# An IP Network Management Model

Yuchen Zhou and Juha Liukko
Helsinki University of Technology
Laboratory of Telecommunications Software and Multimedia

June 7, 2000

**Abstract**

In recent years, a number of network management models have been developed in the network world. Those models offer different services for different purposes. However, they have limitations especially in large and complex network situations. Therefore, a management model is needed for handling the rapidly growing large and complex network of computers, one such model is the IPMAN project at HUT(Helsinki University of Technology). It defines a new four-layer network management model for a massive IP network. The layers in the IPMAN model consist network element management, traffic management, service management and content management. This article provides definitions and descriptions of the basic properties and characteristics of those four management layers.

## INTRODUCTION

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

In order to effectively manage a massive IP network, the IPMAN project has developed a new model, where IP network management is divided into four layers (See figure 1).

The lowest layer of the model is the network element management layer, which is about management of individual system in the IP network. The second layer, called traffic management, intends to manage the network so that expected traffic properties are achieved. The third layer contains, service management contents, security management and accounting management. The fourth layer is the content management layer, which deals with managing the information that is provided by the service applications.

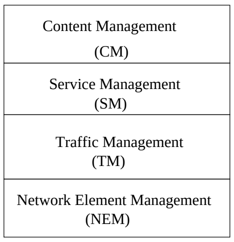


Figure 1: IPMAN Network Management Model

This study presents the IPMAN model in detail. The following section, outlines the basic concepts and three management functions of network element management layer. Then we discuss the main objectives of traffic management, two new service models for traffic management and performance management in traffic management layer. The next section describes the service management contents, especially, security management and accounting management in the service management layer. Finally, we introduce the basic definition and requirements of the content management. At the same time, we examine the web content management as a special case of the content management.

# NETWORK ELEMENT MANAGEMENT LAYER

This section first defines some basic definitions of terminology needed for discussing managing a network. Then, it presents the functions of a network element management layer.

**Network** is a group of two or more computer systems linked together. Such links may be established between many types of computers to form a network. Three examples of such a network are: **LANs** (Local Area Networks), **MANs** (Metropolitan Area Networks), **WANs** (Wide Area Networks).

**Network Element** a "Network Element" (or the equivalent shorter form "Element"), is any component of an internetwork which directly handles data packets and thus is potentially capable of exercising QoS control over data flowing through it. Network elements include routers, subnetworks and end-node operating systems.

**Network Element Management** refers to the broad subject of managing computer networks, such as those described above.

Those definitions provide a foundation to network element management layer. In general, network element management has three basic functional areas which are fault management, configuration management and security management. Each functionality has a set of tasks defined to provide for managing the functional entities. Those functionality are discussed in following sections.

## FAULT MANAGEMENT

One functional area is fault management. It is the process of locating, monitoring and correcting network problems [7]. Moreover, fault management involves three major aspects: 1) the fault must be monitored and identified, 2) the cause of the fault must be isolated, 3) the fault must be corrected. Today, the process of fault management needs to be automated. Rapid and accurate correction of network problems has to be created by the network or by the end user.

The primary benefit of fault management is that it increases network reliability by giving the network management applications to quickly detect problems and initiate recovery procedures. Fault management offers a variety of tools to provide the necessary information about the network's current state. Ideally, these tools can pinpoint exactly when a problem occurs and relay that information immediately to the network administrator, who then can begin to work on the fault and possibly to solve it without users ever becoming aware it existed. Using fault management to break the cycle of one disaster after another will increase the effectiveness of a network as well as the productivity of its administrator.

## CONFIGURATION MANAGEMENT

The second functional area is configuration management. It is the process of obtaining data from the network element and using that data to manage the set up of all network devices [7]. Configuration management consists of gathering information about the current network configuration, using that data to modify the network configuration of the network devices, and storing the data, maintaining an up-to-data inventory, and producing reports based on the data.

