Available online at www.sciencedirect.com
SCIENCE DIRECT®
Computers and Electrical Engineering 31 (2005) 503–524
Computers and Electrical Engineering
www.elsevier.com/locate/compeleceng

A Web-based monitor and management system architecture for enterprise virtual private network

Ruey-Shun Chen *, Change-Jen Hsu, Chan-Chine Chang, S.W. Yeh

Institute of Information Management, National Chiao Tung University, 1001, Ta Hsueh Road, Hsinchu City, Taiwan

Received 30 September 2004; accepted 29 September 2005
Available online 19 January 2006

Abstract

Virtual private network (VPN) not only possesses the low cost, inexpensive fees, and excellent support advantages of the Internet, it also has the benefit of the security as the leased line. How to properly manage the VPN is an issue in which the enterprise IT engineers have to take seriously.

This research is based on the new network management technologies such as policy-based network management, mobile agent, etc., to design a VPN monitor and management system architecture that contains high level management with low network traffic load. This system architecture integrates both VPN devices and general network devices, such the feature can integrate the monitor and manage the VPN and Intranet at the same time.

The result of this research provides enterprises with a VPN architecture for monitoring and managing the enterprises, as well as to establish a prototype for the enterprise VPN monitor and management system. Such system architecture can effectively assist the semiconductor companies to monitor and manage their enterprise VPN in order to utilize the Internet resources, and to reduce the possible operation off time. The prototype system could proof the feasibility of the systematic architecture, it can automatically detect and activate the backup mechanism according to the preset management policy, and to achieve the effective and fast solution for the enterprise network problems.

Keywords: Virtual private network (VPN); Policy-based management system; Mobile agent

* Corresponding author. Tel.: +886 3 5712121/57428; fax: +886 3 5610616.
E-mail addresses: rschen@iim.nctu.edu.tw, rschen@bis03.iim.nctu.edu.tw (R.-S. Chen).

0045-7906/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2005.09.006

1. Introduction

VPN is the abbreviation for virtual private network. In the past, a multinational corporation often uses long distance/international-leased line, frame relay, or telephone/ISDN dial-up to connect the network of each branch office in order to communicate the information with one another. However, with the characteristics of the low cost, low fees, and excellent backup support of the Internet, the enterprises are still use the Internet for sending important data due to the security consideration [4]. Thus, under the premise of lower the cost and enhance the competitiveness, more and more enterprises are applying the VPN technology to replace the existing long distance/international leased line [16,17].

Though after the prevalence of the VPN, there has not any suitable software to provide the enterprises with effective integration to monitor the VPN and the Internet network. The application of the VPN has crossed over the Internet network with the encryptions on all data, in which the general enterprises would find it difficult to utilize the existing Internet management tools to understand and analyze the actual operating condition of VPN virtual tunnel [16]. With the establishing of VPN tunnels, the management and setup are more complex. How to manage properly manage the VPN is an important issue to enterprise IT engineers.

The objective of this research is to design an integrated monitoring and management enterprise VPN and Intranet network system architecture which allows high level management, it is an efficient and does not take up a lot of the Internet bandwidth, so it can be used as a reference for the enterprise managers or IT engineers to apply on the monitoring and management of the enterprise VPN, or for the network management, or network management tools R&D of the VPN firms.

Furthermore, a prototype system to display user interface is in order to verify the advantages and feasibility of the system, and comparison with the benefits.

With the new technology in the network management field and incorporating the actually management and VPN usage experiences and try to break through the constraint of the Internet and encryption tunnel which currently cannot be monitored by the network management system in order to design a enterprise VPN network monitor and management system and to achieve in high level management with low network traffic loads. Finally, to come up with a prototype for the VPN network monitor and management system that can be put to actual operation in order to test concept.

2. Literature review

2.1. Virtual private network

The application of the VPN architecture has following four types [1]:

(1) *Intranet VPN:* for connecting each branch office of the company.
(2) *Remote access VPN:* for connecting the company network and remote or mobile staffs.
(3) *Extranet VPN:* for connecting other companies and its strategic partners, clients, and suppliers.

(4) *Complete VPN architecture:* refers to the integration of the three type architectures as described.

The security service mechanism of VPN can be obtained with the following technologies [7]:

(1) *Firewall:* is a system located between the Intranet and extranet.
(2) *Encryption:* the added encryption technology can be classified into two types, one is symmetric cryptography; the other type is asymmetric cryptography.
(3) *Authentication:* since remote or mobile users may be request to use the company resources anywhere on the Internet in which a fixed IP address may not be possible. Hence, in order to ensure them is an authenticated legal user of the company, the VPN would need to apply with the ID authentication technology.
(4) *Tunneling:* tunnel packet technology is to transmit the information of the private data network on the public data network with a developed information packaging method of encapsulation, which is to establish a secret channel on the public network. The most commonly used tunneling protocols of VPN are point-to-point tunneling protocol (PPTP), layer 2 tunneling protocol (L2TP), and IPSec (Internet security protocol) [1].

2.2. Policy-based network management

The managers do not need to know the various setup methods for each network devices, and let the policy-based network management system making the setup or change command to each network devices. The policy rule can use IF ⟨condition⟩ THEN ⟨action⟩ method to define the logic for service and resource allocations, and then for policy decision points to define the rules in order to further define its legality and convert to the acceptable groups by the policy enforcement points (such as network devices) [1].

Policy-based network management architecture can be classified as the following four layers [1,2]:

(1) *Application layer:* is a centralized enterprise management tool. The manager uses the enterprise system management tool to define policies and to examine the information collected by the resource managers in the information management layer.
(2) *Information management layer:* the place where every category of information is stored and the collecting of the enterprise information resource usage conditions. The catalog server sends the inactive policies to the policy decision point. The resource manager collects the related resource usage conditions of the device layer, and will send to the enterprise management tool and policy decision point for reference.
(3) *Policy control layer:* the policy decision point integrates the received inactive policies with the information provided by the resource manager to convert it to executable groups for the Device Layer, and to proceed with setup or change instructions on the devices of the device layer, or to provide the decision for the device layer.
(4) *Device layer:* is the variety of components on the network, such as network devices, personal computers, applied servers, etc. The device layer proceeds with management operations in accordance with the instructions of the policy decision point.

2.3. Mobile agent

Mobile agent has the mechanism of the mobility and the agency [3]. Mobile agent is an autonomous program, which can transfer from one machine to another under its own control. The application of the mobile agent in network management can solve the above-described constraints on the conventional network management [5,6]. Management application can be moved to the devices on the network and allows the network devices to execute some of the operations in order to reduce the workload of NMS and the network traffic. Mobile agent can be moved from one device to another for executing the required management functions. Moreover, mobile agent can act as an agent for NMS in deciding when and what devices to move to in order to decrease the reciprocal operations with NMS. In recent years, there are many studies which had placed the mobile agent mechanism above the network management, such as Internet service management, distributed heterogeneous network management [8], the architecture of network management [9–11], the improvements of the network management architecture [14,15]. All the examples are utilize the advantages of the mobile agent to solve the problem of heterogeneous network management and to obtain the managing objectives efficiently [12,13].

