Liisa Uosukainen Tuomas Lilja Lasse Metso Seppo Ihalainen Jouni Karvo Ossi Taipale

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

Teknillinen korkeakoulu
Tietotekniikan osasto
Tietoliikenneohjelmistojen ja multimedian laboratorio

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

develop network management paradigm for large IP-networks. The need for large IP-networks is shown in figure 1.1.

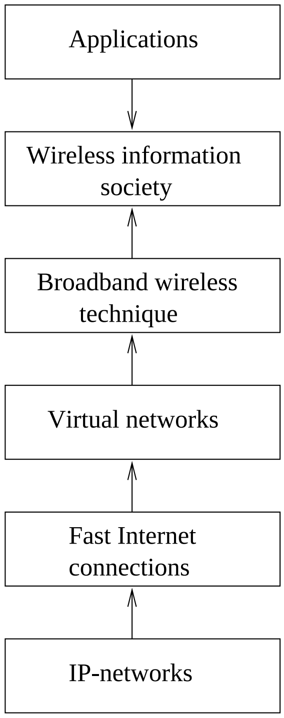

Figure 1.1: IP-networks in the growth strategy.

Large and complex systems need network management tools. In this report we examine models and protocols, that are available for network management. Also future network management models are discussed. The aim of this report is to give basic knowledge of network management. In the professor Martikainen's reference model (see figure 1.2) network

1.1 Changes and challenges

In the future network usage grows, because of new users, servers, applications, network links and traffic. As networks become larger and more complex, tools and applications to ease the management are critical. Network management means providing information to the operator and also to the end users, encompassing the total end-to-end flow information. Time is the critical factor in network management (see figure 3). Managers strive for shorter cycles and customers demand faster response. Shorter cycles lead into lower costs and greater productivity [4].

Networks and distributed processing systems have become critical in the business world. Companies and organizations develop complex networks with more applications and more users. In order to help this complex systems there is a need for network management tools. In this report we examine the problems of the network management. In a reference model of professor Martikainen (see figure 1.2) the network management is divided into four levels. Each level is examined individually.

Introduction of the new equipment and the new technologies means introduction of new information systems, which also increases the number of data repositories and fault management systems. Automated network management is needed [37]. Organizations already have network management tools at their disposal. These tools typically gather and display large volumes of detailed data rather than interpreting and highlighting what

Network management views the computing environment as a collection of co-operating systems connected by various communication mechanisms. The workers at Sun Microsystems express, the network is the computer. This means, that effective system management is thinking the network as a single, multilayer entity, one that requires its own care [33]. An important aspect is that management is useless to a company if it does not solve business problems and the work of operators [42].

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 [4].

Effective and to the business strategy adaptive network management requires:

- The right abstraction level of information
- Information at the right time
- Information in an easy-to-use format [4].

There are three ways to design network management systems: discrete, centralized and hierarchical management systems. To the business strategy adaptive network management contains activities, such as technology selection, network automation, capacity planning, predictive problem avoidance and sophisticated trouble-shooting. These activities all require information that goes beyond the data available to most of the ture. Data will find you where ever you are. When there are no connectors, it means lighter, cheaper and simple devices.”

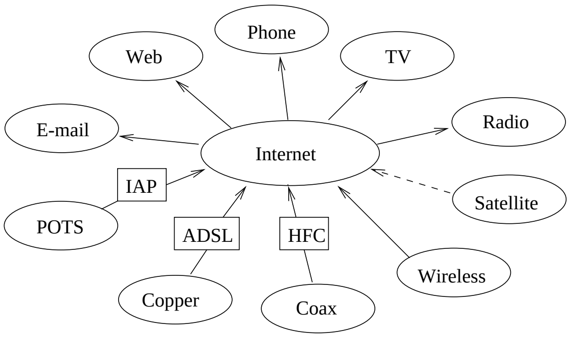

Figure 1.4: The internet picture [17]

”There are big questions, what can/is possible to change in the near future. Can the organization change from technology and product silos to end-to-end service delivery processes? Can fault isolation and problem determination get better in such a complex environment? Can management processes become more disciplined and automated?”

