TTC技術レポート
Technical Report

TR-1053

Customer support functions for home network service platform

Edition 1.1

Established on February 23, 2016

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

Table of Contents

<Reference>

1. Relations with international recommendations and others

The international recommendations related to this technical report are described in this document.

2. Revision history

Edition	Establishment date	Description
1.0	March 20, 2014	Initial edition established.
1.1	February 23, 2016	Corrected the misuse of two words, “failure and fault”.

3. Referenced documents

The documents mentioned herein were mainly referenced.

4. Working group in charge of the creation of this technical report

Edition 1.0: TTC Next-generation Home Network Systems Working Group (SWG3603)

Edition 1.1: TTC Next-generation Home Network Systems Working Group (SWG3603)

5. Organizations involved in the creation of this technical report "Customer Support Functions for Home Network Service Platform"

The draft of this technical report was prepared by the Residential ICT Sub-working Group (led by Yasuo Tan of JAIST/NICT) in the IP Network Working Group of the New Generation Network Promotion Forum. The draft was then reviewed by the TTC Next-generation Home Network Systems Working Group (chaired by Takefumi Yamazaki of NTT) and published as a TTC technical report.

For the discussions in the Residential ICT Sub-working Group, an ad hoc group was formed under the Strategy Vision Taskforce (led by Ryuichi Matsukura of Fujitsu).

Chapter 1 Introduction

This technical report describes the customer support functions, such as monitoring, setting change, and failure diagnosis, that the service platform (PF) needs to provide to enable remote failure cause analysis and recovery for various types of failures that may occur during the execution of a service that uses a device or devices connected to a home network (HN).

1.1 Background

As a result of the spread of the broadband network, it has become common to interconnect devices in the home to build a HN. A HN is made up of a mix of devices that are different in the way they are installed, maintained, and connected to the network and the level of quality they require, such as white goods (home appliances), black goods (audio-visual and other consumer electronics products), set-top boxes (STBs), home gateways (HGWs), silver goods (PCs, smartphones, tablets, etc.), and game consoles. If a failure (inability to connect a device, no image on the screen, etc.) occurs in a HN that has such a complex network configuration, it is difficult to identify which of the multiple simultaneously running systems is responsible for that failure. Moreover, the responsibility for installing a HN and maintaining its operating environment lies with the end user in many cases. Since system administrators, who are experts on HN management, are not present at hand, the operation of a HN is premised on remote maintenance. In the future, as HN services evolve, the mechanism for implementing the failure recovery process from a remote location will become more important.

TTC technical report "Service platform for home network service" (TR-1046) describes a service platform for building services by using HN-connected devices. Building the failure recovery process mentioned above into the service platform described in TTC TR-1046 makes it possible to deal with the whole series of processes, from device and service development to installation, operation, and maintenance, on a total basis. This technical report analyzes causes of failures based on failure cases associated with HN services, examines failure recovery technologies based on these analysis results, describes a system that supports the process of identifying the cause of a failure and achieving failure recovery from a remote location, and discusses the assignment of functions in the service platform.

1.2 HN service platform

HN services are implemented by controlling HN-connected devices. The number of devices that can be connected to a HN is increasing every year. Many black goods that are shipped in Japan support DLNA, and a growing number of white goods are compliant with ECHONET Lite. Since it is not uncommon to run applications over the Internet or cloud, this technical report assumes that services are provided via the cloud. The architecture of the HN service platform is described in TTC TR-1046, and the architecture assumed by this technical report is also based on TTC TR-1046. Figure 1-1 shows the architecture described in TTC TR-1046.

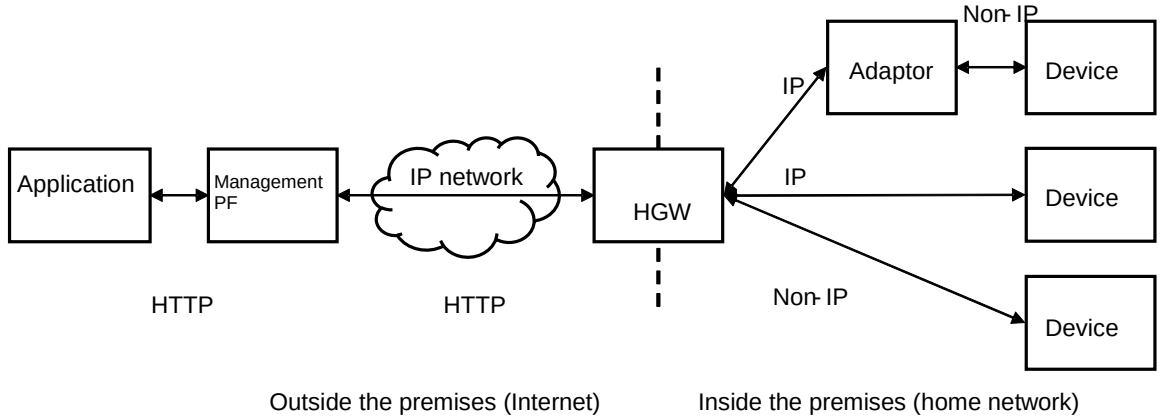

Figure 1-1 Architecture of the service platform (TTC TR-1046)

Devices connected to a HN are assumed to be ECHONET Lite-compliant devices. ECHONET Lite developed by the ECHONET Consortium defines, with regard to more than 80 types of devices that are installed in a residential house, the information possessed by those devices and remotely operable control items (properties) as logical models (device objects). In the service PF defined in TTC TR-1046, such a logical object is represented as a virtual device on the management PF via the HGW and the device is controlled by referencing and operating it from the application running on this virtual device. Standards similar to ECHONET Lite include KNX of Europe and ZigBee Smart Energy Profile (SEP) 2.0 widely used in the U.S.A., and it is considered that this architecture can be applied not only in Japan but also abroad. Even if a device does not support ECHONET Lite, it is possible to make the device compatible with ECHONET Lite by connecting an adaptor to it. Furthermore, the adaptor function can also be built into the HGW, allowing the device to be connected in a flexible manner. The home gateway (HGW) terminates the connection inside the HN and is connected to the Internet. The management PF is connected to the HGW via the Internet and capable of monitoring and controlling the information of devices in the home. Actual services are developed using APIs prepared by the management PF.

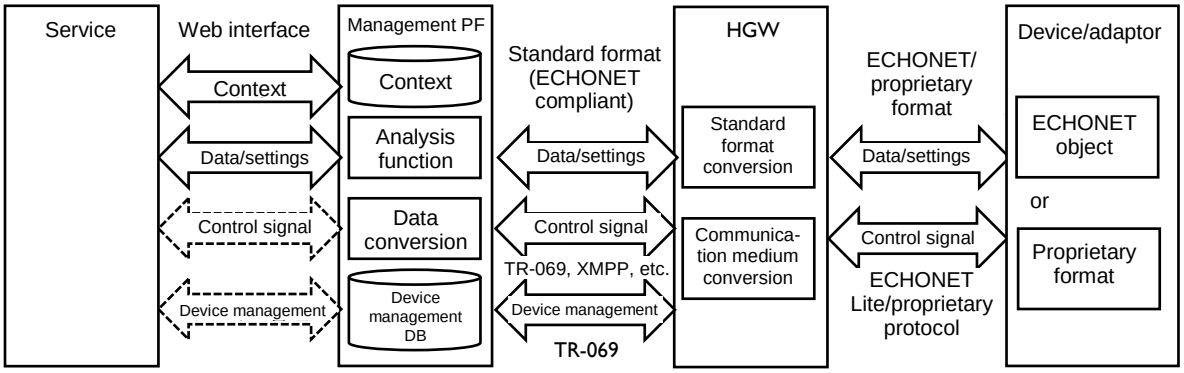

Figure 1-2 Functional architecture (TTC TR-1046)

Figure 1-2 shows the functional architecture. The functions of the individual nodes are as follows.

・Device

When a device is connected to the HGW by using an adaptor, the interface of the adaptor is represented as that of the device. In the device, the communication protocol (control signals) and the data format are separated, allowing the use of common methods. The communication protocol consists of the setting change (SetDeviceProperty), status reference (GetDeviceProperty), and status notification (Inform) signals, and the data format is basically represented as a pair of the device's attribute name and value.

・Home gateway (HGW)

The home gateway (HGW) relays communication between the HN and WAN and converts the physical communication medium and protocol.

For upper-layer protocol conversion, the HGW converts the data communication protocol (GET, SET, and INFORM) defined in ECHONET Lite and the data format. As for the WAN side, it is possible to accomplish communication using HTTP by converting the data format to XML. One candidate protocol is BBF TR-069. Mapping the ECHONET Lite communication protocol to the BBF TR-069 methods (GetParameterValue, SetParameterValue, etc.) and converting the data format to XML as suitable for BBF TR-181 enables the HGW to relay communication transparently.

・Management PF

The management PF acts as an intermediary between a HN-connected device and an application. A

HN-connected device is represented as a virtual device via the HGW. In the data format of the virtual device, a functional object of ECHONET is represented in XML. The actually connected device and network are separately recorded in the terminal management database. As for applications, the management PF has application management and linkage functions. The application management and linkage functions are the basic functions to implement applications, and they are UI, analysis, and data conversion functions. Another important function exists that is used to link multiple services. In the use cases described in TTC TR-1046, behavior grasp, diagnosis result, schedule, device status, failure (sign), and other events can notify and reference one another as the information that links applications.

・Application

An application is run by using the APIs provided by the management PF. A service provider may run applications on its own server or on the server of the operator of the management PF.

TTC TR-1046 refers to an application as a service. However, since the term "service" may be construed to mean the entire system, the term "application" used in this technical report is exclusively used to refer to an application that runs on the platform.

Chapter 2 Use Cases

2.1 Failure cases

Chapter 2 discusses the problems with the HN service platform and the functions needed to solve them. As the HN configuration becomes more complex and more devices are connected to it, more different types of failures can occur. In this chapter, actual failure cases are examined to analyze their causes.

The failure cases are not confined to those associated with the HN. Since HN service failures may also be caused by the connected device, network, application, or combination of these, as well as by other factors including an operation mistake by the user, they need to be examined from many viewpoints. In addition, while some failures currently require action by the user, the remote support functions may make it possible to locate and solve them. Therefore, failure cases were collected as use cases without limiting the range. Table 2-1 lists the collected failure cases.

Table 2-1 Failure cases

	Problem	Outline
1	Interference between services	When a user of a meter reading system for the gas meter (no-ringing service) applied for an ADSL service (superimposed on the telephone line) to use the Internet, the user was unable to use the ADSL service because of interference with the gas meter reading system.
2	Occupation of the communication bandwidth	Some devices (e.g., recording devices) occupy the communication bandwidth temporarily. The communication functions of game consoles (firmware update, file download, and online games) may place a burden on the communication bandwidth. Users are not aware of the communication characteristics of devices.
3	Malfunction due to aging	Although a gas leak detection system (purchased by the user) sounded a major alarm, there was no gas leak. Some residential users use devices beyond their service lives and leave recalled devices uncollected.
4	Interference with an existing wireless device	A user complained that he could not connect his newly purchased PC to a wireless LAN. Since the wireless LAN of the user's existing PC was running normally, it was initially suspected that the new PC might be faulty. The on-site research found, however, that the problem was due to the interference with a wireless AV device (5.1-channel surround speaker system).
5	Influence by another terminal	When a user storing data in a NAS (with a HDD recording function) inside a HN attempted to play back the stored data on a PC inside the same network using dedicated software, the data could not be played back because communication was interrupted. The cause of the problem is considered to be the bug of another software on the PC that damages the data received by the PC.
6	Silent fault (Partial function fault)	A user subscribing to the Hikari-TV service records TV programs on a HDD recorder. He noticed one day that a certain TV program had been recorded with audio only for two consecutive weeks. The preceding program, as well as all other programs, had been recorded normally. And, although the user did not take any action, the program in question was recorded normally on the third week. In this case, it is necessary to isolate the fault of the device from a communication fault.
7	Silent fault (Service outage)	A user found that his fixed-line phone was unavailable when his family informed him. Because he had been able to access the Internet via his PC, he had no idea since when the phone had been out of service. The user called the support center, and restarting the terminating device according to the instructions given by support personnel put the phone back in service. Telephony service is a kind of service whose availability is taken for granted, and service outage often goes unnoticed.
8	Failure due to improper use	This pertains to a monitoring service of a nursing care provider. The service was disabled as the care receiver turned off the power of the monitoring system to save electricity. In another case, the care receiver left the pendant-type terminal of the monitoring system in the bathroom. This led to an emergency response, because the system is designed to notify the nursing station if the terminal does not detect movement or vibration for a certain period of time.
9	Failure due to an improper startup order	This is a problem involving a terminating device and devices equipped with communication capabilities. Even if the supply of power is resumed for all the devices simultaneously after a power outage, each device goes through its own unique process from startup to communication capability recovery. Therefore, some devices may fail to obtain their addresses normally, depending on the order they are started or when they are started.
10	Failure due to a setup mistake	A failure occurred due to a setup mistake made during the installation work.

