High-availability and Low-latency Tap for Network Monitoring

● Toshihide Tsuzuki

Network operators increasingly need to monitor signals on networks so that they can monitor the service quality, measure the traffic performance and perform billing services. In ordinary cases, a small device called a network tap is inserted in series in a communication line to monitor the signals on the line. This network tap needs to have high availability and low latency because it is inserted in series in the network. In this paper, we describe an outline of and problems with network taps, and introduce our new network tap that is being developed. It uses our own unique technology to support 1000BASE-T and enable high availability and low latency.

1. Introduction

Networks today assume important roles in the social infrastructure. Performance deterioration or service quality degradation of networks or their unavailability for communications may cause a significant impact on society. It has become essential to prevent such deterioration and unavailability by monitoring the networks. For that reason, network taps, which are devices for monitoring network signals, are becoming increasingly important.

Based on the current situation with network monitoring, this paper presents an overview of and issues with network taps and Fujitsu's activities for them.

2. Network monitoring and network taps

This section outlines network monitoring and network taps.

2.1 Network monitoring

Network monitoring has important roles in the operation of networks including:

1) Analysis and visualization of traffic for grasping network conditions
2) Early detection or prediction of network errors
3) Monitoring of quality of network services such as voice over IP (VoIP) and video streaming services
4) Performance measurement and monitoring of systems requiring high-speed processing and response such as trading systems
5) Detection of unauthorized access to networks
6) Monitoring of access in corporate networks
7) Packet capture to store network log data for the purpose of compliance and audit

A network monitoring system is composed of a monitoring section for extracting network signals and a processing section for analysis and processing of the extracted signals. For the monitoring section, a network tap is often used. Network signals can be extracted via a repeater hub or the mirror port of a network switch. However, a network tap must be employed in order to introduce a monitoring device in a communication line without making any change in the system configuration by only inserting the device in series in it and to extract all signals flowing in a network in full-duplex mode.

2.2 Network taps

A network tap is a device that splits a flow of signals in a network for their extraction as shown in **Figure 1**. Network taps have the following characteristics.

1) All of the signals flowing in a network including error packets can be extracted.
2) Connection of a network tap does not affect the

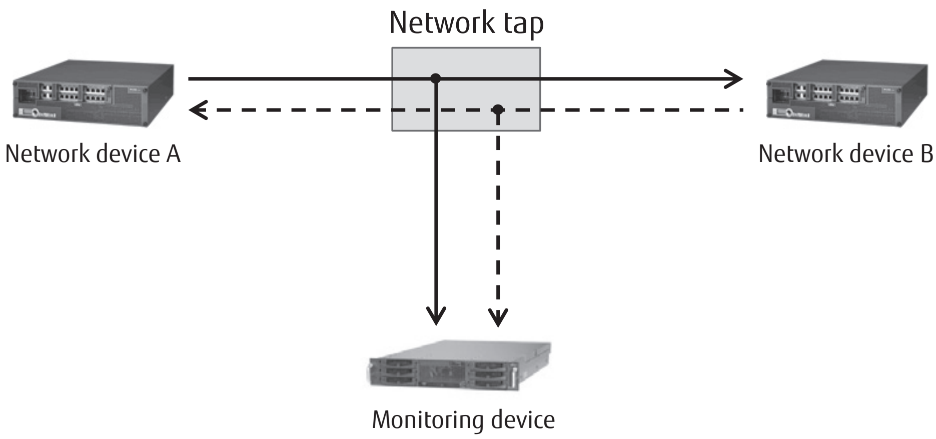

Figure 1
Concept of network tap.

network to be monitored.

3) Signals from a monitoring device connected to the monitor port are not output to the network.

By feeding the extracted signals into a monitoring device that suits the purpose, various services can be realized. For example, connecting a packet analyzer allows the user to grasp the conditions (visualization), measure performance and monitor the quality of a network. If a packet recorder is connected, signals flowing in a network can be stored without hindering communications. By connecting an intrusion detection system (IDS), a system for monitoring unauthorized access can be constructed without changing the existing network configuration.

Network taps include fiber taps (optical taps) used for networks connected with optical fiber cables, and copper taps (metal taps) used for networks connected with twisted pair cables. An optical tap has a simple structure that just splits light by using an optical splitter.

Metal taps for 10BASE-T/100BASE-TX can be realized by splitting electric signals. For metal taps that support 1000BASE-T, however, it is not possible to simply split electric signals.