- Systems Management Functions

Management Model

The Management Model describes a manager-agent concept (figure 2.1). The manager system manages the Managed Objects in distributed manner by issuing remote management requests to agent processes. The agents manage the Managed Objects and are responsible for implementing the functionality needed to execute the requests. They may also return values and send notifications (events or traps generated by Managed Objects) back to the manager. The management operations and notifications are transferred using Common Management Information Protocol (CMIP) [40, 14, 47, 53].

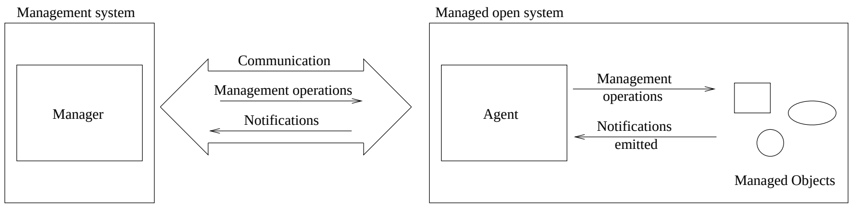

Figure 2.1: The manager-agent concept [15]

A network to be managed can be divided into management domains. A domain is an administrative partition of a managed network or internet. Domains may be useful for reasons of scale, security, or administrative autonomy. Domains allow the construction of both strict hierarchical and fully cooperative and distributed network management systems [53, 15].

(ASN.1), that provides a machine-independent representation for the information [53].

Systems Management Functions

Systems Management Functions 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 [47].

Management Functional Areas - OSI FCAPS model

OSI network management functionality is divided into five management functional areas [14]:

- **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 [14].
- **Configuration Management** identifies, exercises control over, collects data from and provides data to open systems. The purpose of Configuration management is to prepare for, initialize, start, provide the continuous operation of and terminate interconnection services [14].
- **Accounting Management** enables charges to be established for the use of the resources in the OSI environ-

events [14].

2.2 Telecommunications Management Network (TMN)

TMN overview

A Telecommunications Management Network provides management functions for telecommunications networks and services, and offers communications between itself and the telecommunications networks and services. It is an organized architecture that provides the interconnection between various types of Operations Systems (OSs) and/or telecommunications equipment for the exchange of management information [20].

Figure 2.2 shows the general relationship between a TMN and the telecommunications network it manages. A TMN is conceptually a separate network that interfaces a telecommunications network at several different points to send/receive information to/from it and to control it's operations. A TMN may use parts of the telecommunications network to provide it's communications [20].

The top-level standards and recommendations for OSI systems management form the basis for TMN standards [21]. The TMN standards are defined in ITU-T M.3000-series documents [49, page 48].

The scope of network management is broader in telecommunications than in data communications [49, page 48]. Thus a TMN must provide more than just the five Management Functional Areas defined in the OSI FCAPS model [49, page 25]. A TMNs is intended to support management areas which cover the planning, installation, operations, administration, maintenance and provisioning of telecommunications networks and services [20].

TMN Management services

TMN Management Layers

The needed management functionality is implemented using five layers of management. 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 [49, pages 19–21].

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 [49].

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 [49].

Network management layer manages the whole network. It receives data from network element management layer and provides total-network-level views [49].

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 [49].

building blocks [20].

The **physical architecture** describes realizable interfaces and examples of physical components that make up the TMN [20].

Customer Network Management (CNM)

The purpose of Customer Network Management is to provide external users of a telecommunications network with a limited control and view of the managed network. It enables customers to manage a portion of the whole network and subscribe it's services. Figure 2.3 illustrates the CNM functional architecture [49, pages38–42].

Customers are provided with a subset of the TMN management 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 [49, pages 38–44].

2.3 SMART TMN

Smart TMN [46] 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,

Figure 2.3: CNM functional architecture [49, page 39].

- **Technology Integration Map**, which contains recommendations of technologies to adopt for different management applications [45],
- **Central Information Facility** for information store for technical specifications, object models etc., and
- **Catalys Projects** are projects to validate technology concepts.

2.4 Telecommunications Information Networking Architecture (TINA)

TINA overview

TINA is designed to meet the needs of telecommunications services ranging from traditional voice-based services to interactive multimedia, multiparty services, information services, as well as management services. All these services are considered to be software-based applications that operate on a distributed computing platform [31, page 137]. TINA addresses a wide range of issues and provides a complex set of concepts and principles. In this respect it is much more a framework, a compilation of concepts and principles for developing future distributed telecommunications and management services, than a specific architecture [31, page 148].

