Helsinki University of Technology
Publications in Telecommunications Software and Multimedia
Teknillisen korkeakoulun tietoliikenneohjelmistojen ja multimedian julkaisuja
Espoo 1999 TML-XX

IP network management

Version November 5, 1999

Liisa Uosukainen Tuomas Lilja Lasse Metso

Seppo Ihalainen Jouni Karvo Ossi Taipale

Helsinki University of Technology
Department of Computer Science and Engineering
Telecommunications Software and Multimedia Laboratory

Teknillinen korkeakoulu
Tietotekniikan osasto
Tietoliikenneohjelmistojen ja multimedian laboratorio

Distribution:
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
P.O. Box 5400
FIN-02015 HUT
Tel. +358-9-451 2870
Fax. +358-9-451 5014

ISBN 951-XXX
ISSN 95Y Y

ABSTRACT

Author Liisa Uosukainen Tuomas Lilja Lasse Metso

Seppo I-halainen
Jouni Karvo
Ossi Taipale
Title IP network management

joo afsdj ad lökadfas lkökj lsdakj ldasjk ölasjk löadsfjök akjölasdfjk ölasdf öjkldfasj ölkasdf ökjlsdfja öjlkdfasj öklasdj ökjdsaj öklasdf jökldsafjö j ödsjök lasdöj klasdjök dasföj ö k-jadfsöj kasdföjk laöj kljöasdföj kasdföj asdfj ö

UDK koe
Keywords truth

ABBREVIATIONS

IP	Internet Protocol

1 INTRODUCTION

Networks and distributed processing systems have become critical factors in the business world. Companies and organizations develop large and complex networks with an increasing number of applications and users. The need for high capacity IP networks is growing because of the new WWW and multimedia applications, faster data transmission in mobile networks, and IP telephony. Today's routed IP networks suffer from serious problems related to scalability, manageability, reliability and cost.

Helsinki University of Technology has started IPMAN project in 1999. The target of the IPMAN project is to research and develop a network management paradigm for massive IP-networks.

1.1 Changes in network management

Introduction of new equipment and new technologies means introduction of new information systems, which also increases the number of data repositories and fault management systems. As networks become larger and more complex, tools and applications to ease network management are critical. Automated network management is needed [77].

Time is a critical factor in network management (see figure 1.1). Managers strive for shorter cycles and customers demand faster response. Shorter cycles lead into lower costs and greater productivity [24]. Effective use of network facilities can improve a competitive position, create new market opportunities and afford efficient communications between business units and customers.

Network management views the computing environment as a collection of co-operating systems connected by various communication mechanisms. Sun Microsystems expresses that the network is the computer. This means that effective system management is thinking the network as a single, multilayer entity, one that requires its own care [67]. An important aspect is that management is useless to a company if it does not

Figure 1.1: Network management, modified [24]

solve business problems and ease the work of operators [87].

A recent Gartner Group study "Strategies to Control Distributed Computing's Exploding Costs" reports that while the strategic value of systems and networks continues to increase, the escalating cost of managing that technology is undermining the organization's expected return on its investment [24].

Network management that is effective and adapts to business strategy requires:

- The right abstraction level of information,
- Information at the right time, and
- Information in an easy-to-use format [24].

Effective network management that adapts to business strategy contains functions, such as technology selection, network automation, capacity planning, predictive problem avoidance and sophisticated trouble-shooting. These functions all require information that goes beyond the data available to most of network management staff.

1.2 Future trends

Experts forecast the changes that will happen in the next years. According to James Herman in the Sixth IFIP/IEEE International Symposium on Integrated Network Management (May 1999): "The main affect of the Internet is to enable the rise of virtual business and services. There will also be large data volumes (more customers × more interactions with customers × more data per interaction = an explosion). PC will no longer be the dominant access device, the network is the center of everything. There will be more need for mobile and wireless infrastructure. Data will find you wherever you are. When there are no connectors, it means lighter, cheaper and simple devices."

Figure 1.2 expresses the vision of Internet development. Almost every telephone company has become involved in delivering non-telephone services to end users. Plain Old Telephone Service (POTS) is the basic telephone call service . Internet Access Provider's (IAP's) role is to ensure that the end user has a reliable connection to the Internet.

Most cable television (CATV) providers are interested in offering telephone and Internet services as well as video-on-demand services. The Hybrid Fiber-Coax (HFC) network is an emerging cable architecture for providing residential video, voice telephony, data, and other interactive services to end users over fiber optic and coaxial cables . The HFC network can provide the bandwidth that some multimedia applications require, using the spectrum from 5 MHz to 450 MHz for conventional downstream analog information, and the spectrum from 450 MHz to 750 MHz for digital broadcast services such as voice and video telephony, video-on-demand, and interactive television.

An alternative to a coaxial or fiber/coaxial network is offered by a technology that can transmit relatively high-speed data over untwisted or twisted pair cables for distances up to 4000 m. The technology can use existing digital telephone subscriber lines. The High bit-rate Digital Subscriber Line (HDSL) offers bi-directional transmission at 1.5 Mbps with a transmission bandwidth of 200 kHz . Asymmetric Digital Subscriber Line (ADSL) can transmit four one-way 1.5-Mbps video signals, in addition to a full-duplex 384-Kbps data signal, a 16-Kbps control signal, and analog telephone service . ADSL has a transmission bandwidth of 1.1 MHz.

Many end users want to access services not only in their homes, but also outside the homes. Wireless transmission enables the desired mobility among users. Because the bandwidth is shared, users are grouped into small cells. The users in each cell communicate with a single base station, and base stations are linked together by a wired network.

Mobile Ad hoc Networking (MANET) is an autonomous system of mobile nodes, where a node is both a host and a router. Mobile nodes communicate via wireless technology, and they are free to move randomly and organize themselves arbitrarily. MANET supports robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes.

Satellite transmission also facilitates mobility. Because the transmission area covered by a satellite is very large, it is well suited for video and audio broadcasting [104, pages 16–20].

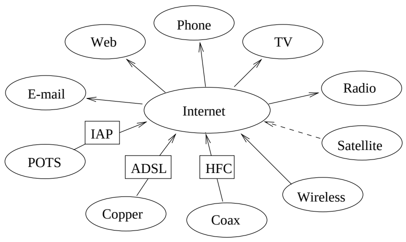

Figure 1.2: The Internet picture [23]

1.3 Structure of this document

Chapter 2 studies models developed to classify and order network management problems. Chapter ?? describes some protocols used for network management, and chapter 4 covers some possible future trends in network management.

Professor Olli Martikainen suggested use of a reference model, where network management is divided into four levels (see figure 1.3).

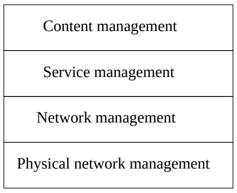

Figure 1.3: Reference model by Professor Olli Martikainen

IPMAN project has developed further the reference model, and has modified its structure (see figure 1.4).

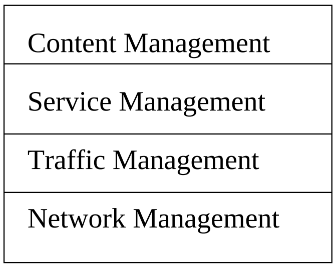

Figure 1.4: Modified reference model

Chapters 5 to 8 study each layer of the reference model. Finally, chapter 9 gives a short summary of commercial network management tools.

2 NETWORK MANAGEMENT MODELS

This chapter describes models that are used to structure the problems and ideas in network management. Section 2.1 studies the OSI network management models, and section 2.2 describes the TMN network management model. Management of customer networks is briefly addressed in section 2.3. SMART TMN, described in section 2.4, has a broader scope on network management. Finally, network management for the TINA architecture is studied in section 2.5.

2.1 OSI Management

The Open Systems Interconnection (OSI) Management is documented in ITU-T and CCITT X.700-series Recommendations [32]. It is based on four components: *Management Model, Information Model, Communication Protocol for Transferring Management Information*, and *Systems Management Functions*. OSI Management functionality is divided into five *Management Functional Areas* according to the *OSI FCAPS model* [27].

Management Model

The Management Model describes a manager-agent concept (figure 2.1). The manager system manages Managed Objects in distributed manner by issuing remote management requests to agent processes. The agents manage the Managed Objects and are responsible for implementing the functionality needed to execute the requests. They may also return values and send notifications (events or traps generated by Managed Objects) back to the manager [98, 17, 94, 105].

A network to be managed can be divided into management domains. A domain is an administrative partition of a managed network or Internet. Domains may be useful for reasons of scale, security, or administrative autonomy. Domains allow the construction of both strict hierarchical and fully cooperative and distributed network management systems [105, 18].

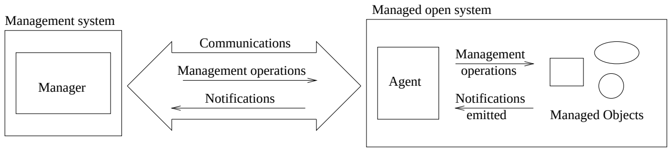

Figure 2.1: The manager-agent concept [18]

Information Model

The information model deals with Managed Objects that are abstractions of the real resources on the network [27]. All information relevant to network management and definitions of the objects to be managed resides in a Management Information Base (MIB) . MIB is a ”conceptual repository of management information”, an abstract view of all the resources to be managed. All information within a system that can be referenced by management protocol is considered to be part of MIB [105].

The logical structure of MIB and the conventions for describing and uniquely identifying MIB information are defined in the Structure of Management Information (SMI). SMI is defined in terms of Abstract Syntax Notation One (ASN.1), that provides a machine-independent representation for the information [105].

Communication Protocol for Transferring Management Information

The transfer of management information in OSI networks is provided by Common Management Information Protocol (CMIP, see page **??**) [17].

Systems Management Functions

Systems Management Functions (SMFs) define common facilities that can be applied to particular Managed Objects corresponding to different resources. The SMFs include mechanisms for controlling access to Managed Objects and the distribution of events, common formats for reporting alarms and status, and mechanisms for invoking and controlling remote test execution [94].

Management Functional Areas — OSI FCAPS model

OSI Management functionality is divided into five management functional areas [17]:

- **Fault Management** encompasses fault detection, isolation and the correction of abnormal operation. It includes functions to maintain and examine error logs, accept and act upon error notifications, trace and identify faults, carry out diagnostic tests and correct faults .

- **Configuration Management** identifies, exercises control over, collects data from and provides data to open systems. The purpose of Configuration management is to prepare for, initialize, start, provide the continuous operation of, and terminate interconnection services .

- **Accounting Management** enables charges to be established for the use of resources in OSI environment, and for costs to be identified for the use of those resources. It includes functions to inform users of costs incurred or resources consumed, to enable accounting limits to be set and tariff schedules to be associated with the use of resources and enable costs to be combined where multiple resources are used .

- **Performance Management** offers functions to report and evaluate the operation of network and it's elements. Statistical data is collected for the analysis and development of the network .

- **Security Management** includes functions to create, delete and control security services and mechanisms, distribute security-relevant information, and report security-relevant events .

2.2 Telecommunications Management Network

A Telecommunications Management Network (TMN) provides management functions for telecommunications network and services. It also offers communications between itself and the network and it's services. It is an architecture that provides interconnection between various types of Operations Systems (OSs) and/or telecommunications equipment for the exchange of management information [31].

The top-level standards and recommendations for OSI systems management form the basis for TMN standards [32]. The TMN standards are defined in ITU-T M.3000-series documents [96, page 48].

Figure 2.2 shows a general relationship between a TMN and the telecommunications network it manages. TMN is conceptually a separate network that interfaces a telecommunications network at several different points to send/receive information to/from it and to control it's operations. A TMN may use parts of the telecommunications network to provide it's communications [31].

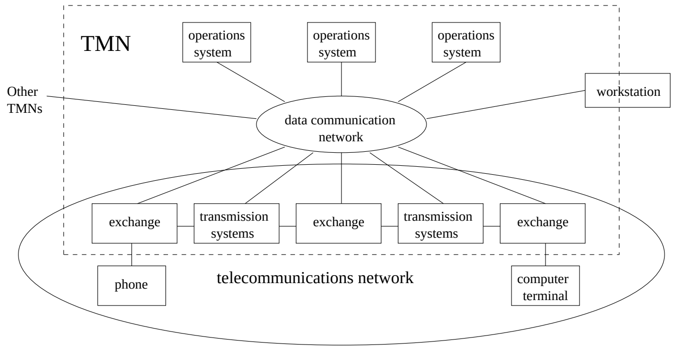

Figure 2.2: General relationship of a TMN to a telecommunications network [96, page 25]

TMN Management services

The scope of network management is broader in telecommunications than in data communications. Thus a TMN must provide more than just the functionality defined in the OSI FCAPS model. TMN Management Services (TMN-MSs) include Customer administration, Network provisioning management, Workforce management, Tariff, charging and accounting administration, Quality of Service and network performance administration, Traffic measurement and analysis administration, Traffic management, Routing and digit analysis administration, Maintenance management, Security administration, and Logistics management. An overview on TMN-MSs is provided in ITU-T Recommendation M.3200. A more detailed description can be found in ITU-T Recommendation M.3400.

A TMN Management Service is made up of TMN Management Function Set Groups. They are further subdivided into Management Function Sets and eventually into Management Functions. A TMN application of any complexity can be created by combining these elementary building blocks. The management functions are then mapped to TMN Systems Management (SM) services. The TMN SM services are provided by OSI Systems Management Functions. These principles are illustrated in figure 2.3. Figure 2.4 shows the mapping of OSI Management Functional Areas (MFAs) and TMN Management Function Set Groups. The Management Function Sets and individual Functions are defined in ITU-T Recommendation M.3400 [96, page 48–53].

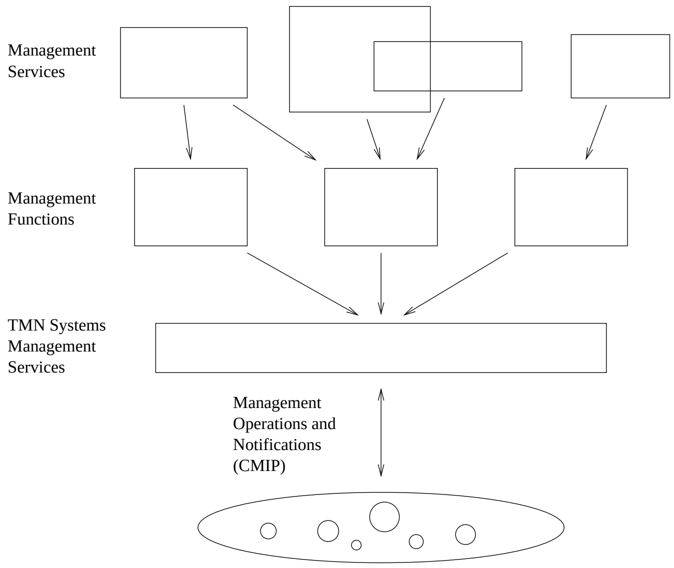

Figure 2.3: TMN Management Services, Management Functions and Systems Management Services [96, page 50].

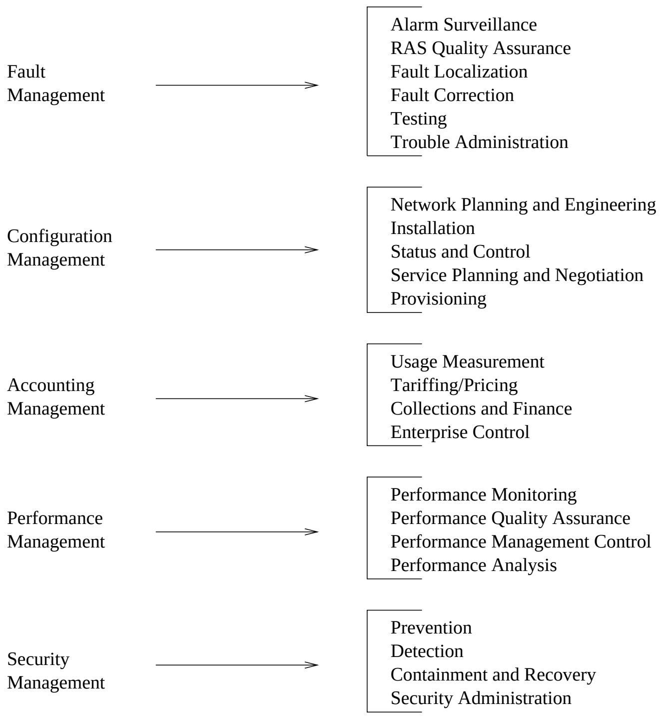

Figure 2.4: Mapping of OSI MFAs and TMN Management Function Set Groups [96, page 53].

