Unlike traditional enterprise networks, where users connect to IT resources within an organization’s demilitarized zone (DMZ), next generation networks (NGN) serve users logging onto virtualized resources from a diverse array of devices and locations. Clearly, NGNs require an integrated approach to the management of security rather than unmanageable and non-integrated add-on solutions.

In contrast to most books on the subject, which limit coverage of security management to discussions of SNMP authentication and confidentiality mechanisms, this book considers it a governance issue that needs to follow the “Plan, Do, Check, and Act” approach pioneered by W. Edwards Deming. Following an account of the evolution of standardized network management concepts over the last twenty years, author Stuart Jacobs:

• Analyzes existing security standards and management frameworks of NGNs
• Reviews authentication, authorization, confidentiality, integrity, non-repudiation, vulnerabilities, threats, risk management, and other key security concepts
• Details effective approaches to encryption and associated credentials management/control
• Considers secure interoperability between telecommunications service provider management systems and between service providers over security domain boundaries
• Highlights the critical need for well-organized information security policies, security structures, and approaches for clearly defining security requirements and security procedures
• Presents an integrated security management framework that expands on TMN and eTOM security functional areas
• Provides in-depth coverage of operations security (OPSEC)—the area in which the “Act” and “Check” aspects are most fully realized

Security Management of Next Generation Telecommunications Networks and Services is a valuable resource for telecommunications and IT professionals, as well as enterprise systems engineers/architects.

STUART JACOBS is Principal Consultant for YCS Consulting LLC and a Lecturer at Boston University Metropolitan College. He serves as an Industry Security Subject Matter Expert for the Telecommunications Management and Operations Committee (TMOC) of the Alliance for the Telecommunications Industry Solutions (ATIS). Mr. Jacobs has also served as a technical editor of ATIS Joint Committee Technical Reports and ITU-T Recommendations.
SECURITY MANAGEMENT OF NEXT GENERATION TELECOMMUNICATIONS NETWORKS AND SERVICES
IEEE Press
445 Hoes Lane
Piscataway, NJ 08854

IEEE Press Editorial Board 2013
John Anderson, Editor in Chief

Linda Shafer  Saeid Nahavandi  George Zobrist
George W. Arnold  Om P. Malik  Tariq Samad
Ekram Hossain  Mary Lanzorotti  Dmitry Golgof

Kenneth Moore, Director of IEEE Book and Information Services (BIS)
SECURITY MANAGEMENT OF NEXT GENERATION TELECOMMUNICATIONS NETWORKS AND SERVICES

Stuart Jacobs

IEEE Press
Series on Networks and Services Management
Thomas Plevyak and Veli Sahin, Series Editors

Sponsored by
IEEE COMMUNICATIONS SOCIETY

IEEE Press

WILEY
This book is dedicated to my wife, Eileen, for her patience with my spending so much time at the keyboard rather than with her.
CONTENTS

Preface xi
Acknowledgments xv

1 INTRODUCTION 1
1.1 Evolution of Networking Concepts 4
  1.1.1 The Public Switched Telephone Network 4
  1.1.2 Computer/Data Communications Networks 5
  1.1.3 Network Architectures 6
  1.1.4 Data Network Complexity 8
1.2 A Network Security Historical Perspective 13
  1.2.1 ISO/IEC 7498–1 (ITU-T X.200) Coverage of Management 14
  1.2.2 ISO/IEC 7498–4 (ITU-T X.700) Coverage of Security Management 15
  1.2.3 ISO/IEC 7498–2 (ITU-T X.800) Coverage of Security and Management 15
  1.2.4 The Security Frameworks (ITU-T X.810–ITU-T X.816) 23
  1.2.5 The ITU-T X.805 Approach to Security 25
1.3 Network and Security Management Systems 26
  1.3.1 Element and Network Management Systems 26
  1.3.2 Operations Support Systems 27
1.4 Evolution of Network and Security Management Concepts 29
  1.4.1 Telecommunications Management Network 29
  1.4.2 Next Generation Operations Systems and Software 47
  1.4.3 Enhanced Telecom Operations Map 50
1.5 How the Need for Information Security has Changed 57
1.6 Summary 61
Further Reading and Resources 62

