TOSHIBA

MULTIFUNCTIONAL DIGITAL SYSTEMS

Operator's Manual for Wireless LAN Module

GN-1041

PRECAUTIONS

Precautions for Use

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

About TOSHIBA Wireless Solution

The Wireless LAN Module is a wireless network Module that complies with the IEEE 802.11 standard on wireless LANs (Revision B/G). The Wireless LAN Module supports data rates up to 54 Mbit/s.

- Wi-Fi (Wireless Fidelity) certified by the Wi-Fi Alliance. This means that your Wireless hardware will communicate with other vendors' IEEE 802.11 B/G compliant wireless LAN product.
- Fully compatible with any of other wireless LAN system based on Direct Sequence Spread Spectrum (DSSS)/Orthogonal Frequency Division Multiplexing (OFDM) radio technology that complies with the IEEE 802.11 standard on wireless LANs (Revision B/G).

Wireless Interoperability

The TOSHIBA Wireless LAN products are designed to be interoperable with any Wireless LAN products that is based on Direct Sequence Spread Spectrum (DSSS)/Orthogonal Frequency Division Multiplexing (OFDM) radio technology, and is compliant to:

- The IEEE 802.11 Standard on Wireless LANs (Revision B/G), as defined and approved by the Institute of Electrical and Electronics Engineers.
- The Wireless Fidelity (Wi-Fi) certification as defined by the Wi-Fi Alliance.

Wireless LAN and your Health

Wireless LAN products, like other radio devices, emit radio frequency electromagnetic energy. The level of energy emitted by Wireless LAN devices however is far much less than the electromagnetic energy emitted by wireless devices like for example mobile phones.

Because Wireless LAN products operate within the guidelines found in radio frequency safety standards and recommendations, TOSHIBA believes Wireless LAN is safe for use by consumers. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature.

In some situations or environments, the use of Wireless LAN may be restricted by the proprietor of the building or responsible representatives of the organization. These situations may for example include:

- Using the Wireless LAN equipment on board of aeroplanes, or
- In any other environment where the risk of interference to other devices or services is perceived or identified as harmful.

If you are uncertain of the policy that applies on the use of wireless devices in a specific organization or environment (e.g. airports), you are encouraged to ask for authorization to use the Wireless LAN device prior to turning on the equipment.

Safety Instruction for Wireless Products

If your computer has wireless function, all safety instructions must be read carefully and must be fully understood, before attempting to use our Wireless Products.

This manual contains the safety instructions that must be observed in order to avoid potential hazards that could result in personal injuries or could damage your Wireless Products.

— Limitation of Liability

For damage occurring due to an earthquake or thunder, fire beyond our responsibility, action by third party, other accident, intentional or accidental mistakes by a user, misuse, use under abnormal conditions, we do not take any responsibility.
For incidental damage (loss of business profit, business interruption, etc.) occurring due to use or disability of the product, we do not take any responsibility.
For damage occurring due to non observance of the contents described in the instruction manual, we do not take any responsibility.
For damage occurring due to erroneous operation or hang up caused by use in combination with products not related to our company, we do not take any responsibility.

— WARNING

Keep this product away from a cardiac pacemaker at least 22 cm.
Radio waves can potentially affect cardiac pacemaker operation, thereby causing respiratory troubles.
Do not use the product inside a medical facility or near medical electric equipment.
Radio waves can potentially affect medical electric equipment, thereby causing an accident due to malfunction.
Do not use the product near an automatic door, fire alarm or other automatic control equipment.
Radio waves can potentially affect automatic control equipment, thereby causing an accident due to malfunction.
Monitor possible radio interference or other troubles to other equipment while the product is used. If any effect is caused, do not use the product.
Otherwise, radio waves can potentially affect other equipment, thereby causing an accident due to malfunction.

— NOTE

Do not use the product in the following places:
Places near a microwave oven where a magnetic field generates and places where static electricity or radio interference generates.
Depending on environment, radio waves can not reach to the product.

Bluetooth™ and Wireless LAN devices operate within the same radio frequency range and may interfere with one another. If you use Bluetooth™ and Wireless LAN devices simultaneously, you may occasionally experience a less than optimal network performance or even lose your network connection.

Regulatory Information

The TOSHIBA Wireless LAN must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product. This device complies with the following radio frequency and safety standards.

Standards below are certified under the operation with the provided antenna (GN-3010). Do not use this product with other antennas.

Canada - Industry Canada (IC)

This device complies with RSS 210 of Industry Canada.
Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of this device.
L'utilisation de ce dispositif est autorisée seulement aux conditions suivantes: (1) il ne doit pas produire de brouillage et (2) l'utilisateur du dispositif doit étre prét à accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.

The term "IC" before the equipment certification number only signifies that the Industry Canada technical specifications were met.

Europe - EU Declaration of Conformity CE 0984

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC with essential test suites as per standards:

EN 300 328-2:
Electromagnetic compatibility and Radio Spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques

EN 301 489-17:
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services;
Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

EN 60950:
Safety of information technology equipment, including electrical business equipment

EN 50371:
Generic standard to demonstrate the compliance of low power electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (10 MHz-300 GHz)

Hereby, TOSHIBA TEC, declares that this GN-1041 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
TOSHIBA TEC vakuuttaa täten että GN-1041 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Hierbij verklaart TOSHIBA TEC dat het toestel GN-1041 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG

Bij deze verklaart TOSHIBA TEC dat deze GN-1041 voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
Par la présente TOSHIBA TEC déclare que l'appareil GN-1041 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
Par la présente, TOSHIBA TEC déclare que ce GN-1041 est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables
Härmed intygar TOSHIBA TEC att denna GN-1041 står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Undertegnede TOSHIBA TEC erklarer herved, at følgende udstyr GN-1041 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF
Hiermit erklärt TOSHIBA TEC, dass sich dieser/diese/dieses GN-1041 in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)
Hiermit erklärt TOSHIBA TEC die Übereinstimmung des Gerätes GN-1041 mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ TOSHIBA TEC ΔΗΛΩΝΕΙ ΟΤΙ GN-1041 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ
Η Toshiba TEC Corporation δηλώνει με το παρόν ότι το μοντέλο GN-1041 ασύρματου προσαρμογέα LAN συμμορφώνεται με τις βασικές απαιτήσεις και τις λοιπές σχετικές διατάξεις της Οδηγίας 1999/5/ΕΚ
Con la presente TOSHIBA TEC dichiara che questo GN-1041 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Por medio de la presente TOSHIBA TEC declara que el GN-1041 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
TOSHIBA TEC declara que este GN-1041 está conforme com os requisitos essenciais e outras disposicões da Directiva 1999/5/CE.
Toshiba TEC Corporation, GN-1041 model Kablosuz LAN Adaptörünün 1999/5/EC Tüzüğünün temel gereksinimlerine ve diğer ilgili uygulamalara uyduğunu beyan eder.
Thoshiba TEC Corpration timto prohlasuje, ze GN-1041 je ve shode se zakladnimi pozadavky a s dalsimi prislusnymi ustanoveni Narizeni vlady c. 426/2000 Sb.
Toshiba TEC Corporation declarã prin prezenta cã adaptorul fãrã fir LAN model GN-1041 este în conformitate cu cerinþele esenþiale ºi cu alte prevederi corespunzãtoare ale Directivei 1999/5/EC

USA-Federal Communications Commission (FCC)

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 20 cm must be maintained between this device and all persons.

