LAPPEENRANTA UNIVERSITY OF TECHNOLOGY

Department of Industrial Engineering and Management

Thesis for the Master of Science in Technology

Service Management in IP Networks

Diplomityön aihe on hyväksytty tuotantotalouden osastoneuvostossa 10.11.1999.

Lappeenranta, 21. January 2000

Lasse Metso

Kiertokatu 6 C 13

53850 Lappeenranta

+358 50 570 2876

TIIVISTELMÄ

Tekijä: Lasse Metso

Tutkielman nimi: Palvelunhallinta IP-verkoissa

Osasto: Tuotantotalouden osasto

Vuosi: 2000 **Paikka**: Lappeenranta

Diplomityö. Lappeenrannan teknillinen korkeakoulu.

82 sivua, 5 kuvaa, 1 taulukko ja 3 liitettä.

Tarkastajana prof. Markku Tuominen.

Avainsanat: IP, Internet, palvelun hallinta, sääntöpohjainen verkon hallinta

Keywords: IP, Internet, service management, policy-based networking

IP-verkoissa tarjottavat palvelut ovat lisääntyneet, on tullut uusia kanavia, jotka tarjoavat IP-pohjaisia palveluja. Internet-palvelujen tarjonta on tullut mukaan kaapelitelevisio- ja matkapuhelinverkkoihin. Lisääntynyt palvelujen tarjonta ja kysyntä ovat lisänneet palvelujen hallinnan merkitystä. IP-verkoissa on ilmennyt turvallisuuteen, skaalattavuuteen ja palvelun laatuun liittyviä ongelmia. Palvelun laadun tärkeys painottuu reaaliaikaisuutta ja suurta kapasiteettia vaativissa sovelluksissa. Tulevaisuudessa IP-liikenteen on ennustettu kasvavan yli satakertaiseksi nykyisestä tasosta kolmen vuoden kuluessa. Tämän vuoksi on kehitetty uusi verkon ja palvelun hallintamenetelmiä, joista tässä työssä on tutkittu sääntöpohjaista verkon hallintaa.

ABSTRACT

Name: Lasse Metso **Title**: Service Management in IP Networks	
Department: Industrial Engineering and Management	
Year: 2000	**Place**: Lappeenranta
Thesis for the Master of Science in Technology. Lappeenranta University of Technology. 82 pages, 5 pictures, 1 table, and 3 appendixes. Supervisor Professor Markku Tuominen.	
Keywords: IP, Internet, service management, policy-based networking **Avainsanat**: IP, Internet, palvelun hallinta, sääntöpohjainen verkon hallinta	
The number of services in IP networks have increased. IP-based services have become available in cable television and in mobile systems. This has raised the importance of service management. In current IP networks, there are security, scalability and Quality of Services promlems. The Quality of Services becomes more important when realtime high-capasity applications are used. In future, the amount of IP traffic is estimated to increase over hundred times in three years. New network and service management systems have been developed. In this thesis policy-based networking is researched.	

ACKNOWLEDGEMENTS

This thesis was made in Telecommunications Software and Multimedia Laboratory of Helsinki University of Technology in Lappeenranta.

I thank my instructor Ossi Taipale and IPMAN project manager Jouni Karvo for their invaluable suggestions and guidance throughout my thesis work. Also, I would like to express my deepest gratitude to my supervisor Professor Markku Tuominen for his time and advises. Special thanks to everybody in the IPMAN project team.

Finally, the biggest thanks belongs to my wife Sari and our lovely daughtres Annika and Emilia for patience, understanding and support throughout this work.

I sincerely thank you all.

ABBREVIATIONS

ACL	Access Control List
AIN	Advanced Intelligent Networks
ASCII	American Standard Code for Information Interchange
CATV	Cable Television
CCB	Customer Care and Billing
CIM	Common Information Model
CMIP	Common Management Information Protocol
COPS	Common Open Policy Service
CoS	Class of service
DEN	Directory Enabled Network
DiffServ	Differentiated Services
DNS	Domain Name System
FIFO	First In First Out
FRC	Flow Rate Control
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IN	Intelligent Network
IntServ	Integrated Services
IP	Internet Protocol
IPsec	IP Security protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider

ITU-T	International Telecommunication Union - Telecommunication standards
LDAPv3	Lightweight Directory Access Protocol version 3
MIT	Massachusetts Institute of Technology
NCC	NetGuard Control Center, a product of Service Strategies Inc.
NFS	Network File System
NNM	Network Node Manager, a product of HP OpenView
OPS	Open Policy System, a product of IPHighway
PBN	Policy-Based Networking
PBNs	Policy-Based Networks
PBNC	Policy Based Network Control, a product of SwitchSoft System Inc.
PHB	Per Hop forwarding Behavior
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial-In User Service
Ret	Retailer Reference Point (in TINA)
RSVP	Resource ReServation Protocol
RTCP	Real-Time Control Protocol
RTFM	Real-time Traffic Flow Measurement
RTP	Real-time Transport Protocol
RTSP	Real-Time Streaming Protocol
SGML	Standardized Generalized Markup Language
SLAs	Service Level Agreements
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TINA	Telecommunications Information Networking Architecture
TMN	Telecommunication Management Network

ToS	Type of Service
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VoD	Video on Demand
VoIP	Voice over IP
WFQ	Weighted Fair Queue
WWW	World Wide Web
QoS	Quality of Service

1 INTRODUCTION

Internet is popular as the basic infrastructure in providing world-wide distributed services to end-users. Internet is an open and distributed environment which allows different types of service providers to provide different types of services on the network. (Kong et al. 1998, p.22)

The number of services deployed over an infrastructure that spans multiple control domains, such as e-commerce, web hosting etc., and their users is increasing. These end-to-end services require co-operation in internetworking between multiple organizations, systems and entities. Service providers' need to deploy interoperability, distributed scaleable architectures, integration and automation of network management systems. The management system must make management easy and flexible to service providers. The management system must also make service providers operations and end goals easier. (Bhoj et al. 1999)

Currently, there are no standard mechanisms to share selective management information between the various service providers or between service providers and their customers. Such mechanisms are necessary for end-to-end service management and diagnosis as well as for ensuring the service level obligations between a service provider and its customers or partners. (Bhoj et al. 1999)

In the current IP networks, there are unresolved questions in service management:

- How management information can be shared across administrative domain boundaries in a secure way? This capability is important when the 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.

In the future, there will more services in the networks. As a result, the system involved in providing services is expanding and is also becoming more complex. The ability to deliver voice, video, and data at higher speeds is also becoming a critical requirement. Different services and technologies over diverse telecommunications and computer networks make management of services difficult. (Udupa 1999, p. 4)

1.1 IPMAN Project

IPMAN project was started in January, 1999, by Telecommunications Software and Multimedia Laboratory of Helsinki University of Technology. The objective of the project is to research how the increase of IP-traffic affects the network architecture and management. The project will research and develop a network management paradigm for massive IP networks.

IPMAN project is financed by TEKES, NOKIA Networks Oy, Operations support Systems, and Open Environment Software Oy. Also, Taipale Engineering Ltd. has provided a researcher for IPMAN project.

It has been estimated that within 5-10 years the volume of TCP/IP-data traffic will increase from the present level 100 or even 1000 times, one of reasons being the increasing supply of new multimedia services. The dramatic increase of IP-based traffic will significantly change the traditional network architecture. The traditional telecommunication network management tools cannot be applied in managing the massive IP networks with the new architecture.

The target of the IPMAN project is to research and develop a network management paradigm for massive IP networks. Today's routed IP networks suffer from serious problems related to scalability, manageability, reliability and cost.

The solution of this problem is important for the business world as networks and distributed processing systems have become critical factors for success. This has led in companies and organizations to development of large and complex networks with an increasing number of applications and users. The new WWW and multimedia applications, faster data transmission in mobile networks and IP telephony require IP networks with higher capacity.

The effective use of network facilities in business can improve a competitive position, create new market opportunities and afford efficient communications between business units and customers. Automated network management is needed to ease management as networks have become larger and more complex.

Network management views the computing environment as a collection of co-operating systems connected by various communication mechanisms. Effective network management that adapts to business strategy requires the right abstraction level of information, information at the right time and information in an easy-to-use format. It 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. (Martikainen 1999)

The main effect of the Internet is that it enables the rise of virtual business and services. This means that there will be an explosion in data volumes - new Internet related services enable more customers added with more interactions with customers and more data per interaction. PC will no longer be the dominant access device, the network will be the center of everything. There will be more need for mobile and wireless infrastructure. The idea is that data will find you wherever you are. When there are no connectors, it means lighter, cheaper and simpler devices. (Herman 1999)

IPMAN project has studied the models developed to classify and order network management problems, described some protocols used for network management and some possible future trends in network management. IPMAN project has also studied the reference model suggested by professor Olli Martikainen. In this reference model network management is divided into four levels. The reference model has been developed further, the modified reference model can be seen in figure 1.

Content management
Service management
Traffic management
Network element management

Figure 1. Modified reference model.

All the layers of the reference model are studied in the project. The main focus is on the service and content management layers. The traffic and network element management layers have been under research for longer time by many researchers. Therefore it is most beneficial to concentrate on the two upper layers. Also, the present commercial network management tools have been under research.

1.2 Scope of the Thesis

Networks and distributed processing systems have become critical factors in the business world. The need for high capacity IP networks is growing because of the new World Wide Web (WWW) and multimedia applications, faster data transmission in mobile networks, and IP telephony. Today's routed IP networks suffer from serious problems related to scalability, manageability, reliability and cost.