A network can benefit from configuration management in numerous ways. In some cases, configuration management automatically gathers and updates data on the network devices. It also provides a central storage location for configuration data. This location could be as simple as a notebook or as complex as a relational database system. Another benefit is that it enables the network administrator to modify network configuration on-line. Moreover, it facilitates the production of network inventory and other reports.

For those reasons, configuration management is an essential part for any network.

## SECURITY MANAGEMENT

The third functional area is security management. It involves protecting sensitive information found on devices attached to a network by controlling access points to that information [7]. Sensitive information is any data an organisation wants to secure, such as that pertaining to payroll, customer accounts, research and development schedules. It consists of

- **protocols and programs for network security:**There are some protocols and programs are developed to provide security over the Internet, such as Secure-HTTP (S-HTTP), Secure Shell (SSH) and Secure telnet (stelnet), Secure Multipurpose Internet Mail Extension (S/MIME) and Secure Socket Layer (SSL). Moreover, IP Security Architecture (IPSec) provides a standard security mechanism and services to the IPv4 and IPv6 in network-level.

- **securing the access points:Encryption** of data as it traverses a LAN and WAN can prevent unauthorised access to sensitive information. **Packet Filtering** stops packets to or from unsecured hosts before they reach an access point that may field sensitive information. Many network devices, such as routers, hubs and firewalls can perform packet filtering based upon network addresses. **Key Authentication** system provides a means to accomplish both host authentication and user authentication with the added advantage of not having to rely solely on the destination host.

The benefits of the security management process is that of securing sensitive information and calming the security concerns of users about attaching hosts to a network.

As computer-based communications and networks that link open systems continue to expand, security management becomes critical. It is a very important factors in the network management.

## TRAFFIC MANAGEMENT LAYER

This layer first describes the definitions of the traffic and relate to traffic management. Then we simply introduce to two new service models in traffic management layer since the QoS requirements of network traffic. Finally, this section concentrates on discussing network performance management.

**Traffic** is the load on a communications device or system. In networking, load refers to the amount of data (traffic) being carried by the network.
**Traffic Management** means techniques for avoiding congestion and shaping and policing traffic. Traffic management allows links to operate at high levels of utilisation by scaling back lower-priority, delay-tolerant traffic at the edge of the network when congestion begins to occur.
**Shaping** is the process of delaying packets within a traffic stream to cause it to conform to some defined traffic profile. [5]
**Policing** is the process of discarding packets (by a dropper) within a traffic stream in accordance with the state of a corresponding meter enforcing a traffic profile. [5]

Data communications in IP networks can be divided into connection-less and connection-oriented communications. However, in IP networks, Quality of Service (QoS) is defined in term of parameters such as bandwidth, delay variation (jitter), and packet loss probability.

To obtain high network utilisation and QoS guarantees, we should effectively control and handle bursty traffic by traffic management. In general, the task of traffic management can be classified into five components: control congestion, provide low delay, provide high throughput, support QoS and provide fair service. Therefore, this is the most important traffic to deliver, especially during times of high congestion. For example, routing protocols such as OSPF (Open Shortest Path First) and BGP (Border Gateway protocol) need to receive updates concerning traffic conditions so that they can adjust routes to try to relieve congestion. Management protocols, such as SNMP(Simple Network Management Protocol), need to be able to report congestion to network management applications and to be able to perform dynamic reconfiguration and to alter performance-related parameters to cope with congestion.

## THE NEW SERVICE MODEL FOR TRAFFIC MANAGEMENT

The current IP architecture dose not support any QoS guarantees because routing is traditionally based on a best-effort principle. This means that each packet of information is treated independently and processed in the order of arrival. To satisfy the requirements of rigid real-time applications while avoiding costs of over-provisioning, the Internet Engineering Task Force (IETF) has three working groups developing the new service model or network architecture. According to the IETF, there are two models for providing QoS:

- **Integrated Services Architecture (IntServ):** The IntServ model is based on reservations-based traffic engineering assumptions [1]. It reserves resources explicitly using a dynamic signalling protocol, that is **RSVP**(Resource Reservation Protocol), and employs admission control, packet classification, and intelligent scheduling to achieve the desired QoS. Its service categories contains **Guaranteed Delay** and **Controlled Load**.

