TTC技術レポート
Technical Report

TR-1057
Customer support guideline for home network service

Edition 1.1

Established on February 23, 2016

THE 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 18, 2015	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

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 that devices and networks need to have to enable failure cause analysis and recovery for various types of failures that may occur when devices connected to a home network (HN) are used.　The customer support functions in general that are necessary during the execution of a HN service have been reported in TTC TR-1053 ("Customer support functions for home network service platform").　This report mainly deals with cases where devices are connected using near field communication and provides a guideline for the functions that end devices and network devices need to feature to discover the information about failures associated with near field communication and allow the platform to collect and manage such information in those cases.

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.　Particularly, when devices are connected using wireless communication, the situation keeps changing constantly and it is possible that a currently connected device may lose the connection or have a slower response one moment later.

TTC TR-1053 describes the cases of failures that devices and networks may experience in relation to a HN to which a variety of devices are connected and discusses how to analyze the causes of failures based on those failure cases as well as how to detect failures and recover from them.　To spread HN services, it is necessary for service providers, platform providers, and device providers to adopt the same standard and provide the customer support functions set forth in TR-1053.　TR-1053 classifies the customer support functions to be implemented by layer (Table 1-1). Regarding these functions required for the individual layers, there are already standards (Wi-Fi, HTIP, etc.) for many of the functions related to end devices and network devices.　When end devices and network devices support these standards, it is possible to realize the stable operation of HN services that are implemented with a combination of end devices and network devices from multiple different manufacturers.　This holds true, however, only when the most part of the network is based on wired communication.　Parts of the basic measurement function for the network layer are not supported in near field communication described in TTC TR-1043.　This report describes these unsupported parts.

Table 1-1 Functions required for each individual layer (Table 3-1 in TR-1053)

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.
	End devices and network devices[1]	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

1.2 Scope

Figure 1-1 shows the scope of this guideline. The overall architecture is as defined in ITU-T Y.2070. In this architecture, the management PF and HGW are common functions. The management PF provides an application interface and manages the information about the individual devices connected to the HGW. The HGW has an interface function and protocol conversion function to deal with diverse types of devices.

On the right side of the HGW is the HN. This figure shows only those network devices related to near field communication and omits wired devices such as hubs and routers. Note that, since this technical report considers that devices can be connected using multi-hop communication, it refers to a device connected at the end as an end device and a device connected in between as a relay node.

An end device may be connected in three ways: (1) wired connection (wired LAN or cable), (2) single-hop communication (e.g., infrastructure mode communication), and (3) multi-hop communication. Note that multi-hop communication is limited to two hops. This is because supporting more than two hops makes it necessary for each

[1] TTC TR-1053 collectively refers to end devices and network devices as terminals. In this technical report, the term "terminals" is not used and they are referred to as end devices and network devices.

node to collect more complex items and requires a complex analysis method. It has been decided, therefore, to consider this matter in the next and later editions.

The near field communication methods covered by this technical report and the assumed protocols are as follows:
Near field communication: Wi-Fi (IEEE 802.11), ZigBee/Wi-SUN (IEEE 802.15.4), Bluetooth (IEEE 802.15.1)
Protocols: HTIP (JJ-300.00/G.9973), LLDP, UPnP, SNMP, ECHONET Lite

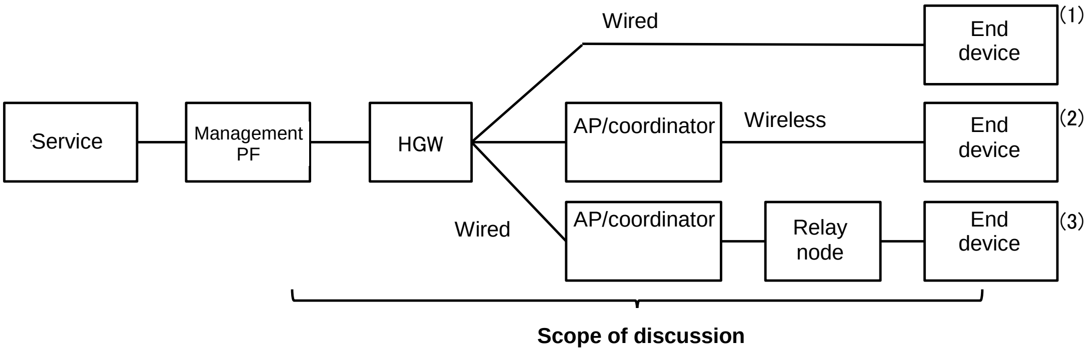


Figure 1-1 Scope of this guideline

The functions described in this guideline are intended to collect the information primarily needed to identify failure causes from individual end devices and network devices. All the HN information is temporarily accumulated in the HGW and then managed in the management PF. The services are intended to display the failure information of end devices that is provided to call centers and support centers and acquire the information about the status of the relevant end device or network from a remote location.

1.3 Relationship with TR-1043

TTC TR-1043 defines the network model of a HN (Figure 1-2). This model corresponds to the model of the JSCA Smart House/Building Standardization and Business Promotion Study Group, and this guideline also complies with this network model. Note that the WAN router corresponds to the access gate way function[2] of the HGW in Figure 1-1. This technical report describes it as the HGW because it includes the service gate function[3].

The method of acquiring the information necessary for failure cause analysis is discussed based on the HTIP. This means that the network topology information in the link layer broadcast domain is acquired. Regarding the network model defined in TTC TR-1043 (Figure 1-2), only A and A' points are applicable and B/B' and C points are not.

[2] The access gateway is the function that relays IP packets between the WAN and HN.

[3] The service gateway is the function that relays application communication between the WAN and HN.

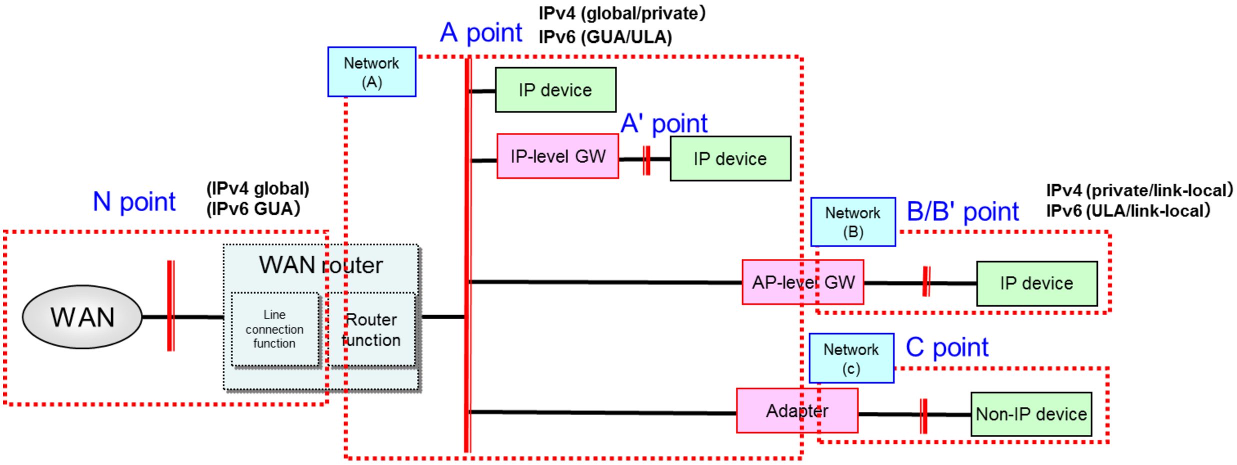


Figure 1-2 Network model (TTC TR-1043)

Chapter 2　Use Case

In this chapter, a HN using wireless LAN is discussed as a use case with regard to the failure detection method to be considered for customer support.

2.1　Challenges for remote HN maintenance

The near field communication technology allows devices to be deployed easily without the need for cabling and is expected to be used actively to spread and advance HN services. When compared with the wired communication method, on the other hand, the situation of a failure is often difficult to grasp in the case of near field communication because it cannot be visually checked which is connected to which. Also, it is widely known that degradation in communication quality is caused by the interference of radio waves from multiple signal sources, and finding out what affects which device requires an identification of problems through investigation by experts using measuring equipment and other tools. This report deals with the near field communication technology, which is not covered by TR-1053, and discusses ways to implement customer support functions in the devices comprising a HN without expert assistance and the functions necessary to enable the situation of a failure to be grasped from a remote location and ensure smooth maintenance.

2.2　Near field communication failures and causes (analysis of failure cases of wireless LAN devices)

Wireless LAN is easy to deploy, as mentioned earlier, and the number of its users is growing. Today, the use of wireless LAN is not limited to just browsing the Internet; there is a gradually increasing number of households that connect the wireless LAN to DLNA- and ECHONET Lite-compatible devices to enjoy home entertainment and other HN services. In addition, the explosive proliferation of smartphones in recent years has resulted in a growing number of people using wireless LAN to operate home appliances via a smartphone or display images and videos captured with a smartphone on the TV screen. As wireless LAN is used in increasingly diverse ways, there have been an increase in reports of wireless LAN-related failures as well. Table 2-1 on the next page summarizes the wireless LAN-related failures that have been collected.