3. Configurations of and issues with metal taps

This section explains configurations of metal taps that support 1000BASE-T and issues with them.

Figure 2 shows an internal configuration of a metal tap for 1000BASE-T that is generally available on the market now. With 1000BASE-T, bidirectional signals flow in the same cable, which makes it difficult to directly split the signals flowing in the network cable. To address this problem, physical layer (PHY) chips respectively connected to network ports in the metal tap are used to terminate signals, and the metal tap separates the signals into transmit data input and receive data output. The receive data outputs are split and fed to the transmit data input of the PHY chips respectively connected to other network ports, and fed to the transmit data input of the PHY chips for monitoring the respective outputs. In this way, the network communication path is ensured and it becomes possible to extract monitor signals. To prevent the network from becoming disconnected due to a failure of the network tap or power-off, hence causing an inability to communicate, a bypass circuit by means of relays is provided.

Operating metal taps in the present conditions has the following issues.

1) Network disconnection accompanying replacement of a metal tap

Generally, a network to be monitored is always in communication so as to provide certain services and the network cannot be disconnected. A tap can be installed while a network is being constructed and before it begins being used to provide services to minimize the impact. However, if the monitoring device needs to be replaced due to a device failure or other reason after the start of service provision then the network needs to be stopped. This gives rise to the need to suspend services or, if the network is redundant, switch to the

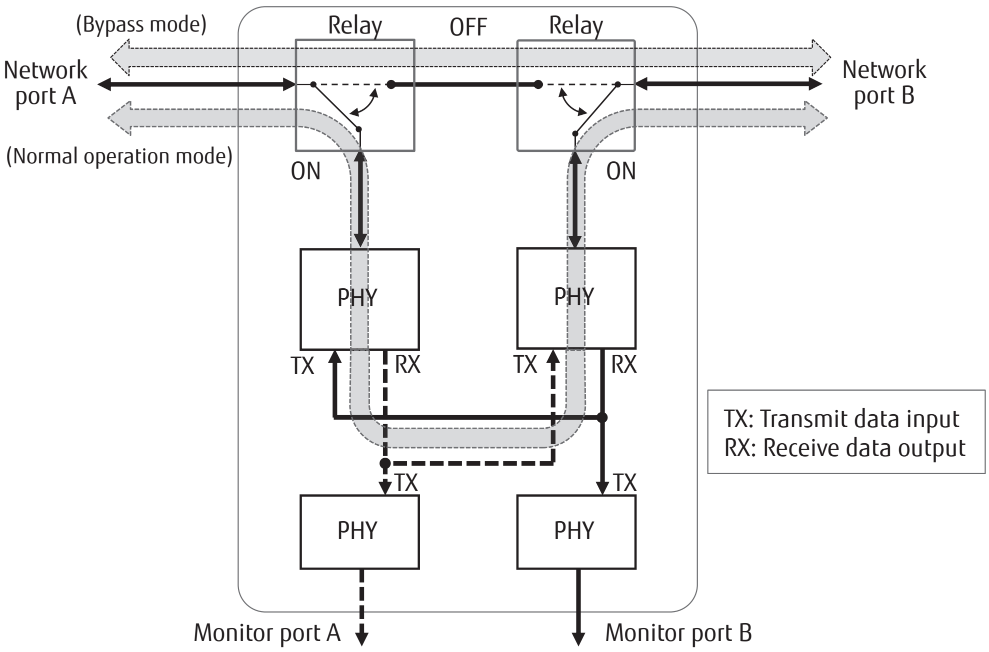

Figure 2
Configuration of commercially-available metal tap.

backup line.

2) Instantaneous network interruption during mode switching

When a metal tap switches from the normal operation mode to bypass mode because of a power outage or device failure, there is a need to mechanically switch relays, and this interrupts the network for a few milliseconds. If the network interruption causes a link-down, the communication will be disconnected for 2 to 3 s until the next link-up for the communication to be restored. This may hinder continuity of services.

3) Degradation of availability of metal tap due to bypass circuit

Failure of a relay used in the bypass circuit may cause the network to disconnect even during normal operation, possibly meaning that it is not possible to bypass the network and degrading the availability of the metal tap.

4) Increase of data transfer time and state notification propagation time

For data transfer, going through two PHY chips generates a latency of a little less than 1 μs. Link state notification monitors the state of the PHY chips and, when any change in the link state is detected, implements link control of the other PHY chip, causing a latency of a few tens of milliseconds.

