

# The Rinpoche System A Web-based Integrated HiNet Network Management System

Hey-Chyi Young, Sharon S. Lin, Jeng-Sen Lin, Chung-Chi Lo,  
Tse-Han Fang, Min-Chang Huang, Yea-Shian Wang, Chung-Hua Hu,  
Chien-Wen Chen, Min-Ta Chang, Shu-Hai Liao, Yen-Cheng Chen,  
Rong-Syh Lin, San-Wei Sun  
Telecommunication Laboratories, Chunghwa Telecom Co., Ltd.  
12, Lane 551, Min-Tsu Road Sec.5  
Yany-Mei, Taoyuan, Taiwan 326, R.O.C.  
[heychyi@ms.chttl.com.tw](mailto:heychyi@ms.chttl.com.tw)

*Abstract* - This paper is to describe a web-based integrated network management system, the Rinpoche, for HiNet, which is the largest Internet service provider in Taiwan. The initiatives for developing such a system is to offer network operators to grasp the global view of the network with a convenient and efficient tool. On this paper, the distributed and hierarchical system architecture of the Rinpoche is given first followed by the system environment description. Several important network management functions are also described. Figures and the graphical user interface windows are included to help illustration.

## I. INTRODUCTION

The HiNet, which is owned by Chunghwa Telecommunications Co., Ltd. and has offered Internet services for over 1.6 million dialup customers and thousands leased line customers, is currently the largest ISP in Taiwan and the fifth largest ISP in the world. The HiNet is currently facing the problem of how to get network management systems to facilitate the management of the complex network. Unfortunately, most commercial network management systems are designed for the purpose of network element management as introduced in ITU-T M.3010 [1]. These proprietary systems are focus on the management of certain kind of network device produced by certain vendor, rather than apply the management functions to different devices or even the same devices with different vendors. However, in a real network it is usually composed of many kinds of devices with many vendors. As a result, an ISP may set up lots of management systems with each for certain kind of device, but still lack of the entire viewpoint of the network. Since all kinds of network elements are tightly connected, problems may propagate and have deep relationship. Without the global picture of the whole network it is difficult to manage the network even though there are a lot of vendor-specific management systems provided.

Another principal issue for traditional network management systems is the user interface. Graphical user interfaces are generally designed in the console or in some dedicated terminals. Operators have to sit in front of them to monitor the network. The mobility is restricted. Using web technologies [2-6] is the new trend of the network management application. It provides several advantages that the traditional approaches can not offer. There is no need for users to follow a complex procedure to install the client application. Every management operation is done through

the web which provides users the familiar graphical user interfaces for access. Also, due to the characteristics of web technology, applications' extensibility is improved and the cost maintenance efforts are reduced greatly. Web-based network management applications have additional features compared to general web applications that usually deal with pure form requests and responses. For network management applications, servers must constantly update the browser side information to reflect the latest network condition from time to time. Therefore, network operators at different sites could monitor and reconfigure the network simultaneously, with the most current network data.

The Rinpoche, a web-based integrated HiNet network management system, is designed to solve the above problems. It is not intended to replace any proprietary network management systems such as STRATAView for CISCO ATM network, but to offer a tool for network operators to catch the global situation of the network in time and to take the most appropriate actions. In the following sections, the management domain and the system architecture of the Rinpoche is first illustrated. Following that, the system environment will be introduced. And then some prominent functions will be described. Finally, a conclusion is given.

## II. THE MANAGEMENT DOMAIN

As Figure 1 shows, customers access the HiNet through the Point of Presence (POP). There are a lot of POPs defined in the whole network. Remote access servers (RASs) in POP are used to connect dialup customers to the HiNet, and access servers are for leased line subscribers. Traffics of several dialup customers are combined into one T1 line. Several T1 lines are accommodated in a RAS. A RAS also contains built in modems corresponding to each connected dialup customer. For leased line customers, POP's access routers are directly connected to the customer-side routers. In addition to RASs and access routers, some other network elements such as ether-switches are also in POP. As to the HiNet backbone, it consists of a set of backbone routers and several important servers like email server, web server... etc. The Rinpoche system is designed to monitor all these devices. The managed resources include RASs, access routers, backbone routers, ether switches, general nodes that have IP addresses, and their interfaces. In addition, the system audits RASs' T1 lines and modems and can also monitor the customer-side routers as well as the leased lines.