2.2 Classification of causes

The causes of the failure cases listed in Table 2-1 in the preceding section were analyzed to examine what happened and where it happened. Table 2-2 below summarizes the results of this analysis. The numbers within parentheses in the Failure case column correspond to the numbers in Table 2-1 Failure cases.

Table 2-2 Classification of causes of failure cases

Network	Layer	Failure case		Cause of the failure
		Installation stage	Operation stage	
HN	User		Failure due to improper use (8)	Failure due to a misunderstanding or operation mistake by the user. Such a failure is not recognized as a failure in the other layers described below.
	Service interference	Influence by another terminal (5) Failure due to an improper startup order (9)	Influence by another terminal (5) Silent fault (6)	Although the terminal, service, and network are fine by themselves, a fault occurs when they are used in combination.
	Terminal	Setup mistake (10)	Malfunction due to aging (3) Silent fault (7)	Failure caused by the hardware or software of the terminal
	Network		Occupation of the communication bandwidth (2) Interference with an existing wireless device (4)	Failure due to insufficient network bandwidth; failure that occurs as the quality of communication degrades because there is a large volume of traffic of another type, because of radio channel interference, etc.
WAN	Service or network	Interference between services (1)	Occupation of the communication bandwidth (2)	Mismatch between the network characteristics (bandwidth and line type) and service requirements

Table 2-2 first classifies the causes of failures into two major categories, according to which network they are associated with (HN or WAN). Then, the causes of failures associated with the HN are further classified into four layers: network, terminal, service interference, and user. Here, the term "terminal" refers to not only the devices shown in Figure 1-1 but also network devices, as described in detail below. While the architecture of the application layer is mainly described with regard to the service platform, the network layer functions also need to be discussed from the perspective of customer support for HN services. Hereinafter, therefore, both the devices on the service platform and network devices are collectively refer to "terminals."

(1) Distinction between HN and WAN

The failure recovery process begins with isolating the section associated with the failure. Specifically, when the HN architecture shown in Figure 1-1 is assumed, the first important step is to determine whether the failure is due to a problem inside the premises (HN section) or a problem outside the premises (WAN section).

Telecom carriers and service providers are responsible for the WAN section, and they manage the equipment and services in this section. By contrast, there is no business entity in charge of managing the HN section in an integrated manner, and the management PF is expected to play that role.

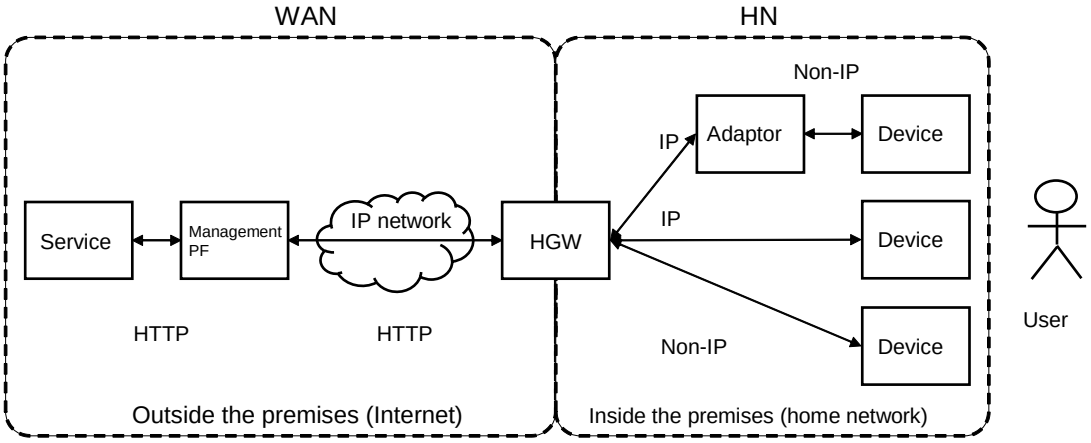

Figure 2-1 Distinction between WAN and HN

(2) Concept of layers (HN/WAN)

Next, the causes of failures were organized by layer.

Specifically, an attempt was made to classify them into four layers: network, terminal, service interference, and user.

Network: Failure due to congestion, insufficient network bandwidth; radio channel interference, etc.

Terminal: Failure of the terminal itself caused by its hardware or software

Service interference: Although both the terminal and network are fine by themselves, a failure occurs when they are used together.

User: Failure due to the user's operation mistake or insufficient understanding of the service. Such a failure is not recognized as a failure in the other three layers described above.

Note that failure cases and causes associated with the WAN can also be classified into layers. Since this technical report focuses on the discussion of the HN, however, only those failure causes that are directly associated with the HN are described herein. Failures associated with the WAN and their causes are to be analyzed on a separate occasion.

Chapter 3 Underlying Technologies

3.1 Overview

This chapter describes the existing technologies used to solve the individual causes of failures analyzed in Section 2.2, as well as technologies that will be needed for the same purpose in the future. Since the functions described in this chapter are divided into two types (customer support functions and failure avoidance support functions), these two types of functions are outlined first.

(1) Customer support functions

An adequate environment needs to be prepared so that a customer wishing to use a HN can decide on the overall configuration of devices and set them up smoothly in the installation stage. If the terminal has functions that pre-check for hardware components, applications, and services that may cause contention on the network, it can notify the customer about potential problems in advance. In the operation stage, the customer can use the terminal without worry if it has functions that check the setup information, network connectivity, and usage status of devices, as well as functions that inform the customer about the traffic information and load durability of the network.

(2) Failure avoidance support functions

Even if the customer sets up a HN according to the guideline accompanying the terminal, he or she may make a setup mistake and a failure may occur due to that mistake. For such a failure, failure avoidance support can be provided if the terminal or adaptor has functions that automatically set up devices (automatic device discovery, setup, and startup order control). In the operation stage, it is desirable that a bandwidth guarantee function based on traffic control (media-specific, app-specific, etc.) be supported between the terminal or adaptor and the linked HGW.

Based on what is mentioned above, Table 3-1 summarizes the functions required for each individual layer. The following sections describe these functions in detail in the order of the terminal which is the smallest unit that makes up the system, network (HN/WAN), and application.

Table 3-1 Functions required for each individual layer

Network	Layer	Item	Required function
HN	User	User behavior check	User operation mistake detection: "Unusual" operations and conditions are detected based on the operation history and other information.
	Service interference	Resource combination check	Service interference detection: Interference-prone combinations of terminals, software products that run on terminals, and communication protocols are identified.
	Terminal	White goods (home appliances)	Basic device information acquisition: Information about the model name and installation date is acquired to identify faults due to aging (ECHONET, DLNA, etc.). Terminal connection check: Network reachability is checked (e.g., ICMP). Terminal operation information acquisition: Device status, error information, and statistics information are collected to identify the cause of a failure (ECHONET, DLNA, etc.). Total information management: The contract information of the terminal is acquired (e.g., asset management). Automatic terminal setup: This function acquires the setup information of the terminal from the outside and sets up the terminal.
		Black goods (audio-visual products)	
		Silver goods (PCs/smartphones)	
		Network devices	
	Network	Load test tools	Basic measurement function: Acquisition of the basic MIB statistics information (TTC HTIP and SNMP) Lower layer load test: Test using a ping flooding or netperf network load tool Application layer load test: Test using a load generation device
WAN	Service/network	Service check	Network layer contention check: Contention check using information acquired with SNMP, OAM, etc. Application layer contention check: Contention check using information acquired with BBF TR-069, UPnP DM, etc.
		Evaluation tool	Connection status: Traffic information collection Bandwidth control: QoS control

3.2 Functions for solving terminal-related problems

This section first describes the terminal, which is the most fundamental element that comprises a HN service. In order to solve terminal-related problems, it is necessary for the terminal to have interfaces needed for failure resolution and automatic setup. An interface needed for failure resolution is one for acquiring internal information. There are various kinds of internal information, ranging from the setup information that the terminal needs to be connected to a HN and perform a minimum range of operations to ownership and contract information necessary for asset management or information management. Sections 3.2.1 to 3.2.4 describe the acquisition of information from different viewpoints, respectively. In relation to settable information, Section 3.2.5 describes the automatic setup function as a mechanism for setting information from the outside of the terminal. The device that communicates with the terminal is the HGW. The HGW further relays communication to the WAN and accomplishes the management of terminals using the Internet server or cloud.

3.2.1 Basic terminal information acquisition

Terminals are ① white goods, ② black goods, ③ silver goods, and ④ network devices. Note that the devices defined as device objects in ECHONET are considered to be white goods. Those devices defined as both ① white

goods and ② black goods, such as TVs, are considered to have different functions, depending on whether they are treated as white goods or black goods. Devices that do not fall into any of the categories of ① to ④ are considered to be white goods and connected within the framework of ECHONET.

Acquiring information from a terminal makes it possible to detect a fault due to aging, find out when the fault occurred and where the recalled product is used and, in the case of a network device, determine whether the performance is sufficient for interaction with other devices. The information to be acquired includes the manufacturer name and product information of the terminal (model name, manufacturing date, and hardware and software information (CPU, memory capacity, and OS)) and the installation information (installation dealer, date, location, and jigs (e.g., information about water heater piping or the platform for a public viewing screen)). One possible method of managing the acquisition of terminal information is to gather the information from the terminal to the HGW (including the case when the connection is established via an adaptor) by using the standard protocol and manage the gathered information in the cloud. Candidates for the standard protocol include ECHONET Lite, DLNA, and UPnP. Since ECHONET Lite has an interface defined for acquiring error codes from devices, the system administrator can reference the information gathered in the cloud via the maintenance interface and resolve failures by utilizing this information.

3.2.2 Terminal connection check

In a HN, a terminal connection check can be conducted by sending a message from the HGW to the terminal and checking the response. However, if any of the network devices on the path between the HGW and terminal is faulty, it is necessary to check the connection on a section-by-section basis by referencing the HN topology and other relevant information.

Various communication interfaces (Wi-Fi, PLC, ZigBee, etc.) are used between the HGW and terminal (including the case when the connection is established via an adaptor), and they are connected using hubs, access points, and gateways. When a sensor or other non-IP terminal is connected via wireless communication, there is a need to have the HGW poll the connection at regular intervals and manage the polling status in order to save the hardware resources of the terminal. The HGW and terminal may be connected using network devices, in which case it is necessary not only to check the connection between the HGW and terminal but also to check each section of the path to see if there is any problem. For this purpose, support of a protocol for acquiring the HN topology information, such as TTC HTIP (ITU-T G.9973), IETF ICMP, IETF SNMP, LLDP, and UPnP, is expected.