3. Analysis the current condition of the enterprise VPN monitor and management

3.1. The architecture of the current enterprise VPN

The VPN architecture may be used by the enterprises as shown in Fig. 1. The network architecture primarily contains one company headquarter regional network, two branch offices regional network, and one enterprise partner regional network. Each regional network utilizes the firewall/VPN devices and Internet connection to the Internet. One of the important branch office leases a separate international leased line with headquarter to connect with each other networks for reciprocating important and instant response information required, while the larger data and information that does not require immediate attention would be sent via the VPN tunnels established on the Internet. Other smaller branches and the company headquarter would rely completely on VPN tunnels established on the Internet for sending information. In addition, there is another VPN device on the headquarters' DMZ network to provide the mobile agents with the ability to link back to the company Intranet resources from outside the company, as the headquarter and its enterprise partners also conveys the important enterprise information via VPN.

3.2. The difficulties of the current enterprise VPN monitor and management

If an enterprise uses the VPN architecture as shown in Fig. 1, have the following problems on the monitor and management:

3.2.1. Complexity of the network routes

The enterprise user will use different network route according to different needs, such as shown in Fig. 2, the 1st data flow is the Internet service demand of the headquarter personnel in general, which will go through a firewall for access; the 2nd data flow is the transmitting of information

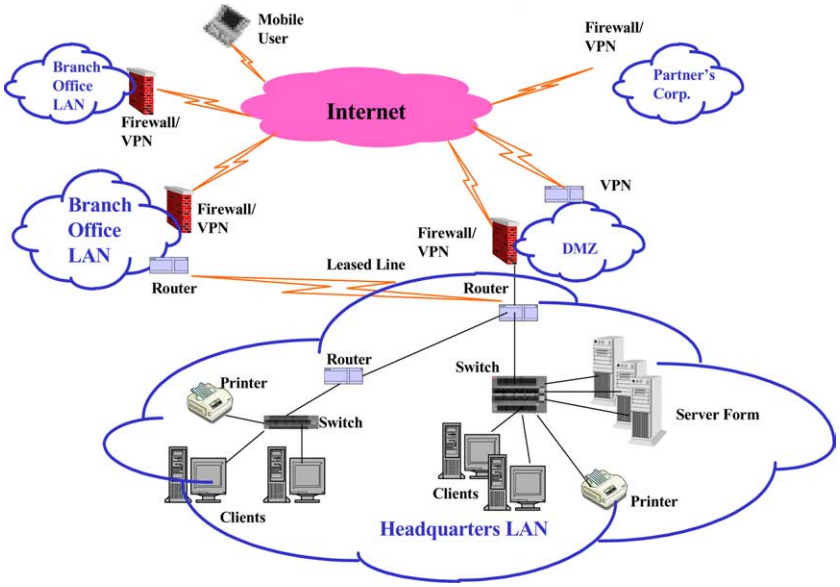

Fig. 1. The architecture for enterprise VPN.

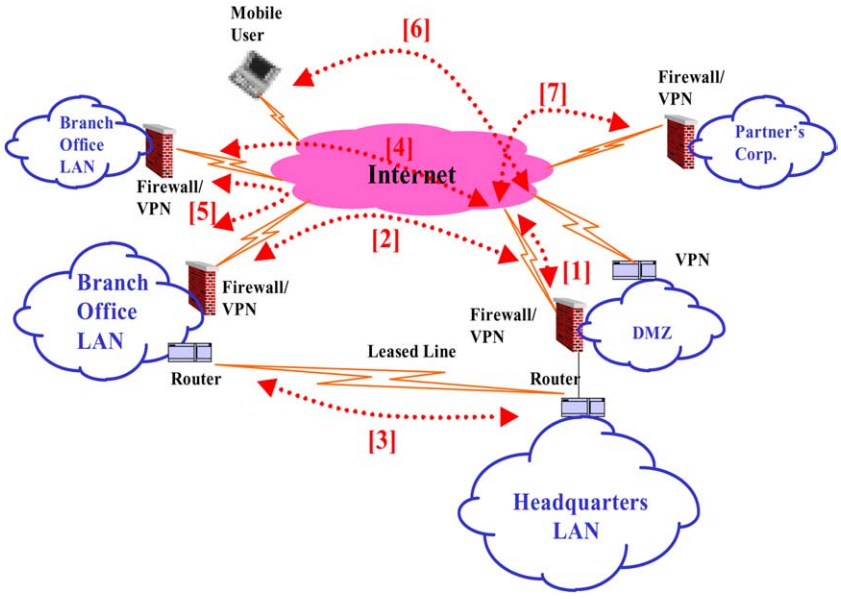

Fig. 2. The data flow on enterprise VPN tunnels, Internet and Intranet.

sharing in general through VPN tunnels between the company headquarter and a larger scale branch office; the 3rd data flow is the executing of the headquarters' specialized on-line application system through long distance/international leased line by a larger scale branch office; the 4th data flow is the transmitting of all the information with VPN tunnels by the headquarter and a smaller scale branch office; the 5th data flow is the transmission between the two branches with

VPN tunnels; the 6th data flow is utilizing of the user end software provided by the VPN product to connect to the Internet devices in order to link back to the company's Intranet resources when the enterprise staffs are on the road or at working from home; the 7th data flow is the important E-Commerce information transmitted through the VPN tunnels between the headquarter and its important enterprise partners to ensure such important enterprise information would not be intersected by the hackers. However, in order to protect its enterprise partners, only the necessary E-Commerce information can be acquired, in which other information regarding the company's operation cannot be obtained as the related precautions setting would also be performed.

3.2.2. Difficult to integrate VPN and Intranet

The IT engineers can utilize the exclusive management tools provided by the VPN devices, and some of the network management system on the market. However, all these tools have some drawbacks in which the problems are unable to integrate. The followings will explain these problems, respectively.

(1) The drawbacks of the monitor and management tools provided by the VPN products:
- VPN products provide an exclusive management interface, and has the following drawbacks: Some products do not provide GUI, which is not convenient for the settings and management; unable to perform policy-based management with network devices, in which it would not be easy for the managers to gain a full comprehension.
- Most VPN products would provide log, but it also has the following drawbacks: it is a text file, which cannot be understood fully at a glance; the file is excessively large, not easily inquired and managed; unable to know the network condition of the Intranet.
- Some of the VPN products provide specialized tools for detecting errors, but it also has the following drawbacks: the specialize error detection tool is too simple, which cannot detect the errors effectively; if it's under the Unix operating system, its command is in text format, information shows during the error detection are in text format, not likely to understand.