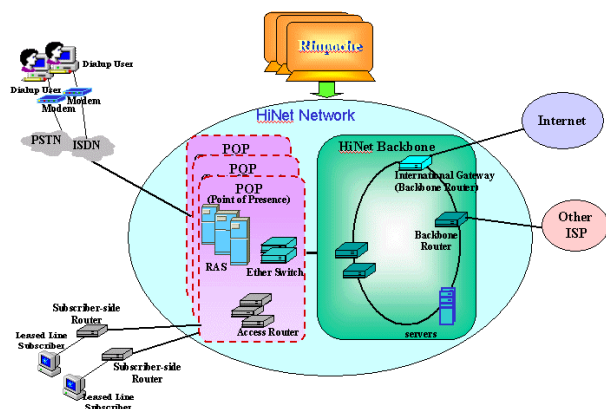


Figure 1 Management Domain of Rinpoche

### III. THE DISTRIBUTED AND HIERARCHICAL SYSTEM ARCHITECTURE

The Rinpoche adopts the distributed and hierarchical system architecture. Figure 2 shows the system which is composed of a number of Element Management Systems called EMSs and one Network Management System called NMS. Each EMS is responsible for managing a set of network elements in one or more management scopes. The network operators define management scope. A set of devices with similar functionality can be defined in one management scope. For example, all the RASs for PSTN dialup customers of a certain POP can be grouped in one management scope, and all the HiNet backbone routers are in another management scope. Besides the management scopes, the Rinpoche also hierarchically defines four management levels in the NMS. They are the headquarters, the region, the sub-region and the operation station. From the viewpoint of the NMS, it is a headquarters that contains a set of regions. Each region contains a number of sub-regions. Each sub-region has several operation stations. Under the operation station, there may have a set of management scopes. The NMS does not monitor the network elements directly, instead it collects summarized information from all the EMSs.

EMSs are installed in somewhere in Taiwan. And the NMS is in the HiNet's central operation center located in Taipei. Network operators who are interested in managing some sub-networks can log into the corresponding EMS directly via the web browsers. However, an operator in the central operation center may have an interest in the whole network, he or she can log into the NMS to find out the global picture through the web browser as well. Once the user notices that some management scopes raise problems, he or she can switch to the corresponding EMSs to see more detail information without re-logging into the EMSs. By use of the characteristics of worldwide web, network operators at different locations can monitor the network simultaneously without interfering with each other.

With this distributed system architecture, management of the network becomes very flexible and extensible. As the HiNet customers increase, more POPs need to be added. To manage those newly created POPs, network operators can configure a set of new management scopes which corresponding to these POPs in one or more existing EMSs. If the computing power of existing EMSs is not accommodated, a new EMS can be dynamically set

up and registers itself to the NMS easily without affecting the current operation.