2 OVERVIEW OF CURRENT AND FUTURE NETWORKS 63
2.1 A Little Network History 63
  2.1.1 Point-to-Point Data Communications 64
2.1.2 Early Commercial Packet Switching 64
2.1.3 The ARPANET: Internet 64
2.1.4 Ethernet and IEEE 802.3 70
2.1.5 Network Address Translation 71
2.2 Common Network Organizations 72
  2.2.1 Wired Local Area Networks 74
  2.2.2 Wireless Networks 83
  2.2.3 Metropolitan Area Networks 87
  2.2.4 Wide Area Networks 94
  2.2.5 Networks Are Now Layered upon Networks 96
  2.2.6 Additional Networking Developments 96
  2.2.7 Security Mechanisms in Modern Networks 105
2.3 Next-Generation Networks and Interfaces 108
  2.3.1 Framework and Topology of the NGN 108
  2.3.2 IP Multimedia Subsystem 125
2.4 Summary 133
Further Reading and Resources 136

3 SECURITY MANAGEMENT IN CURRENT AND FUTURE NETWORKS 139
  3.1 Cybercrime as a Driver for Information Security Management 140
  3.2 Governance as a Driver for Information Security Management 142
    3.2.1 What Is Governance? 142
    3.2.2 Information System Security Governance 143
  3.3 Information Security Management Frameworks 145
    3.3.1 ISO/IEC 27000 Series 146
    3.3.2 The Information Technology Infrastructure Library Framework 164
    3.3.3 COBIT Framework 167
    3.3.4 FISMA Framework 173
  3.4 A Holistic Approach for Security Management 176
    3.4.1 Organizational Aspects of Security Governance and Management 176
    3.4.2 Policies and Policy Hierarchies 180
    3.4.3 Functional and Operational Security Requirements 183
  3.5 Summary 189
Further Reading and Resources 189

4 RISK MANAGEMENT IN CURRENT AND FUTURE NETWORKS 191
  4.1 Asset Identification: Definition and Inventorying 193
  4.2 Impact Analysis 224
    4.2.1 Existing System Impact Analysis 224
CONTENTS

4.2.2 New System Impact Analysis 236
4.2.3 Risk Mitigation Analysis 240
4.2.4 Malicious Security Events and Threat Assessment 243
4.3 Risk Mitigation Controls Acquisition or Development 257
  4.3.1 Procedural Risk Mitigation Controls 257
  4.3.2 New Technical Risk Mitigation Controls 258
4.4 Risk Mitigation Controls Deployment Testing 273
4.5 Summary 274
Further Reading and Resources 275

5 OPERATIONAL MANAGEMENT OF SECURITY 277
  5.1 Securing Management Applications and Communications 278
    5.1.1 Security within Element and Network Management Systems 278
    5.1.2 Telecommunications Management Network Security 279
    5.1.3 Operations Support System Security Needs 281
    5.1.4 Reflections on Past ITU Treatment of Managing Security 285
    5.1.5 Management of Security Services and Mechanisms Revisited 288
    5.1.6 A Security Management Framework 291
  5.2 Security Operations and Maintenance 296
    5.2.1 Operational Security Compliance Programs 297
    5.2.2 Security Operations Reviews and Audits 301
    5.2.3 Security Event Response and Incident Management 302
    5.2.4 Penetration Testing 304
    5.2.5 Common Criteria Evaluated Systems 306
    5.2.6 Accreditation and Certification 309
  5.3 Withdrawal from Service 312
  5.4 Summary 314
  5.5 Concluding Remarks 314
Further Reading and Resources 314

APPENDICES

Italicized appendices will be available at http://booksupport.wiley.com

Appendix A: Role of Cryptography in Information Security

Appendix B: Authentication of Subjects

Appendix C: Network Security Mechanisms

Appendix D: Example Company Security Policy
Appendix E: Example Generic Detailed Security Requirements

