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

IP network management

IPMAN-project Interim report, Dec. 1999

Liisa Uosukainen Tuomas Lilja Lasse Metso Stiina Ylänen

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

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

©1999 IPMAN project

ISBN 951-XXX
ISSN 95Y Y

Contents

Abstract

Abbreviations

1 Introduction
1.1 Changes in network management . . . . .
1.2 Future trends 1
1.3 Structure of this document 1

2 Network Management Models **1**
2.1 OSI Management 1
Management Model 1
Information Model 1
Systems Management Functions 1
Management Functional Areas — OSI FCAPS model . . . 1
2.2 Telecommunications Management Network 1
TMN Management Services 1
TMN Management Layers 1
TMN Architecture 1
2.3 Customer Network Management 1
2.4 SMART TMN 1
2.5 Telecommunications Information Networking Architecture 1
TINA Architecture 1
TINA Network Management Model 2

3 Network Management Protocols **2**
3.1 Simple Network Management Protocol 2
SNMP Development 2
SNMP Security 2
3.2 Common Management Information Protocol 2
3.3 Signalling System #7 2
Management Layers 2
Management Functionality 2
3.4 ATM Network Management 2

4 Future network management **2**
4.1 X/Open Systems Management Reference Model 2
Anticipated Implementation Technologies 2
4.2 Web-based Network Management 2
4.3 Java Management Extensions 2
4.4 CORBA-based Telecommunication Network Management System 2

4.5 Common Information Model . . . 27
4.6 SPIN's Intelligent Network Management . . . 27
4.7 Policy-Based Networking . . . 27

5 Network Element Management 29
5.1 Configuration Management . . . 29
TCP/IP Networks . . . 30
5.2 Security Management . . . 30
Protocols and programs for network security . . . 30
Access Control Tools . . . 32
5.3 Fault Management . . . 35
Transferring information . . . 35
Troubleshooting and Fault Localization . . . 36
Testing . . . 37

6 Traffic Management 39
6.1 Communications in IP Networks . . . 39
Different types of traffic . . . 39
6.2 New service model for IP networks . . . 39
IETF Integrated Services Architecture . . . 40
Differentiated Services Architecture . . . 41
Multi-protocol Label Switching Architecture . . . 41
Traffic Engineering and Constraint-based Routing . . . 42
Difficulties in development of a new service model . . . 42
6.3 Performance Management . . . 43
Performance analysis . . . 43
Performance metrics . . . 43
Performance management control . . . 44

7 Service Management 45
7.1 Introduction . . . 45
7.2 Services in the Network . . . 45
Services . . . 45
IP Networks and Convergence in Telecommunications . . . 46
Service Providers . . . 47
Service users . . . 47
7.3 Security management . . . 47
7.4 Authentication and authorization . . . 48
7.5 Security problems of Internet . . . 50
7.6 Customer Care and Billing . . . 51
Customer Care . . . 51
Billing . . . 52
7.7 Accounting management . . . 55
Internet pricing . . . 56
7.8 Managing New Services . . . 57
7.9 Problems in Service Management . . . 58
7.10 Service Provisioning . . . 58
Service Life Cycle . . . 58
WWW Service Platforms . . . 58

Hybrid Services 6

8 Content management **6**
8.1 Demands of content management 6
8.2 Switching technologies 6
Flow differentiation 6
IP Switching 6
Tag Switching 6
8.3 Management information modeling technologies 6
Markup languages 6
Object-oriented models 6
8.4 Examples of content management 7
Multimedia content management 7
Content management and the end-user 7
The benefits of content management to the content provider 7

9 Commercial Network Management Products **7**

Bibliography **7**

Index **8**

ABSTRACT

Author Liisa Uosukainen Tuomas Lilja Lasse Mets
Stiina Ylänen Seppo Ihalainen Jouni Karvo Os
Taipale

Title IP network management

Helsinki University of Technology, Laboratory of Telecommunication
Software and Multimedia started a project called IPMAN — managemen
of massive IP networks, funded by Tekes and industry partners, in 1999.

The aim of the project is to find out the problems arising when the I
networks grow in number of nodes and volume of traffic. This report is
record of the status of the project in December 1999, after the first year o
studies.

The report contains a litterature study of the current networ
management models and protocols. The original part of the work is th
four-layer network management model used in the report.

The lowest layer of the model is the network element managemen
layer, which is about management of individual elements in the networ
The second layer, called traffic management, intends to manage th
network so that expected traffic properties are achieved. The third laye
service management, manages service applications that use the networ
The fourth and upmost layer is the content management layer, which dea
with managing the information that is provided by the service application

Keywords Internet Protocol, network management, massive networks

ABBREVIATIONS

ADSL	Asymmetric Digital Subscriber Line
CATV	Cable television
CoS	Class of Service
CIM	Common Information Model
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
CAC	Connection Admission Control
CNM	Customer Network Management
DiffServ	Differentiated Services
FCAPS	Fault, Configuration, Accounting, Performance Security Management
GoS	Grade of Service
HDSL	High bit-rate Digital Subscriber Line
HFC	Hybrid Fiber-Coax
IntServ	Integrated Services
IP	Internet Protocol
IKE	Internet Key Exchange
ISAKMP	Internet Security Association & Key Management Pro
IPSec	IP Security Architecture
JMAPI	Java Management API
JMX	Java Management Extensions
MIB	Management Information Base
MANET	Mobile Ad-hoc Networking
MPLS	Multi-Protocol Label Switching
OMG	Object Management Group
ORB	Object Request Broker
OMAP	Operations, Maintenance and Administration Part
POTS	Plain Old Telephone Service
PBN	Policy-Based Networking
PCT	Private Communication Technology
QoS	Quality of Service
RSVP	Resource ReSerVation Protocol
S-HTTP	Secure HTTP
S/MIME	Secure Multipurpose Internet Mail Extension
SSH	Secure Shell
SSL	Secure Socket Layer
SS#7	Signalling System #7
SNMP	Simple Network Management Protocol
SMI	Structure of Management Information
SMFs	Systems Management Functions
TINA	Telecommunications Information Networking Archite
TMN	Telecommunications Management Network

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

Helsinki University of Technology has started IPMAN project in 199 The target of the IPMAN project is to research and develop a networ management paradigm for massive IP-networks.

1.1 Changes in network management

Introduction of new equipment and new technologies means introductio of new information systems, which also increases the number of dat repositories and fault management systems. As networks become large and more complex, tools and applications to ease network managemen are critical. Automated network management is needed [93].

Time is a critical factor in network management (see figure 1.1 Managers strive for shorter cycles and customers demand faster respons Shorter cycles lead into lower costs and greater productivity [29]. Effectiv use of network facilities can improve a competitive position, creat new market opportunities and afford efficient communications betwee business units and customers.

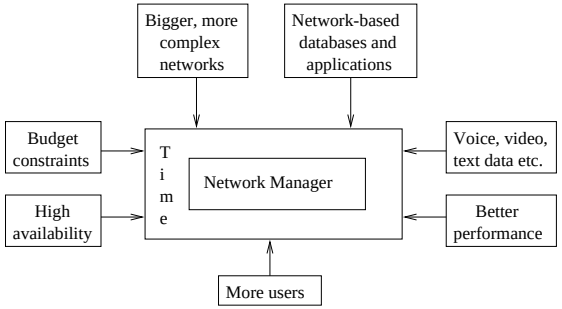

Figure 1.1: Network management, modified [29]

Network management views the computing environment as collection of co-operating systems connected by various communicatio mechanisms. Sun Microsystems expresses that the network is the compute This means that effective system management is thinking the network as single, multilayer entity, one that requires its own care [79]. An importan aspect is that management is useless to a company if it does not solv

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 [29].

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 [29].

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 simpler 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.

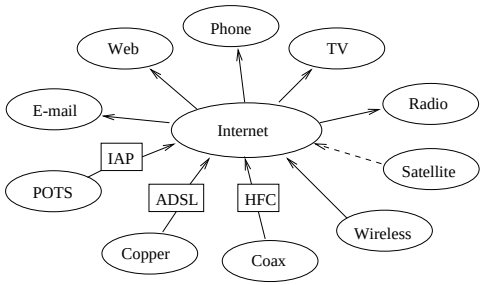

Figure 1.2: The Internet picture [28]

Most cable television (CATV) providers are interested in offerin telephone and Internet services as well as video-on-demand services. Th Hybrid Fiber-Coax (HFC) network is an emerging cable architecture fo providing residential video, voice telephony, data, and other interactiv services to end users over fiber optic and coaxial cables . The HF network can provide the bandwidth that some multimedia application require, using the spectrum from 5 MHz to 450 MHz for conventiona downstream analog information, and the spectrum from 450 MHz to 75 MHz for digital broadcast services such as voice and video telephon video-on-demand, and interactive television.

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

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

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

Satellite transmission also facilitates mobility. Because the transmissio area covered by a satellite is very large, it is well suited for video and audi broadcasting [122, pages 16–20].

1.3 Structure of this document

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

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

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

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

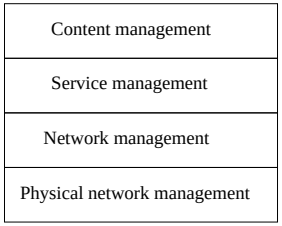

Figure 1.3: Reference model by Professor Olli Martikainen

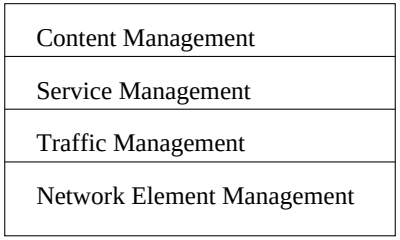

Figure 1.4: Modified reference model

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

2.1 OSI Management

The Open Systems Interconnection (OSI) Management is documented i ITU-T and CCITT X.700-series Recommendations [40]. It is based on fou components: *Management Model, Information Model, Communicatio Protocol for Transferring Management Information*, and *Systems Manage ment Functions.* OSI Management functionality is divided into five *Ma agement Functional Areas* according to the *OSI FCAPS model* [34].

The transfer of management information in OSI networks is provide by Common Management Information Protocol (CMIP, see page 22) [22

Management Model

The Management Model describes a manager-agent concept (figure 2.1 The manager system manages Managed Objects in distributed manne by issuing remote management requests to agent processes. The agen manage the Managed Objects and are responsible for implementing th functionality needed to execute the requests. They may also return value and send notifications (events or traps generated by Managed Objects) bac to the manager [115, 22, 111, 123].

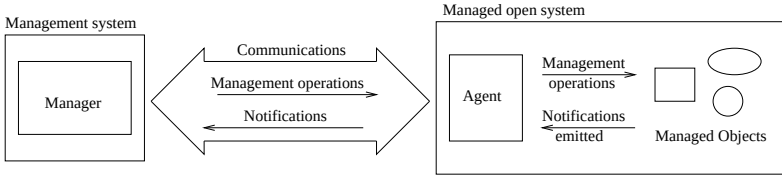

Figure 2.1: The manager-agent concept [23]

A network to be managed can be divided into management domains. domain is an administrative partition of a managed network or Interne Domains may be useful for reasons of scale, security, or administrativ autonomy. Domains allow the construction of both strict hierarchical an

Information Model

The information model deals with Managed Objects that are abstractions of the real resources on the network [34]. 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 [123].

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 [123].

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 [111].

Management Functional Areas — OSI FCAPS model

OSI Management functionality is divided into five management functional areas [22]:

- **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 and exercises control over open systems. It also 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

2.2 Telecommunications Management Network

A Telecommunications Management Network (TMN) provide management functions for telecommunications network and service It also offers communications between itself and the network and it services. It is an architecture that provides interconnection betwee various types of Operations Systems (OSs) and/or telecommunication equipment for the exchange of management information [39].

The top-level standards and recommendations for OSI system management form the basis for TMN standards [40]. The TMN standard are defined in ITU-T M.3000-series documents [113, page 48].