Regulatory Notice for Channel Use in France

The number of channels that can be used for wireless LAN differs from country to country. In France however, user only 4 channels (channel 10, 11, 12, 13) when using wireless networks.

- Channel 10 (2457 MHz)
- Channel 11 (2462 MHz)
- Channel 12 (2467 MHz)
- Channel 13 (2472 MHz)

Approved Countries/Regions for use for the Toshiba Wireless LAN

This equipment is approved to the radio standard by the specific countries/regions. Please ask Toshiba authorized dealer or service engineer.

NOTES!

- The unauthorized reproduction of this document, in whole or in part, is prohibited.
- The specifications, designs, and other contents of this document are subject to change without notice.
- The contents of this document are believed to be accurate, however if any discrepancies noted should be brought to the attention of TOSHIBA authorized dealer or service engineer.
- Notwithstanding the foregoing, the manufacturer is unable to accept any claims for losses or lost profits, etc. Resulting from the use of this product.
- TOSHIBA TEC will not guarantee the machine performance if you perform any setting other than specified in this manual.
- MS, Microsoft, Windows, Windows NT, and MS-DOS are registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.
  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.

Table of Contents

1

SETTING UP WIRELESS NETWORK

This section describes about the preparations before setting up the wireless settings of the equipment.

Before Setting Up Wireless Network

Thank you for purchasing the GN-1041 Wireless LAN Module.
This product is a wireless LAN Module using the 2.4 GHz spectrum diffusion system, and is compatible with IEEE Standard 802.11g and 802.11b for wireless LAN.

When the Wireless LAN is enabled, users can perform the following printing through the Wireless LAN:
- Raw TCP Printing from Windows computers
- LPR Printing from Windows computers
- LPR Printing from Macintosh computers
- LPR Printing from Unix workstation

SUPPLEMENT: The instructions on how set up the client computers for WiFi printing is same as the instructions for wired network printing. For instructions on how to set up the client computers, please see ***Printing Guide***.

NOTES:
- To access the equipment through the Wireless LAN from the client computers, the client computers must have the Wireless LAN Module.
- When you enable the wireless network, the existing NIC will be disabled. This equipment cannot connect the wired network and wireless network at the same time.

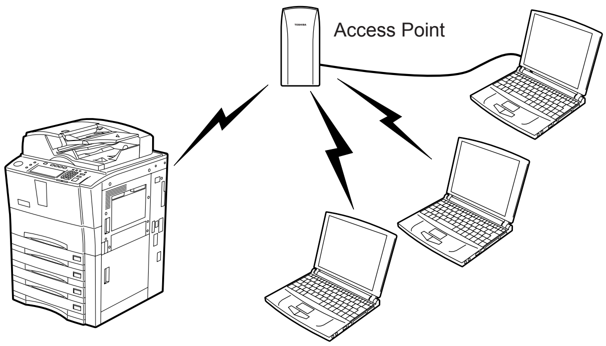
Planning for Installation

Before setting up the Wireless LAN Module for your wireless LAN network, read through this section to understand the information that you require to set up the equipment in your wireless LAN network.

1. Determine the Network Type

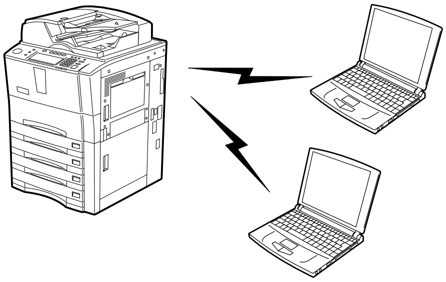
This Wireless LAN Module supports Infrastructure mode and Ad Hoc mode.

Infrastructure Mode



In the Infrastructure Mode, client computers can access to the equipment through a wireless network via an Access Point. The Infrastructure Mode is suitable for the wireless network that many client computers are connected at the same time.
The Access Point will be required to establish the wireless network in the Infrastructure Mode.

Ad Hoc Mode



In the Ad Hoc Mode, client computers can access to the equipment directory through a wireless network without an Access Point. The Ad Hoc Mode is not suitable for the wireless network that many computers are connected, however, it is easy to establish the wireless network because the Access Point is not required.

2. Determine the SSID

In the wireless network, the same SSID (Service Set ID) must be assigned in each wireless device. Only wireless devices that have the same SSID assigned to them can communicate with each other through the wireless network.

In the Infrastructure Mode, the SSID is usually set in the Access Point. Therefore, you must set the same SSID in this equipment to communicate through the wireless network via the Access Point.

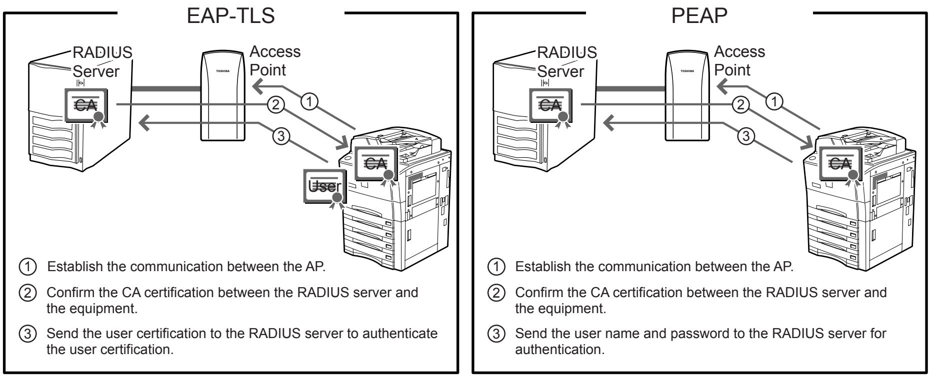
In the Ad Hoc Mode, you must assign the same SSID that is assigned to other client computers. To access the devices each other in the Ad Hoc Mode, the same SSID must be assigned to each device.

3. Determine the Security Mode

This equipment supports the following wireless security modes.

WPA/WPA2/802.1x
Using the WPA/WPA2/802.1x authentication, you can restrict the access to the wireless network using the RADIUS server. The WPA/WPA2/802.1x authentication is available only when the wireless network is established in the Infrastructure Mode.
There are two protocols for the WPA/WPA2/802.1x authentication, EAP-TLS or PEAP. When using the EAP-TLS authentication, you must install user certification file (must be either DER, BASE64, or PKCS#7 encoding format) and CA certification file (must be exported as a private key in PKCS#7 encoding format) in the equipment. This equipment uses the user certification file to authenticate the access rights to the wireless network, and the RADIUS server authenticate this equipment using the user ID and password.

When using the PEAP, you must install the CA certification file (must be either DER, BASE64, or PKCS#7 encoding format) in the equipment. This equipment uses the user name and password to authenticate the access rights to the wireless network, and the RADIUS server authenticate this equipment using the CA certification file.