3.2.3 Terminal operation information acquisition

The operation information of a terminal includes information deemed necessary for failure analysis besides the basic information described in Section 3.2.1. The information to be acquired is information considered to be useful in determining whether the terminal is operating stably, such as the frequency of use (period of continuous use and period during which the terminal is not in use), logs of various events including terminal restarts and failures, and the internal conditions of the terminal that are not included in the basic information. This information is used to perform failure analysis at the time of service outage, as well as to connect a terminal linked with another terminal suspected to have a failure and examine its effect.

The items to be managed may include device operation records, chronological data of the internal conditions of the device, and device failure analysis log (the detail level of the log can be changed). One possible management method is to acquire device operation information and record and collect failure analysis log information by using a communication protocol such as ECHONET Lite or DLNA.

3.2.4 Total information management

From the viewpoint of managing terminals as assets, total information management deals with all the information to be managed from the time when a terminal is connected to a HN for a service until it is disconnected from the HN when the use of the service ends. For example, when a terminal is used beyond the service life specified by the manufacturer, whether the service life has expired cannot be determined if it is unknown when the use of that terminal started. In total information management, therefore, various kinds of information, including the installation date, owner, and contract type of the terminal, is managed. In many cases, total information management is intended for silver goods such as PCs and smartphones, rather than embedded devices such as home appliances and housing equipment. Figure 3-1 shows the configuration of an asset management system that manages the information related to terminals. Asset management software is installed in the operating systems of PC and smartphone terminals, and this software gathers the terminal information to the management server in response to server requests.

The items to be managed (inventory information) may include the hardware information of the terminal (CPU model number, memory capacity, hard disk capacity, OS type and version, and IP address in the case of a PC, smartphone, etc.), operation information (ownership and contract types, installation location, user/administrator, and purchase date), software information (software installed, content of the license, and frequency of use), and security information (settings of the antivirus software, browser, etc. and management of certificates and others).

Figure 3-1 Asset management system

The information to be acquired from the terminal has been described from four viewpoints in Sections 3.2.1 to 3.2.4. There is no clearly defined scope, however, for any of the information to be acquired from these four viewpoints. Therefore, which terminal information should be acquired is to be clarified in individual use cases.

3.2.5 Automatic terminal setup

While a setup mistake of a terminal in a HN may be exposed as a plain failure, such as the terminal being unable to connect to the HN or not working, it is often the case that the mistake becomes a hidden factor that is difficult to locate. Setup mistakes are prone to occur when a non-expert user installs a terminal or when many terminals are installed by a single expert. Therefore, a function that manages terminal setup information in a centralized manner and automatically sets up a terminal at the time of installation is an effective means of reducing setup mistakes. The automatic setup function is effective not only when a terminal is installed but also when the HN configuration is changed or when the software of a terminal is updated.

Figure 3-2 shows the basic system configuration for automatic setup. A setup agent resides in the terminal, and this agent queries the HGW or a server on the Internet to acquire the setup information. The communication standard for implementing this function differs depending on whether the terminal is treated as a network device or a home appliance. Each of these cases is described below.

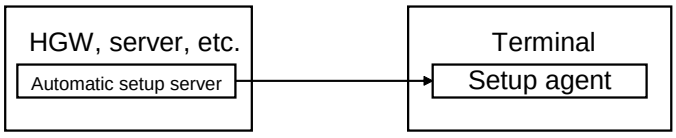

Figure 3-2 Automatic setup system

(1) Automatic setup for a network device

In IPv4 communication, DHCP (Dynamic Host Configuration Protocol) defined in IETF RFC2131 is used to set the parameters necessary for IP communication, such as an IP address and DNS server address, in the terminal. In a HN, the DHCP server function that sends such parameters is usually provided by a network device that connects the HN to the WAN, such as a broadband router or HGW.

In IPv6 communication, two protocols are used to set an IPv6 address in the terminal: DHCPv6 (Dynamic Host Configuration Protocol for IPv6) defined in IETF RFC3315 and RA (Router Advertisement) defined in IETF RFC4861. DHCPv6 is also used as the protocol for setting a DNS server address and other parameters necessary for IP communication in the terminal. In a HN, the DHCPv6 server function or RA transmission function that sends such parameters is usually provided by a network device that connects the HN to the WAN, such as a broadband router or HGW.

(2) Automatic setup for a home appliance

The automatic setup function necessary for the application-level communication is provided by an application protocol. For ECHONET Lite, for example, communication protocols are provided that discover ECHONET Lite-compliant terminals or acquire information about the ECHONET Lite objects managed by ECHONET Lite-compliant terminals. Another example is UPnP, for which communication protocols are provided that discover UPnP-compliant terminals or acquire information about the functions implemented by UPnP-compliant terminals.

3.3 HN troubleshooting functions

This section describes the network of terminals connected to a HN as the elements that comprise a HN service. Since the function for solving the HN problem related to the setup of network devices has already been discussed in Section 3.2, Sections 3.3.1 to 3.3.3 describe how to troubleshoot problems caused by traffic in the HN.

3.3.1 Basic measurement functions

For a HN, there are two basic measurement functions: configuration information acquisition function and statistics information acquisition function. The configuration information acquisition function can be used to acquire information about the connections of terminals that make up the network and the configuration information of individual terminals, both of which are needed for troubleshooting. The statistics information acquisition function can be used to grasp the operating status of each terminal that comprises the network. These two functions are described below, respectively.

(1) Configuration information acquisition function

The configuration information acquisition function is defined as a function that acquires the information about the configuration of individual terminals, including network devices, that make up the system for which customer support is provided. Examples of configuration information include the following. (Figure 3-3)

- Physical function blocks of the terminal (e.g., communication interface card, CPU, and memory)
- Logical function blocks of the terminal (e.g., VLAN and other logical communication interfaces and DVD player and TV functions of a TV with a built-in DVD player)
- Setup information of logical function blocks (e.g., IP address and DNS server's IP address assigned to the logical communication interface)
- Connection information of terminals (e.g., terminal x having MAC address A is connected to logical communication interface 1)

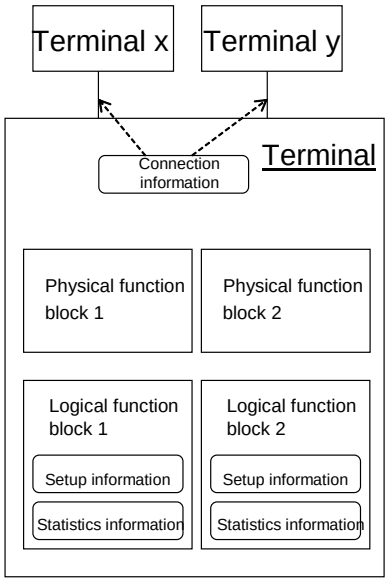

Figure 3-3 Relationship of terminals, configuration information, and statistics information

Examples of existing protocols that implement the configuration information acquisition function include TTC HTIP (Home-network Topology Identifying Protocol) (TTC JJ-300.00 and ITU-T G.9973), LLDP (Link Layer Discovery Protocol), UPnP Forum UPnP (Universal Plug and Play), and IETF SNMP (Simple Network Management Protocol).

(2) Statistics information acquisition function

The statistics information acquisition function is defined as a function that acquires the information about the operating status of individual terminals, including network devices, that make up the system for which customer support is provided. Examples of statistics information include the following. (Figure 3-3)

・Number of packets transmitted, received, and dropped by the logical communication interface
・Number of frames that failed to be played back by the logical function block that implements the video codec function
・Terminal startup time and continuous operating time

An example of an existing protocol that implements the statistics information acquisition function is SNMP standardized by the IETF.

3.3.2 Lower layer load test

The lower layers in this section are defined as layer 2 (Ethernet, etc.), layer 3 (IP, etc.), and layer 4 (TCP, UDP, etc.). The lower layer load test can be used to check whether the communication processing of terminals or the network connecting terminals does not have any problem, by applying a traffic load of a lower layer on the communication between terminals that comprise a HN.

The lower layer load test requires a capability for processing test traffic at the packet (layer 3) or frame (layer 2) level. To implement the test traffic processing capability, the terminals comprising a HN (or some of them) need to have the following two functions. (Figure 3-4)

・Test traffic transmission function

This function transmits packets in a required test traffic pattern from one of the terminals, including network devices, that make up the system for which customer support is provided to another terminal.

・Test traffic reception function

This function causes the test traffic receiving terminal to receive test traffic and check how much of the traffic the terminal can receive.

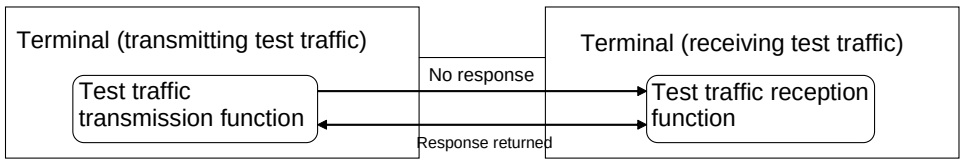

Figure 3-4 Configuration for implementing the test traffic processing capability

The test traffic processing capability can be implemented as in the examples given below.

- Ping (ICMP echo request) is used as test traffic, and a check is made by the receiving terminal returning a response to the transmitting terminal. The advantage of this method is that it may be unnecessary to add special functions as the test traffic transmission and reception functions. The drawback is that layer 4-dependent problems (e.g., insufficient TCP processing capability) cannot be detected.
- Packets that can be received by the receiving terminal are used as test traffic, and the processing status of the test traffic is checked using the statistics information acquisition function of the receiving terminal. While the test traffic transmission function needs to be added, the advantage of this method is that it may be unnecessary to add a special function as the test traffic reception function.
- The dedicated test traffic transmission and reception functions are added. While the amount of development work is increased for the additional functions, this method has the advantage that a test suitable for the service can be implemented, such as measurement of VoIP packet reception jitter.

The more terminals capable of generating test traffic a HN has, the broader range of the HN can be the target of the lower layer load test. On the other hand, however, the problem of increased terminal costs arises from the addition of functions for the lower layer load test. One possible method to avoid this problem is to install the test traffic transmission function only in HGWs and other devices that have sufficient processing capability, although the communication paths that can be used for the test will be limited.

Examples of existing tools that can implement the functions necessary for the lower layer load test are given below.

- Ping flooding: An echo request is transmitted without waiting for an echo reply, by using the ping command option.
- Ethernet OAM: Administration and maintenance function for Ethernet networks standardized in ITU-T Y.1731. For example, a continuity check can be made using Ethernet OAM LB (Loop Back) in the same way as ping.
- iperf: Free software that can execute a load test using TCP and UDP packets. It implements both the test traffic transmission and reception functions.

Before a load test is conducted, it may be necessary to check continuity at a lower layer. For a layer 3 continuity check, ping and traceroute commands can be used with the ICMP echo request and reply. For a layer 2 continuity check, Ethernet OAM LB (Loop Back) and LT (Link Trace) of Ethernet OAM can be used.

3.3.3 Application layer load test

The application layer load test can be used to check whether the data processing of terminals or the network connecting terminals does not have any problem, by applying a traffic load at the application layer.

The application layer load test requires an application-level test traffic transmission function. It is assumed that the test traffic reception function is adapted to the application used in the actual service. (Figures 3-4 and 3-5)

・The test traffic transmission function resides in both the test target terminal (test traffic receiving terminal) and another terminal, and test traffic is transferred via the network.