Table 2-1 Failure cases

Phenomenon	Details	Category
The end device cannot be connected or transmission speed drops depending on the time zone.	The AP is unable to find the timing to transmit signals to the end device because it uses the same channel as a neighboring AP or an adjacent channel.	1
	Although the AP in one's own house is in a standby state, the end device in that house outside the coverage area of the AP in the neighboring house repeatedly transmits signals to the AP in one's own house because the AP in the neighboring house that uses the same or adjacent channel is engaged in communication (exposed node problem).	2
	Since a particular end device occupies the channel, the AP cannot transmit signals to the end device in question.[4]	3
	Since a particular end device occupies the channel, any other end device cannot transmit signals.[4]	4
	Since there are many end devices in the AP coverage area, the AP cannot transmit signals to all the devices (such cases as when the AP needs to control 1000 devices every minute).	5
	When an end device of the neighboring house in the AP coverage area of one's own house uses the same channel and is engaged in communication, the end device in one's own house that cannot be reached by radio waves from the end device of the neighboring house repeatedly transmits signals although the AP in one's own house is in a standby state (hidden node problem).	6
	The propagation of radio waves is affected by a new obstacle put between the AP and the end device, a newly installed door, or a change in the door material.	7
	The device or AP cannot receive signals due to multipath propagation.	8
	Interference of an unintended signal source (foreign-made product not certified for technical standard compliance, indoor wiring, particularly the lead-in wire of a satellite dish, etc.)[5]	9
The device becomes unable to connect to a specific device (from a certain point of time).	The device is gone (disposal device, or the device no longer exists as it has been replaced with another device).	10
	A specific device becomes unable to communicate because of the battery running out or a failure.	11
	The AP has been relocated to a place where the communication environment becomes poor for a specific device, thus making that device unable to communicate (there are many obstacles or the distance from the device is long).	12

[4] Many of the commercially available APs are backward-compatible with wireless LAN standards and can be used in an environment where devices compliant with different standards coexist. However, when devices from different manufacturers are used in such an environment, the connection control implemented by the AP (CSMA-CA), which may differ from manufacturer to manufacturer, may not necessarily be able to establish connections evenly for all end devices, thereby causing this phenomenon.

[5] Examples of an unintended signal source
・Interference caused by the use of a foreign-made product that allocates frequencies differently from Japanese products (e.g., baby monitor and transceiver)
・The distortion of the adjacent channel of a device outside or inside the system may get mixed with the channel in question.
・Poor cabling work resulting in interfering waves being generated (e.g., inappropriate treatment of the lead-in wire of a satellite dish)
・Communication is disabled by interfering signals in the communication channel generated by unwanted emissions from a device outside or inside the system (e.g., microwave oven, illegal radio station, and solar power generation inverter noise).

	The end device has been relocated to a place where the communication environment is poor and thus become unable to communicate with the AP.	13
	Interference of an unintended signal source (foreign-made product not certified for technical standard compliance, indoor wiring, radio waves leaked from the lead-in wire of a satellite dish, etc.)[5]	9
	The device has connected to an unauthorized AP by mistake and cannot communicate with the AP.	14
The device becomes unable to connect to any other device (from a certain point of time).	The device has become unable to communicate because the AP has failed.	15
	Since the device has been restarted because it cannot connect to the AP, its configuration information has been changed.	16
	Interference of an unintended signal source (foreign-made product not certified for technical standard compliance, indoor wiring, particularly the lead-in wire of a satellite dish, etc.)[5]	9

Based on these failure cases, an attempt has been made to categorize the causes of failures in order to help establish a failure isolation procedure and standardize corrective actions with regard to the customer support functions that are needed when any of the failures listed above is reported from a user.

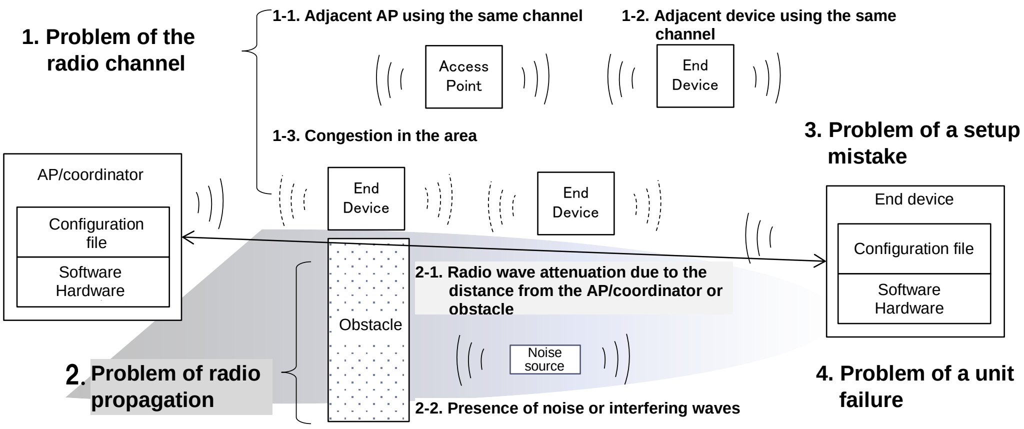

1. Problem of the radio channel
1-1. Adjacent AP using the same channel
1-2. Adjacent device using the same channel
Access Point
End Device
1-3. Congestion in the area
3. Problem of a setup mistake
AP/coordinator
Configuration file
Software
Hardware
End Device
End Device
End device
Configuration file
Software
Hardware
Obstacle
2-1. Radio wave attenuation due to the distance from the AP/coordinator or obstacle
Noise source
2. Problem of radio propagation
2-2. Presence of noise or interfering waves
4. Problem of a unit failure

Figure 2-1 Topology of near field communication and categorization of failures

Figure 2-1 shows four categories of failure causes as elements that may affect the communication or connection in the transmission section between the AP and end device: the problem of a unit failure of the AP and end device that establish communication; the problem of a setup mistake; the problem of the radio channel used; and the problem of radio propagation that mainly affects the propagation of signals.

Table 2-2 Categories of failure causes

No.	Cause category	Outline
1	Radio channel	Problem associated with the radio channel used, such as channel contention with devices outside the coverage area, contention of connection requests between devices, or congestion resulting from many end devices waiting to transmit signals
2	Radio propagation	Problem associated with radio propagation, such as the effect on the carrier waves transmitted and received by the AP and end device, radio wave interference, attenuation, or the effect of multipath propagation caused by reflection
3	Setup mistake	Problem associated with a setup mistake, such as an initial setup mistake for the AP or end device or inadvertent resetting of a device to its factory-set defaults
4	Unit fault	Problem associated with a fault of an individual device, such as a hardware fault, power fault, or battery runout of the AP or end device

As in TR-1053, individual failures will be fit into these cause categories, assuming the architecture defined in ITU-T Y.2070, and the customer support functions necessary for a HN will be discussed.　As the premise, Figures 2-2, 2-3, and 2-4 break down the failure cases mentioned in Table 2-1.

