LAN-HELPER

IEEE802.11a/g conform
54Mbps wireless LAN Micro Access Point

FX-DS540-APDL-U

User's Manual

CONTEC CO.,LTD.

Check Your Package

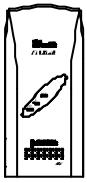
Thank you for purchasing the CONTEC product.

The product consists of the items listed below.

Check, with the following list, that your package is complete. If you discover damaged or missing items, contact your retailer.

Product Configuration List

- Main unit …1
- AC adapter(Cable length1.5m) …1
- Sheet metal for securing DC jack …1
- Cross cable(Cable length1.5m) …1
- Tapping screws …2
- Rubber feet …4
- External-toothed screw (Used for grounding via the ground terminal) …1
- Magnet (for mounting on metallic surfaces) …2
- Installation diagram (Used when the main unit is installed) …1
- This User's Manual (this booklet) …1



Main Unit

AC Adapter
(Cable length1.5m)

Sheet metal
for securing DC jack

Cross cable
(Cable length1.5m)

Tapping screws × 2

Rubber feet × 4

External-toothed screw
(Used for grounding via the ground terminal)

Magnet
(for mounting on metal surfaces) × 2

This User's Manual
(This booklet)

Installation diagram
(Used when the main unit is installed)

Copyright

Copyright 2003 CONTEC CO., LTD. ALL RIGHTS RESERVED

No part of this document may be copied or reproduced in any form by any means without prior written consent of CONTEC CO., LTD.

CONTEC CO., LTD. makes no commitment to update or keep current the information contained in this document. The information in this document is subject to change without notice.

All relevant issues have been considered in the preparation of this document. Should you notice an omission or any questionable item in this document, please feel free to notify CONTEC CO., LTD.

Regardless of the foregoing statement, CONTEC assumes no responsibility for any errors that may appear in this document or for results obtained by the user as a result of using this product.

Trademarks

FLEXLAN is a registered trademark or trademark of CONTEC CO., LTD.
MS, Microsoft, Windows, Windows NT, and MS-DOS are registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

Netscape Navigator is a registered trademark of Netscape Communications.

Other names of companies and products used in this document trademarks or registered trademarks of the related companies. This document does not use the symbols ™, ®, © etc.

Terminology/Abbreviations

⚠ CAUTION

In this manual, the FX-DS540-APDL-U is used in place of FX-DS540-APDL for convenience.

The following terms and abbreviations are used in this manual for convenience.

Full term	Term used in this manual
FX-DS540-APDL-U	FX-DS540-APDL
FX-DS540-APW-U	FX-DS540-APW
FX-DS540-PCD-U	FX-DS540-PCD
FX-DS540-APDL, FX-DS540-AP, FX-DS540-APP, FX-DS540-APW, FX-DS540-APL, FX-DS110-APE, FX-DS110-APL Each access point on the above	Access point / AP
A device with the wireless function	User unit / Wireless terminal
Personal computer	PC
User unit	UU

Table of Contents

Check Your Package i

Copyright ii

Trademarks ii
- Terminology/Abbreviations ii

Table of Contents iii

1. BEFORE USING THE PRODUCT 1

About the FX-DS540-APDL 1
- Features 1

Outline of the FLEXLAN-DS540 series 2
- Features of the FLEXLAN-DS540 series 2
- Introduction to the FLEXLAN DS540 Series 4

Customer Support 5
- Web Site 5

Limited One-Year Warranty 5

How to Obtain Service 5

Liability 5

Safety Precautions 6
- Safety Information 6
- Precautions for Use 6
- Precautions Related to Service 6
- Notes on Radio Interface 6
- Precautions Related to Electromagnetic Interference 7
- Handling Precautions 8
- Environment 9
- Inspection 9
- Storage 9

2. FUNCTIONS AND WIRELESS LINK MODE 11

Roaming Function 11

IP Tunneling Function (To be supported in the near future) 13

MAC Address Filtering 14

Bridge Packet Control 15

Wireless Link Mode Descriptions 16
- Standard Infrastructure Mode 16
- Compatible Infrastructure Mode 17
- Advanced Infrastructure Mode 18
- Wireless Link Mode and Communications 19
- Comparison of Main Functions 20

3. SETUP 23

Component Locations 23

Checking the Network Addresses 25

Setup 26
Wall Installation 26
Attaching Using a Magnet 27
Table Top Installation 28

Cable Installation 29
Network Cable Installation 29
Power Supply Connection 30
Ground the FX-DS540-APDL 31
Securing the DC jack 31

Installation in a Network 32
Features of the Wireless Network 32
Operating Environment and Radio Waves 33
Constructing a Network 34

4. SETUP PREPARATION 37

Setup Methods 37

Setup Using a Web Browser 38
Connecting to the Web Browser PC 39
Connecting to an FX-DS540-APDL 39

Setup Using TELNET 40
Connecting to an FX-DS540-APDL 40
TELNET Key Operation 42
Explanation of Top Menu and IP Settings 43

5. SETUP AND STATUS DISPLAY 45

Setup Item List 45

Settings 48
Basic setting 48
Ethernet 49
Wireless LAN 49
IEEE802.1X 55
Extensions 55
SNMP 56
Log function 58

Status display 59

6. MEINTENANCE 61

Maintenance Tool 61

Log File Collection 61
Using FTP to Get the Log File 61

Saving the Settings File 62
Using FTP to Backup the Settings File 62

Restoring the Software Settings 63
Using FTP to Restore the Settings 63

Upgrading the Firmware 64
Performin g an Upgrade Using FTP 64
Performing an Update Using a Web Browser 64

7. TROUBLESHOOTING 65

When Communication Fails 65
When You Cannot Perform Setup Using a Browser 66
When the AP Will Not Start 66

8. APPECDIX 67

Factory Default Settings List 67
Hardware Setup 67
Initial setup 67

Setup / Status Items list 71
WWW brouser 71
Terminal 72

Product Specifications 74
Physical Specifications 74
Software Specifications 75
Environmental Specifications for Installing the FX-DS540-APDL 75
External Dimensions 76

LEDs 77
During Normal Operation 77
Others 78

Input/Output Interface 78
Pin Assignment for UTP Port 78

Comparison to FLEXLAN DS110 series terminology 79

Glossary 80

1. Before Using the Product

This chapter provides information you should know before using the FX-DS540-APDL.

About the FX-DS540-APDL

The FX-DS540-APDL is a wireless LAN Access point. It conforms to the wireless LAN standard specification IEEE802.11a/IEEE802.11b/IEEE802.11g. The FX-DS540-APDL operates in the 5 or 2.4-GHz radio frequency band.

The FX-D540-APDL enables high-speed communication at up to 54 Mbps and is suitable for constructing 54 Mbs wireless LAN when used in combination with the Contec user unit [FX-DS540-PCD, FX-DS540-PCC, FX-DS540-PCC2] confirmed to IEEE802.11a or [FX-DS110-PCC, FX-DS110-PCC2] confirmed to IEEE802.11b.

While inheriting the proprietary functions highly evaluated mainly by corporate users, such as those for IP tunneling and roaming, the FX-D540-APDL supports data rates of up to 54 Mbps and the 64-, 128-, and 152-bit versions of WEP to provide higher security. It also supports WSL (proprietary encryption), IEEE802.1X (EAP-TLS), ESS ID concealing, and ANY ID rejection as well.

Be sure to read it carefully so that you can use the product correctly.

The FLEXLAN DS540 series employs a wireless LAN chip manufactured by Atheros Communications Inc. The main board, firmware, and enhancements are developed by CONTEC based on its abundant experience and technical skills in LAN.

Features

- It conforms to IEEE802.11a/b/g standard IEEE802.11a/IEEE802.11b/IEEE802.11g and you can select the wireless Lan standard for the various purpose of constructing a network. Capable of effectively using existing wireless network resources.
- Compact housing with internal antenna (for diversity), saving space for installation.
- A single unit of FX-DS540-APDL accepts log-in from up to 254 stations.
- Easy configuration and management using a WWW browser. Assorted maintenance methods are available to different systems and applications, including FTP commands, TELNET.
- IP tunneling feature integrated, enabling communication even at a roaming destination beyond the router without making any changes to network configuration.
- Various securities – MAC address filtering, IEEE802.1X, ESS ID concealing and ANY ID rejection as well as WEP(64, 128, 152bit) – integrated, enabling to provide the robust security.
- SNMP agent feature integrated, enabling network management using SNMP supported network management software (such as CONTEC SNMPc). MIBII and private MIB are supported.
- The FX-DS540-APDL can be powered via a network cable when using the power supply unit POW-CB20 or POW-CBM4.

Outline of the FLEXLAN-DS540 series

The FLEXLAN DS540 series is a wireless LAN devices adopting 5GHz band OFDM, which has the following features.

Features of the FLEXLAN-DS540 series

It conforms to IEEE802.11a/b/g standard(Lisence is not needed).
The FLEXLAN DS540 series corresponds to the wireless LAN standard IEEE802.11 a/b/g and you can select the wireless Lan standard for the various purpose of constructing a network.

IEEE802.11a can coustruct the 5 GHz band wireless network with high-speed and less radio interference. The 5 GH band wireless LAN provides a clearer radio communications environment than the 2.4 GHz band wireless LAN.

IEEE802.11g allows you to construct a 2.4-GHz band wireless network compatible with IEEE802.11b remaining popular so far. The network conforming to this standard can utilize resources of existing IEEE802.11b compliant products, accepting smooth migration from an IEEE802.11b wireless LAN.

The FLEXLAN DS540 series is classified as “radio equipment for a radio station in a low-power data communications system” defined in the Wireless Telegraphy Act, requiring no radio transmission license

Connection-able access point

Series	Type	Description
DS540 Series	FX-DS540-APW	Access point which conforms to IEEE802.11a/b/g and corresponds to Dual band.
	FX-DS540-APDL	Microsoft access point which conforms to IEEE802.11a/b/g and corresponds to Dual band.
	FX-DS540-AP	Access point which conforms to IEEE802.11a.
	FX-DS540-APP	Access point which confirms to IEEE802.11a
	FX-DS540-APL	Microsoft access point which confirms to IEEE802.11a
DS110 Series	FX-DS110-APE	Access point which confirms to IEEE802.11b.
	FX-DS110-APL	Microsoft access point which confirms to IEEE802.11b.

Data transfer rate of 54 Mbps
IEEE802.11a/IEEE802.11g switches its data rate automatically to 54, 48, 36, 24, 18, 12, 9, or 6 Mbps depending on the radio conditions.

Robust security provided
The FLEXLAN DS540 series supports the 64-, 128, and 152-bit types of WEP(RC4). Using WEP in combination with WSL (Wireless Security Link with a proprietary cryptography) provides more robust security. WEP can be used single-handedly, too. The FLEXLAN DS540 series will also support IEEE802.1X(EAP-TLS) specifying the latest protocol for security.

Capable of interconnection with a Wi-Fi compliant wireless LAN device
The FLEXLAN DS540 series can communicate, using basic features, with a Wi-Fi compliant device such as a non-FLEXLAN wireless LAN card, wireless LAN integrated notebook PC. With this feature, you can get the most out of wireless LAN resources.

Note! This feature does not guarantee the connection of the FX-DS540-PCD to all of Wi-Fi compliant devices. Enhancements such as IP tunneling can be used with a product other than the FLEXLAN series.

Multi-channel support

Thirteen channels (channels 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161 and 165) for IEEE802.11a and eleven channels (channels from 1 to 11) for IEEE802.11b/IEEE802.11g can be used at the same time. Using different channels for wireless networks adjacent to each other prevents radio interference and improves the throughput of either network.

IP tunneling function

Even when a wireless terminal with a fixed IP address assigned moves to (roam) a segment different in IP beyond the router, you can continue communication without making changes to settings.

Station feature

Two wired LANs can be interconnected between an access point and a station.

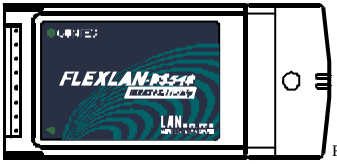
Introduction to the FLEXLAN DS540 Series

User unit (FX-DS540-PCD/PCC/PCC2)
The user unit corresponds to the LAN card for a wired LAN; it is plugged into a PC for use.
There is the user unit FX-DS540-PCC/PCC2 conformed to IEEE802.11a.

FX-DS540-PCC /
FX-DS540-PCC2

Figure 1.1. User unit

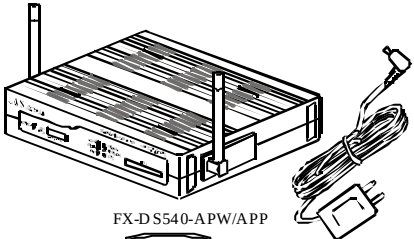
User unit (FX-DS540-PCD)
There is the user user unit FX-DS540-PCD conformed to IEEE802.11a/b/g.



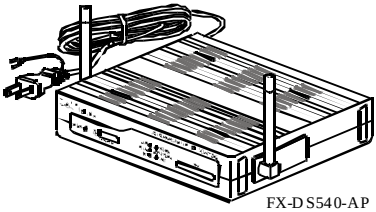
FX-DS540-PCD

Figure 1.2. User unit

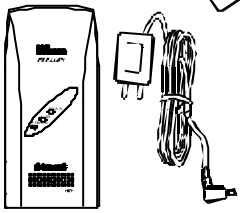
Access point (FX-DS540-APW/AP/APP/APDL/APL)
The access point is used to manage the wireless network, relay messages, and serve as the bridge to a wired LAN.



FX-DS540-APW/APP



FX-DS540-AP



FX-DS540-APDL/APL

Figure 1.3. Access point

Customer Support

CONTEC provides the following support services for you to use CONTEC products more efficiently and comfortably.

Web Site

Japanese	http://www.contec.co.jp/
English	http://www.contec.com/
Chinese	http://www.contec.com.cn/

Latest product information

CONTEC provides up-to-date information on products.
CONTEC also provides product manuals and various technical documents in the PDF.

Free download

You can download updated driver software and differential files as well as sample programs available in several languages.

Note! For product information

Contact your retailer if you have any technical question about a CONTEC product or need its price, delivery time, or estimate information.

Limited One-Year Warranty

CONTEC products are warranted by CONTEC CO., LTD. to be free from defects in material and workmanship for up to one year from the date of purchase by the original purchaser.

Repair will be free of charge only when this device is returned freight prepaid with a copy of the original invoice and a Return Merchandise Authorization to the distributor or the CONTEC group office, from which it was purchased.

This warranty is not applicable for scratches or normal wear, but only for the electronic circuitry and original products. The warranty is not applicable if the device has been tampered with or damaged through abuse, mistreatment, neglect, or unreasonable use, or if the original invoice is not included, in which case repairs will be considered beyond the warranty policy.

How to Obtain Service

For replacement or repair, return the device freight prepaid, with a copy of the original invoice. Please obtain a Return Merchandise Authorization Number (RMA) from the CONTEC group office where you purchased before returning any product.

* No product will be accepted by CONTEC group without the RMA number.

Liability

The obligation of the warrantor is solely to repair or replace the product. In no event will the warrantor be liable for any incidental or consequential damages due to such defect or consequences that arise from inexperienced usage, misuse, or malfunction of this device.

Safety Precautions

Understand the following definitions and precautions to use the product safely.

Safety Information

This document provides safety information using the following symbols to prevent accidents resulting in injury or death and the destruction of equipment and resources. Understand the meanings of these labels to operate the equipment safely.

⚠ DANGER	DANGER indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	WARNING indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	CAUTION indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury or in property damage.

Precautions for Use

This product is classified as "wireless equipment for stations of low-power data transmissions systems" under the Wireless Telegraphy Act, and does not require a radio transmission license. The law prohibits modification of the interior of this product.

Precautions Related to Service

Clean this product by wiping lightly with a soft cloth moistened with water or a cleaning solution.

Take care to avoid the use of benzene, thinners or other volatile solutions which may cause deformation or discoloration.

Notes on Radio Interface

The 2.4 GHz band used by this product covers the operating frequencies of mobile-identification local radio stations (requiring the license), specific low-power radio stations (requiring no license) and amateur wireless stations (requiring the license) as well as industrial, scinetific, and medical equipment such as microwave ovens.