24].

The **computing architecture** defines a set of concepts and principles for designing and building distributed software [52]. It is based on the Basic Reference Model for Open Distributed Processing (RM-ODP, ITU Recommendation X.900) [31, page 148].

The **service architecture** defines a set of concepts and principles for the design, specification, implementation and management of telecommunication services [52, 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 [52, 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 [31, page 163]. However, the TINA management architecture is still under study [52, pages 27–28].

TINA network management model

TINA network management model extends the OSI FCAPS model. Configuration management is divided into *connection management* and *resource configuration management* [31, page 163].

includes the management of the relationships among the resources [16].

Fault management includes alarm surveillance, fault localization, fault correction, testing functions and trouble administration information [16].

Accounting management is responsible for measuring and establishing charges for the use of resources [16].

According to N. von Knorring, the specification process concerning **performance** and **security management** aspects has not been very successful. For the time being, they are still under further study [31, page 29].

network elements [90, 19].

SNMP is based on a agent-manager concept, similar to the one illustrated in figure 2.1. The manager sends requests to agents in network elements. The agents, which are responsible for controlling the network elements, send responses and issue trap messages to the manager. The requests and responses are exchanged using the User Datagram Protocol (UDP), which is a connectionless protocol. Trap-directed polling is used to decrease the management traffic on the network [28].

SNMP disadvantages

According to Lyn Vallillee, SNMP has some disadvantages: SNMP contains large security gaps that can give network intruders access to the information carried along the network. Intruders could also potentially shut down some terminals. The biggest problem with SNMP though is that it is generally considered to be so simple that the information it deals with is neither detailed nor well-organized enough to deal with the expanding networks of the 1990's. This is mainly due to the quick creation of SNMP, for it was never intended to lead network management into the 1990's [50].

These problems were tried to be solved by establishing a new version of SNMP, called SNMPv2. This new version allows for more in-detail specification of variables, including the use of the table data structure for easier data retrieval. Also included are two new PDU's that are used to manipulate the tabled objects. It has also added some security mechanisms that help combat the 3 largest security problems: privacy of data (to prevent intruders from gaining access to information perform tasks that would be impossible under SNMP [40].

In CMIP, requests and responses between managers and agents are exchanged using the OSI connection-oriented transport protocol that provides in-order, guaranteed delivery [28].

However, 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 [50].

3.3 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 Recommendation M.3010 (or ETSI ETR 037) and in OSI Management Recommendations of the X.700-Series [27].

The definition of TMN is concerned with five layers in management, namely business management, service management, network management, network element management, and the elements in the network that are managed. Of these, OMAP currently is not concerned with business management, and interacts with other TMN parts to provide service management [27].

Management functions and resources are provided by OMAP to 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 is provided [27].

- to establish common terminology and

- to establish a problem-oriented approach to the realization of distributed systems management solutions.

The Reference Model describes concepts necessary to build a comprehensive distributed systems management environment. It identifies the mapping between the abstract concepts and some technologies that provide suitable implementation bases for the realization of the Model. The model is intended to enable a network of heterogeneous systems to be managed as a single system [47].

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

The Reference Model consists of 3 basic components:

- Managers, which implement Management Tasks and other composite management functions,

- Managed Objects, which encapsulate the resources,

- Services, which provide the X/Open Systems Management Support Environment.

Anticipated implementation technologies

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

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

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

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

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

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

4.3 Java Management API (JMAPI)

Java Management API [44] is intended to provide a standard interface between different computers and network devices.

prietary, ITU-T/ISO, SNMP and CORBA based network elements [36].

CORBA (Common Object Request Broker Architecture) is an architecture that supports the distribution of management functionality and managed objects [47].

Internetworking between CORBA and TMN systems

In the context of TMN, CORBA is seen to offer potential in two significant areas: in the description and implementation of management interfaces supported by network devices, and in the description and implementation of interfaces within and between management operations systems [36].

4.5 SPIN's Intelligent Network Management

SPIN is a research project in the Institute for Information Technology at Canada's National Research Council [8]. The SPIN Intelligent Network Management project studies and develops new agent-based technologies for controlling, planning and problem definition of heterogeneous networks. The application development of SPIN networks uses integration of the off-the-self NM components, and testing and usage of popular tools, such as HP openview.

duration, which is the duration of pulse width of the start element. Synchronous systems do not have start and stop elements, but consist of a continuous serial stream of information elements or bits. Two of the most common causes of errors are noise and improper timing relationships [22, pages464–470].