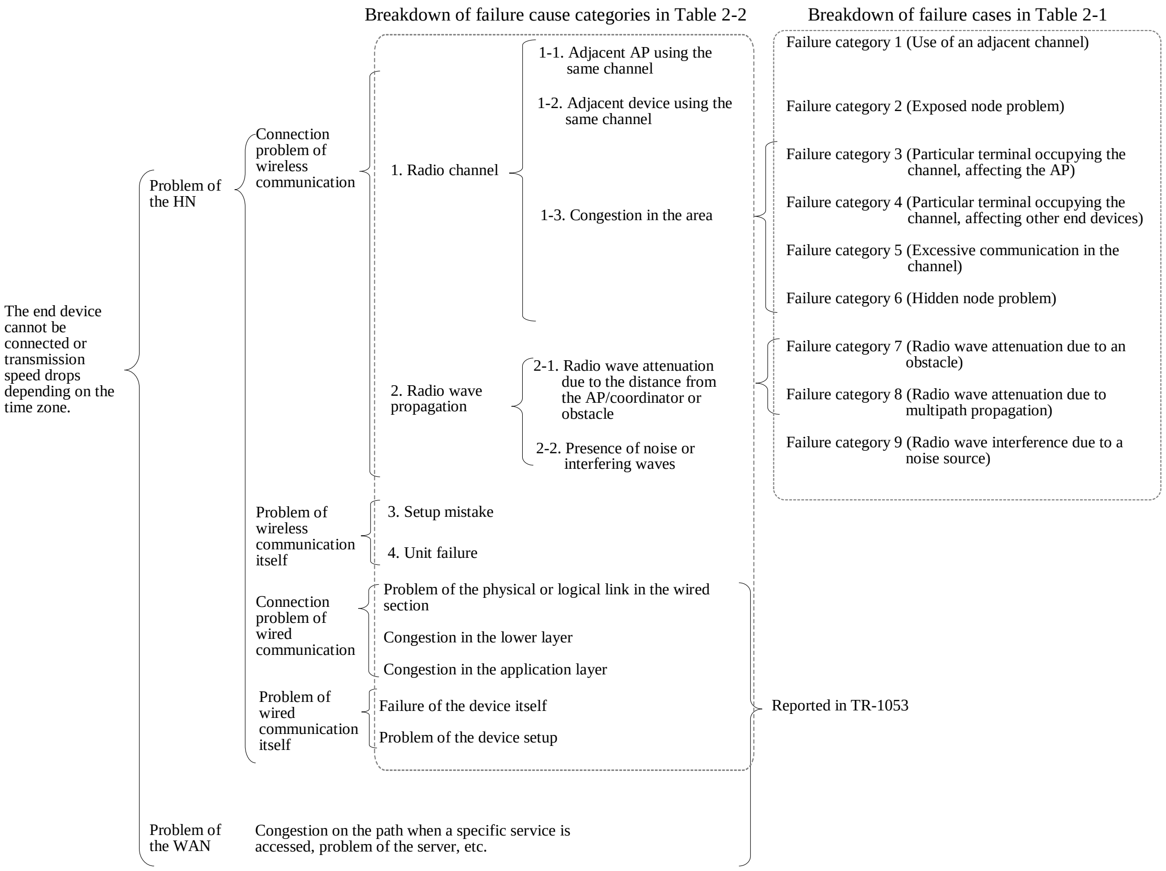

Breakdown of failure cause categories in Table 2-2
Breakdown of failure cases in Table 2-1
The end device cannot be connected or transmission speed drops depending on the time zone.
Problem of the HN
Connection problem of wireless communication
1. Radio channel
1-1. Adjacent AP using the same channel
1-2. Adjacent device using the same channel
1-3. Congestion in the area
2. Radio wave propagation
2-1. Radio wave attenuation due to the distance from the AP/coordinator or obstacle
2-2. Presence of noise or interfering waves
Problem of wireless communication itself
3. Setup mistake
4. Unit failure
Connection problem of wired communication
Problem of the physical or logical link in the wired section
Congestion in the lower layer
Congestion in the application layer
Problem of wired communication itself
Failure of the device itself
Problem of the device setup
Problem of the WAN
Congestion on the path when a specific service is accessed, problem of the server, etc.
Reported in TR-1053
Failure category 1 (Use of an adjacent channel)
Failure category 2 (Exposed node problem)
Failure category 3 (Particular terminal occupying the channel, affecting the AP)
Failure category 4 (Particular terminal occupying the channel, affecting other end devices)
Failure category 5 (Excessive communication in the channel)
Failure category 6 (Hidden node problem)
Failure category 7 (Radio wave attenuation due to an obstacle)
Failure category 8 (Radio wave attenuation due to multipath propagation)
Failure category 9 (Radio wave interference due to a noise source)

Figure 2-2 Breakdown of failure cases associated with the phenomenon: "The end device cannot be connected or transmission speed drops depending on the time zone"

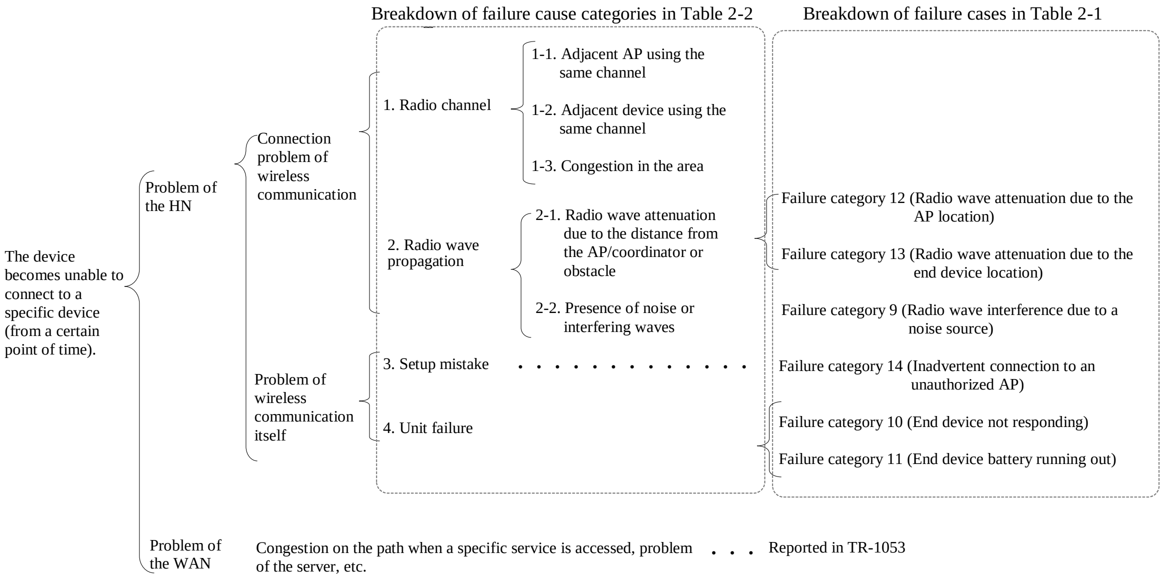

Breakdown of failure cause categories in Table 2-2
Breakdown of failure cases in Table 2-1
The device becomes unable to connect to a specific device (from a certain point of time).
Problem of the HN
Connection problem of wireless communication
1. Radio channel
1-1. Adjacent AP using the same channel
1-2. Adjacent device using the same channel
1-3. Congestion in the area
2. Radio wave propagation
2-1. Radio wave attenuation due to the distance from the AP/coordinator or obstacle
2-2. Presence of noise or interfering waves
Problem of wireless communication itself
3. Setup mistake
4. Unit failure
Failure category 12 (Radio wave attenuation due to the AP location)
Failure category 13 (Radio wave attenuation due to the end device location)
Failure category 9 (Radio wave interference due to a noise source)
Failure category 14 (Inadvertent connection to an unauthorized AP)
Failure category 10 (End device not responding)
Failure category 11 (End device battery running out)
Problem of the WAN
Congestion on the path when a specific service is accessed, problem of the server, etc.
Reported in TR-1053

Figure 2-3 Breakdown of failure cases associated with the phenomenon: "The device becomes unable to connect to a specific device (from a certain point of time)"