- **Differentiated Services Architecture (DiffServ):** The DiffServ model is based on reservation-less traffic engineering assumptions [1]. It classifies packets into distinct Class of Service (CoS) and uses priority mechanisms to provide adequate QoS to the traffic. Diffserv was born against the backdrop of RSVP's fall from grace. It promised to overcome the scalability concerns of RSVP.

  **MPLS (Multi-Protocol Label Switching)** is a forwarding scheme that is based on a label-swapping forwarding (label switching) paradigm instead of standard destination-based hop-by-hop forwarding paradigm. It is important to note that this label state is not per packet or per flow, but usually represents some aggregate (e.g., between some source-destination pair). Therefore, the state produced by MPLS is manageable and scalable.

A network can be managed much more efficiently if the traffic entering the network is smooth. The task if managing the IP networks is thus to regulate the traffic in order to obtain high network utilisation, avoid network congestion, and provide an acceptable QoS to the user at low service cost.

## COMPONENTS OF TRAFFIC MANAGEMENT

The goal of traffic management is to fairly allocate resources to network users, to efficiently utilize network resources such as buffer space and link capacity, and to isolate a traffic class from the effects of other traffic that may be violating its contract. In addition, a traffic management system must provide negotiated QoS guarantees to its constituent users.

Traffic management consists of several components including policing and shaping, buffer management, queuing and scheduling, and feedback control. [10] We briefly discuss these below.

- **Shaping and Policing:** The end systems are responsible for sending data that conforms to a negotiated traffic contract. Informally, a traffic contract typically specifies the average rate, peak rate and maximum burst size of a traffic flow. The end system may use a traffic shaping function to ensure conformance to the contract. The network may police the incoming traffic to test its conformance to the contract. Policing the typically performed at the entrance to the network.
- **Queuing and Scheduling:** At each hop within the network, packets are switched (or routed) to the output port of the next hop and may be queued in the port buffer before being sent out on the link. A scheduling function controls the exit of packets from the queues of a link. The scheduling component services each queue according to a scheduling policy (or service discipline).
- **Buffer Management:** A buffer management component controls the packet into the queue. Depending on the buffer and connection states, the function may discard the packet, or may admit the packet into an appropriate queue. Once admitted, the packet waits for its turn behind other packets in the queue to be scheduled on to the link. The goal of the buffer management is to fairly and efficiently allocate network buffers to user data.
- **Feedback Control:** Nodes within a network may provide feedback to one another about their congestion state. At the IP network, feedback may be provided in the form of ICMP messages.

## PERFORMANCE MANAGEMENT

Performance management is used to evaluate the behavior of managed objects and the efficiency of communications activities [7]. It accomplishes this by monitoring the utilization of network devices and their associated links and ensuring the capacity of devices and links is not overtaxed to the extent of adversely impacting performance.

Performance management is beneficial in that it helps prevent network overcrowding and inaccessibility and thus aids in providing a consistent level of service to users.

- **Performance Analysis:** Performance analysis is involved in the analysis of performance data of an entity. It includes traffic forecasting, exception threshold policy, traffic capacity analysis, and traffic exception analysis, etc. It is necessary to aggregate the traffic and then set priorities directly related to the latency, throughput, loss, and jitters application requirements.

- **Performance Metrics:** Well-defined metrics of delay, packet loss, flow capacity, and availability are fundamental to measurement and comparison of path and network performance. In general, user are most interested in metrics that provide an indication of the likelihood that their packets will get to the destination in a timely manner. Therefore, estimates of past and expected performance for traffic across specific Internet paths, not simple measures of current performance, are important.

  Generally, network performance metrics are classified into two areas: network-centric metrics and end-to-end measurements [3]. However, the tools and techniques required to measure performance characteristics in these two categories are different. In the Internet performance analysis, it has been difficult to define metrics that reflect both perspectives.