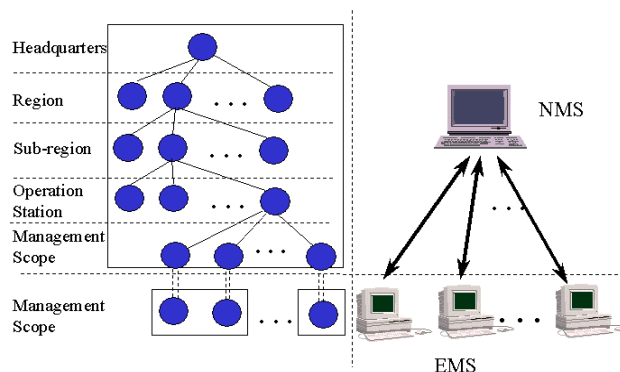


Figure 2 Rinpoche's Hierarchical Management Levels

### IV. THE SYSTEM ENVIRONMENT

Due to the economical reason, Window NT servers are chosen to be the platforms of the Rinpoche's NMS and EMSs. Microsoft's IIS and SQL Server are adopted as the web server and database server respectively. Many state-of-the-art world wide web (www) technologies like HTML, Java Script, Java, Java Applet, Java Servlet, JDBC, JMAPI, JavaBeans are used in the system designed. In order to get the best display, Netscape 4.0 or above web browser is recommended on the client side. Figure 3 shows the communication model of the Rinpoche. The communication protocols used in between web clients and the EMS or NMS servers are the HTTP and TCP/IP. Simple Network Management Protocol (SNMP) [7] is used for servers to retrieve management information from managed resources. The communication between the NMS and the EMSs is accomplished by using TCP/IP protocol. Other protocols like ICMP are used to discover some other network performance data such as round trip time and packet loss rate that is not stored in the management information base [8].

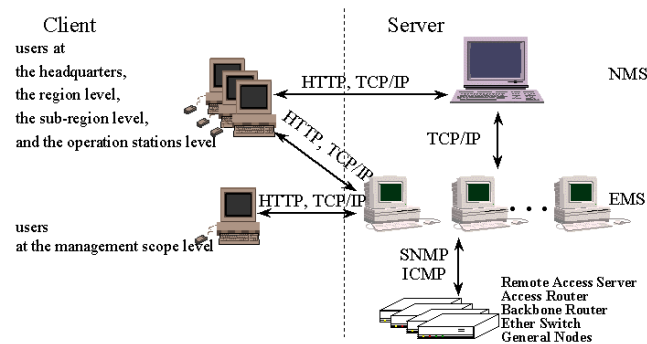


Figure 3 Rinpoche's Communication Model

### V. SYSTEM FUNCTIONS

The Rinpoche provides several functions to facilitate network management. Some important ones are described as followed.

#### V.i. ACCESS CONTROL

Two categories of users are defined for the Rinpoche. One is the system administrator, the other is the general user. System administrator has the privilege to add, delete or modify general users as well as to define their access domain and access right.

According to the management levels mentioned in section II, general users are also classified into five roles, one for each level. For users at a certain level, they have the read or write privilege for one or more domains at that level as defined by the system administrator. For example, users with a specified role at the NMS region level, may have the read or write privilege to manage the "South Region" and the "Central Region". That user can access all the management scopes defined under these regions with the specified access privilege. Figure 4 shows the graphical user interface for the NMS system administrator to create a general user with a role at the region level. Notice that all the existing regions will be listed in a pop-up window for selection. Once a general user for a role is created, the user can log on the Rinpoche system and only the part of network information corresponding to his access domain will be displayed to him.

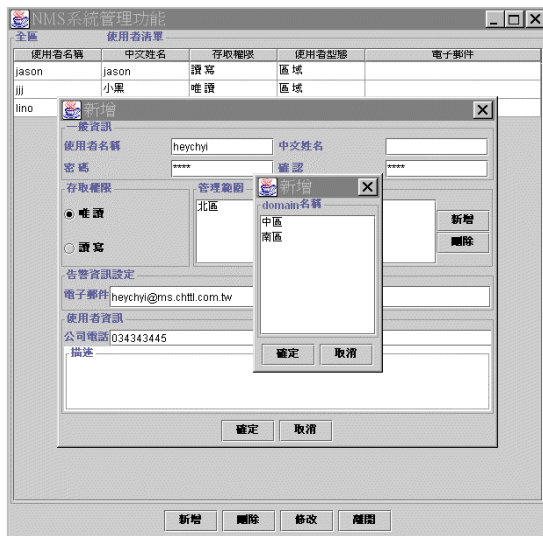


Figure 4 Creating a General User at the Area Level

V.ii. THE DEVICE EXPLODER

The device explorer is a tree hierarchical display GUI to show the logical network topology. Figure 5 shows the device explorer GUI. The levels of the hierarchical tree from NMS to EMS are headquarters, region, sub-region, operation station, management scope and server subsequently. The server level includes many different types of nodes. They are RAS, access router, backbone router, ether-switch, and general server type. Underlying the RASs there are interfaces, T1 slots and modem slots. Below the T1 slots and modem slots are T1 lines and modems. Other server types only have interfaces as their children. Each different type of nodes has different icons to represent it. Icons have attributes including label, icon type and severity status. The nodes of server level have additional information like IP address, packet loss rate and round trip time. The icon type determines the graphical representation of node. The severity status information reflects to the color of its graphical representation. The severity status of a non-leaf node in the tree is the compound status representing a summation of the status of its descendant and itself.