(2) The drawbacks of the monitor and management system by network devices:
- Network devices also provides management interface but with the following drawbacks: the command mode is provided for the management task, the operation is not easy; most of them do not provide Policy-based Management, The specialize management software provided by network devices in general do not offer network architecture diagram.
- All network devices offers error detection commands in text format or with simple error detection function within the provided specialize monitor and management GUI interface, but with the following drawbacks: it is not easy for management in text format, such as forgotten of the commands and the information shown in text format are not easily understood; the specialize error detection tool is oversimplified, unable to integrate with the error detection tools of the VPN product.

3.3. The enterprise expectats for the VPN monitor and management tools

Overall speaking, enterprise has the following thoughts and expectations in regards to the VPN technology and how to monitor and manage the VPN:

1. *Using the effective and cost savings products and technologies:* under the diversification of information products in order to enhance the overall network efficiency and cost saving for the enterprise. Hence, variety of products and technologies are still being integrated during the design of integral enterprise networks by the IT engineers.
2. *Integrated monitor and management tools:* confronting with these new products and technologies, there are no uniform techniques to perform integration. Hence, for IT engineers, an integrated monitor and management system is desperately in need to reduce the management pressure. The enterprises would also hope to allow more efficient management planning by the IT engineers via the integrated monitor and management tools, to decrease the human mistakes.
3. *Decreasing the degree of relying on specialize IT engineers:* enterprise needs to cultivate its own specialize IT engineers in which they must equipped with variety of familiar skills and a strong integrating and analyzing abilities in order to spend lots of time for the monitor and management and planning. Furthermore, relying excessively on the IT engineers may lead to not be able to eliminate the problems instantly when the IT engineers is absent. Therefore, easy use monitor and management system and train several management personnel in order to support one another and to decrease the influences on a enterprise due to the employee turnovers.
4. *Decreasing the waste of network bandwidth due to monitoring:* since the enterprise networks are expanding with each day, the management workload of NMS is becoming greater. In fact, the network management information collected or generated by the NMS has taken up quite a substantial amount of bandwidth from the enterprise network. Therefore, the enterprises would increase the burden of the network because of the network monitoring. Thus, the enterprises that use VPN should be integral enterprise network monitor and management system in order to effectively manage the VPN and Intranet of the enterprise.

4. The proposed architecture for enterprise VPN monitor and management system

4.1. Demand analysis

In order to effectively integrate monitoring and managing enterprise VPN and Intranet network, a system would be designed to solve the following problems frequently encountered by the IT engineers:

1. Variety of products each has its own management interface.
2. Not easy for integrated planning and management.
3. Unable to provide integrated architecture for enterprise VPN and enterprise Intranet.
4. Unable to integrate the related information of each regional network.
5. Unable to provide the integration for the error detection system and reports.
6. Unable to provide the tunneling route analysis for the data flow path.
7. Unable to provide the traffic and efficiency analysis for the data flow path.
8. Unable to integrate with VPN products and general network management tools.
9. Unable to provide integrated automatic warning mechanism.
10. Unable to execute the back-up policy to solve the network termination problems.

The above problems that needs to be resolved, the system still requires to provide with the conveniences for easy installation, easy usage, remote manageable, easily expand, and only spend little bandwidth for transmitting monitor and management information.

Hence, the requirements for enterprise VPN monitor and management system are as following:

1. Web-based management interface, which provides convenient and integrated user interface; with easy installation and usage, allow remote execution.
2. The system architecture work with huge network, and easy to expand.
3. Delivers the monitor and management information with low network traffic load.
4. Provides policy-based management for integrated enterprise VPN management and Intranet network.
5. Shows VPN architecture and enterprise Intranet architecture.
6. Integrates all related information of each region.
7. Provides the integrated error detection system and reports.
8. Routing analysis, traffic flow analysis, and efficiency analysis for the data flow tunnel.
9. Integrates with VPN products and network management tools in general.
10. Provides the mechanism for both automatic warning and execution for backup operation.

4.2. The proposed architecture

4.2.1. System architecture

As shown in Fig. 3, this system provides Web-based management interface, and integrates with the policy-based management, mobile agent, VPN monitor and management capability and network monitor and management capability in general.

The management architecture of such system includes 4 layers: the first layer is application layer, which is the interface for the usage of this system; the second layer is information management layer, for the saving and integration of the related information required by the system; the third layer is policy control and translation layer, the executing of the policy enforcement layer; the fourth layer is policy enforcement layer, enforcing the policies.

The mechanism of the mobile agent is: policy control and translation layer proceeds with the policy decisions and converts the policy into the mobile agent code, and sends the policy enforcement points of the required enforcement policies to the mobile agent, the policy enforcement points enforces such mobile agent, and then transmits the result back to policy control and translation layer through the mobile agent.

4.2.2. System components

As shown in Fig. 4, system components contain Web-based management superset, mail server, directory server, resource server, policy and mobile agent server and each policy enforcement points. Each system component is explained, respectively, as the following:

(1) Web-based management superset:
- Web server, the program group of the Web server end and the Web-based Management console of the client end.

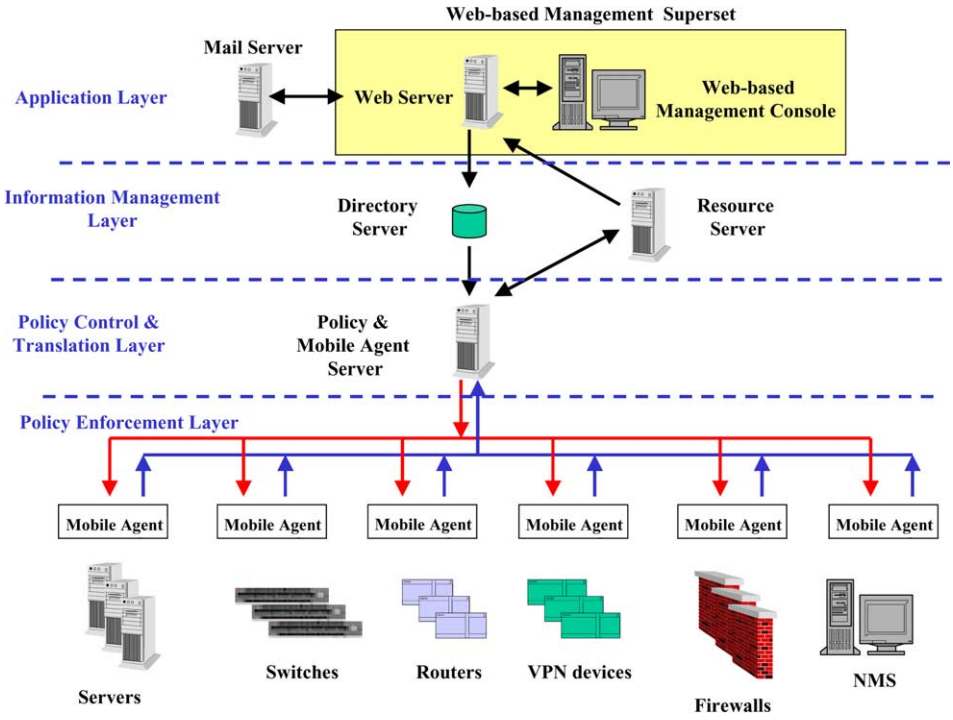

Fig. 3. The architecture of enterprise VPN monitor and management system.