In the past, network management in the telecommunication industry was mostly proprietary. These proprietary solutions were good enough for limited services and limited geographical coverage of telecommunications service providers. Services providers could control introduction and implementation of new technologies. However, deregulation has changed the situation. Deregulation has expanded the operating area of the service providers. They have to look beyond their own national borders. The tendency toward globalization has also increased competition. Also, it has made the management systems more complex. (Udupa 1999, p. 5)

World-wide demand for network services are growing exponentially. Also the data services, which the Internet offers is increasing. (Walrand and Varaiya 1996, p. 20)

The scope of this thesis is to focus on service management level of the reference model. The main focus is to find current problems in IP network, and to try to figure out problems, which might raise in future in the massive IP networks.

The main parts of this thesis are published on IP Network Management report (TML-B2). The publisher is Helsinki University of Technology, Department of Computer Science and Engineering, Telecommunications Software and Multimedia Laboratory.

1.3 Structure of the Thesis

Chapters 1 and 2 introduce main topics related to the thesis and IPMAN project. Chapter 3 discusses security requirements and problems of Internet. Chapter 4 discusses Customer Care and Billing systems and demands, while chapter 5 focuses on accounting management and Internet pricing models. Chapter 6 discusses current Internet service provisioning, while future service platforms are studied in chapter 7. For example, hybrid services are services used in or produced by at least two different networks.

In chapter 8, there is a closer look to Policy-Based Networking (PBN), which tries to solve the Quality of Service (QoS) in complex networks. In chapter 9 are conclusions in service management on the IP networks.

The results of the thesis are reported in nine chapters and the main the main contents are outlined in Figure 2.

INPUT		Chapter		OUTPUT
Impetus Project description Current problems	-->	Chapter 1 Introduction	-->	Research problem Traffic increase Reference model
Definitions	-->	Chapter 2 Services in the Network	-->	Services Convergence
Security problems	-->	Chapter 3 Security Management	-->	Security services
Routine works	-->	Chapter 4 Security Management	-->	Customer care systems Billing and payment
Usage measurement Pricing	-->	Chapter 5 Accounting Management	-->	Accounting systems Internet pricing
Service implementation	-->	Chapter 6 Service Provisioning	-->	WWW, HTTP, HTML Domain Name System DiffServ, IntServ Policies
New requirements	-->	Chapter 7 Future Service Platforms	-->	Web-based Policy-based Hybrid services
Best-effort	-->	Chapter 8 Optimizing Service Management with Policy-based Networking	-->	Priority Policy-based products
Convergence New services	-->	Chapter 9 Conclusions	-->	New service platforms and combination of them

Figure 2. Outline of the thesis.

2 SERVICES IN THE NETWORK

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

2.1 Services

There are many definitions of service:

- "A service is anything that a service provider determines that customers will wish to purchase and that the service provider is willing to supply." (Kong et al. 1998, p. 22)

- "A service is a set of functions offered to a user by an organisation." (Popien and Kuepper 1994, p. 889)

- "A service is an application with a well-defined interface and functionality." (Bhoj et al. 1999)

- Service is defined in International Telecommunication Union - Telecommunication standards (ITU-T) and the International Organization for Standardization (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." (Udupa 1999, p. 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 usage of the services. For example, customers do not want to use different login names and passwords when connecting to services. Microchip cards could be a method used for identification and authentication.

2.2 IP Networks and Convergence in Telecommunications

Massive IP network of the future might include the Internet, but also Cable television (CATV), telecommunication networks, such as Public Switched Telephone 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. (Mori et al. 1997, p. 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. (Walrand and Varaiya 1996, p. 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. (Walrand and Varaiya 1996, p. 20)

Media industry, telecommunications industry and computer industry are converging. Media industry produces the content, for example entertainment and publishing. Computer industry produce equipment and applications, which can make this content available for everyone. Telecommunications industry, both fixed and mobile, produces the connections to networks. See Figure 3. (Svanbäck 1999)

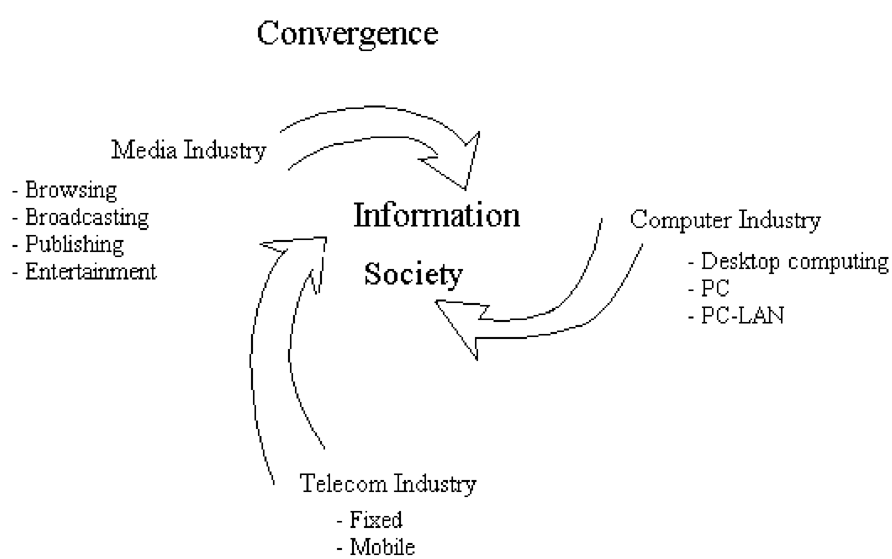

Figure 3. Convergence (Svanbäck 1999)

2.3 Service Providers

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

Service providers are increasingly using Service Level Agreements (SLAs) to define agreements for sharing resources with partners, as well as for offering service quality guarantees to customers. These SLAs contain details of information that are shared, and service level guarantees that are offered by the service provider. (Bhoj et al. 1999)

SLAs might help service providers to offer reliable services in a cost-efficient way. Service providers need to find new and effective ways to (Cisco 1999):

- deploy services more quickly,
- deliver guaranteed services through Service Level Agreements (SLAs),
- evolve from reactive network management to proactive service management, and
- reduce costs by automating network and service management.

2.4 Service Users

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

The service users want that the user interfaces of the services are logical and easy to use. They do not use services that are not operating properly. They also expect that the connection and the billing are reliable, installations are easy and software products are good.

3 SECURITY MANAGEMENT

Basic security services that are defined in ITU-T Recommendation X.800 are access control, authentication, confidentiality, integrity and non-repudiation.

Access control is the property of controlling network and computer resources in such way that only legitimate users can access them within their limits. One approach is to attach to an object a list which explicitly contains the identity of all permitted users an Access Control List (ACL). (Fraser 1997)

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. (Atkinson 1995)

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. (Atkinson 1995)

Integrity is the property of ensuring that data is transmitted from source to destination without undetected alteration. Integrity is often achieved as a by-product of providing confidentiality by encryption. (Atkinson 1995)

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. (Atkinson 1995) This is problematic, since it includes the assumption that no-one can falsely identify himself to the system. Consider a case where a cracker gains unauthorized access to a computer and then uses the computer owner's identity for a business transaction. If non-repudiation is assumed to hold, the other end may then claim that the owner of the computer did the transaction, which is incorrect. (Ellison and Schneier 2000)

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.

3.1 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. (Lynch 1998) Passwords, smart cards and certificates are used to authenticate a user. A user may have a right to use more than one name and identities established by multiple organizations (such as universities and scholarly societies). There might be an advantage if all the user information is available in same directory. All the applications could then use the same information. Users have to log in only once to be able to use all the services and resources. (Mensola 1998).

There are some basic requirements for authentication (Lynch 1998):

- the access management solution needs to work at a practical level,

- the solution needs to be secure,
-
- it should make access easier, minimizing redundant authentication interactions and providing user-friendly information resources,
-
- it needs to scale,
-
- it needs to be robust, for example, a forgotten password should not be an intractable problem,

- it must be able to recognize the need for a user to access a resource independent of his or her physical location (for example, a user must be able to connect to the Internet via a commercial Internet Service Provider (ISP), a mobile IP link, or a cable television Internet connection from home), and

- there should be a simple and well-defined (standard) interface between resource operator and licensing institution.

The basic access management problem is licensing agreements for networked information resources. The situations where institutions agree to share limited access are difficult. There is a need for fine-grained access control where institutions want to limit resource access to only individuals registered for a specific class, for example, when a class may be offered to students at multiple institutions. At present, most access to network information resources is not controlled on a fine-grained basis. There is a danger that by accommodating all the needs for fine-grained access management into the basic access management mechanisms will produce a too complex and costly system. (Lynch 1998)

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

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

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

An institution might choose to manage access by IP source address. IP source filtering means that packets are filtered on the basis of their source address. It does not seem to be a viable solution for access management. However, it may be very useful for some niche applications, such as supporting public workstations. It could be used more widely, although it cannot support remote users flexibly in its basic form. Most real-world access management systems are going to have to employ multiple approaches and IP source address filtering is likely to be one of them. (Lynch 1998)

3.2 Security Problems of Internet

There are security problems in the current Internet, for example, authentication, spying, and scalability.

3.2.1 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 Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) services being able to authenticate only to the granularity of host addresses and not to specific users. For example, an Network Filesystem (NFS) 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).

3.2.1 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.