TMN Management Layers

The needed management functionality is achieved using five layers of management, described in [96, pages 19–21]. Each layer has it's own functions and interfaces to layers above and below. The lower layers perform more specific functions and upper layers are concerned with functions more general. Each layer must interact with the layer below in order to execute it's task.

Business management layer is responsible for management at the enterprise level. The layer is concerned with the network planning, agreement with operators, and executive-level activities such as strategic planning.

Service management layer provides the customer interface. It's functions include service provisioning, opening and closing accounts, resolving customer complaints, fault reporting, and maintaining data on Quality of Service.

Network management layer manages the whole network. It receives data from network element management layer and provides total-network-level views.

Network element management layer is responsible for managing a subnetwork of the whole managed network. The interaction with network elements is provided by network element layer.

Network element layer provides for the agent functions of the managed network elements.

TMN architecture

TMN architecture is divided into three aspects, which can be considered separately when designing a TMN: *functional, information* and *physical architecture*. **Functional architecture** describes the appropriate division and distribution of functionality within the TMN to allow the creation of building blocks, from which a TMN of any complexity can be implemented [31].

Information architecture describes the nature of the information that needs to be exchanged between the building blocks, and also describes the understandings that each building block must have about the information held in other building blocks [31].

Physical architecture describes the implementation of function blocks on physical systems and the interfaces between them [96, page 31].

2.3 Customer Network Management

The purpose of Customer Network Management (CNM) is to provide external users of a telecommunications network with a limited control and view of the managed network. It enables customers to manage a portion of the whole network and subscribe it's services. Figure 2.5 illustrates the CNM functional architecture [96, pages 38–42].

Customers are provided with a subset of the TMN man-

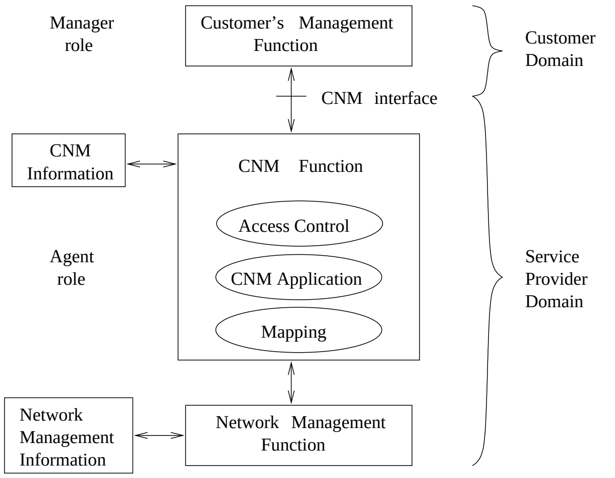

Figure 2.5: CNM functional architecture [96, page 39].

agement services, limited management information, and *CNM supporting services.* CNM supporting services enable customer's management system to request service provisioning and service usage from a service provider [96, pages 38–44].

2.4 SMART TMN

Smart TMN [93] is a program of Telemanagement Forum, a non-profit organization of dozens of product vendors and operators. The goal of SMART TMN is to present a larger scale, business process-driven model of telecommunications networks management.

The SMART TMN consists of four elements:

- **Telecommunications Operations Map (TOM)** which describes key business processes,
- **Technology Integration Map**, which contains recommendations of technologies to adopt for different management applications [92],
- **Central Information Facility** for information store for technical specifications, object models etc., and

- **Catalyst Projects**, which are projects to validate technology concepts.

2.5 Telecommunications Information Networking Architecture

Telecommunications Information Networking Architecture (TINA) is designed to meet the needs of telecommunications services ranging from traditional voice-based services to interactive multimedia, multi-party services, information services, as well as management services. All these services are considered to be software-based applications that operate on a distributed computing platform [58, page 137]. TINA addresses a wide range of issues and provides a complex set of concepts and principles. In this respect, it is much more a framework, a compilation of concepts and principles for developing future distributed telecommunications and management services, than a specific architecture [58, page 148].

TINA architecture

TINA architecture is based on four principles: Object-oriented analysis and design, distribution, decoupling of software components and separation of concern. The purpose of these principles is to ensure interoperability, portability and re-usability of software components, independence from technologies, and to help to create and manage complex systems [95]. The two major separations of concern are the separation between applications and the environment, and the separation of applications into the service specific part and the generic management and control part [95].

Due to the complexity of TINA, it's architecture is divided into four sectors: *computing architecture, service architecture, network architecture* and *management architecture* [101, page 24].

The **computing architecture** defines a set of concepts and principles for designing and building distributed software [101]. It is based on the Basic Reference Model for Open Distributed Processing (RM-ODP, ITU Recommendation X.900) [58, page 148].

The **service architecture** defines a set of concepts and principles for the design, specification, implementation and management of telecommunication services [101, pages 25–26].

The **network architecture** provides generic concepts that describe transport network in general, technology-independent way. The TINA network is a transport network that is capable of transporting information that is heterogeneous in terms of data formats, bandwidth and other quality of service related aspects. The network is capable of handling streams and their point-to-point or multi-point connections [101, page 26].

The **management architecture** is based on the OSI management and TMN standards. In particular, the management architecture adopts the TMN functional layers. All the other TINA architectures are influenced by the management architecture principles [58, page 163]. The TINA management architecture is still under study [101, pages 27–28].

TINA network management model

TINA network management model extends the OSI FCAPS model (see page 17) [58, 20]. Configuration management is divided into *connection management* and *resource configuration management*.

Connection management is considered a fundamental activity in telecommunications network [101]. TINA represents a new approach to the traditional way of connection control [58, page 163]:

Connection control includes the establishment, modification and release of connections. Traditionally these are considered as control operations, which are viewed as being different from management. In TINA, these operations are seen as dynamic management operations. Connection management is used by service architecture components whenever a service requires connections.

Resource configuration management contains installation support, provisioning of network resources to make them available for use, monitoring and control of resource status. It also includes management of the relationships among the resources.

Fault management includes alarm surveillance, fault localization, fault correction, testing functions and trouble administration information.

Accounting management is responsible for measuring and establishing charges for the use of resources.

3 NETWORK MANAGEMENT PROTOCOLS

3.1 Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is the most widely used management protocol in TCP/IP networks. This is due to it's simplicity, expandability, easy implementation and the fact that it poses only little stress on the managed network and the managed nodes [98, 16].

SNMP is based on a agent-manager concept, similar to the one illustrated in figure 2.1: A manager sends requests to agents in network elements. The agents control Managed Objects (see page 16) accordingly, send responses and issue trap messages to the manager. The objects to be managed are defined in a MIB (see page 16) . The requests and responses are exchanged using the User Datagram Protocol (UDP), which is a connectionless protocol. Trap-directed polling is used to decrease the management traffic on the network [51].

The management functionality is centralized in a Network Management Station (NMS), which acts the manager role. Agents are kept simple, and thus SNMP is particularly conservative in the memory and computational requirements placed on devices connected to the network [96].

SNMP development

The first version of SNMP, SNMPv1, became both an IETF (the Internet Engineering Task Force) and a de facto standard. This was due to it's widespread market acceptance. However, due to the lack of adequate security features, a new version of SNMP had to be developed. Various proposals on SNMPv2 were made, but none were adopted as a new standard. SNMPv2 failed because it had lost the simplicity of SNMPv1 [98, 21].

Third version of SNMP, SNMPv3, is now in it's final stages of standardization. It builds on the first and the second versions of SNMP, and is intended to offer new capabilities for open, interoperable, and secure network management. It includes methods for security (authentication, encryption, privacy, authorization, and access control), and a new administrative framework (naming of entities, user names and key management, notification destinations, and proxy relationships, remotely configurable via SNMP operations) [21, pages 501–503].

SNMP security

The SNMP architecture makes a distinction between message security services (integrity, authentication and encryption) and access control services. Both message security and access control services can be provided by multiple security or access control models. The architecture allows coexistence of multiple models in order to allow future updates, in case the security requirements change or cryptographic protocols need to be replaced [79, pages 690–692].

The User-based Security Model (USM) provides integrity, authentication and privacy, and is the standard security model currently used with SNMP version 3 (SNMPv3). The View-based Access Control Model (VACM) provides checking whether the users have proper access rights to access one or more objects in a Management Information Base (MIB) and perform operations on these objects. USM is discussed in RFC 2274 and VACM in RFC 2275.

3.2 Common Management Information Protocol

Common Management Information Protocol (CMIP) is a much more complicated and extensive network management protocol than SNMP. It improves on many of SNMP's weaknesses, the security issues for instance, thus providing a more efficient network management environment. CMIP can also be used to perform tasks that would be impossible under SNMP [98].

In CMIP, requests and responses between managers and agents (see figure 2.1) are exchanged using the OSI connection-oriented transport protocol that provides in-order, guaranteed delivery [51].

CMIP also has some disadvantages: Due to it's complicity CMIP poses a lot of stress on the network and it's implementation is very difficult [98].

3.3 Signalling System #7

Signalling System #7 (SS#7) Operations, Maintenance and Administration Part (OMAP) offers a framework for operation and maintenance in SS#7 networks. OMAP uses principles of management defined in TMN Recommendations (ITU-T M.3010 or ETSI ETR 037, see reference [31]) and in OSI Management Recommendations of the ITU-T X.700-Series. Overview of OMAP and Signalling System #7 management is provided in ITU-T Recommendation Q.750 [45].

Management Layers

The definition of TMN is concerned with five layers in management (see page 20), namely business management, service management, network management, network element management, and elements in the network that are managed. Of these, OMAP provides the three lowest layers. It is not concerned with business management, and interacts with other TMN parts to provide service management [45].

Management Functionality

Management functions and resources provided by OMAP allow management within the SS#7 signalling points. Three categories of management functionality (fault, configuration and performance management) of the five in OSI FCAPS model (see page 17) are provided [45].

3.4 ATM Network Management

ATM Forum has standardised Broadband ISDN, and defined also an ATM network management model. This model is based on TMN, and uses the lower three layers of the reference architecture of ITU-T M.3010 (Network Management, Element Management, and Element Layer) [62]. The interfaces between layers are specified as function points, and leave physical implementation unspecified. ITU-T has also used TMN as a basis in its ATM network management standardisation [80].

ATM-Forum specifications define five managment intefaces: **M1** between *private network manager* and *end user*, **M2** between *private network manager* and *private network*, **M3** between *private network manager* and *public network manager*, **M4** between *public network manager* and *public network*, and **M5** between two *public network managers*.

In addition to M1-M5 network management, ATM-Forum provides a protocol called Interim Local Managment Interface (ILMI), which is a SNMP-based protocol [6].

4 FUTURE NETWORK MANAGEMENT

New technologies, management models, and visions of future network management, that are currently under development, are described in this chapter. Section 4.1 presents Open Group's X/Open Systems Management Reference Model. Web-based network management is discussed in section 4.2, and Java Management API in section 4.3. Section 4.4 presents CORBA-based management, and section 4.6 SPIN's vision on network management. Finally, section 4.7 discusses Policy-based network management.

4.1 X/Open Systems Management Reference Model

Open Group, a vendor-neutral international consortium for buyers and suppliers, has presented an *X/Open Systems Management Reference Model*. It's goals are [94]:

- to identify the crucial aspects of the distributed systems management problem space, especially those that are unique to this topic,
- to establish common terminology, and
- to establish a problem-oriented approach to the realization of distributed systems management solutions.

The reference model describes concepts necessary to build a comprehensive distributed systems management environment. It identifies the mapping between the abstract concepts and some technologies that provide suitable implementation bases for the realization of the model. The model is intended to enable a network of heterogeneous systems to be managed as a single system [94].

The X/Open Systems Management Reference Model uses object-oriented techniques in the specification of systems management. These techniques are derived from those used in the OSI Management Model, as well as the Object Management Group Common Object Request Broker Architecture (CORBA) .

The Reference Model consists of three basic components:

- **Managers**, which implement Management Tasks and other composite management functions,
- **Managed Objects**, which encapsulate the resources, and
- **Services**, which provide the X/Open Systems Management Support Environment.

Anticipated implementation technologies

It is anticipated that the primary vehicle for implementation of the Reference Model will be the Object Management Group's Object Request Broker (ORB) technology . Another significant implementation technology is that embodied by the ISO/CCITT and Internet management protocols, CMIP and SNMP. The X/Open Management Protocols API (XMP) provides a uniform access method to these technologies [94].

In addition to the above, which represent the anticipated future development of distributed systems management, the Reference Model can also be implemented using currently available technologies. These include those based on existing Remote Procedure Call (RPC) technologies, such as ONC NIS and DCE RPC [94].

4.2 Web-based network management

Doing network management operations using Internet/intranet technologies is called Web-based Network Management. Web-based Network management comprises controlling network systems and / or data gathering, delivery of network management tasks and data analysis.

Basic applications of web based network management are web-based configuration and management of individual devices, advanced network wide management capabilities and web reporting of network status information.

For network element configuration with a WWW browser, a management agent with a HTML interface must be used. The HTML agent may configure the element using WWW forms and give reports as WWW pages.

Advanced network wide management capabilities seem to offer a WWW interface for traditional network management tools. Web reporting of network status means reporting statistics and query information of network elements on Intranet pages.

A pro for web based network management is the ability to use cheap hardware and software for user interfaces; the personnel may move physically and use the web interface for network management. However, it seems that web based network management mainly is a user interface improvement and does not add significantly to the actual network management.

4.3 Java Management API

Java Management API (JMAPI) [89] is intended to provide a standard interface between different computers and network devices. The system can be used by Java programmers, and is created in alliance with Sun Microsystems, Bullsoft, Computer Associates, Exide Electronics, Jyra, Lumos Technologies, TIBCO, and Tivoli. Currently, only specification version 0.8 is available. Specification version 2.0 was intended for publication in March 1999.

4.4 CORBA-based Telecommunication Network Management System

The Object Management Group (OMG) is a non-profit international trade association. OMG has presented an outline of an architecture for a CORBA-based Telecommunications Network Management System. One of the objectives of this architecture is to ensure a complete compatibility with proprietary, ITU-T/ISO, SNMP and CORBA based network elements [72].

CORBA (Common Object Request Broker Architecture) is an architecture that supports the distribution of management functionality and managed objects [94].

Inter-networking between CORBA and TMN systems

In the context of TMN, CORBA is seen to offer potential in two significant areas: in the description and implementation of management interfaces supported by network devices, and in the description and implementation of interfaces within and between management operations systems [72].

4.5 Common Information Model

Common Information Model (CIM) is a common data model developed by Distributed Management Task Force, Inc. It is implementation-neutral and can be used to describe management information in a network/enterprise environment. The model is intended to enable interchange of management information between management systems and applications, thus providing for distributed network management [29, 28].

CIM is currently supported by at least Microsoft (Windows NT/98), Hewlett-Packard (HP OpenView), and IBM (Tivoli)[1].

4.6 SPIN's Intelligent Network Management

SPIN is a research project in the Institute for Information Technology at Canada's National Research Council [1]. The SPIN Intelligent Network Management project studies and develops new agent-based technologies for controlling, planning and problem definition of heterogeneous networks. The application development of SPIN networks uses integration of the off-the-self NM components, and testing and usage of popular tools, such as HP Openview.

4.7 Policy-Based Networking

Policy is a combination of rules and services where rules define the criteria of resource access and usage. Policies can contain other policies, they allow to build complex policies from a set of simpler policies, so they are easier to manage. They also enable to reuse previously built policy blocks [96].