5.1 Asynchronous transmission

In start-stop systems the last information bit is most susceptible to cumulative timing errors. Timing error can accumulate inside a character, those 5 or 8 bits of character length. Start and stop bits lowers the rate of transmission efficiency as well. Another problem in asynchronous transmission systems is the multilation of the start element. Once this happens, the receiver starts a timing sequence on the next mark-to-space transition it sees and then continues to print error until, by chance, it cycles back properly on a proper start element [22, pages 477].

One of the earliest methods of error detection is the parity check. Parity check means, that when we have a 7-bit ASCII code, a bit is added for parity, making an 8-bit code. This means also that when we have a parity check-system, a 8-bit codes must be encoded to 7-bit codes [24, pages 400].

5.2 Synchronous transmission

Synchronous transmission require frame alignment and it must be bit-aligned as well. Every data frame starts with a unique field, which tells the receiver when the frame starts. Start-stop erally be highly compressed. Smaller packets will not benefit from compression as much because there is less opportunity to squeeze out redundancies in small amounts of data [12, pages 59].

Text data transmission

When the network is heavily utilized, the combined bandwidth demand occasionally exceeds the network capacity. For text data, this is not a problem, except for some areas of the industrial automation. It simply means that the text data does not arrive as quickly; it is only delayed [7].

However, the time is the important measure of the capacity. Some of the significant metrics are the formation time of the connection and the response time of the service. The quality of the data transmission is described also by the number of the errors per time unit which is measured with a bit error rate (the share of faulty bits of sent bits) [24, pages 379–380].

The errors in the text format data are not usually serious ones. Whereas the binary data message (for example source code) suffers from the errors. The important goal is to minimize the bit error rate. We can not provide transmission channel with no errors. Redundancy can be increased such that the error rate approaches zero. However this lowers the capacity of the communication.

In binary transmission an error is a bit that is incorrectly received. Bit errors occur as single random errors or as bursts of errors. Random errors occur during noise peaks, which can confuse the receiver's decision, weather a 1 or a 0. Burst errors ing voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network. A major advantage of VoIP and Internet telephony is that it avoids the tolls charged by ordinary telephone service [7].

Voice transmission

Video and voice traffic must get a fairly regulated number of packets through to the destination in a timely manner. If video/voice packets are late enough (have missed their window), they are useless. The network should drop traffic that is late so it does not consume network resources [7].

In addition to IP, VoIP uses the real-time protocol (RTP) to ensure that packets get delivered in a timely way. Using public networks, it is currently difficult to guarantee Quality of Service (QoS). There occur delays, which can deteriorate voice almost unrecognized. Better service is possible with private networks managed by an enterprise or by an Internet telephony service provider (ITSP).

5.5 Video

Video has gone through a transformation similar to that of voice. Experts feel that video services will more and more come to be delivered over intranets, the Internet, and other Internet Protocol (IP)-related technologies. The delivery of digital video services can take many forms. It represents the future of conventional home entertainment as well as video-network requirements. Multimedia requires immediate transmission of the requested information, usually from a remote location. The requests for the information (image and sound) are usually uncontrolled and unplanned. In addition, the newer information is isochronous; rigid timing and flow control, which most traditional networks are not designed to provide, are required [37].

A video picture requires an large instantaneous amount of bandwidth and unloaded connections which are not typical for Internet. Targets in multimedia are provisioning of required bandwidth and its flexible management. Multimedia applications, that were originally designed for LANs, place unique demands on the wide area telecommunications network. One bottleneck is a Internet-connection with modem. A video picture requires more capacity than a normal or widely used modem can offer. In LANs, for example Ehernet, it is impossible to send a continuous video picture, because continuous connection is impossible to guarantee.

Misrouted or lost packets may become a problem, if a transfer rate is high. One bit error causes more trouble in compressed data than in uncompressed. What are the acceptable delays depends on the application; if the information is isochronous rigid timing is essential and delays should be no more than milliseconds. In case of broadcast video or audio end-to-end delay is not so crucial and retransmission schemes are feasible.

accessed across the network. For example the time is an important metric in copying large files across the network. Internet service providers have used ping and traceroute to detect and diagnose network problems. Application servers, routers and terminal servers in the different post office protocols (POPs) can be targets for the network connectivity and delay measurements. Ping and traceroute give an indication of changes in the network characteristics, but these tools are not sufficient to quantify the impact of these changes on availability and performance of customer-visible services [18].