Figure 2.2 shows a general relationship between a TMN and th telecommunications network it manages. TMN is conceptually a separat network that interfaces a telecommunications network at several differen points to send/receive information to/from it and to control it's operation A TMN may use parts of the telecommunications network to provide it communications [39].

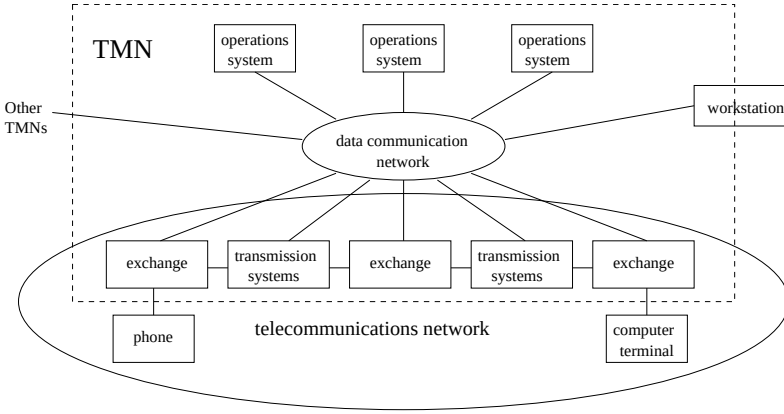

Figure 2.2: General relationship of a TMN to a telecommunication network [113, page 25]

TMN Management Services

The scope of network management is broader in telecommunications tha in data communications. Thus a TMN must provide more than just th functionality defined in the OSI FCAPS model. TMN Managemen Services (TMN-MSs) include

- Customer administration,
- Network provisioning management,
- Workforce management,
- Tariff, charging and accounting 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 [113, page 48–53].

TMN Management Layers

The needed management functionality is achieved by using five layers of management, described in [113, 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

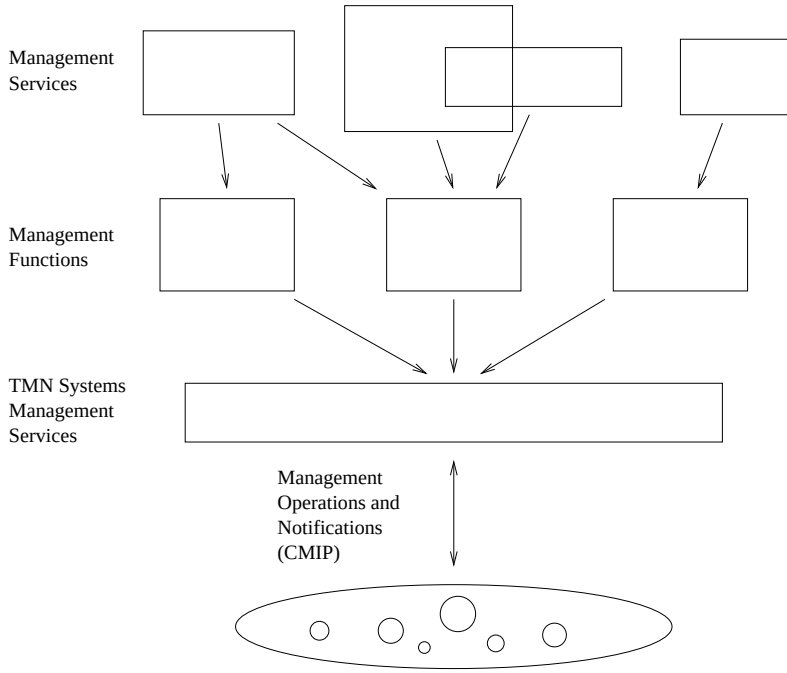

Figure 2.3: TMN Management Services, Management Functions an
Systems Management Services [113, page 50].

TMN Architecture

TMN architecture is divided into three aspects, which can be considere
separately when designing a TMN: *functional, information* and *phy
ical architecture*. **Functional architecture** describes the appropriat
division and distribution of functionality within the TMN to allow th
creation of building blocks, from which a TMN of any complexity can b
implemented [39].

Information architecture describes the nature of the information tha
needs to be exchanged between the building blocks, and also describes th
understandings that each building block must have about the informatio
held in other building blocks [39].

Physical architecture describes the implementation of function block
on physical systems and the interfaces between them [113, page 31].

2.3 Customer Network Management

The purpose of Customer Network Management (CNM) is to provid
external users of a telecommunications network with a limited control an
view of the managed network. It enables customers to manage a portio
of the whole network and subscribe it's services. Figure 2.5 illustrates th
CNM functional architecture [113, pages 38–42].

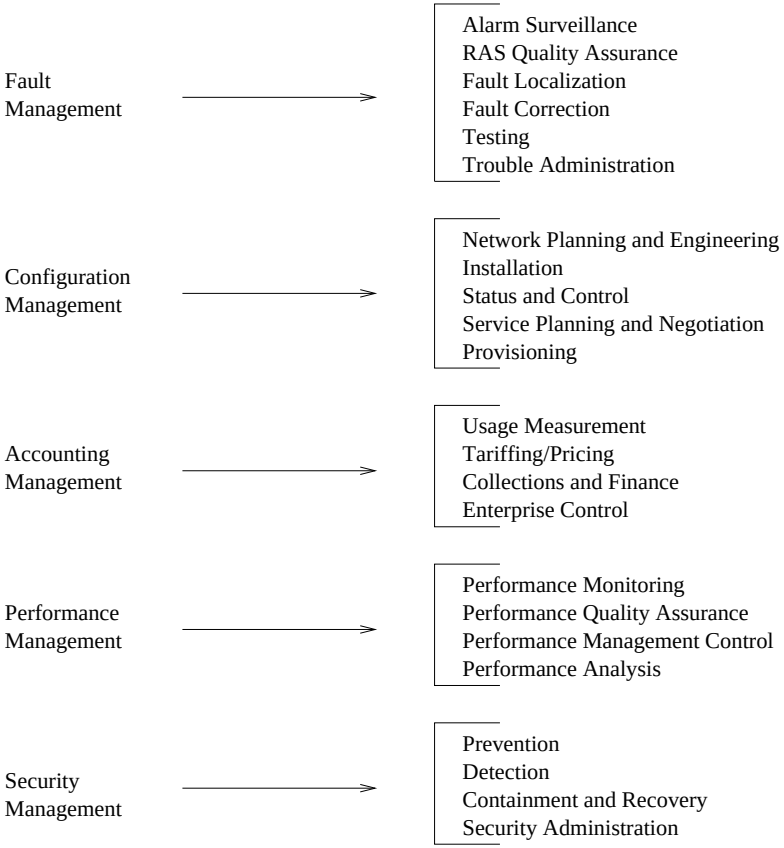

Figure 2.4: Mapping of OSI MFAs and TMN Management Function Set Groups [113, page 53].

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 [113, pages 38–44].

2.4 SMART TMN

Smart TMN [110] 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

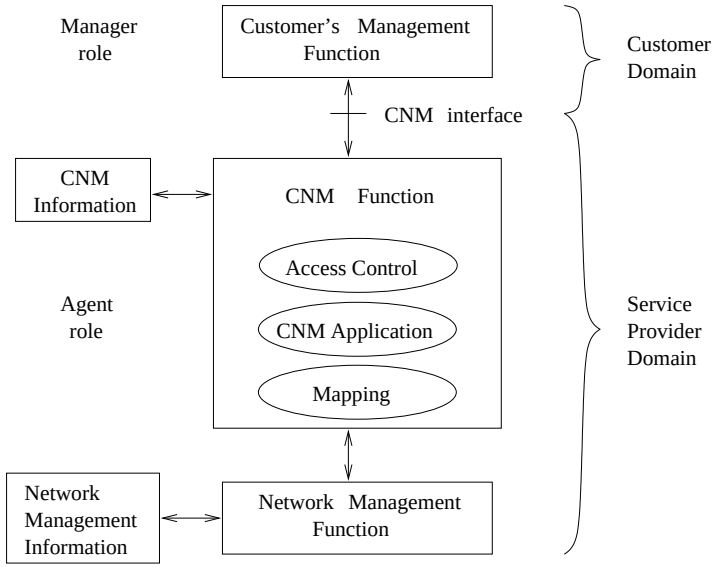

Figure 2.5: CNM functional architecture [113, page 39].

- **Central Information Facility** for information store for technica specifications, object models etc., and
- **Catalyst Projects**, which are projects to validate technology concept

2.5 Telecommunications Information Networking Architecture

Telecommunications Information Networking Architecture (TINA) designed to meet the needs of telecommunications services rangin from traditional voice-based services to interactive multimedia, multi-part services, information services, as well as management services. All thes services are considered to be software-based applications that operate on distributed computing platform [71, page 137]. TINA addresses a wid range of issues and provides a complex set of concepts and principle In this respect, it is much more a framework, a compilation of concep and principles for developing future distributed telecommunications an management services, than a specific architecture [71, page 148].

TINA Architecture

TINA architecture is based on four principles: Object-oriented analysis an design, distribution, decoupling of software components and separatio of concern. The purpose of these principles is to ensure interoperability portability and re-usability of software components, independence fro technologies, and to help to create and manage complex systems [112 The two major separations of concern are the separation betwee applications and the environment, and the separation of application

part [112].

Due to the complexity of TINA, it's architecture is divided into four sectors: *computing architecture, service architecture, network architecture* and *management architecture* [118, page 24].

The **computing architecture** defines a set of concepts and principles for designing and building distributed software [118]. It is based on the Basic Reference Model for Open Distributed Processing (RM-ODP, ITU Recommendation X.900) [71, page 148].

The **service architecture** defines a set of concepts and principles for the design, specification, implementation and management of telecommunication services [118, 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 [118, 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 [71, page 163]. The TINA management architecture is still under study [118, pages 27–28].

TINA Network Management Model

TINA network management model extends the OSI FCAPS model (see page 14) [71, 25]. Configuration management is divided into *connection management* and *resource configuration management*.

Connection management is considered a fundamental activity in telecommunications network [118]. TINA represents a new approach to the traditional way of connection control [71, 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

This chapter describes different existing standard protocols that are used i network management. SNMP (section 3.1) is widely used in IP network and is also basis for some other protocols. CMIP, described in section 3. is an OSI based protocol. Network management protocols used in SS# are described in section 3.3, and network management for the ATM i section 3.4.

3.1 Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is the most widely use management protocol in TCP/IP networks. This is due to it's simplicity expandability, easy implementation and the fact that it poses only littl stress on the managed network and the managed nodes [115, 21].

SNMP is based on a agent-manager concept, similar to the on illustrated in figure 2.1: A manager sends requests to agents in networ elements. The agents control Managed Objects (see page 14) accordingly send responses and issue trap messages to the manager. The objects t be managed are defined in a MIB (see page 14) . The requests an responses are exchanged using the User Datagram Protocol (UDP), whic is a connectionless protocol. Trap-directed polling is used to decrease th management traffic on the network [63].

The management functionality is centralized in a Networ Management Station (NMS), which acts the manager role. Agent are kept simple, and thus SNMP is particularly conservative in the memor and computational requirements placed on devices connected to th network [113].

SNMP Development

The first version of SNMP, SNMPv1, became both an IETF (th Internet Engineering Task Force) and a de facto standard. This wa due to it's widespread market acceptance. However, due to the lack o adequate security features, a new version of SNMP had to be developed Various proposals on SNMPv2 were made, but none were adopted a a new standard. SNMPv2 failed because it had lost the simplicity o SNMPv1 [115, 26].

Third version of SNMP, SNMPv3, is now in it's final stages o standardization. It builds on the first and the second versions o SNMP, and is intended to offer new capabilities for open, interoperable and secure network management. It includes methods for securit (authentication, encryption, privacy, authorization, and access control and a new administrative framework (naming of entities, user name and key management, notification destinations, and proxy relationship

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 [95, 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 [17] and VACM in [125].