The following section presents a metal tap featuring high availability and low latency that resolves these issues.

4. Development of high-availability and low-latency metal tap

The metal tap under development is composed of two modules (**Figure 3**):

1) Signal extractor

Extracts signals flowing in the network.

2) Receiver

Amplifies the extracted signals, eliminates noises from them and receives them for monitor output.

The signal extractor uses the signal extraction circuit to extract only unidirectional signals out of the bidirectional signals flowing in the network cable.

The signal extraction circuit minimizes the impact on the network line while ensuring the line's continuity to eliminate the need for relays or bypass circuit. It is composed of passive components that do not require external power, offering high reliability. Network continuity is ensured even if the power of the metal tap is cut off and there is no communication interruption. In addition, the communication path does not include

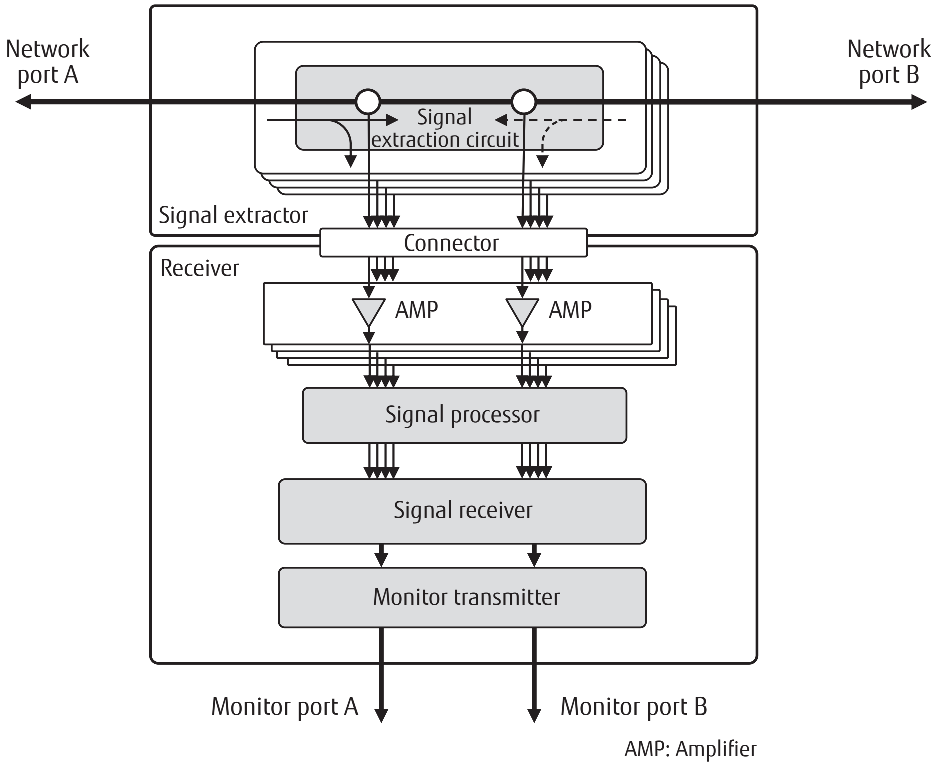

Figure 3
Configuration of high-availability, low-latency metal tap.

any PHY chip and the increase of the network link latency caused by device insertion is negligible.

The receiver amplifies the signals extracted by the signal extractor because they are weak, removes extraction noise, receives the signals and outputs monitor signals at the monitor ports by means of PHY chips.

The signal extractor and receiver have a detachable structure. The signal extractor is composed of passive components. Hence, there is no need for an external power supply and there is a very low possibility of device failure. The structure allows only the receiver to be replaced by leaving the signal extractor intact once the metal tap has been installed. In this way, the receiver can be replaced without stopping communication on the network.

The metal tap currently under development resolves the issues mentioned in the previous section and offers high availability and low latency. The tap is assumed to be applied in the future to networks where a suspension of services would have a great impact in latency-sensitive systems (e.g., trading systems), carrier networks and corporate networks.

5. Conclusion

This paper has described issues with network taps required for network monitoring and presented the high-availability and low-latency network tap under development for resolving the issues. In the future, we intend to commercialize the high-availability and low-latency metal tap and combine it with various network monitoring solutions, thereby making contributions to the improvement of quality of networks that are important to the social infrastructure.

Toshihide Tsuzuki
Fujitsu Ltd.
Mr. Tsuzuki is currently engaged in development of network taps.