GOE (Global Open Ethernet) Concept of Ethernet-Based Reliable, Scalable, and 'Plug & Play' VPN

By Kazuo TAKAGI,* Atsushi IWATA,* Masaki UMAYABASHI,*
Youichi HIDAKA,* Nobuyuki ENOMOTO* and Akira ARUTAKI*

ABSTRACT We propose a GOE (Global Open Ethernet) concept for supporting next-generation provider- and customer-managed Ethernet VPNs, and also present technical detail of GOE tag-switching technology especially for provider-managed VPNs. Next-generation provider-managed VPN services are expected to cost-effectively provide transport functions that are almost equivalent to STM ones, such as reliability and scalability, since they are becoming a lifeline as an alternative to STM-based leased-line ones. On the other hand, with the spread of customer-managed VPNs and broadband access, next-generation customer-managed VPNs are expected to support not only 'site-to-site' and 'person-to-site' connectivity but also 'group-to-group' and 'person-to-person' connectivity. Such VPNs should be required to be based on 'plug & play' technology so that customers can use these networks easily without any security problems. In order to meet these requirements, we propose a GOE concept which is to provide a world-wide Ethernet access to any person, from anywhere, anytime, with 'plug & play.' We approach toward the concept with two categories of GOE technologies. One is based on GOE tag-switching technology, which gives transport functions that are almost equivalent to SONET/SDH ones, to provide scalable and reliable Ethernet networks for provider-managed VPN. The other is based on Ethernet-over-ANY technology called GOE-VPN, which transports Ethernet frames transparently between any sites and/or persons with ease, to provide ubiquitous Ethernet access scheme. GOE would be a driving force for evolving Ethernet to a world-wide network and much wider spreading of Ethernet-based VPNs.

KEYWORDS **Ethernet, VPN, GOE (Global Open Ethernet), VLAN-tag stacking, Protection, Plug & play**

1. INTRODUCTION

Many enterprise customers are rushing to shift from costly STM-based leased-line services to affordable provider-managed VPN (Virtual Private Network) ones, providing virtual fixed 'site-to-site' leased-line connections and networks for data transport. Since such provider-managed VPNs will be used as an alternative to STM-based leased-line, next-generation provider-managed VPNs are expected to provide transport functions that are virtually equivalent to STM ones, such as reliability, scalability, and QoS guarantee. On the other hand, with the spread of customer-managed VPNs and broadband access based on ADSL or FTTH technology which is available not only in homes but also at hotels, coffee shops, airports, and transit stations, the enterprise customers can build their own 'site-to-site' and 'person-to-site' VPNs on demand so that a member can dynamically access his or her LAN from anywhere he or she uses the Internet. By using customer-managed VPN, a customer can build VPNs for dynamic collaborative projects with other companies in the business environment, and for privately family, friends, and Internet schools, according to her or his demand. This means that VPN provide not only 'site-to-site' and 'person-to-site' connectivity but also 'group-to-group' and 'person-to-person' connectivity and it should be 'plug & play' technology every customer can easily use the networks without any security problems.

In terms of provider-managed VPN services, cost-effective Ethernet VPN services have attracted a great deal of attentions. The Ethernet VPN services provide TLSs (Transparent LAN Services) [1] and VPLSs (Virtual Private LAN Services)[2] capable of connecting multiple sites in multipoint-to-multipoint connectivity, which will enable extended LANs to be built between remote business sites. Using Ethernet as a transport interface for enterprise customers is becoming a compelling and important point because Ethernet is an inexpensive and user-friendly technology that has become dominant in enterprises and data center networks. Using Ethernet as a switching technology is also important for SPs (Service Providers) because Ethernet technology provides a 'plug & play' switching that works well without provisioning immediately after the device is turned on, which also reduces the operating cost. Many SPs are now

*Systems Platforms Research Laboratories

rushing to build and promote Ethernet VPN services in metro area networks, as an affordable way to address enterprise customer needs. Since Ethernet technology was not designed for service provider use, Ethernet VPNs are usually built on MPLS (Multi-Protocol Label Switch)[3-6], RPR (Resilient Packet Ring)[7], and/or SONET/SDH technologies to complement the Ethernet technology. However, Ethernet VPNs based on these technologies have several technical problems in terms of simplicity, scalability, and flexibility. SPs are, thus, looking for other technology for their Ethernet VPNs.

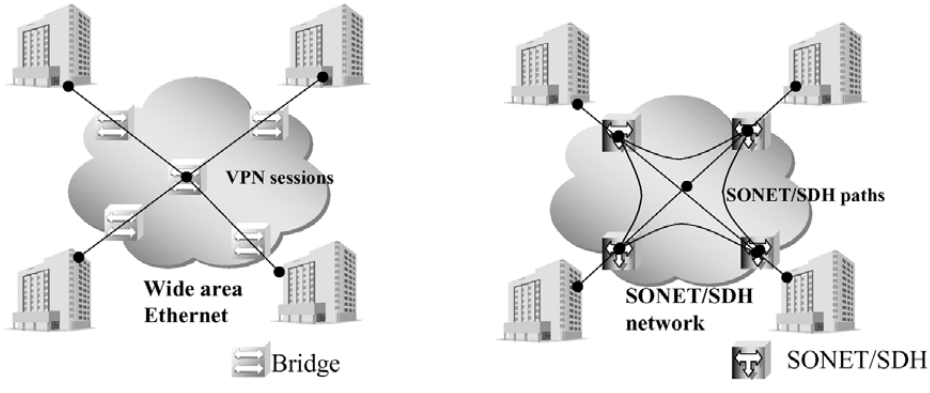
In terms of customer-managed VPNs, we can use L2TP (Layer 2 Tunneling Protocol)[8] and IPsec (IP security protocol)[9]. Although they can actually provide 'site-to-site,' 'person-to-site,' 'group-to-group,' and 'person-to-person' VPNs on demand, they are too complicated for customers to configure, even expert customers, since there are many parameters to set up to build VPNs. Customers expect to be provided 'plug & play' VPNs with security.