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 [115].

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 [63].

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 [115].

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 [39]) 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 [56].

Management Layers

The definition of TMN is concerned with five layers in management (see page 16), 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

view-based access control model (VACM) 22
SS#7 22
SSH 30
SSL 31
Standardized Generalized Markup Language . . . . . *see* SGML
stelnet 30
Structure of Management Information *see* SMI
Systems Management Functions . . . . . *see* SMFs

TCP 50
Telecommunications Information Networking Architecture *see* TINA
Telecommunications Management Network . . . . . *see* TMN
TELNET 50
TINA 19, 63
TMN 15
traceroute 36

UDP 50
Uniform Resource Locator . . . . . *see* URL
URL 59

Video on Demand . . . . . *see* VoD
VoD **45**, 46

web-based architecture 61
web-based network management 26
World Wide Web . . . . . *see* WWW
WWW 45, 51, 58, 59

X.800 47

IntServ 40
IP 46, 49, 50, 57, 58, 60
IP Security Architecture . . . . . *see* IPSec
IP telephony 45
IPSec 31
  IP authentication header (AH) . . . 31
  IP encapsulating security payload (ESP) 31
ISAKMP 31
ISDN 46
ISO 46
ISP 49
ITU-T 46, 47

Java Management API . . . . . *see* JMAPI
Java Management Extensions . . . *see* JMX
jitter **39**, 44
JMAPI 26
JMX 26

logs 36

Management Information Base . . *see* MIB
MANET 11
MIB **14**, 21, 22, 35
Mobile Ad-hoc Networking . *see* MANET
MPLS 41
Multi-Protocol Label Switching . . . . . *see* MPLS

NFS 50
non-repudiation 48

Object Management Group . . . *see* OMG
Object Request Broker . . . . . *see* ORB
OMAP 22
OMG 26
open systems interconnection (OSI) management 13
Operations, Maintenance and Administration Part . *see* OMAP
ORB 25

packet inter net groper . . . . . *see* ping
PBN 28, 60
PCT 31
performance management 14, 16, **43**
  performance analysis 43
  performance management control 44
  performance metrics 43
Plain Old Telephone Service . . *see* POTS
policy 27
Policy-Based Networking . . . . . *see* PBN
policy-based networks . . . . . *see* PBN
polling 35
POTS 10
Private Communication Technology . . *see* PCT
PSTN 46, 62
Public Switched Telecommunications Network . . . . . *see* PSTN

QoS 28, 39, **39**, 42, 52, 56, 60
Quality of Service . . . . . *see* QoS

RADIUS 57
Real-time Traffic Flow Measurement . *see* RTFM
Remote Authentication Dial-In User Service . . . . . *see* RADIUS
Resource ReSerVation Protocol *see* RSVP
routers 32
routing tables 37
RSVP 40
RTFM 57

S-HTTP 30
S/MIME 31
Secure HTTP . . . . . *see* S-HTTP
Secure Multipurpose Internet Mail Extension . . . . . *see* S/MIME
Secure Shell . . . . . *see* SSH
Secure Socket Layer . . . . . *see* SSL
secure telnet . . . . . *see* stelnet
security management 14, 16, **30**
service providers 45, 47, 52, 53, 55, 56, 58, 60, 61
service-level agreements . . . . . *see* SLA
SGML 59
Signalling System #7 . . . . . *see* SS#7
Simple Network Management Protocol *see* SNMP
SLA 45, **47**, 52, 58
SMFs 14
SMI 14
SNMP **21**, 37, 56, 57, 61
  agent-manager concept 21
  network management station (NMS) 21

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 14) are provided [56].

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) [75]. 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 [96].

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 [8].

access control 47
accounting management 14, 16, 20
ADSL 11
alarms 35
Asymmetric Digital Subscriber Line . . *see* ADSL
authentication 48, 49
authorization 48

Cable television . . . . . *see* CATV, 46
CAC 39, 40
CATV 10, 46
CCB 51
CIM 27
Class of Service . . . . . *see* CoS
CMIP 22, 61
CNM 17
Common Information Model . . . *see* CIM
Common Management Information Protocol . *see* CMIP, *see* CMIP
Common Object Request Broker Architecture . . . . . *see* CORBA
confidentiality 48
configuration management . 14, 16, 20, **29**
Connection Admission Control . *see* CAC
constraint-based routing 42
CORBA 25, **27**
CoS **41**, 42
customer care and billing . . . . . *see* CCB
Customer Network Management . . . . . *see* CNM

delay 39
Differentiated Services . . . . . *see* DiffServ
DiffServ 41
  DS field 41
DNS 60
Domain Name System . . . . . *see* DNS
dynamic routing protocols
  IS-IS 42
  OSPF 42
  RIP 42

end-to-end services 45
expert systems 35, **43**

Fault, Configuration, Accounting Performance and Securit Management . . . . . *see* FCAP
FCAPS 1
firewalls
  dual-homed host architecture 3
  packet filtering 3
  proxy services 3
  screened host architecture 3
  screened subnet architecture 3
flows
  elastic flows 3
  stream flows 3
FTP 45, 5

GoS 3
Grade of Service . . . . . *see* Go

HDSL 1
HFC 1
High bit-rate Digital Subscriber Line . *se* HDSL
HTML 59, 6
HTTP 5
hubs 3
Hybrid Fiber-Coax . . . . . *see* HF
hybrid services 62–6
Hypertext Markup Language . . . *see* HM
Hypertext Transfer Protocol . . . *see* HTT

IKE 3
IN 46, 6
Integrated Services . . . . . *see* IntSer
Integrated Services Digital Network . . *se* ISDN
integrity 4
Intelligent Network . . . . . *see* I
International Telecommunicatio Union — Telecommunicatio standards . . . . . *see* ITU-
Internet Key Exchange . . . . . *see* IK
Internet Protocol . . . . . *see* I
Internet Security Association & Ke Management Protocol . . . . . *se* ISAKMP

[124] WENRICH, J. Content management on the internet. Nov 15, 1999, http://joules.swvgs.k12.va.us/wenrich/prelim/paper.html.

[125] WIJNEN, B., PRESUHN, R., AND MCCLOGHRIE, K. View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). *RFC 2275* (Jan. 1998), 36.

[126] WILDE, C. Personal business. *Informationweek* (Aug. 1999). Nov 12, 1999, http://proquest.umi.com/pqdweb?ReqType=301&UserId=IPAuto&Passwd=IPAuto&JSEnabled=1&TS=941

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

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

[129] YU, H. H., AND GELMAN, A. Digital multimedia content management for networked information access: Issues and discussion. In *Advance issues of E-Commerce and Web-Based Information Systems, WECWIS* (Apr. 1999), IEEE, pp. 75–80.

[130] ÄYVÄRI, H. Where is the Internet evolving in the near future? In *Proceedings of the HUT Internetworking Seminar May'97* (1997), Department of Computer Science, Helsinki University of Technology. November 3, 1999, http://www.tcm.hut.fi/Opinnot/Tik110.551/1997/internet.htm.

[131] 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.

4 FUTURE NETWORK MANAGEMENT

New technologies, management models, and visions of future networ management, that are currently under development, are described in th chapter. Section 4.1 presents Open Group's X/Open Systems Managemen Reference Model. Web-based network management is discussed i section 4.2, and Java Management API in section 4.3. Section 4. presents CORBA-based management, and section 4.6 SPIN's vision o network management. Finally, section 4.7 discusses Policy-based networ management.

4.1 X/Open Systems Management Reference Model

Open Group, a vendor-neutral international consortium for buyers an suppliers, has presented an *X/Open Systems Management Reference Mod el*. It's goals are [111]:

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

The reference model describes concepts necessary to build comprehensive distributed systems management environment. It identifie the mapping between the abstract concepts and some technologies tha provide suitable implementation bases for the realization of the mode The model is intended to enable a network of heterogeneous systems t be managed as a single system [111].

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

The Reference Model consists of three basic components:

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

Anticipated Implementation Technologies

It is anticipated that the primary vehicle for implementation of th Reference Model will be the Object Management Group's Object Reque

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 [111].

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 [111].

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 web browser, a management agent with a web (HTML) interface must be used. The management agent may configure the element using web forms and give reports as web pages.

Advanced network wide management capabilities seem to offer a web 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 Extensions

Java Management API (JMAPI) [105] was intended to provide a standard interface between different computers and network devices. The system can be used by Java programmers, and was created in alliance with Sun Microsystems, Bullsoft, Computer Associates, Exide Electronics, Jyra, Lumos Technologies, TIBCO, and Tivoli. Specification version 2.0 was intended for publication in March 1999.

Instead of version 2.0, the product was named Java Management Extensions [106], and released in August, 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

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

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

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

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

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

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

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

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

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

[119] VOYATZIS, G., AND PITAS, I. Problems and challenges i multimedia networking and content protection. In *Workshop o Trends and Important Challenges in Signal Processing, TICS* (June 1998).

[120] W3. HTML 4.0 specification, W3C recommendation, Apr. 199 http://www.w3.org/TR/REC-html40/intro/intro.html#h-2.2.

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

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

[123] WARRIER, U., AND BESAW, L. The common managemen information services and protocol over TCP/IP (CMOT). *RFC 109*

[95] 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.

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

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

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

[99] 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.

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

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

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

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

[104] 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.

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

[106] SUN MICROSYSTEMS. Java^{TM} Management Extensions, draft 2.0, 1999. Aug, 1999, http://www.java.sun.com/aboutJava/communityprocess/first/jsr003/index.html.

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

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

[109] TELEMANAGEMENT FORUM. *SMART TMN^{TM} Technology In-*

One of the objectives of this architecture is to ensure a complet compatibility with proprietary, ITU-T/ISO, SNMP and CORBA -base network elements [87].

CORBA (Common Object Request Broker Architecture) is a architecture that supports the distribution of management functionality an managed objects [111].

Inter-networking Between CORBA and TMN Systems

In the context of TMN, CORBA is seen to offer potential in two significan areas: in the description and implementation of management interface supported by network devices, and in the description and implementatio of interfaces within and between management operations systems [87].

4.5 Common Information Model

Common Information Model (CIM) is a common data mode developed by Distributed Management Task Force, Inc. It implementation-neutral and can be used to describe managemen information in a network/enterprise environment. The model intended to enable interchange of management information betwee management systems and applications, thus providing for distribute network management [36, 35].

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 a Canada's National Research Council [1]. The SPIN Intelligent Networ Management project studies and develops new agent-based technologie for controlling, planning and problem definition of heterogeneou networks. The application development of SPIN networks uses integratio of the off-the-self NM components, and testing and usage of popular tool such as HP Openview.

4.7 Policy-Based Networking

Policy is a combination of rules and services where rules define the criteri of resource access and usage. Policies can contain other policies, they allo to build complex policies from a set of simpler policies, so they are easie to manage. They also enable to reuse previously built policy blocks [113].

Policy groups and rules can be classified by their purpose [91]:

- Service Policies
- Usage Policies
- Security Policies

- Motivational Policies
- 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 [91].

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 [95].

[83] NEWMAN, P., EDWARDS, W., HINDEN, R., HOFFMAN, E., L
AW, F. C., LYON, T., AND MINSHALL, G. Ipsilon's general switc
management protocol specification version 2.0. *RFC 2297* (Ma
1998), 109.

[84] NEWMAN, P., EDWARDS, W. L., HINDEN, R., HOFFMAN, E
LIAW, F. C., LYON, T., AND MINSHALL, G. Ipsilon flo
management protocol specification for IPv4, version 1.0. *RFC 195*
(May 1996), 19.

[85] NEWMAN, P., MINSHALL, G., AND LYON, T. Ip switching: Atr
under ip. *IEEE/ACM Transactions on Networking* (1997).

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

[87] OBJECT MANAGEMENT GROUP. *CORBA-based Telecommunica
tion Management System*. OMG White Paper, May 1996.