Appendix F: Securing Common Network Protocols

Appendix G: Security Mapping between M.3400 and M.3050

Appendix H: State Privacy Laws as of 2010

Appendix I: Example RFP Security Appendix

Appendix J: RFP Security Analysis of ABC Proposal

Appendix K: Example Security Statement of Work

Appendix L: Example Solaris Operating System Audit Procedures

Appendix M: Example Procedure for Basic Hardening of a Windows XP Professional Operating System

Appendix N: Example Network Audit Procedure

Appendix O: Example Unix–Linux Operating System Audit Procedures

Index
This book focuses on the management of information security in next generation networks from the viewpoint of a telecommunications service provider, commercial enterprise or any other type of networked organization as a governance issue that needs to follow the “Plan, Do, Check and Act” approach promulgated by W. Edwards Deming and captured in ISO Standard 27001 as it applies to the management of security. Following a review of the evolution of standardized network management concepts and how networking concepts and context have grown in complexity over the last 20 years, the need for security governance is discussed. Under governance, not only are current management frameworks considered, the need for well-organized information security policies, security organizational structures, approaches for establishing security procedures, and development of security requirements are discussed. Risk management, a core component of information security governance, is then covered starting with asset inventory capture and categorization through vulnerability identification, threat determination, risk mitigation, and prioritization of mitigation plans. The subject of operations security (OPSEC) is then dealt with as OPSEC is where the Deming “Act” and “Check” aspects are most fully realized. The security governance concepts presented herein are equally applicable to both legacy and next generation network environments. A significant number of appendices useful to industry professionals and students are included, which provide examples of information security policies, detailed security requirements derivation, request for proposal security material, evaluation of proposal security submissions, security statements of work for contracts, and operations security procedures for auditing and platform hardening. Three appendices provide overviews covering the role of cryptography in information security, authentication of subjects, network security mechanisms, and securing network protocols.

ORGANIZATION

Chapter 1 discusses:

- How the very concept of networking has evolved over time;
- The evolution of network security concepts from a standards perspective;
- Network and security management systems;
- The evolution of network and security management concepts; and
- How the management of information security needs have changed over time.
Chapter 2 discusses:

- How modern networks have evolved over time;
- Common network organizations including wired, wireless metropolitan area, wide area, Supervisory Control and Data Acquisition (SCADA), sensor networks and clouds;
- Next Generation Network framework and architecture concepts; and
- The evolving Internet Protocol (IP) Multimedia Subsystem organization of services.

Chapter 3 discusses:

- How cybercrime has become a significant information security driver;
- The evolution of Information Security Governance into a core organizational management component;
- The primary Information Security management frameworks and the relative advantages/disadvantages to each framework; and
- A holistic information security management approach leveraging the strengths of existing frameworks.

Chapter 4 discusses:

- Asset identification and developing an inventory of organizational assets;
- Analyzing the impact when organizational assets are damaged, lost, or made unavailable due to accidental or malicious human activities;
- Procedural risk mitigation controls;
- Technical risk mitigation controls acquisition or development; and
- Risk mitigation controls deployment testing.

Chapter 5 discusses:

- Security within Element and Network Management Systems;
- Telecommunications Management Network Security;
- Operations Support Systems Security Needs;
- A Security Management Framework as defined by ITU-T Recommendation M.3410;
- Operational Security Compliance Programs;
- Security Operations Reviews and Audits;
- Security Event Response and Incident Management;
- Penetration Testing;
- Common Criteria Evaluated Systems;
- Accreditation and Certification; and
- Withdrawal from service.
Also included are a variety of appendices as follows:

- **Appendix A**: Provides a synopsis of basic cryptography concepts, explores major aspects of crypto-analysis and key management, and describes the primary approaches for cryptographically based authentication.

- **Appendix B**: Describes the Kerberos authentication system, public key management via Public Key Infrastructures (PKI), reviews issues associated with human authentication, and describes the capabilities of RADIUS-, LDAP- and Diameter-based authentication.