NOTE: This equipment supports following RADIUS server.
- For EAP-TLS: Windows 2000 Server, Windows 2003 Server, Funk Odyssey Server
- For PEAP: Windows 2000 Server, Windows 2003 Server

WPAPSK/WPA2PSK

The WPAPSK/WPA2PSK is an authentication method using the PSK (Pre-Shared Key) between the Access Point and other wireless devices. The WPAPSK/WPA2PSK authentication is available only when the wireless network is established in the Infrastructure Mode.
To access the wireless network using the WPAPSK/WPA2PSK authentication, the same PSK Path Phrase must be assigned in both the Access Point and other wireless devices. If the PSKs are same between the Access Point and other wireless devices, the Access Point allows them to access the wireless network through the Access Point.
The WPAPSK/WPA2PSK has stronger security than WEP because the data encryption is improved over WEP. This equipment supports TKIP and AES(CCMP) encryption for the WPAPSK/WPA2PSK authentication.
The TKIP provides a different key for per packet with a message integrity check. This key will be changed for every fixed interval.
The AES is the next-generation cryptography algorithm that the U.S. government improves to replace the DES and 3DES.
This authentication method is suitable for a small wireless network and easy to add the security because the authentication server is not required unlike the WPA/WPA2/802.1x authentication.

NOTE: When using WPAPSK/WPA2PSK, it is recommended to use a secure password for WPAPSK/WPA2PSK.

WEP

The WEP is a data encryption method using the WEP key between the Access Point and other wireless devices. Compared with WPA/WPA2/802.1x and WPAPSK/WPA2PSK, the WEP is less security. If the wireless network is configured in the Infrastructure Mode and the Access Point supports WPA/WPA2/802.1x or WPAPSK/WPA2PSK, it is recommended to use WPA/WPA2/802.1x or WPAPSK/WPA2PSK rather than WEP.
The WEP authentication is available for both the Infrastructure Mode and Ad Hoc Mode.

Setting Up the Infrastructure Mode

The wireless settings can be operated from the Control Panel of this equipment.
When setting up the equipment for the wireless network in the Infrastructure Mode, follow the steps below.

1. Select the Network Type
   📖 P.13 "Select Network Type"
2. Specify the SSID
   📖 P.16 "Specify SSID"
3. Select the Security Mode
   📖 P.19 "Select Security Mode"

Select Network Type

First access the WIRELESS SETTING screen from the ADMIN menu from the Touch Panel Display to select the network type for the wireless network.

NOTE: If you are not sure what network type to select, see the following section to determine the network type first.
📖 P.10 "1. Determine the Network Type"

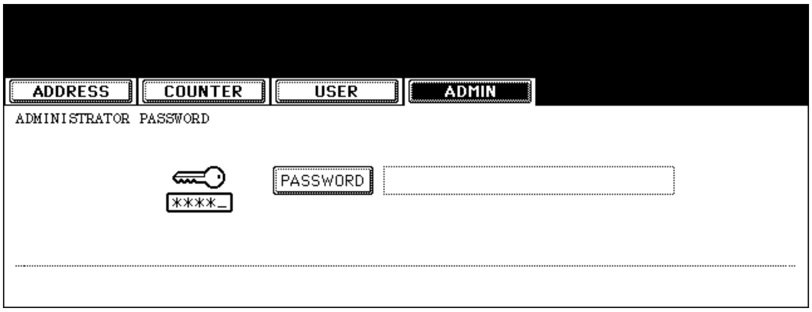
Selecting the network type

1. Press the [USER FUNCTIONS] button on the control panel to enter the User Functions menu.

2. Press the [ADMIN] button.

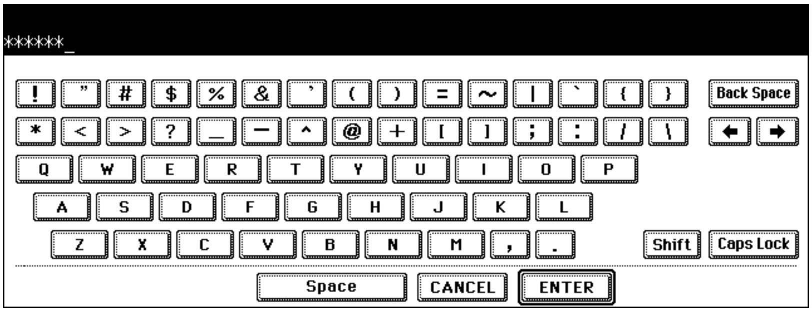
- The ADMINISTRATOR PASSWORD screen is displayed.

3. Press the [PASSWORD] button.



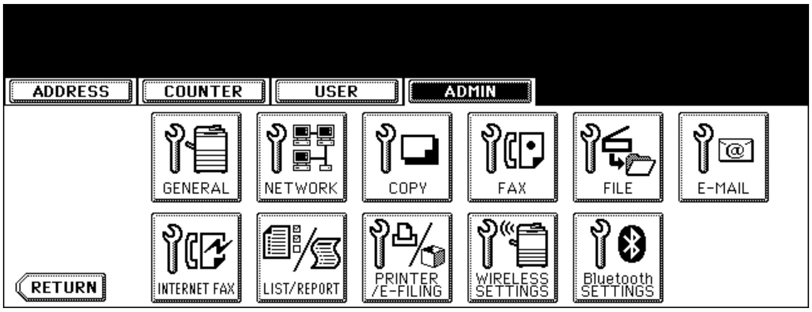
- The input screen is displayed.

4. **Enter the administrator password and press the [ENTER] button.**



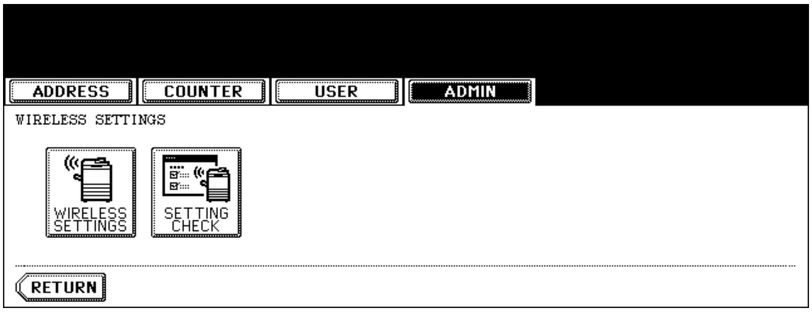
- The ADMIN menu is displayed.

5. **Press the [WIRELESS SETTINGS] button.**



- The WIRELESS SETTINGS menu is displayed.

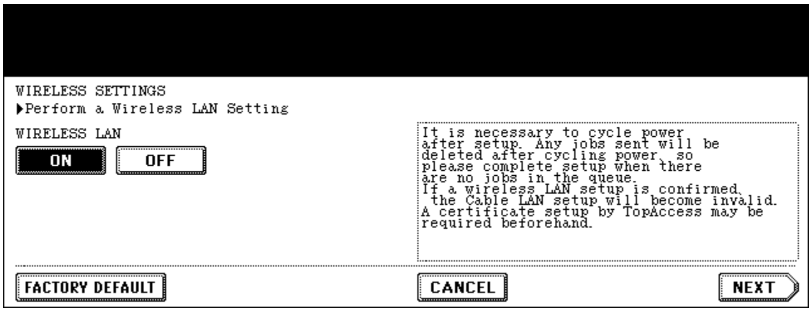
6. **Press the [WIRELESS SETTINGS] button.**



- The WIRELESS SETTINGS screen is displayed.