- The program of the Web client end and Web server end can communicate through CGI.
- Web-based interface, it also offers remote management capability for the managers apart from convenient usage for the users.
- Integrated policy-based management and manages VPN and Intranet networks.
- Provides integrated reports and diagrams charts, integrated error detection tools, and automatic warning capability.

(2) Mail server:
- Provides mail service.

(3) Directory server:
- May be a catalog system, or a data base system.
- Saves the integrated policy of the VPN and Intranet network.

(4) Resource server:
- Resource information integrator, resource information database, and resource reporter.

(5) Policy and mobile agent server:
- Policy decision and mobile agent manager, two roles in the same machine. The part of policy decision includes policy validation, policy decision, and action records. The part

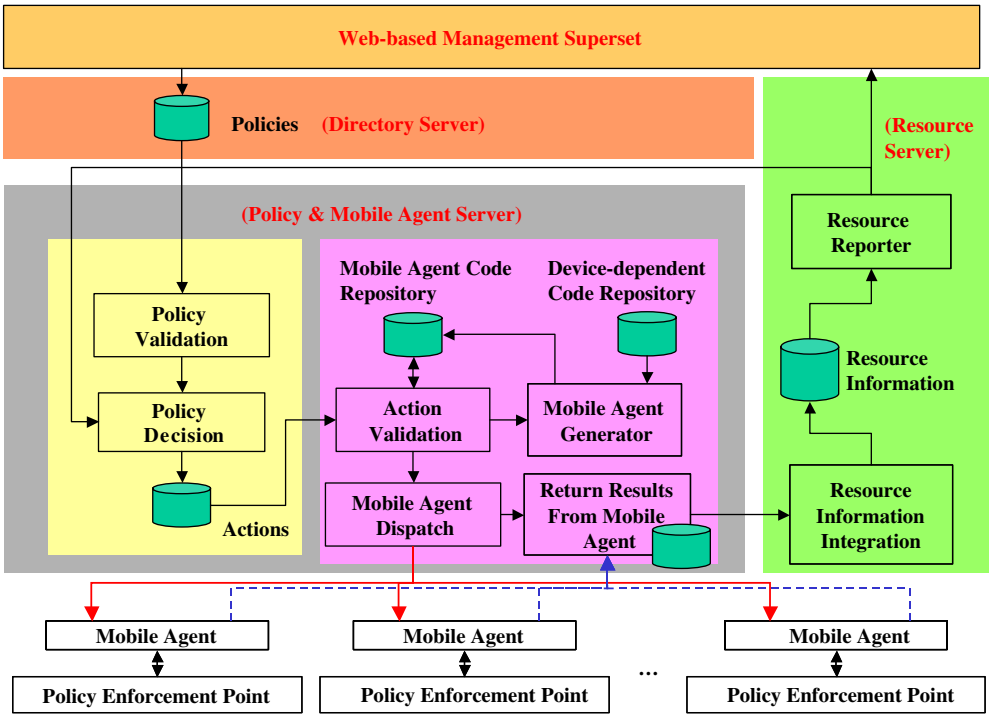

Fig. 4. System components and system operation flow.

of mobile agent manager includes action validation, mobile agent generator, device-dependent code repository, mobile agent code repository, mobile agent dispatch, return results from mobile agent.

(6) Policy enforcement point:
- Each network devices (routers, switches), VPN devices, firewall, general network management tools, network servers, etc.

4.3. Operation process

4.3.1. System operation process

The detail operation system process as shown in Fig. 4, can be divided into four phases.

(1) *Policy setup and decision phase:* the manager enforces the program of the Web server end through Web-based management superset. It via CGI to request resource reporter within the resource server to be saved in the last updated network status of the resource information database. Through the program of the Web server end to read all of the last updated network management policies from the Directory Server, and to understand the current network conditions and policy settings, then to set a new policy according to the manager's needs or to

revise the existing policy and saves the changes to the directory server. It also sends to policy and mobile agent server for the preparation work before enforcing the policy. Among which, the policy is composed with numbers of rules in which the logic of service and resource allocations of each rule is defined by the method of IF ⟨condition⟩ THEN ⟨action⟩.
After policy and mobile agent server receives the policy changes, the policy validation checks if the new policy setting is executable and to further compare with the existing policy for any contradictions as it will immediately respond to the manager for confirmation or revision should problems occurs. If not, it will be processed by the policy decision component. Policy decision proceeds with the decision making process on which action to adopt. If corresponds to the condition, the action for such rule is enforced. Among which, policy decision will search for the required information condition from the resource reporter of the resource server to proceed with decision making. With the Action, it is then transferred to the action validation phase for policy translation.

(2) *Policy conversion phase:* action validation checks if the action has a corresponding mobile agent code; if not, the mobile agent generator will refer to the information of the device-dependent code repository to convert into mobile agent code, and saves this mobile agent code in the mobile agent code repository for the conversion usage by the same policy later. With the corresponding mobile agent code, it is transferred to the mobile agent dispatch component to start the mobile agent executing and reporting phase.
(3) *Mobile agent executing and reporting phase:* mobile agent dispatch distributes each mobile agents to each required policy enforcement points of this policy, and allows each policy enforcement points to execute the policy and report the information back to the policy and mobile agent server.
(4) *Result integrating phase:* policy and mobile agent server transfers the information that has been reported back from the mobile agent to the resource information of the integrator resource server for information integration, and to utilize this integrated information to update the resource information database. Resource reporter will then convert the lower level information from the resource information database needed by the managers into the higher level information that are more easily understood by the managers. When such information needed by the manager, Web-based management superset will convert the high level information generated by the resource reporter into Web charts or diagrams for manager's reference.

4.3.2. Hierarchical operation mechanism

The system provides hierarchical monitor and management model for the policy enforcement layer as shown in Fig. 5, policy and mobile agent server would know how many Web domains from the acquired network information through the resource server; the monitoring command and mobile agent code required by each region is transmitted to a certain policy enforcement points of each network region, the policy enforcement points would temporarily replace the policy and mobile agent server to provide the mobile agent code for other policy enforcement points of this Web domain; and to request for policy execution and reporting as well as integrating all collected information for such domain, and then report back to the policy and mobile agent server.