- **Appendix C**: Reviews the Data Link Layer Security Mechanisms (IEEE 802.1q, IEEE 802.1x, IEEE 802.11i), the IP Security (IPsec) inter-networking security mechanism, network authorization and access control mechanisms (Firewalls, Application-level Gateways, and IPS/IDS), Transport protocol security mechanisms (TLS, DTLS, SSL, and Secure Shell), Application Security Mechanisms, Web Application Security Mechanisms (XML, SOA, SOAP, and SAML), and Anti-Malware Applications, Host-based Firewalls, Modification Scanners, and Host-based IPS/IDS.

- **Appendix D**: Provides an example Organization security policy document based on the ISO/IEC 27002 standard that can serve as a starting point for developing customized policy documents.

- **Appendix E**: Provides an example decomposition of the example security policy document in Appendix D into detailed enterprise security functional requirements that can serve as a starting point for developing customized policy documents.

- **Appendix F**: Provides an overview of commonly used networking protocols in the data link, inter-networking, transport, and application layers along with known attacks that leverage vulnerabilities within different protocols.

- **Appendix G**: Provides a comparison of security functionality covered by ITU-T Recommendations M.3400 and M.3050.

- **Appendix H**: Lists the state level personally identifiable information privacy—breach notification laws enacted within the United States as of 2010.

- **Appendix I**: Provides an example set of detailed information security-related functional requirements that can be used in Requests for Proposals (RFPs).

- **Appendix J**: Provides an example Microsoft Excel spreadsheet that can be used for evaluating supplier proposals based on the requirements found in Appendix I.

- **Appendix K**: Provides an example Security Statement of Work that can be used in contract negotiations.

- **Appendix L**: Provides an example set of Solaris Operating System security audit procedures.

- **Appendix M**: Provides an example set of Microsoft XP Operating System security hardening procedures.

- **Appendix N**: Provides an example set of network security audit procedures.

- **Appendix O**: Provides an example set of generic Unix Operating System security audit procedures.
TARGET AUDIENCE
The major audiences for this book are:

- Graduate students studying Computer/Information Sciences/Engineering, Systems Engineering, and Technology/Business Management, and
- Professionals in the telecommunications field that rely on reliable and trustable information processing and communications systems and infrastructures.

ABOUT THE AUTHOR

Stuart Jacobs holds the position of Lecturer on the faculty in the Boston University Metropolitan College Computer Science (MET CS) department. Stuart’s responsibilities include teaching graduate courses on “Enterprise Information Security,” “Network Security,” and “Network Forensics” along with serving as the MET CS department security curriculum coordinator with responsibility for all MET CS security courses.

Stuart has served as an Industry Security Subject Matter Expert for the Alliance for the Telecommunications Industry Solutions (ATIS) and has served as the Technical Editor of the ATIS Technical Report “Information & Communications Security for NGN Converged Services IP Networks and Infrastructure” and as the Technical Editor of ITU-T M.3410, “Guidelines and Requirements for Security Management Systems.”

Stuart retired from Verizon Corporation in 2007 where he was a Principal Member of the Technical Staff with responsibility for security architecture development, security requirements analysis, and standards development activities. As Verizon’s lead security architect, Stuart was the lead engineer for security on numerous Verizon network equipment RFPs and provided security consulting on wireless and wired networks, SS7, CALEA/LI, vulnerability analysis, intrusion detection, and systems engineering methodologies. Additionally, Stuart served as Verizon’s security subject matter expert for ANSI-ATIS, ITU-T, TMF, OIF, MSF, OMG, and IETF activities. In addition to his other duties, Stuart has also pursued applied research in network design and security, in particular wireless networks, public key infrastructures, network authentication schemes, distributed computing security mechanisms (including autonomous agent systems, authentication mechanisms for Mobile IP, Mobile Ad-Hoc Self Organizing Networks, and Intelligent Agents) for government and commercial organizations and agencies.