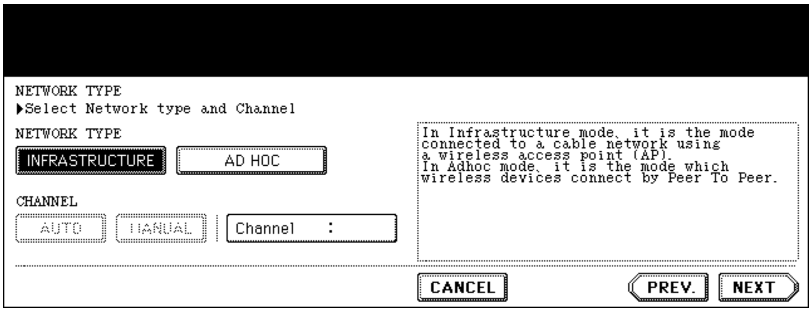
NOTE: It may take a time to display the WIRELESS SETTINGS screen.

7. **Press the [ON] button and press the [NEXT] button.**

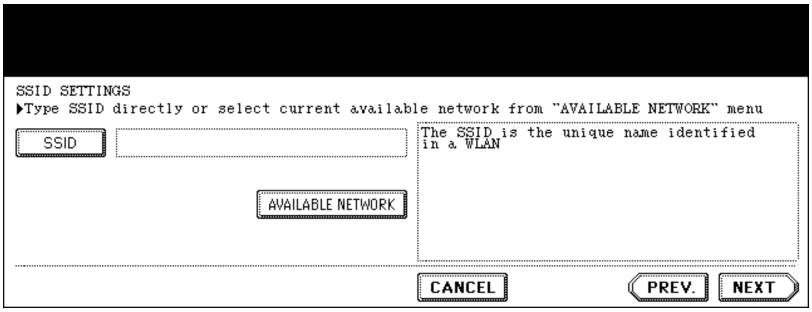


- The NETWORK TYPE screen is displayed.

8. **Press the [INFRASTRUCTURE] button and press the [NEXT] button.**



9. **The SSID SETTINGS screen displayed.**



- Continue to the procedure for specifying the SSID.
📖 P.16 "Specify SSID"

Specify SSID

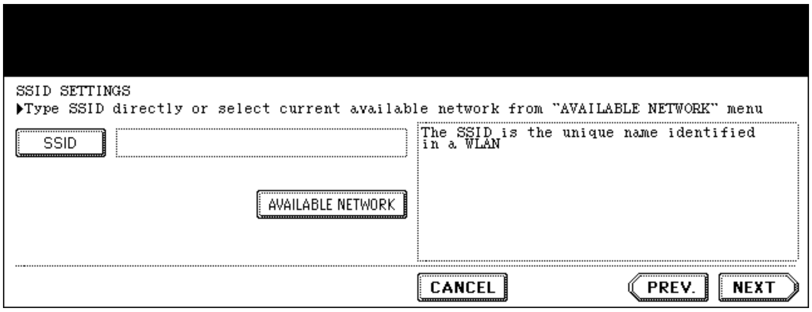
When you select the Infrastructure Mode for the Network Type, you can specify the SSID by selecting the available network list or manually entering the SSID.
P.16 "Selecting the SSID from the available network list"
P.17 "Entering the SSID manually"

NOTE: If you are not sure how the SSID must be specified, see the following section to determine the SSID.
P.11 "2. Determine the SSID"

Selecting the SSID from the available network list

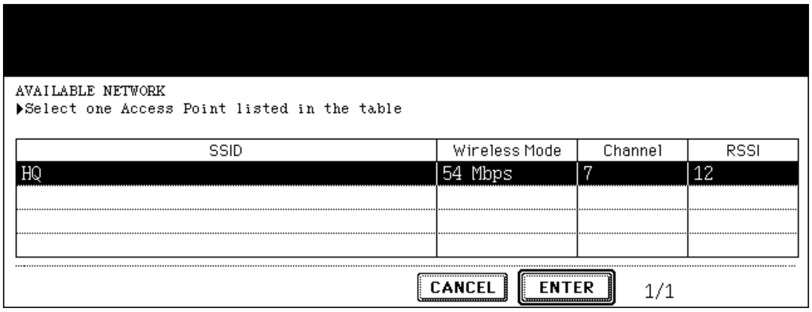
This equipment can search the available SSID automatically from the wireless network. Then you can select the SSID from the list.

1. Press the [AVAILABLE NETWORK] button.



- The AVAILABLE NETWORK screen is displayed.

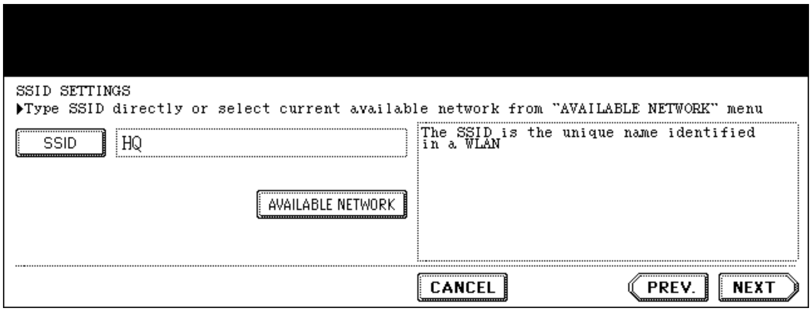
2. Select the SSID that this equipment will connect and press the [ENTER] button.



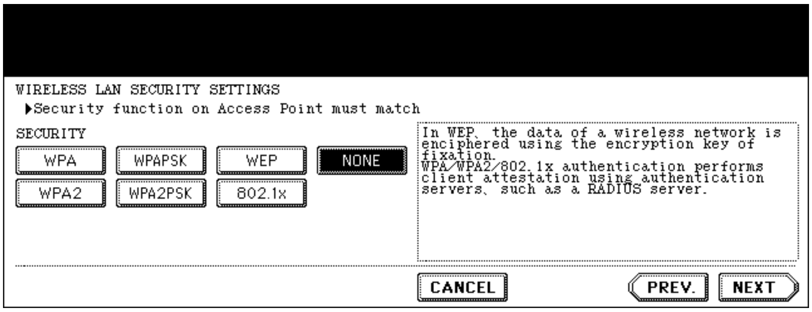
- The screen returns to the SSID SETTINGS screen.

NOTES:
- The available network may not displayed according to the communication environmental conditions.
- If the desired SSID is not displayed, please specify the SSID manually.
  P.17 "Entering the SSID manually"
- This Wireless LAN supports only channel 1 to 11. This equipment cannot connect the Access Point that uses the other channel than these channels. Please make sure to set the channel between 1 to 11 in the Access Point.

3. **Press the [NEXT] button.**



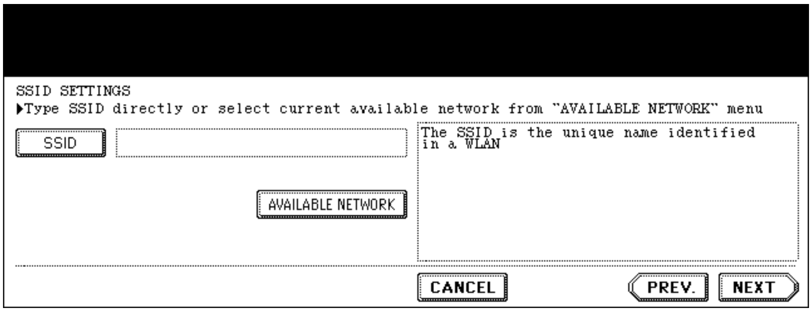
4. **The WIRELESS LAN SECURITY SETTINGS screen is displayed.**



- Continue to the procedure for specifying the Security Mode.
  P.19 "Select Security Mode"

