TD61-2461B

HitachiCable
Empowering Energy & Communication

WirelessIP5000-A
System Integration Manual

HITACHI CABLE, LTD

1. Introduction

This document explains the basic concepts and things to keep in mind when designing networks for the Wireless IP phone WirelessIP5000-A.

This document assumes that you are familiar with the following network technologies.

（1） Ethernet（VLAN）

（2） Wireless LAN 802.11b

（3） TCP/IP Protocol (IP, QoS, ToS)

（4） Authentication 802.1x

2. Wireless LAN Overview

2.1 Wireless LAN Overview

Multiple devices communicate using the wireless LAN (802.11b) at a data rate of up to 11Mb.

The wireless LAN has features differing from a wired LAN.

（1） A wireless LAN operates by sharing bandwidth. In other words, communication is half duplex.

（2） The communication band of the wireless LAN changes with the distance between the wireless LAN client and wireless LAN access point (AP). At larger distances, communication is supported at low data rates.

（3） As all wireless LAN traffic is transmitted into the air, the wireless LAN operates on the premise that any wireless LAN device can capture traffic. Accordingly, increased security needs to be considered.

2.2 Things to Consider Before Designing a Wireless LAN Network

Determine the following before designing a wireless LAN.

（1） Required bandwidth per user and number of users

（2） Wireless LAN service area

（3） Security

- User authentication (802.1x)
- Data encryption (WEP/TKIP/AES) within the wireless area

（4） The hardwired components of the network

Based on the above, decide the following.

(1) Access point layout

(2) VLAN design

(3) Wireless LAN operation

3. Site Survey and Wireless LAN Design Guidelines

3.1 Site Survey

A site survey of the installation environment is necessary before installing wireless LAN.

[Site Survey]

(1) Establish the service area

Confirm the area that needs to be served by the wireless LAN.

(2) Reception signal level

Measure signal strength to check that transmissions from access points laid out among the terminals within the service area can be received. Make note of objects such as metal cabinets that may interrupt the signal, especially in offices.

As shown in the figure below, the WirelessIP5000-A can be used to verify the AP service area. A tool that measures electrical field intensity can also be used.

[Figure. AP service area confirmation]

*** Site scan**
How far does the transmission signal from the access point reach?
You can search for AP's that are receiving transmissions and based on their reception sensitivity, decide their positions.

[Reception Sensitivity]

The following shows the relationship between the reception level of the WirelessIP5000-A and the Antenna display.

1. Reception Sensitivity

   −83dBm at 11Mbps, −87dBm at 5.5Mbps, −88dBm at 2Mbps, −92dBm at 1Mbps with BER 8%

2. Antenna Display and Reception Level

   Antenna 0: to −89dBm, Antenna 1: −89 to −81dBm, Antenna 2: −81 to−74dBm,

   Antenna 3: −74 to −66dBm, Antenna 4: −66 to−58dBm, Antenna 5: −58dBm and up

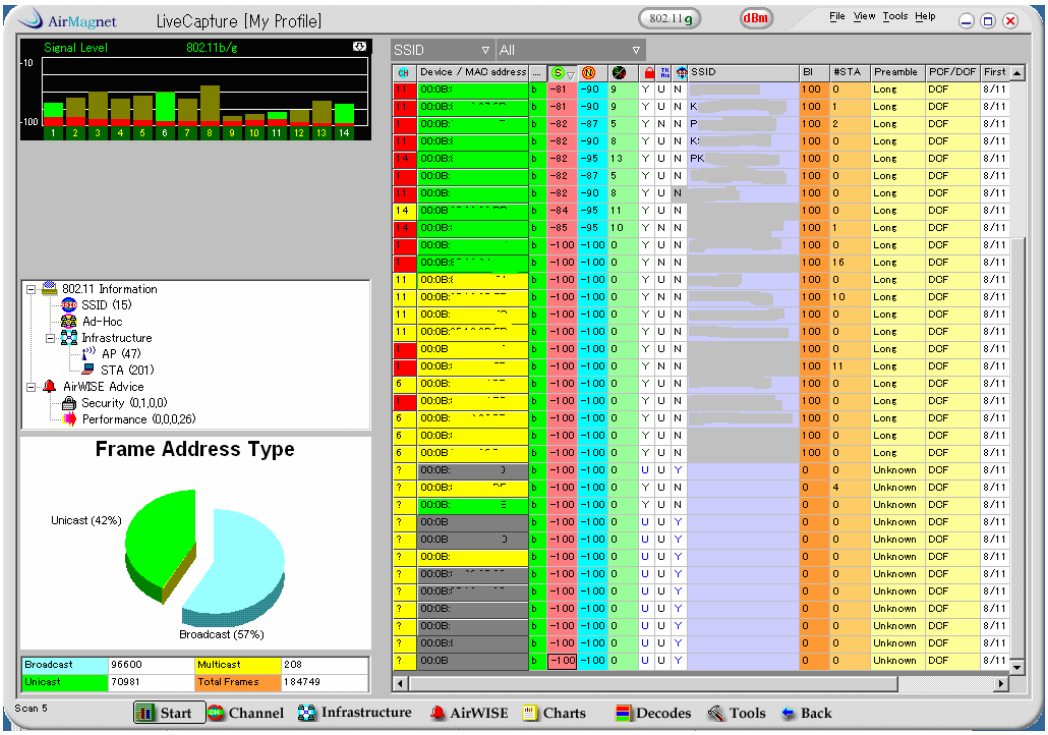
(3) Interference

Determine whether there are wireless LAN transmissions on the same frequency band. If so, channel assignments must be considered.

* Refer to the AP service area confirmation Figure

[Figure. Wireless Monitor Tool Sample Screen]

AirMagnet (TOYO Corporation) can be used to confirm the signal level, SNR and wireless LAN standard (a, b, g) for each BSS-ID from the AP within the service area. Outside signals can also be determined.



(4) Required bandwidth and number of users

We recommend that you do not mix data and voice on a wireless LAN.

The hardwired portions must also be designed with data sharing in mind.

1. Determine the amount of data traffic

   Determine data traffic through the shared wired LAN.

2. Determine the number of terminals

   Determine the number of terminals within the service area.

3. Determine the number of concurrent calls

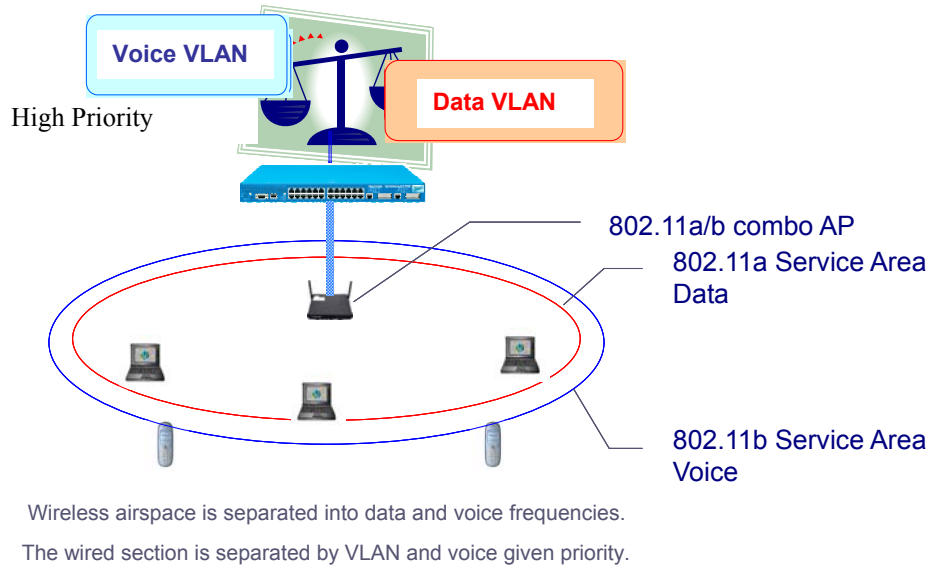
   Determine the maximum number of concurrent calls made on terminals within the service area.

3.2 Wireless LAN Design Guidelines

(1) Mixing Data

The effective throughput of 802.11b is about 6Mbps. Terminals share this bandwidth. As the number of terminals connected to the access point increases, the overhead increases and the throughput decreases. Accordingly, the mixture of data and voice is not recommended in a wireless LAN environment. Even in the upstream wired LAN portion, the communication band including data needs to be sufficiently maintained and the priority of the voice packet communication raised, to control delays, jitters, loss, etc.

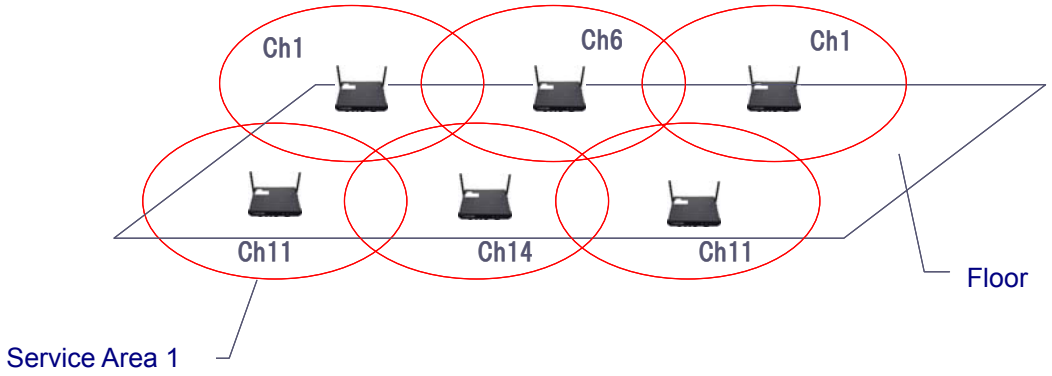
[Figure. Recommendations for Wireless LAN Design]



(2) Service Area

The output levels of the access point vary according to systems and settings. They need to be adjusted to meet the requirements of the environment. The service area of the access point expands with increased output level of the access points. Therefore, service areas may overlap (duplicate receiving ranges). Overlap is necessary to implement handover, but the access points must be laid out so that service areas of those whose frequencies would interfere with each other do not overlap. We recommend that you design service area boundary values based on the handover threshold (Try_RxLevel) settings.

[Figure. AP Layout Design Basics]



■ Arrange the service areas so that they overlap (ensure that no physical location falls outside a service area)

■ Ensure that the frequencies of the AP channels in the service areas do not overlap.

(3) Power save mode

The power save function is specified in the 802.11b standard and conserves electrical power. The terminals and the access points must support the function for it to operate. The details are explained in 7.4 Power Save Mode.

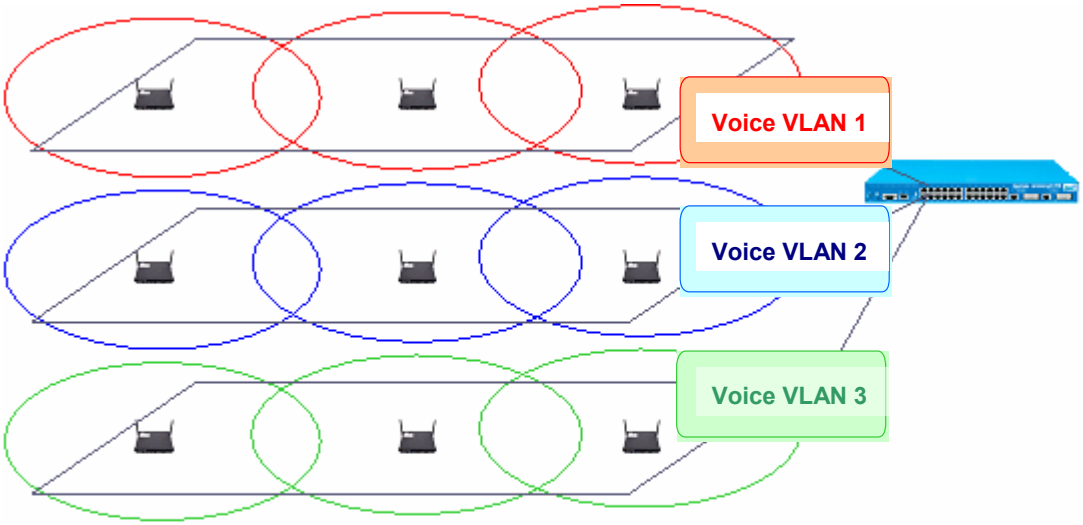
(4) Broadcast Packet

As wireless operates in share mode, broadcast packets target all terminals. The number of packets broadcast needs to be minimized in order to conserve power.

(5) VLAN Design

To separate voice from data and to give it higher priority, VLANs for voice are allocated on the upstream wired LAN. By setting VLANs for exclusive use, operation is separated and security is enhanced.

[Figure. II-1. VLAN Configuration Example]



■ Combine all on one voice VLAN or set up voice VLANs by floor.

* When setting up voice VLANs by floor, L3 handover is possible but L2 handover is not. See 7.2 Operating in a Multiple Network Environment for information about handover when ESSIDs are not the same.

3.3 Wireless LAN Design Checklist

Lay out and design the wireless LAN having considered the following.

No.	Item	Conditions	Remarks
1	AP Reception Sensitivity	Make sure the antenna level within the service area is 3 or more (signal level: over -74 dMm).	Determine using the site survey.
2	SNR (Signal-to-Noise Ratio)	Suppress channel interference (SNR > 20)	Determine using the site survey.
3	Wireless Communication Rate	Check that the communication rate has not decreased due to external factors or effects of external waves.	Determine using the site survey.
4	AP Channel Design	Arrange the AP so that ones using the same frequency band do not interfere with each other.	Follow the arrangement plan of the wireless LAN system being installed. Use the site survey to check for external waves and select the channels accordingly.
5	Wireless LAN Power Save Mode	Must always be used.	If the LAN cannot operate in power save mode, the WirelessIP5000-A standby time decreases to about 1/10th.
6	AP Mode	Do not mix IEEE802.11b and IEEE802.11g.	Use the site survey to check.
7	Wireless LAN Broadcast Packet	Stop unnecessary broadcasts and unicasts.	Burst broadcast packets greatly affect voice quality and also may drain the battery.
8	Number of Connected Clients per AP	Assume up to 20 clients within a single AP service area.	This figure is a rule of thumb and varies according to the wireless LAN system used.
9	Number of Concurrent Calls per AP	The number of terminals making concurrent calls should be fewer than 7.	This figure is a rule of thumb and varies according to the wireless LAN system used.

10	Wired LAN (Uplink LAN) Bandwidth	There should a bandwidth of over twice the data bandwidth peak value + number of concurrent calls x bandwidth of each call	Estimate 180Kbps per call *1
11	Wired LAN VLAN	The voice terminals are divided into VLANs.	
12	Wired LAN QoS	Give priority to voice traffic. The characteristics of the wired LAN section are as follows. Delay: 100ms or less *2 Loss: 0.1% or less Jitter: 10ms or less	These characteristics are estimates and methods include giving priority to voice VLAN, DiffServ, and IP Precedence (similar to WirelessIP5000-A, the terminal needs a function to set the ToS field).

*1 The RTP packet is made up of a 20 byte IP header, 8 bytes UDP header, 12 bytes RPT header, and RTP data. The RTP data is a 20ms voice sample. The RTP data for G729 is 20 bytes and 160 bytes for G711. The total VoIP packet is 200 bytes (IP, UDP, RTP headers + RTP data. The 802.11 header (layer 2 MAC) adds 24 bytes for a total packet size of 224 bytes. Each side transmits 50 packets of RTP data per second (pps), so 100 pps is transmitted for both sides.

For the G711.

256 byte packet size = 2,596,588 bits/second = 324,573 bytes/sec (logical packet rate)

100 packet/sec * 224 bytes/packet = 22,400 bytes/sec = 179,200 bps

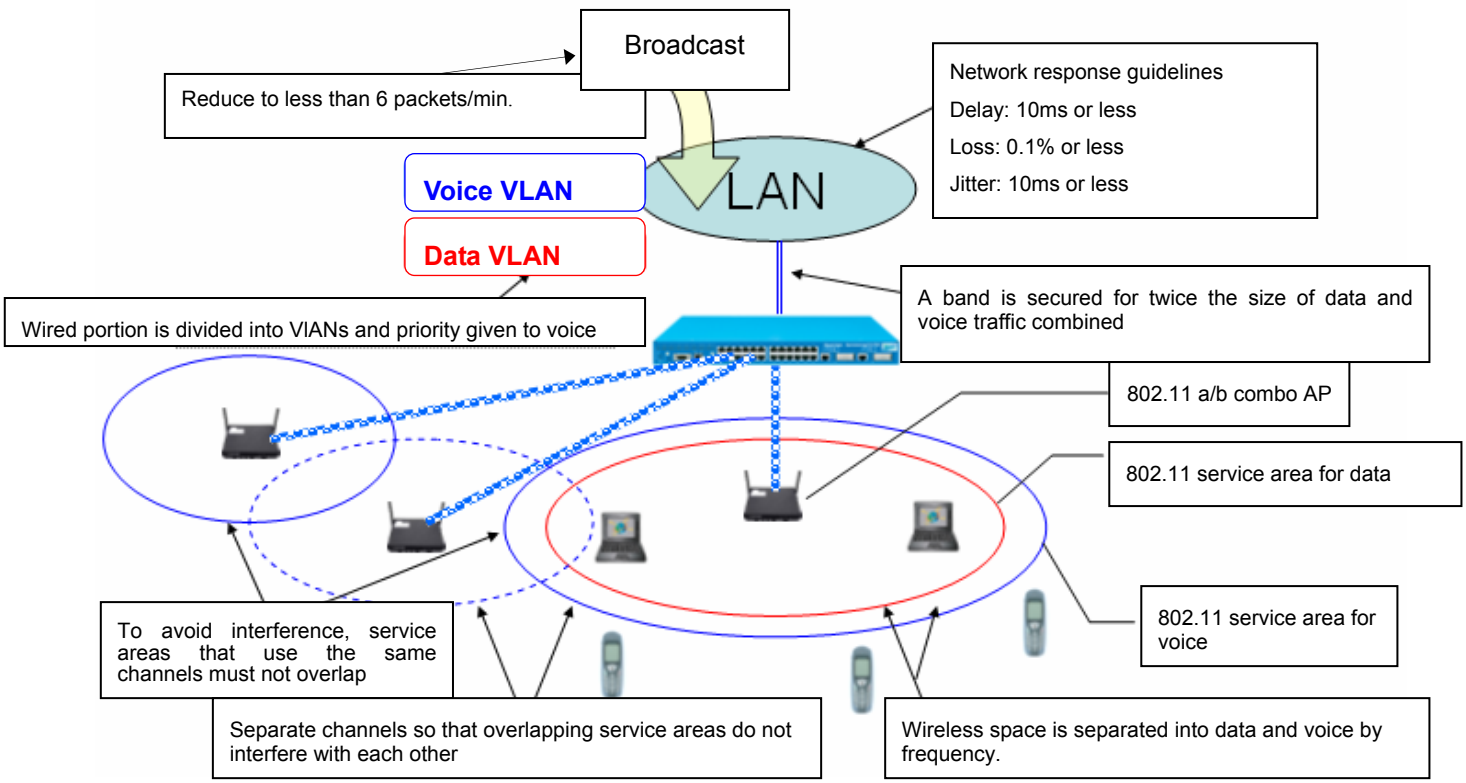
*2 ITU-T G114 (One Way Transmission Time) Recommendations regarding Delays

0 to 150ms: Acceptable by a majority of users.

150 to 400ms: Acceptable when the manager understands the effect of delays on product quality.

Over 400ms: Not acceptable under normal circumstances

[Figure. WirelessIP5000-A Network Summary]



4. Network Operation Design

4.1 Network Operation Design Guidelines

(1) IP Addresses

Taking mobility into account, we recommend automatic address allocation using DHCP.

If you choose to use static IP addresses for some terminals, you will need a way to operate without changing those terminals' IP addresses within the wireless LAN service area (L2 handover).

(2) Wireless LAN Security

This consists of the authentication method to connect to the wireless LAN and encryption in the wireless service area.

ESSID: Key code to access the wireless LAN.

The terminal and the AP must agree on the code in advance. For security reasons, we recommend stealth mode, in which the AP does not announce the ESSID.

WEP: Basic coding technology for wireless LAN's. Generally, 64-bit and 128-bit modes are used. As these keys are fixed, the coded key data must be set on the AP and terminal. We recommend 128-bit mode.

WPA (TKIP):

A wireless LAN data encryption method that uses RC4 algorithm, the same algorithm used in conventional WEP published in October 2002 by the Wi-Fi Alliance, a wireless LAN standards organization).
WirelessIP5000-A supports WPA -PSK and WPA-EAP.

WPA2 (AES):

A wireless LAN data encryption method that uses AES algorithm.
WirelessIP5000-A supports WPA2-PSK and WPA2-EAP. (PMK Cache is available.)

802.1x: Authentication method established by IEEE. Although there are multiple methods, WirelessIP5000-A supports the following modes. All of these need an authentication server.

1. EAP-MD5
2. EAP-TLS
3. EAP-PEAP
4. EAP-TTLS

Although EAP-TLS has the highest security level, it necessitates a system to produce certification data in addition to an authentication server, placing additional burden on user operation.