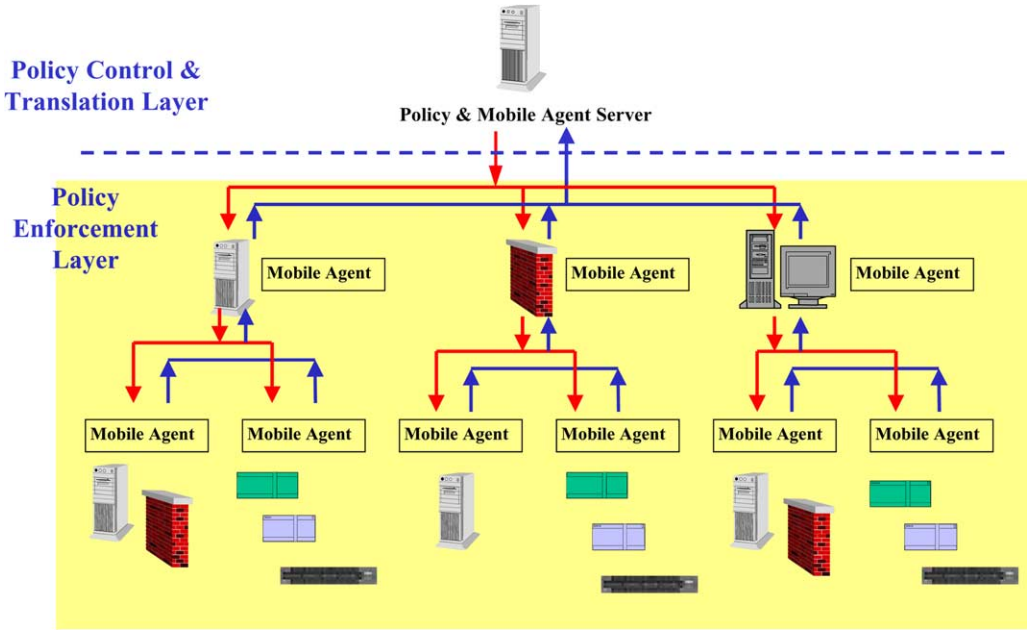

Fig. 5. The hierarchical operation mechanism for mobile agent.

4.3.3. Monitoring methods for VPN and general network devices

VPN products will go through the pockets that correspond with the rules to carry out the process of encryption, and to establish the VPN tunnels for the VPN products of the packets delivery to the other receivers. Therefore, if such packet is intersected after the packets have been encrypted, it would be unable to know the content of the packet as well as the sender and the ultimate receiver of the packet. In order to solve the issue of unable to monitor the packets directly in the VPN tunnels, a software function is added to the VPN device products in which such software will communicate with the VPN products to intervene the executing programs of the VPN products directly, or for the VPN product to create files for each workgroup, rule files, or by intersecting or revising data of each diary log. If the current VPN environment setting can be understood according to each workgroup file and rule file, including those already established VPN tunnels; the executing status of the current VPN tunnels can be understood from each diary log, including the detection of any abnormal condition as well as information such as the application and traffic flow through VPN tunnels. Other monitoring methods of policy enforcement points also can apply the above mechanism for the VPN devices. If the policy enforcement points are unable to execute mobile agent directly, general PC or Unix workstation may be used as an agent computer to log into the mobile agent to communicate with such device to place commands and collecting information. With regard to the method of communication, taking router for instance, standard network communication protocol such as SNMP or COPS can be used, or by remote usage program such as telnet command to log into the router then search for the workgroup settings or change the workgroup settings of the router according to the exclusive command of the router.

4.4. The capability of the enterprise VPN monitor and management system

The system may provide the enterprise VPN and Intranet network with the following monitor and management direct at the enterprises:

1. Web-based management interface and policy-based management for the enterprise VPN and Intranet network of the entire enterprise management.
2. Integrates the VPN and Intranet architecture, and related information of each region.
3. Integrated error detection system and reports.
4. Traffic flow, routing and efficiency analysis for the data flow tunnels.
5. Integration of VPN products and the network management tools.
6. Provides mechanism for integrated automatic warning and performance of backup operation.

Hence, according to above described functions, the system can provide the managers with efficient and easy to use monitoring and enterprise VPN management capabilities, which it will not take up large amount of bandwidth and hardware resources of the managing machine as the network management tools.

5. The prototype of enterprise VPN monitor and management system—as an example of semiconductor industry

5.1. Installation environment and architecture of the prototype system

Using the VPN architectures in semiconductor companies are as the references for the prototype system. Network architecture primarily contains two local area networks, similar to the local area network of the multinational communication headquarter of the semiconductor industry and the local area network of a branch office, in which every local area network all uses firewall/VPN devices and Internet to connect to the Internet in order to establish VPN tunnels on both ends to take advantage of VPNs low cost, inexpensive fees, excellent backup support, and the leased line to reduce the overall information cost for the enterprise and enhances the enterprise competitiveness. There is also a leased line connecting between the two local area networks, which is similar to the reason the semiconductor industry would lease the long distance/international leased line of smaller bandwidth because of their emphasis on the network efficiency and stability, to send the important information which requires instant reply.

The VPN architecture of this prototype has the following characteristics:

1. The functions of the firewall and VPN are run on the same machine.
2. Two local area networks have two site-to-site Intranet data flow tunnel for transmitting information, in which one uses VPN devices and the VPN tunnels set up on the Internet; the other one uses the leased line tunnels built by the leased line.
3. Different applications can use different tunnels according to the needs and characteristics.

4. When problem occurs on certain tunnel, the data flow would need to be guided to other normally operated tunnels.

The environment of the prototype system and software architecture is shown in Fig. 6. Among which, the functions of Client A for the Web server, directory server, resource server and LAN1 is centralized on one single computer for execution due to the resource constraint; the functions of Client B for Web-based management console, policy and mobile agent server and LAN2 is centralized on another computer for execution.

5.2. The prototype system

5.2.1. Web-based management console

Management console is a Web-based GUI, which does not require additional installations and setting. The managers can use it at any time, any place, and can also link back to the office through the use of VPN. Before usage, the account number and passwords are needed for user authentication.

