Visualization of Multicast Virtual Private Network Topology

Tatsuyuki Kimura†, *Takashi Mukai, and Miwaka Ohtani*

Abstract

This article provides an overview of techniques that support multicast-over-VPN (virtual private network) services through network topology visualization. We focus on the multicast VPN as an example of a real service network to introduce various path visualization functions. We made a prototype system for a feasibility study. It collects data about multicast routes periodically to obtain a stable network view, but other methods based on different points of view may be used in other systems.

1. Introduction

Most IP (Internet protocol) services build a logical network on top of the infrastructure IP network using an individual protocol for each service. Clarifying the relationship between the services created by these various service networks and the infrastructure network to establish the appropriate collaborative operation is an important challenge. In this article, we focus on the multicast VPN (virtual private network) as an example of a real service network to introduce path visualization functions that are essential to service network management.

2. Features of a multicast network

In IP multicast, unlike the normal IP unicast communication, transmitted packets are duplicated or branched at a router that has a multicasting function. As a mechanism for this, protocol-independent multicast (PIM) is used between the routers to calculate the paths to be used for multicasting, in addition to the normal routing protocols.

A PIM-SM (PIM sparse mode) path eventually converges to the minimum path between the terminal and the server in the same manner as in unicasting. However, the terminal must announce at the start that it is participating in the multicast group by way of a rendezvous point. That is, when a multicast service is offered to customers, communication from the customer to the rendezvous point must not be blocked.

In addition, it is necessary to confirm that the routers that understand PIM are adjacent to each other (i.e., they are PIM neighbors). Even if they are reachable by unicasting, routers that are unreachable via a PIM-neighbor connection cannot be used in the multicast network. The multicast network shall be configured as a virtual service network consisting solely of routers that understand PIM on the IP unicast network as an infrastructure .

To achieve network management functions, we need to manage the topology of the target network over the infrastructure network. A few commercial network management systems implement a simple multicast network analysis algorithm, but there is no implementation of a multicast VPN analysis method even though source data about topology is important in analyzing a dynamic network such as a multicast network.

3. Path of multicast VPN

The VPN of Rosen's method [1], [2] offers the means to use these multicast networks from a VPN. When the multicasting in the VPN being used by a customer is connected to a carrier's network, the in-VPN packets are encapsulated via the carrier edge router and delivered by multicasting in the carrier network. The multicast network is shown from the customer's and provider's viewpoints in **Fig. 1**. To think

† NTT Network Service Systems Laboratories
Musashino-shi, 180-8585 Japan
Email: kimura.tatsuyuki@lab.ntt.co.jp