Policy groups and rules can be classified by their purpose [75]:

- Service Policies
- Usage Policies
- Security Policies
- Motivational Policies

[1]See ch. 9 for commercial network management products.

- Configuration Policies
- Installation Policies
- Error and Event Policies

Service policies describe services available in the network. These services will be available for usage policies. For example, QoS service classes (Voice-Transport, Video-Transport, ..) are made by using Service policies .

Usage policies describe how to allocate the services defined by Service policies. Usage Policies control the selection and configuration of entities based on specific usage data. For example Usage Policies can modify or re-apply Configuration Policies.

Security Policies identify client, permit or deny access to resources, select and apply appropriate authentication mechanisms, and perform accounting and audit of resources.

Motivational Policies describe how a policy's goal is accomplished. For example the scheduling of file backup based on activity of writing onto disk is a kind of Motivational Policies.

Configuration Policies define the default setup of a managed entity, for example the setup of the network forwarding service or the network-hosted print queue.

Installation Policies define what can be put on the system, as well as the configuration of the mechanisms that perform the installation. Typical installation policies are administrative permissions, and they can also describe dependencies between different components.

Error and Event Policies. For example, if a device fails between 8am and 5pm, call the system administrator, else call the Help-Desk [75].

Policy-Based Networking (PBN) is gaining a wider acceptance in the IP management, because it makes possible more unified control and management in complex IP network [79].

5 NETWORK ELEMENT MANAGEMENT

This chapter discusses network element management. Section 5.1 describes network configuration management. Section 5.2 describes security management, including protocols and programs developed to provide security over the Internet, and network elements used to secure risky areas of networks. Section 5.3 studies fault management, including troubleshooting, fault localization, and testing methods.

5.1 Configuration management

Configuration management means initializing and shutting down parts of a network (for example routers, hubs, and repeaters) and reporting the changes. It is also concerned with maintaining, adding and updating the relationships among components and the status of components during network operation. Network traffic patterns and identified bottlenecks that reduce performance must be understood. Nowadays modern components and subsystems can be configured to support many different applications. The same device can be configured to act either as a router or as an end system node or both. Depending on the configuration, the appropriate software and a set of attributes and values are chosen for the device [84, page 481]. Reconfiguration may be necessary in case of fault isolation or when the network is expanded.

As the network scales up in physical size (capability and complexity), also the management capabilities must be enlarged. The aim is that these actions could be automated. It should also be possible to make on-line changes without affecting the entire element or network [77]. Large-scale network management systems must be constructed to support diverse network elements. They must also be extensible and flexible enough to support new elements and the rapid deployment of new highly customized services.

Activities in network management can be divided into three groups [37]:

- Activities, that do not affect the functioning of an element,

- Activities, that affect the functioning of an element (for example switching off an element in a subnetwork), and
- Activities, that make an element to do a desired function (for example restarting an element).

Dynamic updating of configuration needs to be done periodically to ensure that the existing configuration is known. This is essential for fault management as well.

Configuration management tools have reporting components. When network configuration changes, users must be informed about new network elements and resources. Configuration management is well organized when all the gathered information and operations are in statistical form.

There is a risk of spending money on hardware and services that remain underutilized. On the other hand the underprovisioning usually lowers productivity, which reflects to the service level [13]. When the network is designed, it is essential to predict the growth of the network. The network should also be prepared to varying volumes of users.

By continuously addressing the cost of maintenance (MTBF[1] and MTTR[2] statistics, costs associated with maintaining) the network as a system can be tuned [87].

TCP/IP networks

TCP/IP networks cause more work for system administrators than other networking systems. Administrators have to manually configure each computer for network use when it is added to the network, or when it is moved from one subnet to another. Each computer must manually be assigned a unique IP address and various configuration parameters must be set.

There is a need for tools that automatically assign addresses and set configuration parameters. Some client/server solutions are already available. Client machines find the details of other hosts on the network using the Domain Naming Systems (DNS) protocols, and can be told their network configuration using Bootstrap (BOOTP) protocol. Dynamic allocation of

[1]Mean Time Between Failure

[2]Mean Time To Repair

IP addresses to particular machines can be chosen over static allocation using the Dynamic Host Configuration Protocol (DHCP) [30].

5.2 Security management

Security management covers such areas as detecting, tracking and reporting security violations, and creating, deleting and maintaining security-related services such as encryption, key management, and access control. Distributing passwords and secret keys to bring up systems are also functions of security management [96, page 12].

As computer-based communications and networks that link open systems continue to expand, security management becomes critical. Nevertheless, standardization of security properties has developed slowly. Network management must provide proactive management of security and integrate it with protocols, such as IPSec and services, like VPNs. Security of devices and networks must be compared to possible threats and risks. If the risks are high, the devices and the networks must be provided with more reliable secure properties.

Protocols and programs for network security

Table 5.1 describes protocols and programs, that are developed to provide security over the Internet. Secure-HTTP (S-HTTP) is an application-level protocol that provides security services across the Internet. It provides confidentiality, authenticity, integrity, and non-repudiability. S-HTTP is limited to the specific software that is implementing it, and it encrypts each message individually [4].

Level	Protection Used
Application-level	S-HTTP, SSH, stelnet, S/MIME
Transport-level (TCP, UDP)	SSL, PCT
Network-level (IP)	IPSec

Table 5.1: Protocols and programs developed to provide security over the Internet

Secure Shell (SSH) and Secure telnet (stelnet) are programs that allow you to log in to remote systems and using an encrypted connection. SSH uses public-key cryptography to encrypt communications between two hosts, as well as for user authentication.

Secure Multipurpose Internet Mail Extension (S/MIME) is an encryption standard used to encrypt electronic mail, or other types of messages on the Internet. It is an open standard developed by RSA Data Security Inc.

Secure Socket Layer (SSL) is an encryption method developed by Netscape to provide security over the Internet. SSL is a protocol layer that is located between the network layer and applications, so that, in theory, it can be used with any application. However, it is vulnerable to poor application design. It provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection [4].

The Private Communication Technology (PCT) protocol is developed by the Microsoft Company to be used mainly in their Internet Explorer browser.

IP Security Architecture (IPSec) provides a standard security mechanism and services to the currently used IP version 4 (IPv4) and to the new IP version 6 (IPv6). IPSec is less dependent of individual applications than SSL. It provides IP-level encryption by specifying two standard headers: IP Authentication Header (AH) and IP Encapsulating Security Payload (E-SP) . IP Authentication Header provides strong integrity and authentication. It computes a cryptographic authentication function over the IP datagram and uses a secret authentication key in the computation. IP Encapsulating Security Payload provides integrity and confidentiality for IP datagrams. It encrypts the data to be protected and places it in the data portion of the IP Encapsulating Security Payload. However, these mechanisms do not provide security against traffic analysis. Any specific protocol for key management is not provided by the architecture, only requirements for such systems to be used in conjunction are described [75].

IPSec require a key management protocol. IETF has standardized Internet Security Association & Key Management Protocol (ISAKMP) and Internet Key Exchange (IKE) for this purpose. ISAKMP defines the procedures for authenticating a communicating peer, creation and management of Security

Associations, key generation techniques and threat mitigation (e.g. denial of service and replay attacks). These are necessary to establish and maintain secure communications in an Internet environment. Security Association (SA) is a security-protocol-specifistic set of parameters that defines the services and mechanisms necessary to protect traffic at that security protocol location.

ISAKMP separates the details of security association management and key management from the details of key exchange. It provides a framework for Internet key management, but it does not define session keys by itself. IKE is a protocol that defines key exchange functions for ISAKMP.

Protocols and programs discussed in this subsection are further studied in [4]. IPSec is defined in [49], ISAKMP in [60] and IKE in [35].

Access control tools

Hubs , routers and firewalls can be used to limit the access to the networks or the parts of the networks.

Hubs used in LANs are provided with simple security properties. Hubs protect sensitive data on the network by checking destination addresses on each packet and sending readable packets only to authorized nodes. Hubs automatically detect and/or disable unauthorized log-on attempts and record the events at the management station. Hubs also track changes involving users and devices on the network, giving the manager a complete record. These security level operations can be restricted to a date or a time period.

Routers are provided with security properties as well. A router handles packets up through the IP layer. The router forwards each packet based on the packet's destination address, and the route to that destination is indicated in the routing table [39]. Routers can improve network security, but also introduce new problems: Routing protocols are susceptible to security attacks, and routing mistakes may allow the entrance of unauthorized personnel into the network. Unlicensed remote and local operations of routers must be prevented by using usernames.

Traffic can be controlled with packet filtration based on the access control lists. On the access control lists it is defined what addresses and protocols to each interface can be routed. Properties such as NAT[3], PAT[4], and logging of events and alerts can be attached to the router. However, it has not been possible to expand the capacity of traditional routers as cost-effectively as the capacity of PC workstations or the network traffic volume [41].

Firewall systems control connections between closed networks and outside world. There are two major approaches used to build firewalls: packet filtering and proxy services . Packet filtering systems route packets between internal and external hosts, but they do it selectively. They allow or block certain types of packets in a way that reflects a site's own security policy. The type of router used in a packet filtering firewall is known as a screening router.

Proxy services are specialized application or server programs that run on a firewall host: either a dual-homed host with an interface on the internal network and one on the external network, or some other bastion host that has access to the Internet and is accessible from the internal machines. These programs take users' requests for Internet services (such as FTP and Telnet) and forward them, as appropriate according to the site's security policy, to the actual services. The proxies provide replacement connections and act as gateways to the services. For this reason, proxies are sometimes known as application-level gateways [19].

There are three ways to put various firewall components together:

- Dual-homed host architecture

  A dual-homed host architecture is built around the dual-homed host computer, a computer that has at least two network interfaces. Such a host could act as a router between the networks these interfaces are attached to; it is capable of routing IP packets from one network to another. Systems inside the firewall can communicate with the dual-homed host, and systems outside the firewall (on the Internet) can communicate with the dual-

[3] Network Address Translation is a method of connecting multiple computers to the Internet using one IP address.

[4] Port Address Translation is a method of translating all local private addresses to a single globally registered IP address.

homed host, but these systems can not communicate directly with each other. IP traffic between them is completely blocked.

The diagram below shows the network architecture for a dual-homed host firewall. The dual homed host sits between, and is connected to, the Internet and the internal network [19].

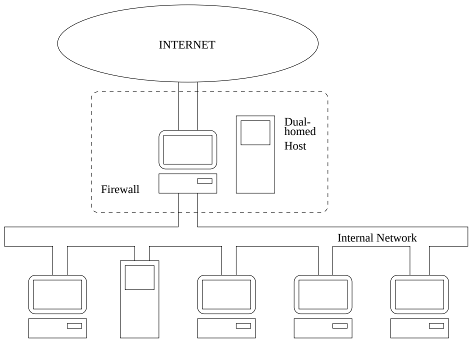

Figure 5.1: Dual-homed host architecture

- Screened host architecture

  Whereas a dual-homed host architecture provides services from a host that is attached to multiple networks (but has routing turned off), a screened host architecture provides services from a host that is attached to only the internal network, using a separate router. In this architecture, the primary security is provided by packet filtering. For example, packet filtering is what prevents people from going around proxy servers to make direct connections. The diagram below shows the network architecture for the screened host architecture [19].

- Screened subnet architecture

The screened subnet architecture adds an extra layer of security to the screened host architecture by adding a perimeter network that further isolates the internal network from the Internet. There are two screening routers, each connected to the

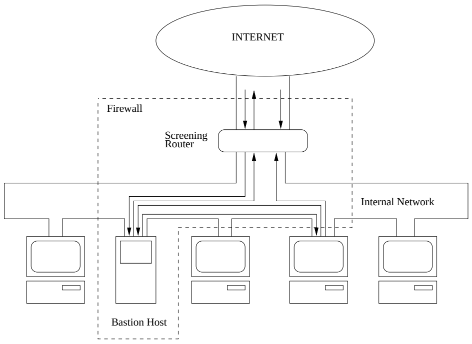

Figure 5.2: Screened host architecture

perimeter net. The perimeter network is another layer of security, an additional network between the external network and the protected internal network. The perimeter net offers an additional layer of protection between attackers and the internal system. One screening router sits between the perimeter net and the internal network, and the other sits between the perimeter net and the external network (usually the Internet). To break into the internal network with this type of architecture, an attacker would have to get past both routers. The diagram below shows the network architecture for the screened subnet architecture [19].

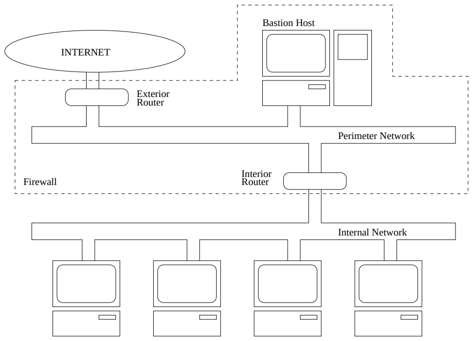

Figure 5.3: Screened subnet architecture

Physical network problems account more than half of all network problems. Locating the origins of such problems as a fiber cut, the earthing is done incorrectly, broken or incorrectly connected adapters, costs network providers time and money. Network management systems have also traditionally focused on the logical connection between the end user and the network destination, since many network problems have been a result of errors created by software applications [77]. Finding and repairing failures of software applications is usually difficult, for example in such a case that the workstation sends but does not receive packets, too many collisions occur or frames are too short or too long.

Fault management is troubleshooting, fault localization, isolation and correction. Today, the process of fault management needs to be automated. Rapid and accurate correction of network problems has to be created by the network or by the end user. Even if the entire network was violated, the network management application should work.

Expert systems provide an efficient and cost effective way of automating network fault management. By automating fault management, problems and possible diagnosis can be done faster and more efficiently. However, real-time performance represents a problem for expert systems [33]. Bounds on response times are difficult to establish. There are also risks pushing the limits of automation through the introduction of new or only partially proven technologies.

Transferring information

There are two mechanisms of transferring network management information from a managed entity to a manager: **polling** and **sending alerts** (messages are initiated by managed network elements). Advantages and disadvantages exist within both methods. Most network management systems use an optimal combination of alerts and polling in order to maintain advantages of each and eliminate disadvantages of pure polling [86].

Most systems poll the managed objects, search for error conditions and illustrate the problem in graphical format or as a textual message. Disadvantages of polling are the response time of problem detection and the increased volume of network management traffic. Having to poll many management information base (MIB) variables per machine on a large number of machines is itself a problem. The ability to monitor such a system is limited. Polling many objects on many machines increases the amount of network management traffic flowing across the network. It is possible to minimize this through the use of hierarchies (polling a machine for a general status of all the machines it polls). Anyway, the response time will be a problem [86].

If a system fails shortly after being polled, there may be a significant delay before it is polled again. During this time, the manager must assume that a failing system is acceptable. While improving the mean time to detect failures, it might not greatly improve the time to correct the failure. The problem will generally not be repaired until it is detected.

There are problems attached also to the second method, sending alerts: There is a possibility to lose of critical information and to over-inform the manager. An ideal management system would generate alerts to notify its management station of error conditions. However, alerts cannot usually be delivered when the managed entity fails or the network experiences problems. It is important to remember that failing machines and networks can not be trusted to inform a manager that they are failing. The manager should periodically poll to ensure connectivity to remote stations, and to get copies of alerts that were not delivered by the network [86].

Alerts in a failing system can be generated so rapidly that they impact functioning resources. An "open loop" system in which the flow of alerts to a manager is fully asynchronous can result in an excess of alerts being delivered. There may be a situation where all available network bandwidth into the manager is saturated with incoming alerts, thus preventing the manager from disabling the mechanism generating the alerts. Methods are needed to limit the volume of alert transmission and to assist in delivering a minimum amount of information to a manager. Alarm correlation is done by filtering secondary alarms, e.g. using expert systems[5].

[5] Expert systems are discussed briefly on page 45

Many management tools also **log** events with different formats and different sources. These events should later be correlated using time stamp to identify the source of the problem. Also topology information is needed to identify the precise location of the problem.