Stuart holds an MSc. degree and CISSP certification; he is completing a Ph.D. degree in Information Systems with a concentration in security and is a member of the:

- Institute of Electrical and Electronics Engineers (IEEE),
- IEEE Computer Society,
- Association for Computing Machinery (ACM), Senior Member,
- International Information Systems Security Certification Consortium (ISC)², and
- Information Systems Security Association (ISSA), Senior Member.
I would like to thank Thomas Plevyak for encouraging me to write this book; Thomas Plevyak and Veli Sahin, the IEEE Press Network Management Series Editors, for all their constructive comments and suggestions; the anonymous reviewers for their comments and advice; my former Verizon co-workers; and members of the New England chapter of the ISSA.
INTRODUCTION

At the very outset of this book, questions worth asking are:

- What is the author referring to by the word “security?”
- What is the author referring to by the words “security management?”
- What are next-generation networks and services?

Security is a word whose meaning seems to change depending on the context where it is used and by the “mindset” or background of the individual. Some people think security is solely about “chain-link” fences, security guards, burglar alarms/video cameras, etc. Other people think security is about the use of encryption, login passwords, “firewalls,” etc. Then there are those who believe security is only an issue for military-intelligence type organizations and of no importance, or a hindrance, to commercial and other enterprises, as allegedly overheard at a meeting of security people (Kaufman et al., 2002):

Speaker: Isn’t it terrifying that on the Internet we have no privacy?
Heckler 1: You mean confidentiality. Get your terms straight.
Heckler 2: Why do security types insist on inventing their own language?
Heckler 3: It’s a denial of service attack.
The aforementioned simply exemplifies how words become confused, misused, or ambiguous, when talking about security.

This problem just grows when the phrase “security management” appears. Does security management refer to:

- the management of technology related to security?
- the management of security activities?
- security for information processing management activities?
- security of organizational management activity?

or

- all of the above?

Again it depends on the individual as to which of the aforementioned is germane.

Then there is the term “Next-Generation Network,” usually abbreviated as NGN. What is an NGN? What technologies are used by an NGN? How does an NGN differ from today’s Internet Protocol (IP)-based networks and the existing Public Switched Telephone Networks (PSTNs)? A wide number of subjects need to be considered to answer the previous questions and should be addressed in an order that builds upon a number of foundation concepts.

The goal of this book is to provide an answer to these questions. This chapter discusses:

- How the very concept of networking has evolved over time;
- The evolution of network security concepts from a standards perspective;
- Network and security management systems;
- The evolution of network and security management concepts;
- How the management of information security needs have changed over time.

Chapter 2 discusses:

- How modern networks have evolved over time;
- Common network organizations including: wired, wireless, metropolitan area, wide area, Supervisory Control and Data Acquisition (SCADA), sensor networks, and clouds;
- Next-Generation Network framework and architecture concepts;
- The evolving IP Multimedia Subsystem (IMS) organization of services.

Chapter 3 discusses:

- How cybercrime has become a significant information security driver;
- The evolution of information security governance into a core organizational management component;
• The primary information security management frameworks and the relative advantages/disadvantages to each framework;
• A holistic information security management approach leveraging the strengths of existing frameworks.

Chapter 4 discusses:
• Asset identification and developing an inventory of organizational assets;
• Analyzing the impact when organizational assets are damaged, lost, or made unavailable due to accidental or malicious human activities;
• Procedural risk mitigation controls;
• Technical risk mitigation controls acquisition or development;
• Risk mitigation controls deployment testing.

Chapter 5 discusses:
• Security within Element and Network Management Systems (EMS/NMS);
• Telecommunications Management Network (TMN) Security;
• Operations Support Systems (OSSs) Security Needs;
• A Security Management Framework as defined by ITU-T Recommendation M.3410;
• Operational Security Compliance Programs;
• Security Operations Reviews and Audits;
• Security Event Response and Incident Management;
• Penetration Testing;
• Common Criteria Evaluated Systems;
• Accreditation and Certification;
• Withdrawal from service.