The application-level function for generating test traffic (video, audio, sensor data, etc. used by the actual application) is installed in a device that has sufficient processing capability, such as a HGW, and the test traffic is transmitted to the test target terminal. (Figure 3-5)

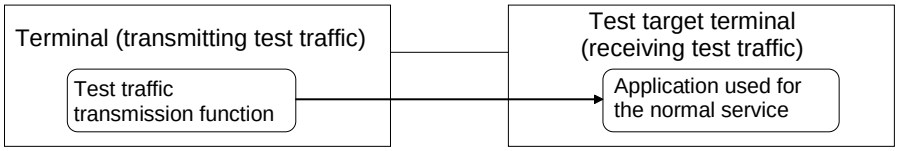

Figure 3-5 When the test traffic transmission function resides in both the test target terminal and another terminal

・The test traffic transmission function resides in the same terminal as the test target terminal (test traffic receiving terminal), and test traffic is transferred inside the terminal.

The application-level function for generating test traffic (video, audio, sensor data, etc. used by the actual application) is installed in the test target terminal. (Figure 3-6)

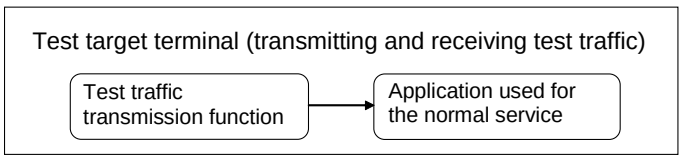

Figure 3-6 When the test traffic transmission function resides in the test target terminal

The application layer load test should preferably be able to check the traffic processing status of the application by using the statistics information acquisition function. However, in cases where the user can judge the service quality through his or her five physical senses, as in a video delivery service, it may be possible to conduct the test without a quantitative index such as statistics information.

3.4 WAN troubleshooting functions

Sections 3.4.1 and 3.4.2 describe the functions that the customer service is required to have in case the cause of degradation in the quality of communication between WAN and HN is assumed to lie on the WAN side. In addition, Section 3.4.3 describes the connection status and test and Section 3.4.4 describes the method of measuring the available bandwidth and the methodology on bandwidth control for coordination between services. Note that equipment faults and similar problems of telecom carriers are excluded from the scope of customer service.

3.4.1 Network layer contention check

Network layer contention can stem from two types of problem: (1) interference between different communication systems or effect of leaked radio waves on the service; and (2) contention of network resources (communication bandwidths).

(1) Interference between communication systems and contention of services

As portable terminals have evolved and come into widespread use, it is becoming increasingly common that multiple broadcast and communication services are used in a single household. These broadcast and communication services have problems concerning signal interference between different systems and leaked radio waves, and service providers are legally required to give an appropriate explanation of such problems to users before starting the provision of a

service (Article 150 of the Broadcast Act and Article 26 of the Telecommunications Business Act). When users wish to subscribe to a new service in addition to the existing service or switch to a different service, they need to judge the availability of that service and make an arrangement with the service provider for themselves, based on an understanding of the conditions for service provision. In reality, however, many users have only a limited knowledge of communication and broadcast technologies and may get into a trouble.

Service providers and device manufacturers are making constant efforts to solve technical problems concerning signal interference and leaked radio waves. General residential users, however, often tend to continue to use old devices as long as they are usable. It is feared, as a result, that technically problematic devices remain in users' homes. Managing the information about such devices will also pose a challenge. Moreover, in the case of a wired service, it is necessary to grasp the usage status of the wiring installed on the premises (piping and line number information of installation wiring or customer premises wiring) and give consideration to the effect on the existing service. Since the user or the owner of the building may have no one in charge of the information about equipment and wiring pathways, managing such equipment information is desired for the purpose of ensuring adequate communication quality and smooth service provision. As for wireless services, it is considered effective to manage the history of radio wave interference and other problems on a building-by-building basis.

What can be done as customer support for these problems is to assist the user in managing information or complement the user's effort so that the devices and services used by the user can be checked for interference between communication systems and contention of services. This is expected to prevent the assumed problems or mitigate their effects.

(2) Contention of network resources

Next, the problem arising from the limit on the bandwidth of the access network (also known as "congestion") is described.

Operations whereby the user on the go manipulates terminals in the HN over the Internet are now widely known, and the use of cloud services provided from the WAN to the HN (video streaming, online gaming, etc.) is steadily increasing. As the HN is used in increasingly advanced ways and more terminals are connected to it, the volume of traffic with the WAN is expected to grow. In the cases mentioned above, where the operability of WAN-based services and the quality of cloud services depend on the quality of communication (delay, packet loss, and jitter), customer support is expected to be required if a problem occurs.

As the first action for customer support, it will be necessary to grasp the communication status. With regard to the volume of traffic between HN and WAN, the HGW needs to support the statistics information functions for traffic processing described below in order to handle the number of transmitted and received packets, number of dropped frames, total number of received bytes, delay time, and other statistics information (number of transferred packets, dropped packets, errors, etc.). Since the burden of dealing with such statistics information for traffic processing is placed on the HGW, the implementation of the HGW is considered to pose a cost problem. To collect this information, SNMP (setup information and statistics information) and BBF TR-069 (setup information) functions can be used.

3.4.2 Application layer contention check

Advances in the use of the HN not only realize the remote operation of terminals but also enable the HN to be linked with diverse types of information and services by utilizing the rich pool of resources of the cloud, thus allowing comfortable, eco-friendly setup of a terminal as well as sequence control and automatic adjustment of multiple terminals. When these uses are considered, on the other hand, it is anticipated that there may be cases where contention occurs between the operation performed for the terminal on the user's premises and the control command

from the cloud service or a command is given that is different from the one specified by the user in the HN. Specifically, two contending room temperature setting services alternately may issue commands to set the room temperature at 20 degrees Celsius and 18 degrees Celsius according to their respective programs, or lights may be switched on and off repeatedly. These phenomena are typical examples. In the case of such inter-service contention, it is often difficult for the contending services to identify the problem and make adjustments mutually because they are both operating and exerting control normally. Solving this problem requires a function that mediates between services from the viewpoint of safety, in addition to the user's intention and decision.

(1) Solution to the problem

In order to solve the problem through customer support, it will be necessary to monitor the status in the home, implement a function that mediates between services, and make a prior agreement and rules with the user for stopping one of the contending services from the viewpoint of safety.

This technical report assumes that, as described in Section 3.4.1, the problem should be solved through dialogue with the user based on an understanding of the services in use and the current status of the HN.

As the means of management and implementation, ECHONET (connected terminal discovery, terminal information, and status reference) and TTC HTIP (connected terminal discovery, terminal information, and topology identification) can be used to monitor the HN status on the premises, as described earlier. However, since these protocols are confined to the link-layer broadcast domain, a function that remotely acquires information on the assumption of using BBF TR-069 (acquiring setup information remotely) or a similar protocol needs to be implemented in the HGW in order to remotely acquire the information mentioned above. It is also possible to use the network layer SNMP (acquiring setup information and statistics information remotely).

(2) Maintaining the user's autonomy in management

There is one issue that pertains to this problem. As the use of cloud-linked distributed, cooperative services becomes common in the HN, there may be cases where applications are installed in terminals without the user's knowledge or the terminal settings are automatically changed. Some users may not want these things happen in their HN, which is supposed to be the most private space, or may prefer to keep these operations under their control.

Therefore, the HN configuration, such as installed software and terminal information, needs to be managed while taking into consideration the wishes of these users. In order to address this issue, it will be necessary to consider implementing a function that analyzes the traffic (frames) passing through the HGW connected to an external network to detect suspicious communication (DPI: Deep Packet Inspection) and a function that blocks the use of specific applications (filtering), among other functions.

3.4.3 Connection status

Sections 3.4.1 and 3.4.2 described the forms of customer support for the problems assumed for the network layer and application layer, respectively, and the functions required for customer support. The following sections, 3.4.3 and 3.4.4, describe the maintenance functions and testing methods necessary for the platform that are common to all those problems.

(1) Continuity check

Continuity test functions are built in the WAN protocol on the assumption that they are used by telecom carriers, and it is possible to use these functions. This, however, requires careful consideration based on how the HN is connected to the access network. Since the point of demarcation also changes depending on whether the HGW is seen as business communication equipment or terminal equipment, this report goes no further than pointing out the problems

to address. If a continuity test is conducted at a layer at and below what TCP/IP defines as the link layer, the diverse communication systems for the access network will pose a problem for customer support. It is a challenge to meet the constant need to support new systems while at the same time ensuring continued support for old standards.

It is assumed that Ethernet OAM (ITU-T Y.1731 and IEEE802.1ag) will be used for Ethernet and that ATM OAM (ITU-T I.610) will be used for ATM. Also, the use of LCP, which is part of the PPP protocol suite, is expected for PPPoE and PPPoA that are used for general Internet access.

In a network, the test using an echo request of ICMP (IETF RFC792 and IETF RFC4443) - also known as a ping test - is effective. For TCP, Telnet (IETF RFC854) can be used.

(2) Delay measurement

The use of ICMP (IETF RFC792 and IETF RFC4443) for the network layer is effective.

(3) Status reference

When the condition of the connection failure is not continuous but temporary or intermittent, it is effective to consider maintenance action by grasping the situation through the use of the HGW statistics information and other related data. This will require the collection of log data such as communication history (link-up time, link-up duration, traffic volume, and alarms) and statistics information (number of dropped frames and number of errors).

3.4.4 Bandwidth control

(1) Measurement of communication quality

The access network connected to the HN and even the Internet at the higher level use the so-called best-effort service and, in fact, the quality of communication varies depending on the user's environment. Therefore, a function that grasps the available bandwidth for each individual user environment will be needed.

There are two methods of measuring the available bandwidth: passive measurement and active measurement. The passive measurement method analyzes the actual traffic of the user to estimate the available bandwidth. Since the measurement depends on the user traffic, this method is inferior in terms of accuracy. The active measurement method, by contrast, transmits test traffic and examines how it is processed, in order to estimate the available bandwidth. The drawback is that the test traffic may interfere with the service in use.

The existing active measurement techniques include PPDP (Packet Pair or Train Dispersion), VPS (Variable Packet Size), SLoPS (Self-Loading Periodic Stream), and TOPP (Train of Packet Pairs).

It is possible to use these active measurement techniques in those cases of customer support where interference with the service is acceptable. There have also been notable research reports on ImTCP (Inline measurement TCP), an active measurement technique that has only a minor impact on the network.

(2) Bandwidth control

After the statistics information of the HGW is checked as described in Section 3.4.1 and the remaining bandwidth is grasped as described in the preceding paragraph, it is necessary to take corrective action. The bottleneck is at the point where the traffic that the HN having a relatively broad bandwidth sends to the WAN that is relatively limited in bandwidth passes through the HGW.

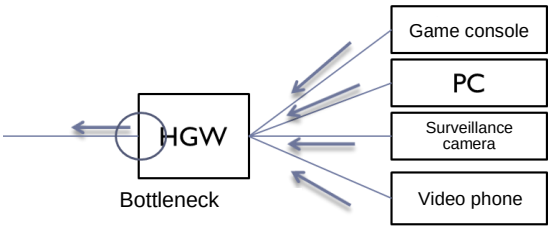

Figure 3-7 Bottleneck in communication between HN and WAN (uplink traffic)

If congestion occurs in the HGW, it is important to prioritize the traffic received from each individual terminal.

Regarding this issue, TTC TR-H.QoS (Sup11) shows the "framework for coordinating home network QoS technologies" (Figures 3-8 and 3-9) in its "Analysis of class-based home network QoS solutions" section.