GOE (Global Open Ethernet) provides solutions for such provider-managed and customer-managed VPNs. Our GOE has been developed based on two technologies: GOE tag-switching technology to provide a transport scheme for provider-managed VPNs and GOE-VPN technology to provide 'plug & play' VPN establishment scheme for customer-managed VPNs.

This paper is organized as follows: In Section 2, we give requirements for next-generation VPNs. In Section 3, we focus on the problems of current technologies supporting provider-managed and customer-managed VPNs. In Section 4, we give a GOE concept and technical overview of GOE. We present a technical detail of GOE tag-switching as an infrastructure supporting Ethernet VPN services in Section 5. We conclude the paper in sections with a summary.

2. REQUIREMENTS FOR NEXT-GENERATION VPNs

Provider-managed VPNs basically provide enterprise customers with private networks connecting fixed remote business sites, such as branches and the headquarters. **Figure 1** shows an example of the provider-managed Ethernet VPN architecture for multipoint-to-multipoint services and the SONET/SDH path network architecture for leased-line services. As shown in Fig. 1(a), VPN connections and sessions are established between the customers' devices and the bridge provided by SPs. Packets sent from the devices though the VPN connections or sessions are forwarded to other devices via the bridge. The VPN services require only *O(N)* connections (*N*: number of sites to connect), whereas STM-based leased-line services require *O(N^2)* connections to provide a full-mesh network comprising any-to-any connections, as shown in Fig. 1(b). This means that VPN services are for less expensive to provide than STM-based leased-line ones. Therefore, many enterprise customers will obviously shift to VPN services in the future. When they begin to use VPN services to transport the same application data they transport using in the STM services, they will expect next-generation provider-managed VPNs to provide the same transport functions as SONET/SDH ones: protection, bandwidth guarantee, delay guarantee, jitter



(a) Ethernet VPN. **(b) VPN using SONET/SDH.**

Fig. 1 Private network architectures using Ethernet VPN and SONET/SDH leased-line services.

guarantee, etc.

On the other hand, customer-managed VPNs can be dynamically built over the Internet by providing peer-to-peer connections between remote sites, whereas provider-managed VPNs are built statically over SP networks prepared for the VPNs. Although customer-managed VPNs have been used to connect the remote business sites ('site-to-site'), they are evolving into a scheme to connect dynamically a person to site ('person-to-site'), as shown in **Fig. 2**. As organizations in companies move from having fixed structures to having flexible ones, and as groups and persons in organizations often join dynamic collaborative projects with other organizations, teams, groups, or companies, such VPNs will evolve into 'group-to-group' and 'person-to-person' VPNs. This means that many VPN communities will be created or removed on demand, and that the number of members of VPN community will become smaller and its number of VPNs become significantly larger. In 'group-to-group' and 'person-to-person' VPNs, a person might actually require access to multiple VPNs, or different communities, at the same time.

Such VPNs have a potential to be expanded to personal use. The persons of a VPN would comprise a specific small community of interest, such as a family, a group of friends, or an Internet virtual school, as shown in **Fig. 3**. If such VPNs become widespread, a person would be surrounded by many kinds of business and personal VPNs, as shown in **Fig. 4**.

Achieving such VPNs requires that the operation of the VPN access be simple for everyone, including the elderly and the young. Current VPN technologies are too complicated for people to configure the network resources, even if they are experts. For example, when people access a VPN using IPsec[9], as a major customer-managed VPN protocol, they have to manually configure the network resource identifications (printers, servers, PCs and etc.), whereas manual configuration is not needed for Ethernet because their terminals automatically configure the network resources immediately after a person accesses the LAN. In other words, if customer-managed VPN services provide automatic configuration functions for accessing the network resource as if the users were using a LAN through Ethernet, the access complexity will be reduced drastically. People will of course expect to be provided with 'plug & play' personal VPN services on demand.

Figure 5 shows an image of a next-generation provider-managed VPNs and customer-managed business and family VPNs managed by SPs. Since next-generation provider-managed Ethernet VPN will be used as an alternative to SONET/SDH leased-line, it is required to:

· Be based on the low cost technology to support VPNs,

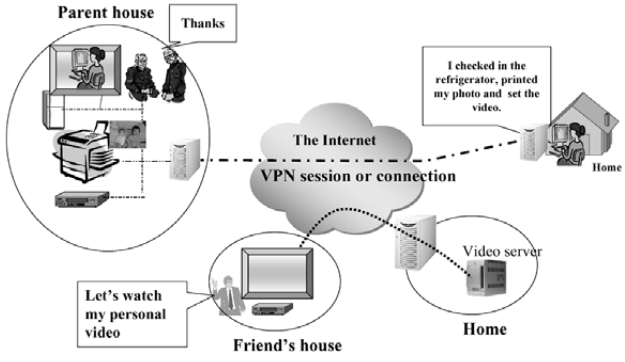


Fig. 3. An example of personal VPNs.

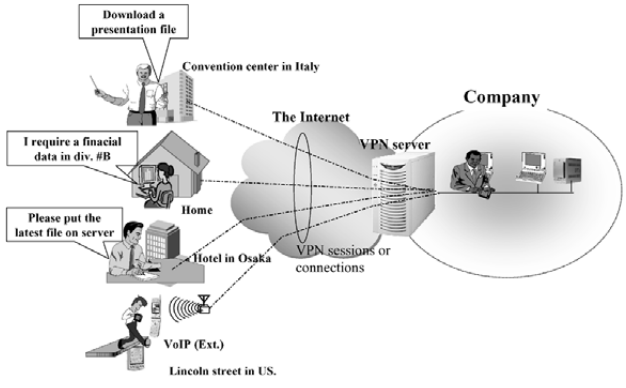


Fig. 2 Customer-managed VPN.

