU plays the role of ODN and ONU combined. We assume that the single-mode fiber is of the water-free type to support the CWDM grid and at a length exceeding 20 km. The next generation grid with 36 channels (10 nm channel separation) doubles the number of channels; more channels and longer distances can be supported by the sparse DWDM with 200 Ghz channel separation; however, the increased bandwidth capacity of DWDM needs careful examination as CWDM technology has an average 40 % lower cost as compared with DWDM. The 16 of the 18 channels for customer data are at one of the three data rates, 1GbE, 2.5 or 10 Gbps. The remaining two channels carry supervisory and control data at a rate of 1 GbE or less.

The ONU-d consists of an optical wavelength demultiplexer (ODemux), SOA amplifiers, two splitters for the two supervisory channels, and 16 optical TDM units (ONU-t). Each unit contains

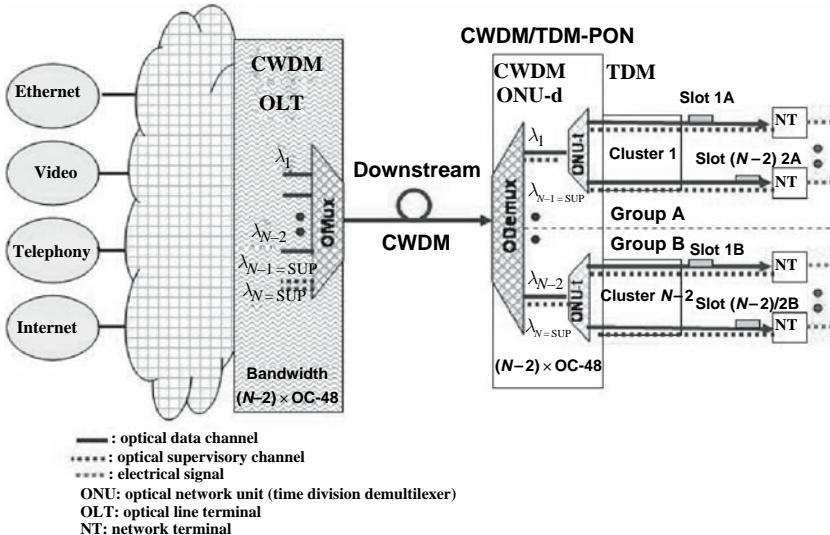


Fig. 3.21 Architecture of the hCT-PON access network (downstream direction)

an optical switch which deflects packets in time slots to their corresponding fiber. The 18 channels are demultiplexed by the ODemux and each channel is amplified by an SOA. The shortest and the longest wavelength of the 18 channels are allocated for supervision; that is, the two most naturally degraded channels are chosen for supervision and because they are at lower data rate, their performance is degraded less. The 16 wavelengths from the ODemux are separated into two groups, A and B, each of eight channels, and each channel is connected with an ONU-t. The two supervisory channels are also separated, one for group A and the other for group B. Each channel is power split in 8 by an 1:8 splitter (not shown).

One of the 16 data outputs from the optical demultiplexer and a supervisory channel from the splitter are routed to an optical time division demultiplexing network unit (ONU-t). The ONU-t time demultiplexes packets of equal length and each demultiplexed packet is routed to a fiber in a cluster of fibers; each fiber in the cluster connects the ONU-t with a network terminating unit (NT), where each NT serves one or more end users. At the ONU-t, the deflection of packets in their corresponding time slots may be implemented with one of several optical technologies (including optical switches or optical rings). The length of each fiber in the cluster is the same in order to eliminate group delay variations; this is easily accomplished by using same length fibers. Each NT determines its own time slot and length from a reference clock and from supervisory messages. In addition, each NT receives one of the two supervisory channels that provides information regarding time reference (this is the same for all NTs in the same group), time slot location and length, payload type, testing, maintenance, security levels, and more.

The point-to-multipoint topology assumes that NTs of the same group are sparsely located. When NTs are closely located, then this topology can be modified in a point to multipoint with an open ring physical topology, Fig. 3.22. Notice that this is an advantage of our proposed network as a properly equipped ONU-d supports both topologies serving simultaneously sparse and dense NTs. However, in dense NTs, capital cost is shifted from the ONU-ds and the fiber plant to more complex NTs. NTs in this case recognize their own packet(s) in the optical stream [8] and mark the instance of their time slot, which must be known for time multiplexing packets in the upstream direction.

The upstream direction works as the downstream direction, Fig. 3.23. In this case, each NT receives traffic from the end user, it packetizes it, and it transmits each packet within its designated

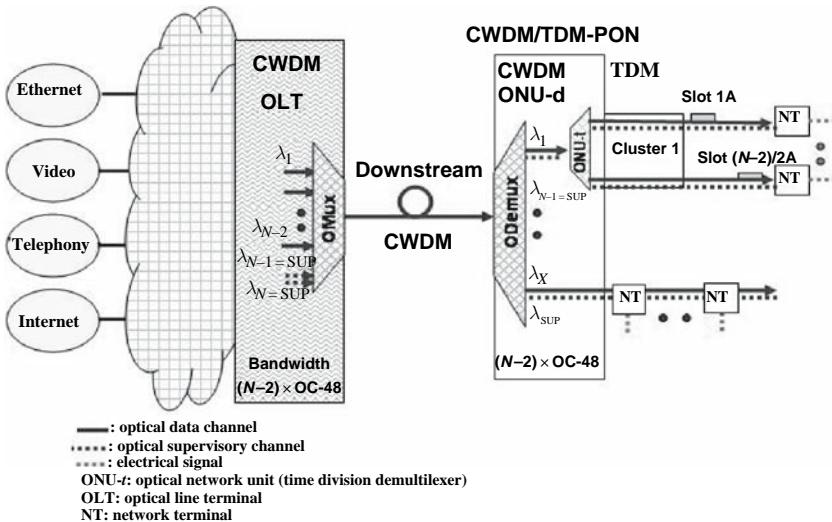


Fig. 3.22 The hCT-PON supports simultaneously two different topologies (downstream direction)

time slot. Each NT does the same with supervisory messages, which now are time multiplexed onto the supervisory channel. Since the data and the supervisory channels are on different wavelengths, the NT wavelength multiplexes the two and couples onto the fiber in the direction to optical time division multiplexing unit (OTDM).

In the upstream direction, each OTDM time multiplexes packets from their cluster and transmits them to the optical multiplexer (OMux). The OTDM in this case is simple, and it consists of a coupler to perform the time division multiplexing function as well as wavelength division multiplexing for data and for supervisory channels. The OMux time division multiplexes messages from the two groups onto the two supervisory channels, and it couples all 18 CWDM channels onto the fiber. The latter is received by the OLT's optical demultiplexer unit (ODemux).

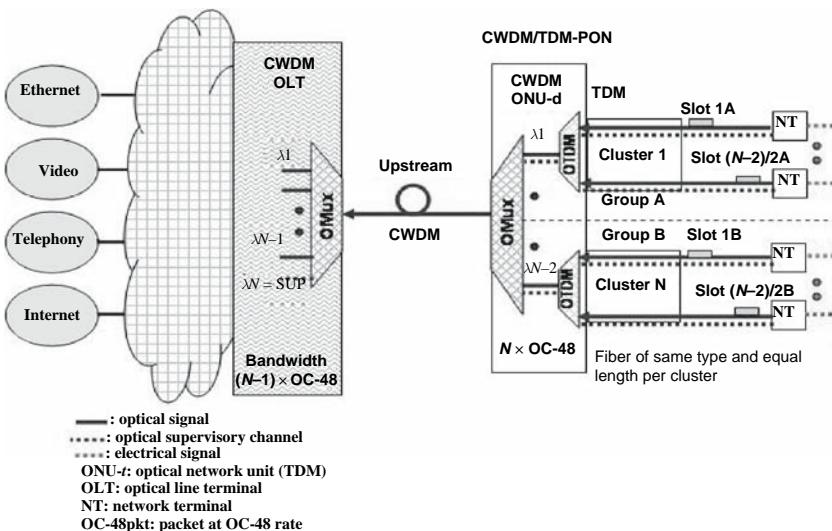


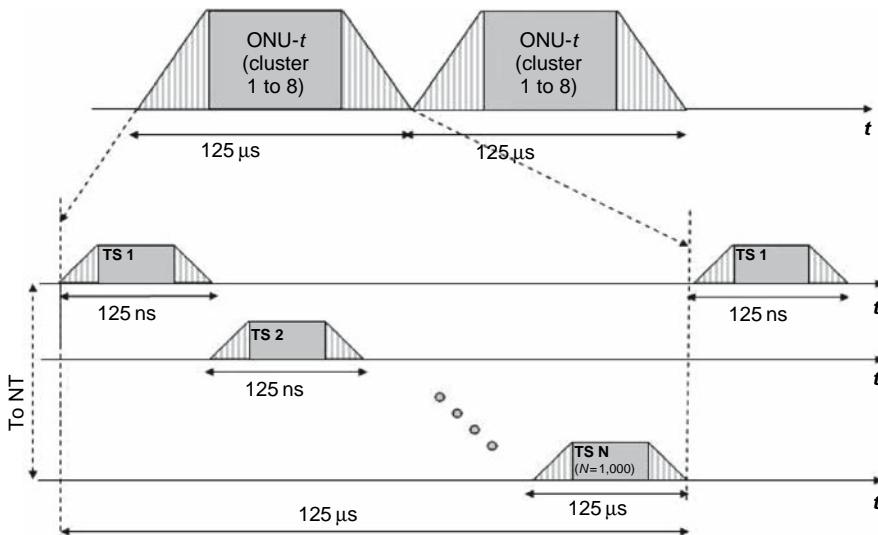
Fig. 3.23 Architecture of the hCT-PON access network (upstream direction)

As in the downstream direction, so in the upstream the hCT-PON supports multiple topologies. The NTs for each case have different design complexity commensurate with that in the downstream direction.

Because the hCT-PON may adapt the DWDM grid (with 200 Ghz channel separation), 40 channels in the C band over standard single-mode fiber may be used. Furthermore, if the C and L bands are jointly used, then the number of channels is doubled to 80. That is, the hCT-PON is highly scalable and the only limitation is cost and technology maturity, both of which are expected to improve over time.

In the downstream direction, although each wavelength arrives at each ONU-t with a small phase difference, it does not affect the transmission method because the outputs from the ONU-t are coupled onto a fiber cluster with each fiber having equal length to eliminate differential delays within the cluster. This engineering rule, equal length and same fiber type within a cluster, substantially simplifies inventory and logistics of the fiber plant while it maintains flexibility and network scalability. Hardware design, protocol complexity, maintenance, and provisioning are also simplified.

The proposed CWDM-PON is characterized by bandwidth elasticity. Assume data rate at 2.5 Gbps per optical data channel; this is a realistic cost-efficient data rate allowing for uncooled lasers and optical components with relaxed specifications. For bandwidth scalability and elasticity, we have chosen a minimal time slot granularity of 125 ns, Fig. 3.24. Thus, 2.5 Gbps bandwidth is subdivided in small amounts of 2.5 Mbps, each delivered in the downstream direction to 1,000 NTs. For many access applications, 2.5 Mbps is a sufficient bandwidth for very fast Internet/Ethernet, voice, high-speed data and compressed video, termed *triple play*. Now, for applications that require more bandwidth, more contiguous time slots per NT may be assigned, and for applications requiring less bandwidth, the 2.5 Mbps may be scaled down to 1.5 or 2 Mbps to emulate DS1 or E11 rates, which may be further demultiplexed to individual DS0 (64 Kbps) and/or ISDN rates (144 Kbps). For applications that demand very high bandwidth, concatenating k time slots ($k = 1\text{--}1,000$), $k \times 2.5$ Mbps may be transported; thus, elastic bandwidth from DS0 to many times 2.5 Mbps (potentially to a full 2.5 Gbps) is achievable. Notice that for cost-efficiency we selected 2.5 Gbps. If 10 Gbps was selected, then a four-tuple aggregate traffic is transported and data elasticity increases accordingly.



Data channels in fiber cluster arrangement

Fig. 3.24 Time division demultiplexing of an optical data channel for a cluster of NTs

In the upstream direction, each NT receives packet data from end devices, and it transmits them in their corresponding time slot. The OTDM time multiplexes data from NTs without optical buffering onto a single channel and sends them to the OMux.

The supervisory channel works in a similar manner. In the downstream direction, time division multiplexed supervisory messages for each NT are sequentially concatenated. Because all NTs have been divided in two groups each containing half the data channels, each supervisory channel addresses half of the NTs in the network. For 1,000 NTs per data channel, each supervisory channel addresses 8,000 NTs (although the potential address space is 2^{16}).

If we assume that two messages per second per NT are sufficient, then 16,000 messages per second are carried by each supervisory channel. Now, a cluster of NTs is addressed within 1/16 of a second or 62.5 ms. Thusly, a cluster is addressed twice per second, and each of the 8,000 NTs in a cluster is addressed with a 7 μ s time slot. At 155 Mbps and for 36 octets per message, approximately a 2 μ s window per NT is centered within the 7 μ s window leaving 5 μ s for guardband or margin and for future-proofing, Fig. 3.25. In the future, messages may expand to 72 octets with 4 μ s margin. Moreover, guardbands are set to zero optical level or to a fixed pattern such as 00100100. The structure of the supervisory (or control) messages consists of a header, a data field, and a CRC trailer.

Another benefit of the very large customer base is the cost of amplification. For example, certain FTTP methods use the C band spectrum to employ EDFA amplifiers. In this case, assuming \$200K for EDFA for 1,000 homes (and for 50 % take rate), the cost is \$200 per home. The CWDM-based hCT-PON however employs semiconductor optical amplifiers or Raman amplifiers, which are much lower in cost (projected to <\$20/home); this also accounts for CWDM, which is less inexpensive than DWDM by 40 %.

In the upstream direction, each NT transmits a 36-octet message back to OTDM, where all messages of a NT cluster are time division multiplexed in their corresponding 62.5 ms. Then, all messages from all eight OTDMs are time division multiplexed at the OMux and coupled onto one of the two supervisory channels. Each of the 62.5 ms intervals has guard bands at each side to relax specifications and avoid collisions.

If the distribution of 1,000 fiber strands per cluster may seem to be challenging (some fiber cables contain 1,000 fiber strands), as bandwidth becomes commodity, and as bandwidth per NT increases, more time slots are assigned to each NT and thus the number of NTs in the cluster decreases, and so

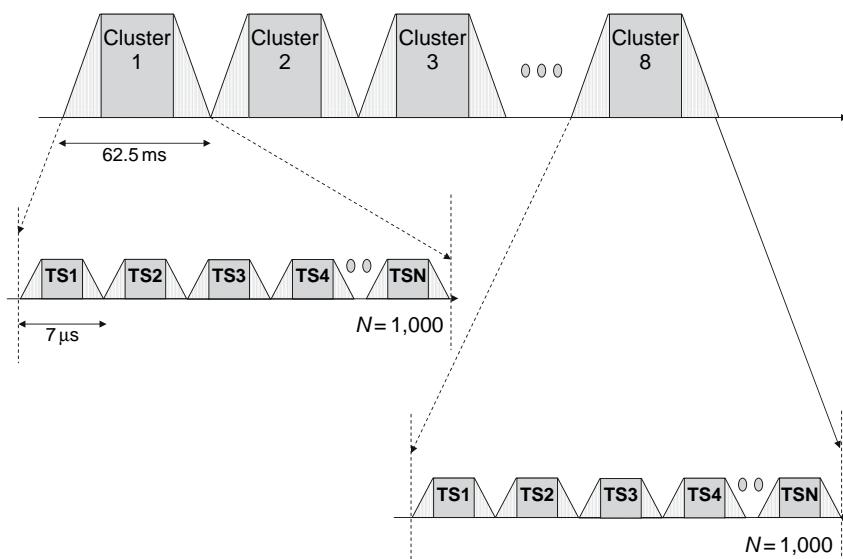


Fig. 3.25 Time division multiplexing of a supervisory channel per eight clusters of NTs

does the number of fibers. Arguably, 1,000 NTs per optical channel demonstrates an access network that is able to deliver multiservices with elastic bandwidth to a very large number of end users. If a smaller network is needed, then the network can be scaled down; in this case, not all the 16 optical data channels are used, not both groups, not all clusters, not both supervisory channels, not all fibers per cluster, and not all time slots are populated. Later, the network is accordingly populated to meet the demand and serve the increasing number of end users.

In the upstream direction, the bandwidth elasticity is similarly demonstrated. NTs deliver 2.5 Mbps or multiples of it. NTs may also be used as aggregation points for DS0, DSL, and ISDN services. If in the upstream direction certain clusters are expected to transport a fraction of 2.5 Gbps (or OC-48) per optical channel, the transmitters in this cluster may be further relaxed to transmit at a lower bit rate, such as OC-12 or even OC-3. In this case, the time slot arrangement remains the same, and time slots are scaled accordingly (4 times for OC-12 and 12 times for OC-3). This possible arrangement of asymmetric traffic further relaxes specifications and lowers the overall network cost.

3.8.6 How Real Is PON?

PON is very real and many countries are already PON-ready. Large networking companies around the globe have made huge investments in PON technology and already have a significant penetration homes/building FTTP passed. Some countries started the FTTP deployment early and some others later. The starting point depended on several factors among which are a common platform and standard specifications, capital and operational cost, optical technology issues, and business drivers.

In the United States, the removal of regulatory barriers made FTTP a good business case. As a result, BellSouth, SBC Communications, Inc., and Verizon adopted a set of common technical requirements that were based on existing industry standards and specifications, known as FTTP (Joint press release, May 29, 2003). Accordingly, Verizon's plan was to reach 1 million homes by the end of 2004 and twice as many by 2005. Similarly, SBC's plan was to deploy FTTP to 300,000 premises per year, starting with 2005.

In Europe (EU 17), by the end of 2005, 2.5 millions buildings/homes passed with FTTP, and this is projected to exceed 6.5 millions by 2008. Among the EU 17, by June 2004 Sweden and Italy led the number of FTTP subscribers: Sweden with 200,000 subscribers and Italy with 190,000; Italy and Sweden also led the number of buildings/homes FTTP passed: Italy with 1.25 million and Sweden with 0.5 million. However, Denmark and the Netherlands led in FTTP penetration: Denmark by >76 % and the Netherlands by >66 %.

In Japan, (according to NTT data) by the end of 2006, was planned for 6.5 million subscribers compared with North America that will have 4.5 million.

Cost of service is very critical in attracting subscribers. Cost of service mainly depends on cost of goods (or capital expenses), operating cost, and also on savings by system and other resource consolidation. This also has the benefit of less staffing and less power consumption. Thus, an FTTP that delivers data to a very large customer-base at very long reach (such as the hCT-PON) eliminates or consolidates many existing systems and small central offices to a larger one. Typically, 20 km reach (CO to home) covers more than 99 % of US subscribers and perhaps 100 % of subscribers in most other countries. Thus, in the United States a projected cost of goods for the ONT is under \$340, and for the OLT (without amplification) is under \$250. In addition, the cost of deployment is projected to under \$1,200 per home passed. Nevertheless, cost of goods and cost of deployment are one-time investment. Therefore, the cost of maintenance should be commensurate to or less than DSL, when computed per kilobits per kilometer; DSL maintenance cost can be as high as \$290/line/year.

Application drivers depend on the availability of specific devices and services that appeal to consumers. Based on this, applications that drive FTTP in the United States currently are e-mail,

e-commerce (which may also be seasonal), search engines, e-banking and other online services, and also downloading (messaging, music, and e-news). However, with novel devices and with lowering cost (as a result of component improvement and of service bundling), new applications will become decisive in increasing bandwidth demand (downloading high definition video, 3-D video, two-way video communication and telepresence, and game-playing). For example, the cost of DTV and HDTV sets is dramatically decreasing although currently not many channels in the United States offer HDTV.

In addition to this, ITU-T standards have been issued for interoperability purposes [63–73], in addition to those already mentioned.

In addition to application drivers, cost of service and cost bundling also stimulates subscription to FTTP. From 2003 NTT data, the monthly charge per 100 Kbps in certain sample countries has been (in US dollars): Japan = \$0.18, Korea = \$0.29; USA = \$2.86; the Netherlands = \$5.13; UK = \$7.18; Switzerland = \$13.9; Finland = \$21.21. Clearly, such a large pricing range depends on many factors that are beyond the purpose of this analysis.

3.8.7 Free Space Optical

Some specific applications require relatively quick point-to-point high bandwidth and low cost connectivity. Typically, such applications aggregate multi-type traffic at an access enterprise point and transport it to another point located from hundreds of meters to few kilometers away. This technology does not use fiber on the link but a laser beam in free space (hence FSO) and therefore it necessitates line of sight; typically from rooftop to rooftop. Because this technology does not need fiber installation and right-of-way licenses, it is deployed quickly and inexpensively.

However, FSO has a severe drawback. Laser light is severely absorbed by fog but not as much by rain. Interestingly, microwaves are affected by rain and not as much by fog. Thus, the two technologies are complementary and can work side by side. If fog is present, the microwave link switches in and if not the FSO does. FSO is preferred because it can transport much more bandwidth (more than 1 Gbps) than the microwave link (few Mbps).

FSO technology may also include multiple wavelengths thus utilizing WDM technology, in which case the aggregate bandwidth is multiplied by the number of wavelengths in the beam.

FSO is already considered in satellite network applications to interconnect a cluster of satellites in a 3-D mesh topology [74, 75]. Optical transmitters suited to this application use neodymium yttrium-aluminum-garnet (Nd:YAG) solid-state lasers. Although satellites are thousands of kilometers apart, space is free from atmospheric phenomena and exerts insignificant attenuation and thus a laser beam travels far. However, maintaining connectivity as satellites move requires good tracking. In addition, as the laser beam travels for many kilometers it diverges and thus the receiver must have a large aperture telescope, typically about 10 cm in diameter.

The initial deployment was a simple point-to-point link. Recently, more complex FSO transceivers have become available to allow for ring and mesh network connectivity as it was envisioned and described in Refs. [4, 76, 77], Fig. 3.26. The ring and particularly mesh topology can transport much larger aggregate traffic, and it is better protected from faults [78].

3.8.7.1 Advantages and Disadvantages of FSO

Advantages of FSO:

- Installation is relatively simpler and faster (about a day) than the typical fiber-optic network (weeks to months).
- FSO transceivers are installed on top of existing buildings (some deployments provide links from window to window).

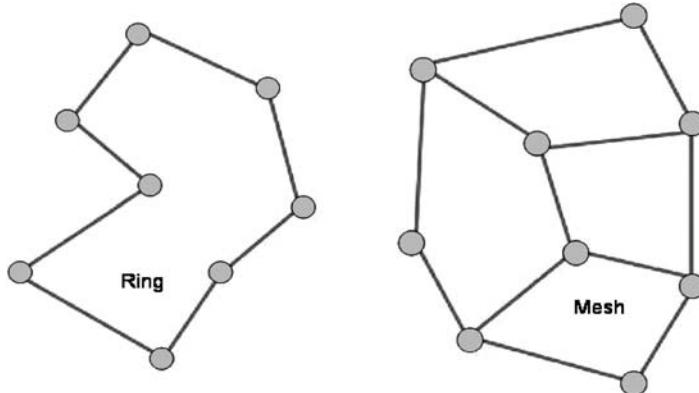


Fig. 3.26 FSO nodes when designed with multiple transceivers may be deployed in ring and mesh topologies

- Connectivity with client network and FSO transceiver is accomplished using vertical cable, which is easily installed in an elevator well or staircase.
- FSO provide a proprietary link compared with a network provider's fiber that may be shared with other clients.
- FSO needs no spectrum licensing since it does not use radio electromagnetic waves.
- It is immune to electromagnetic interference.
- It has relatively low cost per node.
- It does not impose any hazard to life as the laser beam is few megawatts (it uses typical communication laser devices 800–1,550 nm).
- Because the beam is thin, invisible, and at inaccessible heights, FSO links are inherently not interceptable and thus secure.

Disadvantages of FSO:

- FSO links are short (~ 2 km) as compared with fiber optic links (20–100 km).
- FSO links provide less bandwidth (~2.5 and perhaps 10 Gbps) than fiber optic links, which can carry aggregate traffic exceeding terabits.
- FSO suffers from fog and heavy snow attenuation. FSO links become operational from medium fog with about 30 dB/km attenuation to a clear day (visibility >6 km) with about 0.2 dB/km or less attenuation. Thick fog with >50 dB/km attenuation does not sustain FSO communication. The attenuation and the wavelength over the FSO link is related to particle parameter $\sigma = 2\pi r/\lambda$, where it is assumed that particles are spherical with radius r . In general, the longer the wavelength, the lower the atmospheric attenuation and therefore most FSO systems prefer wavelengths at 1,550 nm over 800 nm, in addition.
- FSO suffers from scattering caused by particles airborne in the atmosphere. Scattering is classified into three mechanisms: Rayleigh, Mie, and Geometric [79].
 - Rayleigh scattering is in effect when $r \ll \lambda$ (this is also present within a fiber where attenuation is $\sim \lambda^{-4}$).
 - Mie scattering is in effect when $r \sim \lambda$.
 - Geometric scattering is in effect when $r \gg \lambda$.
- FSO suffers from scintillation caused by air temperature fluctuations and atmospheric turbulence [80]. However, attenuation due to scintillation is small (few dB/km) as compared with fog and snow.
- FSO requires accurate line of sight alignment. The transceiver aperture and tracking mechanisms must account for sway of tall buildings during strong winds to maintain alignment.

Thus, attenuation and scattering depend on particle size and particle density. As a point of reference, molecules are smaller than 1 nm, fog droplets are about 10 μm , and rain drops in the range of 100 μm –10 nm.

In conclusion, FSO is an optical network technology that can be deployed quickly in inner city as well as rural applications. Our research has concluded that in networks (such as in Fig. 3.25) two, three and rarely four transceivers per node may construct a comprehensive mesh network. When these networks have links with RF backup, then the network will continuously provide service, meeting the availability requirements under all atmospheric conditions.

References

1. S.V. Kartalopoulos, “Emerging Technologies at the Dawn of the Millennium”, *IEEE Communications Magazine*, vol. 39, no. 11, November 2001 pp. 22–26.
2. S.V. Kartalopoulos, “DWDM: Shaping the Future Communications Network”, *IEEE Circuits and Devices Magazine*, October/November 2004, pp. 16–19.
3. S.V. Kartalopoulos, “What is DWDM?”, *SPIE Electro-Optic News*, no. 203, November 2000, pp. 4 and 12.
4. S.V. Kartalopoulos, *Introduction to DWDM Technology: Data in a Rainbow*, IEEE-Press, 2000
5. S.V. Kartalopoulos, *DWDM Networks, Devices and Technology*, IEEE/Wiley, 2003.
6. S.V. Kartalopoulos, *Fault Detectability in DWDM: Toward Higher Signal Quality and System Reliability*, IEEE-Press, 2001.
7. ANSI/IEEE 812-1984, *Definition of Terms Relating to Fiber Optics*.
8. J.R. Thompson and R. Roy, “Multiple Four-Wave Mixing Process in an Optical Fiber”, *Optics Letters*, vol. 16, no. 8, April 1991, pp. 557–559.
9. K. Inoue, “Four-Wave Mixing in an Optical Fiber in the Zero-Dispersion Wavelength Region”, *IEEE Journal of Lightwave Technology*, vol. LT-10, no. 11, November 1992, pp. 1553–1563.
10. K. Inoue, “Fiber Four-Wave Mixing in Multi-amplifier Systems with Nonuniform Chromatic Dispersion”, *IEEE Journal of Lightwave Technology*, vol. LT-13, January 1995, pp. 82–93.
11. Y. Chen, M.T. Fatehi, H.J. LaRoche, J.Z. Larsen, and B.L. Nelson, “Metro Optical Networking”, *Bell Labs Technical Journal*, vol. 4, no. 1, 1999, pp. 163–186.
12. ITU-T Recommendation G.694.1, “Spectral Grids for WDM Applications: DWDM Frequency Grid”, May 2002.
13. ITU-T Recommendation G.694.2, “Spectral Grids for WDM Applications: CWDM Wavelength Grid”, June 2002 Draft.
14. ITU-T Recommendation G.654, *Characteristics of a 1550 nm Wavelength Loss-Minimized Single-Mode Optical Fibre Cable*.
15. ITU-T Recommendation G.655 version 10, “Characteristics of a Non-zero Dispersion-Shifted Single-Mode Optical Fiber Cable”, October 2000.
16. ITU-T Recommendation G.652, “Characteristics of a Single-Mode Optical Fiber Cable”, April 1997.
17. ITU-T Recommendation G.653, “Characteristics of a Dispersion-Shifted Single-Mode Optical Fiber Cable”, April 1997.
18. ITU-T Recommendation G.650, “Definition and Test Methods for the Relevant Parameters of Single-Mode Fibres”, 1996.
19. ITU-T Recommendation G.661, “Definition and Test Methods for the Relevant Generic Parameters of Optical Fiber Amplifiers”, November 1996.
20. ITU-T Recommendation G.662, “Generic Characteristics of Optical Fiber Amplifier Devices and Sub-systems”, July 1995.
21. ITU-T Recommendation G.663, “Application Related Aspects of Optical Fiber Amplifier Devices and Sub-systems”, October 1996.
22. L.G. Raman, *Fundamentals of Telecommunications Network Management*, IEEE Press, New York, 1999.
23. N.A. Olsson and J. Hegarty, “Noise Properties of a Raman Amplifier”, *IEEE Journal of Lightwave Technology*, vol. LT-4, no. 4, April 1986, pp. 396–399.
24. Y. Sun, A.K. Srivastava, J. Zhou, and J.W. Sulhoff, “Optical Fiber Amplifiers for WDM Optical Networks”, *Bell Labs Techn. J.*, vol. 4, no. 1, 1999, pp. 187–206.
25. A. Evans, “Raman Amplification in Broadband WDM Systems”, Technical Digest OFC 2001, paper TuF4-1, March 2001.
26. K. Vilhelmsson, “Simultaneous Forward and Backward Raman Scattering in Low-Attenuation Single-Mode Fibers”, *Journal of Lightwave Technology*, vol. LT-4, no. 4, 1986, pp. 400–404.
27. P.M. Krummrich, R.E. Neuhauser, and C. Glingener, “Bandwidth Limitations of Broadband Distributed Raman Fiber Amplifiers for WDM Systems”, Technical Digest OFC 2001, paper MI3-1, March 2001.

28. B. Giles and E. Desurvire, "Modeling Erbium-Doped Fiber Amplifiers", *Journal of Lightwave Technology*, vol. 9, February 1991, pp. 271–283.
29. E. Desurvire, "Erbium-Doped Fiber Amplifiers", Wiley, New York, 1994.
30. S. Aozasa, T. Sakamoto, T. Kanamori, K. Hoshino, K. Kobayashi, and M. Shimizu, "Tn-Doped Fiber Amplifiers for 1470-nm-Based WDM Signals", *IEEE Photonics Technology Letters*, vol. 12, no. 10, October 2000, pp. 1331–1333.
31. G. Eisenstein, "Semiconductor Optical Amplifiers", *IEEE Circuits and Devices Magazine*, vol. 5, no. 4, July 1989, pp. 25–30.
32. R.J. Mears, L. Reekie, I.M. Jauncey, and D.N. Payne, "Low-Noise Erbium-Doped Fiber Amplifier Operating at 1.54 μm ", *Electronic Letters*, vol. 23, no. 19, September 1987, pp. 1026–1028.
33. E. Desurvire, J.R. Simpson, and P.C. Becker, "High-Gain Erbium-Doped Traveling-Wave Fiber Amplifiers", *Optical Letters*, vol. 12, no. 11, November 1987, pp. 888–890.
34. ITU-T Recommendation G.957, "Optical Interfaces for Equipments and Systems Relating to the Synchronous Digital Hierarchy", 1995.
35. ITU-T Draft Recommendation G.959, "Optical Networking Physical Layer Interfaces", February 1999.
36. ITU-T Recommendation G.671, "Transmission Characteristics of Passive Optical Components", November 1996.
37. ITU-T Recommendation G.691 "Optical Interfaces for Single Channel STM-64, STM-256 Systems and Other SDH Systems with Optical Amplifiers", 2000.
38. ITU-T Draft Recommendation G.692, "Optical Interfaces for Multichannel Systems with Optical Amplifiers", October 1998.
39. ITU-T Recommendation G.707, "Network Node Interface for the Synchronous Digital Hierarchy", 1996.
40. ITU-T Draft Recommendation G.709, "Network Node Interface for the Optical Transport Network (OTN)", October 1998.
41. S.V. Kartalopoulos, *Next Generation SONET/SDH: Voice and Data*, IEEE/Wiley, 2004.
42. ITU-T Recommendation G.7041/Y.1303, "The Generic Framing Procedure (GFP) Framed and Transparent", December 2001.
43. ITU-T Recommendation G.7042/Y.1305, "Link Capacity Adjustment Scheme (LCAS) for Virtual Concatenated Signals", November 2001.
44. ITU-T Draft Recommendation G.874, "Management Aspects of the Optical Transport Network Element", October 1998.
45. ITU-T Draft Recommendation G.875, "Optical Transport Network Management Information Model for the Network Element View", October 1998.
46. D.K. Hunter et al., "WASPNET: A Wavelength Switched Packet Network", *IEEE Communications Magazine*, vol. 37, no. 3, March 1999, pp. 120–129.
47. E. Modiano, "WDM-Based Packet Network", *IEEE Communications Magazine*, vol. 37, no. 3, March 1999, pp. 130–135.
48. O. Leclerc, "Optical 3R Regeneration for 40 Gbit/s Line-Rates and Beyond", Technical Digest OFC 2002, paper TuN1, March 2002, pp. 79–81.
49. M.L. Nielsen, "Experimental Demonstration of All-Optical 2R Regeneration at 10 Gb/s in a Novel MMI-SOA Based Device", Technical Digest OFC 2002, paper TuN2, March 2002, pp. 81–83.
50. Telcordia (formerly Bellcore), TR-NWT-917, "Regenerator", October 1990.
51. Y. Wang and S.V. Kartalopoulos, "An Analytic Comparison of Routing and Wavelength Assignment (RWA) Algorithm in WDM Optical Networks", *Proceedings of the 2005 Oklahoma Symposium on Information Technology and Entrepreneurship (ITE'05)*, April 19–20, Oklahoma City, OK, 2005, pp. 65–71.
52. Y. Wang and S.V. Kartalopoulos, "Analysis and Implementation of Reconfigurable Optical Ring Network with Minimal Wavelength Blocking", *Proceedings of the 4th IASTED Multi-Conference, Wireless and Optical Communications*, Banff, Canada, July 8–10, 2004, pp. 808–813.
53. Y. Wang, *A New highly-Efficient Routing and Wavelength Assignment (RWA) Algorithm with QoS Considerations for Multi-service Mesh Topology Optical Networks*, PhD Dissertation, The University of Oklahoma, School of Electrical Engineering, ECE/TCOM, 2005.
54. S.V. Kartalopoulos, "Consumer Communications in the Next Generation Access Network," *Proceeding of the IEEE CCNC 2004 Conference*, Las Vegas, January 5–8, 2004, pp. 273–278.
55. ITU-T Recommendation G.983.1, "Broadband Optical Access Systems Based on Passive Optical Networks (PON)", January 2005.
56. ITU-T Recommendation 984.3, "Gigabit-Capable Passive Optical Networks (G-PON): Transmission Convergence Layer Specification", February 2004.
57. D.B. Buchholz et al., "Broadband Fiber Access: A Fiber-to-the-Customer Access Architecture", *Bell Labs Techn. J.*, vol. 4, no. 1, 1999, pp. 282–299.

58. G.C. Wilson et al., "FiberVista: An FTTH or FTTC System Delivering Broadband Data and CATV Services", *Bell Labs Techn. J.*, vol. 4, no. 1, 1999, pp. 300–322.
59. N. Kashima, *Passive Optical Components for Optical Fiber Transmission*, Artec, Boston, 1995.
60. ITU-T Recommendation G.652, "Characteristics of a Single-Mode Optical Fibre Cable", October 2000 (Table G.652.C lists parameters of the water-free fiber).
61. A. Sierra and S.V. Kartalopoulos, "Evaluation of Two Prevalent EPON Networks Using Simulation Methods", *Proceedings of the Advanced International Conference on Telecommunications 2006 (AICT'06)*, Guadeloupe, French Caribbean, February 19–22, 2006, on CD-ROM, session AICT-3, ISBN: 0-7695-2522-9, Library of Congress: 2005937760.
62. S.V. Kartalopoulos, "Next Generation Hierarchical CWDM/TDM-PON Network with Scalable Bandwidth Deliverability to the Premises", *Optical Systems and Networks*, vol. 2, 2005, pp. 164–175.
63. ITU-T Recommendation G.983.2, "ONT Management and Control Interface Specification for B-PON", 2005.
64. ITU-T Recommendation G.Imp983.2, "Implementer's Guide to G.983.2(2002)", 2006.
65. ITU-T Recommendation G.983.5, "A Broadband Optical Access System with Enhanced Survivability", 2002.
66. ITU-T Recommendation G.983.6, "ONT Management and Control Interface Specification for B-PON System with Protection Features", 2002.
67. ITU-T Recommendation G.983.7, "ONT Management and Control Interface Specification for Dynamic Bandwidth Assignment (DBA) B-PON", 2001.
68. ITU-T Recommendation G.983.8, "B-PON OMCI Support for IP, ISDN, Video, VLAN Tagging, VC Cross-Connections and Other Select Functions", 2003.
69. ITU-T Recommendation G.983.10, "B-PON ONT Management and Control Interface (OOMCI) support for Digital Subscriber Line interfaces", 2004.
70. ITU-T Recommendation G.984.1, "Gigabit-Capable Passive Optical Network (GPON): General Characteristics", March 2003.
71. ITU-T Recommendation G.984.2, "Gigabit-Capable Passive Optical Network (GPON): Physical Media Dependent (PMD) Layer Specification", March 2003.
72. ITU-T Recommendation G.984.3, "Gigabit-Capable Passive Optical Network (GPON): Transmission Convergence Layer specification", July 2005.
73. ITU-T Recommendation G.984.4, "Gigabit-Capable Passive Optical Network (GPON): ONT Management and Control Interface Specification", 2004.
74. S.V. Kartalopoulos, "A Global Multi-satellite Network", 5,602,838, February 11, 1997.
75. S.V. Kartalopoulos, "A Global Multi-satellite Network", ICC'97, Montreal, Canada, 1997, pp. 699–698.
76. S.V. Kartalopoulos, "Free Space Optical Nodes Applicable to Simultaneous Ring & Mesh Networks", *Proceedings of the SPIE European Symposium on Optics and Photonics in Security and Defense*, Stockholm, Sweden, September 11–16, 2006, paper no. 6399-2.
77. S.V. Kartalopoulos, "Free Space Optical Mesh Networks For Broadband Inner-city Communications", *NOC 2005, 10th European Conference on Networks and Optical Communications*, University College London, July 5–7, 2005, pp. 344–351.
78. S.V. Kartalopoulos, "Surviving a Disaster", *IEEE Communications Magazine*, vol. 40, no. 7, July 2002, pp. 124–126.
79. J.M. Wallace and P.V. Hobbs, *Atmospheric Science: An Introductory Survey*, Academic Press, Orlando, 1977.
80. I.I. Kim, M. Mitchell, and E. Korevaar, Measurement of Scintillation for Free-Space Laser Communication at 785 nm and 1550 nm", *Optical Wireless Communications II*, Proceedings of SPIE, vol. 3850, 1999, pp. 11–19.

Chapter 4

Next Generation SONET/SDH

4.1 Traffic and Service Convergence

Voice service has been around for more than hundred years and currently it experiences a moderate growth, not so much because of landlines but because of mobile telephony; to date, almost everyone has a pocket telephone, including most schoolchildren; even remote villages in the Himalayas that previously had no telephones now have mobile telephone service. In contrast, within the last few years, data services have experienced an explosive growth due to the Internet and other data services.

The original synchronous network was developed to be highly reliable and functional in most adverse natural conditions, including power outages and earthquakes. As such, its cost was considered high for asynchronous data services that did not require real-time deliverability. Thus, the originally data-only Internet was developed to offer non-real time service or best effort at low cost. The Internet proved itself for its low-cost service, and also for its unreliability and vulnerabilities to security threats.

In an evolutionary and strategic move, new versions of the Internet protocol have been developed to cope with the addressing space and also to improve the deficiencies of the predecessor protocols; the already dubbed next generation Internet is currently known as IP version 6 or IPv6.

IPv6 defines an extended header with address space of 128 bits (i.e., 2^{128} Internet addresses), dynamic assignment of addresses, improved options, improved scalability, new traffic mechanisms, packet labeling for better defined traffic flow, real-time any-cast services, and it includes authentication and secure encapsulation. That is, IPv6 emulates the robustness and inherent security of the synchronous network and in fact it threatens traditional voice and video services with new Internet offered services such as *voice over the Internet protocol* (VoIP) and *video over the Internet protocol* (Video-o-IP).

In response to market demands for diversified services, the next generation synchronous network also offers traditional and data-centric services with flexible traffic allocation, intelligent routing schemes, elastic bandwidth, multicast capability, better management strategies, future-proofed technology, increased network efficiency and low cost that is competitive with the next generation Internet. Thus, the next generation Internet and the next generation synchronous networks are converging to a network that offers voice, video, and data services with quality of service capability that is defined by the customer, yet maintaining the network reliability, protection, availability, robustness, and real-time services that my grandfather was used to have.

SONET/SDH has been a protocol that was developed in the 1980s for synchronous optical networks with single wavelength over single-mode fiber links to offer services that scale from DS0 to DS3 and higher, meeting real-time, robustness, superb network and service protection, primarily over two-fiber or four-fiber ring optical topology, point-to-point topology and interconnected rings that effectively emulated a mesh topology [1]. The protocol was based on specific size tributary

units (TU in SDH) or virtual tributaries (VT in SONET), Fig. 4.1, that were mapped in specific size payload envelops, Fig. 4.2, using synchronized byte multiplexing.

The capacity and data rate equivalent of VTs depends on the number of columns (the number of rows is always 9) which in SONET are 3, 4, 6, and 12. Because a SONET/SDH frame is transmitted within 125 μ s, so is each TU/VT and each byte in a virtual container/tributary; the data rate of each byte in any TU/VT is equivalent to 64 Kbps; Table 4.1 tabulates the equivalent data rates per VT, and Table 4.2 tabulates it for TU.

For various operation, maintenance, administration, and control functions, the overhead of SONET frames was defined according to line, section, and path, shown in Fig. 4.3. The mapping process follows a specific order, shown in Fig. 4.4.

The network topology, switch to protection, and data-rate objectives were met and perhaps surpassed, and the initially used data rates of up to 622 Mbps (OC-12) were extended up to OC-768 (40 Gbps), Table 4.3.

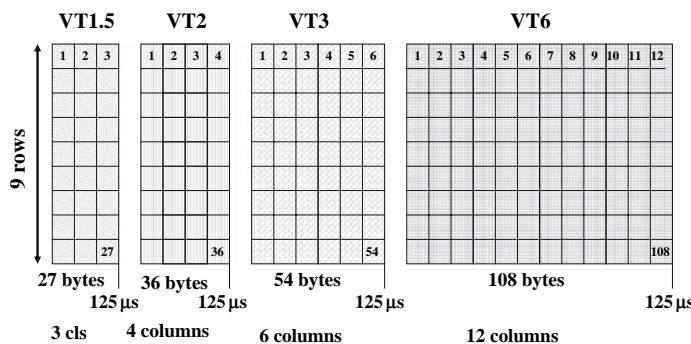


Fig. 4.1 Only specific size containers carry payload in SONET/SDH

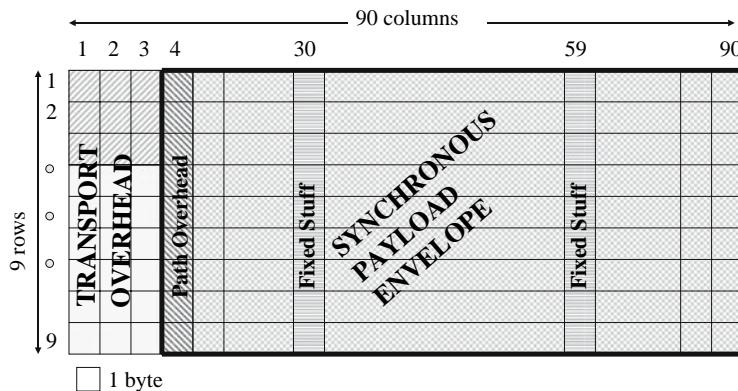


Fig. 4.2 The specific fields of a STS-1 frame

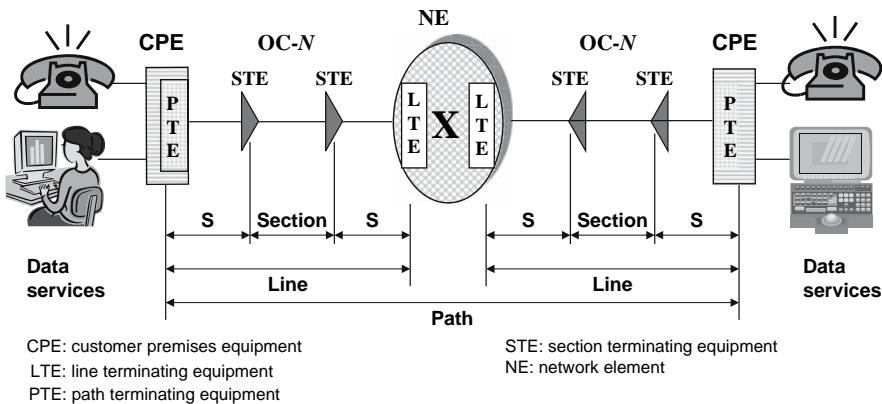
Table 4.1 Equivalent data rate for SONET VTs

VT type	Columns/VT	Bytes/VT	VTs/group	VTs/SPE	VT payload rate (Mbps)
VT1.5	3	27	4	28	1.728
VT2	4	36	3	21	2.304
VT3	6	54	2	14	3.456
VT6	12	108	1	7	6.912

Table 4.2 Equivalent data rate for SDH VCs (per X.85/Y.1321)

VC type	VC bandwidth (Mbps)	VC payload (Mbps)
VC-11	1.664	1.600
VC-12	2.240	2.176
VC-2	6.848	6.784
VC-3	48.960	48.384
VC-4	150.336	149.760
VC-4-4c	601.344	599.040
VC-4-16c	2,405.376	2,396.160
VC-4-64c ^a	9,621.504	9,584.640

^a For further study

**Fig. 4.3** Definition of path, line, and section used in the SONET/SDH frame

SONET/SDH had been so successful that soon the synchronous data rate over fiber was exhausted and the telecommunications industry looked into advanced optical and photonic technology to solve the so-called *fiber exhaust problem*. The technological solution to this problem was wavelength division multiplexing (WDM); that is, multiplex more than one (data-modulated) wavelength in the same single-mode fiber so that one fiber now transports a multiplicity of optical channels, and an equal multiple of data rates.

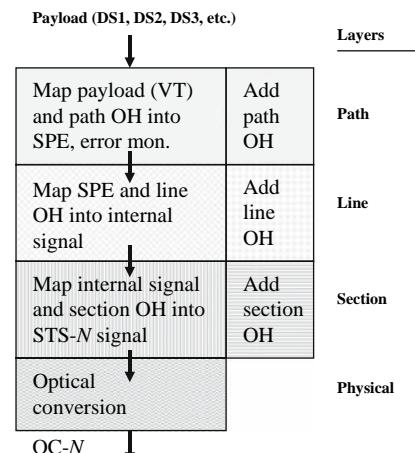
**Fig. 4.4** To achieve a SONET/SDH signal, a specific mapping process is followed by which corresponding overhead is added at each layer

Table 4.3 ITU-T data rates for SONET/SDH

Signal designation			
SONET	SDH	Optical	Line rate (Mbps)
STS-1	STM-0	OC-1	51.84 (52 M)
STS-3	STM-1	OC-3	155.52 (155 M)
STS-12	STM-4	OC-12	622.08 (622 M)
STS-48	STM-16	OC-48	2,488.32 (2.5 G)
STS-192	STM-64	OC-192	9,953.28 (10 G)
STS-768	STM-256	OC-768	39,813.12 (40 G)

OC-*N*: optical carrier-level *N*

STS-*N*: synchronous transport signal-level *N*

STM-*N*: synchronous transport module-level *N*

SONET/SDH over WDM however raised certain issues pertaining to traffic efficiency, service flexibility, service protection, and cost, which with the emergence and competition of data-centric networks (Ethernet, Internet, etc.) became more pronounced and needed to be addressed. This led to a competitive next generation protocol that is known as *next generation SDH/SONET* (NG-S), which was also dependent on specific other new protocols such as the *generic multi-protocol label switching* (GMPLS), *link access procedure SDH* (LAPS), the *generic framing protocol* (GFP) and the *link capacity adjustment scheme* (LCAS). With the new protocols, the NG-S now is capable of transport over adaptable routes in a variety of network topologies (ring and mesh) synchronous traffic such as voice, video, and asynchronous such as Internet, Ethernet, ATM, IP/PPP, fiber channel (FC), fiber connectivity (FICON), ESCON, and other future data protocols intelligently and cost-efficiently [2].

4.2 Next Generation SONET/SDH Networks

Although the original SONET/SDH was developed for the ring topology, the next generation is flexible for ring and for mesh. The mesh topology has excellent link and service protection because nodes may be reconfigured to reroute traffic bypassing failures or congested areas. Faults (channel or link) are detected with optical power detectors and performance estimation thresholds. Reconfiguration can be achieved either autonomously or using sophisticated network management procedures that also include traffic balancing and traffic grooming. Thus, a next generation synchronous optical network was needed to provide a standardized, robust, and efficient method that transports all types of data and packets (e.g., IP, Ethernet, fiber channel) over SONET/SDH (DoS), in addition to synchronous traditional TDM traffic.

4.2.1 Next Generation Ring Networks

The next generation optical ring (NG-OR) will conform to all previously known ring topologies, unidirectional single fiber, bidirectional single fiber, two-fiber bidirectional, four-fiber bidirectional, and so on. In addition, each wavelength will carry data rates from OC-48 to OC-192, and, in certain cases OC-768. Some wavelengths may also carry raw 1 or 10 GbE.

Ring nodes will consist of an optical add-drop multiplexer (OADM) and a network element that disaggregates/aggregates traffic (in the electronic regime). As a consequence, the network elements in the NG-OR support a variety of interfaces that provide aggregation, grooming, and switching capabilities; they respond to alarm and error SONET/SDH conditions, and they support the multi-service provisioning platform (MSPP). Some nodes provide bandwidth and wavelength management

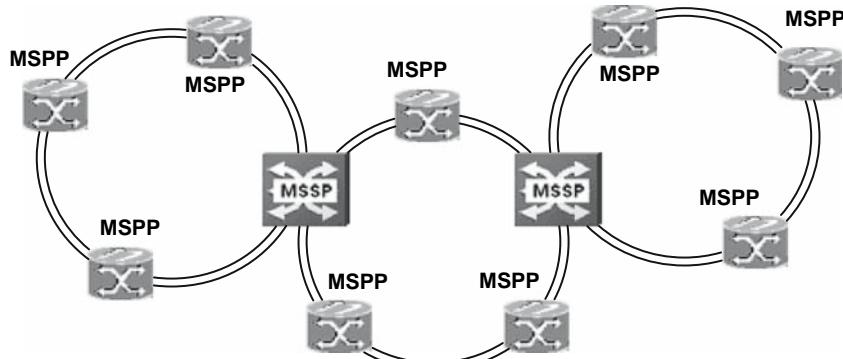


Fig. 4.5 Interconnected next generation optical rings support MSSP and MSPP

and they are able to connect two or more NG-ORs supporting the multiservice switching platform (MSSP), Fig. 4.5. Thus, ring nodes receive a diverse client payload of synchronous and asynchronous data, and they are able to encapsulate in GFP and map in NG-S frames.

The NG-ORs will exhibit advanced fault detection strategies and advanced signaling protocols such as the generalized multi-protocol label switching (GMPLS), which is an evolution of the multi-protocol label switching (MPLS) standard. The key objective is to protect traffic, when a wavelength degrades beyond the acceptable threshold or when a fault occurs, and to allow secure data to flow over a secure network.

4.2.2 Next Generation Mesh Networks

When several next generation ring networks are connected, a mesh network is constructed, which is known as path protected mesh network (PPMN), Fig. 4.6. In this case, the common nodes between two rings are large MSSPs that carry large capacity aggregate traffic from ring to ring.

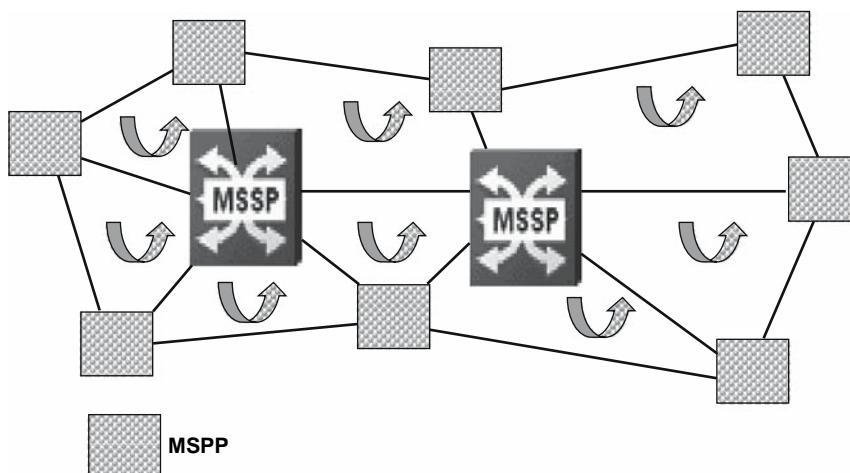


Fig. 4.6 The network elements of the PPMN are MSPPs that are capable of aggregating a variety of client data, including voice/video, and to add-drop and groom traffic

4.2.2.1 Next Generation Mesh Networks—Protection

The PPMN network combines ring and mesh protection strategies. One strategy is based on predetermined redundant paths. For every possible path, an alternate path has been identified. This method allows for the fastest “switch to protection”, although the protection path may not be the best possible at the time of failure, as congestion conditions may occur unpredictably over the end-to-end path, particularly when it crosses subnetworks that are operated by different network operators, Fig. 4.7.

Another strategy is based on algorithms (the shortest path, constraint based, such as the least congested path or most available path, and others well known from the generalized multi-protocol label switching (GMPLS)) to identify the best possible path available. These algorithms require knowledge of the status of network nodes, and, therefore, they require extensive signaling and complex protocols. Such algorithms are slow in finding the protected path but they do find the best available at the time. Yet another strategy combines quick algorithms that, based on network metrics, identify the best available protection path from a set of predetermined redundant paths.

PPMN resolves multiple failure conditions on the network, link, and channel (wavelength) level. Nodes are provisioned to reroute traffic away from a failure or congestion condition. Faults are detected with power detectors and performance parameter thresholds. Reconfiguration can be autonomous according to SONET/SDH standards and new wavelength management strategies or it can be with sophisticated multi-protocols that perform traffic balancing and traffic grooming.

4.2.2.2 Next Generation Mesh Networks—Traffic Management

The next generation intelligent optical mesh network consists of network elements and fiber links. Each fiber link has a maximum capacity calculated from the product (number of wavelength) \times (bit rate per wavelength). However, the effective traffic per fiber link is less than this, as many frames or packets over each wavelength may be either idle or frames for network operations, administration, and management (OA&M). Thus, although the network elements may handle the same amount of maximum traffic, bandwidth management deals with balancing the effective traffic per wavelength and per fiber link: fast, without excessive complexity, and cost-efficiently. This is accomplished by monitoring link status and traffic across the network. Monitoring traffic in the next generation network requires intelligence because traffic is dissimilar (voice, video, high-speed data of various protocols, such as IP, Ethernet, etc.).

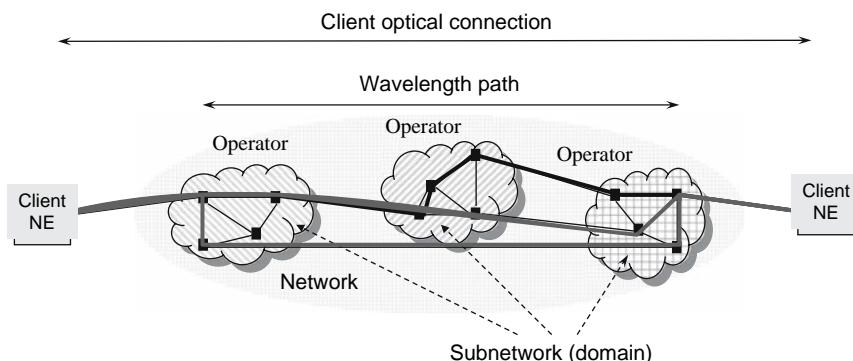


Fig. 4.7 A network may consist of subnetworks. Each sub-net may be managed by a different operator

4.2.2.3 Next Generation Mesh Networks—Wavelength Management

As already described in Chap. 3, when lightpath connectivity is requested, then the best route across a mesh network is searched for. Depending on network capability and routing algorithm, a wavelength assignment over the best path is made, which may consist either of a single (and same) wavelength or concatenated (and different) wavelengths. At this point, it is important to identify certain issues related to wavelength assignment.

In the case of the same wavelength assignment over the complete optical path, each optical switching node on the path has been provisioned with the input–output connectivity. That is, each node “knows” the source, the wavelength number, and the destination for each wavelength through it. However, in the case of concatenated wavelengths and because wavelength conversion (or translation) is needed at each optical switching node, the next node needs to “know” where the source, the destination, and the wavelength number at the input and the wavelength number at the output are.

Clearly, the latter case requires intelligent protocol with extensions and more complex wavelength management over the wavelength switching network. In traditional optical networks, wavelength management did not involve concatenated wavelengths (but only same wavelength continuity). The next generation (DWDM) optical network however becomes more intelligent and more efficient in traffic management, in wavelength, and other resource management (tunable lasers, tunable filters, wavelength converters, etc.), with more intelligent protocols that minimize the probability of blocking and thus increase efficiency.

To describe the relationship between wavelength assignment and blocking probability, consider a (DWDM) network element with a switching fabric with K fibers with N channels (wavelengths) in the ingress direction and K fibers with N channels in the egress; thus, there is a total of $N \times K$ wavelengths to be switched. From this, we assume a 50–50 engineering rule; that is, 50 % of the channels pass through express (or in transit) as a result of static pre-provisioning, and 50 % are to be dynamically switched. Thus, the problem reduces to switching $N \times K/2$ or $N^* \times K$, where $N^* = N/2$. If N^* wavelengths from one fiber are to be switched, then $(N - N^*)$ channels are available from other fibers. However, there are $(K - 1) \times N^*$ potential wavelengths contending for the same wavelength space $(N - N^*)$, where $(N - N^*)$ is much smaller than $(K - 1) \times N^*$. Clearly, this is a wavelength contention situation where blocking may occur. On the positive side, the 50–50 rule increases traffic efficiency of the network, which if intelligently engineered, the number of wavelength converters becomes better manageable and cost-effective since converters are needed for all wavelengths.

Wavelength conversion or translation in opaque switches is indirect; it converts all received optical signals (wavelengths) to electrical and back to optical; thus the wavelength translation is achieved indirectly. In this case, opaque nodes keep connectivity tables with source and destination identification codes as well as wavelength numbers in the ingress/egress directions. Although opaque nodes are cost-inefficient, nevertheless with current optical technology, they are necessary for every 7–10 all-optical concatenated nodes or at the interface between subnetworks. The reason is that currently opaque nodes provide the only satisfactory solution to a comprehensive signal retiming, reshaping, and amplification (or 3R).

Wavelength conversion is predominantly managed with two different strategies: (centralized) network wavelength management and distributed wavelength management.

- In the centralized case, a network wavelength management function provisions each node with *wavelength assignments* establishing semi-static cross-connectivity over selected paths. This case depends on a centralized database and algorithm that finds the optimum shortest and bandwidth efficient path with the fewer wavelength conversions. This case also implies that all communications interfaces with the various subnetworks or domains are compatible; this may become an issue when the path extends over a multi-vendor network.

- In the distributed case, there is an additional optical channel that is common to all nodes and over which control messages flow; this is known as *supervisory channel* (SUPV). These messages contain the input–output wavelength associations, in addition to other management messages. Thus, optimization of wavelength reassignment is left to each node.

The supervisory channel conveys messages from node to node very fast and thus it allows for *dynamic node reconfigurability*. The speed of dynamic reconfigurability is bounded by the switching speed of the fabric, by the acquisition time of wavelength converters and other tunable components on the path (such as filters, lasers, etc.), by the time required to communicate the message to the control unit and back (latency), and by the processing time.

Dynamic system reconfigurability is also required for system and *network upgrades, scalability*, and *service restoration*. Network upgrades entail downloading new software versions and new system configurations. During network scalability and upgrades, service should not be affected.

4.2.2.4 Next Generation Mesh Networks—Network Management

The next generation intelligent optical network will manage the network elements with a simplified management protocol suite. ITU-T has defined the general management functionality known as Fault, Configuration, Accounting, Performance, and Security, which is known as FCAPS. FCAPS is not the responsibility of a specific layer of the TMN architecture but different layers perform portions of FCAPS management functions. For example, as part of fault management, the EML logs in detail each discrete alarm or event, it then abstracts (or filters) the information and forwards it to an NMS (at the NML layer), which performs alarm correlation across multiple nodes and technologies and root-cause analysis.

4.2.2.5 Next Generation Mesh Networks—Service Restoration

The next generation all-optical network consists of a myriad of optical and photonic components over the end-to-end path. As a result, component failure (including fiber cuts), component degradation due to aging, specification degradation due to environmental condition changes (such as temperature and stress), and photon–matter interactions will affect the quality of one or more signals on the path and thus the quality of service. Among the various degradation contributors are spectral drift and spectral noise, jitter, optical power attenuation and also loss, amplification gain drift, and so on.

Despite the significance, each degrading contributor has the quality of each signal and hence service needs to be monitored, and a strategy must be incorporated in each node of the overall network (from access to backbone) to assure that service is delivered at the expected performance level on each link and on the overall end-to-end path. This means that when service is degraded below an acceptable threshold, the network is intelligent enough to perform service restoration either autonomously (in the case of distributed control) or via intelligent centralized control. Service restoration is the action to either remove the affecting cause or to move the affected channel from one wavelength to another. This action requires certain wavelengths to be reserved for service restoration, and in some cases, it may also necessitate wavelength conversion. Nevertheless, in multichannel (WDM) optical networks, service degradation may be on different levels. We classify three service degradation cases: single channel service degradation, multiple service degradation (over a single fiber), and all-channel service degradation (over a single fiber) [3, 4]. Each degradation classification requires different complexity and restoration strategy.

- Single channel service restoration is the simplest of all cases. However, the channel may have been degraded on one or more links over the overall path. Two sub-cases are distinguished, service over the overall path is over a continuous (same) wavelength and service over the overall path is over concatenated wavelengths:

- When service over the overall path is over a continuous (same) wavelength, then the degrading source needs to be localized on the specific link. Then, a process is initiated to find an alternate route and move traffic to another continuous wavelength, possibly from a set of reserved wavelengths. Clearly, this case requires a comprehensive service protection protocol (distributed or centralized) as well as good engineering service protection rules to warranty with high degree of confidence that a reserved wavelength may always be found over the overall path.
- When service over the overall path is over concatenated wavelengths, then the degrading source needs to be localized on the specific link. In this case, an autonomous channel protection over the particular link suffices. However, this case requires good engineering service protection rules to warranty with high degree of confidence that a reserved wavelength may always be found over the degraded link. In either sub-case, if the degraded or faulty component is the laser source, then typically this is addressed by a 1+1 or 1:N fault protection strategy.

- Multiple service degradation (over a single fiber) is similar to but more complex than single channel service restoration. This case is encountered when a group of channels is severely degraded, most likely because components that affect groups of channels are degraded, such as a filter, a demultiplexer/multiplexer, an amplifier, an equalizer, and so on. Service protection is also distinguished in two subcases: service over the overall path is over a continuous (same) wavelength, and service over the overall path is over concatenated wavelengths:
 - When service over the overall path is over a continuous (same) wavelength, then the degrading source needs to be localized on the specific link. Then, a process is initiated to find alternate route for each severely degraded channel. Clearly, this case requires a comprehensive service protection protocol (distributed or centralized) as well as more aggressive engineering service protection rules to warranty with high degree of confidence that a group of reserved wavelengths may always be found over the overall path each service is extended; notice that in this case, a degraded group over a link most likely is neither sourced from the same origin nor terminated at the same destination.
 - When service over the overall path is over concatenated wavelengths, then the degrading source needs to be localized on the specific link. In this case, an autonomous channel protection for each channel in the degraded group suffices. However, this case requires good engineering service protection rules to warranty with high degree of confidence that a group of reserved wavelengths may always be found over the degraded link. In either sub-case, the protection strategy may be 1+1 or K:N.
- All-channel service degradation (over a single fiber) may be caused by a fiber cut, a regenerator failure, a multiplexer or demultiplexer severe degradation, a fiber connector contamination or failure, and so on. This case is simpler to execute as it falls in the well-known fiber protection strategy such as 1+1, 1:1, 1:N, and so on.

In traditional SONET/SDH, the signal quality is monitored via the bit error rate (BER) by calculating the BIP-8 byte in the overhead; there is one BIP-8 for the line and one for the section parts of a SONET/SDH link. These calculations are recorded in the error control byte B3 (and B1, B2) of the corresponding overhead, which the next node reads and responds with a received error indication (REI-L, REI-P) if the error rate has crossed the acceptable threshold of 10^{-n} . When an automatic switch to protection (line, path, or lightpath) is triggered, SONET/SDH accomplishes this in less than 50 ms. When the path changes, the path overhead byte J1 is also updated.

4.3 Next Generation Protocols

The SONET and SDH protocols were defined prior to WDM era to transport more efficiently synchronous TDM traffic than data asynchronous traffic over single-wavelength fiber rings and over long-distance point-to-point networks. Mapping synchronous payload was defined for efficiency onto VTs (SONET) or VCs (SDH), and transport over fiber was using one of the two wavelengths, 1,300 or 1550 nm. Although SONET and SDH proved themselves for high reliability and bandwidth scalability, which over a 10-year period enjoyed a nearly 40-fold growth that indirectly stimulated an exploding growth of data services. This exploding growth however could not be supported by SONET/SDH cost-efficiently because the original SONET/SDH protocol had not defined an elastic bandwidth granularity, lacked overhead definition for a grid of lightpaths, did not utilize data bandwidth efficiently (depending on conditions, efficiency could be as low as 5 %). The reason for this is the nature of packetized data; data is asynchronous and bursty, and data protocols support packets of variable length. The bursty nature of data introduces time gaps between packets which in a synchronous protocol are filled with idle packets or frames, thusly reducing efficiency. To contrast the legacy with the next generation SONET/SDH, a comparison is made of existing versus desired features in Table 4.4.

Additionally, SONET/SDH was not flexible to support newly defined (data) protocols; in fact, although the original SONET/SDH has many overhead bytes reserved for craft communication over the line or section, it has very few for future services and alternate mappings. Thus, in an unanticipated way, SONET/SDH became a victim of its own success and a more intelligent optical network and protocols were in search that could not only support the existing and the newly emerged data services and protocols but also the future ones. In response to this, two different solutions have been defined; the next generation SONET/SDH with new protocols (NG-S) and the optical transport network (OTN).

The next generation SONET/SDH (NG-S) supports the multiservice provisioning platform (MSPP) and the multiservice switching platform (MSSP).

- The MSPP provides aggregation, grooming, and switching capabilities. It responds to alarm and error SONET/SDH conditions, and it supports new protection schemes for different topologies such as ring, multi-ring, mesh, and point to point. The significance of the MSPP is that it is the edge node that interfaces with diverse client payloads, or tributaries (OC-*n*, GbE, IP, DS-*n*). When a tributary fails, then the legacy SONET/SDH practices are adopted. That is, when the MSPP node detects a signal failure at its input, it declares loss of signal (LOS) and it generates

Table 4.4 Feature comparison between legacy and next generation SONET/SDH

	Legacy SONET/SDH	Next generation SONET/SDH
Topology	Ring and point to point only	Many (ring, mesh, point to point, tree)
Bit rate	OC- <i>n</i> (predefined)	OC- <i>n</i> and others (increased granularity)
Interfaces	OC- <i>n</i>	Supports interfaces from DS1 to OC-768
Optical channels	One per fiber (1,300/1,550 nm)	Supports DWDM
Payload efficiency	Synchronous and ATM mapping; less efficient for packet	Support all payload mappings with high efficiency, encapsulation and concatenation
Switching	Low order or high order	High order, low order, packet
Concatenation	Contiguous only	Contiguous and virtual
Reliability	High	High
Functionality	SONET/SDH defined	Multiple, integrated in the same NE
Protection strategy	<50 ms switching to protection but for channel only for ring and point-to-point topology	<50 ms switching to protection for channel, line, and path for many topologies
Cost (bandwidth-km)	High	Low

an alarm indication (AIS-L, AIS-P), which is transmitted in all affected virtual containers (VC). Nodes that receive the alarm indication respond with a received defect indication (RDI-L for line and RDI-P for path)

- The MSSP provides bandwidth and wavelength management via large, non-blocking switching fabrics (cross-connects).

4.3.1 Concatenation

Traditional SONET/SDH had defined *contiguous concatenation*. The next generation SONET/SDH has expanded this by defining *virtual concatenation*.

4.3.1.1 Contiguous Concatenation

Contiguous concatenation (CC) is defined to accommodate mapping of very long packets that exceed the capacity of the NG-S synchronous payload envelope (SPE). According to this, CC allows mapping of the packet over two or more contiguous SONET/SDH frames. However, the efficiency of mapping with CC is correlated with packet length and data rate. For example, the efficiency of 10 Mbps Ethernet mapped in contiguous legacy SONET STS-1s or SDH VC-3s is estimated to be only 20 %. Similarly, the efficiency for 100 Mbps Ethernet mapped in contiguous STS-3c or VC-4 is estimated to 67 %, and for 1 Gbps Ethernet mapped in STS-48c or VC-4-16c is estimated to 42 %.