Many devices have buffers reserved for logs. When a buffer becomes full, new logs are written over the oldest ones. If the buffer becomes full quickly, some important logs may disappear before they are noticed. Buffers also consume disk space that could be used for other purposes.

Troubleshooting and fault localization

Several diagnostic tools are used for troubleshooting and fault localization purposes. These include ifconfig, arp, netstat, ping, nslookup, dig, ripquery, traceroute, and etherfind [39, pages 260–262].

The packet inter net groper (ping) tests whether a remote host can be reached. It sends an internet control message protocol (ICMP) loopback request packet to a target IP address. The receiver accepts the loopback request and issues a loopback response to the initiator of the Ping command. It cannot be determined with echo-response which one of the possible routes is violated, because loopback request and loopback response may use different routes. Ping can only be used to determine whether the target IP-address is available or not. Another usage of ping is to measure the response times of different packet sizes [13, page 33].

Unlike ping, **traceroute** forces every router to send back an ICMP-control message. Most Traceroute applications send a sequence of User Datagram Protocol (UDP)-packets to a randomly selected UDP-port [8, page 202]. Sometimes the firewalls filter these packets from the main traffic, in which case the tracing ends.

After detecting a fault, operators should as soon as possible find the root cause of the problem. Clearly defining the problem helps to isolate the root cause from symptoms [68]. Operators must also determine what troubles it causes and to whom.

At first it is useful to find the parts of the network, where the fault can not be, by eliminating processes. These parts can be neglected. If the problem is very serious and difficult, the network can be divided into smaller parts to be inspected one by one. Connectivity tests are also used to find the violated devices. At the same time it can be detected whether the fault is local or widespread. By testing the data integrity it can be found out if a part of the packets are lost by transmission. Delays are also to be tested, because some faults result from excessive delays [8, page 198].

Testing

Measuring the accessibility of devices helps us to collect information about the status of the network. A few devices are chosen usually from the network, and the functionality of the connections is measured from them to other devices. Measurements are done by a control device. After measurements, the results are interpreted.

Measuring the accessibility is not a perfect method for example, in the case where only routers are controlled. If the router has been set up so that it gives preference to packet switching, it will send packets normally even if it is heavily loaded and perhaps can not answer to messages of the controlling device. Another example is that two devices that can be reached might not have a connection with each other.

Another method of testing is to **control routing tables**. Routing should change only when the topology of the network changes. If there are changes at other times, there is probably something wrong with the network [8, pages 183–189].

Routing tables express the topology of the network. Finding out the network topology from routing tables is more difficult than controlling accessibility. In order to get information from routing tables of routers, routers must be Simple Network Management Protocol (SNMP) compatible, dynamic routing tables must support sending request or routing information must be tapped from a routing protocol. These requirements are not necessarily realized although SNMP is a commonly used protocol. Analysis of the routing tables can concentrate on the parts of the network which are most susceptible to failures.

6 TRAFFIC MANAGEMENT

This chapter discusses data communications in IP networks at OSI network layer and link layer levels. Section 6.1 describes different types of IP network traffic, introducing terms Quality of Service and Grade of Service. In section 6.2, the development of a new service model for IP networks is discussed. Section 6.3 discusses performance management and performance related issues.

6.1 Communications in IP networks

Data communications in IP networks can be divided into *connectionless* and *connection-oriented communications*. Communications based on the Internet Protocol (IP) is connectionless by nature. This means that no end-to-end connection is established before data is transmitted by the protocol [40, page 13]. In IP networks, *Quality of Service* (QoS) is defined in terms of parameters such as bandwidth, delay, delay variation (jitter), and packet loss probability [12] .

Connection-oriented communications in IP networks is enabled by protocols built upon the connectionless IP. This means that a logical connection between communicating network nodes is established before transmission [40, page 20]. *Grade of Service* (GoS) [1] is defined in terms of connection blocking probability (i.e. the probability of failing to establish a connection). Connection blocking can be controlled using *Connection Admission Control* (see page 51) .

Different types of traffic

Traffic in IP networks is composed of individual transactions and flows. A flow is a sequence of packets belonging to an instance of application running between hosts. Flows can be divided into two categories: *stream flows* and *elastic flows* .

Stream flows are generated by real-time audio and video

[1] Grade of Service (GoS) is traditionally related to *connection-oriented telecommunications*. In this document, GoS is used also in the context of IP networks.

applications such as Internet phone and video conferencing. These applications may require a minimum level of QoS in order to function properly, and thus would benefit from guaranteed QoS .

Elastic flows are generated by non-real-time applications (e.g. e-mail and FTP). They don't state critical demands on QoS, but adjust their rates to make full use of QoS available [73] .

6.2 New service model for IP networks

The current IP architecture does not support any QoS guarantees because routing is traditionally based on a best-effort principle. This means that each packet of information is treated independently and processed in the order of arrival [12].

The diversity of applications and their requirements raises a need to develop a new service model for IP networks. The purpose would to satisfy the requirements of rigid real-time applications while avoiding costs of over-provisioning[2] This could be done by introducing a service model with several classes of QoS instead of a single class of best-effort service.

The Internet Engineering Task Force (IETF) has three working groups developing the new service model or network architecture. These working groups are described and compared in following subsections. Also Traffic Engineering/Constraint-based Routing approach is discussed. The relationship between OSI layers and concepts described in this section are illustrated in figure 6.1.

IETF Integrated Services architecture

IETF Integrated Services (IntServ) working group[3] is currently defining an enhanced service model which involves creating two service classes in addition to best-effort service: *Guaranteed service* for applications requiring fixed delay bound, and *controlled-load service* for applications that require reliable and enhanced best-effort service. The model is based on resource reservation initiated by applications. This could be

[2]According to S. Shenker in [81], over-provisioning is not cost-effective in networks with real-time applications because of high variance in traffic.

[3]http://www.ietf.org/html.charters/intserv-charter.html

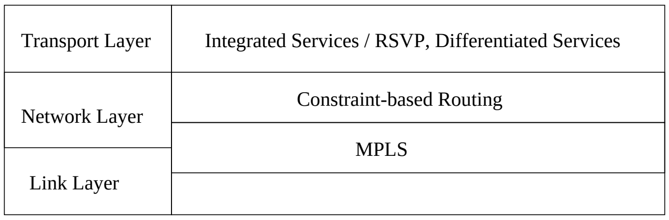

Figure 6.1: The relationship between OSI layers and concepts described in section 6.2 [107].

done e.g. using *Resource Reservation Protocol*[4] [43, 107].

Resource Reservation Protocol (RSVP) is used to signal routers in the network to reserve resources and set up a path for a flow [38, 107]. If RSVP is used in the network, there should be a mechanism to manage resource reservation policies of applications that initiate the reservation. RSVP and resource reservation are further discussed in [38, ch. 13] and in [108]. Standardization of RSVP can be found in [14].

To provide QoS allocated by a reservation protocol, **Connection Admission Control** (CAC) should be used in routers. CAC functions by blocking incoming stream flows[5] if the increase in traffic would drop QoS below an acceptable level for that or any previously accepted flow. On the other hand, CAC affects also on GoS, as the level of GoS is decreased when connections are refused [59, page 33].

Besides the benefits, CAC bears one disadvantage: Implementation of CAC would increase the complexity of networks, already complex enough. Discussion on the benefits and disadvantages of CAC can be found in [81].

According to [107] the Integrated Services architecture has several problems: It doesn't scale well, states high requirements on routers, and requires ubiquitous deployment for

[4] See [106] for the use of Resource Reservation Protocol with Integrated Services architecture.

[5] According to L. Massouliè and J. Roberts in [59], CAC should also be used for elastic flows. They argue that there is a minimum acceptable level of throughput for elastic flows, below which users gain no utility. Besides preserving QoS, CAC would also prevent instability and congestion collapses caused by uncontrolled retransmission of lost packets [59, pages 33–34].

guaranteed service. According to [9] the architecture is suitable only for small networks (e.g. corporate networks or Virtual Private Networks (VPNs)), not for Internet backbone networks.

Differentiated Services architecture

The approach of IETF Differentiated Services (DiffServ) working group[6] involves creating distinct Classes of Service (CoS) , each with reserved resources. The basic difference between IntServ and DiffServ architectures is that while IntServ provides an absolute level of QoS, DiffServ is a relative-priority scheme[7]. Secondly, in DiffServ the QoS in each CoS is defined by an agreement between customer and service provider. This eliminates the need of each application to signal their QoS needs at run time. It also provides better scalability as there is no need to maintain per flow state information in routers [42, 107, 3].

In Differentiated Services, each packet of information is classified by marking the *DS field*[8] in IP datagram. Packets receive their forwarding treatment, or per-hop behavior, according to the classification. The use of the DS field is standardized in [71] and in [11]. A small number of per-hop behaviors will also be defined by the working group [42, 107].

According to [107], DiffServ is more scalable, requires less from routers, and is easier to deploy than IntServ architecture. In [9] the DiffServ architecture, it's possible drawbacks, and related issues are discussed more widely.

Multi-protocol Label Switching architecture

Multi-protocol Label Switching (MPLS) architecture is being standardized by IETF MPLS working group[9]. MPLS is a forwarding scheme that is based on a label-swapping forwarding (label switching) paradigm instead of standard destination-based hop-by-hop forwarding paradigm [44, 100].

---

[6] http://www.ietf.org/html.charters/diffserv-charter.html

[7] Admission Control is not used in DiffServ architecture. Thus only priorities between different classes are guaranteed. Within each class, packets receive best-effort service.

[8] The DS field stands for Type of Service (TOS) byte in IPv4 and for Traffic Class byte in IPv6.

[9] http://www.ietf.org/html.charters/mpls-charter.html

Each packet arriving to an ingress router of an MPLS domain[10] is routed, classified, and given a label[11]. Inside the MPLS domain forwarding decisions are made using the label instead of processing the packet header and running a routing algorithm. The label is used as an index to a forwarding table[12] where the next hop and a new label can be found. The old label is replaced with the new one and the packet is forwarded. The label is removed as the packet leaves the MPLS domain [54].

MPLS labels can be used to provide forwarding along an explicit route, and to identify packets to receive certain QoS. An efficient tunneling mechanism is also provided. These features make MPLS useful for traffic engineering [107, 44].

A disadvantage of MPLS is that it should be extensively deployed, i.e. the MPLS domain of the network should be relatively big. Otherwise MPLS offers no benefit.

Traffic Engineering and Constraint-based Routing

Dynamic routing protocols such as RIP[13], OSPF[14], and IS-IS[15] can cause uneven traffic distribution. *Traffic Engineering* is the process of arranging how traffic flows through the network so that congestion caused by uneven network utilization can be avoided" [107].

Constraint-based Routing can be used to make the traffic engineering process automatic. It enables computing routes that are subject to multiple constraints such as resource availability, QoS requirements, and other policies [107].

Constraint-based Routing increases the size of routing tables, and may introduce instability as routing tables change frequently [107]. Thus it should be considered whether it offers any benefit or just consumes more resources.

[10] An MPLS domain consists of MPLS-capable routers, called Label Switching Routers (LSRs).

[11] Labels are distributed to set up Label Switched Paths (LSPs) using Label Distribution Protocol (LDP) [107].

[12] Forwarding table is constructed as the result of label distribution [107].

[13] Routing Information Protocol, see [38, ch. 4].

[14] Open Shortest Path First, see [38, ch. 5].

[15] Intra-Domain Intermediate System to Intermediate System Routing, see [38, ch. 6].

Difficulties in development of a new service model

The nature of the Internet is decentralized and heterogenous. This causes several problems that need to be solved before new technologies can be deployed:

- Inter-domain QoS guarantees, CoS classifications, and the involved interaction between Internet Service Providers (ISPs) may represent problems due to different policies and diverse architectures of underlying networks .
- Usage of new services should be charged, otherwise they offer no benefit[16]. Charging for network usage in the Internet with a large number of ISPs might be difficult.
- Some proposed technologies demand ubiquitous deployment in order offer any benefit. However, big changes to the best-effort architecture currently in use are difficult, perhaps impossible to deploy.

Some of these problems and other aspects related to development of new service model are addressed in [81] and it's references 4, 8, 30, and 37.

6.3 Performance management

Performance management is used to evaluate the behavior of managed objects and the efficiency of communications activities. It is collecting statistical data, analyzing it, and where appropriate, predicting trends of communications between open systems [48].

A network performance management system must be able to provide reports on the efficiency of the system and its current and previous performance. Reports on a daily, monthly and annual basis are needed.

Performance management is also controlling traffic in the network. It consumes resources, and thus a separate control station is usually needed to collect and analyze traffic statistics. However, controlling traffic is a reliable and cost-effective

[16]Charging would ensure only the most performance-sensitive applications would request higher service.

method to find out problems before they exist. Traffic controlling can be limited to the most important parts of the network [8].

Performance management is related also to configuration management. It is easier for the operator to plan modifications of the network when the usage of the network is known.

Performance analysis

Network performance analysis becomes important when the network increases in size and complexity. Analyzers are used for traffic monitoring, protocol analysis and statistics collection and interpretation of performance-related data. Analyzers are understood as troubleshooting tools, but they should be used as proactive indicators as well.

The analyzers available typically gather and display large volumes of detailed data rather than interpret and highlight the meaning of the data. Many of these tools also look at a single element rather than the network as a whole. Data becomes information when it is organized, correlated and presented in a way that clarifies it's meaning, helping the network manager make the best decisions [24]. Managers must also predict future trends based on historical network trends and business information.

Until the introduction of expert systems, alarms and events were checked manually by the operators. Now expert systems are tested in the automation of this process. There are several artificial techniques that can be used, such as Rule-Based Reasoning (RBR), Bayesian Networks (BN), Neural Networks (NN), Case-Based Reasoning (CBR), Qualitative Reasoning (QR) and Model-Based Reasoning (MBR) [7].

Performance metrics

Generally, network performance metrics are classified into two areas: network-centric metrics and end-to-end measurements [78]. Network-centric metrics are:

- **Router and switch metrics**

  These metrics deal with operation of routers and switches; queuing packets, processing them, and placing them on the appropriate outbound link queue. The metrics include Offered load, Dropped traffic, and Average queue lengths (to assess queuing delays and potential dropped packets at a router).

- **Link metrics**

  These metrics describe the network capacity. They include e.g. Bandwidth Utilization.

- **Metrics for the routing sub-system**

  These metrics describe the impact of the routing traffic and fluctuations on the network performance. The rate of route changes characterizes the stability of the network system.

End-to-end metrics are:

- End-to-end latency and jitter ,
- Effective throughput, usually measured as a function of the packet size and the window size, and
- Packet loss probaility.

The tools and techniques required to measure performance characteristics in these two categories are different. In the Internet performance analysis it has been difficult to define metrics, that reflect both perspectives.

Performance management control

Performance management control is responsible for controlling the performance of a network. It includes such areas as network traffic management policies, traffic control, traffic administration, performance administration, execution of traffic control, and audit reporting [96, page 56].

Traffic control needs resources. Usually a separate control station is needed to collect and analyze traffic statistics. There should be a method to link a control station so that the traffic information is collected from the network. Controlling the traffic is, however, a reliable and cost effective method for finding out problems before they exist. Traffic controlling can be limited to the most important parts of the network [8].

Performance management is also related to the configuration management. It is easier for the operator to plan modifications of the network, when the use of the network is known.

Operator finds out which connections and services are used and which are needed.

7 SERVICE MANAGEMENT

This chapter discusses service management. Section 7.2 describes what kind of services can be in networks, who uses and who offers these services. Section 7.7 discusses accounting as enterprice level, while section 7.6 studies customer care and billing processes. Section 7.10 studies service platforms and hybrid services.

7.1 Introduction

Growing services (such as e-commerce, web hosting etc.) are being deployed over an infrastructure that spans multiple control domains. These end-to-end services require co-operation in internetworking between multiple organizations, systems and entities. Service providers need to deploy interoperability, distributed scaleable architectures, integration and automation of network management systems. The management system must make management easy and flexible to service providers. The management system must also make service providers operations and end goals easier [10].

Service providers need to find new and effective ways to [22]:

- Deploy services more quickly
- Deliver guaranteed services through service-level agreements (SLA)
- Evolve from reactive network management to proactive service management
- Reduce costs by automating network and service management.