3.2.3 Host-based Security Does not Scale

Host-based security does not scale well: as the number of hosts at a site increases, the ability to ensure that security is at a high level for each host decreases. Secure management of just one system can be demanding, managing many such systems could easily result in mistakes and omissions. A contributing factor is that the role of system management is often short-changed and performed in haste. As a result, some systems will be less secure than other systems, and these systems could be the weak links that will break the overall security chain. (Wack and Carnahan 1999)

4 CUSTOMER CARE AND BILLING

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

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

1980's was product oriented time in the telecommunication and data transfer market, whilst customer orientation is leading now. Marketing to the customers as well as the ability to sell more and the ability to high quality customer care are one of the key components to success. Also, it is important to get the products quickly to the market, and to be able to support existing and new services. A good customer care and billing system has to be flexible enough to fulfil these criteria. (IBM 1999)

Even electronic commerce depends on customer relationships says Lester Wanninger, professor at the University of Minnesota. It is important to teach how to make good customer relations for people going to start electronic commerce. Also in electronic commerce a company and a customer should handle all the communication channels. Electronic commerce has to implement functional processes of the company, information systems, databases, and other channels. It is important that a customer gets the same service from any service channel of the company. Ease of use brings more value to the customer. Also, in electronic commerce, the customer buys again only if the customer gets what was promised. WWW-pages can have effect on attitudes, intends, and shopping habits. High quality information, easy use, and new experiences, bind customers to services. Traditional media, such as TV, radio, and printed media are good in getting new customers, where as the Internet is good in keeping old customers. (Karonen 1999)

4.1 Customer Care

Customer care means maintaining customer services and customer relationships and answering routines, for example Help desk functions. Customer care links to the level of the offered service and the connection with the service level and the price of the service. (TAG 1999)

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

A good customer care system enables providing current and accurate information to the customers. It helps in delivering services when promised and resolving problems quickly and keeping customers informed, of the status of their orders. It also enables to 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.

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.

4.2 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 (Lidyard 1999). 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 Sun Microsystems (1999), some of the requirements of the billing systems of the future 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, and
- well-defined interfaces to allow easy integration and data sharing between business systems and the billing system.

4.3 Payment Mechanisms

Internet payment mechanisms can be grouped into three classes: electronic currency systems, credit-debit systems and systems based on secure presentation of credit card numbers. (Neuman and Medvinsky 1996)

Collecting and rating usage, tracking services, managing inventories and reconciling invoices are key features of accounting systems. (Lidyard 1999)

The safety issues are under discussion. Some payment mechanisms are totally anonymous and payers can not be tracked (such as E-cash -- electrical purse, where users 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. (Neuman and Medvinsky 1996)

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. (Crocker et al. 1995)

4.4 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. Anonymity is more important in some communities or for certain kinds of transactions, than they are in other communities. (Neuman and Medvinsky 1996)

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

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

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

Another threat could be pre-paid services. Customers' loyalty to service provider will become more difficult to check when he or she is using pre-paid services. Customers can easily change the service provider, because they can easily buy new pre-paid services from any other service providers. Also, cheating and lost income remains a problem. CCB systems can help to get over and to prevent cheating. New technologies such as certificate based authentication will open more accurate and faster charging for the services. (Kerttula 1998)

5 ACCOUNTING MANAGEMENT

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

- usage measurement,
- tariffing and pricing,
- collections and finance, and
- enterprise control.

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

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

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. (Udupa 1999, 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. (Kauffels 1992, 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 Simple Network Management Protocol version 3 (SNMPv3).

5.1 Accounting Systems

According to Busse (1998) an accounting system should fulfil some basic requirements. It should be:

- cost effective, performant, transparent,
- able to provide 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. (Busse 1998)

5.2 Internet Pricing

Internet pricing contains four basic elements (see figure 4).

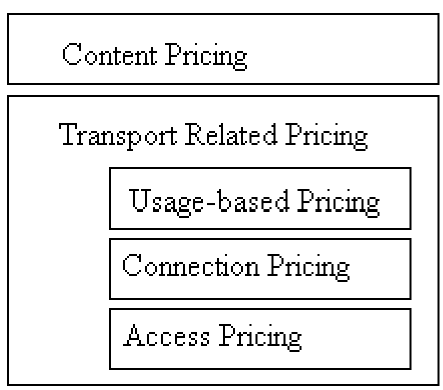

Figure 4. Components of Internet pricing (Stiller et al. 1998)

An access fee 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.

Usage fee can be used to charge services on time-, volume-, or QoS-basis. This fee determines the actual resource usage of a customer.

Content fee 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). (Stiller et al. 1998)

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, and QoS.

Accounting is usually based on mechanisms offered by commercially available routers and switches. The most commonly used approach employs packet filtering and statistical sampling. However, it is difficult to charge for usage-based traffic since the granularity of these methods is too coarse and the measurement overhead significant. (Stiller et al. 1998)

Another problem concerning accounting data collection in routers is whether packets should be counted on entry to or on exit from a router. (Mills et al. 1991)

For volume measurements the Internet Engineering Task Force (IETF) Real-time Traffic Flow Measurement (RTFM) working group has proposed standards to meter flows and to distribute this accounting information via Simple Network Management Protocol (SNMP). (Stiller et al. 1998)

The Remote Authentication Dial-In User Service (RADIUS) is a protocol specified by the IETF radius working group. It helps managing the Internet access links. Since these links are sensitive to security and accounting, a protocol is provided to authenticate dial-in users and negotiate configuration data. RADIUS services are implemented by most router manufactures. Accounting data can be collected on a time-, packet-, or octet-basis for a particular service. (Stiller et al. 1998)

6 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. (Harris 1996, p. 701)

6.1 Managing New Services

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

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 scratch. 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.

6.2 WWW Service Platforms

The World Wide Web (WWW) is an architecture for sharing information. The WWW provides a hypertext system linking people, computers, and information around the world. The WWW consists of information servers and client browser programs, linked together by a set of standards and agreements. The user runs the browser to access WWW servers, which deliver information to the requesting browser. (Stallings 1995, p. 87-88)

The key components of the WWW architecture are the Uniform Resource Locator (URL), the Hypertext Transfer Protocol (HTTP), and the Hypertext Markup Language (HTML). (Stallings 1995, p. 88)

URLs provide standardized specifications for objects or resources located on a network, detailing both the network address of the object and the protocol to be used to interact with that object. See table 1.

Table 1. The Uniform Resource Locator (URL) for various types of resources. (Stallings 1995, p. 88-89)

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

The URL is an enhanced Internet address. WWW clients use the URL to find an object on the network and select the proper protocol for interacting with that object. (Stallings 1995, p. 88-89)

The HTTP is a connection-oriented protocol designed for the rapid transport of files consisting of a mixture of text and graphics. HTTP is a protocol consisting of simple commands that support negotiation between the client and the server. This negotiation allows WWW browsers and servers to develop independently of emerging technologies because the negotiation process established a common basis of communication between the client and the server. (Stallings 1995, p. 89)

A universally understood language is needed when publishing information for global distribution. The publishing language used by the World Wide Web is HTML. (W3 1998) HTML is a standardized document tagging language, based on the Standardized Generalized Markup Language (SGML). (Stallings 1995, p. 89-90)

According W3 (1998), HTML gives authors the means to:

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

HTML has been developed with the vision that all manner of devices should be able to use information on the Web: PCs with graphics displays of varying resolution and colour depths, cellular telephones, hand held devices, devices for speech for output and input, computers with high or low bandwidth. HTML now offers a standard mechanism for embedding generic media objects and applications in HTML documents. The object element provides a mechanism for including images, video, sound, mathematics, specialized applications, and other objects in a document. It also allows authors to specify a hierarchy of alternate renderings for user agents that don't support a specific rendering. (W3 1998)

6.3 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. (Smith 1998, p. 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. (Smith 1998, p. 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 card. 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. (Smith 1998, p. 6)

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

6.4 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. (LDAP 1998)

There is a need to consolidate directory data. When intranet systems are expanded to extranet systems, there is a problem of combining different types of directories and databases. A standardized model of directories will help this integration. Decreasing the number of directories means cost savings, higher data quality and lower security hazards (LDAP 1998). Development of an application is also easier if all the information is available in directories using standardized protocols (Mensola 1998).

6.5 Quality of Services Mechanisms in Internet

New demand on the Internet service is to guarantee the Quality of Service (QoS). Internet Protocol (IP) based applications have used best-effort method in order to approach QoS. Current Internet architecture does not support QoS guarantees. Multimedia applications, such as internet telephony, Video on Demand, video conferencing, groupware, distance education, and remote health care, are examples of applications which have QoS requirements. QoS requirements of applications and services will lead to policies used to manage IP based networks, and specify Service Level Agreements (SLAs) with Internet Service Providers (ISPs). (Blight and Hamada 1999, p. 813)

The Internet Engineering Task Force (IETF) has put a lot of effort in defining a scalable Quality of Services (QoS) architecture for the Internet. So far, no consistent solution has been reached, but there is a lot of useful building blocks.

There are at least three approaches being taken to meet QoS issues in the IP networks:

- Differentiated Services,
- Integrated Services, and
- policies.

Classes of Services (CoS) is included to the work of IETF Differentiated Services (DiffServ) working group. Resource Reservation Protocol (RSVP) is included to the work of IETF Integrated Services (IntServ). Policies can belong to both DiffServ and IntServ.