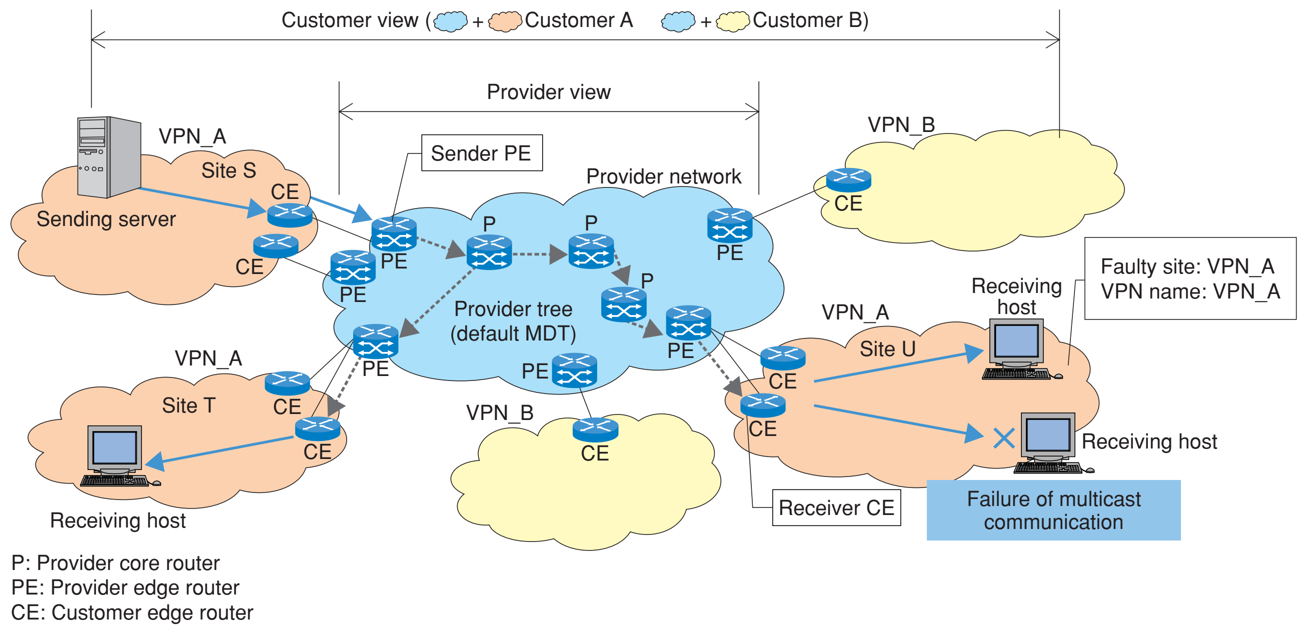


Fig. 1. Service network of multicast VPN.

about the management function of this dual overlay network in terms of service management, it is necessary to consider the management in two phases: a) management of service availability status and b) management of service offering status.

a) Service availability status refers to the status management that ensures that the Join message from the customer can reach the rendezvous point by way of the provider network to enable the customer tree to be configured. The user's Join message is encapsulated via the edge router and delivered to the rendezvous point through the default multicast distribution tree (MDT), which is the multicast tree configured by the mesh of edge routers on the provider network. Therefore, service availability status can be judged by whether or not the default MDT is available as a logical infrastructure network.

b) Service offering status refers to the status management concerning whether or not the user traffic is delivered normally, similar to general network management. A command such as ping or traceroute can check the reach of unicast packets. However, since multicasting can use different routes from unicasting and its reachability cannot be ensured by these commands for unicasting, it is necessary to confirm the packet reachability by using a method that is appropriate for multicasting, as shown in **Table 1**. This table shows the advantages and disadvantages of each method and compares the load on the system at the time of data collection. Since the criteria for evaluation vary with the constraints on service quality, the display and calculation parts are separated to enable the same management function to be provided by any method. The display part has only the user input function and the function for visualizing the received topology data.

4. Prototype of multicast VPN visualization

We made a prototype system for a feasibility study. It is necessary to identify any problems such as time-consuming parameter calculations, test the visualization style for readability, and so on. To make a network management system for multicast VPN services, two functions are essential: checking the establishment of the default MDT and checking the normal operation of the multicast routing protocol. Therefore, we made a prototype of the function for visualizing the multicast VPN and the MDT at the protocol level.

First, the visualization tool selects the VPN. Then, by starting from all the edge routers related to that VPN, it traces the routers that are in the PIM neighbor relationship and displays the tracks as the base topology. The soundness of the service network itself, that is, the service availability status, can be confirmed when there are no isolated edge routers on this base topology screen.

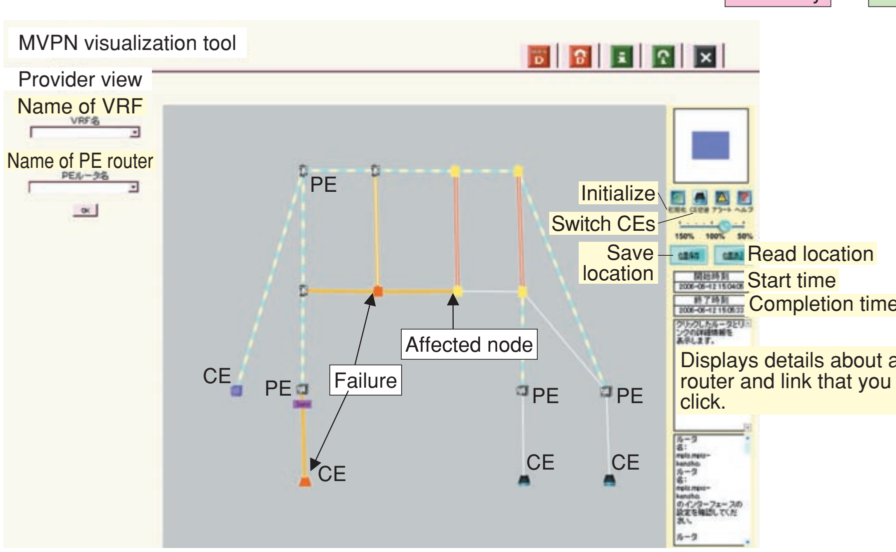
Next, it selects the edge router to display the multicast tree (default MDT) in the VPN, which has the relevant edge router as the sender (**Fig. 2**). On this screen, the offering status of individual services can be monitored.