- **Performance Management Control:** Performance management control is responsible for controlling the performance of a network. It includes network traffic management policy, traffic control, traffic administration, execution of traffic control and audit report [7]. The main objective of performance management is to avoid the congestion of the networks. Traffic control needs resources, resource management in networks is obviously crucial and imminent to maximise the network resource utilisation.

# SERVICE MANAGEMENT LAYER

First, we introduce to a definition of service and service management in this section. The rest of the sections, we present the security and accounting management in details.

**Service** can generically be defined as a collection of capabilities, with each capability being a set of actions performed by an entity (acting like a server) in response to a (constrained) request issued by another entity (being the client). **Service Management** consists of complex tasks that extend network, systems and application management by SLAs (Service-Level Agreements) and the management of customer-specific QoS parameters. Service management cross-sects the entire organisation and spans multiple organisational, administrative and jurisdictional boundaries. It is related to all resources, systems, tools applications, people and workflow that are necessary for a service provider to operate, administer, manage and provision services in heterogeneous environments [9].

## SERVICE MANAGEMENT CONTENTS

The number of services deployed over an infrastructure that spans multiple control domains, such as e-commerce and web hosting, and their users, is increasing. These end-to-end services require co-operation in internetworking between multiple organisations, systems and entities. Service providers need to deploy interoperability, distributed scalable architectures, integration and automation of network management systems. Therefore, the management system must make management easy and flexible to service providers. Generally, service management includes provisioning the requested services within pre-specified time period, if possible and when applicable monitoring or ensuring that security and contracted QoS are being delivered, when applicable upgrade the service without interruption as reliable (and flexibly) as possible as per customers requirements and possibly the customers, for example CNM (Customer Network Management), neverthless, maintenance of proper billing and security for the offered end service and always guaranteeing that the network infrastructure is capable to handle the features of the offered service.

Traditionally, communications media were separate. Services were quite distinct, such as broadcasting, voice telephony and on-line computer services. They operated on different networks and used different "platforms": TV sets, telephones and computers. Each was regulated by different laws and different regulators, usually at national level. Nowadays digital technology allows a substantially higher capacity of traditional and new services to be transported over the same networks and to use integrated consumer devices for purposes such as telephony, television or personal computing. This tendency is called convergence. Convergent services generally include Internet services delivered to TV sets via systems like Web TV, e-mail and World Wide Web access via digital TV decoders and mobile telephones, webcasting of radio and TV programming on the Internet, and using the Internet for voice telephony. All of those services further show security management and accounting management are most important issue in both the convergent services and hybrid services in the future.

## SECURITY MANAGEMENT

Security of services is not an absolute concept. Security of devices and networks must be compared to possible threats and risks. If the risks are high, the devices and the networks must be provided with more reliable secure properties. The network security influences also the security of the company, so they must be planned together. According to a committee of IETF (the Internet Engineering Task Force), the security services include:

- **Access Control:** The basic access management problem is licensing agreements for networked information resources.

- **Authentication:** 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 [4].

- **Confidentiality:** The property of communicating such that the intended recipients know what was being sent but unintended parties cannot determine what was sent [4].

- **Availability:** Probability that an item can perform its required function under stated conditions for stated duration of time.

- **Integrity:** The property of ensuring that data is transmitted from source to destination without undetected alteration [4].

- **Non-repudiation:** 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 [4].

  Effective security management must be involved in all the 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 of the level of network security will affect to the openness of the system and to the cost of maintaining the network.

### ACCOUNTING MANAGEMENT

Accounting management is the process of gathering network statistics. The gathering of these statistics can help the network engineer make decisions regarding the allocation of network resources. Likewise, these numbers are useful in managing system resources such as disk space, processing power, and backup storage. Accounting management involves measuring the usage of network resources by users in order to establish metrics, check quotas, determine costs, and bill users [7]. It includes gathering data about the utilisation of network resources, accounting data is sensitive information. At the same time, the collector must provide confidentiality at the point of collection, through transmission and up to the point where the data is delivered. Moreover, setting usage quotas using metrics, and billing users for their use of the network.