[88] OPSEC (OPEN PLATFORM FOR SECURITY). I-gear for firewall-
3.02. Nov 12, 1999
http://www.checkpoint.co.ip/opsec/partners/framework/urlabs.html

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

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

[91] PULKKI, A. The IP security architecture. In *Proceedings of Helsi
ki University of Technology Seminar on Network Security 199*
(1995), Department of Computer Science, Telecommunication
Software and Multimedia Laboratory, Helsinki University o
Technology. July 7, 1999,
http://www.tcm.hut.fi/Opinnot/Tik-110.501/1995/ip-sec-arch.html.

[92] REKHTER, Y., DAVIE, B., KATZ, D., ROSEN, E., AND SWALLOW
G. Cisco systems' tag switching architecture overview. *RFC 210*
(Feb. 1997), 13.

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

[94] SAN DIEGO SUPERCOMPUTER CENTER. White paper on networ
performance metrics, 1999. July 5, 1999,

[70] 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.

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

[72] 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.

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

[74] 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.

[75] 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.

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

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

[78] 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 Decentralized Systems, ISADS 97* (1997), IEEE, pp. 129–136.

[79] 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.

[80] NETSCAPE NETCENTER. Intranet library. Nov 15, 1999, http://www.intraware.com/ms/itwr/askjms/contentman.html.

[81] 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.

[82] NEUMAN, B. C., AND MEDVINSKY, G. Netcheque, netcash, and the characteristics of internet payment services. *The Journal of Electronic Publishing 2* (May 1996).

5 NETWORK ELEMENT MANAGEMENT

This chapter discusses network element management. Section 5. describes network configuration management. Section 5.2 describe security management, including protocols and programs developed t provide security over the Internet, and network elements used to secur risky areas of networks. Section 5.3 studies fault management, includin troubleshooting, fault localization, and testing methods.

5.1 Configuration Management

Configuration management means initializing and shutting down parts o a network (for example routers, hubs, and repeaters) and reporting th changes. It is also concerned with maintaining, adding and updatin the relationships among elements and the status of elements durin network operation. Network traffic patterns and identified bottlenecks tha reduce performance must be understood. Nowadays modern elements an subsystems can be configured to support many different applications. Th same device can be configured to act either as a router or as an end syster node or both. Depending on the configuration, the appropriate softwar and a set of attributes and values are chosen for the device [100, page 481 Reconfiguration may be necessary in case of fault isolation or when th 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 thes actions could be automated. It should also be possible to make on-lin changes without affecting the entire element or network [93]. Large-scal network management systems must be constructed to support divers network elements. They must also be extensible and flexible enough t support new elements and the rapid deployment of new highly customize services.

Activities in network management can be divided into thre groups [46]:

- activities that do not affect the functioning of an element,
- activities that affect the functioning of an element (for exampl switching off an element in a subnetwork), and
- activities that make an element to do a desired function (for exampl restarting an element).

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

Configuration management tools have reporting components. Whe network configuration changes, users must be informed about new networ elements and resources. Configuration management is well organize

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 [16]. 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 [103].

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 hosts 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 IP addresses to particular hosts can be chosen over static allocation using the Dynamic Host Configuration Protocol (DHCP) [38].

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 [113, 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 [6].

[1] Mean Time Between Failure

[56] ITU-T RECOMMENDATION Q.750. *Overview of Signalling Sy tem No.7 Management*, Mar. 1993.

[57] JOHNSON, R. B. Internet multimedia databases. *IEE, Savoy Plac London* (1998).

[58] JUDD, S., AND (EDITORS), J. S. Directory-enabled network information model and base schema (version 3.0c5, 199 September 6, 1999, http://murchiso.com/den/specifications/directory-enabled-networks

[59] KARONEN, J. Sähköinen kaupankäyntikin on asiakassuhteest kiinni. *WOW!-verkkolehti* (July 1999). 12.7.199 http://www.wow.fi/.

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

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

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

[63] KOTH, A., EL-SHERBINI, A., AND KAMEL, T. A ne interoperable management model for IP and OSI architectures. I *AFRICON, IEEE AFRICON 4th* (Sept. 1996), vol. 2, pp. 944–94

[64] LARSEN, A. K. Network analysis, CIM's missing pieces, 199 CMP's TechWeb, September 16, 1999, http://data.com/tutorials/cim.html.

[65] LDAP. Fulfilling the promise for directory-enabled networks, 199 http://www.cnilive.com/impact/specials/ldap/.

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

[67] LIDYARD, D. New technologies and strategi trends: An introduction to network accounting, 199 http://www.summitonline.com/netmanage/papers/telco1.html.

[68] LOESER, H., AND RITTER, N. iwebdb - web site administratio based on object-relational database technology. In *Database Eng neering and Applications, IDEAS'99* (Aug. 1999), IEEE, pp. 92–9

[69] LOGEAN, X., DIETRICH, F., AND HUBAUX, J.-P. On applyin formal techniques to the development of hybrid services: Challenge and directions. *IEEE Communications Magazine* (July 1999

[41] 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.

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

[43] GLYPHICA. Content management. Nov 15, 1999 http://www.glyphica.com/ContMan.html.

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

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

[46] 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.

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

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

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

[50] IBM RESEARCH. Content management. Nov 15, 1999, http://domino.watson.ibm.com/HDTV/nabproject.nsf/Named/content.htm.

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

[52] INTERNATIONAL LEARNINGS SYSTEMS, INC. Content management. Nov 15, 1999, http://www.ilsinc.com/ExternalWeb/registration/content_mgmt.htm.

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

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

[55] INTERNET ENGINEERING TASK FORCE. Multiprotocol Label Switching working group, 1999. Aug 17, 1999,

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 th Internet

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

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

Secure Socket Layer (SSL) is an encryption method developed b Netscape to provide security over the Internet. SSL is a protocol layer that located between the network layer and applications, so that, in theory, it ca be used with any application. However, it is vulnerable to poor applicatio design. It provides data encryption, server authentication, messag integrity, and optional client authentication for a TCP/IP connection [6].

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

IP Security Architecture (IPSec) provides a standard securit mechanism and services to the currently used IP version 4 (IPv4) and to th new IP version 6 (IPv6). IPSec is less dependent of individual application than SSL. It provides IP-level encryption by specifying two standar headers: IP Authentication Header (AH) and IP Encapsulating Securit Payload (ESP) . IP Authentication Header provides strong integrity an authentication. It computes a cryptographic authentication function ove the IP datagram and uses a secret authentication key in the computation IP Encapsulating Security Payload provides integrity and confidentiality fo IP datagrams. It encrypts the data to be protected and places it in th data portion of the IP Encapsulating Security Payload. However, thes mechanisms do not provide security against traffic analysis. Any specifi protocol for key management is not provided by the architecture, onl requirements for such systems to be used in conjunction are described [91

IPSec require a key management protocol. IETF has standardize Internet Security Association & Key Management Protocol (ISAKMP and Internet Key Exchange (IKE) for this purpose. ISAKMP define the procedures for authenticating a communicating peer, creation an management of Security Associations, key generation techniques an threat mitigation (e.g. denial of service and replay attacks). These ar necessary to establish and maintain secure communications in an Interne environment. Security Association (SA) is a security-protocol-specifistic se of parameters that defines the services and mechanisms necessary to protec

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 [6]. IPSec is defined in [61], ISAKMP in [73] and IKE in [44].

Access Control Tools

Hubs, routers and firewalls can be used to limit access to networks or to parts of the networks. These security level operations can be restricted to a date or to a time period.

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 [48]. 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 alarms 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 [51].

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.

[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

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

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

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

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

[32] CROLL, M., LEE, A., AND PARNALL, S. Content management the users requirements. In *International Broadcasting Convention Conference Publications* (Amsterdam, Sept. 1997), IEEE.

[33] CURTIS, K., AND DRAPER, O. Multimedia content managemen — provision of validation and personalisation services. In *Multime dia Computing and Systems* (June 1999), IEEE, pp. 302–306.

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

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

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

[37] DISTRIBUTED MANAGEMENT TASK FORCE, INC. (DMTF Xml as a representation for management information - a white pape 1998. September 10, 1999, http://www.dmtf.org/spec/xmlw.html.

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

[39] ETSI ETR 037. *Network Aspects (NA); Telecommunications Man agement Network (TMN) Objectives, principles, concepts and re erence configurations*, Feb. 1992. DTR/NA-043202.

[40] ETSI ETR 230. *Network Aspects (NA); Telecommunications Man agement Network (TMN); TMN standardisation overview*, Nov

[15] 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.

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

[17] BLUMENTHAL, U., AND WIJNEN, B. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). *RFC 2274* (Jan. 1998), 76.

[18] BOLL, S., KLAS, W., AND WESTERMAN, U. Multimedia document models — sealed fate or setting out for new shores? In *Multimedia Computing and Systems* (June 1999), IEEE, pp. 604–610 vol. 1.

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

[20] 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.

[21] 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.

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

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

[24] 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.

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

[26] 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.

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

These programs take users' requests for Internet services (such as FTP an Telnet) and forward them, as appropriate according to the site's securit policy, to the actual services. The proxies provide replacement connection and act as gateways to the services. For this reason, proxies are sometime known as application-level gateways [24].

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 ho computer, a computer that has at least two network interfaces. Suc a host could act as a router between the networks these interface are attached to; it is capable of routing IP packets from one networ to another. Systems inside the firewall can communicate with th dual-homed host, and systems outside the firewall (on the Interne can communicate with the dual-homed host, but these systems ca not communicate directly with each other. IP traffic between ther is completely blocked.

  The diagram below shows the network architecture for a dual-home host firewall. The dual homed host sits between, and is connecte to, the Internet and the internal network [24].

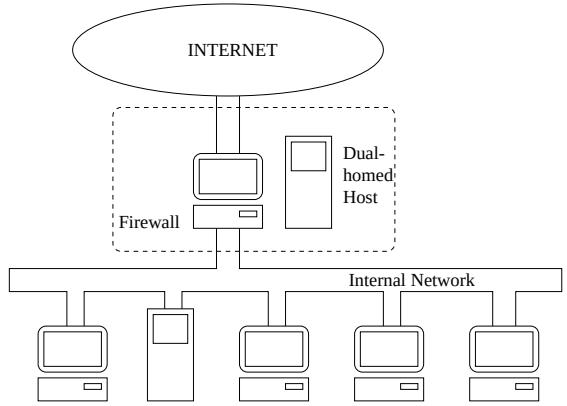

Figure 5.1: Dual-homed host architecture

- Screened host architecture

  Whereas a dual-homed host architecture provides services from host that is attached to multiple networks (but has routing turne off), a screened host architecture provides services from a host that attached only to the internal network, using a separate router. In th architecture, the primary security is provided by packet filtering. Fo example, packet filtering is what prevents people from going aroun proxy servers to make direct connections. The diagram below show the network architecture for the screened host architecture [24].

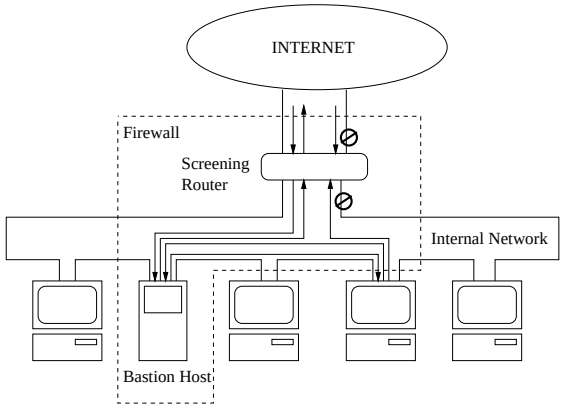

Figure 5.2: Screened host architecture

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 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 [24].

