LAN-HELPER

IEEE802.11a/b/g &
PoE Conform
Micro Access Point

FX-DS540-APDL2-U

User’s Manual

CONTEC CO.,LTD.

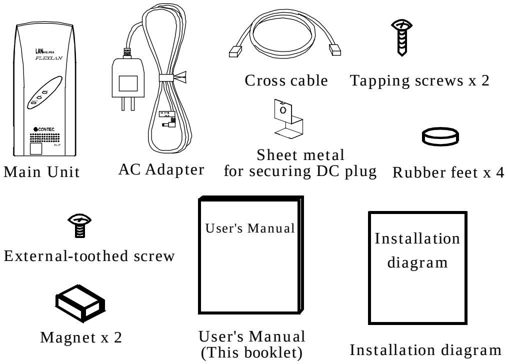
Check Your Package

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 …1
- Cross cable(Cable length1.5m) *1 …1
- Sheet metal for securing DC jack …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
- User’s Manual (this booklet) …1

*1 Please do not use it for power supply to the IEEE802.3af compliant product.



Copyright

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

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

Full term	Term used in this manual
FX-DS540-APDL2-U FX-DS540-APDL(af)-U FX-DS540-APDL-U FX-DS540-APDL-NR5-U FX-DS540-APDL-NR520-U FX-DS540-STB-M-U FX-DS540-STB-NR5202-U	Access point/AP Station/ST
A device with the wireless function	User unit / Wireless terminal
Personal computer	PC

Table of Contents

1. Before Using the Product

About the FX-DS540-APDL2-U

The FX-DS540-APDL2-U is a small & light typed wireless LAN Access point. It conforms to the wireless LAN standard specification IEEE802.11a/IEEE802.11b/IEEE802.11g.
It has a variety of functions such as an advanced security function supporting WPA, XR function, Super A/G function, WDS function, and QoS. The power supply methods include the attached AC adaptor and PoE, allowing you to use an IEEE802.3af-compliant device to supply power from a LAN cable.

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

IEEE802.11a/IEEE802.11b/IEEE802.11g-compliant access point
The channel to be used varies depending on the country in which the product is used.

High-level security features integrated
Conforming to a latest security standard of WPA and supporting 802.1X authentication as well as AES-based secure encrypted communications. Proprietary features such as WSL as a proprietary encryption technology available along with AES and WEP other than “MAC address filtering”, “ESSID hide” and “ANY ID reject”.

IP tunneling feature integrated *1
Enabling communication even at a roaming destination beyond the router without making any changes to network configuration.

Offering a choice of three wireless connection modes for different network configurations

Standard *2	:	Mode to use the features unique to the FLEXLAN Series, such as IP tunneling and WSL
Compatible *2	:	Mode for heterogeneous use along with other vendors' wireless equipment supporting Wi-Fi *3
Advanced *2	:	Mode to allow wireless LAN terminals both in standard mode and compatible mode to be connected on the network at the same time

IEEE802.3af-compliant
Capable of power-supplied through a LAN cable by using an IEEE802.3af compliant device

XR feature integrated *4
XR feature providing stable connectivity even in poor-radio or obstructed environments

Super A/G feature integrated
Super A/G feature improving the speed of communication between supported models.

WDS feature integrated
Up to six units can be connected wirelessly between access points.

QoS support
Supporting QoS (Quality of Service) that allocates bandwidths for specific types of communication, such as VoIP to guarantee communication qualities.

SNMP agent feature integrated
Enabling network management using SNMP supported network management software (such as CONTEC SNMPc). MIBII and private MIB are supported.

Protect Mode available when using IEEE802.11g
Stable communications even when IEEE802.11b products are also used. Communication speeds are improved for IEEE802.11g products.

Others

- Introducing the Diversity Method with a built-in chip antenna.
- Easy configuration and management using a Web browser. Assorted maintenance methods are available to different systems and applications, including FTP commands, TELNET.

*1 The IP tunneling feature is available in standard wireless connection mode.

*2 The official names are as follows :

Standard ••• Standard/infrastructure
Compatible ••• Compatible/infrastructure
Advanced ••• Advanced/infrastructure

*3 This mode does not assure inter-connectivity with other vendors' Wi-Fi products.

*4 The XR feature can be used only when both of the access point and station in the wireless LAN support the XR feature.

The latest versions of software including firmware can be downloaded from the CONTEC’s web site.

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.

Usage limitation

This product has not been developed or manufactured to be used in systems including the equipment which is directly related to human lives *1 or the equipment which involves human safety and may significantly affect the maintenance of public functions *2. Therefore, do not use the product for such purposes. In addition, do not use the product within 40cm from a human body on a regular basis.

*1 : Medical devices such as life-support equipment and devices used in an operating theater.

*2 : Main control systems at nuclear power stations, safety maintenance systems at nuclear facilities, other important safety-related systems, operation control systems within group transport systems, air-traffic control systems, etc.

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, scientific, 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 mobile-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.

CAUTION : To comply with FCC RF exposure compliance requirements, a separation distance of at least 5 cm must be maintained between this device and all persons.

Notes

- FCC WARNING : Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- 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.
- In according with 47 CFR Part15.407 (e) U-NII devices operating in 5.15-5.25GHz frequency bands are restricted to indoor operations only.
- This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.
- This equipment complies with FCC radiation exposure limits set forth for uncontrolled equipment and meets the FCC radio frequency (RF) Exposure Guidelines in Supplement C to OET65. This equipment should be installed and operated with at least 20cm and more between the radiator and person's body (excluding extremities : hands, wrists, feet and legs).

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.
- In the event of failure or abnormality, contact your retailer.
- Be careful not to let the external supply voltage or drive current exceed the rating.
- Do not 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 - 50°C

Humidity

10 - 90%RH (No condensation)

Corrosive gases

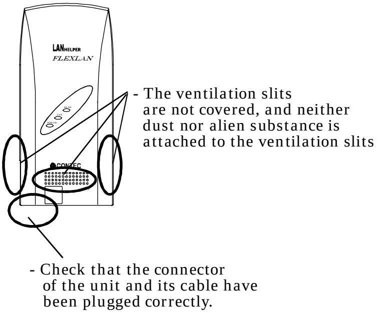
None

Floating dust particles

Not to be excessive

Inspection

Inspect the product periodically as follows to use it safely.



- The ventilation slits are not covered, and neither dust nor alien substance is attached to the ventilation slits

- Check that the connector of the unit and its cable have been plugged correctly.

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.

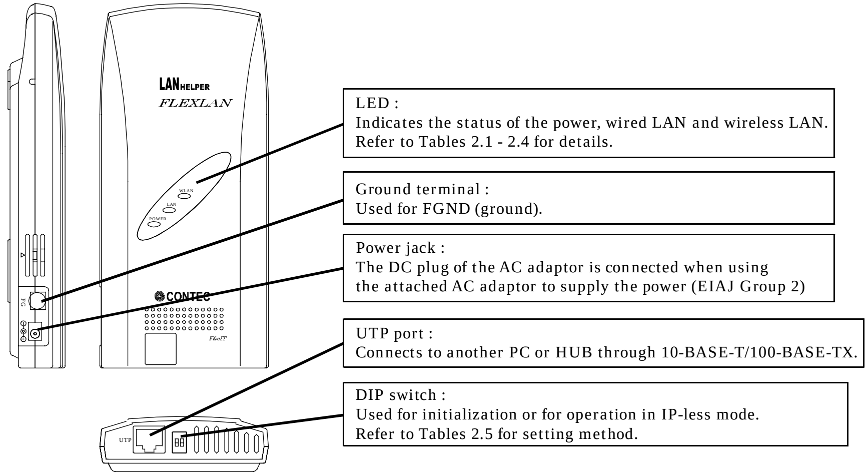
Disposal

When disposing of the product, follow the disposal procedures stipulated under the relevant laws and municipal ordinances.

2. Setup

The antenna must be mounted and properly installed before setting up this product. Follow the setup procedure for the product shown below.

Component Locations



LED :
Indicates the status of the power, wired LAN and wireless LAN.
Refer to Tables 2.1 - 2.4 for details.

Ground terminal :
Used for FGND (ground).

Power jack :
The DC plug of the AC adaptor is connected when using
the attached AC adaptor to supply the power (EIAJ Group 2)

UTP port :
Connects to another PC or HUB through 10-BASE-T/100-BASE-TX.

DIP switch :
Used for initialization or for operation in IP-less mode.
Refer to Tables 2.5 for setting method.

Figure 2.1. Component Locations

LED display

Table 2.1. 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 data is being transmitted to or received from the device connected through wireless LAN.
	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).

Table 2.2. When Writing File

Name	Status	Indicator
POWER LAN WLAN	Flashing simultaneously	Writing file is in progress *1

*1 Except writing of log files (no blinking)

Table 2.3. Error Display

LED name	Status	Display contents
POWER	Blinking twice	Wireless LAN error
WLAN	On	
POWER	Blinking twice	Wired LAN error
LAN	On	

Table 2.4. When Checking Radar Waves during Startup (DFS)

LED name	Status	Display contents
POWER	Blinking	Checking radar waves upon the startup of this product (AP setup : when channels 52, 56, 60 and 64 are used.)
WLAN	Blinking	

DIP switches

Table 2.5. DIP Switches

	ON	OFF	Operation / function
1	INIT	-	Used when initializing this product (restoring the default settings). 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. Reboot the product when the light stops blinking. *1
2	IP LESS	-	Turning this switch on, operating can be done without setting the IP address on the AP. Used when not allocating an IP address to this product on the setup of a station. In this time, you cannot use the setup by Web browser or SNMP agent function.

*1 The blinking continues for a little while after the product is switched off during initialization by switching on and off the INIT switch. This indicates internal memory files are being deleted. The internal memory files may be damaged and the product may not start up properly if the power is switched off before the blinking stops. Always reboot the product after the blinking stops.

Checking the Network Addresses

The Ethernet (wired LAN), wireless LAN MAC address and IP address are defined on the housing seal (on the bottom) of this product. Write down the MAC addresses for Ethernet and wireless LAN in the following table as they are device-individual values and may be required for future setup.

Table 2.6. Network address

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

Power Supply

There are two power supply methods for this product : using the attached AC adaptor; and supplying power from an IEEE802.3af-compatible power supply unit using a LAN cable.

Using the attached AC adapter

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

Using the LAN cable

The FX-D540-APDL2-U can be power-supplied through a LAN cable from an IEEE802.3af-compliant power supply unit.

For details, refer to the power supply unit.

The following gives an example of connection

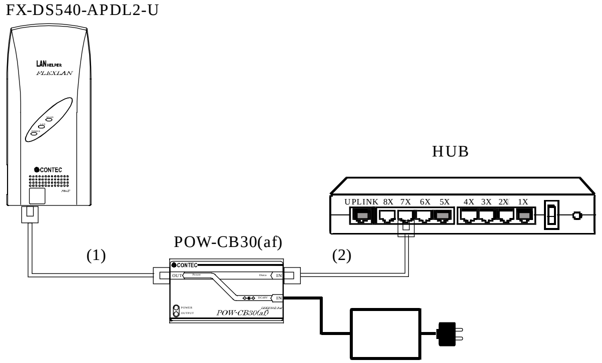


Figure 2.2. Power Supply Connection

Connect a LAN cable in Category 5 or greater to use IEEE802.3af-compliant power supply.

⚠ CAUTION

- The overall length of the LAN cable between the power supply destination and the hub must be up to 100 m.
  Route the cabling such that (1) + (2) is 100 (m) or less.
- Do not connect the output LAN cable to any IEEE802.3af non-compliant device as doing so can cause device faults or accidents.
- When supplying power to the unit via the LAN cable, do not use the bundled AC adapter and do not touch the power jack position.
- Do not connect an AC adapter other than the bundled one as doing so can cause device faults or accidents.
- Once the unit has been powered with the AC adapter, do not turn the DC plug or vibrate the AC adapter.

Ground the FX-DS540-APDL2-U

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.

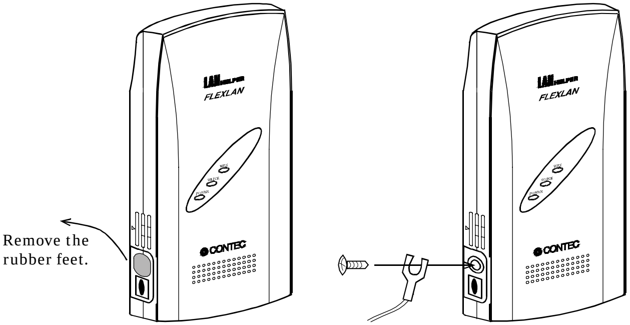


Figure 2.3. Ground the FX-D540-APDL2-U

Securing the DC plug

Using the DC plug clamp bundled standard with the FX-DS540-APDL2-U stops the DC plug from being removed even when the DC cable is loaded, preventing an abrupt power failure.

Fasten the clamp using the bundled external tooth lock screws to secure the DC plug.

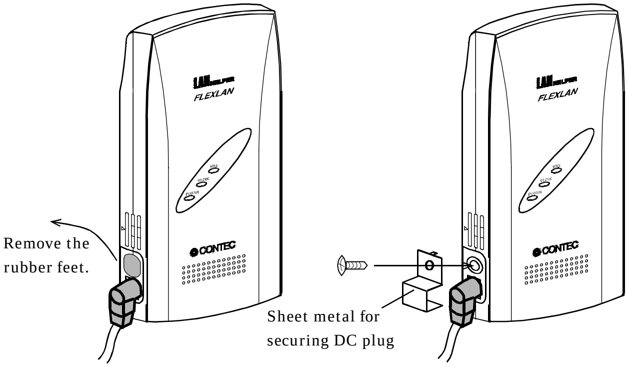


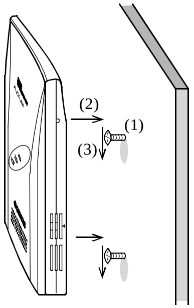
Figure 2.4. Securing the DC plug

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 main unit case such that the two screws on the wall insert into the wall-mounted holed on the case.
(3) Slide the main unit down to hold it in place.

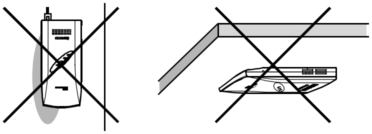
Figure 2.5. Wall Installation

⚠ 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-APDL2-U 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 2.6, 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.

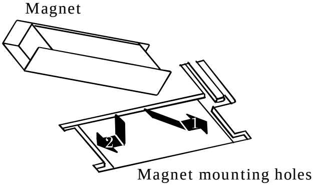


Figure 2.6. Attaching Magnets

To remove, slide the magnet in the direction of arrow 1 in Figure 2.7, then lift in the direction of arrow 2.

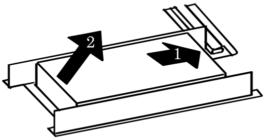


Figure 2.7. Removing Magnets

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.

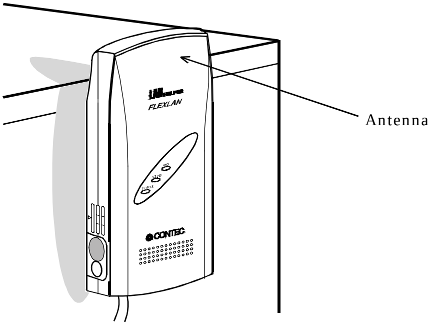


Figure 2.8. Mounting on Steel Desks

⚠ 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.

Wired LAN Connection

Connect your LAN cable to the UTP port on the AP.

A cross cable is used to connect the product to the UP-LINK port of a PC or HUB.   A straight cable is used to connect the product to the normal port of a HUB.

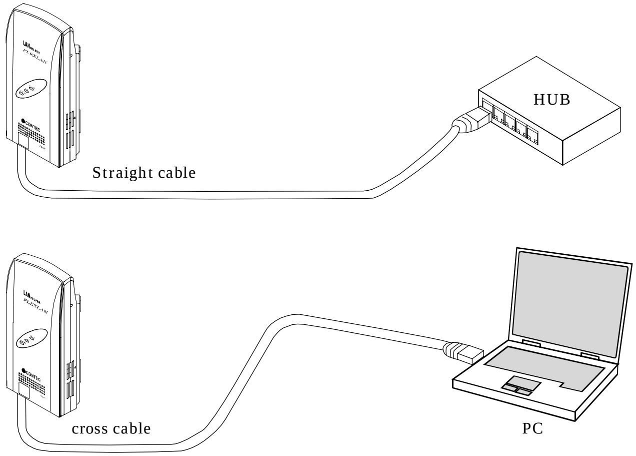


Figure 2.9.   Wired LAN Connection

⚠ CAUTION

- Cable length between this product and PC, HUB is 100 m or less.
- Use LAN cable having category 3 - 6 specifications.

3. Connection to Devices and Setup Methods

This product is set up via a network using a Web browser or TELNET. Follow the setup procedure below once the product is set up.

Setup Methods

Although the FX-DS540-APDL2-U can be set up precisely to construct an advanced wireless LAN environment, there are two different setup methods available : web browser and TELNET.

Web browser

- Provides an easy to use graphical interface.

TELNET

- Text-only display without a “help” section. However, you will find it faster to perform setup once you get used to it.

Preparation before Setup

You must use a PC which can be connected to a network as the product is set up via the network.
The setup is performed by connecting a PC for setup purposes and then using a Web browser or TELNET.

Connecting for the first time

(1) Connect this product to PC on a wired LAN.

(2) Select an IP address 10.XXX.XXX.XXX (e.g. 10.0.0.1) for the PC, which is not the same address as for this product. And then set the subnet mask to 255.0.0.0.

Windows :
Click [Start] - [Control Panel] - [Network Connection], and then right-click the icon for local area connection to open up the [Properties] screen. Select [Internet Protocol (TCP/IP)] from the [General] tab and click [Properties]. Set up the IP address and subnet mask, and if necessary, default gateway and DNS server on the opened [Internet protocol (TCP/IP) properties] window.

Changing the settings

(1) Connect this product to PC on a wired LAN.

(2) Set the network address of the PC to the same network address as for this product.

Setup Using a Web Browser

This section describes the setup method using a Web browser. The following Web browsers can be used (recommended Web browsers). Note that a proper display may not be shown on any browser other than the following ones.

Enable the JavaScript function in the browser setting as it is used.

Supported web browsers (recommended)

- Microsoft Internet Explorer 5.5 or higher
- Netscape Navigator 7 or higher
- Mozilla Firefox 1.0 or higher

Setting the Browser

You may have to change the browser settings as well as the IP address and subnet mask for the PC to be connected to this product via the network.

Changing browser settings

(1) Networks at companies and schools may use broswers with proxy settings. Proxy is not required as a PC is used to set up the product, which is on a local network. Disable the proxy settings temporarily when setting up this product on a Web browser.
For information about how to disable proxy settings, refer to the help section of the Web browser used.

(2) Enable JavaScript.
For information about how to enable JavaScript, refer to the help section of the Web browser used.

⚠ CAUTION

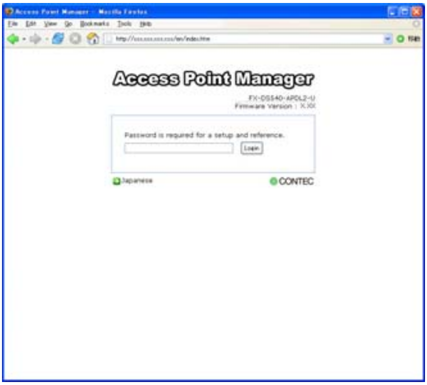
When the Web browser settings have been changed, restore the original browser settings upon the completion of setup of this product.

Connecting to This Product Using Web Browser

Start up a Web browser and enter the IP address of this product after “http : //” in the address bar.
If connecting for the first time, enter the default IP address.　When the default setting IPaddress is 10.144.0.1, enter as follows.

http : //10.144.0.1/

Connecting to this product displays the “Access Point Manager” login screen, shown below.
If the login screen is not displayed, the IP address setting for PC, browser settings, or the URL entered in the address bar of the browser may be incorrect.


Access Point Manager - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://xxx.xxx.xxx.xxx/en/index.htm
Access Point Manager
FX-DS540-APDL2-U
Firmware Version : X.XX
Login
Japanese
CONTEC

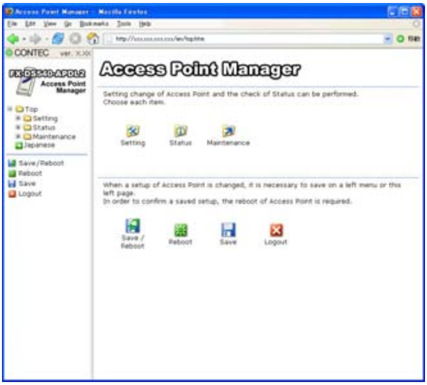
Password is required for a setup and reference.

Figure 3.1. Login screen

Enter a password on the login screen and then click “Login” to log in.

When connecting for the first time, do not enter any password and just click “Login” as no password has been set at the factory.

If the login is successful, the following setup screen will be displayed after a little while.



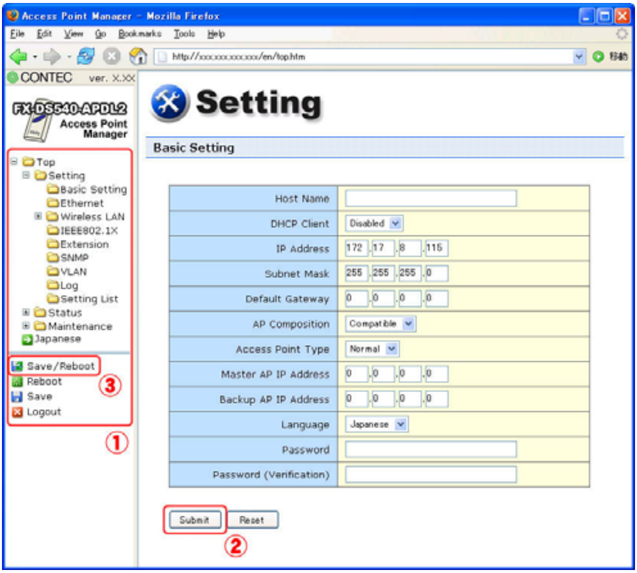
Setting change of Access Point and the check of Status can be performed.
Choose each item.

When a setup of Access Point is changed, it is necessary to save on a left menu or this left page.
In order to confirm a saved setup, the reboot of Access Point is required.

Figure 3.2. Screen after Login

Setup Using Web Browser

Select “Setting” in the left-hand menu ((1) in Figure 3.3) and further select the desired setting items from the opened menu. Information such as setting items will be displayed in the right-hand frame.



Host Name	
DHCP Client	Disabled
IP Address	172 . 17 . 8 . 115
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	0 . 0 . 0 . 0
AP Composition	Compatible
Access Point Type	Normal
Master AP IP Address	0 . 0 . 0 . 0
Backup AP IP Address	0 . 0 . 0 . 0
Language	Japanese
Password	
Password (Verification)	

Figure 3.3. Setting by Access Point Manager

Make sure to click “Submit” ((2) in Figure 3.3) after changing settings on each page to temporarily save the settings in this product.

The settings become valid when the product is restarted after all the setup procedure is completed and the settings are stored. Click “Save/Reboot” ((3) in Figure 3.3) on the left-hand menu.

There will be no problem if you just save the settings now but reboot the product later when necessary. In this case, saving the settings does not actually change the settings of the product. Therefore, make sure to reboot the product later.

For details on setting item, please refer to “chapter 4 Setup and Status Display”.

⚠ CAUTION

It takes approximately 5 - 10 seconds to save settings (writing to internal flash memory). During that period, the LEDs for POWER, LAN and WLAN at the front part of the main unit blink simultaneously. Do not reboot or turn off the product until the screen indicates the completion of the saving process.

The setup file data and firmware data may be damaged and the product may not operate properly if it is rebooted or switched off during the saving process.

Setup Using TELNET

This section describes how to perform setup using TELNET. This procedure requires an application in which TELNET can be used. In Windows, “Command Prompt” can be used.

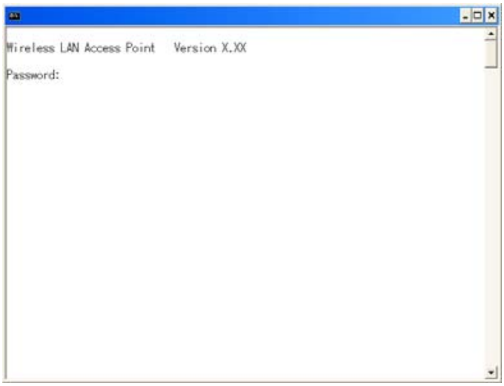
Connecting to an FX-DS540-APDL2-U Using the TELNET

Start up an application in which TELNET can be used (e.g. Command Prompt) and enter the IP address of this product after the telnet command. When connecting for the first time, enter the default IP address. For example, if the default IP address of the AP is [10.144.0.1], enter the following :

```
telnet 10.144.0.1
```

The following login screen is displayed when connected to this product.

If the login screen is not displayed, the IP address setting for the PC may be incorrect.



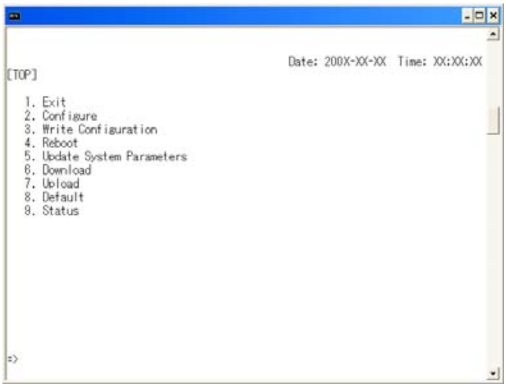
```
Wireless LAN Access Point    Version X.XX

Password:
```

Figure 3.4. Login Screen

Enter a password on the login screen and then click “Login” to log in.

When connecting for the first time, do not enter any password and just click “Login” as no password has been set at the factory.

If the login is successful, the following screen will be displayed after a little while.



```
                                            Date: 200X-XX-XX  Time: XX:XX:XX
[TOP]

   1. Exit
   2. Configure
   3. Write Configuration
   4. Reboot
   5. Update System Parameters
   6. Download
   7. Upload
   8. Default
   9. Status




=>
```

Figure 3.5.   Screen after TELNET Login

⚠ CAUTION

”Shift JIS” is used as the character code displayed during TELNET connection.   Check the character code of the TELNET application if the characters become garbled.

Setup Using TELNET

After login, enter the number of the item shown in the top menu depending on the desired execution, and then press “Enter”.　To perform configuration, enter “2” for “Configure”.
The items in the top menu are as follows.

Table 3.1.　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	Used to check the setting details and the status after startup.

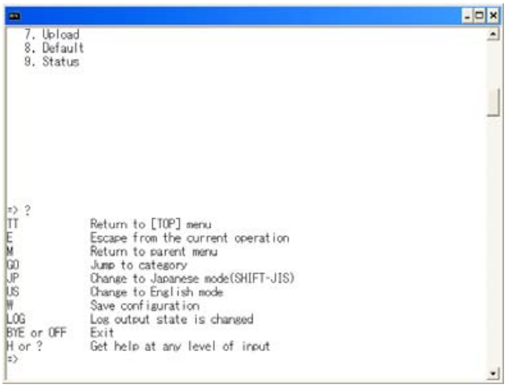
Each item also has further subdivided sub-items. Enter the number of the desired sub-item.

You will be asked to enter a value after selecting a setting sub-item.　Enter an appropriate value.
A list of the values which should be entered can be displayed by entering “H” or “?” when entering a value.　Refer to “H/?” when you do not know which value to enter.

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)



```
   7. Upload
   8. Default
   9. Status







=> ?
TT           Return to [TOP] menu
E            Escape from the current operation
M            Return to parent menu
GO           Jump to category
JP           Change to Japanese mode(SHIFT-JIS)
US           Change to English mode
W            Save configuration
LOG          Log output state is changed
BYE or OFF   Exit
H or ?       Get help at any level of input
=>
```

Figure 3.6. Help Screen

⚠ CAUTION

It takes approximately 5 - 10 seconds to save settings (writing to internal flash memory). During that period, the LEDs for POWER, LAN and WLAN at the front part of the main unit blink simultaneously. Do not reboot or turn off the product until the screen indicates the completion of the saving process.

The setup file data and firmware data may be damaged and the product may not operate properly if it is rebooted or switched off during the saving process.

4. Setup and Status Display

This chapter describes how to setup the AP using a web browser, explains each setting item and status display.　Always read Chapter 2 “Setup” and Chapter 3 “Connection to Devices and Setup Methods” for preparation before performing setup or viewing the status.
This section describes how to perform setup using a web browser.

Settings

Basic setting

Host Name

Enter the host name of the product using 31 or less single-byte alphanumeric characters.　Assigning a name to an AP makes it easier to identify on the network.

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

Specify the IP address of the AP.　Make sure to perform this setting when not enabling the DHCP client.　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

AP Composition

Sets the Access point composition.　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　:　Compatible

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

Master AP IP Address

Specify the IP address of the wireless LAN device that serves as the master.

Factory default setting : 0.0.0.0

Backup AP IP Address

When the wireless LAN device for backup exists, specify its IP address.

Factory default setting : 0.0.0.0

Language

Select either “Japanese” or “English” for the WEB setup screen and TELNET setup display language.

Factory default setting : English

Password

Set a password. Enter a string of up to 31 single-byte alphanumeric characters. The password is case sensitive.

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.

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 Dense

Enabling the link down sense feature stops the wireless function when a link is regarded to be down in the wired LAN at an access point.

The condition for detecting the link down-state is selected as a link-down condition : "Link status" or "Ping". "Link status" sets the condition to "when a physical link is disconnected at the wired UTP port of the access point". "Ping" issues a ping packet periodically to a specified communication destination and sets the condition to "when a reply error occurs".

Factory default setting : Wireless LAN … Disable
Link Down Condition … LinkStatus

Ping Parameter

These parameters are used when "Ping" is selected as the link-down condition.

Specify the IP address of the destination to which to periodically send a ping packet. Be sure to specify a valid IP address of a node connected to the wired LAN.

Specify the transmission interval at which to send a ping packet. Enter a value between 1 and 65535.

Specify the reply wait time (in seconds) for which to wait for a reply to a ping. Enter a value between 1 and 15.

Specify the number of retries for which to retry ping transmission while no reply returns. Enter a value between 0 and 15.

Factory default setting	:	IP Address	… 0.0.0.0
		Interval Time (s)	… 60
		Reply Waiting Time (s)	… 3
		Retry Count	… 3

Wireless LAN

To change the wireless LAN standard, wireless connection mode, 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”.

Basic

Interface

Disabling “Interface” disables the internal wireless LAN module.

When switching from “Disable” to “Enable”, options such as channels do not appear in the “STEP 2 Details” setup as the built-in wireless LAN module function is suspended until this device is rebooted. When you come to STEP 2, select “Save/Reboot” in the menu on the lefthand side of the Web browser to save the settings and reboot the device.

Factory default setting : Enabled

Wireless LAN Standard

IEEE802.11a, IEEE802.11b or IEEE802.11g can be selected as the wireless LAN specification to be used.

Factory default setting : IEEE802.11a

Wireless Link Mode

Select the operation mode of the FX-DS540-APDL2-U from among “Standard Infrastructure”, “Compatible Infrastructure”, and “Advanced Infrastructure *1”.

Factory default setting : Standard Infrastructure

Table 4.1. Wireless Link Mode

Wireless link mode	Outline
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.
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.

*1 : Advanced Infrastructure Mode is available only when the access point is used.

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

XR (eXtended Range)

To enable the XR (eXtended Range) function, set to “Enabled”.

When the XR function is enabled, the transmission rate is fixed to “Automatic”.

Factory default setting : Disable

Details

ESSID

The name of the wireless LAN to which the AP belongs. The same ESSID as for the access point to which you wish to log in should be selected. Enter a name up to 32 alphanumeric characters. The name is case sensitive.

Factory default setting : LocalGroup

Channel No. (Function when setting “Access point”.)

Select the wireless channel to be used. The channel number that can be selected varies depending on the country in which the device is used.

When IEEE802.11a is selected, each country has a particular channel in which the DFS function is enabled based on the regulations of the radio law of that country. When that channel is selected, the DFS function checks for any interference with radar waves for one minute before the device is started up. During that period, no communication will be allowed. Moreover, the current channel will be changed to another channel if radar waves are detected during the operation.

Factory default setting : 36

Transmit Rate *1

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

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

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

*1 These are theoretical values based on their respective wireless LAN standards; they do not indicate actual data transfer rates

Factory default setting : Auto, (Max.) 54Mbps

Beacon Transmit Rate (This item available when the unit type is “Access point”.)

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

Basic Rate (This item available when the unit type is “Access point”.)

This item is available when the wireless LAN standard is "IEEE802.11g" or "IEEE802.11b". Specify the basic rate which is the transmission rate for control communication between access point and station (user unit). Usually, this item should be left untouched as set by default.

When the wireless LAN standard is "IEEE802.11g" and the 11g Only mode is "disabled," either "IEEE 802.11" or "IEEE802.11b" can be selected. When the wireless LAN standard is "IEEE802.11g" and the 11g Only mode is "enabled," either "IEEE802.11g" or "OFDM" can be selected.
When the wireless LAN standard is "IEEE802.11b," either "IEEE802.11" or "IEEE802.11b" can be selected.
Factory default setting : No item

TX Power Level

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

Factory default setting : MAX

Super A/G

This item sets the Super A/G feature for increasing the communication speed of wireless LAN. To use Super A/G, enable the feature. Of the Super A/G feature, enable "Frame bursting" to use the frame bursting function and enable "Real-time compression" to use the compression function.

To enable the Super A/G feature, usually, enable "Frame bursting". As real-time compression has no effect on already compressed data (such as ZIP and jpeg files), enable or disable the function selectively depending on the application of communication.

Factory default setting	:	Function	… Disable
		Frame bursting	… Enable
		Real-time compression	… Enable

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 station (user units) and accepts access only from IEEE802.11g compliant station, resulting in communication with IEEE802.11g station at higher data rates than both types of station coexist with the “802.11g Only” mode disabled.

Enabling the protect mode enables stable communication even in an environment in which IEEE802.11b compliant user units coexist with IEEE802.11g compliant station. 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 higher than that of “RTS-CTS”. This setting is enabled when the protect mode is enabled.

Factory default setting	:	802.11g Only mode	… Disable
		Protect mode	… Enable
		Protect type	… CTS-only

Antenna Select

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

Multi client function (This item available when the unit type is “Station”.)

This item is available when the wireless link mode is "Compatible infrastructure".
Select “Enabled” to enable the multi-client function that allows connection to more than one PC.

Factory default setting : Disable

Statistic Node Address (This item available when the unit type is “Station”.)

This item is available when the wireless link mode is "Compatible infrastructure" and multi client function is “Disable”. Enter the MAC address of the PC to be connected to the FX-D540-APDL2-U.
In general, set this item to connect the unit to a receive-only device such as a POS terminal.

Enter the MAC address “00-00-00-00-00-00”, which consists of nothing but 0, meaning the function is disabled, when not using the function.

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 Login (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 easier; 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	:	IEEE802.11a/g … 24
		IEEE802.11b … 24

Priority AP (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 - 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 - 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 - AP5	… 00-00-00-00-00-00
		Connect to other APs	… Enabled

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 conducted. 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 default setting	:	Rate Control	… Disable
		Transmit Rate	… Auto
		Retry Count	… 0
		Band	… 0

Distance

Extending the ACK time-out interval prevents ACK time-out from occurring during long-distance communication. Select "Less than 1 km", "1 - 10 km", "10-20 km", or "Over 20 km". This item adjusts the ACK time-out interval and each option indicates an approximate setting for the time-out interval. It does not increase transmission output or antenna gain to expand the coverage. Usually, this item should be left untouched as set by default.

Factory default setting : Less than 1 km

Load Balance

Load balancing is the function used when wireless terminals are connected to access points so that no single access point is overwhelmed by wireless terminals. When the load balance function is “enabled”, a wireless terminal is preferentially connected to the access point to which fewer terminals are currently connected.

Note that to use this function, the access point and station must be both FLEXLAN series products and also the load balance function must be enabled for both.

Factory default setting : Function … Disable

Beacon Interval (This item available when the unit type is “Access point”.)

Specify the transmission interval at which the access point transmits a beacon signal. Enter a value between 20 and 1000 in milliseconds (ms).

Factory default setting : 100(ms)

DTIM Period (This item available when the unit type is “Access point”.)

Set the frequency at which to add a DTIM (Delivery Traffic Indication Message) to a beacon signal, which is information for recovering a user unit from power-save mode. Enter a value between 1 and 255.

Setting this item to 1 adds a DTIM to each beacon signal; setting it to 2 adds one to every other beacon signal.

Factory default setting : 1(ms)

QoS

To enable the QoS function, set it to "Enabled".

Factory default setting : Disable

WDS (This item available when the unit type is “Access point”.)

To enable the WDS function, set it to "Enable". In that case, specify the wireless MAC address of the remote AP with which to communicate. Use the "Edit List" button to open another window for setup and set the MAC address.

You can register up to six wireless MAC addresses for inter-AP communication.

When entering a MAC address, insert a hyphen (-) at intervals of two bytes (as in 01-23-45-67-89-ab).

The only types of encryption available to wireless LAN setup are WEP, AES (without WPA), and AES-OCB. Do not use WPA or WPA-PSK. In addition, none of them can be used along with the IEEE 802.1X function.

The WDS function cannot be used when channel 52, 56, 60 or 64 has been selected in IEEE802.11a. Use a different channel.

Factory default setting : Disable

Security

Encryption

This setting specifies whether to enable or disable encryption. You can select a type of encryption from among "WEP", "AES", "AES-OCB", and "TKIP". If you select "AES" or "TKIP", the following WPA function can be used. The WPA function is used whenever "TKIP" is selected.

If you disable encryption, neither key can be used as the default key.

Factory default setting : Disable

Table 4.2. Wireless Link Mode

Encryption	WPA Function	Setup
WEP	x	Neither WPA nor WPA-PSK can be used. Set key #1 - #4 for use.
AES	O	You can select whether to use WPA or WPA-PSK. You do not have to set key #1 - #4 when WPA or WPA-PSK is used.
AES-OCB	x	Neither WPA nor WPA-PSK can be used. Set key #1 - #4 for use.
TKIP	O	You have to use WPA / WPA-PSK. You do not have to set key #1 - #4.

WPA

Specify the authentication type when WPA is used. This item can be set only when encryption has been set to "AES" or "TKIP".

Select "WPA" to use WPA based on authentication specified in IEEE 802.1X. Select "WPA-PSK" to use WPA in home mode using no authentication server. "WPA" requires IEEE 802.1X setting and "WPA-PSK" requires WPA encryption key setting described below.

"Disable" can be selected when encryption is "AES". In this case, the WPA function is not used. When encryption is "TKIP", "Disable" cannot be selected and thus either "WPA" or "WPA-PSK" must be selected.

Factory default setting : Disable

Default Key

Set this item with the WPA function disabled when encryption has been set to "WEP", "AES", or "AES-OCB". Select the key number to be used, from among key #1 - #4.

Factory default setting : #1

Size / Key #1 - #4

Set this item with the WPA function disabled when encryption has been set to "WEP", "AES" or "AES-OCB". Specify the size and value of the key to be used for encryption. The acceptable size and number of digits of the key depend on each type of encryption. Enter the key in hexadecimal (0 - 9, a - f, or A - F).

Factory default setting : (Without input)

Table 4.3. Number of Key Input Digits

Encryption	Size and number of Input Digits	
WEP	64bit	10
	128bit	26
	152bit	32
AES	128bit	32
AES-OCB	128bit	32

AP-ST Key

This item is available when the wireless link mode is "Standard infrastructure" and "Advanced infrastructure".
This item is set when “WPA” or “WPA-PSK” is selected as the WPA function or the IEEE802.1X function is enabled, and also the wireless LAN device of the station in which the IEEE802.1X supplicant function is not enabled is used within the network. Enter the authentication key to be used for communication between the access point and a station.

For WEP, set the key size to the same as the size of the above key #1 - #4 to be used. For AES and TKIP, only "128bit" and "256bit" can be selected, respectively. Enter the key in hexadecimal (0 - 9, a - f, or A - F).

When wireless LAN device of the station where the AP - ST key is not effective doesn't log in this device, it is not necessary to set it. In either case, set the size to "Disable".

Factory default setting : Disable (Without input)

Table 4.4. Number of AP-ST Key Input Digits

Encryption	Size and number of Input Digits	
WEP	64bit	10
	128bit	26
	152bit	32
AES	128bit	32
TKIP	256bit	64

Key Update Time (This item available when the unit type is “Access point”.)

Set this item with the WPA function set to "WPA" or "WPA-PSK". Specify the key update interval between 0 and 65535 in minutes. Setting it to 0 stops key transmission.

Factory default setting : 60(minutes)

WPA Encryption Key (This item available when the unit type is “Access point”.)

Set this item with the WPA function set to "WPA-PSK." Enter a WPA encryption key (Pre-Shared Key) using 8 to 63 single-byte alphanumeric characters.

Factory default setting : (Without input)

WSL(Wireless Security Link)

This item is available when the wireless link mode is "Standard infrastructure" and "Advanced infrastructure". Select whether to enable or disable proprietary encryption (WSL) for wireless data. Note, however, that WSL-enabled and WSL-disabled terminals cannot communicate with each other.

There are two types of WSL : Type 1 using an earlier version of the encryption algorithm and Type 2 using the latest version. When the wireless LAN standard is "IEEE802.11a", only Type 2 can be used. When it is "IEEE802.11b" or "IEEE802.11g", either Type 1 or Type 2 can be selected. Select the right one for the application of the unit.

The WSL key setting takes effect only when the WSL function is enabled. Note that terminals different in WSL key cannot communicate with each other.

Enter the WSL key using a string of 20 hexadecimal digits (0 - 9, a - f, or A - F). (Example : 0123456789abcdef0123)

Factory default setting : Disable (Without input)

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

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

IEEE802.1X

IEEE802.1X

Set this item to “enabled” to enable the function of IEEE802.1X.

Select "WEP" by the security setting of wireless LAN to exchange keys when the IEEE802.1X function is made "enabled", and it doesn't use WPA.

Factory default setting : Disable

Extension

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 rejected 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 to TELNET, FTP, WEB by using access point cannot be done.

Factory default setting :	TELNET / FTP / WEB Server	… Enabled
	Administrator IP Address	… Disable
	Administrator IP Address 1 - 2	… 0.0.0.0
	Wireless Access	… Enabled

Network Delay Time (s)

Specify the maximum delay time acceptable to the network.

When an access point communicates with the server or another access point, a communication time-out may occur if an intermediary line is slow in communication speed. If this is the case, increase the network delay time to prevent a time-out from occurring.

Enter a value between 0 and 15.

Factory default setting : 0

Encryption Config File

When this is “enabled”, the setup files (e.g. CONFIG) are saved with their data encrypted when saving the settings.

Whether the setup file encryption function is “disabled” or “enabled”, both encrypted and unencrypted files can be used when those files are written to the device by file transfer.

The password set in the device (up to 31 single-byte alphanumeric characters) is used as the password for the encryption.

Factory default setting : Disable

SNMP

SNMP Agent

Set this item to “enable” to enable SNMP.

Factory default setting : Disable.

Community

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

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 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

sysContact

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)

sysLocation

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)

sysName

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)

Trap

When the trap function is enabled, a trap is transmitted when the Ethernet or wireless LAN link status changes (goes down). This can be set separately between Ethernet and wireless LAN.

Factory default setting : Ethernet … Disable
Wireless … Disable

VLAN

VLAN (This item available when the unit type is “Access point”.)

Set this item to "Enabled" to enable the VLAN function.

Factory default setting : Disable.

VLAN ID (This item available when the unit type is “Access point”.)

Specify the VLAN ID of the unit between 1 and 4096.

Factory default setting : 1

Guest Access (This item available when the unit type is “Access point”.)

Select whether to permit the guests in the guest VLAN ID group other than the VLAN ID groups registered in the VLAN table to access the station (user unit). To enable guest access, set this item to "Enabled".

Factory default setting : Enable.

Guest VLAN ID (This item available when the unit type is “Access point”.)

Set this item if you set guest access to "Enable." Set the VLAN ID for each guest to a value between 1 and 4096. Guest VLAN IDs must be different from any VLAN ID in any other VLAN group registered in the VLAN table.

Factory default setting : 1

RADIUS Server (This item available when the unit type is “Access point”.)

This item applies when the IEEE802.1X or MAC address authentication function is “enabled”. The RADIUS server to be used for guest VLAN is selected. The number displayed refers to the number of the RADIUS server with IEEE802.1X selected. Tick the RADIUS server number that you wish to allow to connect to the network.

Factory default setting : (Check on all)

VLAN Table (This item available when the unit type is “Access point”.)

Set a VLAN group. You can set up to 16 VLAN groups. Use "Edit List" to open the VLAN group setup window to set VLAN groups. Enter the ESSID and VLAN ID for each VLAN group. The ESSID and VLAN ID must be different from those of any other VLAN group or any guest VLAN group.

If WEP (with IEEE 802.1X not used together), AES-OCB, or AES not used for WPA/WPA-PSK is selected for encryption during wireless LAN setup, the encryption setting for each VLAN group can be changed. In that case, the encryption setting is displayed, letting you set the encryption key for each VLAN group. You can also change the key size when WEP is used.

The RADIUS server to be used by each VLAN group can be specified when the IEEE802.1X or MAC address authentication function is enabled. The number displayed is the RADIUS server number when IEEE802.1X is selected. Tick the RADIUS server number that you wish to allow to connect to the network. This allows you to specify a different RADIUS server for each VLAN group.

Factory default setting : (Without setup)

Log

The FX-DS540-APDL2-U can preserve log information. See Chapter 6 “Maintenance” for details of the logged data and data collection methods.

Log

This specifies whether or not to enable logging. ”Enabled” the function to collect logs.

Factory default setting : Disable

File save

To save collected log information as a file, enable the function. To store it temporarily in the memory, disable the function. “Temporarily” here means the period in which the device is starting up.
Log information will be deleted if the device is rebooted or switched off when the function is “disable”.
Never reboot or switch off the device while saving a file when the function is “enabled”.

Factory default setting : Disable

Overwrite Mode

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 Date Time

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

Factory default setting	:	Function	… Disable
		Start Date / Time	… 0　: 00 1 Jan. 2002

Detailed Setting

You can select the types of events to be logged.　Setting [Login], [Logout], [Log in Refusal], [Roaming], [IP Tunnel Start / Stop], [Application login / logout] and [Authentication] 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”

⚠ CAUTION

Please refer to help of browser setting screen "Access Point Manager" for the explanation of a setting item etc. that increase because it updated it to the latest firmware.
The latest explanation is described in help of the latest firmware.

Setting List

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.

Basic Setting

This includes the firmware version, IP address.

Ethernet

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

Wireless LAN

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

The browser displays log information recorded in the AP. To clear log information, click “Clear log information”.
For main events displayed on the logs and their outlines, see the table below.

Table 4.5. 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.
Auth Success	Successful authentication
Auth Error	Authentication error

5. Wireless Link Mode and Wireless LAN Function

This chapter describes the major functions of the FLEXLAN DS540 series as a wireless LAN system and the wireless link modes of the FX-DS540-APDL2-U along with configuration examples of networks available in the wireless link modes.

Wireless Link Mode

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 “Advanced infrastructure”.
Chapters 3 and 4 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 station (ST) 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.

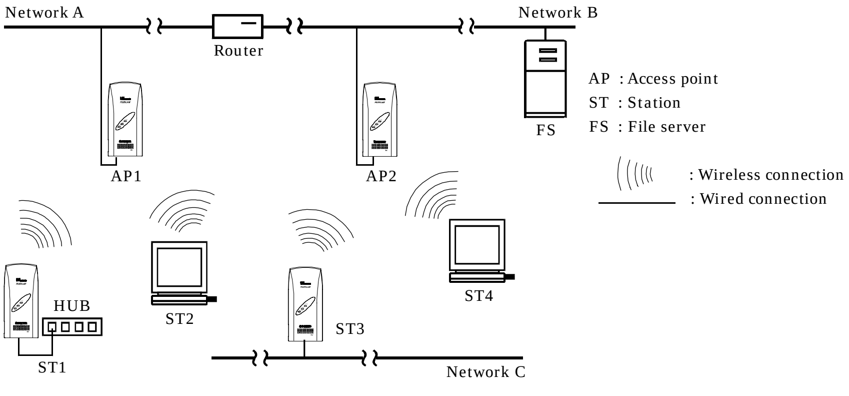


Figure 5.1. Standard Infrastructure Mode

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.

- Advantages

  (1) If the IP tunneling function is used, communication can continue via different routers without needing to change IP address.

  (2) Allows log-in restrictions (security function).

  (3) Capable of improving security based on WSL (Wireless Security Link)

Compatible Infrastructure Mode

This mode allows the FX-DS540-APDL2-U 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.

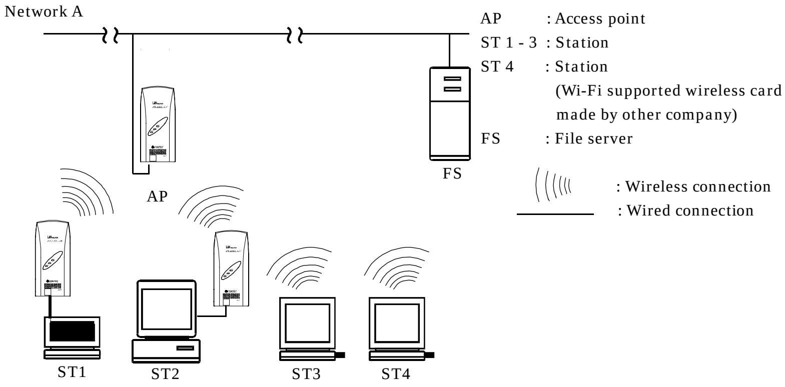


Figure 5.2. Compatible Infrastructure Mode

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 AP within the coverage.

The AP does not provide FXLAN series'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. This mode is available only when the access point is used.

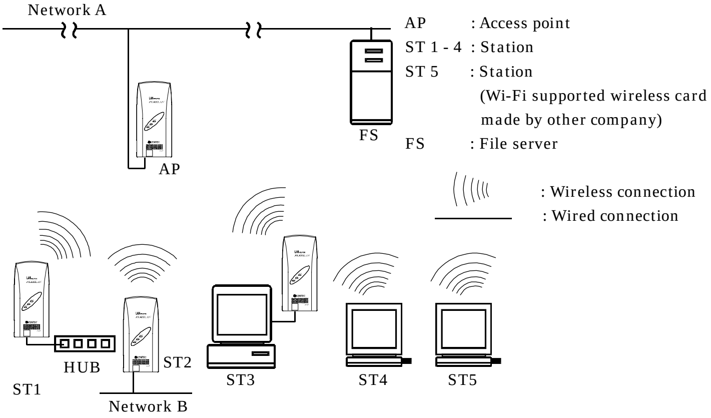


Figure 5.3. Advanced Infrastructure Mode

The terminal set to the Standard Infrastructure mode can use the FLEXLAN DS540 series’s unique features.

The terminal set to the Compatible Infrastructure mode serves as a simple bridge and thus cannot use the FLEXLAN DS540 series’s unique features.

Comparison of Main Functions

The three wireless connection modes mentioned above have different wireless LAN functions.
The following shows a table of the relationship between the operating modes and main functions and gives a brief explanation of each function.

Table 5.1. Comparison of Main Functions

Setting item		Wireless link mode				
		Standard Infrastructure mode		Compatible Infrastructure mode		Advanced Infrastructure mode
		AP	Station	AP	Station	AP fixed
Details	Roaming	O	O	O	O	O
	IP Tunnel	O	-	×	-	O
	Station AP connection	O	O	×	O	O
	SNMP	O	O	O	O	O
	Log collection function	O	-	O	-	O
	MAC address Filtering	O	-	O	-	O
	Bridge Packet Control	O	O	O	O	O
	Data Encryption (WSL)	O	O	×	O	O *1
	Data Encryption (WEP)	-	-	-	O	O
	Super A/G	O	-	O	-	O
	VLAN	-	O	-	O	O
	WDS	O	O	O	O	O
	XR	O	O	O	O	O

Roaming

The roaming function which allows mobile station 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. This function is unique to the FLEXLAN series and cannot be used between the access point that is set to the compatible infrastructure and the station that is set to the compatible infrastructure.

SNMP

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

Log collection function

It is a function to collect event information on a wireless of this product communication etc. 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.

WSL (Proprietary encryption)

WSL (Wireless Security Link) is unique proprietary encryption built only in the FLEXLAN series of devices. It can be used either alone or along with other types of encryption such as WEP and AES. Note, however, that devices using WSL cannot communicate with those not using it.

Data encryption

This function encrypts wireless data. For encryption, four security protocols are available : WEP (Wired Equivalent Privacy), AES, AES-OCB and TKIP. AES and TKIP or WPA and WPA-PSK can be used at the same time.

Super A/G

Proposed by Atheros Communications, Inc., this technology speeds up communication. It improves the throughput of wireless LAN using three techniques : "fast frames" for raising data transfer efficiency by increasing the data packet size, "bursting" for decreasing inter-packet wait time, and "compression" for compressing and decompressing data in real time.

VLAN function

This function organizes terminals on a network into virtual groups regardless of the physical configuration of the network.

WDS function

Inter-AP wireless communication function, enabling an AP to communicate with other APs while communicating with user units.

XR

XR is promoted by Atheros Communications and it is a technology to make the communication distance longer. While the communication speed decreases, the communication distance increases compared with the existing communication. XR can be used both in IEEE802.11a and IEEE802.11g specifications. For communication using XR, the product must be connected to a device which supports the XR technology and has the XR function enabled. If it is connected to any other device, XR will not be used and only the regular wireless communication is available.

Installation in a Network

This section describes how to install the FX-DS540-APDL2-U 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.

Causiton on IEEE802.11a use

To use the IEEE802.11a specification, a network must be built in consideration of the DFS function which is activated.

IEEE802.11a channels include a channel that uses the same frequency band as the weather radar. *1 The DFS function changes the access point channel in order to avoid radio wave interference with the weather radar. The DFS is outlined below.

- When an access point is set to the channel stipulated by the radio law of each country to require the DFS function, the access point checks for any radar wave in that channel for one minute before radio wave transmission starts.
  If a radar wave is detected, an IEEE802.11a channel other than the set channel will be used.
  The access point will check for any radar wave again if that channel is one of the applicable channels.
  If no radar wave is detected, the set channel will be used to transmit radio waves.
- The access point does not use the channel in which a radar wave was detected for 30 minutes after the detection. In other words, the channel in which a radar wave was detected cannot be used for radio communication for at least 30 minutes.
- If a radar wave is detected during the startup of the access point, the transmission of radio waves is halted immediately (radio communication halted). In this case, the access point uses an IEEE802.11a channel other than the one set.

The following points must be considered carefully when building a radio network at channel, which has the DFS function.

- It takes at least one minute for the access point to start up at one of channels, which has the DFS function.
- The access point may start up at a channel other than the set one.
- The channel may be changed during operation even when the access point started up at one of channels, which has the DFS function.

To build a network using any of channels, which has the DFS function, ensure there is no problem even when DFS changes the channel. Take care that a radar wave may still be detected later even when no radar wave was detected during the designing of the network.

Moreover, the “POWER” LED and “WLAN” LED of this product continue to blink independently while checking for a radar wave (one minute) immediately after the startup. As the LEDs blink independently from each other, take care that they may blink simultaneously or differently.

Table 5.2. LED while Checking for Radar Wave

Name	Status	Indicator
POWER	Blinking	Checking for a radar wave upon the startup of this product
WLAN	Blinking	

*1 The channel number corresponding to the DFS function varies depending on the country in which the device is used.

Constructing a Network

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

(1) This product conforms with the standard wireless LAN specifications such as IEEE802.11a, IEEE802.11g and IEEE802.11b, allowing radio communication with the station supporting such specifications. Using different channels for wireless networks adjacent to each other (In IEEE802.11a, set it to 36.44, 8ch or more apart and in IEEE802.11g, 1, 6, 11 5ch or more apart) prevents radio interference and improves the throughput of either network.

(2) Check the coverage (cover area) of the AP. To use the AP with two or more station logged in AP, all the station 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, start the command prompt (MS-DOS) and enter the following command. The example command is for an AP with an IP address of 10.144.0.1.

```
ping 10.144.0.1
```

(3) Two or more stations can log in the AP at the same time However, remember that the communication speed slows due to the increased loading as the number of user units for a particular AP increases.

(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 station, 3m between APs and station, 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.

6. Maintenance

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 and FLEX HELPER. This section describes how to use the tool by the FTP.

For details and applications of FLEX HELPER, contact your dealer.

Log File Collection

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

Log files that use the FTP are collected according to the following procedure.

(1) Move to the folder in which you wish to save the file.

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

(3) Transfer the log file.

(4) Exit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.

In this example, the file will be moved to the saving folder D : \tmp and LOGFILE will be collected after connecting to this product via FTP. The example assumes the IP address as 10.144.0.1.

```
C : \>cd D : \tmp             ----------- (1)
D : \tmp>ftp 10.144.0.1       ----------- (2)
ftp>get LOGFILE               ----------- (3)
ftp>bye                       ----------- (4)
```

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 is used, it's setting file should also be saved. The setting file is stored in memory on the AP with the following file name :

MAC address filtering --- MACFLIST

The file is in the memory even when the MAC address filtering function is not in use It, however, does not have to be saved.

Note that a file of BRGFLIST, 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

Configuration files that use the FTP are collected according to the following procedure.

(1) Move to the folder in which you wish to save the file.

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

(3) Transfer the settings file (CONFIG).

MACFLIST is also transferred if necessary.

(4) Exit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.

In this example, the file will be moved to the saving folder D : \tmp and CONFIG and MACFLIST will be collected after connecting to the product via FTP. The example assumes the IP address as 10.144.0.1.

```
C : \>cd D : \tmp              ------------ (1)
D : \tmp>ftp 10.144.0.1        ------------ (2)
ftp>get CONFIG                 ------------ (3)
ftp>get MACFLIST
ftp>bye                        ------------ (4)
```

Restoring the Software Settings

The software settings of this product can be recovered by using the saved setup file.

Using FTP to Restore the Settings

Follow the procedure below to recover the software settings using FTP.

(1) Move to the folder with file.

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

(3) Transfer the settings file(config).
MACFLIST is also transferred if necessary.

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

(5) Quit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.

In this example, the file will be moved to the folder with file D : \tmp and CONFIG and MACFLIST will be transferred after connecting to the product via FTP. The example assumes the IP address as 10.144.0.1.

```
C : \>cd D : \tmp            ------------ (1)
D : \tmp>ftp 10.144.0.1      ------------ (2)
ftp>put CONFIG               ------------ (3)
ftp>put MACFLIST
ftp>quote crst               ------------ (4)
ftp>bye                      ------------ (5)
```

The reset request command shown in (4) is a command used to reboot the product. There is no problem to skip (4), stop FTP in (5) and reboot the product later.

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

This file can be written over to upgrade the version of the firmware.

There are two ways to upgrade the version of the firmware : FTP; and Access Point Manager with a Web setup screen.

Performing an Upgrade Using FTP

Follow the procedure below for the firmware version up settings using FTP.

(1) Move to the folder with file.

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

(3) Change the transfer mode to binary.

(4) Transfer the firmware file APFIRM.BIN.

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

(6) Quit FTP.

The following is an example for the time when Windows Command Prompt (MS-DOS Prompt) is used.

In this example, the file will be moved to the folder with file D : \tmp and APFIRM.BIN will be transferred after connecting to the product via FTP. The example assumes the IP address as 10.144.0.1.

```
C : \>cd D : \tmp              ------------ (1)
D : \tmp>ftp 10.144.0.1        ------------ (2)
ftp>bin                        ------------ (3)
ftp>put APFIRM.BIN             ------------ (4)
ftp>quote crst                 ------------ (5)
ftp>bye                        ------------ (6)
```

⚠ CAUTION

Do not reboot or switch off the product until the file transfer is completed. The setup file data and firmware data may be damaged and the product may not operate properly if it is rebooted or switched off while the firmware is still being updated (data being written).

Performing an Update Using a Web Browser

To upgrade the version of the firmware on a Web setup screen using a Web browser, follow the procedure below.

(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.

⚠ CAUTION

Do not reboot or switch off the product until you see a screen prompting rebooting.
The setup file data and firmware data may be damaged and the product may not operate properly if it is rebooted or switched off while the firmware is still being updated (data being written).

Initialization

There are three ways to initialize this product (recovering the factory settings).

- Using TELNET
- Using a Web browser
- Using the DIP switch of the main unit (INIT)

Each initialization method is described below.

Using TELNET

Follow the procedure below when using TELNET to initialize the product.

(1) Use TELNET to log in to this product.

(2) In main menu, select “8 default”.

(3) Enter “Y” for the question “Load default setting? (Y/N)”

(4) For the question “Load default IP address? (Y/N)”, enter “Y” to initialize the IP address as well or “N” to leave it unchanged.

(5) From the main menu, select “4. Reboot” - “1. Cold boot”, and then enter “Y” for the question “Save the setting? (Y/N)” to reboot the product.

Saving the setting and rebooting the product after loading the default setting initializes the product.

If the default setting is loaded by mistake, the initialization process can be terminated without changing any settings by selecting “1. Exit” from the main menu and entering “N” for the question “Save the setting? (Y/N)”, rather than rebooting the product.

Using a Web Browser

Follow the procedure below when using Web browser to initialize the product.

(1) Follow the procedure below when using Web browser to initialize the product.

(2) Select “Maintenance” - “Default setting” from the menu.

(3) To leave the IP address of the product unchanged without initialization, tick “Do not set IP address to default”. To initialize the IP address, tick “Set IP address to default” and then click “Default”.

(4) Click “Save/Reboot” on the menu to save the default setting and reboot the product.

Saving and rebooting (4) initializes the product.

If the default setting is selected by mistake, click “Logout” on the menu to close the Web setup screen.

Using the DIP Switch of the Main Unit (INIT)

Follow the procedure below when using the DIP Switch of the Main Unit (INIT) to initialize the product.

(1) Turn on switch 1 of the DIP switches (left switch, INIT) at the front part of the main unit.

(2) Immediately after that, the LEDs of POWER, LAN and WLAN blink for approximately three seconds. Turn off DIP switch 1 during the blinking.

(3) Wait for a while until the blinking of the POWER, LAN and WLAN LEDs stops and then reboot the product (power on/off).

Rebooting (3) initializes the product.

The LEDs of POWER, LAN and WLAN continue to blink for a little while after DIP switch 1 is turned off. Make sure to reboot the product after the blinking stops, as the file in the internal memory may be damaged and the product may not operate properly otherwise.

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 retailer.

When Communication Fails

Check wired LAN communication

Check the wired LAN communication between this product and the connected PC.

- Check that the LAN cable is connected correctly.
- To connect the product to a PC directly, a cross cable must be used. Check to see if a straight cable is used instead for the connection.
- When the product is connected to a PC through a HUB, the cable connecting this product and the HUB must be selected depending on the HUB port. Check if the correct cable is used for the connection. If the HUB port supports AUTO-MDIX, either a straight or cross cable can be used. For the UPLINK port, a cross cable must be used to connect the product.
- Check if the IP addresses and subnet masks of the product and PC are set correctly.
- The communication with this product is not possible unless the TCP/IP protocol is installed in the PC.

Check wireless LAN communication

If no problem is detected in the wired LAN communication between the product and PC, check the wireless LAN communication between the product and access point.

- 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 whether the wireless link mode has been set correctly. The AP to be logged in to and the product must have the same wireless connection mode. (If the access point is set to “standard infrastructure”, this product should also be set to “standard infrastructure”.)
- Check whether communication is restricted by security functions such as the MAC address filtering.
- 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 communication.　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

Setup Screen Unavailable on Web Browser

- Check if communication is possible between the product and PC.
- If no problem is detected in the communication between the product and PC, it may be related to the browser settings.　For the browser settings, see Chapter 3 “Connection to Devices and Setup Methods”.

When the AP Will Not Start

Check the power LED

- Check whether the “POWER” LED is illuminated.　If the LED is not lit, check if the AC adaptor, if used, is properly connected to the power jack and wall socket.
  When an IEEE802.3af-compatible PoE is used, check if the LAN cable is properly connected to the power supply unit and UTP port.
- 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, the problem may be a startup error caused by corrupt data in the memory of this product.
  If you cannot restore it, contact your retailer.

Check the power

- When an AC adaptor is used, check if it is the attached AC adaptor.　Do not use any AC adaptor other than the attached adaptor for this product.
- When an IEEE802.3af-compatible PoE is used, check if an IEEE802.3af-compatible power supply unit is used.　No other power supply can be applied.

8. Appendix

Factory Default Settings List

Hardware Setup

Switch1 : OFF
Switch 2 : OFF

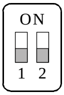


Figure 8.1. DIP Switch

Initial Setting

Table 8.1. Initial Setting List ***< 1 / 4 >***

Item			Specification
Basic setting			
	Host name		(No input)
	DHCP Client		Disable, enable
	IPaddress		(Displays it in the case seal of the main unit)
	Subnet mask		255.0.0.0
	Default gateway		0.0.0.0
	AP construction		Compatibility, integration
	AP type		Normal, master, back up
	IP address of the master AP		0.0.0.0
	IP address of the backup AP		0.0.0.0
	Language setting		English, Japanese
	Passwork		(No input)
Ethernet			
	Port speed		Auto Recognition, 100M/full-duplex, 100M/half-duplex, 10M/full-duplex, 10M/half-duplex
	Link down sense	Wireless LAN	Disable, enable
		Link down condition	Link status, Ping
	Ping parameter	IPaddress	0.0.0.0
		Transmission interval (seconds)	60
		Reply wait time (seconds)	3
		Number of retries	3

11g : It is the function when selecting IEEE802.11g.

Table 8.1. Initial Setting List *< 2 / 4 >*

	Item		Specification
Wireless LAN			
	Interface		Enabled, disable
	Wireless LAN standard		IEEE802.11a, IEEE802.11g, IEEE802.11b
	Wireless link mode		Standard, compatible, advanced (only AP)
	Unit type		AP, station
	XR function		Disable, enable
	ESSID(Alphanumeric character 32 characters, Big and small character distinction)		LocalGroup
	Channel No.		Varies depending on the country in which the product is used (AP) Free fixed (ST)
	Transmission rate (*1)		Auto, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M
	Transmission rate (Max.) (*1)		54M, 6M, 9M, 12M, 18M, 24M, 36M, 48M
AP	Beacon transmission rate		6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M
	Basic rate		IEEE802.11g, OFDM : 11g (11g Only mode enabled) IEEE802.11b, IEEE802.11 : 11g (11g Only mode disable) / 11b
	Transmission output		MAX, 50%, 25%
	Super A/G	Function	Disable, enable
		Frame bursting	Enabled, disable
		Real-time compression	Enabled, disable
11g	802.11g parameter	802.11g Only mode	Disable, enable
		Protect mode	Enabled, disable
		Protect type	CTS-only, RTS-CTS
	Antenna selection		Auto, 1, 2
ST	Priority AP AP 1 - 5		00-00-00-00-00-00 (no specification) [specify the AP MAC address]
ST	Priority AP Connection to the other AP		Enabled, disable
AP	Max login number		254
ST	Multi client function		Disable, enable
ST	Roaming threshold		24, 0 - 95 : 11a,/g 24, 0 - 95 : 11b
AP	Broadcast	Speed control function	Disable, auto, enable
		Transmission speed	Auto, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M
		Number of retries	0, 0 - 10
		Bandwidths	0, 0 - 54
	Communication distance		Less than 1km, 1 - 10km, 10 - 20km, 20km or more
	Load balancing function		Disable, enable
ST	Load balancing, load balancing threshold		30
	Beacon interval		100 (ms)
	QoS		Disable, enable
	WDS		Disable, enable

AP : The function when unit type is access point.

ST : The function when unit type is station.

11g : It is the function when selecting IEEE802.11g.

*1 These are theoretical values based on their respective wireless LAN standards; they do not indicate actual data transfer rates

Table 8.1. Initial Setting List < 3 / 4 >

Item			Specification
Encryption			Disable, WEP, AES, AES-OCB, TKIP
WPA function			Disable, WPA, WPA-PSK
Default key			#1, #2, #3, #4
Size #1 - #4			Disable, 64bit(10digits), 128bit(26digits), 152bit(32digits) : WEP Disable, 128bit(32digits) : AES / AES-OCB Disable : TKIP
Key #1 - #4			(No input)
AP-ST kye	Size		Disable, 64bit(10digits), 128bit(26digits), 152bit(32digits) : WEP Disable, 128bit(32digits) : AES Disable : TKIP
	Key		(No input)
Key update interval			60 (minutes)
WPA encryption key			(No input)
WSL	Type		Disable, enable(Type1), enable(Type2)
	Key		(No input)
ESSID security (only AP)			Disable, enable
MAC address filtering (only AP)			Disable, enable
IEEE802.1X			
	IEEE802.1X function		Disable, enable
Extended function			
	Network time	Function	Disable, enable
	Network time	IPaddress	0.0.0.0 (Disable)
	Network time	Time zone	+09 : 00
	Access control	TELNET server function	Enabled, disable
		FTP server function	Enabled, disable
		WEB server function	Enabled, disable
		Administrator IP specification	Disable, enable
		Administrator Ipaddress 1 - 2	0.0.0.0 (Disable)
		Wireless access	Enabled, disable
	Network dela time (seconds)		0
	Setting file encryption		Disable, enable
SNMP			
	SNMP agent function		Disable, enable
	Community name		public
	Access right		Read/Write, Read Only
	Trap destination IPaddress		0.0.0.0
	sysContact		(No input)
	sysLocation		(No input)
	sysName		(No input)
	Trap	Link state change (ethernet)	Disable, enable
		Link state change (wireless LAN)	Disable, enable

11g : It is the function when selecting IEEE802.11g.

Table 8.1. Initial Setting List ***< 4 / 4 >***

Item			Specification
VLAN			
AP	VLANfunction		Disable, enable
	VLAN ID		1, 1 - 4096
	Guest connection		Enabled, disable
	Guest VLAN ID		1, 1 - 4096
	VLAN table	ESSID	(Empty)
		VLAN ID	(Empty), 1 - 4096
		Encryption	(Empty)
Log function			
	Log function		Disable, enable
	File sabe		Disable, enable
	Overwrite mode		Enabled, disable
	Starting day/time setting	Starting day/time setting function	Disable, enable
		Starting day/time	2002, January 1, 00:00
	Setting on details	Log in	ON, OFF
		Log out	ON, OFF
		Log in regect	ON, OFF
		Roaming	ON, OFF
		IP tunnel start	ON, OFF
		IP tunnel end	ON, OFF
		Application login	ON, OFF
		Application logout	ON, OFF
		Authentication	ON, OFF

AP : The function when unit type is access point.
11g : It is the function when selecting IEEE802.11g.

Specifications

Specifications

Table 8.2. Specifications *< 1 / 2 >*

Item			Specification
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	Varies depending on the country in which the product is used
		Data transmission speed *1	54, 48, 36, 24, 18, 12, 9, 6Mbps (Fixed/Auto)
		Access method	CSMA/CA + ACK(RTS/CTS)
		Wireless category	ISM Baud (5.150 - 5.350GHz, 5.470 - 5.725GHz, 5.725 - 5.825GHz)
		Aerial power	10mW/MHz or less
		Security	WEP(64/128/152bit) or WPA(AES) (128bit) or WPA(TKIP) (256bit) or AES-OCB(128bit) / WSL(Proprietary　encryption) (Usable along with one of the above four types of encryption),
	IEEE802.11b	Transmission format	It conforms to the IEEE802.11b DSSS form
		Channel	Varies depending on the country in which the product is used
		Data transmission speed *1	11, 5.5, 2, 1Mbps (Fix/Auto)
		Access method	CSMA/CA + ACK(RTS/CTS)
		Wireless category	ISM Baud (2.400 - 2.4835GHz)
		Aerial power	10mW/MHz or less
		Security	WEP(64/128/152bit) or WPA(AES) (128bit) or WPA(TKIP) (256bit) or AES-OCB(128bit) / WSL(Proprietary　encryption) (Usable along with one of the above four types of encryption)
	IEEE802.11g	Transmission format	IEEE802.11g standard OFDM　(Orthogonal Frequency Division Multiplexing)
		Channel	Varies depending on the country in which the product is used
		Data transmission speed *1	54, 48, 36, 24, 18, 12, 9, 6Mbps (Fix/Auto)
		Access method	CSMA/CA + ACK(RTS/CTS)
		Wireless category	ISM Baud (2.4 - 2.4835GHz)
		Aerial power	10mW/MHz or less
		Security	WEP(64/128/152bit) or WPA(AES) (128bit) or WPA(TKIP) (256bit) or AES-OCB(128bit) / WSL(Proprietary　encryption) (Usable along with one of the above four types of encryption)

*1　These are theoretical values based on their respective wireless LAN standards; they do not indicate actual data transfer rates.

Table 8.2. Specifications ***< 2 / 2 >***

Item	Specification
Antenna	Chip-type, diversity antenna(Built-in)
External dimension(mm)	81(W) x 26.5(D) x 175(H)
Weight	0.9kg
Length of AC adapter cable	1.5m

Software Specifications

Table 8.3. Software Specifications

Item	Specification
Protocols	IP(RFC791), ICMP(RFC792, UDP(RFC768), TCP(RFC793,896), ARP(RFC826), HTTPD(RFC1866), TELNET(RFC854), FTPD(RFC959), TFTP(RFC783,906), DHCP(RFC2131)

Environmental Specifications for Installing the FX-DS540-APDL2-U

Table 8.4. Environmental Specifications (Environmental Specs)

Item	Specification
Input voltage range	3.2 - 3.5VDC (When using AC adapter) 36 - 57VDC (When using PoE)
Rating input current	1.0A (When using AC adapter) 0.08A (When using PoE)
Operating temperature	0 - 50°C
Operating humidity	10 - 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)

Item	Specification
Input voltage range	90 - 264VAC
Rating input current	0.3A (Max.)
AC supply frequency	47 - 63Hz
Rating output voltage	3.3VDC
Rating output current	2.5A (Max.)
External dimension(mm)	44.8(W) x 30.1(D) x 57.4(H) * No protursions.
Weight	100g
Operating temperature	0 - 40°C
Operating humidity	20 - 90%RH (No condensation)
Airborne dust	Not extreme
Corrosive gases	None

External Dimensions

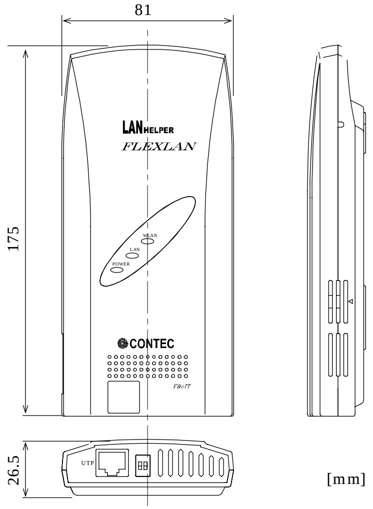
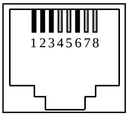


Figure 8.2. External Dimensions(FX-DS540-APDL2-U)

I/O Interface

Pin Assignment of UTP Port

Table 8.6. Pin Assignment of UTP Port



Only Communication

Pin No.	Signal name
1	TX+
2	TX-
3	RX+
4	-
5	-
6	RX-
7	-
8	-

When supplying the UTP cable power

Pin No.	Signal name
1	TX+ / Positive V
2	TX- / Positive V
3	RX+ / Negative V
4	Positive V
5	Positive V
6	RX- / Negative V
7	Negative V
8	Negative V

* Different depending on the output specifications of the supply side. Supporting both of 1/2/3/6-pin supply and 4/5/7/8-pin supply.

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-APDL2-U
User's Manual

CONTEC CO., LTD. March 2006 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/

[03102006]

Management No.	A-59-334
Parts No.	LYFT071