Although contiguous concatenation may seem simple, the receiving end must be able to recognize the contiguous mapping and extract from the contiguous SPEs the packet(s). Contiguously concatenated frames have simplified section and line overhead, and they require a single path overhead column, Fig. 4.8.

4.3.1.2 Virtual Concatenation

The idea of virtual concatenation (VC) is imported from the Internet. Thus, a high-order (HO) frame or a high data rate (such as GbE) is segmented into low order (LO) smaller containers or packets, and each LO container or packet is fit in and transported independently by different SONET/SDH payloads over independent separate paths to meet efficiency. Based on this, high data rates that do not “fit” in a SONET/SDH STS-n/STM-m payload envelop are partitioned to “fit” into more than one, hence, “virtual concatenation”. For example, 1 GbE can be partitioned to “fit” in the payload of

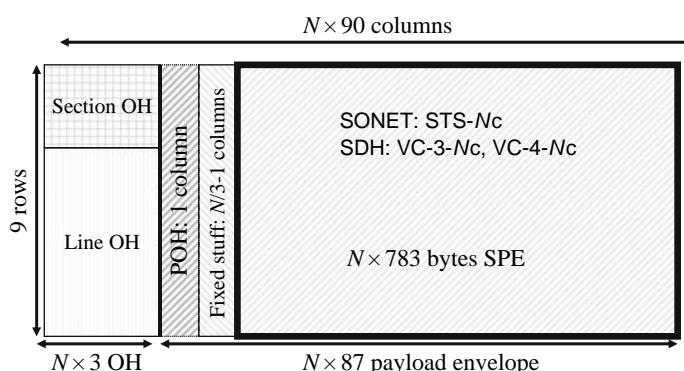
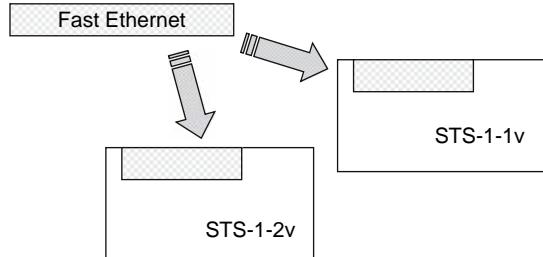


Fig. 4.8 A simplified next generation SONET/SDH supports contiguous concatenation

Fig. 4.9 Virtual concatenation in next generation SDH



two independent STS-12s, called STS-12-1v and STS-12-2v. Similarly, 100BASE-T Ethernet may be mapped in two STS-1s, STS-1-1v, and STS-1-2v, Fig. 4.9.

At a receiving point in the network, the LO containers or packets are collected and they are reassembled to their original form. A consequence of the separate independent paths is that the two containers may arrive with a *differential delay*, which implies that at the destination the containers must be buffered, arranged in the correct order, realigned, and then reassembled. This rearrangement and realignment is accomplished by several mechanisms:

- The four most significant bits of the H4 byte in the path overhead provide a count of the frame in a 16 multiframe.
- The four least significant bits of the last two consecutive H4 bytes in a 16 multiframe construct an 8-bit byte sequence indicator for all members of the same HO VC group.
- The four least significant bits of the first two consecutive H4 bytes in a 16 multiframe construct an 8-bit byte multiframe indicator for HO VC groups. This scheme can compensate for differential delay up to 256 ms.
- The K4 bytes for LO VC groups are used to implement similar frame and multiframe schemes.

Thus, although CC solves the problem of fitting very long containers or packets in SONET/SDH contiguous SPEs, VC solves the problem of transporting long-length and very high data rate packets over independent and separate SPEs with increased efficiency.

4.3.2 Generic Multi-protocol Label Switching

The generic multi-protocol label switching (GMPLS) protocol is a generalization of the previously defined by IETF multi-protocol wavelength switching (MP λ S) in order to support very high data rates and lightpath connectivity in WDM optical networks. MP λ S was an extension of a previously defined multi-protocol label switching (MPLS) protocol to include features needed for optical networking. Therefore, the understanding of these protocols helps to better understand GMPLS.

4.3.2.1 MPLS and MP λ S

The transport of data formatted (or packetized) according to a protocol (such as IP) over a network that is based on another protocol (such as ATM) requires the IP to undergo segmentation and adaptation with the addition of overhead. In general, such adaptation of one protocol (such as IP) over another protocol (such as TM) results in added overhead, latency, processing, and mismatch of supported quality of services and decreases the overall network efficiency. The multi-protocol label switching (MPLS) was defined in an effort to decrease the inefficiency or increase efficiency of multiple data networks that are one on top of the other.

According to MPLS, one or more labels are attached to IP packets when they enter a label edge router (LER) of an MPLS network domain. Labels indicate the next router destination in the MPLS

network and are calculated by a search algorithm and signaling messages to identify and establish the best path throughout the MPLS network; the path from source to destination is known as *tunnel* [5–7].

The MPLS control plane deals with routing issues and it is decoupled from the switching function, which deals with packet forwarding. When a label-switched router (LSR) receives an MPLS packet, it forwards it to one of its outputs which is selected according to the label value in the packet and the port it was received. Thus, the LSR function in the router may swap the label in the packet by another label if the packet is switched to a different output port.

Connections established with the MPLS protocol are called label-switched paths (LSP). Routing protocols determine the LSPs for predefined traffic classes, known as forward equivalent classes (FEC). FECs are specified based on constraints such as QoS parameters, entry port number, and source (originating address). The LSP is defined by the label attached to the packet. Labels are distributed in the MPLS network by a label distribution protocol (LDP); each MPLS node (LSR router) constructs input–output mapping tables based on which it routes MPLS packets. Thus, a path is defined by a sequence of labels as they have been defined and distributed by LDP.

When a failure or congestion is experienced in an LSP, the MPLS protocol provides protection by rerouting traffic. This may be accomplished either by preestablished alternative routes (required for time-critical and high-priority MPLS packets) or by recalculating another route, which requires calculations and signaling, and which is the source of label changes.

When MPLS is over WDM, the optical network control plane needs not only to find the best route available but also to assign and provision a wavelength path, that is, to establish lightpath connectivity over the WDM network. However, as previously described, there are several issues and different methods to establish lightpath connectivity in DWDM that MPLS did not efficiently address. This led to the MPLS extended version, the *multi-protocol wavelength switching* (MPλS) protocol.

4.3.2.2 GMPLS

A GMPLS node advertises its bandwidth availability and optical resources (i.e., link type, bandwidth, wavelengths, protection type, and fiber identifier) to its neighboring nodes and it also requests from its neighbors their own status via signaling messages; this is known as *neighborhood discovery*. Thus, the GMPLS algorithmic runtime must be short so that provisioning is fast and so is switch to path protection and restoration. Fast restoration is particularly important because [8, 9] WDM networks carry traffic at many gigabits per second per wavelength and long restoration time implies an enormous amount of lost packets. Switch to protection is typically according to one of the well-known strategies, 1+1 or 1:N.

GMPLS includes port switching, λ -switching and TDM. It employs search algorithms to find the best path available within a mesh optical network topology (even under impairment conditions), to provide the necessary signaling messages, to establish end-to-end and also link connectivity, topology discovery, connection provisioning, link verification, fault isolation and management, and restoration. Such algorithms are the following:

- the open shortest path first (OSPF); according to this, the routing tables (labels) in each LSR are defined and distributed by LDP;
- the intermediate system to intermediate system (IS-IS);
- the constraint-based routed label distribution protocol (CR-LDP); and
- the resource reservation protocol with traffic extension (RSVP-TE).

These algorithms find the best path that meets the traffic requirements such as required bandwidth, traffic priority, real-time aspects, deliverability, and others, which are familiar to SONET/SDH traffic types and service levels. They also monitor the established path for congestion and failures.

GMPLS, like MPLS, appends a calculated label to the packet. This label describes the physical port, the assigned wavelength, and the fiber. If the lightpath enters another node and departs from it without a change in the established lightpath, then the label remains the same. However, if there is a change in the lightpath (due to congestion, traffic balancing or as a result of switch to protection), then the node finds a new (best) path according to an algorithm; it sends downstream a RSVP-generalized label request or a label request message in CR-LDP, it recalculates a new label and it replaces the old one.

A GMPLS node consists of two functions, one that interfaces the client side or the GMPLS aggregator and another that interfaces the optical WDM network.

The network interface optically multiplexes the received traffic from the aggregator and multiplexes it in the WDM signal. This function is similar to optical add-drop multiplexing with optical cross-connect.

The GMPLS aggregator receives client signals, aggregates them, forms labels, and packets and hands them to the optical network interface. The functionality of the GMPLS aggregator (or router manager) includes the following functions:

- Manage and maintain the database of link states of established LSPs;
- Manage and maintain a database of all resources available in the node;
- The routing controller that reviews the link states and node resources finds the best path based on an algorithm (OSPF);
- The connection controller that takes actions to establish the calculated best path, modify and tear down;
- Generates RSVP Path/Resv messages for LSP setup, for modification and for tear down.

To meet quick route discovery and fast response times, GMPLS assumes distributed control and semi-dynamic provisioning. That is, once the best path has been calculated, the lightpath is established, and as long as the network remains stable, the path remains unchanged for a relatively long period. Thus, switching nodes are fast cross-connects and lightpaths are not established on a “call-by-call” basis or in real time. Instead, the node finds the best path by sending downstream a RSVP-generalized label request in CR-LDP and over a separate path requesting link establishment from one LSR node to another LSR node (according to distributed control principles). When all link requests have been granted, then the end-to-end lightpath and the label mapping at each LSR node are established.

Three standard organizations are responsible for the definition of protocols that make GMPLS possible:

- The Common Control and Management Plane (CCAMP) working group of the Internet Engineering Task Force (IETF) is responsible for GMPLS. IETF is responsible for the link management protocol (LMP), IS-IS, RSVP-TE, and CR-LDP.
- The optical internetworking forum (OIF) is responsible for the optical user-to-network interface (O-UNI), the external and internal optical network-to-network interface (O-NNI).
- The international telecommunications union-telecommunications sector (ITU-T) is responsible for network architectures [10], data communication network [11], neighbor discovery [12], routing and topology discovery, and signaling and connection management [13].

4.3.3 The Generic Framing Procedure

The Generic Framing Procedure (GFP) is a flexible encapsulation framework for traffic adaptation of synchronous broadband transport applications (DS-*n*/E-*n*), packetized data (IP, GbE, FC, etc.), as well as virtual concatenated NG-S frames with improved bandwidth utilization and efficiency by

using LCAS. It supports client control functions that allow different client types to share a channel, and it provides an efficient mechanism to map broadband data protocols (such as fiber Channel, ESCON, FICON, GbE) onto multiple concatenated STS-1 payloads in a revised SONET/SDH frame [14, 15].

The GFP protocol supports mapping of a physical or logical layer signal to a byte synchronous channel, it supports different network topologies (short reach, intermediate reach, and long reach), it exhibits low-latency of packet-oriented or block-coded data streams, and it supports differentiated quality of service (QoS) meeting service level agreement (SLA) requirements. Moreover, the GFP allows for existing circuit switching, SONET/SDH, GbE, and other packet-based protocols to be used as an integrated and interoperable transport platform that provides cost-efficiency, QoS, and SLA, as required by the client.

Accordingly, the next generation SONET/SDH differentiates from legacy SONET/SDH with its flexible encapsulation of diverse protocols onto GFP generalized frames which are mapped onto synchronous payload envelopes (SPE) of SONET/SDH to support both long packets and circuit switching services.

GFP over the next generation SONET/SDH considers that wavelength division multiplexing technology, both coarse and dense (CWDM, DWDM), which is the technology of choice in optical networks. Thus, with the flexibility of GFP over the next generation SONET/SDH over WDM, a single optical channel (wavelength) may carry a diverse client signal to improve bandwidth utilization and efficiency, Fig. 4.10.

4.3.3.1 GFP Header, Error Control, and Synchronization

GFP defines different length frames and different client-specific frame types for payload and management. To increase transmission efficiency, it time multiplexes different frames, frame by frame. If there are no client frames to be multiplexed, it multiplexes idle frames in order to provide a continuous bit stream on the transmission medium.

GFP defines a payload area with its own control fields that include linear point-to-point and ring extensions. Thus, payloads from different clients but of the same type, such as GbE, may be multiplexed using either a sequential round-robin method for synchronous payloads such as DS1 and DS3, or a well-established queuing schedule for asynchronous client payloads with substantial variability in frame length and time of arrival.

GFP defines a flexible frame structure. The GFP frame defines a “core header” and a “payload area”. The “core header” supports non-client-specific data link management functions such as delineation and payload length indication (PLI) and core header error control (cHEC).

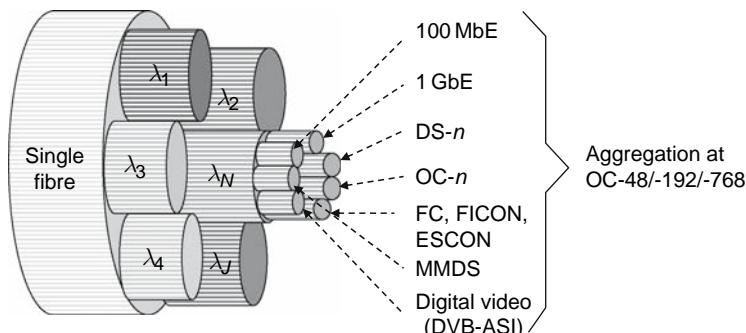


Fig. 4.10 A diverse payload type flows in a single optical channel

The “payload area” supports client-specific client-to-client connectivity and error control. It consists of three fields, Fig. 4.11:

- The “client information data” that may have a fixed or variable length bounded by two fields.
- The “payload header” field that contains specific information that pertain to payload type and error control.
- The “payload frame sequence” (FCS) field which is used for payload error control.

GFP segregates error control between the GFP adaptation process and user data. This allows for sending to the intended receiver frames that have been corrupted under the assumption that end users will use their own error-correcting codes. In synchronous applications such as video and audio, even corrupted frames are better than no frames at all particularly if they can be restored by the end user.

GFP defines two classes of functions: *common* and *client specific*. The common is for PDU delineation, data link synchronization, scrambling, client PDU multiplexing, and client-independent performance monitoring. The client specific is for mapping client PDU into the GFP payload, and for client-specific OA&M (operations, administration, and maintenance).

GFP distinguishes two types of client frames: *client data frame* (CDF) and *client management frames* (CMF). A CMF transports information related to GFP connection or client signal management. A CMF is a powerful feature that allows clients to control the client-to-client connection.

The GFP core header consists of four bytes only, Fig. 4.12. The first two define the length of the payload and the other two a standard cyclic redundancy check code (CRC-16) that protects the integrity of the core header from errored bits. The core header error control (cHEC) is able to identify multiple errors and correct single errors. The cHEC generating polynomial is $G(x) = x^{15} + x^{12} + x^5 + x^0$ with zero initialization value. At the transmitting end, where the GFP is formatted, the 16-bit CRC code is calculated over the core header, and it is stored in the third and fourth byte of

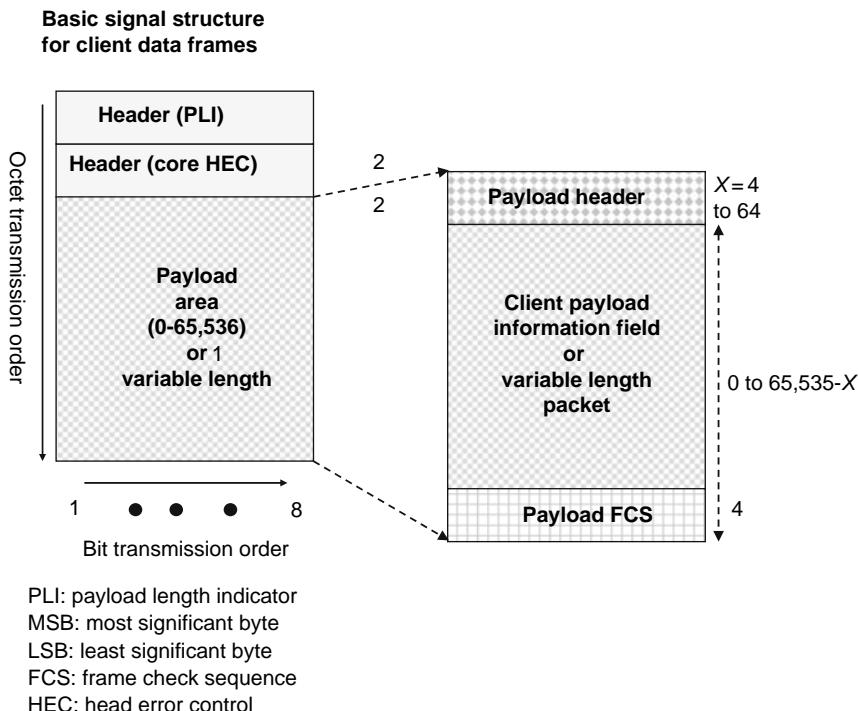


Fig. 4.11 GFP payload area

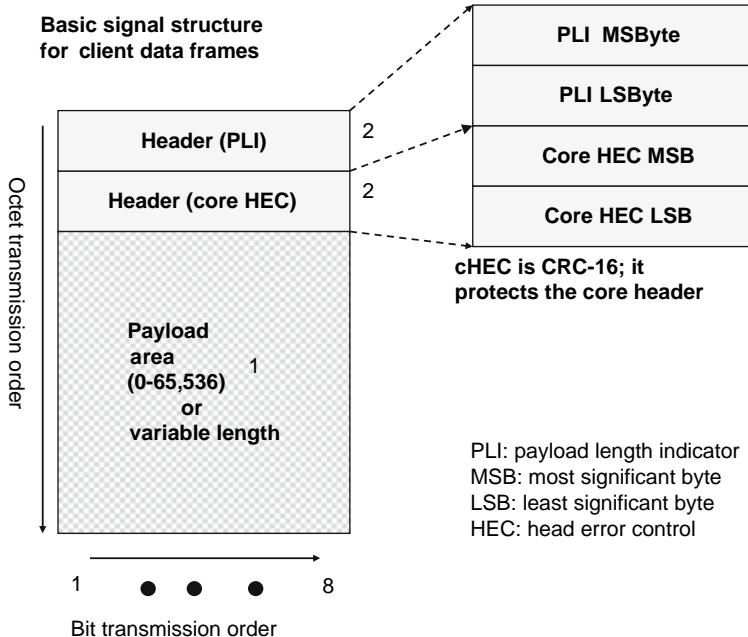


Fig. 4.12 The GFP header

the GFP core header. At the receiving end, the incoming header is calculated in real-time detecting possible multiple errors and correcting single errors.

For frame delineation (or frame synchronization), GFP uses the cHEC; this is a variant of the head-error-control (HEC) and delineation scheme used by ATM [ITU-T Rec. I.432.1]. The delineation function identifies the start of a GFP frame. This is accomplished with the CRC-16 in the two core-HEC bytes. In addition, a field in the GFP frame header contains the payload length; this may either change from frame to frame to allow for variable length PDUs, or it may remain constant to support TDM-like synchronous services.

The delineation state machine is as follows: When the first frame arrives, the CRC-16 is calculated over two bytes and it is compared with the next two bytes. If they do not match, then it advances by a bit/byte and tries again. If they match, then most likely these two bytes are the cHEC stored in the core overhead. Then, the delineation function enters the “hunt” state. From the “hunt” state, the delineation function moves to the “pre-sync” state and from there eventually to the “sync” state. GFP delineation is established when two cHEC consecutive matches. If a cHEC match fails (a non-correctable mismatch), then the delineation state machine moves to the re-synchronization state.

Based on this, payload length and error-control check (cHEC) is all the information needed for boundary delineation; this is in contrast to other methods that require header/trailing codeword delineation patterns and data embedded control bytes that require preprocessing of the client's byte stream. The cHEC delineation mechanism makes GFP applicable to very high speed fiber networks, such as OC-48 (2.5 Gbps) and above.

Because bit-rate impacts bit error rate (BER), cHEC also plays a significant role in the quality of synchronization. Thus, at 40 Gbit/s and at a $\text{BER}=10^{-7}$, the loss of sync (LOS) probability is 5×10^{-12} which amounts to a LOS every 48 min. At $\text{BER} = 10^{-9}$ the LOS probability is 5×10^{-16} and the LOS is once a year. However, an additional factor that affects GFP synchronization is the mean time to frame (MTTF) that is used in framed data applications, such as Ethernet and the like; MTTF is measured in PDUs. At first approximation, MTTF is insensitive to BER and bit rate. Thus, considering that two consecutive cHEC matches require two PDUs, then for a GFP frame

length from 66 and up to 6,000 octets, MTTF remains almost flat varying only between 1.5 and 1.6 indicating that delineation is fast. Thereafter, MTTF rises sharply indicating that delineation is slowing down as frames become longer.

GFP defines *two scrambling operations*, scrambling the core header and scrambling the payload; scrambling is performed at the transmitter and de-scrambling at the receiver. The core header is short and thus it is scrambled using a bit-by-bit complement's-two operation (exclusive OR) with a simple code, such as the pattern $0x\text{B6AB31E0}$. The payload area is much longer and thus a self-synchronizing scrambling algorithm is used. All octets in the payload area are scrambled with the $x^{43} + 1$ polynomial. Scrambling starts at the first octet after the cHEC field, it is disabled after the last octet of the frame, and its state is preserved to continue with the following frame, again starting after the cHEC field.

4.3.3.2 GFP Frame Structure

The type of payload mapped in the GFP payload area is indicated by the binary value of an 8-bit byte, the user payload type (UPI). Currently, the following payload types are defined:

- 0x01: Frame-mapped Ethernet
- 0x02: Frame-mapped PPP (including IP and MPLS)
- 0x03: Transparent-mapped fiber channel
- 0x04: Transparent-mapped FICON
- 0x05: Transparent-mapped ESCON
- 0x06: Transparent-mapped GbE
- 0x07: Reserved
- 0x08: Frame-mapped multiple access protocol over SDH
- 0x09–0xFE: Reserved
- 0x00 and 0xFF: Unavailable

GFP defines two frame types, the user data frame and the client management frame. The frame type is indicated in a 3-bit field, the payload type indicator (PTI) in the payload header, Figs. 4.13 and 4.14.

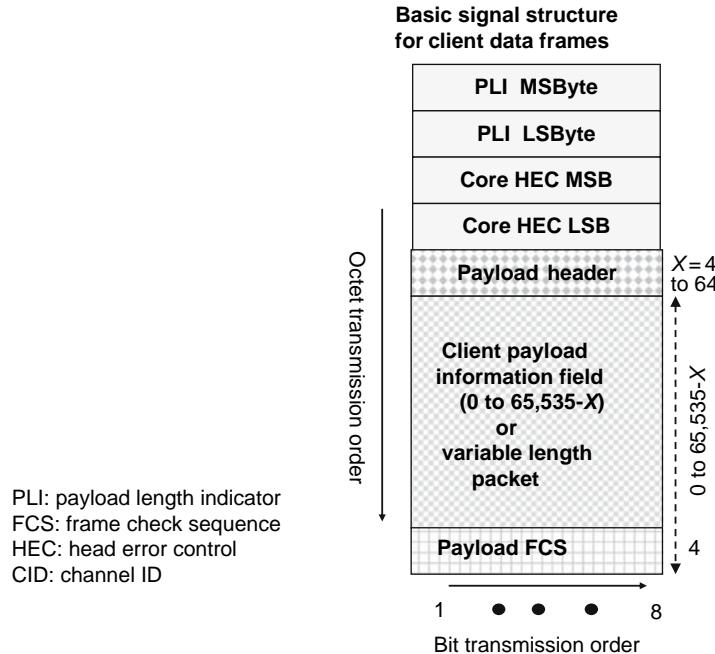
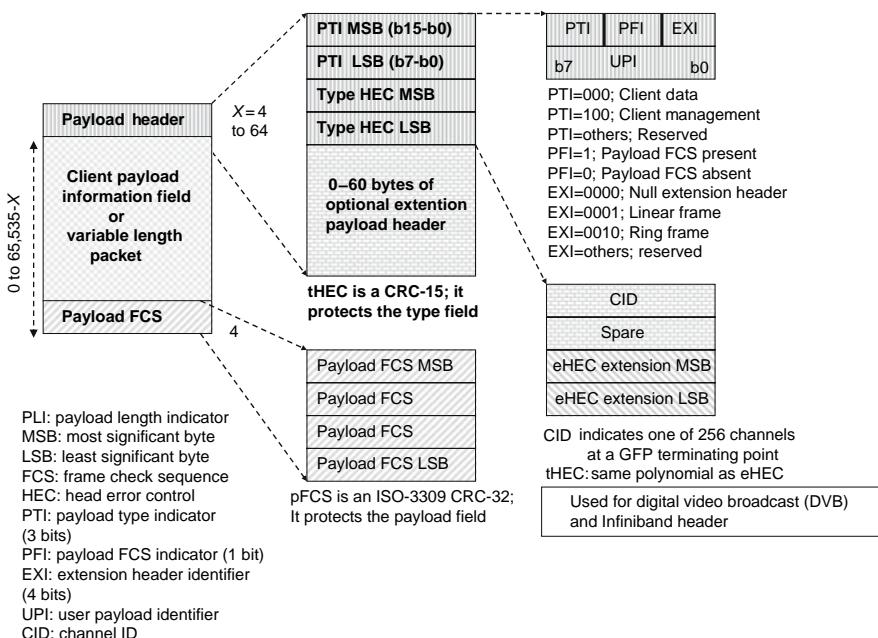
For example, PTI = 100 indicates a management frame. In this case, the value of the UPI has different meanings:

- UPI = 0x01: Failure in the client signal—loss of client signal
- UPI = 0x02: Failure in the client signal—loss of character synchronization
- UPI = Other: reserved

GFP also defines idle frames that are used to fill time during the frame multiplexing process. An idle frame consists of four octets, the core header, with all four fields set to all-zero. However, after scrambling (with a Barker-like scrambler) the all-zero changes to a code with sufficient density of ones. However, client data frames have priority over management frames and idle frames have least priority.

4.3.3.3 GFP-F and GFP-T Modes

GFP specifies two different client types, also known as transport modes, within the same transport channel, the frame-mapped GFP (GFP-F) and the transparent-mapped GFP (GFP-T).

**Fig. 4.13** The general GFP frame**Fig. 4.14** Details of the GFP frame

The GFP-F mode is optimized for packet switching applications including IP, native point-to-point protocol (PPP), Ethernet (including GbE and 10 GbE), and generalized multi-protocol label switching (GMPLS). The GFP-F features are the following:

- Frames are variable;
- It uses cHEC for delineation;
- It supports rate adaptation and multiplexing at packet level;
- It aggregates frames at the STS and VT level;
- It supports most packet data types;
- It requires MAC awareness;
- It requires buffering;
- It introduces latency;
- It supports client data frames (CDF) for both client data frames and management frames. CDF consists of 4-byte core header (CH), and 0-65,535 payload area (PA);
- It supports control frames (for idle and for OA&M).

The GFP-T mode is optimized for applications that require bandwidth efficiency and delay-sensitivity applications to include fiber channel (FC), FICON, ESCON, and storage area networks (SAN). The GFP-T features are the following:

- Fixed frame length;
- N to 1 mapping of client packets;
- It requires no buffering;
- It operates on each arrived byte;
- No latency is introduced;
- No MAC is required. Only 8B/10B coding;
- The PHY (physical) layer is terminated;
- Because there is no buffering, it retains idle frames.

To meet real-time requirements, GFP-T considers a fixed frame length and it operates on each character of a frame as it arrives; thus, it does not require buffering and it does not remove idle packets. As a consequence, special MAC is not required. In this case, in order to meet the fixed frame requirement GFP-T defines superblocks. It segments the client signal in eight octets or 64 bits. To each segment an overhead flag bit is added to form a block. Eight consecutive blocks form a superblock; however, all eight flags are collected to form an octet which is placed at the trailing end of the superblock along with 16 CRC bits, Fig. 4.15. The CRC-16 error check code is calculated over all 536 bits ($8 \times 8 \times 8 + 3 \times 8$) in the superblock and is added at the end of the superblock. The generating polynomial for the CRC-16 is $G(x) = x^{16} + x^{15} + x^{12} + x^{10} + x^4 + x^3 + x^2 + x^1 + x^0$ with zero initialization value.

In summary, according to the general scheme of NG-S, synchronous traffic is mapped in SONET/SDH (VT/TU groups), data (IP, Ethernet, FC, PPP) is encapsulated in GFP (first in GFP client dependent and then in GFP common to all payloads) and then mapped into the payload envelope of NG-S STS- n . During the adaptation to GFP and mapping in NG-S process, overhead bytes and pointers are formed to construct a NG-S frame. Fig. 4.16 depicts the logical major steps to map client traffic over NG-S.

An example of encapsulating Ethernet over GFP over NG-S is shown in Fig. 4.17.

4.3.4 LCAS

The *Link Capacity Adjustment Scheme* (LCAS) allows containers in the NG-S to be added or removed dynamically in order to meet user bandwidth requests and to also balance traffic load; container addition or deletion should be hitless (without traffic flow interruptions), Fig. 4.18.

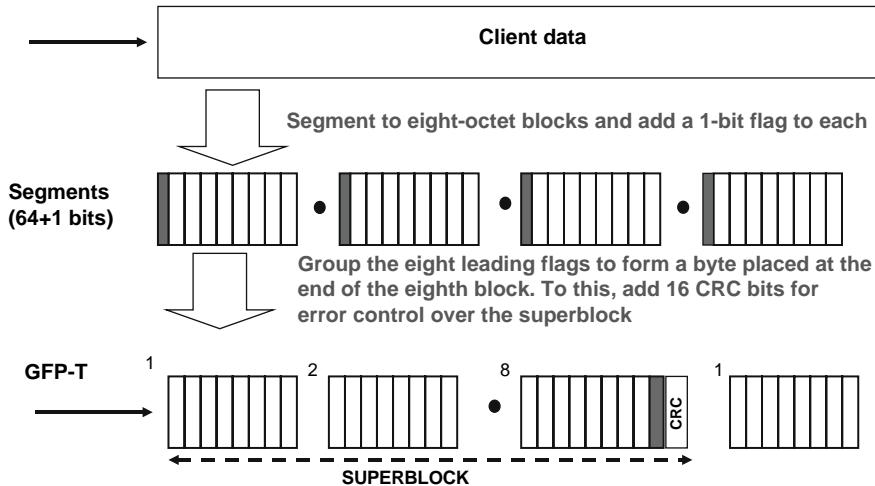


Fig. 4.15 Superblock construction with CRC

LCAS is accomplished using control packets to configure the path between source and destination; it thus adopts a decentralized control process. The control packet is transported over the H4 byte (of SONET/SDH) for high-order VC in a superframe, and over the K4 byte (of SONET/SDH) for low-order VC [16].

A superframe consists of N multiframe where each multiframe consists of 16 frames. A control packet in the current superframe describes the link status of the next superframe. Changes are proactively sent to the receiving node allowing for ample time to reconfigure. Thus, when the data packet arrives, the link reconfiguration is completed and packet switching takes place without delay. The control information in the H4 overhead byte resides in the 4-bit high nibble (bit 5 to bit 8). The nibble value defines the following:

- Fixed (0000): no LCAS mode
- Add (0001): this member to be added
- Norm (0010): no change, steady state
- Idle (0101): no part of group to be removed
- CRC-8 (0110) & (0111): control packet protection
- RS-Ack (1010): from source to destination, requested changes are accepted
- Reserved (1011)

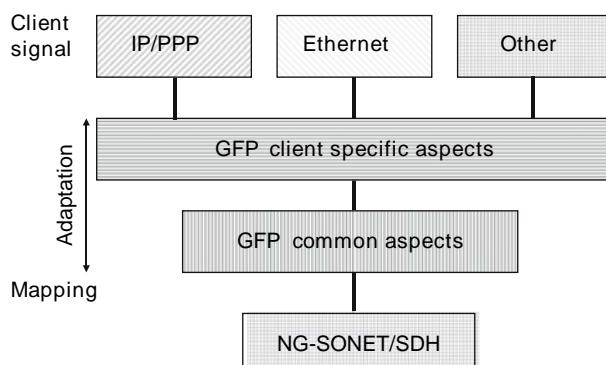


Fig. 4.16 Mapping various payload over GFP over next generation SDH

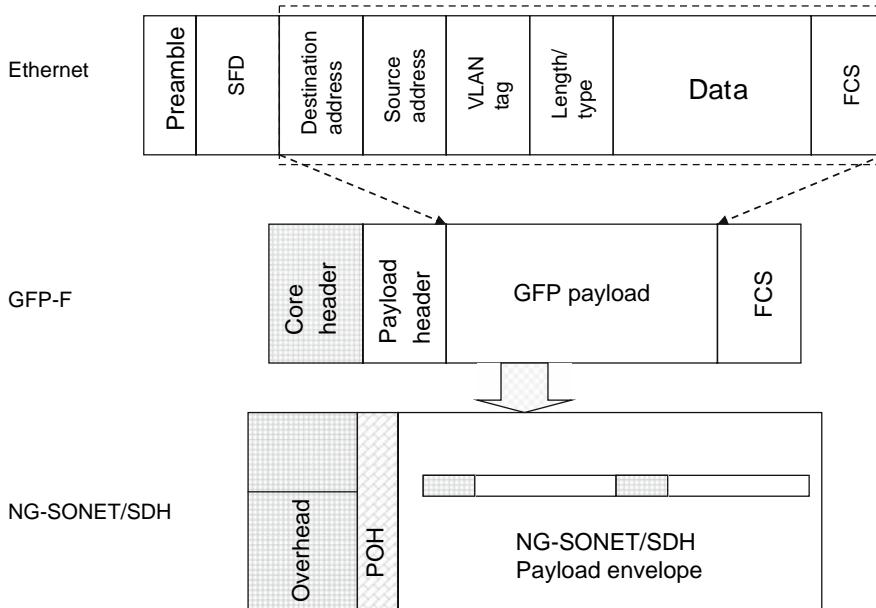


Fig. 4.17 Example: Ethernet encapsulation over GFP over SDH

- Reserved (1100)
- Reserved (1101)

Other control information over the H4 byte in the superframe is

- GID: Group ID; members in a group have same ID
- EOS: end of sequence
- DNU: Do not use, failure detected
- MST: Member status from source to destination, either OK or failed

An example of mapping client traffic over the next generation SONET/SDH including LCAS is illustrated in Fig. 4.19.

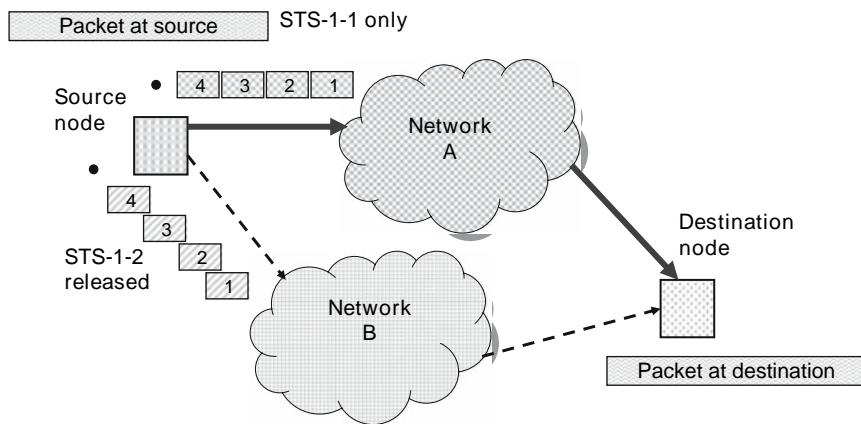
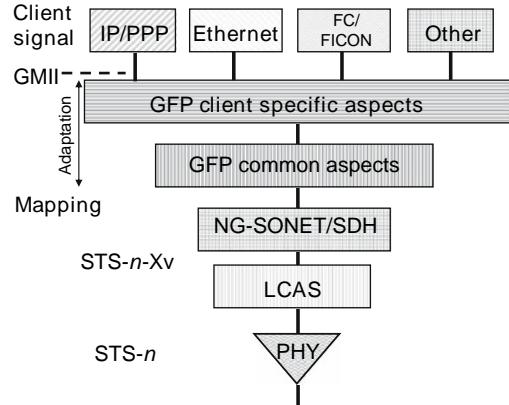


Fig. 4.18 If both STS-1-1 and STS-1-2 were allocated to transport traffic, with LCAS if STS-1-2 is not required, it is released to transport different traffic

Fig. 4.19 Different payloads over next generation SDH using LCAS



4.3.5 LAPS

The *link access procedure-SDH* (LAPS) includes data link service and protocol that are designed to transport point-to-point IP or Ethernet traffic over legacy SDH. ITU-T (X.86, p. 9) defines LAPS as “a physical coding sub-layer which provides point-to-point transferring over *SDH virtual containers* and *interface rates*.” That is, ITU-T specifies LAPS as a low-cost physical coding sub-layer to transport point-to-point IP or Ethernet traffic over SDH virtual containers and interface rates and at the same time provide low latency variance, flow control in bursty traffic, capability of remote-fault indications, ease of use and ease of maintenance. Encapsulation of IPv4, IPv6, PPP, and other layer protocols is accomplished with the *service access point identifier* (SAPI).

Two ITU-T documents address the encapsulation and rate adaptation of IP and Ethernet over LAPS: ITU-T X.85/Y.1321 defines IP over SDH using LAPS and ITU-T X.86 defines Ethernet over LAPS. ITU-T X.85 and X.86/Y.1321 Recommendations treat SONET/SDH transports as octet-oriented synchronous point-to-point links [17–19]. Thus, frames are octet-oriented synchronous multiplex mapping structures that specify a series of standard rates, formats, and mapping methods. Control signals are not required, and a self-synchronous scrambling/descrambling ($x^{43} + 1$) function is applied during insertion/extraction into/from the synchronous payload envelope. The frame structure of LAPS is illustrated in Fig. 4.20.

Starting Flag (0x7E)	Address field (0x04)	Cntl field (0x03)	Payload ID (SAPI)	Data (IPv4/IPv6 or Ethernet)	FCS (CRC)	End flag
-------------------------	-------------------------	----------------------	----------------------	------------------------------------	--------------	----------

Starting flag: It contains the fixed code 0x7E (0111 1110)

Address field: It contains the fixed 0x04 (0000 01000)

Control field: It contains the fixed code 0x03 (0000 0011)

Payload ID: Two octets define the service access point identifier, or the type of data. For example,

0xFE01 identifies Ethernet

0x0021 identifies IPv4

0x0057 identifies IPv6

Data field: It contains an IP or Ethernet packet

Frame check sequence (FCS) field: It contains a 32-bit CRC calculation compliant with RFC 2615

End flag: It contains an octet flag marking the end of the LAPS frame

Fig. 4.20 The LAPS frame structure

To facilitate LAPS encapsulation of IP and Ethernet packets, an octet stuffing procedure is defined (by ITU-T X.85 and X.86) that is known as *transparency*. Since each frame begins and ends with the same flag (in hex $0\times7E$ or binary 0111 1110), there is a probability that the $0\times7E$ octet may be encountered within the information field and thus emulate the frame flag. To avoid this, at the transmitter, such occurrence of the code $0\times7E$ is converted to the code sequence $\{0\times7D\ 0\times5E\}$. Additionally, occurrences of the code $0\times7D$ are similarly converted to the sequence $\{0\times7D\ 0\times5D\}$. The receiver recognizes these sequences ($0\times7D\ 0\times6E$, $0\times7D\ 0\times5D$) and replaces them with the original octets. Full transparency is also guaranteed (by ITU-T X.86) for Ethernet over LAPS, and LAPS over SDH.

The LAPS mapping of asynchronous data frames over the synchronous SONET/SDH requires *rate adaptation*. This means that asynchronous frames must be buffered and adapted to the SDH rate. That is, as asynchronous packets arrive, “empty” (or idle) payload must be filled with special codes, which are recognized and removed at the receiver. In LAPS, the code that fills idle payload is a sequence of $\{0\times7D\ 0\timesDD\}$ as long as necessary. Rate adaptation is performed right after transparency processing and before the end flag is added. At the receiver, the rate adaptation sequence of $\{0\times7D\ 0\timesDD\}$ is detected and removed in a reverse order, right after the end flag is detected and before transparency. In the following, two data examples (Ethernet and IP) illustrate the data over LAPS over SONET/SDH process.

4.3.5.1 Example 1: Ethernet over LAPS over Next Generation SONET/SDH

MAC frames are passed over to LAPS through a *reconciliation sub-layer* and an equivalent media independent interface (MII) without address filtering, Fig. 4.21. ITU-T Recommendation X.85/Y.1321 recommends that only the *full-duplex* GbE is used in GbE over LAPS over SDH.

At the transmitting end, the functions from data packet (MAC layer) to LAPS to SONET/SDH are the following:

- Receive MAC frame (through MII or GMII interface) and detect the start frame delimiter (SFD);
- Synchronize to the SONET/SDH system clock;
- Add the start flag ($0\times7E$), SAPI, Control, and Address fields to the LAPS frame
- Generate FCS generation over Address, Control, SAPI, and LAPS information field (it does not include the Flag, Inter-frame gap, Rate Adaptation sequence, and Abort sequence octets);

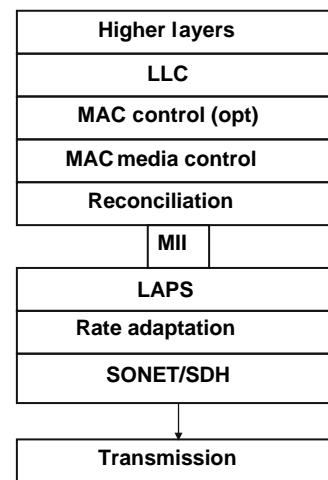


Fig. 4.21 Protocol stack of GbE over LAPS over SONET/SDH with MII interfaces

- Process transparency or stuff with octets within the LAPS frame;
- Rate-adapt by adding sequence(s) of {0x7D, 0xDD};
- Add the end flag (0x7E);
- Fill in Inter-frame-gap (IFG) octet(s) (0x7E), if needed;
- Scramble all octets before sending to SONET/SDH payload.

The format after encapsulating the MAC layer is illustrated in Fig. 4.22.

At the receiving end, the functions from SONET/SDH to LAPS to Ethernet are the following:

- Descramble all octets in the received SONET/SDH payload;
- Remove the inter-frame-gap fill octet(s) (0x7E) if any;
- Detect start flag (0x7E) of LAPS frame;
- Remove rate-adaptation octet(s) {0x7D, 0xDD} within the LAPS frame if any;
- Detect transparency code sequences within the LAPS frame and replace {0x7D 0x5E} by 0x7E and {0x7D 0x5D} by 0x7D;
- Validate Address, Control, and SAPI fields;
- Calculate FCS and correct errors;
- Detect closing flag (0x7E);
- Synchronize the MAC frame to MII receive clock;
- Add preamble and Start Frame Delimiter and send it to MAC (through MII or GMII interface).

Figure 4.23 illustrates the protocol configuration of Ethernet over LAPS over the next generation SONET/SDH according to ITU-T Recommendation X.86 and its amendment [18, 19].

4.3.5.2 Example 2: IP over LAPS over Next Generation SONET/SDH

Figure 4.24 illustrates the Layer/Protocol stack for IP over STM-N using LAPS, and for IP over sub-rate STM-n (sSTM-n) using LAPS over SDH according to ITU-T Recommendation X.85/Y.1321 [17], whereas Fig. 4.25 illustrates the protocol configuration of IP over LAPS over legacy SONET/SDH.

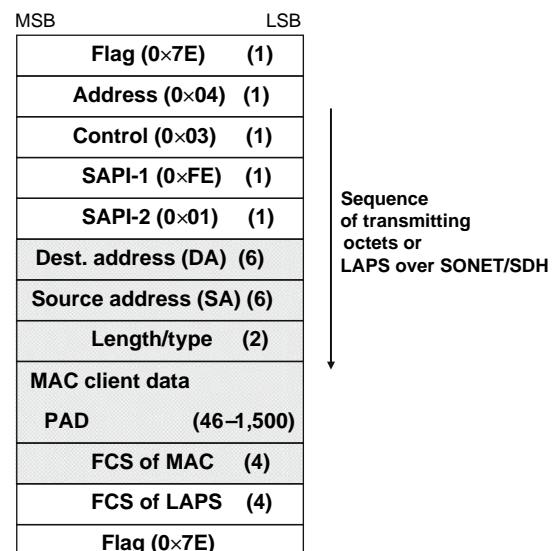


Fig. 4.22 LAPS frame after encapsulating the Ethernet MAC field (per ITU-T Recommendation X.86)

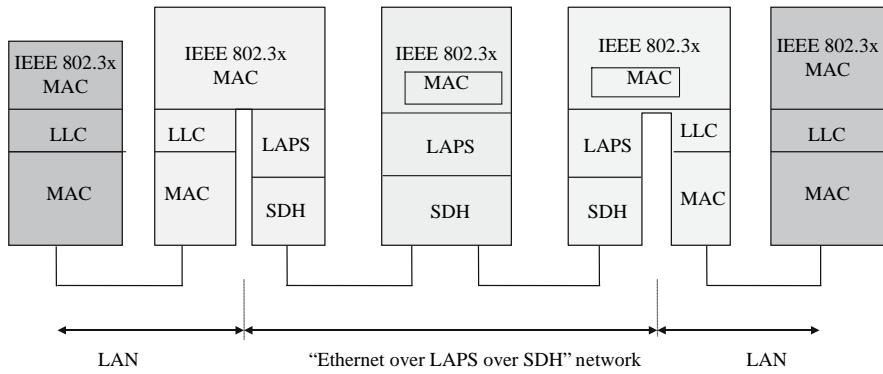


Fig. 4.23 Ethernet over LAPS over SDH (per ITU-T Recommendation X.86)

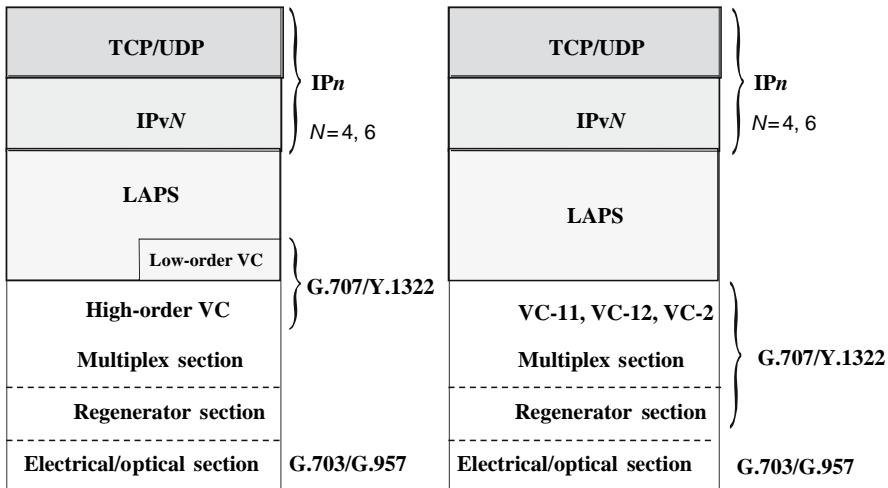


Fig. 4.24 Left: IP over LAPS over STM-*N*. Right: IP over sSTM-*n* using LAPS (per ITU-T Recommendation X.85/Y.1321)

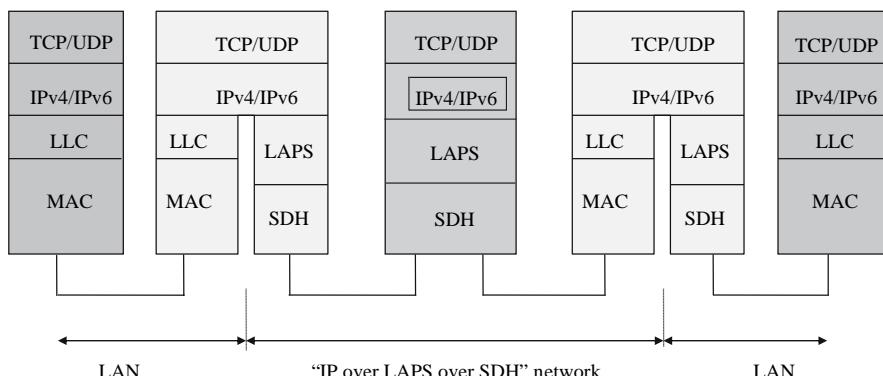


Fig. 4.25 Protocol configuration of IP over SDH with LAPS (per ITU-T Recommendation X.85/Y.1321)

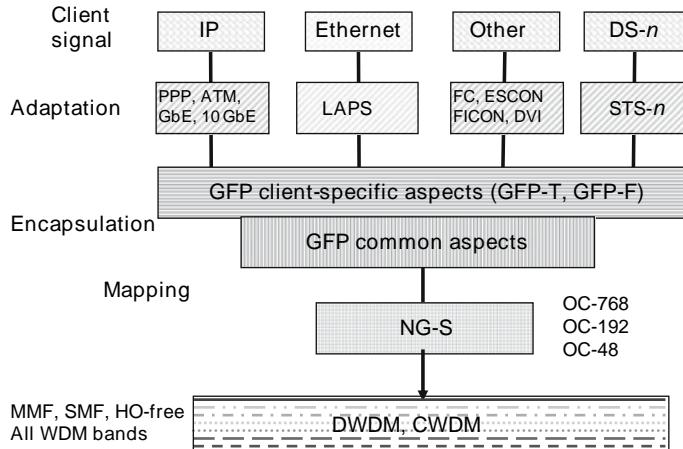


Fig. 4.26 Next generation SONET/SDH supports any client payload over WDM

4.3.5.3 Example 3: Payloads over LAPS over Next Generation SONET/SDH over WDM

A final example illustrates a variety of payloads undergoing adaptation, encapsulation, and mapping over NG-S over WDM, Fig. 4.26.

4.4 Concatenation Efficiency

The original SONET/SDH hierarchy provides bandwidth granularity that is determined by the virtual tributaries (VT in SONET) or virtual containers (VC in SDH), which have a fixed capacity of 1.5, 2, 3, 6, or 45 Mbps. This granularity puts a constraint on smaller or larger payloads and it does not always utilize the full capacity of a container. With virtual concatenation, packets of data are mapped over several concatenated next generation SONET/SDH frames, as already explained, which increases the bandwidth efficiency. We can summarize the concatenation methods as:

- Containers are the building blocks of next generation SONET/SDH.
- Contiguous concatenation is the method of using multiple contiguous containers in the same synchronous payload envelope to construct a larger container.
- Virtual concatenation is the method of using multiple containers in different synchronous payload envelopes to construct a larger container.
- Each SPE transports containers over independent routes in the network.

In conclusion, contiguous concatenation is characterized by:

Contiguous concatenation
Limited granularity of VC size
Contiguous containers travel over the same path
All network elements on the path must be aware of CC
Transparent to network management
No differential delay
No sequential numbering for alignment.

Similarly, virtual concatenation is characterized by

Table 4.5 Efficiency of CC and VC for various payloads

Service	Data rate (Mbps)	CC		Efficiency (%)	VC		Efficiency (%)
		SONET	SDH		SONET	SDH	
Ethernet	10	STS-1	VC-3	20	VT-1.5-7v	VC-12-5v	90
Fast Ethernet	100	STS-3c	VC-4	67	STS-1-2v	VC-3-2v	100
Gbit-Ethernet	1,000	STS-48c	VC-4-16	42	STS-1-21v	VC-4-7v	95
ESCON	200	STS-12c	VC-4-16	33	STS-1-4v	VC-3-4v	100
FC	1,000	STS-21c		85	STS-1-18v		95
ATM	25	STS-1	VC-3	50	VC-1.5-16v	VC-12-12v	98

More flexible low-order and high-order granularity
Containers travel over separate paths
Only the end network element must be aware of VC
Requires network management
Potential differential delay
Requires sequential numbering for alignment.

Table 4.5 tabulates the efficiency for contiguous and virtual concatenation.

References

1. S. V. Kartalopoulos, *Understanding SONET/SDH and ATM*, IEEE Press, 1999.
2. S.V. Kartalopoulos, *Next Generation SONET/SDH: Voice and Data*, IEEE/Wiley, 2004.
3. S.V. Kartalopoulos, *Introduction to DWDM Technology: Data in a Rainbow*, Wiley/IEEE Press, 2000.
4. S.V. Kartalopoulos, *Fault Detectability in DWDM*, IEEE Press/Wiley, 2002.
5. E. Rosen et al., *Multiprotocol Label Switching Architecture*, IETF RFC 3031, January 2001.
6. Y.-D. Lin, N.-B. Hsu, and R.-H. Wang, “QoS Routing Granularity in MPLS Networks”, *IEEE Communications Magazine*, vol. 40, no. 6, June 2002, pp. 58–65
7. H. Christiansen, T. Fielde, and H. Wessing, “Novel label processing schemes for MPLS”, *Optical Networks Magazine*, vol. 3, no. 6, November/December 2002, pp. 63–69.
8. P. Ashwood-Smith, et al., “Generalized MPLS—CR-LDP Extensions”, IETF RFC 3472, January 2003.
9. L. Berger et al., “Generalized MPLS—RSVP-TE Extensions”, IETF RFC 3473, January 2002.
10. ITU-T Recommendation G.8080/Y.1304, *Architecture for the Automatically Switched Optical Network(ASON)*, November 2001.
11. ITU-T Recommendation G.7712/Y.1703, *Architecture and Specification of Data Communication Network*, November 2001.
12. ITU-T Recommendation G.7714/Y.1705, *Generalized Automatic Discovery Techniques*, November 2001.
13. ITU-T Recommendation G.7713/Y.1704, *Distributed Call and Connection Management (DCM)*, December 2001.
14. ITU-T Recommendation G.7041/Y.1303, *The Generic Framing Procedure (GFP) Framed and Transparent*, December 2001.
15. E. Hernandez-Valencia, “Generic Framing Procedure (GFP): A Next-Generation Transport Protocol for High-Speed Data Networks”, *Optical Networks Magazine*, vol. 4, no. 1, January/February 2003, pp. 59–69.
16. ITU-T Recommendation G.7042/Y.1305, *Link Capacity Adjustment Scheme (LCAS) for Virtual Concatenated Signals*, November 2001.
17. ITU-T Recommendation X.85/Y.1321, *IP over SDH Using LAPS*, March 2001.
18. ITU-T Recommendation X.86, *Ethernet over LAPS*, February 2001.
19. ITU-T Recommendation X.86/Y.1323, Amendment 1, “Ethernet over LAPS, Amendment 1: Using Ethernet flow control as rate limiting”, April 2002.

Chapter 5

The Optical Transport Network

5.1 Introduction

Optical networks are comprised of optical nodes that are interconnected in one of the most popular topologies, mesh, ring, and point to point. However, for effectiveness and efficiency, optical networks are described in terms of functionality that is related to payload transport, client payload multiplexing, routing, service survivability and protection, supervision, and network maintenance. To meet network efficiency, the optical transport network at the transmitting side is composed of independent transport layer networks; that is, the network assembles individual client signals that all together are transported over a link. At the receiving side, each layer network is separately partitioned so that the internal structure of that layer network unfolds and client signals are separated to be rerouted to their own direction. In many respects, a node is no more than an airport hub where passengers arrive with the same aircraft, and then each one is transferred to a different gate where a different set of passengers are assembled to depart for another destination; this implies that for each passenger an end-to-end route management is maintained.

The *optical transport network* (OTN) was developed for long-haul transport at data rates from 2.5 to 40 Gbps per optical channel, and it is described in detail by a series of ITU-T recommendations [1–3]. OTN supports unidirectional and bidirectional point-to-point connections and unidirectional point-to-multipoint connections.

5.2 OTN Network Layers

The OTN structure, in addition to the *physical media layer network* that defines the optical fiber type, consists of three layers—the optical channel, the optical multiplex section, and the optical transmission section layer networks:

- The *optical channel layer network* provides end-to-end networking of optical channels to convey transparently client information of different format, such as SONET/SDH, PDH 565 Mbps, ATM. This is accomplished by including capabilities such as optical channel connection rearrangement for flexible network routing, optical channel overhead ensuring integrity of the optical channel adapted information, optical channel OA&M functions (operations, administrations, and maintenance) for enabling connection provisioning, quality of service parameter exchange, and network survivability.
- The *optical multiplex section layer network* provides functionality for networking of a multi-wavelength (WDM) optical signal. This is accomplished by including capabilities such as optical multiplex section overhead to ensure integrity of the multiwavelength optical multiplex section adapted information, optical multiplex section OA&M for enabling section level operations and management functions and multiplex section survivability.

- The *optical transmission section layer network* provides functionality for transmission of optical signals on optical media of various types [4–6]. This is accomplished by including capabilities such as optical transmission section overhead processing to ensure integrity of the optical transmission section adapted information, optical transmission section OA&M for enabling section level operations and management functions and transmission section survivability.

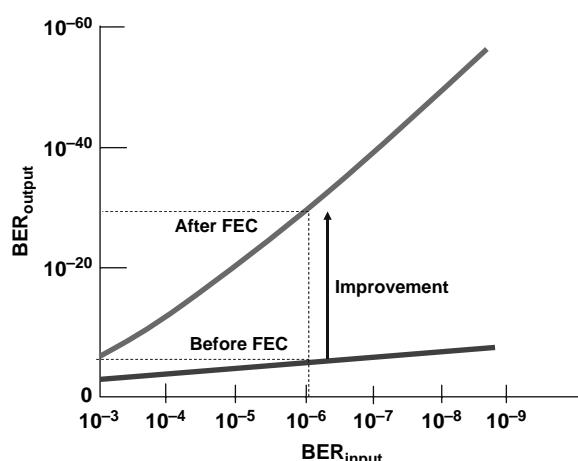
Similar to the Next Generation SONET/SDH, OTN defines a synchronous payload within a fixed frame length with a comprehensive overhead to support a variety of client payloads, and with a forward error correcting (FEC) code placed at the trailing end of the frame, which differentiates it from the NG-S.

FECs are error detection and correction codes that are capable of locating a number of erroneous bits (such as 16) and correcting a smaller number of them (such as 8); FECs that are capable of correcting eight or more errors are known as strong codes, and if fewer than eight are known as soft. For example, the RS(255,239) is a nonbinary code that belongs to the family of systematic linear cyclic block codes; nonbinary means that the FEC code operates on byte symbols. RS codes are generated from binary polynomials, such as the RS(255,239) which is generated by the polynomial $x^8 + x^4 + x^3 + x^2 + 1$ (the interested reader may find a thorough description of this FEC code in ITU-T G.709 Annex A).

In order to appreciate the dramatic contribution of FEC to signal performance, assume a 10^{-12} BER performance objective. Then a signal on a link with performance 10^{-4} BER without FEC is well below the expected performance and the link may become inoperable. However, the same signal is improved to 2×10^{-13} BER with the addition of strong FEC. This improvement is dramatic, and it illustrates that the addition of FEC allows the same signal to be transmitted to much longer distances or a higher bit rate and still meeting the 10^{-12} BER objective. Similarly, a signal with 10^{-7} BER without FEC is improved to 10^{-40} BER with FEC.

The addition of FEC results in fewer overall bit errors at the receiver so that even longer fiber spans or long spans with higher bit rate meet the BER performance objectives (such as, 10^{-12}), which otherwise could not be met. An immediate benefit is that over long-haul and in transoceanic fiber-optic communications, fewer amplifiers and regenerators are needed, or that over the same fiber lengths a higher bit rate can be used. Figure 5.1 demonstrates the dramatic effect FEC has on bit rate and BER performance. However, FEC, as defined by ITU-T [7], implements FEC in the electronic regime; that is, the optical signal must be converted at the terminal transmission equipment (TTE) in electrical. In point-to-point links without regenerators, this is simply implemented at the two ends of the link. However, in very long-haul links ($>1,000$ km), regenerators are unavoidable and FEC conversion from optical to electrical and back to optical is expensive in both capital and operational

Fig. 5.1 BER with and without FEC RS(255/239)
(Adapted from ITU-T standard G.975)



or maintenance costs. Another consequence is that FECs have a fixed correction capability of errored bits (typically eight). If bit errors exceed the FEC capability, then uncorrected errors from regenerator to regenerator accumulate, and a burst of uncorrected errors is formed to the detriment of performance objectives. In addition, the FEC is a physical layer function and therefore it is possible that bit errors are not reported to fault management function.

5.3 FEC in OTN

OTN provides the ability to multiplex SONET/SDH frames to achieve higher transmission data rates. For example, it is defined to multiplex (by interleaving) several STS-48 (SONET)/STM-16(SDH), or STS-192/STM-64 or STS-768/STM-256. When M STS-48 (SONET) or STM-16 (SDH) frames are multiplexed, an aggregate $M \times 2.5$ Gbps transmission data rate is achieved. In this case, the FEC encoding function is performed at each SONET/SDH frame before the interleaving (or frame-multiplexing) function in the terminal-terminating equipment unit. At the receiver, the error detection–correction function is performed after de-interleaving the frames. In OTN, interleaved SONET/SDH frames with FEC attached are called optical payload unit- k (OPU- k). k is a subscript that indicates what SONET/SDH frames are interleaved. Table 5.1 provides the value of k for few OPUs.

OTN has adopted the Reed–Solomon error detection–correction (EDC) code. However, the probability of errored photonic bits, and thus the bit error rate (BER), in addition to parameters such as fiber length, loss, channel density, nonlinearity, signal optical power and receiver sensitivity, depends on the transmission data rate (see Table 5.1). Therefore, in OTN, the Reed–Solomon FEC code is generated using a different polynomial with different detection and correction capabilities for different OPU- k frames. The Reed–Solomon EDC code is typically denoted as RS(x, y), where the arguments in parenthesis indicate the length of data to be detected for errors and y the length of added EDC. For example, the RS(255,239) FEC coder calculates 16 check bytes over 239 data byte-size symbols and appends them to it ($239 + 16 = 255$), Fig. 5.2. Table 5.2 shows the FEC code used in OTN.

Table 5.1 Relationship of STS/STM and OTN OPU- k frames

SONET	SDH	Data rate	OPU- k
STS-48	STM-16	2.5 Gbps	OPU-1
STS-192	STM-64	10 Gbps	OPU-2
STS-768	STM-256	40 Gbps	OPU-3

1 symbol=8 bts ($m=8$)

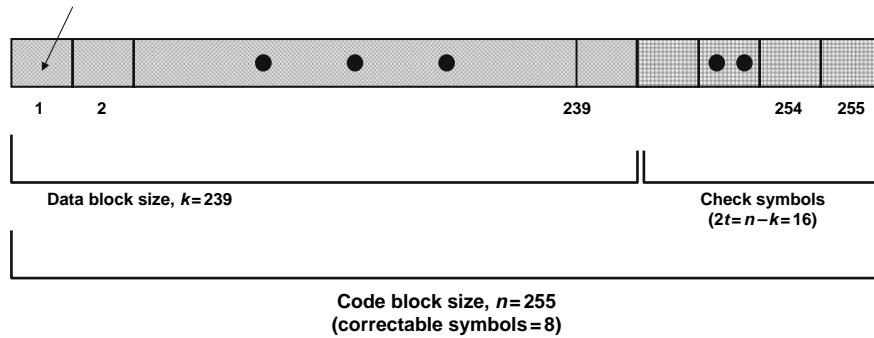


Fig. 5.2 Structure of Reed-Solomon RS(255,239) or RS(255/239) error correction code

Table 5.2 FEC code in OTN OPU-*k* frames

OPU- <i>k</i>	FEC type
OPU-1	RS 239/238 ^a
OPU-2	RS(238/237)
OPU-3	RS(238/236)

^a NO FEC is used in this case; the RS code contains zeroes

5.4 OTN Frame Structure

5.4.1 OPU-*k*

The basic frame unit defined in OTN is the OPU-*k*, in which the client signals are mapped. Taking into account FEC, the nominal transmission bit rate for OPU-*k*, for $k = 1, 2, 3$, is given, Table 5.3.

An OPU-*k* unit consists of four rows of 3,810 bytes each, including 2 bytes overhead placed at the leading end of each row to support adaptation of different client signals, Fig. 5.3. Note that ITU-T G.709/Y.1331 starts the numbering from 15; this numbering will become clear during the construction of the OTN frame.

5.4.2 ODU-*k*

The optical data unit-*k* (ODU-*k*) is formed by adding 14 byte-columns overhead at the leading end of the OPU-*k*, Fig. 5.4.

The first 14 bytes of the first row in the ODU-*k* are defined as follows:

- The FAS (frame alignment signal) field (bytes 1–7) consists of the fixed frame alignment sequence: 0xA1 0xA1 0xA1 0xA2 0xA2 0xA2.
- The MFAS (multiframe alignment signal) field (byte 8) contains the frame number in a 256 multiframe.
- The OTU (optical channel transport unit-*k*) overhead field (bytes 8–14) consists of the section monitoring (bytes 8–10), general communications channel-0 (GCC0) (bytes 11 and 12), and two reserved (bytes 13 and 14).

Table 5.3 Nominal OPU-*k* transmission bit rates

OPU- <i>k</i>	Nominal rate
OPU-1	2,488,320.000 Kbps ± 20 ppm
OPU-2	9,995,276.962 Kbps ± 20 ppm
OPU-3	40,150,519.322 Kbps ± 20 ppm

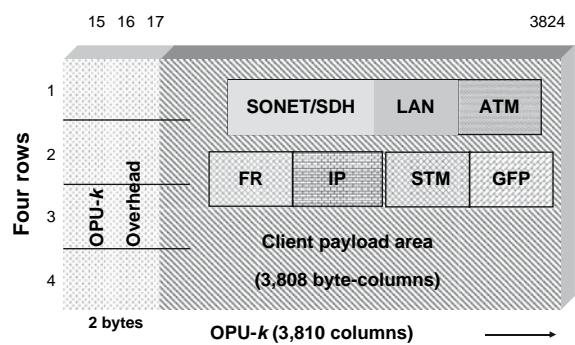


Fig. 5.3 The OPU-*k* unit consists of four rows of 3,810 bytes each, including 2 bytes overhead at the leading end of each row

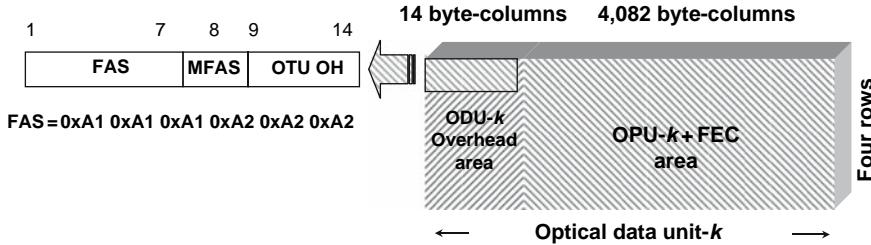


Fig. 5.4 The ODU- k is formed by adding 14 byte-columns overhead at the leading end of the OPU- k

The remaining ODU- k overhead (bytes 1 through 14 of rows 2–4) is partitioned in sections; one section is defined for end-to-end ODU- k path, another section supports six levels of tandem connection monitoring, and others are used for performance, maintenance, and operational functions. The complete overhead functionality is spread over up to 64 ODU- k frames.

The ODU- k path overhead is terminated where the ODU- k is assembled and disassembled. The overhead for tandem connection is added and terminated at the source and sink of tandem connections.

The ODU- k supports the following functions:

- adaptation of client signals via the OPU- k
- end-to-end path supervision via the ODU- k P
- tandem connection monitoring via the ODU- k T.

The OTN standard, in an effort to optimize the transported client bandwidth, has also defined time division multiplexing (TDM) of ODUs while maintaining the end-to-end trail for the TDM'ed lower bit rate channels. Thus, for the currently defined ODU- k s [ITU-T G.802], the following client/server relationships are defined:

- An ODU-2 can transport 4 ODU-1s; an ODU-2 is the equivalent of 4 ODU-1s.
- An ODU-3 can transport 16 ODU-1s, or 4 ODU-2s, or any mix of ODU-1s and ODU-2s as long as the bandwidth limits are not violated.

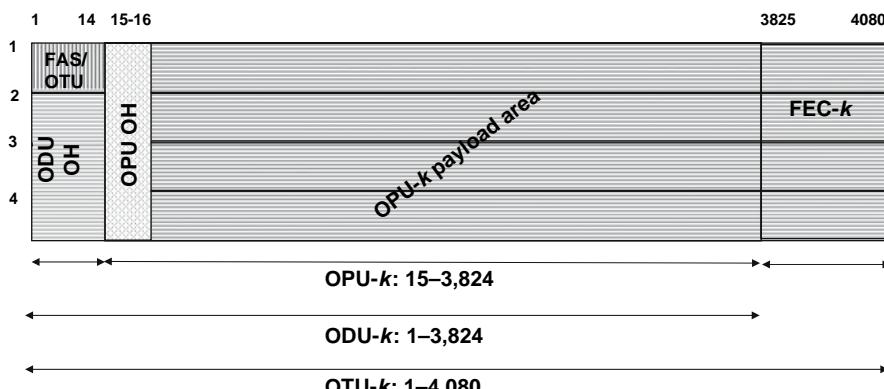


Fig. 5.5 The OTU- k is constructed by adding OTU- k overhead bytes to ODU- k and appending FEC

Table 5.4 OUT-*k* nominal rate (± 20 ppm)

OTU- <i>k</i>	OTU nominal bit rate (Kbps)	Period (μs)
OTU-1	$255/238 \times 2,488,320 = 2,666,057.143$	48.971
OTU-2	$255/237 \times 9,953,280 = 10,709,225.316$	12.191
OTU-3	$255/236 \times 39,813,120 = 43,018,413.559$	3.035

5.4.3 OTU-*k*

The frame construction of the optical channel transport unit-*k* (OTU-*k*) is completed by adding OTU-*k* overhead bytes and by appending the FEC code at the end of the ODU-*k* frame, Fig. 5.5.