5.2.2. Policy-based management function

(1) *Routing policy setting function:* the primary routes and backup routes can be set according to the enterprise requirements. Moreover, one can choose if allows the system to initiate the

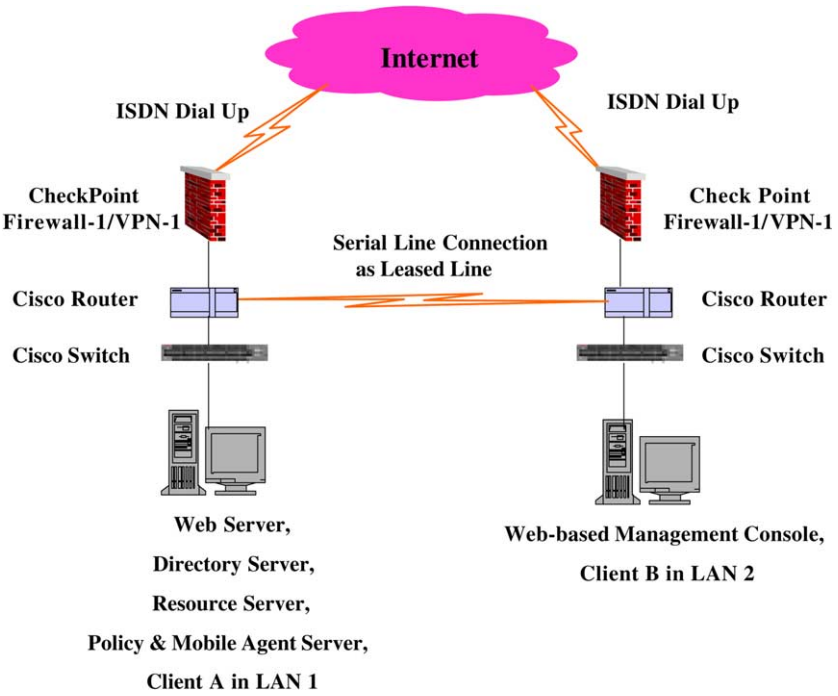

Fig. 6. The environment, software and hardware of the prototype.

detection for the status of the main route. If the main route is down, the system will switch to the backup routes and the system will activate the backup policy instantly to modify the related devices.

(2) *Management report setting function:* the network topology or abnormity report could be activated according to the settings demanded by the network manager. The focus of this prototype is the high level policy management instead of the discovery of all network devices, so the auto-discovery of network devices is not yet implemented and the manual input for device table is required currently. The network topology image is generated according to the device table and download from the Web server to the Web client that is operated by network manager. Once the require setting is done for the activation of the abnormity report, the system will detect the status of each network component on the regular basis. Should any abnormity occurs, apart from showing the time of the abnormity occurrence and the types of abnormity, the system will also record the result of the problem for the network manager to review within the Management Report function in order to trace the status of abnormity.

5.2.3. Management report function

(1) *Network topology function:* once this function is launched, according to the network information collected in advance, this system can automatically map out the current network topology, including VPN tunnels and Intranet tunnels. The illustration in Figs. 7–9 are the status of the network topology at the time when the system performs this function. It shows the related information of each network section, firewalls, VPN devices, routers and hosts, as well as the methods of connections.

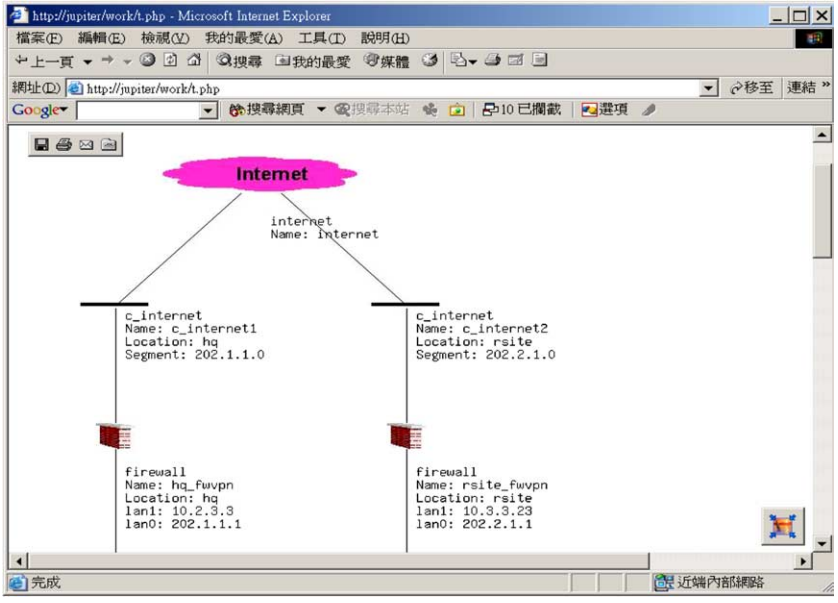

Fig. 7. Network topology.

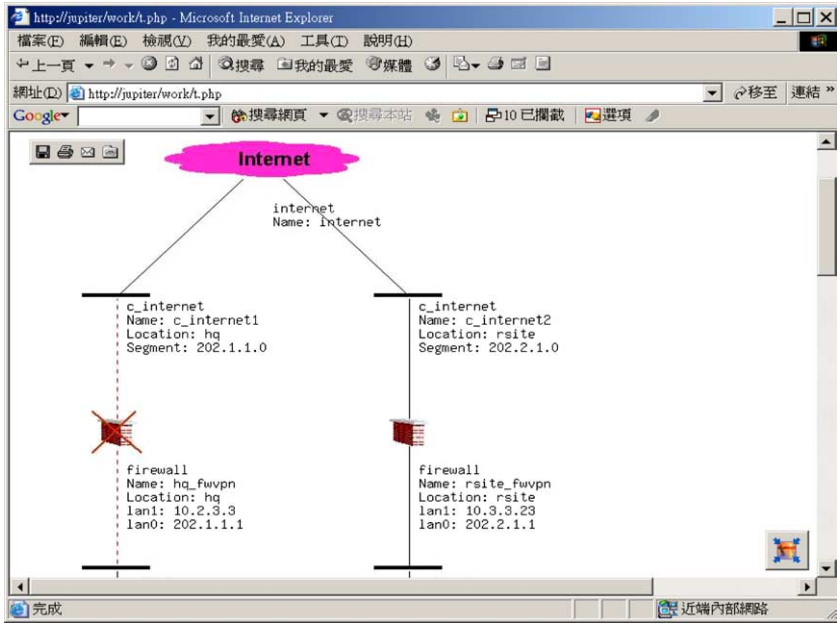

Fig. 8. Result of point of the breakdown detecting function.

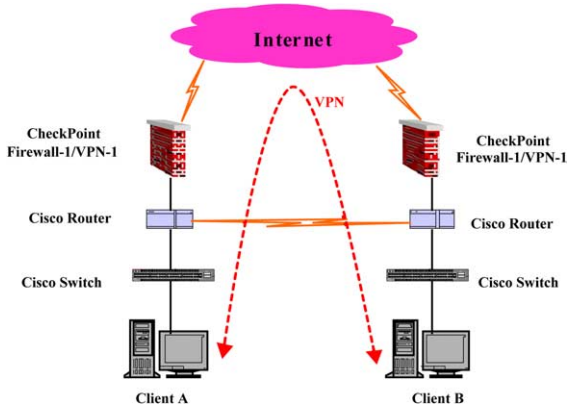

Fig. 9. Network status—normal condition.