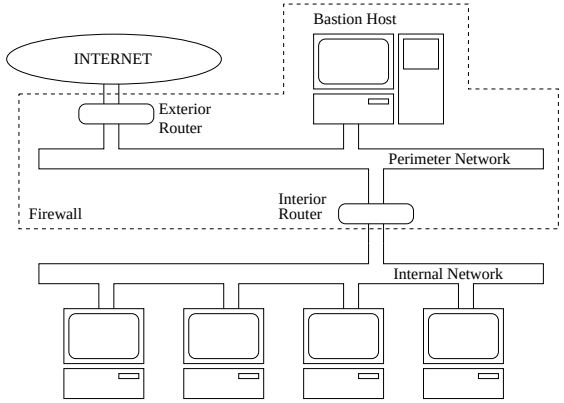

Figure 5.3: Screened subnet architecture

[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/p

[3] 3COM. Applications digital content management. Nov 15, 1999 http://www.3com.com/solutions/applications/dcm/more.html.

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

[5] ARAO, S., HONDA, M., KIND, A., AND NICKLISCH, Component-based policy deployment for service level differentiatio in converging communication networks. *IEEE* (1999).

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

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

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

[9] BACON, A. Expert systems use in fault management systems, 199 April 16, 1999, http://www.cbu.edu/~pong/624arb1.htm.

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

[11] BANTA CORPORATION. Digital content management. Nov 15 1999 http://www.banta.com/tech/brief/9705/dcm.html.

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

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

[14] BLAKE, S., BLACK, D., CARLSON, M., DAVIES, E., WANG, Z AND WEISS, W. An architecture for differentiated service. *RFC*

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

Physical network problems account more than half of all network problem
Locating the origins of such problems as a fiber cut, an incorrect earthing
broken or incorrectly connected adapters, costs network providers time an
money. Network management systems have also traditionally focused o
the logical connection between the end user and the network destinatio
since many network problems have been a result of errors created b
software applications [93]. Finding and repairing failures of softwar
applications is usually difficult, for example in such a case that th
workstation sends but does not receive packets, too many collisions occu
or frames are too short or too long.

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

Expert systems provide an efficient and cost effective way of automatin
network fault management. By automating fault management, problem
and possible diagnosis can be done faster and more efficiently. Howeve
real-time performance represents a problem for expert systems [41
Bounds on response times are difficult to establish. There are also risk
pushing the limits of automation through the introduction of new or onl
partially proven technologies.

Transferring information

There are two mechanisms of transferring network managemen
information from a managed entity to a manager: **polling** and **sendin
alarms** (messages are initiated by managed network elements). Advantage
and disadvantages exist within both methods. Most network managemen
systems use an optimal combination of alarms and polling in orde
to maintain advantages of each and eliminate disadvantages of pur
polling [102].

Most systems poll the managed objects, search for error condition
and illustrate the problem in graphical format or as a textual messag
Disadvantages of polling are the response time of problem detection an
the increased volume of network management traffic. Having to poll man
management information base (MIB) variables per element on a larg
number of elements is itself a problem. The ability to monitor such a syste
is limited. Polling many objects on many elements increases the amoun
of network management traffic flowing across the network. It is possibl
to minimize this through the use of hierarchies (polling an element for
general status of all the elements it polls). Anyway, the response time wi
be a problem [102].

If a system fails shortly after being polled, there may be a significan
delay before it is polled again. During this time, the manager must assum
that a failing system is acceptable. While improving the mean time t
detect failures, it might not greatly improve the time to correct the failure

There are problems attached also to the second method, sending alarms: There is a possibility to lose of critical information and to over-inform the manager. An ideal management system would generate alarms to notify its management station of error conditions. However, alarms cannot usually be delivered when the managed entity fails or the network experiences problems. It is important to remember that failing elements 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 alarms that were not delivered by the network [102].

Alarms in a failing system can be generated so rapidly that they impact functioning resources. An "open loop" system in which the flow of alarms to a manager is fully asynchronous can result in an excess of alarms being delivered. There may be a situation where all available network bandwidth into the manager is saturated with incoming alarms, thus preventing the manager from disabling the mechanism generating the alarms. Methods are needed to limit the volume of alarm 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].

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 [48, 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. Since loopback request and loopback response may use different routes, the violated route cannot be determined with echo-response. 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 [16, 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 [10, 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

HP OpenView
Hewlett-Packard
In addition to traditional network management features, HP OpenVie includes systems management and service management features. Use 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. Differe versions are provided for SOLARIS, Windows and Web/Java-base 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 usin JMAPI technology (for more information on JMAPI, see section 4.3 JDMK helps to develop Web-based management services using Java agen or JavaBeans for Management -technology.
http://sun.com/software

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

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

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

INTEL LANDesk
Intel

The Library Server is the single centralized store of metadata for all content in the studio. Although it is a single logical entity, it can be instantiated as a cluster of machines to achieve high availability and support large amounts of content. Alternatively, in smaller studios, the library server, media servers and even the SRM (Scalable Reliable Multicast) can be implemented on a single machine. The metadata in the library server includes time-invariant and time-variant metadata, among which are shot length and visual motion. Content in the studio will be identified by a single key which will be unique within the studio and, in some cases, industry-wide (such as an extended-ISCI or a SMPTE 298M Universal Media Identifier) [50].

The Annotation Station permits manual annotation and performs automatic annotation for incoming content. As video is ingested, it will perform an automatic annotation that includes shot-boundary detection, face detection, and keyframes selection. The logger may also manually enter bibliographic data, a description of the program, and other metadata. This may include copyright and access information for each clip [50].

cause from symptoms [81]. Operators must also determine what troubles causes and to whom.

At first it is useful to find the parts of the network, where the fault can no be, by eliminating processes. These parts can be neglected. If the problem is very serious and difficult, the network can be divided into smaller part to be inspected one by one. Connectivity tests are also used to find th violated devices. At the same time it can be detected whether the fault local or widespread. It can be found out by testing data integrity if some o the packets are lost in transmission. Delays are also to be tested, becaus some faults result from excessive delays [10, page 198].

Testing

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

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

Another method of testing is to **control routing tables**. Routing shoul change only when the topology of the network changes. If there are change at other times, there is probably something wrong with the network [10 pages 183–189].

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

Companies also feel the need to personalize their Web site
When asked what are the biggest obstacles they face with Web sit
personalization, according to a survey [126] almost a half of th
companies felt that understanding what content to deliver was th
biggest obstacle. Between 10 to 20 percent of the companies fe
that not enough resources, getting the technology to work, analyzin
the data, keeping content fresh or internal organizational challeng
was the biggest problem. Also making personalization easy for user
integrating legacy systems and showing personalizations's value t
users caused some problems [126].

- Case: Content Management in a studio

  Managing content in a studio involves a number of critical issue
  including copyright protection and content re-purposing. Th
  system must be scalable, provide high availability, insure th
  un-compromised integrity of content, limit access to only authorize
  users and enable the quick retrieval of archived material [50].

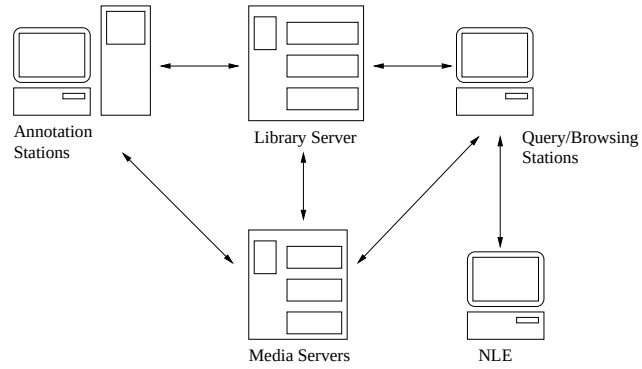

Figure 8.2: Content management in a studio [50]

The architecture of such a content management system is illustrate
in the figure above. The heart of the system is a Library server (c
Content Manager), which maintains the directories and metadat
for the content stored on the Media Servers. The media servers stor
and stream the content to clients in a real-time fashion. In additio
they are responsible for storing and maintaining the time-invarian
metadata of their own content. This includes playout informatio
such as shot and frame indexing. An Annotation Station is provide
for logging (ingesting) new content into the system. As new conter
is ingested, the Annotation Station will create metadata that can late
be used to perform searches on the content. It stores the metadata o
the Library Server and, simultaneously, the content itself is stored o
one of the Media Servers. Once ingested, the Browse Station is abl
to search, browse and retrieve content stored anywhere in the studio
This content includes video, audio, text, data, graphics, animation

The benefits of content management to the content provider

Managing the content creates lower costs in production and in distribution of the content. It also enables the use of new channels of distribution like the Internet, laser disc, DVD and VoD. Accessing the content is also easier. Content management also enables better protection of content by automatically managing intellectual property rights. Personalizing the content for target audiences and individual end-user gives the possibility for the company to gain greater profits. As the company has better control over the information provided, they also have better control over the company image on the global market [11, 43].

Content providers have also realized that they can generate significant profits by reusing, re-expressing, or re-purposing old content. For example, newspapers can be published also on the Internet and TV and motion pictures can be published in a digital TV with digital special effects added. For this reason, media and entertainment companies are seeing that effective management of their old and new content will allow them to maximize their profits [3].

- Web Site administration

  While creating HTML pages is getting more and more simple, the administration of a web site is still a time consuming and a demanding task. Available tools for web content management only cover some of the relevant aspects of the whole task - an integrated, fully functional solution is still missing. Web administrators still have to cope with many problems, such as ensuring validity of documents for instance management of document availability and expiration, or avoiding invalid links. Other current problems concern the maintenance of document validity - as soon as the document gets outdated, it should be removed in order to avoid waste of resources and to guarantee topicality. Besides a topic index many Web sites maintain a search engine helping to find local documents. Nevertheless, documents of interest may not be found because index data is gathered and updated only periodically and documents can exclusively be reached via hyperlinks. Keeping index data topical is a general problem to be solved. On corporate Web sites, a homogeneous page layout is wanted to establish corporate identity. Therefore, templates or style files have been used to create new documents. Nevertheless, due to the multiplicity of information providers and daily changing Web site content, it is rather difficult to observe compliance with internal style guides. It is obvious that Web site administration is a very demanding task [68]. The present content management systems available can though ensure that the site can handle the explosive growth of information, it also allows people to make simple changes without being concerned that a major modification could negatively affect the whole site accidentally [80]. For example iWebDB - Web Site Administration based on Object-Relational Database Technology - is an integrated database for Web content management, designed to meet the

6 TRAFFIC MANAGEMENT

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

6.1 Communications in IP Networks

Data communications in IP networks can be divided into *connectio less* and *connection-oriented communications*. Communications based o the Internet Protocol (IP) is connectionless by nature. This means tha no end-to-end connection is established before data is transmitted by th protocol [49, page 13]. In IP networks, *Quality of Service* (QoS) is define in terms of parameters such as bandwidth, delay, delay variation (jitter), an packet loss probability [15] .

Connection-oriented communications in IP networks is enabled b protocols built upon the connectionless IP. This means that a logica connection between communicating network nodes is established befor transmission [49, page 20]. *Grade of Service* (GoS) [1] is defined in terms o connection blocking probability (i.e. the probability of failing to establis a connection). Connection blocking can be controlled using *Connectio Admission Control* (see page 40) .

Different types of traffic

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

Stream flows are generated by real-time audio and video application such as Internet phone and video conferencing. These applications ma require a minimum level of QoS in order to function properly, and thu would benefit from guaranteed QoS .

Elastic flows are generated by non-real-time applications (e.g. e-ma and FTP). They don't state critical demands on QoS, but adjust their rate to make full use of QoS available [89] .

6.2 New service model for IP networks

The current IP architecture does not support any QoS guarantees becaus routing is traditionally based on a best-effort principle. This means tha each packet of information is treated independently and processed in th order of arrival [15].

[1] Grade of Service (GoS) is traditionally related to *connection-oriented telecommunic*

The diversity of applications and their requirements raises a need to develop a new service model for IP networks. The purpose is 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.