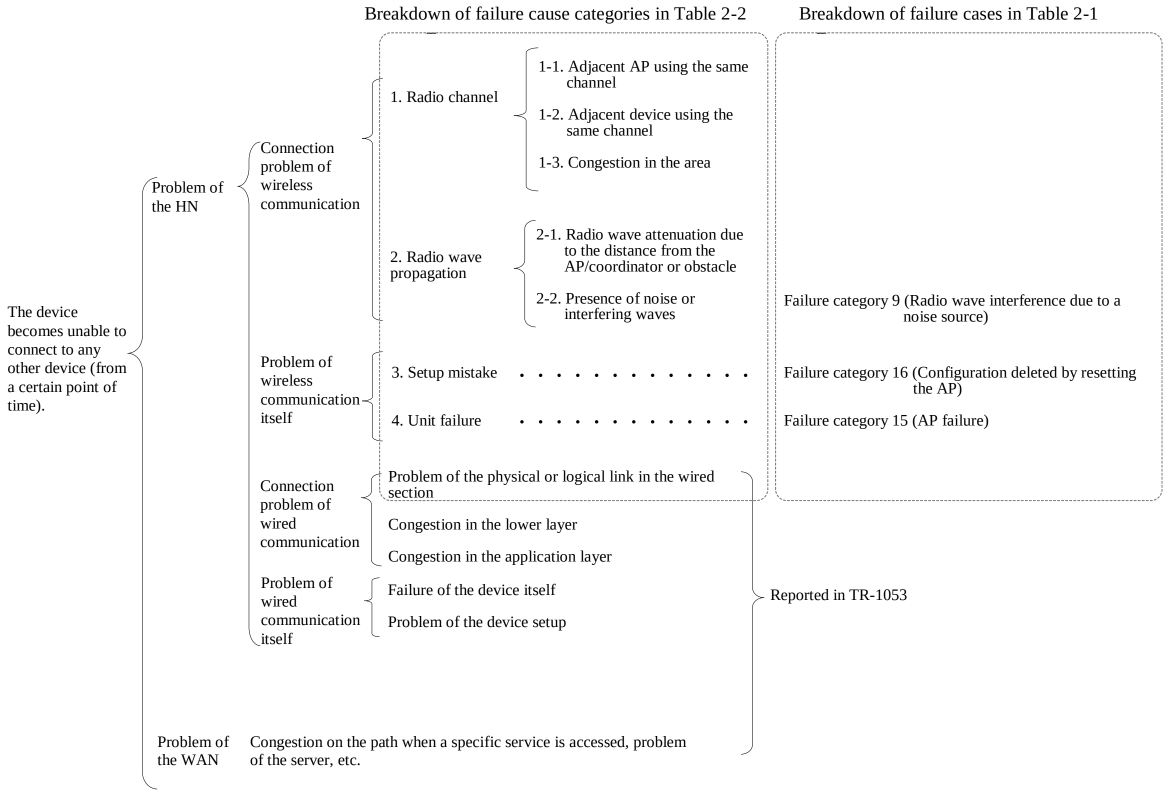

Breakdown of failure cause categories in Table 2-2
Breakdown of failure cases in Table 2-1
The device becomes unable to connect to any other device (from a certain point of time).
Problem of the HN
Connection problem of wireless communication
1. Radio channel
1-1. Adjacent AP using the same channel
1-2. Adjacent device using the same channel
1-3. Congestion in the area
2. Radio wave propagation
2-1. Radio wave attenuation due to the distance from the AP/coordinator or obstacle
2-2. Presence of noise or interfering waves
Failure category 9 (Radio wave interference due to a noise source)
Problem of wireless communication itself
3. Setup mistake
Failure category 16 (Configuration deleted by resetting the AP)
4. Unit failure
Failure category 15 (AP failure)
Connection problem of wired communication
Problem of the physical or logical link in the wired section
Congestion in the lower layer
Congestion in the application layer
Problem of wired communication itself
Failure of the device itself
Problem of the device setup
Reported in TR-1053
Problem of the WAN
Congestion on the path when a specific service is accessed, problem of the server, etc.

Figure 2-4 Breakdown of failure cases associated with the phenomenon: "The device becomes unable to connect to any other device (from a certain point of time)"

Chapter 3　Technical Requirements

This chapter describes the technical requirements for detecting failures in a HN, centering on those cases where end devices in the HN are connected using various wireless technologies. Chapter 2 categorized failures that might mainly occur with wireless LAN. In this and subsequent chapters, the discussions will also cover near field communication based on such standards as ZigBee and Wi-SUN (IEEE 802.15.4).

3.1　Failure causes and detection methods

In order to detect HN failures, it is necessary to provide information that enables HN-connected end devices and network devices to identify the causes of failures directly or indirectly. While there is not a definite method established yet, it is said that information such as listed below makes it easy to identify the causes of failures.

(A) Self-check function (status of the communication interface and internal status of the terminal function)
(B) End device network secession check function
(C) Pairing information output function (including authentication)
(D) Channel usage status acquisition function
(E) Received signal strength indicator measurement function (RSSI of network devices)
(F) Communication error rate measurement function (FER, PER, BER, etc.)

By using the above functions in combination, the four categories of failure causes can be identified as described below. Table 3-1 shows the possible combinations of failure causes and detection methods.

(1)　Problem of the radio channel

The channel usage status of another wireless device operating on the same or adjacent channel can be grasped through a channel scan to check for channel contention.

(2)　Problem of radio propagation

If wireless devices are far apart or have an obstacle (e.g., a wall) between them, or if multipath propagation is caused by reflection, the received signal strength indicator (RSSI) of the other-end device becomes weak. If the channel in use has noise or an interfering wave, the communication error rate becomes higher and the received signal strength indicator of the interfering wave becomes stronger.

(3)　Problem of a setup mistake

By acquiring the pairing information of the AP/coordinator, it is possible to check whether the target device is paired (set up) correctly.

(4)　Problem of a unit fault

By utilizing the self-check function, it is possible to identify the problems related to the fault of an individual device, such as a hardware fault of the AP or an end device.

Table 3-1 summarizes the methods of detecting wireless communication failure causes by using the above-mentioned functions of the end device and AP/coordinator in combination.

Table 3-1 Failure detection methods and detectable failure causes

Detection method	Failure cause			
	Radio channel	Radio propagation	Setup mistake	Unit failure
(A) Self-check				○
(B) End device network secession check	○			
(C) Pairing information output and acquisition			○	
(D) Channel usage status acquisition	○	○		
(E) Received signal strength indicator measurement		○		
(F) Communication error rate measurement		○		

For example, in the failure case of interference of an unintended signal source, a "channel scan" can be performed and, if radio energy of an interfering wave is present on the band used by the local station and the communication error rate is high, it can be presumed that the device is being affected by the interfering wave.

Table 3-2 summarizes the combinations of a wireless communication failure case and a detection method.

Table 3-2 Examples of detection methods for concrete wireless communication failure cases

Category	Details of the phenomenon	Detection method
1	The AP is unable to find the timing to transmit signals to the end device because it uses the same channel as a neighboring AP or an adjacent channel.	D
2	Although the AP in one's own house is in a standby state, the end device in that house outside the coverage area of the AP in the neighboring house repeatedly transmits signals to the AP in one's own house because the AP in the neighboring house that uses the same or adjacent channel is engaged in communication (exposed node problem).	D
3	Since a particular end device occupies the channel, the AP cannot transmit signals to the end device in question.	D
4	Since a particular end device occupies the channel, any other end device cannot transmit signals.	D
5	Since there are many end devices in the AP coverage area, the AP cannot transmit signals to all the devices (such cases as when the AP needs to control 1000 devices every minute).	C,F
6	When an end device of the neighboring house in the AP coverage area of one's own house uses the same channel and is engaged in communication, the end device in one's own house that cannot be reached by radio waves from the end device of the neighboring house repeatedly transmits signals although the AP in one's own house is in a standby state (hidden node problem).	D,F
7	The propagation of radio waves is affected by a new obstacle put between the AP and the end device, a newly installed door, or a change in the door material.	E,F
8	The device or AP cannot receive signals due to multipath propagation.	E,F
9	Interference of an unintended signal source (foreign-made product not certified for technical standard compliance, indoor wiring, particularly the lead-in wire of a satellite dish, etc.)	D,F
10	The device is gone (disposal device, or the device no longer exists as it has been replaced with another device).	B
11	A specific device becomes unable to communicate because of the battery running out or a failure.	A

12	The AP has been relocated to a place where the communication environment becomes poor for a specific device, thus making that device unable to communicate (there are many obstacles or the distance from the device is long).	B,E,F
13	The end device has been relocated to a place where the communication environment is poor and thus become unable to communicate with the AP.	B,E,F
14	The device has connected to an unauthorized AP by mistake and cannot communicate with the AP.	C
15	The device has become unable to communicate because the AP has failed.	A
16	Since the device has been restarted because it cannot connect to the AP, its configuration information has been changed.	B,C

When multi-hop wireless communication is used, a network topology is adopted that also includes relay nodes, such as a wireless router that relays packets while exerting packet path control in the network layer and a wireless repeater that duplicates and relays packets in the MAC layer, in addition to the AP/coordinator that accomplishes network management and end devices that communicate with the parent device as the devices at the end of the network.

As for failures associated with multi-hop wireless communication, the causes of category numbers 1, 2, and 3 in Table 3-2 are modified as shown in Table 3-3.

Table 3-3 Wireless communication failure cases modified for multi-hop wireless communication

Category	Details of the phenomenon	Detection method
1’	The same channel as the adjacent AP/coordinator or an adjacent channel subject to radio wave interference is used and the device cannot find the timing to transmit signals to the AP/coordinator or relay node.	D
2’	The same channel as the adjacent AP/coordinator or an adjacent channel subject to radio wave interference is used and the signals transmitted by the end device cannot be received by the AP/coordinator or relay node.	D
3’	Since a certain wireless device transmits a large volume of data on the same channel or an adjacent channel subject to radio wave interference, the AP/coordinator or relay node cannot transmit signals to end devices and others.	D

3.2 Failure detection methods

3.2.1 Self-check function

An end device or the AP/coordinator detects a failure by itself and notifies the communication status and the failure information in the end device or AP/coordinator function.

In addition to the internal error information unique to the end device or AP/coordinator, the information defined by the object superclasses of an ECHONET Lite device, such as abnormality occurrence status (EPC=0x88) or manufacturer abnormality code (EPC=0x86), is notified.

It is also possible to define a wireless device communication interface that enables the acquisition of the necessary internal information, such as the information about the internal status and settings of a device, which is difficult to prepare by default but needs to be acquired when the end device or AP/coordinator is suspected to be faulty although it does not recognize a failure.

3.2.2 End device network secession check function

The AP/coordinator checks whether the end device is connected to the network and notifies the result.

3.2.3 Pairing information output function

The AP/coordinator holds the information about the device paired with the local station and notifies that information.