Also included are a wide variety of appendices including:

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Presents</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Provides a synopsis of basic cryptography concepts; Explores major aspects of crypto-analysis and key management; and Describes the primary approaches for cryptographically based authentication.</td>
</tr>
<tr>
<td>B</td>
<td>Describes the Kerberos and Public Key Infrastructure (PKI) authentication systems; Reviews issues associated with human authentication; Describes the capabilities of RADIUS-, LDAP- and Diameter-based authentication.</td>
</tr>
<tr>
<td>C</td>
<td>The Data Link Layer Security Mechanisms IEEE 802.1q, IEEE 802.1x, IEEE 802.11i; The IP Security (IPsec) inter-networking Security Mechanism; Network Authorization and Access Control mechanisms for: Firewalls, Application-level Gateways and IPS/IDS; Transport protocol security mechanisms: TLS, DTLS, SSL and Secure Shell (SSH); Application Security Mechanisms; The Web application Security Mechanisms: XML, SOA, SOAP and SAML; and</td>
</tr>
</tbody>
</table>
1.1 EVOLUTION OF NETWORKING CONCEPTS

Through the 1960s and 1970s, there were two approaches to networking:

- the Public Switched Telephone Network (PSTN), commonly referred to as telephony, and
- computer/data communications networks.

Each approach evolved independently of the other and represented very different views regarding how devices should communicate and who should control the technology.

1.1.1 The Public Switched Telephone Network

The Public Switched Telephone Network (PSTN) was a government-sanctioned and regulated monopoly of “telephone companies” with about 65% owned and operated by AT&T,\(^1\) about 30% owned and operated by GTE,\(^2\) with the remaining 5% by some 20 very small independent owners/operators. As AT&T represented the largest PSTN

---

\(^{1}\) American Telephone & Telegraph Corporation (AT&T), also referred to as the Bell System.

\(^{2}\) General Telephone & Electronics (GTE).
operator, its Bell Laboratories was the driving force for the development of most PSTN technologies (especially network interfaces and protocols), since the other much smaller operators all had to interconnect with AT&T’s infrastructure. Only following the 1968 U.S. Supreme Court “Carterphone” decision (and FCC ruling 13 F.C.C.2d 420), regarding modems, were devices not supplied by the telephone company allowed to be interconnected to telephone networks. Even after the “Carterphone” decision, up through the 1990s, PSTN technology evolution was primarily controlled by PSTN operating companies and their equipment suppliers. Starting in the 1990s, Standards Development Organizations (SDOs) and industry forums began to have a major impact on PSTN technology. The major SDOs and forums impacting PSTN technology development have been the:

- International Telecommunication Union-Telecommunications (ITU-T) Standardization Sector whose predecessor was the International Telegraph and Telephone Consultative Committee (CCITT);
- Telecommunications Industry Association (TIA);
- Alliance for Telecommunications Industry Solutions (ATIS);
- European Telecommunications Standards Institute (ETSI);
- International Standards Organization (ISO); and
- 3rd Generation Partnership Project (3GPP).

Presently, these and numerous other organizations have assumed a significant role in defining how telephony-related technology should evolve.

1.1.2 Computer/Data Communications Networks

Computer/data communications network technology through the 1960s and 1970s was predominately controlled by computer manufacturers who developed network capabilities specifically to support their proprietary product lines. During this era, IBM\(^4\) represented over 70% of all computers sold; consequently, other computer manufacturers routinely provided some degree of interoperability with IBM’s networking technology. Virtually all of these proprietary computer networking capabilities were based on bit synchronous link protocols and used of an end-to-end connection approach between end computer systems. Each computer manufacturer developed their unique networking capabilities according to a proprietary network architecture\(^5\) that was not subject to non-company external review or approval. In the 1980s, work on the concept of connectionless packet networking, independent of any single computer manufacturer, started to mature with the publication of the U.S. Government Defense Advanced Research Projects Agency sponsored, and in many cases Internet

\(^3\) A modem (modulator-demodulator) is a device used for converting digital signals into, and recovering them from, quasi-analog signals suitable for transmission over analog communications channels such as the PSTN.

\(^4\) IBM was the common abbreviation for the International Business Machine Corporation.