Currently, there are no standard mechanisms to share selective management information between the various service providers or between service providers and their customers. Such mechanisms are necessary for end-to-end service management and diagnosis as well as for ensuring the service level obligations between a service provider and its customers or partners [10].

7.2 Services in the Network

Today, Internet has many services, such as filetransfer with FT-P, WWW-pages, IP telephony, multimedia services etc. In the future, the amount of services will increase, for example Video on Demand (VoD) services will become available and easy to use; mobility will become important.

Services

According to Kong, Chen and Hussain: "A service is anything that a service provider determines that customers will wish to purchase and that the service provider is willing to supply." [50]

Another service definition: "A service is a set of functions offered to a user by an organisation." [74, page 889]

More service definitions: "A service is an application with a well-defined interface and functionality." [10]

Service is defined in International Telecommunication U-nion — Telecommunication standards (ITU-T) and ISO systems management documents: "An abstract concept that includes the behaviour of a service provider as seen by a service user. Alternatively, the service definition includes a set of capabilities provided to a service user by a service provider. Service definition does not include the internal behaviour of a service provider." [97, pages 82–83]

IP network gets more customers, because more services will be available for customers. This has raised the importance of service management. In the past, technology orientation has placed products and equipment ahead of the services. Today, customers want reliable and easy use of services. For example, customers do not want to use different login names and passwords when connecting to services. Microchips cards could be a method used for identification and authentication.

IP Networks and Convergence in Telecommunications

Internet is popular as the basic infrastructure in providing world-wide distributed services to end-users. The Internet is an open and distributed environment which allows different types of service providers to provide different types of services on the network [50, page 22].

Massive IP network might include the Internet, but also Cable television (CATV), telecommunication networks, such as Public Switched Telecommunications Network (PSTN), Integrated Services Digital Network (ISDN), Intelligent Network (IN), and mobile systems. However, there are two other important network technologies which make new services available: wireless transmission on radio frequencies, and microwave satellite transmission.

Telephone companies are interested in delivering non-telephone services to end-users. CATV providers are interested in telephone and Internet services as well as Video on demand (VoD) services. These companies believe that cost savings are possible through value-added services. Also, the number of end users is increasing. These users have unique interests, and because of their interests, they require different services from the service providers. [66, page 129]

The CATV industry is migrating to a digital transmission technology, in order to increase the number of TV channels and services available to the end users. To provide new services, such as VoD and interactive TV, the CATV industry is designing bi-directional networks. End-users are connected to video servers, and they can select the video program, and the video program is sent over the network to the user [104, pages 16–19].

The differences between telephone, computer, and CATV networks are still great. However, each type of network is now able to provide services that were originally created for other networks. This tendency is convergence [104, page 20].

Media industry, telecommunications industry and computer industry are converging. Media industry produces the content, for example entertainment and publishing. Computer industry produces equipment and applications, which can make this content available for everyone. Telecommunications industry, both fixed and mobile, produces the connections to networks. See Figure 7.1 [90]

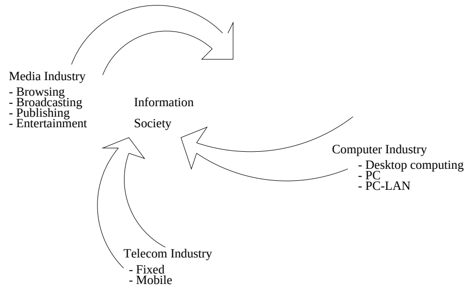

Figure 7.1: Convergence [90]

Service Providers

By service providers we means companies that provide services as a business on the network. Service providers operate on the network, or they integrate the services of other provides in order to deliver services to their customers.

Service providers are increasingly using Service Level Agreements (SLAs) to define agreements for sharing resources with partners, as well as for offering service quality guarantees to customers. These SLAs contain details of information that are shared, and service level guarantees that are offered by the service provider [10].

Service providers offering reliable services in a cost-efficient way will succeed. Service users do not use services that are not operating properly. Cost-efficiency means that service providers can easily add new services or update old services.

Service users

Service users are often called end-users or customers. Service providers have to fulfil end-user needs before the end-user uses any services.

The service users want that the user interfaces of the services are logical and easy to use. They also expect that the connection and the billing are reliable, installations are easy and software products are good.

Basic security services that are defined in ITU-T Recommendation X.800 are:

- **Access control**

  Access control is the property of controlling network and computer resources in such way that only legitimate users can access them within their limits. One approach is to attach to an object a list which explicitly contains the identity of all permitted users (an Access Control List (ACL)) [82]. Access control tools are discussed on page 41.

- **Authentication**

  Authentication is the property of knowing that the data received is the same as the data that was sent and that the claimed sender is in fact the actual sender. Several authentication techniques have been developed, for example technologies that provide passwords that are only used once (commonly called one-time passwords), and Kerberos. Kerberos is software designed and developed at Massachusetts Institute of Technology (MIT) to perform distributed authentication in an insecure network environment.

- **Confidentiality**

  Confidentiality is the property of communicating so that the intended recipients know what was being sent but unintended parties cannot determine what was sent. Encryption is commonly used to provide confidentiality.

- **Integrity**

  Integrity is the property of ensuring that data is transmitted from source to destination without undetected alteration. One way to provide integrity is to produce a checksum of the unaltered file, store that checksum offline, and periodically (or when desired) check to make sure the checksum of the online file hasn't changed (which would indicate the data has been modified) [82].

- **Non-repudiation**

  Non-repudiation is the property of a receiver being able to prove that the sender of some data did in fact send the data even though the sender might later desire to deny ever having sent that data [5].

Effective security management must be involved in all steps of data storage and transfer process. Logs are important security tools and therefore security management is involved with the collection, storage and examination of the audit records and security logs. Increasing the level of network security will affect to the openness of the system and to the cost of maintaining the network.

7.4 Authentication and authorization

Almost all applications utilize user information and presume an authentication of users. Authorization is determining whether an identity is permitted to perform some action, such as accessing a resource [57]. Passwords, smart cards and certificates are used to authenticate a user. A user may have a right to use more than one name and identities established by multiple organizations (such as universities and scholarly societies). There might be an advantage if all the user information is available in same directory. All the applications could then use the same information. Users have to log in only once to be able to use all the services and resources [61].

There are some basic requirements for authentication [57]:

- Access management solution needs to work at a practical level,
- The solution needs to be secure
- It should make access easier, minimizing redundant authentication interactions and providing user-friendly information resources,
- It needs to scale,
- It needs to be robust, for example, a forgotten password should not be an intractable problem,

- It must be able to recognize the need for a user to access a resource independent of his or her physical location (for example, a user must be able to connect to the internet via a commercial Internet Service Provider (ISP), a mobile IP link, or a cable television Internet connection from home), and
- There should be a simple and well-defined (standard) interface between resource operator and licensing institution.

The basic access management problem is licensing agreements for networked information resources. The situations where institutions agree to share limited access are difficult. There is a need for fine-grained access control where institutions want to limit resource access to only individuals registered for a specific class, for example, when a class may be offered to students at multiple institutions. At present, most access to network information resources is not controlled on a fine-grained basis. There is a danger that by accommodating all the needs for fine-grained access management into the basic access management mechanisms will produce a too complex and costly system [57].

Management data represents a problem in the current access framework. The problem is the conflict between private and public data. Most of the data has to be sorted out at the institutional policy level and it may involve making sacrifices in order to ensure privacy. Some institutions may be legally limited in their ability to collect certain management data.

Proxies and credential-based authentication (the user presents a credential to the operator as evidence that he or she is a member of the user community) schemes seem to be viable. Proxy servers will become a focal point for policy debates about privacy, accountability and the collection of management information. Successful operation of a proxy server means that the user trusts the licensee institution to behave responsibly and to respect privacy.

A cross-organizational authentication system based on a credential approach has the advantage of greater transparency. Resource operators can have a higher level of confidence in the access management mechanisms and a greater ability to monitor irregular access patterns. Privacy, accountability and collection of management statistics must be taken up for discussion among a larger group of parties.

An institution might choose to manage access by IP source address. IP source filtering means that packets are filtered on the basis of their source address. It does not seem to be a viable solution for access management. However, it may be very useful for some niche applications, such as supporting public workstations. It could be used more widely, although it cannot support remote users flexibly in its basic form. Most real-world access management systems are going to have to employ multiple approaches and IP source address filtering is likely to be one of them [57].

7.5 Security problems of Internet

The list below describes the security problems in the current Internet.

- **Weak authentication**

  Passwords on the Internet can be cracked by a number of different ways. The two most common methods are cracking the encrypted form of the password, and monitoring communications channels for password packets.

  Another problem with authentication results from some TCP or UDP services being able to authenticate only to the granularity of host addresses and not to specific users. For example, an NFS (UDP) server cannot grant access to a specific user on a host, it must grant access to the entire host. The administrator of a server may trust a specific user on a host and wish to grant access to that user, but the administrator has no control over other users on that host and is thus forced to grant access to all users (or grant no access at all).

- **Ease of spying and monitoring**

  When a user connects to his or her account on a remote host using TELNET or FTP, the user's password travels across the Internet unencrypted. A method to break into systems is to monitor connections of IP packets bearing a username and password, and then use them to login normally. If an administrator-level password is captured, the job of obtaining privileged access is made much easier.

Electronic mail, as well as the contents of TELNET and FTP sessions, can be monitored and used to learn information about a site and its business transactions. Most users do not encrypt e-mail, yet many assume that e-mail is secure and thus safe for transmitting sensitive information.

The increasingly popular X Window System is also vulnerable to spying and monitoring. The system permits multiple windows to be opened at a workstation.

- **Host-based security does not scale**

  Host-based security does not scale well: as the number of hosts at a site increases, the ability to ensure that security is at a high level for each host decreases. Secure management of just one system can be demanding, managing many such systems could easily result in mistakes and omissions. A contributing factor is that the role of system management is often short-changed and performed in haste. As a result, some systems will be less secure than other systems, and these systems could be the weak links that will break the overall security chain [103].

7.6 Customer Care and Billing

Customer care and billing (CCB) processes have been traditionally kept as a background process. CCB processes have not been the key functions in the business. Today, customer care and billing are an important part of making profit.

Good customer care and billing enables getting more profit, better customer relationships, and competition advantage. Today, succeeding in the market depend more on the quality of products and services than just the prices.

1980's was product oriented time in the telecommunication and data transfer market, while customer orientation is leading now. Marketing to the customers as well as the ability to sell more and the ability to high quality customer care are one of the key components to success. Also, it is important to get the products quickly to the market, and to be able to support existing and new services. A good customer care and billing system has to be flexible enough to fulfil these criteria [2].

Even electronic commerce depends on customer relationships, says Lester Wanninger, professor at the University of Minnesota. It is important to teach how to make good customer relations for people going to start electronic commerce. Also, in electronic commerce a company and a customer should handle all the communication channels. Electronic commerce has to implement functional processes of the company, information systems, databases, and other channels. It is important that a customer gets the same service from any service channel of the company. Ease of use brings more value to the customer. Also, in electronic commerce, the customer buys again only if the customer gets what was promised. WWW-pages can have effect on attitudes, intends, and shopping habits. High quality information, easy use, and new experiences, binding customers to services. Traditional media, such as TV, radio, and printed media are good in getting new customers, while the Internet is good in keeping old customers [47].

Customer Care

Customer care means maintaining customer services and customer relationships and answering routines, for example Help desk functions. Customer care links to the level of the offered service and the connection with the service level and the price of the service [91].

Customer care deals with processes needed to deliver services to customers, such as order handling, problem solving, performance reporting, and billing.

Good customer care system enables providing current and accurate information to the customers. It helps in delivering services when promised and resolving problems quickly and keeping customers informed, of the status of their orders. It also enables meet stated service level agreements (SLAs) for performance and availability, and providing accurate billing in a format that customer wants. This all ensures that the customer gets good service from the service provider.

A automation of customer care enables better services and cost savings. The service provider's Help desk can see all the information needed quickly, and then he or she can answer to the customer. Also, new services can be implemented and delivered to the customers easily when customer care processes are automated. Service providers can use the same methods to all services, when customer care processes are automated.

Billing

Internet is becoming able to support heterogeneous applications and services to a diverse user community. Delivered services must be billed. In the future we want to know who is using the network, what the network is being used for and when the network is being used [55]. Pricing mechanism will be necessary in order to manage the quality of services (QoS). Accounting and billing systems must be reliable, scaleable and have high performance, and offer flow-through operation from the other systems.

According to Busse [15], an accounting system should fulfil some basic requirements; it should be

- cost effective, performant, transparent,
- up-to-date information,
- customer configurable, and
- secure.

To be cost effective, the accounting system should be highly automated, based on standards, and easy to interact with. It should provide a reasonable response time. The whole accounting process should be transparent to the customer.

The accounting system should provide up-to-date information, i.e. it has to minimize the time needed to process the usage information from the network elements or other service providers. This is important especially when real-time information should be provided to the customer order status.

The accounting system should be configurable according to customer preferences for example with respect to tariff, billing cycle, details of the bill, local currency and taxes, the format in which the bill is expected, and the method of payment.

The accounting system should fulfil strong security requirements: identification, authentication, access control, confidentiality, integrity, and auditing.

Accounting process (see figure 7.2):

- **Tariff negotiation** The customer and the service provider negotiate the tariff during the subscription and service profile configuration phase. Usually the customer picks one of the standard tariffs offered by the service provider.
- **Usage metering** The service provider meters the usage of the resources during the operational phase. This includes the orders of the customers and the actual usage of the network. Readings are gathered from the network resources.
- **Charging** The tariff and usage information are combined and the charge is computed. This can be done directly after the connection was released, or regularly in order to prepare the bill.
- **Billing** The customer usually gets regular bills, e.g. once a month. The charging information of the period is collected and combined in a bill. Taxes are added. The customer will then be notified and the invoicing process will be triggered.
- **Invoicing** Within the invoicing process the system keeps track of the payment status of the bills of each customer. The customer can pay the bill in the way he or she wants.

Payment mechanisms

Internet payment mechanisms can be grouped into three classes: electronic currency systems, credit-debit systems and systems based on secure presentation of credit card numbers [69].

Collecting and rating usage, tracking services, managing inventories and reconciling invoices are key features of accounting systems [55].

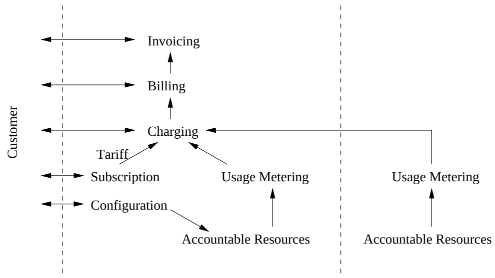

Figure 7.2: Accounting process [15]

The safety issues are under discussion. Some payment mechanisms are totally anonymous and payers can not be tracked (such as E-cash – electrical purse, where you load money and pay with it). The principal advantage of electronic currency is its potential for anonymity. The disadvantage is the need to maintain a large database of past transactions to prevent double spending.

In the credit-debit model (like NetCheque system), customers are registered with accounts on payment servers. Customers authorize charges against those accounts. The credit-debit model is audible. Once a payment instrument has been deposited, the owner of the debited account can determine who authorized the payment, and that the instrument was accepted by the payee and deposited [69].

Some payment mechanisms are based on credit cards (such as CyberCash). Information is often shared with the owner of the credit card, payment service provider and the credit card company. The owner of the credit card does not need to give his credit card number to the merchant without encrypting it. A customer's credit card number is encrypted using public key cryptography. The merchant has a message that it cannot read completely but which authorizes the purchase. The merchant adds his identification information and sends it to the CyberCash server. The entire message is digitally signed by the merchant to prevent tampering in transit. The CyberCash server unwraps the message and creates a standard credit card authorization request. The CyberCash server then forwards the request to the appropriate bank or processing house for authorization and returns the result to the merchant. The advantage is that the customer does not need to be registered with a network payment service; all that is needed is the credit card number [26].