6.5.1 Integrated Services

The Integrated Services working group in the Internet Engineering Task Force (IETF) has developed an enhanced Internet service model called Integrated Services that includes best-effort service and enhanced best-effort service. (Braden et al. 1994)

The enhanced best-effort service will enable IP networks to provide quality of service to multimedia applications. Resource ReSerVation Protocol (RSVP), together with Real-time Transport Protocol (RTP), Real-Time Control Protocol (RTCP), and Real-Time Streaming Protocol (RTSP), provide a working foundation for real-time applications. (Schulzrinne et al. 1996a and 1996b)

IntServ allows applications to configure and manage a single infrastructure for multimedia applications and traditional applications. It is a comprehensive approach to provide applications with the type of service they need and in the quality they choose. RSVP is the network control protocol that allows data receiver to request a special end-to-end quality of service for its data flows. Real-time applications use RSVP to reserve necessary resources at routers along the transmission paths so that the requested bandwidth can be available when the transmission actually takes place. RSVP is a main component of the future Integrated Services Internet which can provide both best-effort and enhanced best-effort services. (Braden et al. 1994)

6.5.2 Differentiated Services

Internet users have diverse needs. Differentiated Services (DiffServ) is a new way to satisfy those needs by providing QoS in the Internet. The basic idea in DiffServ is to get rid of the complex per-flow treatment in the core network and instead offer only a small number of service classes (CoS). The core routers do not need to keep state, because CoS of each packet is encoded within the IP header. This is done in the field Type of Service (ToS). (Isomäki and Tuominen 1999, p. 5)

Classification to CoS is simple, because ToS field is short and fixed. The first 6 bits of the ToS byte are defined as a DiffServ field, and the value of the field is interpreted as a DiffServ code point. The code point is mapped at each router to a certain Per Hop forwarding Behavior (PHB), i.e. traffic class. (Isomäki and Tuominen 1999, p. 5)

It is important to know how much traffic is allowed to each PHB classes. Marking the packets, as well as policing and shaping the individual flows, is performed at each DiffServ domain boundary according to the service level agreements (SLAs) between the customers and the service providers. (Isomäki and Tuominen 1999, p. 5-6)

DiffServ is able to provide both qualitative and quantitative end-to-end services. Quantitative services can be offered by limiting the maximum amount of traffic in a certain PHB class and giving the class adequate resources at each link in the core. Quantitative service is simplest to offer in a point-to point fashion so that the required resources can easily be calculated. (Isomäki and Tuominen 1999, p. 5-6)

The advantages of DiffServ over IntServ are:

- packet forwarding is simpler and more scalable,
- requires less from routers, and
- is easier to deploy. (Xiao and Ni 1999)

7 FUTURE SERVICE PLATFORMS

Current architectures in service management are based on management protocols like Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP) or trouble ticketing interface. (Busse 1998, p. 167)

7.1 Web-based Architecture

In the Web-based architecture the customer downloads an applet that communicates with a proxy server in the service providers domain. The proxy server interacts with the actual inter-domain management system. It is possible to use standard gateways like IBM Webbin or build a service specific solutions in order to simplify the funtionality at the customer site. This makes download times shorter and there is less need for code. (Busse 1998, p. 167)

The inter-domain management system implements the interactions with co-operating service providers. Requests to the local domain are processed by the intra-domain management system and then forwarded down the hierarchy to the network managers and finally to the network element managers. (Busse 1998, p. 167)

Security restrictions in browsers do not allow applets to interact with local resources, i.e. with the file system or local network nodes. In Netscape Communicator, the security restrictions can be configured based on the right to trust relationships with the applet provider. Signed applets can be given the right to access the local network. This provides also a network management solution for customer premises network. (Busse 1998, p. 167)

Figure 5 shows a web-based service management architecture. CPN is Customer Premises Network and PN is Public Network.

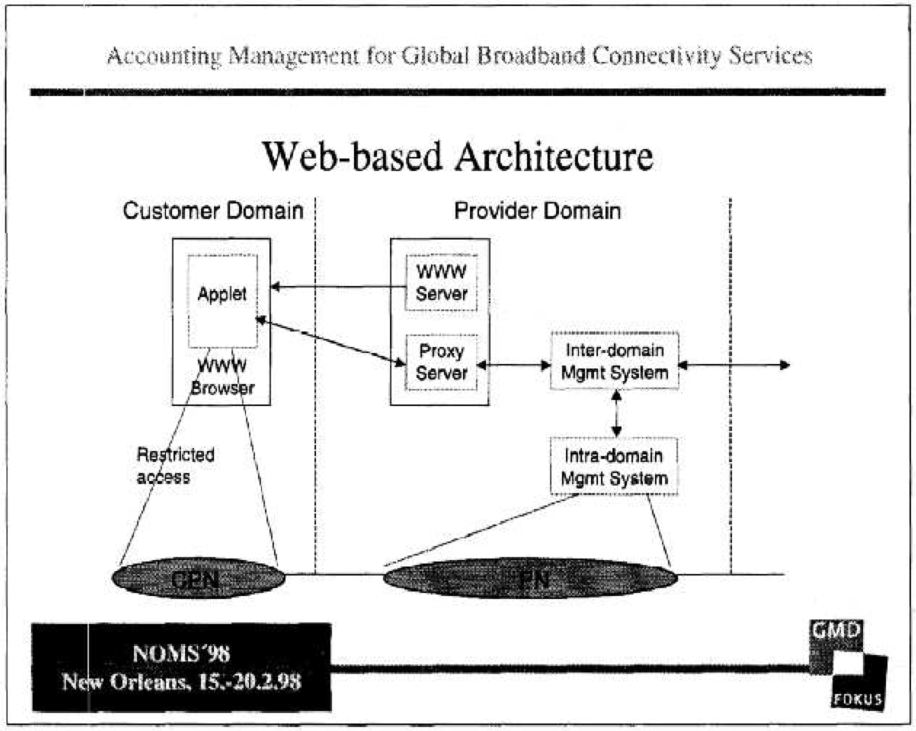

Figure 5. Web-based service management architecture. (Busse 1998, p. 167)

This prototype has been developed providing a web based interface covering subscription management, configuration management, alarm surveillance, trouble ticketing as well as accounting management. The usage of the web and Java (applets) simplifies the service interaction between the customer and the service provider. It will reduce the cost on both sides. For service provider it is important to automate the customer care process in order to cut the costs to survive in the emerging competitive market. (Busse 1998, p. 168)

7.2 Policy-Based Networking

Policy is a combination of rules and services where rules define the criteria of resource access and usage. Policies can contain other policies, they allow to build complex policies from a set of simpler policies, so they are easier to manage. They also enable to reuse previously built policy blocks. (Strassner and Ellesson 1999)

Policy groups and rules can be classified by their purpose (Moore et al. 1999):

- Service Policies describe services available in the network. These services will be available for usage policies. For example, QoS service classes (VoiceTransport, VideoTransport, ..) 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 can ask the user to call the system administrator, if a device fails between 8am and 5pm. Else the user should call the HelpDesk.

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. (Blight and Hamada 1999)

7.2.1 Policies, Conditions and Actions

A policy is the combination of rules and services where rules define the criteria for resource access and usage. Each policy rule is comprised of a set of conditions and a corresponding set of actions. The conditions define when the policy rule is applicable. Once a policy rule is so activated, one or more actions contained by that policy rule may then be executed. These actions are associated with either meeting or not meeting the set of conditions specified in the policy rule. (Strassner and Ellesson 1999)

Policies can contain policies. This notion enables complex policies to be built from a set of simpler policies. It also enables reuse of policy building blocks (policy rules, conditions, and actions). It is important to use and put into practice first as simple as possible definition of policies before more complicated definitions of policies are deployed. Otherwise, it will be much harder to achieve interoperability of policy servers, or other policy entities. (Strassner and Ellesson 1999)

Policy is comprised of three functions according Strassner and Ellesson (1999):

- Decision-making: This compares the current state of the network to a desired state described by an application-specific policy and desides how to achieve or maintain the desired state.

- Enforcement: This implements a desired policy state through a set of management command, when applied to network elements, these management commands change the configuration of the device using one or more mechanisms. These mechanisms may be vendor-specific.

- Monitoring: This is an on-going active or passive examination of the network and its constituent devices for checking network health, whether policies are being satisfied, and whether clients are taking unfair advantage of network services.

Policy conditions consist of two parts, a policy condition type and a policy condition element. A policy condition type is a set of predefined conditions that can be attached to a policy rule for evaluation. This set of conditions represent common conditions that all network vendors can implement. A policy condition element is a policy condition type instance that is being evaluated. Policy condition elements are related together to form a Boolean expression. (Strassner and Ellesson 1999)

A policy action is the changing of the configuration of one or more network elements in order to achieve a desired policy state. This policy state provides one or more behaviors. As with policy conditions, a policy action is comprised of two parts, a policy action type and a policy action element. The policy type defines a set of operations or treatments that can be given to traffic flowing into the network element that is vendor-independent. (Strassner and Ellesson 1999)

7.2.2 Policy Decision, Behavior and State

A policy decision is the abstraction of activating and evaluating one or more policy rules. Each policy rule is interpreted in the context of a specific request for accessing and using one or more resources. It connotes taking one or more pre-determined actions based on whether or not a given set of policy conditions where satisfied. (Strassner and Ellesson 1999)

A policy mechanism is a set of vendor-specific commands that configures a network element to put a policy rule into effect. A policy behavior controls how traffic is treated, what network resources must be utilized, and what network services are provided. Policy behaviors define one or more mechanisms that are used to implement the policy. Therefore, different devices can carry out the same policy using different behaviors. (Strassner and Ellesson 1999)

For example, a router might permit or deny forwarding of traffic based on source and destination address, source and destination port number, protocol type and options, and other factors specific to vendor implementations, such as host name or time of day. Also, a router might use a behavior that permit or deny access to a request resource or service, encrypt the header or the payload, mark or remark the packet, start or stop accounting or auditing, and start or stop logging. (Strassner and Ellesson 1999)

A policy state is a description of the setting of one or more network elements. These settings correspond to providing the set of services to be provided by the network. For example, a Service Level Agreement (SLA) can describe services contracted for by subscribers, this corresponds to a state that various network elements must be put into in order to provide those services. (Strassner and Ellesson 1999)