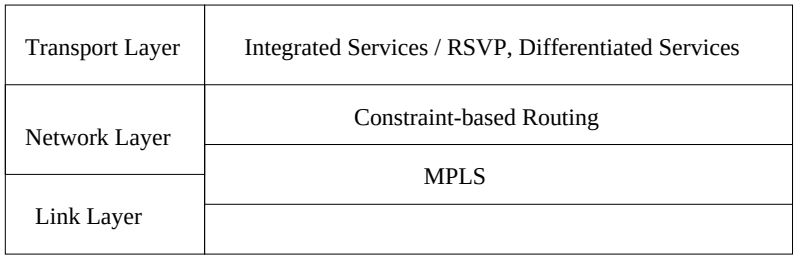

Figure 6.1: The relationship between OSI layers and concepts described in section 6.2 [128].

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 done e.g. using *Resource Reservation Protocol*[4] [54, 128].

Resource Reservation Protocol (RSVP) is used to signal routers in the network to reserve resources and set up a path for a flow [47, 128]. 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 [47, ch. 13] and in [131]. Standardization of RSVP can be found in [19].

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

[2]According to S. Shenker in [97], 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

[4]See [127] for the use of Resource Reservation Protocol with Integrated Services architecture.

[5]According to L. Massoulič and J. Roberts in [72], CAC should also be used for elastic

Server filtering software has the capability to regulate access b requiring the user to have a log-in account. An example of ho I-Gear works: when a Web page from the Internet is requested, th List Agent compares the URL with a list stored in the I-Gear subjec categories, then the URL is either denied or allowed. Next, th DDR (Dynamic Document Review) Agent reviews each page of we traffic looking for unconditionally vulgar words and replaces ther with "—-". The Local DDR Agent also reviews the documents fo any words that have been added to the category list based on loca community standards or determined inappropriate for the setting Finally, the Post Agent views words posted to the Internet an searches for items that have been rated unconditionally vulgar. Base on the criteria set, the agent either allows the requested Web page t be displayed in the browser or the user views a message indicating th reason that the requested page will not be displayed [124]. This kin of software works well for the protection of children at homes an at schools. URLabs I-Gear for FireWall-1 is a content managemer solution for organizations concerned about providing Internet acces for their employees. It enables organizations to ensure that th Internet usage is focused on business during core hours and permi the option of open, unmonitored access after hours [88].

- Potential application value of the Internet

The Internet population is already big and growing fast. The questio is how can the potential value of the Internet be well employed What is the potential value of e-distribution? First of all, technique that facilitate easy and quick browsing, retrieval, manipulation an secure access, transaction and purchasing of multimedia conten through Internet are needed [129].

To illustrate the potential capability and advantages of on-lin information representation, retrieval, browsing, transaction an purchasing we will represent a scenario of a music purchasing wit "EMusicOnline" and a video renting with "EVideoOnline". Instea of going to the store, music can be purchased by logging int EmusicOnline. It is possible to search for new songs and listen t a sample of each song before the decision of buying it. It is als possible to buy just certain songs instead of an entire CD. No on has to worry about the songs being sold out. The distribution take place by downloading the file. With EvideoOnline the renting star by logging into EVideoOnline and specifying the preferred movie As search results the service presents a list of movie titles alone wit a short description. It is possible to see the story board, a list of ke frames and a short presentation video on the chosen video. Rentin is charged with credit card, the rent-per-view fee. Distribution take place again by downloading the file. For these kind of services, ther

ensuring that the media content is technically correct without reference to its actual value. Syntactic validation will ensure that the media is in the correct format and playable by the system expected to receive it. Semantic validation is the process of determining if the content matter is correct in its current use context and whether it can safely be passed to the next stage of the media production process. Semantic validation is the core of any useful validation system. Once a piece of content has been validated, the details of the validation check and its result should be added to the metadata information associated with the content. The information can then be used by future validation services to increase the speed and accuracy of the service. Finally, in order for a validation service to be effective, the information on which a validation result is based must be completely trustworthy. Therefore, it is vital that automatic services for the encryption and digital signing of all content packages is provided as part of any validation service. The inclusion of digital watermarking can also be included under this task [33].

- Filtering programs

  Filtering programs are a part of the semantic validation process. There are a lot of inconvenient content in the web for the audience. What is inconvenient depends on the end-user, are they children surfing in the web or company's employees working at the business hours. There are two types of filtering software - client based software filtering and server based software filtering.

  The client filtering software programs are individual programs, at the moment in the market there are programs that go by names like Surf Watch, Cyber Patrol, Net Nanny and Cyber Sitter. These are mainly meant to filter the unsuitable content to young audience. In general, these software come with a pre-determined list of inappropriate sites with the option to subscribe to the list of updated site. Some of these programs also have controls that can be set to be tighter or looser at filtering based on certain words and/or phrases. However, without updating and continued monitoring, this type of software becomes less effective over time as additional inappropriate sites are placed online. The software works by blocking the unsuitable content from the user [124].

  There are not so many server based filtering software solutions available. One of the more popular server filtering program is I-Gear by URLabs. The server approach involves a main computer, usually designated for Internet only applications. The server is the main gateway between the local network and the Internet. As the gateway, the server is able to function as a web host, an e-mail host and a filtering interface to all of the computers on the local network. By having a server controlling all Internet features of a connection, there are many more options available for management of the content available on the Internet. Server software has the capability to control what computers on the network can access from the Internet and

below an acceptable level for that or any previously accepted flow. On th other hand, CAC affects also on GoS, as the level of GoS is decreased whe connections are refused [72, page 33].

Besides the benefits, CAC bears one disadvantage: Implementation c CAC would increase the complexity of networks, already complex enough Discussion on the benefits and disadvantages of CAC can be found in [97

According to Xiao and Ni [128], the Integrated Services architecture ha several problems: It doesn't scale well, states high requirements on router and requires ubiquitous deployment for guaranteed service. According t Baumgartner *et al.* [12], the architecture is suitable only for small network (e.g. corporate networks or Virtual Private Networks (VPNs)), not fo Internet backbone networks.

Differentiated Services Architecture

The approach of IETF Differentiated Services (DiffServ) working group involves creating distinct Classes of Service (CoS) , each with reserve resources. The basic difference between IntServ and DiffServ architecture is that while IntServ provides an absolute level of QoS, DiffServ is relative-priority scheme[7]. Secondly, in DiffServ the QoS in each CoS defined by an agreement between customer and service provider. Th eliminates the need of each application to signal their QoS needs at ru time. It also provides better scalability as there is no need to maintain pe flow state information in routers [53, 128, 4].

In Differentiated Services, each packet of information is classified b marking the *DS field*[8] in IP datagram. Packets receive their forwardin treatment, or per-hop behavior, according to the classification. The use c the DS field is standardized in [86] and in [14]. A small number of per-ho behaviors will also be defined by the working group [53, 128].

According to Xiao and Ni [128], DiffServ is more scalable, requires les from routers, and is easier to deploy than IntServ architecture. Baumgartne *et al.* [12] discuss more widely the DiffServ architecture, it's possibl drawbacks, and related issues.

Multi-protocol Label Switching Architecture

Multi-protocol Label Switching (MPLS) architecture is being standardize by IETF MPLS working group[9]. MPLS is a forwarding scheme that based on a label-swapping forwarding (label switching) paradigm instead c standard destination-based hop-by-hop forwarding paradigm [55, 117].

Each packet arriving to an ingress router of an MPLS domain[10]

below which users gain no utility. Besides preserving QoS, CAC would also prevent instabili and congestion collapses caused by uncontrolled retransmission of lost packets [72, pages 33 34].

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

[7] Admission Control is not used in DiffServ architecture. Thus only priorities betwee 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 i IPv6.

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

[10] An MPLS domain consists of MPLS-capable routers, called Label Switching Route

routed, classified, and given a label[11]. Inside the MPLS domain forwarding decisions are made by 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 [66].

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 [128, 55].

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" [128].

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 [128].

Constraint-based Routing increases the size of routing tables, and may introduce instability as routing tables change frequently [128]. Thus it should be considered whether it offers any benefit or just consumes more resources.

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.

[11]Labels are distributed to set up Label Switched Paths (LSPs) using Label Distribution Protocol (LDP) [128].

[12]Forwarding table is constructed as the result of label distribution [128].

[13]Routing Information Protocol, see [47, ch. 4].

[14]Open Shortest Path First, see [47, ch. 5].

[15]Intra-Domain Intermediate System to Intermediate System Routing, see [47, ch. 6].

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

delivery to the user, as well as eventual archival or destruction. Th
entails managing content across a number of different organizations an
over an extended time period. Practical experience of the benefits o
providing extensive content management systems has come for exampl
in the areas of interactive television, web services, multimedia kiosks an
video streaming to the corporate desktop [33].

Content management and the end-user

End-users will not continue to use a service, let alone pay for it, just becaus
it has the best technology. They are usually more concerned with th
content of the service [33].

- Content personalization service

  A multimedia service can be significantly enhanced if it
  able to pre-emt the need of each user, automatically supplyin
  the information the user wants without prompting, tailored t
  the user's current environment. This kind of service can b
  called personalization service. Personalization and adaptation o
  information systems to personal needs and personal interests becom
  more and more important. The trend to offer a user the most suitabl
  and narrowed down multimedia information can be seen in researc
  prototypes from different research areas, e.g. an adaptive tutoria
  agent, adaptive textbooks on the WWW, personalized newspape
  personalized news delivery etc. [18].

  The different requirements of each user create a problem for author
  and distributors of information. Typically, the author must eithe
  limit the types of user and client technology that can access th
  information, or else create significantly different versions of th
  information, each targeted to a particular user group. For instanc
  the authors of a simple Web page need to remember that the pag
  should be viewable by a wide variety of clients, including web-t
  personal organizers and advanced mobile phones. The wireles
  application protocol (WAP) provides a service for wireless mobil
  terminals by automatically adjusting Web pages for presentation [33
  Also the end-user has the possibility the view the same content vi
  different delivery channels. For instance it is possible to view
  film via terrestrial analogue, satellite analogue, cable analogue an
  pre-recorded VCR tapes and DVD, soon via digital terrestrial, digita
  satellite and digital cable. This range of distribution channels ca
  actually confuse the viewer (the user of the content). Therefore on
  objective is simplifying the situation for the user. The integration o
  uses of new digital delivery methods together - for instance the cente
  of all digital boxes could be the same in the future - with a degree o
  specialization and cross-referencing would be beneficial [32].

- Content validation service

  Content validation service is the task of ensuring that the medi
  content of the service is correct. Content validation can be broke

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, RMON) are used to talk to the network elements. The network schema extensions for the directory service are used to talk about network elements.

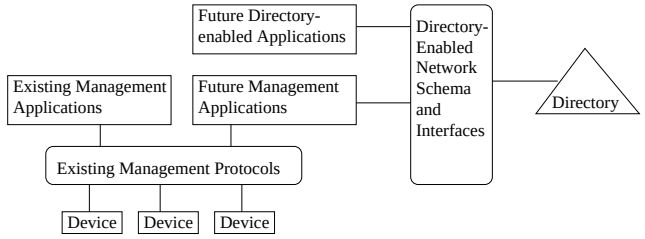

Figure 8.1: Directory service and network management [58]

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 experiences are 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.

8.4 Examples of content management

In the relation of information provider and end-user the core benefit of content management can be described: "information is managed so the right people receive the right information at the right time" [52]. With today's information glut, the value of information increases, when the content is managed in such a way to apply the stored information to the right people in an efficient way. The benefit can be ensured in many ways. The next examples will describe some of these different ways and they also reflect how widely content management is understood by different people. First, this section will deal with the examples where the end-user is the right person, and secondly the benefits of content management for the information provider.