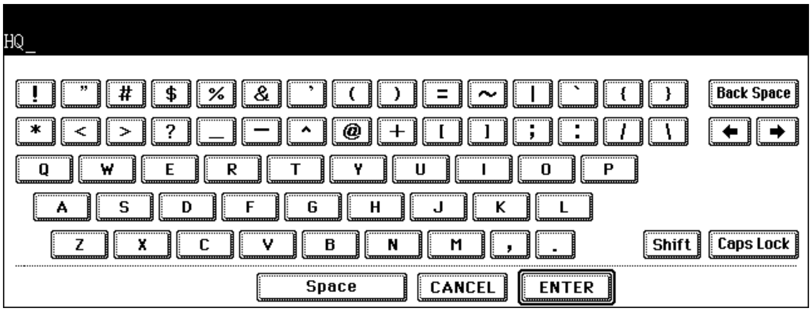
Entering the SSID manually

1. **Press the [SSID] button.**



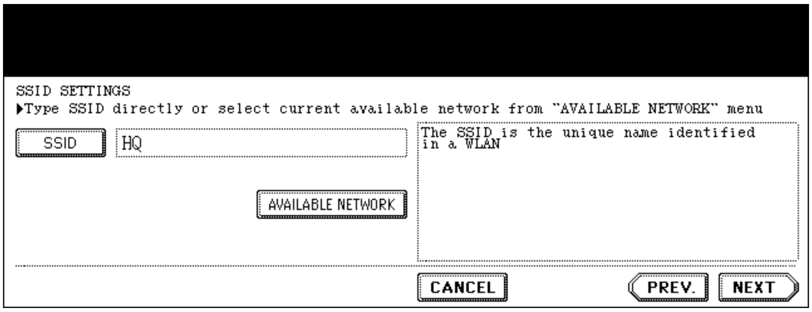
- The letter entry screen is displayed.

2. Enter the SSID using the keyboard and digital keys and press the [ENTER] button.

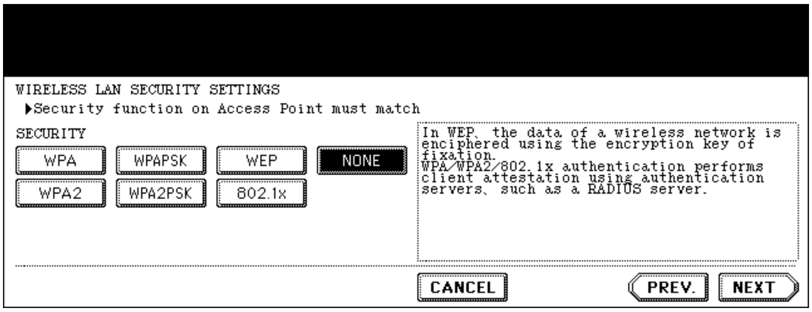


- The screen returns to the SSID SETTINGS screen.

3. Press the [NEXT] button.



4. The WIRELESS LAN SECURITY SETTINGS screen is displayed.



- Continue to the procedure for specifying the Security Mode.
  📖 P.19 "Select Security Mode"

Select Security Mode

After specifying the SSID, you must select the security mode for your wireless network. The procedure to configure the security mode varies depending on the security mode that you select.
P.19 "Selecting WPA/WPA2/802.1x security mode with EAP-TLS protocol"
P.24 "Selecting WPA/WPA2/802.1x security mode with PEAP protocol"
P.28 "Selecting WPAPSK/WPA2PSK security mode"
P.31 "Selecting WEP security mode"
P.33 "Selecting no security mode"

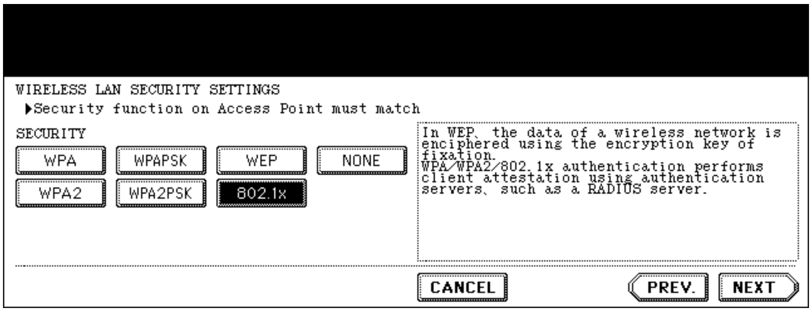
NOTE: If you are not sure what security mode to select, see the following section to determine the security mode.
P.11 "3. Determine the Security Mode"

Selecting WPA/WPA2/802.1x security mode with EAP-TLS protocol

Using the WPA/WPA2/802.1x authentication with the EAP-TLS protocol, you must install user certification file and CA certification file in the equipment. This equipment uses the user certification file to authenticate the access rights to the wireless network, and the RADIUS server authenticate this equipment using the CA certification file.

NOTE: When using the WPA/WPA2/802.1x authentication with the EAP-TLS protocol, you must install the CA certification file and user certification file in the equipment using TopAccess first. For instructions on how to install the CA certification and user certification files using TopAccess, please see ***TopAccess Guide***.

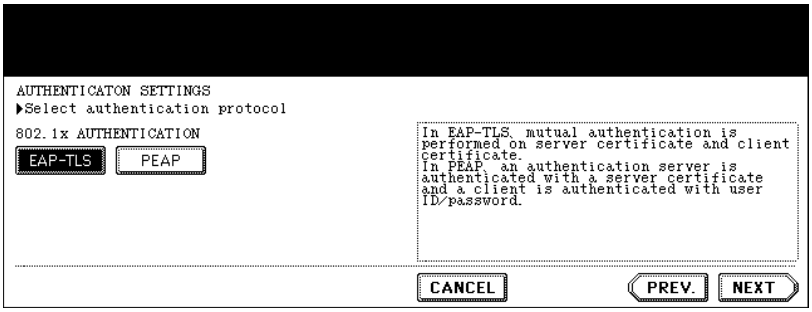
1. **Press the [WPA], [WPA2], or [802.1x] button and press the [NEXT] button.**



- The AUTHENTICATION SETTINGS screen is displayed.

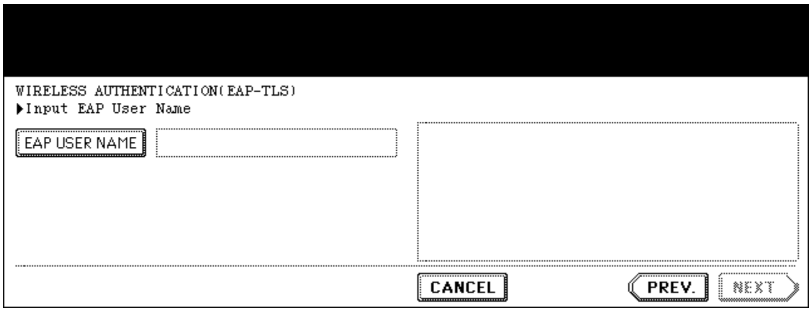
NOTES:
- When the [802.1x] button is selected, only the Dynamic WEP can be selected for the encryption setting. When the [WPA] or [WPA2] button is selected, TKIP or AES(CCMP) can be selected.
- When GN-1040 is connected, the [WPA], [WPA2], and [WPA2PSK] buttons cannot be selected.