The OTU overhead consists of the section monitoring (bytes 8–10), the general communications channel 0 (GCC0) (bytes 11 and 12), and reserved (bytes 13 and 14). The FEC area consists of four rows with 256 bytes each. Thus, the final OTU-*k* frame consists of four rows by 4,080 columns. The OTU-*k* nominal bit rates (with ± 20 ppm tolerance) are calculated in Table 5.4.

The OTU-*k* FEC is calculated at the physical layer of a transmission link as follows: the 3,824 bytes of each row are byte-demultiplexed into 16 subframes of 239 bytes each. Then, by applying the RS(255,239) code, a 16-byte FEC code is calculated for each subframe. Then, they are all byte-multiplexed to construct the 4,080 bytes of each of the four OTU-*k* rows including FEC, Fig. 5.6.

In order to prevent a long sequence of ones or zeroes, the OTU-*k* signal, after the FEC has been added to the OTU-*k* signal and prior to being transmitted, is scrambled using a random sequence length 65,535, generated by the polynomial $x^0 + x^1 + x^3 + x^{12} + x^{16}$. Per ITU-T G.709, the scrambler is initialized to “0xFFFF” at the start of frame, it skips (it does not scramble) the frame alignment bytes (FAS) of the OTU-*k* overhead (bytes 1–7 of the first row), it starts scrambling with the most significant bit of the MFAS byte (eighth byte of the first row), and it runs continuously throughout the complete OTU-*k* frame.

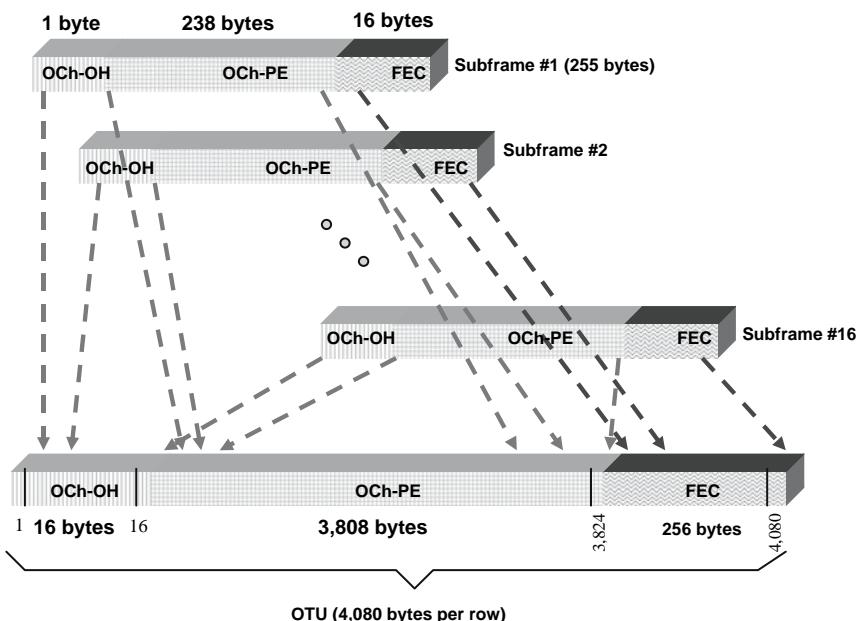


Fig. 5.6 At the physical layer of a transmission link, the RS code is applied on 239 bytes of each subframe in a row, and after 16 FEC bytes and 1 byte overhead are added, they are all byte-multiplexed to construct the four 4,080-byte OTU-*k* rows

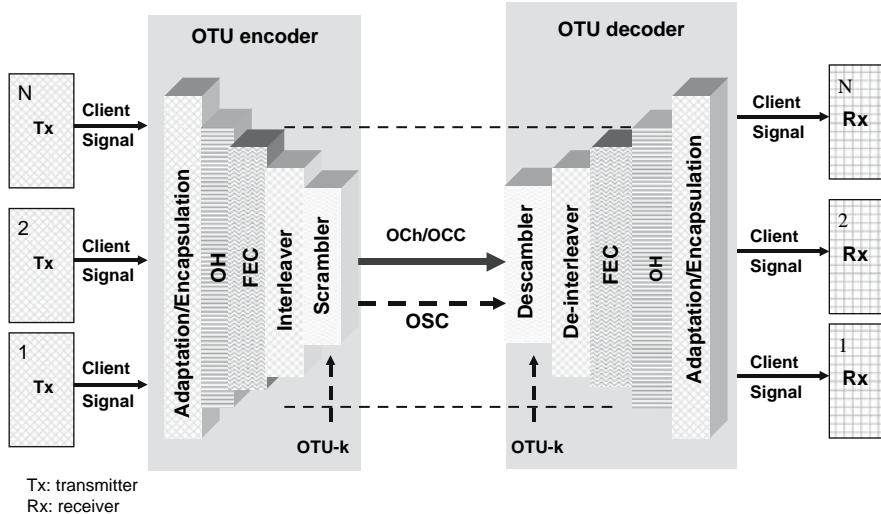


Fig. 5.7 OTU-*k* sequence of basic steps at the transmitting and at the receiving side of a link

As a result of the aforementioned functionality, the sequence of the various functional operations required to form an OTU-*k* frame is shown in Fig. 5.7.

Although not explicitly shown, timing and jitter tolerances are very critical in this process. ITU-T G.8251 provides recommendations for the maximum permissible jitter at OTU-*k* interfaces and for various link lengths; these are provided in terms of Unit Interval peak-to-peak (UIpp) and for jitter measured bandwidth at the -3 dB frequency (in Hz) point [8]. The Unit Interval (UI) in ps of OTU-*k* is calculated from the bit rate and the RS code as follows:

$$\text{OTU-1: } 1 \text{ UI} = (238/255)(1/2.48832) \text{ ns} = 375.1 \text{ ps}$$

$$\text{OTU-2: } 1 \text{ UI} = (237/255)(1/9.95328) \text{ ns} = 93.38 \text{ ps}$$

$$\text{OTU-3: } 1 \text{ UI} = (236/255)(1/39.81312) \text{ ns} = 23.25 \text{ ps}$$

Based on these calculations for UIs, the maximum permissible UIpp jitter for different bandwidths and OTU-*ks* is defined by G.8251 as follows:

OTU-1 for 5 kHz–20 MHz: 1.5 UIpp

OTU-1 for 1–20 MHz: 0.15 UIpp

OTU-2 for 20 kHz–80 MHz: 1.5 UIpp

OTU-2: for 4–80 MHz: 0.15 UIpp

OTU-3: for 20 kHz–320 MHz: 6.0 UIpp

OTU-3: for 16–320 MHz: 0.15 UIpp

5.4.4 The Optical Channel

The OTU-*k* layer so far defined by ITU-T G.709/Y.1331 is an electronic signal. When this signal is converted to optical, then it is known as the optical channel (OCh), the specifications of which are defined in ITUT G.872; additionally, ITUT G.872 defines the OTN layer networks that support network management and supervision functionalities.

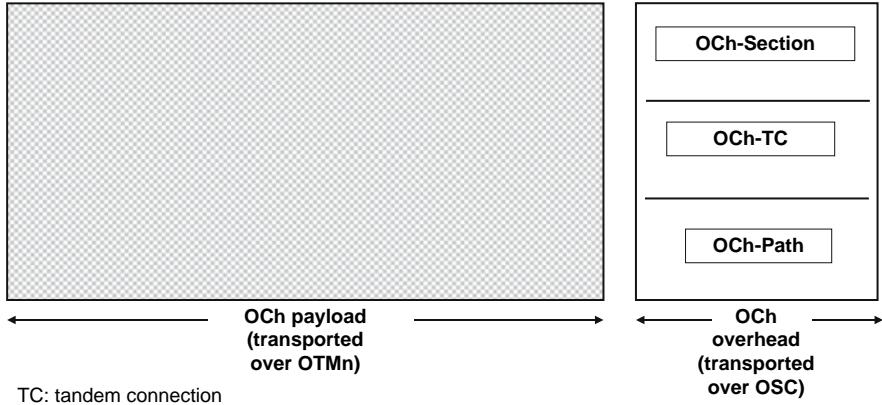


Fig. 5.8 The sub-layers in the basic optical channel (OCh). The OCh is formed and transported separately

Two OChs are defined:

- The optical channel with full functionality (OCh)
- The optical channel with reduced functionality (OChr) that provides transparent network connections between 3R regeneration in the OTN.

The OCh includes nonassociated overhead; this is overhead not embedded in the OCh frame but is transported over a different carrier, Fig. 5.8. The OCh overhead (OCh OH) includes information for maintenance to support fault management and protection. This overhead is terminated where the OCh signal is assembled and disassembled.

5.4.5 Optical Channel Carrier and Optical Channel Group

OTN addresses mapping of an OCh onto a WDM wavelength; for this, the optical channel carrier (OCC) is defined. Two OCCs are defined:

- OCC with reduced functionality (OCCr): this consists of payload (OCCp) only. It carries the OCh payload, and it is assigned a wavelength of the ITU-T grid [9, 10]. There is no associated overhead with OCCr.
- OCC with full functionality (OCC): this consists of payload (OCCp) and of overhead (OCCo). The OCCp carries the OCh payload and it is assigned a wavelength of the ITU-T grid. The OCCo carries the OCh overhead, and it is transported with the optical transport module (OTM) overhead signal information channel.

A group of optical channel carriers (OCC) is known as optical carrier group of order $n[r]$ (OCG- $n[r]$); the tributary OCCs may be of different size. Thus, up to n OCC- $n[r]$ are WDM multiplexed to occupy a fixed set of wavelengths of the ITU-T grid, Fig. 5.9.

Two OCGs are defined:

- OCG- n with reduced functionality (OCG- nr): it consists of up to n OCC payloads (OCCp) and there is no associated overhead with OCG- nr .
- OCG- n with full functionality (OCG- n): it consists of up to n OCC payloads (OCCp) and their associated overhead (OCCo).

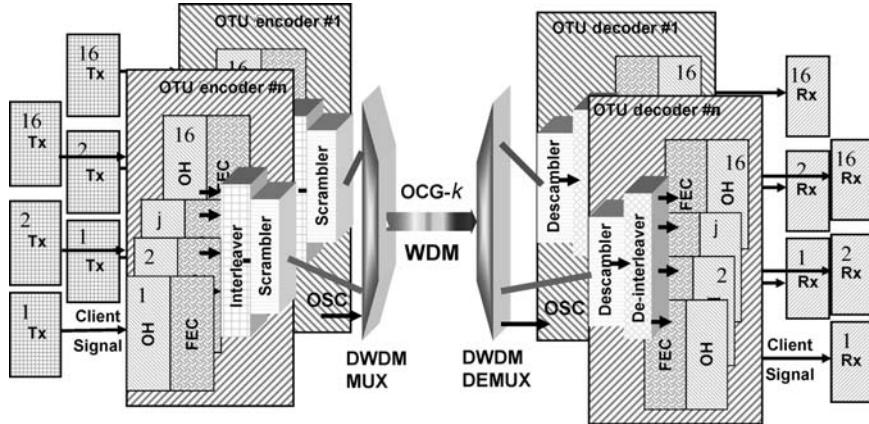


Fig. 5.9 The OCG- k basic structure over DWDM

5.4.6 Nonassociated Overhead

OTN, besides the overhead defined in the OPU- k , ODU- k , and OTU- k , defines nonassociated overhead for OCh (already discussed), OCC, OCG, for the optical multiplex section, and for the optical transmission section.

The optical multiplex section overhead (OMS OH) is added to OCG to create an optical multiplex unit (OMU). This is used for maintenance and operational functions specific to optical multiplex sections. The OMS OH is terminated where the OMU is assembled and disassembled.

The optical transmission section overhead (OTS OH) is added to information payload to create an optical transport module (OTM). This is used for maintenance and operational functions specific to optical transmission sections. The OTS OH is terminated where the OTM is assembled and disassembled. Additionally, the general management communications overhead (COMMS OH) is added to the information payload to create an OTM. This is used for general management communication between network elements.

The ensemble of m OCG- $n[r]$ s entails an optical transport module (OTM- n,m). When the OTM- n,m members have full functionality, the nonassociated overhead is transported by the optical transport module overhead signal (OOS) by an OTN supervisory channel (OSC). There are three OTM types:

- OTM-0, m without OSC that supports a noncolored optical channel over a single span with 3R regeneration at each end;
- OTM-16r, m without OSC that supports 16 optical channels (numbered OCCr #0 to OCCr #15) on a single optical span with 3R regeneration at each end;
- OTM- n,m with full functionality and with OSC that supports up to n optical channels for single or multiple optical spans. 3R regeneration is not required.

The OSC is assigned its own wavelength and it is characterized by its own frame structure, bit rate, and bandwidth, and it is wavelength division multiplexed with the OTM- n,m , Fig. 5.10.

5.4.7 Mapping GFP Frames in OPU- k

With the insertion of idle frames at the GFP encapsulation stage, GFP frames arrive at a continuous bit stream [11]. Thus, mapping GFP frames in OPU- k is achieved by aligning the byte structure

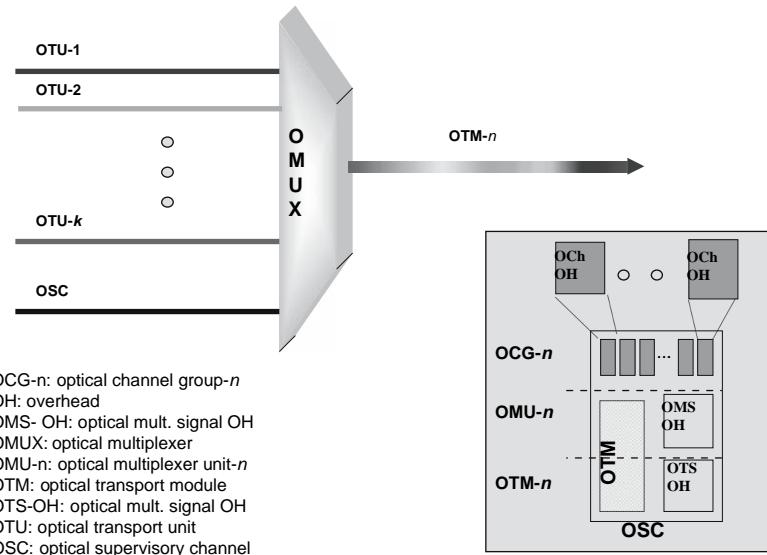


Fig. 5.10 As several OTUs are formed, the OSC channel is constructed, and the OTM-n signal is formed and transported over its own WDM channel

of every GFP frame with the byte structure of the OPU- k payload, Fig. 5.11. Thus, in this case, justification control is not needed and the OPU- k useful payload for GFP mapping consists of $4 \times 3,808$ bytes. Because rate adaptation and scrambling are performed in GFP encapsulation, these two functions are not required during the mapping process. Additionally, because GFP frames may have variable length, they are allowed to cross the OPU- k frame boundary. In this case, the OPU- k overhead consists of seven reserved bytes (RES) and a payload structure identifier (PSI) that includes the payload type (PT) (column 15, row 4).

5.5 OTN and DWDM

The Optical Transport Network is defined to transport different optical signals over DWDM. The mapping sequence of them onto OTN over DWDM is shown in Fig. 5.12.

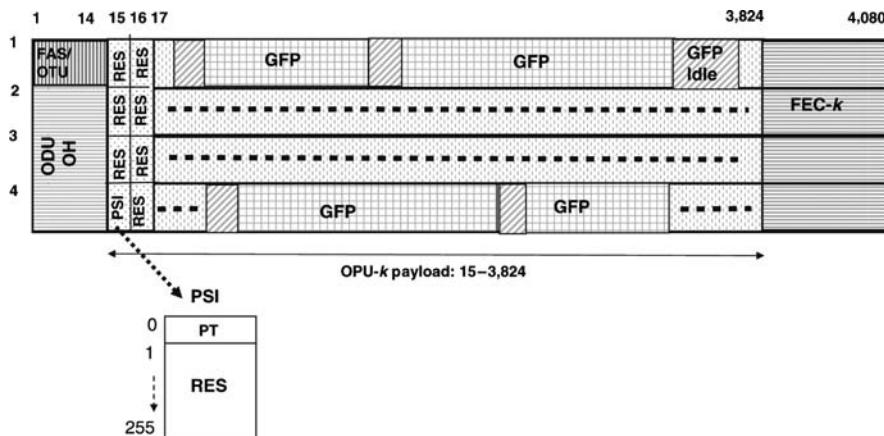


Fig. 5.11 Mapping GFP frames in OPU- k

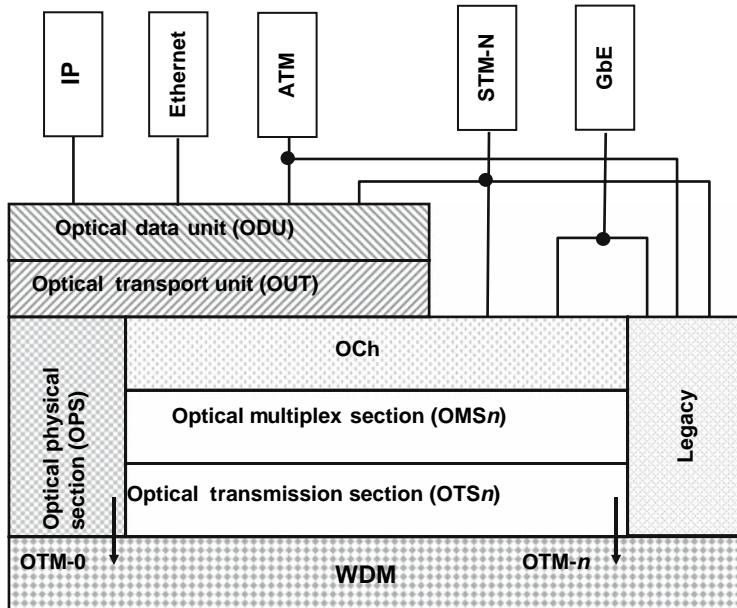


Fig. 5.12 Mapping different payloads onto OTN over WDM

Using the DWDM technology as a transport vehicle it is possible to transmit over optical channels both SONET/SDH frames and Gigabit Ethernet without encapsulating their frames into an optical transport unit. In this case, an optical cross-connect can pass the signal although it does not provide the OAM functions that are associated with an OTU of OTN, which additionally may result in network management limitations.

5.6 OTN Management

To assure that misconnection does not take place or that connections are efficiently established, the OTN supports fault, configuration, and performance management between and within administrative boundaries as well as end to end [12–16]. For it, OTN supports communications between personnel at remote sites, craft terminals and local or remote NEs, OSs and remote NEs, and externally to OTN, and it is achieved by means of detection and notification facilities that

- detect, isolate, and localize faults and initiate recovery actions where applicable. Defect indications in a connection, which is part of a trail (a trail is a series of concatenated link connections), are given in downstream and upstream directions of a bidirectional trail using forward defect indication (FDI), backward defect indication (BDI), and backward quality indication (BQI). In the presence of faults, OTN supports escalation strategies to avoid unnecessary, inefficient, or conflicting survivability actions; such strategies include introduction of hold-off times and alarm suppression methods within a layer and between the server and client layer;
- supervise and ensure the interconnection integrity of transport network entities with compatible adapted or characteristic information; continuity supervision is the set of processes required to monitor the integrity of the continuity of a trail. Connectivity supervision is identified using the trail trace identification (TTI);
- verify quality of service. Signal quality supervision is provided by monitoring the performance of a connection that supports a trail;

- manage client adaptation layer network. This refers to the processes necessary to manage client layer network adaptation to/from the server layer and it is achieved with the payload type identification (PTI); recall that ATM has a three-bit PTI field in its overhead. At connection setup, the PTI ensures that the client layer is assigned to the appropriate source and sink. A PTI mismatch at source or sink adaptations would indicate an incorrectly provisioned or altered client-OCh server layer adaptation.

References

1. ITU-T Recommendation G.709/Y.1331, “Interfaces for the Optical Transport Network (OTN)”, February 2001; ITU-T Recommendation G.709/Y.1331, “Interfaces for the Optical Transport Network (OTN), Amendment 1”, February 2001, and ITU-T Recommendation G.709/Y.1331, Amendment 1, “Amendment 1”, November 2001.
2. ITU-T Recommendation G.872, “Architecture of Optical Transport Networks”, November 2001.
3. ITU-T Draft Rec. G.959, “Optical Networking Physical Layer Interfaces”, February 1999.
4. ITU-T Recommendation G.652, “Characteristics of a Single-mode Optical fibre cable”, October 2000.
5. ITU-T Recommendation G.653, “Characteristics of a Dispersion-Shifted Single-Mode Optical Fibre Cable”, October 2000.
6. ITU-T Recommendation G.655, “Characteristics of a Non-zero Dispersion-Shifted Single-Mode Optical Fibre Cable”, October 2000.
7. ITU-T Recommendation G.959, “Forward Error Correction for Submarine Systems”, October 2000.
8. ITU-T Recommendation G.8251, “The Control of Jitter and Wander Within the Optical Transport Network (OTN)”, November 2001.
9. ITU-T Recommendation G.692, “Optical Interfaces for Multichannel Systems with Optical Amplifiers”, October 1998.
10. S.V. Kartalopoulos, “DWDM, Networks, Components and Technology”, IEEE Press/Wiley, 2003.
11. S.V. Kartalopoulos, “Next Generation SONET/SDH: Voice and Data”, IEEE/Wiley, 2004.
12. S.V. Kartalopoulos, “Fault Detectability in DWDM”, IEEE Press/Wiley, 2002.
13. ITU-T Draft Recommendation G.798, “Characteristics of Optical Transport Networks (OTN) Equipment Functional Blocks”, October 1998.
14. ITU-T Draft Rec. G.873, “Optical Transport Network Requirements”, October 1998.
15. ITU-T Draft Rec. G.874, “Management Aspects of the Optical Transport Network Element”, October 1998.
16. ITU-T Draft Rec. G.875, “Optical Transport Network Management Information Model for the Network Element View”, October 1998.

Chapter 6

Network Synchronization

6.1 Introduction

This chapter discusses the importance of synchronization in optical networks, clock classification in strata, and its expected accuracy. It provides a simplified interpretation of the meaning of “noise”, “jitter”, and “wander”; it discusses noise sources that contaminate the optical signal and degrade synchronization, the performance of the optical receiver, and performance detection strategies.

6.2 Synchronization

Synchronization is a key function in communication networks. A binary string is transmitted at a fixed bit rate that is determined by an accurate clock and it is received faithfully by a receiver with the help of its own local clock tuned to the transmitter’s frequency. Based on the clock frequency at the receiver, a threshold level and a sampling point at the bit period the logic state (0/1) of sampled pulse is determined, the accuracy of which depends on the correct selection of the threshold and sampling points, Fig. 6.1.

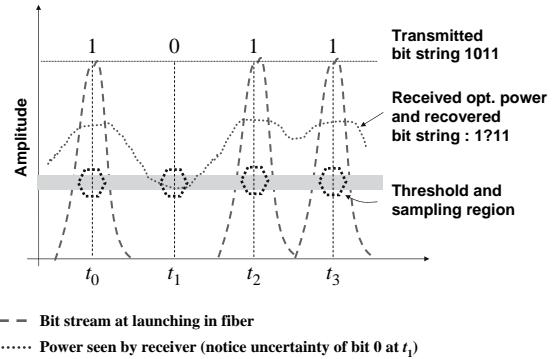
Typically, there are two different transmission methods with regard to clock and timing: fixed clock and same frequency at both transmitter and receiver, and adaptable frequencies whereby the receiver is able to track the transmitting clock and adapt to it.

The first method (fixed frequency) is typically used in synchronous and ultrahigh bit rate optical communications. It is more accurate and simpler, which is a prerequisite for ultrahigh bit rates. Clearly, this synchronization method is not flexible to adapt to other bit rates. For example, at 10 Gbps, the bit period is only 100 ps, and thus a small drift in transmitter and/or receiver clock frequency could easily shift the periodic sampling point and yield excessive erroneous bits that dramatically decrease the signal performance and also cause overflow or underflow.

The second method (adaptable frequency) is typically used in data transmission at moderate and low data rates. For example, when the amount of data (packet size and number of packets) to be transmitted is low or when the data network experiences congestion, the transmitted data rate may scale down automatically according to a specific bandwidth management protocol. This method implies that the transmitter is capable of adapting various bit rates and more importantly the receiver is able to recognize the transmitter frequency and adapt to it with commensurable accuracy. This also implies that the receiving clock has an appropriate dynamic range (min–max frequency bounds) and also low acquisition time or responsiveness (able to quickly adapt to the new frequency).

In both methods, the accuracy of the transmitting and receiving clock frequencies is calibrated according to a reference clock that is derived from a reference clock known as the *primary reference source* (PRS).

Fig. 6.1 The recovered bit string depends on threshold, sampling point, and received signal



6.2.1 The Primary Reference Source

A clock signal is a periodic waveform (of a sinusoidal or almost square form) that is generated by an oscillator located in the timing unit of a node and it provides the heartbeat of a node. Because of its importance, the precision of the clock signal is specified by standards [1–3]. The most accurate clock that is responsible for network synchronization is based on the element cesium, which provides a frequency reference of consistent high accuracy and is calibrated by the National Institute of Standards and Technology (NIST), previously known as National Bureau of Standards (NBS), and provides the primary reference timing source (PRS).

Although the PRS is the highest accuracy clock in telecommunications, not all networks and nodes require the same accuracy. Typically, clock accuracy drops from core to access following the bit rate drop trend, although the latter is changing in optical access (such as fiber to the premises, FTTP) where bit rate has increased beyond broadband to Gbps. Typically, clock accuracy is distinguished in strata and is measured in parts per million (ppm).

The PRS timing accuracy is known as “stratum 1”. This reference clock is broadcasted over a GPS satellite link or over a CDMA wireless link, and it is received by a timing source unit located in each central office of a communications network. The timing source unit has a quartz-based or rubidium-based local oscillator that locks onto the received frequency, and it supplies a dual clock to each communications system, a primary and a secondary timing reference (for backup) at stratum 1 accuracy (as long as the local oscillator is locked onto the received frequency). The output clocks may be 8 kHz, 64 kHz, 1.544 MHz (DS1), 2,048 kHz (E1), or a composite (8 and 64 kHz). This is known as the building information timing supply (BITS), and it is described in various standards (ITU and Telcordia) for central offices and for controlled environment vaults (CEV) [4–7].

In communications networks, even the minimum timing accuracy is 10^{-11} , or 2.5 slips per year; if a regular clock would slip 2.5 ticks per year, one would make a 1-min correction once in a lifetime. Table 6.1 summarizes the accuracy of clock strata.

Based on bit rate and type of network, ITU-T (G.812) distinguishes six synchronization clock types, types I–VI.

Table 6.1 Clock accuracy by stratum level

Stratum	Min accuracy	Slip rate	Notes
1	10–11	2.523/year	Primary Ref. Source (PRS)
2	1.6–8	11.06/day	e.g., 4ESS/5ESS
3	4.6–6	132.48/h	e.g., 5ESS/DCS
4	3.2–5	15.36/min	DCB/COT/DPBX/Access

COT: central office terminal, DCB: digital channel bank, DPBX: digital PBX

- Type I is used at all levels of synchronization of the digital hierarchy in 2,048 Kbps-based networks.
- Types II and III are used at all levels of the synchronization of the digital hierarchy that includes the rates 1,544, 6,312 and 44,736 Kbps.
- Type III is used in end offices that support the 1,544 Kbps digital hierarchy.
- Type IV is used in networks that support the 1,544 Kbps digital hierarchy.
- Type V is used in transit nodes of networks based on both 1,544 and 2,048 Kbps hierarchies, according to G.812, 1988 version.
- Type VI is used in existing local nodes of networks based on the 2,048 Kbps hierarchy according to G.812, 1988 version.

6.2.2 The Node Timing Unit and the Phase Lock Loop

Each node in the network contains a timing unit (TU), which tracks a reference clock at a designated receiving port or the timing reference clock of the building information timing supply (BITS). When the clock is received from BITS, it supplies the reference clock to all outgoing traffic of the node; typically two BITS reference clocks are supplied, the active and the alternate for protection, Fig. 6.2. When clock is extracted from a designated input data port, it supplies reference clock to all outgoing traffic of the node, Fig. 6.3. Other cases are also defined, such as timing through, and so on.

The clock circuitry in a network element consists of a local oscillator, a phase lock loop (PLL), filters, and other supporting circuitry. In communication networks, there are three PLL parameters of interest, hold-over accuracy, free-running accuracy, and pull-in/hold-in. These parameters and their limits are the subject of standards that define them according to network topology, bit rates, and operational practices.

Hold-over stability is the amount of frequency offset that an oscillator has after it has lost its synchronization reference. Hold-over stability has a limited duration, which is several hours. The hold-over accuracy is lower than the PRS accuracy.

Free-run accuracy is the maximum fractional frequency offset of the oscillator when there is no reference clock and it is free running at its own accuracy, which is specified by the oscillator manufacturer. When a clock is not locked to a reference, the random noise components are negligible compared to deterministic effects such as initial frequency offset.

Pull-in/hold-in is the oscillator's ability to achieve or maintain synchronization with a reference. Its range is at least twice its free-run accuracy.

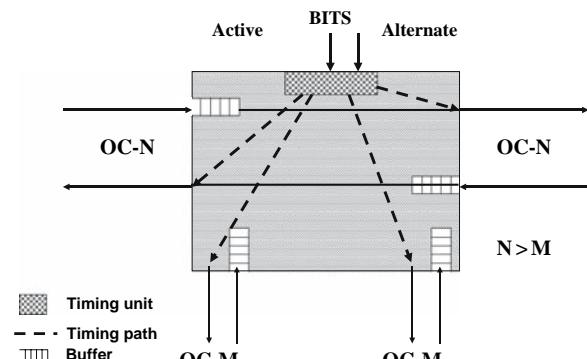
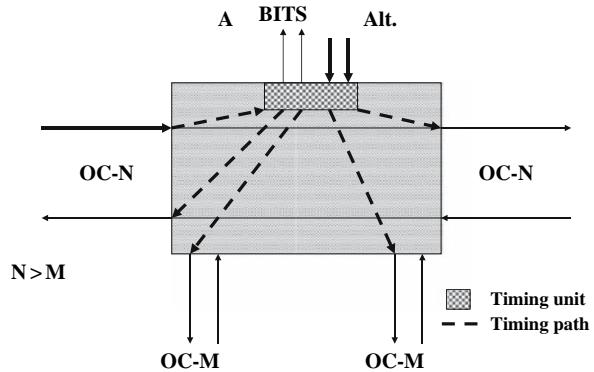


Fig. 6.2 Reference clock received from BITS

Fig. 6.3 Reference clock extracted from a data input port



Based on these definitions and clock types, then

- Type II clock has a more stringent hold-over stability specification than a type I clock.
- Type I and type II have a more stringent hold-over stability specification than a type III.
- Type I has a more stringent hold-over stability specification than type III clock. However, type I clocks can also be deployed in 1,544 Kbps-based networks if their pull-in range, noise generation, and noise tolerance comply with type II and type III clocks, for SDH compatibility.
- Type II clocks with type III clock hold-over stability may be used in 2,048 Kbps-based networks if their noise generation, noise tolerance, and transient behavior comply with type I clock when used in SDH.
- Finally, type V clocks are suitable for 2,048 Kbps-based SDH if their noise generation and short-term stability comply with type I clocks.

Synchronous networks assume a repetitive start of frame and with a prefixed repetition rate, such as SONET/SDH, DS1, and DS3. In all these cases, frames are seamless contiguous at 8,000 frames per second. Conversely, asynchronous networks do not necessarily assume seamless contiguous frames. Despite this, in certain data protocols such as ATM and in data transmitted at ultrahigh data rates (above 1 Gbps), frames are transmitted seamlessly contiguously even if this means that some frames in the stream are idle and do not carry client data. Thus, transmission of high bit rates at data networks is the same or comparable with the timing accuracy of synchronous transmission.

As a consequence, timing and synchronization issues, such as frequency variation and jitter need to be considered, as frequency variation and jitter may cause data buffer overflow or underflow and thus missed bits. As an example, for a binary signal at R bps in a medium L meters long at a speed v , the number of bits in transit at any time is LR/v . Thus, if $L = 100$ km, $R = 10$ Gbps, and the speed in the medium is $v = 2 \times 10^8$ m/s, then there are 5,000,000 bits in transit.

Based on this example, a temperature decrease by 1°F causes a 0.01 % increase in propagation speed. This will cause 500 fewer bits in transit and thus possible buffer underflow. Similarly, when the temperature increases, it may cause a commensurate overflow. Consequently, frequency variation must be compensated for and jitter removed in order to meet transmission performance requirements.

In legacy communication networks, frequency compensation is addressed with a buffer commonly known as *elastic store*. The elastic store smoothes out small variations of the incoming bit rate with respect to the local reference clock, and the start of frame is found from the framing bit embedded in the DSn signal.

In SONET/SDH optical networks, frequency justifications (positive or negative) are made at the receiver using specific octets in the overhead space of a frame. Based on this, the pointer octets, H1, H2, and H3, locate the start of payload in the SONET/SDH frame.

In local area networks, the header precedes the information field, and in some protocols a preamble precedes the header (such as fiber data distributed interface—FDDI), and thus the receiver locks onto the data rate and it identifies the start of frame very quickly.

In ATM, cell delineation (or synchronization) is accomplished using the head error control (HEC) byte.

When data protocols (IP, ATM, and so on) are adapted and mapped onto the SONET/SDH payload, then SONET/SDH frame synchronization is accomplished first and then the IP or ATM start of frame within the payload (SONET overhead bytes indicate type of payload and pointers identify the start of frame in the payload).

In the next generation all-optical network, optical elastic buffers cannot be implemented with all optical components cost-efficiently yet, and thus the elastic store or frequency justification is implemented at the far end of the path, at the receiver. However, research in the area of propagation time control is ongoing, and soon adaptable optical delay lines may become available to address the optical buffering issue.

In conclusion, although the synchronization mechanism is not the same in all cases, the synchronization function and frame detection is equally important in both synchronous and asynchronous networks, and as networks converge to the next generation optical network, synchronization strategies are hierarchically unified and simplified.

6.2.3 Synchronization Impairments

Assuming that clocks are precise and timing units supply the most accurate clock, the simple question with synchronization arises: So, what can go wrong with it?

In reality, there are many effects that affect the quality and precision of synchronization. We distinguish two major categories, environmental conditions and components.

Environmental changes, and particularly temperature, affect the propagation characteristic of signal over the medium. In fiber optics, the dielectric of the medium is a function of wavelength and environmental parameters; temperature and pressure variations may cause drift of the operating frequency [8]. As a consequence, propagation constant, dispersion, and other nonlinear phenomena play a key role, and variations may cause the operating frequency of the transmitting and of the receiving clock to drift, thus affecting synchronization; the effect of temperature on transmission has already demonstrated with an example in Sect. 6.2.2.

Components degrade and fail. Degradation is a gradual slow change that causes parametric variation that leads to timing misalignment between transmitter and receiver. Timing depends on electronic phase lock loops that are frequency stabilized with crystals cut precisely to resonate at a particular frequency. The frequency accuracy depends on material properties, geometry of the cut crystal, and operating temperature. However, even the most accurate phase lock loop has a finite probability of error which is measured in parts per million (ppm), or number of period slips from an expected one million periods. Failure is a permanent condition and causes permanent situations.

A timing reference source may be interrupted for some time. For example, when a fiber that carries the synchronizing tributary (such as a DS1) to a node is cut, the reference clock is lost. If this loss persists, then the oscillator enters a free-running state. Similarly, when a satellite timing source may cease for few or more minutes in which case the reference timing source is lost and the local oscillator enters a hold-over state, where it may remain for up to 8 h. In either state, the oscillator must meet certain accuracy requirements that have been specified by standards.

The most common impairments associated with synchronization are loss of signal (LoS), loss of clock (LOC), loss of frame (LOF), and loss of synchronization (LOS).

Loss of signal (LoS) is caused by a long string of 0s or by a line cut. In this case, monitoring circuitry detects the LoS condition and the local oscillator goes into the holdover state, a state with relaxed frequency accuracy. For example, in SONET,

- If there is no light for 100 ms, then an LoS is declared.
- No LoS is declared if loss of light is less than 2.3 ms.
- If there is no light for more than 2.5 s, the NE sends an alarm message to the operating system (OS).

Loss of clock (LOC) is caused by a long string of 0s or a long string of 1s that exceed the PLL holding time, or by a line cut. In such case, circuitry detects the LOC condition and the local oscillator goes into a hold-over state, a state with lesser frequency accuracy.

Loss of frame (LoF) is caused when there is excessive noise or excessive frequency variation between the local oscillator and the incoming signal, or excessive jitter in the incoming signal. When this occurs, the framer detects LOF and it enters a frame synchronization “hunt” state (in SONET/SDH). That is, it tries to locate the start of frame again; in gigabit-Ethernet, the “hunt” state is not part of the synchronization state machine. In SONET/SDH, if there are excessive errors in the framing pattern due to excessive noise and jitter and if a severely error frame (SEF) persists for more than 3 ms and there are incorrect framing patterns for at least four consecutive frames, then the network element (NE) sends a message to the operating system (OS).

Loss of synchronization (LOS) is caused when there is excessive variation in frequency between the local oscillator and the received signal. Then, the synchronizer goes in the LOS state and tries to resynchronize.

6.3 The Timing Signal

A timing signal $s(t)$ is mathematically described by the sinusoidal function:

$$s(t) = A \sin \Phi(t),$$

where A is a constant amplitude coefficient and $\Phi(t)$ is the total instantaneous phase.

The total phase $\Phi_{\text{id}}(t)$ of an ideal timing signal is expressed as

$$\Phi_{\text{id}}(t) = 2\pi v_{\text{nom}} t,$$

where v_{nom} is the *nominal frequency*.

Because of parameter fluctuations, the phase of the generated signal by an actual oscillator is not perfectly periodic. That is, the intervals between successive equal phase instants are slightly different than the ideal expected phase. Thus, the phase $\Phi(t)$ for actual timing signals is expressed as

$$\Phi(t) = \Phi_0 + 2\pi v_{\text{nom}}(1 + v_0)t + \pi D v_{\text{nom}} t^2 + \varphi(t),$$

where Φ_0 is the initial phase offset, v_0 is the relative frequency offset variation from v_{nom} , D is the linear frequency drift due to oscillator aging, and $\varphi(t)$ is a random phase variation.

The interval between two successive equal phase instants is the “period” T and it is inversely proportional to clock frequency. Period and frequency fluctuations lead to errors of the actual timing signal with respect to the ideal (error-free) timing. Thus, the time function $T(t)$ of a realistic clock is the measure of ideal time t and it is defined as

$$T(t) = \Phi(t)/2\pi v_{\text{nom}}.$$

The time deviation of the phase or period of an actual timing signal from the period of a reference timing source is called *time interval error* (TIE) function:

$$\text{TIE}(t; \tau) = [T(t + \tau) - T(t)] - [T_{\text{ref}}(t + \tau) - T_{\text{ref}}(t)],$$

where τ is the observation interval.

TIE is measured in absolute values of units of time (such as s, ns). Depending on the variability of the actual clock, TIE may vary linearly, sinusoidally, or randomly during an observation time ($\tau = n\tau_0$). Thus, in communication systems and networks, the time error of a clock is the difference between the time (or frequency) of this clock, $T(t)$, and the time (or frequency) of a reference clock, $T_{\text{ref}}(t)$. Thus, a time error function (TEF) $x(t)$ is defined as

$$x(t) = T(t) - T_{\text{ref}}(t).$$

The time error function serves in calculating a clock's stability parameters such as clock noise, wander, buffer characterization, frequency offset and drift, and so on. TEF is a function of time and its value may vary linearly, sinusoidally, or randomly. Thus, the TEF function depends on the timing model such as the maximum time interval Error (MTIE), the Allan deviation (ADEV), the modified ADEV (MDEV), the time deviation (TDEV), and the root mean square of time interval error (TIERms). A full description of this is beyond our purpose; the interested reader may find an analysis in ITU-T G.810, appendix II, and also in Ref. [9].

6.4 Signal Quality

In legacy synchronous communications networks, call arrival, call duration, call discontinued, and so on are probabilistic quantities that often are approximated by a *Poisson* distribution. In asynchronous data communications, this distribution is adopted to packet arrival, packet length (for variable length), and so on.

In general, n samples each with amplitude x_n are statistically distributed or dispersed around a mean value μ . The dispersion of a distribution or *standard deviation*, σ , is calculated from the weighted square of differences as

$$\sigma = \sqrt{\{[1/(n-1)]\sum(x_i - m)^2\}}.$$

The square of the dispersion, σ^2 , is known as the *variance* of the sample, and the ratio of *variance to mean* is known as the *coefficient of over-dispersion*, α :

$$\alpha = \sigma^2/\mu.$$

When $\alpha > 1$, traffic is termed *rough*, when $\alpha < 1$, it is termed *smooth*, and when $\alpha = 1$, it is termed *random*.

Traffic is related to effective bandwidth, which in WDM optical communications is calculated from the bit rate (typically, fixed per lightpath), packet rate (a statistical quantity), and optical channel (OCh) density (typically fixed but it can also be dynamic). Although traffic is not an obvious cause of jitter and bit errors, the probabilistic and statistical behavior of it is particularly in networks with optical add-drop multiplexers. Thus, taking into account the variability of power loss per path and the OCh density, one can deduce that the statistical behavior of traffic impacts the signal noise level, signal jitter, signal cross-talk, and errored bits in the signal.

6.4.1 Noise Sources

Noise can be defined in simple terms as “the superposition of a time-varying undesired signal on a target signal”, or in complex terms as “the mean squared statistical (Poissonian, Gaussian) fluctuation of photon phase and/or amplitude per unit bandwidth, which is caused by undesirable sources” [10, 11].

Noise is studied using a statistical model that best describes the generating mechanism and the statistical distribution of noise, such as Gaussian, Poisson, Fermi, and Bose–Einstein. What is important is that noise is ubiquitous and in communications, noise corrupts the integrity of signal and that under certain conditions bits are so much degraded that they cannot be clearly distinguished by the photodetector, which may yield the wrong bit value.

The initial study of electrical noise in communications started very early in the last century, with Albert Einstein, Brown, J.B. Johnson, H. Nyquist, Schottky, and others who laid the foundations of classical noise and explained also the quantum-mechanical nature of noise in conductors, electronic tubes, semiconductors, electromagnetic waves in space, and in dielectric waveguides. Thus, the electromagnetic nature of photons and their creation from excited atoms are closely related to electrical noise.

In general, based on the effect and the generating mechanism, the most common types of noise are:

- white (random) frequency modulation (WFM)
- white (random) phase modulation (WPM)
- flicker phase modulation (FPM)
- flicker frequency modulation (FFM)
- random walk FM (RWFM)
- thermal noise
- shot noise
- laser noise
- oscillator noise
- noise due to nonlinear light-matter interaction (such as crosstalk, dispersion, four-wave mixing, self-phase modulation, self-modulation or modulation instability, Stokes noise, and Chromatic jitter)
- optical amplifier noise
- quantization noise.

Thermal (or Johnson) noise is the quantum-statistical phenomenon of random movement of charged carriers (such as electrons) due to thermal agitation. Its initial study was based on a classical model of passive devices (R, C, L).

Shot noise is the random and time-dependent fluctuation in discrete-electron flow, as opposed to a steady flow of electrons in a conductor. That is, each electron is independent from the other electrons in the flow. In photon propagation, it is the random fluctuation of photon phase.

Flicker or 1/f noise is the result of impurities in the conductor region of semiconductor MOSFET devices. These impurities trap charged carriers, in which they remain for a short but random time. When carriers are released, they generate a time-dependent current fluctuation that is manifested as noise and is characteristic at frequencies below 10 kHz.

Amplifier spontaneous emission (ASE) is the random emission of photons by excited atoms in the fiber or in an excited semiconductor photonic device. These random photons are in the same spectral band with the signal and are manifested as noise.

Cross-talk, dispersion and dispersion slope, PMD, PDL, FWM, XPM, MI, ISI, and others are also noise sources due to the nonlinear interaction of the dielectric fiber and photons.

Although the understanding of the generating mechanism is important, in signal performance it is more important to know how much noise power has been added to signal power, that is, the ratio *signal to noise power* (SNR); when this ratio refers to optical noise and signal, it is OSNR. Thus, OSNR provides a measure of the clarity of the transmitted optical signal when it arrives at the photodetector. Notice that even if OSNR arrives with the expected performance, the receiver itself is a source of noise such as thermal, shot, flicker, and amplifier. A complete treatment of noise is beyond the purpose of this book as it has been described in the literature.

6.4.2 Quantization Noise

When an analog signal is converted to a binary bit stream and then reconstructed back to analog, the latter is not an exact replica of the original analog signal. That is, the analog signal is sampled periodically and each sample is converted to an n -bit binary code. This implies that the maximum amplitude range of the analog signal is quantized in 2^n steps, and thus each incremental step of the digitizer corresponds to $V/2^n$ V. Thus, between any two samples, there is a small voltage differential that the digitizer cannot discriminate for resulting in a small error called *quantization error*, which generates *quantization noise*. The larger the n , the smaller the quantization error and the smaller the quantization noise; the higher the sampling frequency, the higher the frequency content of quantization noise. The average quantization noise power $S_{n,q}$ into 1Ω load and for a quantization step height q is determined as $S_{n,q} = q^2/12$. Thus, a signal to quantization noise ratio is defined SNR_q (in dB) as

$$\text{SNR}_q = 10 \log_{10}[V_{\text{rms}}^2/(q^2/12)] = 10.8 + 20 \log_{10}[V_{\text{rms}}/q],$$

where it is assumed that quantization is uniform (the quantized increments q are equal), and the quantization error is independent of the sample amplitude, and V_{rms} is the rms value of the input.

Because quantization noise appears at the reconstruction site where the digital signal is converted back to analog (typically at the end of the path), this type of noise is not considered channel impairment but a digitizer technological issue, the choice of which affects the overall noise and traffic bandwidth contribution.

6.5 Transmission Factors

As the signal propagates, its power is attenuated; power attenuation is not the same for all media types and for all frequencies. Similarly, as the signal propagates, it is contaminated with two-dimensional noise, one in the amplitude domain (known as amplitude noise) and one in the time domain (known as jitter). All three, attenuation, noise, and jitter, are evolutionary processes which degrade the SNR of the optical signal, which in turn is closely related to the discrimination ability of the receiver; that is, its ability to separate the signal from the signal + noise. As a result, when the signal reaches the receiver, the receiver's sensitivity "sees" an attenuated and distorted signal and occasionally it cannot deduce the original bit value, so that although the bit that was transmitted as "1 or 0", it is deduced as "0 or 1".

In communications, it is established that an acceptable SNR value over an optical link (transmitter–receiver) is 40 dB.

6.5.1 Phase Distortion and Dispersion

In optical communication networks, the WDM signal travels in the fiber transmission medium with a propagation constant that depends on the dielectric (and refractive index) constant, as well as the signal power and wavelength. The WDM signal consists of many optical channels, and each channel consists of a narrow spectral band. As a result of this, the phase relationship between wavelengths does not remain uniform and thus there is phase distortion within each signal, which is manifested as *chromatic dispersion*.

6.5.2 Frequency Distortion

The monochromaticity of light generated by a laser depends on the uniformity, precision, and stability of the active region of the laser device. However, many random and periodic fluctuations that occur within it influence the generated light in spectral content and in timing, which is manifested as *chirp*.

6.5.3 Polarization Distortion

The polarization of state of photons is distorted by similar mechanisms to frequency distortions. Parametric fluctuations in laser and other nonlinear components on the path cause polarization distortion. In addition, residual birefringence in fiber causes the optical signal to travel in different polarization modes, each at different speeds, thus causing pulse distortion, known as *polarization mode dispersion* (PMD).

6.5.4 Noise due to Nonlinearity of the Medium

The photon–matter interaction is the source of several signal distortions and noise due to four-wave mixing, channel cross-talk, self-phase modulation, self-modulation or modulation instability, Stokes noise, and chromatic jitter [12].

6.5.5 ASE

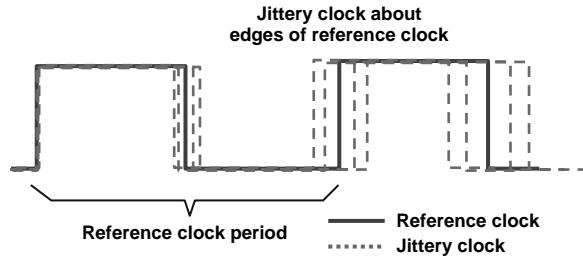
The spontaneous emission of photons during the process of atom excitation and spontaneous photon emission causes photonic noise. This noise is present during Raman amplification as well as during optical fiber amplification such as in erbium-doped fiber amplifiers (EDFA).

6.6 Jitter and Wander

Although the frequency of clocks at the transmitter and receiver conforms to the same specifications and accuracy, there is a relative small frequency shift between them, positive or negative, which may cause bit, frame or payload slips, buffer overflow or underflow, and loss of customer data [13–17].

As a consequence, nodes in the communications networks require a high degree of synchronization accuracy between the clock of a node and the incoming signal, as well as a correction mechanism so that incoming data is retimed or it is rate adjusted. In SONET/SDH, this is known

Fig. 6.4 Definition of jittery clock about the reference clock edges



as *frequency justification*. Under certain circumstances, the incoming clock has *high frequency jitter* that requires fast justifications. Fast justification however becomes another source of jitter (at the outgoing data) known as “*pointer jitter*”.

Jitter is viewed as a variation of the period of a bit stream in the time domain, Fig. 6.4. In optical communications, optical jitter is caused by many sources.

To study the effect of jitter on synchronization, consider two timing sources at the same frequencies. Assume that one of the two sources provides a reference clock whereas the other is a clock that is derived from incoming data; as such, the derived clock may deviate from the reference source; this deviation is oscillatory with its own frequency. Depending on how fast or slow this deviation changes, it causes different effects. Therefore, a distinction is made between “fast” and “slow” that results in two classifications, *jitter* and *wander*.

Wander is defined as a slow variation between a reference frequency and a derived frequency (from incoming data). *Wander* is defined (per ITU-T Recommendation G.810) as “the long-term variations of the significant instants of a digital signal from their ideal position in time”, where long-term implies that these variations are of frequency less than 10 Hz. A similar definition is also given for SONET [18], which also puts the frequency range for wander at below 10 Hz.

Jitter is defined (per G.810) as “the short-term variation of a signal’s significant instants from their ideal position in time”, where short-term implies that these variations have a frequency greater than or equal to 10 Hz. Thus, 10 Hz seems to be the demarcation frequency variation below which is defined as *wander* and above which as *jitter*.

Jitter requirements apply to interfaces between carriers and users, and between two carriers. Compliance with jitter requirements assures that jitter limits at OC-N and STS-N interfaces are met. Jitter and wander drive the specifications (G.823, G.824, and G.825) for synchronization requirements in SDH [19–21].

Jitter may be random, linear, or sinusoidal, Figs. 6.5 and 6.6.

Fig. 6.5 Sinusoidal jitter:
The actual “jittery” clock (B)
is compared with a reference
clock (A). The period
variation between reference
and jittery clocks (C)
is plotted in (D), where
jitter period, UI_{pp} , and
jitter frequency are identified

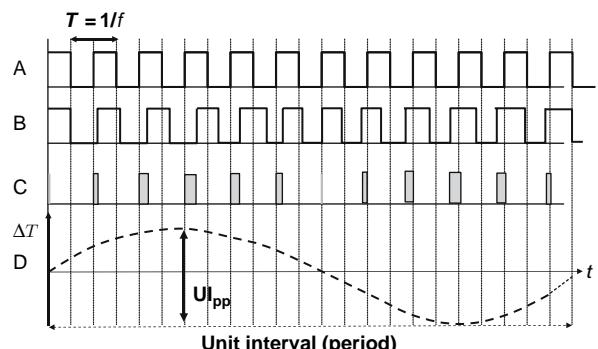
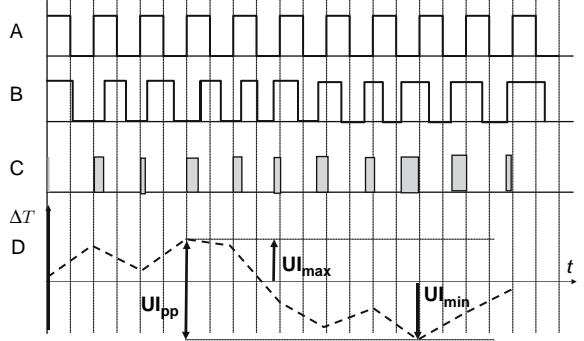


Fig. 6.6 Random jitter:
Plotting the period variation between reference (A) and jittery clock (B) in (C) reveals a random jitter period for which UIppmin and UIppmax are identified



A practical unit that defines a measure of jitter amplitude and peak-to-peak deviation of a real clock from a reference clock over a predefined measuring interval is the unit interval (UI) and the unit interval peak-to-peak (UIpp). The maximum UIpp (UIpp,max) is the maximum of the UIpps.

The UI is dimensionless and independent of the clock frequency, bit rate, and signal coding. For example, the UI values for different SDH STM-N/OC-N are provided in Ref. [22], Table 6.2.

The RMS jitter value represents the average power of jitter within the interval of observation. RMS jitter is defined by the expression

$$J_{\text{RMS}} = \sqrt{\{(1/T) \int [f^2(t)dt]\}},$$

where $f(t)$ is a description of the time signal of jitter and the integral is from 0 to T (or, the interval of observation). Notice that $f(t)$ may represent a random or a deterministic function.

Random jitter (RJ) is attributed to one or more sources such as optical amplifier noise, single sideband noise, photon–matter–photon interaction, random refractive index, and core variability over the length.

Deterministic jitter (DJ) is attributed to several causes such as SONET/SDH framing and pointer justifications, duty cycle distortions and initial frequency offset (when a clock from free-running attempts to lock onto a reference clock). Deterministic jitter is sub-classified to intersymbol interference (ISI), data-dependent jitter (DDJ), pulse-width distortion jitter (PWDJ), sinusoidal jitter (SJ), and uncorrelated bounded jitter (UBJ).

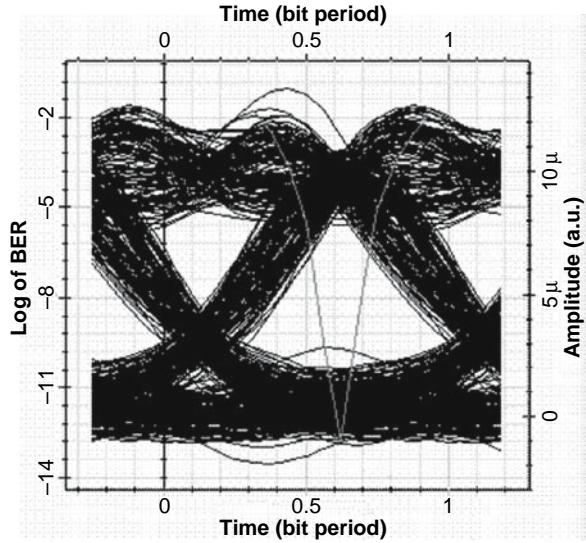
Jitter causes degradation of the received signal in the time domain, it narrows the sampling window at the receiver, and it is manifested by lateral eye diagram closure, Fig. 6.7.

Temporal fluctuation of spectral density is caused by laser drift and optical amplifiers, and when the wavelength is below the zero-dispersion point, it causes temporal broadening of the pulse. In addition, temperature, pressure, filter stability, and other conditions cause drift of the operating frequency. Some temporal fluctuations are also attributed to ambient temperature variations, which affect the signal propagation (group velocity) and polarization states.

Table 6.2 Unit intervals for STM-N/OC-N

STM-1/OC-3	1 UI = 6.43 ns
STM-4/OC-12	1 UI = 1.61 ns
STM-16/OC-48	1 UI = 0.40 ns
STM-64/OC-192	1 UI = 0.10 ns
STM-256/OC-768	1 UI = 0.025 ns

Fig. 6.7 Eye\diagram provides a qualitative indication of signal quality in terms of amplitude noise, pulse shape distortion, jitter, rise/fall time, and fluctuations



6.6.1 Intersymbol Interference

Intersymbol interference (ISI) jitter is the outcome of several optical impairments due to interaction of photon–matter–photon and due to dependence of the dielectric constant on frequency. However, the contribution of ISI on jitter may be considered negligible as compared with other jitter sources.

6.6.2 Data-Dependent Jitter

The pattern-dependent jitter (PDJ) is caused by repetitive patterns, such as the start of frame bytes A1 (Hex F6) and A2 (Hex 28) in the SONET/SDH frame, Fig. 6.8.

The A1 and A2 bytes are not scrambled and they repeat every 125 μ s, and thus the jitter generated by these bytes have an 8 kHz spectral band. All other bytes in the STN-N frame are scrambled and

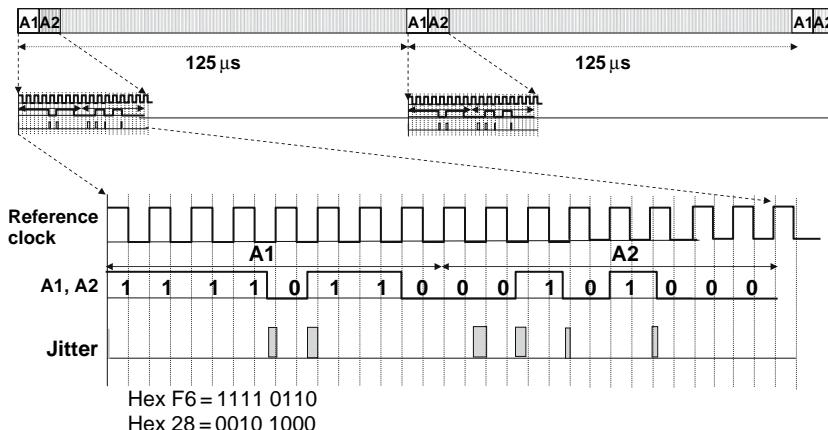


Fig. 6.8 Pattern-dependent jitter caused in SONET/SDH OC-3 by A1 and A3 overhead bytes

thus the generated jitter by them is random. Thus, the jitter component generated by A1 and A2 has a more distinctive spectral band than the jitter component of other bytes in the frame. Consequently, jitter should peak at a very high frequency that is related with the OC-N rate (such as 2.5, 10, or 40 Gbps) and a spectral band of 8 kHz because of frame periodicity. For example, in the case of OC-192 (10 Gbps), PDJ peaks at 3.24 MHz within a spectral band of 8 kHz.

6.6.3 Pulse-Width Distortion Jitter

If an on-off keying (OOK) modulator does not generate a square or symmetric trapezoidal pulse, then the optical pulse is neither symmetric nor the rise and fall time has the same slope. Therefore, as the pulses propagate, the jitter induced at the edges of pulses has different distribution at each edge causing pulse-width distortion jitter (PWDJ).

6.6.4 Sinusoidal Jitter

Sinusoidal jitter (SJ) is caused by sinusoidal variations of timing sources, which couple energy in electrically controlled devices that affect the optical signal. This jitter is also known as *repetitive*, and it may also be caused by switching power supplies that affect the transmitter or receiver functionality.

6.6.5 Uncorrelated Bounded Jitter

Uncorrelated bounded jitter (UBJ) is caused by power supply variations, unpredictable cross-talk, secondary transmission phenomena, and in general sources that are not described in the previous classifications. For example, bursts of jitter may be caused by cross-talk with bursty data, and uncorrelated four-wave mixing interference. It may also be caused by intermittent failures, power or phase-lock-loop glitches, and timing slips.

Thus, the understanding of jitter-generating mechanisms helps to understand the impact jitter has on link and signal performance metrics, such as BER and SNR.

6.6.6 Stokes Noise, Chromatic Jitter, and FWM noise

Optical fiber complies with parameter specifications that are recommended by standards. However, the value of fiber parameters, and particularly of the fiber core, exhibits parameter variation along its length. This variation is typically random. Although parameter variations may be unnoticeable over few hundreds of meters of fiber, it is noticeable over many kilometers and as light propagates, parameter variations affect its propagation and the quality of signal.

When a monochromatic signal propagates in fiber, because of fiber birefringence it is separated into states of polarization, each traveling at different speeds and phase, thus causing polarization mode dispersion (PMD). However, even PMD experiences random polarization variability as the two orthogonal states propagate in the fiber core because of nonuniform fluctuations of fiber-core imperfections. This is known as *Stokes noise*.

When a polychromatic signal from an actual optical source propagates in fiber, the dependence of dielectric on wavelength causes a temporal pulse broadening or chromatic dispersion (CD). However, a random variation of the fiber dielectric along its axis causes random variation of CD manifested as noise and jitter, known as *chromatic jitter*.

Thus, the random variation of the fiber dielectric generates different noise contributions to the propagation light; the sum of noise contributors is manifested as differential group delay (DGD) noise. The square of the relative DGD noise is the sum of squares of the Stokes noise and the chromatic jitter related noise:

$$[d(\Delta\tau)/\Delta\tau]^2 = [d(\Delta S)/\Delta S]^2 + [d(\Delta\omega)/\Delta\omega]^2,$$

where d is the differential operator, $\Delta\omega$ is the frequency variability, and ΔS is the polarization state variability at the output of the fiber. The inverse of the latter is known as the *bandwidth efficiency factor*, α . The bandwidth efficiency factor depends on the measuring method and its value is estimated empirically; this value may be from under 1 to more than 200. The value of α provides an indication of the potential maximum SNR of the optical signal as

$$\text{SNR} \leq \alpha \Delta\tau \Delta\omega.$$

In addition to Stokes and CD noise, there are other noise-generating mechanisms due to fiber parameter variations, such as self-phase modulation (SPM) noise and modulation instability (MI) noise. The square of these noise sources also adds to the overall relative DGD noise, in a general equation such as

$$N_{\text{DGD}}^2 = N_{\text{STOKES}}^2 + N_{\text{CD}}^2 + N_{\text{SPM}}^2 + N_{\text{MI}}^2.$$

In DWDM signals, in addition to self-inflicted noise by a single optical channel, there are additional noise and jitter contributions due to photon–matter–photon interaction. For example, two or more optical channels in close spectral proximity (such as 25 or 12.5 GHz) interact according to four-wave mixing (FWM) to generate a new fourth wavelength, λ_{FWM} . However, the λ_{FWM} product is the result of three uncorrelated channels and thus λ_{FWM} carries random noise; we call this FWM data induced noise. Now, as the λ_{FWM} interferes with another data-carrying channel at the same wavelength, it superimposes its noise power to it.

6.6.7 Sources of Jitter

Many sources contribute to the overall jitter of the DWDM signal, such as the following:

- Transmitter clock instability causes jitter or slow jitter (wander)
- The chirping effect of optical transmitters causes jitter
- Optical receivers may add noise and jitter due to filter, transimpedance amplifier, photodetector noise, and receiver clock instability
- In SONET/SDH, justifications and pointer adjustments cause jitter, similarly, timing variations with tributaries (payload), such as DS-ns
- Fiber nonlinear interactions with the optical signal (cross-talk, XPM, FWM, PMD)
- Interactions between bits of the same signal (such as intersymbol interference)
- Amplifier random noise, such as ASE. ASE may affect the rise/fall time of optical pulses and thus cause jitter. Amplifier jitter is cumulative
- Multiplexing and mapping may cause jitter
- Duty cycle distortions may cause jitter
- Stuffing and variable delay of asynchronous data jitter
- Non-monochromatic optical sources
- Repeater jitter is cumulative and in long haul where there are several repeaters; jitter may reach the maximum permissible value known as “jitter peaking”.

6.6.8 Jitter Generation, Tolerance, and Transfer

Jitter generation, jitter tolerance, and jitter transfer are three jitter characterizations of interest in communications system design and performance.

Jitter generation studies the sources of jitter, the mechanisms by which jitter is coupled with the signal, statistical properties of jitter, and jitter models for the probabilistic estimation of jitter.

Jitter tolerance provides a measure of the maximum amount of jitter without causing an error.

Jitter transfer is the amount of jitter that passes through a device, from input to output. When jitter exceeds the permissible limit, either synchronization would be lost or bit errors would be increased. Thus, the jitter transfer function (JTF) is defined to describe the amount of jitter (in dB) as a function of jitter frequency that passes from input to output through the system:

$$\text{JTF}(f) = 20\log[J_{\text{OUT}}(f)/J_{\text{IN}}(f)],$$

where J_{IN} and J_{OUT} are jitter in and jitter out, respectively.

Knowing the JTF of a system, an assurance about the signal quality at the receiver is provided. Since the JTF acts like a low-pass filter, Fig. 6.9, standards define the various JTF reference models. For example, ITU-T G.783 specifies that the UIpp jitter for STM-64 optical (10Gbps) is 0.3 UIpp in the range 20 kHz–80 MHz, or 0.1 UIpp in the range 4–80 MHz. Similarly, for an STM-256 optical (40 Gbps) is 0.3 UIpp in the range 80 kHz–320 MHz or 0.1 UIpp in the range 16–320 MHz.

6.7 Photodetector Responsivity and Noise Contributors

The gain-current responsivity of a photodetector is [23, 24]

$$R = \eta e G / h\nu = \lambda \eta e G / hc,$$

where η is the quantum efficiency, e is the charge of the electron (1.6×10^{-19} C), G is the gain of the detector, h is Planck's constant (6.63×10^{-34} J s), $\nu = c/\lambda$ is the optical frequency and c is the speed of light in free space ($\sim 3 \times 10^8$ m/s).

Assuming a quantum efficiency $\eta = 0.5$, $G = 1$ and substituting the values of the constant quantities, the responsivity in terms of wavelength (measured in nm) is $R = \lambda \times 4.02 \times 10^{-4}$ mA/mW. The received optical signal consists of the original signal plus the sum of all noise and jitter contributors, Fig. 6.10. However, the receiver itself adds more noise, which consists of three contributors, dark current (N_{dark}), shot noise (N_{shot}) measured in A^2/Hz and (Johnson) thermal

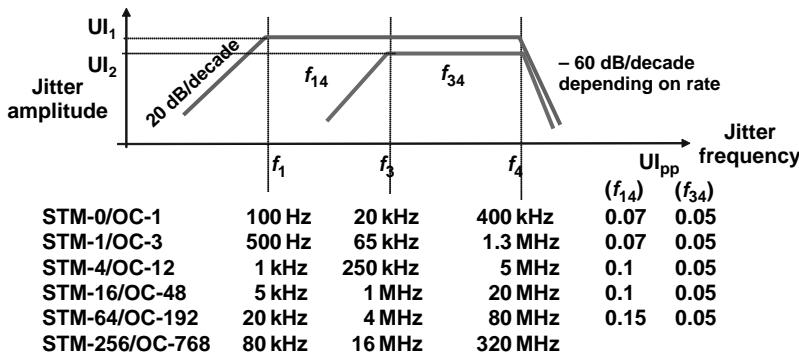
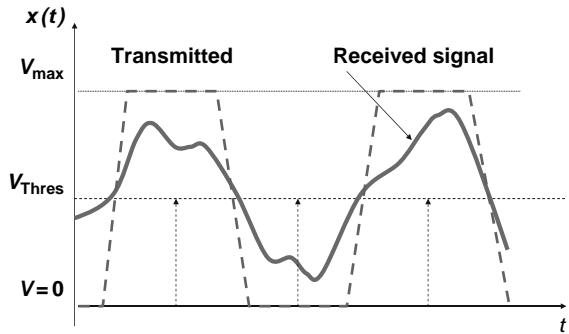


Fig. 6.9 Example of JTF template. The number in parenthesis defines the cutoff for different OC-Ns

Fig. 6.10 Transmitted and received signals



noise (N_J) measured in A^2/Hz . Thus, the SNR is the ratio of the mean square value of the generated current by the receiver to the total noise variance in the photocurrent.

In summary, the final signal performance depends on the sum of many noise and jitter contributors, attenuation, gain, and pulse shape distortions. The sum of these impairments construct a two dimensional distortion system, one dimension affecting the amplitude characteristics of pulses and the other the time domain characteristics.

References

1. ITU-T Recommendation G.781, *Synchronization Layer Functions*, June 1991.
2. ITU-T Recommendation G.810, “Definitions and Terminology for Synchronization Networks”, August 1996.
3. ITU-T Recommendation G.811, “Timing Requirements at the Outputs of Primary Reference Clocks Suitable for Plesiochronous Operation of International Digital Links”, 1988.
4. ITU-T Recommendation G.812, “Timing Requirements at the Outputs of Slave Clocks Suitable for Plesiochronous Operation of International Digital Links”, 1988.
5. ITU-T Recommendation G.813, “Timing Characteristics for SDH Equipment Slave Clocks (SEC)”, 1996.
6. ITU-T Recommendation G.822, “Controlled Slip Rate Objectives on an International Digital Connection”, 1988.
7. Telcordia GR-378-CORE, “Generic Requirements for Timing Signal Generators”, Issue 2, February 1999.
8. S.V. Kartalopoulos, *Fault Detectability in DWDM*, IEEE Press, 2001.
9. S.V. Kartalopoulos, *Optical Bit Error Rate: An Estimation Methodology*, IEEE/Wiley, 2004.
10. A. van der Ziel, *Noise: Sources, Characterization, Measurements*, Prentice-Hall, 1954.
11. F.N. Robinson, *Noise and Fluctuations in Electronic Devices and Circuits*, Oxford University Press, 1974.
12. S.V. Kartalopoulos, “DWDM: Networks, Devices and Technology”, IEEE Press/Wiley, 2003.
13. P.R. Triscitta, and E. Varma, *Jitter in Digital Transmission Systems*, Artec House, 1989.
14. R.P. Singh, S.-H. Lee, C.-K. Kim, “Jitter and Clock Recovery for Periodic Traffic in Broadband Packet Networks”, *IEEE Transactions on Communications*, vol. 42, no. 5, pp. 2189–2196, May 1994.
15. ITU-T Recommendation G.8251, *The Control of Jitter and Wander Within the Optical Transport Network (OTN)*, November 2001.
16. ITU-T Recommendation O.171, *Timing Jitter and Wander Measuring Equipment for Digital Systems Which Are Based on the Plesiochronous Digital Hierarchy (PDH)*, April 1997.
17. ITU-T Recommendation O.172, *Jitter and Wander Measuring Equipment for Digital Systems Which Are Based on the Synchronous Digital Hierarchy (SDH)*, March 2001.
18. Telcordia GR-253-CORE, *Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria*, Issue 2, December 1995.
19. ITU-T Recommendation G.823, *The Control of Jitter and Wander Within Digital Networks Which are Based on the 2048 kbit/s hierarchy*, 1993.
20. ITU-T Recommendation G.824, *The Control of Jitter and Wander Within Digital Networks Which Are Based on the 1544 kbit/s Hierarchy*, 1993.
21. ITU-T Recommendation G.825, *The Control of Jitter and Wander Within Digital Networks Which Are Based on the Synchronous Digital Hierarchy (SDH)*, 1993.