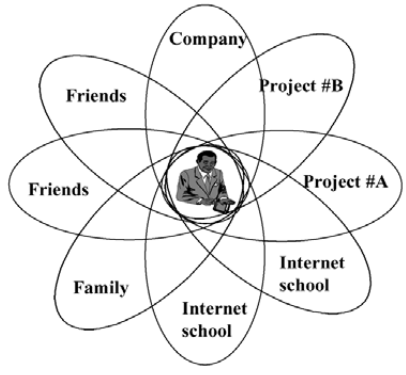
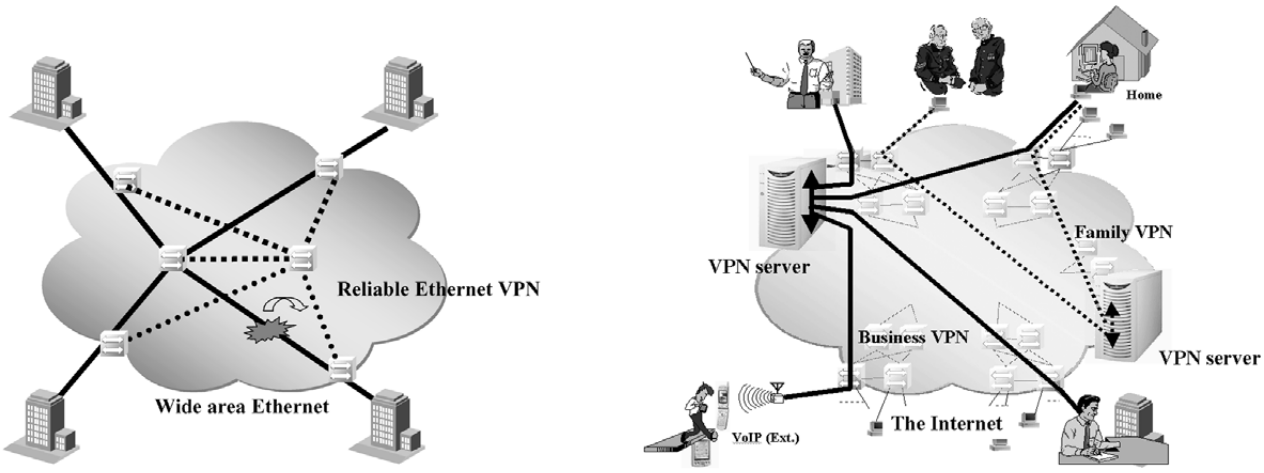


Fig. 4 Business and personal VPNs surrounding a person.



(a) Provider-managed VPNs. **(b) Customer-managed VPNs.**

Fig. 5 Next-generation provider-managed and customer-managed VPNs.

· Provide fast restoration that is almost equivalent to that provided by SONET/SDH technology,
· Accommodate up to several hundred thousand or one million enterprise customers, and
· Provide QoS functions.

On the other hand, next-generation customer-managed VPN technology supporting 'person-to-person' VPN on demand is required to:

· Provide on-demand VPN creation/removal function
· Provide 'plug & play' VPNs without complicated configuration, and
· Allow people to access many person-to-person VPNs simultaneously.

In short, transport technology is the key for next-generation provider-managed Ethernet VPNs, and flexible and easy access is the key for next-generation customer-managed VPNs. In the next section, we focus on current available VPN solutions and discuss the technical issues of them.

3. TECHNICAL PROBLEMS OF CURRENT AVAILABLE SOLUTIONS

In this section, we discuss the technical problems with Ethernet transport for current provider-managed Ethernet VPNs and describe the current available solutions. We also discuss customer-managed VPN solutions supporting 'person-to-person' VPNs.

3.1 Transport Technology for Provider-Managed Ethernet VPNs

Ethernet technology[10] specified by the IEEE 802 committee is designed for private LANs/MANs/WANs. Simply applying conventional Ethernet onto the SP networks causes several technical problems to solve.

(1) Low Reliability

· Several-second failure recovery

The rapid spanning tree protocol (RSTP) can provide fast restoration (~1sec) in the case of fiber and bridge failures but not for root bridge failures. Recovery from a root bridge takes several seconds, even with RSTP, because the whole spanning tree configuration must be completely changed.

(2) Low Scalability

· Small number of VLAN IDs

SPs require millions of VLAN IDs to identify all their customers or customer groups in order to provide VPN services. However, in the IEEE 802.1Q specifications, the number of VLAN IDs is at most 4096.

· Explosion of MAC address entries in forwarding database (FDB).

For SPs with hundreds of thousands or millions of

customers, the bridges have to learn and manage the same number of MAC addresses and VLAN IDs for forwarding purposes. When the bridges forward an Ethernet frame, they must search for one entry among thousands or millions of entries in the forwarding database at rate of 10Gbps or more. This requires a complicated and costly search engine.

(3) Controllability and Manageability

· Non Optimal Forwarding Route

Ethernet frames are transported over a spanning tree, which provides cost-effective routes between the root bridge and other bridges. However, it does not always provide the most cost-effective routes between any two bridges.

· Not In-Service Reconfiguration

When a bridge is inserted into or removed from the Ethernet network, the spanning tree must be reconfigured. The bridges stop forwarding Ethernet frames until the reconfiguration become stable, which takes several seconds.