In addition, as we will discuss later, authentication is necessary at handover, which causes connection to be interrupted for roughly 2 - 3 seconds.

(3) QoS (wired)

To ensure call quality in voice communication over IP networks, we recommend managing packet priority using QoS.

On the WirelessIP5000-A, the ToS (Type of Service) within IP packets can be set as desired. To set this, convert the upper 6 bits of the ToS value to decimal, and set the entries shown below to the result.

DSCP (Diffserv Code Point) refers to the upper 6 bits of the TOS field.

(Example) [NETWORK]

DiffServ Signal = 40 (DSCP setting of the SIP packet)

DiffServ Media = 40 (DSCP setting of the RTP packet)

↑ Convert the upper 6 bits into decimal

ToS value used for the settings: 1 0 1 0 0 0 0 0 (binary)

(4) QoS (wireless)

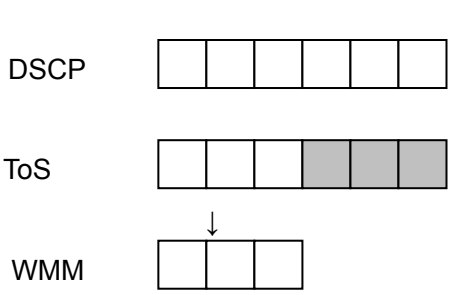
WirelessIP5000-A supports the QoS of wireless zones created by Wi-Fi multimedia (WMM).

The following is an explanation of mapping specifications to DSCP and WMM AC when WMM is enabled.

DSCP and WMM AC Mapping Specifications

You can set DSCP from the Network menu. The upper 3 bits of this DSCP are designated as WMM priority bits. In other words, the set value is the one when DSCP is recognized as a ToS field.

Also, since WMM calls for Voice Priority = 6, 7 (refer to the WMM White Paper excerpt), when WMM is enabled, you must use a DSCP setting of 0x30 (110 000) or higher.



DSCP	Precedence of ToS	WMM（802.1d priority）
0x00(000 000)	0	0
0x08 (001 000)	1	1
0x10(010 000)	2	2
0x18(011 000)	3	3
0x20(100 000)	4	4
0x28(101 000)	5	5
0x30 (110 000)	6	6
0x38 (111 000)	7	7

Refer to the WMM White Paper excerpt

Access Category	Description	802.1d Tags
WMM Voice Priority	Highest priority Allows multiple concurrent VoIP calls, with low latency and toll voice quality	7, 6
WMM Video Priority	Prioritize video traffic above other data traffic One 802.11g or 802.11a channel can support 3-4 SDTV streams or 1 HDTV streams	5, 4
WMM Best Effort Priority	Traffic from legacy devices, or traffic from applications or devices that lack QoS capabilities Traffic less sensitive to latency, but affected by long delays, such as Internet surfing	0, 3
WMM Background Priority	Low priority traffic (file downloads, print jobs) that does not have strict latency and throughput requirements	2, 1

We recommend the following settings.

(Example of recommended settings)

When the WI-100HC is configured to a setting other than DSCP = 8 - 63, set WMM (802.1d priority) to 6.

When the WI-100HC is configured to a setting other than DSCP = 0 - 7, set WMM (802.1d priority) to 0.

Set the DSCP default value to 32 (however, 0x30 or higher is acceptable).

[TOS_WMM]

Precedence_0=0

Precedence_1=6

Precedence_2=6

Precedence_3=6

Precedence_4=6

Precedence_5=6

Precedence_6=6

Precedence_7=6

[NETWORK1]

WMM=1

DiffServ_Signal=32

DiffServ_Media=32

4.2 Handover Methods

Separate transitions on the same subnet (L2 level) and transitions between different subnets (L3 level). We recommend handover using the L2 level when operating on the same LAN (within structures, buildings, etc.)

Estimated Changeover Time (WEP use)

Method	Conditions	Classification	Imple-mented	Estimated Changeover Time
Stand Alone-type AP	L2 Level Placed on the same subnet	Phone conversation	○	Over 300 ms
	L3 Level Placed on a different subnet	Phone conversation	×	－ *L3 level handovers during phone conversations are not supported.
		Standby	○	Can be operated by DHCP
Solution-type AP	L2 Level Placed on the same subnet	Phone conversation	○	About 100 - 300 ms * Differs by system.
	L3 Level Placed on a separate subnet.	Phone conversation	○	About 100 - 300 ms *AP supports the MobileIP function. As the terminal operates without changing the IP address, in essence the terminal operates in a similar fashion to L2.
		Standby	○	
	Operates multiple AP's on the same CH (With Meru Networks, this is called Virtual AP (proprietary)).	Phone conversation	○	The AP arbitrarily switches without the terminal performing a handover.
		Standby	○	

*Supplemental Information

■ Solution type: WLAN controller-type AP.

■ Stand-alone type: Non-WLAN controller-type AP.

4.3 Network Operation Checklist

Design the network operation having considered the following.

No.	Item	Operating Conditions (Example)	Remarks
1	IP Addresses	Use DHCP only for voice VLAN. The terminal can still be used when it is carried into a location with a different network environment.	
2	Wireless LAN Security	Use WEP 128bit. For access control over the network, permit access only to the networks required by the terminal such as between voice VLANs, IP-PBX, SIP servers.	
3	Handover	Use L2 handover within a same structure. Include environments with IP tunneling where handover without IP address change is possible, such as Solution-type L3 level. Limit L3 level transfer to transfers between offices, and operate using DHCP.	

5. Ensuring Call Quality

5.1 CODEC (Speech Encoding)

The WirelessIP5000-A supports the following CODECs.

You can set the priority (priority 1 - 3) and RTP transmission intervals (20 ms - 40 ms) to match the system configuration.

CODEC	Encoding	Transmission Interval	Bit rate
G711-µLaw	PCM	20 ms - 40 ms	64Kbps
G711-ALaw	PCM	20 ms - 40 ms	64Kbps
G729	CS-ACELP	20 ms - 40 ms	8Kbps

- PCM System (G711)

  This is a major system in voice coding and is also used in coding music CD's. The sound quality is considered to be superior to the CELP System (G729). However, the transmitted and received data size is larger than the G729. At larger bandwidths, the number of concurrent calls that can be handled by one access point is less than for the G729.

- CELP System (G729)

  This system converts voice into patterns and sends code corresponding to the individual patterns. The voice quality is considered to be inferior to the PCM system (G711), in which the speech waveforms are faithfully digitized. However, as the voice compression rate is high, and the necessary bandwidth is narrow, the number of concurrent calls that can be handled by a single access point is greater than for the G711.

5.2 Jitter/Jitter Buffer

- **Jitter (Fluctuation)**

  Jitter refers to the irregular arrival of packets due to network delays. At times, this causes interruptions in sound. It is generally accepted that problems occur with the voice signal when the delay time exceeds 150 ms. According to the ITU-T G114 recommendations:

Delay	
Less than 150ms	Acceptable for a majority of user applications.
150ms ～ 400ms	Acceptable if users are made aware of delays in advance.
Over 400ms	Generally not acceptable.

- **Jitter Buffer**

  The jitter buffer refers to a buffer that absorbs jitters. This function temporarily stores received data (RTP packets in the case of voice calls) in a buffer and transfers the voice packets to the call terminal at fixed intervals (RTP transmission intervals). Although increasing the buffer value reduces jitters, it also increases the delay in voice transmission.

  You can change the jitter buffer size for the WirelessIP5000-A using the following parameter.

  [NETWORK1]

  Jitter_Buffer_Size=60

  Default = 60 Settable Range: 20 - 200 ms

  * When using the WirelessIP5000-A, we recommend a jitter buffer size of 3 times the value of the RTP transmission interval.

  (Example) Codec: G711 40ms

  Jitter Buffer: 120ms

5.3 RTP/RTCP

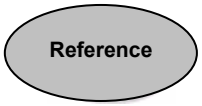
5.3.1 RTP (Real-time Transport Protocol)

This is a data transfer protocol that delivers voice and images in real time. As this is a UDP protocol, there may be packet loss and transmission times cannot be guaranteed.

5.3.2 RTCP (RTP Control Protocol)

RTCP is a session control protocol to transmit and receive data using RTP.
RTCP is used in combination with RTP to control data flow (transmission/reception) and manage the sender and receiver information.

The receiver of the data stream can adjust the transmission rate of the sender by periodically transmitting RTCP packets.



・ The related entries in user.ini are as follows.

```
---------------------------------------------------------------------
[RTP_RTCP]
Use_RTCP=1          … RTCP used/not used
RTP_Port_Min=9000          … Min. port used by RTP/RTCP
RTP_Port_Max=9020    … Max. port used by RTP/RTCP
RTCP_Report_Interval=5000 … transmission interval of RTCP Report
RTCP_CNAME=WirelessIP5000-A … RTCP CNAME
settingsLast_RTP_Received_Timeout=0 … disconnect call if the RTP does
                                                    not receive for this length of time
---------------------------------------------------------------------
```

5.3.3 Used Port

RTP/RTCP selects the port to use from the set values (Min and Max).
The RTP always uses an even numbered port and the RTCP always uses an odd numbered port.

Set the WirelessIP5000-A to use ports 9000 - 9020 (defaults).

5.3.4 SR Report

Of the RCTP packet formats, the WirelessIP5000-A supports SR (sender report).

The SR packet formats sent by WirelessIP5000-A are as follows.

[Figure. SR Packet Format]

```
UDP - User Datagram Protocol
  Source Port:          9001
  Destination Port:     9001
  Length:               88
  Checksum:             0xB642
RTCP SR - Real-time Transport Control Protocol Sender Report
  Version:              2
  Pad:                  0
  RR Count:             1
  Payload Type:         200  SR - Sender Report
  Packet Len:           12
  Sync Src ID:          813295981
  NTP Timestamp Hi:     0x83AB446F Thu Jan 01 23:04:31 1970
  NTP Timestamp Lo:     515396040  fraction
  RTP Timestamp:        0x00008FC0 Fri Feb 08 01:41:36 2036
  Sender Pcket Cnt:     230
  Sender Octet Cnt:     36800
RTCP Reception Report Block #1
  Source ID:            661989574
  Fraction Lost:        0
  Cumulative Lost:      0
  Ext High Seqence:     0
  Interarrival Jitter:  14
  Last Sender Report:   2101886320
  Delay Since Last SR:  22282
RTCP SDES - Real-time Transport Control Protocol Source Description
  Version:              2
  Pad:                  0
  Chunk Count:          1
  Payload Type:         202  SDES - Source Description
  Packet Len:           6
RTCP Source Descriptor Chunk #1
  SSRC/CSRC ID:         813295981
  SDES Type:            1  CNAME - Canonical Name
  SDES Length:          14
  SDES Name:            WirelessIP5000
  SDES Type:            0  END - End of SDES List
  Alignment Pad:        0x7D7977
```

5.4 Number of Concurrent Calls

Large delays in voice packets and packet losses will occur when concurrent calls at a single access point increase and the limits of the wireless bandwidth and packet processes of the access point converge. When this happens, voice quality deteriorates noticeably.

Accordingly, when designing a wireless network, you must take into account the number of terminals that may connect to a single access point at the same time.

The following table is a rough guide to the number of terminals that can be handled concurrently when using the WirelessIP5000-A.

Codec	RTP Transmission Interval	Estimated Number of Concurrent Calls
G711	20 ms	6 calls - 12 units
	40 ms	8 calls - 16 units
G729	20 ms	9 calls - 18 units
	40 ms	11 calls - 22 units

※ The above numbers are rough guidelines. Actual numbers that can be handled may vary according to the access point.

6. Handover Operation

6.1 L2 Handover

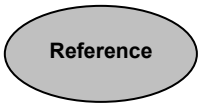
Handover occurs when the WirelessIP5000-A physically moves into the service area of a different AP (allocated to the same subnet as the AP from before the move), within the wireless area. The same operation applies when, as with Solution-type L3 level, handover is accomplished without changing the IP address through IP tunneling.

The handover conditions of the WirelessIP5000-A are displayed as follows.

Conditions for Handover

(1) Signal Strength

The WirelessIP5000-A measures the transmission strength received from the AP it is connected to, and switches to scanning when the strength is below a certain threshold.



・ The related entries in user.ini are as follows.

```
---------------------------------
[ROAMING]
Try_Beacon_Signal_Level=
Try_Rx_Signal_Level=
Level_Diff_Higher_Than_Curr_Site=
---------------------------------
```

・ The strength of the received signal is computed by monitoring the received packets and averaging over 8 packets.

・ When the signal strength indicates that a handover should occur, an "Authentication+Association" handover is executed.
(Re-association is not supported.)

(2) Communication Status

The WirelessIP5000-A checks packet transmission and receiving error statuses and switches in reponse to the latter.

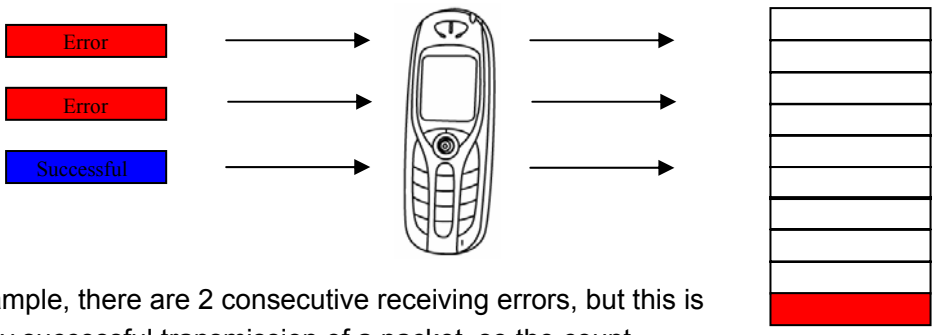
Reference

・ The related entries in user.ini are as follows.

[ROAMING] Try_Over_TxError_Count=10… number of retries when Ack is not returned.

(Example)

When the TxError count value is set to 10 and there are 10 consecutive receive errors, the mode goes into switching operation. Count is decremented when a packet is received successfully.



In this example, there are 2 consecutive receiving errors, but this is followed by successful transmission of a packet, so the count becomes 1.

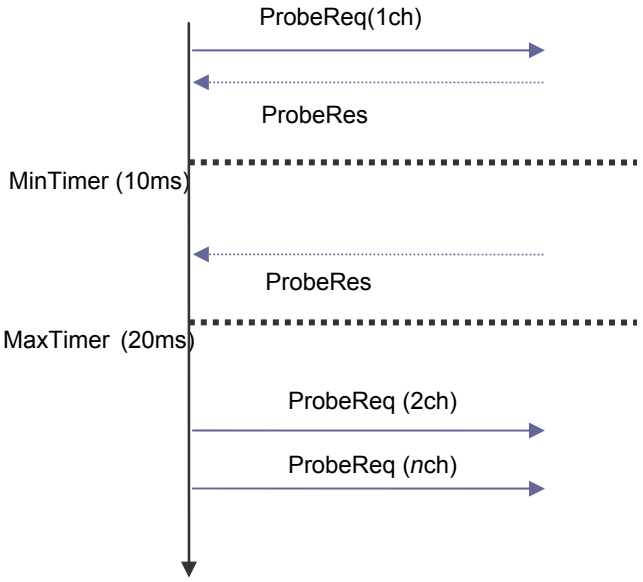
・ When the condition for handover is satisfied, the association with the current AP is cancelled (de-authentication) and handover is done through Association.

Switching Operation

Handover operates as follows.

1. When the aforementioned handover conditions are satisfied, WirelessIP-5000-A scans for APs.

[Figure. AP Scanning Logic]



- If ProbeRes returns before MinTimer, standby until MaxTimer and start scanning the next channels.
- If ProbeRes does not return before MinTimer, start scanning the next channels.
- After completing the scans of all the channels, connect to the AP with the best signal.

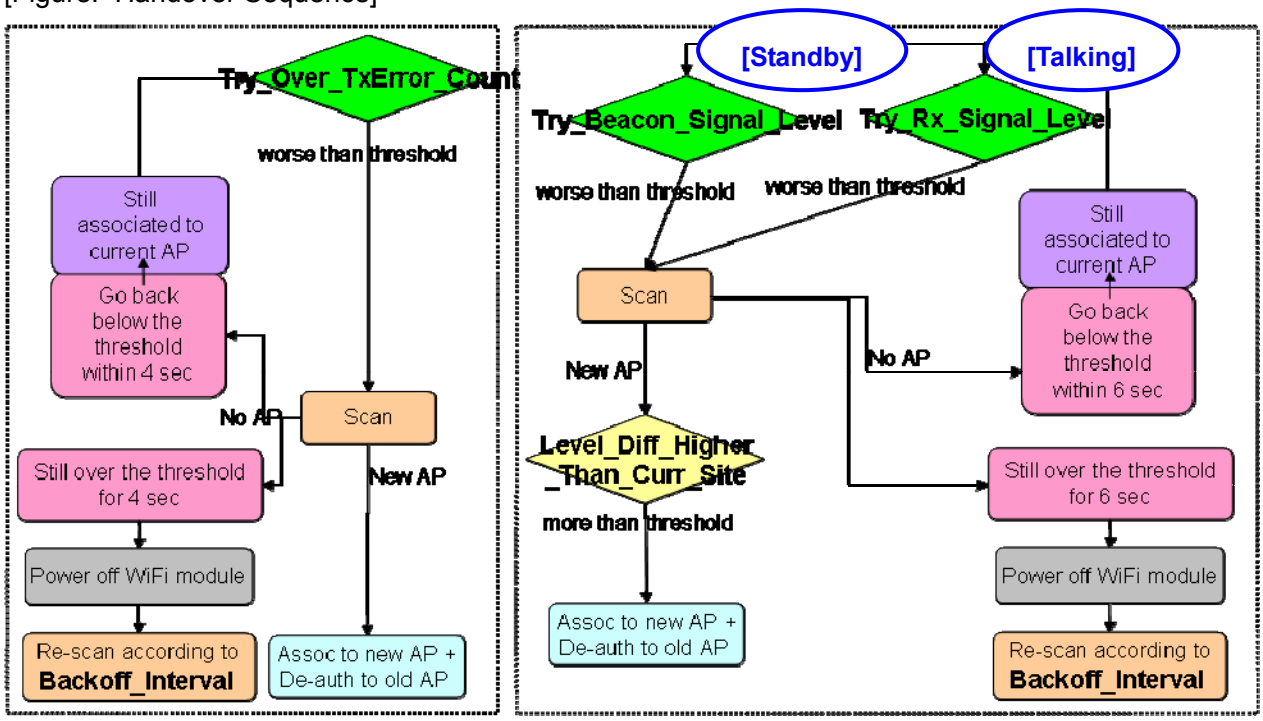
2. As a result of scanning, if one of the APs with the same SSID has a signal level that is a set amount higher than the current AP, the WirelessIP5000-A switches to that AP.

Switching time is the time from when scanning begins to when the switch to the new AP is complete.

Caution

This operation may change without notice.

[Figure. Handover Sequence]



6.2 L3 Handover

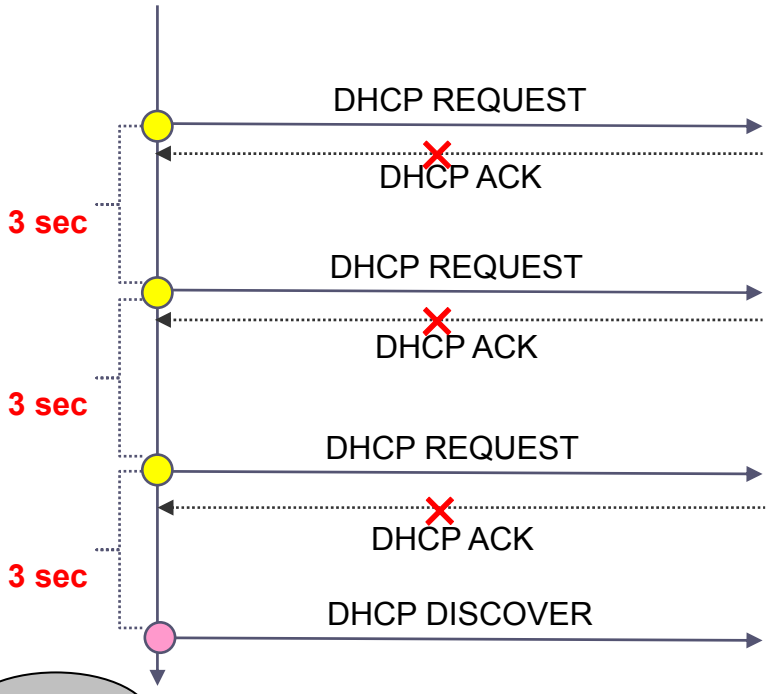
WirelessIP5000-A is compatible with the L3 environment handover. L3 handover occurs when the WirelessIP5000-A physically moves into the service area of a different AP (allocated to a subnet other than that of the current AP), within the wireless area. The IP address of the WirelessIP5000-A needs to be set to DHCP when conducting L3 handover.

[Figure. L3 Handover Sequence]

(1) Send a DHCP REQUEST at intervals set as an AP attribute.