The device explorer function can help network operators to search node by label, IP address, icon type, status or even the combination of these criterion in the tree. For example, network operators could search nodes whose severity is critical. It also provides the entry points for other functions. When clicking the node icon, a function menu will pop up for the user to activate important functions.

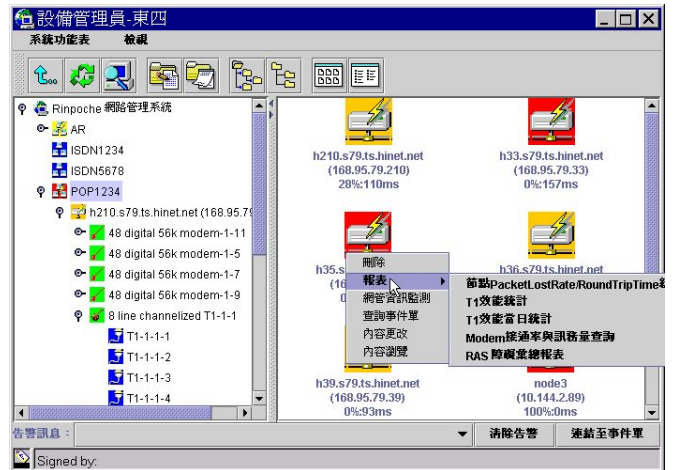


Figure 5 GUI of Device Explorer

V.iii. MANAGEMENT INFORMATION MONITORING

After creating a management scope, the network operator has first to specify what devices are going to be monitored within that scope. It is generally difficult for a network operator to add devices to the management scope one by one. Therefore, a functionality of auto discovering is supported by the Rinpoche system to find out all the nodes located in a specified network segment by giving an IP address range. Network operators can select nodes to be managed from the resulting pool. The Rinpoche also automatically detects all the T1 lines and modems associated with the chosen RASs. For each type of the device, users can determine what types of interfaces are going to be monitored as well. Again, the system will discover the specified interfaces as expected.

Most network element monitoring task is performed periodically by using SNMP to retrieve the information stored in the devices' MIBs [9-14]. Once abnormal conditions are detected, the system submits system events to the event flow management subsystem that will be described in section V.iv. As described in section V.ii, events affect the color of network elements icon displayed in the graphical user interface window according to their severity. Currently, the Rinpoche has categorized about one hundred system events. For each device, the system generates events if the device is restarted. For each interface of a device, the system audits its operational status such as up or down, administration status like enable or disable, and the performance information if required. Users can set another monitoring options for an interface through the interface configuration graphical user interface. According to the specification defined by users, the system can monitor the traffic usage of a network interface as well as the round trip time and packet loss rate of a device that is remotely connected to the interface. And these kinds of data are especially important for applying to leased line management. Other system information is also provided. For example, if a device supports the CPU loading information as defined in Cisco private MIB, the Rinpoche can check if it exceeds the threshold automatically.

The Rinpoche is capable of monitoring more information of RASs. It monitors the operational status, the administration status and the line status of each T1. Besides, it also collects and analyzes the performance data, the port utilization and the line availability of T1. For RAS's modems, the Rinpoche is interested in the states of

modem slots, the number of attempt connections, the number of successful connections, the in and out traffic ...etc. In addition to these data, the system is also capable of receiving SNMP traps issued by managed devices. Furthermore, it makes use of the ICMP protocol through the "ping" instruction, the Rinpoche system surveys the round trip time and packet loss rate for every managed device.

In some cases, proprietary devices store important information in their private MIBs, and therefore that information is not supported by the Rinpoche in default. To access this kind of information, network operator can make use of the "General Management Information Monitor" function given by the system to retrieve this piece of information. As Figure 6 exhibits, users can dynamically specify an arbitrary SNMP object identifier and define the monitoring time interval, the monitored devices and the event associated with it. The Rinpoche system gets information through the object identifier periodically and check if the user-defined event occurs. In addition, a real time data of that object is also produced graphically.