7.2.3 Policy Evaluation, Monitoring and Conflicts

Policy evaluation is the determination of whether or not the network is in a desired policy state. This is usually determined by processing static or dynamic data against one or more policy rules, the key point being that the decision is made by comparing definitional data stored in the policy repository with current data from the network that does not have to be stored in the policy repository. If it is found that the network elements are not in the desired policy state, then one or more policy actions will be taken to move the network elements from their current state to the desired state. This is called policy enforcement. (Strassner and Ellesson 1999)

Policy enforcement is the action of placing the network in a desired state using a set of management commands. When this definition is applied to network elements, these management commands change the configuration of the devices using one or more mechanisms. Enforcement is carried out in the context of a policy rule. (Strassner and Ellesson 1999)

Policy monitoring is an on-going active or passive examination of the network and its constituent devices for checking network health, whether policies are being satisfied, and whether clients are taking unfair advantage of network services. This is done for one or more of the following reasons: to ensure that clients are receiving the services that they have contracted for, to monitor network statistics as part of checking network health, to monitor network statistics as part of checking whether policies that are currently in use are being satisfied, or to ensure that clients of a given set of policies are not abusing their privileges. (Strassner and Ellesson 1999)

7.3 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. (Vanecek et al. 1999, p. 102)

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. The PSTN provides a reliable, available and ubiquotous system, with guaranteed Quality of Service (QoS). Gbaguidi et al. claim that the PSTN and Internet are far from being an ideal ground for developing future hybrid services when taken separately. However, if coupled together they can complement each other effectively. (Gbaguidi et al. 1999, p. 9)

The PSTN includes a powerful service creation and provision platform called Intelligent Network (IN). The design of IN follows a simple principle: separation of service-specific software from basic call processing. Before IN services were incorporated in the network switches in a manner that was specific to each manufacturer. Introducing new services required the modification of software in every switch in the network. It took years to complete such a process, and it made network operators dependent on their equipment suppliers. The IN reduced a great deal of this dependency by using service-specific software. (Gbaguidi et al. 1999, p. 9)

The Internet has no global service creation and provision framework. New services can be created by any user that can afford a server. Creating new services implies developing a distributed application that must be installed and executed in the terminals and servers. Internet applications take advantage of intelligent terminals and powerful user interfaces. (Gbaguidi et al. 1999, p. 9)

Gbaguidi et al. (1999, p. 9-10) claim that hybrid services are expected to play a very important role in the years to come. This is due to both the desire of users to integrate the ways they communicate and the willingness of service providers to differentiate their offers from their competitors. Also, smart cellular phones are expected to fuel the integration of services.

There has been extensive work toward validation of services in the IN or Telecommunications Information Networking Architecture (TINA) services, but there has not been much work on the application of formal methods of Internet to the development of Internet services or hybrid services. (Logean et al. 1999, p. 134) There are main questions:

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

7.3.1 Interworking of Connect-Oriented and Connectionless Services

Hybrid services combine connection-oriented and connectionless techniques. There is no commonly accepted call model for hybrid services. Telecommunications industry use formal methods based on specific call models, such as those used in the IN. Formal methods were applied to standardized architectures such as the IN in which all services were structured in a similar way by using service-independent building blocks, the application and reuse of formal approaches was significantly easier. (Logean et al. 1999, p. 134)

The lack of a common call model for hybrid services implies that most of the work of applying formal techniques to telecommunication systems has to be revised and checked to see whether and how it can be reused and adapted for hybrid services. (Logean et al. 1999, p. 134)

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

In the Internet services are implemented in end users systems, while the telecommunications community normally has a network-centric vision where services are implemented in the network. These two different views of service control may converge to a service-centric vision for the deployment of hybrid services. (Logean et al. 1999, p. 134)

For the use of formal methods in development of hybrid services, it is necessary to consider software running at the user’s site and in the network. (Logean et al. 1999, p. 134)

7.3.3 Decreased Service Lifetime and Time to Market

Introducing new services in a telephone or cellular network was a slow process, and the deployed of services were offered for a rather long period. Compared to typical telecommunication services, the time to market of Internet and hybrid services is significantly redused. 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. (Logean et al. 1999, p. 134-135)

7.3.4 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. (Logean et al. 1999, p. 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. (Logean et al. 1999, p. 135)

7.4 Demands for Future Service platforms

Svanbäck (1999) claims that mobile, fixed and Internet networks converge 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 devices. The telecommunications industry, the computer industry and the media industry are melting together in the market convergence. Martikainen (1999) claims that convergence 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.

There are some demands that are expected for the future service platforms. The service platforms should

- provide extensive network services for converging networks (Svanbäck 1999),
- enable fast time to market for new services,
- provide ease of deployment, configuration, and management,
- use the open, modular, distributed and standardised architecture,
- make use of commercially available hardware and software components
- ensure application-independent high quality of service and fault tolerance,
- ensure high usability and appropriate diagnostics (Martikainen 1999), and
- enable the use of advanced charging mechanisms (Kurki 1999).

8 OPTIMIZING SERVICE MANAGEMENT WITH POLICY-BASED NETWORKING

The current IP architecture does not support any QoS guarantees because routing is based on a best-effort principle. This means that each packet of information is treated independently and processed in the order of arrival. QoS management can be assured by putting high priority or giving enough bandwidth to application flow. This can be done with Policy Based Networking (PBN). PBN uses policies in controlling the traffic of the network.

8.1 Queuing Techniques Used in Policy-based Network Management

Queuing techniques make quality of services (QoS) possible. Every router and switch on the network has a queue in which each packet is put before it is processed by the router or switch. If these queues become full, the device drops packets. Which packet it decides to drop is based on the queuing technique used. (Infoworld 1999b)

The most basic queuing technique is the First In First Out (FIFO). IP's best-effort abilities allow traffic flow with FIFO, and the routers and switches are performing only FIFO. The traffic runs through the network in big bursts, and there is no point at which it maintains any stability. If this kind of traffic is a voice or video transmission, the quality would be miserable, there would be too much delays and too many lost packets. In FTP this lack of quality is not so important, but download times will increase, because TCP can require retransmissions of packets. (Infoworld 1999b)

Cisco's serial interface uses the Weighted Fair Queue (WFQ) as default queuing technique. The queue is designed to maximize the priority of interactive traffic, such as Telnet session. It allows plenty of space to high-bandwidth flows, such as FTP download. WFQ is also designed to prioritize traffic based on the IP header Type of Service (ToS) bits. WFQ is prone to a burst-type nature, as are most queuing techniques in routers. (Infoworld 1999b)

Packeteer's PacketShaper 4.0 uses Flow Rate Control (FRC). FRC is an inspection technology to examine and modify packets as they flow through PacketShaper. This allows the PacketShaper to control when the sender and receiver expect to send and receive traffic. Instead of letting the traffic build up in queues, it is shaped only to be sent when it is expected. This kind of control is suitable to real-time traffic flow across networks. FRC is a vast improvement over WFQ, but it is only required in situations in which the requirements for Quality of Services are very stringent. (Infoworld 1999b)

8.2 Standardization of Policy-Based Networking

Policy-Based Networking (PBN) standardization is controlled by the Internet Engineering Task Force (IETF). IETF has a Policy Framework working group. (Anonym 1999a)

8.2.1 The Internet Engineering Task Force

IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the

Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas. Much of the work is handled via mailing lists. The IETF holds meetings three times per year.

The IETF working groups are grouped into areas, and managed by Area Directors. The Area Directors are members of the Internet Engineering Steering Group (IESG). Providing architectural oversight is the Internet Architecture Board, (IAB). The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is a member of the IAB.

The IETF areas are

- Applications Area,
- General Area,
- Internet Area,
- Operations and Management Area,
- Routing Area,
- Security Area,
- Transport Area, and
- User Services Area.

The Internet Assigned Numbers Authority (IANA) is the central co-ordinator for the assignment of unique parameter values for Internet protocols. The IANA is chartered by the Internet Society to act as the clearinghouse to assign and co-ordinate the use of numerous Internet protocol parameters. (Anonym 1999a)

8.2.2 Policy Framework

Policy-Based Networking standardization is done in Policy Framework working group. The Policy Framework belongs to Operations and Management Area.

There is a need to represent, manage, share, and reuse policies and policy information in a vendor-independent, interoperable, and scalable manner. This working group has three main goals. First, to provide a framework that will meet these needs. Second, to define an extensible information model and specific schemata compliant with that framework that can be used for general policy representation called the core information model and schema. Third, to extend the core information model and schema to address the needs of QoS traffic management called the QoS information model and schemata.

The viability of the framework will be proven by demonstrating that high-level policy information can be translated into device configuration information for network QoS applications. A secondary goal of this framework is to show that this general development process can be extended to other application domains. (Anonym 1999b)

The objectives of Policy Framework working group are to:

- Identify a set of representative use cases to guide us in defining a policy framework, information model, and schemata to store, retrieve, distribute and process policies. These use cases should map to a set of policy rules, and aid us in defining the composition of policies.

- Define a framework for intra-domain policy definition and administration for a heterogeneous set of Policy Decision and Enforcement Points. Here, "intra-domain" refers to policy components that are all under the same administrative control. The framework will be shown to be able to be used to represent, distribute, and manage policies and policy information in an unambiguous, interoperable manner in a single administrative domain. This framework will be applied to network QoS.