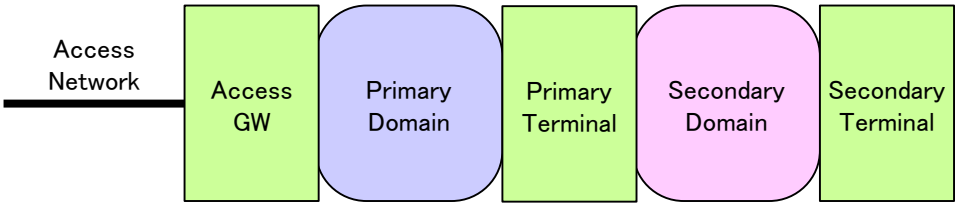

Figure 3-8 Home network application model defined in ITU-T H.622

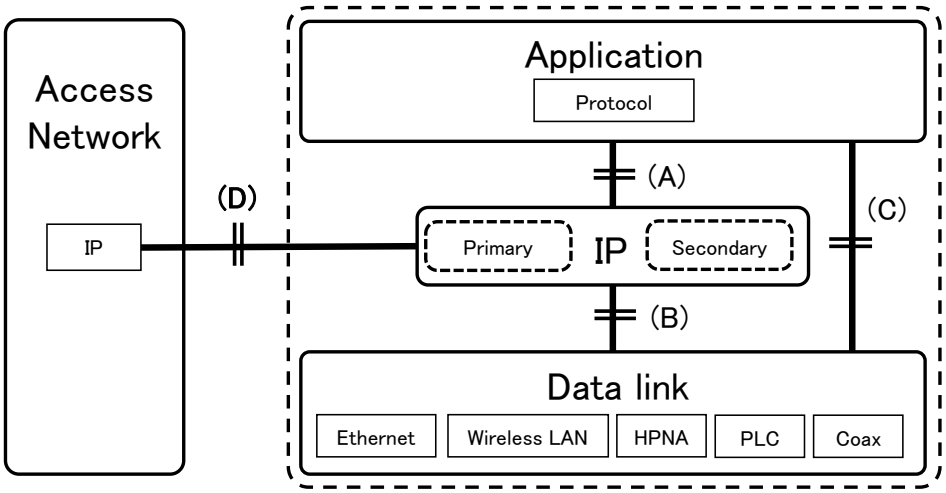

Figure 3-9 Framework for coordinating home network QoS technologies

TTC TR-H.QoS (Sup11) defines four interfaces for QoS adjustment, analyzes the documents from different standardization bodies concerning priority levels and marking, and discusses the direction of coordination of QoS technologies. Since interfaces A and B are intended for closed communication inside the HN, they have been considered in many standardization stages. By contrast, interface D, which concerns communication between WAN and HN, is mentioned in few documents (TTC TR-H.QoS (Sup11), p. 9).

As users come to use the HN in more advanced manners, the standardization bodies will mutually make adjustments and this will need to be considered from the viewpoint of securing critical communication as well.

Assuming such adjustments, it will be necessary for the HGW to have a bandwidth control (priority control) function in order to enable customer support. In addition, the HGW will need a function to prioritize the traffic from individual terminals so as to allocate the bandwidth adequately, and the terminals will need a function to mark the frames and packets they send according to their priority.

3.5 Function to solve service interference

Sections 3.2 to 3.4 have described how to identify the causes of failures that occur at and below the transport layer, such as those due to the terminal, HN, or WAN setup, traffic, or radio wave interference. Sections 3.5 and 3.6 describe how to identify the causes of failures that occur at the application layer.

One possible cause of a failure occurring at the application layer is service interference. For example, in item 5 of the table listing the failure cases, a case is described in which an attempt to play back video data recorded in a NAS (Network Attached Storage) connected to a HN on a PC using dedicated application fails because the communication is shut down. The cause of this failure is the bug of another application running on the same PC, which damages the video data that the PC receives. As in this case, a failure may occur due to the combination of functions of a terminal connected on the HN or software products running on a PC.

In order to solve this problem, it is necessary to create a list of applications and functions (hardware) running on a terminal and manage the information about the combinations of applications or functions that may cause a failure when used simultaneously, in addition to the information about the terminal connected on the HN, as shown in Figure 3-10. The information about such combinations, however, can only be obtained on an empirical basis. The solution is therefore considered to be to accumulate the information about the combinations of contending applications in a database and check the combinations of terminals set up inside the HN and applications installed in those terminals.

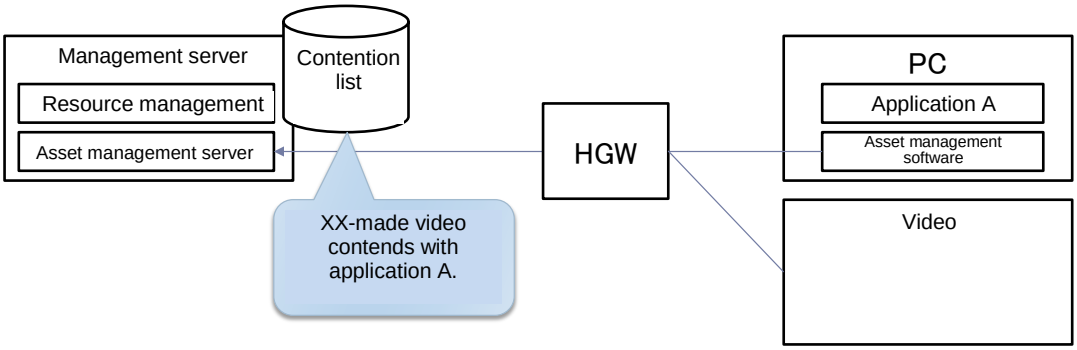

Figure 3-10 Architecture for enabling a contending service check function

Figure 3-10 shows an architecture for checking contention among HN-connected applications. Home appliances connected inside a HN, as well as PCs, smartphones, and other terminals that run on a universal OS are connected. The information about applications running on a PC is discovered by the asset management software that detects installed applications. On the cloud side, there is a total information management function that manages the resources residing on the HN by using a management server. While the terminal information about home appliances is acquired with ECHONET Lite or other similar protocol when they are connected, the asset management system described in Section 3.2.4 is used to acquire the terminal information about terminals that run on a universal OS such as PCs. Specifically, the asset management server runs on the management server and communicates with the asset management software of the PC to acquire the information about the installed applications. The resource management function combines this information with other terminal information to create a list. Also, the resource management function references the database of combinations of contending applications and functions (terminals) to discover contending applications and other resources.

3.6 Functions to solve a failure due to a user operation mistake

A failure due to a user operation mistake refers to a case where the system behaves in an unintended way due to the user's misunderstanding or operation mistake and the user misrecognizes that behavior as a failure although the system itself is operating normally. For example, in the case of a service whereby the physical conditions of a convalescent

patient are monitored with a vital sensor (one that measures biological information such as blood pressure and body temperature), an abnormality is detected if the patient forgets to wear the sensor. In this case, while the system is operating normally, the values of obtained data become abnormal, which is recognized as a failure. Another example is when the user needs to perform three operations A, B, and C but actually performs only two of them, A and C, skipping operation B. After the last operation C is performed, the terminal or service behaves in an unintended way. In this case, too, while the system is operating normally, the user misrecognizes that the system has failed, unless the user realizes that he or she forgot to perform operation B.

While there is no established way of detecting this type of problem, it is necessary to provide some method for notifying the user about the fact that the user operation is unusual. The following detection methods are possible.

(1) Rule-based detection

One possible method is to save the history of the internal states of the terminal or application and the operations by the user and make a judgment based on the relationship between the internal state and operation. This involves creating a set of rules regarding the relationships of operations that are empirically unlikely to occur and internal states and recording operations that meet the rules. When a failure is reported from the user, this history is checked to determine whether the problem is a user operation mistake or system failure.

(2) Statistical processing-based detection

This method is to save the history of the internal states of the terminal or application and the operations by the user and create a list of chronological patterns of normal operations and corresponding internal states from the chronological data of the internal states and operations. When a failure is reported from the user, whether the reported event matches any of the normal operation patterns is checked to determine whether the problem is a user operation mistake or system failure.

Chapter 4 System Technical Requirements

In a HN, multiple systems run simultaneously and many minor problems keep happening. This situation is considered to make it difficult to achieve failure recovery in the HN. Chapter 3 described the information to be acquired for the individual resources - i.e., terminals (terminal hardware), services (terminal software and applications), and networks - as well as the functions to support the recovery process. Chapter 4 describes the framework for enabling the centralized management of simultaneously happening problems and information to be referenced and providing the information that the support provider or department, such as a call center, needs to offer remote support.

4.1 Overview

In a HN service, the system administrator is not present at the place where the terminal is installed, such as the user's home, and the premise is that the service is managed from a remote location. With conventional over-the-phone support, however, it is often difficult to accurately grasp what is happening in the HN, which makes failure recovery difficult as well. In the event of a failure, it is necessary to acquire various kinds of information before conducting an analysis of the cause, including the information about the terminals connected to the HN, HN topology information, traffic information, information about the applications running on PCs, smartphones, etc. These days in particular, the HN tends to have more terminals connected to it than before and a failure can occur due to a complex cause, making it often impossible to identify the cause just by obtaining the information about the failed terminal. Therefore, providing support from a remote location requires a framework for acquiring detailed information that cannot be obtained through the traditional method of hearing directly from the user and aggregating such detailed information to a certain degree for analysis.

Figure 4-1 shows the architecture of the basic functions necessary for remote support. Two kinds of functions are shown in this architecture. One is to remotely check and change the settings of the terminals inside the HN and those of the network. The other is to collect, on a real-time basis, the information about the internal states and traffic of the terminals inside the HN and about those of the network. The content of this figure is briefly described below. The managed agent residing in each terminal manages the setup information and internal states of the terminal and, if a setting change is made from the outside, changes the settings of the terminals accordingly. The WiFi AP (access point) or router inside the HN has functions to manage the network traffic and setup information and return responses to queries. The HGW features the configurator that sets up terminals and network devices and the resource information collector that aggregates internal information and traffic information. In the management PF, the static information such as setup information and the dynamic information such as internal states are managed by resource management. There are two types of applications; one is for customer support (management application) and the other is a general application (service application). The management application displays the status of the HN or a terminal on the user premises in response to an end user's query about a failure and performs an operation as necessary such as changing the settings or generating test traffic. The operations that can be performed by the management application are implemented by using the functions for failure cause analysis and recovery described in Chapter 3.

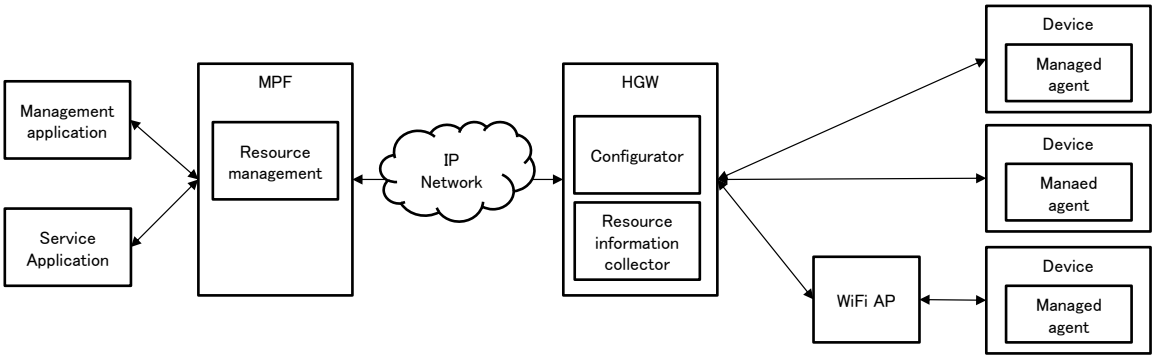

Figure 4-1 Framework for remote support

Using the same architecture, BBF TR-069 supports remote terminal setup and firmware update functions although these functions are limited to device management. Also, a recently developed standard - ISO/IEC 30100 - is intended to manage HN-connected resources from a remote location. ISO/IEC 30100 offers a resource management framework for managing not only HN-connected terminals but the network and software as well. While extending BBF TR-069 and other widely used standards is considered viable at the moment for implementing remote support, it is also anticipated that a new framework, such as that defined in ISO/IEC 30100, will come into widespread use in the future.

The remaining part of Chapter 4 describes ISO/IEC 30100 and the related standards.

