

BeneVision TM80
Telemetry Monitor


Service Manual

Intellectual Property Statement

SHENZHEN MINDRAY BIO-MEDICAL ELECTRONICS CO., LTD. (hereinafter called Mindray) owns the intellectual property rights to this product and this manual. This manual may refer to information protected by copyrights or patents and does not convey any license under the patent rights of Mindray, nor the rights of others. Mindray does not assume any liability arising out of any infringements of patents or other rights of third parties.

Mindray intends to maintain the contents of this manual as confidential information. Disclosure of the information in this manual in any manner whatsoever without the written permission of Mindray is strictly forbidden.

Release, amendment, reproduction, distribution, rent, adaptation and translation of this manual in any manner whatsoever without the written permission of Mindray is strictly forbidden.

mindray,  and **MINDRAY** are the registered trademarks or trademarks owned by Mindray in China and other countries. All other trademarks that appear in this manual are used only for editorial purposes without the intention of improperly using them. They are the property of their respective owners.

This posting serves as notice under 35 U.S.C. § 287(a) for Mindray patents:
<http://www.mindrayna.com/patents>.

For this manual, the issued Date is January 2019 (Version: 3.0).

© 2017-2019 Shenzhen Mindray Bio-Medical Electronics Co., Ltd. All rights reserved

NOTE

- **This manual describes all features and options. The equipment may not have all of them. Contact Mindray service department for any questions.**
-

Manufacturer's Responsibility

Contents of this manual are subject to changes without prior notice.

All information contained in this manual is believed to be correct. Mindray shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Mindray is responsible for the effects on safety, reliability and performance of this product, only if:

- All installation operations, expansions, changes, modifications and repairs of this product are conducted by Mindray authorized personnel;
- The electrical installation of the relevant room complies with the applicable national and local requirements;
- The product is used in accordance with the instructions for use.

WARNING

- **This manual is for biomedical engineers or technicians responsible for troubleshooting, repairing, and maintaining the telemetry monitoring system.**
-

Return Policy

In the event that it becomes necessary to return a unit to Mindray, follow the instructions below.

1. Obtain a return authorization.

Contact the Mindray Service Department and obtain a Mindray Customer Service Authorization Number. The Mindray Customer Service Authorization Number must appear on the outside of the shipping container. Return shipments will not be accepted if the Mindray Customer Service Authorization Number is not clearly visible. Please provide the model number, serial number, and a brief description of the reason for return.

2. Freight policy

The customer is responsible for freight charges when this product is shipped to Mindray for service (including any relevant customs fees or other freight related charges).

3. Return address

Please send the part(s) or equipment to the address offered by Customer Service Department.

Contact Information

Manufacturer: Shenzhen Mindray Bio-Medical Electronics Co., Ltd.
Address: Mindray Building, Keji 12th Road South, High-tech Industrial park, Nanshan, Shenzhen 518057, P.R.China
Website: www.mindray.com
E-mail Address: service@mindray.com
Tel: +86 755 81888998
Fax: +86 755 26582680

Distributor: Mindray DS USA, Inc.
Address: 800 MacArthur Boulevard, Mahwah, New Jersey 07430, USA
Tel: 1.800.288.2121, 1.201.995.8000
Website: <http://www.mindraynorthamerica.com/>

Preface

Manual Purpose

This manual provides detailed information about the assembling, disassembling, testing and troubleshooting of the equipment to support effective troubleshooting and repair. It is not intended to be a comprehensive, in-depth explanation of the product architecture or technical implementation. Observance of the manual is a prerequisite for proper equipment maintenance and prevents equipment damage and personnel injury.

This manual is based on the maximum configuration. Therefore, some contents may not apply to your device. If you have any question, please contact our Customer Service Department.

Intended Audience

This manual is for biomedical engineers, authorized technicians or service representatives responsible for troubleshooting, repairing and maintaining the TM80 Telemetry Monitors.

FOR YOUR NTOES

Table of Contents

- 1 Safety1-1**
 - 1.1 Safety Information 1-1
 - 1.1.1 WARNINGS..... 1-2
 - 1.1.2 Cautions..... 1-3
 - 1.1.3 Notes..... 1-4
 - 1.2 Equipment Symbols 1-4
- 2 Overview2-1**
 - 2.1 Product Overview.....2-1
 - 2.2 Key Features..... 2-2
 - 2.3 Introduction to TM80 Telemetry Monitoring System..... 2-2
 - 2.3.1 Module Configurations for the TM80 Telemetry Monitor 2-3
 - 2.3.2 Connection Diagram of the TM80 Telemetry Monitor..... 2-4
 - 2.4 Architecture of the TM80 Telemetry Monitoring System..... 2-5
- 3 Installation3-1**
 - 3.1 Overview.....3-1
 - 3.1.1 Introduction 3-1
 - 3.1.2 Business Types..... 3-2
 - 3.1.3 Installation Process 3-4
 - 3.2 Network Requirements of the TM80 3-8
 - 3.2.1 Requirements for Network Feasibility..... 3-9
 - 3.2.2 Configuration Requirements for WLAN of TM80.....3-18
 - 3.3 Configuration of Cisco Network Devices.....3-21
 - 3.3.1 Recommended Devices.....3-21
 - 3.3.2 Configuration Description3-22
 - 3.3.3 WLAN Settings.....3-23
 - 3.3.4 CONTROLLER Settings.....3-28
 - 3.3.5 WIRELESS Settings.....3-30
 - 3.4 Configuration of Aruba Network Devices3-35

3.4.1 Recommended Devices	3-35
3.4.2 Login	3-36
3.4.3 Wireless Setting	3-37
3.4.4 Network Setting	3-43
3.5 Configuration of Netgear Network Devices	3-44
3.5.1 Preparation	3-45
3.5.2 Setting Single AP	3-46
3.5.3 Wireless Settings (5G)	3-52
3.5.4 Setting Multiple APs	3-55
3.6 Network Deployment Planning	3-58
3.6.1 Tools and Resources	3-58
3.6.2 Environmental Survey	3-58
3.7 Network Deployment Implementation	3-63
3.7.1 Preparations before Equipment Installation	3-63
3.7.2 Roaming Consideration	3-64
3.7.3 Services Provided During and After Installation	3-64
3.8 Network Verification	3-65
3.8.1 Tools and Resources	3-65
3.8.2 Wi-Fi Signal Calibration	3-65
3.8.3 Confirm Network Feasibility	3-66
3.8.4 Network Verification Process	3-67
3.9 Configuring WLAN Settings of TM80	3-68
3.9.1 WLAN Setup	3-69
3.9.2 EAP Setup	3-70
3.9.3 EAP Certificate Management	3-71
3.9.4 WLAN TEST	3-79
3.9.5 5G Band Channels	3-82
3.10 Network Verification with TM80	3-82
3.10.1 Test Preparation	3-82
3.10.2 Connecting a TM80 to the Central Station	3-83
3.10.3 Test Preparation	3-84
3.10.4 Coverage Confirmation	3-84

3.10.5 TM80Acceptance Confirmation.....	3-86
3.11 Appendices.....	3-87
3.11.1 TM80 Wi-Fi Network Requirement Table.....	3-87
3.11.2 Environmental Survey Table.....	3-91
3.11.3 Network Acceptance Table	3-96
3.11.4 TM80 Verification Confirmation Table.....	3-102
4 Product Principles	4-1
4.1 System Composition.....	4-1
4.2 System Signal Flow	4-4
5 Testing and Maintenance	5-1
5.1 Recommended Maintenance and Test Frequency	5-2
5.2 Inspection before Daily Use.....	5-2
5.3 Preventative Maintenance Procedures.....	5-3
5.4 Parameter Test.....	5-3
5.4.1 ECG Test.....	5-3
5.4.2 Resp Test	5-5
5.4.3 SpO ₂ Test.....	5-6
5.4.4 NIBP Tests.....	5-7
5.5 Miscellaneous Tests.....	5-10
5.5.1 Visual Inspection.....	5-10
5.5.2 Power-On Test	5-11
5.5.3 Nurse Call Test	5-11
5.5.4 Electric Safety Test	5-11
5.5.5 Network Print Test	5-12
5.5.6 Battery Check	5-12
6 Hardware Upgrade.....	6-1
6.1 Adding the SpO ₂ Function	6-1
6.2 Adding the NIBP Module (BP10).....	6-1
6.3 Adding the Number of the TM80 Telemetry Monitors	6-2

6.4 Extending Coverage	6-3
7 Troubleshooting	7-1
7.1 Common Faults.....	7-1
7.1.1 The TM80 Failed to Connect to the Central Station.....	7-1
7.1.2 The TM80 Are Offline Frequently.....	7-2
7.1.3 The TM80 Cannot Be Powered On.....	7-2
7.1.4 The Working Duration of Battery Becomes Short	7-3
7.2 Technical Alarms	7-3
7.3 Other Faults.....	7-12
7.4 Error Codes.....	7-17
8 Disassembly	8-1
8.1 Overview.....	8-1
8.2 Disassembling the TM80	8-2
8.3 Disassembling the BP10.....	8-9
9 Maintenance Materials.....	9-1
9.1 Overview of Maintenance Materials.....	9-1
9.2 TM80 Front Housing Assembly (Wi-Fi).....	9-2
9.3 TM80 Rear Housing Assembly(Wi-Fi)	9-3
9.4 TM80 Main Unit (Wi-Fi).....	9-5
9.5 BP10 Front Housing Assembly	9-6
9.6 BP10 Rear Housing Assembly	9-7
9.7 BP10 Main Unit.....	9-8
9.8 Exploded View of Central Charger	9-9
A Electrical Safety Inspection.....	A-1
A.1 Electrical Safety Tests for the TM80, BP10, and Central charger.....	A-1
A.2 Power Cord Plug.....	A-2
A.3 Device Enclosure and Accessories.....	A-3
A.4 Device Labeling	A-4

A.5 Earth Leakage Test	A-4
A.6 Patient Leakage Current	A-6
A.7 Mains on Applied Part Leakage	A-9
A.8 Patient Auxiliary Current	A-12
A.9 Scheduled Electrical Safety Inspection	A-14
A.10 Electrical Safety Inspection after Repair	A-14
A.11 Electrical Safety Inspection Form.....	A-15

FOR YOUR NOTES

1 Safety

1.1 Safety Information

WARNING

- Indicates a potential hazard or unsafe practice that, if not avoided, could result in death or serious injury.
-

CAUTION

- Indicates a potential hazard or unsafe practice that, if not avoided, could result in minor personal injury or product/property damage.
-

NOTE

- Provides application tips or other useful information.
-

1.1.1 WARNINGS

WARNING

- **The TM80 Telemetry Monitor must be operated by medical personnel inhospitals or medical institutions.**
 - **For continued safe use of the TM80 Telemetry Monitor, the instructions given in this manual must be followed. But instructions in this manual in no way supersede established medical procedures.**
 - **To avoid explosion hazard, do not use the TM80 Telemetry Monitor in the presence of oxygen-rich atmospheres, flammable anesthetics, or other flammable agents.**
 - **The TM80 Telemetry Monitor is not to be used in the vicinity of electrosurgical units because such use may interrupt or interfere with the transmission of signals from the TM80 Telemetry Monitor.**
 - **Do not use the TM80 Telemetry Monitor in conjunction with Electro Surgical Unit (ESU).**
 - **Do not expose the TM80 Telemetry Monitor to a Magnetic Resonance (MR) environment.**
 - **We recommend that the latest WPA2-PSK security encryption mode be used when the TM80 Telemetry Monitor is in use.**
 - **Auditory alarm signal sound pressure levels that are less than ambient levels can impede operator recognition of alarm conditions.**
-

1.1.2 Cautions

CAUTION

- Do not let the display of the TM80 Telemetry Monitor directly touch the patient's skin when the display is on.
 - When the Central Station presents the alarm "Offline", check the network connection status.
 - When disposing of the packaging material, be sure to observe the applicable local waste control regulations and keep it out of children's reach.
 - Mindray takes no responsibility for controlling the radio frequency environment in a hospital. If interference for the operating frequency of telemetry equipment exists, the telemetry equipment performance will be affected. Exercise caution when selecting the operating frequency of all the wireless equipment in a hospital as this is very important to avoid mutual interference among them.
 - Magnetic and electrical fields are capable of interfering with the proper performance of the TM80 Telemetry Monitor. For this reason, make sure that all external equipment operated in the vicinity of the TM80 Telemetry Monitor comply with the relevant EMC requirements. Mobile phone, X-ray equipment, micro-wave oven, interphone, or MRI equipment are a possible source of interference as they may emit higher levels of electromagnetic radiation.
-

1.1.3 Notes

NOTE

- Put the TM80 Telemetry Monitor in a location where you can easily see the screen and access the operating controls
 - The software of the TM80 Telemetry Monitor was developed in compliance with IEC60601-1-4. The possibility of hazards arising from software errors is minimized.
 - This manual describes all features and options. Your equipment may not have all of them.
 - Keep this manual in the vicinity of the equipment so that it can be obtained conveniently when needed. Provides application tips or other useful information.
-

1.2 Equipment Symbols

See *TMS60 Telemetry Monitoring System/TM80 Telemetry Monitor Operator's Manual* for information about the symbols used on this product and its packaging.

2 Overview

2.1 Product Overview

The TM80 telemetry monitor is intended for use on Adult and Pediatric patients over three years old to monitor ECG, Resp, SpO₂, and NIBP physiological data. The physiological data can be reviewed locally on the display of the monitor. The CentralStation will support ECG, Heart Rate, SpO₂, NIBP, Resp, Pulse Rate, Arrhythmia analysis, QT monitoring, and ST Segment Analysis for the TM80.

The TM80 telemetry monitor can only be admitted by the Central Monitoring System (CMS) whose version is 03.00 or above.

WARNING

- **The TM80 Telemetry Monitor must be operated by medical personnel in hospitals or medical institutions.**
- **The TM80 Telemetry Monitor is not designed for monitoring critically ill patients.**
- **As the TM80 Telemetry Monitor transmits data wirelessly, there might be a risk of data loss.**
- **The TM80 Telemetry Monitor can be powered by a rechargeable lithium-ion battery (P/N 022-000196-00) or three AA batteries (P/N 0000-10-10902).**
- **Misuse or improper maintenance of the rechargeable lithium-ion battery can cause a battery to overheat during use.**
- **High temperatures can cause burns to the TM80. Refer to *Chapter 13 Battery of BeneVision TMS60 Telemetry Monitoring System/TM80 Telemetry Monitor Operator's Manual (P/N 046-007056-00)* for the maintenance methods.**

WARNING

- **Before maintaining and repairing the TM80 Telemetry Monitor, familiarize yourself with the *BeneVision TMS60 Telemetry Monitoring System/TM80 Telemetry Monitor Operator's Manual***
-

2.2 Key Features

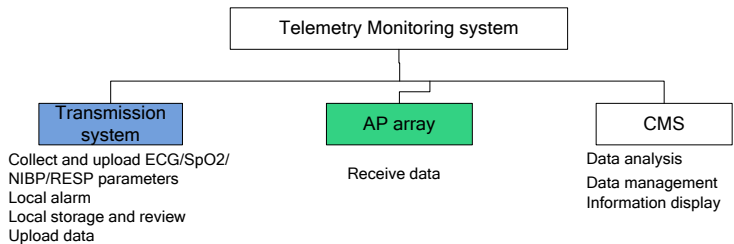
- Easy for clinicians to use and comfortable for patients to wear
- Low power consumption
- Supports IEEE 802.11a/b/g/n/ac and 2.4GHz/5Ghz dual Wi-Fi band
- Able to be accessed to the existing wireless networks in a hospital directly

2.3 Introduction to TM80 Telemetry Monitoring System

The TM80 Telemetry Monitor consists of a transmission system, a receiving system, and a central monitoring system (abbreviated as CMS).

- The transmission system refers to the TM80 Telemetry Monitor with optional BP10 and SAT10 SpO₂ modules. The SpO₂ module is connected to the SpO₂ sensor connector and then plugged into the SpO₂ connector on the TM80. The BP10 is a standalone module and communicates with the TM80 via Mindray Patient Area Network (abbreviated as MPAN).
- The receiving system refers to the Wi-Fi network, including APs, switches, and routers. The TM80 can use the dedicated Wi-Fi network provided by Mindray or share the hospital's network with other devices in the hospital. The network must comply with the wireless specifications of Mindray. For details of specifications, refer to **3Installation**.
- The CMS refers to BeneVision Central Monitoring System. For details about the Benevision Central Monitoring System, refer to ***BeneVision Central Monitoring System Operator's Manual (P/N H-046-010879-00)***.

The following figure shows relationships among the subsystems.



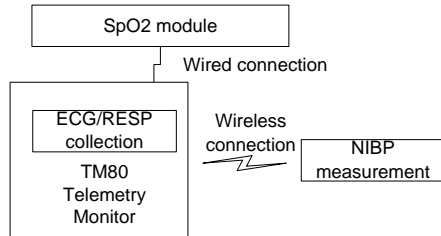
2.3.1 Module Configurations for the TM80 Telemetry Monitor

The table below shows the ECG, Resp, SpO₂, and NIBP configuration status for the TM80 Telemetry Monitor.

Parameter	Standard	Optional
ECG	Yes	/
Resp	/	Yes
SpO ₂	/	Yes
NIBP	/	Yes

2.3.2 Connection Diagram of the TM80 Telemetry Monitor

The following figures illustrates how the ECG, SpO₂, and NIBP modules are connected to the TM80 Telemetry Monitor.

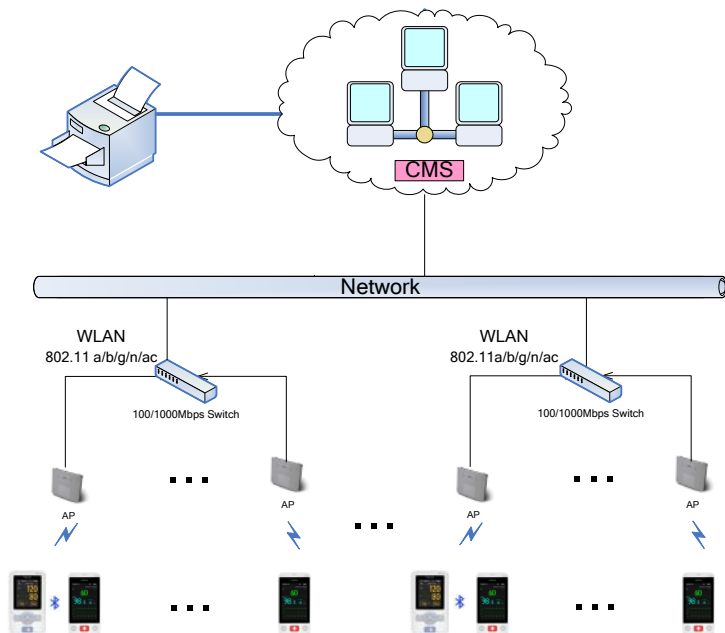


The ECG and Resp collection circuit is designed inside the TM80 Telemetry Monitor. The SpO₂ module and sensor constitute a SpO₂ cable. The SpO₂ module is connected to the TM80 Telemetry Monitor via the SpO₂ cable.

Hard connection is used between the cable and the monitor. The NIBP module is a standalone module and performs short-range wireless communication with TM80 Telemetry Monitor.

2.4 Architecture of the TM80 Telemetry Monitoring System

The following figure illustrates the physical units of the TM80 Telemetry Monitoring System. It shows how these devices and functional units are interconnected to form a complete telemetry monitoring system.



The TM80 Telemetry Monitors are worn on patients. As shown in the figure above, patients' physiological information collected by the TM80 Telemetry Monitors is transmitted through the low power consumption Wi-Fi modules built in the telemetry monitors. Wireless signals are acquired by AP arrays and then are transmitted to the CMS through the existing network system of the hospital. On the CMS, the information is displayed, stored and processed based on a certain algorithm and alarms are generated. In addition, patients can seek for help from nurses on the CMS side by using the nurse call function. When a TM80 Telemetry Monitor is connected to the CMS, doctors can view its patient information in the ViewBed window of the CMS.

FOR YOUR NOTES

3 Installation

3.1 Overview

3.1.1 Introduction

The TM80 Telemetry Monitor (hereinafter called TM80) exchanges data with the CMS via Wi-Fi network. Wi-Fi communication is the core function of the TM80. This chapter guides users to use the Wi-Fi communication function properly and reliably.

WARNING

- **To ensure reliable operation of the TM80 wireless network, deploy the network in strict accordance with relevant requirements in this manual and keep maintaining the network properly after installing the TM80. If the network is not deployed according to this manual, data transmission of the TM80 may be delayed, or even be lost, thus resulting in clinical risks.**

CAUTION

- **Customers are responsible for network management. Changing network after installation may deteriorate the performance of the TM80. Therefore, customers need to sufficiently assess network change so as to avoid impact on clinical use of the TM80.**
-

3.1.2 Business Types

The WLAN deployment requires certain techniques and accumulation of experience. On the market, professional communication technical service companies such as local agents of Cisco implement the engineering in most cases. Mindray recommends hospitals to choose the third-party engineering deployment agencies to complete network environment deployment in preference.

Three processing modes are provided for different circumstances:

- The hospital has built its WLAN: Mindray defines specification requirements and acceptance methods, inspects the hospital by sending field engineers to the hospital and confirms the requirements on site. If the hospital's network cannot meet deployment requirements of the TM80, Mindray informs the hospital of possible consequences such as disconnection and requires the hospital to rectify the WLAN according to requirements of Mindray.
- The hospital builds a new WLAN to cover areas greater than 2000 square meters for the TM80, and IT requirements are complex: Mindray recommends that a third-party construction organization carries out construction and completely uses the network devices and configurations developed and verified by Mindray. Mindray defines specification requirements and acceptance methods, inspects the hospital by sending field engineers to the hospital and confirms the requirements on site after the construction organization completes confirmation. The third-party construction organization must have: documents of detailed internal construction specifications (including construction process, safety precautions, and construction process inspection checklist) and successful engineering cases in schools, hotels, and even hospitals of similar scale.

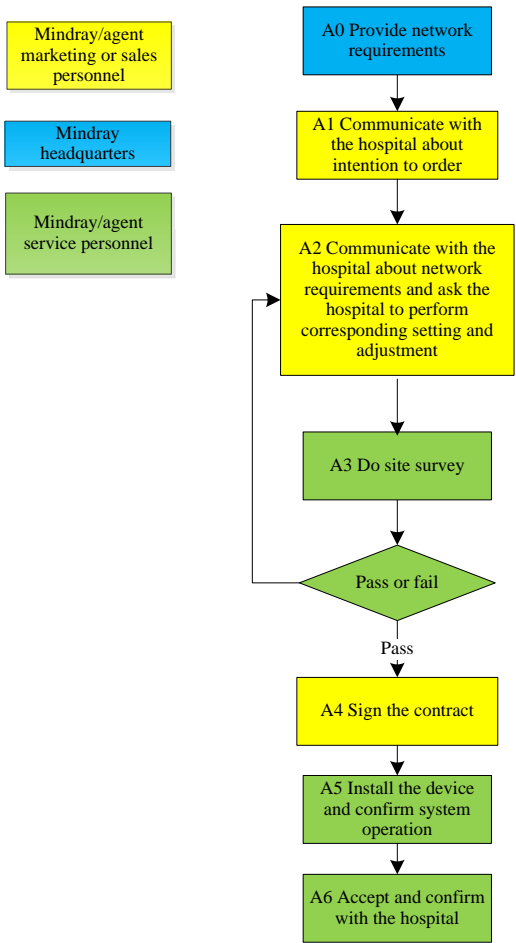
- The hospital builds a new WLAN to cover areas less than 2000 square meters for the TM80 and there are no other requirements except for connection to Mindray monitors: Mindray contacts the construction organization and completely uses the network devices and configurations developed and verified by Mindray. Mindray defines specification requirements and acceptance methods, inspects the hospital by sending field engineers to the hospital and confirms the requirements on site. Compared with the previous circumstance, Party A for network deployment engineering is changed from the hospital to Mindray. Mindray needs to play a greater role in supervision.

This chapter focuses on wireless network deployment requirements. The architecture and configuration requirements of Mindray's wired network are described in another document.

3.1.3 Installation Process

3.1.3.1 Using Hospital's WLAN

If the hospital has built its WLAN, the installation process is illustrated as follows:



List of outputs

Action	Output	Requirements	Template
A0	Basic requirements for deployment of the TM80 network	Determine specific requirements for deployment of the TM80 network.	3.11.1TM80 Wi-Fi Network Requirement Table
A3	Environmental survey report	Confirm that the wireless environment of the customer meets requirements of the TM80 by means of questionnaire and measurement.	3.11.2Environmental Survey Table
A5	Network acceptance report	Confirm that the customer network meets requirements of the TM80 by means of questionnaire and measurement.	3.11.3Network Acceptance Table
A6	Sample verification confirmation table	Confirm the actual operation of the sample after the sample is installed.	3.11.4TM80 Verification Confirmation Table

CAUTION

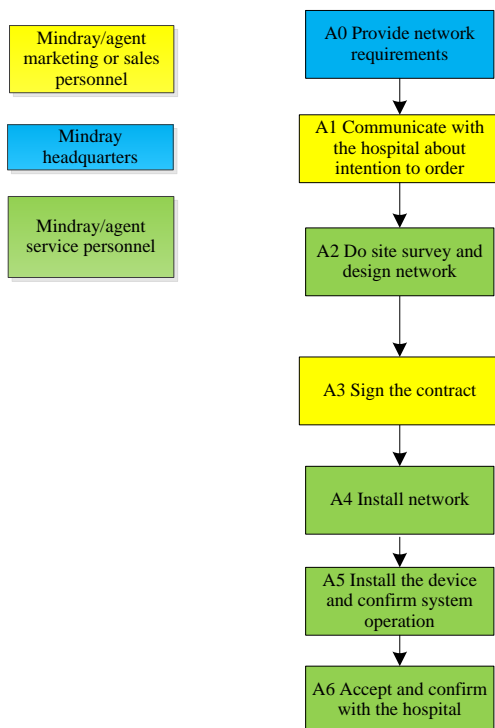
- **If the customer network cannot meet the requirement in 3.11.2Environmental Survey Table, the service personnel should perform pilot run of the TM80 for at least 24 hours first to ensure that the wireless environment is compatible before signing a contract.**
-

NOTE

- **Contents in 3.11.2Environmental Survey Table are actually part of 3.11.3Network Acceptance Table. If service personnel have already performed environmental survey, they can fill the survey results in the Network Acceptance Table directly.**

3.1.3.2 Installing New WLAN for TM80

If the hospital plans to build a new WLAN for the TM80, make sure that there is at least one idle wifi channel that is not in use. Otherwise, you can't make Co-channel interference meet TM80's requirement after the new WLAN is built. The installation process is illustrated as follows:



List of outputs

Action	Output	Requirements	Template
A0	Basic requirements for deployment of the TM80 network	Determine specific requirements for deployment of the TM80 network.	3.11.1TM80 Wi-Fi Network Requirement Table
A2	Network design document, Bill of material	/	/
A5	Network acceptance report	Confirm that the installed network meets requirements of the TM80 by means of self-check and measurement.	3.11.3Network Acceptance Table
A6	Sample verification confirmation table	Confirm the actual operation of the sample after the sample is installed.	3.11.4TM80 Verification Confirmation Table

NOTE

-
- **This manual only shows a reference for installing new WLAN for TM80 in section 3.7. Network deployment project needs much more complex process, you need professional IT engineer's help to finish the job.**
-

3.2 Network Requirements of the TM80

The TM80 transmits vital signs of patients in real time. The requirements for real-time and reliability are higher than those for audio and video services. The TM80 is powered by a battery. It adopts low power Wi-Fi technology. Therefore, the network needs to meet specific requirements to ensure reliable operation.

The network requirements of TM80 can be classified into six types:

- Wireless coverage
- AP capability and compatibility
- WLAN features
- EAP Requirement for RADIUS Server and Certs
- Network service and VLAN
- Some important settings of network device

The first four types are decided by infrastructure of network. They can't be modified easily. If the network does not meet the requirements before TM80 is installed, network dropping-off may happen easily after installation.

The fifth and sixth types belong to configuration of network. They need hospital IT department's help to achieve. According to experience of Mindray, the two types can guarantee reliable performance of TM80 effectively. If any requirement is not met, network dropping-off may happen in certain situation. If the number of devices using the same network is small, and no device needs high wireless bandwidth, the possibility of dropping-off can be reduced.

3.2.1 Requirements for Network Feasibility

Before installing TM80 telemetry monitors, it is very important to confirm network feasibility.

Wireless coverage, WLAN features and AP capability and compatibility are decided by infrastructure of network, infrastructure of network can't be modified easily. If the network does not meet the requirements before TM80 is installed, network dropping-off may happen easily after installation.

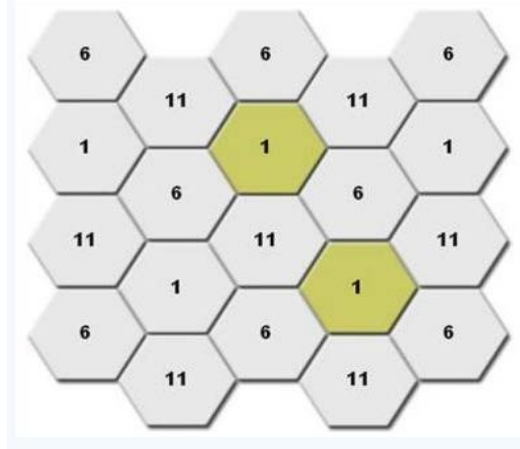
3.2.1.1 Requirements for the Wireless Coverage

The wireless coverage must be well controlled to ensure that TM80 can achieve the maximum data-rate and the lowest packet loss ratio. TM80 data is real-time upstream data streams and is similar to VoIP data. Monitoring data carries real-time physiologic information about patients. Therefore, reasonable wireless coverage must be provided for monitors. In particular, because the telemetry device TM80 is worn on human body, the signal may become poorer due to blocking of human body.