3.2.4 Channel usage status acquisition function

The channel used by the AP/coordinator is scanned, the status (level) of interference with other wireless devices is measured, and the result is notified. This detection method supports two modes: the CS/CCA mode that detects only signals having the same signal format as the local station and the CCA-ED (Energy Detect) mode that detects the average received radio intensity regardless of a signal format[6]. Note that CCA-ED (Energy Detect) is required to grasp the status of all interfering waves.

Detection using CCA-ED (Energy Detect) is desirable. However, the implementation of CCA-ED is an option dependent on the region and the frequency used, and IEEE802.11-2012 requires CCA-ED to be implemented only for frequencies of 3 GHz or higher in North America[7]. In the 2.4-GHz band, CCA-ED may not be implemented or may not be used even if implemented.

3.2.5 Received signal strength indicator measurement function

The received signal strength indicator (RSSI) of the remote station is measured, and the result is notified. Generally, the RSSI value becomes smaller as the distance becomes greater. The appropriateness of the received signal strength indicator can be judged while taking into consideration the reception sensitivity of the local station.

3.2.6 Communication error rate acquisition function

The communication error rate in the actual communication between wireless devices is measured, and the result is notified. The level of stability of the wireless communication can be judged. Generally, the communication error rate becomes high when there is radio wave interference or when the devices are located far apart and the value of the received signal strength indicator is low.

The PER is measured by dividing the number of retransmissions by the number of transmissions in the regular wireless communication and updated for each transmission.

3.3 Aggregation of failure information

The information acquired by each end device and the AP/coordinator is aggregated in the HGW before it is notified to the management PF. The information to be notified is as follows.

An end device notifies the "self-check result," "received signal strength indicator," and "communication error rate" to the AP/coordinator.

The AP/coordinator notifies the "self-check result," "end device network secession check result," "channel scan result," "received signal strength indicator," and "communication error rate" to the HGW. The AP/coordinator also stores the "self-check result" and "received signal strength indicator," acquired from each end device, temporarily before notifying them to the HGW.

Figure 3-1 shows how the information of end devices and the AP/coordinator is notified via the management PF to customer support centers. All information is notified to the general support center unless otherwise requested by the device manufacturer concerned. However, many device manufacturers do not want their failure information to be disclosed to competitors. Therefore, there may be cases where the general support center is notified only about whether failure information exists and manufacturer-specific information is notified only to the maintenance center of

[6] Refer to IEEE802.11-2012 18.3.10.6, CCA requirements. For information about the carrier sense option in DSSS/CCK before OFDM, refer to 16.4.8.5 and 17.4.8.5.

[7] Refer to IEEE802.11-2012, Tables E-1 to E-4.

the corresponding manufacturer. The management PF needs to notify device information only to a specific application.

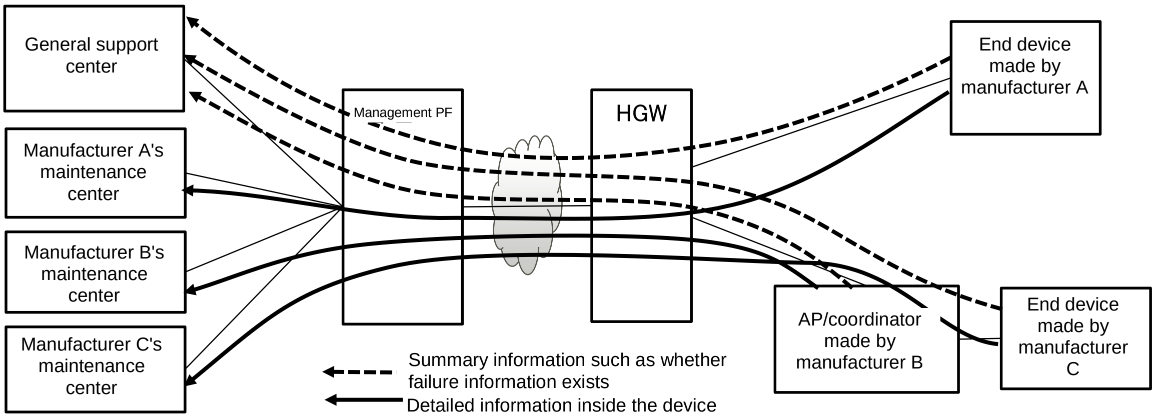

General support center
Manufacturer A's maintenance center
Manufacturer B's maintenance center
Manufacturer C's maintenance center
Management PF
HGW
End device made by manufacturer A
AP/coordinator made by manufacturer B
End device made by manufacturer C
Summary information such as whether failure information exists
Detailed information inside the device

Figure 3-1 Flow of failure information

Chapter 4　Architecture

Chapter 3 described the methods of detecting failures of HN-connected end devices and networks.　Since a HN has multiple end devices connected via various networks, there is a need to aggregate the information from these devices and detect failures and identify their causes based on diverse phenomena that take place simultaneously.

This chapter describes the architecture used for customer support to collect information about failures that occur in end devices and networks.

4.1　Overview

One architecture for enabling HN-connected end devices to be referenced and controlled from the cloud is defined in ITU-T Y.2070.　In this architecture, it is possible to acquire the internal status of end devices and exert power on/off control and other controls.　By extending the architecture to include the end device network functions and network devices, the information about failures that occur in a HN is aggregated in the Internet.

Figure 4-1 shows an architecture that allows customer support to detect failures in a HN from a remote location.

In this architecture, two types of applications run.　One is the service application, and the other is customer support. While these applications run in the same architecture, Figure 4-1 shows only those functions related to customer support.　The part to the right of the HGW represents the HN, where end devices are connected via a network device.

In this architecture, an agent that acquires end device failure information or information necessary for failure detection resides in each end device, and this agent notifies failure information to the HGW.　The information collected from each household to the HGW is aggregated by the resource management function in the management PF and referenced by the application that implements customer support.　The resource information collection function collects such information as the configuration information and internal status of each individual device.　This function works effectively by making it possible for end device manufacturers to reference the information necessary for failure cause analysis from the outside.

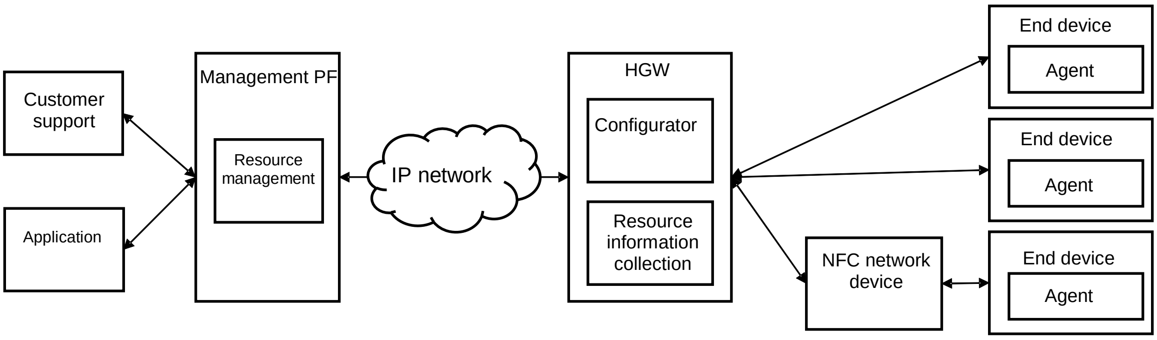


Figure 4-1 Failure detection architecture (Y.2070)

4.2　HN failure information notification

This section describes how the HGW and management PF aggregate the information collected by end devices and network devices.

HTIP is adopted as the protocol for acquiring the network topology information of a HN.　End device attribute information is acquired using such protocols as UPnP/HTIP, ECHONET Lite, and SNMP.　Details will be given in Chapter 5, but the basic idea is that, since different protocols are adopted depending on the field of application of end devices and network devices, the HGW handles the protocol for each end device and network device individually and the resource information collection function manages information in an integrated manner.　The protocols assumed here are often represented as combinations of an internally expressed attribute of an end device or network device and its value. Therefore, the resource information collection function manages all end device information in the format of <attribute name, attribute value>. The end device information expression method (XML, CSV, JSON, etc.) to be used when notifying the management PF about this information and the protocol (HTTP, MQTT, CoAP, WebSocket, BBF TR-069, etc.) to be used for communicating the expressed data will be defined separately.