\(^5\) A network architecture specifies the design of a communications network via a framework for the specification of a network’s physical components, functional organization, protocols, data/message formats, and operational principles and procedures.
Engineering Task Force published, Request for Comments (RFCs) 791, 792, and 793 (defining IPv4, ICMPv4, and TCPv4) that are the foundation protocols for the modern Internet Suite of protocols and defined basic packet internetworking and end-to-end transport capabilities for generalized connectionless networking. By the early 1990s, IPv4 and TCPv4 had become de facto standards for computer-to-computer communications with the responsibility for these, and many other protocols, under the control of the Internet Engineering Task Force (IETF). Virtually all computers now include native Internet Protocol (IP-) and Transmission Control Protocol (TCP)-based communications capabilities. It must be noted that IETF protocol development does not follow any formalized network architecture beyond relying on the use of IP, TCP, and User Datagram Protocol (UDP).

### 1.1.3 Network Architectures

The first approach to developing a non-proprietary network architecture resulted in the publication by the ISO of document ISO/IEC 7498-1 in 1984, known as the Open System Interconnect (OSI) model. It was quickly followed by three other standards, ISO/IEC 7498–2, ISO/IEC 7498–3, and ISO/IEC 7498–4. The major contributions of these standards have been:

- Formal introduction of the concept of layering protocols, that operate on an end-to-end basis upon other protocols that provide interconnection/forwarding capabilities that provide basic communications link functions;
- The concept that a protocol should only utilize information about another protocol (either above it or below it) that is available via a well-defined interface, thereby allowing the internal structure or operation of a protocol to be changed without negatively impacting other protocols; and

---

6 RFC 791, INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, September 1981.
7 RFC 792 INTERNET CONTROL MESSAGE PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, September 1981
8 RFC 793, TRANSMISSION CONTROL PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, September 1981
10 The OSI model goal was to get industry participants to agree on common network standards to provide multi-vendor interoperability.
• Recognition that more than just protocols are necessary for a network architecture, namely, it:
  ◦ provided formalized descriptions of protocol concepts for multiple protocol layers (ISO/IEC 7498–1);
  ◦ introduced a standardized approach for the consideration of communications security capabilities (ISO/IEC 7498–2);
  ◦ recognized the need for standardized naming, addressing, and directory capabilities (ISO/IEC 7498–3); and
  ◦ presented a framework and basic concepts for the management of communications components, features, and services (ISO/IEC 7498–4).

Although the seven protocol layers and specific protocols specified within these ISO standards have not been widely adopted, the general concepts from:

• ISO/IEC 7498–1 (aka ITU-T X.200) of protocol layering and well-defined interprotocol interfaces are widely accepted;
• ISO/IEC 7498–2 (aka ITU-T X.800) for communications security services, security mechanisms, and the management of security mechanisms are considered the de jure definitions for security; and
• ISO/IEC 7498–4 (aka ITU-T X.700) for the management of communications devices, in the form of Fault, Configuration, Accounting, Performance, and Security Management (the “FCAPS” of management), are considered the de jure areas that network management focuses upon.

Figure 1.1 highlights the relationship of protocol layer within the OSI protocol model versus the Internet Suite of protocols. Some consider Internet Suite application protocols to constitute layer 5 protocols.

![Figure 1.1. OSI Model and Internet Suite Protocol Layers.](image-url)
1.1.4 Data Network Complexity

Since the aforementioned ISO standards were published, the complexity of deployed networks has vastly grown. Chapter 2 will explore this increasing complexity in more detail. Up through the 1980s, computer-oriented networks were primarily single facility/location oriented with computers either directly interconnected or connected to a local area network (LAN) that may have included a number of segments interconnected by bridging devices (e.g., Ethernet layer 2 bridges). Interfacility/location interconnection of computers or LANs relied on the use of modems to attach the local network to the PSTN via a modem and dial-up lines/services or a channel service unit to a PSTN-operator-supplied leased line.\(^{14}\)

A “sea change” occurred in computer-data-networking with the concept of a router\(^ {15} \) which was under development through the 1970s and 1980s based on the use of minicomputers. These minicomputer router capabilities were, in this time frame, primarily limited to academic, government, and industrial research networks, given their expense and complexity. In the late 1980s, stand-alone multi-protocol connectionless routers became commercially available. These routing devices radically altered how computer networks were structured. From the late 1980s up to the present, router-based networks frequently utilize multiple routers to structure facility/location networks into logically separate subnets and tie multiple facility/location networks into enterprise networks that span geographic regions. High capacity versions of these routers have been instrumental to the evolution and growth of the Internet, which is really the router-based interconnection of a number of very large corporate or other enterprise-operated router networks. Figure 1.2 depicts the concept of a number of core (backbone) networks operated by AT&T, Verizon Business (formally MCI), Quest, Sprint, Level 3 Communications (L3), NTT Communications (NTTC) and Global Crossing (GBLX), “Tier 1” Internet Service Providers (ISPs), and an example set of commercial/residential access ISPs (the terms “alpha,” “bravo,” “delta,” “echo,” “tango,” and “zulu” are used rather than actual company names for these example commercial/residential access ISPs). The term wide area network (WAN) represents Tier 1 ISP-routed networks that span wide geographic regions, and the term “IP Metro Network” represents access ISP-routed networks that span metropolitan-size geographic areas. As shown in Figure 1.1, the “Internet” is not a single network but many interconnected networks used to interconnect millions of other networks and computers.

Another area of complexity not considered by the ISO standards is at layer 2 of the OSI model. At the time when the ISO standards were published, the OSI layer 2 for local networks was considered to be a simple ability to interconnect two devices in either:

- a point-to-point manner (also called direct connection) as shown in Figure 1.3;

\(^{14}\) A PSTN-operator-supplied leased line is a dedicated circuit between two different facilities at the link layer providing 56Kbps, 1.544 Mbps or sometimes 45 Mbps of bandwidth.

\(^{15}\) A router is a networking device tailored to the tasks of routing and forwarding information between two or more networks based on layer 3 protocol information unlike a bridge or layer 2 switch that forwards information between two or more network segments based on layer 2 protocol information.
Figure 1.2. The Internet Concept of Core and Access ISP Networks.
• a multi-drop manner where a number of devices are interconnected to a common physical medium such as with the early versions of Ethernet (i.e., 10base5 “thick-wire” and 10base2 “thin-wire” coaxial cabled Ethernet) as shown in Figure 1.4; or
• a “star” manner where a number of devices are interconnected to a common device such as with hubbed or switched versions of Ethernet (i.e., 10baseT over-twisted pair cabling) as shown in Figure 1.5.

Interconnection of LANs was expected to rely on some form of intermediate packet switching network, such as a commercially available X.25 network. During the 1990s timeframe, significant layer 2 technological developments resulted in the availability of Synchronous Optical Network (SONET) and Asynchronous Transfer Mode (ATM) layer 2 networking along with continued use of X.25 and its commercial successor Frame Relay networking. These developments resulted in interfacility interconnection of facility/location LANs often using two or three protocols below the layer 3 protocol (routinely IPv4). For example, an organization interconnecting routed subnets at three
1.1 EVOLUTION OF NETWORKING CONCEPTS

locations would configure their routers to use SONET links over which ATM would be used to transport Ethernet frames that carried IP packets. Figure 1.6 depicts various arrangements for layering protocols within layer 2.

In Figure 1.6:

- PON represents Passive Optical Networking
- MPLS represents Multi-protocol Label Switching
- xDSL represents various forms of Digital Subscriber Line technologies
- FR represents Frame Relay
- Serial represents asynchronous dial-up PSTN access
- 802.3 represents Ethernet
- 802.11 represents Wireless Ethernet (aka “WiFi”)
- PPP represents Point-to-Point Protocol
- PPPoE represents Point-to-Point Protocol over Ethernet.

What needs to be pointed out is that:

- SONET technology is not a simple direct-connect, multi-drop, or star technology but actually provides the ability to interconnect many devices in what are called
rings and even interconnect these rings into more complex organizations as shown in Figure 1.7; and

- ATM technology is also not a simple direct-connect, multi-drop, or star technology but actually provides the ability to interconnect many devices in a meshed manner, with multiple links exiting/entering each ATM switch allowing the construction of complex ATM interconnections as shown in Figure 1.8.