There are many components that impact the QoS being delivered. For some network components only limited data has been available. The measured values can often only indirectly describe the quality of service. Information technology organizations (IT) has been under the assumption that the quality of service management is equal to the sum of all of the parts. In mathematics, this assumption is valid, but in the management of IT services, it is false [43].

For services that use TCP, a useful network performance metrics are for example throughput, defined as the rate of reliable transmission of packets between a source and a destination, performance by response times, transactions in a period of time, availability in mean time between failure (MTBF), hours of downtime and time to restore, CPU uptime, dropped packets and network congestion (peak time) [12].

essary to determine what level of service is acceptable. The problem is that service provider lacks some of the necessary information. They do not have adequate information about the value of the service to the client organization [43]. The quality of service or class of service can be connected to address, to protocol or to some else property of transmission. The other method is that the application of the workstation tells to the network what level of service it needs. Microsoft will integrate in future Windows versions properties needed in using class of service. In the future application software can request services of the network with Winsock 2.0 interface. Network applications must be changed to use new interface and class of service [2].

6.3 Future trends

Service providers need to find new and effective ways to [1]:

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

Enlargening services (such as e-commerce, web hosting etc.) are being deployed over an infrastructure that spans muland end goals easier.

6.4 Authentication and authorization

Almost all applications utilize user information and presume an authentication of users. Authentication means that a network user establishes a right to an identity, the right to use a name. Passwords, smart cards and certificates are used to authenticate a user. A user may have the rights to use more than one name and a user may have rights to use identities established by multiple organizations (such as universities and scholarly societies). Authorization is the determining whether an identity is permitted to perform some action, such as accessing a resource [30].

There might be an advantage if all the user information is available in same directory. All the applications could then use same information. Users have to log in only once to be able to use all the services and recourses [32].

Requirements

There are some basic requirements for authentication [30]:

- access management solution needs to work at a practical level
- the solution needs to be secure
- it should make access easier, minimizing redundant authentication interactions and providing a user-friendly information resources

The basic access management problem is licensing agreements for networked information resources today. The situations where institutions agree to share limited-access are difficult. At present, most access to network information resources is not controlled on a fine-grained basis. There is a danger that by accommodating all the needs for fine-grained access management into the basic access management mechanisms will produce a too complex and costly system [30].

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

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

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

the network is being used [29]. Some pricing mechanism will be necessary in order to manage the quality of services (QoS). Accounting and billing systems must be reliable, scaleable and high performance, offering flow-through operation from the other systems.

Payment mechanisms

Internet payment mechanisms can be grouped into three classes: electronic currency systems, credit-debit systems and systems based on credit card numbers [35]. Collecting and rating usage, tracking services, managing inventories and reconciling invoices are key features of accounting systems [29].

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

In the credit-debit model (like NetCheque system), customers are registered with accounts on payment servers. Customers authorize charges against those accounts. The credit-debit model is audible. Once a payment instrument has been deposited, the owner of the debited account can determine who authorized the payment, and that the instrument was accepted by the payee and deposited [35].

Some payment mechanisms are based on credit cards (such as Cybercash). Information is often shared with owner of the transactions, than they are in other communities [35].

- Security: The infrastructure must be usable and resistant to attack 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 a 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 a payment mechanism affects the size of the customer base.
- Flexibility: Alternative forms of payment are needed. The payment infrastructure should support several payment methods including credit cards, personal checks, cashier's checks and anonymous electronic cash.
- Convertibility: There will be several forms of payment, providing different trades.

running into dept (unpaid bills), forgeries, not allowed payments on behalf of another person, double purchases (order twice - pay once), refusal of payments and unsuccessful deliveries.

Future billing requirements

Some of the requirements of new billing systems include:

- Real-time react to market activities
- Flexible billing formats and media to meet customer demands
- Flexible rating engine that allows discounting
- Integrated billing, which includes charges from third-party providers
- Well-defined interfaces to allow easy integration and data sharing between business systems and the billing system [6].