Demands of electronic payment systems

Internet payment system should be secure, reliable, s-calable, anonymous, acceptable, flexible, convertible, effective, easy to integrate with applications and ease to use. An anonymity is more important in some communities or for certain kinds of transactions, than they are in other communities [69].

- **Security** The infrastructure must be usable and resistant to attacks in an environment where modification of messages is easy.
- **Reliability** The infrastructure must be available and should avoid failures.
- **Scalability** The payment infrastructure must be able to handle the addition of users without suffering loss of performance.
- **Anonymity** For some transactions, the identity of the parties to the transaction should be protected. Where anonymity is important, the cost of tracking a transaction should outweigh the value of the information that can be obtained by doing so.
- **Acceptability** A payment instrument must be accepted widely.
- **Customer base** The acceptability of the payment mechanism affects the size of the customer base.
- **Flexibility** Alternative forms of payment are needed. The payment infrastructure should support several payment methods including credit cards, personal checks, cashier's checks and anonymous electronic cash.
- **Convertibility** There will be several forms of payment, providing different trades.

- **Efficiency** Royalties for access to information may generate frequent payments for small amounts. Applications must be able to make these "micropayments" without noticeable performance deterioration.
- **Ease of integration** Applications must be modified to use the payment infrastructure in order to make a payment service available to users.
- **Ease of use** Users should not be constantly interrupted to provide payment information; most payments should occur automatically. Users should be able to limit their losses and monitor their spending.

Threats of misusing electronic currency can lead for example to dept (unpaid bills), forgeries, unauthorized payments on behalf of another person, double purchases (order twice – pay once), refusal of payments and unsuccessful deliveries.

Future billing requirements

Some of the requirements of the new billing systems include [64]:

- Real-time react to market activities
- Flexible billing formats and media to meet customer demands
- Flexible rating engine that allows discounting
- Integrated billing, which includes charges from third-party providers
- Well-defined interfaces to allow easy integration and data sharing between business systems and the billing system.
- Pre-paid services: Customers change to pre-paid service, so customers' loyalty to service provider will become more difficult to check. Customers can easily change the service provider, because they can easily buy new pre-paid services from any other service providers.
- Fraud and bad dept: Cheating and lost income remains a problem. CCB systems can help to get over and to prevent cheating.

- New technologies such as certificate based authentication will open more accurate and faster charging for the services.

7.7 Accounting management

Accounting management deals with information that concerns individual users, including following issues:

- **Usage measurement**

  Usage measurement is collecting data for charging, and processing the data. It has to be reliable, and sometimes it has to be done in real time.

- **Tariffing/pricing**

  A tariff is a set of data used to determine the charges for services used. It depends on the service, origination and destination, tariff period, and day.

- **Collections and finance**

  This includes administration of customer accounts, informing customers, payment dates, payment amount, and collection of payments.

- **Enterprise control**

  Enterprise control is responsible for proper financial management of an enterprise. It includes identifying and ensuring financial accountability of officers. Also, checks and balances needed for financial operation of an enterprise are included [97, pages 64–66].

A system that generates data for accounting purposes is called an accounting management agent. Accounting managers are systems, which interrogate accounting management data or obtain it in other ways. If accounting management is distributed across various systems, all systems may be required to control their own area themselves. Furthermore, a system may request information from other systems in order to square its accounts [48, pages 188–189].

Accounting data is sensitive information. The collector must provide confidentiality at the point of collection, through transmission and up to the point where the data is delivered. The delivery function may also require authentication of the origin and the destination and provision for connection integrity (if connections are utilized). Security services can be provided for example by SNMPv3[1].

Internet pricing

Internet pricing contains four basic elements (see figure 7.3). An accessfee is usually a monthly charge for using an access link of the network. The price depends on the capacity of the link. Setting up connections or making reservations can be charged separately. Usagefee can be used to charge services on time-, volume-, or QoS-basis. This fee determines the actual resource usage of a customer. Contentfee depends on the application content. It may be omitted (e.g., telephony, fax, e-mail services where the content is provided by the user), billed separately (e.g., Helsingin Sanomat on-line edition), or integrated into the telecommunications charging system (e.g., commercial 0900 numbers in Finland) [88].

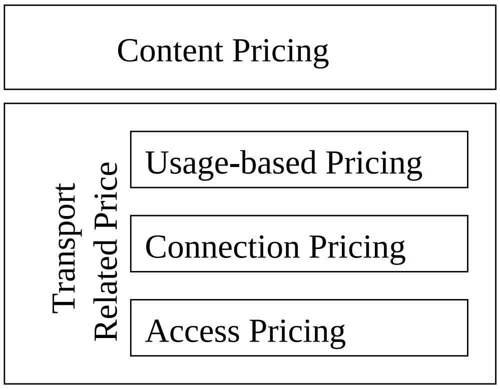

Figure 7.3: Components of Internet pricing [88]

The current pricing model is based on an assumption of a single best-effort service model that provides similar service to all customers. Service provider and customer do not have

[1] See section **??** for Simple Network Management Protocol (SNMP).

a direct control over the actual service in terms of parameters determining volume, connection time[2], and QoS.

Accounting is usually based on mechanisms offered by commercially available routers and switches. The most commonly used approach employs packet filtering and statistical sampling. However, it is difficult to charge for usage-based traffic since the granularity of these methods is too coarse and the measurement overhead significant [88].

Another problem concerning accounting data collection in routers is whether packets should be counted on entry to or on exit from a router[3] [65].

For volume measurements the IETF Real-time Traffic Flow Measurement (RTFM) working group has proposed standards to meter flows and to distribute this accounting information via SNMP [88].

The Remote Authentication Dial-In User Service (RADIUS) is a protocol specified by the IETF radius working group. It helps managing the Internet access links. Since these links are sensitive to security and accounting, a protocol is provided to authenticate dial-in users and negotiate configuration data. RADIUS services are implemented by most router manufactures. Accounting data can be collected on a time-, packet-, or octet-basis for a particular service [88].

7.8 Managing New Services

Managing new services means development of new services and taking care of the economic use of the network. For example implementing a cost-effective service quickly, and guaranteeing the specified service level to all end-users. End-to-end service process automation improves the accuracy and speed of a task while also freeing personnel from routine jobs. The advantages of automating end-to-end service process are in cost reduction and in improved customer service.

Today all service providers have to create their own services in the Internet. Same services are created in many different

[2]Connection time for connectionless communications would be difficult to measure (except for dialup access).

[3]The nature of IP is that not every packet received by a router is actually passed to an output port, but can be discarded for example at times of congestion.

ways, because there does not exist any one method to create new services in a way these services can be reused and modified.

7.9 Problems in Service Management

There are unresolved questions in service management:

- How can management information be shared across administrative domain boundaries in a secure way? This capability is important when a service is composed of components from several service providers.
- How to get measurable aspects from Service Level Agreements (SLAs)? It is unclear how a legal service level agreement document is translated into a measurable specification that can be automatically monitored for compliance.
- How to define metrics and their bounds for service compliance? There are no recommendations and policies to define what metrics are and how their values are computed.

7.10 Service Provisioning

Competition is increasing in service provision. Customer satisfaction is becoming important for service providers. One of the most critical problems faced by service providers today is managing of changes. The ability to focus deployment of new services and network technologies requires a new level of management flexibility to support a new level of customer care. Competitive advantage for service providers will depend on the ability to rapidly deliver end-to-end service solutions. A key management question is to meet these challenges. Service providers have to optimize their service management to meet business and customer needs [36, page 701].

Service Life Cycle

Services are usually implemented when needed in IP networks. Service providers do not have reusable service platform models, so they must always implement services from gratch. Service providers have their own service processes, which can be incompatible with other service providers systems and might be made with incompatible software, for example Java applets can cause problems.

WWW Service Platforms

The World Wide Web (WWW) is an architecture for sharing information. The WWW provides a hypertext system linking people, computers, and information around the world. The WWW consists of information servers and client browser programs, linked together by a set of standards and agreements. The user runs the browser to access WWW servers, which deliver information to the requesting browser [85, pages 87–88].

The key components of the WWW architecture are the Uniform Resource Locator (URL), the Hypertext Transfer Protocol (HTTP), and the Hypertext Markup Language (HTML) [85, page 88].

URLs provide standardized specifications for objects or resources located on a network, detailing both the network address of the object and the protocol to be used to interact with that object. See table 7.1.

Service	*Uniform Resource Locator (URL)*
Anonymous File Transfer	*ftp://ftp.frack.com*
Hypertext Transfer	*http://www.frack.com*
Remote Login	*telnet://frack.com*
Gopher Retrieval	*gopher://gopher.frack.com*
Wide-Area Info Service	*wais://wais.frack.com*
Usenet News	*nntp://news.frack.com*

Table 7.1: The URLs for various types of resources

The URL is an enhanced Internet address. WWW clients use the URL to find an object on the network and select the proper protocol for interacting with that object [85, pages 88–89].

The HTTP is a connection-oriented protocol designed for the rapid transport of files consisting of a mixture of text and graphics. HTTP uses an object-oriented protocol consisting of simple commands that support negotiation between the client and the server. This negotiation allows WWW browsers and servers to develop independently of emerging technologies because the negotiation process established a common basis of communication between the client and the server [85, page 89].

A universally understood language is needed when publishing information for global distribution. The publishing language used by the World Wide Web (WWW) is HyperText Markup Language (HTML) [102]. HTML is a standardized document tagging language, based on the Standardized Generalized Markup Language (SGML) [85, pages 89–90].

According to W3 [102], HTML gives authors the means to:

- Publish online documents with headings, text, tables, lists, photos, etc.
- Retrieve online information via hypertext links, at the click of a button.
- Design forms for conducting transactions with remote services, for use in searching for information, making reservations, ordering products, etc.
- Include spread-sheets, video clips, sound clips, and other applications directly in their documents.

HTML has been developed with the vision that all manner of devices should be able to use information on the Web: PCs with graphics displays of varying resolution and colour depths, cellular telephones, hand held devices, devices for speech for output and input, computers with high or low bandwidth. HTML now offers a standard mechanism for embedding generic media objects and applications in HTML documents. The object element provides a mechanism for including images, video, sound, mathematics, specialized applications, and other objects in a document. It also allows authors to specify a hierarchy of alternate renderings for user agents that don't support a specific rendering [102].

Problems

HTML based pages embedded with images, sounds and video clips are easy to create, but they can be uninteresting and do not allow true interactivity [83, page 5].

Communication between client programs (browsers) and servers is done using non-ideal paradigms (HTML). Instead of that, it should be done in an object-oriented manner, in order to reduce development time and increase ease of maintenance. Internet service developers find it difficult that support systems have to be hand-built for each service and each system must often be managed separately [83, page 6].

The use of services is often based on registration at the providers site. A user of several services has a multitude of login names and passwords. Also, payments for these services go directly to each provider, normally using credit cards. It is risky to send credit card numbers over the web and the user may not have any knowledge of how trustworthy the service provider is [83, page 6].

Today incompatible pages, usually made by Java script, have become a problem. These pages do not work perfectly with different browsers.

Directories

Directories are logical data repositories to save and to search for information. Directory services are important in helping users to find information on the network. Directory services must be reliable and secure in performance. Directories are used for example in saving personal data with telephone numbers and e-mail addresses. Data is often saved in logical tree form.

Special programs on the Internet have basic directory functions (mapping names to addresses and visa versa). The Domain Name System (DNS) provides these directory services on the Internet by mapping domain names to IP addresses and providing e-mail routing information for domain names.

A directory is a logical place for usernames and passwords as well as for public-key data such as certificates and keys. Another use of directories is yellow-pages functions, where searches find all entries in the directory where attributes satisfy some search criteria. Policy-based networks (PBNs) and guaranteed Quality of Service (QoS) applications are also driving the demand for directories [53].

There is a need to consolidate directory data. When intranet systems are expanded to extranet systems, there is a problem of combining different types of directories and databases.

A standardized model of directories will help this integration. Decreasing the number of directories means cost savings, higher data quality and lower security hazards (LDAP 1998). Development of an application is also easier if all the information is available in directories using standardized protocols [61].

Future service platforms

Current architectures in service management are based on management protocols like Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP) or trouble ticketing interface [15, page 167].

Web-based Architecture

In the Web-based architecture the customer downloads an applet that communicates with a proxy server in the service providers domain. The proxy server interacts with the actual inter-domain management system. It is possible to use standard gateways like IBM Webbin or build a service specific solutions in order to simplify the funtionality at the customer site. This makes download times shorter and there is less need for code [15, page 167].

The inter-domain management system implements the interactions with co-operating service providers. Requests to the local domain are processed by the intra-domain management system and then forwarded down the hierarchy to the network managers and finally to the network element managers [15, page 167].

Security restrictions in browsers do not allow applets to interact with local resources, i.e. with the file system or local network nodes. In Netscape Communicator, the security restrictions can be configured based on the right to trust relationships with the applet provider. Signed applets can be given the right to access the local network. This provides also a network management solution for customer premises network [15, page 167].

Figure 7.4 shows a indexweb-based service management architectureweb-based service management architecture. CP-N is Customer Premises Network and PN is Public Network.

This prototype has been developed providing a web based interface covering subscription management, configuration management, alarm surveillance, trouble ticketing as well as

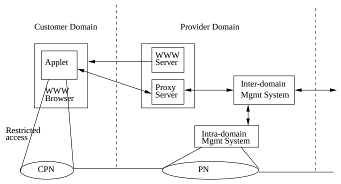

Figure 7.4: Web-based service management architecture [15, page 167]

accounting management. The usage of the web and Java (applets) simplifies the service interaction between the customer and the service provider. It will reduce the cost on both sides. For service provider it is important to automate the customer care process in order to cut the costs to survive in the emerging competitive market [15, page 168].

Demands for Future Service platforms

The convergence wave is coming. Mobile, fixed and Internet networks converge and create needs among consumers and business to access any service from any network. The same functionality and service provision is expected of all terminal devices; telephones, computers, cable televisions and other equipment. In the market convergence the telecommunications industry, the computer industry and the media industry are melting together. This creates new rules for service provisioning, branding and pricing, and opens new business opportunities for agile players, one being the provision of solutions that tie different networks or protocols together.

In the future service platforms follow these demands:

- provide extensive network services for converging networks
- enable fast time to market for new services
- provide ease of deployment, configuration, and management
- use the open, modular, distributed and standardised architecture

- ensure application-independent high quality of service and fault tolerance
- enable the use of advanced charging mechanisms
- make use of commercially available hardware and software components
- ensure high usability and appropriate diagnostics

Hybrid Services

Future services will span many communication infrastructures. Users will be able, for example, to generate telephone calls from their Web browsers. These services are called hybrid services. Hybrid services span different network technologies, for example the public switched telephone network (PSTN) and the Internet. Data networks do not offer much support in enabling such hybrid services other than transport and delivery. Most of the support for switching, billing, and access control of the calls is done in the switched network [99, page 167].

The demand for hybrid services is becoming more important, because cellular networks are already well integrated with the PSTN. These networks have wide penetration. This makes purely Internet-based solutions impractical. Taken separately, the PSTN and Internet are far from being an ideal ground for developing future hybrid services; however, if coupled together they can complement each other effectively [34, page 9].

The PSTN includes a powerful service creation and provision platform called Intelligent Network (IN). The design of IN follows a simple principle: separation of service-specific software from basic call processing. Before IN services were incorporated in the network switches in a manner that was specific to each manufacturer. Introducing new services required the modification of software in every switch in the network. It took years to complete such a process, and it made network operators dependent on their equipment suppliers. The IN reduced a great deal of this dependency by using service-specific software [34, page 9].

The Internet has no global service creation and provision framework. New services can be created by any user that can afford a server. Creating new services implies developing a distributed application that must be installed and executed in the terminals and servers. Internet applications take advantage of intelligent terminals and powerful user interfaces [34, page 9].

Hybrid services are expected to play a very important role in the years to come. This is due to both the desire of users to integrate the ways they communicate and the willingness of service providers to differentiate their offers from their competitors. Also, smart cellular phones are expected to fuel the integration of services [34, pages 9–10].