There are four approaches to resolve these problems: Ethernet over MPLS (EoMPLS), Ethernet over RPR (EoRPR), VLAN tag stacking (Q-in-Q), and MAC encapsulated in MAC (MAC-in-MAC [11]).

In the EoMPLS approach, Ethernet frames are transported on label switched paths (LSPs). EoMPLS takes advantage of all the functions that MPLS provides, such as fast network provisioning, fast failure recovery (roughly equivalent to that of SONET/SDH), MPLS-based VPN management, and traffic engineering. However, because LSPs must be established between any two EoMPLS bridges in full mesh network, this solution is complicated and not scalable. In addition, an expensive router platform is needed to provide Ethernet VPN.

RPR is specified in IEEE 802.17. The RPR solution provides fast restoration (~50ms) (almost equivalent to SONET the protection time), but can be applied to only a single ring network so scalability and flexibility are problematic. This configuration constraint results in inefficient infrastructure upgrades if accurate demand forecast is not accurate.

Q-in-Q and MAC-in-MAC are legacy-Ethernet-friendly technologies. Q-in-Q improves the VLAN ID scalability by adding a VLAN-ID space, and MAC-in-MAC reduces the number of MAC address entries in the FDB by using MAC address aggregation. Both technologies are useful for improving scalability, but they do not solve the reliability, controllability, and manageability problems.

Thus, although current Ethernet VPN approaches solve some or parts of the problems with conventional Ethernet, none solves all of the problems.

3.2 Customer-Managed VPN Technology

VPNs are built over shared networks using tunneling protocols with security functions, as shown in **Fig. 6**. VPN members at remote sites can access their VPNs through Internet after establishing the point-to-point connections or sessions with VPN servers in the demilitarized zone deployed in their networks.

Several kinds of tunneling protocols can be used to access the VPNs: the L2TP (layer 2 tunneling protocol), IPsec, and SSL. As described above, next-generation customer-managed VPNs require a capability of creating 'person-to-person' VPNs easily. In this section, we evaluate the features of these tunneling protocols using the model shown in **Fig. 7**.

(1) L2TP[8]

L2TP provides data link tunnels using the PPP (Point-to-Point Protocol) specified in RFC 2661.

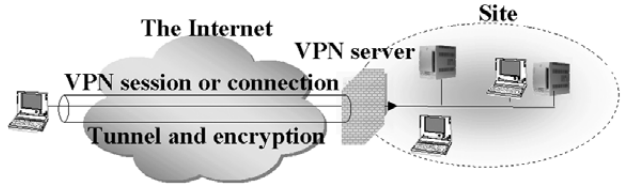


Fig. 6 Principle of tunneling protocol.

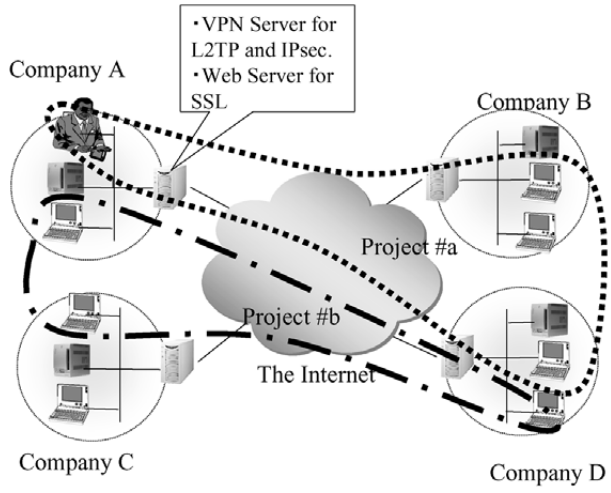


Fig. 7 A model used for evaluating VPN technologies.

Provided that company A has an L2TP VPN server, a member in project #a or project #b can access the other members belonging to same project with Ethernet access after establishing the VPN session with the L2TP server. It is easy to configure the network resources because the network resource information is automatically given through the VPN via the LAN resource management servers. However, if project #a and #b use the same L2TP VPN server, the members in project #a can view the files belonging to project #b. To avoid this situation, company A must separate them, using VLAN and/or filtering technologies, such as MAC and IP filtering, which is difficult or nasty to manage.

(2) IPsec[9]

IPsec provides secure IP tunnels with authentication, encryption, and security functions. Provided that company A has an IPsec VPN server, a member can access other members who have IP access, after establishing a VPN session with the VPN server. In this approach, the members are required to configure the network resource information (IP addresses for their terminals, the printers, other PCs, and servers) in advance. They also must manually set the parameters to secure the IP tunnels. This is a complicated process for general members. In addition, if project #a and project #b use the same IPsec VPN server in company A, the members in project #a can view the files belonging to project #b. To avoid this situation, the company A must separate them using IP filtering technology, which is again difficult or nasty to manage.

(3) SSL[1]

SSL provides tunnels at layer 5, which is the session layer of the OSI stack. SSL works across a variety of socket-based Internet protocols, including HTTP. It is widely used to provide secure Web commerce, but it is increasingly being used for secure remote access VPNs. A member can easily access file servers using standard browser without special software installation, if company A allows the members to access file servers inside company A. Applications over SSL, however, are restricted.

Considering that next-generation customer-managed VPNs should be based on 'plug & play' technology, these current approaches are not suitable. We now are discussing the solutions to solve these issues.

4. GOE CONCEPT

We propose a GOE concept which is to provide a world-wide Ethernet access to any person and/or any site, from anywhere, anytime. GOE solutions based on the concept provide Ethernet-based reliable and scalable provider-managed VPNs, and Ethernet-based 'plug & play' customer-managed VPNs capable of building 'person-to-person' VPNs. Such GOE solutions would be a driving force for evolving Ethernet to world-wide networks and much wider spread of Ethernet VPNs.