6.6 Directories

Directories are logical data repositories to save and to search for information. Directory services are important in helping users to find information on a 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. The data is often saved in logical tree form.

ences are saved in the directory of the network, it can be used by any workstation in the network. At the same time the importance of an individual device and its place decreases. When intranet systems are expanded to extranet-systems, there is a problem combining different type of directories and databases. A standardized model of directories will help this integration.

Centralized directory can also lead to decreasing maintenance costs. The main part of the costs are management and maintenance costs. If the directories are centralized, part of the maintenance can be centralized. The development of an application is also easier if all the information is available in directories using standardized protocols [32].

ment must resolve. They must also understand the network traffic patterns and identify bottlenecks that reduce the performance. Nowadays modern components and subsystems can be configured to support many different applications. The same device can be configured to act either as a router or as an end system node or both. The configuration manager can choose the appropriate software and set of attributes and values for that device [39, pages 481]. Reconfiguration is necessary when the network is expanded or in the fault isolation.

As the network scales up in physical size (capability and complexity), so the management capabilities must be enlarged. The aim is that these actions can be automated. It should also be possible to make on-line changes without affecting the entire element or network [37]. The large-scale network management systems must be constructed to support several network elements and also be extensible to support new elements. It must be flexible enough to support the rapid deployment of new highly customized services.

Activities in the network management are [25]:

- Activities, that do not affect the function of the element (for example changing the parameters of the device)
- Activities, that affect the function of the element (for example switching off the element from the sub-network)
- Activities, that make elements to do desired activities (for example restart)

work should also be prepared to the varying volumes of users.

By continuously addressing the cost of maintenance (Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR) statistics, costs associated with maintaining) the network as a system can be tuned [42].

7.2 Security management

As computer-based communications and networks that link open systems continue to expand, security management becomes critical. The security management should be used to permit access and also to keep unwanted personnel from having access to network control functions. Security management should permit unauthorized access to the network. Thus standardization of security properties has developed slowly.

Security management should include [37]:

- Controlling user authorization
- Maintaining multiple levels of access control
- Reporting access attempts or breaches (breaks) of security
- Maintaining separate security control information
- Limiting access to historical security logs.

Another important area of security is preventing unauthorized access to the physical network environment.

tion). The security level operations can be restricted by the date or by the time period.

Routers

Routers improve the network security, but they bring along new problems. For example routing protocols are susceptible to the security attacks and routing mistakes may allow the entrance of unauthorized personnel into the network. The unlicensed remote and local operations must be prevented with a username. The traffic control through the router is managed with a packet filtration which is based on the list. Some properties can be attached to the router, such as the network address translation (NAT), port address translation (PAT), logging of events and alerts. 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 [2].

Firewalls

The controlled connections between the company's net and a public net are carried out with firewall. The firewall consists usually of routers, nets, isolated firewall devices and software. The firewall can operate also inside the net, if the security demands are high.

Firewall products are divided into three groups:

- Packet filtering: Controlled routing which is based on the addresses and the types of the packets.

- Signaling traffic load
- Error rate

The most commonly used network performance characteristics are [12, pages 92]

- response time (average, long term variation): indicator of performance, the lower the better, should be predictable
- transaction time: some transactions may be configured to have priority over other transactions
- utilization (memory and disk, CPU, network utilization)
- collision rate
- protocol overhead and efficiency
- maximum number of concurrent users
- time to perform a large file transfer
- time to display color image
- dropped packet rate and retransmissions

Analysis

The analysis become more important, when networks increase in size and in complexity. Analyzers are used to determine physical problems, loading problems (for example broadcast) and transmission protocol problems. Analyzers are understood as troubleshooting tools, but they should be used as proactive indicators as well.

It is difficult to choose the right metrics to analyze network efficiency. The tools available today typically gather and display volumes of detailed data rather than interpret and highlight the meaning of the data. Many of these tools look at a single element rather than the network as a whole. Data becomes information when it is organized, correlated and presented in ways that make clear its meaning, helping the network manager make the best decisions [4]. It is important to analyze the network up to date. Managers must also predict future trends based on historical network trends and business information.

Expert systems The network manager is overloaded with data. A stream of detailed data means by itself a little. Effective information is compact. The network management problem thus becomes an information management problem.