There has been extensive work toward validation of services in the IN or TINA services, bur there has not been much work on the application of formal methods of Internet to the development of Internet services or hybrid services [56, page 134]. There are main questions:

- Are Internet services and hybrid services any different from other telecommunication services?
- What do the differences mean for the application of formal techniques?

Interworking of Connect-Oriented and Connectionless Services

Hybrid services combine connection-oriented and connectionless techniques. There is no commonly accepted call model for hybrid services. Telecommunications industry use formal methods based on specific call models, such as those used in the IN. Formal methods were applied to standardized architectures such as the IN in which all services were structured in a similar way by using service-independent building blocks, the application and reuse of formal approaches was significantly easier [56, page 134].

The lack of a common call model for hybrid services implies that most of the work of applying formal techniques to telecommunication systems has to be revised and checked to see whether and how it can be reused and adapted for hybrid services [56, page 134].

Integration of Network-Centric and Terminal-Centric Service Control Mechanisms

In the Internet services are implemented in end users systems, while the telecommunications community normally has a network-centric vision where services are implemented in the network. These two different views of service control may converge to a service-centric vision for the deployment of hybrid services [56, page 134].

For the use of formal methods in development of hybrid services, it is necessary to consider software running at the user's site and in the network [56, page 134].

Decreased Service Lifetime and Time to Market

Introducing new services in a telephone or cellular network was a slow process, and the deployed of services were offered for a rather long period. Compared to typical telecommunication services, the time to market of Internet and hybrid services is significantly reduced. As market pressure increases and time to market decreases, increased development time using formal techniques on the development of hybrid services is hardly acceptable. It seems to be more promising to formally express single properties with which a service should comply, rather than developing large abstract service specifications [56, pages 134–135].

Significantly Increased Heterogeneity

An example of the impact of heterogeneity is the problem of service interactions. A service interaction occurs when the addition of a new feature to a system disrupts the existing services. In most cases it is wanted that the behaviour of a service does not change other services [56, page 135].

Whereas in homogeneous environments the assumptions are relatively easily defined and checked, this is rarely true for telecommunications systems, and definitely not true for hybrid services. As heterogeneity increases in the environment which hybrid services run, more time has to be spent to check whether the implemented service behaves correctly in its environment [56, page 135].

IP traffic on the Internet and private enterprise networks has been growing exponentially for some time. New high-speed and on-demand services create new network requirements. The network must handle special application packets, such as voice over IP and mission critical text-based data, in a way so that the data is delivered to the end user ahead of other traffic. IP networks offer no easy way to identify packets or subsequently give them special handling. This requires a protocol that would first check for available resources (admission control) and then reserve some amount of flow-specific state in the network [63].

This chapter describes content management in the Internet. Section 8.1 gives a definition of content managemen-t. Section **??** studies new technologies that are developed to improve Internet routing technology, such as IP switching, and Tag switching. Section 8.3 gives an overview of management information modeling technologies, such as markup languages, CIM, and DEN.

8.1 Definition of content management

In this project we mean content management as determining what kind of data is transmitted in the network, and managing that data according to its needs. This includes for example, flow differentiation and classification to different categories (services).

The purpose of the content management is to control the flow of content during the creation and delivery of any service. The basic needs for content management are, for example:

- Accounting,
- Monitoring (e.g. tracking network behavior and different flows), and
- Traffic prioritization and traffic guarantees (For example, policy-based networking enables the allocation of network resources to applications, users, and groups

based on a set of defined rules. This approach provides the control over traffic prioritization based on the business importance of applications.).

The content must be managed throughout its entire lifetime, from initial conception and creation, to integration in an application, and delivery to the user, as well as eventual archival or destruction. Information service providers have also multiple distribution options using a wide variety of client and network technologies. The key to commercial success is managing information in such a way that it can be easily located and distributed in a format that matches the requirements of the requesting client [?].

Cost sharing is also an important aspect of the Internet. Internet services that provide QoS (e.g. TV and radio over IP) cannot cover costs using pricing models available today. Full deployment of services with built-in cost sharing functionality could be the final reason to converge for example, broadcast media into the Internet and make them globally available [88].

8.2 Switching technologies

The increase in real-time and multimedia applications have created a need to improve Internet routing technology in terms of bandwidth, performance, scalability, and delivery of new functionalities. Technologies used to develop new systems are combinations of switching and routing technologies. Routing provides robustness (scalability and flexibility) and switching provides performance (high throughput). Noticeable technologies are Ipsilon's IP Switching, Cisco's Tag Switching, IBM's ARIS (Aggregate Route-based IP Switching), Toshiba's CSR (Cell Switching Router), and MPLS (Multiprotocol Label Switching).

This section gives a brief summary of flow differentiation, IP switching, and Tag switching. MPLS is studied in subsection 6.2.

Flow differentiation

A flow is defined as a sequence of packets sent from a particular host to a particular destination. These packets are related in terms of their routing and any local handling policy they may require.

Traffic differentiation is typically based on information in the packet headers of different layers in the IP protocol stack, e.g. protocol type, source/destination port, source/destination address or explicit flow tags. Two packets belong to the same flow if the values of header fields are identical. The higher up the information origins, the higher the semantic content, and thus the more precise differentiation. For example, using the content-type field of HTTP 1.1, packets can be easily identified as being part of a data, voice or video stream. On the downside, header parsing leads to performance drawbacks noticeable as increased induced traffic latency, which is only acceptable up to a certain degree for applications with real-time requirements [**?**].

IP Switching

IP switching is basically an IP over ATM technology. The IP switches use the hardware of ATM switches for the copying mechanism and the IP software for the routing. The IP switches allow packet flows to be switched and bypass the router, when the routing information has been cached in the switch. IP switching is made up of two protocols GSMP (General Switch Management Protocol) and IFMP (Ipsilon Flow Management Protocol). GSMP is defined in [**?**] and IFMP in [70].

When a packet is assembled and submitted to controller in an IP switch it classifies a flow. Ipsilon has defined currently two types of flows. **A host pair flow type** is defined for traffic between same source and destination IP address. There is a local policy in each IP switch from which it makes its own QoS decisions. QoS information can be included in the flow classification decision based upon the application, the type of service field in the IP header, the protocol etc. The Resource Reservation Protocol (RSVP) can give each individual QoS requests for each flow, since the IP switch supports RSVP. **A port pair flow type** is defined for traffic between same source and destination port between same source and destination IP address. It allows differentiating QoS along the flows between the same pair of hosts. Simple flow-based firewall security features can also be supported.

Depending on the classification, the switch decides to forward or switch the next packets of that flow. Usually the controller would decide to forward short term flows like database queries, DNS messages and switch long term flows like ftp or telnet data. Flow classification takes care of classifying only long duration traffic because IP switching performs its best for such traffic. Other traffic is forwarded packet by packet [?].

Tag Switching

Tag switching technology forwards packets based on tags. The tag is a short, fixed length identifier that is assigned to packets belonging to a certain stream. Each packet gets a tag with an index pointer, which has information about the best route for the data stream. The pointer is used with the routing table to find the exact route. The packets will be forwarded by the switch to the next switch where the same procedure will be repeated. The tag switch forwards the packet based on the tag and does not look at the network layer header.

A Tag switching network consists of tag edge routers, tag switches, and tag distribution protocol. Tag edge routers are located at the edge of the network. Tag switches switch tagged packets based on the tags. Tag distribution protocol or extensions to existing routing protocols operate so that the tag information may be distributed in the network.

Tag switching is positioned to support multiple protocols, and to facilitate explicit routing and service differentiation. A tag could be bound to an individual application flow, a single route, group of routes or multicast tree [76].

8.3 Management information modeling technologies

This section gives a brief summary of markup languages and object-oriented models (CIM and DEN) that are developed to model management information.

Markup languages

Markup languages (such as SGML - Standardized Generalized Markup Language, HTML - HyperText Markup Language, and XML - eXtensible Markup Language) are designed to add structure and convey information about documents and data. In markup languages, the main mechanism for supplying structural and semantic information is by adding to the document elements comprising a start tag, optionally some content, and an end tag.

SGML does not enforce any particular set of element types. SGML provides a means by which new element types can be defined. Because of this, SGML is thought of as a language for defining markup languages. XML is similar in concept to HTML. Whereas HTML is used to convey graphical information about a document, XML is used to represent structured data in a document. HTML is an SGML application targeted at display markup for documents, XML is a subset of SGML targeted at data representation. It is possible therefore to imagine the Web as consisting of HTML for display purposes, and XML for data representation and description purposes [**?**].

Object-oriented models

Distributed Management Task Force Inc (DMTF) has developed the **Common Information Model (CIM)**. CIM is used to model management information from desktop and server systems. It is also used to describe management information between different management applications, such as HP Open View, Microsoft SMS, and Tivoli Management Software, in order to provide common understanding of management information.

CIM is an object-oriented conceptual model. It provides a framework, including representation of products, systems, applications, and components that can be managed. It unifies the information coming from many numbers of sources. CIM is not bounded to any particular implementation. It can be implemented as a relational database, as an object database, or as an object/relational database. This allows for the interchange of management information between management systems and applications.

At the present time, there are not any CIM based implementations available. No programming interfaces or protocols are defined by the CIM document, and hence it does not provide an exchange mechanism. CIM does not define a common set of APIs (application program interface) that software developers can use to make Web management applications work together. Nor does it specify how the database of gathered information should be structured. CIM makes also no mention of the communications protocol that should be used for moving all that information around. So it is difficult for vendors to develop software that can integrate data gathered by third-party applications [52].

Version 1.0 of the DMTF's CIM XML encoding specification was announced in 1998. Allowing CIM information to be represented in the form of XML, brings the benefits of XML and its related technologies to management information modeled using the CIM Meta model [25].

The **Directory Enabled Network** (**DEN**) specification provides a schema and informational model for representing network elements and services in a directory. The primary purpose of DEN is to separate the specification and representation of network elements, and services from implementation details.

In a directory enabled network user profiles, applications, and network services are integrated through a common information model that stores network state and exposes network information. This information enables bandwidth utilization to be optimized, it enables policy-based management, and it provides a single point of administration of all network resources.

The philosophy of network management is shown in figure 8.1. Network management protocols (SNMP, CMIP, H-MMP) are used to talk to the network elements. The network schema extensions for the directory service are used to talk about network elements.

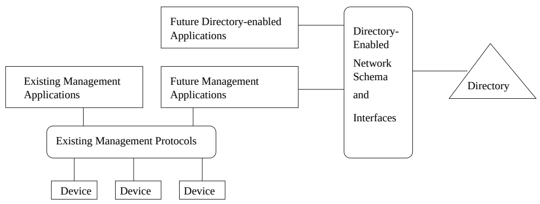

Figure 8.1: Directory service and network management [46]

The integration of the network infrastructure with the directory service allows the applications and users to discover the existence of devices and relationships by querying the directory service. This is more scalable and manageable than contacting the individual devices and aggregating the results. Exposing network elements in the directory enhances their manageability and usability while reducing the load on the network. The end user and administrator experience in enhanced because there is a single authoritative place to obtain the information of interest. One example of how the networkwide data might be used is to set up and tear down a certain level of QoS at a given time for a specified user across many network resources.

HP OpenView
Hewlett-Packard
In addition to traditional network management features, HP OpenView includes systems management and service management features. Users are provided with Web/Java-based and traditional user interfaces.
http://www.openview.hp.com

SUN Solstice
Sun Microsystems
Solstice is a traditional network management application. Different versions are provided for SOLARIS, Windows and Web/Java-based environments, and for TMN and SNMP network management.
http://www.sun.com/solstice

Java Dynamic Management Kit
Sun Microsystems
Java Dynamic Management Kit (JDMK) is the first application using JMAPI technology (for more information on JMAPI, see section 4.3). JDMK helps to develop Web-based management services using Java agents or JavaBeans for Management -technology.
http://sun.com/software

TIVOLI
IBM
TIVOLI is a network management system that contains features that meet the requirements of especially demanding network environments. The product is aimed at both enterprises and network operators.
http://www.tivoli.com

CYBERMANAGE
Wipro Limited
CYBERMANAGE is a Web-based network manager. Development tools are included.
http://cybermanage.wipro.com/index1.html

SPECTRUM
CABLETRON Systems
http://www.cabletron.com/spectrum

INTEL LANDesk
Intel
http://www.intel.com/network/products/LANDesk_srvr_mgr.htm

ASANTEVIEW
Asante Technologies, Inc.
http://www.asante.com/products/p_soft_int.html

UNICENTER TNG
Computer Associates
http://www.cai.com

CONCORD
Concord Communications
http://www.concord.com/products.htm

CLEARSTATS
RedPoint Network Systems
http://www.redpt.com/ClearStats/

NETSCOUT WEBCAST
Netscout
http://www.netscout.com/Products/WebCast/body_webcast.html

[1] *. SPIN homepage, 1999. Jun 2, 1999, http://www.iit.nrc.ca/SPIN_public/english.html.

[2] IBM. Press release, 1999. www2.clearlake.ibm.com/telmedia/ccb/pressa7.htm.

[3] ADISESHU, H., PARULKAR, G., AND YAVATKAR, R. A state management protocol for IntServ, DiffServ and label switching. In *Network Protocols* (Oct. 1998), pp. 272–281.

[4] ARNAUD, D. Security status and issues & Electronic commerce on the Internet, 1995. August 18, 1999, http://ecwww.eurecom.fr/~arnaud/zds/report/report.html.

[5] ATKINSON, R. Security architecture for the internet protocol. *RFC 1825* (1995).

[6] ATM FORUM. *Integrated Local Management Interface (ILMI) Specification Version 4.0*, Sept. 1996. AF-ILMI-0065.000.

[7] BACON, A. Expert systems use in fault management systems, 1999. April 16, 1999, http://www.cbu.edu/~pong/624arb1.htm.

[8] BALLEW, S. M. *IP-verkkojen hallinta Ciscon reitittimillä*. Suomen Atk-kustannus Oy, Helsinki, Finland, 1998.

[9] BAUMGARTNER, F., BRAUN, T., AND HABEGGER, P. Differentiated services: A new approach for quality of service in the internet. In *Proc. High Performance Networking, HPN'98* (Vienna, Austria, Sept. 1998), H. R. van As, Ed., pp. 255–273.

[10] BHOJ, P., SINGHAL, S., AND CHUTANI, S. SLA management in federal environments. In *Integrated Network Management VI* (Boston, USA, May 1999), IEEE, pp. 293–309.

[11] BLAKE, S., BLACK, D., CARLSON, M., DAVIES, E., WANG, Z., AND WEISS, W. An architecture for differentiated service. *RFC 2475* (Dec. 1998), 36.

[12] BLIGHT, D. C., AND HAMADA, T. Policy-Based Networking Architecture fo QoS Interworking in IP management. In *Integrated Network Management VI, Distributed Management for the Millenium* (Boston, USA, May 1999), pp. 813–826.

[13] BLOMMERS, J. *Practical Planning for Network Growth*. Prentice Hall PTR, New Jersey, USA, 1996.

[14] BRADEN, R., ZHANG, L., BERSON, S., HERZOG, S., AND JAMIN, S. Resource ReSerVation Protocol (RSVP) – version 1 functional specification. *RFC 2205* (Sept. 1997), 112.

[15] BUSSE, I. Accounting management for global broadband connectivity services. In *Network Operation and Management Symposium, NOMS'98* (New Orleans, USA, Feb. 1998), IEEE, pp. 159–168.

[16] CASE, J. D., DAVIN, J. R., FEDOR, M. S., AND SCHOFFSTALL, M. L. Internet network management using the simple network management protocol. In *Local Computer Networks, Proceedings 14th Conference on* (1989), pp. 156–159.

[17] CCITT RECOMMENDATION X.700. *Management Framework for Open Systems Interconnection (OSI) for CCITT Applications*, Sept. 92.

[18] CCITT RECOMMENDATION X.701. *Information Technology - Open Systems Interconnection - Systems Management overview*, 1992.

[19] CHAPMAN, D. B., AND ZWICKY, E. D. Firewall design, 1996. September 10, 1999, http://sunsite.cs.msu.su/sunworldonline/swol-01-1996/swol-01-firewall.html.