22. ITU-T Recommendation G.783, *Characteristics of Synchronous Digital Hierarchy (SDH) Equipment Functional Blocks*, October 2000.
23. H. Meyr, M. Moeneclaey, and S.A. Fechtel, *Digital Communications Receivers*, Wiley, 1999.
24. F. Tong, “Multiwavelength Receivers for WDM Systems”, *IEEE Communications Mag.*, vol. 36, no. 12, November 1998, pp. 42–49.

Chapter 7

Network Performance

7.1 Introduction

The meaning of performance itself in communications network is multifaceted as it pertains to network performance, traffic and service performance, and link and signal performance, for which the issues to be addressed, the metrics, and how they are measured are different, as there are the responsibilities and the ramification actions and processes. For example,

- Network performance is mostly concerned with the performance on the network layer, such as faults and degradations of nodes and links; protection strategies to eliminate or minimize congestion spots and traffic delay; traffic throughput increase, degradation or failure detection, and end-to-end signal performance. It is also concerned with optimum path establishment with minimal delay, with switching speed of client payload during path establishment and during congestion, and also with network upgradeability; that is, how the network can continue performing at an acceptable level while software and/or hardware upgrades are implemented.
- Traffic performance and service performance are concerned with the deliverability of individual client payload as well as the aggregate payload in compliance with the expected quality of service (QoS) parameters. Per service level agreement (SLA), among the parameters are end-to-end delay, round trip delay, bit or frame or packet error rate (BER, FER, PER), and expected deliverable bandwidth. Traffic performance is affected by frame overhead and network performance. Therefore, the two are interdependent.
- Link and signal performance is mostly concerned with the performance at the link layer, such as meeting the expected signal performance objectives at the link receiver, at the amplifier and equalizer of the WDM signals. It is also concerned with ramification strategies that monitor, detect, protect, and optimize the performance of WDM signals over the link. Notice that different transport protocols (SONET/SDH, ATM, IP, Ethernet, etc., over a WDM network) are required to meet different performance objectives at the end-to-end (path) and link layers.

In general, the link and path performance is affected by attenuation, noise, and jitter, as already discussed, that affects the probability of receiving a transmitted 0/1 bit. Because bits are the basic symbols in bytes, frames, blocks, and so on, error performance parameters are measured in terms of errored bits in a given sequence of bits, known as a *block*; for example, a SONET/SDH frame constitutes a block of bits and so does an Ethernet frame.

However, what is the key metric from which the aforementioned metrics are derived? In bibliography, one encounters two terms somewhat confusing. The first term is the bit error ratio (BERatio), which is defined as the number of received bits in error over a large number of bits transmitted. The second term is the bit error rate (BERate) defined as the ratio of errored bits to the total bits transmitted in a time interval. This subtle distinction is explained as follows: for the two data rates 1 Mbps and 10 Gbps, 10 errors in a second mean $10/1,000,000$ (or 10^{-5}) and $10/10,000,000,000$

(or 10^{-9}), respectively. Similarly, 10 errors in 1,000,000 bits transmitted means 10 errors per second for the 1 Mbps and 100,000 errors per second for the 10 Gbps. Accordingly, for 10^{-11} BERatio or 1 error in 100,000,000,000 bits received and at 1 Gbps will take 100 s to be observed, whereas for 10^{-11} BERatio at 40 Gbps will take 2.5 s. A consequence, the interval required to observe the performance metric is related to bit rate. Thus, although 10^{-11} itself does not explicitly define a performance metric, when the bit rate is stated then BERatio and BERate become equivalent, and 10^{-11} means 1 error in 100,000,000,000 bits transmitted at a bit rate x Gbps, and hence BER.

The bit error rate pertains to a continuous data stream of synchronous communications. In asynchronous data communications, there may be idle time (or idle packets) between packets that carry customer or control and maintenance data. Because in this case BER is not explicit of channel performance during idle intervals, and it does not provide any indication whether there are bursts of errors or if errors are normally distributed over time. Thus, the number of errored packets and the packet error ratio become more meaningful in asynchronous data. Based on this, standards provide several definitions for performance metrics [1–3]:

- Errored block (EB) is a block with at least one bit in error.
- Errored seconds (ES) or a one second period with at least one EB.
- *Block error ratio* (BER) is the ratio of blocks with at least one bit error to the total number of blocks transmitted in a given time interval. For small values, the block error ratio is comparable to bit error ratio, and for specific error models it is possible to calculate the bit error ratio from the block error ratio.
- Severely errored second (SES) is a one-second period in which more than 30 % of the blocks have errors.
- Severely errored period (SEP) of a sequence of 3–9 consecutive SES. This sequence should be followed by a second which is not a SES.
- Severely errored period intensity (SEPI) or the number of SEP events in available time divided by the total available time in seconds.
- Background block error (BBE) or an EB that does not occur as part of an SES.

Similarly, the error performance parameters for an available path are defined as the following:

- Errored second ratio (ESR) is the ratio of ES to total seconds in available time during a fixed measurement interval.
- Severely errored second ratio (SESR) is the ratio of SES to total seconds in a fixed measurement interval.
- Background block error ratio (BBER) is the ratio of BBE within an available window of time to total blocks in the available window time during a fixed measurement interval.

The performance objectives and performance parameters for an end-to-end path are elaborated in Ref. [2], the detailed description of which is beyond the purpose of this book. As an example, however, it suffices to list a typical example for a 27,500 km international synchronous digital *hypothetical reference path* (HRP):

- For the path type VC-4-16c or TC-4-16c, bit rate 2,405,376 Kbps, and 8,000 blocks (or frames)/s, the SESR is defined as 0.002 and the BBER as 1×10^{-4} .

An important note to be made is that the superiority of method and accuracy of performance measurements should be much higher when they are made out-of-service superior than in-service. In this chapter, we will describe in-service performance, a method that estimates several performance parameters.

7.2 Channel Performance

Medium attenuation combined with noise and jitter affects the level and shape of transmitted bits in the two dimensions, amplitude and time, such that the receiver may erroneously detect the logical value of some bits [4]. Thus, depending on the performance limits that have been determined for a specific application, when the frequency (or rate) of erroneous bits is below the expected received channel performance, the performance becomes unacceptable.

Although it is impossible to predict the logical value of a particular received bit, it is possible to statistically predict with reasonable confidence the ratio of errored bits to bits received if the link parameters for a channel are known, and also the statistical behavior (Gaussian, Poisson) of noise and jitter sources. A model of a link from transmitter to receiver including the transmission medium and all components in between is shown in Fig. 7.1.

Channel performance characterization is important for all transmission media, channels, and modulation methods. Media include wired, atmospheric, ionized, almost-free space, and fiber optic. Channels may be single, multifrequency, multiwavelength, time division multiple access, random, and so on. The channel statistical error behavior is better understood if one assumes a sliding window of time within which BER is calculated; most accurate measuring instruments work this way [5]. Modulation includes amplitude, frequency shift keying, phase shift keying, and multi-level. Therefore, channel performance measurements are distinguished by the method they are achieved as direct in-service, out-of service and else in estimated in-service using probabilistic approaches.

- Direct in-service methods calculate BER using error detection and correction (EDC) codes that are embedded in the data stream. Such EDCs are the cyclic redundancy check (CRC), the Reed–Solomon, the parity check, and bit interleaved parity (BIP). EDCs are routinely used because they are capable of detecting and correcting a limited number of errors; however, burst of errors, exceed the EDC limits and are not detected or corrected. In addition, EDCs require long observation time and they do not calculate other performance metrics such as signal to noise ratio (SNR), min–max received power signal, and Q-factor.
- Out-of-service methods rely on specialized instrumentation, which are large and costly, and therefore, they cannot be incorporated permanently in each data port of a node. These instruments employ pseudorandom bit sequences (PRBS) that are injected at the transmitting end of the medium and are detected at the receiving end; randomness minimizes pattern interference with data scramblers. The PRBS has a maximum sequence length of $2n - 1$, where n is a large odd number (usually 21, although other lengths have been specified). During the measurement time, service for the channel under test is interrupted.
- The probabilistic approach is a new method for channel performance estimation, and it can be used in-service and also out-of-service to estimate all performance parameters, such as BER,

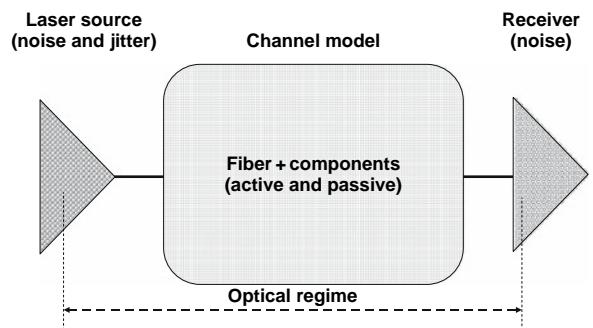


Fig. 7.1 A channel over a link is modeled from source to receiver with all possible impairments, including fiber attenuation, nonlinear phenomena, noise, and jitter

SNR, min–max power levels, Q-factor, and penalty. This method, which is further analyzed in this chapter, estimates the channel performance in a fraction of time (practically in real time), and because it uses the actual data stream it does not require PRBS. However, because this method does not have any correction capability, it can be used in conjunction with already existing EDC.

7.3 Carrier to Noise Ratio and Power–Bandwidth Ratio

In Sect. 6.4.2, we described the quantization noise as a contributor of noise in the end-to-end path and contributor to traffic bandwidth in the network. We also described that the signal to quantization noise ratio is defined SNR_q (in dB) as

$$\text{SNR}_q = 10.8 + 20 \log_{10}[V_{\text{rms}}/q], \quad (7.1)$$

where it is assumed that the quantization is uniform (the quantized increments q are equal), and the quantization error is independent of the sample amplitude, and V_{rms} is the rms value of the input.

If the bit power is E_b and the noise power in the same spectral range is N_0 , then the ratio bit power to noise power is defined as E_b/N_0 . In addition, if the carrier power at the receiver is C , then the ratio carrier to noise, C/N , in dB units is

$$C(\text{dB}) = C/N(\text{dB}) + N(\text{dBm}), \quad (7.2)$$

where N is the net power noise including quantization noise, and the carrier power is the rms value of the signal power at the receiver.

In optical transmission, N is calculated by summing all known noise contributors such as ASE, Boltzmann ($N_B = kTB$), including noise figure and noise margin, where k is the Boltzmann's constant, T is the absolute temperature, and B is the bandwidth of the passband filter for the channel of interest.

As a consequence, the *carrier to noise ratio* (CNR) in dB units is calculated according to

$$\text{CNR} (\text{dB}) = E_b/N_0(\text{dB}) + R_b/B(\text{dB}). \quad (7.3)$$

The ratio bit rate, R_b , to receiver bandwidth, B , is known as the *power–bandwidth ratio* (PBR):

$$\text{PBR} = R_b/B(\text{bits/s/Hz}). \quad (7.4)$$

At the receiver, the channel bandwidth B , under the condition of spectral matching, is equal to the filter bandwidth. Thus, a small change in E_b/N_0 causes a large change in CNR which causes a large change in BER. Thus, knowing CNR and N , the carrier power, C , required at the receiver is calculated.

Now, as the bit rate increases, the energy per bit decreases. However, if the power per bit increases, then interference increases and thus the noise content. That is, the relationship of signal to noise at the expected quality of signal requires careful characterization of the channel parameters over the optical span. Thus, the following relationship in dB units is derived:

$$E_b/N_0(\text{dB}) = 10 \log(\text{CNR}) - 10 \log(\text{PBR}). \quad (7.5)$$

Similarly, a small change in E_b/N_0 causes a large change in CNR, which causes an equally large change in BER and thus in performance.

7.4 Shannon's Limit

As noise with respect to signal increases, the SNR decreases. At some SNR threshold value, the signal becomes so corrupted that is considered unintelligible. In such case, the bits in the bit stream cannot be correctly recovered. Shannon has set mathematically the limit of a channel capacity (in bits/s), C , in terms of the sampling rate R_b and CNR:

$$C = R_b \log_2\{1 + C/N\}, \quad (7.6)$$

where R_b has a sampling interval τ ($R_b = 1/\tau$). If the sampling interval is equal to the bit period and W is the actual channel bandwidth (in Hertz), then

$$C = R_b \log_2\{1 + [R_b/W][E_b/N]\}. \quad (7.7)$$

In terms of the signal to noise ratio (in dB), the latter is expressed as

$$C = W \log_2[1 + \text{SNR}]. \quad (7.8)$$

If the bandwidth equals the bit rate, then bandwidth is known as *normalized bandwidth*, and Shannon's limit is higher than the actual. For example, if for a given BER the CNR ratio is 10 dB, then Shannon's limit for E_b/N_0 is 1.6 dB and not -11 dB.

7.5 Optical Signal to Noise Ratio

The optical signal to noise ratio (OSNR) is the RMS power of signal to RMS power of noise ratio. Therefore, for all practical purposes, OSNR is equal to C/N (or CNR), or

$$\text{OSNR} = C/N = [E_b/N_0][R_b/B]. \quad (7.9)$$

The ratio E_b/N_0 is a function of modulation method, modulation efficiency, and modulation loss. Therefore, this ratio needs to be expressed individually for each modulation case.

OSNR is directly related to the optical bit error rate (OBER) and optical error probability, OPe. However, OBER is not observable until the optical signal is detected by a photodetector and converted to an electrical signal. Thus, when the signal is received and converted to electrical, OSNR needs to be corrected reflecting the receiver and filter noise and gain. In such case, if the particular modulation energy loss factor is β^2 , the filter bandwidth is B , and the total noise is N_T , then the SNR is

$$\text{SNR} = \beta^2[E_b/N_T][R_b/B]. \quad (7.10)$$

This SNR is directly related to the error probability P_e or bit error rate (BER) and to channel performance.

7.6 Factors That Affect Channel Performance

In optical communications, several factors affect the quality of signal and the channel performance. For example,

- Attenuation weakens the optical power of the signal and thus it decreases the signal to noise ratio.
- Nonlinear photon–matter interactions and the dependence of dielectric on optical frequency cause bit spreading, sidetones, and *intersymbol interference* (ISI).
- In DWDM, one channel influences adjacent channels (either because of nonlinear light-matter interactions or because of spectral shift and channel overlapping) that cause *cross-talk*.
- The optical signal is immune to noise due to radio electromagnetic interference (EMI), but it is not immune to optical interference in the spectral band of optical channels, which is manifested as *optical noise*.
- The receiver, even if the optical signal is received at the expected performance level, adds its own noise (thermal, shot, $1/f$).

The key factors that affect the quality of signal and thus the BER at the receiver and the channel performance are the following:

- Stimulated Raman scattering (SRS): optical channels (at ~ 1 W) behave as a pump generating ASE that degrades the *S/R* ratio of longer wavelength channels.
- Stimulated Brillouin scattering (SBS): threshold $\sim 5\text{--}10$ mW (external modulation) and $\sim 20\text{--}30$ mW (direct modulation). It is controlled by lowering the signal power level or by making the source linewidth wider than the Brillouin bandwidth.
- Four-wave mixing (FWM): generated sidebands may deplete the optical signal power. It is controlled by widening the channel spacing selection.
- Modulation instability (MI): it may reduce SNR due to created sidebands (and thus decrease optical power level).
- Self-phase modulation (SPM): optical intensity changes the phase of signal, thus broadening the pulse width and the signal spectrum. However, operating in the anomalous dispersion region, the chromatic dispersion and SPM compensate each other. This may also result in spontaneous formation of solitons.
- Cross-phase modulation (XPM): interacting adjacent OChs induce phase changes and thus pulse broadening. It is controlled by selecting convenient channel spacing.
- Polarization mode dispersion (PMD): it changes randomly the polarization state of a pulse, causing pulse broadening. It is controlled by polarization scramblers, polarization controllers, or by selecting the appropriate fiber.
- Polarization-dependent loss (PDL): this is due to dichroism of optical components. It affects the SNR and Q-value at the receiver. It is controlled by polarization modulation techniques.
- Polarization hole burning (PHB): the selective depopulation of excited states due to anisotropic saturation by a polarized saturating signal in EDFA causes noise buildup. It is controlled by depolarized signals or polarization scramblers.
- Dispersion: OFAs exhibit all fiber properties, including dispersion.
- Noise accumulation: ASE noise is amplified by subsequent OFAs and because it is cumulative; it may exceed signal level ($S/N > 1$) and disable the 0/1 acceptable discrimination ability of the receiver.
- Temperature variations: temperature-sensitive components (e.g., lasers, receivers) require localized temperature stabilization or ambient conditioning.

7.7 Analysis of BER and SNR Related to Channel Performance

When a digital optical signal arrives at the photodetector, the sum of all linear and nonlinear effects affects the quality of the signal so that the shape and amplitude of bits in the signal are contaminated with noise, distortion, and attenuation so that some logic “ones” or “zeroes” are not recognized by the receiver correctly.

If we assume on-off keying NRZ modulation, the photodetector generates a electrical bit stream but adding to it more noise (thermal, shot, $1/f$, photodetector junction noise). The end result is a digital signal with a peak voltage $|V_p|$, in which the noise has a root mean square voltage $\langle V_n^2 \rangle$. Typically, a receiver has a decision voltage, b , and a sampling point positioned approximately in the middle of the bit period ($0.5\text{--}0.6T$). Sampling voltages above the threshold are interpreted as logic “1” and below as logic “0”, Fig. 7.2.

Assuming that the probability of an errored “one” and an errored “zero” is equal (in communications, this is a good assumption for a long string of bits), the total probability that an error to occur, P_ϵ , expressed in terms of the RMS value of the Gaussian standard deviation noise, σ_n , and of the error function $\text{erf}(.)$, is

$$P_\epsilon = \frac{1}{2} \{1 - \text{erf}(V_p/[2\sigma_n\sqrt{2}])\}, \quad (7.11)$$

where the function $\text{erf}(x) = \{2/(\sqrt{\pi})\} \int [exp(-y^2)dy]$ is integrated from 0 to x , and V_p/σ_n is known as the *peak signal to rms noise ratio*.

This error probability is also expressed in terms of the *error complimentary function* $\text{erfc}(.)$ as

$$P_\epsilon = \frac{1}{2} \text{erfc}[V_p/\sigma_n\sqrt{2}]. \quad (7.12)$$

$\text{Erfc}(.)$ values are provided in tables, and $\text{erfc}(.)$ can be expressed as

$$\text{erfc}(x) = \{1/[x\sqrt{(2\pi)}]\}e[\exp(-x^2/2)]. \quad (7.13)$$

The variance, σ_n^2 , is expressed in terms of the number of samples n , the observations x_i , and the mean value x_{mean} of the n observations, as

$$\sigma_n^2 = \{[1/(n-1)]\Sigma(x_i - x_{\text{mean}})^2\}. \quad (7.14)$$

The variance, σ_n^2 , of a discrete random variable x with mean x_{mean} is by definition

$$\sigma_n^2 = \Sigma(x_i - x_{\text{mean}})^2 P_x(i) \text{ over all samples } i \text{ of the variate } x, \quad (7.15)$$

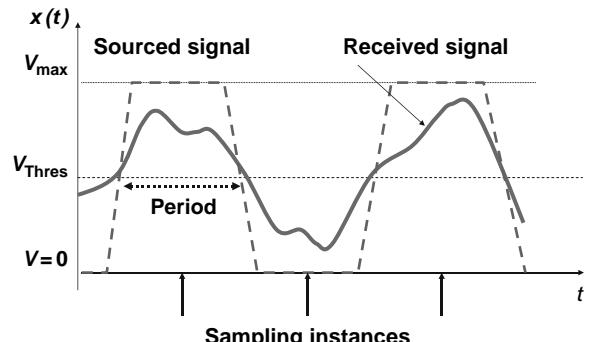


Fig. 7.2 The threshold point in a unipolar signal with noise is set at a point that depends on noise, jitter, and attenuation

where P is the probability function for the discrete case, and the mean is

$$x_{\text{mean}} = \sum_i P_x(i) \text{ for all } i. \quad (7.16)$$

In this case, the SNR is the ratio of peak signal voltage to RMS noise, and from the above analysis, a bit error rate (BER) relationship can be obtained. The probability distributions for “0” and for logic “1” contain the probability of error for “0”, $P_{e,0}$, if the integration from the threshold point to infinity and the probability of error for “1”, $P_{e,1}$, is the integration from zero to the threshold point. Thus, the total BER is the sum of both error probabilities for “1” and “0”:

$$\text{BER} = P_e = \frac{1}{2} (P_{e,1} + P_{e,0}) = \frac{1}{2} [Sf_{e,1}(x)dx + Sf_{e,0}(x)dx]. \quad (7.17)$$

In practice, the BER relationship is expressed in measurable terms of the means (μ_0 and μ_1 for “0” and “1”, respectively), the standard deviations (σ_0 and σ_1) and the decision threshold voltage, V_d :

$$\text{BER} = \frac{1}{2} \operatorname{erfc}\{(|\mu_1 - V_d|)/\sigma_1\sqrt{2}\} + \frac{1}{2} \operatorname{erfc}\{(|\mu_0 - V_d|)/\sigma_0\sqrt{2}\}. \quad (7.18)$$

When the above relationship is worked out in terms of the signal to noise ratio, the latter is expressed as

$$\text{BER} = \frac{1}{2} \operatorname{erfc}\{\sqrt{[\text{SNR}]}\}, \quad (7.19)$$

The signal to noise ratio is a measure of noise in signal. Signal to noise ratio is defined as the ratio of available signal power, P_{so} , to available noise, P_{no} :

$$\text{SNR} = P_{\text{so}}/P_{\text{no}}. \quad (7.20)$$

If P_{si} and P_{ni} are the available signal and noise power at the input of the receiver, then the noise figure (NF) is expressed in terms of the OSNR, as

$$\text{NF} = \frac{P_{\text{si}}/P_{\text{ni}}}{P_{\text{so}}/P_{\text{no}}} = \frac{P_{\text{si}}/kT_o df}{\text{OSNR}}. \quad (7.21)$$

Because the probability for error depends on the particular noise distribution (Gaussian, Poisson), an empirical formula that we have used for BER calculations of optical signals in single mode fiber, for an OSNR value in dB, is

$$\log_{10}\text{BER} = 1.7 - 1.45(\text{OSNR}). \quad (7.22)$$

Example: Assume OSNR = 14.5 dB, then $\log_{10}\text{BER} = 10.3$ and $\text{BER} = 10^{-10}$.

Often, another performance parameter is convenient to know, the quality factor or Q -factor. The Q -factor is defined as the ratio of the difference of means for 1 and 0 ($\mu_1 - \mu_0$) and the difference of standard deviations for 1 and 0 ($\sigma_1 - \sigma_0$):

$$Q = (|\mu_1 - \mu_0|)/(|\sigma_1 - \sigma_0|). \quad (7.23)$$

In traditional communications, in order to achieve a probability of one errored symbol in 10^{10} transmitted, an SNR greater than 15 dB is required. Because small increases in SNR result in rapid decrease of the probability of error and particularly above 15 dB, the region above $\text{SNR} = 15 \text{ dB}$ is known as *the cliff*.

When we consider optical signals, the modulated signal varies at best between zero and a positive power level. Thus, the threshold, V_d , is not set to zero but at some positive value. Then, the probability of bit error for the amplitude shift keying (ASK) modulation method (coherent or synchronous) and for the on-off keying (OOK) is

$$\text{ASK (Coherent): } Pe = (1/2)\text{erfc}\sqrt{[S/(4N)]} \quad (7.24)$$

and

$$\text{OOK: } Pe = (1/2)\text{erfc}\sqrt{(S/N)}. \quad (7.25)$$

The probability for error (or equivalently, BER), assuming that errors are Poisson random and the number of bits n is very large, is

$$\lceil P_n(k) = \lceil \{(np)^k / k!\} e^{-np}. \quad (7.26)$$

Then, the probability that the actual $P(\varepsilon)$ is better than an acceptable set level γ , known as confidence level (CL), is defined as (CL is typically expressed in percent, %)

$$\text{CL} = P(\varepsilon > N|\gamma) = 1 - \lceil [n!/(k!(n-k)!)] P^k (1-\gamma)^{n-k}], \quad (7.27)$$

where the sum is calculated from $k = 0$ to N .

The last equation can be solved for n , the number of transmitted bits required to be monitored for errors. Thus, assuming a confidence level of 99 %, a BER threshold of $\gamma = 10^{-10}$ is calculated; for a bit rate of 2.5 Gbps the required number n to detect a single error is 6.64×10^{10} .

Thus, if the *probability* of a single bit in error within the unit of time or within an equivalent block of bits is p , then the probability of two errors occurring independently within the same block is p^2 , of three errors is p^3 , and so on.

As a consequence, the channel confidence level (or performance) is critical to be set a priori, so that the link is engineered accordingly and also the type of error detection and correction code is selected.

For example, if the channel confidence level is set a priori to 10^{-12} (typical in optical high data rate networks), and the channel performance with all signal degrading influences is estimated to 10^{-5} BER, then an RS(255,239) hard error detection code (that detects 16 errors and corrects 8) increases the performance to more than 10^{-20} (that is, higher than the confidence level).

Although this is powerful, nevertheless estimates and channel qualifications have been made prior to providing service over a link and channel. The question arises, how can we monitor the channel performance on a continuous basis (in real time) and in service, after service has been provided? And how can we develop a strategy so that when excess degradation is detected, service can be provided uninterrupted?

7.8 BER and SNR Statistical Estimation Method

In this section, we describe an estimation methodology that, based on statistical sampling of the arriving signal, determines the performance parameters BER, SNR, Q-factor, NF, min–max power, and more, from virtual probability distributions for “1” and for “0” and the mathematical analysis already outlined.

The estimation method is outlined as follows.

As bits (ones and zeros) arrive at the input with different amplitude. Bits are sampled at an optimum point, $0.5\text{--}0.6T$, to compensate for jitter, and $I_{\text{eye}}/2$, where I_{eye} is the opening of the eye diagram, Fig. 7.3. Samples are categorized according to the threshold value; those above the threshold are placed in category “one” and those below it in category “zero”. Sampled data are digitized and are organized in amplitude ranges, according to frequency of occurrence of samples in each category, Fig. 7.4. Based on this, two virtual histograms are constructed, one for “0” and the other for “1”, Fig. 7.5, which in actuality they represent the probability distribution of “1” and “0” symbols. From these distributions, the statistical parameters $\mu_1, \mu_0, \sigma_1, \sigma_0, I_{1,\min}, I_{0,\max}, E_{\text{eye}}$, and E_{\max} are calculated.

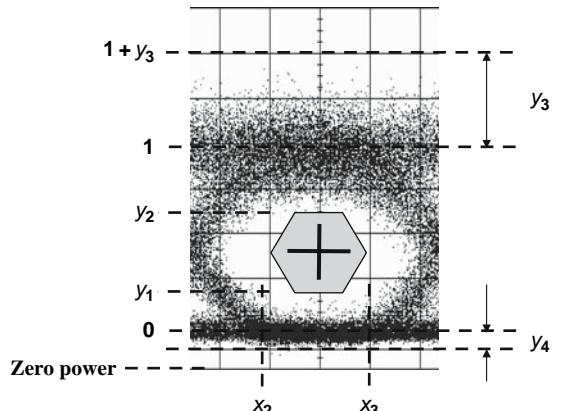


Fig. 7.3 A range within the eye diagram defines the optimum threshold and sampling instance (power and jitter)

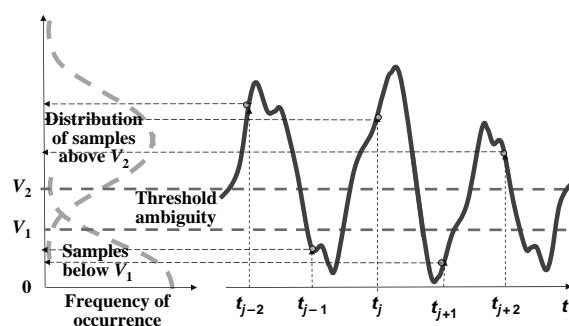


Fig. 7.4 Periodic sampling of the signal constructs the virtual distribution probabilities for “ones” and “zeros”

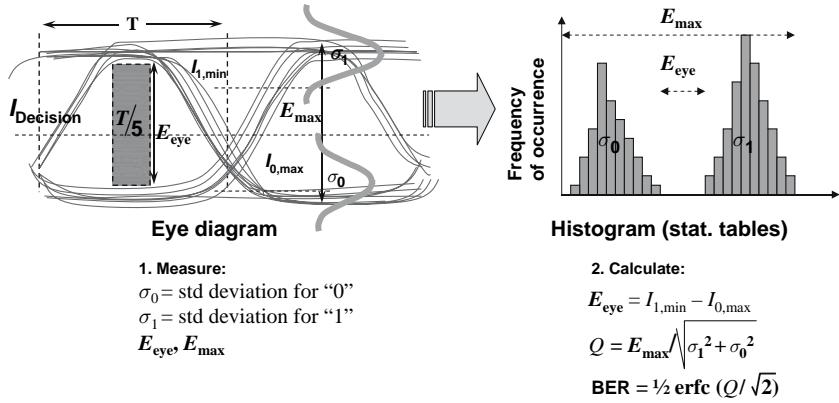


Fig. 7.5 From the two virtual distributions, the mean, variance, standard deviation, and other parameters are easily calculated

From these parameters, the following quantities are calculated:

$$E_{\text{eye}} = I_{1,\min} - I_{0,\max}, \quad (7.28)$$

$$r = E_{\text{max}}/E_{\text{eye}}, \quad (7.29)$$

$$Q = (|\mu_1 - \mu_0|)/(|\sigma_1 - \sigma_0|), \quad (7.30)$$

$$\text{BER} = \frac{1}{2} \operatorname{erfc}[Q/\sqrt{2}], \quad (7.31)$$

$$\text{SNR}_{\text{appr}} = (\rho + 1)/(\rho - 1), \quad (7.32)$$

$$\text{Extinction ratio } R_{\text{ext.}} = \mu_1/\mu_0. \quad (7.33)$$

If the received signal contains overshoot and undershoot, E_{max} and E_{eye} are not exact, in which case an approximated E_{max}^* may be used to compensate for it:

$$E_{\text{max}}^* = E_{1,\text{mean}} + k_1 \sigma_1, \quad (7.34)$$

where $k_1 = 1, 2$, or 3 and $E_{1,\text{mean}}$ is the mean value for logic “1”.

Similarly,

$$E_{\text{eye}}^* = (E_{1,\text{mean}} - k_1 \sigma_1) - (E_{0,\text{mean}} + k_0 \sigma_0), \quad (7.35)$$

where $k_0 = 1, 2$, or 3 and $E_{0,\text{mean}}$ is the mean value for logic 0 .

From the estimated V_p and the calculated BER, the standard deviation of noise is calculated from

$$\text{BER} = \frac{1}{2} \{1 - \text{erf}(V_p/[2\sigma_n\sqrt{(2)}])\}. \quad (7.36)$$

Finally, from the measured input power, the noise characteristics at the receiver, and the estimated SNR value, the noise figure is calculated from

$$\text{NF} = \frac{\text{Psi}/kT_o df}{\text{OSNR}}. \quad (7.37)$$

7.9 Circuit for In-Service and Real-Time Performance Estimation

7.9.1 The Circuit

Based on the method of the previous section, the functional diagram of a circuit is architected so that it can be integrated in a single VLSI, or in a VLSI and a microprocessor (a designer's choice), Fig. 7.6.

According to it, the incoming signal is sampled, converted to digital, and each sample is categorized and placed in a memory which is organized in amplitude ranges to facilitate construction of two virtual distributions. From these distributions, the aforementioned values are calculated either by the VLSI or by a microprocessor [6]. Thus, all performance parameters, BER, SNR, Q, NF, min–max power, and so on, are calculated.

The current performance parameters are also compared with the previous ones so that the rate of performance degradation or improvement is determined. This information is critical to forecast imminent severe degradations and failures in DWDM optical networks, to distinguish between degradation and intrusion [7, 8], and to also perform synchronously multichannel protection, multichannel equalization and to enhance network security [9–11].

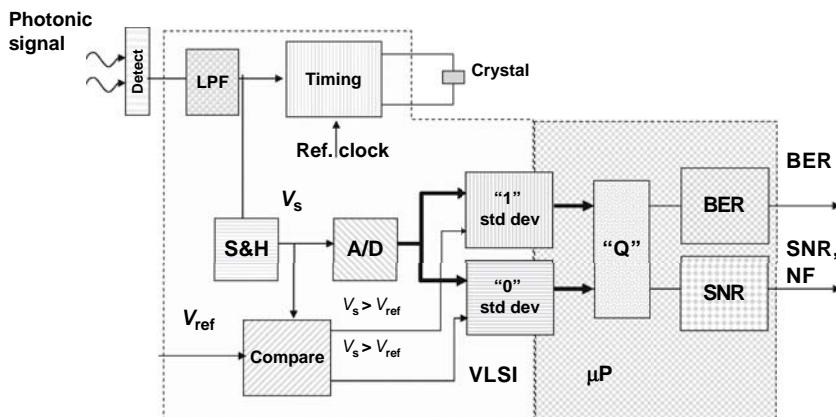


Fig. 7.6 Architecture of a circuit for the statistical estimation of BER, SNR, and other performance parameters

7.9.2 Performance of the Circuit

Because of the statistical nature of the method, few thousands of samples are sufficient. At 10 Gbps, 10,000 samples correspond to 1 μ s, and at 2.5 Gbps, 5,000 samples correspond to 2 μ s, both being extremely short. However, sampling signals at 10 Gbps (a sample per 10 ps) require extremely fast-switching electronic technology. Because errors are random, statistical sampling may be used, such as one every 1,000 bits (i.e., a sample per 10 ns); this sampling rate is feasible with relatively low-cost electronic technology and thus standard VLSI technology can be used. That is, a VLSI may be incorporated in each receiver and because it does not interfere with the receiving signal, it is considered in-service performance estimation [12, 13].

Using the statistical sampling aforementioned (one sample for each 1,000 bits) and for 10 Gbps, 12,500 samples are taken within 125 μ s, and thus 8,000 performance estimations per second. That is, for all practical purposes, this estimation rate is considered real-time in communications [14].

References

1. ITU-T Recommendation G.826, *Error Performance Parameters and Objectives for International, Constant Bit Rate Digital Paths at or Above the Primary Rate*, 1993.
2. ITU-T Recommendation G.828, *Error Performance Parameters and Objectives for International, Constant Bit Rate Synchronous Digital Paths*, March 2000.
3. ITU-T Recommendation G.829, *Error Performance Parameters Events for SDH Multiplex and Regenerator Sections*, March 2000.
4. S.V. Kartalopoulos, *Fault Detectability of DWDM Systems*, Wiley/IEEE, 2001.
5. S.V. Kartalopoulos, *Optical Bit Error Rate: An Estimation Methodology*, IEEE/Wiley, 2004.
6. S.V. Kartalopoulos, "Circuit for Statistical Estimation of BER and SNR in Telecommunications", *Proceedings of 2006 IEEE International Symposium on Circuits and Systems (ISCAS 2006)*, May 21–24, 2006, Island of Kos, Greece, paper #A4L-K.2, CD-ROM, ISBN: 0-7803-9390-2, Library of Congress: 80-646530.
7. S.V. Kartalopoulos, "Optical Network Security: Channel Signature ID", Unclassified Proceedings of Milcom 2006, October 23–25, 2006, Washington, DC, on CD-ROM, ISBN 1-4244-0618-8, Library of Congress 2006931712, paper no. US-T-G-403.
8. S.V. Kartalopoulos, "Optical Network Security: Sensing Eavesdropper Intervention", Globecom 2006, San Francisco, on CD-ROM, NIS03-2, ISBN: 1-4244-0357-X, ISSN: 1930-529X.
9. S.V. Kartalopoulos, "Optical Network Security: Countermeasures in View of Attacks", SPIE European Symposium on Optics and Photonics in Security and Defense, Stockholm, Sweden, September 11–16, 2006, paper no. 6402-9; also in SPIE Digital Library at <http://spiedl.org>, as a part of the Optics and Photonics for Counter-Terrorism and Crime-Fighting conference proceedings: SPIE Paper Number: 6402-9.
10. S.V. Kartalopoulos, "Distinguishing Between Network Intrusion and Component Degradations in Optical Systems and Networks", *WSEAS Transactions on Communications*, vol. 4, no. 9 September 2005, pp. 1154–1161.
11. S.V. Kartalopoulos, "Channel Protection with Real-Time and In-Service Performance Monitoring for Next Generation Secure WDM Networks", ICC 2007, Computer and Communications Network Security Symposium, June 24–28, 2007, on CD-ROM.
12. S.V. Kartalopoulos, "Channel Error Estimation in Next Generation Optical Networks", *WSEAS Transactions on Circuits and Systems*, vol. 3, no. 10, December 2004, pp. 2281–2284, ISSN 1109-2734, and ISBN 960-8457-06-8.
13. S.V. Kartalopoulos, "In-line Estimation of Optical BER & SNR", SPIE Photon East, October 23–26, 2005, Boston, MA, Track: "Optical Transmission Systems and Equipment for WDM Networks IV", session 3, paper no. 6012-8, on CD-ROM: CDS194.
14. S.V. Kartalopoulos, "Real-Time Estimation of BER and SNR in Optical Communications Channels", *Proceedings of SPIE Noise in Communication Systems*, C. N. Georgiades and L.B. White, eds., vol. 5847, 2005, pp. 1–9. Also, invited paper at SPIE Fluctuation and Noise Symposium, May 24–26, 2005, Austin, TX.

Chapter 8

Traffic Management and Control

8.1 Introduction

Communications traffic management and control is in many ways similar to managing and controlling vehicular traffic in a large city. Think of the main avenues as arterial traffic bearing links that bring traffic (vehicles and pedestrians) to intersections with traffic lights. In this case, traffic lights may be considered the equivalent of (traffic) switching nodes, whereas vehicles and pedestrians are the equivalent of packets of information in communications. If traffic lights are well synchronized and they turn green and red for the correct amount of time according to volume of vehicles or pedestrians at the queues, then traffic (frustrating) jams are eliminated or at least minimized. But how do we control all lights to accomplish this? Currently, in large cities, intelligent cameras monitor the flow of cars and the queues at the intersections, and based on a traffic algorithm, lights control the flow to minimize (at least in theory) congestion. However, currently this requires human intervention, and it is not completely automatic. In fact, the scenario of computer-controlling traffic lights has inspired a Hollywood movie.

This city-traffic paradigm, as complex as it may seem, is much simpler than a communications switching node, where there are many input and output fibers, each fiber has many optical channels, and each optical channel carries a signal (e.g., OC-48), which is the multiplex of many tributaries. In this scenario, some signals may need to be switched intact, whereas some others need to be demultiplexed since different tributaries need to be switched to different output ports. Moreover, the signal may contain synchronous payloads (voice, video) and asynchronous (IP, Ethernet, and other data specific); that is, there are different protocols to be executed and different requirements (see Figs. 4.19 and 4.26). Thus, some payloads need to be switched without delay, whereas some others may be temporarily buffered. With such complexity, the city-traffic control problem suddenly seems very simple compared with the communications traffic control. Based on this communications paradigm, in DWDM optical networks, there are two major management types: one is concerned with the wavelength management across the network and the other with client bandwidth management.

In the following, we assume that control messages that are required for bandwidth management and connectivity establishment are accomplished using specific messages and algorithms based on one of the several well-known methods: distributed or centralized control and in-channel or out-of-channel messages.

Centralized control implies that all nodes send configuration and state messages to a centralized system that oversees the operation and connectivity establishment across the overall network, Fig. 8.1. Although centralized control is efficient, an agreement must exist among all network operators (if different) on common network parameters, performance objectives, and protocol languages.

Distributed control implies that all nodes in the overall network partake in the network control, Fig. 8.2. This is accomplished with extensive protocols to find the best route in the network as well

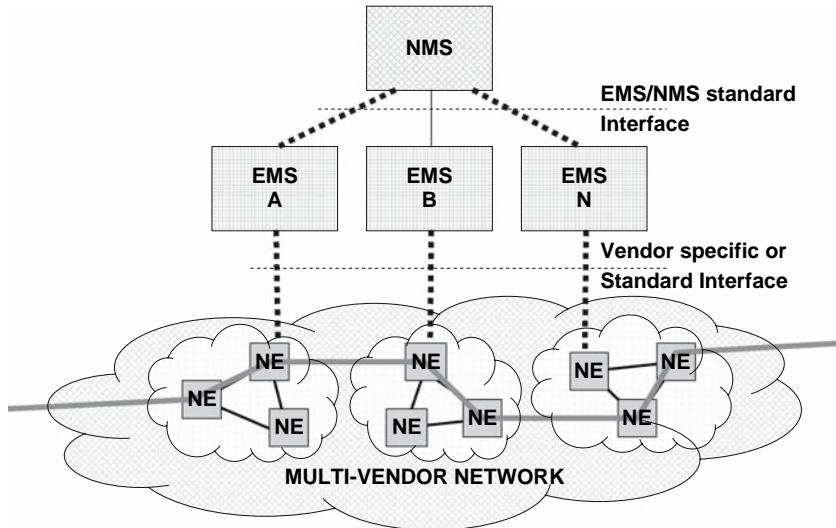
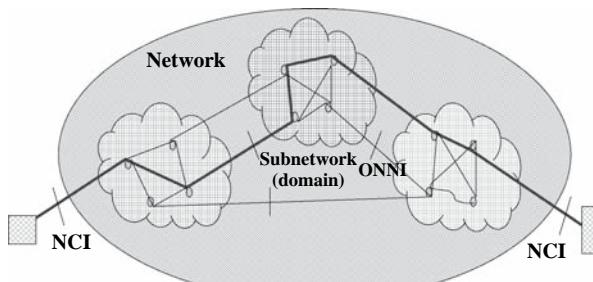


Fig. 8.1 Centralized control of a multi-vendor network environment consists of interconnected network elements (NE) that comprise network domains, and each domain is connected with the network management system (NMS) via element management systems (EMS)

as to manage the health of the network and traffic efficiency. For example, the hop-by-hop route discovery and flooding the network are two well-known algorithms [1]. Because distributed control uses extensive protocols and algorithms, an agreement must exist among all network operators (if different) on common network interface protocols and performance objectives.

In-channel messages are messages embedded in the overhead of the same channel or packet that transports client data. For example, in SONET/SDH, specific control messages (for error control and protection to switching) are included in the overhead. Conversely, out-of-channel messages are messages that use specifically allocated channels or packets; for example, this is the case in ATM which uses specific ATM cells for call admission control and service level agreement negotiation, and in the OTN case, it uses a separate supervisory channel, Fig. 8.3.

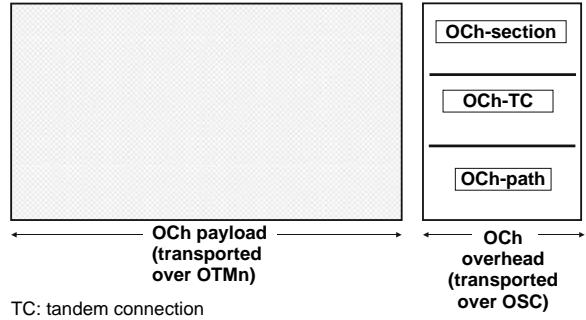


ONNI: opt net-to-net interface

NCI: network to client interface

Fig. 8.2 In distributed control, all nodes partake in the discovery of the best optical route across the overall network, which may consist of subnetworks or domains

Fig. 8.3 In OTN, overhead information about section, path, and tandem connection is transported with an (out of) optical supervisory channel (OSC)



8.2 Client Bandwidth Management

Client bandwidth management is a function that is required by all types of communication systems and networks, voice or data, small or large. This function must assure that client's data is delivered reliably, securely, timely, and with the agreed quality of service [2], regardless of the method it is transported, namely, by means of tributary or container units (as in synchronous traffic), or directly mapped (or bulk filled) in the synchronous payload (see Fig. 2.10), or packetized and transported by means of adaptation.

Client bandwidth management has two objectives: (1) deliver the client's bandwidth according to service level agreement and quality of service and (2) increase the network bandwidth efficiency by filling the payload envelope or the network bandwidth capacity with the client data as much as possible. However, as traffic becomes more elastic [3], as the aggregate bandwidth demand increases, as faults and severe degradations occur in nodes, on fiber links, and in optical channels [4], traffic management becomes more challenging.

8.3 Wavelength Management

In modern DWDM systems, each wavelength of the ITU-T grid is used as a separate optical path, also called a lightpath, which like a highway carries many client signals establishing end-to-end connectivity. Currently, there are two fundamentally different methods for establishing lightwave connectivity. The first method considers a path for which the same wavelength over the entire end-to-end path is assigned even if the lightpath is across several subnetworks, each managed by different network operator; this case is known as *single-wavelength path connectivity*, Fig. 8.4. Although at first glance this method may seem simplistic, in a multinode network, it is complex, and it may result in wavelength contention (or blocking) and thus network inefficiency. The second method considers different wavelengths that are concatenated over a complete path; this method is

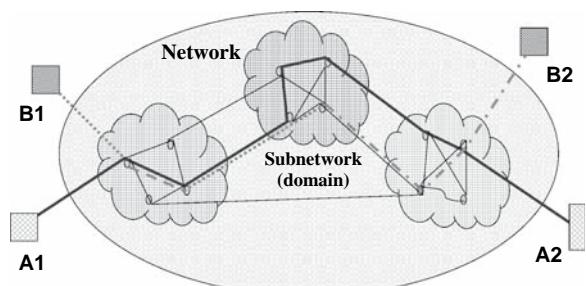


Fig. 8.4 A mesh network may establish connectivity using the same wavelength end to end or multiple concatenated wavelengths

known as *multi-wavelength path connectivity*. The latter method requires either wavelength converters at each node or nodes that are optical–electrical–optical (OEO). This method has the added advantage of utilizing different wavelengths of the ITU-T grid on the links that make up the path and thus it increases wavelength utilization and efficiency. However, this method adds to node design complexity and cost of components substantially, and thus to failure modes, provisioning, and maintenance.

Wavelength management for the single-wavelength path connectivity method is simpler although limited and bandwidth inefficient. The reason is that the network may be unable to find the same wavelength from source to destination for all possible routes leading to potential wavelength blocking. For example, if we consider a mesh DWDM network, the blocking probability is a function of topology, number of fibers per node and number of wavelengths (optical channels) per fiber, and also number of dropped and added channels at each node; we assume that nodes in a mesh network are also optical add-drop multiplexing nodes (OADM). Thus, as the number of fibers per node and wavelengths per fiber increase, the probability for blocking decreases; the key objective in this case is bandwidth efficiency [5].

Wavelength management for the multi-wavelength path connectivity method is more complex although more bandwidth efficient; and because of the added hardware complexity (added wavelength converters), it is costlier. In this case, if we consider a mesh DWDM network with wavelength converters in each node, the blocking probability is a function of topology, number of fibers per node and number of wavelengths (optical channels) per fiber, number of dropped and added channels at each node, and also number of converters in each node. Thus, as the number of fibers per node and wavelengths per fiber increases, the required number of converters in each node increases, the probability for blocking is almost eliminated although the cost of the network and wavelength management increases dramatically. As a result, the objective in this case is to balance bandwidth efficiency and optimize cost. A hybrid method may be used to accomplish this: Allocate a number of wavelengths that provide single wavelength connectivity over selected paths and allocate the remaining wavelengths for the multi-wavelength connectivity path method; this method eliminates several wavelength converters, and it simplifies node design and wavelength management.

A consequence that also needs to be addressed is protection strategy, at the fiber level as well as at the wavelength level due to severe degradation or component hard failure; protection may be simple or complex, depending on the adapted protection strategy, 1 + 1, 1:1, 1:N, and so on.

In DWDM, another issue has arose, namely *wavelength collision*. In traditional single-wavelength networks, wavelength collision has not been an issue since the optical channel was only one (at 1,310 or at 1,550 nm). Thus, moving this channel from one fiber to another, it was a straightforward operation, as long as a protection fiber was available. In DWDM, where one system in one domain is interconnected with a system in another domain (where domains may be operated by different network providers), wavelength collision may occur, Fig. 8.5, wavelength conversion is needed and also wavelength management over the complete end-to-end path. Here, *wavelength collision* is defined as the action by which one optical channel associated with a particular wavelength over a

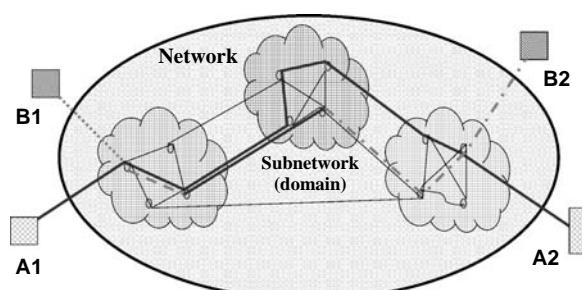


Fig. 8.5 Some same-wavelength lightpaths may overlap over one or more links causing wavelength collision

link is switched from link A to link B, where in link B the same wavelength is already in use for a different path; this definition is extendable to more than one wavelength.

As a result, a substantial effort has been spent to determine the blocking probability for different network topologies, node complexities, and traffic characteristics and also under static and/or dynamic conditions. In this pursue, several algorithms were developed to establish the rules that optimize wavelength assignment procedures and thus traffic routing and network throughput [6–12].

8.3.1 Paths with ROADM

WDM optical point-to-point, mesh or ring networks have nodes that are capable of dropping and adding wavelengths, hence known as optical add-drop multiplexing nodes (OADM); the added/dropped wavelengths carry traffic to be delivered to customers at the location of the OADM. Currently, this is accomplished by designating a priori which wavelengths of the grid is to be dropped as well as the number of wavelengths (depending on application, from 1 to 4.). This is known as fixed OADM configurability.

The next generation intelligent network however needs to be able to drop and add flexible traffic, and thus OADM nodes need to be reconfigurable [as described in 13]; that is, OADM nodes must be able to be programmed either locally or remotely and be able to drop and add from 1 to N wavelengths, as need arises; such nodes are known as reconfigurable OADMs (ROADM). However, because of the dynamic nature of reconfigurability, ROADM need to be fast, reliable, and verifiable. We should also point out that mesh networks with ROADM add an additional level of complexity on the path or route finding algorithms because wavelengths that are available for establishing connectivity may have to be used by ROADM and thus the number of wavelengths for end-to-end connectivity need to be recalculated. Additionally, reconfigurability adds to node design complexity because certain reconfigurable or reassigned wavelengths are dropped and added instead of continuing through or vice versa; thus, this may require optical power budget recalculation and wavelength equalization and dispersion compensation.

Another node complexity is added if at the ROADM certain wavelengths are reassigned to be dropped and added in order to carry multiplexed traffic (such as SONET/SDH), in which some VTs need to pass through (however, this is simplified if traffic is packetized); optimizing traffic efficiency for different traffic types is the subject of current research.

8.4 Traffic Management

Traffic management is related to client traffic and therefore, although related to bandwidth management, has more specific tasks to perform. For example, although bandwidth management addresses the distribution of traffic evenly over network, also known as bandwidth balancing, traffic management is more concerned with client traffic so that it meets the expected quality of service, expected real-time delivery, and also client bandwidth on demand. Traffic management assures that incoming traffic is monitored, it is properly connected, and its quality level is maintained; this is accomplished by policing incoming client traffic at the edge nodes. As a consequence, traffic policing requires continuous monitoring for traffic parameter compliance with the service level agreement (SLA), as well as monitoring for connection parameter violations, and user equipment malfunctioning, a function known in ATM as *connection monitoring*.

The ATM Forum and the ITU-T have defined parameters to maintain the agreed traffic QoS. It has also defined algorithms for policing the traffic at the user–network interface (UNI) for both *constant bit rate* (CBR) and *variable bit rate* (VBR). This algorithm is known as the *generic cell*

rate algorithm (GCRA). The GCRA is implemented with the continuous-state *leaky bucket* and it is based on two parameters: the *increment* (I) and the *limit* (L). The I parameter affects the cell rate; the L parameter affects the cell burst. For example, the parameters utilized in ATM for traffic management are

- *peak cell rate* (PCR) for CBR and VBR connections,
- *sustainable cell rate* (SCR) for VBR connections, and
- *maximum burst size* (MBS) for VBR connections.

These parameters are provided by the user during the connection admission control (CAC) at UNI. In addition, the *burst tolerance* (BT) parameter puts a restriction on the additional traffic above the SCR, before it is tagged excessive traffic.

8.5 Congestion Management

Failures and severe component degradations can be statistically predictable according to manufacturer's failure in time (FIT) data. However, there are also unpredictable failures, such as fiber cuts. Either way, failures and degradations cause statistical fluctuations of traffic flow in the network in an attempt to bypass the fault. Thus, there is a finite probability that traffic through a node or link reaches the maximum capacity establishing a congestion condition manifested by node or link overload, bandwidth lost, or even network crash. In general, congestion management is defined as a network element state unable to meet the negotiated network performance and quality of service (QoS) objectives. As such, congestion management is seriously addressed.

In DWDM, congestion management is very important because severely degraded components or faulty nodes and links affect a humongous amount of traffic. Therefore, traffic rerouting needs to be executed expediently and efficiently. Thus, congestion management needs to consider:

- the type of fault as each fault influences bandwidth flow at a different level,
- types of services supported by the network as each traffic type has different requirements,
- network topology as each topology has different service survivability characteristics,
- size of network, in both bandwidth capacity and number of nodes, and
- internetworking as the overall path may cross several network-provider domains, each consisting of nodes with different system capabilities.

8.6 Routing Algorithms

In DWDM optical networks, a lightpath connects a source with a destination and it may consist of the same wavelength from one end to the other end or it may consist of several concatenated wavelengths, whereby a wavelength changes to another by means of wavelength converters.

A mesh network with many nodes has a large number of possible (source to destination) paths. A DWDM mesh topology may be thought as the superposition of many mesh single-wavelength topologies.

In DWDM optical mesh networks, one path may overlap with another path over one or more links. This makes the routing algorithm more complex as the same wavelength from two different sources cannot coexist over the same fiberlink. If this occurs, cross-talk severely degrades the two channels; some solutions use polarization states to minimize cross-talk but the link must be able to maintain the two polarization states over its full length. Thus, at setup time, there is a finite probability of wavelength blocking, particularly when wavelengths are dynamically assigned. In order to minimize the blocking probability efficiently, optical nodes require specific configuration

features, wavelength conversion strategy, and switching capabilities. This is accomplished with the use of routing and wavelength assignment (RWA) algorithms; RWA algorithms are classified as static and dynamic [14].

Dynamic RWA algorithms assign and remove lightpaths randomly according to network connection requests, traffic utilization, and congestion states. To increase network bandwidth performance, a node advertises its status and wavelength availability to other nodes by means of packets such as addressable, shared, channelized, and hybrid. This includes global network state parameters on links within the network, as well as local node status. Two dynamic routing algorithms are the alternate path routing and unconstrained path routing.

- Alternate path routing assumes that every node stores the first N shortest and predetermined paths to each destination by utilizing global and local node link information. Congestion is determined in part by the number of wavelengths available per path or link.
- Unconstrained routing considers all paths, and it is based on the cost function of all links within the network to determine the optimal end-to-end path.

In general, dynamic routing algorithms process global network state information to determine the end-to-end path. Alternatively, the deflection (or alternate) routing algorithm is limited to state information from neighboring nodes only, in which case links are chosen on a hop-by-hop basis. According to it, at each intermediate node, a control message is processed before being forwarded to the next node. This continues one hop at a time until the destination node completes the final process of the control message and sends it back to the source node. Decisions on wavelength assignment are based on the shortest path first, followed by alternative route considerations if a specific wavelength is unavailable. The least-congested deflection routing scheme chooses from a list of outgoing links based on the largest number of feasible wavelengths. The shortest path first method results in lower blocking with less traffic while a least-congested policy results in lower blocking at heavier traffic loads. Those routing schemes are applicable to single fiber mesh topology, as well as multi-fiber networks.

8.7 Discovery of Optical Network Topology

Wavelength assignment algorithms provide the optimal wavelength connectivity to a connection request. Wavelength assignment is classified as static and dynamic. For static wavelength assignment, a sequential graph coloring approach is used to find the minimum wavelengths (colors) for over a path.

For the optical network to route optical channels, the physical and the logical layer topology of the network must be known. That is, each switching node must know the characteristics of the adjacent switching nodes as well as the interconnected ports among adjacent switching nodes; typically, this is accomplished with self-discovery protocols. Such protocols use signaling messages that learn and share node configuration and traffic information. Using signaling messages, a protocol enables the nodes to establish and maintain an adjacency database that reflects the state of the network about a node. These databases are refreshed whenever a change in the mesh network topology takes place, either because a node has been added/removed, a fault has occurred or because congestion is experienced. Thus, self-discovery is very fast and the bandwidth needed for this task does not represent a significant load in the overall overhead of messages for operations, maintenance, and control [15].

8.8 Node and Network Provisioning

Node and network provisioning refers to the actions that need to be taken so that nodes in the network are configured in order to establish lightpath connectivity, as already captured in Figs. 8.4 and 8.5. Provisioning may be static or dynamic although the demarcation between the two becomes a little fuzzy with semi-static services and services like “bandwidth on demand”. Here, we adopt the following demarcation [16]:

- Static configurability is initiated by the network operator after signing with the client a service level agreement for continuous and semipermanent lightpath connectivity, which at minimum remains so for the life of the agreement (days, weeks, months).
- Dynamic configurability is performed by the network operator after signing with the client a service level agreement for dynamic lightpath connectivity and bandwidth allocation. The instance and the amount of bandwidth are upon the client request and thus *network provisioning* is initiated and terminated by the user on demand. In this case, connectivity remains for the duration of a session. Dynamic configurability is also required for *service restoration* (and network protection), which in this case is initiated by the network itself.

Dynamic network provisioning may be accomplished remotely or locally.

8.9 Wavelength Management Strategies

Wavelength management in DWDM networks is relatively a new concept since it was not an issue in single-wavelength optical networks (such as SONET/SDH) for which path protection, fiber protection, and wavelength protection were all the same.

In dynamically configurable DWDM networks, wavelength conversion due to technological and design limitations may not always be possible, also leading to wavelength contention or blocking. For example, assume K input and K output fibers per switching node and N wavelengths per fiber, that is, $N \times K$ wavelengths to be switched. In general, network engineering rules define the maximum number of switchable wavelengths and the number of wavelengths that pass through expressly or unswitched (the hybrid strategy already outlined). Thus, in a 70–30 case, 30 % of channels pass through express and 70 % are switchable. This means that 30 % of the wavelengths account for statically provisioned lightpaths and corresponding statically provisioned bandwidth capacity. Similarly, 70 % of the wavelengths account for dynamically provisioned lightpaths and corresponding bandwidth. However, this imposes restrictions in wavelength availability that eventually may cause wavelength contention or wavelength blocking if wavelength conversion is not adequate. In this case, the problem reduces to finding the optimum point for which wavelength contention under various wavelength reassignment conditions is minimized. This optimization may be accomplished node-by-node with distributed network management or over the entire network with centralized network management. In either case, the number of switchable channels per node, the switching capacity per node, the number of nodes in the network, the number of converters (if any), and the physical topology of the network are significant parameters.

In the centralized case, a network wavelength management agent keeps records of all input–output relationships based on which it provisions each node with *wavelength assignments* establishing semi-static cross-connectivity over selected routes. This case depends on a centralized database, a hierarchical communications protocol, and an optimization algorithm that finds the best shortest and most bandwidth efficient path with the minimum wavelength conversions. The speed of this strategy however depends on how fast a path can be found, how fast the centralized agent commu-

nicates with all nodes, and how fast each node can be provisioned without interrupting existing service. Clearly, in a heterogeneous network, this case implies that all inter-domain communication interfaces are compatible and that all nodes in each domain are capable of communicating with the same agent. Alternatively, a domain agent may be considered that communicates with all nodes in the domain, and each domain agent with the network agent thus simplifies language incompatibilities.

In the distributed case, connectivity is left to the collective decision of nodes in the network. This is accomplished using a *supervisory channel* (SUPV) that is common to all nodes. The supervisory channel carries messages that convey input–output wavelength associations, QoS service indicators, and maintenance and control messages. The supervisory channel may be inside or outside the spectral range of data channels, and it may or may not be protected. Depending on protection strategy, two supervisory channels may or may not be on the same fiber. Thus, route optimization and wavelength reassignment is left to each node to discover. In a heterogeneous network, this implies that nodes in different domains run comparably efficient algorithms and that the inter-domain interface uses a common language protocol.

In optical communications, supervisory latency consists of two components: one related to propagation speed and another to protocol execution. Current bit rates are high (typically higher than 1 Gbps) and the first component is much smaller than the second. Thus, protocol execution is critical for true *dynamic reconfigurability*. Technologically, reconfigurability is bounded by the efficiency of the communications protocol, the fabric switching speed, the acquisition time of wavelength converters, and other tunable components on the path (filters, lasers, etc.).

References

1. ITU-T Recommendation G.7714/Y.1705, *Generalized Automatic Discovery Techniques*, November 2001.
2. ITU-T Recommendation G.1010, *End-User Multimedia QoS Categories*, November 2001.
3. S.V. Kartalopoulos, “Elastic Bandwidth”, *IEEE Circuits and Devices Magazine*, vol. 18, no. 1, January 2002, pp. 8–13.
4. S.V. Kartalopoulos, *Fault Detectability of DWDM Systems*, IEEE Press, 2001.
5. C. Law and K.-Y. Siu, “On-Line Routing and Wavelength Assignment in Single-Hub WDM Rings” *IEEE Journal on Selected Areas in Communications*, October 2000, pp. 2111–2122.
6. X. Zhang and C. Qiao, “Wavelength Assignment for Dynamic Traffic in Multi-fiber WDM Networks”, *International Conference on Computer Communications and Networks (ICCCN)*, Oct. 1998, pp. 479–485.
7. S. Xu, L. Li, and S. Wang, “Dynamic Routing and Assignment of Wavelength Algorithms in Multifiber Wavelength Division Multiplexing Networks”, *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 10, October 2000, pp. 2130–2137.
8. S. Cho and C. Oh, “A New Wavelength Assignment Algorithm in an Optical Unidirectional Ring with Realistic Wavelength Conversion”, *IEICE Transactions on Communication*, vol. E84-B, no. 8, August 2001, pp. 2301–2304.
9. P. Saengudomlert, E.H. Modiano, and R.G. Gallager, “On-Line Routing and Wavelength Assignment for Dynamic Traffic in WDM Ring and Torus Networks”, *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE*, Vol. 3, March 30–April 3, 2003, pp. 1805–1815.
10. A. Narula-Tam, P.J. Lin, and E. Modiano, “Efficient Routing and Wavelength Assignment for Reconfigurable WDM Networks”, *IEEE Journal on Selected Areas in Communication*, vol. 20, no. 1, January 2002, pp. 75–88.
11. O. Gerstel and S. Kutten, “Dynamic Wavelength Allocation in All-Optical Ring Networks”, *Proceedings of the IEEE International Conference on Communications ICC—1997*, vol. 1, June 8–12, 1997, pp. 432–436.
12. Y. Wang and S.V. Kartalopoulos, “Analysis and Implementation of Reconfigurable Optical Ring Network with Minimal Wavelength Blocking”, *Proceedings of the 4th IASTED Multi-Conference, Wireless and Optical Communications*, Banff, Canada, July 8–10, 2004, pp. 808–813.

13. S.V. Kartalopoulos, *Introduction to DWDM Technology: Data in a Rainbow*, Wiley/IEEE Press, 2000, and also in Chinese, PPTPH, RPC, 2001.
14. Y. Wang and S.V. Kartalopoulos, “An Analytic Comparison of Routing and Wavelength Assignment (RWA) Algorithm in WDM Optical Networks”, *Proceedings of the 2005 Oklahoma Symposium on Information Technology and Entrepreneurship (ITE'05)*, Oklahoma City, OK, April 19–20, 2005, pp. 65–71.
15. Y. Wang and S.V. Kartalopoulos, “An Analytic Comparison of Routing And Wavelength Assignment Algorithms”, TBP in *Designing Software-Intensive Systems: Methods and Principles*, Idea Books Publishers.
16. S.V. Kartalopoulos, “Wavelength Management Strategies in Inhomogeneous DWDM Networks”, Invited Paper, *China Communications Magazine*, inaugural issue December 2004, vol. 1, no. 1, 2004, pp. 97–100.

Chapter 9

Network Protection and Fault Management

9.1 Introduction

Network protection provides the assurance that service will be provided whenever severe degradations and/or failures (permanent or intermittent) occur at the component, link, and node level. Such impairments cause congestion or traffic flow disruption. For example, a fiber cut disrupts the traffic flow of many optical channels which at 2.5 or 10 Gbps amount to an aggregate traffic of Tbps. Thus, because of the huge amount of disrupted traffic, fiber cuts should be detected right away and traffic should be diverted over different links and perhaps different paths. Similarly, when a component fails, it may affect a single optical channel (e.g., a laser or a photodetector) or a group of optical channels. In this category, we also include a component that has degraded so that the channel (or group of channels) performance has degraded below the acceptable performance level for some time, as defined by standards. Thus, network protection is the functionality of monitoring the performance and incoming power of single as well as optical multiple channels, and fault management is the functionality within each node and network that monitors, detects, locates faults, and identifies the type of faults or degradation within the node and the network [1]; we term this fault detection, fault type, and fault localization (FDTL).

When FDTL is accomplished, network protection determines how service will be restored according to the protection and restoration strategy of the network.

In general, restoration is on several levels, channel, link, node, and network.

- Channel restoration implies that a single wavelength has been degraded or lost. A channel may be affected by component degradation or failure, by excessive induced noise, or by excessive optical power attenuation or loss. Service restoration is the action to either remove the affecting cause or reassign the channel from one wavelength to another, or even from one link to another.
- Fiber link restoration implies that all wavelengths in a fiber are affected either because a fiber is cut or because a component is severely degraded or failed affecting all optical channels in the fiber. Service restoration is the action to move all channels from one fiber to another.
- Node restoration implies that traffic on all fibers at a node is affected because of node failure (typically, because of power failure). Service restoration is the action to move all traffic through other nodes bypassing the faulty node.
- Network restoration implies that many nodes (typically a cluster of nodes) in a network have failed; this is also termed *group node failure* or a *disaster*. Service restoration is the action to move all traffic through other parts of the network bypassing the faulty group, termed *disaster avoidance*.

A tool for fast FDTL and service restoration is the control messages and the mechanism to transport them across the network. Typically, these messages are transported over a separate channel (for administration, operations, maintenance, and control), which may also be protected. For example,

in the OTN protocol, the optical supervisory channel (OSC) provides information about optical multiplex sections and tributary channels that are within a link or span and between regenerators [2]. In addition, there are overhead bytes in the optical data unit that transport messages downstream and upstream for the FDTL function (in ITU, FDTL is known as FTFL), see Figs. 5.8 and 5.10.

9.2 Fault Detection and Isolation

When a fault is detected, automatically the corresponding visual indicator (typically a red LED is lit and an alarm indicator is sent to the node fault management function, and depending on protocol, type, and importance of the alarm, a message downstream and/or upstream. Such alarm indicators are in the SONET/SDH protocol (such as the defect indicators in the overhead), in the supervisory channel of the OTN, and so on. The next action is to isolate or localize the fault and protect it if possible (i.e., bypass the fault; this is possible if the fault is in a protected amplifier, protected fiber, and so on). Fault localization must be done immediately as soon as the fault is detected and service should be restored fast to minimize the impact on service interruption. However, during this process, the generation of alarm messages needs to be suppressed in order to avoid network flooding and issue a message indicating that the fault is under isolation or restoration. In addition, it may be necessary to query neighboring nodes for node information and to update databases, as well as keep a record for fault auditing and tracking the history of malfunctions. When the fault is repaired and service is restored, notification messages are sent to the fault management function, which also updates the corresponding database.

As an example, consider a failed or a cut fiber in a DWDM network; this is a common fault that occurs during construction, severe weather phenomena, and other disasters. In this case, a cut affects all optical channels in the fiber, and the fault is detected by detecting no incoming optical power at each port of all optical channels in the same fiber. Clearly, many alarm messages are generated and the fiber cut is deduced by performing a series of tests including the optical demultiplexer. The fiber cut fault generates messages that are communicated to the upstream and downstream nodes, and using a link protection algorithm traffic is diverted over one or more different routes, Fig. 9.1. Clearly, in an all-optical network rerouting traffic is subject to the switching capability of nodes in the network, traffic rerouting strategy, and adopted algorithm as it has been discussed in Chap. 8.

9.3 Fault and Service Protection

The data rate per optical fiber link in a DWDM optical network is humongous, several Tbps. In a mesh network topology, because of the many fiber links, the aggregate data rate is huge. As a result, even a single node failure will affect the traffic flow of the network. As a consequence, the

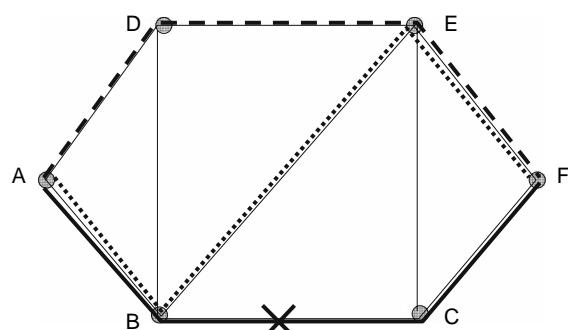


Fig. 9.1 A network link fault (BC) is bypassed by rerouting the fault over a new route (ADEF or ABEF)

next generation intelligent network must be designed in anticipation of situations like that, to be quick to detect faults and restore service, either by bypassing the fault or by rerouting traffic over a different path.