- A general information model, derived from the Common Information Model (CIM) and Directory Enabled Network (DEN) policy model, will be produced. This is intended to serve as a generic means for representing policies and policy information. In addition, a mapping of this information model to a form that can be implemented in a directory that uses Lightweight Directory Access Protocol version 3 (LDAPv3) as its access protocol will also be done.

- Refinements to the above, for representing signaled and provisioned QoS, will be done. That is, both the information model as well as the schema will be extended to focus on network QoS. This will also be used to prove the general extensibility of the model.

- A key part of demonstrating that this model can provide end-to-end translation of high-level policy specifications to device configurations is to ensure that the information model and schemata are compatible with and can use the information developed in other working groups.

- Policy information may be communicated using several protocols. The Common Open Policy Service (COPS) protocol, being developed in the Resource Allocation Protocol (RAP) working group, is an example of one such protocol. The Policy Framework working group will work with the RAP working group to define usage directives for use of the COPS base protocol to support policy information exchange transactions within the framework being standardized in the Policy Framework working group.

- The Policy Framework working group will work closely with the IPsec Working Group to ensure that the IP Security protocol (IPsec) data model fits and can be supported within the general framework defined by the Policy Framework working group.

- The Policy Framework working group will work with other working groups as needed to ensure that the framework, information model, and specific schemata produced meet the needs of these working groups.

- The charter specifically excludes protocol definition and schema attributes or classes that are vendor-specific, although the schema defined in this group will be defined in a way that is extensible by specific vendors.

The Policy Framework working group has a goal to get Policy-Based standardization complete in March 2000. (Anonym 1999b)

8.3 Policy-based Network Management Software

There are several policy-based networking products, for example:

- Aelita Delegation Manager 2.0,
- Cisco Systems Inc., QoS Policy Manager 1.1,
- COMPAQ, DIGITAL clearVISN policy-based network management,
- FORE SYSTEMS, Policy-based Network Management,
- HP, OpenView PolicyXpert,
- IPHighway, Open Policy System 1.0,
- Packeteer Inc., PacketShaper 4.0,
- SSi Service Strategies Inc., NetGuard NT-based Policy Server Technology, and
- SwitchSoft System Inc., Policy Based Network Control (PBNC) 1.41.

Aelita Delegation Manager (Aelita DM) is an administrative tool for medium- and large-scale on Windows NT- and Windows 2000-based network systems. Aelita DM allows organization to create a Windows 2000-like hierarchical administrative structure, to distribute and to delegate administrative privileges to local administrators and help desk personnel across an enterprise network. (Aelita 1999)

Cisco Systems Inc. has a product called QoS Policy Manager. QoS Policy Manager can bring QoS to small Cisco-centric network, but it only supports Cisco devices. It is easy to use, and it supports all of the queuing techniques in Cisco routers. It does not use distributed policy servers, so it is not the best solution in reliability problems. (Infoworld 1999a)

COMPAQ has DIGITAL's clearVISN policy-based network management. ClearVISN is a key building block in DIGITAL's enVISN network architecture. It simplifies the configuration and management of complex networks, setting policies that distributed agents use to control and monitor the devices and technologies in networks. It provides centralized, policy-based administration with distributed enforcement through intelligent devices. ClearVISN can be integrated with network management systems on Windows 95, Windows NT, and UNIX. (Compaq 1999)

FORE SYSTEMS' policy-based network management system is recommended to implement together with Application Aware Networking switches. The administrator can select an application profile by using a graphical Java-based policy console. The profile is deployed to Application Aware ESX switch, which can automatically implement the policy. (Fore 1999)

Hewlett-Packard's (HP) OpenView PolicyXpert is integrated with HP OpenView Network Node Manager (NNM) for centralized management of all tasks and use a common Graphical User Interface (GUI). PolicyXpert includes a console to define policies, a server to administer them, and agents to enforce them. The policy server stores policies, distributes them to policy agents, and maintains the results of the policy enforcement done by each agent. Policy agents run either on the network resources itself, or in proxy to one or more of them. A policy server distributes policies to each policy agents using the Common Open Policy Service (COPS) protocol. An agent transforms the high-level policy rules into configuration details that are then applied to network resources. PolicyXpert 1.0 runs on the Windows NT 4.0 platform, and the next release will support the Solaris and HP-UX platforms. (HP, 1999) PolicyXpert can be used to administer many devices, but setting it up for a large network is not easy because it can not autodetect the network.

In many situations, PolicyXpert will provide adequate prioritization, but for carrier situations in which voice and video are on the network, it is not the best solution. PolicyXpert has a good architecture and core structure. (Infoworld 1999a)

IPHighway's Open Policy System (OPS) 1.0 consists of IPHighway Policy Administrator, IPHighway Policy Server, and IPHighway Policy Client. OPS is designed to support enterprise organisations, network and internet service providers, and telecommunications companies. OPS controls QoS mechanisms in standard-compliant routers, automatically configuring network resources to accommodate mission-critical and time-sensitive applications. 3Com is now IP Highway's strategic partner in Policy-Based Networking. (IPHighway 1999) OPS is easy to use, and it uses a distributed design. It is a good solution for complete control of an enterprise or carrier-class network. (Infoworld 1999a)

Packeteer Inc. has a product called PacketShaper 4.0. The PacketShaper is a hardware-based inspection device that distributes bandwidth per instructions. It is suitable for enterprise resource planning and other time-sensitive applications when guaranteed delivery is needed. PacketShaper provides detailed flow-based traffic management, supports unusual protocols, and offers policy suggestions. (Infoworld 1999a)

SSi Service Strategies Inc. has NetGuard NT-based Policy Server Technology. NetGuard's policy server is called NetGuard Control Center (NCC). NCC is a Windows NT-based system with a unifier user interface that integrates and centralizes QoS services. NCC complies with Microsoft's Active Directory Service standard what enables it to import the network organization and hierarchy from Windows NT, Novell, Unix, and Netscape servers that are located anywhere on the network. (SSi 1999)

SwitchSoft System Inc. has Policy Based Network Control (PBNC) 1.41. It is an architecture that enforces network logon in real time. PBNC automatically configures the network infrastructure based on assigned user security policies. With PBNC it can be set security and QoS requirements. PBNC needs Windows NT 4.0 server, while clients can run on Windows 95, 98, NT 3.51, and NT 4.0. All network connections for supported client workstations must be made using Cisco Catalyst 5000 series switches. (SwitchSoft 1999)

8.4 A Closer Look to HP OpenView PolicyXpert

HP has released the OpenView PolicyXpert, with customer shipments beginning November 1999. PolicyXpert provides a policy-based network management solution to control application and network Quality of Service (QoS). PolicyXpert 1.0 allows the user to assure Service Level Agreements (SLAs) by automating the configuration and control of network bandwidth.

HP OpenView PolicyXpert, version 1.0, focuses on Quality of Services management of an enterprise network.

PolicyXpert can activate policies when wanted. In appendix 1 there are time and date conditions that can activate the policies. Also, PolicyXpert can activate policies in different conditions, i.e. where the traffic flows from. In appendix 2 there are all conditions in which PolicyXpert can activate policies. Traffic characteristics are shown in appendix 3.

HP claim in homepages that PolicyXpert can be implemented to Windows NT, W2000, Solaris, and HP-UX servers in future, but PolicyXpert 1.0 supports only Windows NT. Also, a policy server must be Windows NT version 4.0 Server and service pack 4.0 or later. Also, it supports Intel's and 3Com's Network Interface Cards (NICs). (HP 1999a)

8.4.1 PolicyXpert Scenarios

HP has created scenarios how policies can be used. There are five different scenarios. (HP 1999a)

First scenario is to assure bandwidth for ERP, financial, or other mission-critical applications. The problem is that many applications at branch offices rely on servers at a central site. These applications in combination with e-mail and web result in the lion's share of the overall data produced and consumed by the remote site flowing across the corporate WAN. IP networks provide best-effort service for all traffic. This is adequate when the total traffic does not exceed the capacity of the network. When traffic exceed the capacity of WAN, important traffic competes with less important traffic for the limited bandwidth. The solution for this is to get enough bandwidth or to control how to use the existing bandwidth. PolicyXpert can limit the bandwidth consumed by less important applications, and assure bandwidth for the most important applications. PolicyXpert can assure bandwidth across slower-speed links connecting offices through its Committed Rate policy type. Committed Rate policies deployed to traffic shapers identify important application flows and configure aggregate bandwidth for them. Additional rules in these policies identify unimportant flows and limit them to a small amount of bandwidth. The remaining application flows live within the remaining, available bandwidth.

Second scenario is to reduce congestion by controlling bursty applications. PolicyXpert can clamp down bandwidth hogs that are not delay-sensitive, e.g. FTP, HTTP,e-mail, etc.

Third scenario is to enable rollout of new video or voice applications. PolicyXpert can avoid the need of add bandwidth, to do manual recofiguration, or to prevent the use of new multimedia.

Fourth scenario is to establish classes of services with Service Providers. Specific application flows can be marked for high priority.

And at last the fifth scenario is to give priority treatment to selected e-commerce users. This prioritization is based on managing URLs. (HP 1999a)

8.4.3 PolicyXpert for Cisco Routers

Cisco Proxy Agent Configuration is a utility that allows to configure the Cisco proxy agent. During initial PolicyXpert installation, the Cisco Proxy Agent Configuration utility collects information about managed devices and allows to customize the agent's behavior to specific needs.

The utility can also be run as a standalone application after initial installation to change agent configuration and to configure new devices. Cisco Proxy Agent Configuration can be run on any machine where agents are installed.