4.2 ISO/IEC 30100

ISO/IEC 30100, established in 2013, concerns HN resource management. This standard defines location information (installation locations), device information (internal function states), network information, and service information as HN resources. These types of information is collected from the HN by the HN resource management function residing on the Internet, and the collected information is referenced by the management application. The management application is referenced by call center operators and maintenance personnel, who assist the user in failure recovery or perform recovery work by changing the terminal settings (terminal or network device) and other necessary operations from a remote location.

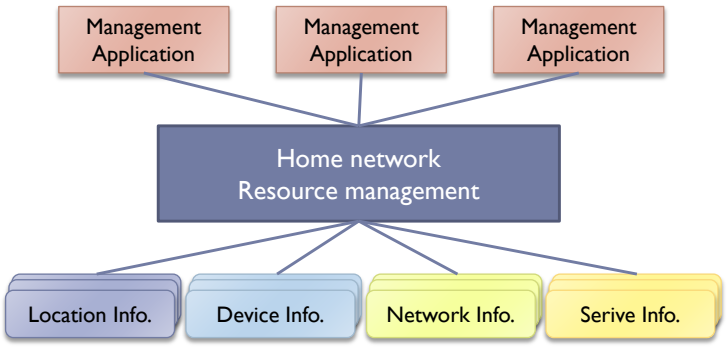

Figure 4-2 HN resource management model

Also, the relationships of resources can be defined, and it is possible to reference related information based on the relationship information in the event of a failure.

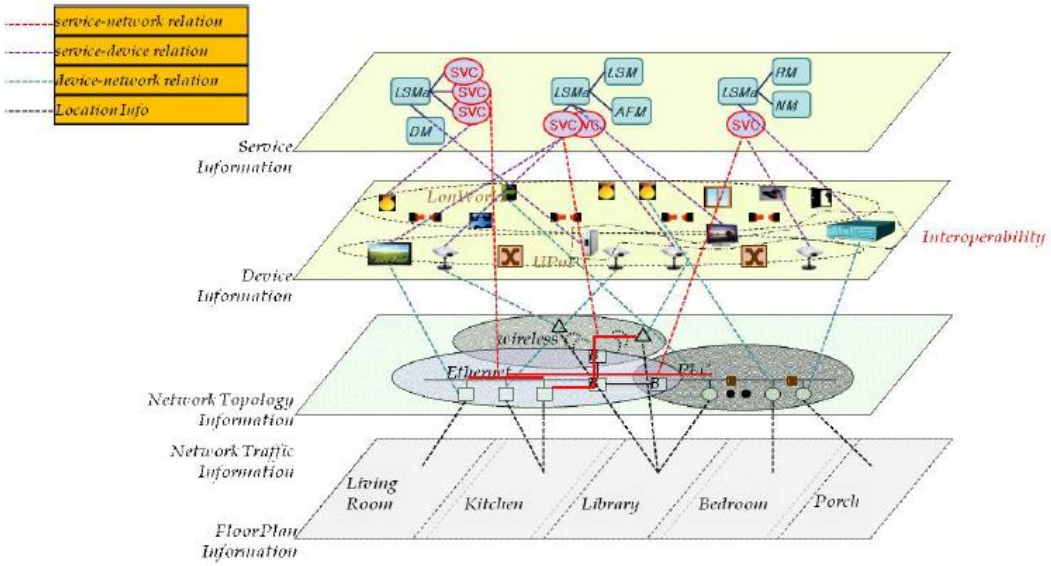

Figure 4-3 Logical concept of the HN resource management architecture

ISO/IEC30100 references Building Information Model (ISO/PAS 16739) as an example of location information, KNX (ISO/IEC 14543-3 Series) as an example of terminal information, SNMP (RFC 1098) as an example of network information, and OSGi (OSGi Alliance) as an example of service information.

4.3 Related standards

4.3.1 IEC 62608

IEC 62608 is a standard being developed by the TC 100 Committee and provides a reference model used to configure the settings of terminals that are connected to a HN. The standard consists of Parts 1 to 3, with Part 1 approved so far.

IEC 62608 adopts the model shown in Figure 4-4. The configurator configures the settings necessary for a HN-connected terminal to operate. The configured agent residing in the terminal transmits the items to be configured to the configurator, and the configurator returns the necessary setup information.

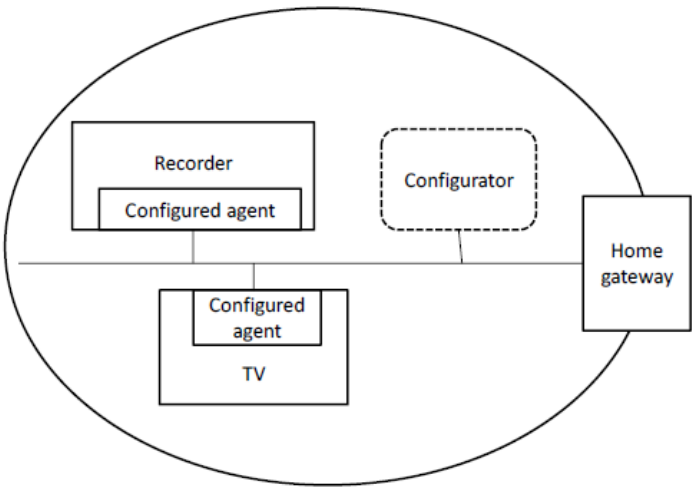

Figure 4-4 Configurator system model

The use of G.9980 (TR-069) is currently considered as a method of managing the information that the configurator returns to the agent via the Internet.

4.3.2 G.9980 (BBF TR-069)

G.9980 references BBF TR-069. BBF TR-069 is a protocol (CPE WAN Management Protocol) for managing HN-connected terminals (CPE: Customer Premises Equipment) over the Internet. Figure 4-5 shows the architecture of BBF TR-069. Terminals are connected to the WAN via a gateway (Managed Internet Gateway Device) and then to the configuration server residing on the WAN (ACS: Auto-Configuration Server). The ACS has the setup information for the terminals to be connected to the HN. When a terminal is connected, its setup information is notified and necessary firmware can be downloaded. In the figure, call centers and other facilities are connected on the left side of the ACS (Northbound interface), and this interface is used to reference setup information in such cases as when a query from the end user is received.

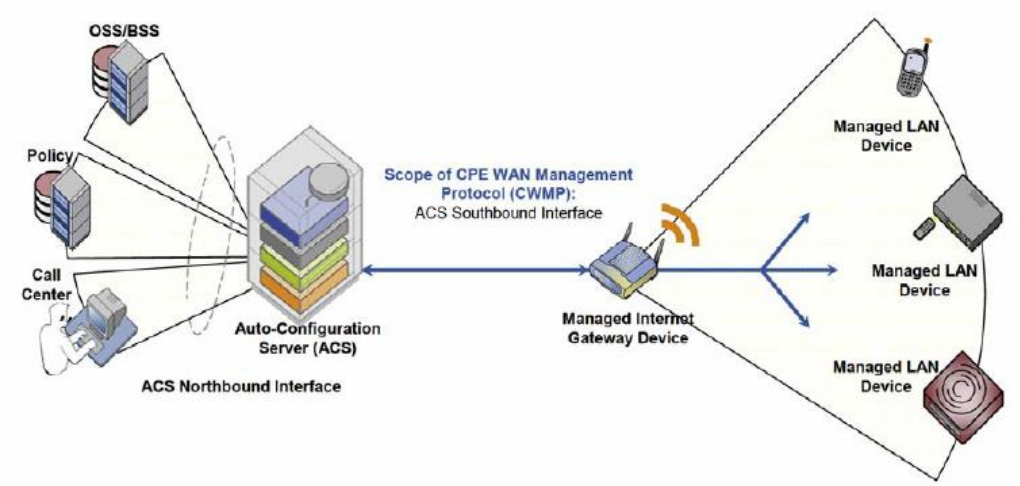

Figure 4-5 Architecture of BBF TR-069

4.3.3 UPnP DM

UPnP is a standard developed by the UPnP Forum and defines a basic framework whereby a terminal is automatically configured and made available when it is connected to the network. UPnP DM is a standard for implementing device management by using UPnP. Figure 4-6 shows the device management framework of UPnP.

The UPnP manageable device is a terminal that is connected by using LAN IP. The configurable information is defined as a device data model. The UPnP control point (CP) configures the UPnP manageable device by using the UPnP protocol. The setup information held by the UPnP CP can be managed in the cloud via the WAN.

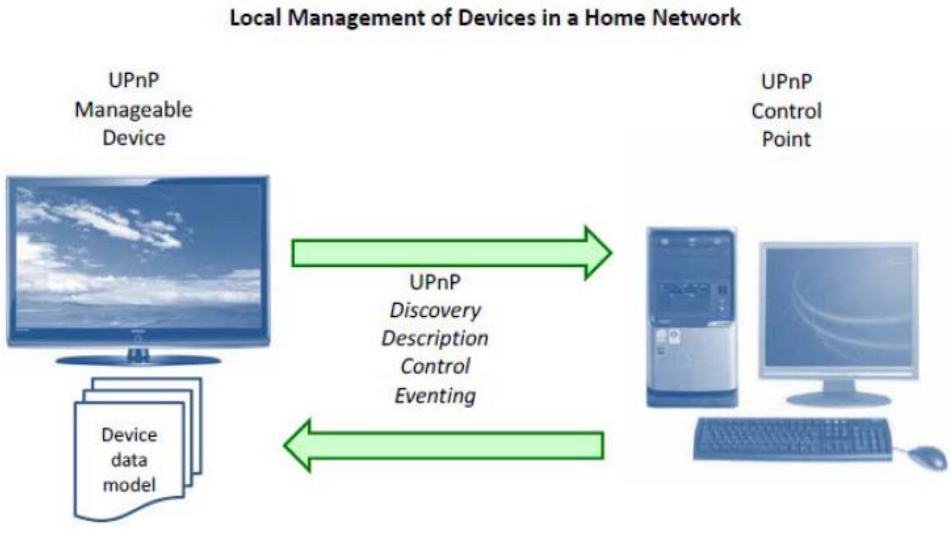

Figure 4-6 Device management using UPnP

4.3.4 OSGi RMP

The OSGi (Open Service Gateway initiative) framework is a system that consists of modules. It is a service platform that allows Java-programmed components to be introduced dynamically. Components are called bundles, and they can be installed, started, stopped, updated, and uninstalled without restarting the system. A remote management protocol to control bundles is defined, and this protocol is used to manage HN terminals.

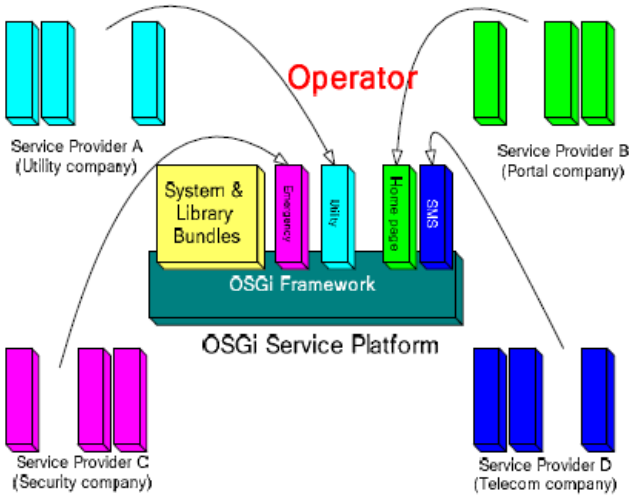

Figure 4-7 OSGi remote management protocol

4.3.5 OMA DM

The OMA (Open Mobile Alliance) develops open specifications for mobile operators. These specifications are aimed at providing service enablers that are common to all countries, operators, and terminals. OMA DM is a device management protocol for managing portable terminals including mobile phones, smartphones, and PDAs.