Before the expert systems, alarms and events were checked manually by the operators. Now expert systems are tested in automation of this process. Various expert systems can be used in the network management. There are several artificial techniques that can be used, such as Rule-Based Reasoning (RBR), Physical network problems account more than half of all network problems. Technicians spend most of their time locating the origins of such problems (fiber cut, the earth is incorrect, adapter is broken or incorrectly joined). This costs network providers time and money. Network management systems have also traditionally focused on the logical connection between the end user and the network destination, since most network problems have been a result of errors created by software applications [37]. Finding and repairing failures of software applications is usually difficult, for example the workstation sends but does not receive packets, too many collisions, frames are too short or too long.

Fault management is trouble shooting, fault isolation and fault correction. There are two mechanisms of transferring network management information from a managed entity to the manager: polling and the sending of alerts. Alerts are information delivered to a manager that is not the result of a specific query. Advantages and disadvantages exist within each method. Most network management systems use an optimal combination of alerts and polling. Doing so maintains the advantages of each and eliminates the disadvantages of pure polling [41].

Today, the process of fault management needs to be automated. Rapid and accurate correction of network problems need to be created by the network or by the end user. It is important to clearly define the problem so that it describes the root problem [5]. Although the entire network is violated, the network management application must work [38].

erally not be repaired until it is detected.

Polling many objects on many machines increases the amount of network management traffic flowing across the network. It is possible to minimize this through the use of hierarchies (polling a machine for a general status of all the machines it polls). Anyway, the response time will be a problem [41].

Sending alerts

The problem of sending alerts is potential loss of critical information and potentiality to over-inform the manager. They may also fail to be delivered, and critical information may be lost. Alerts are usually not to be delivered when the managed entity fails or the network experiences problems. It is important to remember that failing machines and networks cannot be trusted to inform a manager that they are failing.

Alerts in a failing system can be generated so rapidly that they impact functioning resources. An ”open loop” system in which the flow of alerts to a manager is fully asynchronous can result in an excess of alerts being delivered. There may be a situation where all available network bandwidth into the manager is saturated with incoming alerts and this could prevent the manager from disabling the mechanism generating the alerts. Methods are needed to limit the volume of alert transmission and to assist in delivering a minimum amount of information to a manager.

Alarm correlation makes it possible for network operators to more quickly determine the cause of an immediate problem. It does this by filtering secondary alarms, thereby allow-also topology information to identify the precise location of the problem.

Many devices have buffers reserved for logs. The buffer takes disk space from the other operations. When the buffer is full, new logs are overwritten to the oldest ones. If the buffer becomes full quickly, some important logs may disappear before they are noticed.

Fault detection

After detecting a fault, operators should as soon as possible find the root cause of the problem. They must determine what troubles it causes and to whom. At first the operator might try to find the parts of the network, where the fault can not be, by eliminating processes. These parts can be neglected. If there is a very serious and difficult problem, the network can be divided into smaller parts and the parts are inspected one by one [10].

Operators can by connectivity tests find the violated devices. By the same time can be detected if the fault is local or widespread. They can also test the data integrity to find out whether a part of the packets are lost by transmission. Delays are also tested, because some faults are results of excessive delays.

Ping

The packet inter net groper (Ping) is used for troubleshooting purposes. It sends an internet control message protocol (ICMP) loopback request packet to a target IP address. The packets from the main traffic, when the tracing has come to an end.

8.3 Operation management

Every device in the network (bridges, routers, hubs, servers, workstations) can be manageable and statistical information (sender, receiver, volume of transported information, time stamps, used resources) can be gathered. All terminal equipment do not need to be manageable [51]. For example workstations send alerts about violated connections, because they are shutted up and down continuously.

Operators decide what is the essential information to gather periodically and to analyze. Extra data takes CPU capacity from real network operations. Measuring and controlling should not happen at the cost of normal network operations. Sufficient basic measurements are however essential, so that the analysis can be done.

Accessibility

Measuring the accessibility of devices helps us to collect information about the status of the network; although it isn't a complete method. In general some points are selected to measure connections. After measurements the results shall be interpreted correctly. For example controlling the routers is not enough. If the setup of the router has been specified so that it gives the preference to packet switching, it will send packets normally although it is heavily loaded and it perhaps can not ble, dynamic routing tables must support sending request or routing information must be able to solve by tapping routing protocol. These requirements are not necessarily realized although SNMP is common. Analysis of the routing tables can concentrate on the parts of the network which are most susceptible to failures.