[20] CHAPMAN, M., AND MONTESI, S. Overall Concepts and Principles of TINA. Tech. rep., TINA-C, Feb. 1995.

[21] CHERKAOUI, O., RICO, N., AND SERHROUCHNI, A. SNMPv3 can still be simple? In *Integrated Network Management VI, Distributed Management for the Millenium* (Boston, USA, May 1999), pp. 499–516.

[22] CISCO SYSTEMS INC. Service management systems — white papers, 1999. http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/cms_wp.html. 1999.

[23] CLARK, D. The Internet picture, shaping the Internet of tomorrow. In *The New World of Information, International Seminar* (Helsinki, Finland, Mar. 1999), LSC International Seminar.

[24] CONCORD COMMUNICATIONS, INC. Managing network empowered businesses: Support for embattled network managers, 1999. April 20, 1999, http://www.concord.com/library/wpapers/02.htm.

[25] COVER, R. The SGML/XML web page, DMTF common information model (CIM), 1999. September 1, 1999, http://www.oasis-open.org/cover.

[26] CROCKER, S., BOESCH, B., HART, A., AND LUM, J. Cybercash: Payments systems for the internet. In *Commercial and Business Aspect, INET'95, ElectronicMoney* (1995), IEEE.

[27] DERI, L., AND MATTEI, E. An Object-Oriented Approach to the Implementation of OSI Management. *Computer Networks and ISDN Systems 27*, 9 (Aug. 1995), 1367–1385.

[28] DISTRIBUTED MANAGEMENT TASK FORCE, INC. Common information model faq, 1999. Aug 25, 1999, http://www.dmtf.org/spec/cimfaq.html.

[29] DISTRIBUTED MANAGEMENT TASK FORCE, INC. Common information model tutorial, 1999. Aug 25, 1999, http://www.dmtf.org/educ/tutorials/cim/.

[30] DROMS, R. Dynamic host configuration protocol. *RFC 2131* (Mar. 1997), 45.

[31] ETSI ETR 037. *Network Aspects (NA); Telecommunications Management Network (TMN) Objectives, principles, concepts and reference configurations*, Feb. 1992. DTR/NA-043202.

[32] ETSI ETR 230. *Network Aspects (NA); Telecommunications Management Network (TMN); TMN standardisation overview*, Nov. 1995. DTR/NA-043207.

[33] FULLER, W. Network management using expert diagnostics - a white paper, 1999. April 26, 1999, Summit On Line, http://www.summitonline.com/netmanage/papers/stanford1.html.

[34] GHAGUIDI, C., HUBAUX, J.-P., AND HAMDI, M. A programmable architecture for the provision of hybrid services. *IEEE Communications Magazine* (July 1999), 110–116.

[35] HARKINS, D., AND CARREL, D. The internet key exchange (IKE). *RFC 2409* (Nov. 1998), 41.

[36] HARRIS, S. J. Proactive service management: Leveraging telecom information assets for competitive advantage. In *Network Operations and Management Symposium* (1996), IEEE, pp. 700–710.

[37] HAUTANIEMI, M. TKK/Atk-keskuksen TCP/IP-vekon valvonta ja hallinta. Master's thesis, Department of Computer Science and Engineering, Helsinki University of technology, 1994. April 23, 1999, http://www.hut.fi/~hau/thesis/verkonhall_toteutus.html.

[38] HUITEMA], C. *Routing in the Internet*. Prentice-Hall, Inc., 1995.

[39] HUNT, C. *TCI/IP Network Administration*. O'Reilly & Associates, Inc., Sebastopol (CA), USA, 1993.

[40] HUNT, C. *TCP/IP Network administration*. O'Reilly & Associates, Inc, May 1994.

[41] ICL. ICL:n verkkoaapinen, verkkoratkaisut ja palvelut, 1999. August 25, 1999,
http://www.icl.fi/.

[42] INTERNET ENGINEERING TASK FORCE. Differentiated Services working group, 1999. Aug 10, 1999,
http://www.ietf.org/html.charters/diffserv-charter.html.

[43] INTERNET ENGINEERING TASK FORCE. Integrated Services working group, 1999. Aug 10, 1999,
http://www.ietf.org/html.charters/intserv-charter.html.

[44] INTERNET ENGINEERING TASK FORCE. Multiprotocol Label Switching working group, 1999. Aug 17, 1999,
http://www.ietf.org/html.charters/mpls-charter.html.

[45] ITU-T RECOMMENDATION Q.750. *Overview of Signalling System No.7 Management*, Mar. 1993.

[46] JUDD, S., AND (EDITORS), J. S. Directory-enabled networks, information model and base schema (version 3.0c5, 1998. September 6, 1999,
http://murchiso.com/den/specifications/directory-enabled-networks-v3-lastcall.pdf.

[47] KARONEN, J. Sähköinen kaupankäyntikin on asiakassuhteesta kiinni. *WOW!-verkkolehti* (July 1999). 12.7.1999, http://www.wow.fi/.

[48] KAUFFELS, F.-J. *Network Management, Problems, Standards and Strategies.* Addison-Wesley Publishing Company, New York, USA, 1992.

[49] KENT, S., AND ATKINSON, R. Security architecture for the internet protocol. *RFC 2401* (Nov. 1998), 66.

[50] KONG, Q., CHEN, G., AND HUSSAIN, R. Y. A management framework for internet services. In *Network Operation and Management Symposium, NOMS'98* (New Orleans, USA, Feb. 1998), IEEE, pp. 21–30.

[51] KOTH, A., EL-SHERBINI, A., AND KAMEL, T. A new interoperable management model for IP and OSI architectures. In *AFRICON, IEEE AFRICON 4th* (Sept. 1996), vol. 2, pp. 944–949.

[52] LARSEN, A. K. Network analysis, CIM's missing pieces, 1997. CMP's TechWeb, September 16, 1999, http://data.com/tutorials/cim.html.

[53] LDAP. Fulfilling the promise for directory-enabled networks, 1998. http://www.cnilive.com/impact/specials/ldap/.

[54] LE FAUCHEUR, F. IETF Multiprotocol Label Switching (MPLS) Architecture. In *ICATM-98* (June 1998), pp. 6–15.

[55] LIDYARD, D. New technologies and strategic trends: An introduction to network accounting, 1999. http://www.summitonline.com/netmanage/papers/telco1.html.

[56] LOGEAN, X., DIETRICH, F., AND HUBAUX, J.-P. On applying formal techniques to the development of hybrid services: Challenges and directions. *IEEE Communications Magazine* (July 1999), 132–138.

[57] LYNCH, C. A white paper on authentication and access management issues in cross-organizational use of networked information resources, 1998. May 5, 1999, Coalition for Networked Information Revised Discussion Draft, http://www.cni.org/projects/authentication/authentication-wp.html.

[58] MAGEDANZ, T., AND POPESCU-ZELETIN, R. *Intelligent Networks - Basic Technology, Standards and Evolution.* Thomson, 1996.

[59] MASSOULIÈ, L., AND ROBERTS, J. Arguments in favour of admission control for TCP flows. In *Proc. ITC-16, Teletraffic Engineering in a Competitive World* (Edinburgh, United Kindom, June 1999), P. Key and D. Smith, Eds., vol. 3a, pp. 33–44.

[60] MAUGHAN, D., SCHERTLER, M., SCHNEIDER, M., AND TURNER, J. Internet security association and key management protocol (ISAKMP). *RFC 2408* (Nov. 1998), 86.

[61] MENSOLA, S. IP-verkon kommunikaatiopalveluiden hallinta. Master's thesis, Department of Electrical and Communications Engineering, Helsinki University of Technology, 1998. May 3, 1999, http://kyyppari.hkkk.fi/~k23332/dippa/luku2.htm.

[62] MESEROLE, T. A., AND HALL, M., Eds. *M4 Interface Requirements and Logical MIB: ATM Network Element View*. ATM Forum, Oct. 1998. AF-NM-0020.001.

[63] METZ, C. Ip qos: Traveling in first class on the internet. *IEEE Internet Computing* (Mar. 1999).

[64] MICROSYSTEMS, S. Products and solutions, telecommunications billing systems, an overview, 1999. http://suncom.bilkent.edu.tr/products-n-solutions/telco/billing_bkgrounder.html.

[65] MILLS, C., HIRSH, D., AND RUTH, G. Internet accounting: Background. *RFC 1272* (1991).

[66] MORI, K., YAMASHITA, S., NAKANISHI, H., HAYASHI, K., OHMACHI, K., AND HORI, Y. Service accelerator (SEA) system for supplying demand oriented information services. In *Autonomous Dezentralized Systems, ISADS 97* (1997), IEEE, pp. 129–136.

[67] MUSCIANO, C. Network or nightmare? Adding computers adds complexity. How do you keep up?, 1998. April 20, 1999, http://www.sunworld.com/swol-09-1998/swol-09-network.html.

[68] NETWORK GENERAL CORPORATION. Proactive solutions to the five most critical networking problems, 1997. April 21, 1999, Summit On Line, http://summitonline.com/netmanage/papers/netgen2.html.

[69] NEUMAN, B. C., AND MEDVINSKY, G. Netcheque, netcash, and the characteristics of internet payment services. *The Journal of Electronic Publishing 2* (May 1996). http://ing.ctit.utwente.nl/WU5/literature/works/NeumNetPay.html.

[70] NEWMAN, P., EDWARDS, W. L., HINDEN, R., HOFFMAN, E., LIAW, F. C., LYON, T., AND MINSHALL, G. Ipsilon flow management protocol specification for IPv4, version 1.0. *RFC 1953* (May 1996), 19.

[71] NICHOLSA, K., BLAKE, S., BAKER, F., AND BLACK, D. Definition of the differentiated services field (DS Field) in the IPv4 and IPv6 headers. *RFC 2474* (Dec. 1998), 20.

[72] OBJECT MANAGEMENT GROUP. *CORBA-based Telecommunication Management System.* OMG White Paper, May 1996.

[73] OUESLATI-BOULAHIA, S., AND OUBAGHA, E. An Approach to Routing Elastic Flows. In *Proc. ITC-16, Teletraffic Engineering in a Competitive World* (Edinburgh, United Kindom, June 1999), P. Key and D. Smith, Eds., vol. 3b, pp. 1311–1320.

[74] POPIEN, C., AND KUEPPER, A. A concept for an ODP service management. In *Network Operations and Management Symposium* (1994), IEEE, pp. 888–897.

[75] PULKKI, A. The IP security architecture. In *Proceedings of the HUT Network Seminar '96* (1995), Department of Physics, Helsinki University of Technology. July 7, 1999, http://www.tcm.hut.fi/Opinnot/Tik-110.501/1995/ipsec-arch.html.

[76] REKHTER, Y., DAVIE, B., KATZ, D., ROSEN, E., AND SWALLOW, G. Cisco systems' tag switching architecture overview. *RFC 2105* (Feb. 1997), 13.

[77] ROBINSON, C. Integrated network management for multimedia networking, 1999. April 19, 1999, http://engineer.home.mindspring.com/book.htm.

[78] SAN DIEGO SUPERCOMPUTER CENTER. White paper on network performance metrics, 1999. July 5, 1999, http://www.sdsc.edu/DOCT/Publications.html.

[79] SCHÖNWÄLDER, J., AND QUITTEK, J. Secure management by delegation within the Internet management framework. In *Integrated Network Management VI* (Boston, USA, May 1999), IEEE, pp. 690–692.

[80] SEPPÄNEN, K. Network management in ATM based B-ISDN. In *Proceedings of the Seminar on Telecommunications Architectures'99* (1999), J. Karvo, Ed.

[81] SHENKER, S. Fundamental design issues for the future internet. *IEEE Journal on Selected Areas in Communications 13*, 7 (Sept. 1995), 1176–1188.

[82] Site security handbook. *RFC 2196* (1997). Fraser, B., Ed.

[83] SMITH, C. Applying TINA-C service architecture to the Internet and Intranets. In *Global Convergence of Telecommunications and Distributed Object Computing, TINA 97* (1997), IEEE, pp. 4–12.

[84] STALLINGS, W. *Local and Metropolitan Area Networks*, 4 ed. Maxwell MacMillan International, New York, USA, 1993.

[85] STALLINGS, W. *Internet Security Handbook, Protection and Survival on the Information Superhighway*. McGraw-Hill Book Company, London, 1995.

[86] STEINBERG, L. Techniques for managing asynchronously generated alerts. *RFC 1224* (1991).

[87] STEVENSON, D. W. Network management - what it is and what it isn't, 1995. May 26, 1999, http://netman.cit.buffalo.edu/Doc/Dstevenson.

[88] STILLER, B., FANKHAUSER, G., PLATTNER, B., AND WEILER, N. Charging and accounting for integrated Internet services - state of the art, problems, and trends. In *The Internet Summit, INET'98* (Switzerland, July 1998), IEEE.

[89] SUN MICROSYSTEMS. Java^{TM} Management API (JMAPI), 1999. Jun 2, 1999, http://www.javasoft.com/products/JavaManagement/.

[90] SVANBÄCK, R. Mobile business trends. In *The 8th Summer School on Telecomminications* (Aug. 1999), Lappeenranta University of Technology.

[91] TAG, 1999. www.tag.co.uk/techterm.nsf/all.

[92] TELEMANAGEMENT FORUM. *SMART TMN^{TM} Technology Integration Map*. Telemanagement Forum, Oct. 1998.

[93] TELEMANAGEMENT FORUM. SMART TMN overview, 1999. Jun 2, 1999, http://www.tmforum.org/pages/overview/tmfovr.html.

[94] THE OPEN GROUP. X/Open Guide, Systems Management: Reference Model, 1997. Apr 5, 1999, http://www.opengroup.org/onlinepubs/009279299/toc.htm.

[95] TINA-C. Principles of TINA, 1999. Apr 11, 1999, http://www.tinac.com/about/principles_of_tinac.htm.

[96] UDUPA, D. K. *Telecommunications Managemement Network*, 1 ed. McGraw-Hill, 1999.

[97] UDUPA, D. K. *TMN Telecommunications Management Network*. McGraw-Hill, New York, USA, 1999.

[98] VALLILLEE, L. SNMP and CMIP - An Introduction to Network Management, 1999. May 26, 1999, http://Home.InfoRamp.Net/~kjvallil/t/work.html.

[99] VANECEK, G., MIHAI, N., VIDOVIC, N., AND VRSALOVIC, D. Enabling hybrid services in emerging data networks. *IEEE Communications Magazine* (July 1999).

[100] VISWANATHAN, A., FELDMAN, N., WANG, Z., AND CALLON, R. Evolution of Multiprotocol Label Switching. *IEEE Communications Magazine 36*, 5 (May 1998), 165–173.

[101] VON KNORRING, N. Tina management principles. In *Proceedings of the Seminar on Telecommunications Architectures'99* (1999), J. Karvo, Ed.

[102] W3. HTML 4.0 specification, W3C recommendation, Apr. 1998. http://www.w3.org/TR/REC-html40/intro/intro.html#h-2.2.

[103] WACK, J. P., AND CARNAHAN, L. J. *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls.* NIST Special Publication 800-10, U.S.Department of Commerce, National Institute of Standards and Technology, 1999. August 16, 1999, http://csrc.nist.gov/nistpubs/800-10/main.html.

[104] WALRAND, J., AND VARAIYA, P. *High-Performance Communication Networks.* Morgan Kaufman Publishers Inc., San Francisco, USA, 1996.

[105] WARRIER, U., AND BESAW, L. The common management information services and protocol over TCP/IP (CMOT). *RFC 1095* (1989).

[106] WROCLAWSKI, J. The use of RSVP with IETF integrated services. *RFC 2210* (Sept. 1997), 33.

[107] XIAO, X., AND NI, L. Internet QoS: a big picture. *IEEE Network 13*, 2 (Mar. 1999), 8–18.

[108] ZHANG, L., DEERING, S., ESTRIN, D., SHENKER, S., AND ZAPPALA, D. RSVP: A new resource ReSerVation Protocol. *IEEE Network 7*, 5 (Sept. 1993), 8–18.