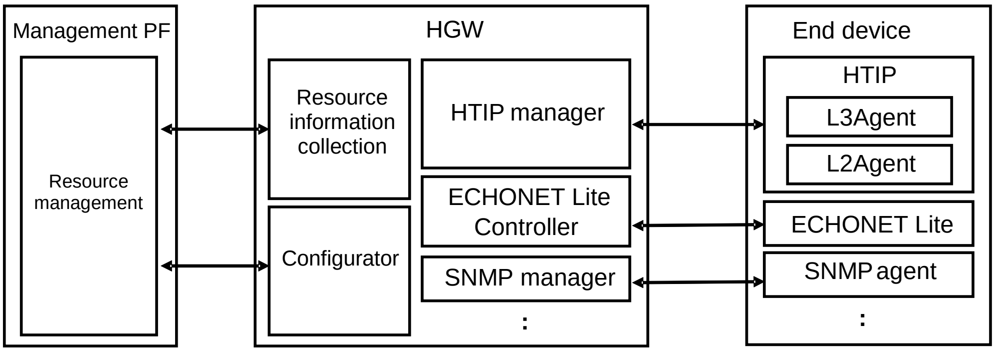


Figure 4-2 Failure information notification and recovery setting

4.3 Failure information notification in single-hop wireless communication

The network information (devices and connection) is handled by extending HTIP. Details of the protocol will be given in Chapter 5. This section described the notification method.

(1) Self-check function

The AP/coordinator notifies the HGW of its self-check result. The AP/coordinator is required to send this notification at regular intervals and may have extended functions to support on-demand notification at the time of abnormality detection and give a notification in response to a request from the HGW.

An end device notifies the HGW of its self-check result via the AP/coordinator. The end device is required to send this notification at regular intervals and may have extended functions to support on-demand notification at the time of abnormality detection and give a notification in response to a request from the HGW.

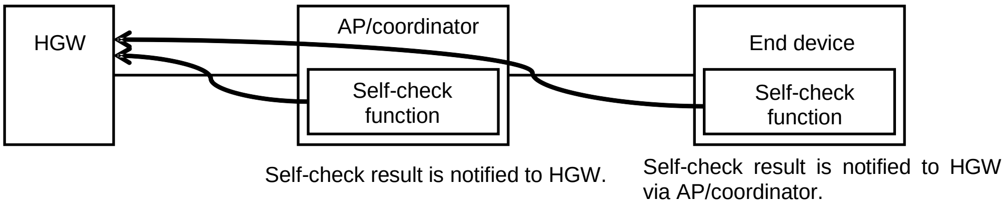

HGW
AP/coordinator
Self-check function
End device
Self-check function
Self-check result is notified to HGW.
Self-check result is notified to HGW via AP/coordinator.

Figure 4-3 Self-check function (single-hop wireless communication)

(2) End device network secession check function

The AP/coordinator checks whether the end device is seceded from the network (e.g., based on the fact that the end device has failed to return a response several times) and notifies the HGW about the result.

The AP/coordinator is required to send this notification at regular intervals and may have extended functions to support on-demand notification at the time of abnormality detection and give a notification in response to a request from the HGW.

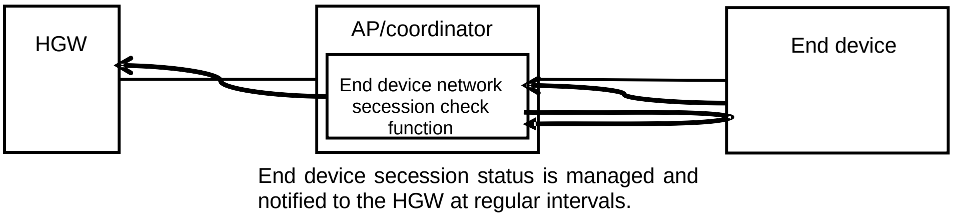

HGW
AP/coordinator
End device network secession check function
End device
End device secession status is managed and notified to the HGW at regular intervals.

Figure 4-4 End device network secession check function (single-hop wireless communication)

(3) Pairing information output function

The AP/coordinator manages the status of pairing with each end device (not complete, authentication in progress, or complete) and notifies the HGW. The end device is required to send this notification at regular intervals and may have extended functions to support on-demand notification at the time of abnormality detection and give a notification in response to a request from the HGW.

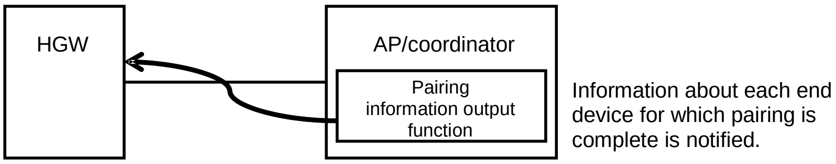

HGW
AP/coordinator
Pairing information output function
Information about each end device for which pairing is complete is notified.

Figure 4-5 Pairing information output function (single-hop wireless communication)

(4) Channel usage status acquisition function

When a new network is built, the AP/coordinator performs a channel scan and decides which channel to use for the entire network.

If the AP/coordinator detects an interference factor, such as a strong RSSI and a high PER, consecutively for a certain period of time, it re-scans the channel used at that point of time. If the channel in use is judged to be congested, the AP/coordinator notifies the HGW.

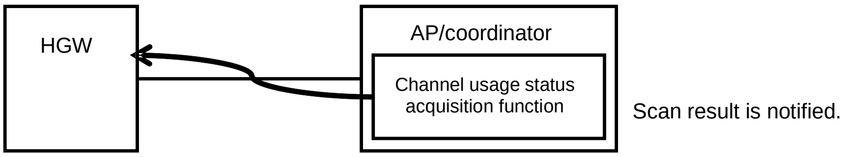


Figure 4-6 Channel usage status acquisition function (single-hop wireless communication)

(5) Received signal strength indicator measurement function

The AP/coordinator manages the RSSI value of the last packet (or last several packets) it received from each end device on an individual end device basis. The end device is required to send this notification at regular intervals and may have extended functions to support on-demand notification at the time of abnormality detection and give a notification in response to a request from the HGW.

The end device manages the RSSI value of the last packet (or last several packets) it received from the AP/coordinator.

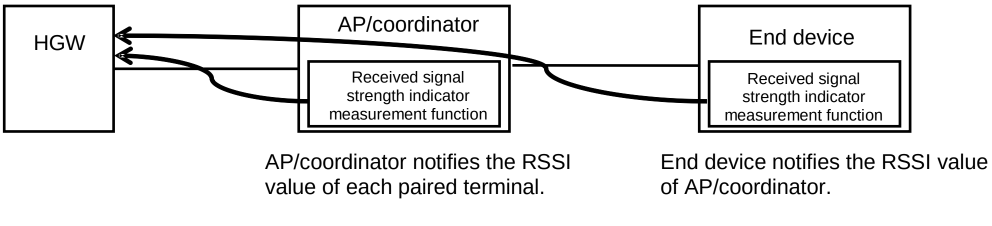

HGW
AP/coordinator
Received signal strength indicator measurement function
End device
Received signal strength indicator measurement function
AP/coordinator notifies the RSSI value of each paired terminal.
End device notifies the RSSI value of AP/coordinator.

Figure 4-7 Received signal strength indicator measurement function (single-hop wireless communication)

(6) Communication error rate measurement function

During the regular communication with each end device, the AP/coordinator records the number of retransmissions for the specified number of transmissions. The AP/coordinator updates the number of retransmissions for each transmission and manages the latest value obtained by dividing the number of retransmissions by the specified number of transmissions.

The AP/coordinator is required to send this notification at regular intervals and may have extended functions to support on-demand notification at the time of abnormality detection and give a notification in response to a request from the HGW.

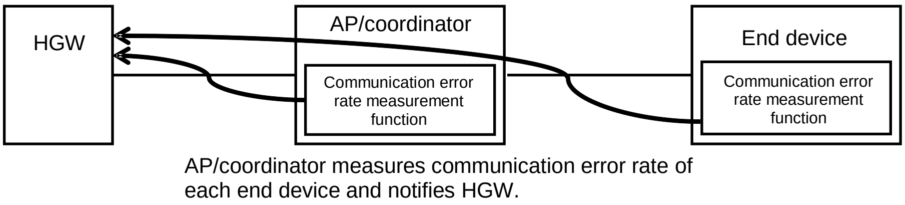

HGW
AP/coordinator
Communication error rate measurement function
End device
Communication error rate measurement function
AP/coordinator measures communication error rate of each end device and notifies HGW.

Figure 4-8 Communication error rate measurement function (single-hop wireless communication)

4.4 Failure information notification in multi-hop wireless communication

The notification methods for the individual failure detection methods applicable when using multi-hop wireless communication are described below.

(1) Self-check function

Each device makes a self-check at regular intervals and manages its own abnormalities. The device is required to send a notification at regular intervals and may have extended functions to support on-demand notification at the time of abnormality detection and give a notification in response to a request from the HGW.

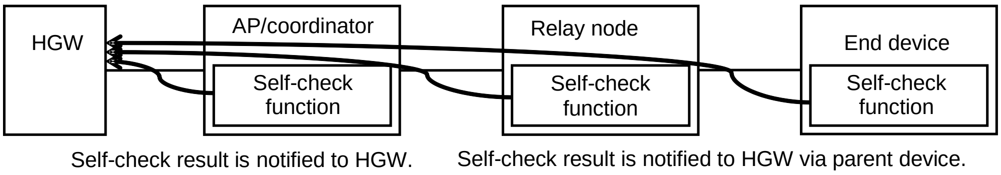


Figure 4-9 Self-check function (multi-hop wireless communication)

(2) End device network secession check function

If the AP/coordinator and relay node to which an end device is connected detect that no response has been returned from the end device for several consecutive times, they judge that the end device is seceded from the network. End device secession information is periodically aggregated to the AP/coordinator, which manages the connection status of the entire network.