2. Press the [EAP-TLS] button and press the [NEXT] button.



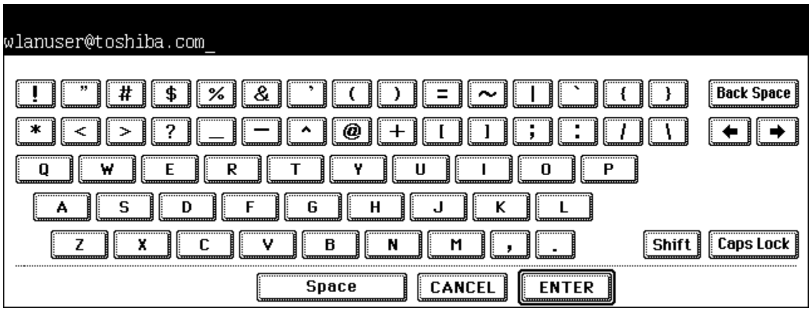
- The WIRELESS AUTHENTICATION (EAP-TLS) screen is displayed.

3. Press the [EAP USER NAME] button.



- The letter entry screen is displayed.

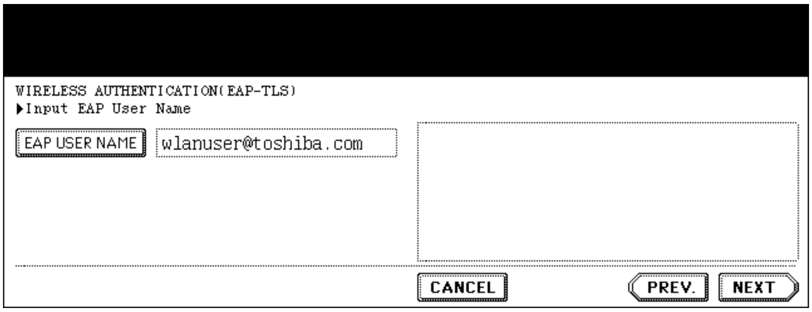
4. Enter the EAP user name using the keyboard and digital keys and press the [ENTER] button.



- The screen returns to the WIRELESS AUTHENTICATION (EAP-TLS) screen.

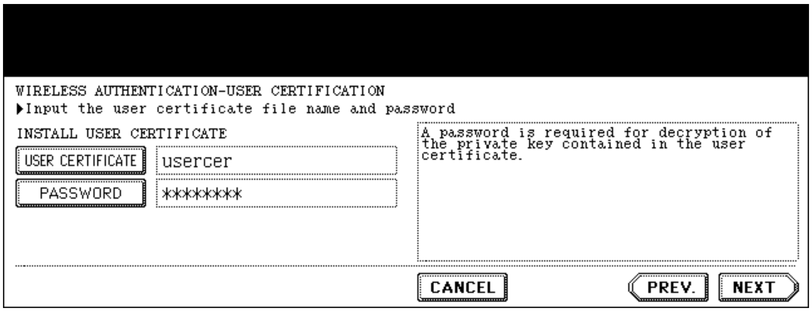
NOTE: In the EAP USER NAME, enter the user name in “User Name@FQDN” format.
Example: wlanuser@toshiba.com

5. Press the [NEXT] button.



- The WIRELESS AUTHENTICATION - USER CERTIFICATION screen is displayed.

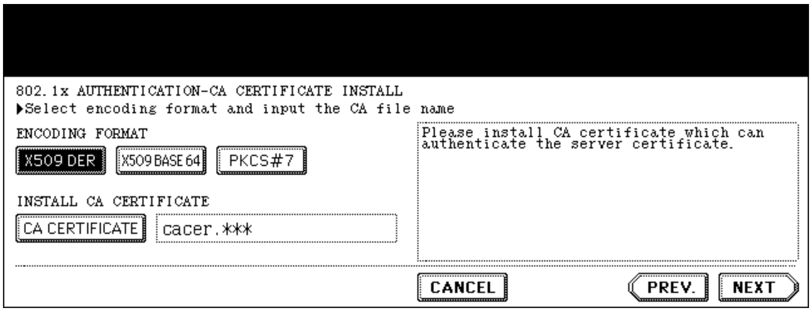
6. Specify the following items and press the [NEXT] button.



- **[USER CERTIFICATE]**
  Press this to enter the file name of the user certification file that you install in the equipment using TopAccess. If the specified certification file is not installed in the equipment, the error message to input correct file name will be displayed.
- **[PASSWORD]**
  Press this to enter the password for the user certification file.

SUPPLEMENT: When pressing the [USER CERTIFICATE] or [PASSWORD] button, the letter entry screen is displayed. Enter the value using the keyboard and digital keys, and press the [ENTER] button to set the entry.

7. Specify the following items and press the [NEXT] button.

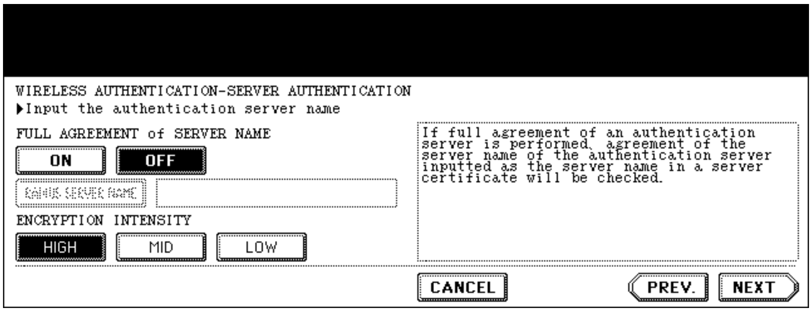


- **ENCODING FORMAT**
  Select the encoding format of the CA certification file.

- **[CA CERTIFICATE]**
  Press this to enter the file name of the CA certification file that you install in the equipment using TopAccess. If the specified certification file is not installed in the equipment, the error message to input correct file name will be displayed.

SUPPLEMENT: When pressing the [CA CERTIFICATE], the letter entry screen is displayed. Enter the value using the keyboard and digital keys, and press the [ENTER] button to set the entry.

8. Specify the following items and press the [NEXT] button.

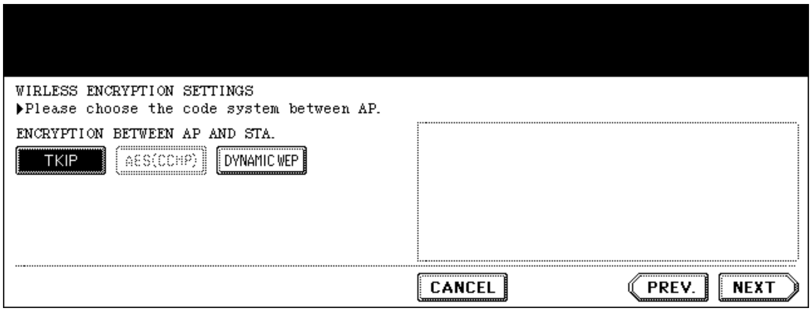


- **FULL AGREEMENT of SERVER NAME**
  Select the [ON] button to confirm whether the RAIUS server name in the server certification file and the input RADIUS server name is same or not. When the [ON] button is selected, press the [RADIUS SERVER NAME] button to enter the RADIUS server name.

NOTE: In the RADIUS SERVER NAME, enter the user name in “Server Name@FQDN” format. Example: wlanserver@toshiba.com

- **ENCRYPTION INTENSITY**
  Select the encryption intensity.