The primary benefit of accounting management is that it enables the engineer to measure and report accounting information based on individual and group of users and then use this data to bill those users, allocate resources, and compute the cost, by user, of transmitting data across the network. It has the added benefit of adding to the engineer's understanding of the user utilisation of network resources, which can help in the creation of a more productive network.

## CONTENT MANAGEMENT LAYER

IP traffic on the Internet and private enterprise networks has been growing exponentially for some time. Today, the convergence of computing, telecommunication and digital media is enabled by the technology, but it is actually driven by the content. In this section, we first examine the definition of the content and content management. Then we discuss the demands of content management. Finally, we issue the web content management.

**Content** is meaning that is recorded on a medium. The content can take various forms such as media content and information, but it can also contain enables for further activities, for example various software packages [6].
**Content Management** is systems and methods that contain ownership and transfer methods, rights and origin notarised time-stamped transactions, correct use statement, color management, media types and workflow components. It also encompasses all business practices and technical processes that are performed for the purpose of capturing, maintaining, sharing and preserving recorded meaning [8].

The purpose of the content management system is to control the flow of content during the creation and delivery of any service offering. The content must be managed throughout its entire lifetime, from initial conception and creation, to integration in an application, and delivery to user, as well as eventual archival or destruction. This entails managing content across a number of different organisations and over an extended time period.

## REQUIREMENTS OF CONTENT MANAGEMENT

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

- **General Demands of Customers:** Basic requirements of customers of a system include cataloging, search and retrieval, browsing interface and network protocol.

- **Secure Content Access:** Security is an important issue that is preventing the use of Internet for business related applications. A commercial database without secure access assurance will lose their customer as well as their products.

  There is a demand for content protection, to provide content owner/supplier a mechanism that can robustly protect copyright and identify rightful ownership in the court of law, and to prevent illegal distribution and easy tracking of fraud. Techniques used for content protection are for example, cryptography, authentication, watermarking, and access control in different services. Those protection techniques guarantee the security and copyright at the satisfactory level. Therefore, the capability of secure Internet content access can benefit both the content owner/suppliers and the customers.

- **Billing:** In the Internet environment, billing has been based on flat rates and monthly billing and only seldom on the traffic itself. The development of services with built-in cost sharing functionality could be the final reason to converge services, such as broadcast media, into the Internet and make them globally available.

## WEB CONTENT MANAGEMENT

Web content management is the foundation for any Web application, regardless of whether it is for e-business, customer relationship management or knowledge management. However, the explosion of Web content has led to management nightmares, and organisations are having difficulty keeping their Web applications current to meet the growing demands. Web sites and their applications are expected to roll-out quickly and change often and to execute corporate strategy for gaining, keeping, and serving customers.

Early content management systems have either tried to force fit complex unstructured data into a rigid database schema, or have simple ignored the problem. This has left organisations with a costly and impractical job of converting existing content. The lack of a file system interface has forced unpopular and expensive retraining to proprietary editing tools of low functionality. Therefore, next generation content management should take hybrid architecture for content management maximises the benefits of both database and file system assets, providing a single integrated environment to manage and deploy both database and file system content.

### MANAGEMENT OF DATABASES AND FILE SYSTEMS ON THE WEB

Although superficially databases and file systems seems to do the same basic job of storing data, they in fact have very different but complimentary strengths and weaknesses [2]. Most large Web sites have implemented a hybrid architecture that utilises the best of both: databases for retrieval of structured data and file systems for the retrieval of unstructured files, especially those files that are never effectively queried.