Provided that provider-managed Ethernet VPN services have reliability and scalability, SPs can offer them as a cost-effective lifeline to the customers and can expand Ethernet VPN markets from metro area to global wide area. From customer point of view, although several customers could require two different VPNs where one of them is used as a backup in case of failures, they do not require such a backup VPN which leads to raise the cost in the reliable Ethernet VPN service. By achieving reliability and QoS, customers can transport time- and failure-sensitive applications, such as VoIP, via such Ethernet VPNs, as an alternative to STM-based lines.

On the other hand, provided that Ethernet-based 'plug & play' customer-managed VPNs are achieved, customers can establish their own VPNs on demand and can share the network resources, such as the files and printers, easily. Such VPNs will impact customer business style, because customers can create VPNs at anywhere they can access the Internet, such as coffee shops. The VPNs will impact customer personal life as well, as described in Section 2.

To achieve the concept, we propose GOE technologies for provider-managed VPNs and customer-managed VPNs, respectively. One of GOE technology for provider-managed VPNs is based on tag-switching which gives transport functions that are almost equivalent to SONET/SDH ones. Another GOE technology for customer-managed VPN is based on Ethernet-over-ANY technology called GOE-VPN, which transports Ethernet frames transparently between any sites and/or persons with ease, to provide ubiquitous Ethernet access scheme. **Figure 8** shows an overview of the GOE concept.

We discuss a technical detail of GOE tag-switching technology in next section and GOE-VPN will be described in a separate paper.

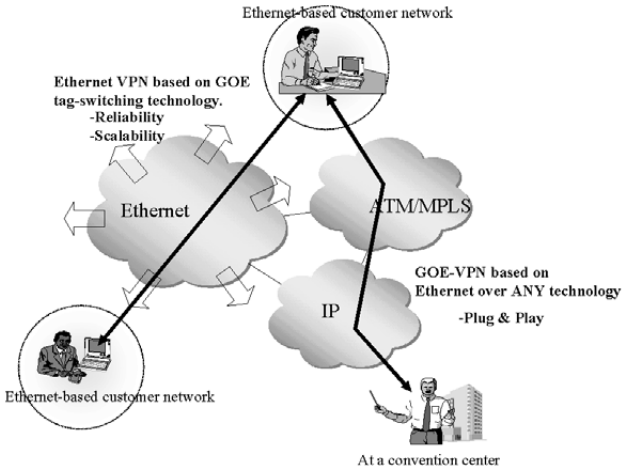


Fig. 8 An overview of GOE concept.

5. GOE TAG-SWITCHING TECHNOLOGY FOR RELIABLE AND SCALABLE TRANSPORT SOLUTION

The GOE tag-switching infrastructure is well-suited for provider-managed Ethernet VPN services. In this section, we give a technical detail of GOE tag-switching and discuss its functionality.

5.1 Technical Detail

The basic GOE tag-switching technology provides simple Ethernet VPNs with scalability and reliability, based on a simple extension of the Ethernet stacked VLAN-tagging scheme in a cost-effective way.

A GOE tag-switching network consists of GOE edge and GOE core bridges. Each bridge uses the MSTP (Multiple Spanning Tree Protocol)[12] which can create a spanning tree for VLAN independently and RSTP[13] for quick failure recovery. Each edge bridge creates a spanning tree, with itself as the root, using a combination of MSTP and RSTP to establish forwarding routes from any other GOE edge bridges.

Figure 9 shows an example of spanning trees that edge bridge #X and #Y create. The edge bridges transport the Ethernet frame on the spanning tree with the destination edge bridge creates as the root. Since the spanning tree always provides the most cost-effective (the shortest) route between the root bridge and any other each bridges, the Ethernet frames are transported over a cost-effective route. This approach provides a quick failure recovery function via RSTP.

Since a spanning tree appears to be created for each destination bridge, we call this spanning tree configuration technology PD-MRSTP (Per-Destination Multiple Rapid Spanning Tree Protocol), which is completely compatible with the legacy Ethernet standards.

Figure 10 shows the frame formats and processing scheme in the GOE network. The edge bridge receives customer Ethernet frames with or without an IEEE 802.1Q VLAN tag and inserts a GOE header after an Ethernet destination MAC address field. The GOE header has a flexible and extensible length structure based on conventional VLAN tag stacking technology. The header basically consists of the forwarding tag and customer ID tag. The GOE edge bridge resolves identification of the destination edge the received Ethernet frame is transported to, by referring to destination MAC address and received port, and then it stores the destination edge bridge ID in the forwarding tag field and the customer ID in the customer ID tag field. The edge sends it on the spanning tree with the destination edge bridge as the root. The core bridges refer only to the forwarding tag field and then send it to the destination edge bridge via the spanning tree. The destination edge bridge removes the GOE header and sends the Ethernet frame to the destination terminal.

The forwarding tag is a key component for forwarding in the GOE network, whereas the customer ID tag is used only for identifying customers and for applying customer-specific traffic processing. Decoupling

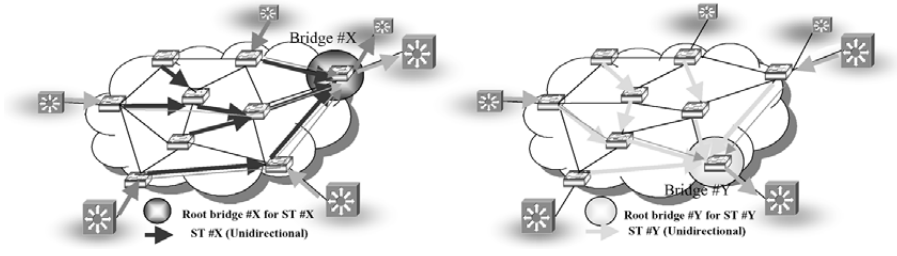


Fig. 9 GOE network architecture and PD-MRSTP.