The Cisco proxy agent supports only policy type priority and committed rate. Supported policy conditions are IP address (source and destination), IP subnet (source and destination), IP port (traffic with a specified port number in either the source or destination port), and Type of Service (IP precedence). Cisco series 2600, 3600, 4500, and 7000 routers are the only supported devices. (HP 1999b)

8.4.4 PolicyXpert for PacketShapers

The Packeteer Proxy Agent allows to manage the PacketShapers in the network with policies. Each PacketShaper has two resources that can accept policies - inbound and outbound. Policies applied to the inbound resource affect traffic coming into network across the PacketShaper. Policies applied to the outbound resource affect traffic leaving network across the PacketShaper.

PolicyXpert policies are converted to PacketShaper matching rules. Each rule of a PolicyXpert policy may map to one or more PacketShaper matching rules. The PacketShaper matching rules are named consistently with the PolicyXpert policy and rule names.

The Packeteer Proxy Agent periodically polls the PacketShaper to ensure that no changes have been made to the PolicyXpert policies that it has deployed. If it detects any changes to the deployed PolicyXpert policies, it will redeploy the current effective policy for the PacketShaper.

The Packeteer Proxy Agent supports only the PacketShaper 2000 and PacketShaper 4000, versions must be 4.10 or later.

The Packeteer Proxy Agent supports the Priority, Committed Rate, and Per-flow Assured Rate policy types. The Priority policy type can use DiffServ mechanisms, IEEE 802.1p packet marking or IP Type of Service (ToS) precedence marks. The Committed Rate policy type allows the administrator to construct QoS policies that identify important application flows and configure aggregate bandwidth for them. All condition types except for VLANID are supported, see appendix 1, 2, and 3. Protocol type parameter is limited to IPv4. (HP 1999b)

8.4.5 PolicyXpert for Motorola Vanguard Edge Devices

PolicyXpert might support in future Motorola's Vanguard multi service edge devices. The Vanguard multi service edge devices support QoS services such as Protocol Priority and DiffServ starting at software release 5.4. Device support includes the Vanguard 6520, 6560, 6450, 6430, 6425, 320 and 305. The Vanguard multi service edge devices are ready for beta testing in PolicyXpert. (HP 1999a)

8.5 PolicyXpert Implementation

The implementation of Policy-Based Networking should start with business objectives. These business objectives should translate into Service Level Objectives. After that is done, it is time to make decision which devices the policy agent will manage, and where to place policies. (HP 1999a)

When these are done the next step is to create a policy. When that policy has been tested, it can be assigned and deployed into the system. The policy must be verified to be sure that it is doing what was intended. (HP 1999a)

IPMAN project got the evaluation version of HP OpenView PolicyXpert 1.0. We had a Windows NT 4.0 Server for a policy server, three Cisco routers (Cisco Catalyst 5000 series, Cisco Hyperswitch A100, and Cisco 4000 series), and a Fore's switch. Unfortunately, PolicyXpert Proxy Agent did not support our routers and switch.

We could not test PolicyXpert in the network, but we could create policies in the policy server. Policies were easy to create, but they could not be tested and deployed to the network. "DSOM'99 Active Technologies for Network and Service Management" conference was in Zürich at October 1999. There Jürgen Schönwälder (from Technical University Braunschweig) claimed that policies are easy to create, but there must be different kind of policies to different level of network management what makes the implementation difficult. Rules are not enough to deal with the real-world devices; routers and switches.

Network optimization with PolicyXpert was not so easy than HP of homepages claimed because devices were not supported.

There is an unpleasant feature in PolicyExpert, administration console cannot directly configure the proxy agents it uses to manage Cisco and Packeteer products, the configuration must be done in a separate program. Also, configuring the Cisco proxy agent for log-in security is very difficult, the configuration file must be edited manually. (Infoworld 1999a)

9 CONCLUSIONS

Today, Internet offers many services to users, and convergence will increase the amount of services available on the networks. Services can be composed of components from several service providers. This makes the security matters important. New service platforms, such as Policy-Based Networking (PBN), Web-Based architecture, and hybrid services, try to solve security problems.

PBN have security policies which can identify client and permit or deny access to service. Web-based architecture security restrictions are based on signed applets. Web-based architecture simplifies the service interaction between the service provider and service user.

Policy-Based Networking (PBN) enables more unified control and management in complex IP networks. It is possible to monitor the network an on-going or passive examination with PBN. Policies can be built from a set of simpler policies, which make them easy to manage, and policies can easily re-used. Each policy has it's own conditions when the policy rule activates, and the defined action will be done. There must be different kind of policies to different level of network management what makes the implementation difficult, because rules are not enough to manage routers and switches.

In the future, services will span to many communication infrastructures, there is a need to manage services from different networks. Hybrid services span different network technologies, for example the public switched telephone network and the Internet. New services can be developed more quickly on hybrid service than in the current IP architecture.

It is difficult to measure service. There are no recommendations how to translate Service Level Agreements (SLAs) into a measurable specification.

Service management is needed today more than any time in the past because applications are more distributed, and more diverse. Large-scale applications add distribution. In future, the convergence of media, new services, different protocols and platforms lead to more diverse network management systems than now. There might be a need to combine of different kind of technologies and methods to get a solution to future network management.

10 SUMMARY

In the future, the amount of service users will increase, because new services will be available and easily used. IP networks of the future might include the Internet, but also Cable television, telecommunication networks, and mobile systems.

Security management in the Internet is based on access control, authentication, confidentiality, integrity, and non-repudiation. However, there are weaknesses on the security in the Internet. New service platforms, such as Policy-Based Networking, have new security mechanisms which help to security management.

New services need better QoS than best-effort method can guarantee. For example, video needs more capacity than e-mail. Current Internet architecture does not support QoS guarantees. Service providers use SLAs to define agreements for offering service quality guarantees to customers. There are different approaches to meet QoS issues in the IP networks, for example CoS, RSVP, and policies. CoS offers a small number of service classes and gets rid of the complex per-flow treatment in the core network. RSVP allows data receiver to request a special end-to-end quality of service for its data flows.

Policy-Based Networking is a new service platform. A policy is a combination of rules and services where rules define the criteria of resources access and usage. Policies can optimize the network assuring bandwidth to important services, and limiting bandwidth for less important services. Policy agents control routers and packet shapers.

REFERENCES

Aelita, Aelita software homepage, 1999, [Cited 2.12.1999].
Available: http://www.aelita.com/

Anonym, Overview of the IETF, 1999a, [Cited 2.12.1999].
Available: http://ietf.org/overview.html

Anonym, Overview of the IETF, 1999b, [Cited 2.12.1999]
Available: http://www.ietf.org/html.charters/policy-charter.html

Atkinson, R. Security Architecture for the Internet Protocol, IEEE, RFC 1825, Network Working Group, August, 1995.

Blight, David C., Hamada, Takeo, Policy-Based Networking Architecture for QoS Interworking in IP management. Integrated network management VI, Distributed Management for the Networked Millennium 1999, Proceedings. IM 98, IEEE, pp 811-826.

Bhoj, P., Singhal, S., and Chutani S., SLA management in federal environments. In integrated Integrated Network VI, Distributed Management for the Networked Millennium 1999, Proceedings. IM 98, IEEE, pp 293-309.

Braden, R., Clark, D., and Shenker, S., Integrated Services in the Internet Architecture: an Overview, IETF, Network Working Group, RFC 1633, 1994.

Busse, Ingo, Accounting Management for Global Broadband Connectivity Services, Network Operation and Management Symposium, 1998, NOMS'98, IEEE, Volume 1, pp 159-168

Cisco Service Management Systems, White Papers, 1999, [Cited 6.11.1999]. Available: http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/cms_wp.html.

Compaq, Homepages, clearVISN policy-based network management, 1999, [Cited 2.12.1999].
Available: http://www.networks.digital.com/dr/npg/clrvn-mn.html

Crocker, Stephen, Boesch, Brian, Hart, Alden , Lum, James, CyberCash: Payments Systems for the Internet, Commercial and Business Aspect, INET'95, ElectronicMoney, 1995.

Ellison, C., and Schneier, B., Ten risks of PKI: What you're not being told about public key infrastructure, 2000.

Fore, Homepage, Policy-based Network Management, 1999, [Cited 2.12.1999].
Available: http://www.fore.com/solutions/applications/den/

Gbaguidi, Constant, Hubaux, Jean-Pierre, Hamdi, Maher, A Programmable Architecture for the Provision of hybrid Services, IEEE Communication Magazine, July, 1999.

Harris, Stephen J. 1996. Proactive Service Management: Leveraging Telecom Information Assets for Competitive Advantage. Network Operations and Management Symposium 1996, IEEE, Volume 3, pp 700-710.

Herman, James, Integrated Management for the Networked Millenium, In Integrated Network Management VI, Distributed Management for the Millenium, Boston, USA, May 1999.

HP, Homepage, 1999a. [Cited 2.12.1999].
Available: http://www.hp.com

HP, OpenView PolicyXpert help topics ,1999b.

IBM, Press release, 1999, [Cited 22.7.1999].
Available: www2.clearlake.ibm.com/telmedia/ccb/pressa7.htm

ICL, ICL:n verkkoaapinen, verkkoratkaisut ja palvelut, [Cited 7.6.1999].
Available: http://www.icl.fi/infra/verkkoratkaisut/kirja.

Infoworld, Info World Electric, Test Center, 13.9.1999, 1999a. [Cited 22.11.1999].
Available: http://www.infoworld.com/cgi-bin/displayTC.pl?/991115comp.htm

Infoworld, Lining up traffic queuing techniques, 1999b, [Cited 16.12.1999].
Available: http://www.infoworld.com/cgi-bin/displayTC.pl?/991115sb5-que.htm

IPHighway, Homepage, [Cited 2.12.1999].
Available: http://www.iphighway.com

Isomäki, Markus, Tuominen, Jussi, End-to-End of Service for Real-time Voice in Corporate IP Networks - an Architecture and Test Results, Research

Report, Workshop "Internet and Future Network Technologies", Proceedings of the 8th Summer School on Telecommunications, 1999, Lappeenrannan teknillinen korkeakoulu.