(2) If no DHCP ACK is received or if DHCP NACK is received, DHCP REQUEST is resent only for the number of times specified as a parameter, and the old address is released.

(3) Send DHCP DISCOVER and acquire the IP address of the AP segment of the new physical location.



Reference

・ The related parameter values of the user.ini files are as follows.

```
-----------------------------------------------------------------
[DYNAMIC_NETWORK]
DHCP_Verify_Count=3
DHCP_Verify_Interval=3
-----------------------------------------------------------------
```

* When these parameters are used, send the DHCP REQUEST for L2 handovers as well.

・ When DHCPVerifyCount = 0, the time for reacquiring DHCP is the time the device returns to the AP from DHCP lease timer, NetworkFail status.
・ Using the these settings, reacquiring the address takes a minimum of 9 seconds.

7. WirelessIP5000-A Installation Procedures

Once the network design is complete based on the previous sections, use it to add the WirelessIP5000-A. In this section, you will find basic information you need to use the device. The WirelessIP5000-A User.ini Manual explains all of the possible settings.

7.1 WirelessIP5000-A Settings

7.1.1 Network Environment

(1) Wireless LAN

1) Wireless LAN Mode

As the wireless LAN uses the access point, set it to infrastructure mode.

2) SSID

Set the SSID to the one set in the wireless LAN access points.

(2) TCP/IP

1) Using DHCP

Set to “Use” when using DHCP.

2) IP Address

Set the IP address, netmask, gateway address, address of the DNS server, etc., when not using DHCP.

(3) WEP

1) Using WEP

Set to “Use” when using WEP.

2) Configuring the number of WEP bits

This is set only when using WEP. We recommend setting it to 128 bit.

3) Default Key ID

Set to the WEP key number to use.

4) WEP Key 1 - 4

Set the number key specified in 3). Enter using ASC + ASCII characters or HEX + hexadecimal format.

(4) Authentication

1) Mode

This specifies whether to use authentication, and the method to use when it is used.. When you use EAP-TLS, EAP-PEAP, or EAP-TTLS, the certification data must be entered on the WirelessIP5000-A.

2) Number of WEP bits

This is set only when using WEP. We recommend setting it to 128 bits.

3) Default Key ID

Set to the WEP key number to use.

7.1.2 SIP Environment

7.1.2.1 SIP Summary

The SIP consists of the user agent (client terminal) that requests connections and the SIP server that connects in response to the request.

Typically, the SIP server is made up of

1) Proxy server

2) Redirect server

3) Registrar server

1) Proxy server

The proxy server is an agent for connection requests between terminals, similar to Web proxy servers. It receives requests from user agents and other proxy servers and transfers them to other user agent servers, and sends responses to other user agents.

The proxy server performs the necessary processing on requests from user agents and sends the request to the next address, but does not generate requests.

2) Redirect server

The redirect server differs from the proxy server in that it does not transfer or relay requests. It receives requests from user agent clients and proxy servers and passes back the responses.

3) Registrar server

The registrar server receives requests to register IP addresses, phone numbers, and other information from user agents. It helps to prevent unauthorized use of the SIP network by changing and deleting registered information, and not only registering, but also authenticating user agents.

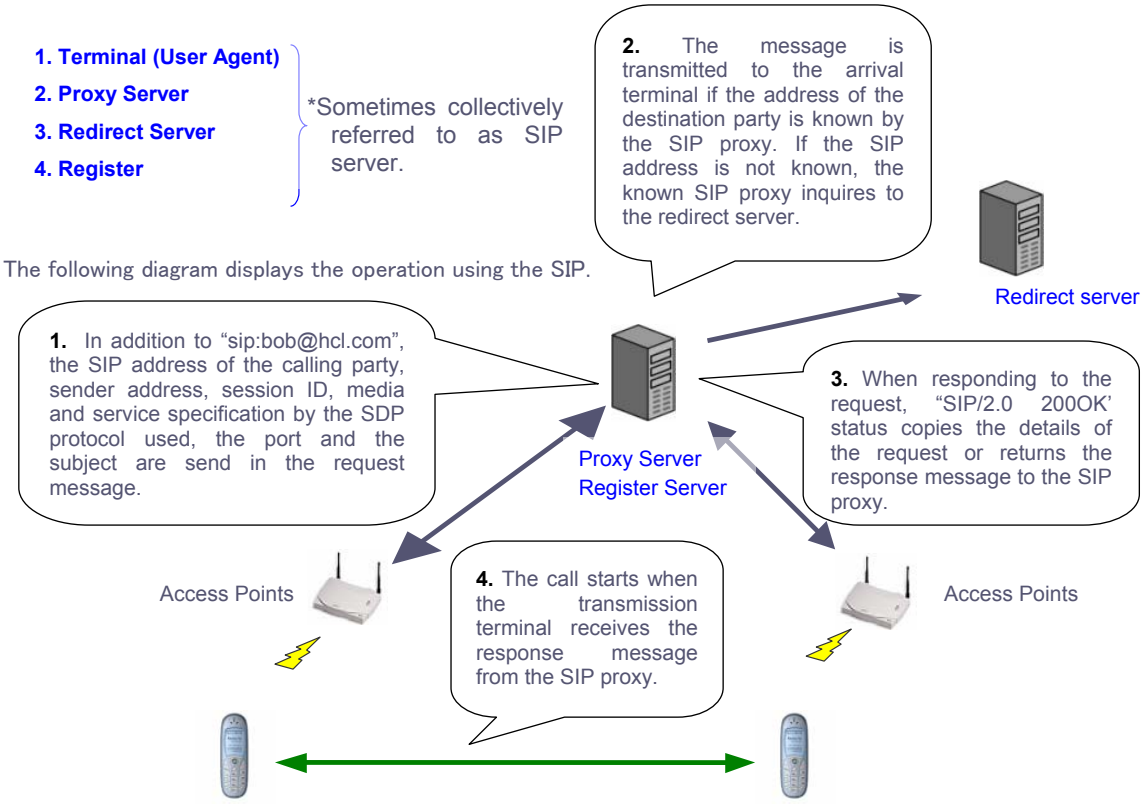
SIP Operation Summary

Main components when configuring a system

1. Terminal (User Agent)
2. Proxy Server
3. Redirect Server
4. Register

*Sometimes collectively referred to as SIP server.

The following diagram displays the operation using the SIP.



(1) Primary Server

1) Domain

Set the primary SIP server information. Enter in domain format or as an IP address. If you enter this in domain format, the IP address is resolved by inquiry to the DNS server.

2) Registrar

Set the IP address of the registrar server.

* If all of the functions are performed by the same server, set only the domain information.

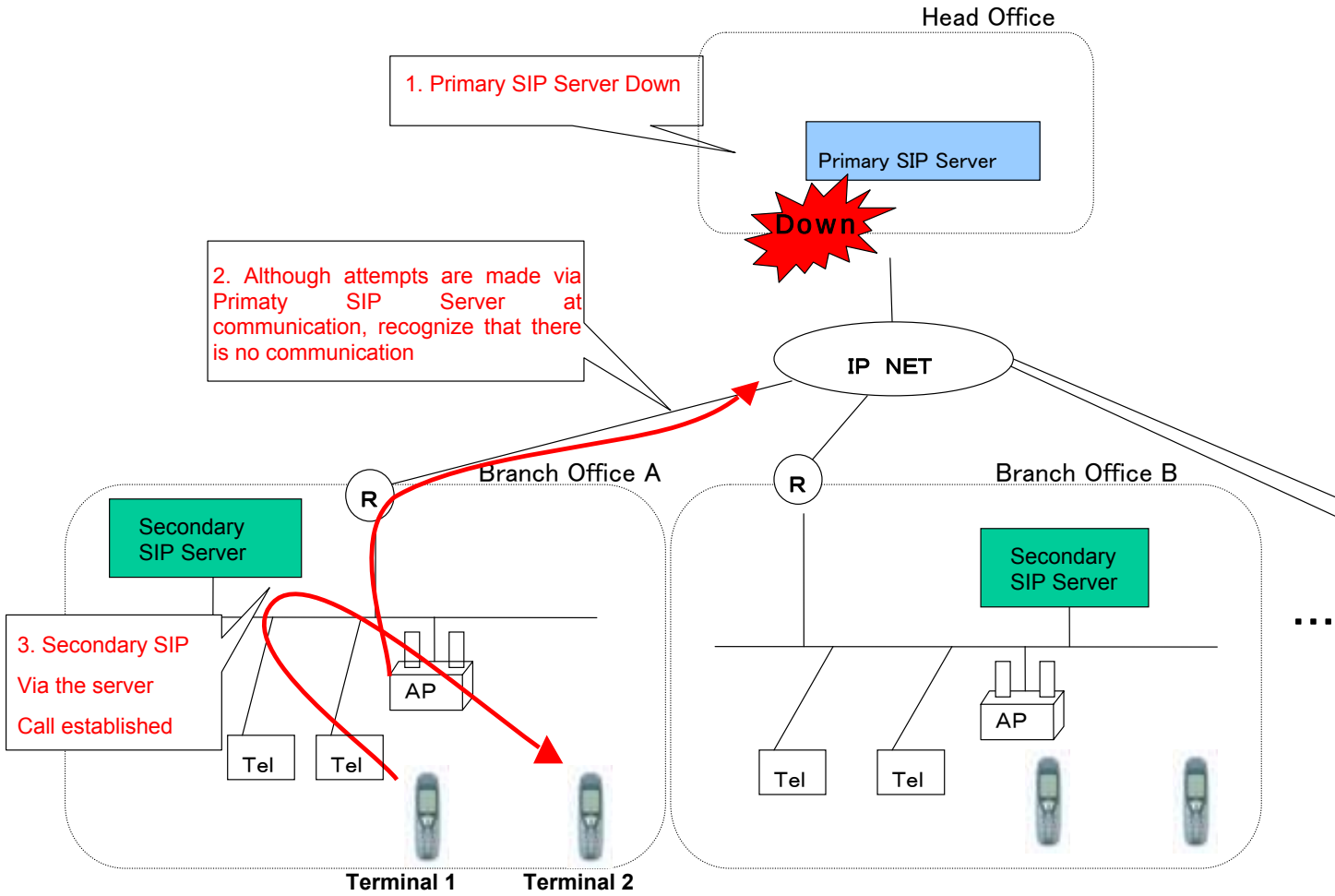
*Outbound Proxy

Set using the network settings.

(2) Secondary Server

The support of the secondary server depends on the operation of the server system.

[Figure. Example of a Redundant Configuration



1) Domain

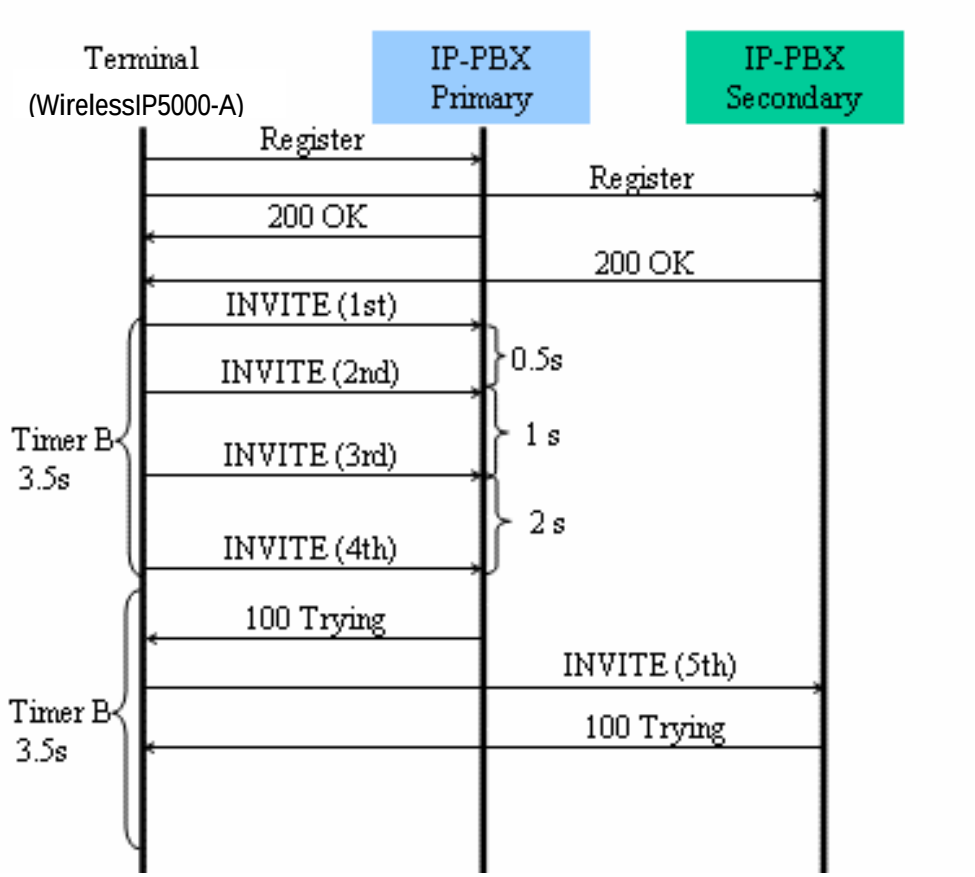
Set the secondary server information. Set it in the same way as the primary server.

2) Registrar

Set the IP address of the secondary registrar server. Set it in the same way as for the primary server.

[Redundancy Configuration Operation]

The redundancy operation is different for every system, but basically works as follows.



When the primary goes down, retransmission to the primary is conducted for TimerB (3.5s), and an INVITE is sent to the secondary if there is no response.

INVITE recipient priority for the terminal Regist status.

No	Register		INVITE	
	Primary	Secondary	Primary	Secondary
1	○	○	Priority 1	Priority2
2	○	×	Priority 1	×
3	×	○	×	Priority 1
4	×	×	×	×

(Example of User.ini/Web-Config-Tool Settings)

When Primary Proxy Server/ Register Server ＝10.1.1.100

and Secondary Proxy Server/ Register Server = 192.168.1.100

[SERVER_SETTINGS]
1st_Proxy=10.1.1.100 → Primary Proxy Server IP Address or FQDN

1st_Registrar=10.1.1.100 → Primary Register Server IP Address or FQDN

2nd_Proxy=192.168.1.100 → Secondary Proxy Server IP Address or FQDN

2nd_Registrar=192.168.1.100 → Secondary Registry Server IP Address or FQDN

Domain_Realm=voip.hitachi-cable.co.jp → SIP Domain Name →

[REDUNDANCY]

Mode=0(Registration Oriented Mode) → Redundancy format

Request_Timeout=4000 → Wait time until primary down

Use_Fixed_Primary_Server=1 → Whether or not to fix primary

Use_DNS_Additional_Records=1 → Whether or not to use redundancy

---

(3) Alias

1) URL Scheme

Select SIP or TEL format.

2) Displayname

Specify the display name. This is shown on the standby display of the terminal.

3) UserInfo

Set the user information (phone number, extension number, etc.) to register to SIP.

(4) Authorization

1) Username

Set to the user ID used for SIP authentication.

2) Password

Set to the digest authentication password for the user ID.

(5) Expire

Configure the expiration of the various timers. (unit: seconds)

1) Regist Expire

Set the expiration of the registration. WirelessIP5000-A executes the re-registration process at an interval of one half of this setting. If a value is specified on the server side, the interval is based on the server side setting.

2) Session Expire

Set the expiration of the SIP session. WirelessIP5000-A executes the re-invite process at an interval of one half of this setting. If a value is specified on the server side, the interval is based on the server side setting.

3) Presence Expire

Set the resend interval at which to send subscription for presence registration using the presence function. WirelessIP5000-A executes the re-registration process at an interval of one half of this setting.

You may need to set other Expires to match the system.

7.1.3 Time Display

As WirelessIP5000-A does not store the time, it sets the time to the default of “1970-01-01 9:00” when restarting.

We recommend that an external source (NTP/SIP Date header) be consulted for the time.

After the power is turned on, the timing of the terminal regarding the change in time is as follows.

(1) When acquiring the time from NTP.

(2) When acquiring the time from the SIP REGISTER (200OK) packet.

(3) When the user changes the time from Menu -> Setup -> Advanced -> Time -> Current time.

Reference

・ If NTP is set to “Disabled” in the terminal settings, the WirelessIP5000-A obtains the time from the date header if a date header is included in the SIP REGISTER packet.

・ The NTP clock synchronization repeats at the interval in the following User.ini setting.

[TIME]

NTP_Refresh_Interval=7200

7.1.4 Hold Method

WirelessIP5000-A supports the following 4 hold types.

1. Mixed (compatible with both RFC2543 and RFC3264)
2. RFC2543
3. RFC3264
4. RTP (deemed) hold

Reference

・RTP (deemed) hold cannot be used with the G729 codec.

Configure the WirelessIP5000-A User.ini (or Web-Config-Tool) as follows.

[HOLD]

Mode=0 (Mixed)

Mode=2543 (RFC2543)

Mode=3264 (RFC3264)

Mode=1 (RTP hold)

2. Mode=2543 (RFC2543)

This uses the Connection-Address (c=0.0.0.0) within the SDP of the re-invite sent from the WirelessIP5000-A to implement a hold.

3. Mode=3264 (RFC3264)

This operates according to RFC3264 (An Offer/Answer Model with the Session Description Protocol) and implements a hold using attributes such as “a=sendonly”, a=recvonly, a=inactive, of the SDP within an invite.

4. Mode=1 (RTP hold)

This implements a hold by sounding the hold tone at the hold terminal rather than setting the destination for the hold tone using re-invite.

7.1.5 DTMF

DTMF stands for Dial Tone Multi Frequency. This is the sound you hear each time you press a button on a telephone, and is sometimes called a push tone or tone signal. 2 tones with different pitches are emitted when one button is pressed. The exchange determines the phone number based on the signal tone. As one tone is selected from among 4 high pitched tones and another from among 4 low pitched tones to create each sound, there are 16 possible combinations, which represent the numbers 0 to 9, symbols * and #, and the letters A to D.

WirelessIP5000-A supports the following 4 DTMF types.

1. RTP
2. SIP-INFO
3. RFC2833
4. RTP＋SIP-INFO

Configure the WirelessIP5000-A User.ini (or Web-Config-Tool) as follows.

[DTMF]

Mode=0 (RTP)

Mode=1 (SIP-INFO)

Mode=2 (RTP2833)

Mode=3 (RTP+SIP-INFO)

1. Mode=0 (RTP system)

This sends DTMF information as sound source information using RTP packets.

2. Mode=1 (SIP-INFO system)

This sends DTMF information as SIP-INFO.

3. Mode=2 (RFC2833 system)

This sends DTMF information by including it in the Payload of the RTP.

4. Mode=3 (RTP＋SIP-INFO system)

This simultaneously transmits the RTP and SIP-INFO methods.

7.1.6 Bell/Vibrator Selection

These modes can be selected separately for EXT1, EXT2, INT1 and INT2, and the ring tone, ring mode, and LED can be set separately for each line. To distinguish ring tones, the value set on the WirelessIP5000-A must match the value set on the SIP server.

Use the same value for the WirelessIP5000-A User.ini (or Web-Config-Tool) as the SIP server (Alert-info) setting. (The following are sample settings.)

[RING]

ID_String_External1=External1

ID_String_External2=External2

ID_String_Internal1=Internal1

ID_String_Internal2=Internal2

ID_String_Silence=Silence

1. ID_String_External1

   The string for the EXT1 ring tone.

2. ID_String_External2

   The string for the EXT2 ring tone.

3. ID_String_Internal1

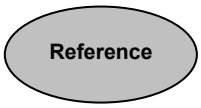
   The string for the INT1 ring tone.

4. ID_String_Internal2

   The string for the INT2 ring tone.

5. ID_String_Silence

   The string for the silent mode.



If the incoming call has no identification, the ring tone set for EXT1 will sound whether the call is internal or external.