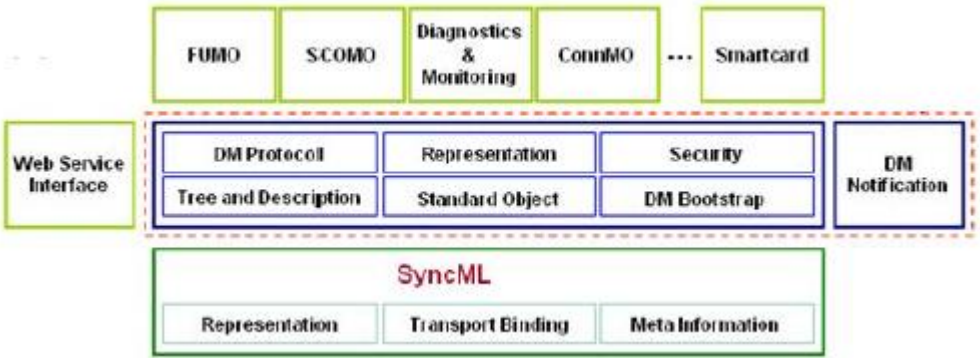

Figure 4-8 OMA DM protocol stacks

4.3.6 SNMP

The SNMP (Simple Network Management Protocol) is the Internet standard protocol for managing terminals on an IP network. Terminals supported by the SNMP include routers, switches, servers, and printers. It is a management system intended to monitor terminals that can be connected to the network, and its purpose is to inform the network administrator about the network status. The SNMP consists of the standard network management functions, and the application-layer protocol, database, and data objects are defined.

Chapter 5 Business Models and Architectures

5.1 Business models

This section describes the assumed business models that use a service platform capable of dealing with HNs and customer support. Three business models can be assumed: intermediary provider model, cloud service provider model, and service sellout model. These three business models are described below.

(1) Intermediary provider model

In this business model, the intermediary provider that provides the service platform manages all information and offers APIs to the service provider and support provider so that necessary information can be exchanged. (Figure 5-1)

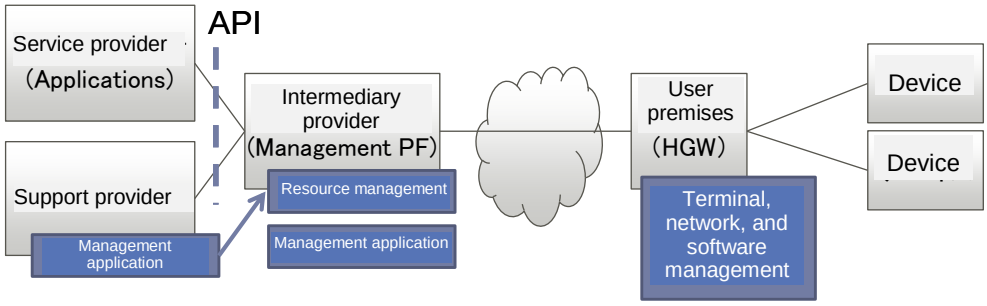

Figure 5-1 Intermediary provider model

Terminal, network, and software management in Figure 5-1 provides functions to collect and control information about individual terminals on the user premises. Resource management combines the information collection and control functions given on the user premises, provides database and other information management functions as well, and offers them as APIs. The management application implements functions for the customer support service (e.g., failure cause identification and failure recovery action execution) by using the functions that resource management offers as APIs. The roles of terminal, network, and software management, resource management, and the management application are the same in the cloud service provider model and service sellout model to be described later.

(2) Cloud service provider model

In this business model, the service provider takes the initiative in organizing the business and outsources the maintenance of terminals to the support provider. (Figure 5-2)

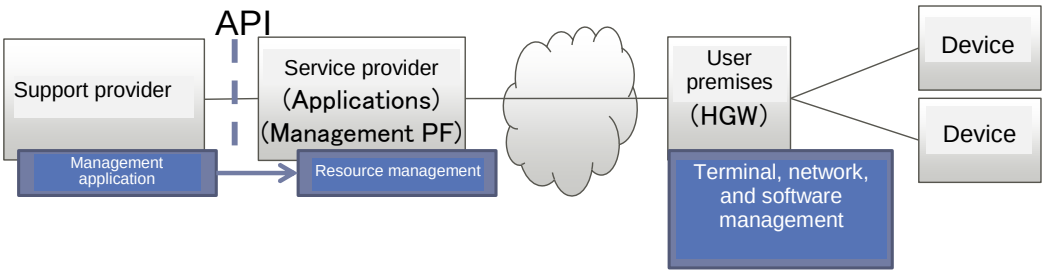

Figure 5-2 Cloud service provider model

(3) Service sellout model

The support provider directly connects to the user premises without involvement of the intermediary provider or service provider and places almost all the functions, including resource management, on the user premises. In this business model, it is possible to place the simple management application on the user premises as well and have the support provider take care of only those problems that the user cannot solve by himself or herself. (Figure 5-3)

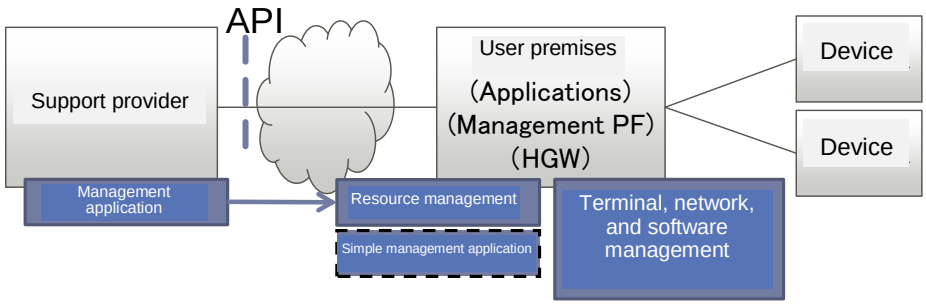

Figure 5-3 Service sellout model

5.2 Case study

This section describes the operations of the customer support functions that have been discussed thus far based on the use cases. Here, the procedure is explained for recovering from a failure that occurs after an end user or agent registers for a HN service, installs terminals, and starts the use of the HN service. Note that the descriptions given below assume the intermediary provider model described in (1) of Section 5.1.

The service described below is a residential power consumption visualization service using a power sensor. The system configuration is shown in Figure 5-4. The terminal that displays power consumption in a graph is a smartphone, which shows the graph using its browser. The smartphone is connected via the mobile phone network or the WiFi AP on the premises. The power sensor is an ECHONET Lite device and can acquire the information defined by the ECHONET Lite protocol.

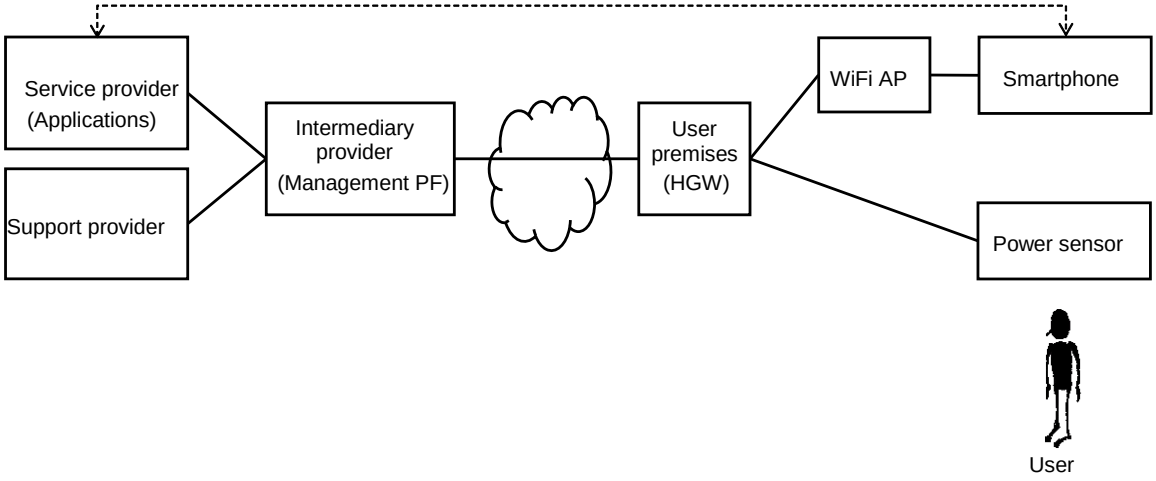

Figure 5-4 System configuration for the visualization service

The following descriptions are based on this system configuration. It is assumed that the installation and setup of the network devices are already complete and that the procedure starts with the step of installing the devices necessary for the HN service.

(1) Service and device registration

For the end user to use the visualization service, he or she needs to register the service and necessary terminals. Figure 5-5 shows the flow of this process.

Since the visualization application is provided as a Web application, the service is registered via the Web browser of the smartphone. When the service is registered, the information about the user premises (user ID, power sensor information, etc.) is registered with the application. The application registers the service information with resource management. When the power sensor is connected to the HN on the end user premises, the HGW discovers the terminal and device management in the HGW transmits the terminal information to resource management in the management PF. The received information is compared to the user ID and terminal information registered in advance by the application and, if they match, the terminal is officially registered.

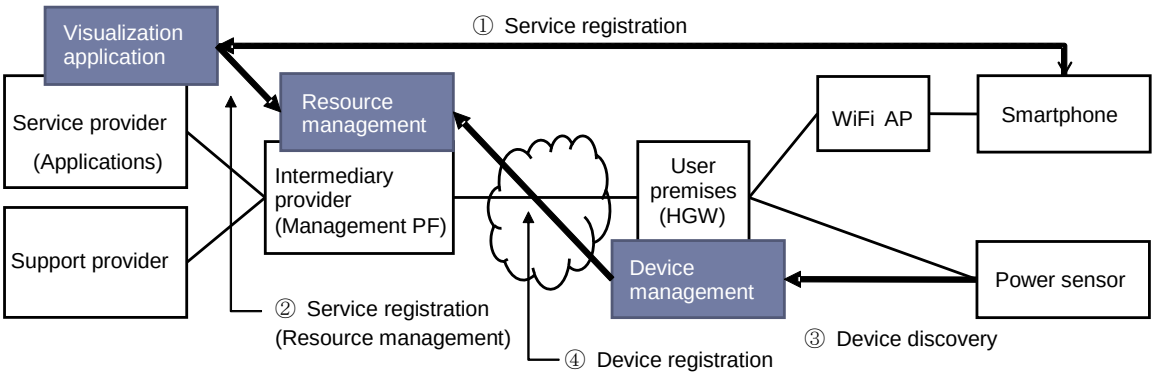

Figure 5-5 Service and device registration

(2) Automatic device setup

Once the terminal is registered, the necessary setup information is transmitted to the power sensor via the HGW and the sensor is automatically set up (Figure 5-6). When the setup of the power sensor is complete, resource management is notified of the setup completion via the HGW, although it is not shown in Figure 5-6. Upon receiving this notification, resource management notifies the visualization application that the device registration is complete. With this notification, the power consumption visualization service becomes available on the user premises.