Controlling the traffic

Third method is to control traffic and analyze statistical distribution of the traffic. Statistical analysis gives also hints of malfunction in the network. 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. By controlling sizes of packets the dominating traffic in the network can be found. By finding out traffic peaks unnecessary load can be avoided.

Traffic control needs resources. Usually a separate control station is needed to collect and analyze traffic statistics. There should be a method to link control station so that the traffic information is collected from the network. Controlling traffic is however reliable and cost effective method to find out problems before they exist. Traffic controlling can be limited to the most important parts of the network [10].

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

Java Dynamic Management Kit
Sun Microsystems
JDMK is the first application using JMAPI technology. It helps to develop Web-based management services using Java agents or JavaBeans for Management -technology.
http://sun.com/software

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

CYBERMANAGE
Wipro Limited
CYBERMANAGE is a Web-based network manager. It includes development tools.
http://cybermanage.wipro.com/index1.html

SPECTRUM
CABLETRON Systems

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

[4] *. Managing network empowered businesses: Support for embattled network managers. *http://www.concord.com/library/wpapers/02.htm*.

[5] *. Proactive solutions to the five most critical networking problems, network general. *http://summitonline.com/netmanage/papers/netgen2.html*.

[6] *. Telecommunications billing systems: An overview. *http://suncom.bilkent.edu.tr/products-n-solutions/telco/billing_bkgrounder.html*.

[7] *. Voice and video over IP networks. *http://www.3com.com/technology/tech_net/white_papers/503016.ht*

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

[9] BACON, A. Expert systems use in fault management systems. *http://www.cbu.edu/ pong/624arb1.htm*.

[10] BALLEW, S. M. *IP-verkkojen hallinta Ciscon reittimillä*. Suomen Atk-kustannus Oy, Helsinki, 1998.

[11] BHOJ, P., SINGHAL, S., AND CHUTANI, S. SLA management in federated environments. In *Integrated Network Management VI* (Boston, USA, May 1999), pp. 293–308.

Management overview, 1992.

[16] Chapman, M., and Montesi, S. Overall Concepts and Principles of TINA. Tech. rep., TINA-C, Feb. 1995.

[17] Clark, D. The internet picture, shaping the internet of tomorrow. In *The New World of Information, International Seminar* (Helsinki, Mar. 1999).

[18] Darst, C., and Ramanathan, S. Measurement and management of internet services. In *Integrated Network Management VI* (Boston, USA, May 1999), pp. 125–140.

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

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

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

[22] Freeman, Roger, L. *Telecommunication System Engineering, 3rd ed.* John Wiley & Sons Inc, New York, 1996.

1999).

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

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

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

[30] LYNCH, C. A white paper on authentication and access management issues in cross-organizational use of networked information resources. *http://www.cni.org/projects/authentication/authentication-wp.html* (1998).

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

[32] MENSOLA, S. *Diplomityö: IP-verkon kommunikaatiopalveluiden hallinta*. Teknillinen korkeakoulu, Sähkötekniikan osasto, *http://kyyppari.hkkk.fi/ k23332/dippa/luku2.htm*, 1998.

[33] MUSCIANO, C. Network or nightmare? adding computers adds complexity. how do you keep up?

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

[38] ROSE, M. T. *The Simple Book, An Introduction to Management TCP/IP-based internets.* Prentice Hall, USA, 1991.

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

[40] STALLINGS, W. *SNMP, SNMPv2, and CMIP*. Addison-Wesley, 1993.

[41] STEINBERG, L. Techniques for managing asynchronously generated alerts. *RFC 1224* (May 1991), 24.

[42] STEVENSON, D. W. Network management — what it is and what it isn't.
http://netman.cit.buffalo.edu/Doc/Dstevenson (1995).

[43] STURM, R. Managing quality of service.
http://www.summitonline.com/service/papers/rick1-serv.html.

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

http://www.tmac.com/about/principles_of_tmac.htm (1999). apr 11, 1999.

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

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

[51] VINCENT, P. Network administration. *http://www.enic.fr/people/vincent/CNMI/6-NETADMIN.HTM*.

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

[53] WARRIER, U., AND BESAW, L. The Common Management Information Services and Protocol over TCP/IP (CMOT). *RFC 1095*.