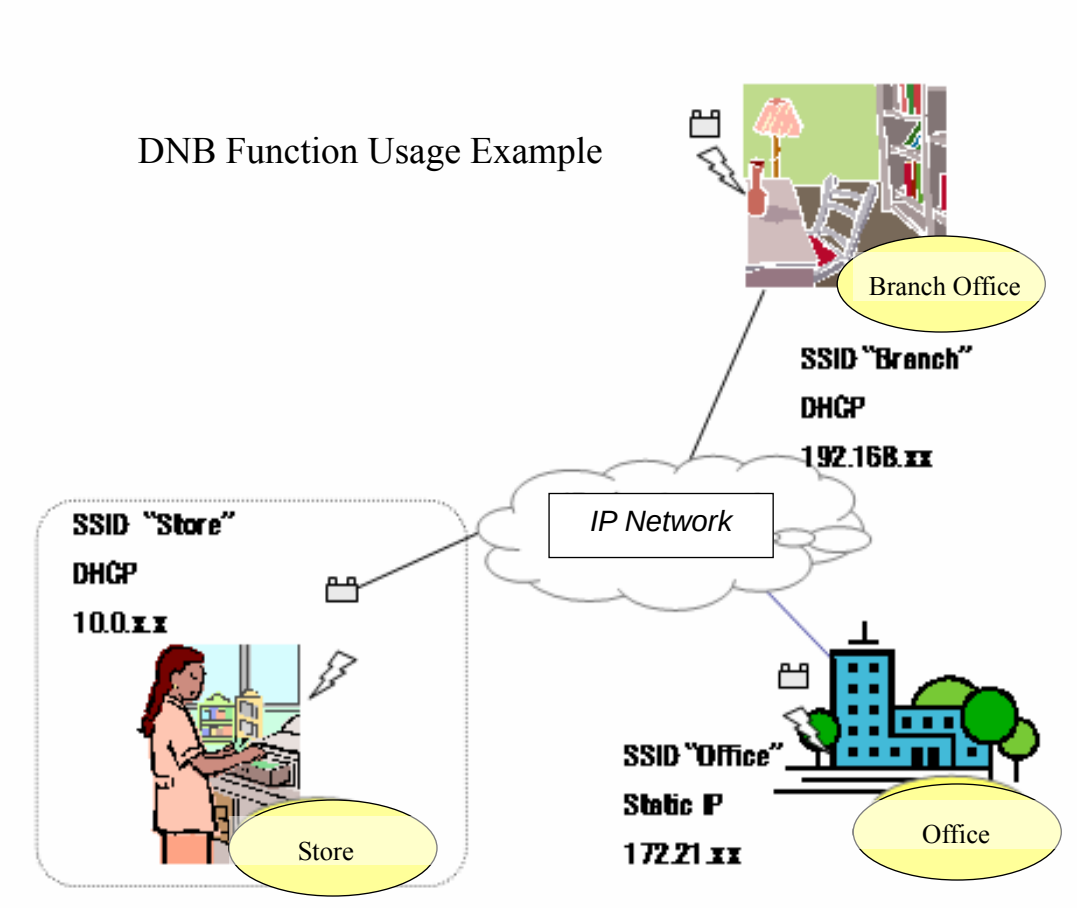
7.2 Operating in a Multiple Network Environment

The following explains the settings of the WirelessIP5000-A when it is moved between offices with different network settings. This function is called DNB (Dynamic Network Binding).

For example, when a WirelessIP5000-A that is used at Office A is to be also used at Office B, then the WirelessIP5000-A can be used by configuring the network settings to match the operation of the wireless LAN for the two offices. But in the past, if the offices used different network types (for example, Office A uses DHCP and Office B uses static IP), the settings of WirelessIP5000-A had to be changed. Once the settings for the different networks are stored in the WirelessIP5000-A, the DNB function can automatically switch the network settings on the WirelessIP5000-A.

* The DNB function can be configured with up to 5 network settings. The profile to connect is automatically selected using priorities assigned to each profile.

The following is an example of settings and operation.



As shown above, the DNB function is used when the networks of the different offices are of different types. The WirelessIP5000-A uses the network settings corresponding to the access point SSID at each office.

The SSID of the network settings set by the user is the basis for selecting the access points to try to connect to when scanning for access points. Of the network settings set in advance by the user, those with the corresponding SSIDs are the targets for association. For example, if a user has set up three SSID settings as Office, Store, and Branch, the access points with these three SSIDs among those detected during scanning will be the targets for association. If association is successful with one of these access points, the WirelessIP5000-A can operate with the correct network settings.

If access point is not found or Association fails for all access points, it enters the Wi-Fi energy-saving state.

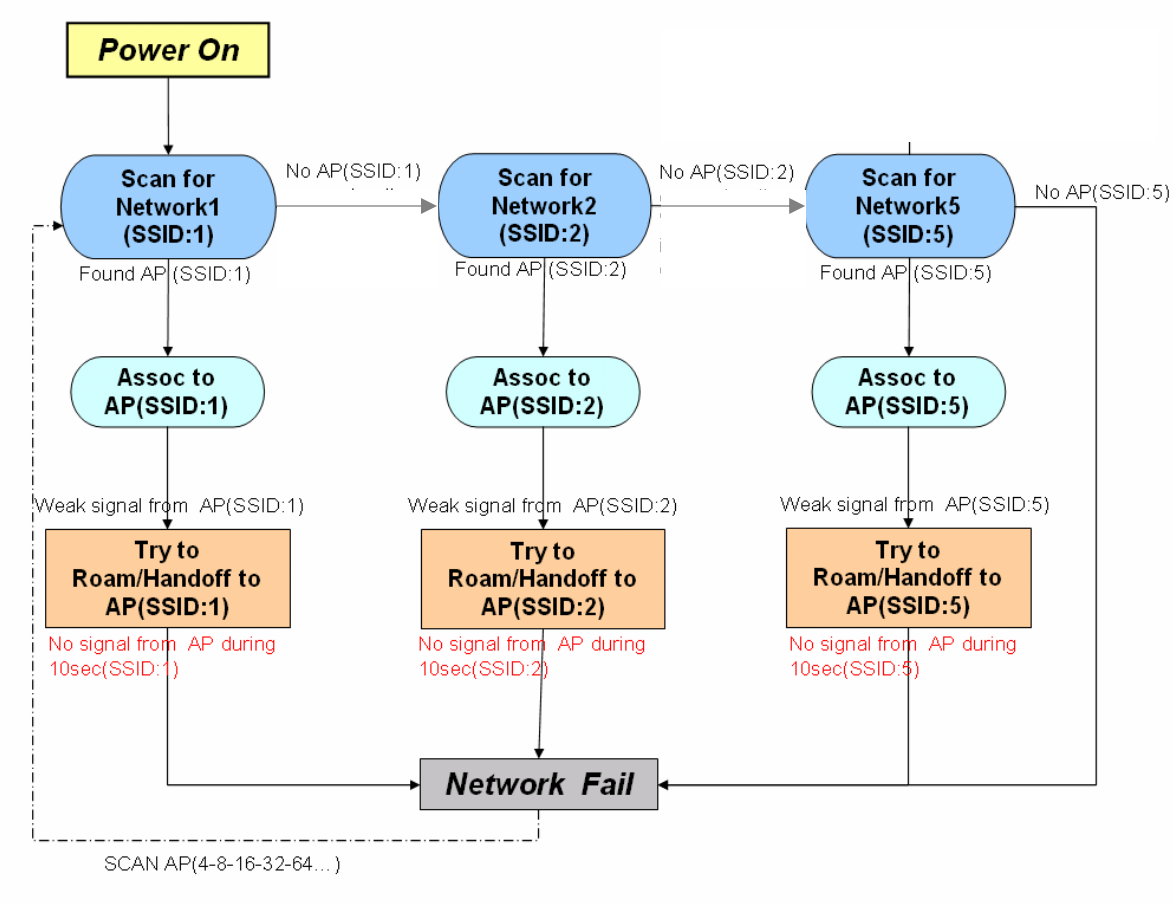
Caution

- Use in an environment where several of the profiles (SSID) set in the terminal are present, is not supported.
- Depending on the number of profiles that are set, the battery standby time of the WirelessIP5000-A may differ from specification.
- The auto-switching of profiles is carried out only when the terminal goes outside the range of the connected network.
- Handovers between different networks (profiles) (ESSID) is not supported. Also, because the terminal does not go out of range, handovers (switchover by standby transfer) is not possible. You must end the phone call and reboot the terminal.

Reference

- Although it is possible to have multiple network profiles (5), the terminal's phone number is common to all of them.

[Figure. DNB Sequence]



7.3 Handover Settings

Handover may require that the WirelessIP5000-A's wireless LAN parameters be adjusted to conform to the wireless LAN system to be used. Here, we explain the basic concepts.

See 6.1 L2 Handover for a discussion of settings related to handovers.

(1) Standalone type

The access points of standalone type operate independently. Accordingly, handover between these access points happens through the operation of the WirelessIP5000-A. Normally, the occasion for the switching operation is triggered by a change in the signal strength received from the access point. Deterioration in transmission may also trigger a switch. The following is an example of WirelessIP5000-A parameter settings relating to handover. The parameters are set using User.ini, described later.

[ROAMING]

*Try_Beacon_Signal_Level=-72

*Try_Rx_Signal_Level=-72

*Try_Over_TxError_Count=8

*Level_Diff_Higher_Than_Curr_Site=5

7.4 Power Save Mode

The actual implementation of the power save mode may also differ depending on the wireless LAN access points. The following are points to keep in mind.

(1) Support for power save mode

This depends on whether the access points support power save mode.
Power save mode is set and clear by the NULLFunction packet from WirelessIP5000-A. The WirelessIP5000-A enters power save mode during standby. After that, it periodically and repeatedly cancels and sets power. Power save mode is cleared when in a conversation state such as message transmission and reception.
In the event that message arrives (INVITE) while in power save mode, the access point notifies the WirelessIP5000-A through the beacon frames that a packet arrived. The WirelessIP5000-A receives the notification, sends polling to the access point, receives the buffered data, and begins reception operations.

Figure 7-4 shows the reception operations when the WirelessIP5000-A is in power save mode.

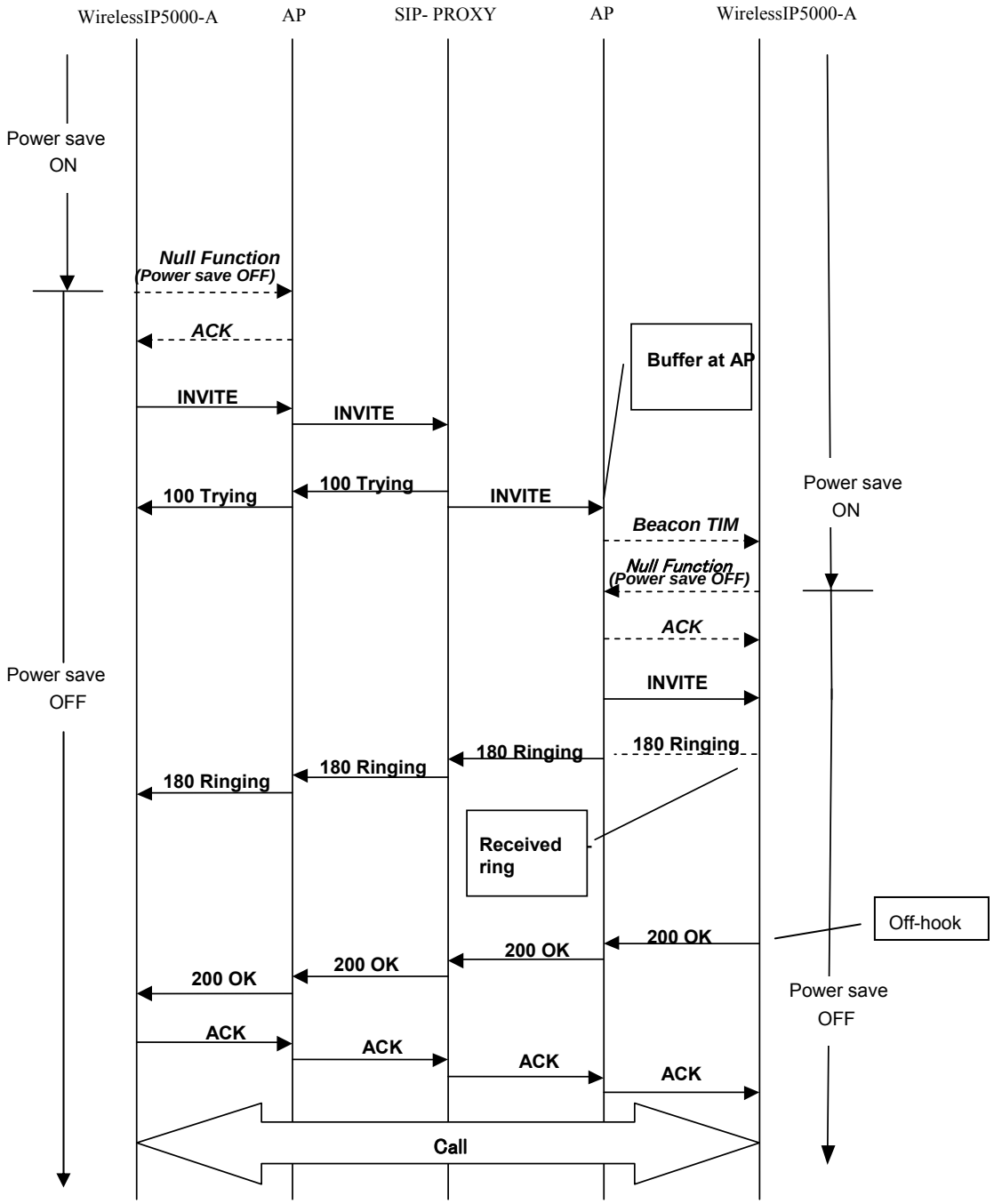
(2) Timer for power save mode

Even if the wireless LAN system (access points) supports power save mode, it is necessary to check whether the timer has been set for a terminal that is in power save mode.
A terminal that has entered power save mode normally does not send data on its own. From the viewpoint of an access point, it becomes difficult to confirm the terminal's presence. When, for example, a terminal does not respond to the beacon notifying of packet arrival (explicit condition), the access point might cancel the terminal's connection (Association). Similarly, there may be cases where the connection status of the terminal is canceled under implicit conditions such as timer monitoring. These conditions vary depending on the access point, so pay attention to this.
For instance, the connection may be canceled if there is no packet transmission from a terminal within a fixed period (monitoring of no-communication time).

(3) Power save mode timer refresh

When monitoring no-communication time, the conditions under which the monitoring timer is refreshed must be ascertained and examined. The WirelessIP5000-A sends out NullFunction packets periodically (every 30 seconds). To refresh the timer during this operation, the timeout value must be longer than the NullFunction packet transmission interval of the WirelessIP5000-A. Some access points refresh the monitoring timer not by NullFunction packets, but by user packets. In this case, the timeout value must be at least half of the WirelessIP5000-A's Registration Expire timer value.

Figure 7-4


WirelessIP5000-A
AP
SIP- PROXY
AP
WirelessIP5000-A
Power save ON
Null Function (Power save OFF)
ACK
Buffer at AP
INVITE
INVITE
100 Trying
100 Trying
INVITE
Power save ON
Beacon TIM
Null Function (Power save OFF)
ACK
Power save OFF
INVITE
180 Ringing
180 Ringing
180 Ringing
180 Ringing
Received ring
Off-hook
200 OK
200 OK
200 OK
200 OK
Power save OFF
ACK
ACK
ACK
ACK
Call

(4) Power saving

Other than the above-mentioned power save mode, it is necessary to take into consideration the following points when designing the wireless LAN and carrying out settings for the WirelessIP5000-A.

- **BeaconInterval and DTIM**

【Beacon Interval】

BeaconInterval is the interval at which beacon frames are sent. A value of at least 100 ms is recommended when using the WirelessIP5000-A.

If you make the interval smaller, the power consumption of the WirelessIP5000-A increases.

※ This setting is on the access point side.

【DTIM】

DTIM packets give notification to a terminal in power save mode that the access point is in client standby. When a wireless client receives a DTIM and there is a package addressed to it, it exits power save and receives the data buffered by the access point. Assuming that the DTIM value is set to 10, a DTIM packet is sent for every 10 beacon frames. DTIM frame reception consumes a minute amount of power. Consequently, the smaller the DTIM value, the more the battery is drained during standby.

※ This setting is on the access point side.

【Listen Interval】

ListenInterval is the beacon-receiving interval in power save mode. In WirelessIP5000-A, the method is for the ListenInterval value to follow that of DTIM, and so DTIM = ListenInterval.

(Note) There is a WirelessIP5000-A setting as mentioned below, but it is the value to put into the ListenInterval field of AssociationRequest. In reality, the ListenInterval value follows DTIM.

[WIFI]

Default_Listen_Interval=10

See the WirelessIP5000-A User.ini Manual for more details.

- **Operations under multiple network environments**

If you are using the Dynamic Network Binding function (see 7.2 Operating in a Multiple Network Environment), access point scanning is done against all network configurations (SSID) that are set. The increase in access point scanning increases power consumption during scanning, and the battery will drain somewhat quicker.

7.5 Security

7.5.1 Encryption

WPA-PSK

With encryption protocols used by conventional WEP encryption, data is encrypted cyclically using the same key, making the encryption easy to break. To address this weakness, TKIP expands the random number sequence IV (initialization vector) used to generate encryption keys from the 24 bits used in WEP to 48 bits. Also, TKIP makes the encryption process more complex by using different encryption keys for each MAC address and automatically updating group keys on a regular basis.
This helps to prevent the breaking of encryption keys and spoofing, and provide a level of security that surpasses that available with conventional WEP.

WPA-EPA

When using radius server with TKIP. WPA-EAP should be selected for security.

WPA2-PSK

When AES is needed without radius server. WPA2-PSK should be selected for security.

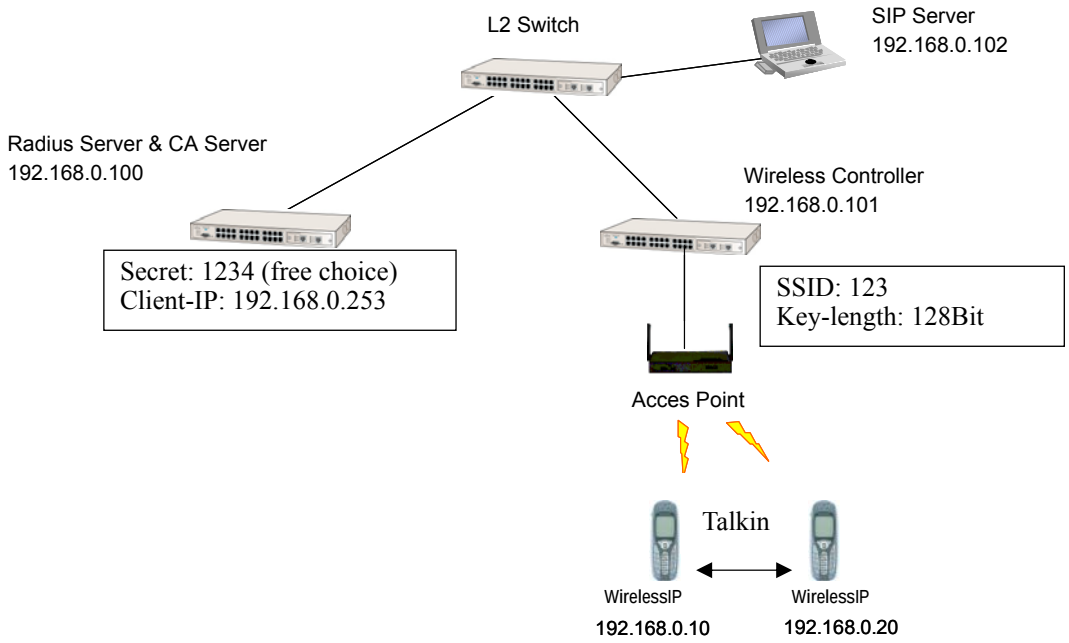
WPA2-EAP

When using radius server with AES. WPA2-EAP should be selected for security.

7.5.2 802.1x

The 802.1x authentication is not a standard that is exclusively for wireless LAN, but is also used by wired LAN. It is a standard in which mutual authentication is performed between the authentication server and the client using electronic certificates or ID/password, and the port is only opened to approved users. The sequence is shown in the figure in section 7.5.2.2. In 802.1x authentication, the client is called the supplicant, and the access point or switch that is between supplicant and authentication server (RADIUS server) is called the 802.1x authenticator.
The vulnerability of WEP encryption in previous wireless LAN has been pointed out, and this is because the WEP key used in encryption could be analyzed by capturing of signals. While WEP encryption uses a fixed WEP set in the access point and the client PC (wireless LAN card), with 802.1x authentication, the WEP key can be changed at each re-authentication, eliminating the vulnerability. Because of this, interest in this technology is increasing for use in wireless LANs.

[Figure. 802.1x Authentication Environment (Example)]



7.5.2.1 Supported 802.1x Types

At present, the WirelessIP5000-A supports four 802.1x types, as shown in the table below.

(Reference)

The EAP protocol used in the 802.1x authentication is an extension of PPP. PPP only supports CHAP and PAP authentication, but 802.1x supports authentication methods such as TLS and one-time password. The widely used EAP is described in Table 7- 5.
As can be seen from the table, each EAP has points that require attention. In the case of EAP-TLS, since electronic certificate is required at the client side also, it is necessary to manage the issuance/invalidation of certificates for the number of client PCs.