There are several scenarios and protection strategies that a network may adopt. The most popular and well known are three, the 1 + 1, 1:1, and 1:N.

- According to the 1+1 protection strategy, two identical but separate links connect the two end terminals (transceiver ports). The transmitter feeds the same traffic in the two separate fiber links, and the receiving end monitors the two links and it selects the link that performs best, Fig. 9.2. When the selected link is severely degraded or faulty, then the receiving port autonomously switches to the other link. This implies that 1 + 1 protection systems have redundant fabrics, and they have fast monitors to reliably compare the performance of both links. This protection strategy provides service protection quickly; it does not depend on supervisory messages between nodes; it selects the best-performing path autonomously; it is suitable to high-reliability long-haul transmission, but it commits twice the resources.
- According to 1:1, connectivity between two nodes is established over a single link (the servicing or working link), and although a second link (the protection) is committed, the same data does not flow in it, but different data, perhaps of lower priority. In the 1:1 case, the integrity of the signal is monitored and performance messages are sent between the two connected nodes over a supervisory channel. If the performance of the servicing link is degraded below an acceptable threshold level, then the receiving node sends messages to the transmitting node to switch to the protection link. In this case, the low-priority data is either rerouted in whole or partially (according to a best effort algorithm), or it is dropped, Fig. 9.3. This strategy is slower than the 1 + 1, it does not commit the same resources, and is more suitable to medium- and short-haul transmission.
- According to the 1:N protection strategy, similarly with 1:1, N servicing links are protected by one link, and thus if one of the N paths experiences severe degradation or failure, then its traffic is passed over the protection link. Thus, only a single failure out of N possibilities is protected but no more and thus it is the most economical in terms of network resources; the reasoning is that the probability of simultaneous double failures is negligible in medium- and short-haul networks.

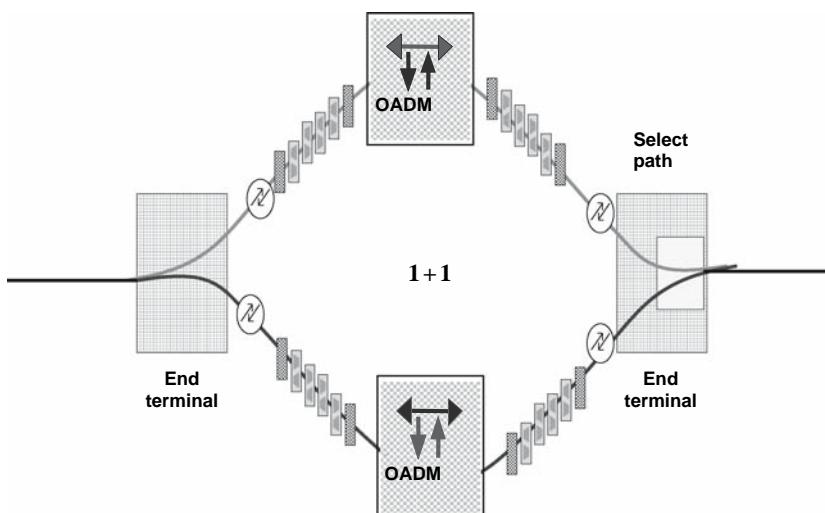


Fig. 9.2 1 + 1 service protection strategy commits twice the resources. It is autonomous and fast and it does not require protocols

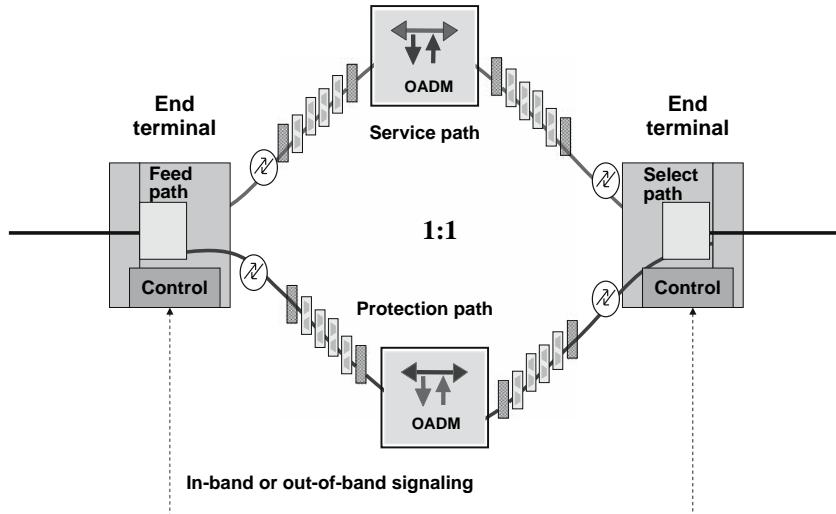


Fig. 9.3 1:1 protection requires fast and reliable supervisory channel for signaling. High-priority traffic is transported over the service path and low priority over the protection path. When the service path fails, high-priority traffic is switched onto the protection path and low priority is dropped

The above scenarios are typical for point to point with or without optical add-drop multiplexers (OADM). With reconfigurable OADMs (ROADM), however, reconfigurability also raises additional issues, such as speed of reconfiguration, acquisition time of tunable filters and switching components, design complexity, and protocols in the ROADM. In general, ROADMs consist of an optical demultiplexer and an optical multiplexer and a reconfigurable or programmable switching array that selects which wavelengths from the grid will be dropped and added, and also tunable filters and perhaps semiconductor optical amplifiers (SOA). The technology of the ROADM is not fixed as different manufacturers offer solutions that fit in specific applications.

In the following, we examine the fit of a protection strategy for point to point, ring, and mesh topology networks.

9.4 Point-to-Point Networks

9.4.1 Medium-Haul and Short-Haul Optical Networks

Medium-haul DWDM systems, also known as *intermediate reach* (IR), are very similar to long-haul (LH) networks. However, because the path length is shorter than 4,000 km (1,000–1,500 km), system requirements and design parameters are relaxed to fit particular business models [3]. However, they require advanced wavelength and bandwidth management. For example, they are engineered for more add-drops than the LH, the data rate per optical channel can be the highest possible since shorter spans need fewer optical amplifiers, compensators (chromatic and polarization). Consequently, depending on data rate, type of service, and quality of service planned for, the network protection strategy may be 1:1 or 1 + 1.

Short-haul systems, also known as *short reach* (SR) and *very short reach* (VSR), have a path distance that is in the order of 500 km (SR) or shorter (VSR) [4]. They have several add-drops on the path, and the total aggregate bandwidth is large. Like MH, they too require wavelength and bandwidth management.

9.5 Mesh Network Protection

The protection strategy of DWDM mesh networks depends largely on optical cross-connecting (OXC) nodes, detection facilities incorporated in the receiving port, protocols and protection strategy with rerouting algorithms supported by nodes, and the DWDM network. Depending on fault type, traffic on a fiber may be partially lost (one or more channels) or totally (fiber cut). As a consequence, each DWDM node in the network and the network protection strategy should support protection on the tributary layer, channel layer, and fiber layer.

- Tributary protection implies that at least one of the client data is corrupted or lost, and that the detection facility is after the electrical de-interleaver as in SONET/SDH; typically, data corruption occurs at the access or edge of the network or during the tributary interleaving process.
- Channel protection implies that detection facilities (signal power, performance parameters BER and SNR) are incorporated in the receiving port. This case also applies to a group of channels. The protection strategy in this case requires that one or more channels of the grid are allocated for protection, according to protection strategy adopted by the node and network (1 + 1, 1:1, 1:N, K:N).
- Link protection is similar to channel protection, but in this case all channels in a fiber are lost; this implies that multiple channel faults are detected and correlated to deduce fiber fault (a preferred method) or that a power detector is placed before the DWDM demultiplexer (this method requires a power splitter, is faster but not conclusive). Link protection in DWDM mesh networks requires protection and routing protocols, the sophistication and complexity of which depends on whether nodes include wavelength converters or not, and also on the flexibility of ROADM.

DWDM mesh networks with optical cross-connecting nodes provide the ability to intelligently and automatically reroute one or many optical channels around a fault in the network. However, this intelligence is gained with intelligently distributed monitors at the receiving port of each node and with fast signaling and efficient protocols that trigger appropriate actions for expedient service restoration. The restoration scheme needs to be fast (50 ms or less) and facilitate efficient bandwidth management, fast provisioning, and good capacity planning assurance for continuous and uninterrupted service.

In DWDM networks, the protecting route may be dynamically found according to a route algorithm as soon as a fault is detected and localized. However, this method, depending on the type of fault, may require a longer period till service is restored, during which period service is interrupted. Alternatively, the protecting route may have been precalculated or partially precalculated and the final protection route is determined by performing minimal calculations based on the current state of certain variables; the latter is more reliable as it takes into account the current congestion state of the network. In either case, the various possible routes between two nodes in the network are calculated based on traffic parameters and classified as best, next best, and so on. In traditional optical networks, the various paths would be easily found based on number of nodes (or hops) and length of links. Clearly, the network efficiency in determining the best protecting route depends on network architecture and complexity, Fig. 9.4, and also whether protection is centralized (centralized fault management) or distributed (nodes collectively calculate the protection route). In centralized fault management, the best protecting route requires longer time but it frees nodes from executing algorithms and handling routing protocols. In distributed fault management, the best protection route is collectively determined, and therefore, it requires complex algorithms, extensive tables, and sophisticated routing algorithms by each node in the network.

In general, mesh networks have superior survivability and restoration efficiency, they protect against link, node, channel, and tributary failures, and they are sufficiently fast (the typical

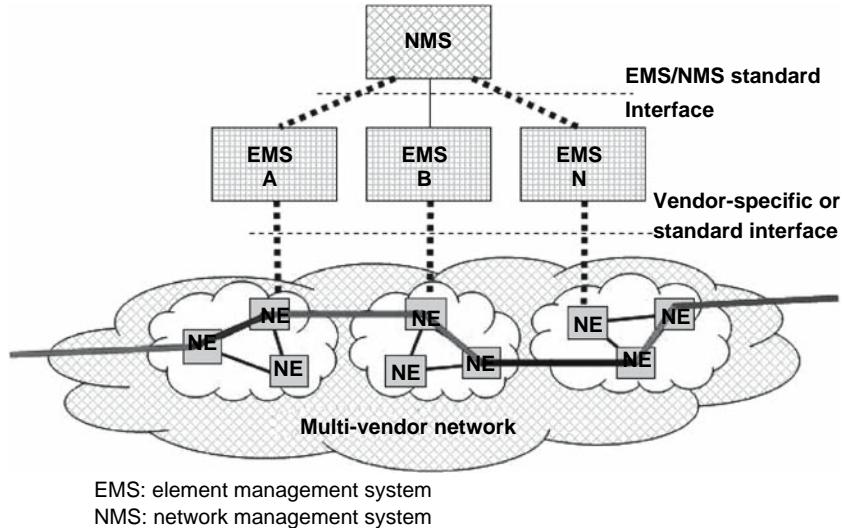


Fig. 9.4 An optical large network with centralized fault management finds the best possible route when a fault is encountered on the network. This method requires longer time but it frees nodes from executing algorithms and handling routing protocols

SONET/SDH restoration time is 50 ms). Conversely, they require overcapacity, but this depends on network applicability and traffic priority and grades of service. Overall, mesh networks are scalable and thus they can add nodes and capability as needed.

9.6 Ring-Network Protection

Ring networks are classified by their size (circumference, number of ROADMs, number of wavelengths per fiber, and data rate per optical channel). They may be small simple single rings (small Metro and LAN), medium two-ring, and large four-ring networks. Each ring classification has its own applicability, complexity, and cost structure.

The single fiber ring may be unidirectional without protection; a fiber cut between two nodes will disable the complete ring. However, it may also be bidirectional path-switching rings (BPSR/1); certain channels flow clockwise and certain others counterclockwise and data flows in both directions simultaneously. Thus, a faulty link between two nodes is bypassed by looping back traffic at each end of the link, Fig. 9.5.

Two fiber bidirectional path-switching ring (BPSR/2) networks have 1 + 1 protection and provide better protection than the BSFR/1. In this case, traffic flows clockwise through one fiber ring and the same traffic through the protection ring. When a link failure occurs, loopback mechanisms isolate the faulty ring.

Four-fiber rings (4F) are bidirectional path-switching rings (BPSR/4) with 1 + 1 protection. BPSR/4 rings consist of two dual counter-rotating fiber rings. One is the working (or service) pair and the other the protection. They also require protected supervisory channels per pair. In certain applications, the protection pair may also be used for low priority traffic. When a fiber is faulty, the fault is bypassed using loopbacks and/or path switching within the ROADM nodes at each end of the fault, Fig. 9.6.

Fig. 9.5 Bidirectional single ring and link protection

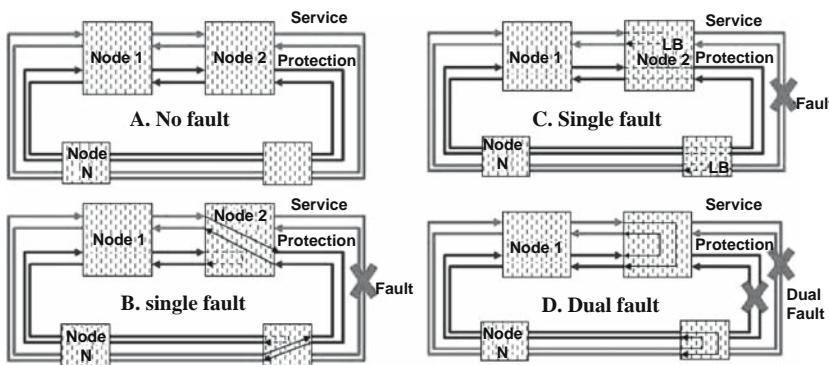
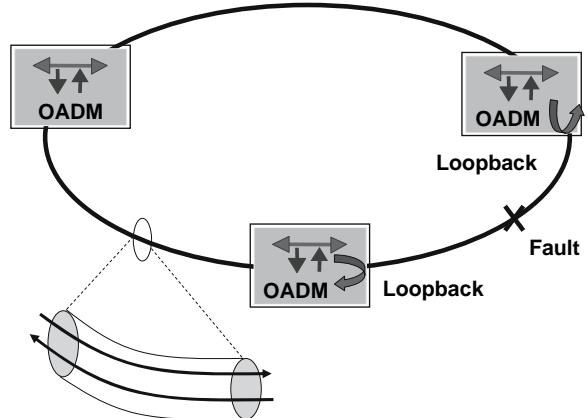


Fig. 9.6 A BPSR/4 large Metro with protection, loopback, and path switching

9.7 Ring-to-Ring Protection

In addition to protecting a failing optical channel or fiber in a ring network, a protection strategy is needed when two peer ring networks are interconnected. Two ring networks may be interconnected with a single link, in which case the link is not protected, or may be interconnected with two links. That is, two or more nodes have been designated as hub or bridge nodes; in this case, the ring-to-ring link appears as 1 + 1 protected, Fig. 9.7.

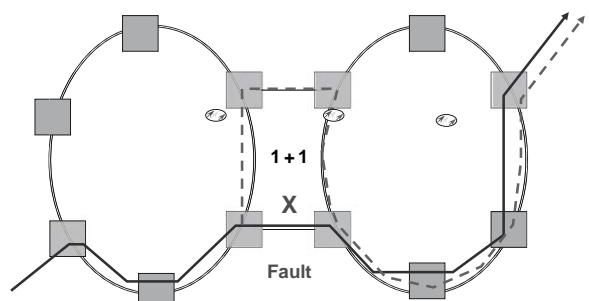


Fig. 9.7 1 + 1 ring-to-ring protection schemes

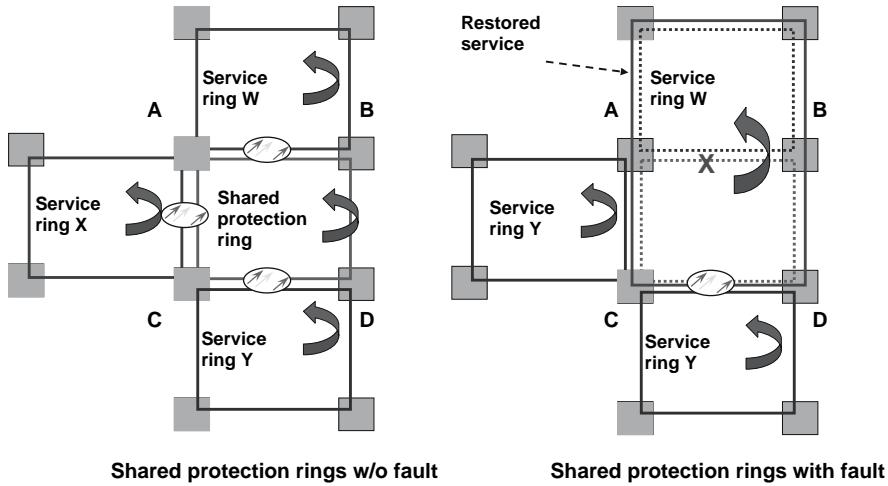


Fig. 9.8 Shared protection rings

9.8 Multi-ring Shared Protection

The multi-ring shared protection topology is a special case that consists of several adjacent rings in pseudo-mesh architecture in which some or all links are shared by neighboring rings, Fig. 9.8. This network utilizes the same fiber resources by more than one ring. For example, ring W shares the fiber link AC with ring X and the fiber link CD with ring Y, but each in different directions of traffic flow. This implies that optical transmission in single fiber links is bidirectional. In such case, when a fault occurs, nodes are provisioned to bypass the faulty link and include the shared protection ring; notice that the direction of traffic flow is maintained.

References

1. S.V. Kartalopoulos, *Fault Detectability of DWDM Systems*, Wiley/IEEE, 2001.
2. ITU-T Rec. G.872, “Architecture of Optical Transport Networks”, November 2001.
3. ITU-T Recommendation G.691, Optical Interfaces for Single Channel STM-64, STM-256 and Other SDH Systems with Optical Amplifiers, October 2000.
4. ITU-T Recommendation G.692, Optical Interfaces for Multichannel Systems with Optical Amplifiers, October 1998.

Chapter 10

Network Security

10.1 An Old Concern

The delivery of private or secret messages has always been an issue of concern regardless of method of transport. Since antiquity and up to the nineteenth century, sending a private or secret message with a messenger without being compromised was risky. Thus, methods were developed to assure that the message would be unintelligible if in enemy hands and also that the recipient of the message would be able to detect the compromised message. Although our intention is not to provide a historical treatise on this subject, it is worth mentioning some examples of interest.

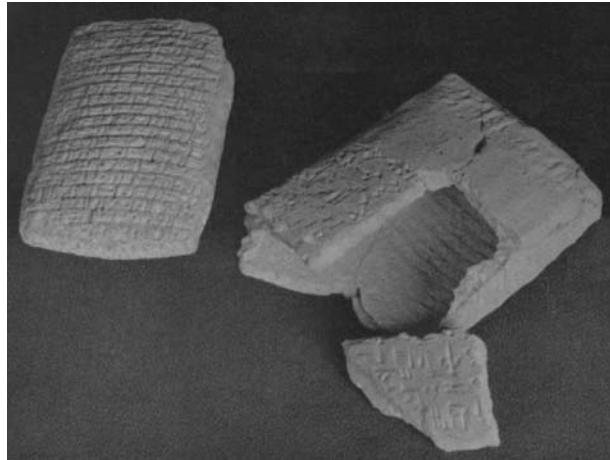
Ancient Mesopotamians would write a private message in cuneiform script on a fresh clay tablet, which was exposed to sun to dry. This tablet was then enclosed in a clay envelope on which the addressee's name was written; replace clay with paper and you have a modern letter, Fig. 10.1. When the envelope was dry it was dispatched with a messenger. If this letter was intercepted, the clay envelope had to be broken, thus revealing that the message was compromised. In other cultures, clay was substituted by papyrus, bark of tree, parchment or pergamenta (baby lamb skin), or by paper on which text was written with a stylus and ink, then it was rolled or folded, and sealed with Spanish wax on which a symbol was impressed using either a signet ring or a stamping implement. Similarly, the ancient Chinese had a method of hiding messages; they hid the letter in a cake (known as *moon cake*), which they passed through the unsuspecting emperor's guards. The Egyptians used their own secret methods as is discerned in hieroglyphs, and so did the ancient Greeks as is discerned in ancient texts. We mention the following three examples which have some similarities with modern encryption methods.

Short messages would be memorized and sent with a trustworthy dispatcher. A notable example is that of the soldier Philippides who ran from Marathon to Athens, a distance of about 40 km, to deliver to Athens the message that the battle at Marathon was won, hence the *Marathon race* that commemorates a key victory in the history of civilization, democracy, and Philippides' accomplishment.

Optical messages were transmitted from tower to tower to reach far destinations quickly, a method now dubbed as the "Agamemnon's Link"; Agamemnon was the Greek campaign general in the Trojan War (ca. twelfth century BCE). According to Aeschylus, with this method, it took few hours for a message from Troy to arrive at Argos, a distance more than 600 km; at that time that seemed remarkable [1].

Additionally, Herodotus writes more occurrences of communicating with light over long distances. However, we do not know if and how their messages were encoded. We know however that about 350 BCE, optical messages were encoded using a method that was developed by the military scientist Aeneas Tacitos of Stymphalos. According to Polybius, *communicating with encrypted light messages became the greatest service in war* [2].

Fig. 10.1 Ancient Assyrian clay letter with envelop



It is believed that the encryption key changed from hour to hour (i.e., a *cryptoperiod* method) using a clepsydra, a water clock made with a leaky jug in which the level of water determined the encryption key to be used. Polybius (203 BCE–120 BCE), a Greek historian, cryptographer, and navigator, wrote about encoding light messages that did not depend on time like Aeneas'. Although this method was initially invented by *Cleoxenos the engineer* and *Demokleitus the inventor*, it was perfected by Polybius, and it is known as the *Polybius square*. The latter is of current interest so we provide a brief description.

Arrange the alphabet letters in a matrix 5×5 ; we use the Latin alphabet and therefore since there are 26 letters, the two least used letters of the alphabet (say Y and Z) can be placed in the same element of the matrix. Each row of the matrix is written in a tablet, and the five tablets are numbered 1–5. Each letter on the tablet is also numbered left to right from 1 to 5.

Letter number on tablet:	<u>1 2 3 4 5</u>
Letters on tablet # 1:	A B C D E
Letters on tablet # 2:	F G H I J
Letters on tablet # 3:	K L M N O
Letters on tablet # 4:	P Q R S T
Letters on tablet # 5:	U V W X Y/Z

Both the transmitting and the receiving sites have five lit torches. When the transmitting site wants to send a message, they raise two torches, and the receiving site in response raises two torches as well, which are subsequently lowered; this establishes the *request to send* and the *acknowledgment* steps of the communications protocol. Now, to transmit the message VICTORY, the message is written on a tablet and each letter is encoded by writing the tablet number where the letter is, followed by the letter number on the tablet, or 52, 24, 13, 45, 35, 41, and 55. Now, to send the first letter, five torches are raised and lowered followed by two torches; to make up the number 52 (for letter V). Then, two torches are raised and lowered, followed by four torches to make up the number 24 (for letter I), and so on. For this process to be error free, Polybius provides training guidelines, optimum distance between torches, dimensions of relay towers, “viewing tubes” and screens, and more. What he has not publicized (and for obvious reasons) however is whether the letters of the alphabet were arranged on the tablets in the order in our example or whether they were arranged in a random order, in which case all stations on the transmitting path should have copies of the same tablets. In fact, the tablets could change periodically to assure secrecy of the code.

Wrapping a ribbon helicoidally around a baton or staff of specific diameter that the Spartans called “skytale” and then writing a message alongside would produce an unintelligible message on the unraveled ribbon, Fig. 10.2. The message could be read only if the recipient had a baton of the

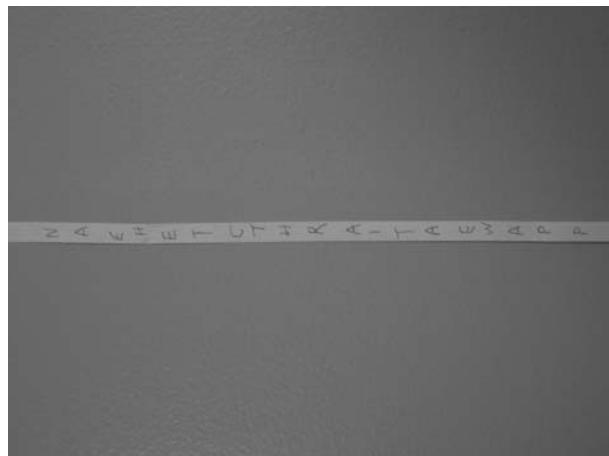


Fig. 10.2 A skytale and a ribbon made up a reasonable cryptographic tool for the Spartans (a). A marker and a paper ribbon demonstrate the principle. (message reads, “SPARTANS (make) PEACE WITH ATHENS” (b). The ciphered text reads NAEHETCTHRAITAEWAPP (c)

same diameter with the original one and if the ribbon would be wrapped around the baton in the same helicoidal sense and direction. This method was frequently used by the Spartans who would send secret messages to their ambassadors when they were negotiating with rival city-states such as Athens and Thebes (this method has been recently captured in a Hollywood movie).

The Athenian Demeratus [3] used a different method to transport a written message through enemy ranks; this method gave birth to the modern terms “cryptography” (from *crypto* and *graphe* meaning “hidden message”) and “steganography” (from *steganos* and *graphe* meaning “sealed message”). Scraping the wax off a writing tablet, then writing directly on the wooden substrate a message with a carbon stick (a pencil), and then spreading the wax over it, on which an unclassified message was written, Fig. 10.3, literally hid the confidential message. According to Herodotus, Demaratus’s method worked.

During the Roman era, Julius Caesar (100 BCE–44 BCE) proposed an encryption method, hence known as *Caesar’s Cipher*. This method replaces a letter in a message by another letter of the alphabet at a fixed distance from the letter to be replaced; that is, it shifts the letter in the message to another letter of the alphabet in a linear manner. For example, if a letter in a message is replaced by the next letter in the alphabet then the word *HELLO* becomes *IFMMP*, and if by the one after the next letter in the alphabet then it becomes *JGNNQ*, and so on. Notice however that with this algorithm, occurrences of the same letter (such as L in Hello), although encoded to another letter, are still the same character (M or N); that is, the frequency of occurrence of letters and their statistics in the text remain the same, thus making the cryptographic algorithm very vulnerable and breakable.

A more general encryption algorithm replaces each letter of a text by another letter of the alphabet according to a specified random shifting algorithm. Because of the randomness, the same letter in the text is not shifted to the same letter in the alphabet. This cryptographic method is currently known as *Shift Cipher* and it uses randomized arithmetic based on modulo m operations.



Fig. 10.3 Ancient Greek tablets were hinged at one side and the wax spread on the surface was suitable for keeping notes with a stylus. The size and style of such tablets were similar to modern laptops

In recent times and until World War II, the German intelligence used an encryption method known as the *enigma*. This method was based on a modified typewriter, the *enigma typewriter*, which encrypted messages as they were typewritten. The enigma typewriter consisted of three rotating alphabets that rotated separately after an alphabet key was depressed, thus yielding a combination of $26 \times 26 \times 26 = 17,576$ alphabets [4, 5]. The United States National Cryptologic Museum, affiliated with the National Security Agency (NSA), is adjacent to NSA Headquarters, Fort George G. Meade, Maryland, has a collection of thousands of artifacts related to cryptology, including a World War II German Enigma machine.

As the operator typed each letter of the message on the keyboard, the enigma typewriter would scramble it to another, thus producing an unintelligible message. Conversely, typing the scrambled message on the enigma typewriter recovered the original message. The exact relationship of the three alphabets as they rotated established the “cryptographic key”. Clearly, this method required two exact replicas of the enigma typewriters to cipher a message and to decipher it.

With the advent of radio transmission and particularly during World War II, message encoding gained particular importance because electromagnetic waves would reach both friendly and foe antennas. As a result, cryptography entered the realm of science (modulation methods) and mathematics (statistics, probability, and number theory), and several encryption algorithms were developed to provide authentication, no repudiation, data integrity, and confidentiality. These algorithms required two fundamental elements: a unique *cipher key* that ciphers and deciphers a message that no one can break and a unique *key distribution method* that no one can successfully intercept. However, key unbreakability and key distribution are two concepts that are difficult to test. Thus, in parallel to developing unbreakable cipher keys and safe key distribution methods, another effort of equal importance is on the way: intercept the transport layer to copy the key or to interrupt the key distribution process. In fact, many encryption algorithm methods have been internationally challenged to test the unbreakability of the cryptographic process and the tolerance of the key distribution method; this is known as cryptanalysis.

In the following sections, we examine some fundamental encryption algorithms and key distribution methods.

10.2 Network Security Issues

Since the advent of modern communications with electrical means and prior to the Internet explosion, accessing the loop side of circuit-switched communications network required moderate networking know-how to tap a 2-wire pair and eavesdrop a conversation, and more know-how to mimic signaling codes, with the so-called blue box, in order to establish end-to-end connectivity without being billed. The second intervention was easily identified, and enhancements in the network signaling protocol and the signaling method eliminated the “blue box”. Similarly, at the core network, demultiplexing end-user time slots required bulky and specialized equipment so that the network was not challenged with eavesdropping and virus attacks and the like by outside bad actors. Virus and other malicious soft attacks appeared with the spread of the software-based Internet nodes and network and “cyber-security” was born in an attempt to deter the humongous attempts on the network and end terminals, PCs, and the like; in fact, “cyber-security” and “software virus” are terms that go in hand with Internet and computer communication networks [6].

The key differences between the synchronous public-switched digital network (PSDN) and the Internet are that the latter transports packets in an asynchronous manner in contrast to the former that transports byte-size information in a continuous and synchronized manner (such as digitized voice samples every $125\text{ }\mu\text{s}$ or real-time video) with strict real-time requirements. When packets enter a data node or router, they are buffered in a memory buffer or queue until they are switched to

the output buffer. In general, the route of this “connectionless” network is not under network control and it is determined with one of several methods, depending on network protocol and quality of data service. It is the node buffering of routers that allow smart but malicious programs to creep into their computer-based execution ability and initiate one of many undesirable actions such as spoofing, cloning, file deletion, file copying, and data harvesting. In contrast, the public-switched digital network (PSDN) is based on standardized synchronized frames such as DS1 and SONET/SDH [7], which are not buffered since the path through a switching or cross-connecting node has been established during the call initiation procedure or during node provisioning. Moreover, node provisioning and software upgrades of PSDN nodes are accomplished over an overlay signaling network using a proprietary Intranet or proprietary and secure memory hard disks that only authorized and trained technical personnel can handle. In summary, end-user data in routers can be remotely accessible with specialized know-how, whereas end-user data is transparent to circuit-switched networks.

Besides the PSDN and the data packet network (such as the Internet), the cellular wireless telephony had also been vulnerable to eavesdropping and to calling number mimicking. In fact, accessing calling numbers and pin codes from the airwaves has been relatively an easy task. Therefore, in order to reduce this risk, enhanced user authentication and secure calling number identity procedures have been included in the cellular wireless protocols; although this has substantially reduced the risk it has not eliminated it.

The glassy fiber in optical networks transports Gbps per optical channel or Tbps per fiber allowing true triple play (voice, real-time video, fast data) services. 1 Tbps corresponds to more than 10 million simultaneous conversations, or about half a million simultaneous video channels, or many millions of classified documents and transactions; all this through a glassy fiber that is about 1/10 the thickness of human hair [8]. Although optical technology is more complex than its predecessors, it attracts bad actors because of the huge amount of information that it transports. Bad actors with the proper know-how and sophisticated tools may attack the medium and harvest huge amounts of information, mimic the source, alter information, or disable the proper operation of the network. Thus, in order to eliminate this risk and assure data security and privacy, highly complex, difficult, and sophisticated algorithms are necessary for the generation of the cipher keys and for the key distribution. Moreover, the network itself should be sophisticated and be able to detect malicious attackers and outsmart them by adopting sophisticated countermeasure strategies.

In general, information assurance and security is a concern with many dimensions that aims to ensure a level of trust to the client and by the client that is commensurate with client expectations. Such expectations include information or data protection during its creation, use, transformation, storage, transport, and deletion at the application layer, at the layer boundaries of the reference model (such as the ISO, ATM, TCP/IP), at the transport layer, and in a computation environment. Information security also aims to ensure that access to information and the network is controllable and capable for self-defense and countermeasures; this is accomplished by specific mechanisms that monitor, detect, react, and respond to attacks, vulnerabilities, and deficiencies.

10.3 Definitions

We discuss certain important definitions that are frequently used in security in communications.

Cryptography is a process that transforms data (or *plain text*) into an unintelligible and undetectable form, *the cipher text*. The cipher text is undetectable and unintelligible to all but the rightful recipient who possesses special knowledge and proper authorization to transform the cipher text back to its original form. In this case, unintelligible means that if the cipher text is viewed by a third party, an eavesdropper, the original text cannot be read from it. Similarly, undetectable

means that if an unauthorized party looks for a particular cipher text, the cipher text cannot be singled out from others. Cryptography is viewed as one of the strongest mechanisms to securely transport information in electronic or optical networks and in protocols.

Cryptography performs several important information security services: source and destination *authentication*, *authorization*, data *integrity*, message *confidentiality*, and *non-repudiation*.

- *Authentication* is the process that verifies the identity of the source, that a received message was sent by the rightful sending entity and detects if the message has been altered. [9–11]. The questions asked in authentication are, Is the received information from the source that generated it? Is the destination the intended destination? Authentication is accomplished with cryptographic checksums the *authentication code*, which are calculated according to an approved cryptographic algorithm. The authentication code is also known as *message authentication code*. A message authentication code is a one-way hash function that is computed from a message and a secret key. It is difficult to forge without knowing the secret key.
- *Authorization* is the process that grants access privileges to an entity such as the intended destination or to a third party. Authorization to the destination is granted after verification of the destination. To a third party, access is granted after the official and justified request to access a message and perhaps modify the message. Access is under the control of an *access authority* (or function), which is responsible for monitoring and granting privileges to other authorities that request access.
- *Data integrity* pertains to identifying possible unauthorized alterations in the transported information. The question asked is, Is the data received exactly the same data that was sourced, or some of it or all of it has been altered? In communications, one of the mechanisms that secures data integrity is watermarking, that is invisible text superimposed to the original text that only the rightful recipient knows how to remove. Thus, when part or all of the text is altered by an unauthorized entity, the watermarking has been altered as well.
- *Message confidentiality* is the service that warrants that information during its transport from source to destination will not be disclosed to one or more unauthorized parties. Cryptography with strong encoding is the mechanism that ensures message confidentiality. The network also provides an *accountability* function that monitors and ensures that actions of any entity on the network security can be traced back to it.
- *Non-repudiation* provides proof of the integrity and the origin of a message to a third party. Non-repudiation also prevents an entity from denying involvement or receipt of a message. For example, a signed message provides undeniable proof that the message was received. In communications, this is accomplished using a digital signature that is calculated with a secret key.

In cryptography, the term *key escrow system* or *escrow* means that the two components that comprise a cryptographic key are entrusted to two key component holders called *escrow agents*. The escrow agents provide the components of the key to a *grantee* entity only upon fulfillment of specified conditions. When the grantee entity obtains the key component, it reconstructs the unique key and obtains the session key which is then used to decrypt the cipher text that is sent to it [12].

The cryptographic process includes a secure mechanism for transporting the special knowledge to the rightful recipient. It also includes a process for transforming the cipher text back to its original form. The cryptographic process that changes the form of the original data (the *plain text*) to unintelligible is called *encoding* or *ciphering*. The result of encoding is the *cipher text*. The process of restoring the original form of data is called *decoding* or *deciphering*.

Because the cipher text may contain sensitive or secret information intended to the rightful recipient only, a malevolent or bad actor may want to know the content of the cipher text, gain unauthorized access to the cipher text, and by trying different possible keys may be able to *break* the cipher text. This is known as *brute attack*.

In order to produce a cipher text that only the rightful recipient can read, the sender needs a secret code known as *cipher key*. The method by which the cipher key is exchanged and agreed upon by both sender and receiver is a process known as *key establishment*. When the key has been agreed upon, it may be registered in a *key depository* or *key management archive* by a *key registration authority*. Similarly, a *public key certificate* uniquely identifies an entity, it contains the entity's public key, it uniquely binds the public key with the entity, and it is digitally signed by a trusted *certificate authority*, as part of the X.509 protocol (or ISO Authentication framework).

If the key is suspected to be *compromised*, it may be *revoked*. In this case, the key establishment may restart and the key may be *updated*.

As an example, if the message in binary notation is the string 10001101|00001101|01001101| and the established cipher key is 01010100|11110110|00011011|, where the vertical bar | delineates each byte, then the cipher text is obtained by the bit-by-bit modulo-2 or Exclusive OR (XOR) logic operation between the message and the cipher key, as 11011001|11111011|01010111|. The ciphering and deciphering process is captured in Fig. 10.4.

Text:	10001101 00001101 01001101 ...
Cipher key:	01010100 11110110 00011011 ...
Cipher text:	11011001 11111011 01010111 ...

Mathematically, this is denoted as $C_t = C_k \oplus T_x$, where C_t is the cipher-text, C_k is the cipher key, and T_x is the text.

Based on the XOR property, if $C = A \oplus B$ then $A = B \oplus C$. Thus, using the same cipher key on the cipher text at the receiving end, the original text is recovered.

Cipher text:	11011001 11111011 01010111 ...
Cipher key:	01010100 11110110 00011011 ...
Text:	10001101 00001101 01001101 ...

From the cipher text, the initial plain text is obtained by executing a modulo-2 bit-by-bit with the same cipher key. This is known as *decrypting* or *deciphering*. In this case, it is important that both the sender and the receiver have the exact same key, the first to cipher the message and the second to decipher the cipher text. The reason for performing bit-by-bit XOR and not parallel is simple: in serial communications, a long key would require two complex deserializers, long buffers, many XORs, and a serializer, not counting the delay introduced for buffering.

The method of encoding/decoding with the same key is known as *symmetric cryptography* and the key is known as a *symmetric key*. To generate the symmetric key another symmetric key is needed first, the *seed key*; which is used to encode the final key, hence known as the *key encrypting key*; this process is known as *key wrapping*.

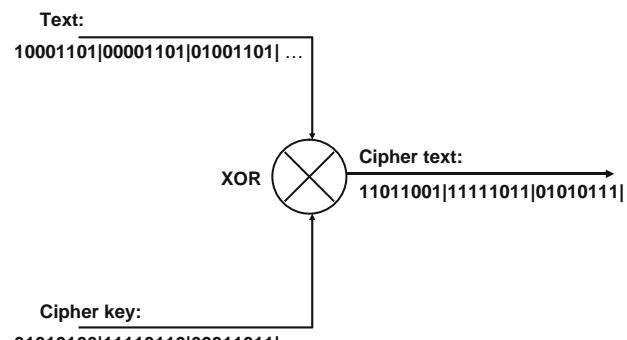


Fig. 10.4 XOR logic function is used to cipher and to decipher text bit by bit

In the example above, the message is represented by a block of bytes and thus the cipher key, which is random and long as the message, is known as *block cipher*. Certain encryption algorithms use a long key to create a cryptographically strong *keystream*. It is this keystream that is exclusive-ORed with the plain text. This is known as *stream cipher* algorithm. Cipher keys may be *permanent*, they may change periodically (in which case a *cipherperiod* is defined), or they may change for each message (known as *one-pad keys* or *ephemeral keys*).

In certain applications where the text is binary serial (as in digital and data communications), the cipher key operates on the serial bit-stream bit or byte at a time using the XOR. Such cryptographic methods are also known as *stream ciphers* denoting the serialization of data. The stream cipher text is decoded serially by applying the same XOR logic operation with the same key. The key in this case is generated by a pseudorandom generator, which in this case is also called a *keystream generator*.

One of the issues with the symmetric cryptography method is the *key distribution*, that is, the transportation or communication of the key from the sender of the cipher text to the rightful recipient. If the cipher key is intercepted by an intruder during its transportation, the value of the cipher text is meaningless in cryptography. However, if the secrecy of key distribution is an issue, symmetric cryptography is very strong since the key can be as random as possible and as long as needed.

If the cryptographic method uses one key for encoding and another for decoding, then the cryptographic method is known as *asymmetric cryptography*. This method is particularly interested because intercepting the encoding key during its transportation does not reveal the decoding key. Therefore, the encoding key may be transported openly or *publicly*. However, because the encoding key is produced after mathematical manipulation knowing the decoding key, the latter needs to be communicated to the sender. Thus, the asymmetric key method has a lot of appeal, and it is the method that has inspired some more complex cryptographic methods applicable to the Internet and other applications. Among them is the *public key cryptography*. Public key cryptography uses a pair of two key ciphers, one which is public and another which is private. Plain text encrypted with the public key can only be decrypted with the associated private key. The public key cryptography is also used in conjunction with one-way hash functions to produce a digital signature. According to this, messages signed with the private key can be verified with the public key [13, 14].

A cryptographic technology aims to embed a secret text A within a non-secret text B, the *carrier* to form a composite text known as *steganogram*. In this case, the steganogram looks like the intelligible and detectable text B, but text A in it is neither detectable nor intelligible but only to the rightful and authorized recipient who holds the *steganographic key*. This form of cryptography is known as *steganography*. Steganography takes advantage of the fact that there is quantization noise after digitizing an analog signal (picture, voice, or text). Thus, if the steganogram (A + B) has the same statistical characteristics of the carrier signal B, then it is very difficult to extract signal A from the steganogram if the *steganographic key* is not known. In traditional telephony and in the μ -law-encoded signal, the least significant bit of certain time slots is superimposed by signaling bits. This is known as *bit robbing*; it does not affect the quality of voice signal as heard by the end-user and it may be considered one form of steganography in telecommunications. As a consequence, a 64 Kbps clear voice channel becomes 56 Kbps. One application of steganography uses a digitized picture, some random bits of which have been used to embed the digitized secret text.

Another form of cryptographic technology, known as watermarking, aims not to make a text unintelligible and undetectable but to embed a visible text A within another text B such that the two are inseparable to any one but to the authorized end users. As an example, the word draft or classified is superimposed on the page of a text. Similarly, the name of the owner is superimposed on a picture and the two cannot be separated unless the *watermarking key* is known.

Several algorithms map a bit string of arbitrary length to a bit string of fixed length according to an approved function known as *hash function*. The result of applying the hash function on the bit string is the *hash value*. Hash functions satisfy the property that it is computationally infeasible

to map any input string length to a prespecified output bit string and also that it is computationally infeasible for two distinct input strings to map onto the same output prespecified string [15].

In contrast to cryptography that aims to cipher a text, *cryptanalysis* aims to decipher cryptograms. Cryptanalysis is a double-edge sword: a bad actor attempts to break the key of a cipher text, and a cryptographer commissions an independent party to break the key of an algorithm in order to test the strength of a cryptographic method.

10.4 Security Levels

Consider a cryptographic module that contains computer encryption subunits, cryptographic public and private keys, plain text and cipher text, memory, and registers. The physical module has data input–output ports, a maintenance port, a door, or a cover. In addition, the proper operation of the module may depend on electromagnetic interferences, environmental fluctuation, and power fluctuation. Thus, bad actors, by Murphy’s law, will explore weaknesses and vulnerabilities of the module and look for an opportunity to gain unauthorized access into the cryptographic mechanism and the keys. Security management provides requirements that safeguard the physical entity of the module.

FIPS 1402 defines four security levels [16–20]. A synopsis of the four levels follows.

Security level 1 (SL-1) provides the lowest level of security specifying basic requirements for a cryptographic module such as a personal computer encryption board so that software and firmware components are executed on an unevaluated general purpose computing environment. No specific physical requirements are provided for a SL-1 module. When performing physical maintenance, all plain text secret and private keys and other *critical security parameters* (CSP) contained in the cryptographic module shall be zeroed; this is performed procedurally by the operator or autonomously by the cryptographic module.

Security level 2 (SL-2) protects against unauthorized physical access by adding the requirement for tamper-evidence coatings (that may be opaque to visible spectrum), seals, and locks on door and covers. Thus, when access to plain text cryptographic keys and CSPs is needed, the tamper-evidence mechanism in the module is violated and the cryptographic module provides the evidence of it. At this level, when an operator needs to gain access to perform a corresponding set of services, the operator requests authorized access and the cryptographic module authenticates the authorization access. To accomplish this, the SL-2 requires at minimum role-based authentication. SL-2 enhances LS-1.

Security level 3 (SL-3) attempts to prevent an intruder from gaining access to CSPs in the cryptographic module. Thus, SL-3 requires physical security mechanisms that exhibit high probability of detecting attempts to physical access as well as reporting mechanisms. When the enclosure is violated, it should cause serious damage to the cryptographic module; a physical protection mechanism to passive locks can be a hard opaque coating such as epoxy. To accomplish this security level, SL-3 requires identity-based authentication mechanisms. SL-3 requires physically separate input–output ports for ciphered text or plain text to be ciphered by the cryptographic module. Circuitry detects an attempt to open the cover or the door of a module or to access the maintenance access interface. Then, the circuitry zeroes the plain text secret and public cryptographic keys and CSPs contained in the cryptographic module. SL-3 enhances LS-2.

Security level 4 (SL-4) provides a complete envelope of physical security around the cryptographic module, and it increases the probability of detecting any attempt of penetrating the cryptographic module and gain access of the cryptographic keys. SL-4 also protects against security compromise as a result of external environmental avert conditions and fluctuations. To accomplish this, the cryptographic module contains either *environmental failure protection* (EFP) or *environmental failure testing* (EFT) mechanisms. Attempting to remove or dissolve the protective coating should result in serious damage of the cryptographic module.

10.5 Security Layers in Communication Networks

Security in communications is not limited to *text security* or *text integrity*. The old practice was limited to assuring messages were delivered to its rightful recipient without been compromised, read, or altered by a third party. However, much of this depended on the integrity of the courier and other factors; let us think of the courier as the channel of a communications network that transports a message.

In modern communication networks, security has more dimensions than ciphering messages only. Messages enter computer-based nodes and are temporarily stored in memory. Nodes are provisioned and maintained on-site or remotely with network control messages. Messages (information) are transmitted electronically, optically, or over radio waves, which with the right technology and know-how may be intercepted. Thus, the opportunities for attack are many and are not limited to old practices any more.

For example, an encrypted message implies that the transported message is secure. This may be correct if we had an encryption algorithm that generates and distributes keys that cannot be broken by any means. To date, several algorithms have claimed this but time has proved the opposite. Intelligent bad actors have broken keys with brute force using supercomputers or other means. So, encrypting a message is only one of the dimensions in communications security, which is the responsibility of end users. We call this *security at the information layer*.

Suppose that a bad actor taps the physical layer of the communications network (at the link or at the node) to eavesdrop and copy messages that flow through them, even if messages are encrypted. If the bad actor can break the cipher key, then there are two possibilities: decipher the encrypted text, or, decipher the encrypted text, alter it, encode it again, and retransmit it to its destination. In this case, monitoring and detecting network malicious interventions require intelligent methods. Thus, *network physical layer security* is another dimension, which is the responsibility of network provider.

Suppose that a bad actor is not interested in eavesdropping messages but in disabling the network from establishing the key and transmitting messages, destroying messages in routers and end terminals, harvesting data from computer-based nodes, altering the security and destination address in packetized messages, or even alter the information field of messages. This can be accomplished on-site or remotely and cause network congestion, reconfigure a node or router, or plant in it an executable program that can be activated under specific conditions (such as a command or a clock), disable the authentication and the key distribution process, and so on. This is another dimension of *security on the MAC/Network layer*. Thus, monitoring and detecting proper network protocol execution is another dimension in security.

In addition to monitoring and detecting malicious acts on the information, MAC/Network, and link layers, the network should include intelligent mechanisms to avoid or outsmart malicious actors and malicious events. Such mechanisms are known as *countermeasures*. For example, when the link is compromised, the intelligent network may reassign traffic to another link. Similarly, if the channel is compromised, the intelligent network may reassign traffic to another channel. Unfortunately, there is no mechanism on the network level to identify that an encryption key is broken because a bad actor who has done so will not advertise it for obvious reasons. In this case, the security of the encryption algorithm relies on the vigilance of the creator and on the scientific effort of benevolent actors who make a serious effort to break it, learn from it, and develop a harder algorithm.

10.5.1 Security on the Information Layer

Assume that one creates a text and needs to transmit it to a destination. If the text is classified, some precautions must be taken to make it unintelligible to a third party. The first level of assurance is to

encrypt the text, provided there is a mechanism in place between the sender and the receiver, so that the latter can decipher it when the ciphered text arrives. In other words, the encrypted text is assumed to be transparent to the transporting mechanism. Ciphering the text at the source and deciphering at the receiving end constitute the information security layer. Thus, this layer is not concerned with the transporting mechanism itself but with the following:

- Which algorithm at the source can encrypt the message and which one can decrypt it at the rightful destination, so that even if it is intercepted by a third party it remains unbreakable?
- How a secure key can be established between the source and the receiver before the encrypted message is transported?

In general, cryptographic keys are classified into symmetric cipher keys and asymmetric cipher keys.

Regardless of cryptographic method in use, the security offered by the cryptographic method depends on the difficulty a third party has to compute the cipher key. Similarly, the efficiency for the cryptographic method depends on the speed the cipher text is converted to plain text and also on the length of the key; the shorter the key the faster the deciphering but also the easier to compute the key by a third party. In this chapter, we examine certain cryptographic methods, some simple (as already described) and some difficult; in fact, the most difficult ones depend on the difficulty to compute algebraic algorithms and also on special properties of quantum particles.

10.5.2 Security on the MAC/Network Layer

The media access control layer (MAC) in communication network nodes and routers is computational-based. In general, this layer is responsible for reliable data delivery, network access, and security (user authentication, authorization). Depending on network and protocol, network control may be centralized or distributed. Thus, the MAC layer partakes in granting access to requests to transmit, partakes in the network path/route selection process, determines the integrity of data frames, discards frames, retransmits frames, or reroutes frames, and more. The point to be made is that this layer is very critical in the proper operation of the network and if not functioning properly, then it may cause topical congestion or even network congestion. As such, the security of this layer is also critical as it may present an opportunity for malicious attacks.

Accessing the MAC layer is accomplished either on-site by directly connecting a terminal to one of its ports or remotely via the Intranet or Internet, typically via a local area network. Security of the node for on-site direct authorized access is assured by the security levels already discussed; this constitutes the first level of defense against attacks. In this case, authorized access is granted by providing security passwords by personnel that have proper clearances. Security of the node for remote authorized access is granted by proper screening (firewalls) and dynamically updated passwords. However, the data network has proved repeatedly to be vulnerable to attacks as a result of the packet *store and forward* or *partially store and forward* process of routers. In this case, malicious executable programs may hide in packets of information and enter the router at the MAC layer. It is needless to enumerate the different attack opportunities a bad actor has on the data network. Virus planting, cloning, spoofing, flooding, Trojan horses, and so on are among the malicious attacks of bad actors who do not even have to be in proximity to the node under attack.

All methods currently are based on the difficulty of accessing the computer-based MAC layer in a node. As packet technology improves, routers expedite the packet throughput processing and disengage the computer from the packet information field, processing only the destination address and some specific fields in the packet header to improve authorization access and increase security

of information. Similarly, control packets are checked for authentication, the effectiveness of which however depends on the robustness of the protocol and its ability to differentiate between valid and invalid control packets.

10.5.3 Security on the Link Layer

The link layer is the communications medium between the sender and the receiver. In communication networks, the medium may be guided or unguided. Among the guided is twisted pair copper (TP), coaxial cable (CB), and single mode fiber (SMF). Among the unguided are electromagnetic waves in atmosphere or in space, or a free space optical laser beam in atmosphere. The link length may be from hundreds of meters long to many kilometers. In this case, it is possible that the link includes between sender and receiver communication modules such as repeaters, add-drop multiplexers, switches, or routers. As a result of the security levels already discussed even if we can trust the physical integrity of the modules on the link, the medium cannot be trusted since it cannot be guarded over its full length, thus offering an opportunity to attack. In fact, the twisted copper pair is easily tampered, although the amount of information it carries is moderate. Coaxial cable is a little more difficult to tamper, but it is more attractive because it carries more information than TP. The fiber medium is the most difficult to tamper, although not impossible to a bad actor with the proper equipment, and it is very attractive because of its very long length and the unprecedented amount of information it carries. In the case of unguided medium, the electromagnetic waves in the atmosphere reach both friendly and foe antennas and therefore this medium is the most vulnerable to attack, both eavesdropping and source mimicking. The free space optical beam is relatively secure because the beam is very narrow, it is invisible to the human eye, and it requires line of sight to operate.

The transmission medium, besides transporting information (ciphertext), also transports the cipher key during the key distribution process. Thus, if a bad actor is able to capture or compute the key in reasonable time, then the ciphertext is not secure. Therefore, in cryptography and security assurance, the key distribution method and algorithm is as critical as the development of the cipher algorithm. In fact, modern key distribution methods are as complex as cipher methods, and they may engage more than one media to transport the public and the private keys and some employ principles from quantum mechanics, hence quantum cryptography and quantum key distribution.

All methods currently are based on the difficulty of computing the key in reasonable time. However, advances change this and history has proved repeatedly that what is difficult today is trivial tomorrow. Therefore, the communications link should be able to continuously monitor its integrity, detect interventions, authenticate the channel and link identification or signature, and include countermeasure strategies. In the following we describe some security methods on the information layer and the link layer. Security on the MAC layer is standards dependent (as described in other chapters of this book), and therefore, it suffices to say that enhancing security on this layer is a current topic of research.

10.6 Mathematical Foundations for Security Coding

10.6.1 Prime Number

Prime numbers have fascinated ancient and modern mathematicians because of their elegance and because of their difficulty to find and manipulate. Their difficulty is of main importance in cryptography where they have found a widespread applicability; there are still many unsolved problems with prime numbers [21].

The philosopher-students of Pythagoras's school (500 BCE–300 BCE) were interested in the harmonic relationship among numbers, and they understood *perfect* numbers, *amicable* numbers, and the idea of primality. Similarly, in around 300 BCE, a *perfect number* is one whose proper divisors sum to the number itself. The proper divisors 1, 2, and 3 of number 6 sum up to 6. Similarly, the proper divisors 1, 2, 4, 7, and 14 of number 28 sum up to 28. A *pair of amicable numbers* is a pair of numbers such that the proper divisors of one number sum to the other and vice versa.

A prime number p is a positive integer that is exactly divisible by 1 and by itself only [22]. By this definition, the numbers 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, and so on are prime numbers; the numbers 1, 2 can be excluded since 1 is the very first integer of all positive numbers and 2 is the only even prime. It turns out that all prime numbers, with the exception of 2, are integer odd numbers; an even number cannot be prime since it would be divisible by at minimum 1, 2, and itself. Thus, 5 is a prime and 4 is not.

Euclid had provided a proof of the *Fundamental Theorem of Arithmetic*, postulating that every integer can be written as a product of primes in an essentially unique way (Euclid, Book IX, *Elements*), and also that if the number $2^n - 1$ is prime, then the number $2^{n-1}(2^n - 1)$ is a perfect number. In addition, his second theorem postulates that there is an infinite number of primes; this has triggered a quest among many notable mathematicians (Euler, Fermat, Legendre, Gauss, to mention a few) to advance prime number theory and find the largest prime number ever; by the year 2005, the largest prime number had 7,816,230 digits. The fundamental theorem of arithmetic states that any positive integer can be represented in exactly one way as a product of primes.

The number of prime numbers $p(x)$ in the range $(2, x)$ is approximated to be $p(x) \sim x/\ln x$. For example, the number of prime numbers in the range 2–40 is $40/\ln 40 = 40/3.6 = 10.8$ or ~ 11 . In addition, the n th random number p_n is within the numbers $n/\ln n < p_n < n[\ln(n) + \ln \ln(n)]$, for $n > 5$.

A very difficult problem with prime numbers is to determine the prime factors of a given integer known as *factoring prime numbers*. Officially, there is no known general purpose prime factorization algorithm to efficiently accomplish this. Several algorithms have been devised but all differ in complexity. The simplest known prime factorization method for a given integer is the *direct search factorization*, which tests systematically by trial division if all possible factors divide the given integer; such method is also known as *brute force*. Clearly, it is very easy to multiply two large prime numbers producing a huge number that can act as the cipher key, but to calculate the original prime numbers the product was derived from it would take an unrealistic amount of time; you see, the primes need to be calculated in order to decode the cipher text. As a consequence, even if an eavesdropper intercepts the product of primes, it will be very difficult for him/her to calculate from it the original primes. However, if a smart method is devised that efficiently and quickly factors large prime numbers, then the cryptographic value of methods based on primes comes to an end. Bill Gates in his book *The Road Ahead* pointed out (in paraphrase) that the development of an easy way to *factor large prime numbers* that defeats the cryptographic system could be a disaster [23].

Another category is the *twin primes*. Two prime numbers are called *twins* if their distance is 2, that is, $p_1 = p$ and $p_2 = p + 2$. For example, the primes 3 and 5 are twins, and so are the prime numbers pairs (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), and so on [24].

10.6.2 Modulus Arithmetic

Modulus arithmetic uses a notation such as $R = \alpha(\text{mod } \beta)$ or simply $R = \alpha \bmod \beta$, denoting that when α is divided by β the remainder is R ; the divisor β in this case is called the *modulus*. Using this notation, the previous example would be written as $1 = 13(\text{mod } 3)$; that is, 13 divided by 3 leaves a remainder of 1.

Modulus arithmetic has certain interesting properties with excellent applicability to cryptography and to Shift Cipher method.

For example

$R = 0$ when α is exact multiple of β .

Two numbers A and B are equal if after division by m they yield the same remainder; that is, $A = B$ if $A(\text{mod } m) = B(\text{mod } m)$; this notation is often simplified to $A = B(\text{mod } m)$.

The latter property is important as large numbers can be reduced using arithmetic modulo m operations. For example, consider the number $11 \times 17 = 187$. Then, assuming mod 12 operation, there is $187 = 15 \times 12 + 7$, $7 = 187(\text{mod } 12)$, or $11 \times 17 = 7$ in modulus 12.

In addition, the following exponential properties are of interest in cryptography:

$$(g \text{mod} a)^x = (g^x) \text{mod} a$$

$$(g^x \text{mod} a)^y \text{mod} a = g^{xy} \text{mod} a$$

$$g^{xy} \text{mod} a = g^{yx} \text{mod} a$$

10.6.3 Greatest Common Divisor

In many cryptographic algorithms it is necessary to compute the greatest common divisor (gcd) of two positive numbers. The precise computation of the gcd is a tedious task, complex, time consuming, and expensive. As a consequence, several algorithms have been devised to compute the gcd with fewer computational steps and an accuracy that is commensurate with the particular algorithm. Thus, there is the classical Euclidean algorithm, the nonclassical binary algorithm, the Lehmer gcd algorithm, and the binary extended Euclidean algorithm. We describe the classical Euclidean gcd algorithm and the binary gcd algorithm.

The Euclidean algorithm for computing the gcd of two integer numbers a and b with $a > b$, is as follows:

1. While $b > 0$, calculate $a \text{mod} b$, move b to a , move the calculated value $a \text{mod} b$ to b .
2. Return a .

A numerical execution of the Euclidean algorithm for $a = 2,136$ and $b = 936$ yields a $\text{gcd} = 24$ as follows:

a	$Q \times b$	$R = a \text{mod} b$
1. 2,136	= $2 \times 936 +$	264
2. 936	= $3 \times 264 +$	144
3. 264	= $1 \times 144 +$	120
4. 144	= $1 \times 120 +$	24
5. 120	= $5 \times 24 +$	0
6. 24	-	-

where a becomes the dividend, b the divisor, Q is the quotient, and R is the remainder ($a \text{mod} b$).

The *binary gcd algorithm* entails repeated divide by two operations. Binary division is accomplished by shifting the binary number in a shift register (which is a very fast and inexpensive process), and it is described with the following algorithmic example.

For two positive numbers a and b , $a > b$, and three registers, a , b , and g :

1. Preset the two shift registers with the values a and b , and initialize the divisor register g to 1.
2. For as long as $a > 0$ and $b > 0$, do the following:

- 2.1 For as long as both a and b are even,
 keep dividing a and b by 2,
 and keep the latest divisor value in register g ; that is, if there are n iterations the value in g is $g = 2^n$.
- 2.2 For as long as a is even but not b , keep dividing a by 2,
 else for as long as b is even keep dividing b by 2.
- 2.3 If both a and b are odd, then put the value $|a - b|/2$ in a temporary register t .
- 2.4 If $a \geq b$, then move the contents of t into a ,
 else move t into b .
- 2.5 Return the product $g \times t$ to step 2.
3. If $a = 0$ or $b = 0$, the $\gcd = g \times t$.

A numerical problem using the aforementioned binary algorithm for $a = 2,136$ and $b = 936$ yields $\gcd = 24$ as follows (notice that a and b remain odd after the third division):

$i:$	1	2	3	4	5	6	7	8	9	10
$a:$	2136	1068	534	267	75	75	27	3	3	3
$b:$	936	117	117	117	117	21	21	21	9	3
$g:$	1	$2^1 = 2$	$2^2 = 4$	$2^3 = 8$	8	8	8	8	8	8
$g \times t:$	—	—	—	—	—	—	—	—	—	$3 \times 8 = 24$

That is, the \gcd value is calculated to 24.

10.6.4 Groups

A group $G(*)$ consists of a set of elements (or numbers) with a custom-defined binary operation $(*)$ on G that satisfies the three abstract axioms:

- The associative operation $a * (b * c) = (a * b) * c$ for all (a, b, c) in G holds.
- The group G has an identity element I such that $a * I = I * a = a$ for all elements a in G .
- There is an inverse of a in G , a^{-1} , such that $a * a^{-1} = a^{-1} * a = I$.

Furthermore,

- The group G is abelian (or commutative) if $a * b = b * a$.
- The group G is finite if $|G|$ is finite.
- Order of group is the number of elements in the finite group G .

Example 1: Consider the finite group of integers Z_n with elements from 0 to $n - 1$, and basic operation the traditional addition $+$ instead of $(*)$. Then,

The associative operation $1 + (2 + 3) = (1 + 2) + 3$ holds;

The identity element is 0, since $0 + a = a + 0$;

The inverse of any integer a in the group Z_n is defined as $-a$, such that $a + (-a) = (-a) + a = 0$.

Example 2: Consider the set of integers M with traditional multiplication \times as the abstract operation $(*)$. Then,

The associative operation $1 \times (2 \times 3) = (1 \times 2) \times 3$ holds;

The identity element is 1, since $1 \times a = a \times 1$;

The inverse of any integer a in the group M is defined as a^{-1} , such that $a \times a^{-1} = a^{-1} \times a = 1$.

The custom-defined arithmetic rules make them difficult to solve and therefore groups are suitable in cryptography. Two groups are used in cryptography: group Z_n defines the *additive group of integers modulo a number n*, and group Z_p defines the *multiplicative group of integers modulo a prime number p*.

- Group Z_n (with n elements) defines as basic operation the traditional addition $+$ which ends by reducing the result modulo n . Doing so, the (addition result)mod n always yields numbers in the range 0 to $n - 1$. In addition, each element a in an additive group has an additive inverse element $-a$ such that $a + (-a) = 0$.

Example: Consider the group Z_{19} . Then

$$(13+17)\text{mod}19 = 30\text{mod}19 = 11, \text{ and in simplified } Z_{19} \text{ reduced notation } 30 = 11.$$

$$(5+14)\text{mod}19 = 19\text{mod}19 = 0, \text{ and in simplified } Z_{19} \text{ reduced notation } 15 = 0.$$

Finally, the additive inverse of 5 is -5 , in which case $-5 = 14\text{mod}19$ since $(5+14)\text{mod}19=0$ or $[5 + (-5) + 14]\text{mod}19=14\text{mod}19 = -5$.

- Group Z_p (with integers from 1 to $p - 1$, where p is a prime) defines as basic operation the traditional multiplication \times which ends by reducing the result modulo n , thus assuring closure. The (product)mod n always yields numbers in the range 1 to $p - 1$. In addition, each element a in a multiplicative group has an additive inverse element b^{-1} such that in $Z_p a \times (b^{-1}) = 1$ or in full notation as $a \times (b^{-1})\text{mod}n = 1$.

Example: Consider the group Z_{19} . Then

$$(5 \times 17)\text{mod}19 = 85\text{mod}19 = 9, \text{ or in reduced } Z_{19} \text{ notation } 85 = 9$$

$$\text{Similarly, } (15 \times 18)\text{mod}19 = 270\text{mod}19 = 4, \text{ or in } Z_{19} 270 = 4$$

The multiplicative inverse of 17 is 9^{-1} , in which case $9^{-1} = 17\text{mod}19$ since $(9 \times 17)\text{mod}19 = 153\text{mod}19 = 1$.

10.6.5 Rings

A ring $(R, +, \times)$ consists of a set of elements R with two binary operations, $+$ for addition and \times for multiplication on R that satisfy the axioms:

- $(R, +)$ is an abelian group.
- The operation \times is associative: $a \times (b \times c) = (a \times b) \times c$ for all (a, b, c) in R .
- There is a nonzero identity so that $1 \times a = a \times 1 = a$ for all a in R .
- The operation \times is distributive over the operation $+$, such that $a \times (b + c) = (a \times b) + (a \times c)$ for all (a, b, c) in R .
- The ring is commutative if $a \times b = b \times a$.

Example 1: The set of integers with the traditional addition and multiplication comply with the above axioms and is a commutative ring.

Example 2: The set of integers with the addition and multiplication modulo n is a commutative ring.

An element b is an *invertible element* of a if $a \times b = 1$, where both a and b are elements of the ring R .

10.6.6 Fields

A field F is a commutative ring in which all nonzero elements have multiplicative inverses.

The characteristic of a field is 0 if $1 + 1 + 1 \cdots + 1$ (m times) $\neq 0$, for $m \geq 1$.

Example: The rational numbers Q , the real numbers R , and the complex numbers C comply with the aforementioned definitions and thus they form fields. Conversely, the ring of integers in example 1 above does not form a field since the only nonzero elements with multiplicative inverses are 1 and -1 .

A field is finite if it contains a finite number of elements. The *order* of F is the number of elements in F .

If the finite field F contains p^m elements for some prime p and integer $m \geq 1$, then for every prime power order p^m , there is a unique finite field of order p^m . This field is denoted F_{pm} , or $GF(p^m)$; we will meet this notation in elliptic curve cryptography.

The finite field F_p where p is a prime number consists of the numbers from 0 to $p - 1$ and the basic operations are defined to be the additive and multiplicative and all calculations end with the reduction modulo p ; operations such as division, subtraction, and exponentiation are derived in terms of addition and multiplication. In this case, all nonzero elements have a multiplicative inverse.

Example in F_{23} :

$$(10 \times 4 - 12) \bmod 23 = 28 \bmod 23 = 5$$

$7 \times 10 \bmod 23 = 70 \bmod 23 = 1$, thus 7 and 10 are inverse of each other:

$$7^{-1} \bmod 23 = 10 \text{ and } 10^{-1} \bmod 23 = 7$$

$$(9^3 / 10) \bmod 23 = (729 / 10) \bmod 23 = (16 / 10) \bmod 23 = (16 \times 7) \bmod 23 = 272 \bmod 23 = 20.$$

10.7 Ciphers

10.7.1 Symmetric Ciphers

The method of symmetric ciphers implies that the created cipher key is the same at both ends of the path and that both the sender and the receiver use the same key. In this case, we will see that many algorithms that create the cipher key are based on prime numbers and common divisors. Therefore, before we describe any algorithm, we outline the prime numbers (pn) and the calculation of the greatest common divisor (gcd).

10.7.2 Shift Cipher

The Shift Cipher cryptographic method uses modular arithmetic. To explain this, consider two rational numbers α and β . In a general form, the division of the two numbers is written as

$$\alpha = \beta \times Q + R, \quad (10.1)$$

where \times denotes *multiplication*, α is the dividend, β the divisor, Q is the quotient, and R the remainder. Thus, the number $13/3$ yields $Q = 4$ and $R = 1$.

In Shift Cryptography, assume that we have the 26 letters of the English alphabet, A–Z and that we associate a number to each letter, from A=>1 to Z=>26, as

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	U	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Assume that we want to shift each letter by 9 letters (thus the *shift key* is 9), and from the result we want the modulus 26 (since there are 26 letters in the alphabet). Then, using the numerical association of the initial message (The mountain is tall), using shifting by 9 and perform modulus 26 arithmetic, the ciphered text is obtained as

T H E M O U N T A I N I S T A L L	(spaces are for legibility)
20 8 5 13 15 21 14 20 1 9 14 9 19 20 1 12 12	corresponding numbers
3 17 14 21 24 4 23 3 10 18 23 18 2 3 10 21 21	key shifted and modulus 26
C Q N U X D W C J R W R B C J U U	ciphered text

To decipher the ciphered text, one has to convert it to the corresponding numbers in the alphabet, subtract 9 (mod26) and then convert the sequence of numbers to a sequence of letters in the alphabet.

Executing this operation may yield negative or positive numbers. For example, subtracting 9 from 3 yields -6 . However, adding -6 to modulus 26 yields 20, which is the correct answer. Similarly, subtracting 9 from 23 yields 14, which is the correct answer. That is, the correct number in this case is always within 1 and 26. Notice that this cryptographic method still has a problem: the same letters in the text are encoded to same letters in the cipher text.

Although, this method may seem complex, if the text is long the substitution sequence using a very fast computer may be quickly found.

10.7.3 The Substitution or Random Shift Cipher

This cryptographic method replaces each alphabetic character in a text by a unique character association of the alphabet and in a random manner. Thus, A may be replaced by B, B by W, C by K, D by Z, and so on. Although the number of different substitutions is very large, there are ways to find out the substitution sequence using a very fast computer.

10.7.4 The Permutation Cipher

This cryptographic method does not replace each character of the alphabet in a text by another. It simply rearranges the letters of the same text in a specific random-like order. Thus, the message

THE MOUNTAIN IS TALL may be rearranged to

EOI TMUAHNTN LI SLTA.