The AP/coordinator is required to notify the HGW at regular intervals and may have extended functions to support on-demand notification at the time of abnormality detection and give a notification in response to a request from the HGW.

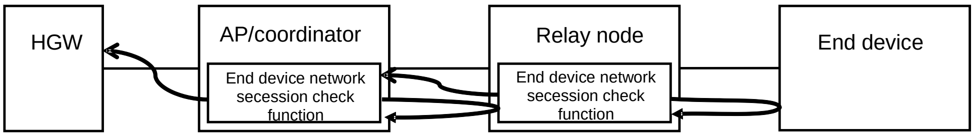
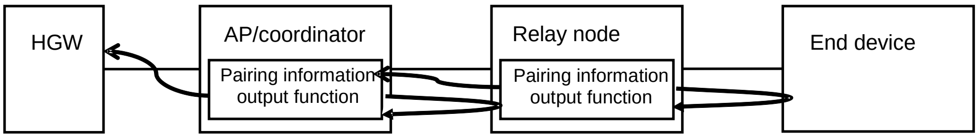

HGW
AP/coordinator
End device network secession check function
Relay node
End device network secession check function
End device

Figure 4-10 End device network secession check function (multi-hop wireless communication)

(3) Pairing information output function

The AP/coordinator and relay node to which end devices are connected manage the status of pairing with each end device (not connected or complete). The pairing information is periodically aggregated to the AP/coordinator, which manages the pairing status of the entire network.

The AP/coordinator is required to notify the HGW at regular intervals and may have extended functions to support on-demand notification at the time of abnormality detection and give a notification in response to a request from the HGW.


HGW
AP/coordinator
Pairing information output function
Relay node
Pairing information output function
End device

Information about each end device for which pairing is complete is notified.

Figure 4-11 Pairing information output function (multi-hop wireless communication)

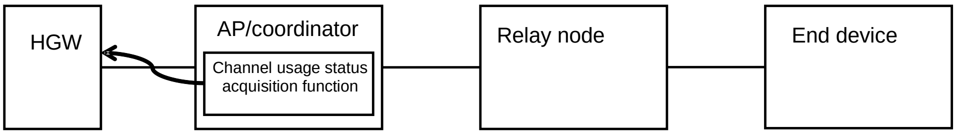
(4) Channel usage status acquisition function

When a new network is built, the AP/coordinator performs a channel scan and decides which channel to use for the entire network.

If the AP/coordinator detects an interference factor, such as a strong RSSI and a high PER, consecutively for a certain period of time, it re-scans the channel used at that point of time. If the channel in use is judged to be congested, the AP/coordinator notifies the HGW.

An extended function may be implemented to scan other channels and switch the channel used for the entire network to a vacant channel.

When multi-hop wireless communication is used, it is highly likely that the radio waves from the AP/coordinator do not reach a relay node and end device that are two or more hops away, in which case the channel scan by the AP/coordinator cannot determine whether the channel is congested. A mechanism may be implemented as an extended function whereby channel scan capability is incorporated into the relay node to perform a channel scan locally in each remote location and have the results managed by the AP/coordinator.



Channel scan results (each channel's RSSI value, etc.) are notified.

Figure 4-12 Channel usage status acquisition function (multi-hop wireless communication)

(5) Received signal strength indicator measurement function

The AP/coordinator and relay node to which end devices are connected manage the RSSI value of the last packet (or last several packets) it received from each end device on an individual end device basis.

The relay node and end device manage the RSSI value of the last packet (or last several packets) it received from the AP/coordinator and notify the AP/coordinator at regular intervals.

The RSSI information is periodically aggregated to the AP/coordinator, which manages the RSSI status of the entire network. The AP/coordinator is required to notify the HGW at regular intervals and may have extended functions to support on-demand notification at the time of abnormality detection and give a notification in response to a request from the HGW.

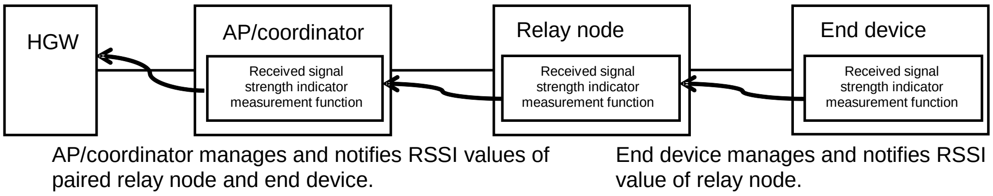

HGW
AP/coordinator
Received signal strength indicator measurement function
Relay node
Received signal strength indicator measurement function
End device
Received signal strength indicator measurement function
AP/coordinator manages and notifies RSSI values of paired relay node and end device.
End device manages and notifies RSSI value of relay node.

Figure 4-13 Received signal strength indicator measurement function (multi-hop wireless communication)

(6) Communication error rate measurement function

The AP/coordinator and relay node to which end devices are connected record the number of packets retransmitted to each end device during the last several transmissions and manage the status of communication with each end device.

The AP/coordinator and end device record the number of packets retransmitted to the parent device during the last several transmissions, manage the status of communication with the AP/coordinator and relay node, and notify the parent device at regular intervals.

The communication status information is periodically aggregated to the AP/coordinator, which manages the communication status of the entire network. The AP/coordinator is required to notify the HGW at regular intervals and may have extended functions to support on-demand notification at the time of abnormality detection and give a notification in response to a request from the HGW.

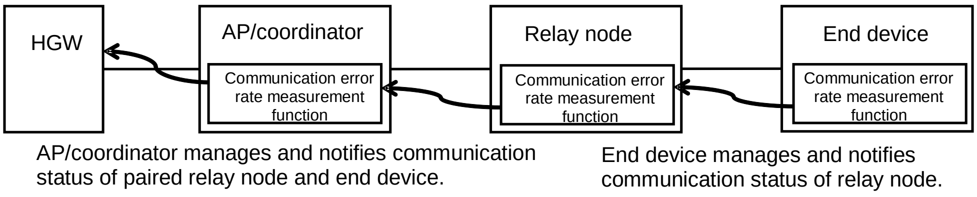

HGW
AP/coordinator
Communication error rate measurement function
Relay node
Communication error rate measurement function
End device
Communication error rate measurement function
AP/coordinator manages and notifies communication status of paired relay node and end device.
End device manages and notifies communication status of relay node.

Figure 4-14 Communication error rate measurement function (multi-hop wireless communication)

Chapter 5　Communication Interface

5.1　Overview of HTIP and its extension method

5.1.1　Overview of HTIP

HTIP is a protocol defined in TTC JJ-300.00 and JJ-300.01 used to acquire network topology information in the link layer broadcast domain of a HN. There are two extended protocols used for HTIP to acquire network topology information: LLDP and UPnP. The LLDP and UPnP protocols are described below.

・LLDP

LLDP (Link Layer Discovery Protocol) is a protocol defined in IEEE 802.1AB and transmits network topology information by storing the information in Ethernet frames in the TLV (Type Length Value) format. In HTIP, network devices (Ethernet switches) use this protocol to notify network topology information and TLV types are added.

・UPnP

UPnP (Universal Plug and Play) is a protocol defined in the UPnP Device Architecture of the UPnP Forum and transmits device information by storing the information in XML data carried using UDP, TCP, or HTTP. In HTIP, terminals use this protocol to store device information for HTIP and XML tag types are added.

5.1.2　Extensions to HTIP

(1) Addition of information necessary to detect network failure causes

The information described in Section 3.2 that is necessary to detect network failure causes (self-check result, end device network secession check result, pairing information, channel scan result, received signal strength indicator (RSSI), and communication error rate) is added to the network topology information that is handled by HTIP.

・An extended connection topology information notification TLV for notifying the information necessary to detect network failure causes is added to the LLDP of the L2 Agent function used by the HTIP-network device.

・An extended connection topology information notification tag for notifying the information necessary to detect network failure causes is added to the UPnP of the L3 Agent function used by the HTIP-end terminal.

・Since the information that can be acquired differs depending on the communication module used, only the information that can be acquired can be notified.

(2) Support of non-Ethernet data link layers

The data link layers for which HTIP is originally intended are Ethernet data link layers (wired LAN and wireless LAN). Extensions to support non-Ethernet data link layers (802.15.1 family set forth in [TTC TR-1043], 802.15.4 family, ITU-T G.hn, and ITU-T G.9903 data link layers) for the HTIP-network device and HTIP-end terminal are described below.