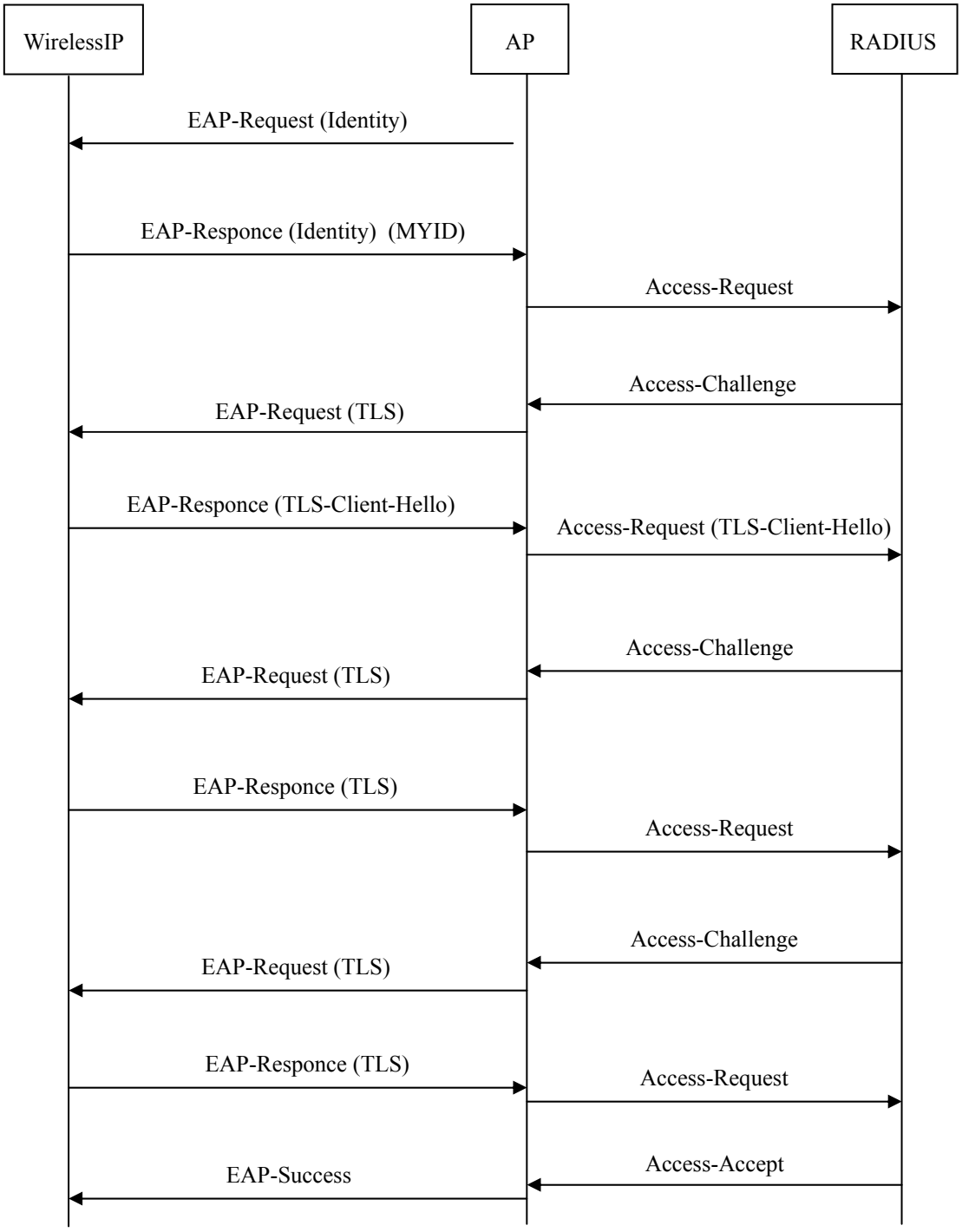
Table 7-5

Electronic certificate			Mutual authentication between client/server	Features	Supported by WirelessIP5000-A?
Type	Server	Client			
EAP-MD5	Not required	Not required	ID/PW server authentication is not carried out	As there is no dynamic distribution of key, the security level is low.	Yes
EAP-TLS	Required	Required	Electronic certificate	Although the security level is high since there is mutual authentication based on electronic certificate, electronic certificates must be managed.	Yes
EAP-TTLS	Required	Not required	Server's electronic certificate and ID/PW	Since the electronic certificate is required at the server side only, management is simple. However, separate supplicant software is required.	Yes
LEAP	Not required	Not required	ID/PW	Since electronic certificate is not required, management is simple. Cisco's wireless LAN devices (access point, card) and RADIUS server are required.	No
PEAP	Required	Not required	Server's electronic certificate and ID/PW	Since the electronic certificate is required at the server side only, management is simple.	Yes (PEAPv0, v1)

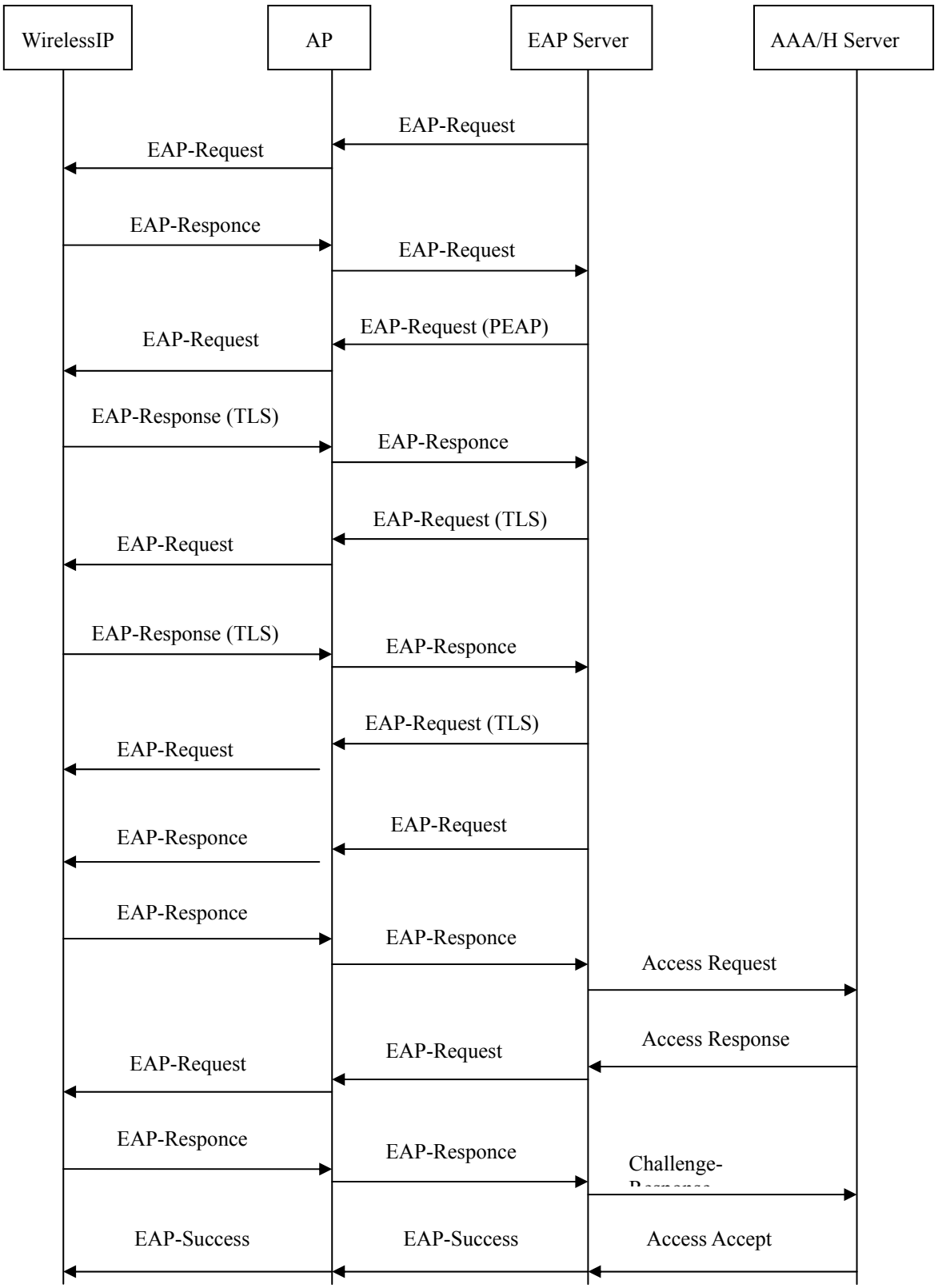
7.5.2.2 802.1x Sequence

The following is an 802.1x sequence that uses wireless LAN. This complies with the standard.

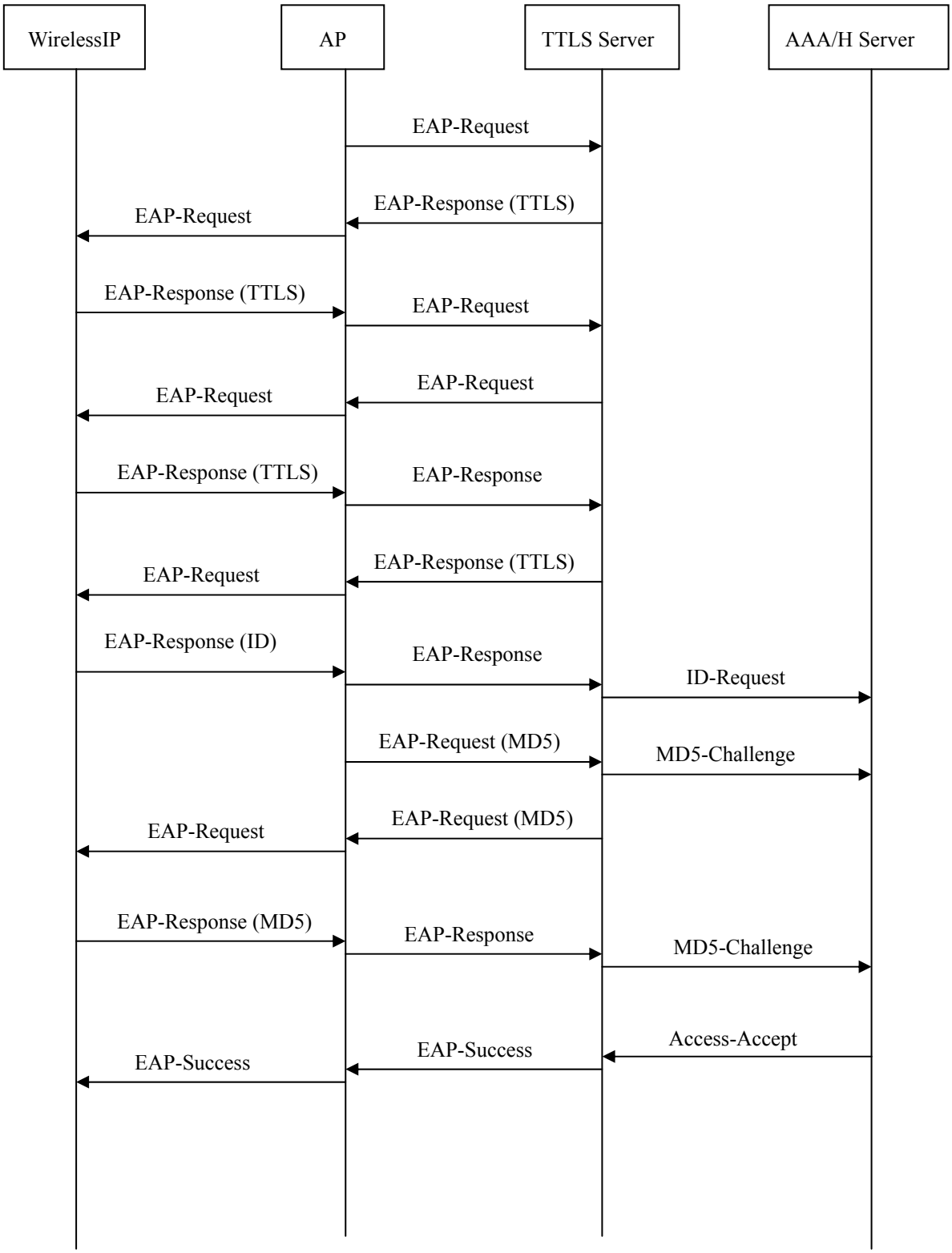
<EAP-TLS>



<EAP-PEAP>


WirelessIP
AP
EAP Server
AAA/H Server
EAP-Request
EAP-Request
EAP-Responce
EAP-Request
EAP-Request (PEAP)
EAP-Request
EAP-Response (TLS)
EAP-Responce
EAP-Request (TLS)
EAP-Request
EAP-Response (TLS)
EAP-Responce
EAP-Request (TLS)
EAP-Request
EAP-Responce
EAP-Request
EAP-Responce
EAP-Responce
Access Request
Access Response
EAP-Request
EAP-Request
EAP-Responce
EAP-Responce
Challenge-
EAP-Success
EAP-Success
Access Accept

<EAP-TTLS>


WirelessIP
AP
TTLS Server
AAA/H Server
EAP-Request
EAP-Response (TTLS)
EAP-Request
EAP-Response (TTLS)
EAP-Request
EAP-Request
EAP-Request
EAP-Response (TTLS)
EAP-Response
EAP-Response (TTLS)
EAP-Request
EAP-Response (ID)
EAP-Response
ID-Request
EAP-Request (MD5)
MD5-Challenge
EAP-Request
EAP-Request (MD5)
EAP-Response (MD5)
EAP-Response
MD5-Challenge
Access-Accept
EAP-Success
EAP-Success

7.5.2.3 Multi-Authorization Method

WirelessIP5000-A v2.2.x onwards can be used even when multiple authentication types are set at the RADIUS server.

7.5.2.4 Certificate Installation Procedures

Certificates are installed on the WirelessIP5000-A via the TFTP server.

(Certificates can also be installed from USB cable.)

■ Installation procedure for EAP-TLS certificate

[Prerequisites]

The following items are required. Issue these in advance and place them in the root directory of the TFTP Server.

- Root certificate: DER, CER, PEM encoding are supported
- Private certificate: .pfx, .p12 encoding are supported

* If private certificate is installed, jot down the ID and password.

* Note that the ID/password for private certificate may differ from the ID/password for connection authentication. The settings procedure becomes involved. The following describes such a situation.

If the ID/password pairs are identical, steps 4 and 13 to 17 in (2) Private Certificates are not required.

[Installation method]

(1) Root certificate

1) Select “Network config” > “Certs Manager” from the Admin menu
2) Select “3. Down(load) RootCA”
3) “Enter” (press the lever) when warning screen appears
4) “Yes” when asked whether to upgrade
5) Enter the TFTP server’s IP address
6) Enter the file name to download

(This may take a little time)

If an exception message displays, repeat steps 1 through 6 after checking the settings.

(2) Private certificate

1) Select “Network config” > “Certs Manager” from the Admin menu
2) Select “3. Down(load) PrivateCA”
3) “Enter” (press the lever) when warning screen appears
4) “Yes” when asked whether to upgrade
5) Enter the TFTP server’s IP address
6) Enter the file name to download

(This may take a little time)

If an exception message displays, repeat steps 1 through 6 after checking the settings.

7.5.2.5 Certificate Reference Procedure

See the WirelessIP5000-A Administrator Manual.

7.5.2.6 Certificate Deletion Procedure

See the WirelessIP5000-A Administrator Manual.

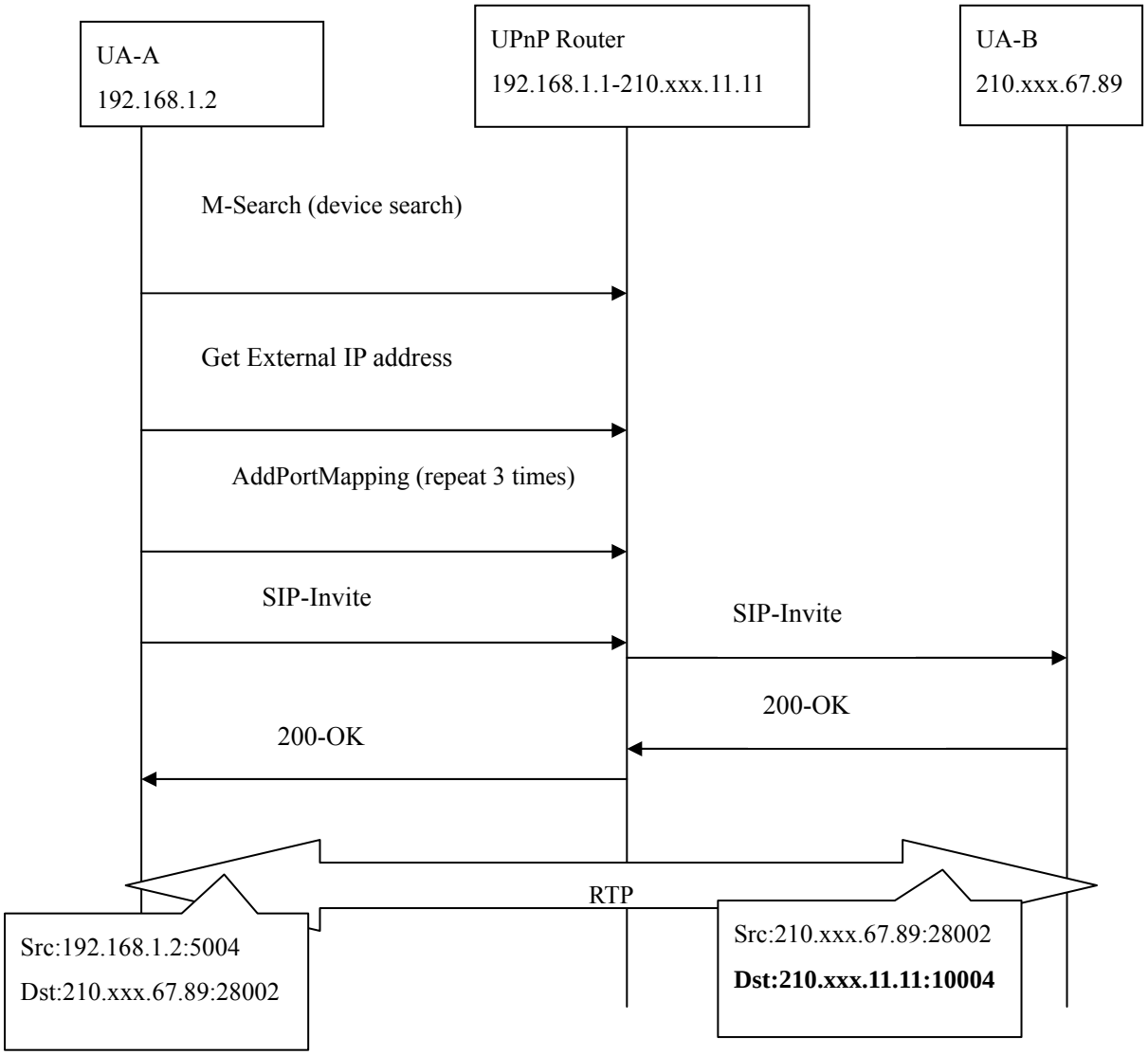
7.6 NAT Function

7.6.1 UPnP（Universal Plug and Play）

This is a technical specification that allows devices that are connected to a network, such as PCs and peripheral devices, to recognize each other and interoperate. It was proposed by Microsoft® in 1999 and the standardization work is being carried out by the Universal Plug and Play Forum. UPnP brings together standard Internet technologies such as XML, DHCP, SOAP and GENA. It allows auto detection of devices connected to the network, information exchange between devices, and control.

* UPnP-ready routers are required.

<UPnP flow>



7.6.2 SNAT（Static NAT）

This is the static NAT function used between the WirelessIP5000-A and wireless APs (or routers). Static NAT setting is also required in the wireless APs (or routers).

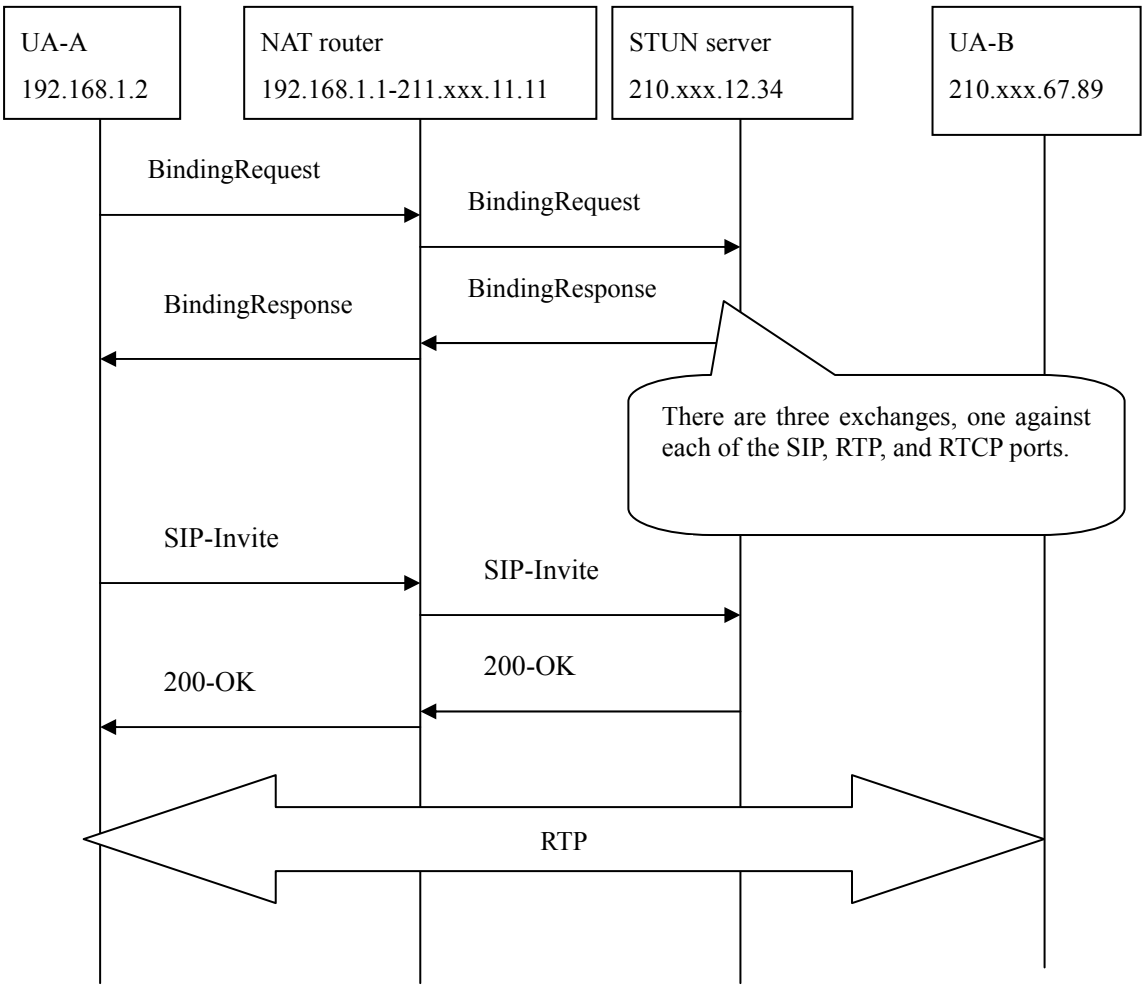
- External IP: Set the external address.
- Port number: Set the port to use for communicating with external devices.