Clearly, the longer the text the more complex the permutation is and also the longer the key. However, even for moderate text lengths a very fast computer can easily decode such cipher text.

10.7.5 The Data Encryption Standard (DES)

In contrast to single alphabetic manipulations that can be decoded relatively easily, one may envision methods that use a mix of permutations, rearrangements, and ciphering. In addition, a message may be encrypted in blocks of characters or bits and not single character at a time. When an encryption method uses blocks of characters or on blocks of bits, it is classified as *block cipher*. The first block cipher using complex and convoluted methods with 128-bit keys was developed by IBM in 1970 and it was code named *Lucifer*. This was adopted in 1977 by the National Institute of Standards and Technology (NIST, previously known as National Bureau of Standards) and it was renamed *Data*

Encryption Standard (DES) but with a reduced key length of 56 bits. DES divides a binary message into 64-bit blocks. The DES has been a widely used symmetric encryption algorithm. In one mode, it uses a block cipher with a 56-bit key and an 8-byte block size (64 bits); the low bit of each key byte is set to odd parity in that key byte. DES in a different mode uses three independent keys and three encryptions are used for each block of data. The latter uses 168 bits of key and provides the equivalent of 112 bits of security [25].

The full description of the complex DES algorithm is beyond the purpose of this book; however, in this section, we make an attempt to trivialize its operation. DES uses a 56-bit key to transpose the 64 bits in the block; the actual key has eight additional bits for key error detection and correction (EDC). The transposed block is then permuted using another 56-bit key which is derived from the initial key. The result of this step undergoes 16 more encryption steps, each using 56-bit keys that are derived from the initial key. The result of this undergoes a swap operation and then a final transposition.

Each of the 16 encryption steps consists of a very complex process that starts with partitioning the 64-bit blocks into two halves, each of 32 bits. The first half, A₃₂, remains as is, whereas the second half, B₃₂, is expanded to 48 bits by transposing some bits and duplicating others. The expanded second half is XOR ciphered with a 56-bit key. The ciphered 48 bits are then subdivided into eight 6-bit groups. Each 6-bit group by substitution produces a 4-bit result and all eight reduced groups form a 32-bit string. Bits in the string are transposed and the result C₃₂ is XORed with the first 32-bit half, A₃₂, from the initial partitioning. Now, the result of this and B₃₂ is combined to form a 64-bit encrypted block.

As complex, convoluted, and confused this cryptographic method is, it eventually failed the cryptanalytic test. In 1998, the Electronic Frontier Foundation built a computer-based machine that was called the *DES cracker*, which was able to decipher DES encrypted messages.

10.7.6 The Advanced Encryption Standard (AES)

After the demise of DES, in 1997, NIST issued a request for proposals for an Advanced Encryption Standard. From the 15-candidate submitted proposals in 2000, NIST announced that it had selected the *Rijndael algorithm*, which had been developed by V. Rijmen and J. Daemen (hence Rijndael). The Rijndael algorithm is a block cipher and it is mathematically complex encompassing field theory, Galois fields, irreducible polynomials, equivalence classes, and so on [26–28].

The block and the key sizes are 128-, 192-, or 256- bit long. The block is subdivided into a sequence of subblocks, such as 8-bit bytes, which are organized in a matrix (for 128-bit blocks a 4×4 matrix of bytes is constructed, whereas for 192-bit blocks a 4 rows by 6 columns matrix). Then a ten-round iterative process of XOR ciphering followed by a round of highly complex mathematical operations for *byte substitution*, *shift row*, *mix column*, and *round key addition* is performed. The end result after the ten rounds is the final cipher text.

10.7.7 The RC4 Algorithm

The RC4 Algorithm, designed by Ron Rivest in 1987, is a symmetric cryptographic method, for which a variable key-size stream cipher is generated by a pseudo-number generator. According to it, an initial key (from 1 to 256 bytes) in a temporary vector T is used to create a variable 256-byte key in a state vector S ; thus, the RC4 performs byte-wise operations and random permutations. The state vector consists of 256 state elements $S[0], S[1], \dots, S[255]$. At initialization, the state elements $S[i]$,

$i = 0\text{--}256$ of the state vector S contain one of the $2^8 = 256$ binary combinations in an ascending order, 0 (00000000) to 255 (11111111).

The temporary vector T also consists of 256 elements. At initialization, T is preset with the cipher key. If the key is 256 bytes long, it fills all elements of T . If the key is less than 256 bytes, say k bytes ($k < 256$), then k bytes fill the first k elements of T and the key repeats itself as many times as necessary to fill T .

The role of each T element, $T[i]$, is to cause a swap of element i in S , $S[i]$, with element j in S , $S[j]$. The swapping process is an iterative process and it starts from element $i = 0$, $S[0]$, and ends with element $i = 255$, $S[255]$. The swap of element i , $S[i]$, with element j , $S[j]$, is defined according to an algorithm. To find the element j with which element i is swapped, one executes a modulo256 calculation between $S[i]$, $T[i]$, and j . Thus, for element $i = 0$, element j_0 is calculated from $j_0 = \{S[0] + T[0]\}\text{mod}256$. Now, for element $i = 1$, the value of the next j , j_1 , is calculated from $j_1 = \{j_0 + S[1] + T[j_0]\}\text{mod}256$. Similarly, for element $i = 2$, the value of the next j , j_2 , is calculated from $j_2 = \{j_1 S[2] + T[j_1]\}\text{mod}256$, and so on, to the final element $j_{255} = \{j_{254} S[255] + T[j_{254}]\}\text{mod}256$.

Since the initial vector S is predefined (0–255), and the temporary vector T is also predefined (it contains the pseudorandom initial key), it does not seem difficult to perform all swapping calculations a priori and then use vector S in its final (swapped) state as the cipher key (this would require one memory to store the cipher key in S , eliminating T). Alternatively, if T is generated byte at a time, then since the initial S is known, all is needed is a one line iterative calculation, the result of which is stored in a register and which is the current element of the cipher key.

Because of the algorithmic simplicity of the RC4, RC4 has found acceptance in several protocols such as the WiFi protected access (WPA), the wired equivalent privacy (WEP) and in secure sockets layer/transport layer security (SSL/TLS). RC4 was initially an RSA security private algorithm, but it was posted on the Internet anonymously.

10.7.8 Asymmetric Ciphers

The cipher systems that we explained in the previous section used a key and an encryption procedure that must be known to both, the message sender and the rightful message receiver. Regardless of how complex the cryptographic method is, if it becomes known to a third party it automatically loses its value.

In 1967, it was proposed [29] that it is possible to have an encryption algorithm that even if it is known to the public it is difficult to find the key and decipher the cipher text by a third party.

Now, as intriguing as this proposal may seem, in reality it uses two keys, one public and one private. Although the public key is used to cipher the message and is known to all (hence public), the private key is used to decipher the message and it is known to the rightful receiver. Hence, such methods are classified *asymmetric cryptography* because a single key is not used at both ends of the communications channel, and also *public key cryptography* because they use two or more keys, one of which is public. A parallel to asymmetric keys is the keys of safe deposits at banks. Two keys are needed to unlock a safe deposit box, one key that fits in all boxes in the safe and which the bank holds (the public key) and one private key that the rightful owner holds. One key by itself cannot unlock a box.

In cryptography with asymmetric keys, security depends on the intractability of mathematical manipulations that are required for defining the cryptographic keys. Therefore, before we continue with the description of certain cryptographic methods, we need to define certain mathematical concepts as we did in Sect. 10.5.1.

10.7.9 The Integer Factorization Problem

Given a positive integer n , express it in its prime factorization. This means finding the pairwise distinct primes p_i such that $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}$, where the exponents $e_i \geq 1$.

Before attempting to factor the integer n , the integer should be tested to assure that it is prime (or composite).

The *nontrivial factorization* problem $n = ab$, where the *nontrivial factors* a and b are not necessarily prime and are $1 < a < n$ and $1 < b < n$. This problem is solved by splitting n algorithmically into factors a and b . When a and b are found, they are tested for primality.

10.7.10 Elliptic Curve Factoring

The elliptic curve factoring algorithm considers a random elliptic curve group over Z_p . The order of such group is roughly uniformly distributed in the interval $p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}$.

If the order of the group is smooth with respect to some preselected bound, the elliptic curve algorithm most likely will find a nontrivial factor of n , else it will fail (in the following, a more rigorous treatment on elliptic curves is provided).

10.7.11 The RSA Algorithm

This algorithm, developed by Rivest, Shamir, and Adleman (hence RSA algorithm), uses prime numbers in addition to Euler's and Fermat's theorems.

The RSA algorithm chooses two prime numbers p and q and it calculates the products $N = pq$ and $O = (p-1)(q-1)$. Then it selects a number k such that the gcd of k and O is 1. Then, it finds a number k' such that $kk' - 1$ is evenly divisible by $(p-1)(q-1)$.

This algorithm considers the key k public with which the text is ciphered and the k' private. The cipher text then is $C = M^k \bmod n$ and the deciphered original text $M = C^{k'} \bmod n$.

For example:

- Assign a number to each letter of the alphabet, as

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	U	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- Then, divide the message to be encrypted into groups of letters; the size of group is chosen so that two groups are not identical. For example, assume that a message consists of the word ABCD. In this case, the length of the group is a single letter such as A, B, C, and D. Then, the letters are replaced by their corresponding numbers in the alphabet, as A B C D => 1 2 3 4.
- The algorithm continues with choosing a number N which is the product of two prime numbers, p and q . In this case, we select $p = 3$ and $q = 7$, and thus $N = 3 \times 7 = 21$, and $O = 2 \times 6 = 12$.
- Then, a prime number k is selected that is within the product $(p-1)(q-1)$. In our case we select $k = 7$ which is within 12.

The prime number $k = 7$ constitutes the cipher key.

- Then, the message is encrypted as follows:

each number is raised to the power of the key times ($\bmod n$):

$1^7 \bmod 15, 2^7 \bmod 15, 3^7 \bmod 15, 4^7 \bmod 15$, or

$1 \bmod 15, 128 \bmod 15, 2187 \bmod 15$, and $16384 \bmod 15$, or

14, 8, 12, 4, and thus the encrypted message is N H L D.

To decrypt this message:

- The recipient of the encrypted message N H Q D converts it to letter numbers of the alphabet, 14, 12 and 4.
- Then, a process starts to calculate the decipher key. To do so, the recipient has to find a value k' such that $k \times k' - 1$ is evenly divisible by $(p-1) \times (q-1)$, or $[k \times k' - 1] / [(p-1) \times (q-1)] = P$ where P is an even number. In modular notation, this is equivalent to $k \times k' - 1 = 0 \bmod [(p-1) \times (q-1)]$.
- Then, k' constitutes the decipher key.

In our trivial example, $(p-1) \times (q-1) = 2 \times 6 = 12$ and $(7 \times k' - 1)/12 = P$ yields $k' = 7$ as $P = 4$; that is, the cipher key and the decipher key turn out to be the same. This is because we used very small prime numbers to illustrate easily each step of the method. However, if one uses large numbers and a computer to do the arithmetic, then the two keys k and k' are not the same and thus the method is asymmetric (as an exercise, use the numbers $k = 11$, $p = 13$, and $q = 19$ and find k').

- Now, knowing the key k' , the decrypted message is recovered by following a similar process as encrypting it. To do so, the corresponding numbers of the cipher text are raised to the power of k' mod n and the result is the deciphered text.

Based on the last step, our example continues as:

$14^7 \bmod 15$, $8^7 \bmod 15$, $12^7 \bmod 15$, $4^7 \bmod 15$, or

105,413,504 mod 15, 2,097,152 mod 15, 410,338,673 mod 15, and 16,384 mod 15, which yields

1, 2, 3, 4, and produce the deciphered and original text A B C D.

The actual RSA algorithm involves large exponentials and large prime numbers. Thus, the RSA algorithm is based on mathematical computability to make the job of a bad actor difficult. However, all an eavesdropper needs to know is the cipher k and N , which is the product of two prime numbers, p and q , and thus it should not be impossible to compute with a supercomputer. Therefore, if the assumption is that the sender and the receiver have fast computers to perform the arithmetic for ciphering and deciphering respectively, then so does the eavesdropper (who can have a faster computer or a smarter solution). For example, the open challenge that RSA had set for breaking its code RSA-129 (\$100 to whoever cracks it) was met in the summer of 1994 by an international team, dubbed the *wisecrackers*, which was distributed in every continent and worked on approximately 1,600 computers, for 1 year; the RSA-129 had a 129-digit key.

10.8 Quantum Cryptography

Current cryptographic methods base their effectiveness of secrecy on the complexity of the method, algorithmic or computational, and the inability of the casual eavesdropper to decode messages. This however, although effective, does not ease users who need guaranteed unbreakability of the cipher text and truly secure key distribution. For example, if a bank transfers billions of dollars from one account to another or if a government sends a top secret message to its embassy in a hostile region, the success of secure deliverability cannot be expressed in probabilities and percentages but in absolute 100% secure deliverability. Thus, a *platinum grade cryptographic method* was in need that was dubbed the *Holy Grail of cryptography*, implying that this is a true mathematical and technological challenge. However, if such method was discovered, it would be a cryptographic panacea and it could be used in high-end applications as well as in personal privacy and information security and the problem of eavesdropping would have been solved.

In pursue of the unbreakable cipher key, in about 1970 Stephen Wiesner wrote “Conjugate Coding” [30] planting the seed of Quantum Cryptography, but his idea did not receive the proper attention. In 1990, however, Wiesner’s idea was further elaborated and was brought to life by C.H. Bennett (who knew of Wiesner’s idea) and others [31–33] who experimentally demonstrated the feasibility of the concept.

Quantum mechanics (QM) theory [34] dwells on the atomic and subatomic nature of matter supporting that the properties of nature in that microcosm are not continuous but quantized, in contrast to classical mechanics, which supports that in macrocosmic sizes nature behaves in a continuous manner. Quantum mechanics also describes the properties and nature of photons, and photons are used in optical communications and optical networks to transport huge amounts of information. It is this quantum-mechanical explanation of photon properties that becomes the centerpiece of a new mathematical computation called *quantum computing* [28] and of a new cryptographic method known as *quantum cryptography* [35–37]; when deployed in communications it coins the term *quantum communications* [38–40].

The theory of QM is complex and it involves meanings and mathematical notations that are not taught in high school or non-Physics undergraduate programs. In order to describe a complex subject in a simple manner, it is educational to clarify some notations, which are often encountered in quantum mechanics.

The starting point of quantum mechanics is the time-space differential equation of a wave function known as the Schroedinger equation and which describes how a state vector $|\psi(t_0)\rangle$ evolves in time:

$$i\hbar \frac{\partial \psi(1, t)}{\partial t} = H(p, q)\psi(q, t) \quad (10.2)$$

This wave function may be considered a mathematical artifice since it does not represent a real quantity. However, the square of it is related with the probabilities of existence of the states. The wave function uses a notation that involves the symbols $<$ and $>$. If the two symbols together $<>$ denote a bracket, then in quantum mechanical symbolism $<$ is the bra and $>$ is the ket, both with specific properties; a treatment of this may be found in numerous texts in quantum mechanics, and therefore it is beyond the purpose of this book. With this notation in mind, the wave equation that describes the spin of two particles is

$$|\Psi\rangle = [1/\sqrt{2})(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle), \quad (10.3)$$

where the symbols $|\uparrow\rangle$ and $|\downarrow\rangle$ denote single particle kets for the singlet states *spin up* and *spin down*. To trivialize this, this notation describes that two particles A and B emitted from a source with possible spins up or down interact, and because of this they are in such a state that it is difficult to predict with accuracy the spin state of each particle. Solving this relationship, one obtains the probabilities of particles A and B being in spin state up or down but not the exact value of the spin (this is known as *local realism*). When the two particles are *disengaged* and independent, only then can their spin be accurately measured. The argument with this is that when the two particles are engaged, measuring the spin of one affects the spin state of the other and vice versa, and therefore it is impossible to know with certainty the spin of each particle. When the two particles are disengaged, independent measurements yield the spin state of each particle accurately. In quantum mechanics, the common terms engaged and disengaged are known as *entangled* and *disentangled*; one of the cryptographic methods in *optical quantum cryptography* uses *entangled photons*.

In optical networks, the properties of photons may be used in alignment with quantum mechanical principles to develop cryptographic methods, and particularly key distribution methods. Thus, *quantum cryptography* (QC) is the art of cryptography using quantum-mechanical principles and

quantum key distribution (QKD) is a key distribution method that employs certain quantum properties of particles and especially of photons. One of such properties is the photon polarization state.

Optical quantum cryptography uses a cipher key that has been generated typically by an asymmetric key generated using one of the well-known methods, such as Diffie–Hellman, elliptic curve cryptography, or similar to it. Then, the message is ciphered bit by bit using a modulo2 or XOR operation. The XOR may take place in the electronic regime (before it is converted to optical) or directly in the optical regime [41, 42].

10.9 Key Distribution

The main objective of a key distribution processes is to transmit to the receiving end the cipher key in such a way that an eavesdropper cannot capture or copy the key. This may seem simple but indeed is of paramount importance to cryptography. If the key is known to a third party, then the cryptosystem has no meaning. The motto a secret is not a secret if it is known by two people is also critical in cryptography. In fact, a serious effort in the key distribution establishment is to be able to develop a key such that only one end of the communications path knows the details of its key; that is, the transmitting end knows its ciphering key, the receiving end its deciphering key, but both ends do not know each other's key, yet be able to cipher and decipher the same text. In all, a true puzzle.

10.9.1 Merkley's Algorithm

In one scenario known as the *Merkley's algorithm*, also known as *Merkley's puzzle*, a brute force approach is used as follows: the sending end A of a link sends to the receiving end B several keys, each with an identification number. B tries to break them one at a time by brute force and if it is successful in breaking one of them it sends back to A the ID number of the key which establishes the encryption/decryption key. Thus, the secret key is known to both A and B but an eavesdropper does not know which key is in use. Clearly, a sophisticated eavesdropper may break all keys by brute force (if B can so the eavesdropper) and then either detect the ID number when it is sent from B to A or copy the cipher text and perform a parallel decryption to find out the actual key in use.

10.9.2 Shamir's Key Distribution Method

The Shamir's key distribution method considers that no single member of a group is trustworthy for the whole key [43], but if the key is divided into m pieces, then each piece of the key can be distributed to each of the m members. The cipher key is the coefficient a_0 of an $m - 1$ polynomial $f(x) = a_0 + a_1x + \dots + a_{m-1}x^{m-1}$ and all other coefficients are random elements. According to Shamir's method, all members of the group m know the field of the polynomial, and each one receives a point (x,y) of the polynomial. Thus, although any individual member of the group or any subgroup cannot solve Shamir's puzzle, all m together can determine the key. As a consequence, an eavesdropper can copy one of the pieces but not all m .

10.9.3 Diffie–Hellman Key Exchange

In secure communications, one of the main issues is to allow the end users of a path to exchange the cipher key securely. Algorithms with such an objective are known as *public key algorithms*. The

Diffie–Hellman discrete algorithm was the first published public key algorithm [44]. This algorithm is based on the difficulty of solving the *discrete logarithm problem* (DLP).

In short, DLP can be stated as follows:

Given a prime number p , a generator α of Zp , and a non-zero element β in Zp , find the unique integer k such that $\beta = \alpha^k \text{mod } p$; k is in the range from 0 to $(p - 2)$ and it is called the discrete logarithm of β to the base α .

Based on the DLP, the Diffie–Hellman algorithm defines a primitive root α of a prime number p such that its powers generate all integers from 1 to $p - 1$. Thus,

$\alpha \text{mod } p$, $\alpha^2 \text{mod } p$, $\alpha^3 \text{mod } p$, and $\alpha^{p-1} \text{mod } p$ are distinct and consist of the integers 1 through $p - 1$ in some permutation.

The order of an element g (in a multiplicative group) is defined as the smallest positive integer m such that $g^m = 1$.

An element α having order $(p - 1) \text{mod } p$ is called *primitive element mod p*. Element α is a primitive element mod p if and only if $\alpha^{(p-1)/q} \neq 1 \text{mod } p$ for all primes q such that $q|(p - 1)$.

For example, consider the prime number $p = 13$. We calculate successive powers of 2 and verify that 2 is a primitive element mod 13:

$$2^0 \text{mod} 13 = 1, 2^1 \text{mod} 13 = 2, 2^2 \text{mod} 13 = 4, 2^3 \text{mod} 13 = 8, 2^4 \text{mod} 13 = 3, 2^5 \text{mod} 13 = 6,$$

$$2^6 \text{mod} 13 = 12, 2^7 \text{mod} 13 = 11, 2^8 \text{mod} 13 = 9, 2^9 \text{mod} 13 = 5, 2^{10} \text{mod} 13 = 10, 2^{11} \text{mod} 13 = 7.$$

The element 2^i is primitive if and only if $\gcd\{I, 12\} = 1$. Alternatively, the element 2^i is primitive if and only if $i = 1, 5, 7$, and 11, or the primitive elements modulo 13 are 2, 6, 7, or 11.

In the Diffie–Hellman algorithm, both the primitive root α and the prime number p are publicly known. Now, if two end users A and B want to exchange a key, user A selects a random integer $X < p$ and computes $K_A = \alpha^X \text{mod } p$. Similarly, user B independently selects a random integer $Y < p$ and computes $K_B = \alpha^Y \text{mod } p$. User A makes known to user B the computed value K_A , but keeps the integer X private; vice versa user B sends to A the computed value K_B and keeps Y private. Thus, no one else knows the integers X and Y but users A and B, respectively. Now, user A calculates the key $C_A = (K_B)^X \text{mod } p$, and user B the key $C_B = (K_A)^Y \text{mod } p$. It turns out that these two keys are the same, $K = C_A = C_B$; that is, the final cipher key that will be used by each end is $K = \alpha^{XY} \text{mod } p$, Fig. 10.5. The proof of this is straightforward:

$$C_A = (K_B)^X \text{mod } p = [\alpha^Y \text{mod } p]^X \text{mod } p = [\alpha^X \text{mod } p]^Y \text{mod } p = [K_A]^Y \text{mod } p = C_B$$

The security feature of the Diffie–Hellman algorithm lies in the secrecy of integers X and Y and the difficulty to calculate discrete logarithms. For example, in order to calculate the key from the

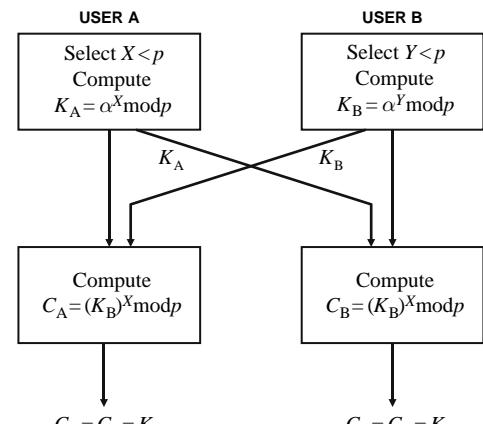


Fig. 10.5 Diffie–Hellman key exchange protocol

publicly known values, an intruder must first calculate Y (or X) from the relationship $\alpha^{XY} \bmod p$ using discrete algorithms, a calculation which is very difficult and particularly if the prime number is very large.

10.9.4 Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is based on the mathematical properties of certain members of a family of elliptic curves E over a field F described by the general equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2a_4x + a_6$.

An elliptic curve to be useful in cryptography should not have points on the curve at which both partial derivatives vanish; that is, the curve must be smooth.

If F is not a characteristic of 2, then the coefficients a_1 and a_3 can be set to zero without loss of generality.

10.9.4.1 Fundamentals of Elliptic Curves

The well-known public key algorithms, RSA and Diffie–Hellman (DH), are based on the use of elementary number theory and on computing difficulty. The RSA algorithm is based on the difficulty of factoring the product of two large primes. Thus, a user selects two large prime numbers, and their product is published as the public key. The secrecy of this method depends on the difficulty of factoring a very large number to find from the public key the private key. The DH algorithm is based on the difficulty of solving *discrete logarithms* for large finite groups. That is, in a large finite group, the solution of $a^x = c$ for x , even when a and c are publicly known, involves difficult discrete logarithms. In cryptography, we distinguish the discrete logarithm problem in two cases, one assumes the finite field that has a large prime (or odd characteristic) and the other the binary or characteristic 2 (i.e., 2^m).

Interestingly, although both schemes are formulated differently, their security is comparable as it is based on the difficulty of solving the problem. In the meantime, significant progress on factoring and discrete logarithms has stimulated a steady increase of attack algorithms. Despite the fact that these attack algorithms are currently slow to execute in order to break the key in meaningfully short time, if special purpose supercomputers are deployed they will execute much faster to the detriment of security. As a consequence, new secure methods are needed, which cryptographically perform better than their predecessors and are immune to attacks. One such cryptographic method is based on elliptic curves dubbed *elliptic curve cryptography* (ECC), which is an approach to public key cryptography.

The use of elliptic curves in cryptography was suggested in 1985 independently by Neal Koblitz [45] and Victor S. Miller [46]. Since then, many advances in ECC have been made [47–52], the US National Security Agency endorsed ECC technology and NIST included it in its *Suite B* set of recommended algorithms.

Mathematically, an elliptic curve is an equation of the form $y^2 = f(x)$ or $F(x, y) = y^2 - f(x)$, which is smooth at any point. This means that the slope at any point on the curve or the first differential of F with respect to x and y does not vanish. In fact, one may envision the relationship $F(x, y)$ as projective curves on the plane through the origin, in 3-space, of an equivalent class $(x:y:z)$ of curves so that they are reduced to regular (x, y) coordinates. Then, the set of points $(x:y:0)$ is called the *line at infinity*. As an example, consider a cone. Then, all conics can be projected on a plane through the origin and be transformed into each other by a linear transformation. Similarly, an elliptic curve is a two-variable plane curve, on which a group of points in the affine plane satisfy a certain cubic equation.

We consider two cases of elliptic curve groups. One is over the field of real numbers $F(n)$ and the other over the field $F(p)$, where p is a prime and over the field $F(2^m)$ which is a binary representation with 2^m elements.

10.9.4.2 Elliptic Curves over Real Numbers $F(n)$

In the real number case, the defining equation has the form

$$E^{a,b}(GF(n)) : y^2 = x^3 + ax + b, \text{ where } x, y, a \text{ and } b \text{ are real numbers.} \quad (10.4)$$

If there are no repeated factors in $y^2 = x^3 + ax + b$ or if $4a^3 + 27b^2 \neq 0$, then the elliptic curve can form a group. Each value of a and b yields a different elliptic curve, which is symmetric around the x axis, Fig. 10.6.

The following code generates a set of elliptic curves $y^2 = x^3 + ax + b$ for different values of a and b , some of them already shown in Fig. 10.6.

For $b = (0 \text{ to } 4, \text{ step } 1)$

For $a = (0 \text{ to } 4, \text{ step } 1)$

For $x (-10 \text{ to } 10, \text{ step } 0.5)$

If $x^3 + ax + b \geq 0$; test if y value is on the elliptic curve

$$w = x^3 + ax + b$$

$$y_1 = +\sqrt{w}, y_2 = -\sqrt{w}; \text{ find } y$$

Plot $(x, y_1), (x, y_2)$; two symmetric points (or a single point if $y_1 = y_2$)

Else,

return

Print (a, b)

return

return

An elliptic curve over real numbers consists of all points on the curve together with a special point O called the *point at infinity*; its purpose becomes clear if we notice that the elliptic curve as defined is *symmetric around axis x*. Thus, because elliptic curve groups are additive, if we were to add two points P and P' that are symmetric around the x axis, the result would be “null” or the point at infinity O . Although the point at infinity O has no affine coordinates, it is convenient to represent it using a pair of coordinates which do not satisfy the defining equation. For example, $O = (0, 0)$ if $b \neq 0$ and $O = (0, 1)$ otherwise. *Affine coordinates* are the coordinates (x, y) of a locus. For example, the elliptic curve for which $a = -3$ and $b = 3$ has the (x, y) loci on the curve $\{(-2.1, +/-0.20), (-2.0, +/-1), (-1.0, +/-2.24), (0.0, +/-1.73), (1.0, +/-1), (2.0, +/-2.24), (3.0, +/-4.58), (4.0, +/-7), (5.0, +/-10.63)\}$. The additive property of elliptic curves is examined in the remainder of this section.

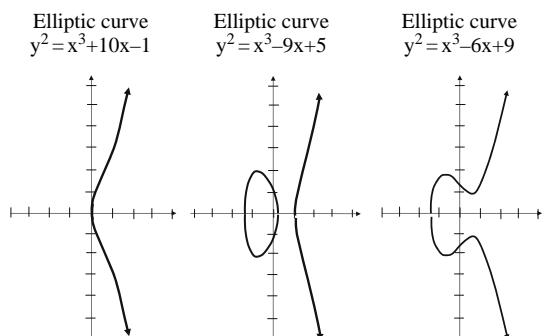
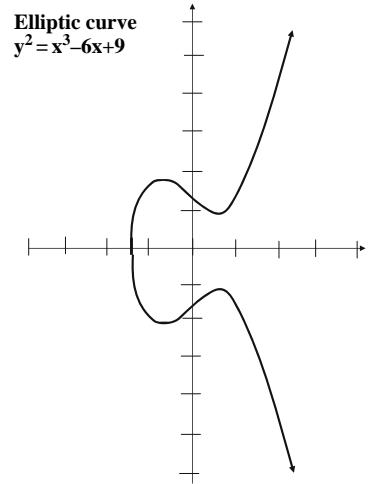


Fig. 10.6 Set of elliptic curves $y^2 = x^3 + ax + b$ for different values of a and b

Fig. 10.7 Elliptic curve
 $y^2 = x^3 - 6x + 9$



Similarly, some of the loci of the elliptic curve with $a = -6$ and $b = 9$ (rounded to the second decimal point), illustrated in Fig. 10.7, are $\{(-2.93, \pm 1.26), (-0.80, \pm 3.65), (0.93, \pm 2.06), (2.93, \pm 4.06), (5, \pm 10.2)\}$.

Consider two points on the elliptic curve P and Q . Point P has coordinates (x_1, y_1) and its symmetric point on the curve and around the x axis is $-P = (x_1, -y_1)$. Point Q has coordinates (x_2, y_2) and it is such that $Q \neq -P$. Adding the two points P and Q geometrically entails to drawing a straight line through points P and Q until it intersects the elliptic curve at a third point, R' . Then, the symmetric of point R' around the x axis, point R , is the solution to $P + Q = R = (x_3, y_3)$. Algebraically, the point $R = P + Q$ on the curve with coordinates (x_3, y_3) for the elliptic curve $y^2 = x^3 + ax + b$ is found as follows [53]:

$$x_3 = S^3 - x_1 - x_2,$$

and

$$y_3 = S(x_1 - x_3) - y_1,$$

$$S = (y_2 - y_1)/(x_2 - x_1) \text{ if } P \neq Q, \text{ or } S = (3x_1^2 + a)/2y_1 \text{ if } P = Q \text{ (i.e., } P \text{ is a double point),}$$

where S is the slope of the line through the points P and Q (when $P \neq Q$) or the slope of the tangent at point P (when $P = Q$).

Similarly, the coordinates (x_3, y_3) of $P + Q = R$ for the elliptic curve $y^2 + xy = x^3 + ax^2 + b$ are defined as follows:

For $P \neq Q$:

$$x_3 = [(y_1 + y_2)/(x_1 + x_2)]^2 + (y_1 + y_2)/(x_1 + x_2) + x_1 + x_2 + a, \text{ and}$$

$$y_3 = [(y_1 + y_2)/(x_1 + x_2)](x_1 + x_3) + x_3 + y_1, \text{ and}$$

For $P = Q$ (i.e., P is a double point):

$$x_3 = x_1^2 + b/x_1^2, \text{ and}$$

$$y_3 = x_1^2 + (x_1 + y_1/x_1)x_3 + x_3.$$

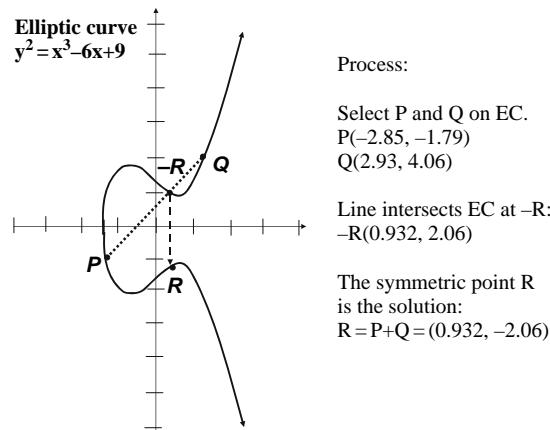


Fig. 10.8 Finding the point R from P and Q

Example: Consider the elliptic curve $y^2 = x^3 - 6x + 9$, Fig. 10.8. In this case, point $P = (-2.85, -1.74)$, $Q = (2.93, 4.06)$ and $P + Q = R = (0.932, -2.06)$.

Now, if a single point P on the elliptic curve is selected then the tangent at P intersects the elliptic curve at another point $-R$ from which the symmetric point R is the solution to $2P = R$ (i.e., point P is a *double point*), Fig. 10.9.

10.9.4.3 Elliptic Curves over Prime Numbers $F(p)$

Working with real numbers produces imprecise results due to the rounding of numbers which cause errors. For instance, $5/3 = 1.666666666^*$, which one may write 1.667 or 1.6667 if accuracy to the third or fourth decimal is sufficient; this introduces an error of approximately 0.0003. Similarly, the product 1.35×2.97 produces 4.0095, which if rounded to the second decimal is 4.01 introducing an error of 0.0005. In cryptography, precision is very critical, and therefore fields with integers, primes and powers of 2, are more convenient.

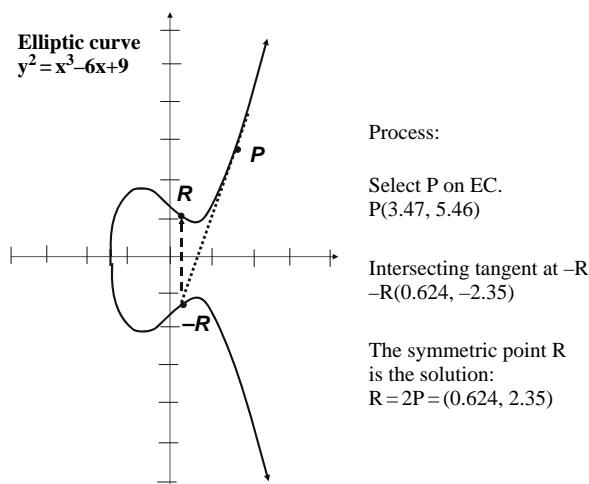


Fig. 10.9 Finding the point R from a double point P

In the prime case, the defining equation has the form $E^{a,b}(GF(p))$: $y^2 = x^3 + ax + b$, where a and b are constants in $F(p)$ such that $4a^3 + 27b^2 \bmod p \neq 0$, where p is a prime number in the range 0 to $p - 1$, and the right side of the equation has no repeated factors. In this notation, $E^{a,b}(GF(p))$ denotes the group of curves over the field $F(p)$ for the prime case. Thus, an elliptic curve consists of all points (x,y) that satisfy the elliptic curve equation modulo p , $y^2 \bmod p = (x^3 + ax + b) \bmod p$, along with a special point O called point at infinity; in addition, the relationship $4a^3 + 27b^2 \bmod p \neq 0$ must be satisfied. An elliptic curve over prime consists of the points on the curve together with a special point O called the *point at infinity*; its purpose was explained in the previous section. The negative of a point $P = (x_P, y_P)$ on the elliptic curve is point $-P = (x_P, -y_P \bmod p)$.

As in the case with real numbers, two points P and Q on the elliptic curve $E^{a,b}(GF(p))$ may be added to produce a third point R . The coordinates of point $R = (x_R, y_R)$ are

$$x_R = S^2 - x_P - x_Q \bmod p, \text{ and } y_R = -y_P + S(x_P - x_R) \bmod p,$$

where $S = (y_R - y_Q)/(x_P - x_Q) \bmod p$ is the slope of the straight line that connects points P and Q .

If there is only one point P on the curve at which the tangent is considered (also called double point), then the point R is calculated from $2P = R$, in which case (x_R, y_R) are:

$$x_R = S^2 - 2x_P \bmod p, \text{ and } y_R = -y_P + S(x_P - x_R) \bmod p,$$

where $S = (3x_P^2 + a)/(2y_P) \bmod p$ is the slope of the tangent at point P .

Example: Consider a simple elliptic curve in $F(23)$ with $a = 1$ and $b = 0$, $y^2 = x^3 + x$. Examine if point $(x, y) = (9, 18)$ is a point on the elliptic curve.

First, the coefficient relationship $4a^3 + 27b^2 \bmod p$ is examined: since $4 \bmod 23 \neq 0$ this condition is satisfied.

Now, to examine if the point $(x, y) = (9, 18)$ is a point on the elliptic curve, substitute x and y by the coordinate values:

$18^2 \bmod 23 = (9^3 + 9) \bmod 23$ or $324 \bmod 23 = 738 \bmod 23$ or $2 = 2$; this confirms that point $(9, 18)$ is a point on the selected elliptic curve.

Exercise: There is a total of 23 points that satisfy the elliptic curve defined in the aforementioned example. Using the previous example, verify that points $(1, 5)$, $(9, 5)$, $(11, 13)$, $(17, 13)$, and $(19, 1)$ are among them.

10.9.4.4 Elliptic Curves over $F(2^m)$

In the binary case, the defining equation has the form $E^{a,b}(GF(2^m))$: $y^2 + xy = x^3 + ax^2 + b$, where a and b are unequal constants in $F(2^m)$, $b \neq 0$, and m is a large integer. In this notation, $E^{a,b}(GF(2^m))$ denotes the group of curves over the field $F(2^m)$ for the binary case. As in the previous cases, $F(2^m)$ consists of all points on the elliptic curve and the point at infinity O . Notice that points in the binary case are expressed in their binary representation with the two symbols (1,0), where m denotes the number of symbols in the string. For example, if $m = 4$ then 0110 is one of the 16 possible strings. In addition, since we deal with binary strings, calculations are executed with the Exclusive Or (XOR) function. In a realistic cryptographic system, m is very large, such as > 100 , to be meaningful.

In the binary case, the form $E^{a,b}(GF(2^m))$ takes a more general expression where the coefficients a and b are also binary strings and thus they are replaced by the binary form g^m (g is known as the *generator*) as

$$E^{a,b}(GF(2^m)) : y^2 + xy = x^3 + g^m x^2 + g^n.$$

Then, for the simple elliptic curve $E^{a,b}(GF(2^2))$ with generator $g = (0010)$, the powers of g are in binary form:

$$\begin{aligned} g^0 &= (0001), g^1 = (0010), g^2 = (0100), g^3 = (1000), \\ g^4 &= (0011), g^5 = (0110), g^6 = (1100), g^7 = (1011), \\ g^8 &= (0101), g^9 = (1010), g^{10} = (0111), g^{11} = (1110), \\ g^{12} &= (1111), g^{13} = (1101), g^{14} = (1001), g^{15} = (0001); \text{ that is, } g^0 = g^{15}. \end{aligned}$$

Example: Consider the elliptic curve $E^{a,b}(GF(2^2))$: $y^2 + xy = x^3 + g^4x^2 + g^0$ ($a = g^4$ and $b = g^0$) and the generator $g = (0010)$. Verify that the point $(x, y) = (g^3, g^8)$ lies on the elliptic curve.

Replacing for x and y , there is

$$(g^8)^2 + g^3g^8 = (g^3)^3 + g^4(g^3)^2 + g^0 \text{ or}$$

$g^{16} + g^{11} = g^9 + g^{10} + g^0$, or and replacing with the corresponding binary codes (notice that when the exponent becomes greater than 15, they are modulo reduced and thus $g^{16 \bmod 15} = g^1$):

$$(0010) + (1110) = (1010) + (0111) + (0001), \text{ and performing XOR operations between them, } (1100) = (1100).$$

In the binary case of elliptic curves, there is a negative point R so that $R + (-R) = O$ and $P + O = P$, where O is the point at infinity. In addition, two points P and Q are added to produce a point $R(P + Q = R)$, the coordinates of which are (remember that all calculations are modulo-based)

$$x_R = S^2 + S + x_P + x_Q + a, \text{ and } y_R = S(x_P + x_R) + x_R + x_P,$$

where $S = (y_P - y_Q)/(x_P + x_Q)$.

Similarly, if the point P is double at which the tangent is drawn, the coordinates of the point R , $2P = R$, is calculated from

$$x_R = S^2 + S + a \text{ and } y_R = x_P^2 + (S + 1)x_R,$$

where $S = x_P + y_P/x_P$.

10.9.4.5 Cyclic Groups

A concept that helps the understanding of elliptic curve manipulation in the context of cryptography is the *cyclic groups*. First, raising an element a to the power n (where n can be a finite positive or negative integer, or 0): $a^0 = 1$, $a^1 = a$, $a^2 = aa$; $a^n = a^k a^m = a^{k+m}$, $a^n = a^{n-1}a$; and $a^n = aaa\dots a$ (n times); the latter in additive notation is written as $n \times a$ or $n.a$.

Consider the group of elements $a^0, a^1, a^2, a^3, \dots, a^k, \dots, a^{n-1}$; all elements in the group $G(a^k)$ are powers of a , and k is a finite integer, $k = 0$ to $n - 1$. Also consider that the modulus n of last term of the group, a^{n-1} , results in the identity element or simply the unit; that is, $a^{n-1} \bmod n = 1$, and in simplified notation (in which $\bmod n$ is implicit) as $a^{n-1} = 1$. When $a^{n-1} \bmod n = 1$, the group is termed a *cyclic group* of order n or the field size is n , F_n ; that is, the first and the last elements in a cyclic group is the unit. In this case, a is said to be a *generator* of the cyclic group of size n , denoted as C_n , or that the group is generated by a . For example, the field F_{23} has a size of 23 elements from 0 to 22 (notice that 23 is a prime). The prime 23 acts like a field, F_{23} , and the 23 elements of the group for the generator $a = 5$ (assuming mod23 operation for each term) are $5^0 = 1, 5^1 = 5, 5^2 = 2, 5^3 = 10, 5^4 = 4, 5^5 = 20, 5^6 = 8, 5^7 = 17, 5^8 = 16, \dots, 5^{21} = 14$, and $5^{22} = 1$; that is, the field F_{23} returns to 1 after 23 terms. Cyclic groups are abelian, but all abelian groups are not cyclic.

10.9.4.6 Applicability of Elliptic Curve Cryptography

The applicability of elliptic curves in cryptography with simple mathematical language is illustrated if we consider the algebraic closed elliptic curve and a straight line that cuts the elliptic curve at three points, as already shown. If the line is tangent to the elliptic curve, the tangent point is considered twice. Then, if two of the intersection points are rational, so is the third, and if two of the points are known, it is possible to compute the third. All solutions of the equation together with a point at infinity form an *abelian group*, with the point at infinity as the identity element. An abelian group G is said to be a *commutative group* if $a + b = b + a$ and $a^*b = b^*a$ for all (a, b) in G ; this means that it does not matter in which order a binary operation is performed. Thus, if the coordinates x and y are chosen from a large finite field, the solutions also form a finite abelian group. In common language, the third intercepting point is calculated from the two previous ones using the additive operation $P + Q = R$.

The ECC method suggested by Koblitz and Miller was based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP), which is stated as follows:

Given a prime power p , where F_p denotes the finite field containing p elements, and an elliptic curve, E , defined over a finite field F_p , determine the integer n in the range $(0, n - 1)$, such that a point P on the elliptic curve $E(F_p)$ and another known point Q on the elliptic curve $E(F_p)$ are related by $nP = Q$; that is, point Q is an integer multiple of point P , provided such integer exists.

It is believed that solving the elliptic curve discrete logarithm problem (if we know P and n , then we can generate Q) is computationally more difficult than solving the discrete logarithm problem used in the Diffie–Hellman (DH) method, although algorithms to solve this problem have been proposed. As a consequence, it is believed that for comparable or better security, the secret cryptographic key derived from elliptic curves is much shorter than the DH method.

Example: Consider the elliptic curve $y^2 = x^3 + 9x + 17$ over F_{23} . What is the discrete logarithm k of $Q = (4, 5)$ to the base $P = (16, 5)$?

Using the brute force approach, one would calculate all possible multiples of P starting with $k = 1$ and progressing with $k=2$, and so on until the solution that satisfies $kP = Q = (4, 5)$ is found. Doing so, the first few multiples [54, 55] are $P=(16,5)$, $2P = (20, 20)$, $3P = (14, 14)$, $4P = (19, 20)$, $5P = (13, 10)$, ..., $9P = (4, 5)$. Thus, the discrete logarithm of Q to the base P is $k = 9$.

The number of points or loci on elliptic curves that are useful in elliptic cryptography is important, as also are the number of points that make the elliptic curve discrete logarithm breakable [56–58]. In general, the elliptic curve may be vulnerable to attacks if the number of points on E over F is the same as the number of elements of F .

Now, suppose we have a^m and that m is written as $m = nQ + R$, where $0 \leq R < n$ for some integer Q ; remember that $m = nQ + R$ is also expressed as $R = m \bmod n$. Replacing m with the latter, one obtains $a^m = a^{nQ+R} = a^{nQ}a^R = (a^n)^Qa^R = (1)^Qa^R = a^R$. This means that all powers are in the range $[0-n]$, in which case the cyclic group of order n is written $C_n = \langle a \rangle$, where a is the generator and n is a prime. Thus, the additive cyclic group is considered similar to a multiplicative group of powers of an integer $a \bmod (\text{prime } n)$, and the problem of powers of finding k given points (kC and C) constitutes the *elliptic curve discrete logarithmic problem* (ECDLP); if prime numbers are used, it is known as the *prime case*, and if binary numbers (2^n) as the *binary case*.

To set up an elliptic curve cryptosystem, one needs to first establish the system parameters. This consists of the following steps:

- Select a finite field and a representation of the elements in it.
- Select an elliptic curve and the *generator* point G on the curve.
- Generate the public–private key pairs. These keys consist of a random, secret integer k , which acts as the private key, and the multiple of the generator point, kG , that acts as the public key.

It is the number of points N in the group of elliptic curve cryptosystems that makes ECC difficult to compute the private key k from the public key kG and thus offer high security. This requires a sequence of elliptic curve additions where each addition consists of several arithmetic operations in the finite field.

In contrast to ECC, the RSA cryptosystem requires

- no system parameters, but two primes of appropriate size;
- the generation of the public–private key pairs, the public modulus n from the product of the two primes, a process which is less computationally intensive than setting up the elliptic curve system parameters [59];
- additionally, the secret exponent d is computed, although this computation is insignificant when compared to generating the primes.

For RSA cryptosystems, it is the difficulty of computing the length of the modulus and a sequence of modular multiplications that offers security.

To summarize, the elliptic curve cryptography (ECC) is considered to be more difficult, and it offers higher security than its predecessors with equal or shorter keys [60, 61]. In terms of offered security, an ECC over a 160-bit field $GF(2^{160})$ offers roughly the same security as a 1,024-bit RSA modulus [62, 63] and a $GF(2^{136})$ as a 768-bit RSA. Comparing the key sizes recommended by NIST [13, 14] for the Diffie–Hellman RSA and the ECC, there is a dramatic difference in key length, 1,024 versus 163, 3,072 versus 256, 7,680 versus 384, and 15,360 versus 512, respectively.

Have we exhausted the subject of cyclic groups? Have we stated all properties of cyclic groups? To both questions the answer is NO. The objective of this section was to identify the complexity of the ECC and ECDLP subject (the surface of which we have barely scratched) and trigger further interest. Currently, there is active research in this field in order to identify the minimum key size, elliptic curves without hard points that can be attacked, and, conversely, identify hard points on elliptic curves that can be attacked; the sooner we know them, the more secure cryptography is. It is believed that the hardness of the discrete logarithm on elliptic curves constitutes a better solution than before, for at least few more years. Some outcomes of this research have been the following.

The hardest ECC broken to date has key that provides about 55 bits of security. For the prime field case, it was broken in 2003 using 10,000 Pentium class PCs running continuously for over 540 days, and for the binary field case it was broken in 2004 using 2,600 computers for about 510 days.

10.9.5 Digital Signature

Authentication is the process that identifies that a received message was sent by the rightful sending entity or source and also that detects if the sent message has been received altered.

It is important that when a message is received, the authenticity of the source of the message is beyond doubt and also that when an acknowledging message is sent back to the sourcing entity, the latter cannot deny that it never sent the message. Thus, non-repudiation is as important because it prevents an entity from denying involvement or receipt of a message and this is accomplished by a digital signature in a message.

Functionally, digital signatures are based on integer factorization, conventional discrete logarithms, and elliptic curve discrete logarithms [64–66].

10.9.6 The Trusted Third Party or Key Escrow Encryption System

To assure security of the cipher text and that the authorized user only can decipher it, certain other methods have been used that also provide portability of the key; that is, the authorized user, in addition to password that allows him/her to access a server, he/she needs a second key to encrypt/decrypt. In such system, a third trusted entity holds special data recovery master keys, which do not decrypt the cipher text but they are sent to the authorized user to compute the cipher key. Because these special keys are in the trust and safeguard of a third party or escrowed, this method is known as *trusted third parties* (TTP) or *key escrow encryption system* (KEES).

The *key escrow encryption system* consists of the key escrow component. This is managed and operated by a trusted and accountable party (an escrow agent) and it is part of the public key certificate management infrastructure. Escrow agents may be private, commercial, or government; they are identified by name, location, and time-stamp (time and date). It also consists of the user security component, a hardware device that supports the key escrow function and is capable of encrypting and decrypting. Finally, it consists of the data recovery component that includes the cryptographic algorithm and the communications protocol for user and device authentication. The cryptographic algorithm and the communications protocol in use depend on the service provider of the key encryption system. Such encryption devices may include registered portable tags, smart cards, tamper-resistant encryption chips, or PC cards, that execute from a variety of encryption algorithms.

Clearly, the security the key escrow system provides is commensurate with protection against loss, detection of compromised and abused escrow devices and keys, reliability, accountability and liability of the third party, and authentication of the authorized device and user.

10.10 Quantum Key Distribution

Quantum cryptography is based on quantum mechanics and it takes advantage of Schrödinger's equation and Heisenberg's uncertainty principle [67–73]. This principle supports that probing a quantum system in order to measure its state, disturbs its state and yields incomplete information about it. That is, the measured state is not the same before the measurement because at the microcosmic level the probe interacts with the quantum system altering its properties. According to it, in an optical cryptographic system based on the quantum properties of photons for encrypting messages, an eavesdropper would cause unavoidable disturbance in the quantum communication channel, which the sender and the receiver would detect. Thus, if the quantum mechanical properties of particles are employed in a cryptographic system, then a secret random cryptographic key distribution method can be established between two entities providing security against an eavesdropper; the key distribution using quantum principles is known as *quantum key distribution* (QKD).

The first experimental demonstration of QKD was by C.H. Bennett et al. [74–76], verifying the ideas of S. Wiener, as already described previously. Bennett et al. also demonstrated the notion of secret message *multiplexing*, which they called *quantum oblivious transfer* [77]. According to it, it is possible to send to a destination simultaneously two encrypted messages. The end user receives both messages but when one of the two messages is read, the other is automatically destroyed. Quantum oblivious transfer may be useful in discreet decision making.

Quantum key distribution is best applicable to optical communications [78] and thus it considers photon behavior and quantized states of photons, such as polarization, phase, photon entanglement, and photon wavelength. However, it should be mentioned that when photons propagate in optical matter, they are subject to interactions with the nonlinearity of the dielectric fiber and also to propagation loss, discontinuity reflections, and so on [79].

In addition to be able to utilize the Heisenberg's uncertainty principle, on which quantum cryptography is based, single or multiple photons with a specific quantized property (such as a polarization state) must be used. Single photon transmission provides better protection against eavesdropping, but with current technology it is difficult and very expensive to produce in a controllable manner single photons that can be transmitted in common single mode fiber. Conversely, multiple photon transmission is easy and relatively inexpensive to produce in a controllable manner; they can travel further (considering fiber attenuation), but it provides lower protection against eavesdropping since few photons may be extracted from the stream. As a consequence, most current demonstrations use "manicured" quantum cryptographic system with linear, polarization maintaining, and continuous fiber that supports almost lossless single photon transmission.

In the following, we examine a QKD method that depends on polarization and one that depends on teleportation or entanglement.

10.10.1 Polarization-Based Quantum Key Distribution

In classical theory, a binary system has two distinct states, represented with the logic symbols "1" and "0". Quantum mechanics predicts that an unprobed (or unmeasured) system can be in one of the two extreme states, "1" and "0", and also with equal probability in states between the two states; that is, there is an uncertainty concerning the state of the system. Thus, the state of the system is in a superposition of all states, "1", "0", and all possible states between the two, as a result of the uncertainty principle. Only when the system state is measured, then the state is known and Heisenberg's principle does not hold. One may think of tossing the coin; as long as the coin flips in mid air, one cannot tell of its "head" or "tail" state, but only when it lands. So, when it lands, its state is "1" or "0", and when the coin is in mid air its state probability is $|\psi\rangle = (1/\sqrt{2})a|1\rangle + b|0\rangle$, where a and b are two positive constants smaller than 1 and $|\cdot\rangle$ is the *ket* function. This nonclassical superposition principle gives rise to quantum computation that is based on "qubits" instead of "bits". If instead of the sides of a coin we consider the spin states of an electron, $+\frac{1}{2}$ and $-\frac{1}{2}$, or the polarization states of photons [80–85], or some other quantized property of photons [86], then the principles of quantum computation are applicable to quantum cryptography and quantum key distribution (QKD).

Indeed, the polarization states of photons have been used in quantum cryptography and particularly in quantum key distribution. In this section, we examine the QKD with a method that uses photon polarization. We follow the convention of naming the two ends of an optical link as the sending station named Alice (A), the rightful receiving end as Bob (B), and the bad actor on the link, Evan the eavesdropper [86–91]. Using this convention, Alice communicates an asymmetric quantum key that only she knows to Bob, who although will never know the details of the key can decipher Alice's cipher text.

In general, a photon may be in one of many polarization states, linear horizontal, linear vertical, linear in an angle, elliptic, circular, and so on. The Poincaré sphere helps visualize the polarization states mapped on a sphere, Fig. 10.10.

With polarization states in mind, a QKD method is described as follows.

Consider an optical quantum cryptographic system, which is based on *states of polarization* (SoP). Consider also that the Poincaré sphere is partitioned into two hemispheres; for now, the actual partitioning is not so important. Thus, all states on one hemisphere are associated with logic "1" and all states in the complimentary hemisphere are associated with logic "0", Fig. 10.11; that is, logic "1" and logic "0" are associated with more than one polarization state, such as $(0^\circ, 45^\circ, 90^\circ, 135^\circ)$ and $(180^\circ, 225^\circ, 270^\circ, 315^\circ)$, respectively. In a more complex scheme, the SoPs for "1" and "0" may be quite random.

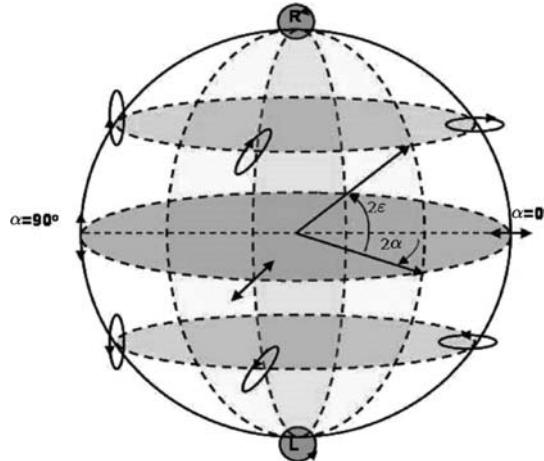


Fig. 10.10 Poincaré sphere on which SoPs are mapped

Additionally, assume that the fiber medium is perfect (homogeneous, isotropic, stress-free, loss-less, dispersion-less, continuous, and so on) and that randomly polarized *single* photons are serially and synchronously transmitted from Alice to Bob. The objective is to develop a QKD method that establishes an encryption secret key that only Alice knows, Bob can use (but he does not know its details) and Evan cannot copy.

This QKD key establishment method (first demonstrated by Charles Bennett, John A. Smolin, and Gilles Brassard of IBM Thomas J. Watson Research Laboratory) considers two separate connecting paths between Alice and Bob. One path is the optical fiber and the other a public channel, such as the Internet or the public wireless network, Fig. 10.12.

Notice that when in 1976, W. Diffie and M. Hellman introduced the public key cryptographic system, they defined a pair of keys, e and d , where e is a publicly available key and d is a private key. Although several public key protocols have been devised, here we describe a straightforward one [92, 93]:

1. Alice passes a string of photons through random polarization filter which is controlled by a sequence of binary bits, say 100110111011; logic “1” will produce a polarization state from one of the Poincaré hemisphere, and logic “0” from the complimentary hemisphere. However,

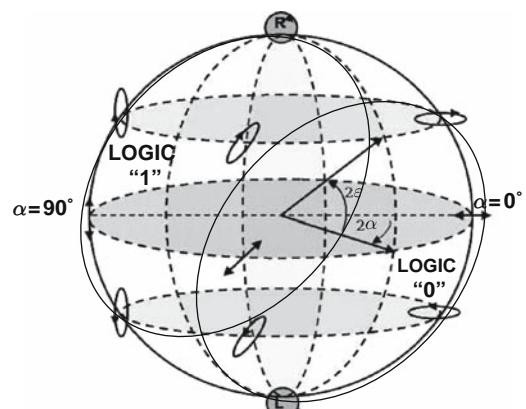


Fig. 10.11 Partitioned Poincaré sphere so that SoPs are mapped in one continent represent logic “1” and in another logic “0”

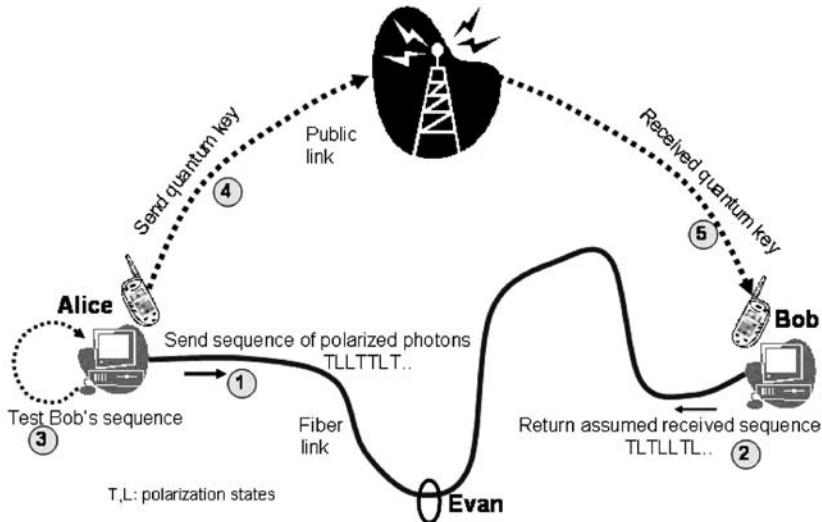


Fig. 10.12 The quantum key distribution uses an optical path and a public path between Alice and Bob to establish a secret key. If Evan intercepts the optical path, then he changes the polarization state and it prevents the establishment of the key

the association of polarization states with logic “1” and “0” is known to Alice only and unknown to anyone else, including Bob.

2. Bob receives the sequence of polarized photons which he now passes through his independently randomly varying polarization filter, but Bob does not know the association between logic value and polarization state.
3. The random polarization states of his filter pass or reject randomly polarized photons from Alice. That is, Bob generates a new sequence of logic “1”’s and “0”’s, in which (statistically speaking and over a long string of bits) some bits have the correct logic value that Alice sent, but not all.
4. Now, assume that Bob’s randomly varying polarization filter generates the sequence 010110101001 from the sequence received from Alice. Although this sequence is not what Alice transmitted, the common bits between the two sequences are important here. However, up to this step, neither Alice nor Bob knows which bits are common.

Now, the next steps in QKD are crucial.

1. Bob tells Alice, over the public unsecured channel, the polarization sequence that he used while receiving Alice’s polarized photons. However, Bob does not reveal to Alice the logic sequence that he generated.
2. Based on Bob’s response, Alice performs an experiment. She passes the logic sequence that she sent to Bob through Bob’s polarization sequence. Then, she compares the initial bit string with the one generated from the experiment and she identifies the common bits in the two bit strings.
3. Alice tells Bob which of his filter polarization states in the sequence were used correctly, but without telling him their polarization association with logic “1” and “0”. The polarization states that were used correctly constitute the quantum key.
4. When all this is done, Alice encrypts her message with the established key using a bit-by-bit modulo-2 (XOR) operation, and transmits the encrypted message to Bob, who deciphers it using

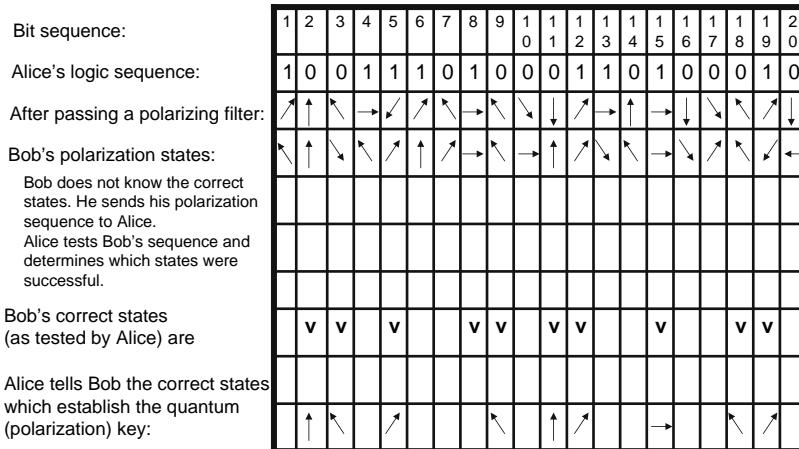


Fig. 10.13 The quantum key establishment between Alice and Bob using states of polarization (the sequence of events is from top to bottom)

the same encryption key. Figure 10.13 illustrates the key establishment with the described polarization method.

10.10.2 Entangled States and Quantum Teleportation

Teleportation has been a debatable issue for quite some time until a team of six scientists put an end to it using an old theory and an experimental finding. The theory was a mysterious quantum-mechanical phenomenon that was coined by Schroedinger *entanglement* in a two-part paper that appeared in 1935 and 1936 [94, 95]; these two papers were based on conversations with Einstein, Podolsky, and Rosen, who since 1930 were questioning the completeness of quantum mechanics for physical reality [96]. In fact, this phenomenon appeared in theory so paradoxically mysterious that Einstein called it a *spooky action at a distance*. Since then, the mysterious phenomenon has been known as the *Einstein–Podolsky–Rosen correlation* (EPR), and it is based on the *entangled states* of two particles, which still influence the state of each other even after they have been separated and placed at far distances! In cryptography, this effect is known as *teleportation* and it is. Teleportation supports that under certain circumstances, one particle can (mysteriously) affect the state of another particle even if they are completely separated and afar.

To understand the mystery behind this phenomenon, consider two initially entangled particles that have been separated and positioned at an arbitrarily far away distance and without communication between them; even so, when the state of one changes, the state of the other changes simultaneously. How can it be? Do these disentangled photons have extra sensory perception? Well, it is this *mysterious* behavior that has excited Hollywood’s imagination and in science fiction movies energy, people, food and animals are teleported at superluminal speeds, that is, faster than the speed of light.

The experimental finding by J. Bell in 1964 demonstrated that two individual particles that were previously entangled when untangled and far from each other did not exhibit random behavior but strong correlation; that is, they were still influencing each other. This is known as *Bell state quantum eraser*, and it is not explainable with classical mechanics [97].

Entangled photons are two photons in close proximity and in orthogonal polarization states. That is, one state of polarization may be linearly vertical and the other linearly horizontal, and as the two photons travel together, they interact with each other, although we do not know exactly how.

Orthogonal polarized states are not new; ordinary and extraordinary photons are photons with orthogonal polarization states that are created when unpolarized photons propagate through a strongly birefringent crystal, Figs. 10.14 and 10.15. Such crystal is the beta-barium borate ($\beta\text{-BaB}_2\text{O}_4$ or BBO). BBO crystals have a trigonal structure and nonlinear optical properties; they are transparent in the spectral range 189–3,500 nm and exhibit strong birefringence, with refractive indices (extraordinary and ordinary) $n_e = 1.5425$ and $n_o = 1.6551$ at 1,064 nm, $n_e = 1.5555$ and $n_o = 1.6749$ at 532 nm, and $n_e = 1.6146$ and $n_o = 1.7571$ at 266 nm. BBO crystals are known to split a high-energy photon that propagates through them into two photons, each at half the energy and at orthogonal entangled quantum states.

John Bell's experiment uses a BBO crystal and a laser that emits high-energy photons to demonstrate the effect of teleportation. This experiment in a simplified version is described as follows.

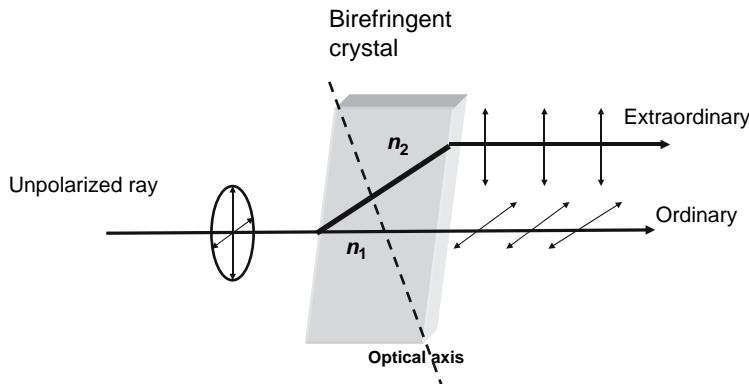


Fig. 10.14 A birefringent crystal splits an optical beam into two orthogonal polarizations, each traveling within the crystal at different speeds. The emerging rays are still orthogonally polarized. Under certain circumstances, the two emerging photons can be entangled

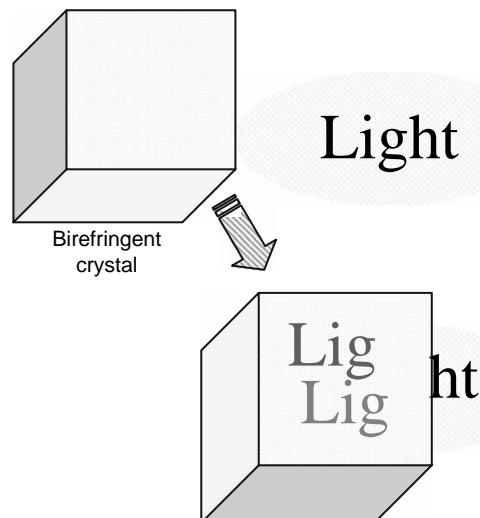


Fig. 10.15 Placing a birefringent crystal on top of a page will split the image (word “light”) in two

An ultraviolet laser (high energy and not visible to human eye) emits single photons to a BBO crystal. As photons travel through the crystal, probabilistically some are split into two photons, A and B, which now are orthogonally polarized. The two photons exit the BBO crystal (which is optically transparent at these frequencies) and each has half the ultraviolet frequency and energy (this frequency is visible to human eye). The resulting two orthogonally polarized photons are entangled.

Subsequent to this, the entangled photons are separated but they retain their polarization orthogonality. The one photon (A) is directed to a photodetector (D_A) through a polarizing filter (P_A), and the other photon (B) is directed to pass through a double slit and then it is detected by photodetector (D_B), Fig. 10.16. When the two photons impinge on their respective photodetectors, one would expect since the two photons by now are completely independent, whatever happens to one photon should not affect the other. Well, this is where the mystery lies.

When the polarizing filter P_A allows photon A to pass (because the polarization axis of filter P_A coincides with that of photon A), photon A is detected as well as photon B. However, when the filter P_A is rotated by 90° and does not allow photon A to pass (because the polarization axis of the polarizing filter P_A is perpendicular to photon A's polarization, known as *polarization erasure*), not only photon A but also photon B is not detected! That is, in some mysterious way, the state of photon A at the polarizer affects the polarization state of photon B even though photons A and B have been separated at an arbitrary distance; else, the state of photon A is teleported to the state of photon B instantaneously.

In actuality, Bell's experiment is a little more complex as each slit has a polarizing substance so that one slit passes counterclockwise linear polarization and the other slit clockwise. Thus, the observable quantity is the presence or absence of interference patterns; when photon A passes and is detected, the interference patterns at B are detected, and when photon A does not pass, the interference patterns at B disappear. Thus, the obvious question, How do photons at detector B know of the polarizations state of photons at detector A?

Following Bell's experiment, more experiments have yielded the same results, and recently one international team has announced five-photon entanglement and another team has announced quantum teleportation between light and matter [98]. As incredible as this may sound, even if some view teleportation with skepticism, one thing is for sure: the future will be full of excitement and surprises!

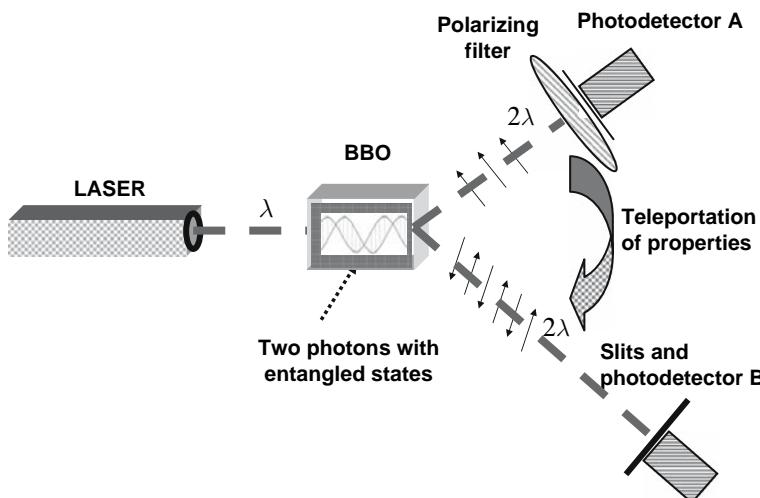


Fig. 10.16 A simplified diagram of the Bell experiment that demonstrated photon state teleportation (after Bell)

10.10.3 Quantum Teleportation and Quantum Key Distribution

Teleportation, when fully understood and explained, promises a secure mechanism for the distribution of the quantum cryptographic key in optical communications.