The tree calculation starts from the edge router and the multicast routing table is read out using the router's mroute command to determine the paths in a

Table 1. Evaluation of path collection methods.

Method	Number of router accesses at path checking	Load on the router at path checking	Number of router accesses at polling	Total load to generate path data	Characteristics
Check using test packet	Conducts the test on every router.	Checks the arrival of the test packet.	No periodic connection	Communication + packet check + path make	Heavy load on the router to conduct the test
Periodic check using test packet	Uses the periodic collection result.	Checks the arrival of the test packet.	Periodic testing of every router	Communication + packet check + path make	Heavy load on the router to conduct the test
Check by mtrace command	Path check on every tree towards every edge	Sends mtrace packet.	No periodic connection	Communication	Many mtrace commands take a long time to collect
Periodic check by mtrace command	Uses the periodic collection result.	Sends mtrace packet.	Path check on every tree towards every edge	Communication	Many mtrace commands take a long time to collect
Path trace by mroute command	Sequential access to routers belonging to the trees	Reads out multicast routing table.	No periodic connection	Communication + path analysis	Tree acquisition takes time and is unsuitable for immediate execution.
Periodic collection of path table data by mroute	Uses the periodic collection result.	Reads out multicast routing table.	Sequential access to routers belonging to every tree	Database access + path analysis	Consists mostly of internal calculation. The actual path can be checked.
Path simulation in server	Uses the definition file.	No router access	No periodic connection	Minimum route calculation	Deviation from the actual path is possible.
Check of simulation result in the router	Conforms to mtrace or mroute.	Conforms to mtrace or mroute.	No periodic connection	Minimum route calculation	Short calculation time, but requires communication with the part to be checked.

too heavy   used in this prototype



VRF: virtual routing and forwarding

Fig. 2. Screen image of multicast VPN (MVPN) path visualization tool.

hop-by-hop manner. In this method, the strict multicast packet paths cannot be used; however, there are advantages in that the logical behavior of the router can be understood and that direct access to each router can clarify the location of the fault in the event of a communication failure.

When a failure occurs, it is useful to have a function for checking the difference between the current network topology and the original one. However, since the change in base topology caused by the PIM communication failure makes the core router itself invisible, a history display function is provided to call up the previously displayed topology. To check the change in topology at the time of failure, the current version of the system calls the normal status displayed in the past and draws a comparison.

5. Conclusion

With this prototype tool, we verified the fundamental visualization function. The next challenges are to improve the collaboration between the service management function and the IP-level monitoring, address multiple service methods, and speed up the data collection part. We will make use of our findings from this system prototyping effort in future network operation development and strive to build an easy-to-operate network.

References

[1] E. Rosen and Y. Rekhter, "BGP/MPLS VPNs," draft-ietf-l3vpn-rfc2547bis-03.txt, Oct. 2004.

[2] E. Rosen, Y. Cai, and I. Wijnands, "Multicast in MPLS/BGP IP VPNs," draft-rosen-vpn-mcast-08.txt, Dec. 2004.

Tatsuyuki Kimura
Senior Research Engineer, Network Software Service Project, NTT Network Service Systems Laboratories.

He received the B.E. degree in mechanical engineering from Keio University, Tokyo, in 1990. He joined NTT in 1990. Since then, he has mainly been engaged in research on transmission network management. He is currently working on the modeling of network management functions and multilayered network management systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Takashi Mukai
Research Engineer, Fourth Promotion Project, NTT Network Service Systems Laboratories.

He received the M.E. degree in administration engineering from Keio University, Tokyo, in 1990. He joined NTT in 1990. Since then, he has mainly been engaged in research on switch systems management. He is currently working on the engineering of network management systems and multilayered network management systems. He is a member of IEICE.

Miwaka Ohtani
Researcher, Fourth Promotion Project, NTT Network Service Systems Laboratories.

He received the M.S. degree in computer science from the University of Tokyo, Tokyo, in 1990. He joined NTT in 2004. Since then, he has mainly been engaged in research on service network management. He is currently working on the modeling of network management functions and service network management systems. He is a member of IEICE.