7.6.3 STUN（Simple Traversal of UDP over NATs）

1. This protocol is used for traversing NATs using UDP. The traversal of NATs by UDP packets occurs after examining the port number mapped to the external address of a NAT router and the mapping algorithm of the router.
2. Set forth in RFC 3489.
3. Valid only when the NAT router is using cone NAT.
4. There is validity period for the address translation table in the NAT router.

※ Cone NAT is a NAT in which all requests from the same internal address and port is mapped to the same external address and port.

<STUN flow>


UA-A
192.168.1.2
NAT router
192.168.1.1-211.xxx.11.11
STUN server
210.xxx.12.34
UA-B
210.xxx.67.89
BindingRequest
BindingRequest
BindingResponse
BindingResponse
There are three exchanges, one against each of the SIP, RTP, and RTCP ports.
SIP-Invite
SIP-Invite
200-OK
200-OK
RTP

7.7 Web Authentication

The web authentication function authenticates users attempting to access secured login pages on their Web browsers through their user names and passwords.

<Web authentication sequence>
(1) ----> HTTP request
(2) <---- Redirect to login page
(3) ----> HTTPS request
(4) <---- Login request
(5) ----> Login
(6)<----- GW Open

<WirelessIP5000-A parameters>
・・・ UAM_URL

・・・ UAM_Login_URL
・・・ UAM_IDTag_Name, UAM_PWTag_Name
・・・ ID_Tag_Name, PW_Tag_Name

Reference

・ The related entries in user.ini are as follows.

UAM_Use_Manual	Whether Web authentication (Login_URL, IDTag_Name, PWTag_Name) is to be done manually.
UAM_Login_URL	Login_URL for Web authentication (e.g.: https:// login.yahoo.co.jp/login/login.cgilogin.hitachi-able.co.jp/login.cgi).
UAM_IDTag_Name	login_name <input> tag for Web authentication <input> tag.
UAM_PWTag_Name	login_password <input> tag for Web authentication <input> tag.
UAM_URL	URL for Web authentication (e.g.:http://hitachi-cable.co.jp). If this parameter is set to 0.0.0.0, HTTP requests are sent to the gateway.
UAM_ID	Login user for Web authentication.
UAM_Password	Login password for Web authentication.

* Depending on the provider, you may not be able to connect.

7.8 Wireless LAN Parameter

Here are some points to watch for when communicating with wireless LAN access points.

(1) Speed

For 802.11b, there are four communication speeds: 11 Mbps, 5.5 Mbps, 2 Mbps, and 1 Mbps. At slower speeds, the time required for sending the same amount of data is longer, so we recommend that the communication speed of the access point be fixed at 11 Mbps.

By changing the following terminal parameter, you can fix the transfer rate of data packets (RTP) to Auto or a desired value.

```
---------------------------------------------------------------------------------------------------------
 [WIFI]
 Data_Packet_TxRate = 0
---------------------------------------------------------------------------------------------------------
```

* Default is 0 (Auto).
Valid values: 0 (Auto), 1, 2, 5, 11

(2) Preamble

The preamble used in the packet format in the wireless zone may be short or long. Here too, when it is important to keep communication time down, you may want to use only short preamble.

(3) Specifying the scan channel

When scanning for the access point, it is possible to specify the scan channel. To use this function, specify the scan count and scan channel in the parameters described below.

```
---------------------------------------------------------------------------------------------------------
[WIFI_SCAN]
Scan_Channel_List = 1,2,3,4,5,6,7,8,9,10,11,12,13,14
Scan_Mode = 0
---------------------------------------------------------------------------------------------------------
```

・Scan_Mode → This parameter specifies the scan method.

WirelessIP5000-A is compatible with Active Scan and Passive Scan for searching for APs.

0: Active Scan: Searches for APs by exchanging Probe Requests/Responses.

1: Passive Scan: Searches for the AP by receiving beacon signals from APs.

• Scan_Channel_List → This is the list of channels to be scanned.
Specify as comma-separated values.
* Default is channels 1-14 (all channels).

(4) BackoffInterval

When the WirelessIP5000-A is disconnected (=Network-Fail) from a wireless LAN, this is the interval at which 802.11 Probe Requests are sent to get assigned to an access point.

```
---------------------------------------------------------------------------------------------------------
[DYNAMIC NETWORK]
  Backoff Interval = 4, 8, 16, 32, 64
---------------------------------------------------------------------------------------------------------
```

The unit seconds, and the last value (64 in the above example) is repeated indefinitely.

(5) 802.1x-BindTimeout

When the WirelessIP5000-A is attempting to connect (=Network-Binding) to a wireless LAN using 802.1x, if 802.1x authentication does not succeed after a certain period, it throws an 802.11 Disassociation and disconnects.

After this, the interval for reattempting authentication is the BackoffInterval set under DYNAMIC network.

```
---------------------------------------------------------------------------------------------------------
[DYNAMIC Network]
  8021X_Bind_Timeout = 15
---------------------------------------------------------------------------------------------------------
```

The default is 15 (seconds).

7.9 WirelessIP5000-A Configuration Procedure

Here, we show how to configure the wirelessIP5000-A.

A list of settings is provided in the WirelessIP5000-A User.ini Manual. You can use any of the following methods to make settings.

7.9.1 Configuration Methods

(1) Using the UI (user interface)

The settings are done from the WirelessIP5000-A operation menu. There are user-level settings and administrator-level settings. Administrator password is required for the administrator-level setting items.

For specific procedures, see the WirelessIP5000-A Administrator Manual and WirelessIP5000-A Users Manual.

(2) Using USB

User.ini file can be read into a PC through a dedicated USB cable. Parameter/value pairs are stored in User.ini. You can also read in phone lists and certificate files.

You need an administrator computer, USBManager (dedicated WirelessIP5000-A software), and USB cable (dedicated WirelessIP5000-A USB cable). For specific procedures, see the WirelessIP5000-A USB Manual and WirelessIP5000-A USB Users Manual.

(3) Using tftp

User.ini file can be downloaded via the network. The settings are stored in User.ini.

You need an administrator computer and tftp server software. For specific procedures, see the WirelessIP5000-A Administrator Manual and WirelessIP5000-A Users Manual.

(4) Using the Web

WirelessIP5000-A settings can be modified using a Web browser.

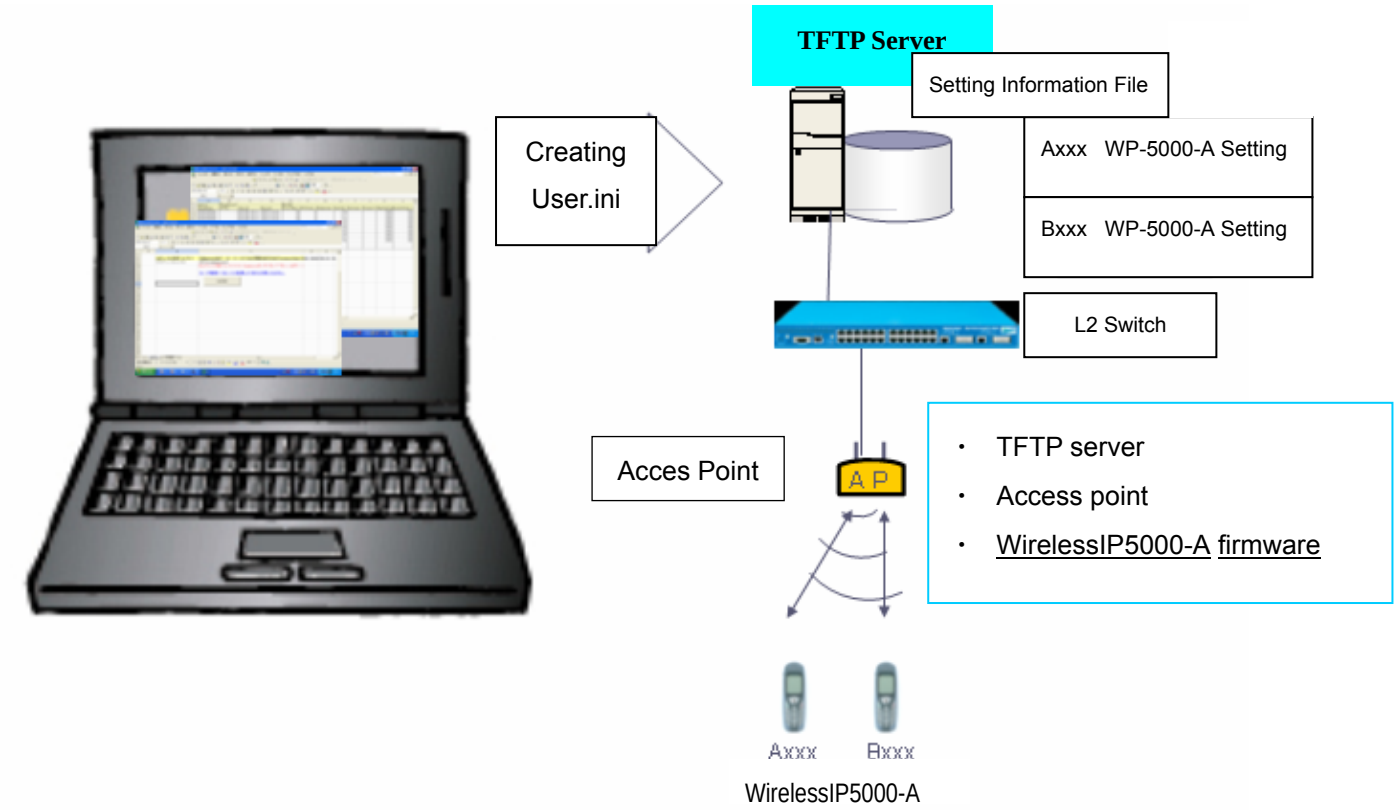
You need an administrator computer to connect the WirelessIP5000-A to the Internet. For specific procedures, see the WirelessIP5000-A Administrator Manual and WirelessIP5000-A Users Manual.

7.9.2 Configuration when Introducing Multiple Devices

Here we show how to configure the WirelessIP5000-A when you are bringing in multiple sets.

(1) Preparations

First, prepare to setup the WirelessIP5000-A. For more information, see the WirelessIP5000-A User.ini Manual.



If the terminals require different settings, prepare User.ini using the following steps.
Here, the method of using the lower 3 bytes of the MAC address as the method of identifying the respective terminals is explained.

1. Create individual files for the different settings.

2. Change the file names used by the WirelessIP5000-A units to:

<Lower 3 bytes of MAC address>user.ini

(Example) If the MAC address is xx:xx:xx:00:3c:7a, then the file name is 003c7auser.ini.

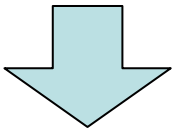
(2) Preparing loadrun.ini

Prepare the loadrun.ini file for the WirelessIP5000-A.

If the terminals require different settings, prepare loadrun.ini using the following steps.

1. Change the section shown below in the loadrun.ini on the TFTP server as follows:

```
[3]
name=user.ini
```



```
[3]
name=%muser.ini
```

In the example above, %m is replaced by 3 bytes of MAC address of the WirelessIP5000-A unit. In other words, the file named “3 bytes of MAC address + User.ini” is downloaded.

(3) Finally, download User.ini from the tftp.

Caution

- The tftp server requires the following 4 files:

g729a.bz. ipphone.bz, loadrun.ini, ******user.ini

- If there is an error in the user.ini name, the user.ini download will fail.
- If * is not attached to the user.ini file entry name, the parameter values will not be updated.

For more information, see the WirelessIP5000-A Administrator Manual.

7.9.3 Auto-Upgrade

The WirelessIP5000-A can automatically upgrade its firmware configuration update using the tftp server.

you can use this capability by selecting [Upgrade] => [Setup] => [Auto Upgrade] from the Admin menu.

Select the upgrade time from the Time menu, and when to upgrade from the Recurrence menu. If you select Daily, the upgrade is carried out daily.

Also, add version=(version name) to the [options] section of loadrun.ini on the tftp server.

(Example)

```
[options]
run=1
version=v2.2.0
```

Auto-upgrade works only if the firmware of the upgrading WirelessIP5000-A differs from the version name in loadrun.ini.

Caution Upgrading the firmware will result in the current configuration being overwritten by the configuration (user.ini) in the TFTP folder. If you want to keep the configuration currently in use, replace the configuration (user.ini) in the TFTP folder with the one that contains the values that are in use. See the WirelessIP5000-A User.ini Manual regarding editing the user.ini file.

The related User.ini (Web-Config-Tool) parameters are:

[AUTO_UPGRADE]

Enable=1

Time=0

Repeat=0

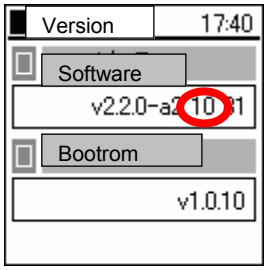
7.9.4 VendorID, VendorPW

VendorID and VendorPW for the respective SIP servers are set in the WirelessIP5000-A firmware.

(1) VendorID confirmation method

The number (10 in the example below) after the version (v2.2.0-a2) in Menu > Setup > Information > Version > is the VendorID.

* You can also check the VendorID from the Web settings screen.



(2) VendorID and VendorPW parameters

See the WirelessIP5000-A User.ini Manual for information concerning VendorID and VendorPW.

[SYSTEM]

* Vendor_ID=

*Vendor_Password= （8 characters）

(3) Confidentiality

The VendorPW that is associated with the VendorID is set in advance. Consequently, the setup does not allow the VendorID to be changed if it does not match the VendorPW.

(4) Cautions when Upgrading to Another Version

When upgrading firmware version and configuration, always set the correct VendorID and VendorPW, and add * in front of these entries as shown below.

[SYSTEM]

* Vendor_ID=

*Vendor_Password=

If VendorID and VendorPW are not set correctly, the upgrade (upload) fails, and the message "Invalid VendorID or VendorPW!" pops up. When this happens, the previous settings are preserved. Also, running Format from the BootROM menu does not clear the VendorID and VendorPW. If you inadvertently set an incorrect VendorID and VendorPW after formatting, the “Invalid VendorID or VendorPW!” pops up on the standby screen after a fixed interval, and only the Settings and Network menus are displayed on the menu screen. Set correct values for VendorID and VendorPW and restore the phone.

7.10 Types of Dial Tones

Here we discuss the types of tones that can be set on the WirelessIP5000-A.

7.10.1 Tone Type Parameters

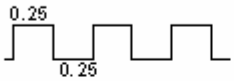
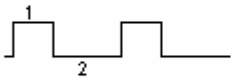
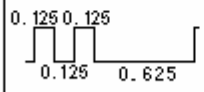
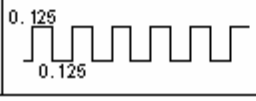
[TONE_TYPE]
Dial_Tone_Type_On_Idle=2
Dial_Tone_Type_On_Hold=0
Send_Dial_Tone_Type=1

(1) Dial_Tone_Type_On_Idle
This sets the tone that is heard by depressing SEND while on standby.
（0: silent, 1: PDT, 2: CDT）

(2) Dial_Tone_Type_On_Hold=
This sets the tone that is heard at a terminal that is on hold.
（0: silent, 1: SDT）

(3) Send_Dial_Tone_Type
This sets the tone that is heard after sending out INVITE up until RBT is heard.
（0: silent, 1: SDT, 2: HST）

7.10.2 Tone Specifications

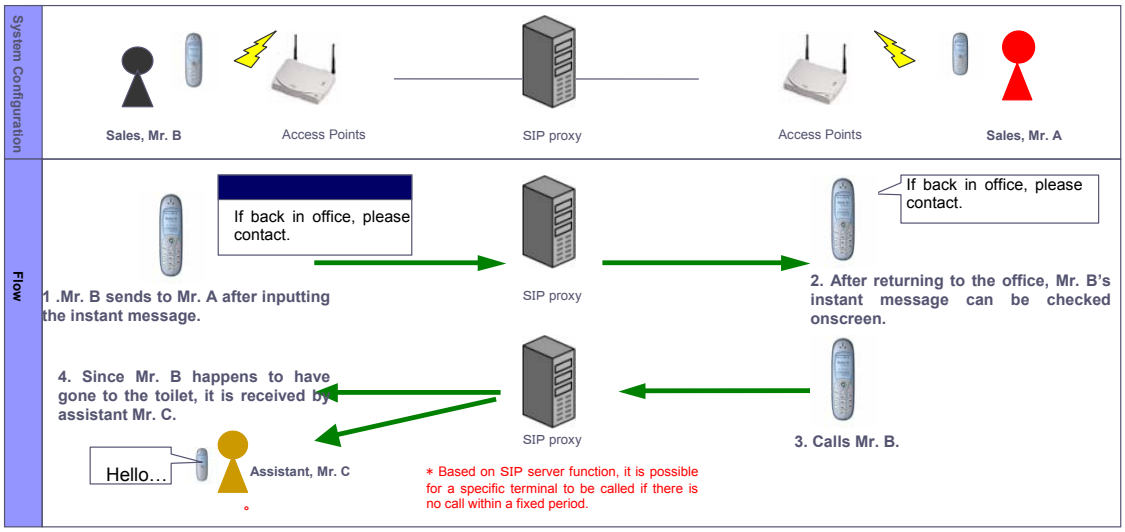
	Freequency (Hz)	Spec	note
CDT	400		dial tone
PDT	400		dial tone
RBT	400 & 420		ring back tone
HST	400		hold tone
SDT	500		send tone

* Japanese Tones

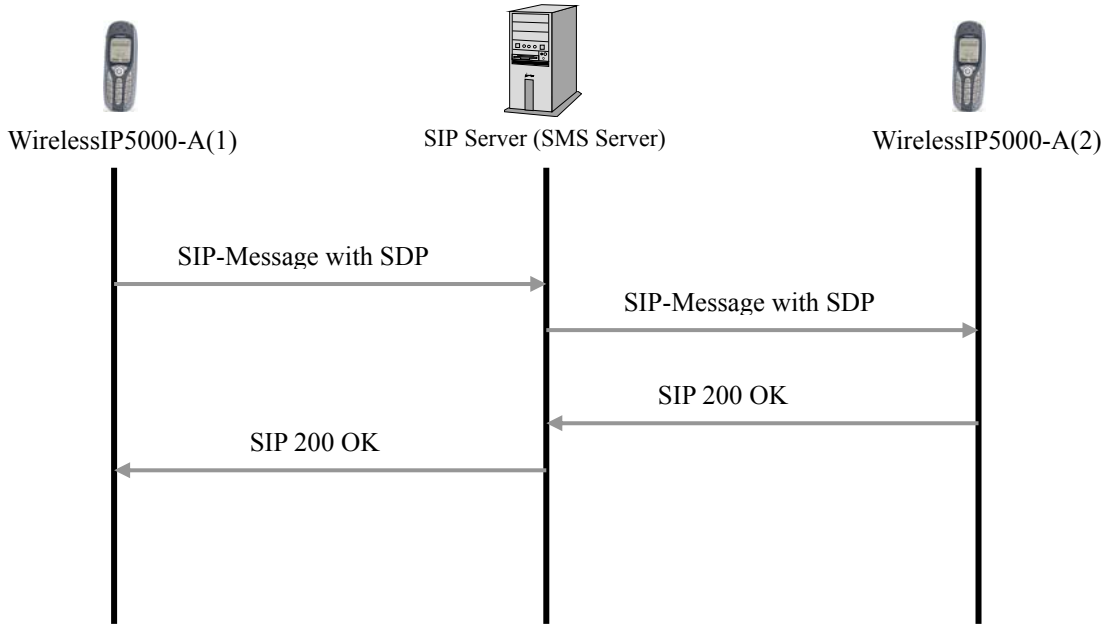
8. Other Functions

8.1 Instant Messaging

This allows you to send brief messages in real time from the terminal. (SIMPLE)
The message can be seen on the display at the receiving terminal.