The requirements of the TM80 for wireless coverage are as follows:

No.	Item	Requirements of the TM80	Description
1	Received signal strengths (RSSI)	≥ -65 dBm Signal coverage requirement for APs connected to the TM80: RSSI value displayed on the TM80	The requirement must be met.
2	Co-channel interference*	≤ -20 dB Measured on the same channel of the TM80	The requirement must be met.
3	Ping delay	The mean delay of PC or cell phone with normal wifi module is smaller than 100ms and the packet lost rate shall be less than 1%.	The requirement must be met.

Co-channel interference is the most obvious interference for Wi-Fi. The signal strength of the nearest AP perceived by the wireless monitor must be 20 dB higher than that of other APs on the same channel. Take 2.4 GHz band as an example. The following channel deployment is recommended to realize Wi-Fi coverage similar to cellular coverage.



For co-channel interference, the interference between floors needs to be considered and the following case should be avoided: a pair of APs is set nearby between two floors and is working on the same channel. Different SSIDs of the same AP do not generate co-channel interference (CCI) . CCI from different AP but Same SSID can be accepted in 2.4G band, but this is highly recommended to be avoided.

3.2.1.2 Requirements for the AP capability

Because the low-power WIFI module is sleeping periodically and the capability for dealing with wireless data is reduced, it is necessary to use high-performance AP to enhance the stability of total system. Mindray tested a lot with TM80 and Cisco APs, the compatibility of Cisco AP is proven good.

We recommend using the network equipment verified by Mindray. This verification activity includes confirmation of network architecture, equipment model, firmware version, and specific configurations.

If network equipment whose compatibility is not confirmed by Mindray is used, potential risks may exist during operation of the TM80. In this case, Mindray recommends the customer to perform pilot run of the TM80 for at least 24 hours first to ensure that the equipment is compatible.

Device density needs to be controlled. If too many devices are mounted under one AP, competition among devices becomes fiercer. For low power consumption Wi-Fi, high data loss probability will be caused. Therefore, the number of devices under the same AP must be controlled. The TM80 requires one AP to mount a maximum of 16 devices.

No.	Item	Requirements of the TM80	Description
1	Recommended AP	Mindray's recommendations: Cisco: WLC 2504 (version 7-4-121-0 or later) + LAP: 2802 or 2602 or FAT AP:2602 Aruba: 7500 series+LAP: APIN0205 Netgear: WNDAP350 Notes: If the AP is 2802 or WNDAP350,TM80 can only use 5G	Nice to meet
2	AP capability	1.The anticipated number of devices connecting to one AP must be lower than the AP capability ,and capability should has a margin of 50%. For example, In the coverage of one AP, the typical number of devices	The requirement must be met.

No.	Item	Requirements of the TM80	Description
		connected to this AP is 16, then the announced number of devices than can connect to AP simultaneously must be more than 32. 2. The AP Can create several SSIDs.	
3	Device density	The maximum number of devices connected to one AP simultaneously is 16 (including TM80 and other devices).	The requirement must be met.
4	AP compatibility	When customer using APs not from Cisco, compatibility test should be passed	The requirement must be met.

3.2.1.3 Requirements for WLAN Features

The requirements of the TM80 for WLAN features are as follows. If WLAN is of other features, e.g. using 802.11ac, TM80 will not support, and can't connect to network. The TM80 adopts low power consumption Wi-Fi technology. If the amount of broadcast or multicast data is too large on the network, the device wake-up time increases, the standby duration is shortened, and even Wi-Fi transmission interruption is caused. Therefore, the TM80 must use an independent VLAN and work in a different network segment from the CMS, so as to control the amount of broadcast data. An AP can be configured with multiple SSIDs and associated with a VLAN. The TM80 needs to use an independent SSID.

No.	Item	Requirements of the TM80	Description
1	802.11 protocol	TM80 only support 802.11 a/b/g/n, WLAN can't use other protocols	The requirement must be met.
2	Security mode	TM80 supports: WPA/WPA2-PSK or WPA2-Enterprise EAP method: PEAP-GTC, PEAP- MSCHAPv2,EAP-TLS WPA2-PSK is highly recommended. WPA2-Enterprise may increase probability of offline when roaming, so not be recommended. WLAN can't use other security mode.	The requirement must be met.
3	AP MAC address	The broadcast MAC address of AP is fixed (BSSID). AP BSSID is used to locate the TM80 device. If it is changed, failure to locate the TM80 may occur.	The requirement must be met.
4	AP channel width	If the AP supports 802.11n/ac, set the channel width to 20Mhz, don't use HT40 or even HT80.	The requirement must be met.
5	Dedicated VLAN	The TM80 needs to work on a dedicated VLAN. Using VLAN can minimize Broadcast or multicast data which can affect TM80 stability.	The requirement must be met.

3.2.1.4 EAP Requirements for RADIUS Server and Certs

RADIUS Server

The following RADIUS Server is validated by Mindray:

- Cisco ACS
- FreeRADIUS
- Network Policy Service(in Windows Server 2008 R2 and Windows Server 2012 R2)

Algorithm

The following table list the EAP methods and TLS1.0 algorithm that TM80 supported for each RADIUS Server:

RADIUS Server	EAP Methods	TLS Cipher Suites
NPS	PEAP-MSCHAPV2 EAP-TLS	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5
ACS	PEAP-MSCHAPV2 PEAP-GTC EAP-TLS	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(Elliptic curve: secp256r1) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(Elliptic curve: secp256r1) TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5
FreeRADI	PEAP-MSCHAPV2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA(Elli

RADIUS Server	EAP Methods	TLS Cipher Suites
US	PEAP-GTC EAP-TLS	ptic curve: secp256r1) TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(Elli ptic curve: secp256r1) TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_RC4_128_SHA TLS_RSA_WITH_RC4_128_MD5

Certification:

The general requirements for the CA Cert:

- Supported Public Key Algorithm: RSA
- Supported Key Size: 512, 1024, 2048
- Supported Hash Algorithm: SHA1 and MD5
- Supported File Format: PEM(.PEM)
- Do not support certification chain and CRL

The general requirements for the User Cert:

- This User Cert should contain both the user certification and the **unencrypted** pkcs#8 private key
- Supported Key Algorithm: RSA
- Supported Key Size: 512, 1024, 2048
- Supported Hash Algorithm: SHA1 and MD5
- Supported File Format: PEM(.PEM)

The specified requirement for FreeRADIUS:

- The supported algorithm used to encrypt the keys of CA and User Cert:
3DES, AES128, AES256
- The requirement for DH file on FreeRadius:
 1. The *number bits* of the DH file should be: 512, 1024, 2048
 2. The DH file should not be generated with *dsaparam*.
 3. The DH file size should less than 2K bytes

Specified requirements:

The specified requirement for ACS:

- On the page of **Access Policy ->Access Services->Allowed Protocols**

NOTE

- **DO NOT check both "Send Crypto binding TLV" and "Allow PEAPv0 only for legacy clients".**

▼ ☒ Allow PEAP

PEAP Inner Methods

☒ Allow EAP-TLS

☒ Allow EAP-MS-CHAPv2

☐ Allow Password Change Retries: 1

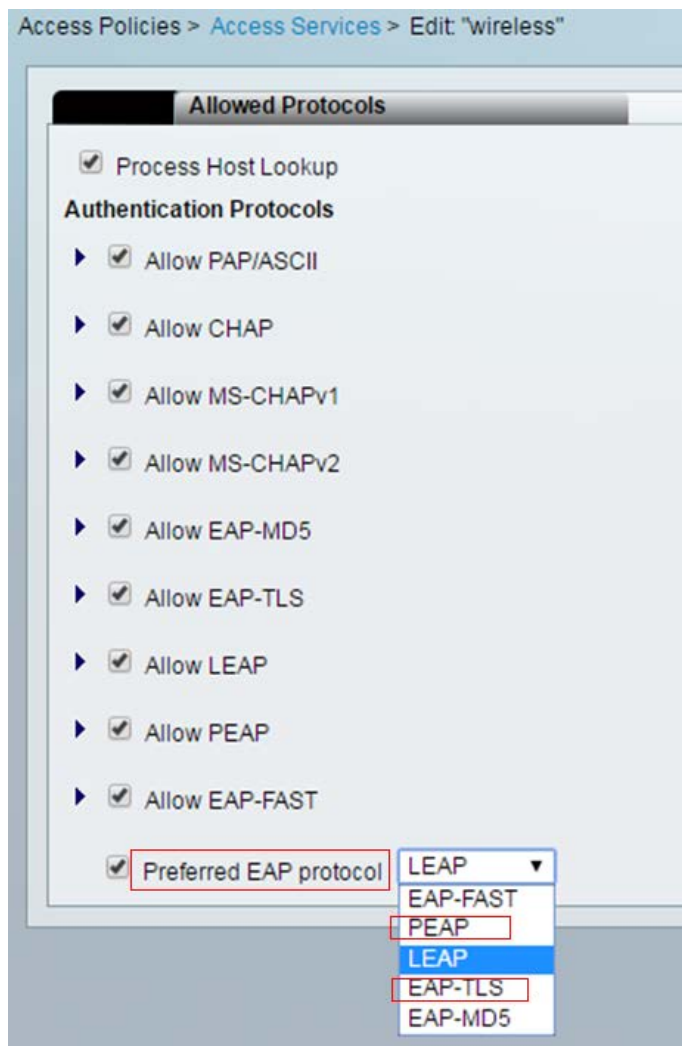
☒ Allow EAP-GTC

☐ Allow Password Change Retries: 1

☒ Send Crypto binding TLV

☒ Allow PEAPv0 only for legacy clients

- "Preferred EAP protocol" should set to PEAP or EAP-TLS.



3.2.2 Configuration Requirements for WLAN of TM80

Requirements include two types: Network service and VLAN, some important settings of network device.

3.2.2.1 Network Service and VLAN

No.	Item	Requirements of the TM80	Description
1	Port	UDP ports 5500 and 6678 are enabled. TCP ports 6587 and 7779 are enabled.	The requirement must be met.
2	VLAN bandwidth	The planned bandwidth of TM80 must be larger than $N \times 100$ kbps (N is the number of installed TM80 products). For example, if 10 TM80 products are working at the same time, the VLAN needs to meet the bandwidth of 1000 kbps.	The requirement must be met.
3	Network continuity	In the coverage area of TM80, the network belongs to the same WLAN. All APs use the same SSID and encryption mode.	The requirement must be met.

■ Service port

The TM80 needs UDP ports 5500 and 6678 and TCP ports 6587 and 7779 on the network to be enabled so as to ensure that the TM80 can be discovered by the CMS, establish network connections, and transmit monitoring data.

■ Bandwidth

The VLAN serving the TM80 may share wired network trunks with other VLANs. The hospital must ensure that bandwidth utilization of trunks does not exceed 80%. If the bandwidth of a VLAN can be configured, the bandwidth configured for the VLAN serving the TM80 is recommended to be decreased by 50%. If 10

TM80s are working at the same time, VLAN bandwidth must be larger than 1Mbps, better to be greater than 2Mbps.

■ Network continuity

TM80 needs to roam across Aps. TM80 can't roam across different IP subnet and different SSID;

3.2.2.2 Some Important Settings of Network Device

No.	Item	Requirements of the TM80	Description
1	DHCP	The DHCP server reserves a sufficient number of IP addresses for the telemetry VLAN to ensure that the TM80 can obtain an IP address.	The requirement must be met.
2	IGMP snooping	If CMS accepts TM80, use multicast, enable IGMP snooping.	Nice to meet
3	Multicast	The multicast function is enabled. Otherwise, the TM80 can only connect to the CMS in unicast mode.	The requirement must be met.
4	Beacon & DTIM	AP DTIM = 1, Beacon = 100ms	The requirement must be met.
5	AP data rate	Close the data rate of 1Mbps,2Mbps,5.5Mbps in 802.11b	Nice to meet
6	QOS	The switch or router must support QoS and the QoS level of TM80's subnet must be set to the highest level.	Nice to meet

The configuration of wireless devices is critical to reliable operation of Mindray monitors. Special attention needs to be paid to the following items:

■ DHCP

The WLC is not recommended to be used as DHCP server. It is recommended to enable the WLC DHCP agent function. A dedicated DHCP server is used to assign IP addresses. The DHCP server needs to reserve a sufficient number of IP addresses for the telemetry VLAN to ensure that the TM80 can obtain an IP address. If static IP addresses are used, make sure that the IP address of each device is unique.

■ Multicast

The TM80 transmits device discovery packets over UDP so that the CMS can discover it and establish a connection. Transmission over UDP can be in multicast or unicast mode. If the customer uses the multicast mode, multicast transmission must be enabled on the network. IGMP snooping must be enabled to avoid transmitting unwanted multicast data to the TM80.

■ DTIM

Set DTIM = 1, Beacon = 100ms for TM80 vlan. TM80 is working under low-power mode and waked up by according to AP's DTIM. If the DTIM is too long, TM80 need more time to wake up so that the throughput become lower, the probability of offline may increase.

■ Data rate

If the network supports the low data rate, the channel will become crowded .As a result, the probability of offline may increase.

If low data rate are closed, be sure that the RF coverage meet TM80's requirement.

- Quality of Service (QoS)

If the network is used by TM80 and other devices at the same time, it's recommended that the QoS level of the SSID and VLAN used by TM80 is set to highest level to make sure that the data is real-time.

3.3 Configuration of Cisco Network Devices

This section describes how to configure Cisco WLC and APs to meet wireless networking requirements of Mindray telemetry monitors. It consists of two parts: list of supported network devices and specific configuration requirements.

Because the IT infrastructures of different hospitals are different, below configuration is only for your reference. You need to modify the configuration according to your hospital IT department.

3.3.1 Recommended Devices

- WLC: Cisco 2500series
- AP: Cisco 2802 Or 2602

3.3.2 Configuration Description

3.3.2.3 Login

On the command line interface (CLI), set the IP address of the WLC to 192.168.30.253 and subnet mask to 255.25.255.0 and enable login on the web page. Set the user name for login to admin and the passcode to Cisco123. The user name and passcode should be set in a unified way so as to facilitate maintenance and change of the configuration later.

Set the IPv4 address of the PC to 192.168.30.1 and the subnet mask to 255.255.255.0 and connect the network port of the PC to port 1 of the WLC by using a network cable.

Considering compatibility with the AC, Firefox browser is preferred. Internet Explorer is secondly preferred. Enter <https://192.168.0.253> in the address bar and choose to trust the website. On the login page, click Login and enter the user name and passcode to access the configuration page. Figure 1 shows the login page.



NOTE

- **Although the default settings of some WLCs are not changed, the specific settings are displayed during setup due to the importance of configuration. The operator just needs to confirm the settings without the need to change them. If no specific description is provided during setup, retain the default settings of WLC.**

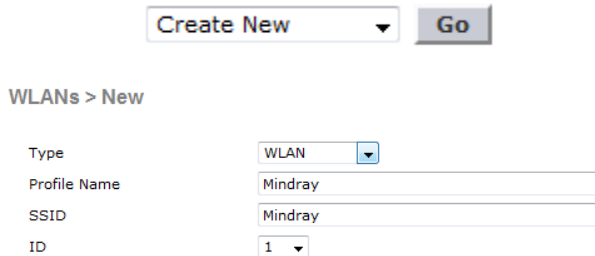
After logging to the WLC, configure the WLC by performing the following steps:

1. Set the WLAN. This part includes SSID creation, General setting, Security setting, QoS setting, and Advanced setting.
2. Set **CONTROLLER**. This part includes the General setting and Multicast setting.
3. Set **WIRELESS**. This part includes the setting of 802.11b/g/n and setting of APs.

3.3.3 WLAN Settings

3.3.3.1 Creating an SSID

1. Choose **WLANs**→**New**. The configuration page is displayed.
2. Perform the following configuration on the page, as shown below.



The screenshot shows a web interface for creating a new WLAN. At the top, there is a 'Create New' button with a dropdown arrow and a 'Go' button. Below this, the breadcrumb 'WLANs > New' is displayed. The configuration form consists of four fields: 'Type' is a dropdown menu set to 'WLAN'; 'Profile Name' is a text input field containing 'Mindray'; 'SSID' is a text input field containing 'Mindray'; and 'ID' is a dropdown menu set to '1'.

3. Click **Apply** and **Save Configuration**.

3.3.3.2 General Settings

1. On the page, enable the WLAN, select a protocol supported by the WLAN, select the VLAN where the WLAN is located, and enable broadcast SSID.
2. Choose **WLANs**→**WLAN ID**→**General**. The configuration page is displayed.
3. Perform the following configuration on the page.
 - ◆ Status=Enabled
 - ◆ Radio policy=All
 - ◆ Interface/Interface Group=VLAN ID
 - ◆ Broadcast SSID=Enabled

NOTE

- **Select the VLAN corresponding to the SSID for VLAN ID.**

The figure below shows the specific General configuration.

The screenshot shows the 'General' configuration tab for a WLAN profile. The profile name is 'yaoce', type is 'WLAN', and SSID is 'yance'. The status is 'Enabled'. The security policy is '[WPA2][Auth(PSK)]'. The radio policy is set to 'All', and the interface/group is 'management'. The broadcast SSID is 'Enabled', and the NAS-ID is 'hardware2504'.

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	yaoce			
Type	WLAN			
SSID	yance			
Status	<input checked="" type="checkbox"/> Enabled			
Security Policies	[WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)			
Radio Policy	All			
Interface/Interface Group(G)	management			
Multicast Vlan Feature	<input type="checkbox"/> Enabled			
Broadcast SSID	<input checked="" type="checkbox"/> Enabled			
NAS-ID	hardware2504			

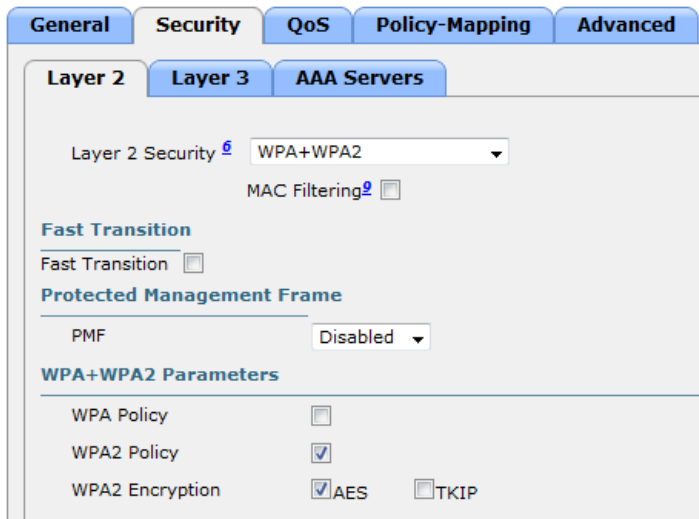
4. Click **Apply** and **Save Configuration**.

3.3.3.3 Security Settings

On the page, configure WLAN security and encrypt physiological information of patients.

1. Choose **WLANs**→**WLAN ID**→**Security**→**Layer 2**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ Layer 2 Security=WPA+WPA2
 - ◆ MAC Filter=Disabled
 - ◆ WPA Policy=Disabled
 - ◆ WPA2 Policy=Enabled
 - ◆ WPA2 Encryption=AES
 - ◆ Authentication Key Management=PSK
 - ◆ PSK Format=ASCII

The figure below shows the specific Security configuration.



3. Click **Apply** and **Save Configuration**.

3.3.3.4 QoS Settings

On the page, set QoS. By default, the WLC considers all frames in the WLAN as ordinary data and adopts the best-effort processing mode. However, the physiological data of patients has the highest priority.

1. Choose **WLANs**→**WLAN ID**→**QoS**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ Quality of Service(QoS)=Platinum(voice)
 - ◆ WMM Policy=Required

The figure below shows the specific QoS configuration.

The screenshot shows a configuration page with five tabs: General, Security, QoS, Policy-Mapping, and Advanced. The QoS tab is selected. Under the QoS tab, there are four settings: Quality of Service (QoS) set to 'Platinum (voice)', Application Visibility with an 'Enabled' checkbox, AVC Profile set to 'none', and Netflow Monitor set to 'none'. Below these is a section titled 'WMM' which contains three settings: WMM Policy set to 'Required', 7920 AP CAC with an 'Enabled' checkbox, and 7920 Client CAC with an 'Enabled' checkbox.

Tab	Quality of Service (QoS)	Application Visibility	AVC Profile	Netflow Monitor	WMM Policy	7920 AP CAC	7920 Client CAC
General							
Security							
QoS	Platinum (voice)	<input type="checkbox"/> Enabled	none	none	Required	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
Policy-Mapping							
Advanced							

3. Click **Apply** and **Save Configuration**.

3.3.3.5 Advanced Settings

On the page, various advanced WLAN settings can be configured, including disabling coverage hole detection, disabling customer exclusion, disabling load balancing, and enabling Off Channel Scan.

1. Choose **WLANs**→**WLAN ID**→**Advanced**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ Coverage Hole detection=Enabled
 - ◆ Enable Session Timeout=Disabled
 - ◆ Aironet IE=Enabled
 - ◆ Customer Exclusion=Disabled
 - ◆ Scan Defer Priority=Enable only 6 and 7
 - ◆ Scan Defer Time(msecs)=2000
 - ◆ DHCP Server(override)=Disabled
 - ◆ DHCP Addr. Assignment=Disabled
 - ◆ Management Frame Protection(MFP)=Disabled
 - ◆ 802.11a/n(1-255)=1
 - ◆ 802.11b/g/n(1-255)=1
 - ◆ Customer Load Balancing=Disabled
 - ◆ Customer Band Select=Disabled

The figures below show the specific Advanced configuration.

General	Security	QoS	Policy-Mapping	Advanced
Allow AAA Override	<input type="checkbox"/> Enabled			
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled			
Enable Session Timeout	<input type="checkbox"/>			
Aironet IE	<input checked="" type="checkbox"/> Enabled			
Diagnostic Channel	<input type="checkbox"/> Enabled			
Override Interface ACL	IPv4: <input type="text" value="None"/> IPv6: <input type="text" value="None"/>			
Layer2 Acl	<input type="text" value="None"/>			
P2P Blocking Action	<input type="text" value="Disabled"/>			
Client Exclusion ²	<input type="checkbox"/> Enabled			
Maximum Allowed Clients ⁸	<input type="text" value="0"/>			
Static IP Tunneling ¹¹	<input type="checkbox"/> Enabled			
Wi-Fi Direct Clients Policy	<input type="text" value="Disabled"/>			
Maximum Allowed Clients Per AP Radio	<input type="text" value="200"/>			
DHCP				
DHCP Server <input type="checkbox"/> Override				
DHCP Addr. Assignment <input type="checkbox"/> Required				
OEAP				
Split Tunnel (Printers) <input type="checkbox"/> Enabled				
Management Frame Protection (MFP)				
MFP Client Protection ⁴ <input type="text" value="Disabled"/>				
DTIM Period (in beacon intervals)				
802.11a/n (1 - 255) <input type="text" value="1"/>				
802.11b/g/n (1 - 255) <input type="text" value="1"/>				
NAC				
NAC State <input type="text" value="None"/>				

General	Security	QoS	Policy-Mapping	Advanced
Maximum Allowed Clients Per AP Radio	<input type="text" value="200"/>			
Clear HotSpot Configuration	<input type="checkbox"/> Enabled			
Client user idle timeout(15-100000)	<input type="checkbox"/>			
Client user idle threshold (0-10000000)	<input type="text" value="0"/> Bytes			
Off Channel Scanning Defer				
Scan Defer Priority	<input type="checkbox"/> 0 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input type="checkbox"/> 7			
Scan Defer Time(msecs)	<input type="text" value="2000"/>			
FlexConnect				
FlexConnect Local Switching ²	<input type="checkbox"/> Enabled			
FlexConnect Local Auth ¹²	<input type="checkbox"/> Enabled			
Learn Client IP Address ⁵	<input checked="" type="checkbox"/> Enabled			
Vlan based Central ¹³	<input type="checkbox"/> Enabled			
NAC State <input type="text" value="None"/>				
Load Balancing and Band Select				
Client Load Balancing <input type="checkbox"/>				
Client Band Select <input type="checkbox"/>				
Passive Client				
Passive Client <input type="checkbox"/>				
Voice				
Media Session Snooping <input type="checkbox"/> Enabled				
Re-anchor Roamed Voice Clients <input type="checkbox"/> Enabled				
KTS based CAC Policy <input type="checkbox"/> Enabled				
Radius Client Profiling				
DHCP Profiling <input type="checkbox"/>				
HTTP Profiling <input type="checkbox"/>				
Local Client Profiling				
DHCP Profiling <input type="checkbox"/>				
HTTP Profiling <input type="checkbox"/>				

- Click **Apply** and **Save Configuration**.

3.3.4 CONTROLLER Settings

In the **CONTROLLER** directory, enable broadcast and multicast.

3.3.4.1 General Settings

1. Choose **CONTROLLER**→**General**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ Broadcast Forwarding=Enable

The figure below shows the specific General configuration.

General

Name	<input type="text" value="hardware2504"/>	
802.3x Flow Control Mode	<input type="button" value="Disabled"/> ▾	
LAG Mode on next reboot	<input type="button" value="Disabled"/> ▾	(LAG Mode is currently disabled).
Broadcast Forwarding	<input type="button" value="Enabled"/> ▾	

3. Click Apply and Save Configuration.

3.3.4.2 Multicast Settings

1. Choose **CONTROLLER**→**Multicast**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ Enable Global Multicast Mode=Enabled
 - ◆ Enable IGMP Snooping=Enabled

The figure below shows the specific Multicast configuration.

MONITOR	WLANs	CONTROLLER	WIRELESS
Multicast			
Enable Global Multicast Mode	<input checked="" type="checkbox"/>		
Enable IGMP Snooping	<input checked="" type="checkbox"/>		
IGMP Timeout (seconds)	<input type="text" value="60"/>		
IGMP Query Interval (seconds)	<input type="text" value="20"/>		
Enable MLD Snooping	<input type="checkbox"/>		
MLD Timeout (seconds)	<input type="text" value="60"/>		
MLD Query Interval (seconds)	<input type="text" value="20"/>		

3. Click Apply and Save Configuration.

3.3.5 WIRELESS Settings

In the **CONTROLLER** directory, you can enable 2.4G and 5G bandwidth, configure the data rate, configure support for 802.11N, and set RRM to optimize the wireless environment.

This section describes configuration of 802.11b/g/n. Because the configuration option of 802.11a/n is similar to this configuration, this configuration is not described in detail here.

3.3.5.1 Setting 802.11b/g/n (2.4G)

Network Settings

On the page, enable 2.4G and configure the data rate.

1. Choose **WIRELESS**→**802.11b/g/n**→**Network**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ 802.11b/g Network Status=Enabled
 - ◆ 802.11g=Enabled
 - ◆ Data Rates: Set **1Mbps, 2Mbps, 5.5Mbps**, and **11Mbps** to **Mandatory** and other items to **Supported**.

The figure below shows the specific Network configuration.

802.11b/g Global Parameters

General

802.11b/g Network Status	<input checked="" type="checkbox"/> Enabled
802.11g Support	<input checked="" type="checkbox"/> Enabled
Beacon Period (milliseconds)	<input type="text" value="100"/>
Short Preamble	<input checked="" type="checkbox"/> Enabled
Fragmentation Threshold (bytes)	<input type="text" value="2346"/>
DTPC Support.	<input checked="" type="checkbox"/> Enabled
Maximum Allowed Clients	<input type="text" value="200"/>
RSSI Low Check	<input type="checkbox"/> Enabled
RSSI Threshold (-60 to -90 dBm)	<input type="text" value="-80"/>

CCX Location Measurement

Mode	<input type="checkbox"/> Enabled
------	----------------------------------

Data Rates**

1 Mbps	Mandatory ▼
2 Mbps	Mandatory ▼
5.5 Mbps	Mandatory ▼
6 Mbps	Supported ▼
9 Mbps	Supported ▼
11 Mbps	Mandatory ▼
12 Mbps	Supported ▼
18 Mbps	Supported ▼
24 Mbps	Supported ▼
36 Mbps	Supported ▼
48 Mbps	Supported ▼
54 Mbps	Supported ▼

3. Click Apply and Save Configuration.

RRM Settings

The RRM provides multiple algorithms and can automatically adjust the transmit power, channel number, and coverage according to the wireless environment to optimize the wireless environment.

TPC Setting

On the page, enable dynamic transmit power adjustment and select the TPC algorithm.

- 1. Choose **WIRELESS**→**802.11b/g/n**→**RRM**→**TPC**. The configuration page is displayed.
- 2. Perform the following configuration on the page.
 - ◆ TPC Version=Coverage Optimal Mode (TPCv1)
 - ◆ Power Level Assignment Method=Automatic

The figure below shows the specific TPC configuration.

MONITORWLANSCONTROLLERWIRELESSSECURITYMANAGEMENTCOMMANDSHelpFEEDBACK

802.11b > RRM > Tx Power Control(TPC)

TPC Version

☐ Interference Optimal Mode (TPCv2)

☒ Coverage Optimal Mode (TPCv1)

Tx Power Level Assignment Algorithm

Power Level Assignment Method

☒ Automatic

☐ On Demand

☐ Fixed

Every 600 secs

Invoke Power Update Once

1

Maximum Power Level Assignment (-10 to 30 dBm)

30

Minimum Power Level Assignment (-10 to 30 dBm)

-10

Power Assignment Leader

hardware2504 (192.168.30.253)

Last Power Level Assignment

432 secs ago

Power Threshold (-80 to -50 dBm)

-70

Power Neighbor Count

3

- 3. Click Apply and Save Configuration.

DCA settings

On the page, enable dynamic channel adjustment and set the range of adjustable channels, start time for adjustment, and interval.

- 1. Choose **WIRELESS**→**802.11b/g/n**→**RRM**→**DCA**. The configuration page is displayed.
- 2. Perform the following configuration on the page.

- ◆ Channel Assignment Method=Automatic (interval needs to be 8 hours or more, anchor time= 0)
- ◆ DCA Channel List=1, 6, 11

The figure below shows the specific DCA configuration.

802.11b > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

Channel Assignment Method: ☒ Automatic Interval: 10 minutes AnchorTime: 0

☐ Freeze ☐ OFF

Invoke Channel Update Once

Avoid Foreign AP interference: ☒ Enabled

Avoid Cisco AP load: ☐ Enabled

Avoid non-802.11b noise: ☒ Enabled

Avoid Persistent Non-WiFi Interference: ☐ Enabled

Channel Assignment Leader: hardware2504 (192.168.30.253)

Last Auto Channel Assignment: 446 secs ago

DCA Channel Sensitivity: Medium STARTUP (5 dB)

DCA Channel List

DCA Channels: 1, 6, 11

Select	Channel
<input checked="" type="checkbox"/>	1
<input type="checkbox"/>	2
<input type="checkbox"/>	3
<input type="checkbox"/>	4
<input type="checkbox"/>	5

Event Driven RRM

EDRRM ☐ Enabled

3. Click **Apply** and **Save Configuration**.

NOTE

- When configure the 802.11a/an DCA channel list, the DFS channel mustn't be in the list .For example,The channel list mustn't include the 52~64 and 100~140 in US.

Coverage Settings

On the page, enable coverage hole detection and set the detection standard.

1. Choose **WIRELESS**→**802.11b/g/n**→**RRM**→**Coverage**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ Enable Coverage Hole Detection=Enabled

The figure below shows the specific Coverage configuration.

The screenshot shows a configuration page with two sections: 'General' and 'Coverage Threshold'. In the 'General' section, 'Enable Coverage Hole Detection' is checked. In the 'Coverage Threshold' section, four settings are configured: Data RSSI (-60 to -90 dBm) at -80, Voice RSSI (-60 to -90 dBm) at -80, Min Failed Client Count per AP (1 to 75) at 3, and Coverage exception level per AP (0 to 100 %) at 25.

General	
Enable Coverage Hole Detection	<input checked="" type="checkbox"/>

Coverage Threshold	
Data RSSI (-60 to -90 dBm)	-80
Voice RSSI (-60 to -90 dBm)	-80
Min Failed Client Count per AP (1 to 75)	3
Coverage exception level per AP (0 to 100 %)	25

3. Click Apply and Save Configuration.

3.3.5.2 Setting Access Points (2.4G)

1. Choose **WIRELESS**→**Access Point**→**Radio**→**802.11b/g/n**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ Admin Status=Enabled
 - ◆ RF Channel Assignment(Assignment method)=Global
 - ◆ Tx Power Level Assignment(Assignment method)=Global

The figure below shows the specific AP configuration.

General	RF Channel Assignment
AP Name Admin Status Operational Status Slot #	AP74a0.2f40.676c Enable UP 0
11n Parameters	Current Channel Channel Width Assignment Method
11n Supported	11 20 MHz Global
CleanAir	Tx Power Level Assignment
CleanAir Capable CleanAir Admin Status Number of Spectrum Expert connections	1 Global
Yes Enable 0	
Antenna Parameters	Performance Profile
Antenna Type Antenna	View and edit Performance Profile for this AP Performance Profile
Internal A B C D	Note: Only Channels 1,6 and 11 are nonoverlapping Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.
<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	

3. Click **Apply** and **Save Configuration**.

3.4 Configuration of Aruba Network Devices

This section describes how to configure Aruba WLC and APs to meet wireless networking requirements of Mindray telemetry monitors. It consists of two parts: list of supported network devices and specific configuration requirements.

Because the IT infrastructures of different hospitals are different, below configuration is only for your reference. You need to modify the configuration according to your hospital IT department.

3.4.1 Recommended Devices

- WLC: Aruba 7005 series
- AP: Aruba APIN0205

3.4.2 Login

On the command line interface (CLI), set the IP address of the WLC to 192.168.30.253 and subnet mask to 255.25.255.0, and enable login on the web page. Set the user name for login to admin and the password to aruba123. The user name and password should be set in a unified way so as to facilitate maintenance and change of the configuration later.

Set the IPv4 address of the PC to 192.168.0.1 and the subnet mask to 255.255.255.0 and connect the network port of the PC to port 1 of the WLC by using a network cable.

Considering compatibility with the WLC, Firefox browser is preferred. Internet Explorer is secondly preferred. Enter <https://192.168.0.253> in the address bar and choose to trust the website. On the login page, click Login and enter the user name and password to access the configuration page. Figure 1 shows the login page.



After logging to the WLC, configure the WLC by performing the following steps:

1. Set the **Wireless**. This part includes SSID creation, General setting, Security setting and Advanced setting.
2. Set **Network**. This part includes the DHCP setting and Multicast setting.

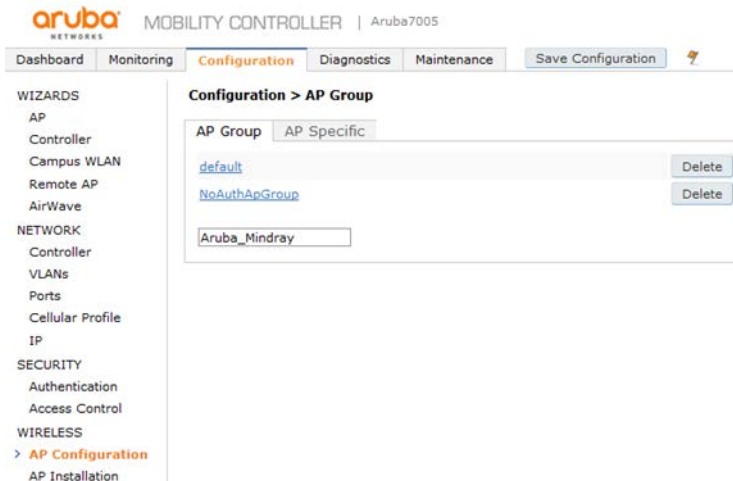
NOTE

- **Although the default settings of some WLCs are not changed, the specific settings are displayed during setup due to the importance of configuration. The operator just needs to confirm the settings without the need to change them. If no specific description is provided during setup, retain the default settings of WLC.**

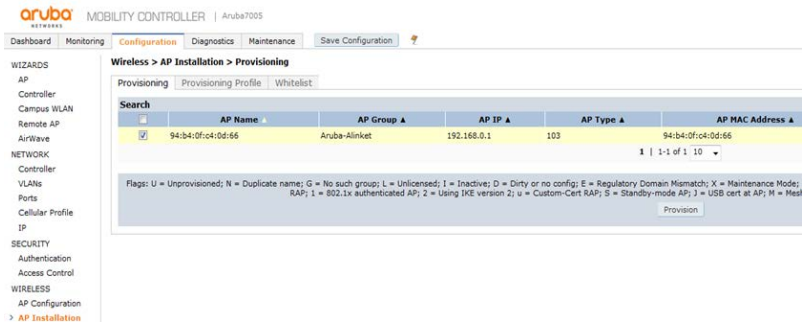
3.4.3 Wireless Setting

3.4.3.1 AP Group Setting

1. Choose Configuration>Wireless>AP Configuration>AP Group>New, The configuration page is displayed. Input Aruba_Mindray in the box, and click the Add. Perform the following configuration on the page, as shown below.



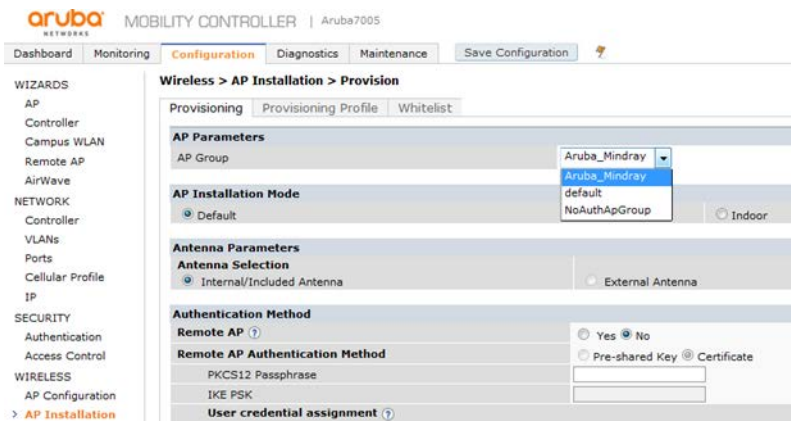
2. Choose Configuration>Wireless>AP Installation>Provision, The configuration page is displayed. Select the used AP, Perform the following configuration on the page, as shown below.



3. Click Provision, The configuration page is displayed. Perform the following configuration on the page:

AP Group=Aruba_Mindray

The figure below shows the specific configuration.



4. Click **Apply** and reboot, and **Save Configuration**.

3.4.3.2 Virtual AP setting

1. Choose **Configuration>Wireless>AP Configuration>AP Group>Aruba_Mindray>Wireless LAN>Virtual AP**, input Mindray in the box, and click the Add. The figure below shows the specific configuration.



2. Choose **Configuration>Wireless>AP Configuration>AP Group>Aruba_Mindray>Wireless LAN>Virtual AP>Mindray**, Perform the following configuration on the page:

Virtual AP enable=enable

VLAN=VLAN ID (1)

Forward mode=tunnel


Allowed band=all

Steering Mode=prefer-5 ghz

Drop Broadcast and Unknown multicast=Disable

The figure below shows the specific configuration.

Virtual AP > Mindray

Basic	Advanced
Virtual AP enable	<input checked="" type="checkbox"/>
VLAN	1 
Forward mode	tunnel
Allowed band	all
Band Steering	<input type="checkbox"/>
Steering Mode	prefer-5ghz
Dynamic Multicast Optimization (DMO)	<input type="checkbox"/>
Dynamic Multicast Optimization (DMO) Threshold	5
Drop Broadcast and Unknown Multicast	<input type="checkbox"/>
Convert Broadcast ARP requests to unicast	<input type="checkbox"/>
Authentication Failure Blacklist Time	3600 sec
Blacklist Time	3600 sec
Deny inter user traffic	<input type="checkbox"/>
Deny time range	--NONE--
DoS Prevention	<input type="checkbox"/>
HA Discovery on-association	<input checked="" type="checkbox"/>
Mobile IP	<input checked="" type="checkbox"/>
Preserve Client VLAN	<input type="checkbox"/>
Remote-AP Operation	standard
Station Blacklisting	<input checked="" type="checkbox"/>
Strict Compliance	<input type="checkbox"/>
VLAN Mobility	<input type="checkbox"/>
FDB Update on Assoc	<input type="checkbox"/>

- Click **Apply** and reboot, and **Save Configuration**
- Choose **Configuration>Wireless>AP Configuration>Wireless LAN>Virtual AP>Mindray>SSID**, Perform the following configuration on the Advanced page:

SSID Enable=Enable

ESSID=Mindray

Encryption=wpa2-psk-aes

PSK AES Key=12345678

DTIM interval=1 beacon periods

802.11a basic Rates=6/12/24

802.11a Transmit Rates=ALL

802.11b basic Rates=1/2/5.5/11

802.11b Transmit Rates=ALL

WPA Passphrase=12345678

The figure below shows the specific configuration.

		<input checked="" type="checkbox"/> wpa2-psk-aes	
		<input type="checkbox"/> wpa2-psk-tkip	
		<input type="checkbox"/> wpa2-tkip	
Enable Management Frame Protection	<input type="checkbox"/>	Encryption mode.	
Require Management Frame Protection	<input type="checkbox"/>		
DTIM Interval	1	beacon periods	
802.11a Basic Rates	<input checked="" type="checkbox"/> 6	<input type="checkbox"/> 9	<input checked="" type="checkbox"/> 12
	<input type="checkbox"/> 18	<input checked="" type="checkbox"/> 24	
	<input type="checkbox"/> 36	<input type="checkbox"/> 48	
	<input type="checkbox"/> 54		
802.11a Transmit Rates	<input checked="" type="checkbox"/> 6	<input checked="" type="checkbox"/> 9	<input checked="" type="checkbox"/> 12
	<input checked="" type="checkbox"/> 18	<input checked="" type="checkbox"/> 24	
	<input checked="" type="checkbox"/> 36	<input checked="" type="checkbox"/> 48	
	<input checked="" type="checkbox"/> 54		
802.11g Basic Rates	<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> 2	<input checked="" type="checkbox"/> 3
	<input type="checkbox"/> 6	<input type="checkbox"/> 9	<input checked="" type="checkbox"/> 11
	<input type="checkbox"/> 12	<input type="checkbox"/> 18	
	<input type="checkbox"/> 24	<input type="checkbox"/> 36	
802.11g Transmit Rates	<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> 2	<input checked="" type="checkbox"/> 3
	<input checked="" type="checkbox"/> 6	<input checked="" type="checkbox"/> 9	<input checked="" type="checkbox"/> 11
	<input checked="" type="checkbox"/> 12	<input checked="" type="checkbox"/> 18	
	<input checked="" type="checkbox"/> 24	<input checked="" type="checkbox"/> 36	
	<input checked="" type="checkbox"/> 48	<input checked="" type="checkbox"/> 54	

- Click **Apply** and reboot, and **Save Configuration**

3.4.3.3 RF Management setting

This section describes configuration of 802.11a/n. Because the configuration option of 802.11b/g/n is similar to this configuration, this configuration is not described in detail here.

- Choose **Configuration>Wireless>AP Configuration>RF Management>802.11a radio**, Perform the following configuration on the Advanced page:
 - Radio enable=enable
 - Mode=ap-mode
 - Channel=20Mhz
 - Spectrum Load Balancing=disable
 - Beacon Period=100msec

The figure below shows the specific configuration.

802.11a radio profile > default

Show Reference Save As Reset

Basic Advanced

Radio enable	<input checked="" type="checkbox"/>
Mode	ap-mode
High throughput enable (radio)	<input checked="" type="checkbox"/>
Very high throughput enable (radio)	<input checked="" type="checkbox"/>
Channel	
Transmit EIRP	0
Non-Wi-Fi Interference Immunity	2
Enable CSA	<input type="checkbox"/>
CSA Count	4
Advertise 802.11d and 802.11h Capabilities	<input type="checkbox"/>
Spectrum Load Balancing	<input type="checkbox"/>
Beacon Period	100 msec
Beacon Regulate	<input type="checkbox"/>
Advertized regulatory max EIRP	0
ARM/WIDS Override	OFF
Reduce Cell Size (Rx Sensitivity)	0 dB
Energy Detect Threshold Offset	0 dB
Management Frame Throttle interval	1 sec
Management Frame Throttle Limit	20
Maximum Distance	0 meters
RX Sensitivity Threshold	0 dB
RX Sensitivity Tuning Based Channel Reuse	disable

Channel Width:
☒ 20MHz ☐ 40MHz ☐ 80MHz

- Click **Apply** and reboot, and **Save Configuration**
- Choose **Configuration>Wireless>AP Configuration>RF Management>802.11a radio>Adaptive Radio Management**, Perform the following configuration on the Basic page:

Assignment=single-band

Allowed bands for 40Mhz channels=None

80Mhz support=disable

Max Tx EIRP=127

Min Tx EIRP=3

Client Match=disable

The figure below shows the specific configuration.

Basic Advanced

General

Assignment	single-band
Allowed bands for 40MHz channels	None
80MHz support	<input type="checkbox"/>
Max Tx EIRP	127
Min Tx EIRP	3
Client Match	<input type="checkbox"/>

- Click **Apply** and reboot, and **Save Configuration**

3.4.3.4 AP setting

1. Choose **Configuration>Wireless>AP Configuration>RF Management>AP >Ethernet interface 4 port configuration>Regulatory Domain**. Perform the following configuration on the Basic page:

Country code=US

Valid 802.11g Channel=1/6/11

Valid 802.11a Channel=36~48 and 149~165

The figure below shows the specific configuration.

Country Code	US - United States		
Valid 802.11g channel	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3
	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input checked="" type="checkbox"/> 6
	<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9
	<input type="checkbox"/> 10	<input checked="" type="checkbox"/> 11	
Valid 802.11a channel	<input checked="" type="checkbox"/> 36	<input checked="" type="checkbox"/> 40	<input checked="" type="checkbox"/> 44
	<input checked="" type="checkbox"/> 48	<input type="checkbox"/> 52	<input type="checkbox"/> 56
	<input type="checkbox"/> 60	<input type="checkbox"/> 64	<input type="checkbox"/> 100
	<input type="checkbox"/> 104	<input type="checkbox"/> 108	<input type="checkbox"/> 112
	<input type="checkbox"/> 116	<input type="checkbox"/> 132	<input type="checkbox"/> 136
	<input type="checkbox"/> 140	<input type="checkbox"/> 144	<input checked="" type="checkbox"/> 149
	<input checked="" type="checkbox"/> 153	<input checked="" type="checkbox"/> 157	<input checked="" type="checkbox"/> 161
	<input checked="" type="checkbox"/> 165		

2. Click **Apply** and reboot, and **Save Configuration**

3.4.4 Network Setting

1. Choose **Configuration-IP-IP interface-edit**. Perform the following configuration on the page.

IP Version=IPv4

DHCP Helper Addresses=192.168.0.50 (The DHCP server's IP)

Enable IGMP=enable

Enable IGMP Snooping=enable

The figure below shows the specific configuration.

IPv4 ▾

1

DHCP Helper Addresses

192.168.0.50 Delete

Add

Option-82	None ▾
MTU [1280 - 1500]	1500
Enable Suppress ARP	<input checked="" type="checkbox"/>

IGMP

Enable IGMP	<input checked="" type="checkbox"/>
Enable IGMP Snooping	<input checked="" type="radio"/>
Enable IGMP Proxy	<input type="radio"/>
<input checked="" type="radio"/> Interface GigabitEthernet 0/0/0 ▾	<input type="radio"/> Port-Channel ID 0 ▾

2. Click **Apply** and reboot, and **Save Configuration**

3.5 Configuration of Netgear Network Devices

This section describes how to configure Netgear APs to meet wireless networking requirements of Mindray monitors. The model recommended by Mindray is WNDAP350. Because the IT infrastructures of different hospitals are different, below configuration is only for your reference. You need to modify the configuration according to your hospital IT department.

3.5.1 Preparation

3.5.1.1 Tools and Resources

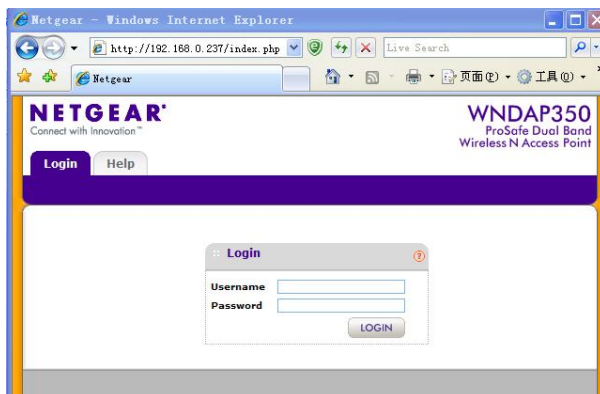
- WNDAP350 to be configured and power cable of WNDAP350
- One network cable
- One PC



Hardware to be prepared

3.5.1.2 Login

1. Set the IPv4 address of the PC to **192.168.0.1** and the subnet mask to **255.255.255.0** and connect the network port of the PC to the network port of the WNDAP350 by using a network cable.
2. Open the IE, enter the default IP address of WNDAP35, namely **192.168.0.237**, default user name **admin**, and passcode **passcode**, and click **LOGIN**, as shown below.



Note

- After the AP setting is changed, click **APPLY** in the lower right corner so that the setting can take effect.

3.5.2 Setting Single AP

3.5.2.1 System Settings

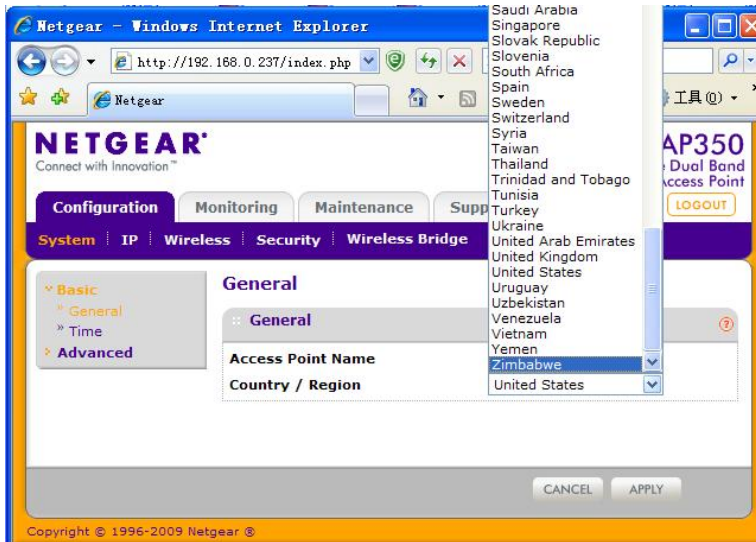
On the page, set the country where the network is built and time.

- Country Setting
 1. Choose **Configuration**→**System**→**Basic**→**General**. The configuration page is displayed.
 2. Perform the following configuration on the page.
 - ◆ Country/Region=United State

NOTE

- Select a country according to the country where the network is built.

The figure below shows the specific configuration.



3. Click **APPLY** in the lower right corner to save the setting.

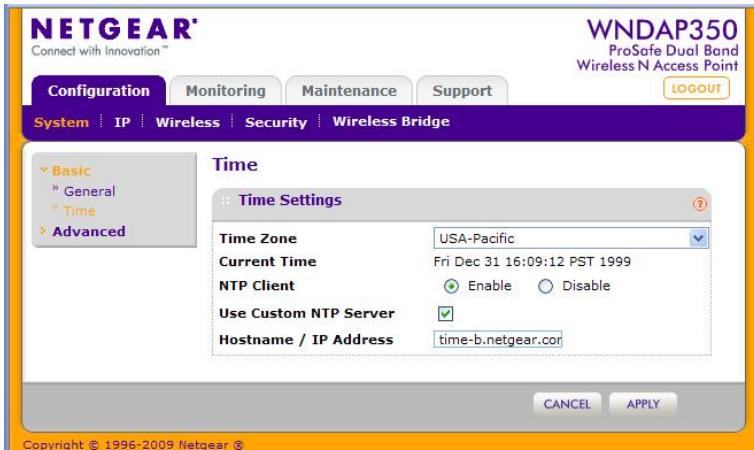
■ Time Settings

1. Choose **Configuration**→**System**→**Basic**→**Time**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ Time Zone=USA-Pacific
 - ◆ NTP Client=Enable
 - ◆ Use Custom NTP Server=Enable

NOTE

- Select a time zone according to the country where the network is built.

The figure below shows the specific configuration.



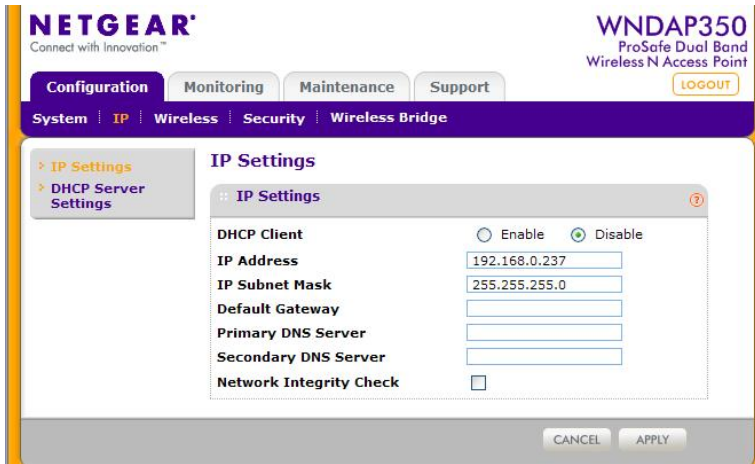
3. Click **APPLY** in the lower right corner to save the setting.

3.5.2.2 IP Settings

Setting AP's IP

1. Choose **Configuration**→**IP**→**IP Settings**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ DHCP Client=Disable
 - ◆ IP Address=192.168.0.237
 - ◆ IP Subnet Mask=255.255.255.0

The figure below shows the specific configuration screen.



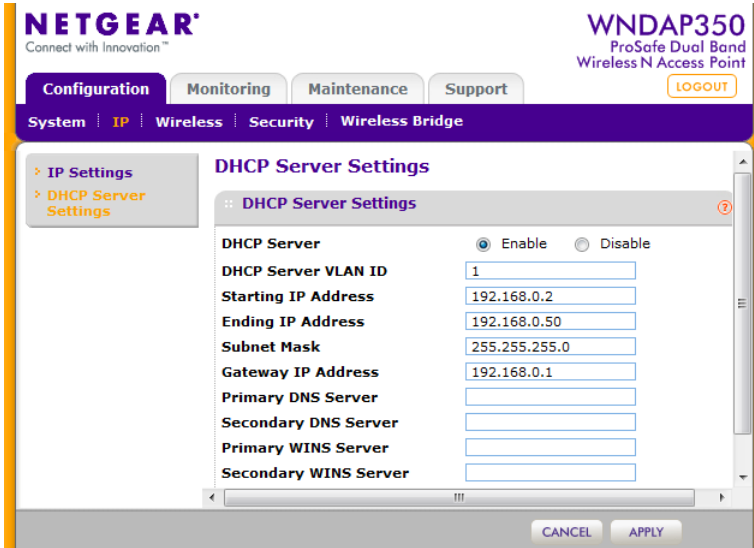
3. Click **APPLY** in the lower right corner to save the setting.

Setting IP of a Wi-Fi Device

Connect devices to the AP, use the AP as the DHCP server, and assign an IP address.

1. Choose **Configuration**→**IP**→**DHCP Server Settings**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ DHCP Server=Enable
 - ◆ DHCP Server VLAN ID=1
 - ◆ Starting IP Address=196.76.0.2
 - ◆ Ending IP Address=196.76.0.100
 - ◆ Subnet Mask=255.255.255.0
 - ◆ Gateway IP Address=196.76.0.254

The figure below shows the specific configuration. Please note that the IPs of below picture is different. You need to modify the DHCP setting according to hospital IT department. However, please make sure the TM80 and BeneVision CMS can communicate with each other.

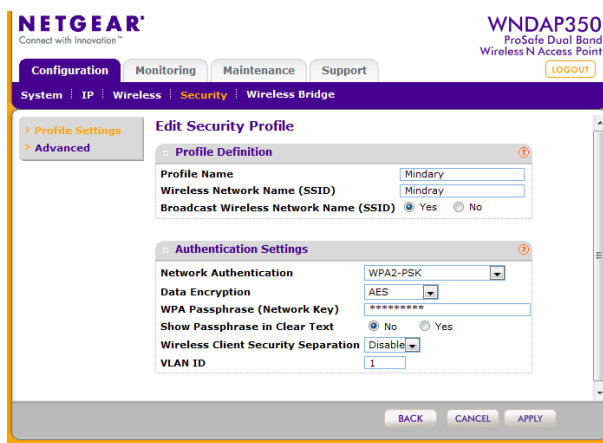


3. Click **APPLY** in the lower right corner to save the setting.

NOTE

- To establish a Wi-Fi network consisting of multiple APs, do not use the APs as the DHCP server. Set a dedicated DHCP server in the wired network and make the IP addresses of APs in the same network segment as the IP addresses provided by the DHCP server.

1. Click the circle on the left and click **EDIT**. On the configuration page, perform the following configuration:
 - ◆ Network Authentication=WPA2-PSK
 - ◆ Data Encryption=AES
 - ◆ For the Network Key, please set it according to hospital IT. And you need to input this key in TM80 menu.
 - ◆ Show Passphrase in clear Text=No
 - ◆ Wireless Customer Security Separation=Disable
 - ◆ VLAN ID=1
 - ◆ The figure below shows the specific configuration.



2. Click **APPLY** in the lower right corner to save the setting.

3.5.3 Wireless Settings (5G)

This section describes configuration of 802.11a/na. Because the configuration option of 802.11b/g/ng is similar to this configuration,so it is not detailed here.

3.5.3.1 Wireless On-Off

1. Choose **Configuration**→**Wireless**→**Basic**→**Wireless On-Off**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ Wireless On-Off=Off

The figure below shows the specific configuration.

The screenshot shows the Netgear WNDAP350 configuration interface. The top navigation bar includes 'Configuration', 'Monitoring', 'Maintenance', and 'Support'. Below this, a secondary bar shows 'System', 'IP', 'Wireless', 'Security', and 'Wireless Bridge'. The 'Wireless' section is expanded, showing 'Basic', 'Wireless Settings', 'Wireless On-Off', 'QoS Settings', and 'Advanced'. The 'Wireless On-Off' page is displayed, featuring a 'Wireless on-off' section with radio buttons for 'On' and 'Off' (selected). Below this is a 'Radio off schedule' section with a table for days of the week (M, T, W, T, F, S, S) and checkboxes for each day. The 'Radio ON Time' is set to 7:00 hrs and the 'Radio OFF Time' is set to 19:49 hrs. The 'APPLY' button is visible in the bottom right corner.

Radio off schedule						
M	T	W	T	F	S	S
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

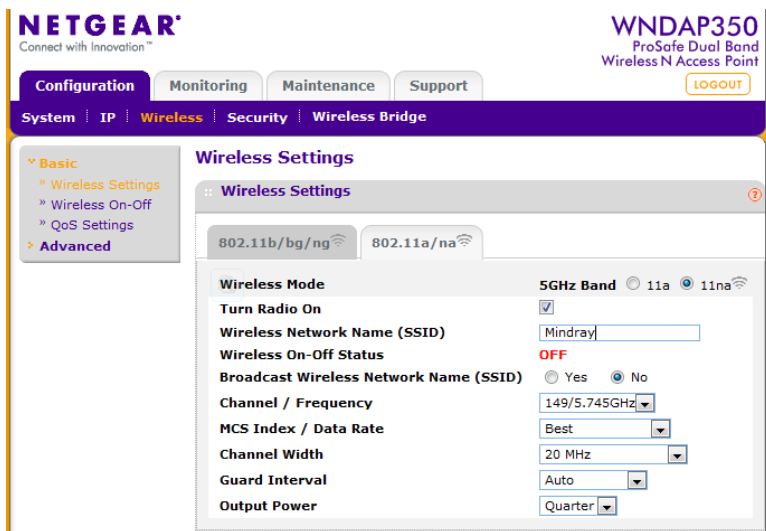
Radio ON Time: 7 : 00 hrs
Radio OFF Time: 19 : 49 hrs

3. Click **APPLY** in the lower right corner to save the setting.

3.5.3.2 Wireless Settings

1. Choose **Configuration**→**Wireless**→**Basic**→**Wireless Settings**→**802.11a/na**.
2. On the configuration page, perform the following configuration:
 - ◆ Wireless Mode=11na
 - ◆ Turn Radio on=enable
 - ◆ Wireless Network Name(SSID)=Mindray. You can modify this SSID according to hospital IT. After you change this name, please also modify the TM80 SSID setting.
 - ◆ Broadcast Wireless Network Name(SSID)=Yes
 - ◆ Channel/Frequency=149/5.745GHz. You need to set the channel according to the Wi-Fi survey result.
 - ◆ Output Power=Quarter

The figure below shows the specific configuration.



NOTE

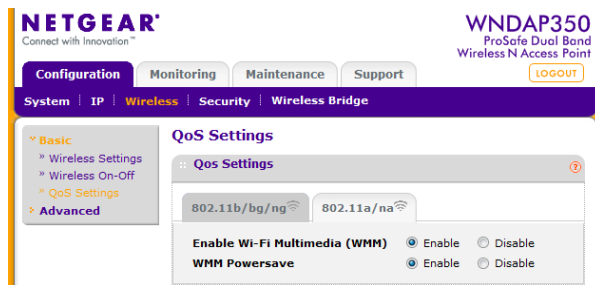
- According to the field survey data based on wireless survey tool, select the minimum channel as a fixed channel.

3. Click **APPLY** in the lower right corner to save the setting.

3.5.3.3 QoS Setting (5G)

1. Choose **Configuration**→**Wireless**→**Basic**→**QoS Settings**. The configuration page is displayed.
2. Perform the following configuration on the page.
 - ◆ Enable Wi-Fi Multimedia (WMM)=Enable
 - ◆ WMM Powersave=Enable

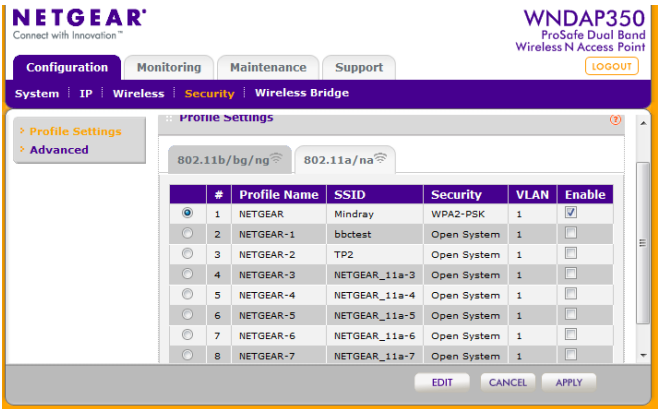
The figure below shows the specific configuration.



3. Click **APPLY** in the lower right corner to save the setting.

3.5.3.4 Security Settings (5G)

3. Choose **Configuration**→**Security**→**Profile Settings**→**802.11a/na**. On the configuration page, click the box to enable the SSID, as shown below.



3.5.4 Setting Multiple APs

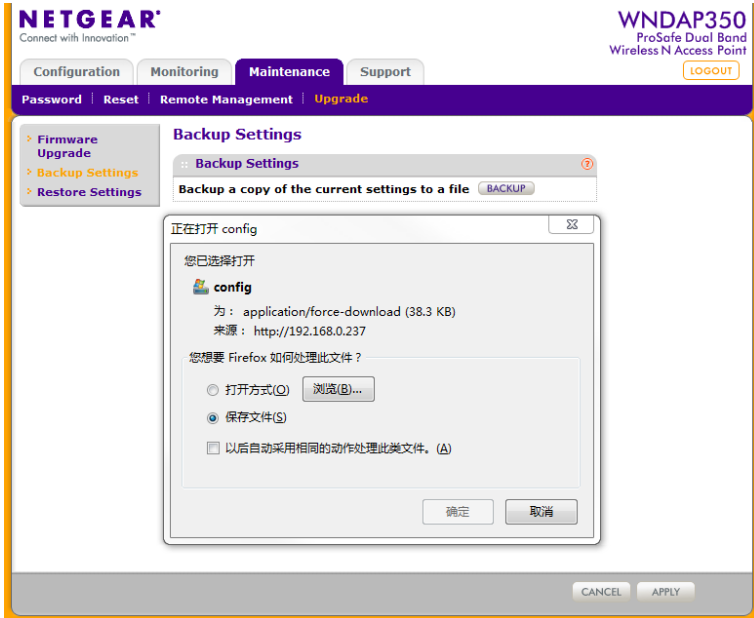
In the multi-AP setting, export the configuration file of a configured AP and import the configuration file to APs to be configured.

NOTE

- In the single-AP setting, the channel of the AP is allocated automatically. In the multi-AP setting, manually fix a channel and ensure that adjacent channels use non-overlapped channels.

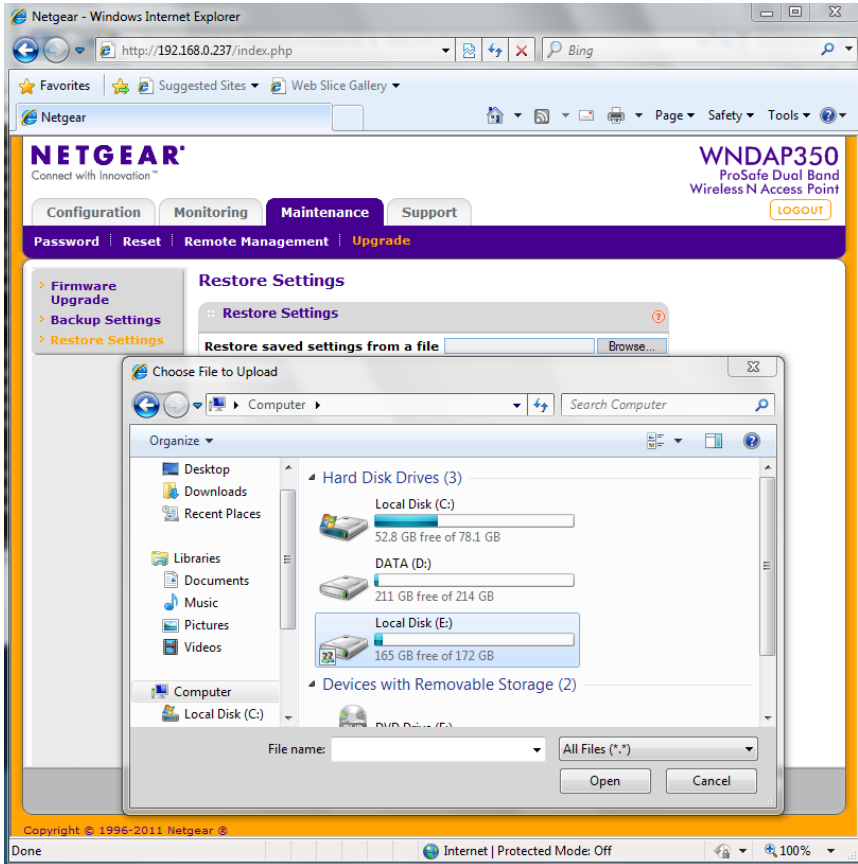
3.5.4.1 Exporting a Configuration File

1. Choose **Configuration**→**Maintenance**→**Upgrade**→**Backup Settings**.
2. On the page for exporting configuration files, click **BACKUP** and export the configuration file to a local directory, as shown below.



3.5.4.2 Importing a Configuration File

1. Choose **Configuration**→**Maintenance**→**Upgrade**→**Restore Settings**.
2. On the page for importing configuration files, click **Browse**, select a local configuration file, and import it to the APs to be configured, as shown below.



3. Click **APPLY**.

3.6 Network Deployment Planning

3.6.1 Tools and Resources

- Laptop computer, where Windows 7 or operating system of a later version is installed and wireless network card is equipped. wireless network card's RSSI dynamic range should be at least 45dB(e.g the highest value is -45dBm,the lowest value is -90dBm).
- Wireless network survey tool, we suggest to use professional survey tool such as tamograph, Wirelessmon or other professional network survey tool.
- TM80 main unit
- Customer TM80 coverage plan
- Test APs
- Professional network engineer

NOTE

- **The personnel who implement the Wi-Fi site survey and network deployment should be well trained about Wi-Fi. If you are not professional network engineer, please ask some third party for help.**
-

3.6.2 Environmental Survey

Mindray personnel meet with hospital IT, biomedical engineer and clinicians to agree on network plan and clinical workflow requirements. The network plan should include coverage, network topology, channel planning, and device model initially selected.

3.6.2.1 Environment Confirmation

First obtain the following information:

- The layout and current pipe distribution map of the floor
- coverage requirements
- Number estimation of potential wireless terminal users

Then pre-plan bandwidth allocation and location distribution of main devices.

Finally, conduct a site survey. Site survey covers internal decoration structure of the building (floor area, floor height, wall and ceiling materials, and areas to be covered), and location where APs can be mounted.

Preparations before field test

- Ask the customer to provide the site floor plan, schematic diagrams of floors and floor height and collect building design drawings and official documents, so as to get ware of the power supply for rooms and structure foundation (for example, metal fire path, wall, doors, and passageway).
- Ask the customer to provide the schematic diagram of wireless coverage requirements.
- Ask the customer to determine whether all areas need redundancy coverage or which areas need redundancy coverage.
- Ask the customer to provide personnel who are familiar with site conditions so as to ask them questions about coverage, site layout, available installation points, and channel planning and estimate the number of potential Wi-Fi devices under each AP with them (a maximum of 16 devices are recommended for each AP).

Site test and report

1. Check that the surrounding environment and placement of devices during the test are consistent with those actually in use.
2. Learn distribution of Wi-Fi devices and other 2.4G products in the wireless scope.
3. According to the site environment, initially determine the rough installation locations of APs, find the cleanest channel by using Wireless network survey tool, for example, channel 11 is relatively cleaner, open the test AP, and set the channel to channel 11. Use the Wireless network survey tool to test wireless coverage and ensure that the test can be passed in the expected coverage of the test AP.

Go to the next expected AP installation location, perform the test again, and record the results.

Field personnel must ensure that no blind spot exists in the required coverage and that co-channel interference does not exceed the limit.

3.6.2.2 Preliminary Network Deployment Design

Cabling rules:

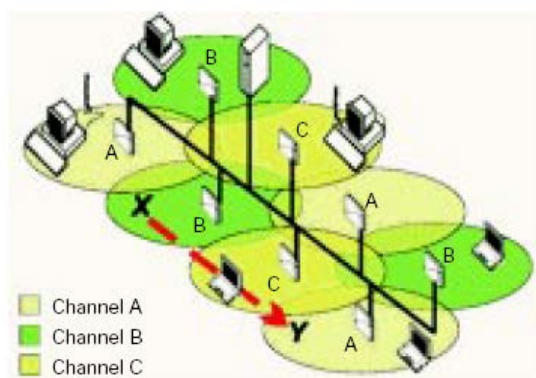
The figure below shows the degree of attenuation of various materials for radio wave.

Barrier	Degree of attenuation	Example
Open ground	No	Cafeteria and courtyard
Wooden product	Low	Interior wall, office partition wall, door and floor
Gypsum	Low	Interior wall (new gypsum has greater impact on wireless signal than old gypsum)
Synthetic material	Low	Office partition wall
Coal cinder brick	Low	Interior wall and outer wall

Barrier	Degree of attenuation	Example
Asbestos	Low	Ceiling
Glass	Low	Colorless window
Metal net in glass	Medium	Door and partition wall
Metal colored glass	Low	Colored window
Human body	Medium	Large group of people
Water	Medium	Damp wood, glass jar and organism
Brick	Medium	Damp wood, glass jar and organism
Marble	Medium	Interior wall, outer wall and ground
Ceramic product	High	Ceramic tile, ceiling and ground
Paper	High	A roll or pile of paper
Concrete	High	Ground, outer wall and load-bearing beam
Bullet-proof glass	High	Safety shed
Silver plating	Very high	Mirror
Metal	Very high	Office table, office partition wall, concrete, elevator, file cabinet and ventilating device

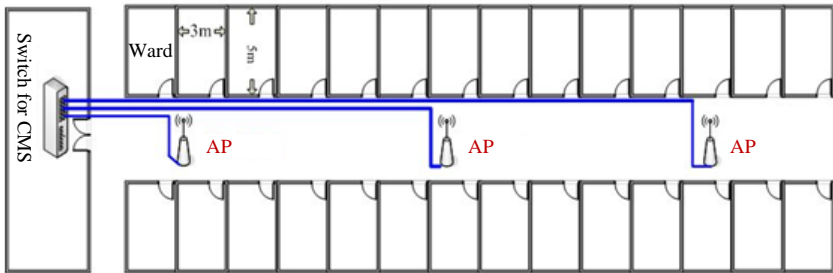
1. The maximum indoor transmission distance of wifi is about 50m. In practice, the distance of distinct vision is recommended to be 25m to guarantee coverage. If a brick wall blocks the way, the recommended distance should be divided by 2; if two brick walls block the way, the recommended distance should be divided by 2 again. If a load bearing wall blocks the way, the transmission distance would be greatly reduced. For one load bearing wall, the transmission distance would be divided by 4.
2. After completing cabling construction, draw the AP cabling diagram to facilitate system operation and maintenance in the future.
3. Initially select locations of APs according to the actual scenario and requirements and then make adjustment through field measurement. Follow the rules: Ensure that all areas can be covered and try to reduce the number of needed APs.

4. Channels occupied by coverage areas of APs should comply with certain specifications. APs in nearby coverage areas cannot use the same channel; otherwise, co-channel interference would be caused during signal transmission of APs. Take 2.4G band as example, to utilize band resources to the maximum extent, the most common method is to select three non-overlapped channels (channels 1, 6, and 11) as the operating band of the whole system. the channels 1, 6, and 11 are mutually adjacent and partially overlapped (as shown in the figure below) so as to eliminate blind spots and avoid co-channel interference while obtaining the largest coverage area.



5. APs that implement wireless roaming network must use the same network name (SSID) and IP address in the same network segment. Otherwise, wireless customers cannot implement the roaming function.

Examples of AP layout



3.7 Network Deployment Implementation

This section describes the approximate process of network deployment, which is performed by professional third party and adjusted according to actual conditions.

3.7.1 Preparations before Equipment Installation

1. According to the site test report, determine locations and install the network cable and power supply cable.
2. Test the network cable and power supply cable for connectivity.
3. Prepare installation tools: mounting brackets needed by APs and mechanical tools.
4. Ask the customer to provide climbing equipment (if needed) and available time for operation (daytime, night and specific time).

3.7.2 Roaming Consideration

The following operation is recommended to guarantee the roaming performance:

- Plan possible roaming areas, optimize AP coverage, and reduce the number of AP handovers on the roaming path.
- Donot make tm80 roam across different IP subnet.
- Ensure that the same SSID is set for APs in the coverage area.
- Ensure that all APs on the roaming path are under the control of the same WLC.
- Try not to use enterprise-class encryption, which results in longer roaming time.

3.7.3 Services Provided During and After Installation

1. During installation, perform the following tests for wireless devices (including APs and laptop computers) at the same time: network connectivity, security performance, and software operation.
2. Make sure that the configurations of APs meet requirements of this document.
3. According to requirements of the contract, provide wireless device settings and maintenance training.
4. Provide technical consulting service after installation to ensure that equipment is used properly.

3.8 Network Verification

3.8.1 Tools and Resources

- Laptop computer, where Windows 7 or operating system of a later version is installed and wireless network card is equipped. We recommended laptop configured with Intel Centrino Wireless-N adapter. If your laptop is configured with some other wireless adapter, please make sure the adapter has a high degree of accuracy.
- Wireless network survey tool, we suggest to use professional survey tool such as tamograph, Wirelessmon or other professional network survey tool.
- TM80 main unit
- TM80 coverage plan
- Professional network engineer

NOTE

-
- **The personnel who implement the Wi-Fi network survey should be well trained about Wi-Fi. If professional network engineers are not available, please ask some third party for help.**
-

3.8.2 Wi-Fi Signal Calibration

Before a Wireless network survey tool (running on laptop computer) is used to test network coverage, calibrates the RSSI of wireless network survey tool with TM80.

Keep the TM80 and Wireless network survey tool close. The distance between them is not greater than 30cm and the distance from human body is above 50 cm. Move the TM80 and Wireless network survey tool at the same time (maintain the previous distance). When the TM80 reads the following RSSI values: -50dBm, -60dBm, -70dBm and -80dBm, record the RSSI values read by Wireless network survey tool.

Then calibrate the RSSI of Wireless network survey tool to TM80 when do site survey (the RSSI of TM80 is the benchmark to wireless coverage).

3.8.3 Confirm Network Feasibility

Wireless coverage and AP capability and compatibility are decided by infrastructure of network, it can't be modified easily. If the network does not meet the requirements before TM80 is installed, network dropping-off may happen easily after installation.

Verify these requirements to confirm network feasibility. For verification contents and method, see **3.11.2 Environmental Survey Table**.

- Site survey: To confirm coverage, perform coverage test in the asserted areas including toilet ,corridor, stairs and other place where TM80 may be used. The service person can finish the wireless network survey via third-party professional survey tool such as tamograph, Wirelessmon or other professional network survey tool. The RSSI of TM80 is the benchmark to wireless coverage. So it's necessary to calibrates the RSSI of the wireless network survey tool with TM80. The site survey must be carried out when the network is operational and other devices are wirelessly connected. During the test, the WLAN SSID broadcasting function must be enabled for TM80.
- RF environment simulation: Some customers may carry out theoretic design for deployment of APs by using a simulation tool or deploying analysis tool. The work can accelerate network deployment but air interface detection cannot be omitted. This is because the location, power, and channel of an AP may be adjusted during actual deployment.

3.8.4 Network Verification Process

Network Verification aims to confirm coverage, connectivity, service ports, and network bandwidth. In addition, other configuration requirements of the TM80 need to be confirmed with the IT Dept. of the hospital. For the Verification content and method see 3.11.3 **Network Acceptance Table**.

This part is completed through two ways: First the hospital completes items requiring self-check of the hospital's IT Dept., as indicated in the Network Verification Table. Then customer service personnel or authorized party confirms items on site and finally completes the Network Acceptance Table. If any item is found incompliant during network Verification test, adjustment should be made before the TM80 is installed.

A laptop computer needs to be used to simulate the TM80 main unit, so as to test coverage, connectivity, service ports, and network bandwidth. During the test, the SSID broadcast needs to be enabled to ensure that the SSID can be scanned.

3.9 Configuring WLAN Settings of TM80

This table lists the items that need to be configured to make proper operation of the TM80.


Item	Description	Remarks
Main Menu->Maintenance -> Network->IP Address Setup	Set static IP address or DHCP	For details, please refer to <i>BeneVision TMS60 Telemetry Monitoring System/TM80 Telemetry Monitor Operator's Manual</i>
Main Menu -> Maintenance-> Network-> WALN Setup	Configure SSID, passcode, EAP, etc.	For details, please refer to <i>BeneVision TM80 Telemetry Monitor Operator's Manual</i> and <i>3.9Configuring WLAN Settings of TM80</i> in this manual
Main Menu -> Maintenance ->Network-> Connect CMS	Configure how to connect to the CMS.	For details, please refer to <i>BeneVision TMS60 Telemetry Monitoring System/TM80 Telemetry Monitor Operator's Manual</i> If CMS and TM80 are not in the same subnet, multicast TTL should be greater than 1. It is recommended to set QoS to High .
Main Menu -> Maintenance-> Network-> Wireless Setup	Select to use 2.4G band or 5G band	5G band is highly recommended. If 2.4G is selected, the TM80 can only roam between 2.4G channels, but never goes to 5G channels. Vice verse. For more details, refer to <i>3.9.55G Band Channels</i> .
Main Menu -> Maintenance-> Network->EAPCertificate	Manage CA certificates and user certificates	For details, please refer to <i>BeneVision TM80 Telemetry Monitor Operator's Manual</i> and <i>3.9.2EAP Setup</i> in this manual.
Main Menu->Maintenance ->Service-> WLAN test->Roaming Test	Configure roam parameters that will affect TM80's roaming performance	For details, refer to <i>3.9.4.4</i> Roaming Test.

Item	Description	Remarks
Main Menu->Maintenance ->Service->WLAN test->WIFI Regulatory domain	Set the region where the TM80 will be used	For details, refer to 3.9.4.3 WiFi Regulation Domain .

NOTE

- After changing the setting in Main Menu ->Maintenance->Service, you should reboot TM80 to make sure that TM80's settings take effect.


3.9.1 WLAN Setup

1. Press  to enter the main menu.
2. Tap **Maintenance** → enter the required passcode → tap **Network** → tap **WLAN Setup**.
3. Enter a network name for Network Name.
4. Set **Security Type** to **WPA/WPA2 EAP or WPA/WPA2 PSK**.

Some important information for security types:

Security Type of TM80	Compatible Security Type of AP	Remarks
WPA/WPA2 PSK	WPA with AES WPA with TKIP WPA with AES+TKIP WPA2 with AES WPA2 with AES+TKIP	Do not use WPA2 with TKIP
WPA/WPA2 EAP	WPA2 with AES WPA2 with AES+TKIP	Do not use WPA. Do not use WPA2 with TKIP.

3.9.2 EAP Setup

1. Press  to enter the main menu.
2. Tap **Maintenance** → enter the required passcode → tap **Network** → tap **WLAN Setup**.
3. Enter a network name for Network Name.
4. Set **Security Type** to **WPA/WPA2 EAP**.
5. Select the desired EAP method. Then items related to this EAP method will be displayed. Different items need to be configured for corresponding EAP method.

This table shows correspondence between EAP method and Configuration Items.

EAP type	Identity	Anonymity	Passcode	CA Certificate	User Certificate
PEAP-MSCHAPV2	Y	O	Y	O	N
PEAP-GTC	Y	O	Y	O	N
TLS	Y	N	Y	Y	Y

Note: **Y** means Yes, and configuration is required; **N** means No and configuration is not required; **O** means optional.

Configuration items are defined as below:

- **Authentication(Phase2 Auth):** After selecting PEAP as the EAP method, you need to select **MSCHAPV2** or **GTC** as the PEAP inner method.
- **Identification:** i.e. user identity. It is the user name in the AD, LDAP or local user management on the RADIUS server.
- **Anonymous :** This item does not impact the authentication process. It is used to hide the real name(Identity).
- **Network Passcode:** The passcode for the Identity.
- **CA Certificate:** Select the desired CA certificate.
- **User Certificate:** Select the desired user certificate.

CAUTION

- **TM80 supports EAP only when using 5G band. When change band from 5G to 2.4G, WLAN settings must be re-configured to use WPA/WPA2 PSK.**
-

NOTE

- **TM80 supports three type of RADIUS server : FreeRadius, acs, and windows server.**
-

3.9.3 EAP Certificate Management

You can import up to 10 certificates from a USB drive or delete certificates from the TM80.

NOTE

- **After restoring factory defaults, all certificates will be deleted automatically by TM80.**
-

3.9.3.1 Preparing Certificates

The following RADIUS Server is validated by Mindray:

- Cisco ACS
- FreeRadius
- Network Policy Service(in Windows Server 2008 R2 and Windows Server 2012 R2)

Currently, X.509.v3 is a mainstream certificate standard. It has two main coding formats: DER and PEM. Certificates in DER format are mainly suffixed with ".cer", ".der", and ".crt". Certificates in PEM format are mainly suffixed with ".pem".

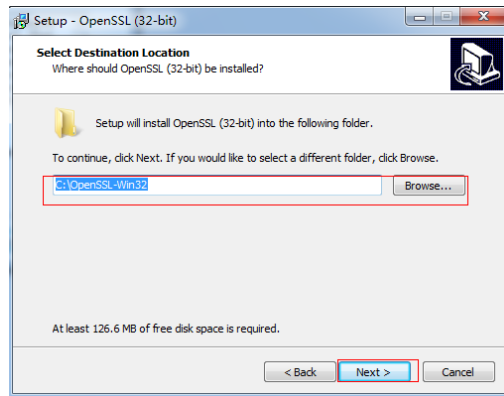
The TM80 only supports certificates in PEM format. If you need to use certificates in other formats, you need to convert the certificates before importing them into the TM80. The openssl tool (version 1.0.2c or later) is recommended for the conversion, and you can get the setup file on internet conveniently.

openssl tool preparation consists of two steps: installing an openssl tool and configuring environment variables.

■ Installing an openssl tool

You can install the openssl tool as default. Win32OpenSSL-1_0_2c.exe is taken as an example.

1. Click the setup file to start.
2. Click **Next** to continue.
3. Select "I accept.." and click **Next** to continue.
4. Select the install path and click **Next** to continue



5. Click **Next** to continue until setup is finished.

■ Configure environment variables

You must add the install path (in Step4 above) to the computer's environment variables. After this, you can use openssl in the command line interface as shown below:

```
C:\Users\50213155>openssl  
OpenSSL>
```

Check your certificates' suffix. If it's not "pem" you should select the appropriate command to convert.

■ Steps to converting CA Certs:

Before start converting, we need to know the format of the CA Cert. It could be DER or Base64.

The DER cert is binary format, and the Base64 cert is text format. So we can figure out the format by open the cert with notepad. If the content displayed in the notepad contains "BEGIN CERTIFICATE", then the CA Cert is in Base64 format, otherwise it is in DER format.

- ◆ Command for converting the DER CA Cert to PEM cert
openssl x509 -inform der -in [ca].cer -out [ca].pem
- ◆ Command for converting the Base64 CA Cert to PEM cert
openssl x509 -inform PEM -in [ca].cer -out [ca].pem

NOTE

-
- **The file size of the CA Cert should less than 2KB**
-

■ Steps for converting User Cert

● If the User Cert is .pfx file, then use the following steps for converting:

1. Get the file only containing cert

`openssl pkcs12 -in [user cert].pfx -clcerts -nokeys -out [user cert].pem`

2. Get the file only containing key

`openssl pkcs12 -in [user cert].pfx -nocerts -out [user cert key in pkcs12].pem`

3. Convert the key from pkcs12 to pkcs8

`openssl pkcs8 -topk8 -inform PEM -in [user cert key in pkcs12].pem -outform PEM
-nocrypt -out [user cert key in pkcs8].pem`

4. Merge the cert and key to one file

1) Open the [user cert].pem with notepad, only keep the lines between "-----BEGIN
CERTIFICATE-----" and "-----END CERTIFICATE-----" and delete the other lines.

The cert file is shown below:

[illegible]

- If the User Cert is .PEM file, you should separate the key from this file.

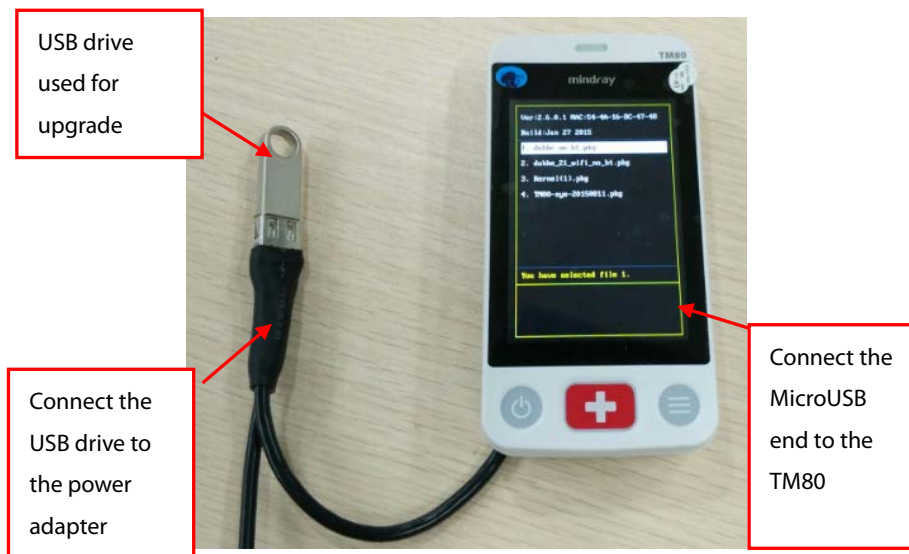
Open the .PEM file with notepad, save the lines between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" to a separate cert file, for example, [user cert].pem, and save the lines between "-----BEGIN PRIVATE KEY-----" and "-----END PRIVATE KEY-----" to a separate key file, for example, [user key].pem.


Follow the steps in 3 and 4 to convert it to pkcs8

3.9.3.2 Importing Certificates


Required tools

- An empty USB drive (FAT data format and at least 256 MB space)
 - One USB upgrade cable (P/N: 009-005409-00)
 - One computer used to prepare USB drive tools
 - One power module with USB port (output voltage: 5 V, output current not less than 1 A)
1. Insert a USB drive to the USB port of your computer
 2. Create the folder named "Cert" in the USB drive.
 3. Copy the desired certificates to the "Cert" folder.
 4. Remove the battery from the TM80's compartment and find the MicroUSB socket inside the battery compartment. Connect the MicroUSB end of the USB upgrade cable (P/N: 009-00549-00) to the MicroUSB socket, insert the prepared upgrade USB drive on the USB female connector of the upgrade cable, and connect the USB male connector of the upgrade cable to the USB power adapter as shown below.




5. Power on the TM80.
6. Press  to enter the main menu → tap **Maintenance** → enter the required passcode → tap **Network** → tap **EAP Certificate** → tap **USB** and then select the desired certificate.
7. Tap **Import**.

3.9.3.3 Deleting Certificates

1. Press  to enter the main menu → tap **Maintenance** → enter the required passcode → tap **Network** → tap **EAP Certificate**.
2. Tap **Local**.
3. Select the desired certificate.
4. Tap **Delete**.

3.9.4 WLAN TEST

1. Press  to enter the main menu → tap **Maintenance** → enter the required passcode.
2. Tap **Service** → enter the required passcode → tap **WLAN test**.

In this menu, users can learn more details about WLAN, and make some important configurations.

3.9.4.1 WLAN information

This table lists TM80 WLAN information:

Item	Description
Network name	If the TM80 is connected to an AP, the AP's SSID is displayed If the TM80 is not connected to an AP, it is blank.
Channel	If the TM80 is connected to an AP, the AP's working channel is displayed. If the TM80 is not connected to an AP, it is blank.
RSSI	If the TM80 is connected to an AP, The AP's signal strength for TM80 is displayed If the TM80 is not connected to an AP, it is blank.
AP MAC address	If the TM80 is connected to an AP, the AP's MAC address is displayed. If the TM80 is not connected to an AP, it is blank.
Local MAC Address	Displays the MAC Address of TM80
Local IP	If the TM80 is connected to an AP, TM80's IP address is displayed. If the TM80 is not connected to an AP, it is blank.

Item	Description
Connection Status	If the TM80 is connected to an AP, Connected is displayed. If the TM80 is connected to an AP, Disconnected is displayed.
Security Type	Displays the security type selected in the WLAN Setup Menu.

3.9.4.2 Connection Test

When the TM80 is connected to an AP, you can type the desired IP address and tap **Test**, TM80 will ping to the IP address once to check whether the network is Ok.

3.9.4.3 WiFi Regulation Domain

Before using the TM80 in certain country or region, you need to select the correct WiFi regulatory country or region.

NOTE

-
- **Service personnel should make sure that the correct WiFi regulation domain is selected. Otherwise, the TM80 may work abnormally.**
-

3.9.4.4 Roaming Test

TM80 roaming performance is subject to the four parameters.

Item	Description	Remarks
Trigger	The TM80 will start scanning to search for a better AP when the signal intensity (RSSI) of current connected AP is weaker than Trigger.	It is recommended to set the trigger value to the RSSI value of expected weakest coverage in the hospital, which cannot be lower than -70 dBm. The TM80 requires that the network deployed in the hospital meet the requirement of -65 dBm. It is reasonable to set the trigger value in the range of -70 to -65.

Item	Description	Remarks
Delta	If the TM80 finds a new AP with RSSI "Delta" higher than current connected AP, it will choose to roam to the new AP.	5dB is recommended. If the network deployment density of the hospital is very high and the weakest coverage can reach -60dBm, it is more reasonable to set Delta to 10dB. This can reduce switch between different APs, and make wifi function more stable.
Scan Period	When the RSSI of current connected AP is weaker than trigger, but the TM80 does not find a better AP, it will scan for better AP once every scan period.	5s is recommended.
AutoTrigger	autotrigger is the threshold when the TM80 will try additional attempt to roam.	Additional attempt to roam is a work-around method, and may decrease wifi stability. If user does not encounter roaming problem, set this parameter to -99dBm. If user finds TM80 sticks to a far AP and does not roam to a nearby AP, set autotrigger value this way: it must be at least 5db lower than trigger value and should be higher than -75dBm.
Auto band	When enabled, TM80 can automatically change wifi band if current band can't work well.	Default enabled. If WLAN can only support 2.4G or 5G, disable this.

3.9.5 5G Band Channels

There are DFS channels in 5G band. Prior to transmitting on a DFS channel, AP must first listen for the presence of a radar system. If radar is detected, the channel must be vacated and flagged as unavailable. AP must continue to monitor the environment for the presence of radar during operation and, if radar is detected, must move to an unoccupied channel and instruct all associated client devices to do the same. Client devices like TM80 may not transmit on a DFS channel unless instructed by an infrastructure device that the channel is free from radar.

When in roaming, TM80 can only use passive scan to find a better AP. Because a passive scan may take hundreds of milliseconds per DFS channel, especially in the FCC and ETSI regulatory domains where there are 15 DFS channels. Due to these limitations, DFS compliance will impact Wi-Fi performance and reliability of TM80. So TM80 disable DFS channel supporting.

The TM80 can only use channels in U-NII-1 (channel 36, 40, 44, 48) and U-NII-3 (channel 149, 153, 157, 161, 165, not supported in ETSI regulatory domain).

NOTE

- **Generally, the 5G band has much less RF interference than the 2.4G band, so Mindray recommends customer to use 5G band if possible.**
-


3.10 Network Verification with TM80

Equipment: TM80 and CMS PC

3.10.1 Test Preparation

Perform settings according to steps in the Operator's manual.

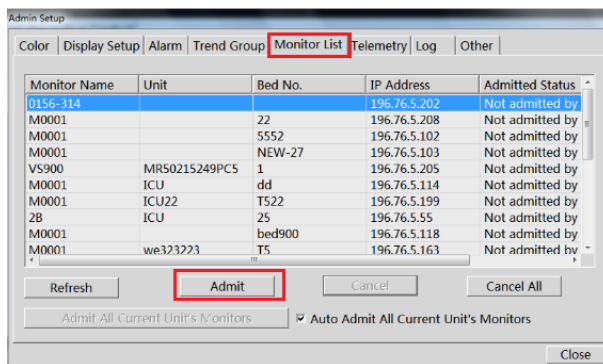
3.10.2 Connecting a TM80 to the Central Station

1. On the TM80, press  to enter the main menu.
2. Tap **Maintenance**, enter the passcode, and select **Accept**.
3. Tap **Network** and select **IP Address Setup**. Slide the button on the right of DHCP to the right or left to allow obtaining IP address in a dynamic or static way. For details on how to use DHCP, see 3.5.2.2 "IP Settings".

CAUTION

- **Set the status of the DHCP function properly according to the actual conditions of a hospital.**

4. Tap **WLAN Setup** and **Network Name** and enter the network name of the network where the CMS is located. Then tap **Accept**.
5. Tap **WLAN Setup** and **Network Passcode** and enter the network passcode of the network where the CMS is located. Then select **Accept**.
6. In **System Setup** of the CMS, select **Admin Setup**, enter the passcode, and select **OK**.
7. Select **Monitor List**, find the TM80, and select **Admit**, as shown in the figure below:



8. Click **Close** to close the **Admin Setup** screen.

3.10.3 Test Preparation

Connect the TM80 to the CMS, set the **Display Auto Off** of the TM80 to **Off**, and put the TM80 into Demo mode. In this case, the TM80 continuously transmits ECG waveform data to the CMS. Click the Wi-Fi status icon on the screen, as shown by



in the figure below. Then you can observe the Wi-Fi RSSI value of the TM80.




3.10.4 Coverage Confirmation

To confirm coverage, perform coverage test in the areas where patients often go (for example, ward and toilet) and areas where it is difficult to provide coverage and patients will enter, for example, corridor and stairs.

Check whether coverage meets requirements by observing the signal strength icon on the CMS and observing whether offline occurs.

When necessary, adjust locations of APs or add APs to ensure the overage effect.

Do as follows:

1. Set the TM80 to access to CMS.
2. Ping the TM80 on the CMS (input "ping -t -l 32 -w 1500 IP adress" in window CLI (Ping the TM80 persistently ,The packet is 32 bytes ,the timeout of reply is 1500ms) , after ten minutes , input "ctrl + c"(finish the ping), make sure that the mean delay is smaller than 250ms and the packet lost rate shall be less than 1%.
3. Hold the TM80 with a hand (hold the battery part to avoid blocking the Wi-Fi antenna) and avoid blocking by people. Walk in the expected coverage areas, for example, all corners of the ward, toilet, smoking area, corridor, and elevator.
4. Offline event times should be less than 10% of TM80 roaming times; at least three grids of signal exist on the CMS icon (), and the RSSI value displayed on the TM80 is not lower than -65dBm.
5. If the signal strength is lower than -65dBm during walking, stop at the location and observe for 30s. If the RSSI value is not lower than -65 dB in more than 66 percent of the time, the coverage requirement is met.
6. Make TM80 running at the place where the signal strength is the weakest for 24h, The time percentage when a TM80 fails to transmit data to the central station shall not exceed 0.1% over a 24-hour period(86 s).

3.10.5 TM80Acceptance Confirmation

Test or Observation Item	Result(Pass, Fail or NA)
Ping the TM80 from the CMS and make sure that the mean delay is less than 250 ms and the packet lost rate shall be less than 1%.	
Hold the TM80 and walk in the scope of different APs. After walking through the whole expected telemetry coverage area, observe continuous waveform on the CMS. Offline event times should be less than 10% of TM80 roaming times.	
In the location where coverage is the poorest, signal strength displayed on the screen is higher than -65dBm.	
When the signal strength is the weakest , the amount of time each TM80 transporting data to central station is not available shall be less than 86s over a 24 hour period	

CAUTION

- **When the TM80 is held in one hand, the TM80 should be held in the location close to the battery in the lower part of the device. If the device is held in a location in the upper part of the device, wireless signal radiation will be affected.**
-

3.11 Appendices

3.11.1 TM80 Wi-Fi Network Requirement Table

No.	Item	Requirements of the TM80	Description
Wireless coverage requirements			
1	Received signal strengths (RSSI)	≥ -65 dBm Signal coverage requirement for APs connected to the TM80: RSSI value displayed on the TM80	The requirement must be met.
2	Co-channel interference	≤ -20 dB Measured on the same channel of the TM80	The requirement must be met.
3	Ping delay	The mean delay of PC or cell phone with normal wifi module is smaller than 100ms and The packet lost rate shall be less than 1%.	The requirement must be met.
The requirements of AP capability			
1	Recommended AP	Mindray's recommendations: Cisco: WLC 2504 (version 7-4-121-0 or later) + LAP: 2802 or 2602 or FAT AP:2602 Aruba: 7500 series+ LAP: APIN0205APIN0205 Netgear: WNDAP350	Nice to meet
2	AP capability	1, The anticipated number of devices connecting to one AP must be lower than the AP capability, and capability should has a margin of 50%. For example, In the coverage of one AP, the typical number of devices connected to this AP is 16,	The requirement must be met.

		then the announced number of devices that can connect to AP simultaneously must be more than 32. 2, The AP Can create several SSIDs.	
3	Device density	The maximum number of devices connected to one AP simultaneously is 16 (including TM80 and other devices).	The requirement must be met.
4	AP compatibility	When customer using Aps not from Cisco, compatibility test should be passed	The requirement must be met.
WLAN features			
1	802.11 protocol	TM80 only support 802.11 a/b/g/n, WLAN can't use other protocols	The requirement must be met.
2	Security mode	TM80 supports: WPA/WPA2-PSK or WPA2-Enterprise EAP method: PEAP-GTC, PEAP-MSCHAPv2,EAP-TLS WPA2-PSK is highly recommended. WPA2-Enterprise may increase probability of offline when roaming, so not be recommended. WLAN can't use other security mode.	The requirement must be met.
3	AP MAC address	The broadcast MAC address of AP is fixed (BSSID). AP BSSID is used to locate the TM80 device. If it is changed, failure to	The requirement must be met.

		locate the TM80 may occur.	
4	AP channel width	If the AP supports 802.11n/ac, set the channel width to 20Mhz, don't use HT40 or even HT80.	The requirement must be met.
5	Dedicated VLAN	The TM80 needs to work on a dedicated VLAN. Using VLAN can minimize Broadcast or multicast data which can affect TM80 stability.	The requirement must be met.
Network service and VLAN			
1	Port	UDP ports 5500 and 6678 are enabled. TCP ports 6587 and 7779 are enabled.	The requirement must be met.
2	VLAN bandwidth	The planned bandwidth of TM80 must be larger than $N \times 100$ kbps (N is the number of installed TM80 products). For example, if 10 TM80 products are working at the same time, the VLAN needs to meet the bandwidth of 1000 kbps.	The requirement must be met.
4	Network continuity	In the coverage area of TM80, the network belongs to the same WLAN. All APs use the same SSID and encryption mode.	The requirement must be met.
Important settings			
1	DHCP	The DHCP server reserves a sufficient number of IP addresses for the telemetry VLAN to ensure that the TM80 can obtain an IP	The requirement must be met.

		address.	
2	IGMP snooping	If CMS accepts TM80 use multicast, enable IGMP snooping	Nice to meet
3	Multicast	The multicast function is enabled. Otherwise, the TM80 can only connect to the CMS in unicast mode.	The requirement must be met.
4	Beacon & DTIM	AP DTIM = 1, Beacon = 100ms	The requirement must be met.
5	AP data rate	Close the data rate of 1Mbps,2Mbps,5.5Mbps in 802.11b	Nice to meet
6	QOS	The switch or router must support QoS and the QoS level of TM80's subnet must be set to the highest level.	Nice to meet
EAP requirements			
1	EAP requirements	Refer to 3.2.1.4 for detail	The requirement must be met.

3.11.2 Environmental Survey Table

After completing the environmental survey, fill in the survey results in the **Check Results** column.

NO	Item	Requirements of TM80	Verification Method	Check Results
Wireless coverage requirements				
1	Signal strength (RSSI)	≥ -65 dBm Signal coverage requirement for APs which TM80 is connected. RSSI value is that perceived by the TM80	Service person performs the test by using network survey tool. Make sure that all expected coverage areas such as ward, corridor, toilet, stairs, and elevator are tested.	
2	Co-channel interference	≤ -20 dB Measured on the operating channel of TM80	Service person performs the test by using network survey tool. Make sure that all expected coverage areas such as ward, corridor, toilet, stairs, and elevator are tested.	

3	Ping delay	The mean delay of PC or cell phone with normal wifi module is smaller than 100ms and The packet lost rate shall be less than 1%.	Service person performs the test: 1. Connect PC or cell phone with normal wifi module to AP. 2. Connect another pc to the LAN port where central monitoring system is connected to. Run command" "ping -t -l 32 -w 1000 IPaddress-of -cellphone" for 10 minutes, then run" ctrl+c".	
WLAN features				
1	802.11 protocol	TM80 only support 802.11 a/b/g/n, WLAN can't use other protocols	Check with hospital IT if this requirement is met or not.	
2	Security mode	TM80 supports: WPA/WPA2-PSK or WPA2-Enterprise EAP method: PEAP-GTC, PEAP-MSCHAPv2, EAP-TLS WPA2-PSK is highly recommended. WPA2-Enterprise may	Check with hospital IT if this requirement is met or not.	

		increase probability of offline when roaming, so not be recommended. WLAN can't use other security mode.		
3	AP MAC address	The broadcast MAC address of AP is fixed (BSSID). AP BSSID is used to locate the TM80 device. If it is changed, failure to locate the TM80 may occur.	Check with hospital IT if this requirement is met or not.	
4	AP channel width	If the AP supports 802.11n/ac, set the channel width to 20Mhz, don't use HT40 or even HT80.	Check with hospital IT if this requirement is met or not.	
5	Dedicated VLAN	The TM80 needs to work on a dedicated VLAN. Using VLAN can minimize Broadcast or multicast data which can affect TM80 stability.	Check with hospital IT if this requirement is met or not.	
Requirements of AP capability				

1	Recommended AP	Mindray's recommendations: Cisco: WLC 2504 (version 7-4-121-0 or later) + LAP: 2802 or 2602 or FAT AP:2602 Aruba: 7500 series+LAP: APIN0205APIN0205 Netgear: WNDAP350	Service person Check with hospital IT if this requirement is met or not. Get the AP model from related hospital people or observe directly.	
2	AP capability	1. The anticipated number of devices connecting to one AP must be lower than the AP capability, and capability should have a margin of 50%. For example, in the coverage of one AP, the typical number of devices connected to this AP is 16, then the announced number of devices that can connect to AP simultaneously must be more than 32. 2. The AP can create several SSIDs.	Service personnel get the AP model from related hospital people or observe directly. According to the model, get the data sheet of AP to make sure the capability.	
3	Device density	The maximum number of devices	Check with hospital IT if this	

		connected to one AP simultaneously is 16 (including TM80 and other devices).	requirement is met or not.	
4	AP compatibility	When customer using Aps not from Cisco, compatibility test should be passed	Mindray or Mindray's agent service engineer uses a TM80 to confirm in advance. Refer to section 3.10 Network Verification with TM80 with TM80, Set TM80 to access to CMS, observe the performance of roaming and stability to make sure the AP compatibility.	
EAP requirements				
1	EAP requirements	Refer to 3.2.1.4 for detail	Check with hospital IT if this requirement is met or not.	

3.11.3 Network Acceptance Table

After completing the network verification, fill in the verification results in the **Check Results** column.

NO	Item	Requirements of TM80	Verification Method	Check Results
Wireless coverage requirements				
1	Signal strength (RSSI)	≥ -65 dBm Signal coverage requirement for APs which TM80 is connected. RSSI value is that perceived by the TM80	Service person performs the test by using network survey tool. Make sure that all expected coverage areas such as ward, corridor, toilet, stairs, and elevator are tested.	
2	Co-channel interference	≤ -20 dB Measured on the operating channel of TM80	Service person performs the test by using network survey tool. Make sure that all expected coverage areas such as ward, corridor, toilet, stairs, and elevator are tested.	
3	Ping delay	The mean delay of PC or cell phone with normal wifi module is smaller than 100ms and The packet lost rate shall be less than 1%.	Service person performs the test: 1, Connect PC or cell phone with normal wifi module to AP. 2, connect another pc to the LAN port where central station will connect to. Run	

			command"ping -t -l 32 -w 1000 IPaddress-of -cellphone" for 10 minutes,then run" ctrl+c".	
WLAN features				
1	802.11 protocol	TM80 only support 802.11 a/b/g/n, WLAN can't use other protocols	Check with hospital IT if this requirement is met or not.	
2	Security mode	<p>TM80 supports: WPA/WPA2-PSK or WPA2-Enterprise EAP method: PEAP-GTC, PEAP-MSCHAPv2, EAP-TLS</p> <p>WPA2-PSK is highly recommended. WPA2-Enterprise may increase probability of offline when roaming, so not be recommended. WLAN can't use other security mode.</p>	Check with hospital IT if this requirement is met or not.	
3	AP MAC address	<p>The broadcast MAC address of AP is fixed (BSSID). AP BSSID is used to locate the TM80 device. If it is</p>	Check with hospital IT if this requirement is met or not.	

		changed, failure to locate the TM80 may occur.		
4	AP channel width	If the AP supports 802.11n/ac, set the channel width to 20Mhz, don't use HT40 or even HT80.	Check with hospital IT if this requirement is met or not.	
5	Dedicated VLAN	The TM80 needs to work on a dedicated VLAN. Using VLAN can minimize Broadcast or multicast data which can affect TM80 stability.	Check with hospital IT if this requirement is met or not.	
The requirements of AP capability				
1	Recommended AP	Mindray's recommendations: Cisco: WLC 2504 (version 7-4-121-0 or later) + LAP: 2802 or 2602 or FAT AP:2602 Aruba: 7500 series+LAP: APIN0205APIN0205 Netgear: WNDAP350	Service person Check with hospital IT if this requirement is met or not. Get the AP model from related hospital people or observe directly.	

2	AP capability	<p>1, The anticipated number of devices connecting to one AP must be lower than the AP capability, and capability should have a margin of 50%. For example, In the coverage of one AP, the typical number of devices connected to this AP is 16, then the announced number of devices that can connect to AP simultaneously must be more than 32.</p> <p>2, The AP Can create several SSIDs.</p>	Service personnel get the AP model from related hospital people or observe directly. According to the model, get the data sheet of AP to make sure the capability.	
3	Device density	The maximum number of devices connected to one AP simultaneously is 16 (including TM80 and other devices).	Check with hospital IT if this requirement is met or not.	
4	AP compatibility	When customer using Aps not from Cisco, compatibility test should be passed	Mindray or Mindray's agent service engineer uses a TM80 to confirm in advance. Refer to 3.10 network survey with TM80, Set TM80 to	

			access to CMS, observe the performance of roaming and stability to make sure the AP compatibility.	
Network service and VLAN				
1	Port	UDP ports 5500 and 6678 are enabled. TCP ports 6587 and 7779 are enabled.	Check with hospital IT if this requirement is met or not.	
2	VLAN bandwidth	The planned bandwidth of TM80 must be larger than $N \times 100$ kbps (N is the number of installed TM80 products). For example, if 10 TM80 products are working at the same time, the VLAN needs to meet the bandwidth of 1000 kbps.	Check with hospital IT if this requirement is met or not. Service person perform the test by using TamoSoft Throughput Test tool	
3	Network continuity	In the coverage area of TM80, the network belongs to the same WLAN. All APs use the same SSID and encryption mode.	Check with hospital IT if this requirement is met or not. Service person perform the test by using Wireless network survey tool	
Important settings				
1	DHCP	The DHCP server reserves a sufficient	Check with hospital IT if this requirement is met or not.	

		number of IP addresses for the telemetry VLAN to ensure that the TM80 can obtain an IP address.		
2	IGMP snooping	If CMS accepts TM80 use multicast, enable IGMP snooping	Check with hospital IT if this requirement is met or not.	
3	Multicast	The multicast function is enabled. Otherwise, the TM80 can only connect to the CMS in unicast mode.	Check with hospital IT if this requirement is met or not.	
4	Beacon & DTIM	AP DTIM = 1, Beacon = 100ms	Check with hospital IT if this requirement is met or not.	
5	AP data rate	Close the data rate of 1Mbps,2Mbps,5.5Mbps in 802.11b	Check with hospital IT if this requirement is met or not.	
6	QOS	The switch or router must support QoS and the QoS level of TM80's subnet must be set to the highest level.	Check with hospital IT if this requirement is met or not.	
EAP requirements				
1	EAP requirements	Refer to 3.2.1.4 for detail	Check with hospital IT if this requirement is met or not.	

NOTE

- **Contents in 3.11.2Environmental Survey Table are actually part of 3.11.3Network Acceptance Table. If service personnel have already performed environmental survey, they can fill the survey results in the Network Acceptance Table directly.**

3.11.4 TM80 Verification Confirmation Table

Test or Observation Item	Result(Pass, Fail or NA)
Ping the TM80 from the CMS and make sure that the mean delay is less than 250 ms and the packet lost rate shall be less than 1%.	
Hold the TM80 and walk in the scope of different APs. After walking through the whole expected telemetry coverage area, observe continuous waveform on the CMS. Offline event times should be less than 10% of TM80 roaming times.	
In the location where coverage is the poorest, signal strength displayed on the screen is higher than -65dBm.	
When the signal strength is the weakest , the amount of time each TM80 transporting data to central station is not available shall be less than 86s over a 24 hour period	

4 Product Principles

4.1 System Composition

The TM80 consists of dedicated functional modules (MPAN module and Wi-Fi module), parameter front-end processing module, main control processor module and power module.

Dedicated functional modules: include the Wi-Fi module and MPAN module. The MPAN module is managed and controlled by the parameter front-end processor and the Wi-Fi module is managed by the main control processor.

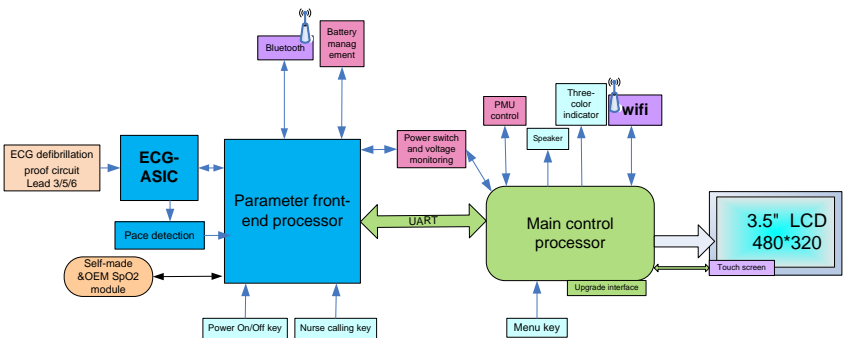
Parameter front-end processing module: The module is the core of the whole system and realizes parameter collection and communication control. The module completes ECG parameter sampling, obtains SpO2 parameter data, controls the MPAN module in completing communication with the NIBP module, packs parameter data and transmits it to the main control processor over protocol. It is also responsible for power management and key (power on/off key and nurse calling key) detection.

Main control processor: The main control processor realizes exchanging physiological parameter data with the front-end processor in real time, local parameter algorithm, data forwarding (transmission to the CMS over Wi-Fi) and collaboratively completes system power control with the parameter front-end. In addition, it drives the LCD display and touch screen, displays parameter waveforms and values in real time, and realizes man-machine interactive operation.

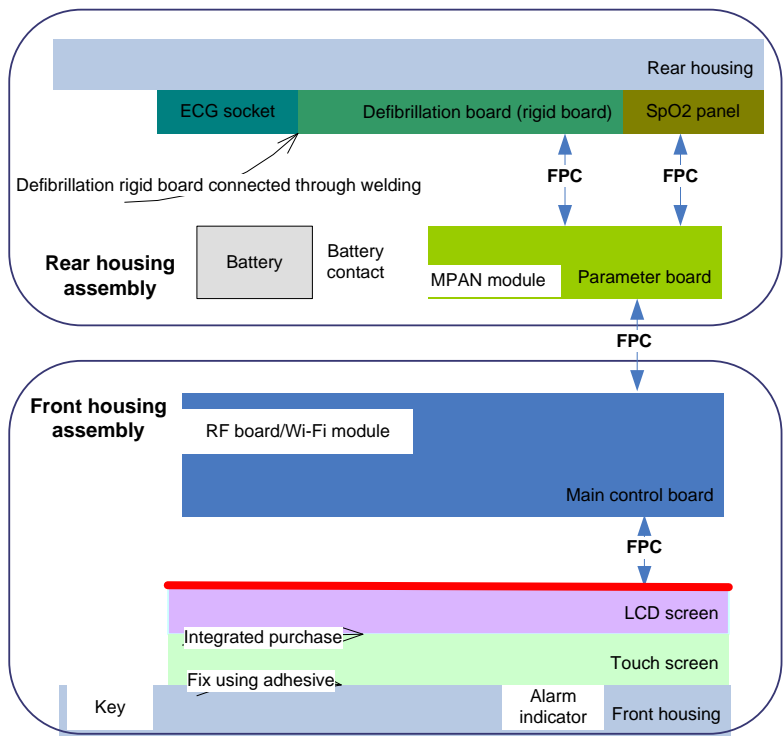
The parameter front-end exchanges data and information with the main control processor and the two work collaboratively. The parameter front-end exchanges data and control command with the main control processor through serial port. The parameter front-end transmits parameter data, information about keys and technical alarm information to the main control processor and the main control processor delivers data to the parameter front-end through serial port.

Based on the preceding description, the block diagram of system function deployment can be drawn:

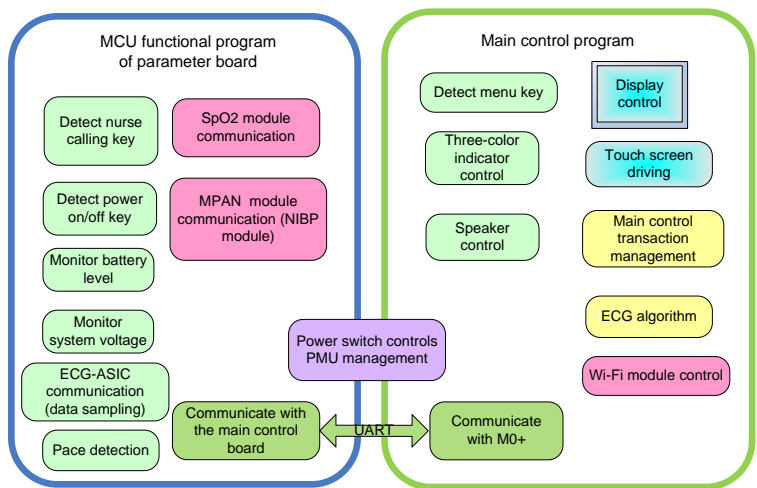
The following figure shows logical connections of the system:



The figure below shows physical connections of components inside the main unit of the TM80.

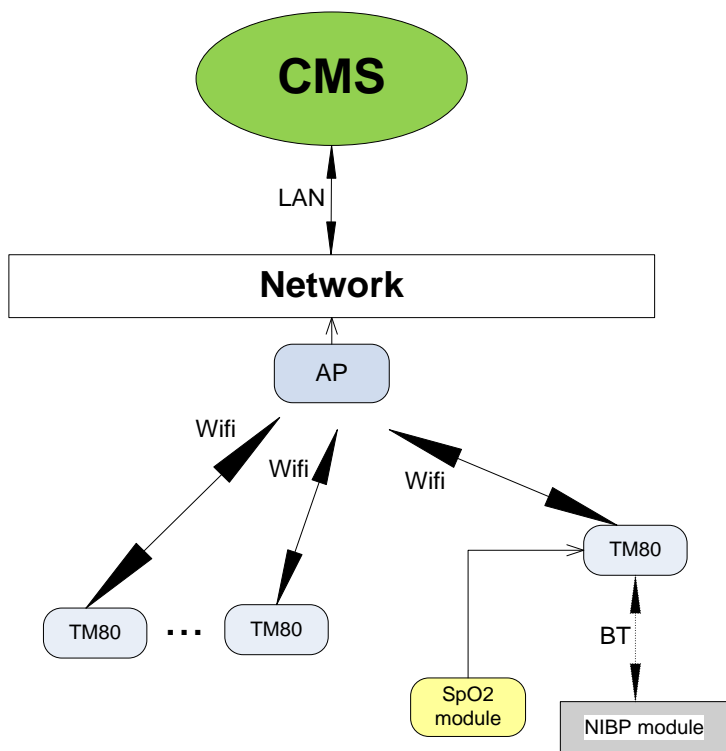


The figure below shows the software function deployment diagram:



4.2 System Signal Flow

The figure below shows the data flow of the TM80 Telemetry Monitor. The patients' physiological data (ECG, SpO₂ and NIBP) monitored by the TM80 is transmitted through the built-in low power consumption Wi-Fi module. The AP array picks up wireless signal and forwards it to the CMS through the network system of the hospital.



FOR YOUR NOTES

5 Testing and Maintenance

To ensure the TM80 always functions normally, qualified service personnel should perform regular inspection, maintenance and test. This chapter provides a checklist of the testing procedures for the TM80 with recommended test equipment and frequency. The service personnel should perform the testing and maintenance procedures as required and use appropriate test equipment.

The testing procedures provided in this chapter are intended to verify that the TM80 meets the performance specifications. If the TM80 or some of its functional module fails to perform as specified in any test, repairs or replacement must be done to correct the problem. If the problem persists, contact our Customer Service Department. If circuit diagrams, component part lists, descriptions, calibration instructions, or other information to assist service personnel to repair parts are required, contact our Customer Service Department.

CAUTION

- **All testssould be performed by qualified service personnel only.**
 - **Care should be taken to change the settings in theMaintenance menu to avoid loss of data.**
 - **Service personnel should acquaint themselves with the test tools and make sure that test tools and cables are applicable.**
-

5.1 Recommended Maintenance and Test Frequency

Check/Maintenance Item		Frequency
Visual inspection		When first installed or reinstalled.
Power-on test		<ul style="list-style-type: none">■ When first installed or reinstalled.■ Following any repairs or replacement of device components
ECG test	Performance test	<ul style="list-style-type: none">■ If the user suspects that the measurement is incorrect.■ Following any repairs or replacement of relevant module.■ At least twice every two years. <p>Note: NIBP test should be performed at least once a year.</p>
	Calibration	
Resp	Performance test	
SpO ₂ test		
NIBP test	Pressure check	
	Leakage test	
Nurse call test		If the user suspects that the nurse call functionality does not work properly.
Electrical safety tests		<ul style="list-style-type: none">■ After the TM80 or central charger falls off.■ At least once every two years or as needed.
Network print test		<ul style="list-style-type: none">■ When first installed.■ Whenever the printer is serviced or replaced.
Battery check	Functionality test	<ul style="list-style-type: none">■ When first installed.■ Whenever a battery is replaced.
	Performance test	For rechargeable lithium-ion battery: once every two months or when the battery runtime is reduced significantly.

5.2 Inspection before Daily Use

Perform visual inspection before daily use.

5.3 Preventative Maintenance Procedures

The following provides the item list for which preventive maintenance is required for the monitor.

- Visual inspection
- NIBP test and calibration

The recommended frequency of periodic maintenance for NIBP test and calibration is at least twice a year. For how to perform NIBP test and calibration, refer to **5.4.4 NIBP Tests**.

5.4 Parameter Test

5.4.1 ECG Test

5.4.1.5 ECG Performance Test

Tool required:

- Medsim 300B patient simulator recommended

Follow this procedure to perform the test:

1. Connect the patient simulator with the ECG module using an ECG cable.
2. Set the patient simulator as follows: ECG sinus rhythm, HR=80 bpm with the amplitude as 1mV.
3. Check the ECG waves are displayed correctly without noise and the displayed HR value is within 80 ± 1 bpm.
4. Disconnect each of the leads in turn and observe the corresponding lead off message displayed on the screen.
5. Set that the simulator outputs paced signals and set **Paced** to **Yes** on the TM80. Check the pace pulse marks on the TM80's screen.

5.4.1.6 ECG Calibration

The ECG signal may be inaccurate due to hardware or software problems. As a result, the ECG wave amplitude becomes greater or smaller.

Tool required:


- Vernier caliper

1. In the main menu, select **Parameter Setup**.
2. Select **ECG**.
3. Set **Filter** to **Monitor**.
4. Return to the main menu and select **Maintenance**.
5. Input the maintenance passcode.
6. Tap Accept.
7. In the **Maintenance** menu, select **General**.
8. Enable **Calibrate ECG**. A square wave appears on the screen and the message **ECG Calibrating** is displayed in the technical alarm area of the device's screen. Compare the amplitude of the square wave with the wave scale. The difference should be within 5%.
9. After completing the verification, disable **Calibrate ECG**. If necessary, you can print out the square wave and wave scale through the recorder and then measure the difference.

5.4.2 Resp Test

5.4.2.7 Enabling Resp Functionality

Before performing the Resp performance test, you need to enable the Resp functionality. Follow this procedure to enable the Resp functionality:

1. After powering on the TM80, press  to enter the main menu of the transmitter.
2. Select **Maintenance**→input the maintenance passcode→tap **Accept**→select **Service**.
3. Input the passcode.
4. Tap **Accept**.
5. Enable **Support Resp**.
6. Return to the main menu.
7. Select **Maintenance**→input the maintenance passcode→tap **Accept**→select **General**.
8. Enable **Resp**.

5.4.2.8 Resp Performance Test

Tools required:

- Medsim300B patient simulator

1. Connect the patient simulator to the TM80 using an ECG cable and set lead II as the respiration lead.
2. Configure the simulator as follows: lead II as the respiration lead, base impedance line as 500 Ω ; delta impedance as 1 Ω , respiration rate as 20 rpm.
3. Verify that the Resp wave is displayed without any distortion and the displayed Resp value is within 20 ± 1 rpm.

5.4.3 SpO₂ Test

Tool required:

- None

Follow this procedure to perform the test:

1. Connect an adult SpO₂ sensor to the SpO₂ connector of the TM80.
2. In the main menu, select **Patient Info** and set **Patient Category** to **Adult** on the TM80.
3. Measure SpO₂ on your finger. (Assume that you stay healthy)
4. Check the Pleth wave and PR reading on the screen and make sure that the displayed SpO₂ is within 95%-100%.
5. Remove the SpO₂ sensor from your finger and make sure that an alarm of SpO₂SensorOff is triggered.

Measurement accuracy verification:

The SpO₂ accuracy has been verified in human experiments by comparing with arterial blood sample reference measured with a CO-oximeter. Pulse oximeter measurements are statistically distributed and about two-thirds of the measurements are expected to come within the specified accuracy range compared to CO-oximeter measurements.

NOTE

- **A functional tester cannot be used to assess the accuracy of a pulse oximeter monitor. However, it can be used to demonstrate that a particular pulse oximeter monitor reproduces a calibration curve that has been independently demonstrated to fulfill a particular accuracy specification.**
-

5.4.4 NIBP Tests

Perform NIBP accuracy test and leakage test at the BP10.

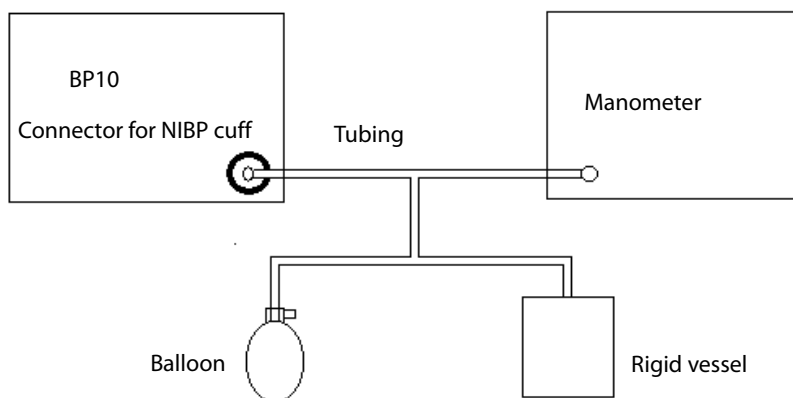
5.4.4.9 NIBP Accuracy Test

Tools required:

- T-shape connector
- Appropriate tubing
- Balloon pump
- Rigid Vessel with volume 500 ± 25 ml
- Reference manometer (calibrated with accuracy equal to or greater than 1 mmHg)

Follow this procedure to perform the test:

1. Connect the equipment as shown below.



4. Before inflation, the reading of the manometer should be 0. If not, turn off the balloon pump to let the whole airway open to the atmosphere. Turn on the balloon pump after the reading is 0.

3. On the main menu of the BP10, select **System→Maintenance→NIBP Accuracy Test**.
4. Check the manometer values and the values displayed on the BP10. Both should be 0mmHg.
5. Raise the pressure in the rigid vessel to 50 mmHg with the balloon pump. Then, wait for 10 seconds until the measured values become stable.
6. Compare the manometer values with the values displayed on the BP10. The difference should be 3 mmHg. If it is greater than 3 mmHg, contact your service personnel.
7. Raise the pressure in the rigid vessel to 200 mmHg with the balloon pump. Then, wait for 10 seconds until the measured values become stable and repeat step 6.

NOTE

- **You can use an NIBP simulator to replace the balloon pump and the reference manometer to perform the test.**
 - **You can use an appropriate cylinder and a cuff instead of the rigid vessel.**
-

5.4.4.10 NIBP Leakage Test

NOTE

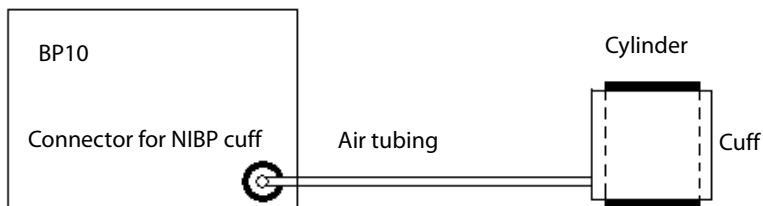
- **You should perform NIBP accuracy test and make sure the test result is pass prior to NIBP leakage test.**
-

Tools required:

- NIBP cuff for adult patient
- Appropriate tubing
- Cylinder

Follow this procedure to perform the test:

1. Set Patient Category to Adult.
2. Connect the NIBP cuff with the NIBP connector on the monitor.
3. Apply the cuff to the cylinder as shown below.



4. On the main menu of the BP10, select **System**→**Maintenance**→NIBP Leakage Test. The NIBP parameter area displays Leakage Testing....
5. The cuff automatically deflates after 20s, which means NIBP leakage test is completed. If no message is displayed in the NIBP parameter area, it indicates that the system has no leakage. If the message **NIBP Pneumatic Leak** is displayed, it indicates that the system may have a leakage. In this case, check if all connections are good and the cuff and tubing have no leakage. Perform the test again after making sure all connections are good and the cuff and tubing have no leakage.

You can either perform a manual leakage test:

1. Perform Steps 1 to-4 in the ***NIBP Accuracy Test*** section.
2. Raise the pressure in the rigid vessel to 250 mmHg with the balloon pump.
Then, wait for 5 seconds to let the measured values becoming stable.
3. Record the current pressure value and meanwhile use a time counter to count time. Then, record the pressure value after counting to 60s.
4. Compare the two values and make sure the difference should not be greater than 6 mmHg.

5.5 Miscellaneous Tests

5.5.1 Visual Inspection

Perform a visual inspection before the equipment is first used every day. Verify that the equipment meets the following requirements:

- The housing and display screen are free from cracks or other damages.
- All keys function properly.
- Connectors are not loose, cracked, or bent and cables have no cuts, nicks, or fraying.
- ECG leadwires are securely connected with the equipment.
- Battery pack is installed and has sufficient charge.
- Chest electrodes are free from cracks and limb electrodes can properly clamp.
- The external connectors are not loose and the pins are not bent.
- The safety labels and data plates on the equipment are clearly legible.


5.5.2 Power-On Test

This test is to verify that the TM80 can be powered on correctly. Follow this procedure to perform the test:

1. Install a lithium-ion rechargeable battery pack or AA batteries into the device's battery compartment.
2. The TM80 will be powered on automatically. The alarm light will momentarily illuminate cyan to indicate that the equipment is starting.
3. The boot screen appears, the TM80 sounds a beep, and its alarm light flashes red, yellow, and cyan in turn, and then turns off. This indicates that the alarm system functions correctly.
4. When the boot screen disappears, the main screen displays and the device finishes starting.

5.5.3 Nurse Call Test

Follow this procedure to perform the test:


1. Press the nurse call button  on the device.
2. Observe corresponding display on the central station. If a nurse call icon appears, it indicates that the nurse call test passes.

5.5.4 Electric Safety Test

Refer to ***AElectrical Safety Inspection***.

5.5.5 Network Print Test

Follow this procedure to perform the test:

1. Power on the device.
2. Connect the device to the central station wirelessly.
3. Press  to enter the main menu of the device or swipe your finger up from the bottom of the main screen to display the quick keys area.
4. Select **Print**.
5. Verify that the network printer shall print out a report correctly.

5.5.6 Battery Check

Tool required:

None

Performance Check

See the chapter about battery in the Operation Manual to check performance and verify the battery supply time specification.

Refer to 13 Battery in the BeneVision TMS60 Telemetry Monitoring System/TM80 Telemetry Monitor Operator's Manual for methods to check battery status and verify battery supply specifications

6 Hardware Upgrade

6.1 Adding the SpO₂ Function

The TM80 is equipped with the SpO₂ interface and the SpO₂ function can be added through upgrade during later use. The SpO₂ module is on the SpO₂ extension cable.

Required materials

If you need to add the SpO₂ function, you need to purchase the dedicated SpO₂ extension cable and SpO₂ sensor of the TM80. For the SpO₂-related bill of materials, see *9 Maintenance Materials*.

Upgrade method

Plug the SpO₂ sensor connector into the SpO₂ module and then connect the SpO₂ module to SpO₂ connector in the TM80.

Verification method

Apply the SpO₂ sensor to appropriate site of a patient. SpO₂ waveforms and values are displayed on the screen. For a health adult, the SpO₂ value should be above 90% and SpO₂ waveforms are rhythmic. On the CMS, corresponding waveforms and values can be seen.

6.2 Adding the NIBP Module (BP10)

The TM80 is connected to the BP10 module over MPAN and the NIBP function can be added through upgrade during later use. The BP10 module is an independent module. It completes NIBP measurement independently and sends data to the TM80 over MPAN.

Required materials

BP10 module. For the specific BOM, see NIBP-related bill of materials, see **9 Maintenance Materials** or consult Mindray engineers.

Upgrade method

Connect the BP10 module to the TM80 over MPAN as instructed in **Chapter 10 of BeneVisionTMS60 Telemetry Monitoring System/TM80 Telemetry Monitor Operator's Manual**.

Verification method

Start NIBP measurement on the BP10 module. Measurement results can be seen on the TM80 and CMS.

6.3 Adding the Number of the TM80 Telemetry Monitors

The number of the TM80 Telemetry Monitors can be added flexibly. If you need to add one TM80 Telemetry Monitor, you only need to set CMS information in the TM80 menu and admit the TM80 on the CMS. The new TM80 monitor can work in the system.

Required materials

TM80 monitor. For the specific BOM, see the chapter about maintenance material in the manual or consult Mindray engineers.

Upgrade method

See the *Operation Manual* and connect the new TM80 monitor to the CMS.

Verification method

Connect the TM80 to a simulator or human body or enable demo mode on the TM80. Relevant measurement results can be seen on the TM80 and CMS.

NOTE

- **The Demo Mode must be disabled before putting the TM80 into clinical use.**
-

6.4 Extending Coverage

The coverage of the TM80 depends on the signal coverage of the Wi-Fi network used for the TM80 and is irrelevant to the TM80. To extend the coverage of the TM80, add the number of APs to extend the range of telemetry Wi-Fi network.

Required materials

- If the telemetry Wi-Fi network is provided by Mindray, increase the number of APs to extend telemetry coverage.
- If the telemetry Wi-Fi network is provided by a hospital, communicate with the hospital to extend coverage of the Wi-Fi network.

Upgrade method

Extend the coverage of Wi-Fi network per requirements on Wi-Fi network described in *3Installation*.

Verification method

Refer to section 3.10 Network Verification with TM80.

FOR YOUR NTOES

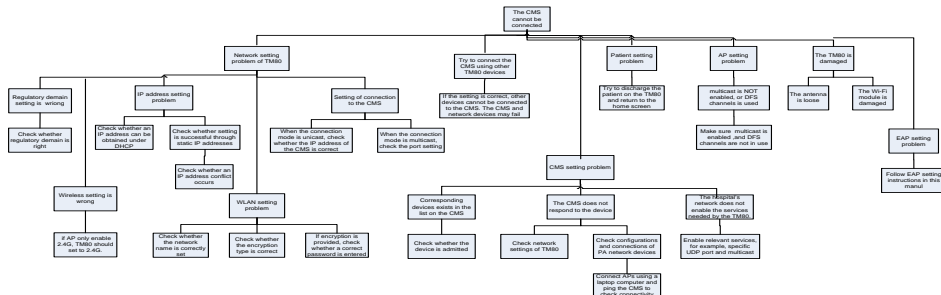
7 Troubleshooting

In this chapter, TM80 problems are listed along with possible causes and recommended corrective actions. Refer to the tables to check the device, identify and eliminate the troubles.

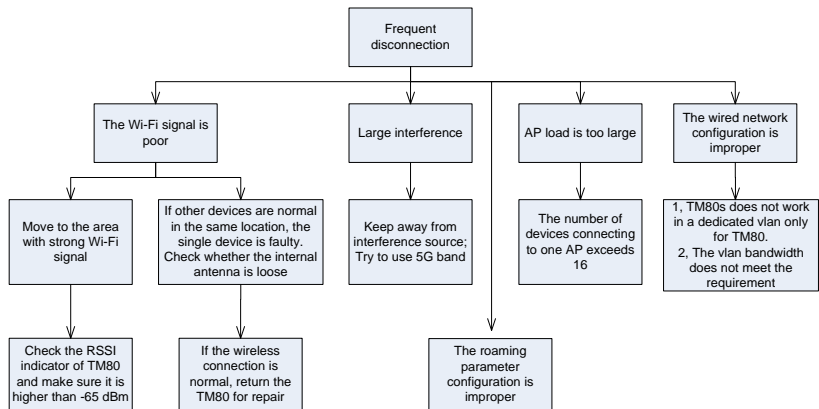
The troubles we list here are frequently arisen difficulties and the actions we recommend can correct most problems, but not all of them. For more information on troubleshooting, contact our Customer Service Department.

7.1 Common Faults

7.1.1 The TM80 Failed to Connect to the Central Station

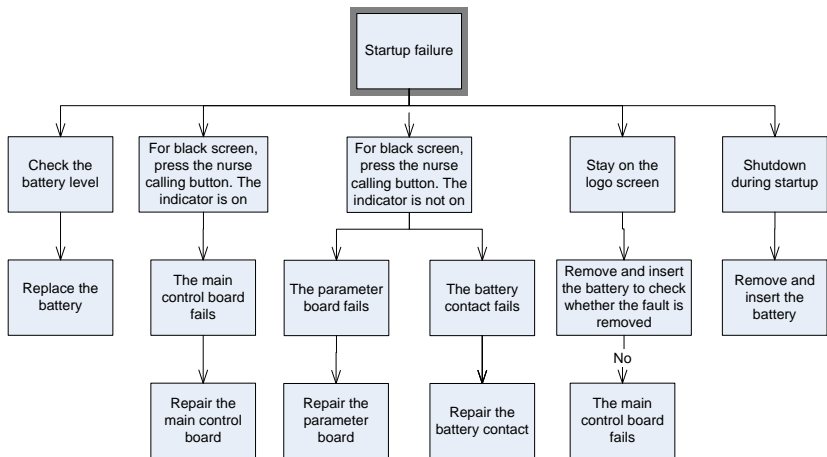


7.1.2 The TM80 Are Offline Frequently



7.1.3 The TM80 Cannot Be Powered On

Diagnosis of the fault that the TM cannot be powered on:



7.1.4 The Working Duration of Battery Becomes Short

Possible causes:

- The lithium-ion battery is aged or is not fully charged.
- AA batteries are not of the type specified by Mindray.
- Wi-Fi signal is poor and frequent operation is performed on the screen.

7.2 Technical Alarms

Item	Alarm Message	Possible cause	Solution
ECG	ECG Lead Off	The electrode has become detached from the patient or the lead wire has become disconnected from the adapter cable.	Check the connections of the electrodes and leadwires.
	ECG XX** Lead Off		
	ECG Module Error	<ul style="list-style-type: none">■ An error occurred to the ECG module.■ There is a problem with the communications between the module and the TM80.	Restart the TM80. If the problem persists, contact your service personnel.

Item	Alarm Message	Possible cause	Solution
ECG	ECG Noise	The ECG signal is noisy.	Check for any possible sources of signal noise around the cable and electrode, and check the patient for great motion.
	ECG Cable Type Error	Connect wrong ECG leadwire.	Reconnect the 3 or 5 lead ECG leadwire.
	HR Overrange	HR exceeds the measurement limit.	Contact Mindray or your service personnel.
Resp	Electrode Poor Contact	The electrode has been used for a long time or the electrode contact is poor.	Check the electrode application. Reposition or replace the electrodes if necessary.
SpO ₂	SpO ₂ Sensor Off	The SpO ₂ sensor has become detached from the patient or the module.	Check the sensor application site and the sensor type, and make sure the sensor is not damaged.
	SpO ₂ Sensor Fault		
	SpO ₂ No Sensor	There is a fault with the SpO ₂ sensor.	Reconnect the sensor

Item	Alarm Message	Possible cause	Solution
SpO ₂	SpO ₂ Module Error	An unspecified SpO ₂ sensor has been used.	or use a new sensor.
	SpO ₂ Too Much Light	There is too much light on the SpO ₂ sensor.	Move the sensor to a place with lower level of ambient light or cover the sensor to minimize the ambient light.
	SpO ₂ No Pulse	SpO ₂ sensor failed to obtain pulse signal.	Move the sensor to a site with better perfusion.
	SpO ₂ Unplugged	SpO ₂ module connector is disconnected from the TM80.	Reconnect the SpO ₂ module to the TM80.
	PR Overrange	The measured PR value exceeds the measurement range.	Contact Mindray or your service personnel.
NIBP	MPAN Disconnected	The MAPN is disconnected.	Enable the MPAN switch.
	NIBP Clock Needs To Be Set	The button cell does not have sufficient charge.	Reset the system time for the BP10.

Item	Alarm Message	Possible cause	Solution
NIBP	NIBP Error	An error occurred to the NIBP module. There is a problem with communication between the TM80 and BP10.	Restart the BP10.
	NIBP Cuff Loose	The NIBP cuff is not properly connected. There is a leak in the airway.	Check the patient's condition and verify patient category. Replace with an appropriate cuff and connect it correctly.
	NIBP Airway Error	An airway error occurs.	Check the airway.
	NIBP Weak Signal	The patient's pulse is weak or the cuff is loose.	Check the patient's condition and change the cuff application site. If the error persists, replace the cuff.
	NIBP Overrange	The measured NIBP value is not within the specified range.	Contact your service personnel.

Item	Alarm Message	Possible cause	Solution
NIBP	NIBP Excessive Motion	Patient's arm moves too much.	Check the patient's condition and reduce the patient motion.
	NIBP Cuff Overpressure	The NIBP airway may be occluded.	Check the airway and measure again.
	Cuff or Airway Leak	The NIBP airway may leak air.	Verify that the cuff is properly connected. 2. Verify that the airway does not leak air.
	NIBP Timeout	Time is out. The measurement time is over 120 seconds.	Check the patient's condition and NIBP connections. Replace the cuff.
	NIBP Cuff and Patient Mismatch	The cuff type applied mismatches the patient category.	Check the patient's category. Replace the cuff.
	Intervals Not Set	The interval in Sequence mode is not set.	Set the intervals.
	NIBP-S Overrange	The measured NIBP value is not within the	Contact your service personnel.

Item	Alarm Message	Possible cause	Solution
NIBP	NIBP-Sys Over upper range	measurement range.	
	NIBP-Sys Over lower range		
	NIBP-DiaOverrange		
	NIBP-Dia Over upper range		
	NIBP-Dia Over lower range		
	NIBP-M Overrange		
	NIBP-Mean Over upper range		
	NIBP-Mean Over lower range		
	NIBP Battery Error	The lithium-ion battery communication has an error.	Replace with a known good battery.
	NIBP Battery Depleted	The battery charge is almost depleted.	

Item	Alarm Message	Possible cause	Solution
NIBP	NIBP Voltage Error	The battery voltage is abnormal.	
	NIBP Battery Maintenance Required	The lithium-ion battery is aging.	
Power	Low Battery	The battery charge is low.	Replace with a known good battery.
	Critically Low Battery	The battery charge is almost depleted.	
	Battery Maintenance Required	The lithium-ion battery is aging.	
	Battery Error	The lithium-ion battery communication is error.	
	Battery Type Error	The battery contacts are in bad contact.	


Item	Alarm Message	Possible cause	Solution
System	Device Error	The self-test error occurs to the TM80 main board. The self-test error occurs to the parameter module, wireless module or Mindray PAN module. The self-test error occurs to the parameter module communication or initialization.	Restart the TM80. If the problem persists, contact your service personnel.
	Restoring Last Defaults Failed	Restoring the last default configuration is error.	
	Loading Defaults Failed	Loading the default configuration is error.	
	No CMS	<ul style="list-style-type: none"> ■ The battery of the TM80 is used up and the TM80 is powered off automatically. ■ The patient has walked out of the Wi-Fi signal coverage area. ■ The Wi-Fi antenna 	<ul style="list-style-type: none"> ■ Replace the battery with a fully charged lithium-ion battery or new AA battery. ■ Make sure that the patient is within the signal coverage area. ■ Access the

Item	Alarm Message	Possible cause	Solution
System		<p>of the TM80 fails.</p> <ul style="list-style-type: none"> ■ The patient is not admitted by the CMS. ■ Serious WLAN interference and AP failure make the TM80 unable to connect the network on the CMS. ■ An IP address conflict occurs. 	<p>system maintenance screen and make sure that the RSSI of network signal is displayed normally.</p>
			<ul style="list-style-type: none"> ■ Admit the patient on the CMS or discharge the patient at the TM80. ■ Make sure that the network signal interface is normal. ■ Make sure the IP address of the TM80 is unique.
	Searching for signal	<ul style="list-style-type: none"> ■ The Wi-Fi signal of the TM80 is poor. ■ Wi-Fi signal interference occurs. 	<ul style="list-style-type: none"> ■ Check whether the patient is at the edge of signal coverage. ■ It is recommended

Item	Alarm Message	Possible cause	Solution
System			<p>to check whether network interference signal exceeds the limit by using a signal survey tool.</p> <ul style="list-style-type: none"> ■ If APs in hospital support 5G band, configure the TM80 to work in the 5Gband.

7.3 Other Faults

Symptom	Possible cause	Solution
ECG noise	The noise interference is overlapped with ECG waveforms	<ul style="list-style-type: none"> ■ Check that the electrodes are in good contact with the skin. ■ Check that the ECG leadwires are connected securely. ■ Check that the patient does not contact any ungrounded electric equipment.
ECG signal saturated	The TM80 detected ECG signal saturation or overload.	<ul style="list-style-type: none"> ■ Check the ECG leadwires. ■ Check that the electrodes are in good contact with the skin.

Symptom	Possible cause	Solution
		<ul style="list-style-type: none"> Check that the electrodes are not expired.
The TM80 or SpO ₂ module is started repeatedly.	The battery capacity for the TM80 is depleted.	Replace with a known good battery.
No pulse	The SpO ₂ sensor fails to obtain the pulse signal.	Check the patient's physiological conditions and change the sensor's application site for SpO ₂ measurement. If the fault persists, replace the sensor.
The SpO ₂ data is not displayed on the CentralStation.	<ul style="list-style-type: none"> The SpO₂ module is not connected to the TM80. There might be a problem with the SpO₂ module. 	<ul style="list-style-type: none"> Connect the SpO₂ module to the TM80. Replace the SpO₂ module with a known good one.
The TM80 cannot be connected to the Central Station wirelessly and the Wi-Fi symbol  on the main screen of the TM80 is displayed.	The wireless access point (AP) in the vicinity is not enabled.	Make sure that the AP is enabled and belongs to the Virtual LAN (VLAN) where the TM80 is covered.
	The TM80 is not powered on under the AP coverage area.	Put the TM80 within the AP coverage area and restart it. Ensure that the signal strength displayed on the TM80 is greater than -65dBm and the co-channel interference meets the requirements.
	Items like SSID, IP acquisition mode are not configured correctly for the TM80.	Follow section 3.9 to re-configure all WLAN related settings.

Symptom	Possible cause	Solution
	The working channel of AP is not configured properly. TM80 can't work in DFS channels in 5G band.	Contact your service personnel.
	WiFi Regulatory domain setting is wrong	Set WiFi Regulatory domain the same with region of the hospital, and make sure AP's WiFi Regulatory domain is also the same with region of the hospital,
	The TM80 has a fault.	Check whether other TM80 monitors can be online. If other TM80 monitors can be online, restart the TM80 and make sure that the configurations are the same. If the configurations are the same but the TM80 cannot be online, the TM80 needs to be returned for repair.
	EAP setting is wrong	Contact your service personnel.
	EAP certificate is out of date	Contact your service personnel.
The TM80 has been connected to the wireless network but cannot be connected to the Central	The TM80 is not admitted by the Central Station yet.	Admit the TM80 again on the CMS.
	IP addresses cannot be obtained. IP addresses in the IP address pool of the DHCP server are used up.	<ul style="list-style-type: none"> ■ Attempt to connect to the CMS by using another network device and check whether IP addresses can be obtained. ■ Contact your service personnel.

Symptom	Possible cause	Solution
Station.	Static IP conflict	■ Check whether repeated IP addresses are assigned.
	The network link fails.	Contact your service personnel.
	Multicast TTL is not large enough	Main Menu-> Maintenance -> Network -> Connect CMS , a user can find TTL parameter. If CMS and TM80 are not in the same subnet, TTL should be greater than 1.
	The hospital's network does not enable the services needed by the TM80.	Contact the IT Dept. to handle the problem.
Single TM80 is offline occasionally.	The TM80 is located in the blind area of Wi-Fi coverage.	Contact your service personnel.
	The TM80 has a fault.	In the same location, check whether one TM80 monitor becomes offline more frequently. Restart the TM80. If the fault persists, return the TM80 for repair.
	Static IP conflict	Check whether repeated IP addresses are assigned.
Some TM80s are offline occasionally.	AP in some area is damaged.	Make sure that APs are started and are working properly.
	Roaming parameter is not properly set.	Refer to 3.9.4.4Roaming Test in this manual.
	EAP certificate is out of date.	Contact your service personnel.

Symptom	Possible cause	Solution
	Severe interference occurs in some areas.	Contact your service personnel.
	The signal strength is weak some areas.	
All the TM80s are offline occasionally.	Partial wired network is not configured properly.	<ul style="list-style-type: none"> ■ Confirm the configurations by using a wired monitor and make sure that VLAN bandwidth configured on the switch is sufficient and has a margin greater than 50%. ■ Confirm interference by using Wireless network survey tool. If obvious interference sources are found, eliminate the interference or change WLAN deployment until Mindray's requirements are met.
The TM80 cannot find the BP10.	The BP10 is faulty.	Return the BP10 for repair.
The TM80 cannot establish connection with the BP10.	Configuration error	Verify that the MPAN switch at the TM80 is enabled and the MPAN key on the BP10 is pressed.
The TM80 and BP10 are prone to offline.	When the TM80 and BP10 are secured to the patient, signals may be blocked by the patient's body.	Put the TM80 and BP10 closer.

Symptom	Possible cause	Solution
The TM80 and BP10 are prone to offline in certain area.	As there are many Wi-Fi devices in this area, communication between the TM80 and BP10 is interfered seriously.	Contact your service personnel.
Some TM80 or BP10 is prone to offline.	Device malfunction	Use other monitors to confirm the fault. If only monitor is faulty, return the monitor for repair.

7.4 Error Codes

Error code	Description
001	Module Selftest Err(0xff)
002	ECG ASIC Init Err
003	ECG ASIC 3.3V Err
004	SPO2 Init Err
006	MPANInit Err
008	Battery Comm Err
011	Power 2.5V Err(0xff)
013	SPO2 Selftest: AFE4490
014	SPO2 Selftest: CPU
015	SPO2 Selftest: FLASH
016	SPO2 Selftest: POWER
017	SPO2 Selftest: RAM
018	SPO2 Selftest: WATCHDOG

Error code	Description
019	SPO2 Selftest: REGISTER
020	ECG Selftest(0xff)
021	Module Watchdog Err
103	RTC Comm Err
104	E2PROM Err
105	ECG Init Err
106	ECG Comm Stop
107	ECG Comm Abnormal
108	ECG COMM Err
109	SPO2 Init Err
110	SPO2 Comm Stop
111	SPO2 Comm Abnormal
112	SPO2 Comm Err
113	SPO2 Board Fault
114	Module Init Err
115	Module Comm Err
116	Main Board Selftest Err

8 Disassembly

8.1 Overview

This chapter describes how to disassemble the TM80 and the BP10.

Before disassembling the TM80 and the BP10, make the following preparations:

- Ensure that the TM80 or the BP10 is not used for monitoring a patient and has been disconnected from the patient.
- Disassemble the TM80 or the BP10 on the workbench of the equipment maintenance room.
- The personnel who will disassemble the TM80 or the BP10 must be qualified for maintenance of medical equipment or have received training given by Mindray or have been authorized by Mindray.
- In the disassembly process, the personnel disassembling the TM80 or the BP10 must take protective measures related to Electro-Static discharge (ESD).

NOTE

- **During re-installation after disassembling the device, the sealing strip must be installed correctly. Improper installation of the sealing strip may degrade the waterproof performance of the device.**
-

8.2 Disassembling the TM80

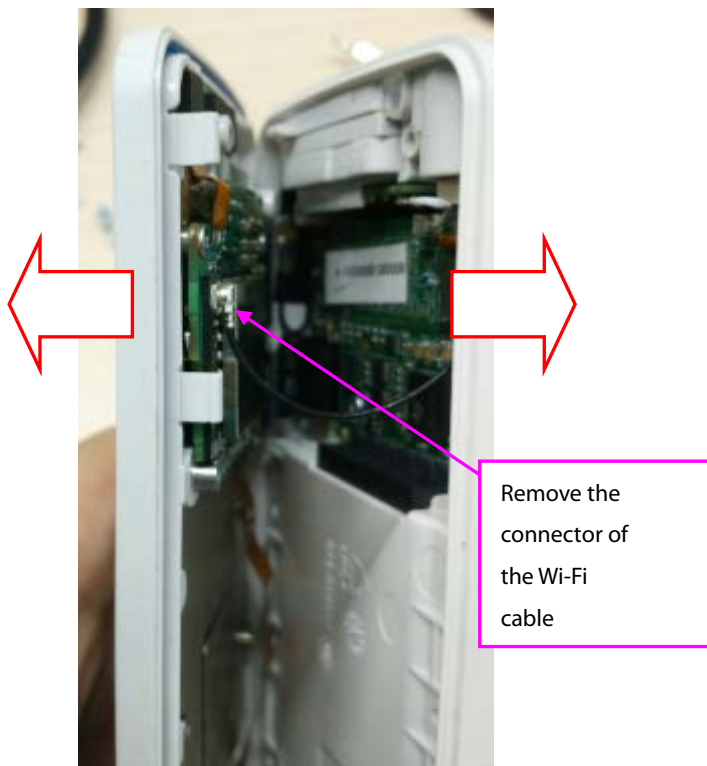
1. Remove the label on the rear housing of the TM80 and remove the battery. Unscrew the screws on the front and rear housing by using a Phillips screwdriver.



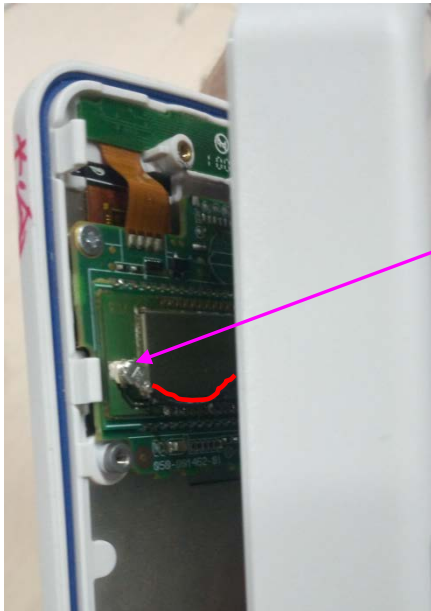
2. Hold the display and let it face your left palm, open the front and rear housings, and remove the connector of the Wi-Fi cable.

CAUTION

- **Do not pull apart the Wi-Fi cable of the TM80.**
-

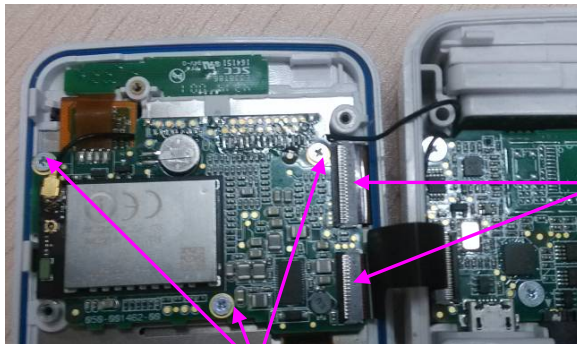


3. Connect the WiFi antenna connector before assembling the back cover. Note that the WiFi antenna wire should be in the position indicated by the red curve.



Assemble the wifi antenna connector, the wire direction should be inside, as shown in red.

4. Remove the three M1.6x2.4 cap head screws on the main control board, open the card fasteners of the FPC socket, and remove the two FPCs.



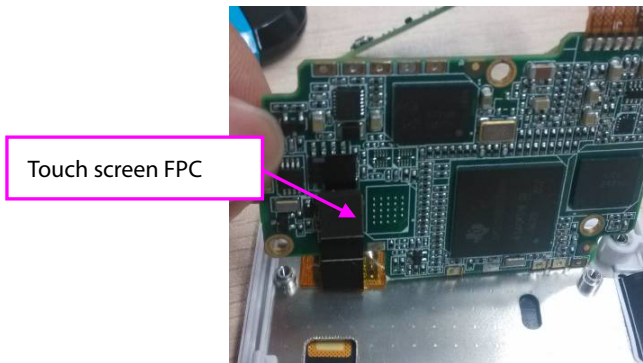
Three M1.6×2.4 cross recessed cheese head screws

Open card fasteners of the two FPCs and remove the two FPCs

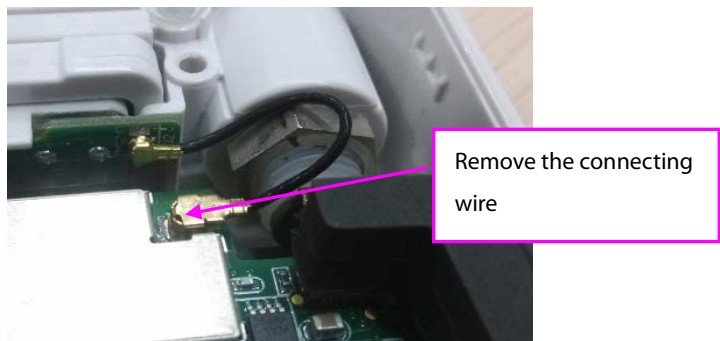
NOTE

- **As FPC is fragile and easy to be broken, do not drag FPC hardly. When assembling FPC, make sure that the Goldfinger is thoroughly inserted into the connector.**
-

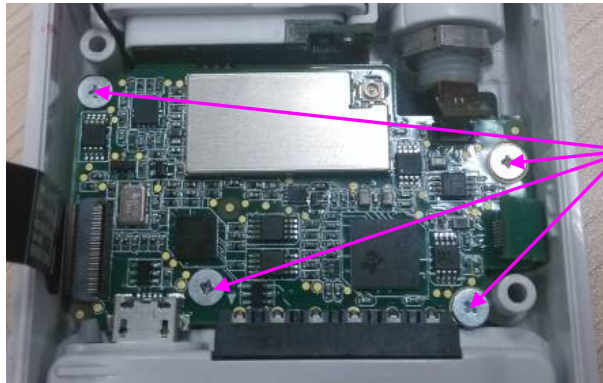
5. Remove the touch screen FPC at the back of the main control board.



6. Remove the connecting wire on the parameter board and ECG panel.

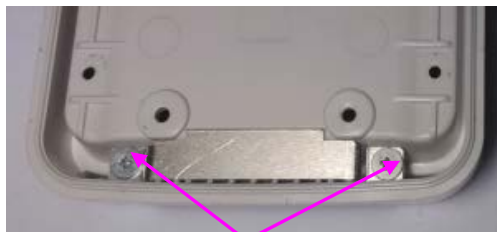


7. Remove the four M1.6X3.5 cap head screws on the parameter board and remove the parameter board from the rear housing.



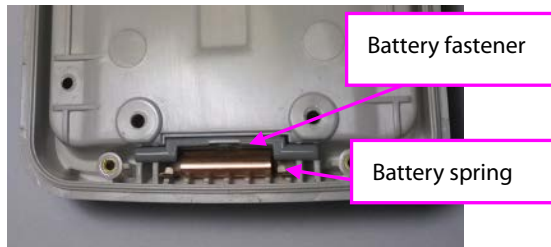
Four
M1.6
× 3.5
screws

8. Remove 2 M1.6x3.5 cap head screws and take down the fastening sheet metal of the battery spring.



Remove two M1.6 × 3.5 screws

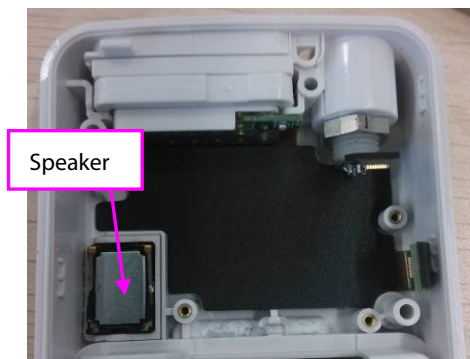
9. Take out the battery spring and battery fastener.



NOTE

- The two bending parts of the battery spring face upward.

10. Remove the speaker.



NOTE

-
- The contact spring of the speaker is in the upper part.
-

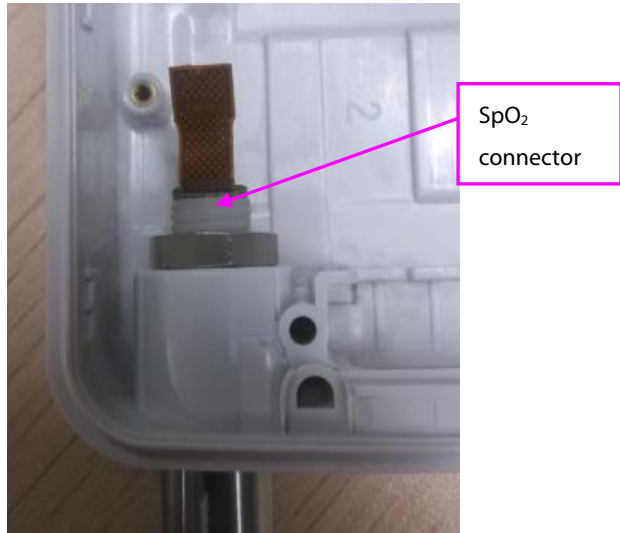
11. Take down the ECG limit stop and remove the paddles.



NOTE

-
- The gap of the ECG limit stop is on the right.
-

12. Unfasten the nuts of the SpO₂ connector by using needle-nose pliers and remove the SpO₂ connector.

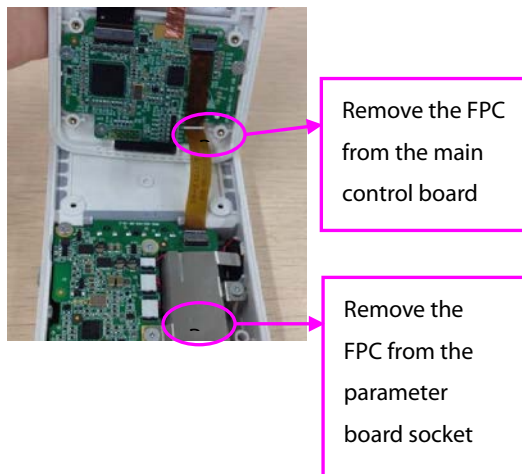


8.3 Disassembling the BP10

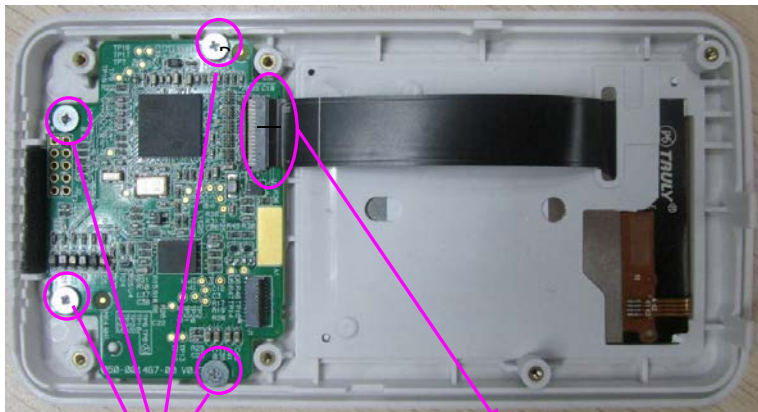
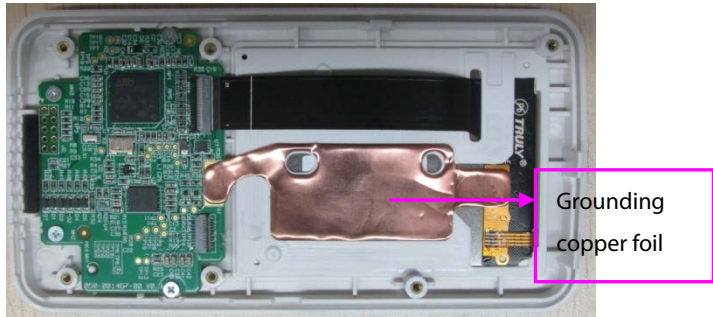
1. Remove the label on the rear housing of the BP10 and remove the battery.
Remove screws on the front and rear housings by using a Phillips screwdriver.



2. Open the front and rear housings and remove the FPCs that connect the front and rear housings.

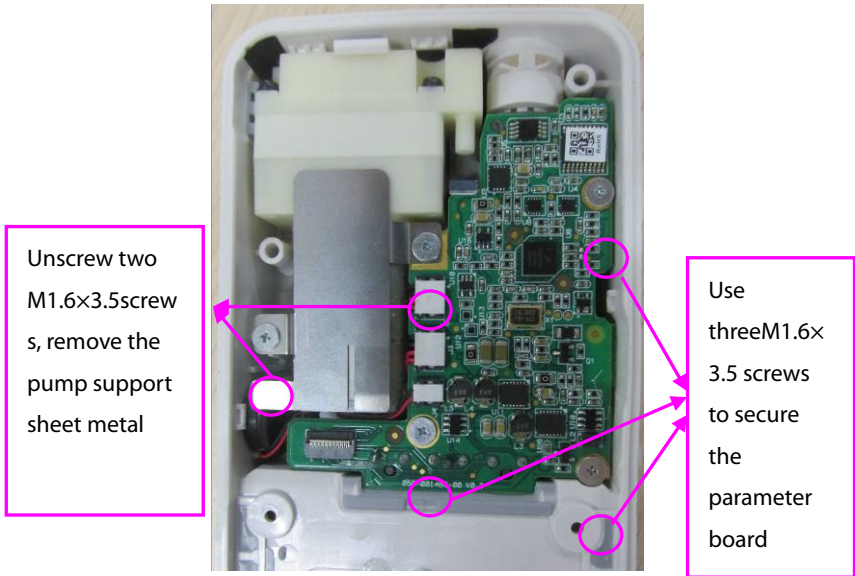


3. Remove the grounding copper foil and four M1.6x2.4 cap head screws on the main control board, open the card fasteners on the FPC socket, and remove the two FPCs.

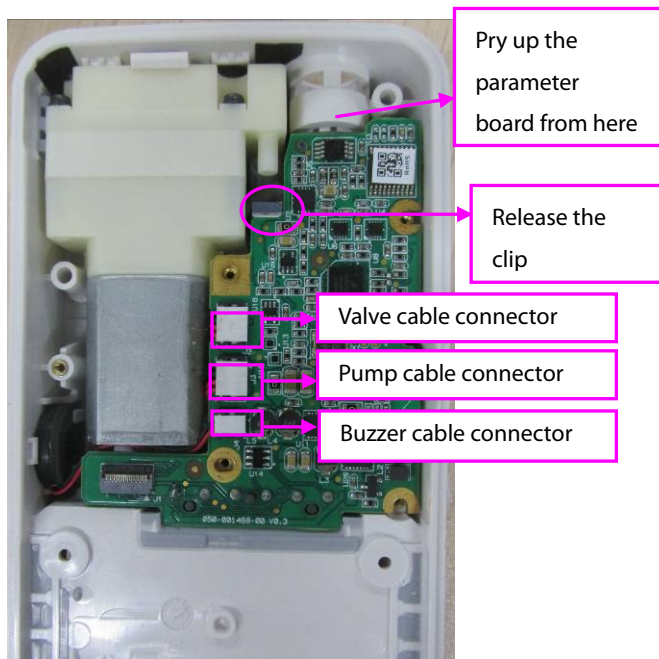


Four M1.6×2.4cap head screws

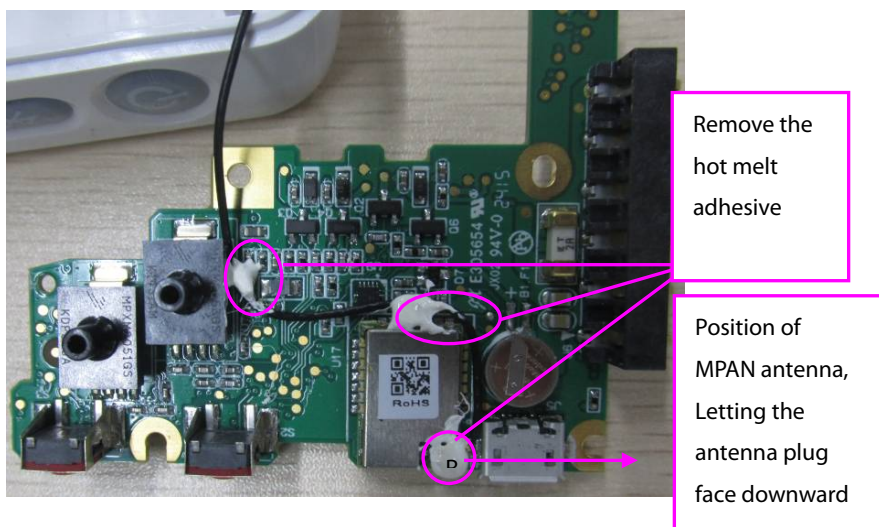
4. Remove the five M1.6x3.5 cap head screws on the parameter board and take down the pump support sheet metal.



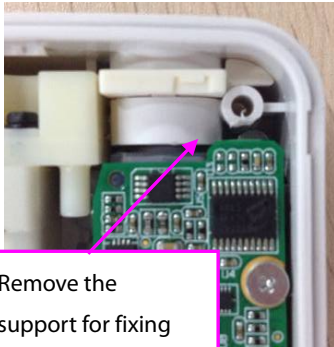
5. Pull up connectors of the buzzer, pump and valve and remove the parameter board from the rear housing. To remove the parameter board, first release the clip on the integrated circuit and then pry up the board from the end close to the air tap.



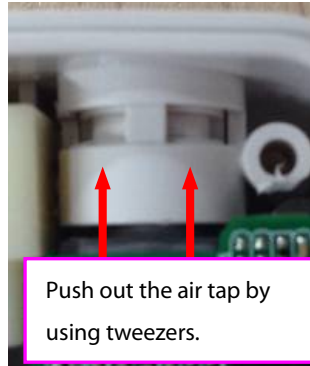
6. Remove the MPAN antenna connected to the parameter board. Be sure to remove the hot melt adhesive.



7. Remove the support for fixing the air tap and push out the air tap by using tweezers.

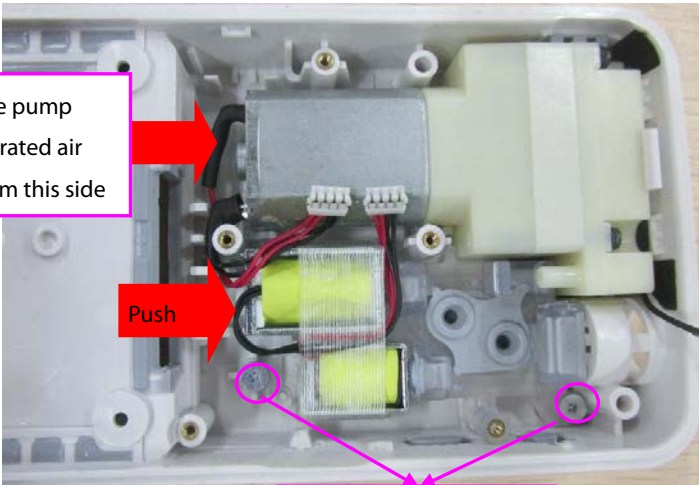


Remove the support for fixing



Push out the air tap by using tweezers.

8. Remove the two M1.6x3.5 cap head screws and pry up the integrated circuit and pump from the side close to the battery compartment.

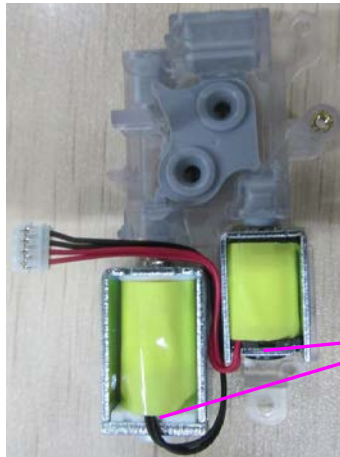


Pry up the pump and integrated air circuit from this side

Push

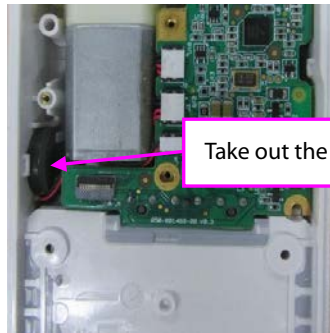
Two M1.6x3.5 screws

9. Separate the pump from the integrated gas circuit, remove the fiber tape, and take out the valve from the integrated gas circuit.



Remove the fiber tape and take out the valve from the integrated gas circuit

10. Take out the buzzer from the groove on the left of rear housing.



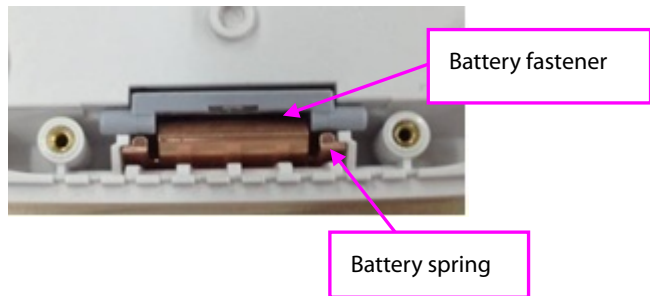
Take out the buzzer

11. Remove two M1.6x3.5 cap head screws and take down the fastening sheet metal of the battery spring.



Two M1.6x3.5 cap head screws

12. Take out the battery spring and battery fastener.



NOTE

- **The two bending parts of the battery spring face upward.**

FOR YOUR NOTES

9 Maintenance Materials

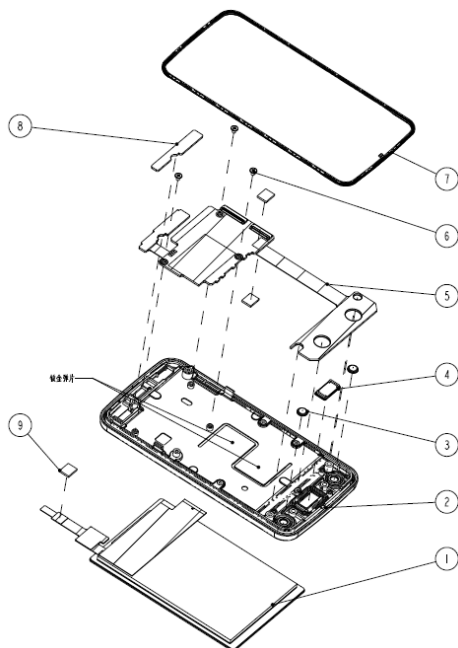
9.1 Overview of Maintenance Materials

As both the TM80 and the BP10 are structurally compact, it is difficult to replace some components of them separately. We provide maintenance materials for such components.

NOTE

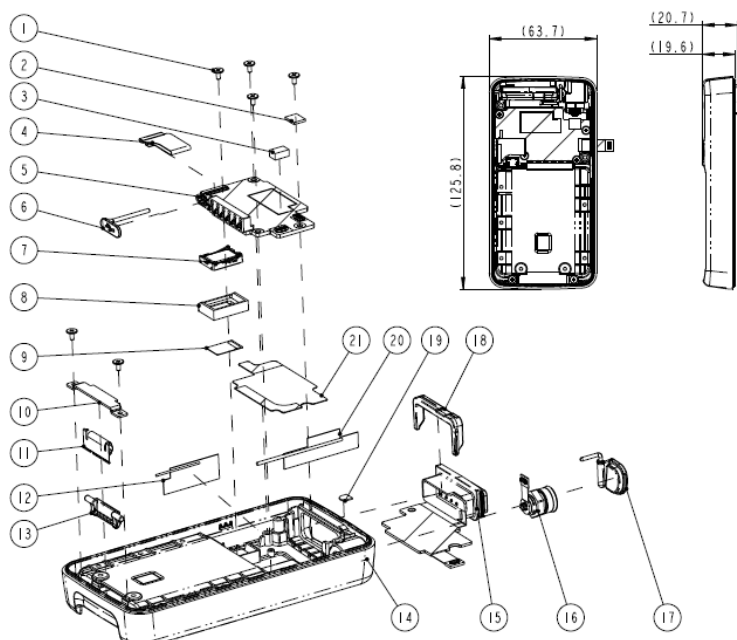
- **Mindray may improve the hardware of equipment so as to achieve better performance. After improvement, components incompatibility may occur. Therefore, before purchasing any component, you are suggested to contact engineers in Mindray to ensure that your desired components have correct part numbers. Mindray may update this service manual without prior notice. Please make sure that your manual is applicable to your devices.**
-

9.2 TM80 Front Housing Assembly (Wi-Fi)



No.	P/N	Description	Remarks
1	115-035605-00 (old plastic old LCD) 115-053698-00(ne w plastic new LCD)	TM80 front housing assembly maintenance kit	/
2			
3			
4			
5	051-003297-00	0156 main control board PCBA	/
6	115-032161-00	Telemetry maintenance kit	Contain parts that may be consumed during disassembly.
8			
9			

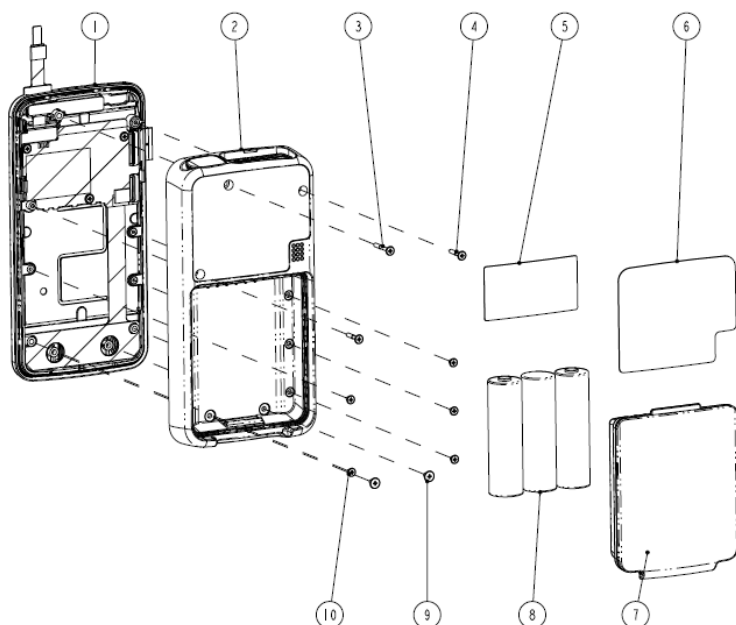
9.3 TM80 Rear Housing Assembly(Wi-Fi)



NO.	P/N	Description	Remarks
1	115-032161-00	Telemetry maintenance kit	Contain parts that may be consumed during disassembly.
2			
3			
19			
21			
4	050-001539-01	0156 FPCs for the main control board and parameter board	/
5	051-002059-01	ECG board PCBA (new telemetry Wi-Fi edition)	/
6	115-032160-00	Rear housing assembly	/
7			
8			
9			

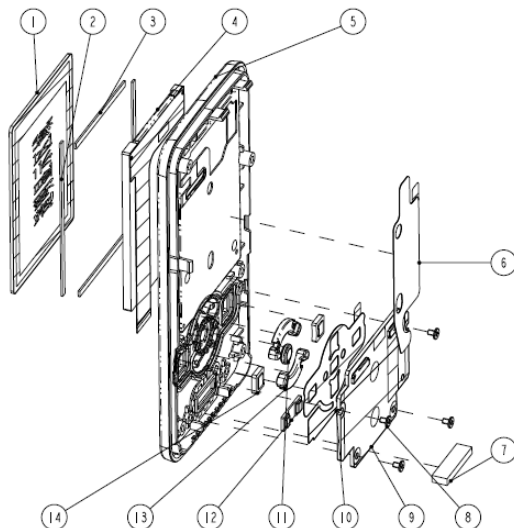
NO.	P/N	Description	Remarks
12			
14			
17			
20			
10	115-032156-00	Battery fastener material package	/
11			
13			
15	115-032159-00	ECG panel assembly	/
18			
7	115-032158-00	Speaker component	/
8			
9			
16	051-001709-00	New telemetry SpO2 interface board PCBA	/

9.4 TM80 Main Unit (Wi-Fi)



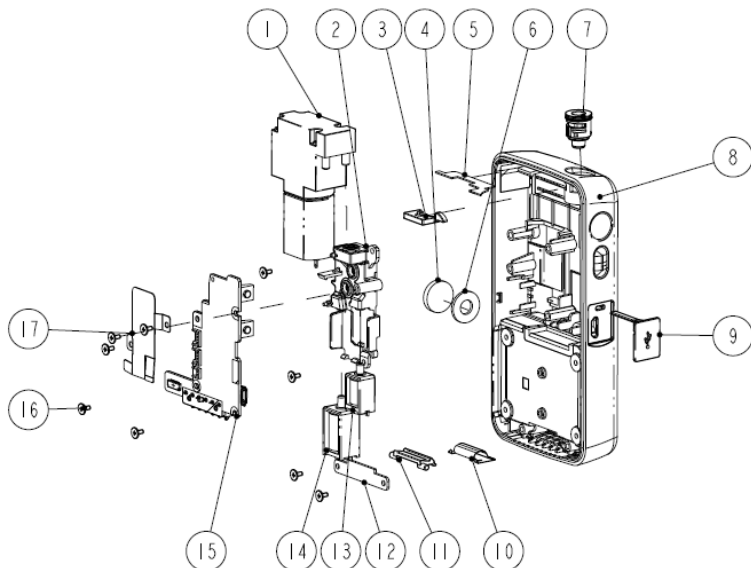
NO.	P/N	Description	Remarks
1	/	TM80 front housing assembly (Wi-Fi)	/
2	/	TM80 rear housing assembly (Wi-Fi)	/
3	115-032161-00	Telemetry maintenance kit	/
4			
5			
9			
10			
6	/	0156 Main Unit Label (FDA)	/
7	045-001699-01	TP-three AA battery tray assembly	/
8	0146-00-0077-01	Dry battery Alkaline 1.5 VAA(Size 5)	/

9.5 BP10 Front Housing Assembly



NO.	P/N	Description	Remarks
1	115-035519-00	BP10front housing assembly(FRU)	/
2			
3			
4			
5			
6			
7			
11	115-035518-00	BP10 main control board (FRU)	/
12			
13			
14			
8	/	Self-made cross recessed cap head screws M1.6x3.4 mm	/
9	115-035518-00	BP10 main control board (FRU)	/
10			

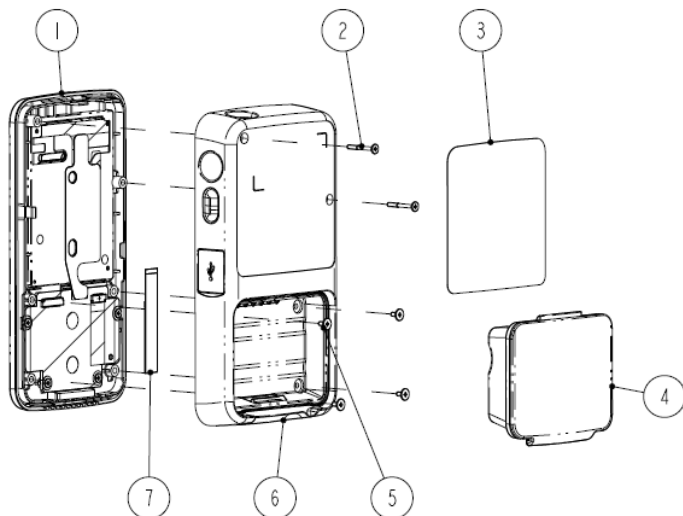
9.6 BP10 Rear Housing Assembly



NO.	P/N	Description	Remarks
3	115-035520-00	BP10 rear housing assembly (FRU)	/
5			
7			
8			
9			
10			
11			
12			
1	082-002009-00	Air pump DC 4.2 V 300 mmHg	/
2	115-035522-00	BP10 integrated gas circuit and valve assembly (FRU)	/
13			/
14			/
4	115-035521-00	BP10 maintenance kit (FRU)	/
3			/
6			/

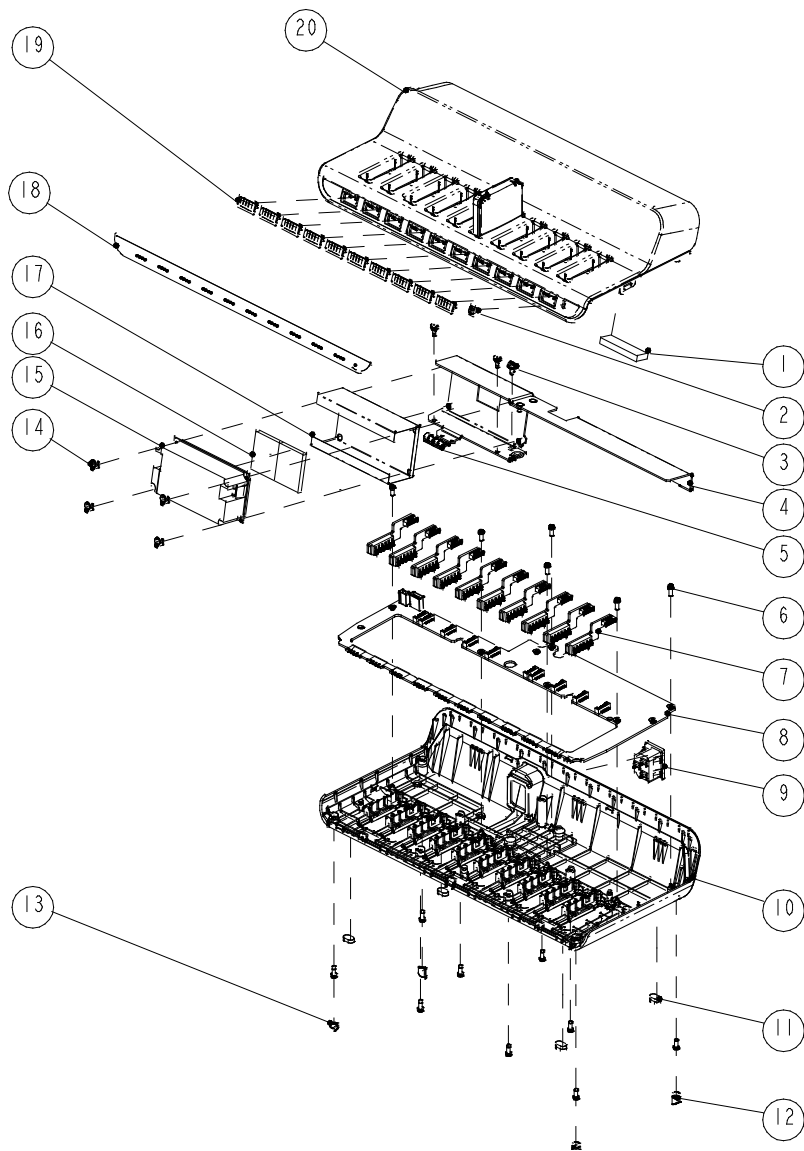
NO.	P/N	Description	Remarks
7			
16			
15	051-001707-00	NIBP POD parameter board PCBA	/
17	/	BP-POD pump support sheet metal	/

9.7 BP10 Main Unit



NO.	P/N	Description	Remarks
1	/	NIBP-POD front housing assembly	/
6	/	NIBP-POD rear housing assembly	/
2	115-035521-00	BP10 maintenance kit (FRU)	/
5			
7			
3	/	0156 main unit label (FDA)	/
4	045-001700-00	BP-two AA battery tray assembly	/

9.8 Exploded View of Central Charger



NO.	P/N	Description
1	/	Gasket of top housing
2	/	AC light pipe
3	/	Pan head screw M4X8
4	/	Charger-main-support
5	/	Spring, EMI
6	/	ST3.3X8 screw
7	/	Charger Connector Board PCBA
8	/	Charger Charge main Board PCBA
9	/	AC power socket & connecting cable
10	/	Charger bottom housing(SY)
11	/	FOOT-VS
12	/	Screw hole cover 1
13	/	Screw hole cover 2
14	/	Screw, Pan Head W/Washer Phillips M3X6
15	/	POWER SUPPLY BOARD 15V 63W
16	/	Thermal Pad
17	/	AC-DC insulating trip
18	/	Indicator label
19	/	Light pipe of central charger
20	/	Charger top housing
21	/	The host label(FDA)
22	/	Main board wire
23	/	Battery interface board wires

A Electrical Safety Inspection

A.1 Electrical Safety Tests for the TM80, BP10, and Central charger

The following electrical safety tests are recommended as part of a comprehensive preventive maintenance program. They are a proven means of detecting abnormalities that, if undetected, could prove dangerous to either the patient or the operator. Additional tests may be required according to local regulations.

All tests can be performed using commercially available safety analyzer test equipment. These procedures assume the use of a 601PROXL International Safety Analyzer or equivalent safety analyzer. Other popular testers complying with IEC 60601-1 used in Europe such as Fluke, Metron, or Gerb may require modifications to the procedure. Follow the instructions of the analyzer manufacturer.

The consistent use of a safety analyzer as a routine step in closing a repair or upgrade is emphasized as a mandatory step if an approved agency status is to be maintained. The safety analyzer also proves to be an excellent troubleshooting tool to detect abnormalities of line voltage and grounding, as well as total current loads.

A.2 Power Cord Plug

Test Item		Acceptance Criteria
The power plug	The power plug pins	No broken or bent pin. No discolored pins.
	The plug body	No physical damage to the plug body.
	The strain relief	No physical damage to the strain relief. No plug warmth for device in use.
	The power plug	No loose connections.
The power cord		No physical damage to the cord. No deterioration to the cord.
		For devices with detachable power cords, inspect the connection at the device.
		For devices with non-detachable power cords, inspect the strain relief at the device.

A.3 Device Enclosure and Accessories

A.3.1 Visual Inspection

Test Item	Acceptance Criteria
The enclosure and accessories	No physical damage to the enclosure and accessories.
	No physical damage to meters, switches, connectors, etc.
	No residue of fluid spillage (e.g., water, coffee, chemicals, etc.).
	No loose or missing parts (e.g., knobs, dials, terminals, etc.).

A.3.2 Contextual Inspection

Test Item	Acceptance Criteria
The enclosure and accessories	No unusual noises (e.g., a rattle inside the case).
	No unusual smells (e.g., burning or smoky smells, particularly from ventilation holes).
	No taped notes that may suggest device deficiencies or operator concerns.

A.4 Device Labeling

Check the labels provided by the manufacturer or the healthcare facility are present and legible.

- Main unit label
- Integrated warning labels

A.5 Earth Leakage Test

Run an Earth Leakage test on the device being tested before performing any other leakage tests.

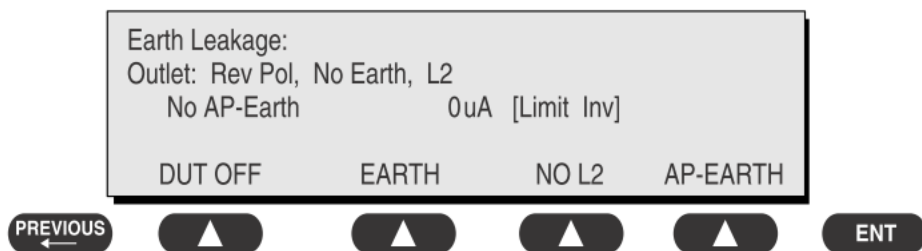
Leakage current is measured the following ways:

- Earth Leakage Current, leakage current measured through DUT outlet Earth
- Earth Leakage Current AP-EARTH (ALL Applied Parts connected to Earth), leakage current measured through DUT outlet Earth

There is no need to attach a test lead; the 601PRO automatically connects the measuring device internally.

To Perform the Test

1. From the MAIN MENU, or with the outlet unpowered, plug the DUT into the 601PRO front panel outlet, and turn on the device.
2. Attach the device's applied parts to the 601PRO applied part terminals if applicable.
3. Press shortcut key 4. The Earth Leakage test appears on the display, and the test begins immediately:



- SOFT KEY 1 toggles the DUT outlet Polarity from Normal to Off to Reverse.
 - SOFT KEY 2 toggles the DUT outlet from Earth to No Earth.
 - SOFT KEY 3 toggles the DUT outlet from L2 to No L2.
 - SOFT KEY 4 toggles the AP to Earth to No AP to Earth.
4. Press the print data key at any time to generate a printout of the latest measurement.

In Case of Failure

- Check any broken of the enclosure. Replace any defective part.
- Inspect wiring for bad crimps, poor connections, or damage.
- Test the wall outlet; verify it is grounded and is free of other wiring abnormalities. Notify the user or owner to correct any deviations. As a work around, check the other outlets to see if they could be used instead.
- Change another probe to confirm if the fail is caused by console.
- If the leakage current measurement tests fail on a new unit and if situation can not be corrected, submit a Safety Failure Report to document the system problem. Remove unit from operation.
- If all else fails, stop using and inform the Customer Service Engineer for analysis and disposal.

LIMITS

For UL60601-1,

- ◆ 300 μ A in Normal Condition
- ◆ 1000 μ A in Single Fault Condition

For IEC60601-1,

- ◆ 500 μ A in Normal Condition
- ◆ 1000 μ A in Single Fault Condition

A.6 Patient Leakage Current

Patient leakage currents are measured between a selected applied part and mains earth. All measurements have a true RMS only response.

Preparation

Perform a calibration from the Mains on Applied Part menu.

The following outlet conditions apply when performing this test:

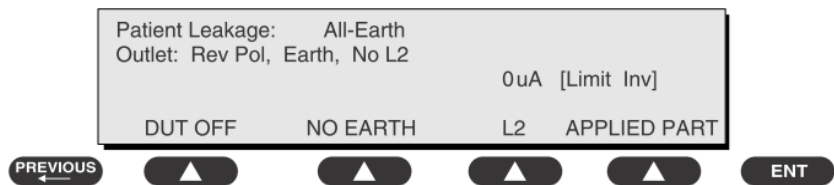
- Normal Polarity, Earth Open, Outlet ON Normal Polarity, Outlet ON
- Normal Polarity, L2 Open, Outlet ON Reversed Polarity, Outlet ON
- Reversed Polarity, Earth Open, Outlet ON Reversed Polarity, L2 Open, Outlet ON

WARNING

- **If all of the applied parts correspond to the instrument type, the applied parts will be tied together and one reading will be taken. If any of the applied parts differ from the instrument type, all applied parts will be tested individually, based on the type of applied part. This applies to Auto and Step modes only.**
-

To Perform the Test

1. From the MAIN MENU, or with the outlet unpowered, plug the DUT into the 601PRO front panel outlet, and turn on the device.
2. Attach the applied parts to the 601PRO's applied part terminals.
3. Press shortcut key 6. The Patient Leakage test is displayed, and the test begins immediately.



4. Press APPLIED PART (SOFT KEY 4) at any time to select the desired applied part leakage current.
5. Modify the configuration of the front panel outlet by pressing the appropriate SOFT KEY on the 601PRO.
6. Press the print data key at any time to generate a printout of the latest measurement.

In Case of Failure

- Check any broken of the enclosure. Replace any defective part.
- Inspect wiring for bad crimps, poor connections, or damage.
- Test the wall outlet; verify it is grounded and is free of other wiring abnormalities. Notify the user or owner to correct any deviations. As a work around, check the other outlets to see if they could be used instead.
- Change another probe to confirm if the fail is caused by console.
- If the leakage current measurement tests fail on a new unit and if situation can not be corrected, submit a Safety Failure Report to document the system problem. Remove unit from operation.
- If all else fails, stop using and inform the Customer Service Engineer for analysis and disposal.

LIMITS

For CF  applied parts

- 10 μ A in Normal Condition
- 50 μ A in Single Fault Condition

For BF  applied parts

- 100 μ A in Normal Condition
- 500 μ A in Single Fault Condition

A.7 Mains on Applied Part Leakage

The Mains on Applied Part test applies a test voltage, which is 110% of the mains voltage, through a limiting resistance, to selected applied part terminals. Current measurements are then taken between the selected applied part and earth.

Measurements are taken with the test voltage (110% of mains) to applied parts in the normal and reverse polarity conditions as indicated on the display.

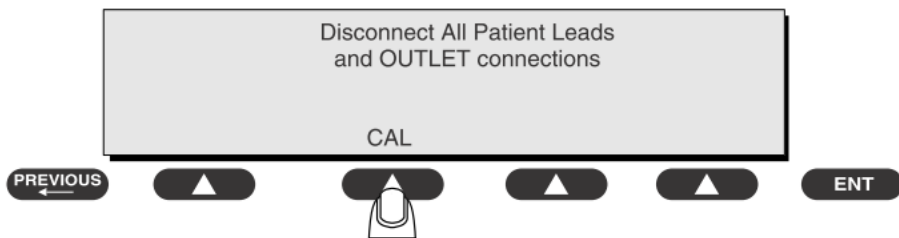
The following outlet conditions apply when performing the Mains on Applied Part test.

- Normal Polarity;
- Reversed Polarity

Preparation

To perform a calibration from the Mains on Applied Part test, press CAL (SOFT KEY 2).

1. Disconnect ALL patient leads, test leads, and DUT outlet connections.
2. Press CAL to begin calibration, as shown:



If the calibration fails, the previously stored readings will be used until a passing calibration has occurred. Also, the esc/stop key has no effect during calibration.

3. When the calibration is finished, the Mains on Applied Part test will reappear.

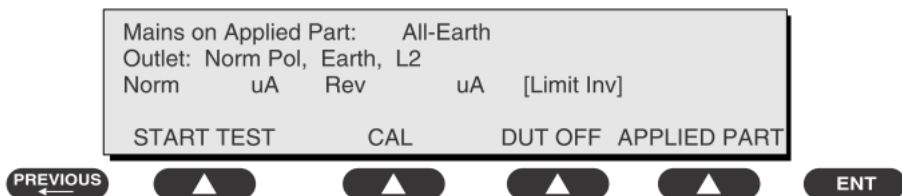


WARNING

- **A 2-beep-per-second signal indicates high voltage present at the applied part terminals while a calibration is being performed.**
 - **High voltage is present at applied part terminals while measurements are being taken.**
-

To Perform the Test

1. From the MAIN MENU, or with the outlet unpowered, plug the DUT into the 601
2. Attach the applied parts to the 601PRO applied part terminals.
3. Attach the red terminal lead to a conductive part on the DUT enclosure.
4. Press shortcut key 7. The Mains on Applied Part test is displayed.



5. Select the desired outlet configuration and applied part to test using the appropriate SOFT KEYS:
6. Press START TEST (SOFT KEY 1) to begin the test.
7. Press the print data key to generate a printout of the latest measurement.

NOTE

- **If all of the applied parts correspond to the instrument type, the applied parts will be tied together and one reading will be taken. If any of the applied parts differ from the instrument type, all applied parts will be tested individually, based on the type of applied part. This applies to Auto and Step modes only.**
-

In Case of Failure

- Check any broken of the enclosure. Replace any defective part.
- Inspect wiring for bad crimps, poor connections, or damage.
- Test the wall outlet; verify it is grounded and is free of other wiring abnormalities. Notify the user or owner to correct any deviations. As a work around, check the other outlets to see if they could be used instead.
- Change another probe to confirm if the fail is caused by console.
- If the leakage current measurement tests fail on a new unit and if situation can not be corrected, submit a Safety Failure Report to document the system problem. Remove unit from operation.
- If all else fails, stop using and inform the Customer Service Engineer for analysis and disposal.

LIMITS

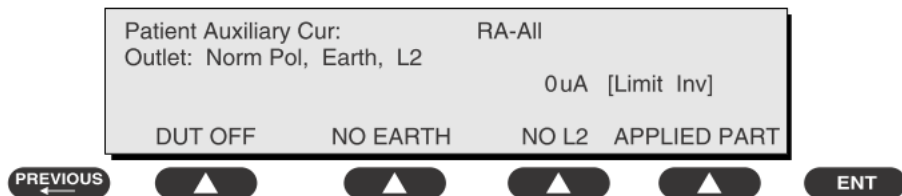
- For CF  applied parts: 50µA
- For BF  applied parts: 5000 µA

A.8 Patient Auxiliary Current

Patient Auxiliary currents are measured between any selected ECG jack and the remaining selected ECG jacks. All measurements may have a true RMSonly response.

Preparation

1. From the MAIN MENU, or with the outlet unpowered, plug the DUT into the 601PRO front panel outlet, and turn on the device.
2. Attach the patient leads to the 601PRO ECG jacks.
3. Define the Lead Types from the View Settings Option (refer to: Lead Type Definitions in Section 5 of this chapter).
4. Press shortcut key 8. The Patient Auxiliary Current test is displayed, and the test begins immediately. Display values are continuously updated until another test is selected.



5. Press SOFT KEYS 1-4 to select leakage tests
6. Press APPLIED PART (SOFT KEY 4) at any time to select the desired applied part leakage current:
7. Modify the configuration of the front panel outlet by pressing the appropriate SOFT KEY on the 601PRO:
8. Press the print data key at any time to generate a printout of the latest measurement.

In Case of Failure

- Check any broken of the enclosure. Replace any defective part.
- Inspect wiring for bad crimps, poor connections, or damage.
- Test the wall outlet; verify it is grounded and is free of other wiring abnormalities. Notify the user or owner to correct any deviations. As a work around, check the other outlets to see if they could be used instead.
- Change another probe to confirm if the fail is caused by console.
- If the leakage current measurement tests fail on a new unit and if situation can not be corrected, submit a Safety Failure Report to document the system problem. Remove unit from operation.
- If all else fails, stop using and inform the Customer Service Engineer for analysis and disposal.

LIMITS

For CF  applied parts,

- 10 μ A in Normal Condition
- 50 μ A in Single Fault Condition

For BF  applied parts,

- 100 μ A in Normal Condition
- 500 μ A in Single Fault Condition

A.9 Scheduled Electrical Safety Inspection

For scheduled electrical safety inspection, perform all the test items listed in **A.11 Electrical Safety Inspection Form**.

A.10 Electrical Safety Inspection after Repair

The following table specifies test items to be performed after the equipment is repaired. Refer to **A.11 Electrical Safety Inspection Form** for the description of the test items.

For the TM80

Repair with main unit not disassembled		Test items: 1, 2,
Repair with main unit disassembled	When patient electrically-connected PCBA is repaired or replaced	Test items: 1.2.3.4.5

For the BP10

Repair with main unit not disassembled		Test items: 1, 2,
Repair with main unit disassembled	When patient electrically-connected PCBA is repaired or replaced	Test items: 1.2.

For the central charger

Repair with main unit not disassembled		Test items: 1, 2, 3
Repair with main unit disassembled	When power supply PCBA is repaired or replaced	Test items: 1, 2, 3, 4,

A.11 Electrical Safety Inspection Form

For the TM80

Inspection and Testing			Limit
1	Device Enclosure and Accessories		/
2	Device Labeling		/
3	Patient Leakage Current	Normal condition (NC)	Max:
		Single Fault condition (SFC)	CF applied part: NC:10μA, SFC: 50μA BF applied part: NC:100μA, SFC: 500μA
4	Mains on Applied Part Leakage		Max: CF applied part: 50μA BF applied part: 5000μA
5	Patient Auxiliary Current	Normal condition (NC)	Max:
		Single Fault condition (SFC)	CF applied part: NC:10μA, SFC: 50μA BF applied part: NC:100μA, SFC: 500μA

For the BP10

Inspection and Testing		Limit
1	Device Enclosure and Accessories	/
2	Device Labeling	/

For the central charger

Inspection and Testing			Limit
1	Power Cord Plug		/
2	Device Enclosure and Accessories		/
3	Device Labeling		/
4	Earth Leakage	Normal condition (NC)	Max:
		Single Fault condition (SFC)	NC: 300μA(refer to UL60601-1) SFC: 1000μA