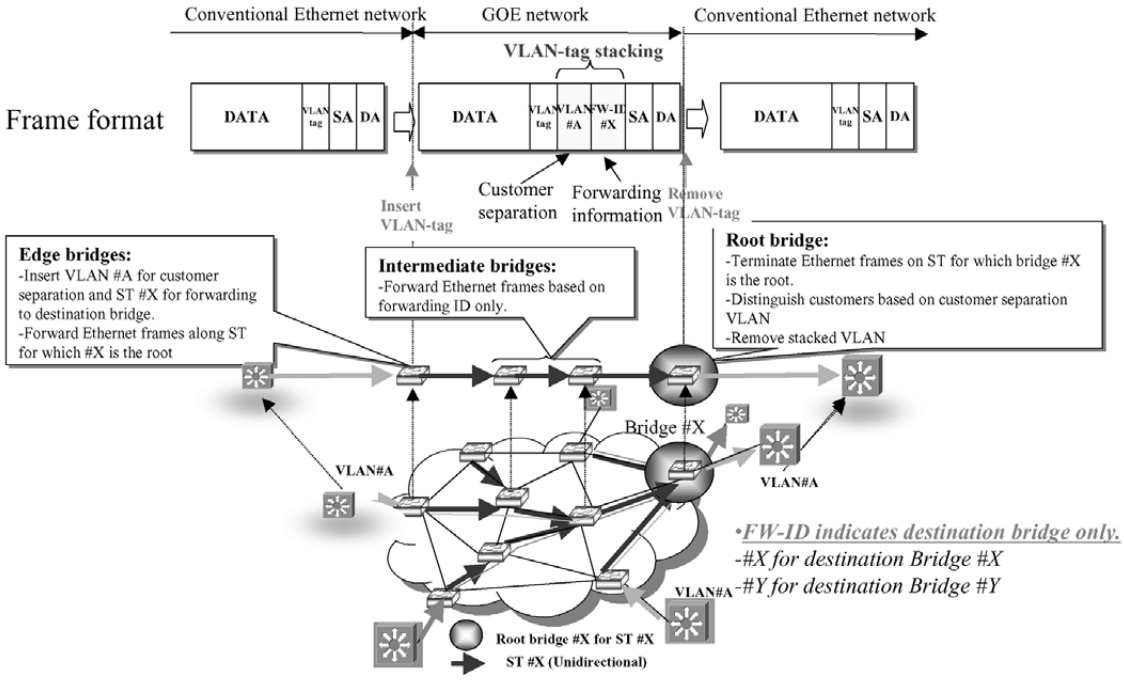


Fig. 10 GOE basic frame format and processing.

forwarding and customer information into different tag fields separates network and customer management, which enables simple and scalable network operation.

The forwarding tag uses the destination bridge ID, unlike current VLAN tag usage, so the forwarding tables created by GOE form a uni-directional path, similar to an MPLS path. Although MPLS uses the same virtual-circuit mechanism (i.e., a connection-oriented paradigm) as ATM network, GOE performs the bridge ID based forwarding mechanism (i.e., connection-less paradigm), similar to that used in IP networks.

5.2 GOE Tag-Switching Functionality

(1) Protection

As described above, RSTP can recover failures within a second in any topology, except for a root bridge failure where it takes several seconds to elect a new root bridge among all the bridges and to stabilize the spanning tree from the new root bridge. The proposed PD-MRSTP, on the other hand, can recover any failures within a second, because a root bridge failure means a destination bridge failure, which does not require selection of a new root bridge (i.e. N/A in the FDB table) as shown in **Fig. 11**. Thus, the forwarding should be recovered using another destination bridge, which is dual-homing to users to access. Moving from an old destination bridge to a new dual-homed destination bridge takes less than a second, which is a significantly smaller recovery time than RSTP.

(2) Reduced Size of FDB in GOE Core Bridges

The GOE core bridges look at only the forwarding tag for forwarding Ethernet frames. The forwarding tag is 12 bit long (4,096), so that only 4,096 entries for forwarding are required in the FDB. Compared with the FDB size of legacy Ethernet switches other typical vendors implement, the FDB size in GOE is reduced by about 1/2,500. By this drastic reduction of FDB size, a simple FDB searching engine can be applied.

(3) In-Service Reconfiguration

In the standard MSTP/RSTP, once a new bridge is added or an existing bridge is removed, the spanning tree algorithm must be run again to create a new spanning tree. Until the new spanning tree is created, existing packet may be discarded in business sites where the spanning tree direction has to be changed. If there are N business sites with a change in the tree direction, packets are discarded N times in an interval of several seconds (The interval time could be several tens of seconds in total.).

PD-MRSTP, on the other hand, can support

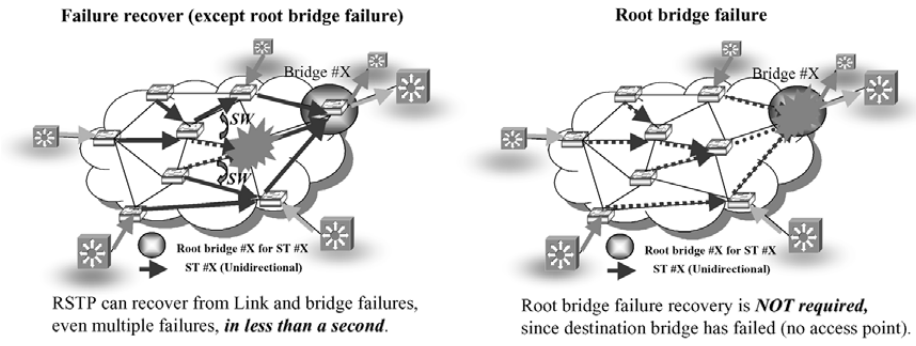


Fig.11 GOE protection overview.