In simple terms, teleportation works as follows:

Consider a particle Z that processes the information to be teleported but its state is not known; particle Z is at the sending station where Alice is. Its state in quantum mechanical notation is

$$|\Psi_z\rangle = a|H\rangle + b|V\rangle,$$

where a and b are two constants.

Two photons X and Y are generated at some point with entangled and unknown states and which are independent of Z and not in contact with it. Quantum mechanically, since we do not know the individual polarization state of photons X and Y, their superposition of states is expressed by the ket relationship:

$$|\Psi_{XY}^-\rangle = \frac{1}{\sqrt{2}}(|H_X\rangle|V_Y\rangle - |H_Y\rangle|V_X\rangle),$$

where H and V denote conventional horizontal and vertical polarization states; that is, the two states are orthogonal and entangled.

Now, photon X is sent to Alice and photon Y to Bob, Fig. 10.17.

Up to this point, the inventory of photons is that Bob has photon Y and Alice photons X and Z. Now, At Alice's station, photons Z and X are allowed to interact with each other. This is known as *scanning the states*. The result of this interaction yields multiple states, all with equal probability of occurrence.

The interaction of the two photons produces a state which depends on the state of Z and X. As this interaction takes place, the states of both X and Z are destroyed or *erased* and the mysterious nonclassical effect gets into play; the scanned information from photon Z has affected the state

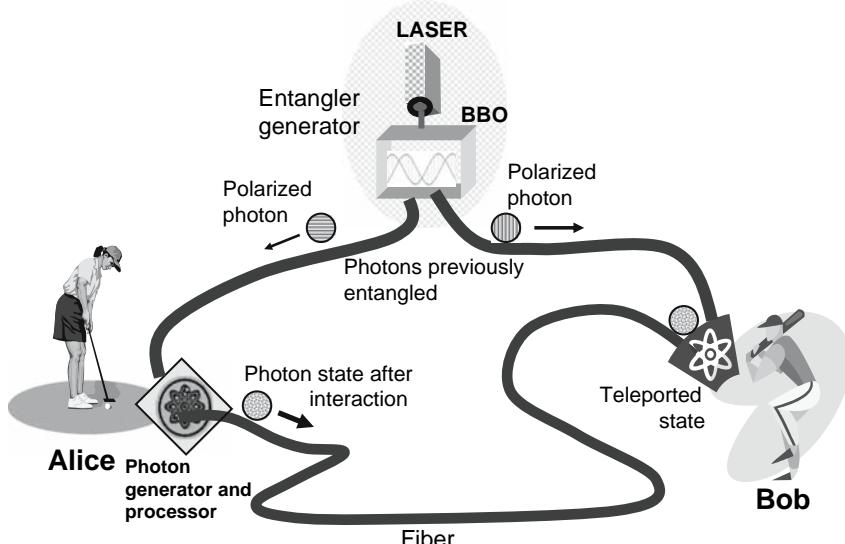


Fig. 10.17 The teleportation concept for quantum key distribution

of photon Y at Bob's station, or it has been teleported. Now, Alice measures the product of the interaction in a classical way and she transmits this measurement to Bob where now the state of the Y photon is adjusted to exactly the state of Z.

Thus, the system with all states involved is complete:

$$|\Psi_{XYZ}\rangle = \frac{a}{\sqrt{2}} (|H_Z\rangle |H_X\rangle |V_Y\rangle - |H_Z\rangle |H_Y\rangle |V_X\rangle) + \frac{b}{\sqrt{2}} (|V_Z\rangle |H_X\rangle |V_Y\rangle - |V_Z\rangle |H_Y\rangle |V_X\rangle),$$

The nonclassical information of Z has been teleported and the classical information transmitted: Thus, Evan, the eavesdropper, can capture the classical information but it is not sufficient to calculate the cipher key, since the nonclassical information has been (mysteriously) teleported [99–114].

It is precisely the teleportation effect that promises secure quantum key distribution in practical optical communications. Photon Z is at Alice's sending station and it possesses the information to be teleported to Bob's station. Two photons X and Y are first entangled and then separated. Photon X is sent to Alice's station, and photon Y to Bob's. At Alice's station, photon X interacts with photon Z and the quantum state of the interaction is teleported to photon Y at Bob's station. Alice also measures the state of interaction and sends it to Bob's station. The teleported quantum state and the measured classical state interact and photon Y becomes an exact replica of the initial state of X. Thus, the security of teleportation lies in the inability of Evan the eavesdropper to capture the teleported state and compute the cipher key.

10.10.4 A Trivialized Example

Does this sound too complicated? Here we make an attempt to trivialize the previously described process.

Consider two particles in entangled states each described by a binary code (we chose two binary orthogonal states to be consistent with the notion of entangled orthogonal states) X=1010, and Y=0101.

X and Y are detangled and X is sent to Alice's station where particle Z (represented by the code 1101) is and which we want to teleport; particle Y is sent to Bob's station.

At Alice's, X and Z interact (as in $A \otimes B$) producing the *scanned* information S=0111. After this interaction, the individual states of A and B vanish, and the produced information S, which does not resemble the original state of X or Z, is now teleported or sent to Bob's station.

At Bob's station, we manipulate the state of Y. We chose to transform Y to Y' by orthogonalizing it (or inverting it) yielding Y'=1010, and then we allow Y' to interact with S=0111, such as $Y' \otimes S = 1101 = Z$. Thus, the state of Z has been “teleported” to Bob's station, QED.

Thus, since Evan the eavesdropper may copy the state 0111, he does not know the states of X at Alice's ending station or the state of Y at Bob's station, and thus it is difficult to decode from the copied information 0111 the original code of Z (of course, a realistic code is many more bits than 4 as in this trivialized example).

10.10.5 Current Issues

The process we described in the previous sections is experimental and as such it is performed in a controlled and (almost) perfect environment. However, in pragmatic systems, one has to also consider pragmatic parameters, which raise certain critical issues, such as the following:

- Transmit the separated entangled photons through common fiber and connectors, the nonlinearity and the attenuation of which may alter the states and destroy entanglement.
- Difficulty to generate a long sequence of single photons at a highly synchronized and deterministic rate. Currently, laboratory experiments use an argon-ion single-photon laser source which may be impractical in commercial systems. The key bit rate in optical cryptographic systems ranges from few bits per second to few Kbps—compare with Gbps for optical data rates.
- Polarizers that can easily distinguish 0° from 180° , 90° , 270° , and so on.
- Polarizers that can easily discriminate 0° from 90° between two photons without destroying one of the two.
- Explain the physics of teleportation and find the distance limits.

Yet, another critical issue is the security of teleportation. Recent experiments claim five-photon entanglement and also state teleportation between photons and matter, and future experiments may demonstrate more unexpected effects. Therefore, the assumed inability of Evan to attack the teleportation loop may change as he may be able to capture nonclassical states and make the QKD process impossible.

10.11 Current Vulnerabilities in Quantum Cryptography

To date, several quantum cryptographic algorithms have been developed which have been examined and found to have vulnerabilities to eavesdropping [115]. Analysis of weaknesses and vulnerabilities of quantum cryptographic algorithm or method is used as a tool to assure the security level before a method is generally deployed. Some current vulnerabilities, inefficiencies, and weaknesses of the QC method are [116, 117].

1. There is no simple off-the-shelf optical source with controllable single photon rate generation and controllable photon polarization.
2. Optical fiber must maintain the polarization state of photons: manufactured fiber must comply with tight physical, optical, and mechanical specifications. However, variability of these specifications is real and so are attenuation, birefringence, dispersion, and dielectric nonlinearity that collectively affect the properties of propagating photons in the fiber.
3. As photons propagate in birefringent single-mode fiber, the polarization state of photons does not remain constant. In fact, polarization may gradually change state to state going through a full revolution within few meters of fiber, a distance known as *beat length*.
4. The fiber link in point-to-point links should remain intact and uniform without splices, connectors, and other optical components that may change the polarization state.
5. A not-perfectly coupled single photon source onto optical fiber: typical photonic power coupled onto fiber suffers from attenuation. There is no reason to believe that coupling a single photon source onto fiber will not suffer from loss which may result in photon loss and thus increased quBit Error Rate (qBER).
6. Optical fiber has absorption or scattering centers: at about 1,400 nm, absorption peaks due to OH-, below 1,300 nm and above 1,620 nm increases due to absorption and Rayleigh scattering. Currently, there is no zero-loss fiber in any part of the useful spectrum. In fact, to overcome this, researchers are thinking of quantum repeaters, that is, subsystems that will receive the polarized signal, restore its strength, and retransmit it. This of course may defeat the purpose of QKD because Evan can also have the same subsystem which with minor modifications can receive the signal, copy the polarized key, restore the polarization state of photons and retransmit it to Bob.
7. A very long random bit sequence is required to warranty a good encryption key. Because the two filters at each end of the fiber are randomly and independently polarized, the number of bits from

Alice's sequence that will pass through Bob's filter is fewer; it is those bits that constitute the encryption key. Thus, in order to warranty a relatively long encryption key (few hundred bits), very long sequences must be used.

8. No acknowledgment by Bob that the negotiated encryption key works reliably or correctly. Bob must know if his polarizing filter behaves as prescribed by Alice from the first arriving photon in the encrypted message. Deciding when the first photon arrives is a task of its own.
9. There is no mechanism to confirm that the key has been correctly constructed and that the encrypted message has been correctly received and decrypted. This identifies a potentially serious issue with QC robustness and a lack of verification. What if a malicious attacker affects one or the other polarizing filter? What if a malicious attacker adds propagation delay on the line so that filter synchronization is shifted by a bit period? Will Bob recognize it and reconstruct the message?
10. To date, only dedicated point-to-point QC and QKD solutions are contemplated, thus underutilizing the full bandwidth capacity of WDM. Only one experimental network contemplates a combined QKD (at 1,310 nm) and a channel in the DWDM C-band, thus not utilizing the complete potential of DWDM spectrum.
11. An eavesdropper may easily attack the transmitted polarization states on purpose. So far, the focus in QKD has been to prevent eavesdropping. However, it is equally important to prevent or countermeasure attacks. An attacker may tap the medium and maliciously destroy the QKD process and thus hamper transmission of the encrypted message. In such a case, an eavesdropper is not only a person who needs to "listen" but also one who hinders and deters successful communication between point A and point B; jamming is a well known form of communications deterrence.
12. If multiphoton bit transmission is contemplated, then a small part of the photonic pulse may be extracted from the fiber (by sophisticated tapping) and thus break the encrypted message (assuming that the sophisticated eavesdropper can also "listen" to the conversation between Adam and Bob).
13. If two entangled photons, A and B, have been separated, does photon A interact with a third photon, C, that emulates the polarization state of B? This is a key question in teleportation for secure communications. Current experiments supporting five-photon entanglement and photon-matter entanglement may find the important applications but may also prove that photon entanglement may not be such a secure method as we think.

Thus, if quantum cryptography would have to be applied on a practical optical network today, then Evan, a sophisticated malicious actor, who does not want to eavesdrop but to attack the ability of establishing secure communications, may accomplish this by altering the properties of the optical medium with very simple tools, such as by twisting the fiber, stretching the fiber, or even pinching the fiber with simple paperclips [118–120]. Doing so, it will perform the following:

- Change the propagation and polarization properties of photons in the fiber such that the polarization states transmitted by Alice arrive at Bob altered.
- Bob sends back to Alice an entirely inconsistent polarization pattern.
- Alice, not knowing what Evan has done, tests the received pattern that Bob sent her, finds the (erroneous) common bits, establishes a key but wrongly, and sends Bob the encrypted message using a wrong quantum key.
- Bob receives the cipher text but he cannot decipher it successfully.
- Although Alice and Bob realize that the security of the quantum channel has been compromised, secure communication has been disrupted. To continue with secure communication, Alice and Bob must try another fiber, which also may have been compromised.

Although the aforementioned steps may seem hypothetical, it is a simple, inexpensive, and reasonable scenario. In a simple simulated experiment, it has been confirmed that to alter the state of polarization is very simple, and all it takes is very small tensile or bending force on the fiber.

10.12 Countermeasures in Optical Networks

10.12.1 Classification of Security Networks Regarding Countermeasures

The speed and efficiency of any countermeasure strategy depend on its ability to monitor and detect fast fault and severe degradations, on its ability to discriminate between faults and degradation and malicious interventions and also on how fast a countermeasure strategy (if any) is executed [121, 122].

When Evan attacks the network (we assume that Evan attacks the link between Alice and Bob), his action is manifested as an inability to establish the quantum secret key (as already elaborated), or as a degradation of the signal performance as it is measured at Bob's station (when Evan is eavesdropping, he removes part of the optical power).

In general, there are three classifications of networks in regard to link security.

The first network classification detects and discriminates between faults and malicious interventions but it does not react to the intervention, other than sending an alarm to some management unit and discontinuing transporting encrypted data. We will call this *detection with alarm and discontinuing service* (DADS).

The second network classification detects and discriminates between faults and malicious interventions but it does not react to the intervention, other than sending an alarm to some management unit and continuing to transport encrypted data on the belief that the key is unbreakable anyway and that Evan in vain attempts to eavesdrop. We will call this *detection with alarm and continuous service* (DACS).

The third network classification detects and discriminates between faults and malicious interventions, it sends an alarm to some management unit, and it assumes that Evan is a sophisticated attacker and he should not be taken for granted. In this case, the network has a built countermeasure strategy that lets Evan to believe that the data captured by him is good, although the true encrypted data has been moved to another channel or even medium. We will call this *detection with alarm and countermeasure intelligence* (DACI).

In the remainder of this section, we examine the optical signal performance and how it can be used to discriminate between link faults, degradations, and malicious attacks.

10.12.2 Discriminating Between Faults and Attacks

In general, discriminating between faults or degradations and intrusion requires a network that monitors the signal performance continuously and in-service at each receiver [123, 124].

In optical communications, the factors that influence the signal performance are linear and non-linear:

- attenuation
- cross-talk
- dispersion and dispersion slope
- dispersion group delay (DGD)
- polarization mode dispersion (PMD)
- polarization dispersion loss (PDL)
- four-wave mixing (FWM)

- cross-phase modulation (XPM)
- self-phase modulation (SPM)
- modulation instability (MI)
- intersymbol interference (ISI)
- noise and jitter.

These factors are analytically known [125] for a particular link and channel, and the signal performance parameters form a vector that constitutes the channel signature ID [126].

How these parameters affect the signal performance is identified in Table 10.1 [127].

Thus, the key signal performance parameters that constitute the performance vector $P\{\mathbf{x}\}$ of an optical channel are Q-factor, BER, SNR, min–max power levels, noise factor, noise floor, ringing, and optionally skew, kurtosis, and jitter. During the link setup, the initial performance vector $P(\mathbf{x}, t_0)$ constitutes the signal signature or ID and its parameters are stored in the performance vector. Thereafter, any parameter change for whatever reason will affect $P(\mathbf{x}, t_0)$, or the channel ID. However, in order to be able to discriminate between an attack and a fault or degradation, it is necessary that the channel signature is monitored continuously. Then, the type and rate of change, Fig. 10.18, provide the forensics for root-cause analysis to discriminate between degradation, failure, or malicious attack. For example, ITU-T G 821 (1996) for digital transmission systems and for rates below the primary recommends performance thresholds as follows: BER performance is *acceptable* if it is better than 10^{-6} for more than 1 s, *degraded* if it is between 10^{-6} and 10^{-3} for any 1–s period, *severely errored* beyond that point and for 1 s, and *unavailable* if the severely errored performance persists for more than ten consecutive seconds.

In general, in order to distinguish between degradation/failure and intrusion, the following pragmatic assumptions need to be made (and the action to be taken):

- Component degradation is slow and so is the rate of performance change of one or more optical channels (we consider wavelength division multiplexing technology). It is detected by continuously monitoring the performance vector and performing time-base analysis; that is, compare current with previous performance vectors to determine the rate of change.
- Component failure is abrupt and it affects one or a group of optical channels causing permanent disruption of service to affected channels. It is detected by correlating reports from receivers and is localized by correlating reports from detectors strategically distributed on the link.
- Intrusion causes abrupt performance change in one or more channels but not disruption of service. Intrusion localization is accomplished by correlating reports from detectors at the receivers and detectors strategically located on the link.

Table 10.1 Parameters and their effect on signal performance

Parameter	Effect on signal
Optical signal power level	Reduces eye opening; increases SNR and BER
OCh center frequency deviation	Reduces eye opening; increases BER; increases cross-talk
OCh width (broadening)	Reduces eye opening; increases SNR and BER; increases cross-talk
OChs (spacing) separation	Reduces eye opening; increases BER (combined effects of items 2 and 3)
Dispersion (chromatic, polarization)	Eye closure due to chromatic dispersion; eye closure due to PMD-induced DGD; increases ISI, SNR, and BER
State of polarization instability	Increases BER; increases jitter/wander
Modulation depth (peak to valley)	Reduces eye opening; increases BER
Modulation stability (peak and valley)	Reduces eye opening; increases BER
Signal echo and singing	Adds to laser chirp, signal jitter, and noise
Dielectric (fiber) nonlinearity	Eye closure due to DGD caused by SPM, induces XPM, SPM, and FWM on multiplexed opt signals

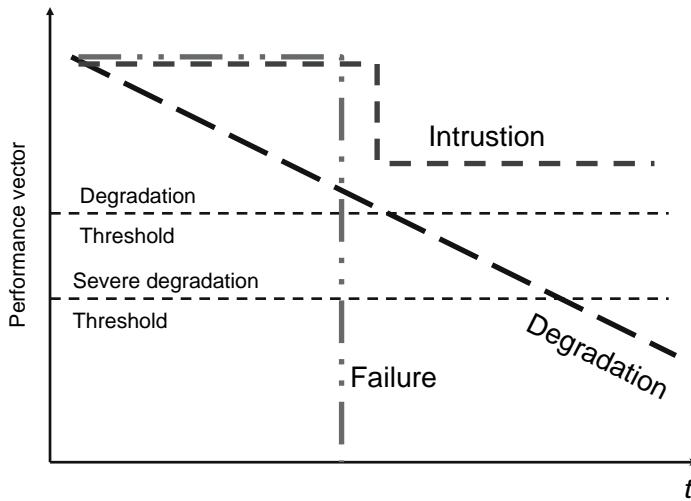


Fig. 10.18 Rate of performance vector change

10.12.3 Estimating the Performance Vector In-Service and in Real Time

Continuous in-service monitoring and detecting of the performance vector is critical in discriminating between faults, degradations, and attacks. Current methods are limited to estimating BER as part of the error detecting and correcting (EDC) mechanism that is embedded in data. However, this method may be considered slow because many frames are needed to estimate BER reliably. For example, at 10 Gbps and for an expected performance 10^{-15} BER, it may take up to 26 h or 1.7 min for 10^{-12} BER.

However, if the relatively new method of statistical performance estimation is used, then the performance vector is estimated in real time and in-service with simple integrated circuitry [128–130].

A complete treatise of the statistical estimation method is beyond the scope of this section as the method is analytically described in Ref. [128]. However, briefly this is described as follows.

The incoming optical signal is sampled and it is compared to a threshold level, Fig. 10.19. All samples are digitized and those that are greater than the threshold level are organized in one memory, whereas those that are less than the threshold are organized in a second memory. The organization of the digitized samples is such that two virtual statistical histograms are formed from which the standard deviations are evaluated, the Q-factor, BER, SR, noise factor, power levels, and so on. At optical data rates of 2.5–10 Gbps, histograms are formed in microseconds, and thus for all practical purposes, the performance vector is evaluated in real time and in-service since real data is used. These estimates are stored in registers to form the current performance vector and are compared with previously stored vectors to determine the rate of change, if any.

10.12.4 Detection with Alarm and Countermeasure Intelligence (Daci)

Networks that monitor the performance vector in-service and in real-time at each receiver of a node may also support an autonomous countermeasure mechanism. We describe a possible countermeasure strategy which is based on the following assumption:

The optical network supports WDM technology.

Optical links are full duplex (single, dual fiber, or quad-fiber).

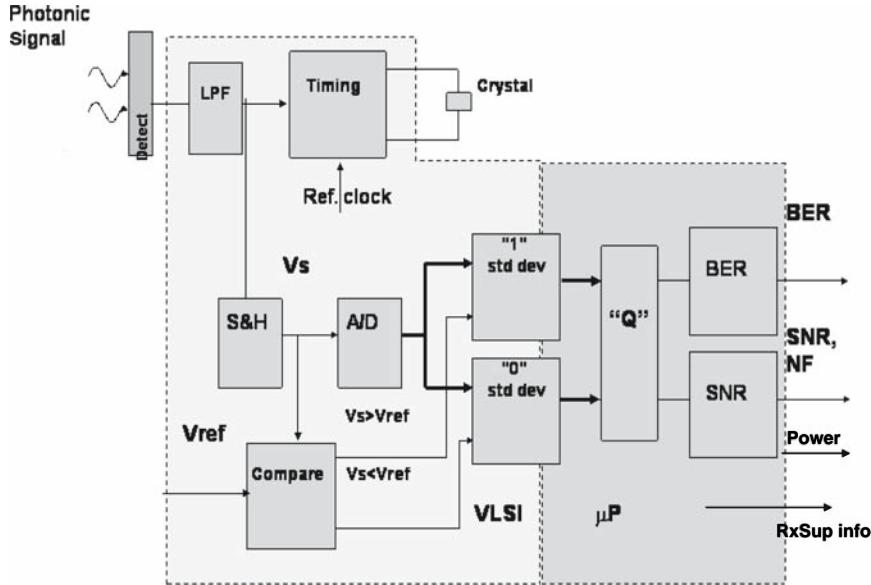


Fig. 10.19 Functional block diagram of the circuitry for performance vector estimation

Optical links include data channels and also an encrypted out-of-band (or optionally in band) supervisory channel; it can also be two supervisory, a working and a standby.

Each optical port includes a performance vector monitoring mechanism (as already described). Each port consists of a transmitter (laser), a receiver (photodetector and ancillary functional components), a performance vector monitoring circuitry (as already described), and a communication link to a management unit (on board or out of board).

Certain optical channels have been reserved for protection, which is common practice in telecommunications.

Based on the aforementioned assumption, one version of the full-duplex link should look like that in Fig. 10.20.

Based on the link shown in Fig. 10.20, the countermeasure strategy is follows:

Current performance vectors are compared with previous ones; if there is no difference or the difference remains above a lower acceptable level, then the channel performance is considered stable; this level has been predetermined by channel parametric fluctuation analysis, which is beyond the scope of this description. In this case, the receiver sends to the source over the supervisory channel a (“NO DIFF”) short control message indicating no performance difference, Fig. 10.21.

- If the difference is such that the channel is degrading and a degradation threshold is reached, then a control channel reassign request (“CHNL REASSIGN RQST”) message is sent to the source over the supervisory channel. The latter searches for available protection channels from the pool of reserved ones and it responds with a wavelength (re)assignment control message (“ λ -REASSIGN”) to the receiving end, while it moves traffic from the degraded to the newly reassigned wavelength. The receiving end assigns the newly assigned wavelength to the receiving port, and it starts monitoring the performance of the newly assigned channel and thus transmission continues with minimal or no traffic interruption. The same process is followed when a channel fails; in this case, the performance difference is a step function and the threshold is set much lower (close to the noise floor) than the degradation threshold.

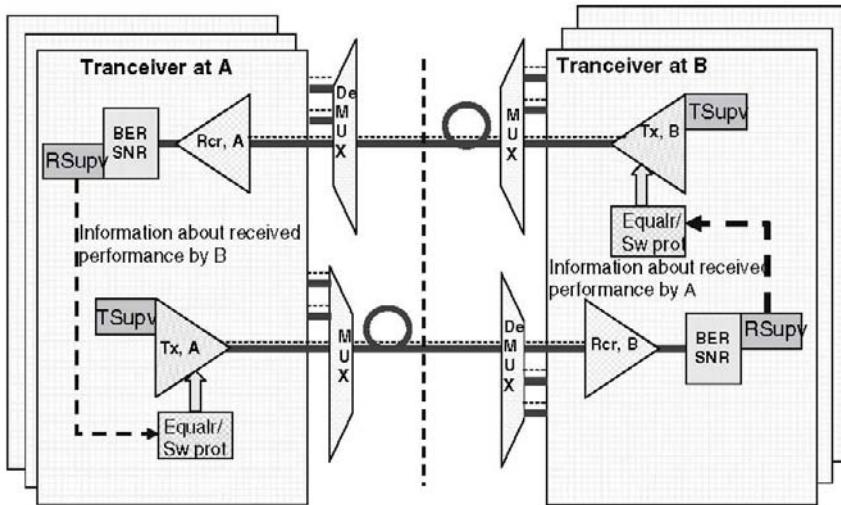


Fig. 10.20 A full-duplex link with performance vector estimation, channel protection, and link attack countermeasure

- If after the reassignment to protection degradation continues, the receiver sends another “CHNL REASSIGN RQST” and so on.
- If a second reassignment does not remediate the problem, then a link failure is declared by both the transmitting and the receiving ends.
- Conversely, if the transmitting end does not find any available wavelengths in the protection pool, then a “NO λ PROT AVAIL” control message is sent to the receiver, and in this case service continues even if it is degraded. In this case, the receiver continues monitoring the channel performance and keeps sending requests for new wavelength reassignment.

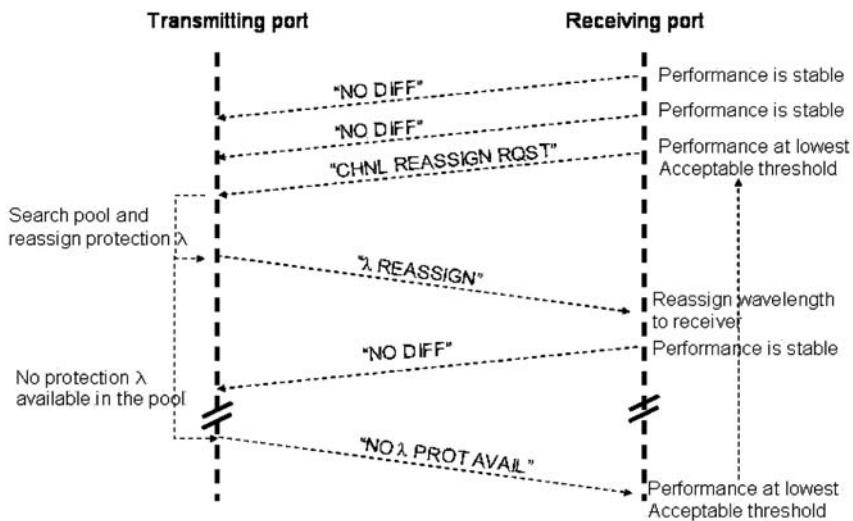


Fig. 10.21 Protocol for channel and link protection and countermeasure

In this model, when performance degradation has been identified at the port, the degradation threshold is set somewhat higher than the minimum acceptable performance in order to compensate

for protocol execution time during the channel reassignment. Thus, a *channel proactive reassignment algorithm* (CPRA) takes place that minimizes information (or packet) loss.

Because each WDM port acts autonomously, multiple channel degradations may take place simultaneously. Clearly, the number of channels that can be protected can be as many as the number of protection wavelengths reserved at the source. However, considering that currently there are up to 320 wavelengths in the C and L bands, then depending on application, one of the well-known protection strategy (1+1, M:N) may be adopted. In fact, combining this strategy with the channel proactive reassignment algorithm (CPRA), by a fast switch to protection is achieved.

Besides degradations and failures, the difference of the channel performance vector may reveal malicious attack on one or more channels. In such case, the algorithm for channel protection is the same with the addition of the following.

The receiver sends to the source a request for channel reassignment with continued service over the existing channel (“CHNL REASSIGN RQST+”). Based on this, service over the compromised channel continues, but data is neither sensitive nor proprietary, whereas the sensitive encrypted data passes over the newly assigned channel that only the source and destination know about. In this scenario, if channels keep being compromised, then the complete link may be declared compromised and under attack and traffic may be routed to another fiber, following a link protection strategy 1:1 or M:N.

10.13 Biometrics and Communication Networks

Biometrics is a technology that authenticates a person's identity (ID) when access to a building, a computational device, a network, a machine, a vehicle, and so on, is requested [131].

Biometrics has been addressed with rudimentary methods such as a photograph, a fingerprint, and a signature on an ID or passport. These methods however have been repeatedly defeated by masters of disguise and impostors, as it has been convincingly depicted in the movie “National Treasures”.

Currently, biometry is gaining popularity because of a dramatic increase of identity theft and unauthorized access and entry. Recent authentication methods rely on feature extraction from biometric data obtained from fingertip(s), palm, iris, face, voice, writing style, and also DNA.

In biometric applications, ID authentication may be *local* (open the door of a car, home, machine), with no authentication request over any network, short haul or long haul, or it may be *remote* (access to a corporate building and sections, access to a home supervised by a security entity, access to banking accounts, ATM machines, and so on). Local authentication is considered a narrow application and therefore it is not of concern in communication networks. In *remote* applications, however, biometric terminals entail end devices of the access communications network that is connected with the public or private network, Fig. 10.22.

There are two classifications in the remote biometric database:

- *Centralized* biometric database. The biometric apparatus extracts features which are transmitted over the network to a remote central database for comparison and verification. Results are sent back to the authenticating apparatus over the network to grant or deny access, Fig. 10.23. In this case, data to and from the central database must be encrypted and the network be secure from attacks.
- *Distributed* biometric database. A biometric apparatus requests authentication by a regional database which is periodically updated by a central database. The distributed database is faster than the centralized but it also increases the risk for attack.

As a consequence, identity authentication must consider not only the sophistication of the bio-

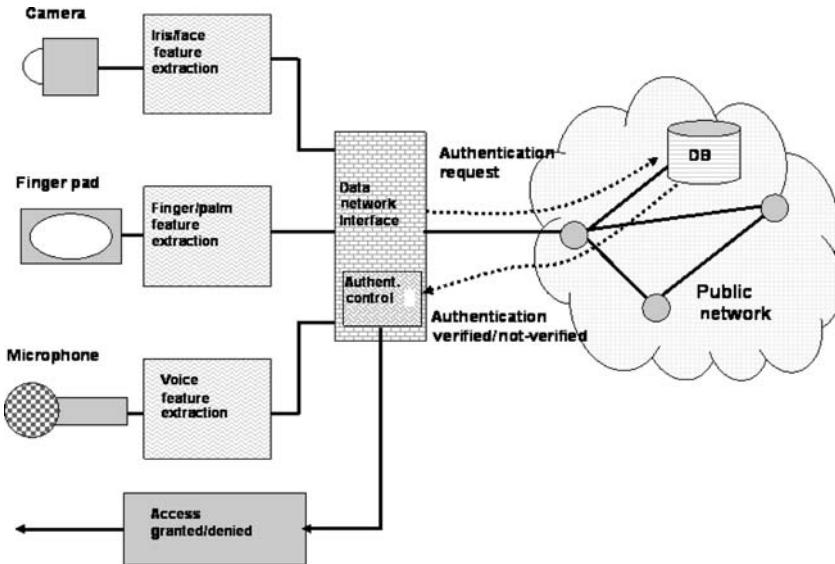


Fig. 10.22 Biometric devices are connected to the communications network to retrieve stored ID data for user authentication

metric method and the sophistication of the data encryption, but also the security of the network as the latter also presents many opportunities for attack, Fig. 10.23.

10.14 Security in the Next Generation Optical Networks

The wavelength division multiplex (WDM) next generation optical network transports a huge aggregate traffic (Tbps) per fiber [132]. The next generation optical network is based on the OTN standard protocol (most suitable for long-haul applications) [133–144] and on the next generation SONET/SDH protocol that includes link access procedure SDH (LAPS) [145, 146], the generic

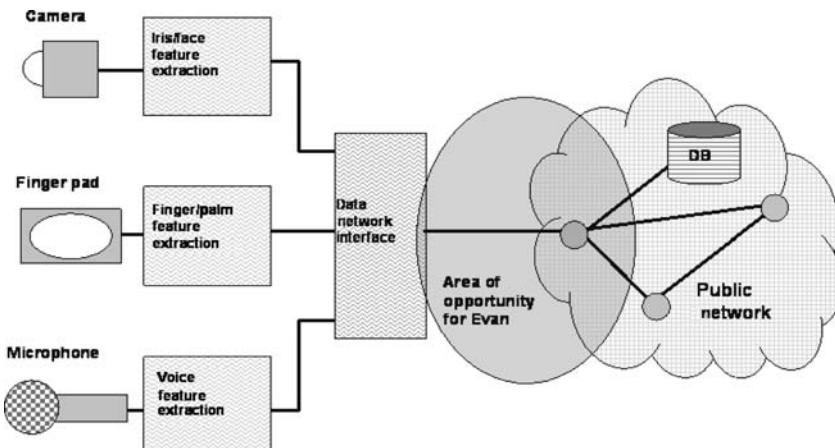


Fig. 10.23 A diverse range of protocols is defined over next generation SDH over WDM. The security layers are mapped on the adaptation and mapping process

framing procedure (GFP) [147–150], concatenation strategies (contiguous and virtual) according, the link capacity adjustment scheme (LCAS) [151, 152] with a suite of protocols mapped over GFP over next generation SONET/SDH over WDM, Fig. 10.24, and OTN over WDM, Fig. 10.25.

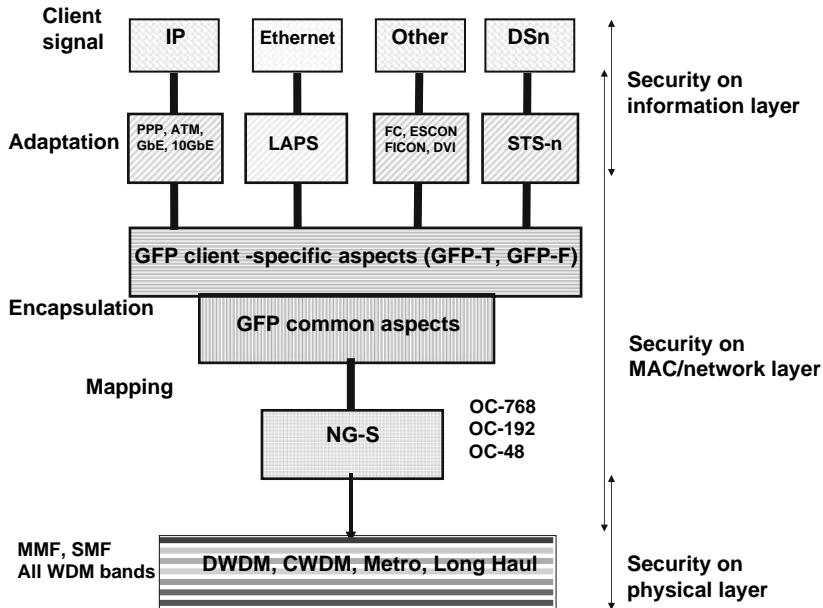


Fig. 10.24 A diverse range of protocols is defined over OTN over WDM. The security layers are mapped on the adaptation and mapping process

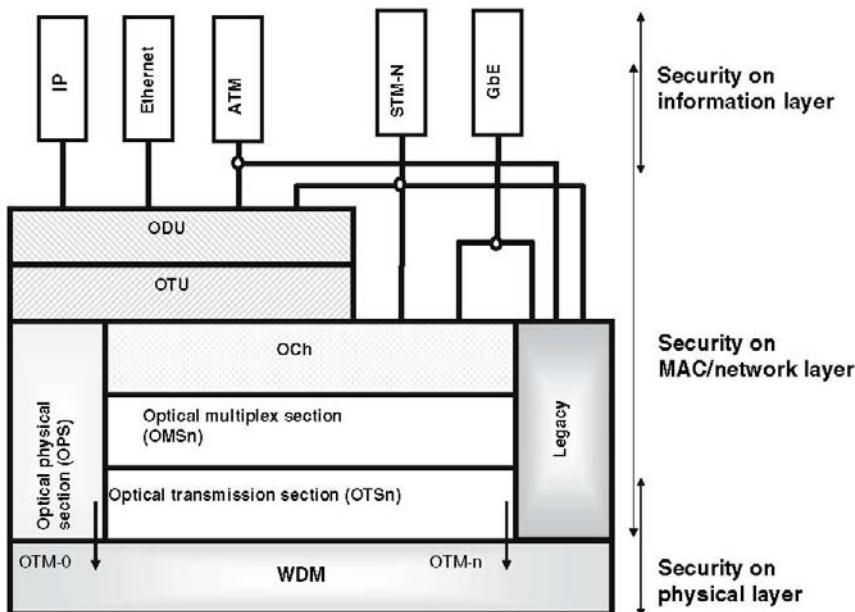


Fig. 10.25 A diverse range of protocols is defined over OTN over WDM. The security layers are mapped on the adaptation and mapping process

In addition, the telecommunications management network (TMN) assists network providers in providing flow control from distributed network elements to operations support systems. In all, the next generation optical network will be more cost-efficient, it will be better protected against failures and degradations, it will be scalable, it will better balance traffic avoiding congestion spots, it will better route traffic meeting real-time requirements, it will perform better to meet quality of signal and also quality of service, and it will provide user flexibility to define type of data (voice + high-speed data + one-way video + interactive video + other services), bandwidth elasticity, robustness, and security. It is possible that some data in encapsulated payload frames, such as Internet, may contain sophisticated viruses, but the fiber optic transmission medium and the all-optical network are not vulnerable to hidden viruses until they are electronically buffered. However, as the sophistication of the network increases, so is the sophistication of malicious attackers. Thus, an attacker may not attack via the payload space but via control messages, which are in packets in-line with data packets or over the Ethernet/Intranet network; control messages contain executables and perhaps text-like messages (i.e., the MAC/network layer described in this chapter). A malicious actor may also cause denial of service by affecting the fiber medium, as also described. An area of opportunity is also in the fiber to the premises (FTTP). Fiber to the enterprise and to the home may entice eavesdroppers as the average residential user may not have sophisticated encryption algorithms, and thus facilitate the malicious intentions of eavesdroppers.

Because of the huge aggregate traffic, good part of which is sensitive and confidential, malicious attackers are expected to attempt eavesdropping, mimicking the source, or cause denial of service.

A proposed WDM link layer security method uses multiple optical channels to transmit multiplexed payloads from various tributaries on the WDM; it has been called *wavelength bus*. Although the bit rate per channel on the medium is fixed, the data rate of each tributary can be at a different data rate. This allows client data rates from sub-wavelength rate to above wavelength rate. For example, an eight-channel wavelength bus with bit rate 10 Gbps per channel (or 80 Gbps capacity) can accept tributaries at under Gbps to up to 80 Gbps [153, 154], Fig. 10.26a and b.

In DWDM, the fiber is a transporting medium of a large number of channels, which for practical and economic reasons are modulated at the same rate. Thus, each data channel acts upon an optical

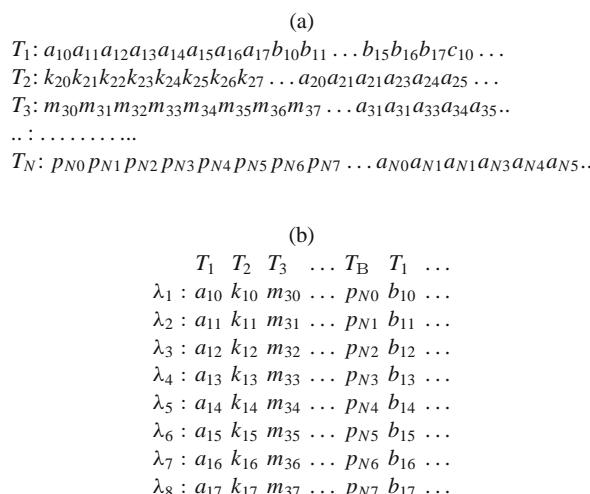


Fig. 10.26 (a) Serial tributaries T_1 to T_N may be at different data rates. (b) Tributaries T_1 to T_N are serialized and byte multiplexed

modulator to generate an optical serial bit stream, each stream at different wavelength; for simplicity of description, consider a group of eight streams, λ_1 to λ_8 , onto a fiber as follows:

Moreover, the wavelength bus has excellent link layer security features that may remind an expanded DNA code structure [155]. Research has indicated that an optical link based on the WDM wavelength bus is secured by multiple methods, three of which are

- the multiplexer random scheduler
- the temporal wavelength-bus randomizer
- the hybrid method.

The security encryption mechanism that can be employed is visualized in Fig. 10.27. For 4,294,967,296 permutations or more, an eavesdropper will have to process trillions of bytes due to the randomizer alone; this requires a *supercomputer with execution time in the sub-picosecond regime!*

In conclusion, security in the next generation communication networks that consists of many communication technologies over a path is of extreme importance, Fig. 10.28. It has become apparent that in addition to end-to-end encryption algorithms and network management security, it is necessary to secure optical links so that eavesdroppers tapping the light stream from a fiber are unable to decipher, mimic information, or cause denial of service. In conclusion, in order to be able to combat the potential attacker, the next generation network must adopt cryptographic strategies that are robust for a highly sophisticated and adaptable attacker, it should be able to discriminate between failures/degradations and attacks, and it must include fast countermeasure strategies. Is quantum cryptography and quantum key distribution the “Holy Grail” of cryptography? Time will show; whichever method is employed must be intelligently adaptable, pragmatic, and affordable.

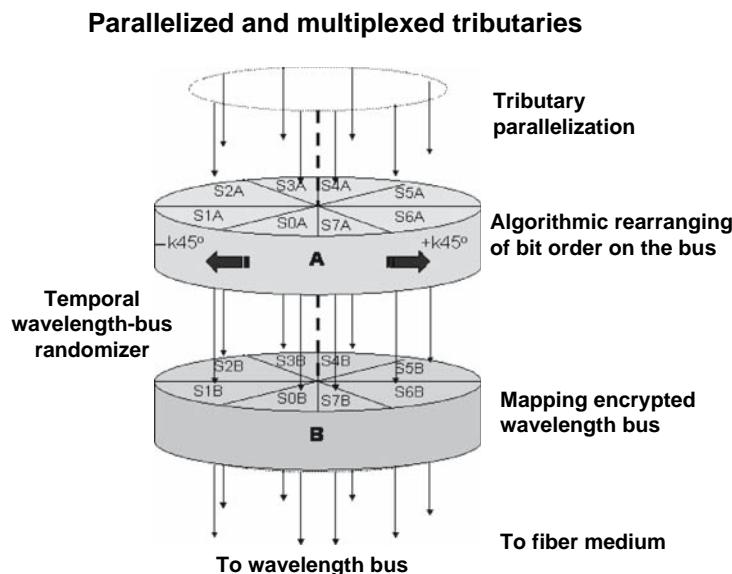


Fig. 10.27 Parallelized and byte-multiplexed tributaries are encrypted in the time domain according to an encrypted algorithm

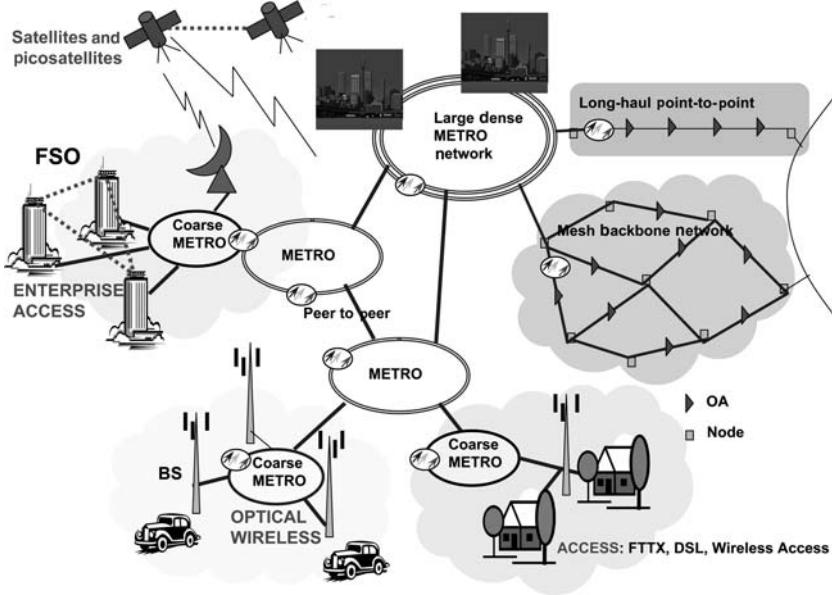


Fig. 10.28 The diverse range of communication technologies presents a variety of opportunities to malicious actors.

References

1. Aeschylus, *Agamemnon*, Loeb Classical Library.
2. Polybius, *Histories*, Book X, Loeb Classical Library.
3. Xenophon, *Anabasis*, Loeb Classical Library.
4. D. Kahn, “Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939-1943”, 1991.
5. A. Stripp, “The Enigma Machine: Its Mechanism and Use”, in *Codebreakers: The Inside Story of Bletchley Park*, F.H. Hinsley and A. Stripp eds. pp. 83–88, Oxford University Press, 1993.
6. S.V. Kartalopoulos, “A Primer on Cryptography in Communications”, *IEEE Communications Magazine*, vol. 44, no. 4, 2006, pp. 146–151.
7. S.V. Kartalopoulos, *Understanding SONET/SDH and ATM*, IEEE Press, 1999; also Prentice Hall of India.
8. S.V. Kartalopoulos, *Introduction to DWDM Technology: Data in a Rainbow*, Wiley/IEEE Press, 2000; published also in India and China.
9. FIPS Pub 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 28, 1994.
10. FIPS Pub 196, *Entity Authentication Using Public Key Cryptography*, February 1997.
11. FIPS Pub 198, The Keyed-Hash Message Authentication Code (HMAC), March 2002.
12. FIPS Pub 185, Escrowed Encryption Standard, February 9, 1994.
13. FIPS Pub 186-2, *Digital Signature Standard*, January 2000.
14. FIPS Pub 186-2 change notice, *Digital Signature Standard*, October 2001.
15. FIPS 180-2, *Secure Hash Standard (SHS)*, August 2002.
16. FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, 2002.
17. FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, Annex A: Approved Security Functions, Draft, 2005.
18. FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, Annex B: Approved Protection Profiles, Draft, 2004.
19. FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, Annex C: Approved Random Number Generators, Draft, 2005.
20. FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, Annex D: Approved Key Establishment Techniques, Draft, 2005.
21. R.K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, New York, 2004.
22. R. Crandall and C. Pomerance, *Prime Numbers*, Springer, New York, 2001.
23. Bill Gates, *Road Ahead*, 1995, Viking Publishers, p. 265.

24. P. Ribenboim, "Twin Primes" § 4.3 in *The New Book of Prime Number Records*, Springer, New York. 1996, pp. 259–265.
25. FIPS Pub 46-3, *Data Encryption Standard (DES)*, October 25, 1999.
26. FIPS 197, *Advanced Encryption Standard*, November 26, 2001,
27. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
28. <http://csrc.nist.gov/encryption/aes//rijndael/Rijndael.pdf>.
29. W. Diffie and M.E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, vol. 13, November 1967, pp. 644–654.
30. S. Wiesner, "Conjugate Coding", *Sigact News*, vol. 15, no. 1, 1983, pp. 78–88; (original manuscript written circa 1970), 31.
31. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography", *Journal of Cryptology*, vol. 5, no. 1, 1992, pp. 3–28. Preliminary version in Advances in Cryptology—Eurocrypt '90 Proceedings, May 1990, Springer, pp. 253–265.
32. C.H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical Quantum Oblivious Transfer", Advances in Cryptology|Crypto '91 Proceedings, August 1991, Springer, pp. 351–366.
33. G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, "A Quantum Bit Commitment Scheme Probably Unbreakable by Both Parties", *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, November 1993, pp. 362–371.
34. A.C. Phillips, *Introduction to Quantum Mechanics*, Wiley.
35. J. Gruska, *Quantum Computing*, McGraw-Hill, London, 1999.
36. C.H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical Quantum Oblivious Transfer", Advances in Cryptology|Crypto '91 Proceedings, August 1991, Springer, pp. 351–366.
37. G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, "A Quantum Bit Commitment Scheme Provably Unbreakable by Both Parties", *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, November 1993, pp. 362–371.
38. H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs Classical Communication and Computation", ACM Press, *Proceedings of the 30th Annual ACM Symposium on the Theory of Computation*, El Paso, 1998, pp. 63–88.
39. D. Deutch, "Quantum Computational Networks", *Proceedings of the Royal Society of London A*, vol. 425, 1989, pp. 73–90.
40. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography", *Review of Modern Physics*, vol. 74, 2002, pp. 145–195.
41. S. Kartalopoulos, "All-Optical XOR Gate for Quantum Ciphertext in Optical Communications", Proceedings of SPIE Defense and Security, September 26–29, 2005, Bruges, Belgium, paper no 5989A-14, on CD-ROM: CDS191.
42. S. Kartalopoulos, "Cascadable All-Optical XOR Gates for Optical Ciphertext and Parity Calculations", Proceedings of SPIE Optics and Optoelectronics 2007, April 16–20, 2007, Prague, Chech Rep., on CD-ROM, vol. 6581–6588.
43. A. Shamir, How to Share a Secret, *Communications of the ACM*, vol. 22, no. 11, 1979, pp. 612–613.
44. W. Diffie and M.E. Hellman, "New directions in Cryptography", *IEEE Transactions on Information Theory*, vol. IT-22, 1976, pp. 644–654.
45. N. Koblitz, Elliptic Curves Cryptosystems. *Mathematics of Computation*, vol. 48, 1987, pp. 203–209.
46. V.S. Miller, "Uses of Elliptic Curves in Cryptography", Advances in Cryptology CRYPTO'85, Lecture Notes in Computer Science, vol. 218, Springer, 1986, pp. 417–426.
47. N. Koblitz, *Introduction to Elliptic Curves and Modular Forms. Graduate Texts in Mathematics*, No. 97, 2nd ed., Springer, New York, 1993.
48. N. Koblitz, *Algebraic Aspects of Cryptography, Algorithms and Computation in Mathematics*, vol. 3, Springer, New York, 1998.
49. D. Hankerson, A. Menezes, and S.A. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2004.
50. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society 265, Cambridge University Press, 1999.
51. Blake, G. Seroussi, and N. Smart, (ed.), *Advances in Elliptic Curve Cryptography*, London Mathematical Society 317, Cambridge University Press, 2005.
52. L. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman & Hall/CRC, 2003.
53. N. Koblitz, A. Menezes, and S. Vanstone, "The State of Elliptic Curve Cryptography", *Design, Codes and Cryptography*, vol. 18, 2000, pp. 173–193.
54. A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer, 1993.
55. A. Menezes, *Elliptic Curve Cryptosystems*, CryptoBytes, vol.1, no.2, Summer 1995.

56. V. Mueller, A. Stein, and C. Thiel, “Computing Discrete Logarithms in Real Quadratic Congruence Function Fields of Large Genus”, *Mathematics of Computation*, vol. 68, 1999, pp. 807–822.
57. I. Biehl, B. Meyer, and V. Müller, “Differential Fault Analysis on Elliptic Curve Cryptosystems”, *Advances in Cryptology—CRYPTO 2000*, Lecture Notes in Computer Science 1880, pp. 131–146.
58. C. Lim and P. Lee, “A Key Recovery Attack on Discrete Log-Based Schemes Using a Prime Order Subgroup”, *Advances in Cryptology—CRYPTO 97*, Lecture Notes in Computer Science 1294, pp. 249–263.
59. N. Demytko, A New Elliptic Curve Based Analogue of RSA, *Advances in Cryptology*, Eurocrypt’93, pp. 40–49, Springer, 1994.
60. H.W. Lenstra, Jr. Factoring Integers with Elliptic Curves. *Annals of Mathematics*, vol. 126, 1987, pp. 649–673.
61. A. Menezes, T. Okamoto, and S.A. Vanstone. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pp. 80–89, ACM, 1991.
62. V.S. Miller, Use of Elliptic Curve in Cryptography, *Advances in Cryptology*, Crypto’85, pp. 417–426, Springer, 1986.
63. P. Fahn and M.J.B. Robshaw. Results from the RSA Factoring Challenge. Technical Report TR-501, version 1.3, RSA Laboratories, January 1995.
64. R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, *Communications of the ACM*, vol. 21, no. 2, February 1978, pp. 120–126.
65. T. ElGamal. “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, *IEEE Transactions on Information Theory*, vol. IT-31, 1985, pp. 469–472.
66. FIPS PUB 186: *Digital Signature Standard*, May 19, 1994.
67. C.H. Bennett, and G. Brassard, “An Update on Quantum Cryptography”, *Advances in Cryptology: Proceedings of Crypto 84*, August 1984, Springer, pp. 475–480.
68. I. Stewart, “Schrodinger’s Catflap”, *Nature*, vol. 353, October 3, 1991, pp. 384–385.
69. C. Crépeau, “Cryptographic Primitives and Quantum Theory”, *Proceedings of Workshop on Physics and Computation*, PhysComp 92, Dallas, October 1992, pp. 200–204.
70. P. Wallich, “Quantum Cryptography”, *Scientific American*, May 1989, pp. 28–30.
71. C.H. Bennett, “Quantum Cryptography: Uncertainty in the Service of Privacy”, *Science*, vol. 257, August 7, 1992, pp. 752–753.
72. R. Clifton, J. Bud, and H. Halvorson, “Characterizing Quantum Theory in Terms of Information-Theoretic Constraints” *Foundations of Physics*, vol. 33, 2003, pp. 1561–1591.
73. M.A. Nielsen, I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
74. C.H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, “Practical Quantum Oblivious Transfer”, *Advances in Cryptology|Crypto ’91 Proceedings*, August 1991, Springer, pp. 351–366.
75. G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois, “A Quantum Bit Commitment Scheme Provably Unbreakable by Both Parties”, *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, November 1993, pp. 362–371.
76. S. Wiesner, “Conjugate Coding”, *Sigact News*, vol. 15, no. 1, 1983, pp. 78–88; original manuscript written circa 1970.
77. A.K. Ekert, “Quantum Cryptography based on Bell’s Theorem”, *Physical Review Letters*, vol. 67, no. 6, August 5, 1991, pp. 661–663.
78. P.D. Townsend and I. Thompson, “A Quantum Key Distribution Channel Based on Optical Fibre”, *Journal of Modern Optics*, vol 41, no 12, December 1994, pp. 2425–2434.
79. S.V. Kartalopoulos, *DWDM: Networks, Devices and Technology*, IEEE/Wiley, 2003.
80. C.H. Bennett, “Quantum Cryptography Using Any Two Nonorthogonal States”, *Physical Review Letters*, vol. 68, no. 21, May 25, 1992, pp. 3121–2124.
81. A. Muller, J. Breguet, and N. Gisin, “Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over more than 1 km” *Europhysics Letters*, vol. 23, no. 6, August 20, 1993, pp. 383–388.
82. C.H. Bennett and G. Brassard, “Quantum Cryptography: Public-Key Distribution and Coin Tossing”, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, pp. 175–179, and also “Quantum Public Key Distribution System”, *IBM Technical Disclosure Bulletin*, vol. 28, no. 7, December 1985, pp. 3153–3163.
83. J.D. Franson and H. Ilves, “Quantum Cryptography Using Polarization Feedback”, *Journal of Modern Optics*, vol 41, no 12, December 1994, pp. 2391–2396.
84. B. Huttner and A. Peres, “Quantum Cryptography with Photon Pairs”, *Journal of Modern Optics*, vol 41, no 12, December 1994, pp. 2397–2404.
85. A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma, “Practical Quantum Cryptography Based on Two-Photon Interferometry”, *Physical Review Letters*, vol. 69, no. 9, 31 August 1992, pp. 1293–1295.

86. S.M. Barnett, B. Huttner, and S.J.D. Phoenix, "Eavesdropping Strategies and Rejected-Data Protocols in Quantum Cryptography", *Journal of Modern Optics*, vol. 40, no. 12, December 1993, pp. 2501–2513.
87. D. Deutsch, "Quantum Communication Thwarts Eavesdroppers", *New Scientist*, December 9, 1989, pp. 25–26.
88. G.P. Collins, "Quantum Cryptography Defies Eavesdropping", *Physics Today*, November 1992, pp. 21–23.
89. A.K. Ekert, "Quantum Keys for Keeping Secrets", *New Scientist*, 16, January 1993, pp. 24–28.
90. P.D. Townsend and S.J.D. Phoenix, "Quantum Mechanics Will Protect Area Networks", *Opto and Laser Europe*, July 1993, pp. 17–20.
91. C.H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, "Eavesdrop-Detecting Quantum Communications Channel", *IBM Technical Disclosure Bulletin*, vol. 26, no. 8, January 1984, pp. 4363–4366.
92. S.V. Kartalopoulos, "Is Optical Quantum Cryptography the 'Holy Grail' of secure communication?", *SPIE Newsroom Magazine*, April 2006, available at <http://newsroom.spie.org/x2260.xml?highlight=x537>.
93. J.G. Rarity, P.C.M. Owens, and P.R. Tapster, "Quantum Random Number Generation and Key Sharing", *Journal of Modern Optics*, vol. 41, no. 12, December 1994, pp. 2435–2444.
94. E. Schroedinger, "Discussion of Probability Relations Between Separated Systems", *Proceedings of the Cambridge Philosophical Society*, vol. 31, 1935, pp. 555–563.
95. E. Schroedinger, "Discussion of Probability Relations Between Separated Systems", *Proceedings of the Cambridge Philosophical Society*, vol. 32, 1936, pp. 446–451.
96. A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality be considered complete?", *Physical Review*, vol. 47, 1935, pp. 777–780. Reprinted in *Quantum Theory and Measurement* (J.A. Wheeler and W.Z. Zurek, eds.), Princeton University Press, 1983.
97. J.S. Bell, "On the Einstein–Podolsky–Rosen Paradox", *Physics*, vol. 1, 1964, pp. 195–200.
98. J.F. Sherson, H. Krauter, R.K. Olsson, B. Julsgaard, K. Hammerer, I. Cirac, and E.S. Polzik, "Quantum Teleportation Between Light and Matter", *Nature*, vol. 443, October 5, 2006, pp. 557–560.
99. C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, *Teleporting an Unknown Quantum State via Dual Classical and Einstein–Podolsky–Rosen Channels*, *Physics Review Letters*, vol. 70, 1993, pp. 1895–1899.
100. G. Brassard, S. Braunstein, and R. Cleve, *Teleportation as a Quantum Computation*, *Physica D* vol. 120, 1998, pp. 43–47.
101. G. Rigolin, *Quantum Teleportation of an Arbitrary Two Qubit State and Its Relation to Multipartite Entanglement*, *Phys. Rev. A*, vol. 71, 2005, 032303.
102. L. Vaidman, *Teleportation of Quantum States*, *Physics Review A*, 1994.
103. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental Quantum Teleportation", *Nature* vol. 390, 6660, 1997, pp. 575–579.
104. D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, "Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein–Podolsky–Rosen channels", *Physics Review Letters*, 80, 6, 1998, pp. 1121–1125.
105. I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, "Long-Distance Teleportation of Qubits at Telecommunication Wavelengths", *Nature*, vol. 421, 2003, p. 509.
106. R. Ursin et al., "Quantum Teleportation Link Across the Danube", *Nature*, vol. 430, 2004, p. 849.
107. D. Gottesman and I. Chuang, "Teleportation as a Computational Primitive", *Nature*, vol. 402, 1999, pp. 390–393.
108. L. Vaidman, Using Teleportation to Measure Nonlocal Variables, [quant-ph/0111124](#).
109. Thomas D. Angelidis, "On the Problem of a Local Extension of the Quantum Formalism", *Journal of Mathematical Physics*, vol. 34, 1993, p. 1635.
110. Thomas D. Angelidis, "A Minimal Local Extension of the Quantum Formalism" in *Causality and Locality in Modern Physics*, Kluwer, 1998, pp. 451–462.
111. Alain Aspect et al., "Experimental Tests of Bell's Inequalities Using Time-Varying Analyzers", *Physics Review Letters*, vol. 49, 1982, pp. 1804–1807.
112. John Bell, *Speakable and Unspeakable in Quantum Mechanics* (collected papers on quantum philosophy), Cambridge University Press, 1987.
113. Mark Buchanan, "Quantum Teleportation", *New Scientist*, March 14, 1998.
114. A. Poppe et al., "Practical Quantum Key Distribution with Polarization Entangled Photons", *Optics Express*, vol. 12, no. 16, 2004, pp. 3865–3871.
115. <http://arxiv.org/archive/quant-ph>. This is an excellent archive of published quantum related papers.
116. D.R. Kuhn, "Vulnerabilities in Quantum Key Distribution Protocols", [quant-ph/0305076](#), May 12, 2003.
117. S.V. Kartalopoulos, "Link-Layer Vulnerabilities of Quantum Cryptography", SPIE International Congress on Optics and Optoelectronics, Warsaw, Poland, August 28, 2005 to September 2, 2005, *Proceedings of SPIE*, vol. 5954, pp. 5954OH-1 to 5954OH-7.
118. S.V. Kartalopoulos, "Identifying Vulnerabilities of Quantum Cryptography in Secure Optical Data Transport", *Unclassified Proceedings of Milcom 2005*, October 17–20, 2005, Atlantic City, session: Comm. Security I, invited paper # 678, on CD-ROM, ISBN # 0-7803-9394-5.

119. S.V. Kartalopoulos, "Secure Optical Links in the Next-Generation DWDM Optical Networks", *WSEAS Transactions on Communications*, vol. 3, no. 2 April 2004, pp. 456–459 (ISSN 1109–2742). Also, presented at ICCC'04, WSEAS 8th International Conference on Communications and Computers, International Workshop on Cryptography, Vouliagmeni, Athens, Greece, July 12–15, 2004.
120. S.V. Kartalopoulos, "Optical Network Security: Sensing Eavesdropper Intervention", *Globecom 2006*, San Francisco.
121. S.V. Kartalopoulos, "Optical Network Security: Countermeasures in View of Channel Attacks", Unclassified Proceedings of Milcom 2006, October 23–25, 2006, Washington, DC, on CD-ROM, ISBN 1-4244-0618-8, Library of Congress 2006931712, paper no. US-T-G-404.
122. S.V. Kartalopoulos, "Optical Network Security: Countermeasures in View of Attacks", Proceedings of SPIE European Symposium on Optics and Photonics in Security and Defense, Stockholm, Sweden, September 11–16, 2006, on CD-ROM, paper no. 6402-9; also in SPIE Digital Library at <http://spiedl.org>
123. S.V. Kartalopoulos, "Per-Port Circuit for Statistical Estimation of Bit Error Rate and Optical Signal to Noise Ratio in DWDM Telecommunications", *Proceedings of the SPIE Conference on Fluctuation and Noise*, May 25–28, Las Palmas, Gran Canaria, Spain, 2004, pp. 131–141.
124. S.V. Kartalopoulos, "Distinguishing Between Network Intrusion and Component Degradations in Optical Systems and Networks", *WSEAS Transactions on Communications*, vol. 4, no. 9, September 2005, pp. 1154–1161.
125. S.V. Kartalopoulos, "Factors Affecting the Signal Quality, and Eye-Diagram Estimation Method for BER and SNR in Optical Data Transmission", *Proceedings of the International Conference on Information Technology*, ITCC-2004, Las Vegas, April 5–7, 2004, pp. 615–619.
126. S.V. Kartalopoulos, "Optical Network Security: Channel Signature ID", Unclassified Proceedings of Milcom 2006, October 23–25, 2006, Washington, DC, on CD-ROM, ISBN 1-4244-0618-8, Library of Congress 2006931712, paper no. US-T-G-403.
127. S.V. Kartalopoulos, *Fault Detectability in DWDM: Towards Higher Signal Quality and Network Reliability*, IEEE Press, New York, NY, 2001.
128. S.V. Kartalopoulos, *Optical Bit Error Rate*, IEEE Press/Wiley, New York, NY, 2004.
129. D. Marcuse, "Derivation of Analytical Expressions for the Bit-Error Probability in Lightwave Systems with Optical Amplifiers", *Journal of Lightwave Technology*, vol. 8, no. 12, 1990, pp. 1816–1823.
130. M.D. Knowles and A.I. Drukarev, "Bit Error Rate Estimation for Channels with Memory", *IEEE Transactions on Communications*, vol. 36, no. 6, 1988, pp. 767–769.
131. S.V. Kartalopoulos, "Communications Security: Biometrics over Communications Networks", *Proceedings of IEEE Globecom 2006 Conference*, San Francisco, CA.
132. S.V. Kartalopoulos, *Next Generation SONET/SDH*, IEEE Press/Wiley, New York, NY, 2004.
133. ITU-T Recommendation G.709/Y.1331, "Interfaces for the Optical Transport Network (OTN)", February 2001.
134. ITU-T Recommendation G.709/Y.1331, "Interfaces for the Optical Transport Network (OTN), Amendment 1", February 2001.
135. ITU-T Recommendation G.709/Y.1331, Amendment 1, "Amendment 1", November 2001.
136. ITU-T Draft Recommendation G.798, "Characteristics of Optical Transport Networks (OTN) Equipment Functional Blocks", October 1998.
137. ITU-T Recommendation G.805, "Generic Functional Architecture of Transport Networks", October 1998.
138. ITU-T Recommendation G.872, "Architecture of Optical Transport Networks", November 2001.
139. ITU-T Draft Recommendation G.873, "Optical Transport Network Requirements", October 1998.
140. ITU-T Draft Recommendation G.874, "Management Aspects of the Optical Transport Network Element", October 1998.
141. ITU-T Draft Recommendation G.875, "Optical Transport Network Management Information Model for the Network Element View", October 1998.
142. ITU-T Recommendation G.957, "Optical Interfaces for Equipments and Systems Relating to the Synchronous Digital Hierarchy", 1995.
143. ITU-T Draft Recommendation G.959, "Optical Networking Physical Layer Interfaces", February 1999.
144. ITU-T Recommendation G.8251, "The Control of Jitter and Wander Within the Optical Transport Network (OTN)", November 2001.
145. ITU-T Recommendation X.85/Y.1321, "IP over SDH Using LAPS", March 2001.
146. ITU-T Recommendation X.86, "Ethernet over LAPS", February 2001.
147. ITU-T Recommendation G.7041/Y.1303, "The Generic Framing Procedure (GFP) Framed and Transparent", December 2001.
148. E. Hernandez-Valencia, M. Scholten, and Z. Zhu, "The Generic Framing Procedure (GFP): An Overview", *IEEE Communications Magazine*, vol. 40, no. 5, May 2002, pp. 63–71.

149. E. Hernandez-Valencia, "Generic Framing Procedure (GFP): A Next-Generation Transport Protocol for High-Speed Data Networks", *Optical Networks Magazine*, vol. 4, no. 1, January/February 2003, pp. 59–69.
150. M. Scholten, Z. Zhu, E. Hernandez-Valencia, and J. Hawkins, "Data Transport Applications Using GFP", *IEEE Communications Magazine*, vol. 40, no. 5, May 2002, pp. 96–103.
151. ITU-T Recommendation G.7042/Y.1305, "Link Capacity Adjustment Scheme (LCAS) for Virtual Concatenated Signals", November 2001.
152. ITU-T Recommendation X.86/Y.1323, Amendment 1, "Ethernet over LAPS, Amendment 1: Using Ethernet Flow Control as Rate Limiting", April 2002.
153. S.V. Kartalopoulos, "Bandwidth Elasticity with DWDM Parallel Wavelength-Bus in Optical Networks", *SPIE Optical Engineering*, vol. 43, no. 5, May 2004, pp. 1092–1100.
154. S.V. Kartalopoulos, "Parallel WDM Transmission for Ultra-high Bandwidth Remote Computer Communication", *WSEAS Transactions on Communications*, vol. 1, no. 1 July 2004, pp. 99–102, (ISSN 1790-0832).
155. S.V. Kartalopoulos, "DNA-Inspired Cryptographic Methods in Optical Communications, Source Authentication and Data Mimicking", Unclassified Proceedings of Milcom 2005, October 17–20, 2005, Atlantic City, session: Comm. Security II, invited paper # 1470, on CD-ROM, ISBN # 0-7803-9394-5.

Chapter 11

Concluding Remarks

11.1 Bandwidth Evolution

The optical network of the 1980s evolved at an amazing rate from 2.5 Gbps per fiber, in just two decades, to few terabits, that is, 1,000-fold. Interestingly, it took about two decades before that to evolve from a 1,000-fold to 2.5 Gbps (from copper to fiber). If this evolution establishes a trend, then one can expect in another two decades to have petabits.

The 1990s witnessed an overdeployment of fiber as a large percent of fiber installed was dark; that is, it was never used or laser light did not pass through it (hence, it was never lit). This was the result of an access bottleneck; the access was still out of traffic balance compared with the DWDM backbone. However, with the evolution of wireless networks and their migration from analog to digital transmission (and thus higher bandwidth) in conjunction with new services that stimulated traffic increase and smart marketing approaches that put a wireless phone in every pocket, the percent of dark fiber started getting smaller. With the addition of xDSL technology that delivers hundreds of kilobits or few megabits to the home, and fiber in the access network (FTTP) will deliver megabits to gigabits, so that remaining dark fiber will soon be, lit in which case the optical backbone network may find itself short of bandwidth again. Having fiber to the premises will flood the main network with all traffic types, voice, Ethernet, Internet, video, interactive video, text, games, music, and so on. This is an issue to be addressed, research for which is on going for the last 20 years.

11.2 Convergence

Convergence is a term that has existed in the communications industry for more than a decade. However, because in an environment in which end users require personalized communications experiences (i.e., a personalized multiplay that meets their own needs and with more customer data control), the current business models are redefined, and the communications boundaries become blurry because of an interplay of technologies to enable the multiplay needed by the end user.