Instance messaging uses SIP messages. The transmission flow is as follows. The contents of the message are stored as SDP-Info in SIP-Message.



To exchange instant messages between WirelessIP5000-A terminals or between a WirelessIP5000-A and an external terminal, the text code used for the messages must match between the terminals, the SIP server, and the short mail server.

The related User.ini parameters are:

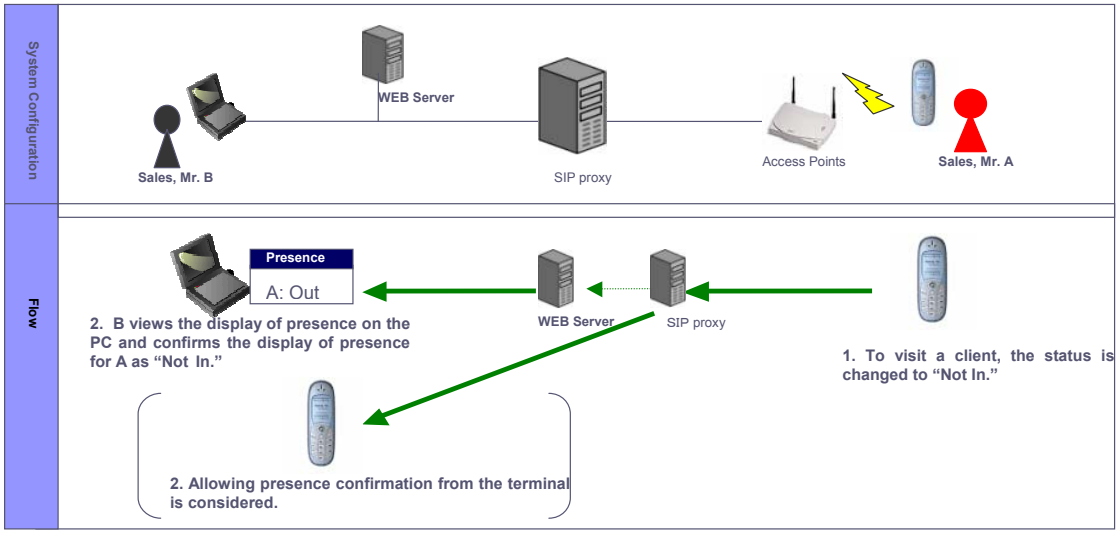
[SMS]	
Use_SMS	Short mail function is - 0: disabled, 1: enabled
Message_Server	Short Mail Server Address (when blank, the SIP server address is used)
Message_Content_Type	MESSAGE Content-Type (0 : text/plan, 1 : text/html)

[UNICODE]
Use_Unicode_On_SMS
Whether or not to use Unicode (UTF-8) for SMS Content.
0 : Use EUC-JP（Default）
1 : Use UTF-8

8.2 Presence

This is typically used to get the status of the party on the other end of a conversation.

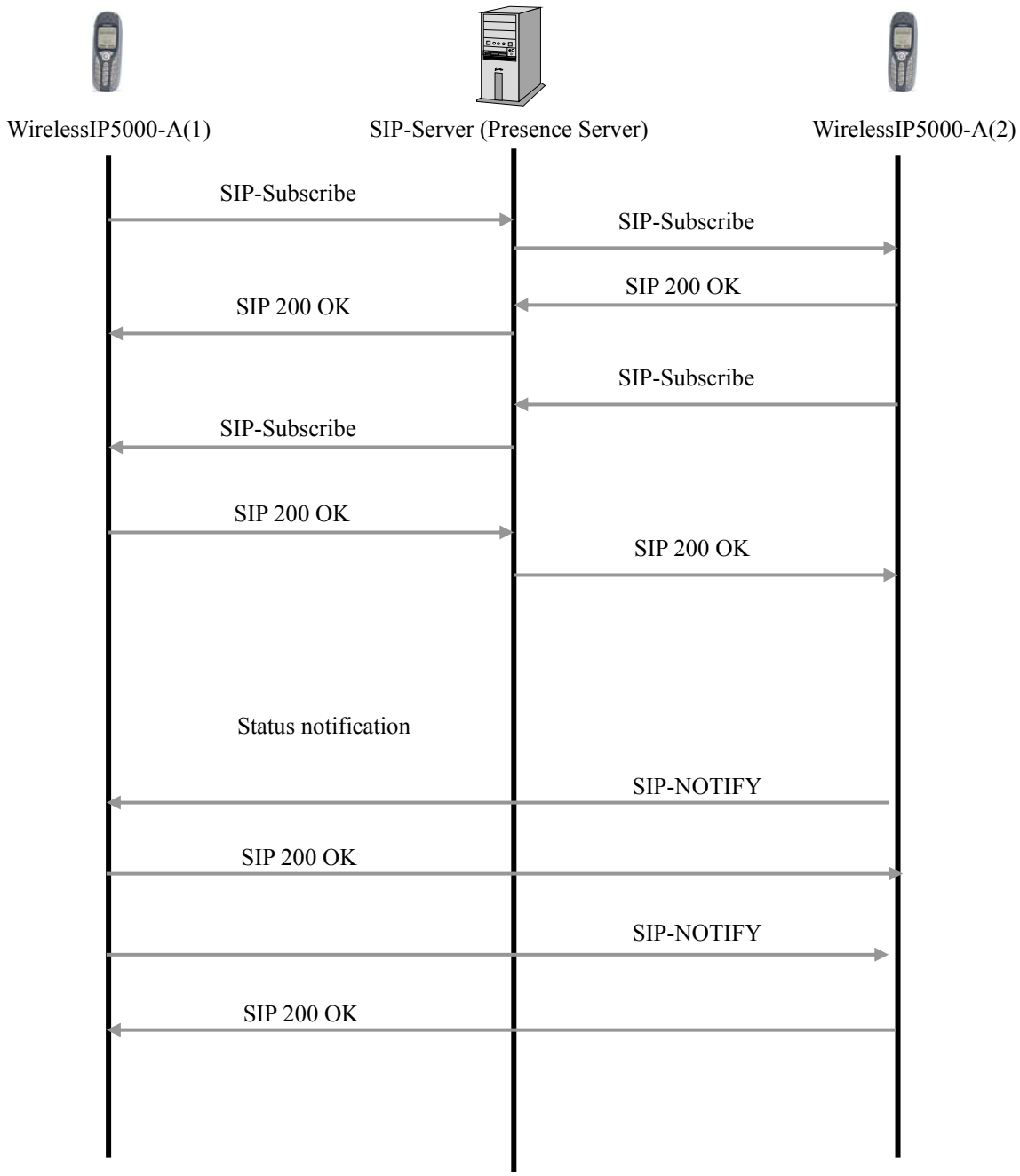
The status of the other party (out, in a meeting, ...) can be checked from the Presence display on the terminal screen.



The flow of the Presence function is shown below. The Presence function is carried out by sending out SIP-Subscribe at terminal boot-up to all the clients that are registered on the WirelessIP5000-A. Status change is notified by SIP-Notify.

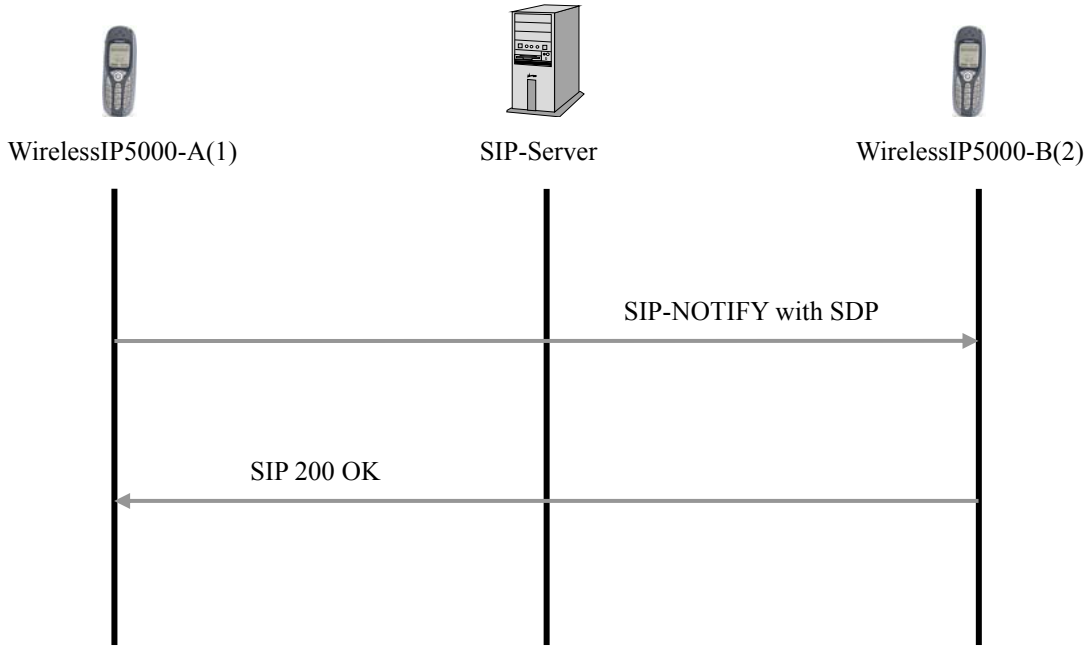
(1) The flow during registration and when Presence-Expire-Time expires

The flow is the same when Presence-Expire-Time expires and during registration.



(2) The flow during change in Presence status

When the status of Presence changes for a WirelessIP5000-A, SIP NOTIFY is used, and the flow is as shown. The changed status is notified through SDP-Info “msnsubstatus” sent with SIP-NOTIFY.

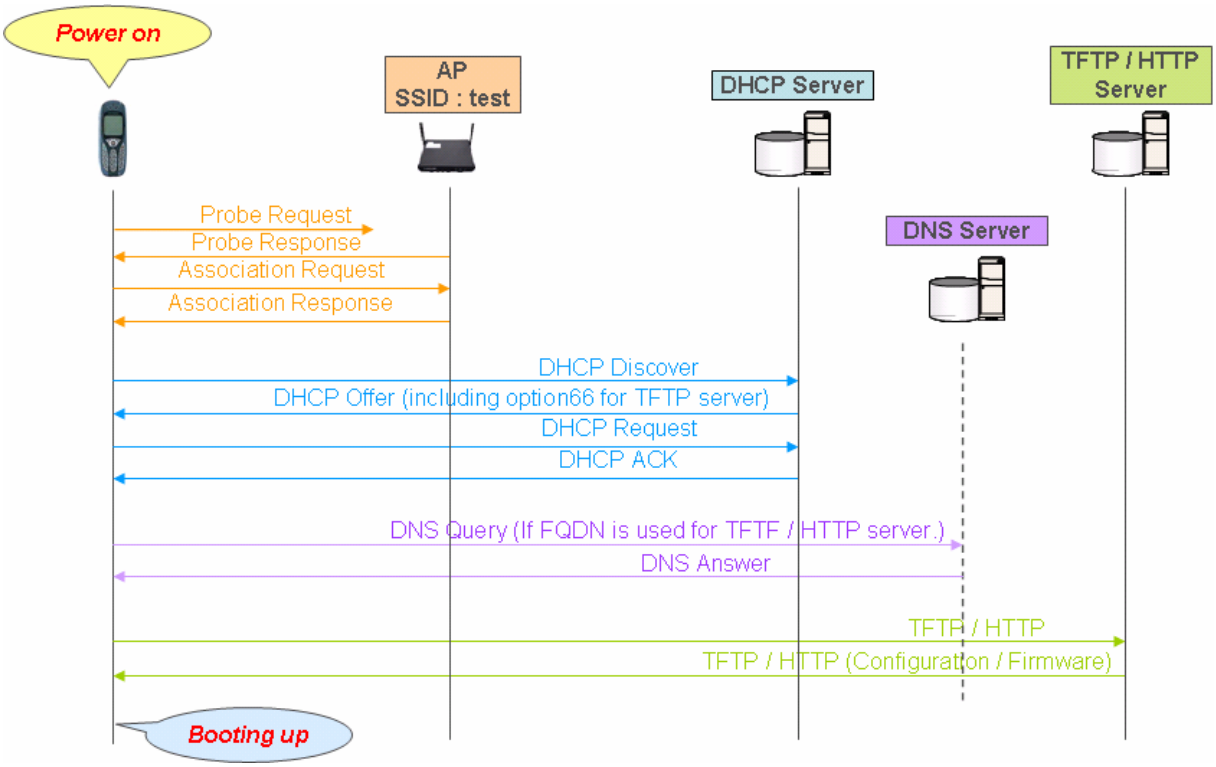


The related parameters are:

[PRESENCE]	
Use_Presence	Presence is - 0: disabled, 1: enabled
	Enable_Online_Ring Notify when a registered person logs in (0: No, 1: Yes)
Online_Ring_Type	Type of ring tone to use when a registered person logs in, if enabled
Online_Ring_Mode	Ring mode to use when a registered person logs in (0: Ring, 1: Vibrate, 2: Ring + Vibrate, 3: Lamp)
Subscribe_Expire	Presence Subscribe expiration time in seconds
Presence_Server	Presence Server Address (when blank, the SIP Server address is used)
Use_Register	Send REGISTER sent to the presence server (0: No, 1: Yes)

8.3 Auto-Provisioning

When a terminal is turned on, it automatically accesses the TFTP/HTTP server and downloads the configuration file and firmware.

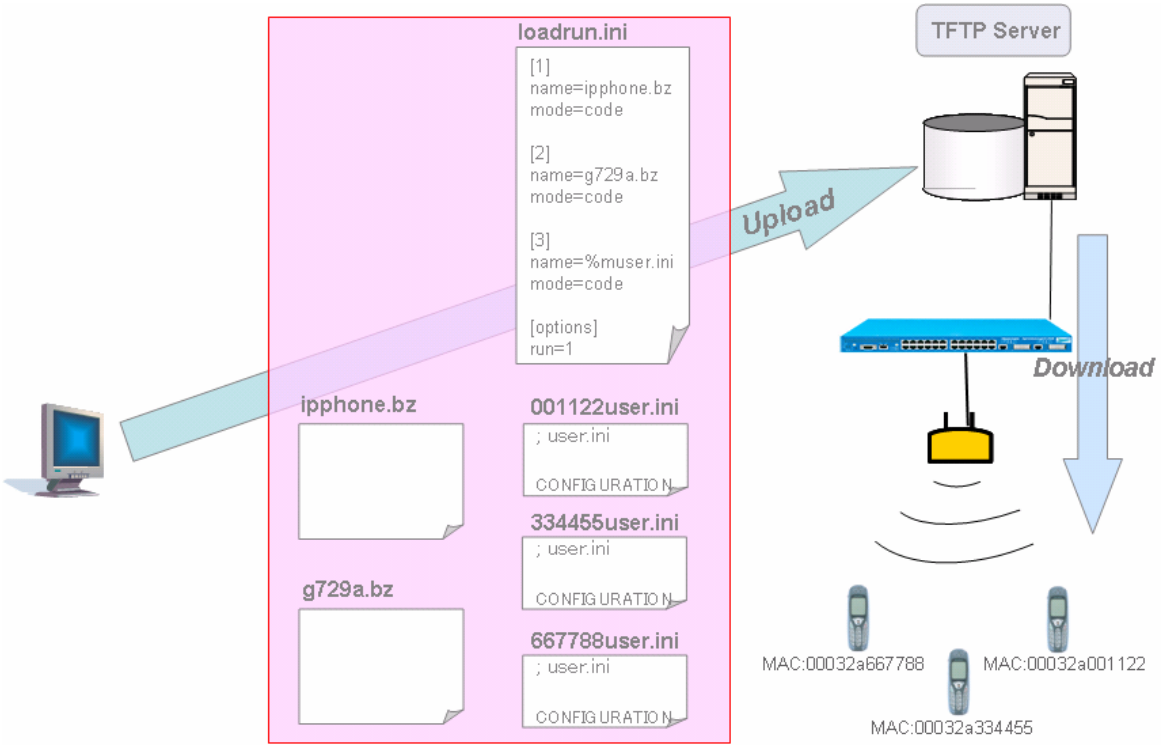


(1) Using tftp.

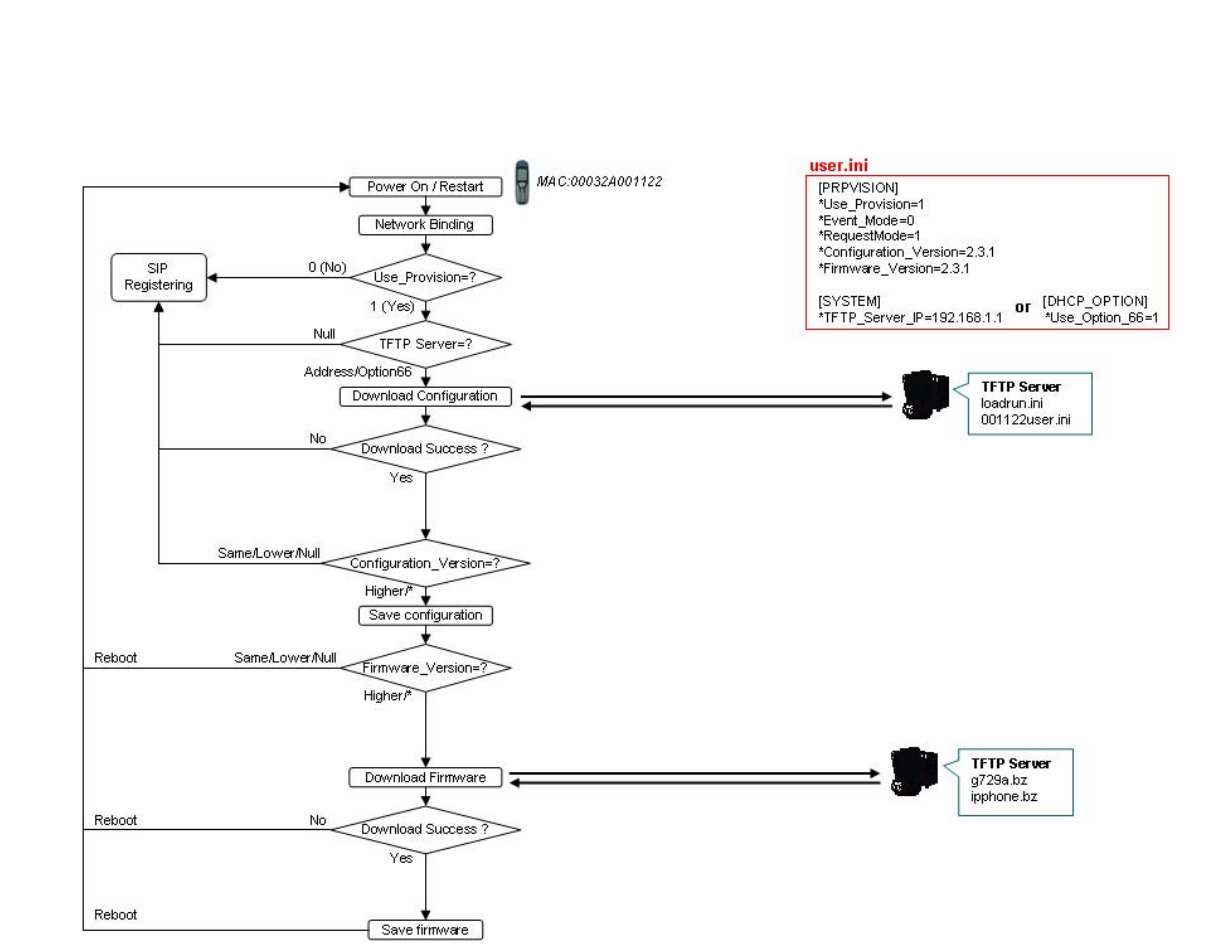
1. Set the following parameters.

```
-------------------------------------
[PROVISON]
Use_Provision=
Event_Mode=
Request_Mode=
Configuration_Version=
Firmware_Version=

[SYSTEM]
TFTP_Server_IP=

 [DHCP_OPTION]
Use_Option_66=
-------------------------------------
```

2. Upload all the files (loadrun.ini, ipphone.bz, g729a.bz, user.ini) to the same TFTP download directory.



3. Below is the flow chart when using tftp (Including a sample configuration).



(2) When using HTTP.