Multimedia content management

The purpose of a multimedia content management system is to control the flow of content during the creation and delivery of any multimedia service offering. The content must be managed throughout its entire lifetime,

- Some proposed technologies demand ubiquitous deployment i order to offer any benefit. However, big changes to the best-effo architecture currently in use are difficult, perhaps impossible t deploy.

Some of these problems and other aspects related to the developmen of a new service model are addressed in [97] and it's references 4, 8, 30 and 37.

6.3 Performance Management

Performance management is used to evaluate the behavior of manage objects and the efficiency of communications activities. It is collectin statistical data, analyzing it, and where appropriate, predicting trends o communications between open systems [60].

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

Performance analysis

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

The analyzers available typically gather and display large volumes o 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 networ as a whole. Data becomes information when it is organized, correlated an presented in a way that clarifies it's meaning, helping the network manage make the best decisions [29]. Managers must also predict future trend based on historical network trends and business information.

Until the introduction of expert systems, alarms and events wer checked manually by the operators. Now expert systems are tested in th automation of this process. There are several artificial techniques tha can be used, such as Rule-Based Reasoning (RBR), Bayesian Network (BN), Neural Networks (NN), Case-Based Reasoning (CBR), Qualitativ Reasoning (QR) and Model-Based Reasoning (MBR) [9].

Performance metrics

Generally, network performance metrics are classified into tw areas: network-centric metrics and end-to-end measurements [94 Network-centric metrics are:

- **Router and switch metrics**

  These metrics deal with the operations of routers and switche queuing packets, processing them, and placing them on th appropriate outbound link queue. The metrics include Offered load Dropped traffic, and Average queue lengths (to assess queuing delay

- **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 probability.

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 [113, 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 [10].

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.

SGML does not enforce any particular set of element types. SGM provides a means by which new element types can be defined. Becaus of this, SGML is thought of as a language for defining markup language XML is similar in concept to HTML. Whereas HTML is used to conve graphical information about a document, XML is used to represe structured data in a document. HTML is an SGML application targeted a display markup for documents, XML is a subset of SGML targeted at dat representation. It is possible therefore to imagine the Web as consistin of HTML for display purposes, and XML for data representation an description purposes [37].

Object-oriented models

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

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

At the present time, there are not any CIM based implementation 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) tha software developers can use to make Web management applications wor together. Nor does it specify how the database of gathered informatio should be structured. CIM makes also no mention of the communication protocol that should be used for moving all that information around. So is difficult for vendors to develop software that can integrate data gathere by third-party applications [64].

Version 1.0 of the DMTF's CIM XML encoding specification wa announced in 1998. Allowing CIM information to be represented in th form of XML, brings the benefits of XML and its related technologies t management information modeled using the CIM Meta model [30].

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

In a directory enabled network user profiles, applications, and networ services are integrated through a common information model that store network state and exposes network information. This informatio

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 [85].

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 [92].

8.3 Management information modeling technologies

This section gives a brief summary of markup languages and object-oriented models (CIM and DEN) 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

7 SERVICE MANAGEMENT

This chapter discusses service management. Section 7.2 describes wha kind of services can be in networks, who uses and who offers these service Section 7.7 discusses accounting as enterprice level, while section 7. studies customer care and billing processes. Section 7.10 studies servic platforms and hybrid services.

7.1 Introduction

Growing services (such as e-commerce, web hosting etc.) are bein deployed over an infrastructure that spans multiple control domain These end-to-end services require co-operation in internetworking betwee multiple organizations, systems and entities. Service providers need t deploy interoperability, distributed scaleable architectures, integration an automation of network management systems. The management syste must make management easy and flexible to service providers. Th management system must also make service providers operations and en goals easier [13].

Service providers need to find new and effective ways to [27]:

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

Currently, there are no standard mechanisms to share selectiv management information between the various service providers or betwee service providers and their customers. Such mechanisms are necessary fo end-to-end service management and diagnosis as well as for ensuring th service level obligations between a service provider and its customers o partners [13].

7.2 Services in the Network

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

Services

According to Kong, Chen and Hussain: "A service is anything that a servic provider determines that customers will wish to purchase and that th

Another service definition: "A service is a set of functions offered to a user by an organisation." [90, page 889]

More service definitions: "A service is an application with a well-defined interface and functionality." [13]

Service is defined in International Telecommunication Union — 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." [114, 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 [62, 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. [78, 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 [122, 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 [122, page 20].

Different customer needs must be provided by traffic prioritizatio and traffic guarantees. For example, policy-based networking enable the allocation of network resources to applications, users, and group based on a set of defined rules. This approach provides th control over traffic prioritization based on the business importanc of applications.

8.2 Switching technologies

The increase in real-time and multimedia applications have created th need to improve Internet routing technology in terms of bandwidth performance, scalability, and delivery of new functionalities. Technologie used to develop new systems are combinations of switching and routin technologies. Routing provides robustness (scalability and flexibility and switching provides performance (high throughput). Noticeabl technologies are Ipsilon's IP Switching, Cisco's Tag Switching, IBM's ARI (Aggregate Route-based IP Switching), Toshiba's CSR (Cell Switchin 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 particular destination. These packets are related in terms of their routin and any local handling policy they may require.

Traffic differentiation is typically based on information in the packe headers of different layers in the IP protocol stack, e.g. protocol type source/destination port, source/destination address or explicit flow tag Two packets belong to the same flow if the values of header fields ar identical. The higher up the information origins, the higher the semanti content, and thus the more precise differentiation. For example, using th content-type field of HTTP 1.1, packets can be easily identified as bein part of a data, voice or video stream. On the downside, header parsin leads to performance drawbacks noticeable as increased induced traffi latency, which is only acceptable up to a certain degree for application with real-time requirements [5].

IP Switching

IP switching is basically an IP over ATM technology. The IP switche use the hardware of ATM switches for the copying mechanism and the I software for the routing. The IP switches allow packet flows to be switche and bypass the router, when the routing information has been cached in th switch. IP switching is made up of two protocols GSMP (General Switc Management Protocol, see [83] for a specification) and IFMP (Ipsilon Flo Management Protocol, see [84] for a specification).

When a packet is assembled and submitted to a controller in an I switch it classifies a flow. Ipsilon has currently defined two types of flow **A host pair flow type** is defined for traffic between same source an

applications require the security features the most. There is also a demand for content protection, to provide content owner a mechanism that can robustly protect copyright and identify rightful ownership in the court of law and to prevent illegal distribution and easy tracking of fraud. Techniques used to content protection are for example, cryptography, authentication, watermarking, and access control in different services. Users should also be able to check the originality of the content of a digital product. Content verification can be performed by attaching digital signatures to the transmitted data [119].

In the broader sense content could also mean communications content, such as desktop videoconference, e-mail, discussion forums etc. The difference between the copyright content and the communications content is that communications content is produced and consumed at the same time, and it is not stored for the further commercial use [130].

- Billing

  Internet services that provide QoS (e.g. TV and radio over IP) cannot cover costs using billing models available today [104]. In the Internet environment the billing has been based on flat rates and monthly billing and only seldom on the traffic itself. 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.

- Location and delivery

  Today the information contained on the Internet is unstructured, unsorted, and difficult to find. For example, current search engines are limited to textual keywords. There is the desire for Internet multimedia search engines capable of searching and locating the relevant sources containing the desired media types given a description of the specific content. This will be beyond the bounds of text currently used to formulate queries. Such capabilities could be achieved with pre-defined, hierarchical categories and natural language use [57].

  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 also have 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 [33]. The issues of secure access, and secure content and payment transaction are also essential to the distribution of content.

are converging. Media industry produces the content, for exampl entertainment and publishing. Computer industry produces equipmen and applications, which can make this content available for everyone Telecommunications industry, both fixed and mobile, produces th connections to networks. See Figure 7.1 [107]

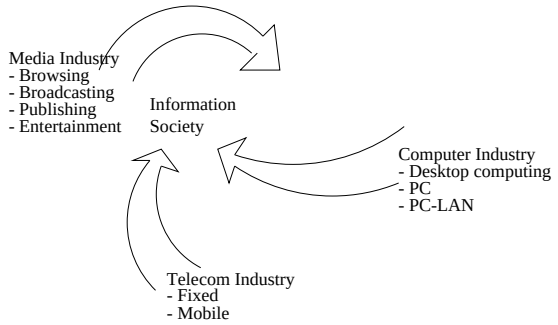

Figure 7.1: Convergence [107]

Service Providers

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

Service providers are increasingly using Service Level Agreement (SLAs) to define agreements for sharing resources with partners, as we as for offering service quality guarantees to customers. These SLAs contai details of information that are shared, and service level guarantees that ar offered by the service provider [13].

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

Service users

Service users are often called end-users or customers. Service provider 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 logica and easy to use. They also expect that the connection and the billing ar reliable, installations are easy and software products are good.

7.3 Security management

Basic security services that are defined in ITU-T Recommendation X.80 are:

- **Access control**

  Access control is the property of controlling network and compute

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)) [98]. Access control tools are discussed on page 32.

- **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) [98].

- **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 [7].

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 [70]. 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).

8 CONTENT MANAGEMENT

IP traffic on the Internet and private enterprise networks has been growin exponentially for some time. Today the convergence of computing telecommunication and digital media is enabled by the technology, bu it is actually driven by the content. For example, in the case of electroni publishing lack of established advertising/billing models and insufficien results have hindered online advertising [130].

Markus Kajanto states in his doctoral dissertation the notion o virtualization of content. The initial content is called by Kajanto primar content, which is divided into two parts: a virtual part and a physical par The virtual part of the content is distributable through the informatio network, but the physical part is distributed outside the informatio network. What the primary content is, depends on the industry an application in question. From the Internet service provider's point of vie it is essential that more and more products are already virtual of the basic nature or can be virtualized by exploiting information technolog information networks. Same applies also to many business processes, suc as commerce, marketing, and customer service [130].

This chapter describes content management on the Interne Section 8.1 gives an overview why content should be managed. Section 8. studies new technologies that are developed to improve Internet routin technology, such as IP switching, and Tag switching. Section 8.3 give an overview of management information modeling technologies, such a markup languages, CIM, and DEN. Finally, section 8.4 gives examples o content management.

8.1 Demands of content management

In this project we mean content management as determining what kind o data is transmitted in the network, and managing that data according to th needs of content suppliers, information intermediaries and customers. Th purpose of the content management is to control the flow of content durin the creation and delivery of any service.

Content supplier usually creates and formulates the original conten both the physical and the virtual part. Information intermediary (servic provider) is an organization, which matches the content suppliers to th relevant end customers. It will also have the knowledge of the conter preferences, consumption habits of the end customers, and what ma be the optimal choice for them [130]. Customers then use the conter through the Internet and they may also pay for it. It should be notice that content supplier, information intermediary, and customer usually hav different kinds of demands of content management. The needs for conter management are, for example:

- Security, proprietary rights and licenses

  Security and copyright issues must be guaranteed at the satisfyin

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 [69, 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 [69, 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 [69, page 135].

directory. All the applications could then use the same information. User have to log in only once to be able to use all the services and resources [74

There are some basic requirements for authentication [70]:

- Access management solution needs to work at a practical level,
- The solution needs to be secure
- It should make access easier, minimizing redundant authenticatio interactions and providing user-friendly information resources,
- It needs to scale,
- It needs to be robust, for example, a forgotten password should no be an intractable problem,
- It must be able to recognize the need for a user to access a resourc independent of his or her physical location (for example, a use must be able to connect to the Internet via a commercial Interne Service Provider (ISP), a mobile IP link, or a cable television Interne connection from home), and
- There should be a simple and well-defined (standard) interfac between resource operator and licensing institution.

The basic access management problem is licensing agreements fo networked information resources. The situations where institutions agre to share limited access are difficult. There is a need for fine-grained acces control where institutions want to limit resource access to only individua registered for a specific class, for example, when a class may be offere to students at multiple institutions. At present, most access to networ information resources is not controlled on a fine-grained basis. Ther is a danger that by accommodating all the needs for fine-grained acces management into the basic access management mechanisms will produc a too complex and costly system [70].