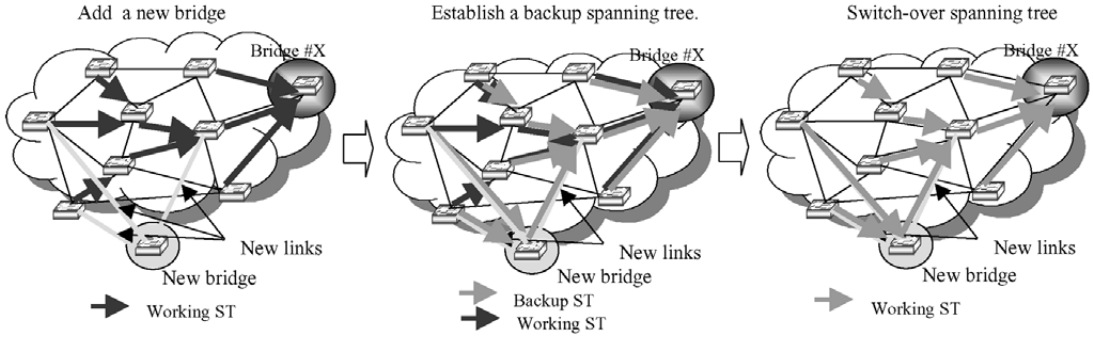


Fig. 12 In-service reconfiguration without packet loss.

reconfiguration without discarding. **Figure 12** shows an example of adding a new core bridge to the operating network. Given that two edge bridge IDs (default ID and alternate ID) are given to each edge bridge, once a new core bridge is added, a new spanning tree based on the alternate ID is created. The existing spanning tree based on the default ID continues to work while the new spanning tree is being created. After the new spanning tree become stable, the root bridge sends a trigger message to each bridge over the new spanning tree to switch over to the new spanning tree. GOE can thus provide in-service reconfiguration without any service disruption, although there may be packet reordering when the delay through the existing spanning tree is longer through the new spanning tree. However, packet reordering problems could solve by enforcing buffering at the ingress bridge until the last packet in transit reaches the egress bridge.

(4) Traffic Engineering

The GOE architecture can provide the shortest-widest path both statically and dynamically from each bridge to the destination bridge. This is quite a useful feature for traffic engineering and load balancing. When connecting multiple sites into a single VLAN, MSTP and RSTP have to choose one of the bridges as a root bridge.

Some of the traffic from a bridge goes to this root bridge, while the rest goes to another bridge. This means that the latter traffic has to go through the root bridge to the destination bridge, which causes the root bridge to become congested. This happens at all root bridges for each VLAN in MSTP and RSTP. PD-MRSTP, on the other hand, uses a per-destination based spanning tree, in which each bridge can send traffic by the lowest-cost route and perform a static route optimization, or 'spatial reuse.' This lowest-cost route is actually the shortest-widest route, which is selected as route having the most available physical bandwidths. As specified in IEEE802.1w[12], the route-cost function is simply the inverse of 'physical link bandwidth.' Thus, PD-MRSTP automatically provides static physical and topological load balancing, resulting in higher network utilization.

A promising approach to providing much higher network utilization more dynamically is to extend the static route cost functions to the dynamic route-cost

one, which can be calculated by the inverse available link bandwidth. This is the residual bandwidth that can be still used (instead of the physical link bandwidth). After monitoring the available link bandwidth to get the dynamic route-cost from each physical link, we can obtain a new optimized spanning tree to the destination bridge (using an alternate bridge ID) independently of an existing tree. After the new optimized tree becomes stable, the ingress bridge switches over to the new tree from the existing tree without discarding any packets. This approach can adapt to the current network load and provide dynamic traffic engineering functions.

6. CONCLUSION

We described the GOE concept especially for supporting next-generation provider- and customer-managed Ethernet VPNs, and also presented technical detail of GOE tag-switching technology for provider-managed VPNs.

The GOE concept is to provide world-wide Ethernet access to any person/site, from anywhere, anytime, with plug & play. From technical point of view, for provider-managed VPNs, GOE is based on tag-switching technology which gives transport functions that are virtually equivalent to SONET/SDH ones. For customer-managed VPNs, GOE is based on Ethernet-over-ANY technology which transports Ethernet frames transparently between any sites and/or persons with ease.

The GOE tag-switching technology gives a solution for next-generation provider-managed VPNs services where it provides a simple Ethernet VPN service with scalability and reliability, based on a simple extension of Ethernet VLAN-tag stacking scheme in a cost-effective way. The technology accommodates: (a) fast protection (almost equivalent to that of SONET/SDH,) (b) remarkable reduction in the size of the Forwarding Date Base (FDB), (c) in-service network reconfiguration capability, and (d) traffic engineering functions. It can, thus, be considered a cost-effective simple VPN solution with clear advantages in terms of functionality, management and performance.

ACKNOWLEDGMENT

The authors would like to thank people, who have been promoting our activities, for providing many valuable comments and suggestions.