1. Set the following parameters.

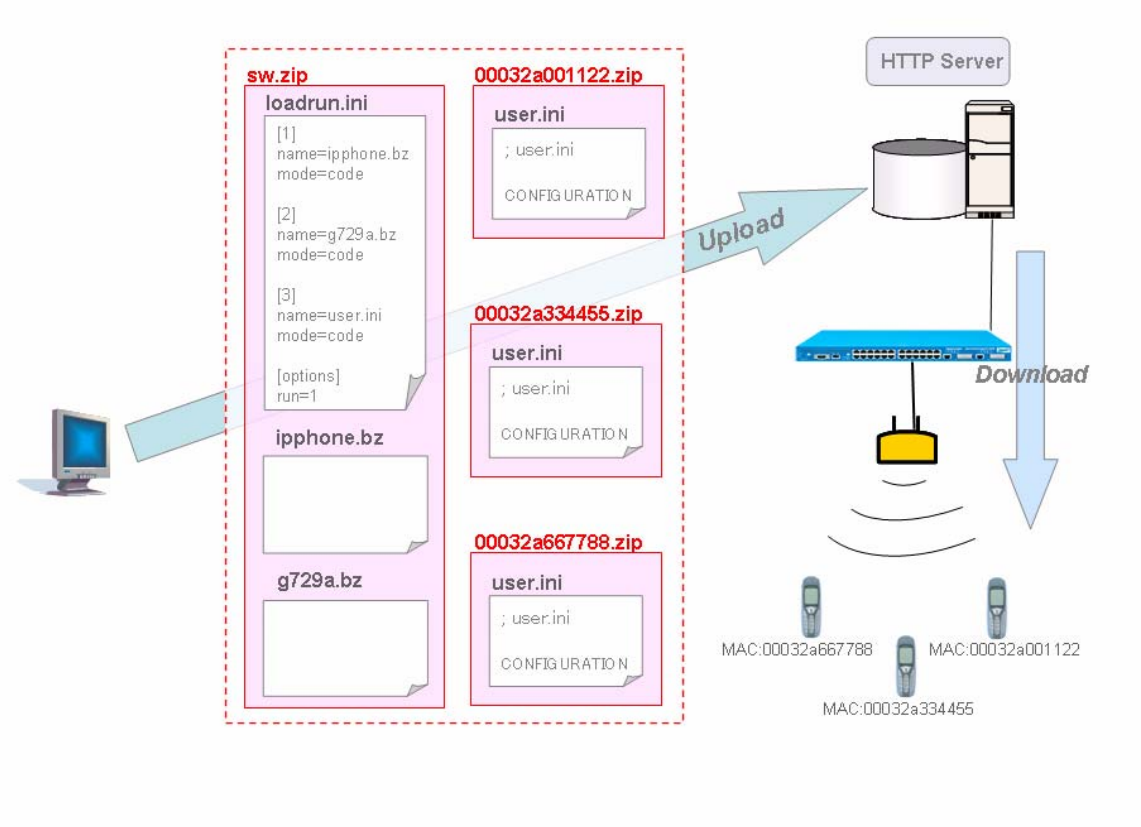
```
-------------------------------------
[PROVISON]
Use_Provision=
Event_Mode=
Request_Mode=
Configuration_URL=
Firmware_URL=
Configuration_Version=
Firmware_Version=
Enable_HTTP_Keep_Alive=
-------------------------------------
```

2. Compress the three files (loadrun.ini, ipphone.bz, and g729a.bz) into a single ZIP file with level zero compression. (Do not compress the files with folder/directory.)

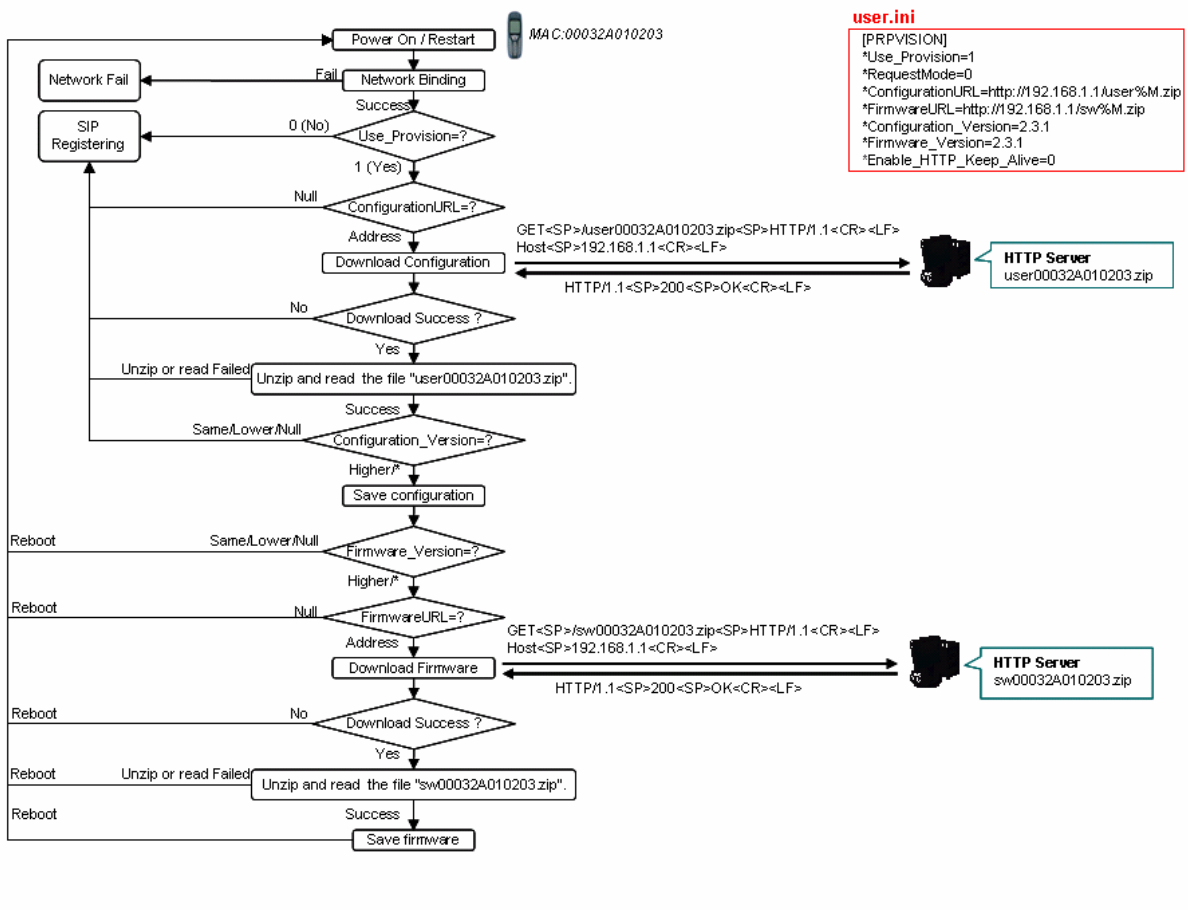
Caution Do not change the file names “loadrun.ini”, “ipphone.bz” and “g729a.bz” Also, Do not edit the file “loadrun.ini”.

3. Compress user.ini into a single ZIP file with level zero compression. (Do not compress the file with folder/directory.)

4. Upload the ZIP files to the HTTP server.



5. Below is the flow chart when using HTTP (Including a sample configuration).



9. Maintenance Procedures

9.1 Information about the WirelessIP5000-A Device

(1) Device Information

1. Information on the back of the unit with the battery pack removed
   - Serial No.
   - MAC address
2. Main information displayed on the screen

From the main screen, Menu > Setup > Information displays:

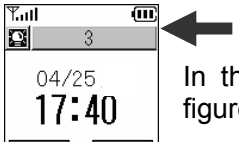
- TCP/IP information (IP address)
- Server/phone information
- MAC address
- Version

9.2 Information on the Display

(1) Antenna

Reception strength is indicated using antenna bars. Maximum strength is shown with 5 bars. If the display shows “Out of Range”, there is no available access point.

(2) Connection status



In the phone number display area above the time display (arrow in the figure), the current connection status is shown as follows.

1. Phone number (Userinfo and Displayname)

Displayed if correctly registered on the SIP server.

2. Network Bind

Displayed when connecting to a wireless network. An access point is selected using Dynamic Network Binding, the device connects, does DHCP processing up to the IP-related part.

3. Network Fail

Displayed when connection to the wireless network failed.

4. Registering

Displayed during registration to the SIP server after connecting to a wireless network.

5. Not register

Displayed when registration to the SIP server fails.

9.3 Troubleshooting Basics

Here are some functions required in troubleshooting the WirelessIP5000-A.

(1) Ping

This is the protocol for checking whether network is reachable. This may be executed using either of the following two methods.

1. Menu > Network > Ping test
2. Admin Menu > Network config > Ping test

You can select the IP address to be confirmed via ping from among 1) Manual, 2) 1st Proxy , 3) 2nd Proxy, 4) Gateway, 5) TFTP server. Select from these choices, enter the IP address, then press the center of the multi-function key.
The router (gateway address) can be pinged to check whether network is reachable.

(2) Wireless LAN Information

Information on the connected wireless LAN can be looked up.
Use Menu > Setup > Information > W-LAN
The information that can be looked up is as follows:
SSID, signal (dBm): reception level, mode, channel, MAC address (BSSID), beacon interval, and whether WEP is in use.

(3) Network Scan

Information on access points that can receive signals can be looked up. There are two ways to do this.

1. Menu > Network > Site scan
2. Admin Menu > Network config > Site scan

Information on available access points is gathered and the access point list is displayed together with the antenna bars (signal level), channel, and SSID information.
* For access points not broadcasting an SSID, the SSID column is left blank.

Furthermore, access point information can be looked up by selecting using top or bottom of the multi-function key and pressing the center. The information that can be looked up is as follows:
SSID, signal (dBm): reception level, mode, channel, MAC address (BSSID), beacon interval, and whether WEP is in use.

(4) Network connection

It is possible to specify the network settings and reboot.
From Admin Menu > Network config > Network reload, it is possible to select the settings using left and right of the multi-function key, and reboot by pressing the center.

9.4 Troubleshooting

9.4.1 Viewing the Display

The display shows **"Network Fail"**.

The device failed to connect to the wireless network. Check the following.

■ Is the connection method set to “Auto”?

When the connection method is set to “Manual”, wireless connection is not made automatically for that profile.

Check: Admin Menu > Network config > Network config > Config1 > Basic info

■ Are the SSID settings correct?

Check: Admin Menu > Network config > Network config > Config1 > WLAN

■ Are the WEP settings (WEP key, authentication algorithm, key index) correct?

Depending on the type of access point, Shared Authentication may not be supported. In such cases, set the authentication algorithm to Open Authentication.

Check: Admin Menu > Network config > Network config > Config1 > Security

■ Is the authentication method correct?

Check: Admin Menu > Network config > Network config > Config1 > Authenticate

* When running only WEP, select “None".

■ If running 802.1x authentication, has the certificate been installed?
Are the user ID and password correct?

Check: Admin Menu > Network config > Network config > Config1 > Authenticate

■ Are the IP address setting correct?

Check: Admin Menu > Network config > Network config > Config1 > TCP/IP

■ Do the Scan Channel settings match the operating environment?

Check the following user.ini file entry to confirm that all the channels used for operations have been included.

```
[WIFI_SCAN]
  Scan_Channel_List=1,6,11,14
```

The display shows “**Not register**”.

SIP server registration has failed. Check the following.

■ Does ping reach the proxy server?

Check: Menu > Network > Ping test

■ Are the user account settings correct? If using digest authentication, are the user ID and password correct?

Check: Admin Menu > Network config > SIP > User account

■ Are the SIP domain and proxy server address settings correct?

Check: Admin Menu > Network config > SIP > Server setup

The time and date do not match

■ If using NTP, is the NTP setting set to “Enabled”?

Check: Menu > Setup > Advanced > Time > Time server

■ Does ping reach the NTP server?

Check: Menu > Network > Ping test

■ If synchronizing the time using SIP messages, is the NTP setting set to “Disabled”?

When the NTP setting is set to “Disabled”, time synchronization using SIP messages is conducted automatically. Some SIP servers do not support this function. Check with your network administrator.

Check: Menu > Setup > Advanced > Time > Time server

An error message is displayed.

Refer to the next section, 9.4.2 Error Messages.

9.4.2 Error Messages

When you see the following error messages, take the following steps.

Message		Meaning/Action
000	Unable to find AP. Please find a wireless zone.	Device cannot connect to any AP. Check the AP signals, or SSID and authentication method.
001	WEP Authentication failed. Please verify WEP setting.	WEP authentication failed. Review the WEP settings.
002	Connection denied by AP.	Connection denied by AP. Contact the network administrator.
003	Connection with AP lost. Please find a wireless zone.	Lost connection with AP. Go back to an area covered by the wireless network.
100	AP may not be 8021.X capable. Please check network setting.	It is possible that the AP does not support 802.1X. Check the AP settings.
101	No response from server. Please check network setting.	No response from server. Check the settings of the authentication server and network.
102	Failed to load PrivateCert. Please check PW.	Check the password for rolling out private certificate.
103	No PrivateCert found. Please download PrivateCert.	Private certificate is not installed. Download a valid private certificate.
104	Invalid PrivateCert. Please check and re-download PrivateCert.	Private certificate is not valid. Download a valid private certificate.
105	No RootCert found. Please download RootCert.	Root certificate is not installed. Download root certificate.
106	Invalid RootCert. Please check and re-download RootCert.	Root certificate is not valid. Download a valid root certificate.
107	Authentication denied by server. Please check ID/PW.	Authentication denied by server. Check the ID/password.
108	Authentication denied by server. Please check Certificate.	Authentication denied by server. Check the certificate.
109	802.1X authentication failed due to time out.	Authentication failed due to timeout.
110	Authentication mode not supported by server. Please check authentication mode.	The server does not support this authentication mode. Check the authentication mode.
111	802.1X authentication failed due to unknown reason.	802.1x authentication failed. If this keeps happening, contact the network administrator.
200	DHCP server doesn' respond	There is no response from the DHCP server. Check the DHCP server settings.
201	IP is duplicated	There are duplicate IP addresses. Change the IP address.
202	Invalid IP Address	IP address is invalid. Check the IP address, subnet mask, and DefaultGateWay settings.

Details of Display		Items to be Checked
400	Your network firewall type is symmetric. Please ask your network administrator	The network type is symmetric. Contact the network administrator.
401	Your network firewall type is blocked. Please ask your network administrator	The network access is restricted. Contact the network administrator.
402	STUN Server address is invalid. Please check stun configuration item.	The STUN server address is invalid. Check the STUN settings.
500	DNS doesn't respond or SIP server address is invalid	There is no response from the DNS server or the SIP server address is invalid. Review the settings.
501	Register is failed (Unauthorized)	The registration failed (not authorized). Check the ID/password for digest authentication.
502	Register is failed (User is not approval)	The registration failed (not approved). Check to ensure that there is no problem with the ID for digest authentication.
503	Register is failed (User is not found)	The registration failed (user not found). Check to ensure that there is no problem with the ID for digest authentication.
504	Register is failed (Unknown)	The registration failed. Check to ensure that there is no problem with the ID for digest authentication.
505	Register is failed, SIP server doesn't respond	The registration failed. There is no response from the SIP server.

9.4.3 Other Problems

Phone call quality is poor.

■ The number of supported concurrent calls has been exceeded.

When the number of phone calls exceeds the maximum for a single channel, phone call quality will deteriorate severely.

See 5.4 Number of Concurrent Calls in this manual.

■ Signal interference/collision

If signal interference on the same channel results in collisions between wireless zones, voice quality may deteriorate. Check the following.

- Are there any external signals or invalid APs (unauthorized device brought in by a user)?
- Is signal interference resulting from adjacent AP channels using the same channel?
- Is traffic overload causing collisions?

■ The signal reception level (RSSI) is low

When the AP signal power is weak or when the AP is too far away, the terminal signal reception level may get too low and result in the deterioration of call quality.

Battery drains too quickly

■ The terminal is in an area where the signal is weak.

If the terminal signal reception level is weak, the number of scan operations will increase, resulting in short battery life.

■ The terminal is out of range

The device is designed to conduct AP scans regularly if the terminal is out of range. Thus, if the terminal is out of range for a long time, the battery will deplete quickly.

■ Broadcast Packet

If ARP, DHCP, etc. packets frequently flow into the wireless zone, the terminal will be more likely to exit power save mode, resulting in shorter battery life.

■ Battery Pack Wear

When used over a long period of time with repeated recharging, the battery pack will deteriorate to a point where it is unable to hold a charge.

■ AP Settings (DTIM, Beacon Interval)

In general, the smaller the values set for DTIM or the beacon interval, the quicker the battery will run down.

■ Insufficient Charge

If the battery is not recharged sufficiently, the battery will deplete in a shorter amount of time. Make sure to charge the battery until the blue LED is OFF.

■ Talk Time

Significant power is consumed when in conversation mode and the battery will drain quickly.

The recharge lamp does not turn on when the device is placed on the charger.

■ The device is not completely on the cradle.

When charging, make sure to place the device in the cradle by pressing down until you hear a click and then confirm that the blue LED is ON.

■ Over-discharge

Even if you remove the battery pack from the unit, the battery will discharge over time. If you do not charge the battery for too long, the battery may over-discharge and you will no longer be able to charge the batter pack. When you purchase the device, even if you do not plan to use it for some time, make sure you fully charge the battery once before storing and recharge the battery at least once every six months. When voltage falls below a certain level due to discharge, the LED lamp may not turn ON when you charge the battery, but this is because a protector circuit works to reduce the initial charge current. After several minutes, the LED will turn ON and recharging will begin. (If the LED does not turn ON within one hour, the battery may have aged beyond use.)

■ Full charge

When the battery is fully charged, the blue LED on the terminal turns OFF.

Cannot transmit

■ Not registered

You cannot transmit when the display shows “Not registered” (not registered in the SIP server).

■ Signal level is low

When the AP signal becomes weak or when the AP is too far away, the terminal signal reception level may get too low and the device may not be able to transmit.

■ Repeated transmission

If the number of transmissions exceeds ICT_Transaction_Max_Count over a 31.5 second period (TimerD), the terminal displays the message “Cannot transmit”.

Cannot receive transmission

■ Signal level is low

When the AP signal becomes weak or when the AP is too far away, the terminal signal reception level may get too low and the device may not be able to receive transmissions.

Forwarding Settings

Messages will not reach the terminal if forwarding has been setup on the SIP server. Make sure you disable forwarding.

Call becomes one way.

■ Mute Settings

You can enable mute by pressing the right soft key during a conversation. This will halt the transmission of voice packets from your terminal. To cancel this setting, press the right soft key again.

If this does not solve the problem, investigate the network (access point/SIP server) side.

No response to key operations

■ Not registered

If the terminal shows that the device is not registered (in the SIP server), dial key operations are disabled.

■ Key lock

Confirm that the key lock is not enabled. See Enabling/Disabling the Key Lock in section 6 of the User Manual.

No Ring Tone

■ Ring tone settings

Check that the ring tone is not set to the lowest level (silent). See Adjusting the Volume in section 6 of the User Manual.

■ Silent Mode

Confirm that the device has not been set to silent mode. See Setting/Canceling Silent Mode in section 6 of the User Manual.

Cannot hear key tones

■ Key tone volume

Confirm that the key tone volume has not been set to the minimum level (silent). See Setting/Canceling Silent Mode in section 6 of the User Manual.

* If the above does not solve your problem, there may be a problem with the hardware. Contact the dealer or store from which you purchased the device.

9.4.4 SYSLOG Message Table

The following table lists the SYSLOG messages for the WirelessIP5000-A.

From Menu > Settings > Log Display > Error Logs, set SYSLOG Use/Do Not Use and the server address.

Log message	Level	Description
SIP connection Information : SRC IP(%s), PORT(%d)	Info	SIP registeration is completed.
DHCP bind succeeded : IP address(%s)	Info	DHCP binding is completed.
Program upgrade SUCCEEDED : version (%s)!!!	Info	Version up is succeeded.
Program upgrade FAILED : version (%s)!!!	Info	Version up is failed.
Configuration upgrade SUCCEEDED!!!	Info	Configuration update is succeeded.
Configuration upgrade FAILED!!!	Info	Configuration update is failed.
Network Binding : Program Version(%s), Bootrom Version(%s), H/W Version(%s)	Info	Network binding is succeeded after powered on.
Received invalid SIP message	Warning	Invalid SIP messasge is received.
ReINVITE : Non-Supported Payload Type, RemoteIP(%s), Remote Port(%d)	Warning	Non-supported payload type is received.
200OK : Call or Transaction does not exist	Warning	200OK for unknown transaction is received.
BYE : Call/Transaction does not exist	Warning	BYE for unknown transaction is received.
Failure response : Call/Transaction does not exist	Warning	4xx, 5xx or 6xx for unknown transaction is received.
Informative response : Call/Transaction does not exist	Warning	1xx, 2xx or 3xx for unknown transaction is received.
Fail to send SUBSCRIBE for pickup	Warning	Sending SUBSCRIBE for pickup is failed.
Fail to send SUBSCRIBE for presence	Warning	Sending SUBSCRIBE for Presence is failed.
Reigstration[%d] : authentication fail	Warning	Registration with authentication is failed.
Registration[%d] : no response, retry after %d millisecond	Warning	No response from SIP server.
Extension method : Non-supported SIP method(%s)	Warning	Non-supported SIP method is received.
Fail to send SUBSCRIBE for MWI	Warning	Sending SUBSCRIBE for MWI is failed.
Initial-INVITE : invalid ip address in sdp	Error	Initial INVITE with invalid IP address in SDP is received.
Fail to send Subscribe : Send to bad destination address (%s).	Error	Sending SUBSCRIBE with invalid destination address is failed.
DNS : host information for %s not found	Error	No answer from DNS server.

First Edition, October 2006
Second Edition, April 2007