Management data represents a problem in the current acces 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 may involve making sacrifices in order to ensure privacy. Some institution may be legally limited in their ability to collect certain management data

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

A cross-organizational authentication system based on a credentia approach has the advantage of greater transparency. Resource operators ca have a higher level of confidence in the access management mechanism and a greater ability to monitor irregular access patterns. Privacy accountability and collection of management statistics must be taken u

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 [70].

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

their equipment suppliers. The IN reduced a great deal of this dependenc
by using service-specific software [42, 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. Creatin
new services implies developing a distributed application that must b
installed and executed in the terminals and servers. Internet application
take advantage of intelligent terminals and powerful user interfaces [42
page 9].

Hybrid services are expected to play a very important role in the year
to come. This is due to both the desire of users to integrate the ways the
communicate and the willingness of service providers to differentiate the
offers from their competitors. Also, smart cellular phones are expected t
fuel the integration of services [42, 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 applicatio
of formal methods of Internet to the development of Internet services o
hybrid services [69, page 134]. There are main questions:

- Are Internet services and hybrid services any different from othe
  telecommunication services?

- What do the differences mean for the application of forma
  techniques?

Interworking of Connect-Oriented and Connectionless Services

Hybrid services combine connection-oriented and connectionles
techniques. There is no commonly accepted call model for hybrid service
Telecommunications industry use formal methods based on specific ca
models, such as those used in the IN. Formal methods were applie
to standardized architectures such as the IN in which all services wer
structured in a similar way by using service-independent building block
the application and reuse of formal approaches was significantly easier [69
page 134].

The lack of a common call model for hybrid services implies that mos
of the work of applying formal techniques to telecommunication system
has to be revised and checked to see whether and how it can be reused an
adapted for hybrid services [69, page 134].

**Integration of Network-Centric and Terminal-Centric Service Con
trol Mechanisms**

In the Internet services are implemented in end users systems, whil
the telecommunications community normally has a network-centric visio
where services are implemented in the network. These two differen
views of service control may converge to a service-centric vision for th
deployment of hybrid services [69, page 134].

For the use of formal methods in development of hybrid services,
is necessary to consider software running at the user's site and in th
network [69, page 134].

Decreased Service Lifetime and Time to Market

Introducing new services in a telephone or cellular network was

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 [116, 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 [42, 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

can be demanding, managing many such systems could easily resu
in mistakes and omissions. A contributing factor is that the role o
system management is often short-changed and performed in haste
As a result, some systems will be less secure than other systems, an
these systems could be the weak links that will break the overa
security chain [121].

7.6 Customer Care and Billing

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

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

1980's was product oriented time in the telecommunication and dat
transfer market, while customer orientation is leading now. Marketing t
the customers as well as the ability to sell more and the ability to hig
quality customer care are one of the key components to success. Also,
is important to get the products quickly to the market, and to be able t
support existing and new services. A good customer care and billing syster
has to be flexible enough to fulfil these criteria [2].

Even electronic commerce depends on customer relationships, say
Lester Wanninger, professor at the University of Minnesota. It is importan
to teach how to make good customer relations for people going to sta
electronic commerce. Also, in electronic commerce a company and
customer should handle all the communication channels. Electroni
commerce has to implement functional processes of the company
information systems, databases, and other channels. It is important tha
a customer gets the same service from any service channel of the company
Ease of use brings more value to the customer. Also, in electroni
commerce, the customer buys again only if the customer gets what wa
promised. WWW-pages can have effect on attitudes, intends, and shoppin
habits. High quality information, easy use, and new experiences, bindin
customers to services. Traditional media, such as TV, radio, and printe
media are good in getting new customers, while the Internet is good i
keeping old customers [59].

Customer Care

Customer care means maintaining customer services and custome
relationships and answering routines, for example Help desk function
Customer care links to the level of the offered service and the connectio
with the service level and the price of the service [108].

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

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 [67]. 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 [20], 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

available in directories using standardized protocols [74].

Future service platforms

Current architectures in service management are based on managemer protocols like Simple Network Management Protocol (SNMP) an Common Management Information Protocol (CMIP) or trouble ticketin interface [20, page 167].

Web-based Architecture

In the Web-based architecture the customer downloads an applet tha communicates with a proxy server in the service providers domain. Th proxy server interacts with the actual inter-domain management system. is possible to use standard gateways like IBM Webbin or build a servic specific solutions in order to simplify the funtionality at the customer site This makes download times shorter and there is less need for code [20, pag 167].

The inter-domain management system implements the interaction with co-operating service providers. Requests to the local domain ar processed by the intra-domain management system and then forwarde down the hierarchy to the network managers and finally to the networ element managers [20, page 167].

Security restrictions in browsers do not allow applets to interact wit local resources, i.e. with the file system or local network nodes. In Netscap Communicator, the security restrictions can be configured based on th right to trust relationships with the applet provider. Signed applets can b given the right to access the local network. This provides also a networ management solution for customer premises network [20, page 167].

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

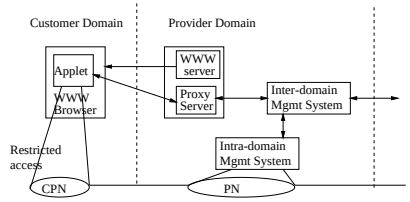

Figure 7.4: Web-based service management architecture [20, page 167]

This prototype has been developed providing a web based interfac covering subscription management, configuration management, alarm surveillance, trouble ticketing as well as accounting management. Th usage of the web and Java (applets) simplifies the service interactio between the customer and the service provider. It will reduce the cost o both sides. For service provider it is important to automate the custome care process in order to cut the costs to survive in the emerging competitiv market [20, page 168].

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 [120].

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 [99, 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 [99, 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 [99, 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 [65].

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

phase. Usually the customer picks one of the standard tariffs offere by the service provider.

- **Usage metering** The service provider meters the usage of th resources during the operational phase. This includes the orders c the customers and the actual usage of the network. Readings ar gathered from the network resources.

- **Charging** The tariff and usage information are combined and th charge is computed. This can be done directly after the connectio 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 i a bill. Taxes are added. The customer will then be notified and th invoicing process will be triggered.

- **Invoicing** Within the invoicing process the system keeps track of th payment status of the bills of each customer. The customer can pa the bill in the way he or she wants.

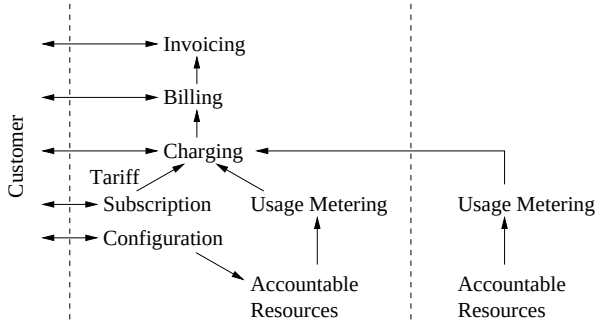

Figure 7.2: Accounting process [20]

Payment mechanisms

Internet payment mechanisms can be grouped into three classe electronic currency systems, credit-debit systems and systems based o secure presentation of credit card numbers [82].

Collecting and rating usage, tracking services, managing inventorie and reconciling invoices are key features of accounting systems [67].

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

In the credit-debit model (like NetCheque system), customers ar registered with accounts on payment servers. Customers authorize charge

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 [82].

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 [31].

Demands of electronic payment systems

Internet payment system should be secure, reliable, scalable, 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 [82].

- **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

agreements. The user runs the browser to access WWW servers, whic deliver information to the requesting browser [101, pages 87–88].

The key components of the WWW architecture are the Uniform Resource Locator (URL), the Hypertext Transfer Protocol (HTTP), and th Hypertext Markup Language (HTML) [101, page 88].

URLs provide standardized specifications for objects or resource located on a network, detailing both the network address of the object an 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 th URL to find an object on the network and select the proper protocol fo interacting with that object [101, pages 88–89].

The HTTP is a connection-oriented protocol designed for the rapi transport of files consisting of a mixture of text and graphics. HTT uses an object-oriented protocol consisting of simple commands tha support negotiation between the client and the server. This negotiatio allows WWW browsers and servers to develop independently of emergin technologies because the negotiation process established a common bas of communication between the client and the server [101, page 89].

A universally understood language is needed when publishin information for global distribution. The publishing language used by th World Wide Web (WWW) is HyperText Markup Language (HTML) [120 HTML is a standardized document tagging language, based on th Standardized Generalized Markup Language (SGML) [101, pages 89–90

According to W3 [120], HTML gives authors the means to:

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

HTML has been developed with the vision that all manner of device should be able to use information on the Web: PCs with graphics display

Today all service providers have to create their own services in the Internet. Same services are created in many different 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 [45, 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

- **Efficiency** Royalties for access to information may generate frequer payments for small amounts. Applications must be able to make thes "micropayments" without noticeable performance deterioration.
- **Ease of integration** Applications must be modified to use th payment infrastructure in order to make a payment service availabl to users.
- **Ease of use** Users should not be constantly interrupted to provid 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 dep (unpaid bills), forgeries, unauthorized payments on behalf of anothe person, double purchases (order twice – pay once), refusal of payment and unsuccessful deliveries.

Future billing requirements

Some of the requirements of the new billing systems include [76]:

- 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 provider
- Well-defined interfaces to allow easy integration and data sharin between business systems and the billing system.
- Pre-paid services: Customers change to pre-paid service, s customers' loyalty to service provider will become more difficult t check. Customers can easily change the service provider, becaus they can easily buy new pre-paid services from any other servic 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 ope more accurate and faster charging for the services.

7.7 Accounting management

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

- **Usage measurement**

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

- **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 [114, 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 [60, 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) [104].

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

[1] See section 3.1 for Simple Network Management Protocol (SNMP).

[2] Connection time for connectionless communications would be difficult to measure (ex-

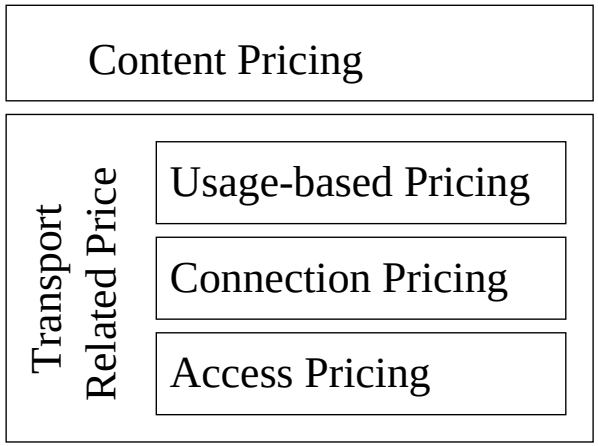

Figure 7.3: Components of Internet pricing [104]

Accounting is usually based on mechanisms offered by commerciall available routers and switches. The most commonly used approac employs packet filtering and statistical sampling. However, it is difficu to charge for usage-based traffic since the granularity of these methods too coarse and the measurement overhead significant [104].

Another problem concerning accounting data collection in route is whether packets should be counted on entry to or on exit from router[3] [77].

For volume measurements the IETF Real-time Traffic Flo Measurement (RTFM) working group has proposed standards to mete flows and to distribute this accounting information via SNMP [104].

The Remote Authentication Dial-In User Service (RADIUS) is protocol specified by the IETF radius working group. It helps managin the Internet access links. Since these links are sensitive to securit and accounting, a protocol is provided to authenticate dial-in users an negotiate configuration data. RADIUS services are implemented by mo router manufactures. Accounting data can be collected on a time-, packet or octet-basis for a particular service [104].

7.8 Managing New Services

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

[3] The nature of IP is that not every packet received by a router is actually passed to a