This then beg the question about content management. How can I make dynamic changes to my file system content? The answer lies in the focused application of databases. Usually, the content management system tracks every change that has taken place, so that changes can be merged quickly and efficiently. The most important aspect of successfully integrating operational data is the architecture. This needs to take into account each of the following areas [2]:

- **Performance:** The Production Database will have been sized for a certain capacity and volume of transactions and data. Additional Web traffic not only adds further users and data, but the fact that Web traffic typically tends to grow rapidly means that it can be difficult to accurately predict and plan capacity. It is bad enough if a sudden burst of Web traffic brings down your site, without it also bringing down the operational systems behind it. Even if your business is 100% Web, a secondary protected database can acts as an active back-up to the primary Web database.
- **Security:** Operational Systems having been developed behind the firewall have often not been designed from the outset to handle outside users and so require a firewall to protect against unauthorised access. Data flows between the Web area and the production database can be restricted to pre-defined transactions.
- **Ease of Implementation and Management:** Having a separate Web database from the production minimises impact on the existing operational systems, but raises the question of how the Web and production databases should be kept in synchronisation. Second, by de-coupling the two databases, it is possible to change both the technology and database design to suit the application. Further, the database design could be tuned for the respective types of database access with the gateway/replication process transforming the data as required.

Once content has been developed there should be an efficient content replication capability. There must be a secure, rules-based application for distributing and synchronizing content. The system should be capable of deploying large amounts of content and handling many Web sites. Also, it should provide immediately recovery, and report successful execution. As Web sites continue to handle more sophisticated Web assets, a deployment application must execute automated scripts and take appropriate action in the event of an unexpected condition during deployment. The deployment application should be able to fall back, recover and notify the appropriate personnel regarding failure during a development.

# SUMMARY

Introduction of new equipment and new technologies means introduction of new information systems, which also increases the number of data repositories and fault management systems. The effective system management is thinking the network as a single, multilayer entity, one that requires its own care. As networks become larger and more complex, tools and applications to ease network management are critical.

IPMAN project has developed one new network management model for massive IP networks. This management model divided IP networks into four-layer management entity. The detail definition and characteristics, different functions and tasks of the every layers are described in this article. This management model basically covers all of the contents of the network management. It is both used in current IP network management and helpful for the future network development.

### ACKNOWLEDGEMENTS

We would like to thank Jouni Karvo for helpful discussions and guidelines. We also thank Stiina Ylänen for her support when finalising this paper.

## References

[1] *TRILLIUM IP QUALITY OF SERVICE WHITE PAPER* (1998). http://www.trillium.com/whats-new/wp_ipqos.html.

[2] *Databases and File Systems on the Web* (1999). Interwoven, Inc.

[3] *White paper on network performance metrics* (1999). http://www.sdsc.edu/DOCT/Publications.html.

[4] Atkinson, R. Security architecture for the internet protocol(RFC 1825). 1995.

[5] Blake, S., and Black, D. A architecture for differentiated services, internet engineering task force (Obsoletes RFC 2475). 1998.

[6] Kajanto, M. Strategic framework for the interactive information networks. Acta Polytechnica Scandinavica.

[7] Leinwand, A., and Fang, K. *Network Management A Practical Perspective*. Addison-Wesley Publishing Company,Inc., 1993.

[8] N. Brownlee, C. Mills, and G. Ruth. Traffic flow measurement: Architecture. Network Working Group, RFC 2722, Obsoletes: 2063, Category: Informational, 1999.

[9] Pras, A. *Network Management Architectures*. CTIT ph.D - thesis series, University of Twente, Enschede. no.95-02.

[10] Rohit Goyal, B.S., M. *Traffic Management for TCP/IP over Asynchronous Transfer Mode (ATM) Networks*. Dissertation, The Ohio State University. 1999.

## BIOGRAPHIES

Yuchen Zhou (zhou@cc.hut.fi) is a Ph.D. student studying in Laboratory of Telecommunications Software and Multimedia, University of Helsinki of Technology.

Juha Liukko (jliukko@tcm.hut.fi) has received an M. Sc. degree from Tampere University of Technology in 1994. In 1995 he had a training period in Helsinki Puhelin Oy (nowadays Elisa Communications) - Telecommunication operator company. Since 1996 he has worked in Nokia Networks in the area of telecommunication network management (concepts, specification and product management), where he is currently working as a product manager. He is a postgraduate student in Tampere University of Technology. He is also working as a part-time researcher in Helsinki University of Technology, Laboratory of Telecommunications Software and Multimedia in a TEKES project.