9. Specify the following items and press the [NEXT] button.

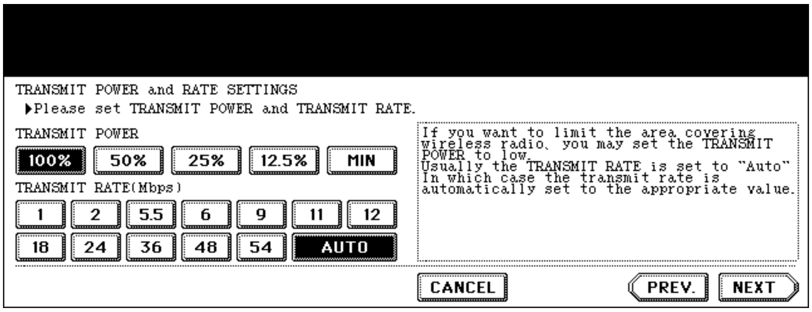


- **ENCRYPTION BETWEEN AP AND STA.**
  Select the encryption type that is used for the communication between Access Point and this equipment.
  [TKIP] — Select this to use TKIP encryption. The TKIP provides a different key for per packet with a message integrity check. This key will be changed for every fixed interval.
  [AES(CCMP)] — Select this to use AES encryption. The AES is the next-generation cryptography algorithm that the U.S. government improves to replace the DES and 3DES.
  [Dynamic WEP] — Select this to use Dynamic WEP encryption. The Dynamic WEP provides the encryption using WEP technology and it allows the WEP key to change dynamically for every fixed interval. The Dynamic WEP does not support the PEER KEY for IEEE802.1x.

NOTES:
- When WPA or WPA2 is selected for the security mode, only [TKIP] or [AES(CCMP)] can be selected.
- When 802.1x is selected for the security mode and GN-1040 is used, either [TKIP], [AES(CCMP)], or [Dynamic WEP] can be selected.
- When 802.1x is selected for the security mode and GN-1041 is used, only [Dynamic WEP] can be selected.

SUPPLEMENT: The encryption intensity between each encryption is:
AES(CCMP) > TKIP > Dynamic WEP

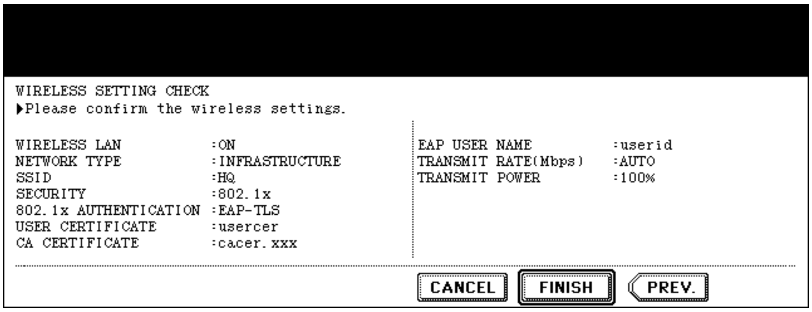
10. Specify the following items and press the [NEXT] button.



- **TRANSMIT POWER**
  Select the low transmit power if you want to limit the area that the wireless communication is enabled. If you do not have to limit the area, select [100%].

- **TRANSMIT RATE**
  Select the transmit data capacity for wireless communication. If you do not have to specify the fixed rate, select [AUTO]. When [AUTO] is selected, this equipment will use appropriate rate depending on the condition.
  Generally select [AUTO]. The communication may fail unexpectedly if you select a static transmit rate.

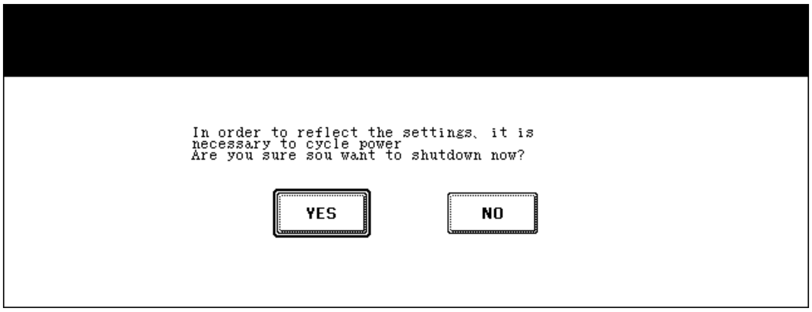
11. Confirm the settings and press the [FINISH] button.



- The shut down screen is displayed.

SUPPLEMENT: If you want to change the settings, press the [PREV] button to move back to the screen that you want to change and then repeat the operation.

12. Press the [YES] button to shut down the equipment.



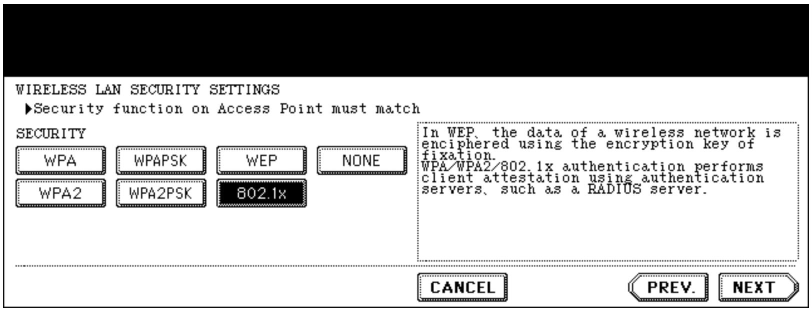
- The wireless settings apply after restarting the equipment.

Selecting WPA/WPA2/802.1x security mode with PEAP protocol

Using the WPA/WPA2/802.1x authentication with the PEAP protocol, you must install the CA certification file in the equipment. This equipment uses the user name and password to authenticate the access rights to the wireless network, and the RADIUS server authenticate this equipment using the CA certification file.

NOTE: When using the WPA/WPA2/802.1x authentication with the PEAP protocol, you must install the CA certification file in the equipment using TopAccess first. For instructions on how to install the CA certification using TopAccess, please see ***TopAccess Guide***.

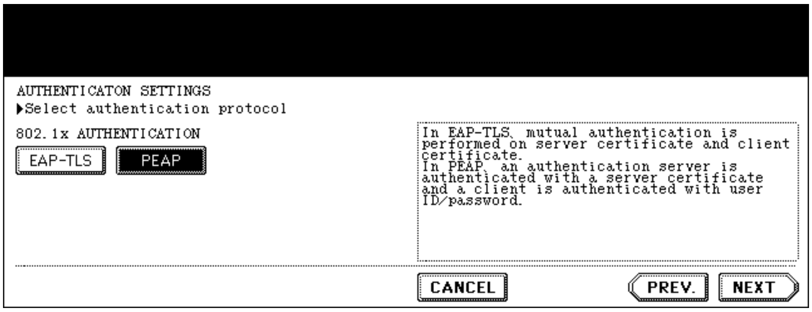
1. Press the [WPA], [WPA2], or [802.1x] button and press the [NEXT] button.



- The AUTHENTICATION SETTINGS screen is displayed.