1. Before using this product, make sure that there is no mobile-identification local radio station, specific low-power radio station and amateur wireless station operating near the product.
2. If the product should cause radio interface with any mobil-identification local radio station or specific low-power radio station, immediately change the operating frequency to avoid the radio interface.
3. Contact your local retailer or CONTEC if the product has trouble such as recurrent radio interface with mobile-identification local radio stations or specific low-power radio stations.

Precautions Related to Electromagnetic Interference

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions : (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with part 15 of the FCC rules. Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

Handling Precautions

⚠ DANGER

Do not use the product where it is exposed to flammable or corrosive gas. Doing so may result in an explosion, fire, electric shock, or failure.

⚠ CAUTION

- This product contains precision electronic elements and must not be used in locations subject to physical shock or strong vibration.
  Otherwise, the board may malfunction, overheat, or cause a failure.
- Do not use or store this device in high temperature or low temperature surroundings, or do not expose it to extreme temperature changes.
  Otherwise, the board may malfunction, overheat, or cause a failure.
- Do not use or store this device where it is exposed to direct sunlight or near stoves or other sources of heat. Otherwise, the board may malfunction, overheat, or cause a failure.
- Do not use or store this device near strong magnetic fields or devices emitting electromagnetic radiation. Otherwise, the board may malfunction, overheat, or cause a failure.
- If an unusual smell or overheat is noticed, unplug the power cable immediately.
- Be careful not to let the external supply voltage or drive current exceed the rating.
- Do no place an object that blocks ventilation slits on top of this product or on its sides.
- The specifications of this product are subject to change without notice for enhancement and quality improvement.
  Even when using the product continuously, be sure to read the manual and understand the contents.
- Do not attempt to modify this device. The manufacturer will bear no responsibility whatsoever for the device if it has been modified.
- Regardless of the foregoing statements, CONTEC is not liable for any damages whatsoever (including damages for loss of business profits) arising out of the use or inability to use this CONTEC product or the information contained herein.

Environment

Use this product in the following environment. If used in an unauthorized environment, the board may overheat, malfunction, or cause a failure.

Operating temperature

0 to 50ºC

Humidity

10 to 90%RH (No condensation)

Corrosive gases

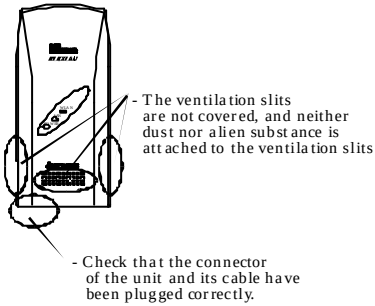
None

Floating dust particles

Not to be excessive

Inspection

Inspect the product periodically as follows to use it safely.



Storage

When storing this product, keep it in its original packing form.

(1) Wrap it in the packing material, then put it in the box.

(2) Store the package at room temperature at a place free from direct sunlight, moisture, shock, vibration, magnetism, and static electricity.

2. Functions and Wireless Link Mode

This chapter describes the major functions of the FLEXLAN DS540 series as a wireless LAN system and the wireless link modes of the FX-D540-APDL along with configuration examples of networks available in the wireless link modes.

Roaming Function

The roaming function maintains the connection to the LAN by automatically changing the access point to which the user unit is connected when the unit moves. If access points are positioned so as to cover the entire area where the wireless LAN is to be available, the user unit can be used from anywhere.

When the wireless link mode of a FLEXLAN-DS540 user unit is "Standard Infrastructure" or "Compatible Infrastructure", it is designed to continuously monitor the AP (access point) signal strength and change to the AP that provides the most reliable communications.

In the following example, the signals from the APs do not cover the entire range in which the mobile station UU1 moves and therefore the connection to the wired LAN is lost when UU1 is in position (2).

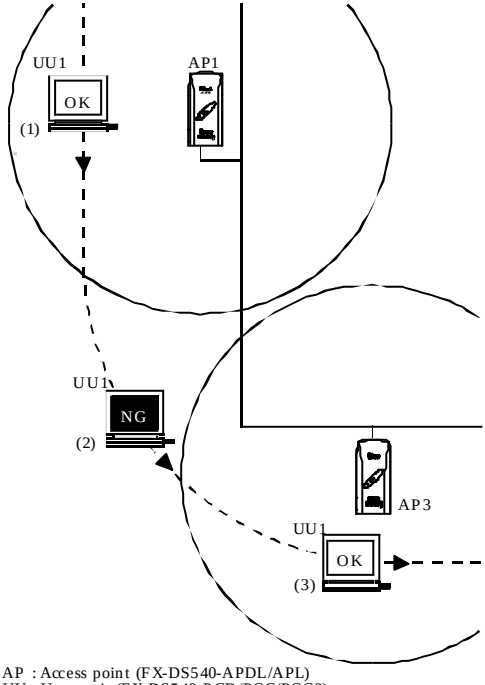


Figure 2.1. Roaming Function 1

With the addition of an extra AP, however, the mobile station can now continue communications seamlessly.

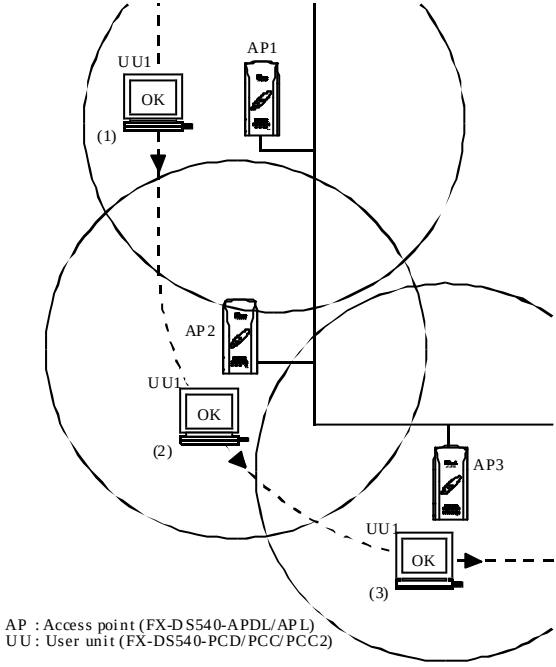


Figure 2.2. Roaming Function 2

IP Tunneling Function (To be supported in the near future)

In TCP/IP, packets belonging to different network groups cannot normally be used. However, a technique called tunneling or IP tunnel technology can be used to temporarily modify packets belonging to different network groups so that they can be used. This technique can enable user units to communicate with the wired LAN as usual even when connected via an AP from a different network group.

The following example shows how user unit UU1, which belongs to network group A, can connect via a router to terminal PC1, also in network group A, despite UU1 being connected to the LAN via AP2 which belongs to network group B.

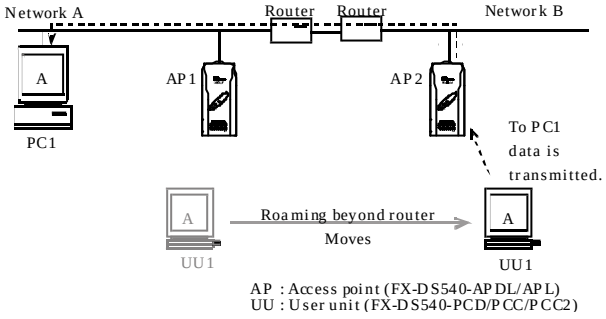


Figure 2.3. IP Tunneling Function

MAC Address Filtering

MAC address filtering is the function to permit only the user units whose MAC address has been registered for an AP to log in to the AP. Using this function can reject an attempt to log in to an AP by an unidentified user unit not registered in the AP.

Figure 2.4 shows a sample image of connections under control of MAC address filtering. The example assumes that the MAC addresses of UU1 and UU2 are registered in the MAC address filtering list for the AP while UU3's MAC address is not registered in the list. In this case, UU1 and UU2 can log in to the AP but UU3 cannot. To permit UU3 to log in to the AP, the AP 's administrator has to add the UU3's MAC address to the MAC address filtering list for that AP.

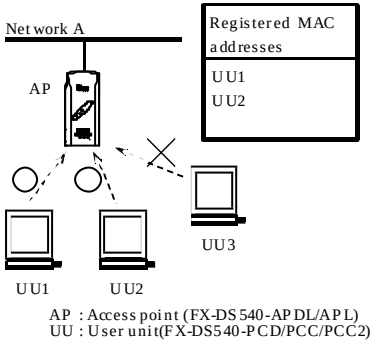


Figure 2.4. MAC address filtering

Bridge Packet Control

Bridge packet control is the function that allows an AP to pass only data from those network devices whose MAC address has been registered for the AP to its clients. Using this function can restrict communication between user units.

Figure 2.5 shows a sample image of connecting under bridge packet control. The example assumes that, for bridge packet control, only the MAC address of the router is registered in AP1 and AP2. In this case, UU1, UU2, and UU3 can exchange data with the external network through the router while they cannot communicate with one another. When the router is connected to the Internet, UU1, UU2, and UU3 can access the Internet while they cannot communicate directly with each other.

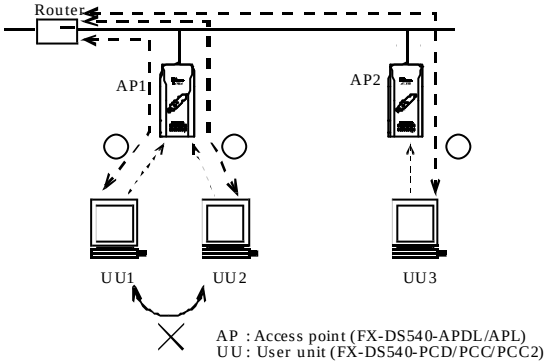


Figure 2.5. Bridge Packet Control (with MAC address registered)

If the bridge packet control list for the AP contains no entry with the bridge packet control function enabled, communication is unconditionally permitted between a wired unit and a wireless unit but rejected between wireless units.

When the bridge packet control list for AP1 and AP2 contains no entry in the above example, UU2 and UU3 can communicate with each other via AP1 and AP2 while UU1 and UU2 cannot.

Bridge packet control is suitable for a wireless LAN constructed in a public space.

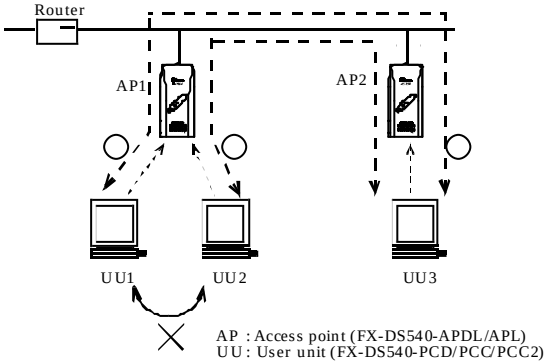


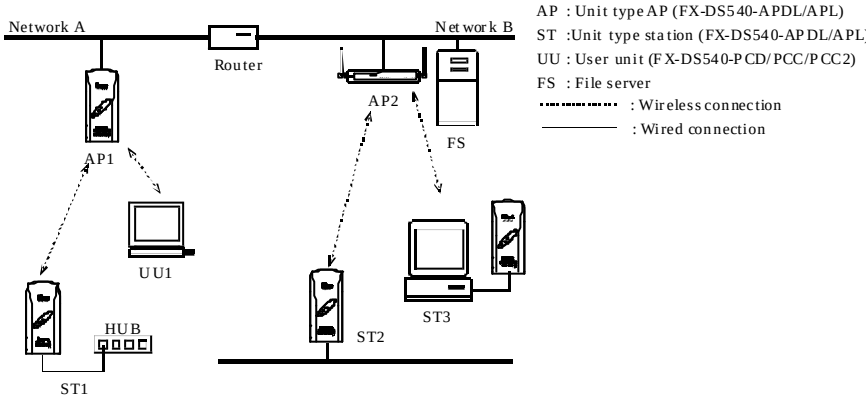
Figure 2.6. Bridge Packet Control (with MAC address not registered)

Wireless Link Mode Descriptions

The AP has three wireless link modes. The available functions and network configurations differ depending on the mode. Use the wireless link mode most suitable to the type of network you are constructing. The factory default setting is simple mode. Chapters 4 and 5 describe the software setting procedures for the wireless link modes and related items.

Standard Infrastructure Mode

In this mode, each access point (AP) can accommodate user units (stations) to make up a network. This mode allows the use of multiple AP's to configure wide-area wireless LAN's. All communication between wireless terminals must go through an AP.



Note : An AP operating as a station has the same status as a user unit, as an AP managed by (logged in with) an AP.

Figure 2.7. Standard Infrastructure Mode

In the above standard infrastructure mode, all wireless terminals communicate via unit type APs. Roaming functions are supported, allowing logged in on any unit type AP.

For IP tunneling to work correctly, one of the APs must be setup as the master AP (See "Setting Item List" in Chapter 5).

- Advantages
  - (1) Capable of accommodating APs as stations.
  - (2) If the IP tunneling function is used, communication can continue via different routers without needing to change IP address.
  - (3) Allows log-in restrictions on unit type AP's (security function).
  - (4) Capable of improving security based on WSL (Wireless Security Link)

Compatible Infrastructure Mode

This mode allows the FX-DS540-APW to be networked with other manufacturers' Wi-Fi certified wireless terminals other than the CONTEC's FLEXLAN series. Communications between the wireless terminals are always made via the APs.

⚠ CAUTION

The Compatible Infrastructure mode does not guarantee interconnection with Wi-Fi compliant products of other manufacturers.

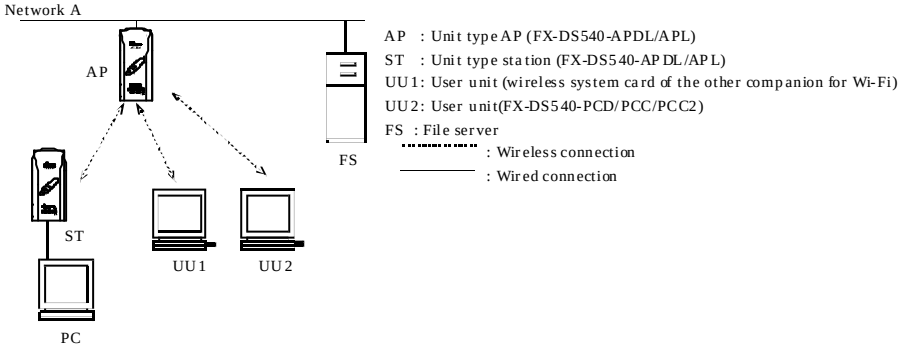


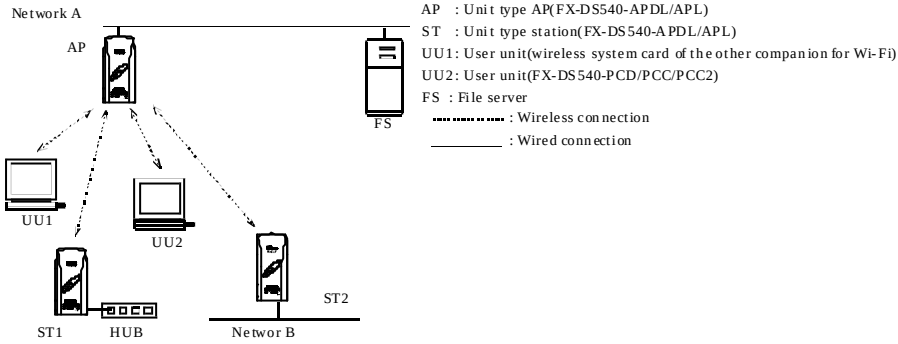
Figure 2.8. Compatible Infrastructure Mode

In the Compatible Infrastructure mode, each wireless terminal performs communication via the AP as in the Standard Infrastructure mode. As the roaming function is supported, the wireless terminal can log in to any unit type AP within the coverage.

The unit type AP does not provide FX-DS540-APDL's unique features as it works as a simple bridge.

Advanced Infrastructure Mode

The Advanced Infrastructure mode is a mixture of the Standard Infrastructure and Compatible Infrastructure modes.



Note: An AP operating as a station has the same status as a user unit, as an AP managed by (logged in with) an AP.

Figure 2.9. Advanced Infrastructure Mode

The terminal set to the Standard Infrastructure mode can use the FX-DS540-APDL's unique features.

The terminal set to the Compatible Infrastructure mode serves as a simple bridge and thus cannot use the FX-DS540-APDL's unique features.

Wireless Link Mode and Communications

The table below shows which wireless terminals can communicate with each other depending on the operating mode of the AP and user unit.

[Table notation and notes]

1. UU stands for "user unit".
2. AP⇔UU indicates communications between a unit type AP and user unit.
3. ST indicates an "AP managed by (logged in to) another AP" which operates in the same way as a user unit. See Chapter 5 for details of the setup procedure.

Table 2.1. Wireless Link Mode and Communications

AP Wireless Link Mode	Terminal able to communicate	
	AP⇔UU	AP⇔ST
Standard Infrastructure	O	O
Compatible Infrastructure	O	×
Advanced Infrastructure	O	O

Comparison of Main Functions

The FX-DS540-APDL has three wireless link modes. The available functions are different for each mode. The following shows a table of the relationship between the operating modes and main functions and gives a brief explanation of each function.

Table 2.2. Comparison of Main Functions

Setting item	Standard Infrastructure mode	Compatible Infrastructure mode	Advanced Infrastructure mode
Roaming	O	O	O
IP Tunneling	O	O *2	O *1
Station AP connection	O	×	O
SNMP	O	O	O
Log collection function	O	O	O
MAC address Filtering	O	O	O
Bridge Packet Control	O	O	O
Data encryption (WSL)	O	×	O *1
Data encryption (WEP)	O	O	O
IEEE802.1x(EAP-TLS)	O	O	O

*1 Not available between the devices in Compatible Infrastructure mode

*2 When compatible infrastructure mode, PC which is capable of connecting to the station AP is 1 unit.

Roaming

The roaming function which allows mobile user units to switch log-in between multiple APs can only be used. Roaming can be used to construct large scale wireless LANs.

IP tunneling

This function modifies the IP address so that units can connect to the desired network group even via. It can be used in the Advanced Infrastructure and Standard Infrastructure modes.

Station AP connection

A station (unit type ST) indicates an AP managed (logged in) by another AP; it is used to serve as a bridge.

SNMP

This function enables remote management by software that supports SNMP. Available in all modes.

Log collection function

This function lists the wireless terminals logged in to the AP and collects times and other event information. See Chapter 6 for details.

MAC address filtering

This function enables connection of only the terminals whose MAC address has been registered.

Bridge Packet Control

This function allows the AP to pass only that data to terminals which comes from network devices having a registered MAC address. Communication between wireless terminals can be rejected when their MAC addresses are unregistered.

Data encryption

This function encrypts wireless data. For encryption, three security protocols are available: WSL (Wireless Security Link: proprietary cryptography), WEP (Wired Equivalent Privacy) and AES. WSL and WEP or WSL and AES can be used at the same time. Note, however, that devices using WSL and those not using it cannot communication with each other.

IEEE802.1X(EAP-TLS)

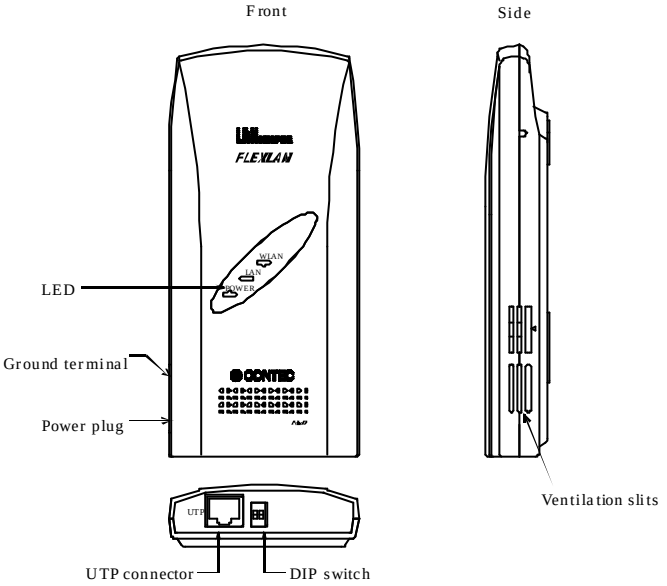
This function performs authentication using digital certificates. After authentication, the AP dynamically broadcasts the WEP key.

The function of IEEE802.1X cannot be used when the unit type of the AP is "station".

3. Setup

This chapter describes how to install the AP and points to note when installing.

Component Locations



Notes : Not cover the ventilation slits because of misoperation caused by overheating.

Figure 3.1. Component Locations

LED indicator

Three LEDs indicate the user unit connection, transmission/reception, power supply, and wired LAN connection status.

Table 3.1. LED Display during Normal Operation

Name	State	Indicator
POWER	On	Indicates that the device is operating.
	Flashing	Indicates that the device is being started (going to operate after the power switch was turned on).
LAN	On	Indicates that a wired LAN has been connected.
	Flashing	Indicates the sending / receiving state between the terminal and data connected by the wired LAN.
	Off	Indicates that a wired LAN has been unconnected.
WLAN	On	Indicates that a user unit has been logged in (With access point). Indicates that a user unit has not been logged in access point (With station).
	Off	Indicates that a user unit has not been logged in (With access point). Indicates that a user unit has not been logged in access point (With station).
	Flashing	Indicates that a user unit has not been logged in.

DIP switches

The DIP switches are used to initialize the AP and select the IP-less mode.

Table 3.2. DIP Switches

	ON	OFF	Indicator
1	INIT	-	Used to initialize the AP. Turning on this switch makes the LED of POWER, LAN, WLAN blink. Turning this DIP switch off before (about 3 seconds) staying illuminated from being blinking resets all the AP's settings to their factory defaults the next time the AP is started.
2	IP LESS	-	Turning this switch on, operating can be done without setting the IP address on the AP In this time, you cannot use the setup by WWW browser or SNMP agent function.

Connectors

Table 3.3. Connectors

Item	Operation / function
UTP 10/100M	Connects to a 10BASE-T or 100BASE-TX LAN.
Ground terminal	Grounds the AP via the ground terminal.
Power supply jack	3.3VDC power supply input jack. Supply the power with this connector when using the bundled AC adapter. - Power supply plug - Standard : EIAJ RC-5320A Voltage category 2 - Polarity : Outside terminal is negative (-) and center terminal is positive (+) - Plug diameter : 4.0mm (external diameter), 1.7mm (internal diameter)

⚠ CAUTION

Use either the AC power supply or DC power supply on the FX-DS540-APDL.
Using both power supplies at the same time may damage the AP.

Checking the Network Addresses

The Ethernet MAC address and IP address are defined on the housing seal (on the bottom)of this product. Note the addresses in the following list for later use.

Table 3.4. Network address

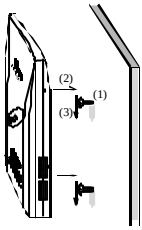
Housing seal description	Explanation	Keeping from column
I/A	Default IP Address	
E/A : C	Ethernet MAC Address	
E/A : W	Wireless MAC Address	

Setup

Wall Installation

In case of using the supported screw

Refer to the main unit installation drawing to drive the screws into a wall and hang the main unit on them.



(1) Drive the screws into the wall. The dimensions are shown in the figure above. (2 locations)
(2) Attach the AP case such that the two screws on the wall insert into the wall-mount holes on the case.
(3) Slide the AP unit down to hold it in place.

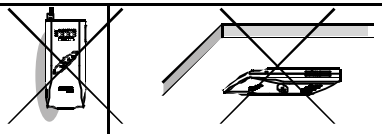
Figure 3.2. Wall Installation

⚠ CAUTION

Do not obstruct the ventilation slits. This can cause the temperature inside the product to rise and can damage the components inside.

⚠ WARNING

Do not install this product downward or on a ceiling.
It can be overheated inside to catch fire.



Attaching Using a Magnet

The magnet provided with the FX-DS540-APDL makes it easy to attach or remove the AP from metal surfaces such as steel partitions or desks.

⚠ CAUTION

- Do not place magnets near monitors, floppy disks, or other sensitive objects.
- Moving the AP while it is mounted on a steel desk or similar surface can cause paint scratching.

Attaching and removing magnets

To mount the unit using a magnet, push the magnet into the magnet mounting hole in the direction of arrow 1 as shown in Figure 3.3. , then insert the entire magnet into the mounting hole.

Next, slide the magnet in the direction of arrow 2 to hold the unit in place.

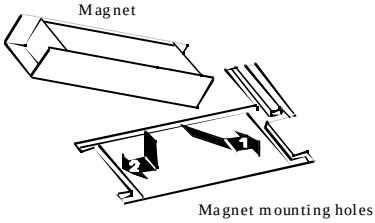


Figure 3.3. Attaching Magnets

To remove, slide the magnet in the direction of arrow 1 in Figure 3.4. , then lift in the direction of arrow 2.

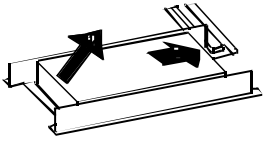


Figure 3.4. Removing Magnets

Mounting on steel desks

The unit can be mounted directly on steel desks. Pull lightly to make sure that the AP does not come off easily. Select a location that gives good radio reception.
The unit provides better receiver sensitivity with the internal antenna inside the top protruding above the steel surface.

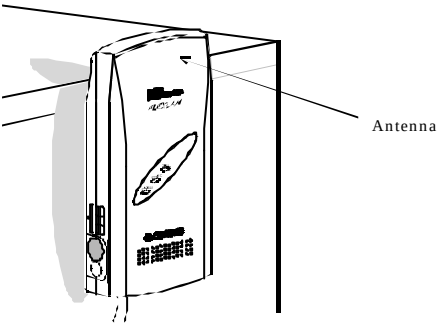


Figure 3.5. Mounting on Steel Desks

⚠ CAUTION

Do not obstruct the ventilation slits. This can cause the temperature inside the product to rise and can damage the components inside.

Table Top Installation

Set it by using the supported rubber feet.

If installing on a desktop, place the unit on a stable and flat base and ensure that adequate space is provided for ventilation (5cm). As far as possible, locate the unit in a high place with an unobstructed view as this gives better radio transmission and reception performance and increases the operating range.

⚠ CAUTION

Do not obstruct the ventilation slits. This can cause the temperature inside the product to rise and can damage the components inside.

Cable Installation

Network Cable Installation

Connect your network cable to the network connector on the AP. This model has a single 10/100BASE-TX connector.

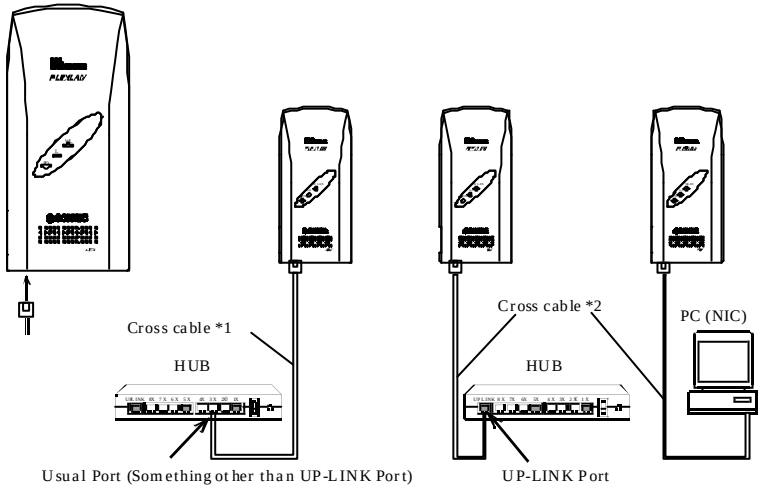
10BASE-T or 100BASE-TX connection

⚠ CAUTION

- When connecting this product to a personal computer or hub use a twisted pair cable no more than 100m in length.
- Use UTP cable or STP cable having category 3, 4, or 5 specifications.
- When connecting with a personal computer (NIC) or hub up-link port, use a UTP cross cable (TP-X).

(1) Connect the UTP cable (straight-through cable) to the UTP port in a hub or bridge.

(2) Connect the other end of the UTP cable to the UTP port on the FX-DS540-APDL.



*1 : Optional TP-03(3m), TP-05(5m), TP-10(10m), TP-20(20m), TP-50(50m), TP-100(100m) can be used.
*2 : Optional TP-X(Cross cable and attachment which are 30cm tall) can be used.
* Cable length between this product and PC or HUB is less than 100m.

Figure 3.6. 10BASE-T or 100BASE-TX Connection

Power Supply Connection

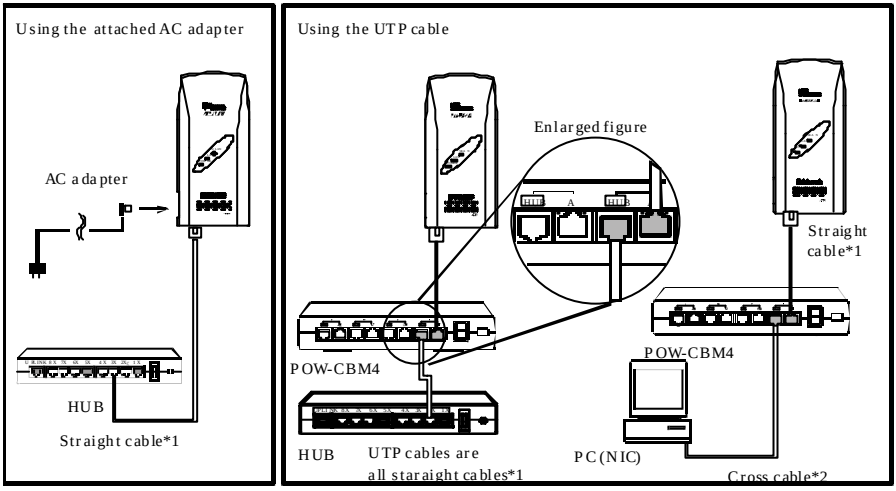
This product has two methods to supply the power.

Using the attached AC adapter

Plug the AC adapter into a wall outlet, then connect the DC jack to the power plug in the main unit.

Using the UTP cable (Optional POW-CB20, POW-CBM4 are necessary.)

As the FX-DS540-APW contains a power supply separator unit, it can be powered directly from the POW-CB20 or POW-CBM4. Power supply separator unit POW-SP20 is not used.
To supply power to the unit using a UTP cable, refer to the PW-CB20 or POW-CBM4's instruction manual to connect it correctly. And use UTP cable having category 5.



*1 : Optional TP-03(3m), TP-05(5m), TP-10(10m), TP-20(20m), TP-50(50m) can be used.
*2 : Optional TP-X (Cross cable and attachment which are 30cm) can be used.
*Cable length between this product and PC or HUB is less than 90m.

Figure 3.7. Power Supply Connection

⚠ CAUTION

- Do not connect any AC adapter other than the accessory. Doing so may result in a failure in the device or an accident. Note, in particular, that the AC adapters bundled with the FX-DS540-APP and FX-DS540-APW are different in voltage while being identical in shape.
- The power supply from the UTP cable is corresponding to the optional POW-CB20/POW-CBM4. You cannot use the power supply unit of another company. Doing so may result in a failure in the device or an accident.
- **Do not connect the AP-side UTP cable of the POW-CBM4 to a device such as a hub as doing so can cause a device fault or accident.**
- The power supply cannot be done by the power supply separator unit POW-SP20. Doing so may result in a failure in the device or an accident.

Ground the FX-DS540-APDL

Remove the rubber plug from the ground terminal on the main unit and connect a ground wire to the terminal using the bundled external-toothed screw.

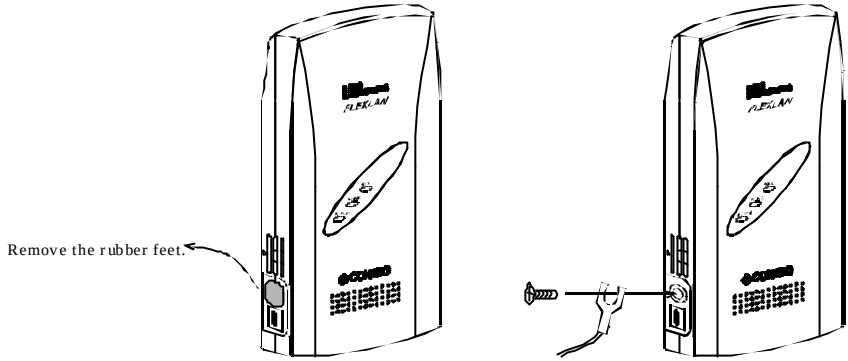


Figure 3.8. Ground the FX-D540-APDL

Securing the DC jack

Using the DC jack retaining bracket as a standard accessory stops the DC jack from being removed when the DC cable is loaded to be pulled, preventiing the power from being shut off abruptly.

Fix the metal fittings by using the bundled external-toothed screw and then fix the DC jack.

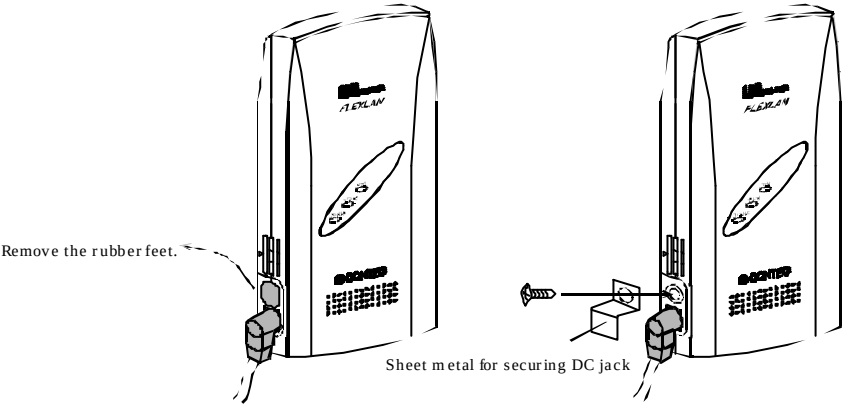


Figure 3.9. Securing the DC jack

Installation in a Network

This section describes how to install the FX-DS540-APDL to construct a network with improved performance and discusses the general features and radio characteristics of the wireless LAN as well as the guidelines for constructing the network.

Features of the Wireless Network

In general, the operation of a wireless network is the same as for most other types of LAN. The most prominent feature of the wireless network is that it uses radio waves as its medium, eliminating the need for cabling. The wireless network thus requires no cabling cost and has other advantages as listed below:

- Quick construction of a LAN
- Temporary installation of a LAN
- Higher flexibility in layout of connected PCs (terminals)
- Assured mobility of connected PCs (terminals)

On the other hand, the wireless network has the following drawbacks from the operational point of view due to the nature of radio waves:

- Signal attenuation
- Signal interference

Also, although this unit does not require a radio license, it is subject to radio regulations.

Operating Environment and Radio Waves

When using this product to construct a network, install and operate it considering the radio environment to optimize the performance.

Is allowed to use radio equipment at the installation location?

In some medical institutions and laboratories, radio-sensitive precision instruments are used and it may be prohibited to use radio equipment.

Radio waves are attenuated.

Although a radio wave is attenuated naturally as it travels from its transmission source, it may also be attenuated by an object existing in its way. Major obstacles that attenuate radio waves are as follows:

- Concrete wall
- Metal surfaces in the vicinity of the antenna

Obstacles blocking radio waves include metal walls and walls containing a metal firewall.

Strictly speaking, nearly all objects in the path of the radio waves (such as partitions or people) cause some attenuation but these do not have a significant impact on network performance.

RSSI (Receive Signal Strength Indication) utility is available as a means of knowing the signal strength of an incoming radio wave. Placing this product for a greater RSSI value makes the communication state more stable. If the RSSI value is small and slightly moving the position of the product does not increase the RSSI value, it indicates radio wave attenuation either to the distance or by an obstacle.

Pay attention to radio interference.

Radio interference means the reception of radio waves in the frequency band used by this network that are generated by equipment that is not part of the network to which this product belongs. Listed below are major examples of sources of interfering radio waves generated in general environments excluding plants and factories:

- 5GHz (using by IEEE802.11a) or 2.4GHz (using by IEEE802.11b/IEEE802.11g) band wireless networks that do not comply with IEEE802.11
- Using by IEEE802.11b/IEEE802.11g. Ex. microwave ovens, security gates (installed near the entrances of some department stores and rental shops), copiers which give off the 2.4GHz electric waves.

Where there is a large metal wall such as in a warehouse, the radio wave generated from the sender is reflected, resulting in those radio waves reaching the receiver which have taken different routes (thereby phase-shifted). This has the similar effect as the generation of interfering radio waves, possibly slowing down data transfer.

Most of the interfering radio wave sources other than wireless networks have local and/or temporary effects, not so affecting network performance. Rarely, however, the date rate is reduced and, in the worst case, communication is disabled temporarily. In such cases, change the location of this product and the channel used for communication. This may solve the problem.

Constructing a Network

This section gives some pointers and cautions relating to constructing a network using the AP and user units, and provides some practical examples.

(1) Check the coverage (cover area) of the AP. To use the AP with two or more user units logged in an infrastructure mode, all the user units must be installed within the cover area. The AP's coverage varies with obstacles (concrete walls, iron doors, elevator halls, etc.). Note also that the number of transmission/reception errors increases beyond a certain transmission distance.

When setting up the network, check the RSSI level then confirm that communication works correctly with the application you plan to use. For a TCP/IP system, for example, you can use the Windows PING command. To use PING, open an MS-DOS prompt window and enter the following command. The example command is for an AP with an IP address of 10.168.132.15.

```
C:\WINDOWS>ping 10.168.132.15
```

(2) The maximum number of user units that can log in to an AP at one time is 254. However, remember that the communication speed slows due to the increased loading as the number of user units for a particular AP increases.

(3) This product can be set to one of the four channels according to the Wireless Telegraphy Act.

(4) If a pair of wireless terminals are communicating via a particular channel, no other communications can use that channel within the range of the radio signal (the exception is broadcasting which transmits to all terminals). As a result, communication speed tends to drop as the density of wireless terminals increases although this depends to a large extent on how frequently the network is used.

(5) If the AP is connected to an Ethernet hub or similar, a unexpectedly large load can occur on the AP if the Ethernet traffic is heavy and this may reduce the performance of the wireless network. This can be solved by changing the hub connected to the AP to a switching hub (bridge).

(6) Setup the software in accordance with how the network will be used.

(7) The communication speed may also drop due to interference if two wireless terminals are located close to each other. In general, maintain a gap of about 1m between user units, 3m between APs and user units, and 3m between APs.

(8) The best performance is achieved from antennas if they are located in an open space free from obstructions. Avoid locating antennas where they will be hidden. In particular, when communication distance is an important consideration, it is recommended that you install antennas in a high location with a clear view.

(9) Floors often contain steel beams or metal firewalls and therefore communication between floors is often not possible.

Example 1 Use example

This example constructs a network with 48 user units. Although the small area to be covered means that one AP should be enough, two APs are used to provide a backup and to ensure a reasonable level of communication speed. If AP1 or AP2 is down, the roaming feature allows user units to log in to the other AP and so provides a backup network connection. Also, as notebook PCs are often brought to the meeting room and used to exchange data and access the server, and as the concrete walls of the meeting room block radio signals and result in a low RSSI value, another AP is also located in the meeting room.

Each of the APs has a wired connected to the Ethernet network.

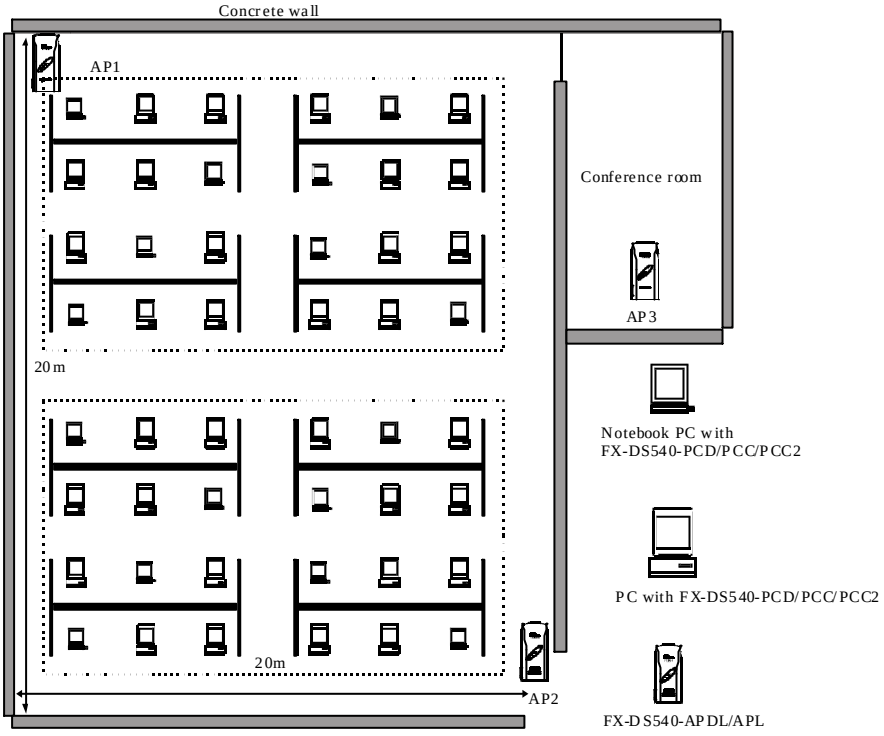


Figure 3.10. Use example

Example 2 Medium-sized wireless LAN

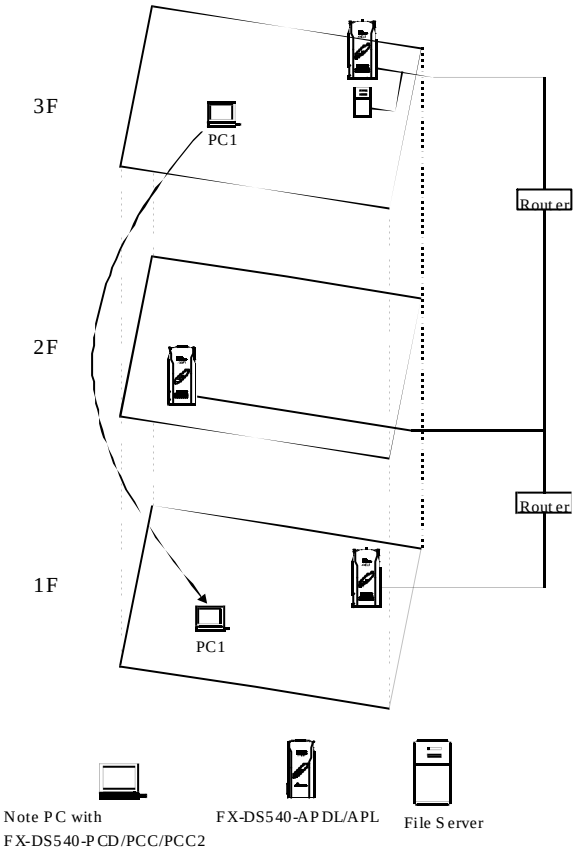


Figure 3.11. Medium-Sized Wireless LAN

This example constructs a wireless LAN operating over three floors of a building. A different department is located on each floor and these are separated by routers.

User PC1 belongs to the 3rd floor but sometimes takes his PC and works on the1st floor. As the IP tunneling server function is enabled on the AP, PC1 can still perform operations such as sending and receiving mail and accessing the 3F file server while roaming on the 1st floor away from the 3rd floor router.

To keep the various APs separated, the APs on different floors are installed on opposite sides of the building so that they are not directly above or below each other.

4. Setup Preparation

This chapter gives an overview of how to setup the AP and describes how to access the AP settings using a web browser.

Setup Methods

Although the FX-D540-APDL can be set up precisely to construct an advanced wireless LAN environment, there are two different setup methods available: web browser and TELNET.

The key features of each setup method are as follows.

WWW browser

- Provides an easy to use graphical interface.
- Setup can be performed remotely (via a LAN or modem).
- Independent of PC platform (type of OS, etc.).
- Requires that the network IP address of the AP be the same as the network IP address of the PC used for setup.

TELNET

- Setup can be performed remotely (via a LAN or modem) and even from older PCs.
- This setup assumes that the IP address of the AP and that of the PC used for setup belong to the same network group.
- It is necessary to connect the setting device to this product directly.
- Cumbersome text-only interface.

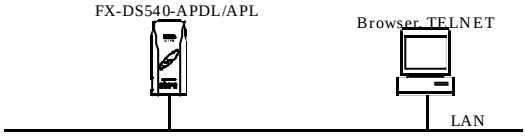


Figure 4.1. Setup image

Setup Using a Web Browser

You can setup the AP software from a PC running a web browser via the LAN or a modem. As this provides a graphical interface, setup using a web browser is much easier than using a TELNET.

The factory default IP address for the AP is listed on the underside of the case. You can use this address to connect to the AP from a web browser but this requires that you change the IP address of the PC to be in the same network group as the AP's IP address (when finished, set the IP address back to its original value).

Supported web browsers (recommended)

- Microsoft Internet Explorer 5.01 or higher
- Netscape Navigator 6 or higher

Connecting to the Web Browser PC

When using a web browser to setup the AP, you can connect via either a LAN or a modem. Use the following procedure to connect the web browser.

Connecting via a LAN

(1) Connect the PC on which you will run the web browser to the same network as the AP.
Alternatively, you can use a UTP cable to connect the PC directly to the AP. In that case, use a crossed-cable.
The connection will not work if you use a standard straight-through cable.

⚠ CAUTION

You may not be able to establish a connection if the web browser is setup to use a proxy. In this case, change the setting to not use a proxy.
Remember to change the proxy setting back when you have finished setting up the AP.

Connecting to an FX-DS540-APDL

To connect the web browser to the AP, the IP address of the PC on which you run the web browser must be in the same network group as the IP address of the AP. The factory default IP address set in the AP is always in the class A network group starting with [10] (that is, 10.xxx.xxx.xxx). Accordingly, set the IP address of the PC to also start with [10] ([IP 10.1.1.1, MASK 255.0.0.0], for example). Remember to set the IP address of the PC back to its previous value after you have finished with the connection for setting up the AP. You can also change and set the AP's IP address according to the PC being used for setup.

(1) Start the web browser
Recommended web browsers are Microsoft Internet Explorer 5.01 or later and Netscape Navigator 6.0 or later.

(2) After starting the web browser, enter the IP address of the AP in the URL field.
For example, if the IP address of the AP is [10.66.1.1], enter the following:

http://10.66.1.1 /

Refer to Chapter 5 below as you perform software setup.

(3) When connecting it to the product, input screen of the password is displayed. Enter the password. No password has been set by factory default. When you log in at first, not input anything in the form and then click the "Log-in" button to log in.

(4) Click on [Setup] in the Top Menu and open the Setup submenu. Choose and click on the desired item in the submenu to open its setup dialog box.

(5) After changing the setting of each item, press the [Send] button on the page to send the new setting to the AP. The setting sent to the AP is temporarily retained in the AP.
To save temporary data retained in the AP, click on the [Save] button on the left menu or top page, then choose "Yes" in the confirmation dialog box.
For the saved settings to take effect, click on the [Restart] button and choose "Yes" in the confirmation dialog box to restart the AP.
To save settings and restart the AP at the same time, click on the [Save/Restart] button and choose "Yes" in the confirmation dialog box.

For details of setup or Confirmation of status, refer to Chapter 5 to set up software.

Setup Using TELNET

Run Telnet on a PC connected within the same LAN to set up this product. As Telnet is a text based program, it requires a bit complicated setup operations but it can be used for setup even on an old PC with a browser which does not support setup through a web browser.

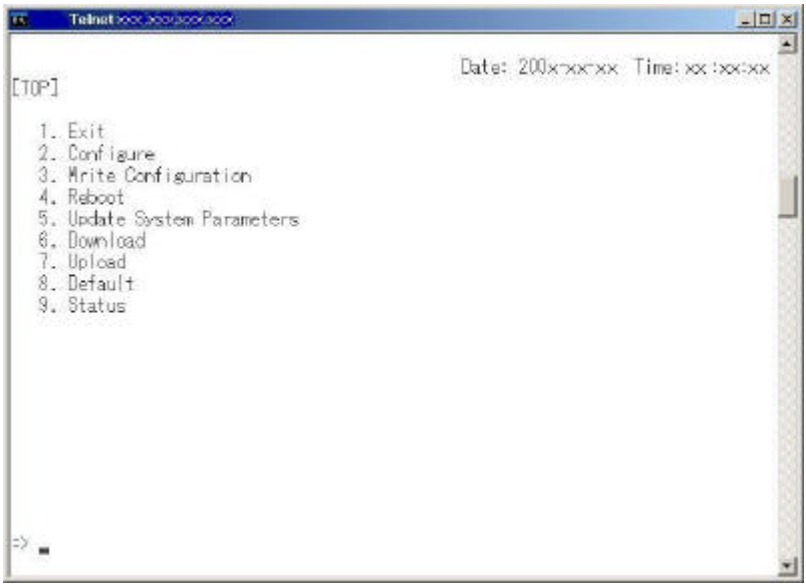


Figure 4.2. Example of TELNET Setting Screen

Connecting to an FX-DS540-APDL

For connecting the PC for setup to the AP using TELNET, the PC's IP address and the AP's IP address must belong to the same network group. The IP address factory-set for the AP belongs to the class-A network group beginning with 10, such as 10.xxx.xxx.xxx. For the PC to be used for setup, therefore, assign an IP address beginning with 10 (for example, [IP 10.1.1.1, MASK 255.0.0.0]). After connecting the PC to the AP and setting it up, restore the original IP address of the PC. The IP address of the AP should be changed when it is set up.

You can also change and setup the IP address of AP depending on PC to set.

(1) Bring up the command prompt. In Windows 98 or Windows ME, choose "MS-DOS Prompt" from "Programs" in the Start Menu. In Windows 2000 or Windows XP, choose "Command Prompt" from "Programs" in the Start Menu.

(2) Connect it by using TELNET and then connect it to AP by using telnet command. For example, if the IP address of the AP is [10.66.1.1], enter the following:

```
telnet 10.66.1.1
```

(3) Enter the password at the [Password:] prompt.
The default factory setting is no password. To login, just press the Enter key without entering anything.

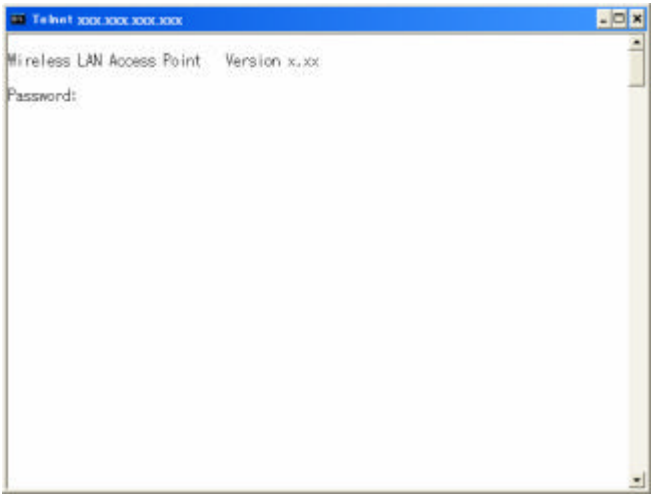


Figure 4.3. Password entry screen

(4) When password is entered correctly, TOP menu is displayed.

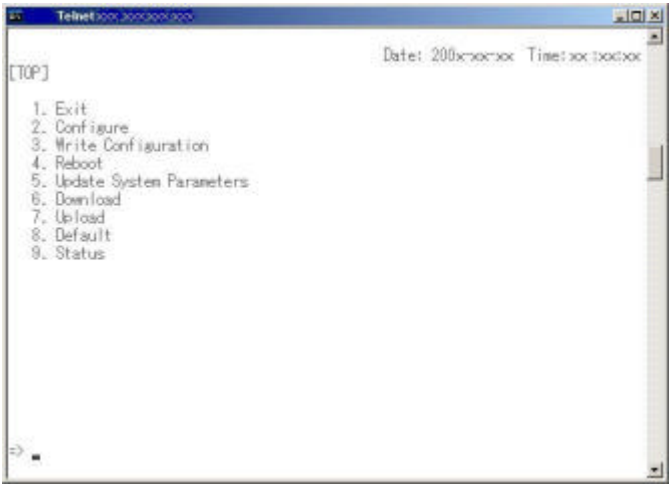


Figure 4.4. TOP menu

⚠ CAUTION

The console program uses the “Shift-JIS” character set for Kanji codes. If characters do not display correctly, check the Kanji code setting for the terminal.

TELNET Key Operation

Select items from the TELNET menus by entering the corresponding number. In addition to entering numbers, you can also use the following commands. The operation of each key is the same for all menus.

- TT Return to top menu
- E Escape from the current operation
- M Return to previous menu
- GO Jump to the specified category
- JP Change to Japanese mode (SHIFT-JIS)
- US Change to English mode
- W Save settings
- BYE / OFF End
- H or ? Display a list of commands (Help screen)

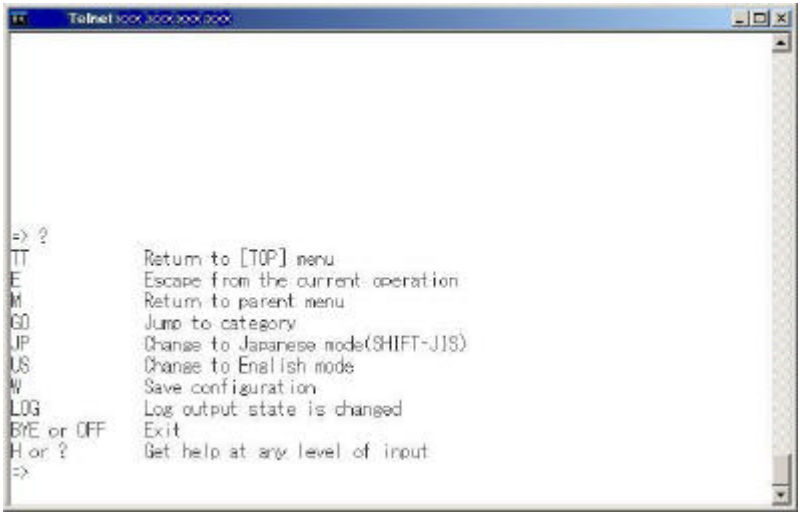


Figure 4.5. Help Screen

Explanation of Top Menu and IP Settings

This section describes the top menu, with the IP address and subnet mask settings as examples. Although individual menu items are not detailed here, they are almost the same as the settings available in the web browser. Accordingly, see Chapter 5 for details.

Table 4.1. TOP Menu

Menu	Description
1.End	Exit terminal setup.
2.Setup	Select to setup AP.
3.Writing	Use this command to save the settings.
4.Reboot	Reboots the AP. Perform a reboot after modifying the settings (after saving). The new settings become effective from after the reboot.
5.Change system parameters	Change the password or date.
6.Download	Download the settings file and firmware from the AP.
7.Upload	Send the settings file or firmware from the PC (terminal) to the AP and update on the AP.
8.Default	Restore all AP settings to their factory defaults. The IP address can be excluded.
9.Status	Use this command to check the AP settings.

Setting the IP address

(1) Select [2. Setup].

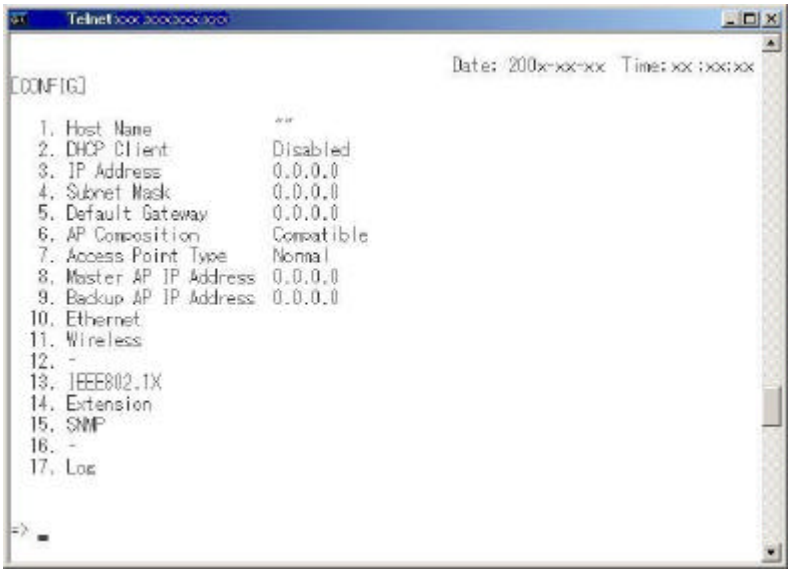


Figure 4.6. IP Address Setting Screen

(2) Select [3. IP Address] and enter the IP address assigned to the AP on the wired LAN.

(3) Select [4. Sub-Net Mask] and enter the sub-net mask for the IP address set in step 2.

(4) Select [5. Default Gateway] and enter the IP address of the default gateway.
You do not need to enter an IP address if there is no default gateway.

(5) Press the [W] key or return to the top menu and select [3. Writing] to save the settings, then enter [BYE] or return to the top menu and select [1. Exit] to disconnect the terminal.
After restarting the AP, setting is enable.
This completes network setup. You can now use a web browser for setup and perform network management using SNMP.

5. Setup and Status Display

This chapter describes how to setup the AP using a web browser, explains each setting item and status display. Before you can setup the AP, perform the preparation described in "Chapter 4 Setup Preparation".

This section describes how to perform setup using a web browser.

Setup Item List

Setup items are listed in the following table. The items that can be set vary with the wireless link mode. The symbols O and – indicate the items that can be set and the items that are not available, respectively.

Table 5.1. Setup Item List(1/3)

Setting item		Wireless Link Mode				
		Standard Infrastructure mode		Compatible Infrastructure mode		Advanced Infrastructure mode
		AP	Station	AP	Station	AP fixation
Basic setting						
Host name		O				
DHCP client		O				
IP address		O				
Subnet mask		O				
Default gateway		O				
Access point construction		O				
Access point type		O				
IP address of master AP		O				
IP address of backup AP		O				
Language setting		O				
Password		O				
Ethernet						
Port speed		O				
Link down sense		O	–	O	–	O
Wireless LAN						
Basis	Interface	O	O	O	O	O
	Wireless LAN standard	O	O	O	O	O
	Wireless Link Mode	Standard		Compatible		Advanced
	Unit type	AP	Station	AP	Station	AP fixation
Details	ESSID	O	O	O	O	O
	Channel number	O	–	O	–	O
	Transmission rate	O	O	O	O	O
	Beacon transmission rate	O	–	O	–	O
	Transmission output	O	O	O	O	O

Table 5.1. Setup Item List(2/3)

Setting item			Wireless Link Mode				
			Standard Infrastructure mode		Compatible Infrastructure mode		Advanced Infrastructure mode
			AP	Station	AP	Station	AP fixation
Details	802.11g parameter	802.11g Only mode	O	–	O	–	O
		Protect mode	O	O	O	O	O
		Protect type	O	O	O	O	O
	Antenna selecting		O	O	O	O	O
	Statistic node address		–	–	–	O	–
	Maximum number of logged in devices		O	–	O	–	O
	Roaming threshold		–	O	–	O	–
	Broadcast	Speed control function	O	–	O	–	O
		Transmission speed	O	–	O	–	O
		Transmission retry count	O	–	O	–	O
		Band	O	–	O	–	O
	Prioritized APs	AP1 to AP5	–	O	–	O	–
		Connect to other APs	–	O	–	O	–
Security	Encryption	Functions	O	O	O	O	O
		Default key	O	O	O	O	O
		Size / Key 1 to 4	O	O	O	O	O
	WSL		O	O	–	–	O
	MAC address filtering		O	–	O	–	O
	ESSID security		O	–	O	–	O
IEEE802.1X							
IEEE802.1X function			O	–	O	–	O
Re-authentication interval			O	–	O	–	O
Radius server list (1 to 4)		IP address	O	–	O	–	O
		Port number	O	–	O	–	O
		ESSID	O	–	O	–	O
		Shared secret	O	–	O	–	O
Extensions							
Bridge packet control			O	–	O	–	O
Network time		Function	O				
		IP address	O				
		Time zone	O				

Table 5.1. Setup Item List(3/3)

Setting item		Wireless Link Mode				
		Standard Infrastructure mode		Compatible Infrastructure mode		Advanced Infrastructure mode
		AP	Station	AP	Station	AP fixation
Access control	TELNET server function	O				
	FTP server function	O				
	WEB server function	O				
	Specifing Administrator IP	O				
	Administrator IP address1	O				
	Administrator IP address2	O				
SNMP						
SNMP agent function		O				
Community name		O				
Access permission		O				
Trap destination IP address		O				
Administrator contact information		O				
Device location		O				
Device name		O				
Log function						
Log function		O				
Overwrite mode		O				
Start time setting	Beginning date set function	O				
	Beginning date	O				
Detailed setting	Log in	O				
	Log Out	O				
	Log in refusal	O				
	Roaming	O				
	IP tunnel start	O				
	IP tunnel exit	O				
	Application log in	O				
	Application log out	O				
Setting list						
Setting list		O				

*: When connecting a station to the AP in the Advanced Infrastructure mode, set the station to the Standard Infrastructure mode.

*: When the AP is set as a station in compatible infrastructure mode, only one PC is connected to the station.

Settings

Basic setting

Host name

Assigning a name to an AP makes it easier to identify on the network. Enter a name of up to 16 alphanumeric characters.

Factory default setting : (Not input)

DHCP client

Enabling "DHCP client" makes the access point available as a DHCP client.

Factory default setting : Disable

IP address

Sets the IP address of the AP. Always set the IP address. When setting via a LAN using a browser running on a PC, the network address of the AP must be the same as the network address of the PC.

Factory default setting : (Specified on the housing seal)

Subnet mask

If using a subnet, specify the subnet mask.

Factory default setting : 255.0.0.0

Default gateway

Specify the IP address of the router for the network to which the AP belongs.

Factory default setting : 0.0.0.0

Access point construction

Sets the Access point construction.
This setting affects "Access point type", "IP address of the masuterAP", "IP address of the backup AP".

Select "Compatible, when AP is coustructed by only FLEXLAN DS540 series.

Select "Integrated" when the AP includes the DS110 series as well as the DS540 series.

Factory default setting : Compatibility

Access point type

The application type of the access point can be set by selecting "normal", "master", or "backup".
The "master" device integrates access points on the network and the "backup" device substitutes for the master AP if the master AP stops working for some reason.

Factory default setting : Normal

IP address of the master AP

When the master AP exists, specify the IP address of the AP that serves as the master AP.

Factory default setting : 0.0.0.0

IP address of the backup AP

When a backup AP exists, specify its IP address.

Factory default setting : 0.0.0.0

Language setting

Select the language displayed by the terminal or browser from "English" or "Japanese.

Factory default setting : English

Password

Set a password. Enter a string of up to 31 single-byte alphanumeric characters. The password is case sensitive. At the password input prompt when starting software setup, you can log in by clicking on the [Setting] button with no password entry.

If you forget your password, initialize the AP using the DIP switch (INIT).

The password is cleared when the AP is initialized. Note, however, that initializing the AP resets all of its settings to their factory defaults, requiring you to make settings over again. For using the DIP switches, see Chapter 3.

Factory default setting : (Not input)

Ethernet

Port speed

Select the port speed setting. Select one of "Auto", "100M Full Duplex", "100M half Duplex", "10M Full Duplex", or "10M half Duplex".

Factory default setting : Auto

Link down sense

Enabling "link down sense" stops the wireless capabilities when the wired link of the access point is disconnected.

Factory default setting : Disable

Wireless LAN

To change the wireless LAN standard (IEEE802.11a/802.11b/802.11g), wireless connection mode, and unit type, take three steps of "Basic" -> "Details" -> "Security" to make their respective settings.

For any other item, you can change the setting on under "Details" or "Security".

Basis

Interface

Disabling "Interface" disables the internal wireless LAN module.

Factory default setting : Enabled

Wireless LAN standard

Sets the wireless LAN standard to use. When the unit type is "Access point", you can select one of checkboxes. When the unit type is "Station", you can select more than one check boxes according to the standard of the access point to be connected. The wireless LAN standard to be used is determined automatically depending on the destination access point.

Factory default setting : Check only IEEE802.11a.

Wireless Link Mode

Select the operation mode of the FX-DS540-AP/APP from among "Standard Infrastructure", "Compatible Infrastructure", and "Advanced Infrastructure".

Factory default setting : Standard Infrastructure

Table 5.2. Wireless Link Mode

Standard Infrastructure	Each access point can accommodate stations (such as wireless LAN cards) to make up a network. This mode provides scalability from a middle- or large-scale system with multiple access points connected by LAN to a small-scale system based on a single access point.
Compatible Infrastructure	This mode allows the AP to be networked with other manufacturers' Wi-Fi certified wireless terminals other than the FLEXLAN series. Note, however, that functions such as IP tunneling cannot be used in this mode.
Advanced Infrastructure	The access point can be used in both of the Standard Infrastructure and Compatible Infrastructure modes. This mode is a mixture of the two.

Unit type

Select either "Access point" or "Station". "Access Point" means the Access point manages user units and other Access Points that are operating as stations. "Station" means the Access Point is managed by (logs in to) another Access Point and is set when the Access Point is used as a bridge or similar.

Factory default setting : Access point

Details

ESSID

The name of the wireless LAN to which the AP belongs. Changing the ESSID causes the AP to be disconnected from the network. Enter a name up to 32 alphanumeric characters. The name is case sensitive.

Factory default setting : LocalGroup

Channel number (This item available when the unit type is "Access point".)

Sets the channel number. Setting-able channel numbers are from "36" to "64", "149" to "165" when IEEE802.11a and from "1" to "11" when IEEE802.11b/IEEE802.11g.

Factory default setting : 36ch (Wireless Lan standard is IEEE802.11a)

Transmission rate

Sets the wireless transmission rate.
Select one from "Auto", "54Mpbs", "48Mbps", "36Mpbs", "24Mpbs", "18Mpbs", "12 Mpbs", "9 Mpbs", "6 Mpbs" when IEEE802.11a.

Select one from "11Mpbs", "5.5Mbps", "2Mpbs", "1Mpbs" when IEEE802.11b.

Select one from "Auto", "54Mpbs", "48Mbps", "36Mpbs", "24Mpbs", "18Mpbs", "12 Mpbs", "9 Mpbs", "6 Mpbs", "11Mpbs", "5.5Mbps", "2Mpbs", "1Mpbs" when IEEE802.11g.

Factory default setting : Auto

Beacon transmission rate

Specify the beacon transmission rate. The options available to this item are the same as those for the above transmission rate except "Auto".

Factory default setting : 6Mbps (Wireless Lan standard is IEEE802.11a)

Transmission output

You can decrease the transmission output to "50%" or "25%" by software setting. To decrease the output, select either.

Factory default setting : MAX

802.11g parameter

This item is available when "IEEE802.11g" is selected as the wireless LAN standard. Parameter about IEEE802.11g can be set.

Enabling the "802.11g Only" mode rejects access from IEEE802.11b compliant user units and accepts access only from IEEE802.11g compliant user units, resulting in communication with IEEE802.11g user units at higher data rates than both types of user units coexist with the "802.11g Only" mode disabled. This setting is the item when unit type is "Access point".

Enabling the protect mode enables stable communication even in an environment in which IEEE802.11b compliant user units coexist with IEEE802.11g compliant user units. Disabling the protect mode makes communication a bit unstable but increases the data rate to some extent.

For the protect type, specify the data packet configuration method. "CTS-only" uses only CTS to transmit and receive data. "RTS-CTS" uses both RTS and CTS to transmit and receive data.
Data rate of "CTS-only" is higer than that of "RTS-CTS". This setting is enabled when the protect mode is enabled.

Factory default setting : 802.11g Only mode … Disabled
Protect mode … Enabled
Protect type … CTS-only

Antenna selecting

You can specify the antenna to use. When "Auto", use the both antenna connected to the built-in wireless module. When "1" or "2" is set, either of them is used.

Factory default setting : Auto

Statistic node address (This item available when the unit type is "Station".)

You can set it when "Compatible Infrastructure" mode.

Enter the MAC address of the PC to be connected to the FX-D540-APDL whose unit type has been set to "Station". In general, set this item to connect the unit to a receive-only device such as a POS terminal. The factory default indicates no setting (00-00-00-00-00-00).

When specifying a MAC address, enter a hyphen (-) at intervals of two bytes.
(Example: 01-23-45-67-89-ab)

Factory default setting : 00-00-00-00-00-00

Maximum number of logged in devices (This item available when the unit type is "Access point".)

The number of user unit to log in AP is limited. From 1 to 254 are input.

Factory default setting : 254

Roaming threshold (This item available when the unit type is "Station".)

When the RSSI value of the currently connected access point is smaller than the setting, the unit searches for a roaming-accessible access point and roams into that access point if possible. Threshold can be set from 0 to 95. Increasing this value makes roaming easiers; decreasing it makes roaming harder.

This function is enabled when unit type is "Station." and is disabled when it is "Access point".

Factory default setting : 15

Broadcast (This item available when the unit type is "Access point".)

It can be set when the mode type is "Standard infrastructure".

It is set when the data transmission is couducted. To set the transmission rate and transmission retry count manually, set "Speed control function" to "Manual" and set "Transmission speed" and "Transmission retry count" to the desired values.

To set the transmission rate and transmission retry count automatically, set "Speed control function" to "Auto" and set "Band" to the band to be used for broadcasting within the range from 0 to 54.

Factory defaults : Speed control function …Disable
Transmission speed …Auto
Transmission retry count …0
Band …0

Prioritized APs (This item available when the unit type is "Station".)

This item allows you to specify the access point to be connected preferentially. Wireless MAC address of access point is input in AP1 to AP5. Wireless MAC address of access point can be confirmed by using "Status" of each access point and "Wireless MAC address" of the "Wireless LAN" items.

The access points to be connected are assigned priorities in ascending order beginning with AP1 (followed by AP2, …, AP5). By inputting the wireless MAC address, this function is enabled. When this function is not used, all MAC addresses are set to all zeroes (00-00-00-00-00-00).

When entering a MAC address, place a hyphen (-) between adjacent pairs of bytes in the MAC address. (Example : 01-23-45-67-89-ab)

Enable "Connect to other APs" to permit connection, if the unit fails to be connected to any of the access points AP1 to AP5, to any other AP. To prohibit connection to any access point other than the prioritized APs, disable "Connect to other APs".

Factory default setting : AP1 to AP5 …00-00-00-00-00-00
Connect to other APs … Enabled

Security

Encryption

This setting specifies whether to enable or disable encryption. To enable encryption, select WEP or AES under "Functions". Specify the default transmission key no. to use when you transmit the data.
Enter the key hexadecimally (uppercase and lowercase alphanumeric characters can be used). To use the WEP protocol, enter ten digits for a 64-bit key, 26 digits for a 128-bit key, or 32 digits for a 152-bit key. Enter 32 digits for a 128-bit key when AWS. If you disable encryption, neither key can be used as the default key.

Note that enabling encryption prevents communications from being performed between terminals using different security protocols or keys.

Factory defaults : Function ...Disable
Default key …#1
Key #1 to #4 …Disable, (Not enter)

WSL(Wireless Security Link)

Select whether to encrypt wireless transmission data. Note that WSL-enabled and WSL-disabled terminals cannot communicate with each other. The WSL key can be set only when WSL has been enabled. Note, also, that terminals different in WSL key cannot communicate with other.

Factory default setting : Disable (Not input)

MAC address filtering (This item available when the unit type is "Access point".)

Select whether to use the MAC address filtering function. Enabling the function rejects an attempt to log in to the access point by other than the clients having authorized MAC addresses.

MAC addresses can be registered either individually or in a range.
You can register up to 8192 entries.
When specifying a MAC address, enter a hyphen (-) at intervals of two bytes.
(Example: 01-23-45-67-89-ab)

Factory default setting : Disable

ESSID security (This item available when the unit type is "Access point".)

ESSIC security is the composite function as the combination of "ANY ID reject" and "ESSID hide". Enabling this function rejects access by ANY ID terminals (those with on ESSID assigned) and hides the AP's ESSID from external references to the access point. Using the function restricts illegal access using ANY ID and prevents the ESSID from being easily known to third parties.

Factory default setting : Disable

IEEE802.1X

IEEE802.1X function

Set this item to "enable" to enable the function of IEEE802.1X.

Factory default setting : Disable

Re-authentication interval

Specify the time interval at which to perform re-authentication, between 2 and 4320 minutes.

Factory default setting : 60(minutes)

RADIUS server

Up to four RADIUS servers can be registered by entering their IP address, port number, and shared secret. Even when one RADIUS server goes down, clients can connect to another RADIUS server as long as there are two or more RADIUS servers registered. RADIUS server 1 is assigned the highest priority. If the client cannot connect to it, the client will attempt to connect to RADIUS servers 2 to 4 sequentially.

Enter the IP address of RADIUS server in "IP address".

Enter the port number to use for communication with RADIUS server in port number.

For "ESSID", specify the ESSID of the access point to which to change upon switching to the RADIUS server defined with the above "IP address". Set th item only when this function is used.
When this function is not used, leave the field blank.

Enter the shared secret of IEEE802.1X in "Shared secret".

Factory defaults : IEEE802.1X function …Disable
Re-authentication interval …60 (minutes)
(RADIUS server 1 to 4) IP address …0.0.0.0
(RADIUS server 1 to 4) Port number …1812
(RADIUS server 1 to 4) ESSID …(Not input)
(RADIUS server 1 to 4) Shared secret … (Not input)

Extensions

Bridge packet control

Enabling the bridge packet control function can restrict communication between clients accommodated by the same access point.

You can specify the network in which to share files by editing the bridge packet control list. Register the MAC address of the router that permits the clients to share files.

When specifying the MAC address, enter a hyphen (-) at intervals of two bytes.
(Example: 01-23-45-67-89-ab)

Factory default setting : Disable

Network time

Enabling the network time function can synchronize the access point time with the network time. The factory default setting is "disable".

Before you can enable this function, you have to set the IP address and time zone of a network time server on the network. (Example: For use in Japan, enter "+09:00" (meaning UTC + 9 hours) as the Japan standard time is nine hours ahead of Universal Time Coordinated (UTC).)

Factory default setting : function …Disable
IP address … 0.0.0.0
Time zone … +09:00

Access control

Set the access control for the access point. Disabling TELNET, FTP, WEB server function can be refecte the connection to each server. Disabling all sets, it cannot be connected to Access point.

Enabling specification of administrator IP, you can specify the IP address to connect to TELNET, FTP, WEB. Up to two administrator IP addresses can be registered in "Administrator IP address 1" and "Administrator IP address 2". When using this function, you need to enable TELNET server function. When the disabled IP address is not registered, connection toTELNET, FTP, WEB by using access point cannot be done.

Factory default setting : TELNET / FTP / WEB server function …Disable
Administrator IP addresse …Disable
Administrator IP addresse 1 to 2 …0.0.0.0

SNMP

SNMP agent function

Set this item to "enable" to enable SNMP.

Factory default setting : Disable.

Community name

Enter the SNMP authentication string. The SNMP authentication string serves as a password to access the AP using SNMP. Programs use this community name to access the AP's MIB.

Enter a string of up to 32 single-byte alphanumeric characters. The community name is case sensitive.

Factory default setting : public

Access permission

Set the access permission for the community. Select "Read/Write" or "Read Only". The factory default setting is "Read/Write".

Factory default setting : Read / Write

Trap destination IP address

Trap is the function to notify a user of a change made within the SNMP agent system. The trap function can be enabled by specify the IP address of the destination user. The SNMP manager having the IP address specified here can manage trap information about the AP. If the network contains more than one AP, it is advisable to register the same IP address so that all the APs can be managed on one machine. Up to three destination IPs can be registered.

Factory default setting : 0.0.0.0

Administrator contact information

Enter contact information about the AP administrator. An example is the name and telephone number of the network administrator. The string can be up to 32 characters long when all the characters are single-byte alphanumeric characters or up to 16 characters long (within 32 bytes) when they are all double-byte Japanese characters.

Factory default setting : (Not input)

Device location

Specify the physical location of the AP. An example is "Administration Division, 2F". The string can be up to 32 characters long when all the characters are single-byte alphanumeric characters or up to 16 characters long (within 32 bytes) when they are all double-byte Japanese characters.

Factory default setting : (Not input)

Device name

Specify the device name of the AP under SNMP. Enter a string of up to 32 single-byte alphanumeric characters. The device name is case sensitive.

Factory default setting : (Not input)

Log function

The FX-DS540-APDL can preserve log information. See Chapter 6 for details of the logged data and data collection methods.

Log function

This specifies whether or not to enable logging. The collected log data (2048 at Max.) is stored in internal memory.

Factory default setting : Disable

Overwrite setting

This specifies whether or not to overwrite old data when the number of log entries reaches the maximum. If disabled, log collection halts when the maximum number of entries is reached.

Factory default setting : Enable

Start time setting

This specifies whether or not to set a logging start time. If enabled, set the time at which to start logging.

Factory default setting : Beginning date set function …Disable
Beginning date …0 :00 1 Jan. 2002

Detailed setting

You can select the types of events to be logged. Setting [Log in], [Log Out], [Log in refusal], [Roaming], [IP tunnel start / exit] and [Application log in / log out] to "ON" allows the selected events to be logged. Setting them to "OFF" prevents them from being logged.
Factory default setting : All of the events are set to "ON"

Table 5.3. Events to Be Logged

Event	Introduction
Start	Indicates that the AP has been activated.
Link Up	Indicates that the wired link has been connected and the link speed.
Link Down	Indicates that the wired link has been disconnected.
Login	Indicates the MAC address of the wireless terminal connected to the AP.
Logout	Indicates the MAC address of the wireless terminal disconnected from the AP.
Login NG	Indicates that the filter function rejected an attempt to log in by an unregistered wireless terminal.
Roaming	Indicates the MAC address of the wireless terminal roaming into the AP.
Tunnel Start	Indicates the MAC address of the wireless terminal that has started IP tunneling.
Tunnel Stop	Indicates the MAC address of the wireless terminal that has terminated IP tunneling.
Application Login	Indicate the IP address of the terminal that has used an application (such as telenet or FTP).
Application Logout	Indicates the termination of an application and the IP address of the terminal that used the application.
Write Firmware	Indicates that firmware has been reprogrammed. (Example: Update from Ver1.15 to Ver1.20)
Write Config	Indicates that the Config file has been edited.
Manual Reset	Indicates that the AP has been restarted by the terminal or browser.

Status display

A list of status information on this product can be displayed by selecting "Status" after logging in through a web browser or Telnet.

This displays the following information.

Configuration data

This includes the firmware version, IP address.

Interface information

The browser displays information about the Ethernet, wireless LAN, and series interfaces.

Wireless LAN information

The browser displays wireless LAN information, wireless packet statistical information, and Wireless node information.

MAC address table

The browser displays information on the user units and stations that have been logged in to the AP.

Log information

The browser displays log information recorded in the AP.

6. Meintenance

This chapter describes how to perform maintenance on the AP and explains the tools to be used. Here, “maintenance” means the following: log file collection, firmware upgrades, and saving and restoring the software settings.

Maintenance Tool

This maintenance tool is available for the FTP.
This section describes how to use the tool.

Log File Collection

The AP collects the following log data.

To collect the log file, you collect it by using FTP via the LAN.

The log file is in text format and can be displayed in the Notepad or WordPad programs that come with Windows.

The collected log file is stored the CF card with the following file name.

File name : LOGFILE

⚠ CAUTION

To collect the log file, log collection must be enabled. Note also that the contents of the log file differ depending on the operating mode and software settings.

Using FTP to Get the Log File

(1) Run FTP to log in to the AP.

(2) Transfer the log file.

(3) Exit FTP.

The following example shows how to get the log file using the FTP command coming standard with Windows. Invoke the MS-DOS prompt or command prompt and follow the procedure below to get the log file.The example assumes the IP address as 10.168.132.15.

```
C:\>ftp 10.168.132.15          ---------- (1)
ftp>get logfile                ---------- (2)
ftp>bye                        ---------- (3)
```

Saving the Settings File

Making a backup of the AP software settings file has the following benefits:

- If you have more than one AP and all APs have the same settings, you just need to setup one AP then use the resulting settings file for the other APs. (However, as this sets the same IP address for all APs, you need to change the IP address separately.)
- The old settings can be restored easily if a fault causes the settings file to be erased.

The settings file is stored the CF card with the following file name.

File name : CONFIG

If the MAC address filtering and bridge packet control functions are used, their settings files should also be saved. The settings files are stored in memory on the AP with the following file names:

MAC address filtering --- MACFLIST

Bridge packet control --- BRGFLIST

Note that a file of LOGFLIST may be stored in the AP's memory but it is not used as a setup file.

Using FTP to Backup the Settings File

(1) Run FTP to log in to the AP.

(2) Transfer the settings file.

When the MAC address filtering and bridge packet control functions are in use, MACFLIST, LOGFLIST, and BRGFLIST are also transferred.

(3) Exit FTP.

The following example shows how to get the log file using the FTP command coming standard with Windows.

Invoke the MS-DOS prompt or command prompt and follow the procedure below to get the settings file. The example assumes the IP address as 10.168.132.15.

```
C:\>ftp 10.168.132.15          ---------- (1)
ftp>put config                 ---------- (2)
ftp>get macflist
ftp>get brgflist
ftp>bye                        ---------- (3)
```

Restoring the Software Settings

Using this function has the following benefits:

- If you have more than one AP and all APs have the same settings, you just need to setup one AP then use the resulting settings file for the other APs. (However, as this sets the same IP address for all APs, you need to change the IP address separately.)
- The old settings can be restored easily if a fault causes the settings file to be erased.

Using FTP to Restore the Settings

(1) Run FTP to log in to the AP.

(2) Transfer the settings file(config).

When the MAC address filtering and bridge packet control functions are in use, MACFLIST, and BRGFLIST are also transferred.

(3) Issue the reset request command(command : quote crst).

(4) Quit FTP. The AP will be restarted.

The following example shows how to update the firmware using the FTP command coming standard with Windows.
Invoke the MS-DOS prompt or command prompt and follow the procedure below to restore AP settings.

The example assumes the IP address as 10.168.132.15.

```
C:\>ftp 10.168.132.15          ---------- (1)
ftp>put config                 ---------- (2)
ftp>quote crst                 ---------- (3)
ftp>bye                        ---------- (4)
```

When the MAC address filtering function is in use, MACFLIST and LOGFLIST must be transferred along with CONFIG. When the bridge packet control function is in use, BRGFLIST must be transferred along with CONFIG. If both of the functions are in use, the above example is replaced by the following:

```
C:\>ftp 10.168.132.15          ---------- (1)
ftp>put config                 ---------- (2)
ftp>put macflist
ftp>put brgflist
ftp>quote crst                 ---------- (3)
ftp>bye                        ---------- (4)
```

Upgrading the Firmware

The AP firmware may be upgraded to resolve any bugs found in the software or to add new functions. Contact CONTEC via our web site for details of the latest firmware.

The firmware is stored the AP memory with the following file name.

File name : apfirm.bin

Performing an Upgrade Using FTP

(1) Run FTP to log in to the AP.

(2) Change the transfer mode to binary.

(3) Transfer the firmware file.

(4) Issue the reset request command (quote crst).

(5) Quit FTP. The AP will be restarted.

The following example shows how to update the firmware using the FTP command coming standard with Windows.

Invoke the MS-DOS prompt or command prompt and follow the procedure below to restore AP settings. The example assumes the IP address as 10.168.132.15.

```
A:\>ftp 10.168.132.15        ---------- (1)
ftp>bin                      ---------- (2)
ftp>put apfirm.bin           ---------- (3)
ftp>quote crst               ---------- (4)
ftp>bye                      ---------- (5)
```

Performing an Update Using a Web Browser

(1) Start a web browser and access and log in to the AP.

(2) Open the “Maintenance” menu and then open the “Upgrade Firmware”page.

(3) Click the [Browse…] button and select the desired firmware then, click the [Update] button to transfer the firmware.

(4) Upon completion of transfer of the firmware, the screen changes with the AP restarted.

7. Troubleshooting

This chapter describes common problems that may occur with this product and what to do about them. If any problems occur that are not described here, check to confirm that the re-occur, then contact the store where you purchased the product.

When Communication Fails

Check hardware

- If connecting via the wired LAN, check that the LAN cable is connected correctly.
- Check that there are no obstructions in the way of this product.

Check software

- The FLEXLAN-DS540 series is designed to handle a variety of operating formats, and requires software setting for each type of operation. Check that the settings are appropriate for the type of operation, and check the format in which communication is being attempted. Also check DIP switch settings.
- The terminals that cannot communicate with each other may have the same ESSID. Two terminals with the same ESSID cannot communicate with each other.
- Check that the AP IP address and subnet settings have been entered.
- Check whether the wireless link mode has been set correctly.
  To use the AP in an infrastructure mode, use the user unit in the infrastructure mode as well.
- Check whether communication is restricted by security functions.
- Check whether the data encryption setting is the same as that of the recipient.
  Communication cannot be performed while data encryption is being switched between ON (enabled) and OFF (disabled).

Check the peripheral environment and place of installation

- A nearby source of electromagnetic interference can prevent communicat ion. In general locations (excluding factories) the following may be sources of electromagnetic emissions.
  - 5GHz band not conforming to IEEE802.11(when using by IEEE802.11a) or 2.4GHz band(when using by IEEE802.11b/IEEE802.11g) wireless network.
  - Electric devices which give off 2.4GHz band electric wave - microwave oven, security gate (it is a antitheft gate in the shop), copy machine and so on.

Most electromagnetic sources other than wireless networks are local and not continuous, and therefore by moving the location of the unit and waiting briefly, communication may be possible.

- Sometimes communication is hindered by attenuation of electric waves. Attenuation occurs naturally as distance from the source of transmission increases, but may also be caused by objects in the path of the transmission. The objects primarily responsible for attenuation are the following.
  - Concrete walls
  - Metallic surfaces around this product

When You Cannot Perform Setup Using a Browser

- Check that you are using the correct IP address for the AP.
- Check that the IP address of your PC is in the same network group as the IP address of the AP.
- Use a recommended browser (Microsoft Internet Explorer 5.01 or later, Netscape Navigator 6 or later)
- You cannot use a browser to communicate with the AP if the TCP/IP protocol is not installed on your PC.

When the AP Will Not Start

Check the power LED

- Check whether the "POWER" LED is illuminated. If not, check the power cable and confirm that the power plug and mains plug are correctly connected.
- Check whether the Power LED is flashing. If the power LED is still flashing more than 5 minutes after the power is switched on, the problem may be an AP firmware failure. In this case, contact your retailer.

8. Appecdix

Factory Default Settings List

Hardware Setup

- FX-DS540-APDL
  switch1 : OFF
  switch 2 : OFF

Figure 8.1. DIP Switch

Initial setup

Table 8.1. Initial setup list (1/4)

	Setting item	Setting contents(First default)
	<Base setting>	
	Host name (Enter a string of up to 16 single-byte alphanumeric characters.)	(Blank)
	DHCP client	Disable / Enable
	IP address (When disabled setting of DHCP client sets : enable)	Seal on the back of housing
	Subnet mask	255.0.0.0
	Default gateway	0.0.0.0
	Access point construction	Compatible, Integrated
	Access point type	Normal, Master, Backup
	IP of master AP (It is set when normal or backup)	0.0.0.0
	IP of backup AP (It is set when normal or backup)	0.0.0.0
	Language setting	Japanese, English
	Password (single-byte alphanumeric characters can be up to 31 characters long and .the password is case sensitive.)	(Blank)
	<Ethernet>	
	Port speed	Recognization automatically, 100M/full, 100M/half duplex, 10M/full, 10M/half duplex
	Link down sense	Disable, Enable (corresponding to 5/2.4GHz only when unit type access point.

11g: The function when selecting IEEE802.11g.
AP: The function when unit type is access point.
ST: The function when unit type is station.

Table 8.1. Initial setup list (2/4)

Setting item		Setting contents(First default)
	<Wireless LAN>	
	Interface	Enable, Disable
	Wireless LAN standard	IEEE802.11a, IEEE802.11b, IEEE802.11g
	Wireless connection mode	Standard, Compatible, advanced infrastructure
	Unit type	Access point, Station *In compatible mode, you can not select station.
	ESSID (single-byte alphanumeric characters can be up to 32 characters long and .the password is case sensitive.)	LocalGroup
AP	Channel number	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165 : 11a 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 : 11g, 11b *In station, Free is fixed.
	Transmission rate	Auto, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M
	Encryption	Disable, WEP, AES
	Default key	#1, #2, #3, #4
	Size / key#1	Disalbe, 64bit(10-digits), 128bit(26-digits), 152bit(32-digits) : WEP 128bit(32-digits) : AES
	Key#1 hexadecimal value (0 to 9, a to f or A to F)	
	Size / Key#2	Disable, 64bit(10-digits), 128bit(26-digits), 152bit(32-digits) : WEP 128bit(32-digits) : AES
	Key#2 hexadecimal value (0 to 9, a to f or A to F)	
	Size / key#3	Disable, 64bit(10-digits), 128bit(26-digits), 152bit(32-digits) : WEP 128bit(32-digits) : AES
	Key#3 hexadecimal value (0 to 9, a to f or A to F)	
	Size / Key#4	Disable, 64bit(10-digits), 128bit(26-digits), 152bit(32-digits) : WEP 128bit(32-digits) : AES
	Key#4 hexadecimal value (0 to 9, a to f or A to F)	
	WSL (Wireless security link)	Disable, Enable(20-digits)
	Key WSL hexadecimal value (0 to 9, a to f or A to F)	
	Transmission output	MAX, 50%(-3dB), 25%(-6dB)
AP	MAC address filtering	Disable, Enable [List edit : MAX 8192 entries]

11g: The function when selecting IEEE802.11g.
AP: The function when unit type is access point.
ST: The function when unit type is station.

Table 8.1. Initial setup list (3/4)

Setting item		Setting contents(First default)
11g	802.11g Onlymode	Disable, Enable
11g	Protect mode	Enable, Disable
11g	Protect type	CTS-only, RTS-CTS
AP	Antenna selecting	Auto, 1, 2
AP	Broadcasting speed control function	Disable, Auto, Enable
AP	Broadcasting transmission speed	Auto, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M
AP	Broadcasting transmission retry count	0, 0 to 10
AP	Broadcasting band	0, 0 to 54
AP	ESSID security	Disable, Enable
ST	Roaming threshold	15, 0 to 95 : 11a, 11g 24, 0 to 95 : 11b
ST	Prioritized APs AP 1	00-00-00-00-00-00(No designation) [Speficy the MAC address of AP]
ST	Prioritized APs AP 2	00-00-00-00-00-00(No designation) [Speficy the MAC address of AP]
ST	Prioritized APs AP 3	00-00-00-00-00-00(No designation) [Speficy the MAC address of AP]
ST	Prioritized APs AP 4	00-00-00-00-00-00(No designation) [Speficy the MAC address of AP]
ST	Prioritized APs AP 5	00-00-00-00-00-00(No designation) [Speficy the MAC address of AP]
ST	Prioritized APs Connect to other APs	Enable, Disable
AP	Maximum number of logged in devices	254, 1 to 254
	<IEEE802.11X>	
	IEEE802.1X function	Disable, Enable
	Re-authentication interval(minutes)	2, 2 to 4320
	RADIUS server1, IP address	(Set 0.0.0.0 when it is not used./IP address of authentication server.)
	RADIUS server1, Port number	1812 (UDP port number of RADIUS)
	RADIUS server1, ESSID	(Blank)
	RADIUS server1, Shared secret	(Single-byte alphanumeric characters can be up to 128 characters long. Encryption key to use between authentication server)
	RADIUS server2, IP address	(Set 0.0.0.0 when it is not used./IP address of authentication server.)
	RADIUS server2, Port number	1812 (UDP port number of RADIUS)
	RADIUS server2, ESSID	(Blank)
	RADIUS server2, Shared secret	(Single-byte alphanumeric characters can be up to 128 characters long. Encryption key to use between authentication server)
	RADIUS server3, IP address	(Set 0.0.0.0 when it is not used./IP address of authentication server.)
	RADIUS server3, Port number	1812 (UDP port number of RADIUS)
	RADIUS server3, ESSID	(Blank)
	RADIUS server3, Shared secret	(Single-byte alphanumeric characters can be up to 128 characters long. Encryption key to use between authentication server)
	RADIUS server4, IP address	(Set 0.0.0.0 when it is not used./IP address of authentication server.)
	RADIUS server4, Port number	1812 (UDP port number of RADIUS)
	RADIUS server4, ESSID	(Blank)
	RADIUS server4, Shared secret	(Single-byte alphanumeric characters can be up to 128 characters long. Encryption key to use between authentication server)

11g: The function when selecting IEEE802.11g.
AP: The function when unit type is access point.
ST: The function when unit type is station.

Table 8.1. Initial setup list (4/4)

	Setting item	Setting contents(First default)
	< Extensions >	
	Bridge Packet Control (MAX 32 entries)	Disable, Enable [List edit : MAX 32 entires]
	Network time, function	Disable, Enabled
	Network time, IP address	(IP address of network time server)
	Network time, time zone	+09:00 (Japanese time zone is between +09:00.)
	Access control	
	Access control, TELNET	Enabled, Disable
	Access control, FTP	Enabled, Disable
	Access control, WEB server	Enabled, Disable
	Access control, administrator IP	Disable, Enabled
	Access control, administrator IP address1	0.0.0.0
	Access control, administrator IP address2	0.0.0.0
	<Terminal>	
	Baud rate	9600, 1200, 2400, 4800, 19200, 38400, 57600, 115200
	<SNMP>	
	SNMP agent function	Disable, Enabled
	Community name (Single-byte alphanumeric characters can be up to 32 characters long and .the password is case sensitive.)	public
	Access permission	Read/Write, Read Only
	Trap destination IP address (1 point)	0.0.0.0
	Administrator contact information (sysContact)	(Blank), (The string can be up to 32 characters long when all the characters are single-byte characters or up to 16 characters long when they are all double-byte characters.)
	Device location (sysLocation)	(Blank), (The string can be up to 32 characters long when all the characters are single-byte characters or up to 16 characters long when they are all double-byte characters.)
	Device name (sysName)	(Blank), (The string can be up to 32 characters long when all the characters are single-byte characters or up to 16 characters long when they are all double-byte characters.)
	<Log function>	
	Log function	Disable, Enabled
	Overwriting mode	Enabled, Disable
	Beginning day/time setting Beginning day/time setting function	Disable, Enabled
	Beginning day/time setting Beginning day/time	Year Month Day Time Minutes
	Log setting in detail log-in	ON, OFF
	Log setting in detail log-out	ON, OFF
	Log setting in detail log-in rejection	ON, OFF
	Log setting in detail Roaming	ON, OFF

11g: The function when selecting IEEE802.11g.
AP: The function when unit type is access point.
ST: The function when unit type is station.

Setup / Status Items list

WWW brouser

Setting
|– Basic setting

|– Ethernet
|– Wireless LAN
  |– Basis
  |– Details
  |_ Security
|– IEEE802.1X
|– Extensions
|– Function
|– SNMP
|– Log function
|_ Setup list
Status
|– Environmental information
|– Interface
|– Wireless LAN
|– MAC address table
|_ Log information
Meintenance
|– Firware version up

Terminal

Fxit
Setting
|– Host name
|– DHCP client
|– IP address
|– Subnet mask
|– Default gateway
|– Access point construction
|– Access point type
|– IP address of the masuter AP
|– IP address of the backup AP
|– Ethernet
| |– Port speed
| |_ Link down sense
|– Wireless
| |– Interface
| |– Wireless LAN standard
| |– Wireless connection mode
| |– Unit type
| |– Access point type
| |– IP address of the masuter AP
| |– IP address of the backup AP
| |– ESSDI
| |–Channel No.
| |–Transmission rate
| |– Transmission output
| |– Security
| | |– Encryption
| | |– Default transmitting key
| | |– Key1
| | |– Key2
| | |– Key3
| | |– Key4
| | |– Wireless security connection(WSL)
| | |– ESSID security
| | |– MAC address filtering
| | |_ MAC address filtering list
| |_ Extensions
| |– Roaming threshold
| |– Prioritized APs
| | |– Prioritized APs 1
| | |– Prioritized APs 2
| | |– Prioritized APs 3
| | |– Prioritized APs 4
| | |– Prioritized APs 5
| | |_ Connect to other APs
| |– Statistic node address
| |– Maximum number of logged in devices
| |– Broadcasting speed control
| |– Broadcasting transmission speed
| |– Broadcasting transmission retry count
| |– Broadcasting band
| |– Beacon tr ansmission speed
|– Antenna selecting
|_ 802.11g paremeter
| |– 802.11g-Only mode
| |– Protect mode
| |_ Protect type
|– IEEE802.1X
| |– IEEE802.1X function
| |– Re-authentication interval(minutes)
| |_ RADIUS server list
|– Extensions
| |– Bridge Packet Control
| |– Bridge packet list
| |– Network type
| |– Time server IP address
| |– Time zone
| |_ Access control
| |– TELNET server function
| |– FTP server function
| |– WEB server function
| |– Access from wireless
| |– Administrator IP designation
| |– Administrator IP address1
| |_ Administrator IP address2
|– SNMP
| |– SNMP agent function
| |– Community
| |– Access permission
| |– Trap destination IP address
| |– sysContact
| |– sysName
| |_ sysLocation
|_ Log
|– Log function
|– Overwriting mode
|– Beginning day/time
|– Detailed setting
|– Log-in
|– Log-out
|– Log-in rejection
|– Roaming

Writing
Re-start
|– Cold boot
|_ Warm boot
System parameter
|– Password
|_ Date / Time
Download
|– Farmware
|_ Setting file
Up loading
|– Setting file
|_ Log file
Default
Status
|– Environment
| |– Lauder version
| |– Firmware version
| |– Hardware version
| |– Ethenet address
| |– Wireless MAC address
| |– IP address
| |– Subnet mask
| |_Default gateway
|– Interface
|– Wireless
| |– Wireless LAN specification
| |– Wireless communication mode
| |– Unit type
| |– Module ID
| |– Wireless MAC address
| |– Belonging A P
| |– ESSID
| |– Channel no.
| |– Transmission rate
| |– Receiving rate
| |– RSSI
| |– Integrated information
| |– Wireless node table
| |– Access point administration
| |– Integrated information
| |– Access point table
| |_ Station table
|– MAC address table
|– DHCP
|– MIB
| |– system
| |– interfaces
| |– at
| |– ip
| |– icmp
| |– tcp
| |– udp
| |– snmp
|_ Log

Product Specifications

Physical Specifications

Table 8.2. Product Specifications

Specification			FX-DS540-APDL
Wired LAN unit	Ethernet standard		IEEE802.3(10BASE-T) IEEE802.3u(100BASE-TX)
	Data transmission speed		10/100Mbps
	Access method		CSMA/CD
	Communication type		Half Duplex, Full Duplex
	Number of ports		1(10BASE-T/100BASE-TX)
Wireless LAN unit	IEEE802.11a	Transmission format	IEEE802.11a standard OFDM (Orthogonal Frequency Division Multiplexing)
		Channel	13ch(36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165)
		Data transmission speed	54, 48, 36, 24, 18, 12, 9, 6Mbps (Fix / Auto)
		Access method	CSMA/CA + ACK(RTS/CTS)
		Wireless category	ISM Baud (5.150 to 5.350GHz, 5.725 to 5.825GHz)
		Aerial power	10mW/MHz or less
		Security	WEP(64/128/152Bit) and AES(128Bit) / WSL(Wireless Security Link) Compatible of using both WEP, AES and WSL. MAC address filtering, IEEE802.1X
	IEEE802.11b	Transmission format	It conforms to the IEEE802.11b CCK, QPSK, BPSK form
		Channel	11ch(1 to 11)
		Data transmission speed	11, 5.5, 2, 1Mbps(Fix / Auto)
		Access method	CSMA/CA + ACK(RTS/CTS)
		Wireless category	ISM Baud (2.4 to 2.4835GHz)
		Aerial power	10mW/MHz or less
		Security	WEP(64/128/152Bit) and AES(128Bit) / WSL(Wireless Security Link). Compatible of using both WEP, AES and WSL., MAC address filtering, IEEE802.1X
	IEEE802.11g	Transmission format	IEEE802.11g standard OFDM (Orthogonal Frequency Division Multiplexing)
		Channel	11ch (1 to 11)
		Data transmission speed	54, 48, 36, 24, 18, 12, 9, 6Mbps(Fix / Auto)
		Access method	CSMA/CA + ACK(RTS/CTS)
		Wireless category	ISM Baud (2.4 to 2.4835GHz)
		Aerial power	10mW/MHz or less
		Security	WEP(64/128/152Bit) and AES(128Bit) / WSL(Wireless Security Link). Compatible of using both WEP, AES and WSL. MAC address filtering, IEEE802.1X
Antenna			Chip-type, diversity antenna(Built-in)
External dimension(mm)			81(W) x 26.5(D) x 175(H)
Weitht			0.2kg
Length of AC adapter cable			1.5m

Software Specifications

Table 8.3. Software Specifications

Specification	FX-DS540-APDL
Protocols	IP(RFC791), ICMP(RFC792), UDP(RFC768), TCP(RFC793,896), ARP(RFC826), HTTPD(RFC1866), TELNET(RFC), FTPD(RFC959), TFTP(RFC783,906), DHCP(RFC2131)

Environmental Specifications for Installing the FX-DS540-APDL

Table 8.4. Environmental Specifications (Environmental Specs)

Specification	FX-DS540-APDL
DC supply voltage(Input)	3.3VDC±5% 1.3A(Max.) (AC adapter(bundled))
Operating temperature	0 to 50°C
Operating humidity	10 to 90%RH (No condensation)
Airborne dust	Not extreme
Corrosive gases	None
Permitted transient power failure	17ms or less (100VAC@25°C) An automatic reset is performed when low voltage is detected.

Table 8.5. AC Adapter Environmental Conditions (Environmental Specs)

Specification	FX-DS540-APDL's accessory
AC supply voltage(Input)	100 to 240VAC 0.3A(Max.)
AC supply frequency	47 to 63Hz
DC supply voltage(Output)	3.3VDC±5% 1.5 A(Max.)
Operating temperature	0 to 50°C
Operating humidity	20 to 90%RH (No condensation)
Airborne dust	Not extreme
Corrosive gases	None

External Dimensions

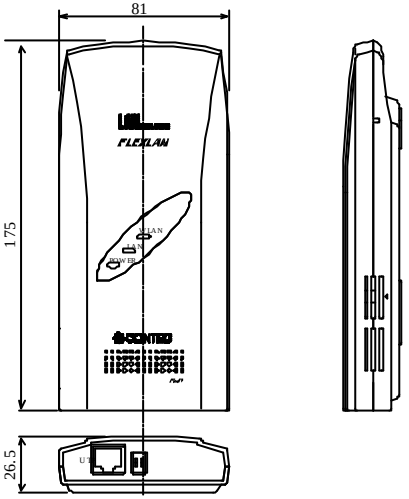


Figure 8.2. Exte rnal Dimensions(FX-DS540-APDL)

LEDs

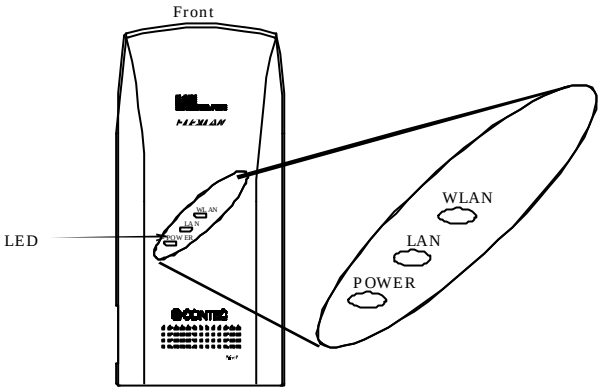


Figure 8.3. FX-DS540-APDL(Front)

During Normal Operation

Table 8.6. During Normal Operation

Name	Status	Indicator
POWER	ON	Indicates that the device is operating.
	Flashing	Indicates that the device is being started (going to operate after the power switch was turned on)
LAN	ON	Indicates that a wired LAN has been connected.
	Flashing	Indicates the transmitting / receiving between terminal connected by the wired LAN and the data.
	OFF	Indicates that a wired LAN has been no connected.
WLAN	ON	It displays that user unit is logged-in (When access point). It displays that user unit is logged-in access point (When station).
	Flashing	Indicates the transmitting / receiving between terminal connected by the wireless LAN and the data.
	OFF	It displays that user unit is not logged-in (When access point). It displays that user unit is not logged-in access point (When station).

Others

Table 8.7. When Writing Firmware

Name	Status	Indicator
POWER	Flashing simultaneously	Writing firmware is in progress
LAN		
WLAN		

Table 8.8. Error Display(The POWER LED blinks twice)

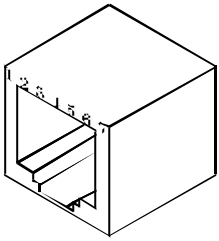
Name	Status	Indicator
LAN	Flashing	Wired LAN error
WLAN	Flashing	Wireless LAN error

Input/Output Interface

Pin Assignment for UTP Port

Table 8.9. UTP Port Pin Assignments

Pin.No	Signal
1	TD +
2	TD –
3	RD +
4	Not used *
5	Not used *
6	RD –
7	Not used *
8	Not used *



* : When supplying the power form UTP cable.

4, 7pin LANVCC(+24)

5, 8pin LANGND(0V)

Comparison to FLEXLAN DS110 series terminology

The table below compares terms used for the FLEXLAN DS540 series and those for the FLEXLAN DS110 series.

Table 8.10. FLEXLAN DS540/DS110 terminology comparison table

FLEXLAN DS540series		FLEXLN DS110series
Name	Abbreviation	
Wireless Link Mode	WLM	Operating Mode
Standard Infrastructure	if-std	Standard Mode
Compatible Infrastructure	if-comp	Interconnection Mode
Advanced Infrastructure	if-adv	Integrated mode, Standard Mode + Interconnection Mode, Interconnection Mode Plus
Simple Adhoc	ad-simp	Simple Mode, Adhoc
Compatible Adhoc	ad-comp	Compatible Adhoc
Wireless Security Link	WSL	WEP, Standard Mode

Glossary

SQE(Signal Quality Error) (Heartbeat)

This uses the same signal line as the collision signal for the purpose of notifying the transmitting terminal that the packets sent from the terminal are sent correctly over the cable.

PPP(Point to Point Protocol)

A protocol for communicating using TCP/IP over a serial line.

IEEE(Institute of Electrical Electronics Engineers)

"I-triple-E," involved in a wide range of fields from communications and computer to medicine and biology, with primary activities related to publishing articles and sponsoring conferences, but also recommending and setting of standards. The organization sponsoring Committee 802, which is responsible for LAN related matters.

IEEE802.11/ IEEE802.11a/IEEE802.11b/IEEE802.11g

The wireless LAN standard established by the IEEE.

OFDM(Orthogonal Frequency Division Multiplexing)

OFDM is a modulation technique for transmission using different bandwidths. It is characterized by immunity to fading and multipath.

MIB(Management Information Base)

The value of a MIB is determined by the Internet standard control information structure.

SNMP(Sinmple Network Management Protcol)

A function necessary for network control, provides three functions: Get (acquire), Set (modify), and Trap (notify event). Conceived as an easily installable control protocol that places as little load on the network as possible.

Diversity

A method of using multiple antennas, and selecting the one with the best receiving conditions.

Router

A device for relaying between LAN's. The router determines data addresses by the combination of a network address assigned to the network and an individual computer address. Used particularly in medium-scale and larger LAN systems with very large number of clients, to reduce traffic (congestion) on communication lines.

Bridge

A device for relaying between LAN's. The bridge determines whether to relay data based on the address of the computer to which the data is being sent. It can be used to connect networks having different protocols, or when data for broadcast to all computers is received, can send this to all connected networks.

Brouter

A router with an added bridge function. When data received from one network cannot be processed by the router because a different protocol is used, the bridge function can be used to send the data on to the other network.

LAN(Local Area Network)

A network configured from mutual connections between computers within a limited area. Also called an "intranet" or "business or regional data communications network."

RSSI(Receive Signal Strength Indication)

A numeric indicator of incoming signal strength.

Spectrum diffusion transmission

A method of transmission in which signals that are normally transmitted over a given limited frequency band undergo narrow band modulation (primary modulation), then again diffuse modulation (secondary modulation) to intentionally diffuse the signal over a broad frequency spectrum.

DS(Direct Sequence)

A type of spectrum diffusion signal using narrow band modulation with phase modulation, in which the diffusion is by means of phase modulation using a broad band diffusion signal (pseudo random strings).

CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance)

CSMA is a method of avoiding collision by which wireless terminals listen before transmitting and do not transmit if they can year transmissions from other wireless terminals. CSMA/CA is CSMA plus additional collision avoidance functions.

Hidden Terminal Problem

When wireless terminals are farther apart then their electric signals can reach, or their signals are obstructed by objects, neither may be able to receive the other's signals. Any two such wireless terminals are said to be hidden from each other. In Ad Hoc mode, because the carrier sense function is not effective between hidden terminals there is a higher probability of collisions and throughput (the volume of information sent in a given time interval) is reduced.

RTS(Reqest To Send)

In communication via AP, transmission is controlled by CSMA/CA plus RTS. In RTS, a wireless terminal asks the AP if it is all right to transmit, and only transmits after an OK-to-send acknowledgement signal is returned. This serves to avoid unnecessary collisions when hidden terminals exist because hidden terminals cannot transmit.

Roaming

This term has the same meaning as roaming for a portable phone or PHS. The AP is in the role commonly called the 'antenna/base station' for the phone or PHS, and the user unit is in the role of the phone itself.

Peer-To-Peer

A network in which two or more nodes can communicate directly with each other without going through another device.

AP(ACCESS POINT)

Access point. In the FLEXLAN DS540 series, the access point serves as a bridge between a wired network and a wireless network and provides IP tunneling; it is indispensable for the versatility and scalability of the wireless network.

User Unit

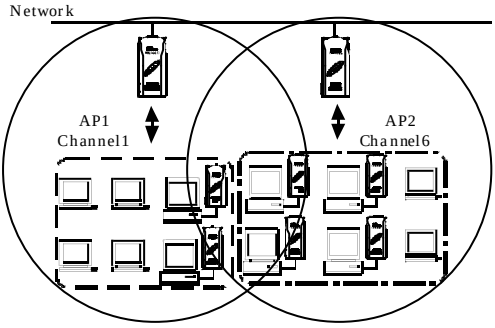
In FLEXLAN DS540 series, user unit means the device loading FX-DS540-PCC/FX-DS540-PCC2/FX-DS540-PCD.

ESSID(Extended Service Set ID)

In the FLEXLAN DS540 series, the ESS ID is like a name assigned to the wireless LAN network to which a unit belongs. The same name must not be given to more than one wireless terminal. Conversely, a wireless network can be partitioned by using different ESS ID names.

Channel

This has the same meaning as in TV and radio terminology. The 5.15 to 5.35 GHz band (namely 36, 40, 44, 48, 52, 56, 60, 64, total : 8channels) and the 5.725 to 5.825 GHz band (namely 149, 153, 157, 161, 165, : 5channles) used by this products is stipulated by IEEE802.11a to be divided into a total of thirteen channles.
The 2.4 to 2.4835GHz band (namely from 1 to 11, total : 11channels) used by this products is stipulated by IEEE802.11b/g to be divided into a total of eleven channles.
Radio transceivers different in channel cannot communicate with each other even when they belong to the same network.



Atheros, ABG and Total 802.11 are trademarks
of Atheros Communications, Inc.
CONTEC CO.,LTD is using the Atheros trademarks
with permission from and on behalf of Atheros Communications, Inc.

FX-DS540-APDL

User's Manual

CONTEC CO., LTD. December 2003 Edition

3-9-31, Himesato, Nishiyodogawa-ku, Osaka 555-0025, Japan
Japanese http://www.contec.co.jp/
English http://www.contec.com/
Chinese http://www.contec.com.cn/

No part of this document may be copied or reproduced in any form by any means without prior written consent of CONTEC CO., LTD. [08062003]

[12222003] Management No. A-46-824
Parts No. LYDE681