As a result, convergence currently means different things. There is convergence of technologies, devices, services, and networks. For example:

- Technology convergence integrates electronic, opto-electronic, photonic, optical and wireless technologies in a single device.
- Currently, there is a multitude of communications devices or gadgets targeted for business, communications, entertainment (music and video), text composition, messaging (short messaging and e-mail), and so on. Device convergence brings all that in a single miniaturized device.
- Service convergence allows for various fundamentally different applications to coexist on the same communications platform as well as devices so that all types of payload and data protocols (synchronous, video, data, IP, Ethernet, etc.) will be able to be transported by a single network.

- Network convergence indicates that a single intelligent network, which combines the goodness of both switched and packet routing networks, harnesses the interplay of diverse technologies, fundamentally heterogeneous payloads, and different standards to offer the value-added services requested by the end user or the customer.

11.3 Why Do Not I Have Fiber to My Home?

Despite the technological advancements and the defined protocols, the question still exists: Why do not I have fiber to my home? And, why xDSL is not better affordable?

These are good questions, but their answers are not technical based; a huge investment is already made, and there is no rush to replace it with another network. However, the network diversity that exists today eventually will catch up with the maintenance cost and network management such that at the end of the day, a uniform network will be the obvious solution. In fact, in several countries (such as Korea) FTTP is reality, and in several other countries (such as Sweden) xDSL has a high penetration. Moreover, depending on country, the xDSL monthly cost to users varies from under \$10 to about \$40; this is a huge gap, which is not easily explained, as it is not easily explained the cost of wireless services that vary from country to country or from one service provider to another. A simplistic answer lies on service value added, aggressive marketing, and a smart pricing strategy; that is, how much the subscriber is willing to pay for a service, and who the subscriber is?

11.4 What About Traditional Services?

The aggregate voice traffic has been exceeded by data traffic (Internet, e-mail, music, video, etc.). The emergence of video over IP and voice over IP also threaten the synchronous network.

But how real is this threat? Many network designers and network providers battle with this question. The synchronous network is fundamentally different than the (asynchronous) packet network. But is it? In reality, although the data network is fundamentally asynchronous by virtue of the natural data rate, on the physical layer, the network (assuming a realistic high data rate one) is synchronous, meaning that packets are transmitted continuously even if the payload is idle. Similarly, the packet switched network is fundamentally different than the traditional circuit switched network. But is it? The modern packet switched network has come very close to the circuit switched network in an attempt to minimize node throughput delay in order to meet real-time requirements necessary for voice and video traffic. Additionally, the high-aggregate data traffic demands an optical network which on the aggregation (backbone) is a synchronous optical WDM network, with a technology that is transparent to payload type and protocol.

11.5 How About Security of Information and of the Network?

Security is expected to be increasing in interest and in events. Besides the malicious attackers, cracking codes, gain access, and so on have become a challenge to adults as well as young ones. The worry however is the sophisticated malicious attacker, regardless of age. This attacker may have the means, in addition to know-how, to intrude and eavesdrop, mimic, alter data, make unauthorized transactions, or cause denial of service. Therefore, the sophistication of encrypting (or scrambling) data, the method of generating the encryption key, and the method of distributing the key are very

important. Will eventually quantum cryptography prove itself in the realistic optical network? And, will the intruder be unable to clone photons? Or, a smart physicist will find a method to indirectly detect the polarization state of photons without disturbing them? I know that this question has caused laughter, but so did when the particle nature of photons was first introduced, quantum mechanics, as well as the structure of subatomic particles.

11.6 Number Portability

Number portability means different things to different people, or network providers. We have witnessed the first step in this direction, your wireless telephone number can be carried with you from one service provider to another. However, what I would like to have in my house is a wireless phone that has the same number from a city to any city of the world. I want a single phone regardless of where I am and be charged as if I make a long-distance phone call when I am in an area outside my serving area, no more no less. In addition, I would like my landline phone to work, be able to be switched off, and transfer the number to my portable wireless phone, so that I do not have two numbers, one at home and one in my pocket. That is, I want a single phone number that is truly portable.

11.7 How Is the Network Managed?

Overall network management is an important topic. A comprehensive, uniform, and simple to operate hierarchical protocol is necessary for managing degradations, failures, and node provisioning to assure that the network, bandwidth, and service are provided with the expected QoS. Smaller network domains however may be self-managed. Such domains may be self-organized ad hoc simplifying the management burden of the overall network.

One comprehensive language per network layer interface greatly simplifies management, which is “multilingual” in the traditional network. The key feature in any layer language is its flexibility to adopt to meet new emerging network managing needs. This may sound very fuzzy as stated, yet the type of services expected to be offered in the near future as well as specific network developments will require protocol scalability commensurate with the network and services.

In all, the next generation network is here, and the future of communication networks looks bright and very challenging, and definitely not boring. The next generation network will allow truly integrated services, which with the help of optical and high-bandwidth wireless access the all-in-one handheld device that will become ubiquitous and affordable to all.

11.8 The Bottom Line

The next generation intelligent network will enable services at cost-points that make sense to both customer and service/network providers.

The end user will enjoy simplified, miniaturized, and secured devices that support a set of services that are selected and managed by the end user; it adapts to an evolving environment of experiences and supports portability of services in a global environment.

Similarly, the service/network provider provides a service repertory and a scalable and secure network platform that meets end-user needs with reciprocal business models.

Finally, bandwidth will be almost free as the incremental bandwidth granularity to end user will increase above megabits; that is, 1,000-fold of the current bandwidth granularity.

Appendix

VPIsystems—Demonstration Examples

Introduction

The following 12 examples have been added to demonstrate important engineering aspects of Chapter 3. The user can play with each example in real time by accessing the website <http://www.vpiphotonics.com/VPIplayer.php>. This particular website is maintained by VPIsystems GmbH and it is provided at no cost to the user. Any difficulties opening the website or any software improperly functioning should be addressed directly to

VPIsystems GmbH, Carnotstr. 6, 10587 Berlin, Germany, Phone +49 30 398 058-0, Fax +49 30 398 058-58

Application Example 1

Title

System impairments in 10 Gbps NRZ-based WDM transmissions

Description

This setup illustrates the impact of ASE noise and fiber nonlinearities on the performance of a 10 Gbps NRZ-based WDM system. The BER of each channel can be investigated individually.

The user can adjust the number of spans (transmission length), switch off/on the fiber nonlinearities and modify the EDFA noise figure.

Application Example 2

Title

Performance of NRZ, RZ, and Duobinary modulation format in 10 Gbps transmission

Description

The setup compares the performance of the NRZ, RZ, and Duobinary modulation formats in a single channel 10 Gbps transmission. The BER obtained with each modulation format are displayed against the accumulated dispersion or the OSNR.

The user can adjust the OSNR (respectively the accumulated dispersion) as well as the 3 dB bandwidth of the optical filter in front of the receiver.

Application Example 3

Title

Performance comparison of NRZ, DPSK, and DQPSK in 40 Gbps transmission

Description

The setup investigates the performance of NRZ, DPSK, and DQPSK modulation in a single channel 40 Gbps transmission. The BER obtained with each modulation format are displayed against the accumulated dispersion or the OSNR.

The user can adjust the OSNR (respectively the accumulated dispersion) as well as the 3 dB bandwidth of the optical filter in front of the receiver.

Application Example 4

Title

Variation of OSNR over an OADM chain

Description

This setup illustrates the variation of OSNR over a chain of OADMs where channels are randomly added and dropped. The OSNR is displayed over the number of passed OADM for three different random add-drop sequences.

The user can specify the number of cascaded OADMs as well as their insertion loss.

Application Example 5

Title

EDFA transients and their control in dynamic networks

Description

The setup demonstrates the transient behavior of a dynamically controlled EDFA after switching off one of four WDM channels. The power control of the EDFA is achieved by adjusting the pump power with a controller.

The user can adjust the feedback gain of the EDFA controller, which affects the settling time and shape of the controlled EDFA's transient response.

Application Example 6

Title

Impact of the dispersion map on nonlinear impairments in 10 and 40 Gbps RZ systems

Description

The setup illustrates the impact of the dispersion map on nonlinear impairments in single channel 10 or 40 Gbps RZ systems. Each span consists of 80 km of SSMF and a pre- and post-compensation modules. The line is considered noiseless in order to focus on the impact of nonlinear impairments. ASE is added in front of the receiver to achieve a given OSNR. An ideal DCM is placed in front of the receiver side for (partial) compensation of the dispersion accumulated in the line. The BER is displayed against the amount of residual dispersion at the receiver side.

The user can adjust the OSNR as well as the amount of pre- and post-compensation per span that affect the nonlinear propagation of the signal in the line.

Application Example 7**Title**

Reducing FWM effect using different channel spacing

Description

This setup illustrates the impact of four-wave mixing on the performance of WDM systems utilizing low dispersion fibers (DSF, NZDSF) and high signal powers. The BER and the magnitude of FWM products are displayed against the channel input power.

The user can adjust the emission frequencies of the channels. The channel spacing can be set unequal so that the degradation due to FWM is reduced.

Application Example 8**Title**

Influence of PMD in 40 Gbps transmission

Description

This setup models the random variation of the bit error rate due to polarization mode dispersion. The amount of PMD is randomly changed for each iteration. The spread of BER results demonstrates the difficulty in measuring the power penalty due to PMD.

The user can adjust the modulation format (between NRZ and RZ) and the number of iterations.

Application Example 9**Title**

Reduction of nonlinear penalties in 40 Gbps transmissions using alternate polarization modulation

Description

This setup demonstrates the advantages of alternate polarization modulation format over standard formats (NRZ). To apply alternating polarization between adjacent bits is an effective technique in suppressing intra-channel nonlinear distortions.

The user can adjust the propagation distance and the WDM input power.

Application Example 10

Title

Multi-pump Raman optimization

Description

Flat Raman gain is achieved over C and L bands by adjusting pump wavelengths and powers. The Raman gain and noise figure are displayed over the wavelength. Raman amplification between the pumps can be observed in an OSA.

The user can modify the wavelength and power of the pumps and observe the changes in the Raman gain.

Application Example 11

Title

10G–40G upgrade using Raman amplifier

Description

This setup demonstrates the benefits of Raman amplification allowing an upgrade from 10 s to 40 Gbps. Distributed Raman amplification is achieved by backward pumping the transmission fiber from the receiver terminal end.

The user can change the bit rate from 10 to 40 Gbps and adjust the Raman pump power.

Application Example 12

Title

MLSE versus classical receiver performance

Description

This setup demonstrates the advantage of the Viterbi-MLSE receiver over classical receiver in the presence of intersymbol interferences. The BER of a 10 Gbps NRZ signal is displayed for a constant OSNR against the amount of residual dispersion for both receivers.

The user can adjust the OSNR as well as the length of the sequences and the number of states used for Viterbi-MLSE detection.

Acronyms

10Base-T: 10 Mbps over twisted pair
100Base-T: 100 Mbps over twisted pair
1000Base-T: 1,000 Mbps over twisted pair
2B1Q: two bits to one quaternary
2f-BLSR: two-fiber bidirectional line switched ring
3R: re-amplification, reshaping, and retiming
4B/5B: four bit to five bit coding
4f-BLSR: four-fiber bidirectional line switched ring
8B/10B: eight bit to ten bit coding

AAL: ATM adaptation layer
ABR: available bit rate
ADC: analog to digital conversion
ADM: add-drop multiplexer
ADPCM: adaptive differential pulse code modulation
ADSL: asymmetric digital subscriber line
AES: advanced encryption standard
AIS: alarm indication signal
ALP: application layer protocol
AM: administration module; amplitude modulation
AMI: alternate mark inversion
AON: all-optical network
AP: access point
APD: avalanche photodetector
APDU: application protocol data unit; authentic protocol data unit
API: access point identifier
APON: ATM-based broadband PON
APS: automatic protection switching
ARM: access resource management
ASE: amplified spontaneous emission
ASIC: application-specific integrated circuit
ASK: amplitude shift keying
ATM: asynchronous transfer mode
AU: administrative unit
AU-*n*: administrative unit, level *n*
AUG: administrative unit group
AUG-*N*: administrative unit group-*N*

B8ZS: bipolar with eight-zero substitution
B: B channel (ISDN)
BB: broadband
BBER: background block error ratio
BBO: beta-barium borate
BCD: binary coded decimal

BDI: backward defect indication
 BDI-O: backward defect indication overhead
 BDI-P: backward defect indication payload
 BEI: backward error indication
 BER: bit error rate; basic encoding rules
 BI: backward indication
 B-ISDN: broadband integrated services digital network
 BIP-8: bit interleaved parity 8 field
 BITS: building information timing supply
 BML: business management layer
 bps: bits per second
 BPSR: bidirectional path-switching ring
 BRI: basic rate interface
 BSHR: bidirectional shelf-healing ring
 BSHR/2: 2 fiber bidirectional shelf-healing ring
 BSHR/4: 4 fiber bidirectional shelf-healing ring

 C-*n*: container-level *n*; *n* = 11, 12, 2, 3, or 4
 CAC: connection admission control
 CAM: content addressable memory
 CAP: carrierless amplitude phase
 CAS: channel associated signaling
 CBR: constant bit rate
 CCAMP: common control and management plane
 CDMA: code division multiple access
 CELP: code excited linear prediction
 CEPT-*n*: conference of European posts and telecommunications-level *n* (see E1)
 CIT: craft interface terminal
 CLEC: competitive local exchange carrier
 CLP: cell loss priority
 CLR: cell loss rate
 CM: communications module; connection management; connection monitoring
 CMI: coded mark inversion
 CMIP: common management information protocol
 CMISE: common management information service element
 CMIS/P: common management information service/protocol
 CMT: coupled-mode theory
 CNM: customer network management
 CO: central office
 CODEC: COder-DECoder
 COP: connection-oriented protocol
 COPS: common open policy service
 CORBA: common object request broker architecture
 COT: central office terminal
 CP: customer premises
 CPE: customer premises equipment
 CPN: calling party's number; customer premises network
 CPRING: client protection ring
 CRC: cyclic redundancy check
 CRC-*N*: cyclic redundancy check, width *N*
 CS: convergence sub-layer
 CS-PDU: convergence sub-layer-PDU
 CSA: carrier serving area
 CSDC: circuit switched digital capability
 CSES: consecutive severely errored seconds
 CSMF: conventional single-mode fiber
 CSMD/CD: carrier sense multiple access/collision detection
 CSP: critical security parameters
 CTD: cell transfer delay
 CU: channel unit

CW: continuous wave

CWDM: coarse wavelength division multiplexer

D: D channel (ISDN)

DACI: detection with alarm and countermeasure intelligence

DACS: detection with alarm and continuous service

DADS: detection with alarm and discontinuing service

dB: decibel

dBm: decibel with 1 mW reference

DCC: data country code; data communication channel; digital clear channel

DCE: data circuit-terminating Equipment

DCF: distributed coordination function

DCN: data communications network

DCS: digital cross-connect system

DDD: direct distance dialing

DDS: digital data service

DES: data encryption standard

DFB: distributed feedback

DFI: domain format identifier

DH: Diffie–Hellman algorithm

DiffServ: differentiated services

DL: data link

DLC: digital loop carrier

DLP: discrete logarithm problem

DMT: discrete multitone modulation

DPBX: digital PBX

DPCM: differential pulse code modulation

DPDU: data link PDU

DPE: distributed processing environment

DPSK: differential PSK

DQDB: distributed queue dual bus

DR: dynamical routing

DRI: dual-ring interface

DS: defect second

DSAP: destination service access point

DSCF: dispersion-shift compensated fiber; dispersion-slope compensated fiber

DSF: dispersion shifted fiber

DSL: digital subscriber line

DSLAM: digital subscriber line access multiplexer

DS-n: digital signal level n ; $n = 0, 1, 2, 3$

DSN: digital switching network

DS-SMF: dispersion shifted single-mode fiber

DSU: data service unit

DTE: data terminal equipment

DTMF: dual-tone multifrequency

DTS: digital termination service

DWDM: dense wavelength division multiplexing

DXC: digital cross connect

DXI: data exchange interface

E0: ITU-T G.703 electrical interface signal 64 kbit/s

E1: ITU-T G.703 electrical interface signal 2,048 kbit/s

E11: ITU-T G.703 electrical interface signal 1,544 kbit/s

E12: ITU-T G.703 electrical interface signal 2,048 kbit/s

E22: ITU-T G.703 electrical interface signal 8,448 kbit/s

E31: ITU-T G.703 electrical interface signal 34,368 kbit/s

E32: ITU-T G.703 electrical interface signal 44,736 kbit/s

E4: ITU-T G.703 a broadband digital facility at 139,264 kbit/s

EBC: errored block count

EBCDIC: extended binary coded decimal interchange code
 ECC: elliptic curve cryptography
 ECDLP: elliptic curve discrete logarithm problem
 EDC: error detection code
 EDCV: error detection code violation
 EDFA: erbium-doped fiber amplifier
 EFI: errored frame indicator
 EFP: environmental failure protection
 EFS: error-free second
 EFT: environmental failure testing
 ELAN: emulated LAN
 EM: element manager
 EMC: electromagnetic compatibility
 EMF: equipment management function
 EMI: electromagnetic interference
 EML: element management layer
 EMS: element management system
 E/O: electrical to optical
 ER: extinction ratio
 ES: error seconds; electrical section
 ESCON: enterprise systems connectivity
 ESF: extended superframe format
 ESR: errored seconds ratio

FAS: frame alignment signal; fiber array switch
 FCAPS: fault, configuration, accounting, performance, and security
 FCC: Federal Communications Commission
 FDDI: fiber distributed data interface
 FDI: forward defect indicator
 FDI-P: forward defect indicator-payload
 FDI-S: forward defect indicator-OSC
 FDM: frequency division multiplexing
 FDMA: frequency division multiple access
 FEBE: far end block error (renamed as REI)
 FEC: forward error correction; forward equivalency class
 FER: frame error rate
 FET: field effect transistor
 FFT: fast fourier transforms
 FFTS: fiber feeder transport system
 FIT: failure in time
 FITL: fiber in the loop
 FM: frequency modulation; fault management
 FOT: fiber optic terminal
 FOTS: fiber optic transmission system
 FPGA: field programmable gate array
 FPS: fast packet switching
 FR: frame relay
 FS: frame start signal
 FSI: FEC status indication
 FSK: frequency shift keying
 FSO: free space optical communications systems
 FTTB: fiber to the building
 FTTC: fiber to the curb
 FTTCab: fiber to the cabinet
 FTTD: fiber to the desk
 FTTH: fiber to the home
 FTTO: fiber to the office
 FTTT: fiber to the town
 FWM: four-wave mixing
 FXC: fiber cross-connect

GbE: gigabit Ethernet
Gbit/s: gigabits per second
GB/s: gigabytes per second
Gbps: gigabits per second = 1,000 Mbps
gcd: greatest common divisor
GFC: generic flow control
GFP: Generic Framing Procedure
Ghz: gigahertz (10^9 Hz)
GNE: gateway network element

HDLC: high-level data link control
HEC: header error control
HFC: hybrid fiber coax
HIPPI: high-performance parallel interface
HO: higher order
HOVC: higher order virtual container
HTML: hypertext markup language
HTTP: hypertext transfer protocol

ID: identifier
IDI: initial domain identifier
IDL: interface definition language
IDLC: integrated digital loop carrier
IDSL: ISDN DSL
IEC: Interstate Electro-technical Commission
IEEE: Institute of Electrical and Electronics Engineers
IETF: Internet Engineering Task Force
ILEC: incumbent local exchange carrier
ILMI: interim local management interface
IM: inverse multiplexer; intelligent multiplexer
IM/DD: intensity modulation with direct detection
IMS: information management system
IN: intelligent network
IntServ: Internet services
IOF: Interoffice framework
ION: intelligent optical networks
IP: Internet protocol; intelligent peripheral
IPng: Internet protocol next generation
IPv6: Internet protocol version 6
ISDN: integrated services digital network
ISP: Internet service provider
ITSP: Internet telephony service provider
ITU: International Telecommunications Union
ITU-T: ITU Telecommunications Standardization Sector
IXC: inter-exchange carrier

JIT: jitter transfer function

Kbps: kilobits per second = 1,000 bps
KEES: key escrow encryption system

LAC: link access control
LAN: local area network
LAPD: link access protocol for the D channel
LAPF: link access protocol for frame relay
LASER: light amplification by stimulated emission or radiation
LB: loop back
LCAS: link capacity adjustment scheme

LD: long distance
 LEC: local exchange carrier
 LED: light emitting diode
 LER: Label edge router
 LH: long haul
 LLC: logical link control
 LMDS: local multipoint distribution service
 LO: low order
 LOA: loss of alignment; generic for LOF, LOM, LOP
 LOF: loss of frame
 LOH: line overhead
 LOI: lower order interface
 LOM: loss of multiframe
 LOP: loss of pointer
 LOS: loss of signal; loss of synchronization
 LOVC: lower order virtual container
 LP: lower order path
 LPC: linear prediction coding
 LPF: low pass filter
 LSB: least significant bit
 LSO: local serving office
 LSP: label-switched path
 LSR: label switch-router
 LSS: loss of sequence synchronization
 LSSU: link status signaling unit
 LTE: line termination equipment
 LVC: low order virtual container

M1: level 1 multiplexer
 M12: level 1- to 2 multiplexer
 M2: level 2 multiplexer
 M23: level 2- to 3 multiplexer
 M13: level 1- to 3 multiplexer
 MAC: media-specific access control
 MAN: metropolitan area network
 MB/s: megabytes per second
 Mbit/s: megabits per second
 MBps: megabytes per second
 Mbps: megabits per second (1,000 Kbps)
 MBS: maximum burst rate
 MCN: management communications network
 MH: medium haul
 Mhz: megahertz (10^6 Hz)
 MI: management information
 MIB: management information base
 MII: Ministry of the (China) Information Industry
 MIM: management information model
 MPI: multiple path interference
 MRTIE: maximum relative time interval error
 MS-AIS: multiplex section AIS
 MSB: most significant bit
 MSDSL: multirate SDSL
 msec: millisecond
 µsec: microsecond
 MSO: multiple service operator
 MSOH: multiplexer section overhead
 MSP: multiplex section protection
 MTBF: mean time between failure
 MTIE: maximum time interval error

MUX: multiplexer
mW: milliwatts
NAP: network access provider
NASA: National Aeronautics and Space Administration (USA)
NC: network connection
NDF: new data flag
NE: network element
NEBS: network equipment building system
NEF: network element function
NEL: network element layer
NEXT: near-end cross-talk
NF: noise figure
NGI: next generation Internet
NIC: network interface card
NIST: National Institute for Standards and Testing
NIU: network interface unit
nm: nanometer
NML: network management layer
NMS: network management system
NNI: network to network interface; network node interface
NOLM: nonlinear optical loop mirror
NRM: network resource management
NRL: Naval Research Laboratory (USA)
ns: nanosecond
NSA: US National Security Agency
NSN: network service node
NSP: network service provider
NT: network termination
NTU: network termination unit

OA: optical amplifier
OAM: operations, administration, and management
OADM: optical ADM
OAMP: oam and provisioning services
OAR: optically amplified receiver
OAS: optical amplifier section
OAT: optically amplified transmitter
OC: optical carrier
OCG: optical channel group; optical carrier group
OCh: optical channel with full functionality
OCI: open connection indication
OC-*n*: optical carrier level *n* (*n* = 1, 3, 12, 48, 192)
OD: optical demultiplexer
ODBC: open database connectivity
ODL: optical data link
ODMA: open distributed management architecture
ODP: optical diverse protection; open distributed processing
ODSI: optical domain service interconnect
ODU: optical data unit
ODU-*k*: optical channel data unit-*k*
O-E: optical to electrical conversion
OEIC: opto-electronic integrated circuit
OEM: original equipment manufacturer
OEO: optical–electrical–optical converter
OFA: optical fiber amplifier
OH: overhead
OLC: optical loop carrier
OLE: object linking and embedding
OLS: optical line system

OLTM: optical line terminating multiplexer
 OLTS: optical loss test set
 OM: optical multiplexer
 OMA: object management architecture
 OMAP: operations, maintenance, and administration part
 OMS: optical multiplex system; optical multiplex section
 OMS-OH: optical multiplex section overhead
 OMU: optical multiplex unix
 ONNI: optical network node interface
 ONTC: Optical Networks Technology Consortium
 ONU: optical network unit
 OOF: out of frame
 OOK: on-off keying
 OOS: otm overhead signal; out of synchronization
 OPLDS: optical power loss detection system
 OPLL: optical phase-locked loop
 OPM: optical protection module
 OPS: optical protection switch
 OPU: optical payload unit
 OPU- k : optical channel payload unit- k
 OS: operating system
 OSA: optical spectrum analyzer
 OSC: optical supervisory channel
 OSF: operating system function
 OSI: open system interconnect
 OSI-RM: open system interconnect reference model
 OSNR: optical signal-to-noise ratio
 OSS: operations support system
 OTDM: optical time division multiplexing
 OTDR: optical time domain reflectometer
 OTE: optical terminating equipment
 OTM: optical transport module
 OTN: optical transport network
 OTS: optical transmission section; off-the-self
 OTS-OH: optical transmission section overhead
 OTU: optical transport unit
 OTU- k : optical channel transport unit- k
 OUI: organization unit identifier

 PAD: packet assembler and disassembler
 PAM: pulse amplitude modulation
 PBX: private branch exchange
 PC: payload container; protection channel; personal computer
 PCM: pulse coded modulation
 PCS: personal communication services
 PD: photodiode; propagation delay
 PDH: plesiochronous digital hierarchy
 PDL: polarization-dependent loss
 PDN: packet data network; passive distribution system
 PDU: protocol data unit
 PE: payload envelope
 PG: pair gain system; pointer generator
 PHY: physical layer
 PLCP: physical layer convergence protocol
 PLI: payload length indication
 PLL: phase-locked loop
 PM: performance monitoring; path monitoring
 PMC: polarization mode coupling
 PMI: payload missing indication
 PMD: physical medium dependant; polarization mode dispersion

PN: pseudorandom numerical sequence; prime number
PNNI: private nni
POH: path overhead
PON: passive optical network
POP: point of presence
POTS: plain old telephone service
PP: pointer processing
ppm: parts per million
PPP: point-to-point protocol
PRC: primary reference clock
PRI: primary rate interface
PRS: primary reference source
PS: protection switching
PSI: payload structure identifier
PSK: phase shift keying
PSTN: public switched telephone network
PT: payload type
PTE: path-terminating equipment
ptp: peak to peak
PTT: postal telephone and telegraph Ministries
PVC: permanent virtual circuit
PVP: permanent virtual path

QAM: quadrature amplitude modulation
QC: quantum cryptography
QKD: quantum key distribution
QM: quantum mechanics
QoS: quality of service; quality of signal
QPSK: quadrature PSK; quaternary PSK; quadriphase PSK

RADSL: rate adaptive DSL
RAM: random access memory
RBOC: Regional Bell Operating Company
RDI: remote defect indicator, formerly FERF; aka yellow alarm
REI: remote error indicator
RF: radio frequency
RFI: remote failure indication; radio frequency interference
Rijndael: Rijmen and Daemen
RM: resource management
RMN: ring-mesh network
ROM: read only memory
ROSE: remote operation service element
RS: reed-solomon
RSA: Rivest, Shamir Adleman Algorithm
RSM: remote switch module
RSOH: regenerator section overhead
RSTE: regenerator section-terminating equipment
RSU: remote switch unit
RSVP: resource reSerVation setup protocol
RT: remote terminal
RTT: round trip time; radio transmission technology
RTU: remote termination unit
RX: optical receiver
RZ: return to zero

SAP: service access point
SAR: segmentation and reassembly
SBS: stimulated Brillouin scattering
SCR: sustainable cell rate
SDH: synchronous digital hierarchy

SDLC: synchronous data link control protocol
 SDSL: symmetric DSL
 SDU: service data unit
 SF: signal fail; super frame
 SH: short haul
 SHR: self-healing ring
 SI: step index
 SIP: SMDS interface protocol; series in-line package
 SIR: signal-to-interference ratio
 SL: signal label
 SL-*N*: security level *N*, *N* =1,2,3 ...
 SLA: service level agreement
 SLC: synchronous line carrier; subscriber loop carrier
 SLM: synchronous line multiplexer
 SM: switching module
 SMDS: switched multi-megabit digital services
 SMF: single-mode fiber; service management function
 SML: service management layer
 SMN: SONET management network; SDH management network
 SMS: SDH management subnetwork
 SN: sequence number; service node
 SNA: systems network architecture
 SNAP: sub-net access protocol
 SNCP: subnetwork connection protection
 SNI: service node interface; subscriber to network interface
 SNMP: simple network management protocol
 SNMS: subnetwork management system
 SNP: sequence number protection
 SNR: signal to noise ratio
 SOA: semiconductor optical amplifier
 SoF: start of frame
 SOH: section overhead
 SONET: synchronous optical network
 SP: switching point
 SPDU: session protocol data unit
 SPE: synchronous payload envelope
 SPM: self-phase modulation
 SPRING: shared protection ring
 SQM/BQI: signal quality monitoring and backward quality indication
 SR: short reach; software radio; symbol rate
 SRS: stimulated raman scattering
 SS7: signaling system #7
 SSAP: source service access point; session service access point (ISO)
 SS-CDMA: spread spectrum CDMA
 SSL/TLS: secure sockets layer/transport layer security
 SSMF: standard single-mode fiber
 STE: section terminating equipment; switching terminal exchange
 STM-*n*: synchronous transport module level *n* (*n* =1, 4, 16, 64)
 STP: shielded twisted pair; signal transfer point
 STS: synchronous transport signal; space-time-space switch
 SVC: switched virtual circuit
 SWC: service wire center

T1: a digital carrier facility used to transmit a ds1 signal at 1.544 mbps
 T3: a digital carrier facility used to transmit a ds3 signal at 45 mbps
 TA: terminal adapter
 Tbps: terabits per second: 1,000 gbps
 TC: tandem connection
 TCP: transmission control protocol

TCAM: telecommunications access method
TCAP: transaction capabilities part
TCM: tandem connection monitoring
TCMOH: tandem connection monitoring overhead
TCP: transmission control protocol; trail connection point
TCP/IP: transmission control protocol/Internet protocol
TDM: time division multiplexing
TDMA: time division multiple access
TE: terminal equipment; trans-electric
TEI: terminal endpoint identifier
TEP: traffic engineering policy
TE-RSVP: traffic engineering resource reservation protocol
Thz: terahertz (1,000 Ghz)
TI: trace identifier
TIA: Telecommunications Industry Association
TIM: trace identifier mismatch
TINA: Telecommunications Information Networking Architecture Consortium
TL1: transport language 1
TLV: threshold limit values
TM: traffic management; terminal multiplexer; trans-magnetic
TMM: transmission monitoring machine
TMN: telecommunications management network
TOH: transport overhead (SOH + LOH)
TP: twisted pair; transport layer protocol
TPC: transmit power control
TTP: trusted third parties
T&R: tip and ring
TS: time stamp; time slot
TSI: time slot interchanger
TTA: Telecommunications Technology Association
TU: tributary unit
 $TU-n$: tributary unit level n ; $n = 11, 12, 2$, or 3
 $TUG-n$: tributary unit group n ; $n = 2$ or 3
TX: optical transmitter
TxTI: transmitted trace identifier

UBR: unspecified bit rate
UDC: universal digital channel
UDP: user datagram protocol
UI: unit interval
ULH: ultralong haul
ULR: ultralong reach
UNEQ: unequipped
UNI: user to network interface
UPC: usage parameter control
UPSR: unidirectional path switch ring
URL: uniform resource locator
USART: universal synchronous/asynchronous receiver transmitter
USHR: unidirectional shelf-healing ring
USTIA: United States Telecommunications Industry Association
UTP: unshielded twisted pair
UV: ultraviolet
UWB: ultra-wideband

VBR: variable bit rate
VC: virtual channel
 $VC-n$: virtual container level n ($n = 2, 3, 4, 11$, or 12)
 $VC-n-Mc$: virtual container level n , M concatenated virtual containers
 $VC-n-X$: X concatenated virtual container- ns
 $VC-n-Xc$: X contiguously concatenated VC- ns

VC-*n*-Xv *X* virtually concatenated VC-*ns*
VCC: VC connection
VCI: virtual circuit identifier
VCSEL: vertical-cavity surface-emitting laser
VDSL: very-high-bit rate DSL
VF: voice frequency
VHF: very high frequency
VLAN: virtual LAN
VLSI: very large scale integration
VOA: variable optical attenuator
VOD: video on demand
VoIP: voice over IP
VP: virtual path
VPC: VP connection
VPI: virtual path identifier
VPN: virtual private network
VSR: very short reach
VT: virtual tributary
VTOA: voice telephone over ATM

WADM: wavelength add-drop multiplexer
WAN: wide area network
WAP: wired equivalent privacy
WATS: wide area telephone service
WATM: wireless ATM
W-CDMA: wideband DS-CDMA
W-DCS: wideband digital cross-connect system
WDM: wavelength division multiplexing
WGR: waveguide grating router
WIS: wavelength independent switch
WIXC: wavelength interchanging cross-connect
WLAN: wireless LAN
WPA: wifi protected access
WPON: WDM PON
WSC: wavelength selective coupler
WSS: wavelength selective switch
WSXC: wavelength selective cross-connect
WW II: world war II
xDSL: any-DSL
XML: extensible markup language
XOR: exclusive or

Short Bio

Stamatis V. Kartalopoulos, PhD, is Williams Professor in Telecommunications Networking with the University of Oklahoma in the ECE/TCOM Engineering graduate program. His research emphasis is on optical communication networks (long and medium haul, FTTH, and FSO), optical technology including optical metamaterials, and optical networks security including quantum cryptography and quantum key distribution protocols and biometrics. Prior to academia, he was with Bell Laboratories where he defined, led, and managed research and development teams in the areas of DWDM networks, SONET/SDH and ATM, cross-connects, switching, transmission and access systems. He has received the Presidents Award and many awards of Excellence.

He holds 19 patents in communications networks, and he has published more than hundred fifty scientific papers, seven reference textbooks in advanced fiber optic networks and technology, in neural networks and fuzzy logic, and he has contributed several chapters to other books.

He has been as IEEE and a Lucent Technologies Distinguished Lecturer, and has lectured worldwide at Universities, NASA, and conferences. He has been a keynote and plenary speaker at major international conferences, has moderated executive forums, has been a panelist of interdisciplinary panels, and has organized symposia, workshops, and sessions at major international communications conferences.

Dr. Kartalopoulos is an IEEE fellow, chair and founder of the IEEE ComSoc Communications & Information Security Technical Committee and past chair of ComSoc SPCE and of Emerging Technologies Technical Committees, member at large of IEEE New Technologies Directions Committee, editor-in-chief of IEEE Press and area-editor of IEEE Communications Magazine/Optical Communications, member of IEEE PSPB, and VP of IEEE Computational Intelligence Society.



Index

- Access optical networks (AON), 84
- Adaptation layers (AAL), in ATM protocol, 30
- Add-drop multiplexing (ADM), 73
 - See also* Optical add-drop multiplexers (OADM)
- Advanced Encryption Standard (AES), 210
- Agamemnon's link, optical messages, 191
- Allan deviation (ADEV) model, 147
- Alternate path routing
 - algorithm, 179
 - in DWDM, 82–83
- American Telephone and Telegraph Corporation (AT&T), 1
- Amicable numbers, 204
- Amplifier spontaneous emission (ASE), 148, 150
- Amplitude shift keying (ASK), 167
- Analog electrical signals, 1
- Ancient Greek tablets, 194
- Ancient Mesopotamian message delivery, 191
- ANSI/TIA/EIA-568-A cabling requirement, 34
- Asymmetric ciphers, 211
- Asymmetric cryptography, 199
- Asynchronous networks
 - data traffic in, 25–26
 - synchronization and timing in, 25*See also* SONET/SDH (synchronous optical networks)
- Asynchronous transport/transferring mode (ATM) protocol, 8, 21, 27
 - adaptation layers (AAL) in, 30
 - connection admission control (CAC) process, 31
 - connection establishment, 31–32
 - errors, type of, 31
 - frame in, 28
 - header fields, 28–29
 - segmentation and reassembly in, 29
 - service level agreement (SLA), 30–31
 - services by, 31
 - SONET/SDH, 32
 - traffic shaping (TS) in, 30
 - ATM PON (A-PON), 84
- Background block error (BBE)/and ratio (BBER), 160
- Backward defect indication (BDI), 139
- Backward quality indication (BQI), 139
- Bandwidth elasticity, 3
- 3B/4B block coding, 46
- 8B/10B block coding, 46–47
- Bell experiment, for photon state teleportation, 231
- BER, *see* Block error ratio (BER)
- Bidirectional path-switching rings (BSPR), 188
- Biometric database classification, 241
- Biometrics and communication networks, 241–242
- Birefringence
 - crystal and splits of optical beam, 230
 - in optical communication, 61
- Bit-by-bit modulo-2, 198
- Bit error rate (BER/BERate), 25, 109, 131, 159, 160, 165–167
- Bit error ratio (BERatio), 159, 160
- Bit interleaved parity (BIP), 161
- Block error ratio (BER), 160
 - analysis, in channel performance, 165–167
 - performance and bit rate, FEC affecting, 130
 - statistical estimation method, 168–170
- Blue box, 195
 - See also* Network security
- Broadband services, 9–10
- Brute attack, 197
- Brute force, 204
- Building information timing supply (BITS), 142
- Burst tolerance (BT) parameter, 30, 178
- Business management layer (BML), 77
- Caesar's cipher, 194
- Calling name database (CNAM), 8
- Carrier sense multiple-access/collision detection (CSMA/CD), 33
- Carrier to noise ratio (CNR), 162
- Cell loss rate (CLR), in ATM protocol, 31
- Cell transfer delay (CTD), in ATM protocol, 31
- Cellular wireless telephony, 196
- Channel and link protection and countermeasure, protocol for, 240
- Channel isolation/channel separation in optical communications, 58
- Channel performance in networks, 161–162
 - characteristics, model and measurements, 161
 - factors affecting, 164
- Channel proactive reassignment algorithm (CPRA), 241
- Channel protection, in DWDM network, 81–82

- Channel restoration, 183, 187
 Chirp, in optical communication networks, 150
 Chromatic dispersion (CD), 61, 154
 in fibers, 67–68
 in optical communication networks, 150
 Chromatic dispersion coefficient (CDC), 68
 Chromatic jitter, 68–69, 154–155
 Ciphering, *see* Encoding
 Ciphers
 advanced encryption standard (AES), 210
 asymmetric ciphers, 211
 data encryption standard (DES), 209
 elliptic curve factoring, 212
 integer factorization problem and, 212
 permutation cipher, 209
 RC4 algorithm, 210
 RSA algorithm, 212
 substitution/random shift cipher, 209
 symmetric and shift ciphers, 208–209
 Cipher text, 198
 Circuit architecture in BER and SNR estimation, 170
 Circularly polarized wave in light polarization, 59–60
 Clepsydra, 192
 Client bandwidth management, 175
 Client data frame (CDF), 116–117, 120
 Coarse wavelength division multiplexing (CWDM), 64–66, 84, 87–93
 Coder-decoder (CODEC), 1
 Common channel signaling (CCS), 8
 Common Control and Management Plane (CCAMP), 114
 Common management information service element (CMISE), 77
 Communication networks, security layers
 information layer and, 201
 link layer and, 203
 MAC/Network layer and, 202–203
 Communications hierarchy and networking, 6
 Communications overhead (COMMS OH), 137
 Communication technologies, 245–246
 Computer telephony (CT), 5
 Concatenation
 contiguous, 111
 efficiency, 127–128
 virtual, 111–112
 Confidence level (CL), 167
 Congestion management in DWDM, 178
 Connection admission control (CAC), 178
 Constant bit rate (CBR), 177
 Continuous wavelength (CW), 82
 Cooperative Association for Internet Data Analysis Group (CAIDA), 42
 Core header error control (cHEC), 115–117, 118, 120
 Craft interface terminal (CIT), 8
 Critical security parameters (CSP), 200
 Cross-phase modulation (XPM), 164
 Cryptographic keys classification, 202
 Cryptography
 definition, 196–197
 information security services and, 197
 symmetric key, 198
 and technology, 199
 CWDM-PON in WDM system access, 87–88
 Cyber-security, 195
 Data-dependent jitter (DDJ), 152–154
 Data encryption standard (DES), 209–210
 Data networks
 and protocols, 8–9
 synchronous and asynchronous, requirements of, 5
 Data packet network, 196
 Data services, synchronous and asynchronous network, 101–104
 Data traffic explosion, 3
 Data transport efficiency, 5
 Decoding, 197
 Detection with alarm and countermeasure intelligence (Daci), 238–241
 Deterministic jitter (DJ), 152
 Differential group delay (DGD) noise, 155
 Differentiated services model (*Diffserv*), 27–28
 Diffie-Hellman key exchange, 215–217
 Digital cross-connects systems (DACS or DCCS), 8
 Digital service levels (DS), 1
 Digital subscriber lines (DSL), 1, 5
 Digital transmission and analogue, 1–3
 Diplex method, in bidirectional traffic, 85
 Direct in-service methods, 161
 Direct search factorization, 204
 Dispersion-compensated fiber (DCF), 68
 Dispersion-flattened compensated fiber (DFCF), 68
 Dispersion-flattened fiber (DFF), 68
 Dispersion-shift compensated fiber (DSCF), 68
 Dispersion shifted fiber (DSF), 66
 Dispersion-slope compensated fiber (DSCF), 68
 Distributed biometric database, 241
 Distributed traffic control, 173–174
 Dual-fiber method, in bidirectional traffic, 86
 Duplex method, in bidirectional traffic, 85
 DWDM (Dense wavelength division multiplexing), 55, 56, 63, 64, 87, 89, 92, 93
 EDFA amplification in, 71–72
 DWDM mesh networks, fault protection in, 187–188
 DWDM networks, 73–74
 channel and link protection, 81–82
 group protection in, 82
 network topologies, 74–75
 network switching, 78–80
 optical mesh networks, 178
 optical network interfaces, 75–77
 routing in, 82–83
 timing and synchronization, 81
 Dynamic configurability in network provisioning, 180
 Dynamic RWA algorithms, types, 179
 EDC codes, *see* Error detection–correction (EDC) codes
 EDFA, *see* Erbium-doped fiber amplifiers (EDFA)
 Einstein-Podolsky-Rosen correlation (EPR), 229

- Electro-optic effect in optical communication, 62
Element management systems (EMS), 77, 174
Elliptically polarized wave in light polarization, 59, 60
Elliptic curve discrete logarithm problem (ECDLP), 223
Elliptic curves
 cryptography, 217
 factoring, 212
 over $F(2^m)$, 221–222
 over prime numbers $F(p)$, 220–221
 over real numbers $F(n)$, 218–220
Encoding, 197
Entangled states and quantum teleportation, 229–231
Enterprise systems connection (ESCON) protocol
 features of, 50
 frame structure, 50–51
Erbium-doped fiber amplifiers (EDFA), 57, 150
 amplification in DWDM, 71–72
Error detection–correction (EDC), 131
 codes, 161, 210
Errored block (EB), 160
Errored second ratio (ESR), 160
Errored seconds (ES), 160
Error performance parameters path, 160
Ethernet CSMA/CD and, 33
 encapsulation, 122
 frame format, 33
 origin of, 32
 PON (E-PON), 84
 ports on SONET/SDH, demands for, 4
 traffic, 123
 variants of, 33
 See also Gigabit Ethernet (GbE)
Euclidean algorithm for greatest common divisor (gcd), 205
Exclusive OR (XOR) logic operation, 198
Extinction ratio (ER), in optical communications, 60–61
- Factoring prime numbers, 204
Failure in time (FIT), 178
Fault and service protection
 DWDM mesh networks and, 187–188
 multi-ring protection, 190
 in point-to-point networks, 186
 in ring-networks, 188–189
 strategies for, 185–186
Fault detection, in networks
 in DWDM network, 184
 localization of fault, 184
Fault protection strategies, 185–186
Fiber birefringence
 minimization steps, 61
 in optical communications, 67
Fiber channel (FC) protocol
 bit rates, 47
 congestion control in, 50
 frame structure, 48
 layers in, 47–48
 loop initialization process (LIP) in, 49
 topology in, 48–49
- Fiber connection (FICON) protocol, 51
Fiber cut, 183, 188
Fiber distributed data interface (FDDI), 24
 frame, 37–38
 protocols in, 37
 station standard, 38
Fiber-in-the-loop (FITL), 84
Fiber link and restoration, 106, 183
Fiber to the business (FTTB), 84
Fiber to the cabinet (FTTCab), 84
Fiber to the curb (FTTC), 84
Fiber to the home/curb/cabinet/premises/office or x (FTTx), 5
Fiber-to-the-home (FTTH), 84
Fiber to the premises (FTP), 73, 84
Fibre optics, 3
Flicker frequency modulation (FFM), 148
Flicker or 1/f noise, 148
Flicker phase modulation (FPM), 148
Forward defect indication (FDI), 139
Forward error correcting (FEC), 130
Four-fiber ring (4-F), 74
Four-wavemixing (FWM)
 noise, 154, 155, 164
 in optical communication, 62–63
Frame alignment signal (FAS), 132
Frame relay (FR), 8, 39
Free-run accuracy, of PLL parameter, 143
Frequency distortion in optical communication networks, 150
Frequency division multiplexing (FDM), 87
FSO (Free space optical), in WDM system access, 95–97
Fullwidth half maximum (FWHM), 69
- General communications channel-0 (,), 132, 134
Generic cell rate algorithm (GCRA), 177–178
Generic framing procedure (GFP), 5, 77
 client information data, 116
F mode optimization, packet switching, 120, 121
frames mapping in OTN frame structure, 138–139
frame structure, 118
length frames, 115
protocol, 104
 See also Next generation protocols
 scrambling operations, 118
 synchronization, 117–118
 transport modes, 118
Generic multi-protocol label switching(GMPLS), 104, 112–114
 GMPLS algorithms, 113
 MPLS and MPλS, 112–113
Gigabit Ethernet (GbE)
 bit rates, 36
 10 Gigabit ethernet (10GbE), 36–37
 layers in, 33–34
 MAC layer and, 34
 media, types of, 34–35

- Gigabit media independent interface (GMII) layer, 35–36
- Gigabit PON (G-PON), 84
- GR-253–CORE specification, 25
- Group node failure, in networks, 183
- Group protection, in DWDM network, 82
- HCT-PON, 89
- access network, architecture, 90
 - topologies, 91
 - See also* Hierarchical CWDM/TDM-PON in WDM system access
- Head error control (HEC) byte, 145
- Hierarchical CWDM/TDM-PON in WDM system access, 89–94
- Hold-over stability of PLL parameter, 143
- Home locations register (HLR), 8
- Hypothetical reference path (HRP), 160
- IEEE 802.3 standard, 32, 36
- IETF internet protocol performance metrics group (IETF IPPM), 42
- In-channel control messages, 174
- Insertion loss (IL) in optical communications, 58
- In-service and real-time performance estimation, circuit, 170–171
- Instantaneous transmission rate, 36
- Integer factorization problem, 212
- Integrated services digital network (ISDN), 1, 43–44, 76
- Interfaces, types, 75–76
- Intermediate reach (IR), *see* Medium-haul optical networks
- Internet protocol (IP), 41–42, 101, 123
- Inter-network interface (INI), 76
- Intersymbol interference (ISI) jitter, 152, 153, 164
- Jitter
- definition and types, 25
 - generation in communications system, 156
 - in optical communications networks, 150–153
 - characterizations of, 156
 - sources of, 155
 - tolerance in communications system, 156
 - transfer in communications system, 156
- Jitter transfer function (JTF), 156
- Jittery clock, 151–152
- Just-enoughtime (JET) switching, 79
- Just-in-time (JIT) switching, 79
- Kerr effect, in electro-optic effect, 62
- Key depository/key management archive, 198
- Key distribution
- Diffie-Hellman key exchange, 215–217
 - digital signature, 224
 - elliptic curve cryptography, 217
 - Merkley's algorithm, 215
 - Shamir's key distribution method, 215
 - trusted third party/key escrow encryption system, 225
- Key escrow encryption system (KEES), 225
- Key escrow system, 197
- Key establishment, 198
- Key registration authority, 198
- Keystream generator, 199
- Key wrapping, 198
- Label distribution protocol (LDP), 113
- Label-switched router (LSR), 113
- Landline telephony, voice services, 101
- Last mile bottleneck, 84
- Light polarization
- elliptically polarized wave in, 59, 60
 - linearly polarized wave in, 59, 60
- Light propagation
- in fiber, 57–63
 - in matter, 56–57
- Lightwave connectivity establishment methods, 175–176
- Line information database (LIDB), 8
- Line overhead, in SONET frames, 18–19
- Link access procedure SDH (LAPS), 104, 123–127
- Link and signal performance, 159
- Link capacity adjustment scheme (LCAS), 104, 120–123
- Link control protocol (LCP), frame structure, 44
- Link layer, 203
- Link protection, 187
- in DWDM network, 81–82
- Local number portability (LNP), 8
- Loop initialization process (LIP), in Fiber Channel protocol, 49
- Loss of clock (LOC), 145–146
- Loss of frame (LOF), 145–146
- Loss of signal (LoS), 145–146
- Loss of synchronization (LOS), 145–146
- MAC/network layer, 201
- Manhattan street network (MSN), 38
- Maximum acceptable optical power density, 66
- Maximum burst size (MBS), 178
- Maximum time interval error (MTIE) model, 147
- Media access control layer (MAC), in communication network, 202
- Medium-haul optical networks, 186
- Merkley's algorithm, 215
- Mesh DWDM networks, fault protection, 187
- Metro ring topology, 52
- μ -law (transfer function), 2
- Minimum cell rate (MCR), 31
- Mobile telephony, voice services, 101
- Modal dispersion in fibers, 67
- Modified ADEV (MDEV) model, 147
- Modulation instability (MI) noise, 155, 164
- Modulus arithmetic, 204–205
- Multiframe alignment signal (MFAS), 132
- Multimode fiber (MMF) in fiber-optic communications, 65, 66
- Multiple protocol label switching (MPLS), 27, 112–113
- Multiple protocol wavelength switching (MP λ S), 112–113
- Multiple service degradation, 108, 109

- Multiservice switching platform (MSSP), 104–105, 110–111
See also Next generation ring networks, OADM
- Multi-wavelength path connectivity, 176
- Narrowband services, 9–10
- National Institute of Standards and Technology (NIST), 142
- Network control protocol (NCP), 45
- Network elements (NE), 77, 174
- Network management, intelligent optical network, 108
- Network management system (NMS), 77, 174
- Network performance
- BER and SNR
 - analysis, 165–167
 - estimation method, 168–170
 - channel performance, 161–162
 - factors affecting, 164
 - definition of, 159
 - in-service and real-time performance estimation
 - circuit performance, 170–171
 - noise ratio and power-bandwidth ratio, carrier, 162–163
 - OSNR, 163
 - Shannon's limit, 163
- Network physical layer security, 201
- Network protection and fault management, 183–190
- fault and service protection, 184–186
 - fault detection and isolation, 184
 - mesh network protection, 187–188
 - multi-ring shared protection, 190
 - point-to-point networks, medium-haul and short-haul
 - optical networks, 186
 - ring network protection, 188–189
 - ring-to-ring protection, 189
- Network provisioning, dynamic configurability in, 180
- Network restoration, 183
- Networks
- channel performance in, 161–162
 - characteristics, model and measurements, 161
 - factors affecting, 164
 - fault detection in, 184
 - See also* Network protection and fault management
 - traffic barriers, 3–5
 - See also specific types*
- Network security, 191–246
- definitions of, 196–200
 - issues of, 195–196
 - security levels of, 200
- Network switching methods, 78–80
- in DWDM network, 78–80
- Network synchronization, in optical networks
- Jitter and Wander in, 150–156
 - photodetector responsivity and noise contributors, 156–157
 - signal quality, 147–149
 - noise sources, 148–149
 - quantization noise, 149
- synchronization, 141–146
 - impairments, 145–146
 - node timing unit and phase lock loop, 143–145
 - primary reference timing source (PRS), 142–143
 - timing signal, 146–147
- transmission factors, 149–150
- Network termination (NT), 85
- time division multiplexing, 93
- Network topologies, 102
 - and optical technology, 75
- Next generation mesh networks
- network management, 108
 - path protected mesh network (PPMN), 105–106
 - protection strategies, 106
 - routing algorithm, 107
 - service restoration, 108
 - traffic management, 106
 - wavelength management, 107–108
- Next generation optical network, 242–246
- Next generation protocols, 110–127
- concatenation, 111–112
 - generic framing procedure, 114–120
 - GMPLS, 104, 112–114
 - optical transport network (OTN), 110
- Next generation ring networks, OADM, 104–105
- Next generation SONET/SDH networks
- link access procedure SDH (LAPS), 123–127
 - link capacity adjustment scheme (LCAS), 120–123
 - next generation mesh networks, 105–109
 - next generation ring networks, 104–105
- Node and network provisioning, 180
- Node restoration, 183
- Node timing unit in optical communication networks, 143–145
- Node-to-node interface (NNI), 76
- Noise
- contributors in optical networks, 156–157
 - DGD noise, 155
 - Flicker or 1/f noise, 148
 - and nonlinearity of medium, 150
 - quantization noise and error, in optical communication networks, 149
 - shot noise, 148
 - sources in optical communication network, 148–149
 - SPM noise, 155, 164
 - Stokes noise, 68–69, 154–155
 - thermal (or Johnson) noise, 148
- Noise figure (NF), 166, 170
- Noise ratio and power-bandwidth ratio, carrier, 162–163
- Nontrivial factorization, 212
- Non-zero-dispersion-shifted fiber (NZDSF), 66, 68
- OADM, *see* Optical add-drop multiplexers (OADM)
- OA&M (operations, administration, and management) network, 7, 129, 130
- OCC, *see* Optical channel carrier (OCC)
- On-off keying (OOK) modulator, 154, 167
- Open shortest path first (OSPF), 113
- Open system interconnect (OSI) model, 76

- Optical add-drop multiplexers (OADM), 73, 79, 104, 176, 177, 186
 principles, 74
See also Next generation ring networks, OADM
- Optical amplifiers, characteristics and types of, 69–70
- Optical carrier level-N (OC-*N*), in SONET, 16
- Optical channel
 with full functionality (OCh), 134–137, 140, 147
 overhead (OCh OH), 136
 sub-layers and types, 136
 layer network, 129
 in OTN frame structure, 135–136
 with reduced functionality (OChr), 136
- Optical channel carrier (OCC), 135–137
 and OCGs, types of, 136
 overhead (OCCo), 136
 payload (OCCp), 136
 with reduced functionality (OCCr), 136
- Optical channel group (OCG), 136–138
 OCG-k, structure, 137
 OCG-n
 with full functionality (OCG-n), 136
 with reduced functionality (OCG-nr), 136
- Optical channel transport unit-k (OTU-k), 137–138
 basic steps, 135
 formation and nominal rate, 133–134
 frame construction, 134
- Optical communication network
 chirp in, 150
 polarization distortion in, 150
 quantization noise and error in, 149
 timing signal in, 146–147
 Wander in, 150–153
- Optical communications
 channel isolation/channel separation in, 58
 components
 historical perspectives, 55
 isolation in, 58
 dispersion in, 61–62
 electro-optic effect in, 62
 extinction ratio (ER) in, 60–61
 fiber loss in, 57
 fiber-optic, spectrum in, 63–65
 fibers technology in
 fiber birefringence and dispersion, 67–69
 non-linear phenomena, 69
 optical power limit, 66
 types of, 65–66
 major and minor principal transmittance in, 60
 phase shift of wave in, 61
 power density in, 66
 power loss in, 57–58
 principal transmittance in, 60
- Optical cross-connecting (OXC) nodes, 187
- Optical data unit-k (ODU-k), 132–134, 137
 formation and function, 133
- Optical-electrical-optical (OEO), 176
- Optical fiber amplifiers (OFA), 71
- Optical fibers
 in optical communication, 55–63
 light propagation in fiber, 57–63
 light propagation in matter, 56–57
 as transmission medium, 2
- Optical line termination (OLT), 85
- Optical multiplexer (OMux), 91
- Optical multiplex section layer network, 129
- Optical multiplex section overhead (OMS OH), 137
- Optical multiplex unit (OMU), 137
- Optical network demultiplexing unit (ONU-d), 89
- Optical network (ON), 83, 107, 108
 countermeasures
 DACI, 238–241
 faults and attacks, 236
 performance vector in-service and in real time, 238
 security networks, classification of, 236
 interfaces in DWDM networks, 75–77
 next generation, 4
 reliability of, 12
 routing performance factors, 78
 security in, 12–13
 topology discovery, 179
 traffic and services evolution in, 12
- Optical network termination (ONT), 85
- Optical network unit (ONU), 85–91
 authentication in PON topology, 86
- Optical packet switching of network switching, 79
- Optical power limit, 66
- Optical rings, in optical packet switching, 80
- Optical signal to noise ratio (OSNR), 163
- Optical supervisory channel (OSC), 175, 184
- Optical time division multiplexing unit (OTDM), 91
- Optical transmission, 3
- Optical transmission section layer network, 130
- Optical transmission section overhead (OTS OH), 137
- Optical transport module (OTM), 137
- Optical transport network (OTN)
 and DWDM, 138–139
 FEC in, 131–132
 frame structure
 GFP frames mapping, 137–138
 nonassociated overhead, 137
 OCC and OCG, 136–137
 ODU-k, 132–134
 optical channel, 135–136
 OPU-k, 132
 OTU-k, 134–135
 management, 139–140
 network layers, 129–131
 OPU-k frames, FEC code, 132
 over WDM
 mapping, 139
 and range of protocols, 242–243
 supervisory channel (OSC), 137
- Optical wavelength demultiplexer (ODemux), 89–91
- OPU-k transmission bit rates, 132
- OTM, *see* Optical transport module (OTM)
- OTN, *see* Optical transport network (OTN)

- OTN supervisory channel (OSC), 137
OTU, *see* Optical channel transport unit-k (OTU-k)
- Packet networks, services provided by, 26–28
Packet switching
 applications, point-to-point protocol (PPP), 120
 principles, 79
 supervisory channel, 80
Pair-gain systems, 6
 See also Subscriber Loop Carriers (SLC)
Parallelized and byte-multiplexed tributaries and encrypted algorithm, 245
Passive optical network (PON), 84
 architecture, 84–85
 reality in WDM system access, 94–95
 topology
 installation methods, 86–87
 protection strategies and traffic symmetry, 86
 in WDM system access, 83–97
Path overhead, in SONET frames, 18
Path protected mesh network (PPMN), 105–106
 See also Next generation mesh networks
Payload length indication (PLI), 115
Payload type identification (PTI), 140
PBX (Public business exchange), 7
Peak cell rate (PCR), 178
Perfect number, 204
Performance metrics, definitions, 160
Performance vector in-service and in real time, 238
Permutation cipher, 209
Phase distortion and dispersion in optical communication networks, 150
Phase lock loop (PLL), in communication networks, 143–145
Phase shift of wave, in optical communication, 61
Photodetector responsivity in optical networks, 156–157
Platinum grade cryptographic method, 213
Pockel effect, in electro-optic effect, 62
Poincaré sphere and states of polarization (SoP), 226–227
Point-to-multipoint topology, 90
Point-to-point networks, fault protection in, 186
Point-to-point protocol (PPP), 44–46
Point-to-point topology in DWDM networks, 74–75
Polarization-based quantum key distribution, 226–229
Polarization-dependent loss (PDL), 60, 67, 69, 164
Polarization distortion, in optical communication networks, 150
Polarization hole burning (PHB), 164
Polarization mode dispersion (PMD), 68, 150, 154, 164
Polarization-preserving fiber (PPF), 67
Polybius square, 192
POTS (plain old telephone service), 1, 6
Power-bandwidth ratio (PBR), 162–163
Power density in optical communication, 66
Power loss in optical communications, 57–58
Primary reference timing source (PRS), 81
 clock accuracy, 142
Prime numbers, 203–204
Probabilistic approach in channel performance, 161–162
Pseudorandom bit sequences (PRBS), 161
Public key cryptography, 199
Public-switched digital network (PSDN), 195, 196
Public switch transport network (PSTN), 7
 and SS7 protocol, 5–8
Pull-in/hold-in of PLL parameter, 143
Pulse coded modulation (PCM), 1
Pulse-width distortion jitter (PWDJ), 152, 154
Quality of service (QoS), and ATM protocol, 30
Quantization noise and error in optical communication networks, 149
Quantum computing, 214
Quantum cryptography, 213–215
 vulnerabilities in, 234–236
Quantum key distribution
 entangled states and quantum teleportation, 229–231
 polarization-based, 226–229
Quantum key distribution (QKD), 225–226
Quantum mechanics (QM) theory, 214
Quantum oblivious transfer, 225
Quantum teleportation, 229–233
Raman
 amplification in DWDM, 70–71
 gain efficiency, 71
 super-continuum, 70
Random Jitter, 152
Random walk FM (RWFM), 148
Rayleigh scattering, 57
RC4 algorithm, 210–211
Real-time control protocol (RTCP), 41
Real-time transport (RTP) protocol, 41
Reconfigurable OADMs (ROADM), 177, 186, 187
Reed-Solomon EDC code, 131
Resilient packet ring (RPR)
 network architecture, 53
 packet format and services, 52
Rijndael algorithm, 210
Ring–mesh network (RMN), 38
Ring-networks, classification and fault protection in, 188–189
Ring topology, in DWDM networks, 74, 79
RMS jitter, 152
Root mean square of time interval error (TIErms)
 model, 147
Routing algorithms, 178–179
Routing and wavelength assignment (RWA)
 algorithms, 179
RS and FECs codes, 130
Section overhead, in SONET frames, 18
Security coding, mathematical foundations
 fields, 208
 greatest common divisor, 205–206
 groups, 206–207
 modulus arithmetic, 204–205
 prime number, 203–204
 rings, 207

- Security levels, 200
 Security networks, classification of, 236
 Segmentation and reassembly (SAR) process, 25
 Self-phase modulation (SPM) noise, 155, 164
 Semantic transparency, 31
 Semiconductor optical amplifiers (SOA), in DWDM, 73, 186
 Service control point (SCP), 7
 databases maintained by, 8
 Service level agreement (SLA), 159, 177
 in ATM protocol, 30–31
 Service management layer (SML), 77
 Service node interface (SNI), 85
 Service switching point (SSP), 7, 8
 Severely errored period (SEP), 160
 Severely errored period intensity (SEPI), 160
 Severely errored second ratio (SESR), 160
 Severely errored second (SES), 160
 Severely error frame (SEF), 146
 Shamir's key distribution method, 215
 Shannon's limit, in network performance, 163
 Shift Cipher method, applicability of modulus arithmetic to, 205
 Short-haul optical networks, 186
 Short reach (SR), *see* Short-haul optical networks
 Shot noise, 148
 Signaling network management protocol (SNMP), 77
 Signal quality, in communication network, 147–149
 noise sources, 148–149
 quantization noise, 149
 Signal to noise power, 149
 Signal to noise ratio (SNR), 161
 analysis, in channel performance, 165–167
 statistical estimation method, 168–170
 Signal to quantization noise ratio (SNR_q), 149, 162
 Signal transfer point (STP), 7
 types of, national and gateway, 8
 Silica fiber, in fiber-optic communications, 63
 Single-fiber ring (1-F), 74
 Single-mode fiber (SMF), 16, 36, 65, 66
 Single optical channel, 115
 Single-wavelength path connectivity, 175
 Sinusoidal Jitter (SJ), 151, 152, 154
 Skytale message writing method, 192
 Sliding-window flow control, 26
 SONET/SDH (synchronous optical networks), 110–111, 115, 120–121, 123–127
 ATM and, 32
 bit rates in, 4
 in communication networks, 144–145
 data services, 101–104
 ethernet ports on, demands for, 4
 frames in
 features of, 17
 overheads, 18–19
 synchronization issue, 19
 frequency justification in, 151
 introduction, 15–17
 maintenance of, 23–24
 network layers in, 17
 protocol, 184, 243
 standard interfaces, 15–16
 STS-1 frame, 17–18
 STS-N frames
 concatenation in, 22–23
 scrambling process in, 23
 success factors, 15
 topologies in, 16
 virtual tributaries (VT) in
 capacity of, 20
 definition, 19
 multiplexing of, 21
 transportable bandwidth, 21
 vs. SDH, 16
 WDM, 103
 See also Next generation SONET/SDH networks
 Spartans and secret messages, 192–194
 Specific size tributary unit, 101–102
 See also SONET/SDH (synchronous optical networks)
 SS7 (*signaling system 7*) network, functional nodes of, 7
 Star topology, 75
 Statistical estimation method and vector, 238
 Steganogram, 199
 Stimulated Brillouin scattering (SBS), 164
 Stimulated Raman scattering (SRS), 70, 164
 Stokes noise, 68–69, 154–155
 Stop-and-wait flow control, 26
 Storage area network (SAN), 36
 Stream cipher algorithm, 199
 Subscriber Loop Carriers (SLC), 7
 Substitution/random shift cipher, 209
 Superblock construction CRC, 121
 Supervisory channel (SUPV), 108, 181
 Sustainable cell rate (SCR), 178
 Switched multi-megabit data services (SMDS), 39
 Switches “static”, 8
 Symmetric and shift ciphers, 208–209
 Symmetric cryptography, 198
 Synchronization in optical communication network
 in communication networks, 141–146
 impairments, 145–146
 See also SONET/SDH (synchronous optical networks)
 Synchronized clock types, 142–144
 Synchronous and asynchronous network, data services, 101–104
 Synchronous optical networks, *see* SONET/SDH (synchronous optical networks)
 Synchronous transport signal level-N (STS-N), in SONET, 15
 TDM, *see* Time division multiplexing (TDM)
 TDM-PON
 vs. WDM-PON in WDM system access, 89
 in WDM system access, 87–89
 Telecommunications management network (TMN), 244
 five-layer architecture, 77

- Telecommunications non-optical network, bit rates in, 3
Teleportation
concept for quantum key distribution, 232
quantum, and entangled states, 229–231
Terabits, 4
Terminal transmission equipment (TTE), 130
Text integrity/security, 201
Thermal (or Johnson) noise, 148
Time deviation (TDEV) model, 147
Time division multiplexing (TDM), 87, 133
and data traffic, comparison of, 27
Time interval error (TIE), assessment, 147
Timing and synchronization, in digital communications, 81
Timing signal, in optical communication network, 146–147
Traffic and service convergence, 101–104
Traffic barrier, breaking of, 3–5
Traffic control, centralized, 173
Traffic management and control
client bandwidth management, 175
congestion management in DWDM, 178
management of traffic, 177–178
node and network provisioning, 180
optical network topology discovery, 179
routing algorithms, 178–179
wavelength management
ROADMs paths, 177
single and multi-wavelength path connectivity method, 175–177
strategies, 180–181
Traffic performance and service performance, 159
Trail trace identification (TTI), 139
Transmission
of analog electrical signals, 1
digital, and analog, 1–3
medium, 2
Transmission control protocol (TCP), 39–40
Tributaries, parallelized and byte-multiplexed, and encrypted algorithm, 245
Tributary protection, mesh networks, 187–188
Tributary units (TU), in SDH, 20–22
Trusted third party/Key Escrow encryption system, 225
Twisted pair wire, transmission of analog electrical signals, 1
Two-fiber ring (2-F), 74

Ultraband services, 9–10
Unconstrained path routing, in DWDM routing, 82–83
Unconstrained routing algorithm, 179
Uncorrelated bounded Jitter (UBJ), 152, 154
Unipolar signal with noise, threshold point, 165
Unit interval peak-to-peak (UIpp), 135, 152
Unit Interval (UI), 135
User datagram protocol (UDP), 40
User-to-network interface (UNI), 75–76, 85, 177

Variable bit rate (VBR), 177
VCSEL lasers, 36
Vector estimation
circuitry for performance, 239
full-duplex link with performance, 240
Vertical cavity surface emitting lasers (VCSEL), 63
Videophone, 1
Virtual containers (VC), 5
Virtual tributaries (VT), 102, 127
in SONET, 5, 20–21
See also SONET/SDH (synchronous optical networks)
VLAN tagging, 34
Voice and data networks
circuit switched *versus* store and forward, 10–12
data networks and protocols, 8–9
narrowband, broadband, and ultraband services, 9–10
optical networks
reliability of, 12
security in, 12–13
traffic and services evolution in, 12
PSTN and , protocol, 5–8
Voice over IP
protocols for, 43
services by, 42
Voice services, 101

Wander, in optical communications networks, 150–153
WAN interface sub-layer (WIS), 36
Watermarking, 199
Wavelength assignment (WA), 78
algorithms, 83, 179
problem, in DWDM network, 82
Wavelength collision in DWDM, 176
Wavelength concatenation (WC), 82
Wavelength division multiplexing (WDM), 4, 55, 103, 110–111, 113–115, 242
mesh network, 78–80
optical technology, 5
system access, 83–84
CWDM-PON, 87
free space optical, 95–97
FSO in, 95–97
hierarchical CWDM/TDM-PON, 89–94
PON reality, 94–95
PON topology, 84–87
TDM-PON, 87–89
TDM-PON *versus* WDM-PON, 89
Wavelength management, 107–108
in DWDM
ROADMs paths, 177
single and multi-wavelength path connectivity method, 175–177
strategies, 180–181
resource management, 107–108
Wavelength switching, of network switching, 78
WDM, *see* Wavelength division multiplexing (WDM)
WDM technology and networks in communications systems
DWDM networks, 73–83
channel and link protection, 81–82

- DWDM network topologies, 74–75
DWDM routing, 82–83
network switching, 78–80
optical network interfaces, 75–77
timing and synchronization, 81
(OADM), 73
optical amplifiers, 69–70
 EDFA amplification, 71–72
 Raman amplification, 70–71
 SOA amplification, 73
optical communications spectrum, 63–65
optical fiber in communication network, 55–56
 light propagation in fiber, 57–63
 light propagation in matter, 56–57
optical fiber types, 65–66
 fiber birefringence and dispersion, 67–69
 non-linear phenomena, 69
 optical power limit, 66
White (random) frequency and phase modulation
 (WFM/WPM), 148
World Economic Forums, 3