(2-1) HTIP-network device

・On the assumption that IP communication is available, LLDP frames extended for HTIP are transmitted using an encapsulation protocol for transferring such frames over an IP network (GRE is specified as the protocol that must be supported at least; another protocol such as EtherIP, L2TPv3, or VXLAN may be used).

・The destination IP address is a broadcast address.

・The source MAC address of the LLDP frames is a fixed value that is not dependent on the device.

- The device is identified using the MAC address of the data link layer that is set in the Chassis ID TLV of the LLDP frame. The value of the Chassis ID Subtype in the Chassis ID TLV is 4 (MAC address (IEEE Std 802)), as currently defined, and it is possible to set a MAC address that is not 6 octets long.
- An extended TLV for MAC address list notification is defined to support MAC addresses that are not 6 octets long.
- To establish correspondence between information acquired by HTIP and information acquired by another protocol such as ECHONET Lite, the IP address is notified using the standard TLV of LLDP on the assumption that the target device has an IP address.

(2-2) HTIP-end terminal

- On the assumption that IP communication is available, UPnP packets extended for HTIP are used.
- Since the IP address information of the HTIP-end terminal can be acquired from the UPnP packet, correspondence between information acquired by HTIP and information acquired by another protocol such as ECHONET Lite can be established.
- To ensure a lighter implementation of the HTIP-end terminal, the HTIP-end terminal is allowed to use LLDP in addition to UPnP.

(3) Extensions to the terminal category information list defined in JJ-300.01

The terminal category information list is extended to add the information about the protocols other than HTIP supported by the device to the network topology information handled by HTIP.

- The terminal category is added that indicates the protocol supported by the device.
- The format of the terminal category string indicating the protocol is PROTOCOL_xxx (where xxx is the protocol name such as ECHONET_Lite or SNMP).
- The HN resource manager can judge which protocol is available for communication with the terminal based on the terminal category information acquired by HTIP.

5.2 Protocols other than HTIP

Besides UPnP supported by HTIP, there are many other protocols that can be used to handle end device information. This section describes SNMP, ECHONET Lite, CLI, and NETCONF as the candidate protocols in this guideline.

5.2.1 SNMP

SNMP (Simple Network Management Protocol) is an Internet standard protocol used to manage terminals on the IP network. Terminals that support SNMP include routers, switches, servers, and printers. The protocol provides a management system for monitoring terminals that can be connected to the network, and its purpose is to notify the network administrator about the ongoing situation. While it consists of the standard network management functions, application-layer protocols, databases, and data objects are defined.

Since SNMP was developed as a protocol used for network management, various types of information concerning network devices are defined as MIBs. Recently, however, the IETF launched the Energy Management WG (eman), and work has been underway to define end devices in smart grids and homes as MIBs. End devices used in a HN are also being defined as MIBs.

5.2.2 ECHONET Lite

ECHONET Lite is a communication protocol developed by the ECHONET Consortium. Intended for devices and sensors for smart houses, this protocol has been adopted as an ISO/IEC standard. ECHONET Lite supports more than 80 types of devices that are connected in a smart house, including air conditioners, lighting equipment, water heaters, photovoltaic power generation systems, storage battery cells, and smart meters. In ECHONET Lite, the end device functions are defined as attributes and operations called properties. A set of properties is defined for each device, and such a set is called an object. The ECHONET Lite protocol is implemented by communicating these properties and their values.

5.2.3 CLI

Network devices equipped with management functions have setting interfaces using serial terminals connected via RS-232C. These are collectively called the command line interface. In many cases, the same interface is provided to virtual terminals over the network and can be used with the TELNET and SSH protocols. While this interface is originally intended for administrators, it can also be used to configure settings between devices if necessary commands are mechanically generated. Note that, since most setting commands are device-dependent, there is a need to take extra steps such as creating a command database for the device in use.

Since Cisco Systems is very influential in the market of routers and other network devices, some products from other companies have setting interfaces that emulate Cisco Systems' command line interface. Given this situation, the CLI is sometimes referred to as the Cisco Lite Interface.

Also, these days, there are network devices - mainly home-use products - that offer setting interfaces as HTTP-based Web pages without using the CLI in order to allow simpler setting operations. In the case of such devices, it is also possible to configure settings between devices if the information that is supposed to be input via the browser is mechanically generated.

5.2.4 NETCONF

The need is growing year by year for the capability to dynamically configure the network devices comprising the system while they are running. To meet this need, a network device setting function based on API (Application Programming Interface) has been developed. NETCONF, standardized by IETF, provides a protocol whereby the configuration application program running on the network device to be configured can accomplish device configuration using a RPC (Remote Procedure Call). In NETCONF, the configuration content, design operation, remote procedure call (RPC), and transport protocol are separated. As the transport protocol, SSH, SOAP, BEEP, and TLS can be used.

The CLI and Web interfaces are designed on the assumption that settings are made by humans. In contrast, SNMP assumes protocol-level interaction between programs, and NETCONF assumes that programs interact at the API level.

Currently, NETCONF is used for clusters of network devices in data centers and other facilities. Whether the use of this protocol will spread to home appliances and other general consumer devices remains to be seen.

Chapter 6 Conclusion

This technical report has described customer support functions, which are anticipated to become a major issue as HN services will come into wider use. Based on TTC TR-1053, consideration has been given to this issue, with the focus on how customer support functions in the cloud can aggregate the information about end devices and networks that is necessary for failure detection and cause analysis. Particularly, failures associated with near field communication are likely to grow in prominence in the future, and the collaboration between the platform and end devices and networks is projected to become increasingly important. It is hoped that in-depth discussions will be continued based on actual use cases and that findings will be reflected in this technical report.

Reference Documents

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

[ITU-T G.9980] ITU-T Recommendation G.9980 (2012), Remote management of customer premises equipment

[BEEP] IETF RFC3080, The Blocks Extensible Exchange Protocol Core.

[Bluetooth] Personal Area Networking Profile version 1.0, Bluetooth SIG, February 14, 2003

[CoAP] IETF RFC7252, The Constrained Application Protocol (CoAP)

[CSV] RFC 4180, Common Format and MIME Type for Comma-Separated Values (CSV) Files

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

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

[EtherIP] IETF RFC3378, EtherIP: Tunneling Ethernet Frames in IP Datagrams.

[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

[ITU-T G.9973] ITU-T G.9973, Protocol for identifying home network topology

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

[TTC JJ-300.01] TTC JJ-300.00 v1.1 (2011), Home-network Topology Identifying Protocol (HTIP)

[HTTP] IETF RFC2616, Hypertext Transfer Protocol -- HTTP/1.1

[ITU-T G.hn] ITU-T G.9960, Unified high-speed wireline-based home networking transceivers - System architecture and physical layer specification.
ITU-T G.9961, Unified high-speed wire-line based home networking transceivers - Data link layer specification.
ITU-T G.9963, Unified high-speed wireline-based home networking transceivers - Multiple input/multiple output specification.
ITU-T G.9964, Unified high-speed wireline-based home networking transceivers - Power spectral density specification.
ITU-T G.9972, Coexistence mechanism for wireline home networking transceivers.

[ITU-T G.9903] ITU-T G.9903, Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks.

[ITU-T Y.2070] ITU-T Y.2070, Requirements and architecture of home energy management system and home network services.

[JSON] IETF RFC4627, The application/json Media Type for JavaScript Object Notation (JSON)

[L2TPv3] IETF RFC3931, Layer Two Tunneling Protocol - Version 3 (L2TPv3).

[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

[MQTT] OASIS MQTT Version 3.1.1

[Netconf] IETF RFC6241, Network Configuration Protocol (NETCONF).

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

[SSH] IETF RFC4251, The Secure Shell (SSH) Protocol Architecture.

[SOAP] W3C SOAP Version 1.2 Part 1: Messaging Framework (Second Edition).

[TLS] IETF RFC5246, The Transport Layer Security (TLS) Protocol Version 1.2.

[TTC TR-1043] TTC TR-1043 (2013), Implementation guidelines of Home network communication interface

[TTC TR-1053] TTC TR-1053 (2014), Customer support functions for home network service platform

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

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

[VXLAN] IETF RFC7348, Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks

[WebSocket] IETF RFC6455, The WebSocket Protocol

[Wi-Fi] IEEE 802.11-2012, IEEE

[Wi-SUN] IEEE Std 802.15-2011, IEEE Standard for Local and metropolitan area networks- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).
IEEE Std 802.15.4g-2012, Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks.
IEEE Std 802.15.4e-2012, Amendment 1: MAC sub layer

[XML] W3C Extensible Markup Language (XML) 1.0 (Fifth Edition)
W3C Extensible Markup Language (XML) 1.1 (Second Edition)

[ZigBee] IEEE Std 802.15-2011, IEEE Standard for Local and metropolitan area networks- Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).
IEEE Std 802.15.4g-2012, Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks.