A new technology for visualizing network topologies

Takahiko Ohta
Takeshi Shingu

Keywords
SNMP, MAC address table, RSTP, network configuration, network redundancy

In response to the growth in size and complexity of network systems that accompanies the multi-vendorization of system equipment, we have developed a technology for automatically detecting the configuration of networks, and we have experimentally produced a system-monitoring application that visualizes the configuration. By analyzing the information in an SNMP-compatible switching hub, this technology is able to detect the local network devices in their hierarchical structure. This technology significantly reduces the time and cost required to check the configuration of a network when constructing or operating a network system.

1. Introduction

Recently, networks are growing in size and complexity as IoT and cloud services become widespread and more devices are connected to networks. In addition, with the spread of the COVID-19 coronavirus, companies are showing increasing interest in the creation of new ways of working, for example by promoting teleworking, which has led to fewer personnel onsite.

Although many organizations and companies are using networks in their own buildings and on their own premises, the need for manual work to build, operate, and maintain those networks has also become an issue. When building a new network, one must visually or manually confirm that the network is configured as specified in the design drawing. When changing a network configuration to expand or alter it, the design drawing must be updated. In addition, if a fault occurs, one must visually or manually check the network against the design drawing to locate the cause. However, there are times when the design drawing has not been properly updated. In such cases, checking takes more time.

Given this background and these problems, we developed a technique to automatically detect a network's configuration, and we prototyped a system-monitoring application that uses this technique.

2. Issues related to network monitoring

With an IPv4 network, conventional automatic network configuration detection technologies generally just enumerate the devices connected to the network in the system by accessing all addresses in the network address range. For example, an ARP (Address Resolution Protocol) request*1 is sent 254 times to detect connected devices in the network segment from 192.168.1.1 to 192.168.1.254. However, it is also necessary to understand the hierarchical structure of switches to check that the network is actually correctly configured and follows the design drawing. Therefore, conventional methods are insufficient when it comes to accurately confirming that a network is built according to the design drawing. As a result, the cost of visual and manual confirmation increases in proportion to the network's size.

In addition, redundant networks using the STP (Spanning Tree Protocol) and other protocols are recently being applied to many systems. These require confirmation that redundant configuration information is properly built into the network as well. Currently, however, while a blocking port, which provides a redundant line, can easily be detected, there is no method for automatically detecting the port that the blocking port is connected to. This means that it must be visually or manually detected, which makes confirmation costly.

3. A network configuration detection technique

This section describes a technique for automatically detecting the configuration of multiple switches in a local network. This technique detects the switch and the number of the switch port to which each switch is connected in order to visualize physical connection information across the network.

To automatically detect the network configuration, MAC address tables*2 are obtained for analysis from all the switches on the network with the Simple Network Management Protocol (SNMP). Note that this method assumes that all the switches on the network are SNMP-compatible and that MAC address tables can be obtained from them.

3.1 Simple Network Management Protocol (SNMP)

SNMP is a protocol for managing the devices connected to an IP network. SNMP manages a wide range of components including switches, routers, servers, PCs, security devices, and network printers. This protocol can obtain information such as interface, ARP table, MAC address table, and port status from the managed components. Management information is standardized in a management information base (MIB).

*1. ARP is a protocol used to obtain MAC addresses from IP addresses and to check for devices on a network.

*2. A MAC address is a unique network device ID used by devices on a local network to communicate with each other. MAC address tables are described in section 3.2.

3.2 MAC address table

A MAC address table is a correspondence table between the physical ports of the switch and the MAC addresses of the connected devices. Each switch has its own MAC address table. The MAC address table automatically obtains information whenever there is communication through the switch and uses it for efficient switch communication. The information is automatically erased if there is no communication for a certain amount of time.

3.3 Network configuration detection

This method mainly consists of the following two steps:
(1) MAC address table data acquisition
(2) MAC address table analysis

3.3.1 MAC address table data acquisition

The MAC address table in each switch is made to acquire data from all the other switches. Each switch is made to send a broadcast message so that its MAC address can be stored in the MAC address tables of all the other switches. This is done by using a ping whose sender is specified as a dummy IP address that does not exist on the network. The switch that receives the ping tries to reply to the sender. However, since the nonexistent IP address is not registered in its ARP table, the switch broadcasts an ARP request to obtain the MAC address. For example, in the network configuration shown in figure 1, with the MAC address tables empty, if a ping whose sender is a dummy IP address is sent to switch C, the MAC address table in each switch changes as shown in figure 2. Note that figure 2 only shows switch-related information in the MAC address table. In this way, when a ping is sent to all switches, and a dummy IP address that does not exist on the network is specified as the sender, all the switches on the network communicate with one another. As a result, the MAC address table in each switch acquires data from all the other switches. MAC address tables in this state are shown in figure 3. Figure 3 only shows switch-related information in the MAC address table.

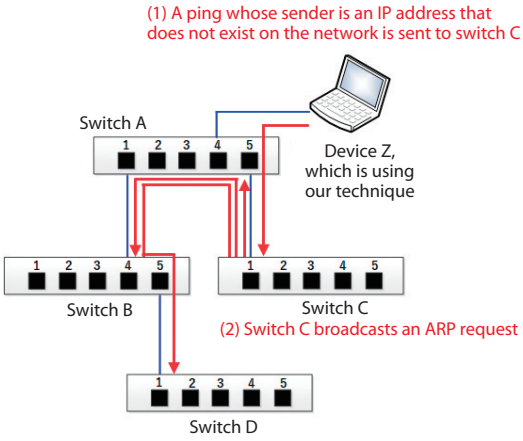

Fig. 1. A ping using a nonexistent IP address

MAC address table in switch A

MAC address	Port No.
MAC address of C	5

MAC address table in switch B

MAC address	Port No.
MAC address of C	4

MAC address table in switch D

MAC address	Port No.
MAC address of C	1

MAC address table in switch C

MAC address	Port No.

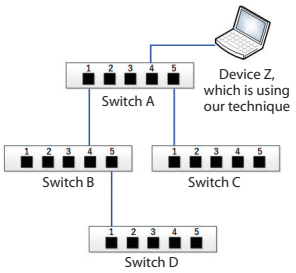

Fig. 2. Example of data acquisition by MAC address tables

MAC address table in switch A

MAC address	Port No.
MAC address of B	1
MAC address of D	1
MAC address of C	5

MAC address table in switch B

MAC address	Port No.
MAC address of D	5
MAC address of A	4
MAC address of C	4

MAC address table in switch D

MAC address	Port No.
MAC address of B	1
MAC address of A	1
MAC address of C	1

MAC address table in switch C

MAC address	Port No.
MAC address of A	1
MAC address of B	1
MAC address of D	1

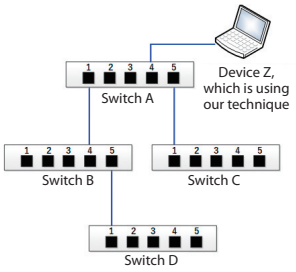

Fig. 3. Result of data acquisition by MAC address tables

3.3.2 MAC address table analysis

The MAC address tables which are made to acquire data from all the switches on the network (section 3.3.1) is then analyzed. The switch at the end of the network is determined from the MAC address table information. Then, the switch connected above it in the hierarchy is determined, and the process is repeated to detect the configuration of the network.

The switch at the end of the network is searched for first. The MAC address table in each switch is referenced and the switch which has the MAC addresses of all the other switches registered in any one port (as in the red frame in figure 4) is the switch at the end of the network. Figure 4 only shows switch-related information in the MAC address table.

Next, the switch at the next highest level, directly connected to this end switch, is sought. The MAC address table in each switch is referenced and the switch with a port for which only the MAC address of the end switch is registered is determined to be directly connected to the end switch. Data for the switch whose connection was confirmed is deleted from the MAC address tables in each switch and the search for the higher-level switch as described above is repeated. The network configuration is detected as a result of this process.

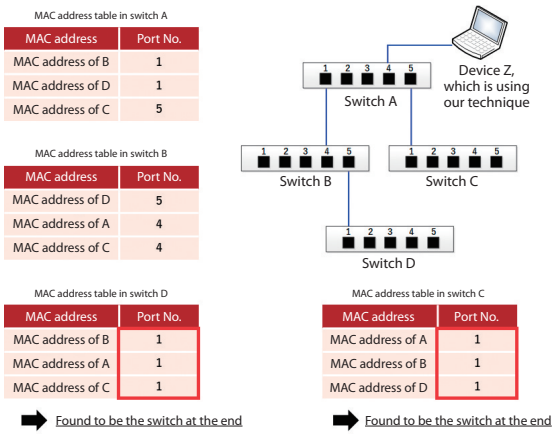

Fig. 4. Determination of the end switch

4. Redundant network configuration detection technique

This section describes a technique for automatically detecting the port to which a blocking port is physically connected in a redundantly configured network by using a redundancy protocol such as the Spanning Tree Protocol (STP).

The port to which the blocking port is connected can be automatically detected by analyzing port status information and the MAC address table in each switch. Note that this technique assumes that all the switches on the network are SNMP-compatible and that MAC address tables can be obtained from them as in section 3. It also assumes that there is one redundant configuration.

4.1 Spanning Tree Protocol (STP)

STP is a protocol that makes redundant network configurations possible. Redundancy refers to having multiple physical paths on a network to use as bypasses in case of a fault. However, a network that has a loop-shaped path cannot be used as is because it would cause the network to crash due to a broadcast storm. STP is used to block and logically disconnect some ports to avoid completing the loop. If a fault occurs, disconnecting some paths, the blocking ports are changed to forwarding mode and are enabled for communication so that new paths can be used. STP is standardized in IEEE 802.1D and is applicable to networks consisting of devices from different vendors. In addition, high-speed RSTP (Rapid STP) and high-functionality MSTP (Multiple STP) are standardized in IEEE 802.1w and IEEE 802.1s, respectively. Currently, RSTP is generally used.

4.2 Redundant network configuration detection

This technique mainly consists of the following two steps:
(1) MAC address table data acquisition
(2) Searching for blocking ports and their connections

4.2.1 MAC address table data acquisition

The MAC address table in each switch is made to acquire data from all the other switches and devices. The MAC address tables must be made to acquire data from all the switches and devices because the status of all ports and the devices connected to each switch must be referenced to search for blocking ports and their connections as described below in 4.2.2. For switch data, the system uses a ping whose sender is specified as a dummy IP address that does not exist on the network, as described in 3.3.1. For device data, ARP is used to search for IPv4 devices and Multicast Listener Discovery (MLD) is used for IPv6 devices.[1] Replies from each device are used to build the MAC address table.

4.2.2 Search for blocking ports and their connections

Status information on all the ports is collected from all the switches on the network. First, blocking ports are searched for. Checking the collected status information on all the ports reveals that one blocking port is found and that the other ports are in forwarding mode. Note that unconnected ports are disabled. Figure 5 shows an example of a redundantly configured network and the status of each port. STP blocks port 5 of switch D to logically disconnect switches C and D.

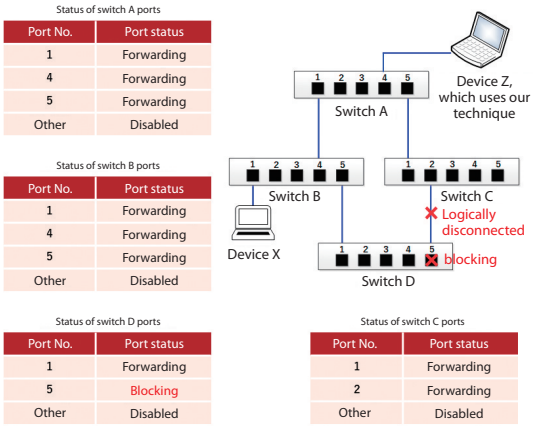

Fig. 5. Port status in a redundant network

Next, MAC address table information is collected from all the switches on the network and the port connected to the blocking port is searched for. MAC address table information in each switch is referenced and the port in forwarding mode for which a corresponding MAC address is not registered is determined to be connected to the blocking port. The port connected to the blocking port is connected by a physical cable and is in forwarding mode. However, because the port to which it is connected is blocking, the two ports are logically disconnected and there is no communication of data. Figure 6 shows the MAC address table in each switch for the redundant network in figure 5. Because the only port in forwarding mode for which a corresponding MAC address is not registered is port 2 of switch C, it is the port connected to the blocking port (port 5 of switch D).

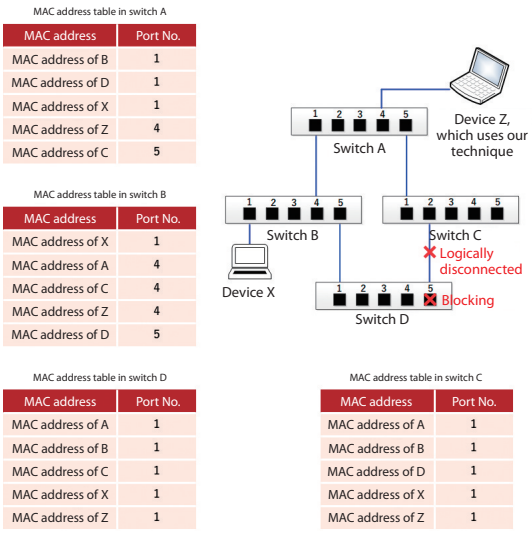

Fig. 6. MAC address tables in a redundant network

5. Achievements

We developed a technique to detect devices in local networks in a hierarchical structure by analyzing the information in SNMP-compatible switches, and a technique to detect the configuration of redundant networks. In addition, to verify that it is possible to significantly reduce*3 the cost of checking network configuration, and to quickly identify the location of a fault if one occurs during operation, we prototyped a system-monitoring application that uses these techniques. In the past, accomplishing these goals in order to build, expand, or alter a network system required visually or manually referencing drawings.

The implemented functions of the system monitoring application are as follows:

(1) Detection of multilevel switch configuration

The configuration of an entire network can be detected by automatically detecting the hierarchical structure of the switches on the local network and expressing it in tree format.

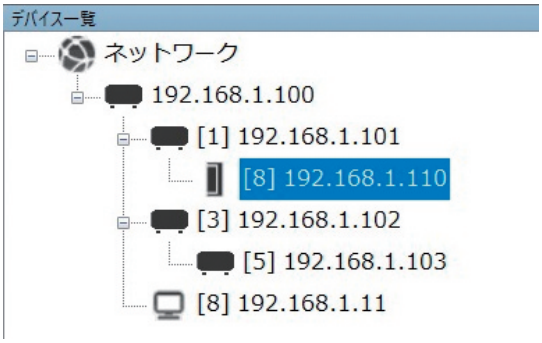

Fig. 7. Detected network configuration expressed in tree format

Figure 8 is an example of the display when the system monitoring application detects a fault. As a sample application, when a new network is constructed or begins operation, this function can search the whole network in a normal state and store the address information of the devices in the network in a white list. Then, during operation, this function monitors packets in the network. If the function finds a device not included on the white list based on the packet sender address information, it displays a warning about the unauthorized device at the top of the display. The location of the problem can be quickly detected, as shown by the red frame on the left.

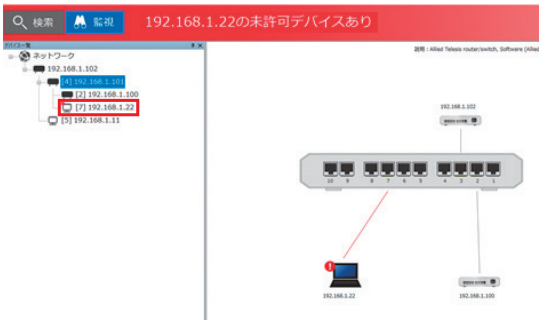

Fig. 8. Identification of fault location

(2) Redundant network configuration detection

This function can detect the root bridge, blocking port, and connected port in a redundant network configuration as shown in figure 9.

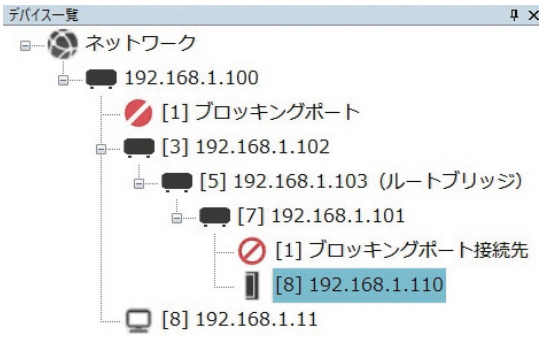

Fig. 9. Detection of redundant configuration information

6. Conclusions

This article has described techniques to detect the hierarchical structure of devices in a network.

A future challenge is to develop network configuration detection technology applicable to any network. This is because networks and devices using 5G will become widespread and networks are expected to further grow in size and complexity in the future. The techniques described in this article assume that all switches in the network support the acquisition of MAC address tables, and they only detect the configuration of wired devices. In the future, we aim to make them applicable to any network configuration regardless of the switch type and whether the connected devices are wired or wireless.

References

1. Taichi Sasaki, Takahiko Ohta, and Daiji Sanai. "Detection of Promiscuous IPv6 Nodes" (in Japanese). *Technical Review*, April 2020, pp. 15–18.

Authors

Takahiko Ohta — Development Department 2, Development Headquarters, Building Systems Company, Azbil Corporation

Takeshi Shingu — Development Department 2, Development Headquarters, Building Systems Company, Azbil Corporation

*3. Detection is completed within one minute in a class C environment with 254 devices. This would take several days in the past.