(2) *Abnormal reporting function:* this function can show the time of the abnormity occurrence and the types of abnormity, time of the recovery, and the methods of handling by the system when various situations occurred.

5.2.4. Error detection tool function

(1) Point of the breakdown detecting function: as shown in Fig. 8, network point of the breakdown can be detected through this function in order to understand the reason for the current

down time, such as trouble in the router, firewall/VPN devices, Internet offline, or breakdown on a certain computer, etc. It can also be shown in the form of network topology, in which the location of the problem can be tell at a glance, which would be convenient for further handling by the network manager.

(2) Routing analysis function: it can analyze each network component as to which route was used for transmitting by the current related applications, which make it more convenient for the network manager to confirm on currently the most efficient and accurate route for transmitting data; and in the situation if the transmitting slowdown should occur, the network management tool can be used to perform investigation according to such route.

5.2.5. *Simulation test*

The procedures for the simulation test are as follows:

(1) Observing the data flow—via VPN: as shown in Fig. 9, two computers are communicating through the use of VPN.
(2) Internet connection failure—automatically switch to VPN route through leased line: disconnect the Internet hookup; system automatically detects the Internet connection failure and performs automatic modification for the related setting; automatically switching from the VPN route to leased line.
(3) Once again observing the data flow—via leased line: as shown in Fig. 10, two computers are communicating via the use of the leased line.
(4) Internet connection restores—automatically switches to VPN route: reconnect the Internet hookup; system automatically detects the recovery of the Internet connection and automatically performs the modification of the related settings; automatically switches the VPN.

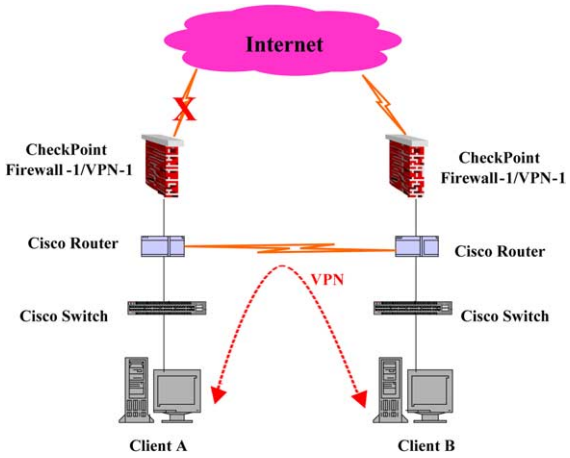

Fig. 10. Network status—Internet offline.

5.3. Result analysis and comparison

5.3.1. Analysis and comparison of the system functions

The distinctions between the proposed architecture of enterprise VPN monitor and traditional centralized network management system are shown in Table 1. The proposed Architecture is a feasible and Web-based interface. It provides a convenient and easily installed and used to enable remote execution. It provides high level policy-based management for the overall enterprise VPN and Intranet network. It also can simultaneously show the architecture of VPN and enterprise Intranet, and can provide the integrated error detection system and reports. Enhancing efficiency and saving network bandwidth, adopting the mobile agent and hierarchical operation mechanism, enhancing overall system operating efficiency. Perform VPN and routing analysis for data flow tunnel of site-to-site Intranet, traffic flow analysis, and efficiency analysis. It can provide with automatic warning function and performs integration and analysis; to locate the most possible breakdown point according to the information of network architecture; as well as automatically performs backup operation according to the policy.

Table 1
Functional comparisons with the conventional centralized network management system

	Convention centralize network management system	The proposed enterprise VPN monitor and management system
User interface	Mostly adopts the GUI researched. It takes time to learn the GUI	Web-based interface, convenient and integrated user interface easy installation and usage, offer remote execution
Police-based integrated management	No policy-based management and integrated report, no integrate management of VPN and Intranet. Only well-trained manager can manage network	Provides policy-based management, integrated information and integrated report; easily monitor and manage the enterprise network without manual connection and setting for each network device; easier to use and manage
Network traffic and performance impact	The centralized monitor and management approach introduces excessive processing load and heavy network traffic	Mobile agent and hierarchical operation results low transmission data volume Higher efficiency and easy to expand
Routing analysis for the data flow	Only manually login and extract information on specific devices	To know the existing settings for each data flow tunnel and which router and VNP device it passes through; and know the currently used data flow tunnels
Tunnel traffic analysis for the data flow	Only provides general traffic information	Integrate with Internet network traffic and traffic flow information of VPN virtual tunnel application on the Internet link
Efficiency analysis for the data flow tunnel	Unable to provide the efficiency analysis for the VPN virtual data flow tunnel	Analysis the integrated efficiency of VPN and Intranet tunnel, and to know currently loaded to capacity
Integrated auto-warning and auto-backup mechanism	Unable to provide the integrated auto-warning and auto-backup mechanism	Policy enforcement points can automatic warning according policy demand, point out the failed devices. Auto-backup operation to reduce the off time of enterprise network

5.3.2. Comparisons of the simulation results

If without this prototype system, the simulating case would require the following steps in order for the enterprise operation to be restored by the network manager

(1) Observing VPN data flow—via VPN: as the architecture shown in Fig. 10, two computers are communicating via VPN, requires the network manager that are familiarized with network management to proceed.
(2) Internet connection failure—manually switches from VPN route to leased line: disconnect the Internet hookup; user cannot use VPN network; the system administrator needs to locate the breakdown point and manually connects to the related devices for settings; after the setting is completed, performs self test to confirm the routing modification is correct.
(3) Again observing the data flow—via leased line: two computers are communicating via the leased line; requires the network manager that are familiarized with the network management to proceed with observation with the use of network management tools and commands.
(4) Internet connection restored—manually switches to VPN route: since switching from VPN route to leased line is a backup plan, which would make the leased line extremely busy, and hence decreases the important application efficiency of the original leased line. Therefore, as soon as the Internet connection is restored to normal, it is best to switch the route to VPN in order to release the leased line bandwidth back for the original important application usage. However, the network manager would need to observe constantly if the Internet connection has indeed restored, which not only a waste of human resource but may result in the line not been switch back to the VPN route after the recovery of the Internet connection due to the negligence by the network manager, when the network manager realizes the Internet connection is back to normal, manually connect to the related devices to proceed

Table 2
Comparison of the results for before and after using prototype system for the simulation test

	After the use of the prototype system	Before the use of the prototype system
Execution time	Allows the system to automatically execute according to the policy, in which the time required for execution is shorter	Requires network manager to determine the breakdown point and try to manually handling the problem, which takes more time to execute
Execution	Prototype is easy to understand and use, even the backup network managers also can manage well. Authorized managers, agents, and each network manager all use this system to easy execution	Only the well-trained network managers are familiarized with firewall, router and network management. However, all the tasks are executed manually, the human errors might be happen
Enterprise operation	The system automatically switches the route in order for the transmission of the enterprise information to be restored within a very short period of time	Excessive time spent on fixing the problem, the transmission for the enterprise information need a long time, which affects the enterprise operations
Enterprise costs	The enterprise cost is reduced since the VPN recovered in the shortest time, once Internet is up. Enterprise can save much money for the backup plan of each route	The unstable routes may be affecting the enterprise operation, the enterprises are required to spend huge fees on making separate backup plan for each route

with the setting is required; after the setting is completed, automatic self test will be performed to confirm the routing modification is correct.