REFERENCES

[1] T. Dierks, et al, “The TLS protocol version 1.0,” RFC 2246.
[2] W. Augustyn, et al., “Requirements for Virtual Private LAN Services (VPLS),” IETF Internet Draft, draft-ietf-ppvpn-vpls-requirements-01.txt, Oct. 2002.
[3] E. Rosen, et al., “Multiprotocol Label Switching Architecture,” RFC3031, Jan. 2001.
[4] L. Martini, et al., “Encapsulation Methods for Transport of Layer 2 Frames over MPLS,” IETF Internet Draft, draft-martini-l2circuit-encapmpls-05.txt, Apr. 2003.
[5] K. Kompella, et al., “Layer 2 VPNs Over Tunnels,” IETF Internet Draft, draft-kompella-ppvpn-l2vpn-03.txt, Apr. 2003.
[6] K. Kompella, et al., “Virtual Private LAN Service,” IETF Internet Draft, draft-kompella-ppvpn-vpls-02.txt, Apr. 2003.
[7] IEEE 802.17 Resilient Packet Ring Working Group, http:/www.ieee802.org/17.
[8] W. Townsley, et al., “Layer 2 tunneling protocol ‘L2TP,’” IETF RFC 2661, Aug. 1999.
[9] IETF IP security protocol, http://www.ietf.org/html.charters/ipsec-charter.html.
[10] ANSI/IEEE Draft Standard, “Part 3: Media Access Control Bridges,” IEEE802.1D 1998 Edition.
[11] Marc Holness, et al., ‘Bridging Solution for the MAN: Service Separation,’ IEEE802.1, http://www.ieee802.org/1/files/public/docs2002/Bridging in MAN Part II Issue.pdf.
[12] IEEE Draft Standard, P802.1s/D13, “Standard for Local and Metropolitan Area Networks - Amendment 3 to 802.1Q Virtual Bridged Local Area Networks: Multiple Spanning Trees,” Jun. 1998.
[13] ANSI/IEEE Standard 802.1w-2001, “Part 3: Media Access Control (MAC) Bridges, Amendment 2—Rapid Reconfiguration,” http://standards.ieee.org/getieee802/802.1.html, 2001.

Received April 15, 2004

* * * * * * * * * * * * * * * *

Kazuo TAKAGI was born in Shinminato, Toyama, Japan, in 1966. He received his B.E. and M.S. degrees in electrical engineering from Keio University, in 1989 and 1991, respectively. He joined NEC Corporation in 1991, and is a Research Staff member at System Platforms Research Laboratories, NEC Corporation, Kanagawa, Japan. Since joining NEC, he has researched and developed optical ATM switches, all optical access systems, ATM access systems, and WDM ring systems in Networking Research Laboratory. He worked in the Network Product Research Department in C&C Research Labs., NEC Laboratories America, from 2002 to 2003. His current interest is the design of next-generation Ethernet architectures.

Atsushi IWATA was born in Fukuoka, Japan, in 1964. He received his B.E. and M.E. degrees in electrical engineering from the University of Tokyo, Japan, in 1988 and 1990, respectively. He joined NEC Corporation in 1990, and is a Principal Researcher at System Platforms Research Laboratories, NEC Corporation, Kanagawa, Japan. From 1997 to 1998, he was a Visiting Researcher at the University of California, Los Angeles. He also received a Ph.D degree in electrical engineering from the University of Tokyo, Japan, in 2001. He received the best paper award of the Institute of Electronics, Information and Communication Engineers (IEICE) Switching Systems Technical Group in 1999, and IEICE Network Systems Technical Group in 2004. His current research interest is the design and analysis of network architectures, routing algorithms and protocols for computer communication networks.

Dr. Iwata is a member of the IEICE of Japan.

Masaki UMAYABASHI was born in Tokyo, Japan, in 1973. He received his B.E. and M.E. degrees in electrical engineering from Keio University, Japan, in 1995 and 1997, respectively. He joined NEC Corporation in 1997, and is a member of the Research staff at System Platforms Research Laboratories, NEC Corporation, Kanagawa, Japan. His current research interest is the design and analysis of traffic control and protocols for communication networks.

Mr. Umeyabashi author is a member of the IEICE of Japan.

Youichi HIDAKA was born in Osaka, Japan, in 1973. He received his B.E. and M.E. degrees in information systems science from Soka University in 1995 and 1997, respectively. He joined NEC Corporation in 1997 and was with the LAN division, NEC Corporation. He was a network hardware engineer of the LAN Division and was engaged in network solutions for the hardware design, development and evaluation of LAN/WAN network devices from 1997 to 2001. More recently, he joined System Platforms Research Laboratories, NEC Corporation, Kanagawa, Japan, in 2002. His current research interest is the design and analysis of network architectures, hardware architectures, network management, traffic management, protocols for computer communication networks.

Mr. Hidaka is a member of the IEICE of Japan.

Nobuyuki ENOMOTO was born in Tokyo, Japan, in 1977. He received his B.E. and M.E. degrees in the School of Science and Engineering, Waseda University, Tokyo, Japan, in 1999 and 2001, respectively. He joined NEC Corporation in 2001, and is a Research staff member at System Platforms Research Laboratories, NEC Corporation, Kanagawa, Japan. His current research interest is the design and analysis of network architectures, routing algorithms and protocols for computer communication networks.

Mr. Enomoto is a member of the IEICE of Japan.

Akira ARUTAKI received his B.E. degree in electrical engineering and M.E. in electronics and communications engineering from Tohoku University in 1978 and 1980, respectively. Joining NEC Corporation in 1980, he was engaged in research and development of PCM, ISDN and ATM systems. From 1987 to 1990 he stayed at Washington University in St. Louis, MO, as a scholarship recipient, and was transferred to NEC America, Inc. in 1990. After coming back to Japan in 1994, he managed research and development of IP based communication systems such as routers, Ethernet switches and VoIP, and is currently the General Manager of System Platforms Research Laboratories covering R&D activities in Broadband, Mobile, Computer, and Storage arenas. He received the best paper award of the Institute of Electronics, Information and Communication Engineers (IEICE) Network Systems Technical Group in 1999. He is a co-author of Multimedia ATM-LAN (in Japanese) published by Triceps in 1994.

Mr. Arutaki is a member of the IEICE of Japan and the IEEE.

* * * * * * * * * * * * * * * * *