Johanna Karonen, Sähköinen kaupankäyntikin on asiakassuhteesta kiinni, WOW!-verkkolehti, 12.7.1999, [Cited 14.7199].
Available: http://www.wow.fi/

Kaufels, F.-J., Network Management, Problems, Standards and Strategies. Addison-Wesley Publishing Company, New York, USA, 1992.

Kerttula, Esa, 1630 Telematiikka, luentomoniste, LTTK, 1998.

Kong, Qinzhen, Chen, Graham, Hussain, Rubina Y., A Management Framework for Internet Services. Network Operations and Management Symposium, 1998. NOMS 98, IEEE. Volume 1, 1998, pp 21-30.

Kurki, M., Sisältötuotantoa tukevat verkkopalvelut, tarpeet ja mahdollisuudet, 1999. Teknologiakatsaus 73/99, TEKES.

Lidyard, D., New technologies and strategic trends: An introduction to network accounting, 1999, [Cited 5.8.1999].
Available: http://www.summitonline.com/netmanage/papers/telco1.html

LDAP, Fulfilling the promise for directory-enabled networks, 1998, [Cited 16.8.1999].
Available: http://www.cnilive.com/impact/specials/ldap/.

Logean, Xavier, Dietrich, Falk, Hubaux, Jean-Pierre, On Applying Formal Techniques to the Development of Hybrid Services: Challenges and Directions, IEEE Communications Magazine, July, 1999.

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, [Cited 6.7.1999].
Available: http://www.cni.org/projects/authentication/authentication-wp.html

Martikainen Olli, Älykkäät palvelut ja Internet, March 1999.

Mensola S., IP-verkon kommunikaatiopalveluiden hallinta, Master's thesis, Department of Electrical and Communications Engineering, Helsinki University of Technology, 1998.

Mills C., Hirsh D., and Ruth G., Internet accounting: Background, IEEE, Network Working Group, RFC 1272, November, 1991.

Moore, B., Ellesson, E., and Strassner, J., Policy Framework Core Information Model, IETF, Internet draft, 1999, [Cited 18.11.1999].
Available: http://www.ietf.org/internet-drafts/draft-ietf-policy-core-info-model-01.txt

Mori K., Yamashita S., Nakanishi H., Hayashi K., Ohmachi K., Hori Y. Service Accelerator (SEA) System for Supplying Demand Oriented Information Services. Autonomous Dezentralized Systems, 1997. Proceedings. ISADS 97. Third International Symposium, pp 129-136

Neuman, B. Clifford and Medvinsky, Gennady, NetCheque, NetCash, and the Characteristics of Internet Payment Services, The Journal of Electronic Publishing, May, 1996 Volume 2, Issue 1, [Cited 5.8.1999].
Available: http://ing.ctit.utwente.nl/WU5/literature/works/NeumNetPay.html

Passero, P.; Hollenbach, S., Utilizing intelligent network technology in customer care applications, Intelligent Network Workshop, 1996. IN '96, IEEE Catalog Number: 96TH8174, Vol. 2, pp 196-258

Popien, C, Kuepper, A. A Concept for an ODP Service Management. Network Operations and Management Symposium 1994, IEEE, Volume 3, pp 888-897.

Purkayastha, S.; Ramamoorthy, R.; Tyagi, V., Customer care and billing-service differentiator in PCS, Personal Wireless Communications, 1996, IEEE Catalog Number: 96TH8165, pp 182-183

Rana, Sohail, Sellin, Eric, Implementation of a pan-European TINA-compliant service management platform, Computing & Control Engineering Journal, April 1999, Vol. 10, Issue 2, pp 73-78

Schulzrinne, H., Casner, S., Frederick, R., and Jacobson, V., RTP: A Transport Protocol for Real-Time Applications, IETF, Network Working Group and Audio-Video Transport Working Group, RFC 1889, January, 1996a.

H. Schulzrinne, RTP Profile for Audio and Video Conferences with Minimal Control, IETF, Network Working Group and Audio-Video Transport Working Group, RFC 1890, January, 1996b.

Smith, Chris 1998. Applying TINA-C Service Architecture to the Internet and Intranets. Global Convergence of Telecommunications and Distributed Object Computing, 1997. Proceedings. TINA 97, 1998, pp 4-12.

SSi, Service Strategies Inc., Homepage, [Cited 2.12.1999].
Available: http://www.ssimail.com/

Stallings, William 1995. Internet Security Handbook, Protection and Survival on the Information Superhighway. McGraw-Hill Book Company, London, 1995.

Stiller, B., Fankhauser, G., Platter, 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.

Strassner, John and Ellesson, Ed, Terminology for describing policy and services, IETF, Internet draft, 1999, [Cited 13.12.1999].
Available: http://www.ietf.org/internet-drafts/draft-ietf-policy-terms-00.txt

Sun microsystems, Products and Solutions, Telecommunications billing systems, An overview ,1999, [Cited 15.7.1999].
Available: http://suncom.bilkent.edu.tr/products-n-solutions/telco/billing_bkgrounder.html

Svanbäck, Rolf, Mobile Business Trends, The 8 th Summer School on Telecomminications, 1999.

SwitchSoft, SwitchSoff System Inc., Homepage, 1999, [Cited 2.12.1999].
Available: http://www.switchsoftsystems.com/

TAG, Brochure, 1999, [Cited 24.9.1999].
Available: www.tag.co.uk/techterm.nsf/all

Udupa, Divakara K. TMN Telecommunications Management Network, 1 ed. McGraw-Hill, New York, USA, 1999.

Vanecek, George, Mihai, Nelu, Vidovic, Nino and Vrsalovic, Dalibor, Enabling Hybrid Services in Emerging Data Networks, IEEE Communications Magazine, July 1999.

Wack, J. P., and Carnahan, L. J., Keeping Y-our Site Comfortably Secure: An Introduction to Internet Firewalls. NITS Special Publication 800-10, U.S.Department of Commerce, National Institute of Standards and Technology, 1999, [Cited 26.7.1999].
Available: http://csrc.nist.gov/nistpubs/800-10/main.html

Walrand, Jean, Varaiya, Pravin, High-Performance Communication Networks, Morgan Kaufmann Publishers Inc, 1996.

Wessels, D., and Claffy, K., Internet Cache Protocol (ICP), version 2, IEEE, Network Working Group, RFC 2196, September, 1997.

W3, HTML 4.0 Specification, W3C Recommendation, revised on 24-Apr-1998, [Cited 31.8.1999].
Available: http://www.w3.org/TR/REC-html40/intro/intro.html#h-2.2

Xiao, X., Ni, L., Internet QoS: a big picture. IEEE Network 13, 2 (Mar. 1999), pages 8-18.

Appendix 1. HP OpenView PolicyXpert time and date conditions that can activate the policies.

Condition	**Description**	**Valid values**
Date range	A range of dates during which the policy is active	Start day End day
Day of month	The days of the month that the policy is active	1-31; last n days
Day of week	The days of the week that the policy is active	Sunday-Saturday
Month of year	The month(s) during which the policy is active	Jan - Dec
Time range	The start time and the end time during which the policy is active	00:00 to 24:00
Year range	The year(s) in which the policy is active	any

Appendix 2. HP OpenView PolicyXpert packet conditions that can activate the policies.

Condition	**Description**	**Valid values**
Application traffic	The name of the networked application whose traffic is to be managed, and the direction of the traffic	Traffic type Traffic destination
Destination Ipaddress	The IP address of the device to which the traffic is flowing	IP address in standard dot notation
Destination Ipport	The protocol used and the port number of the devise to which the traffic is flowing	IP port Port type (TCP or UDP)
Destination Ipsubnet	The subnet number and subnet mask of the device to which the traffic is flowing	Base network address Subnet mask
Ipaddress	The IP address used for source or destination IP traffic	IP address in dot notation
Ipport	The port number used for source or destination IP traffic	IP port Port type (TCP or UDP)
Ipsubnet	The base network address and subnet mask used for source or destination traffic	Base network address Subnet mask
Message type	The type of RSVP message	RESV, PATH, RESVERR, PATHERR)
Protocol type	A protocol type	List of Appletalk, ARP, DECNet, IBM, SNA, IPv4, Novell IPX, Novell SPX
Source Ipaddress	The IP address of the device from which the traffic is flowing	IP address in standard dot notation
Source Ipport	The protocol used and the port number of the device from which the traffic is flowing	IP port Port type (TCP or UDP)
Source Ipsubnet	The subnet number and subnet mask of the device from which the traffic is flowing	Base network address Subnet mask
Type of service	The IP precedence bits for which the policy is active	IP precedence bits (0-7)
URL	Specify the URL for which the policy is active	String
VLANID	The VLAN ID of the device	12-bits value

	sending or receiving traffic	

Appendix 3. HP OpenView PolicyXpert traffic characteristics conditions that can activate the policies.

Condition	Description	Valid values
Incoming interface	An integer identifier for a specific interface	Integer range 0 to 256
Minimun Data Rate	The amount of bandwidth (true if less than)	Amount of bandwidth in bytes per second
Maximum Data Rate	The amount of bandwidth (true if less than)	Amount of bandwidth in bytes per second
Outgoing interface	The IPv4 address of a specific interface	Integer range 0 to 256