The comparison of the results as shown in Table 2.

6. Conclusion

The proposed enterprise VPN monitor and management system architecture, adopting policy-based management and mobile agent mechanism, with high level management and low network traffic loading features, could integrate the VPN and Intranet. Enterprise VPN monitor and management system can be a reference for the enterprises in general to develop their own monitor and management system in order to solve the enterprise VPN management problem; it can also be a reference for the firms in commercial development of network management system.

This paper proposes an architecture for the enterprise VPN as well as Intranet monitor and management system, and establish a prototype, with the result roughly as shown following:

1. *Architecture of enterprise VPN monitor and management system:* to propose a feasible and needed monitor and management system architecture, including system components, operation flow and all the required functions.
2. *With Web-based management interface:* to provide a convenient and integrated user interface that's easily installed and used, as well as enables remote execution.
3. *Integrated policy-based management:* to provide high level policy-based management for the overall enterprise VPN management and Intranet network. It can simultaneously show the architecture of VPN and enterprise Intranet, and can also provide the integrated error detection system and reports.
4. *Enhancing efficiency and savings on network bandwidth:* adopting the mobile agent and hierarchical operation mechanism; enhancing overall system operating efficiency, and savings on the network bandwidth.
5. *Analysis for the data flow tunnel:* it can perform VPN and routing analysis for data flow tunnel of site-to-site Intranet, traffic flow analysis, and efficiency analysis.
6. *Automatic warning and automatic execution of backup operation:* it can provide with automatic warning function and performs integration and analysis; to locate the most possible breakdown point according to the information of network architecture; as well as automatically performs backup operation according to the policy.
7. *Testing and verification of the prototype system:* the establishing of the prototype system and the execution of the simulating cases to test and verify the feasibility and advantages of this system.

The above results can help the semiconductor companies to monitor and manage their enterprise VPN with efficient, utilizing the network resources and reduce the possible downtime during the operation. Hence, the convenient and effective management tools are required in order for the enterprises to rest assured for using the new information technology. The proposed system architecture make the system conveniently and more effectively monitoring and managing the enterprise VPN.

Therefore, the enterprises would be more willing to use the VPN that can save a great amount of expenses and to expand on the area of usage in order to enhance the overall enterprise efficiency.

References

[1] Wang C. Policy-based network management. In: International conference on communication technology proceedings, vol. 1, 2000. p. 101–5.
[2] Nomura Y, Chugo A, Adachi M, Toriumi M. A policy based networking architecture for enterprise networks. IEEE Int Conf Commun 1999;1:636–40.
[3] Vu Anh P, Ahmed K. Mobile software agents: a overview. IEEE Commun Mag 1998.
[4] Gray RS. Agent Tcl: a flexible and secure mobile-agent system. In: Proceedings of the fourth annual Tcl/Tk workshop, 1997.
[5] Bieszczad A, Pagurek B, White T. Mobile agents for network management. IEEE Commun Surveys 1998;1(1):2–9.
[6] Puliafito A, Tomarchio O. Advanced network management functionalities through the use of mobile software agents. In: Proceedings of the 3rd international workshop on intelligent agents for telecommunication applications (IATA'99), LNCS, vol. 1699, 1999. p. 33–45.
[7] Gunter M, Braun T. Internet service monitoring with mobile agents. IEEE Network 2002;16(3):22–9.
[8] Liu Zg, Wang Gx. An approach to distributed heterogeneous network management of mobile agent architecture based. Int Conf Intell Agent 2001;2:228–33.
[9] Zhang D. Network management using mobile. Int Conf Intell Agent 1998;2:5.
[10] Lefebvre J, Chamberland S, Pierre S. A network management framework using mobile agents. IEEE CCECE'03 2003;2:737–40.
[11] Kona MK, Xu C-Z. A Framework for network management using mobile agents. In: Proceedings of international conference on parallel and distributed processing symposium, IPDPS 2002. p. 227–34.
[12] Buchanan WJ, Naylor M, Scott AV. Enhancing network management using mobile agents. In: Proceedings of seventh IEEE international conference and workshop on engineering of computer based systems, 2000. p. 218–26.
[13] Papavassiliou S, Puliafito A, Tomarchio O, Ye J. Mobile agent-based approach for efficient network management and resource allocation: framework and applications. IEEE J Sel Areas Commun 2002;20(4):858–72.
[14] Gavalas D, Greenwood D, Ghanbari M, O'Mahony M. Advanced network monitoring applications based on mobile/intelligent agent technology. Comput Commun J 2000;23(8):720–30.
[15] Chou L-D, Tang K-C, Kao C-C. Multiple/mobile-agent-based network management systems for Taiwan's national broadband experimental networks. In: IEEE global telecommunications conference, GLOBECOM '02, vol. 2, 2002. p. 1975–9.
[16] Kim EC, Hong CS, Song JG. The multi-layer VPN management architecture. In: Proceeding of the sixth IFIP/IEEE international symposium on distributed management for the networked millennium, 1999. p. 187–200.
[17] Qiu X, Xiong A, Meng L. The study and implementation of the VPN service management system. In: Fifth IEEE symposium on computers and communications, 2000. p. 66–71.

Ruey-Shun Chen is an associate professor in the Institute of Information Management, National Chiao-Tung University. He received his PhD in Department of Computer Science and Information Engineering, National Chiao-Tung University. His research interest: Information System Applications, Internet Networks, Information system Management.

Change-Jen Hsu is a PhD Student, Institute of Information Management, National Chiao-Tung University in Taiwan. Research Interest: VPN, Network, Internet Networks, Information Management.

Chan-Chine Chang is a PhD Student, Institute of Information Management, National Chiao-Tung University in Taiwan. Research Interest: Network, Internet Networks, Information Management.

S.W. Yeh is a Master Student, Institute of Information Management, National Chiao-Tung University. Research Interest: Information Retrieval, Internet Networks, Information Management, Enterprise resource Planning.