Figure 6 General Management Information Monitoring

V.iv. THE EVENT FLOW MANAGEMENT

The system generates event tickets when something occurred. The Rinpoche has an event flow management function that deals with the processing flow of events. Two categories of event tickets are defined by the system. One is for system events, the other is for audit events and another one is for general events. System events are arisen whenever the system finds out some important or abnormal conditions of the network elements. Whenever a system event ticket is generated, the ticket is in an open state. A ticket will be in a hold state if someone has received the event and take some actions to correct the problem. It will enter a close state only when the abnormal conditions associated with that event is removed or when the user closes it manually. A system event ticket carries a lot of detailed information like the ticket id, the subject, the event source, the severity, the state, the time happened, the action suggested to be taken, the responsible person, ...etc. Audit events are issued at the time when a user enters in the system, when the network configuration is changed or when a significant setting of system is occurred. In general, audit events are used for the system administrator to trace what and when and by whom a security-related action is performed.

All tickets are saved in the system for six months. Like Figure 7 shows, the Rinpoche provides event ticket windows at many

management levels for users to check systematically. Many search criteria can be set for users to locate the target tickets they are interested in. Basically, they can view tickets by event attributes. This mechanism is very convenient for users to manage the network in a strategic way.

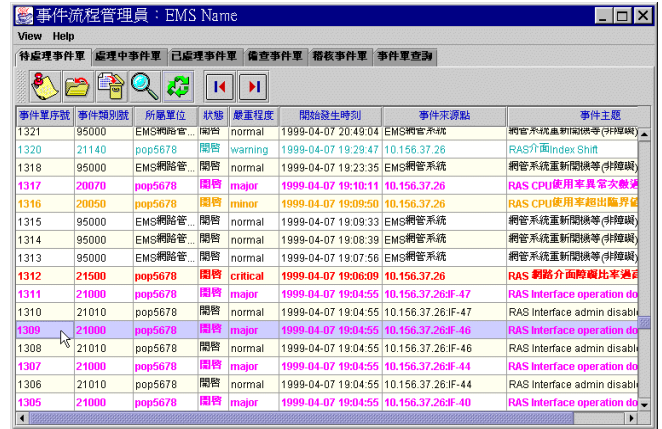


Figure 7 GUI for Event Flow Management Function

V.v. ALARM NOTIFICATION

Alarm notification is very important for network management. The system should have the ability to automatically notify users that some attention is required. In addition to change the color of network element icons displayed in the device exploder or refreshing the contents of event ticket window, several mechanisms are provided by the Rinpoche to achieve the goal of reporting alarms immediately. These include playing audio alarms on the web clients, sending emails to the users and paging the users' pagers or mobile phones. The Rinpoche introduces two kinds of profiles aiming for flexible alarm notification. One is the event profile, the other is the alarm profile. In an event profile, users can set the threshold for issuing event tickets, specify the method of alarm notification, assign the paging information and define if alarms are submitting repeatedly for each type of event. The alarm profile is used to specify the destinations of email and paging alarms. Users define the email addresses and pager or mobile phone numbers along with their working time periods in the profile. Several event profiles and alarm profiles may exist in the system and be shared by some management scopes. When creating a management scope, the user specifies the event profile and alarm profile associated with it. These profiles are referred to alarm notification whenever there are events generated within the scope. To be more flexible, the alarm profile of a management scope can be overwritten at the device or in lower levels, so that email and paging alarms generated for some particular devices can be sent to the persons who are responsible for the maintenance of these devices. As to audio alarms, the web client sides will play different music according to the severity of events.

V.vi. STATISTICAL REPORTS

The Rinpoche offers several kinds of statistical reports and query facilities to help network operators monitor and diagnose unsatisfactory condition in the entire network. Many statistical reports are stored for six months and are provided at each management level. Detailed information is presented at the lower management levels. In contract, more summarized information is contained in higher level reports. Users can also follow the hyperlinks provided in the reports to trace the more elaborate data. For example, for RASs' T1 lines, various statistical reports are