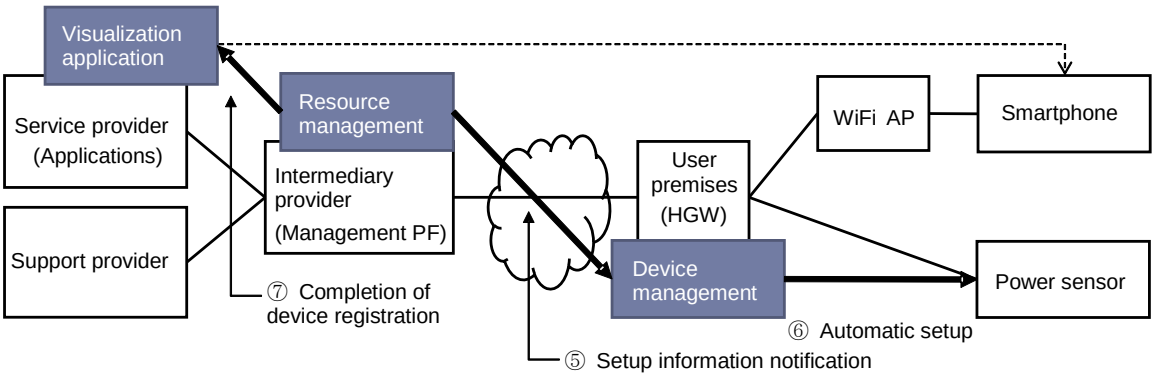

Figure 5-6 Automatic device setup

(3) Start of use of the service

Figure 5-7 shows the flow of data applicable when the service is running normally. To use the service, the end user accesses the visualization application from the Web browser of the smartphone. The application transmits periodically collected data of the power sensor (power consumption) to the smartphone or creates a visualization

window and displays the window in the browser. In the meantime, the HGW periodically acquires data from the power sensor using the ECHONET Lite protocol or has the data transmitted to it periodically. The HGW transmits the collected data to the management PF. Receiving data from the management PF, the application accumulates the necessary data. The accumulated data is provided in response to a request from the smartphone.

Note that, even while the service is running normally, the HGW and management PF periodically collect the HN resource information of the user premises by using the functions described in Chapter 3.

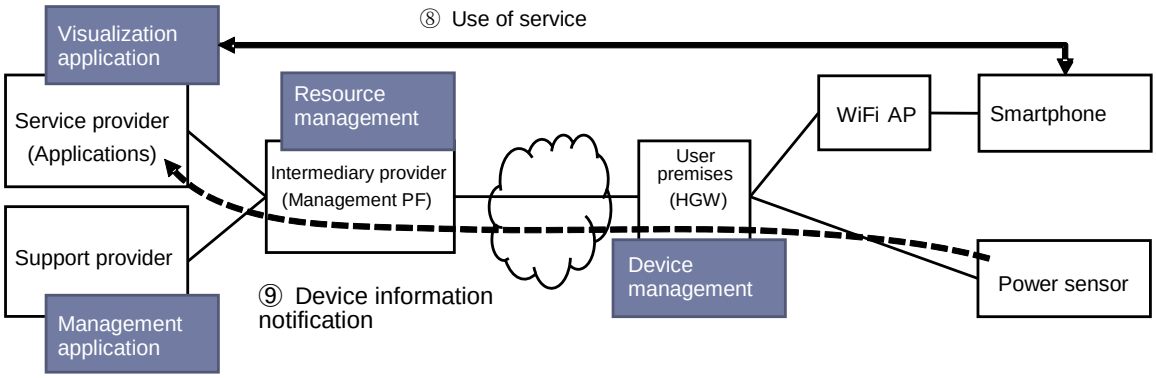

Figure 5-7 Start of use of the service

(4) Failure notification from the end user

Figure 5-8 shows the case in which a failure occurs on the end user premises and the call center is notified of it by telephone, email, or other means. When the user notifies the call center, its maintenance personnel references the resource information of the user premises, accumulated in the management PF, via the management application. In this case, the status of the device used for the visualization application (power sensor) is referenced. When the latest device information has been acquired, the management PF displays that information. Otherwise, the management PF queries device management in the HGW to acquire the information.

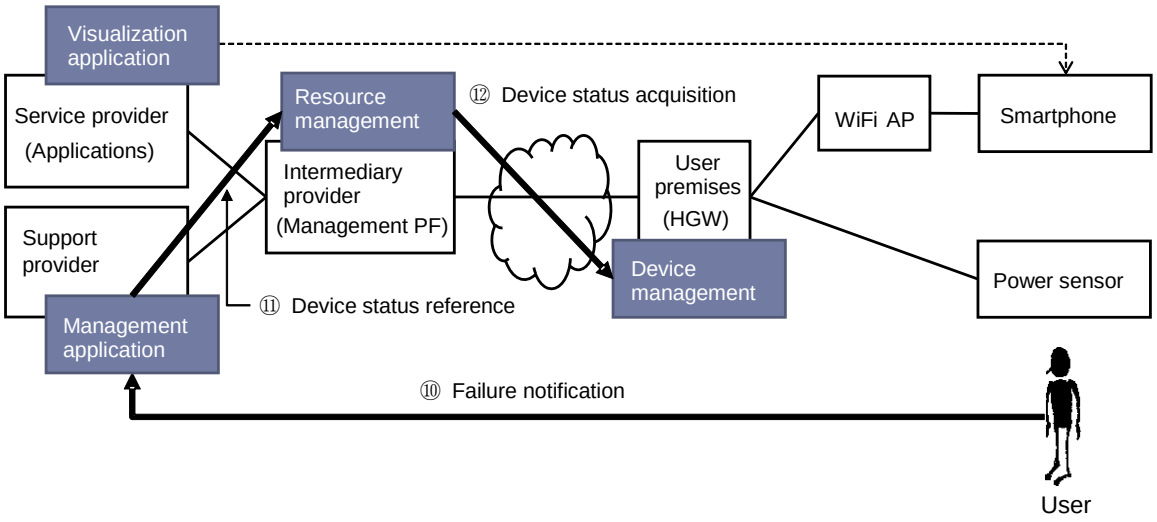

Figure 5-8 Failure notification from the end user

(6) Recovery from the failure

Figure 5-9 shows that the maintenance personnel analyzes the cause of the failure based on the acquired device information. Here, it is assumed that the setup information of the terminal is invalid. In this case, the call center notifies the user that the setup information of the terminal needs to be changed to recover from the failure and, after the user's consent is obtained, the support provider takes the following step. First, the support provider accesses resource

management via the management application and changes the device information set for the user premises. When resource management in the management PF notifies device management in the HGW on the user premises about the setup information of the terminal, the setup information of the device (power sensor) is automatically set based on the setup information registered in device management and the failure is solved.

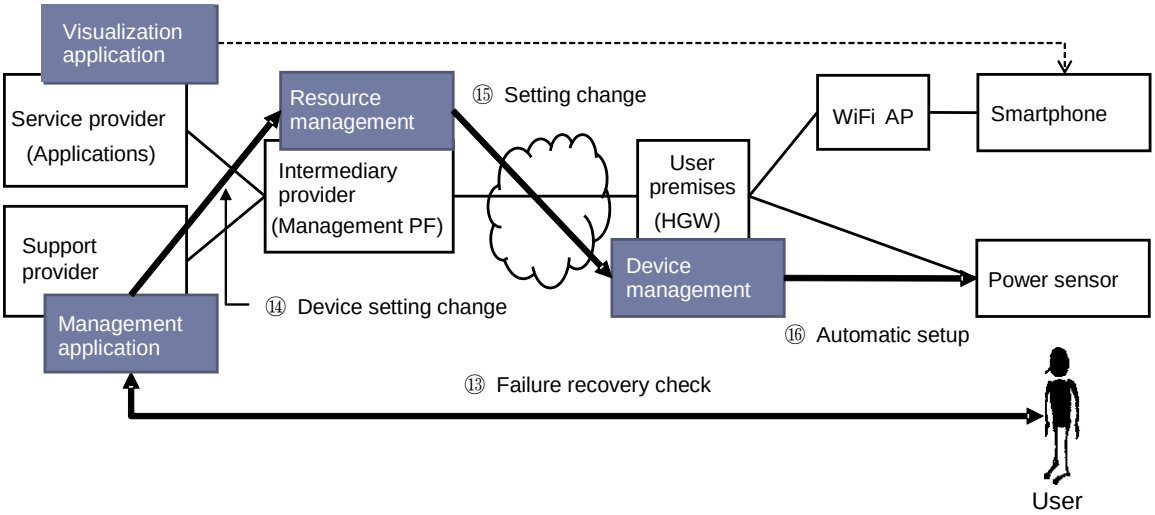

Figure 5-9 Recovery from the failure

Chapter 6 Conclusion

This technical report has discussed customer support functions, which are anticipated to become a major issue as HN services come into widespread use. With an increasing number of terminals expected to be connected to the HN and a diverse mix of communication systems and protocols present, it is considered likely that the HN configuration will become complex. In order to realize effective customer support in this situation, it is necessary to grasp the conditions of HN terminals and the network individually, clearly define an architecture that integrates with the HGW and management PF in the upstream network, and implement the functions required respectively as described herein. This architecture will also need a mechanism whereby customer support functions obtain an accurate grasp of a failure occurring on the user premises and execute a failure recovery process for the user by changing the settings, transmitting test traffic, and so on as necessary. Also, since an administrator with expert knowledge is not present at the home where the HN is built, it is likely that the user may not be able to receive sufficient help from customer support functions because of his or her inability to explain the situation of the failure well enough. The challenges to be addressed from now on are to conduct case study research to demonstrate the effectiveness of individual customer support functions, assuming general users with poor IT literacy, based on the functions to be featured by terminals that are defined herein, and to explore ways to make the effectiveness of such functions better known to multiple terminal providers and encourage them to implement those functions.

Reference Documents

[ATM OAM] ITU-T Recommendation I.610 (1999), B-ISDN operation and maintenance principles and functions

[ISO/IEC 30100] ISO/IEC 30100-1 (2013), Information technology – Home network resource management – Part 1: Requirements

[IEC 62608] IEC 62608-1 (2013), Multimedia home network configuration – Basic reference model – Part 1: System model

[ITU-T G.9980] ITU-T Recommendation G.9980 (2012), Remote management of customer premises equipment over broadband networks – customer premises equipment WAN management protocol

[BBF TR-069] BBF TR-069 (2011), CPE WAN Management Protocol

[BBF TR-181] BBF TR-181 (2012), Device Data Model for TR-069

[DLNA] IEC 62481-1 (2006), DLNA Home networked device interoperability guidelines Part 1: Architecture and Protocols

[DHCP] IETF RFC2131 (1997), Dynamic Host Configuration Protocol

[DHCPv6] IETF RFC3315 (2003), Dynamic Host Configuration Protocol for IPv6

[Ethernet OAM] ITU-T Recommendation Y.1731 (2013), OAM functions and mechanisms for Ethernet based networks

[ICMP] IETF RFC792 (1981), Internet Control Message Protocol, IETF RFC4443 (2006), Internet Control Message Protocol for the Internet Protocol Version 6 (IPv6) Specification

[LLDP] IEEE 802.1ab (2005), Station and Media Access Control Connectivity Discovery

[MIB] IETF RFC1213 (1991), Management Information Base for Network Management of TCP/IP-based internets: MIB-II

[PPPoA] IETF RFC2364 (1998), PPP Over AAL5

[PPPoE] IETF RFC2516 (1999), A Method for Transmitting PPP Over Ethernet

[SNMP] IETF RFC1157 (1990), A Simple Network Management Protocol

[RA] IETF RFC4861 (2007), Neighbor Discovery for IP version 6

[Telnet] IETF RFC854 (1983), Telnet Protocol Specification

[TTC HTIP] TTC JJ-300.00 v1.1 (2011), Home-network Topology Identifying Protocol (HTIP)

[TTC TR-1046] TTC TR-1046 (2013), Service platform for home network service

[TTC TR-H.QoS(Sup11)] TTC TR-H.QoS(Sup11) (2009), H-Series Supplement 11

[KNX] ISO/IEC 14543-3-x (2006), OSI-based network communication protocol for intelligent buildings

[ZigBee SEP2.0] ZigBee Alliance, Smart Energy Profile 2.0 Application Protocol.

[ECHONET Lite] ECHONET Consortium, ECHONET Lite Specification Version 1.01.

[UPnP] ISO/IEC 29341-x (2011), Information technology – UPnP Device Architecture

[UPnP DM] UPnP DM (2012), UPnP Device Management: 2