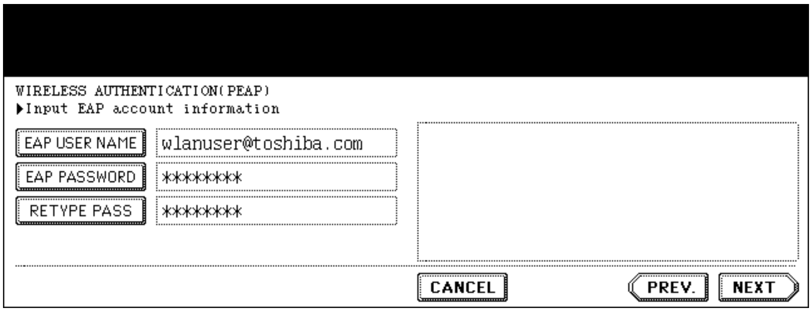
NOTES:
- When the [802.1x] button is selected, only the Dynamic WEP can be selected for the encryption setting. When the [WPA] or [WPA2] button is selected, TKIP or AES(CCMP) can be selected.
- When GN-1040 is connected, the [WPA], [WPA2], and [WPA2PSK] buttons cannot be selected.

2. Press the [PEAP] button and press the [NEXT] button.



- The WIRELESS AUTHENTICATION (EAP-TLS) screen is displayed.

3. Enter the following items and press the [NEXT] button.



- **[EAP USER NAME]**
  Press this to enter the EAP user name that is used for the authentication.

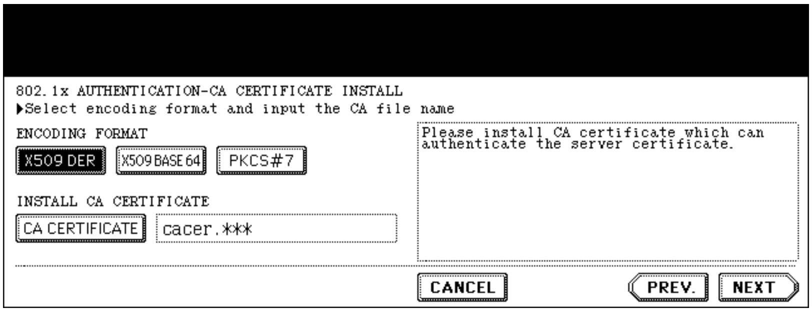
NOTE: In the EAP USER NAME, enter the user name in “User Name@FQDN” format.
Example: wlanuser@toshiba.com

- **[EAP PASSWORD]**
  Press this to enter the EAP password that is used for the authentication.

- **[RETYPE PASS]**
  Press this to enter the EAP password again that you enter in the EAP PASSWORD field.

SUPPLEMENT: When pressing each button, the letter entry screen is displayed. Enter the value using the keyboard and digital keys, and press the [ENTER] button to set the entry.

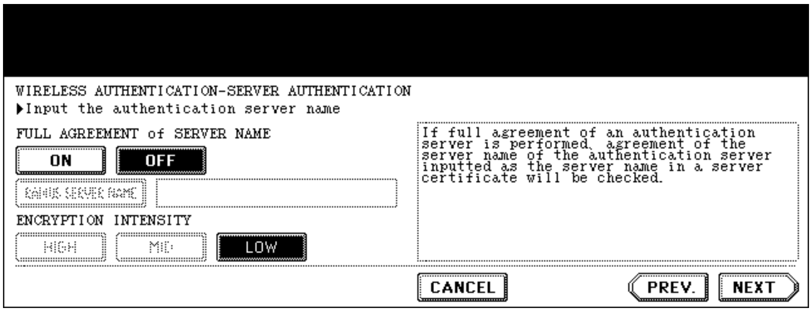
4. Specify the following items and press the [NEXT] button.



- **ENCODING FORMAT**
  Select the encoding format of the CA certification file.
- **[CA CERTIFICATE]**
  Press this to enter the file name of the CA certification file that you install in the equipment using TopAccess. If the specified certification file is not installed in the equipment, the error message to input correct file name will be displayed.

SUPPLEMENT: When pressing the [CA CERTIFICATE], the letter entry screen is displayed. Enter the value using the keyboard and digital keys, and press the [ENTER] button to set the entry.

5. Specify the following items and press the [NEXT] button.

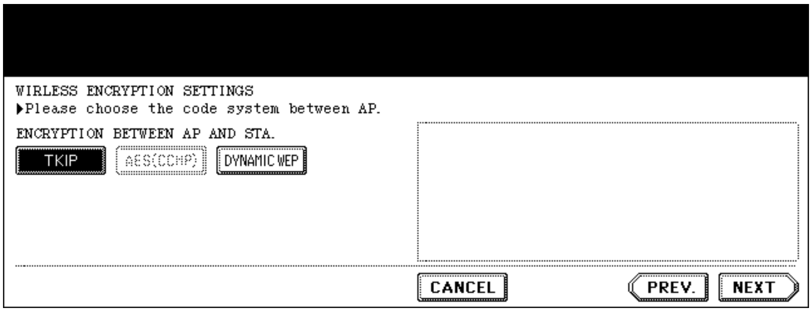


- **FULL AGREEMENT of SERVER NAME**
  Select the [ON] button to confirm whether the RAIUS server name in the server certification file and the input RADIUS server name is same or not. When the [ON] button is selected, press the [RADIUS SERVER NAME] button to enter the RADIUS server name.

NOTE: In the RADIUS SERVER NAME, enter the user name in “Server Name@FQDN” format. Example: wlanserver@toshiba.com

- **ENCRYPTION INTENSITY**
  Select the encryption intensity. When the PEAP protocol is selected, only [LOW] can be selected.

6. Specify the following items and press the [NEXT] button.

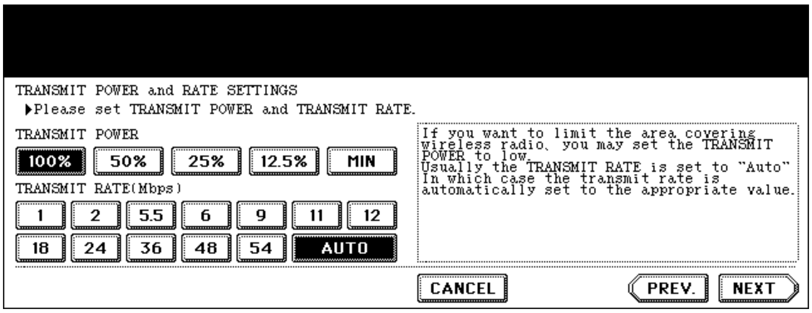


- **ENCRYPTION BETWEEN AP AND STA.**
  Select the encryption type that is used for the communication between Access Point and this equipment.
  [TKIP] — Select this to use TKIP encryption. The TKIP provides a different key for per packet with a message integrity check. This key will be changed for every fixed interval.
  [AES(CCMP)] — Select this to use AES encryption. The AES is the next-generation cryptography algorithm that the U.S. government improves to replace the DES and 3DES.
  [Dynamic WEP] — Select this to use Dynamic WEP encryption. The Dynamic WEP provides the encryption using WEP technology and it allows the WEP key to change dynamically for every fixed interval. The Dynamic WEP does not support the PEER KEY for IEEE802.1x.

NOTES:
- When WPA or WPA2 is selected for the security mode, only [TKIP] or [AES(CCMP)] can be selected.
- When 802.1x is selected for the security mode and GN-1040 is used, either [TKIP], [AES(CCMP)], or [Dynamic WEP] can be selected.
- When 802.1x is selected for the security mode and GN-1041 is used, only [Dynamic WEP] can be selected.

SUPPLEMENT: The encryption intensity between each encryption is:
AES(CCMP) > TKIP > Dynamic WEP

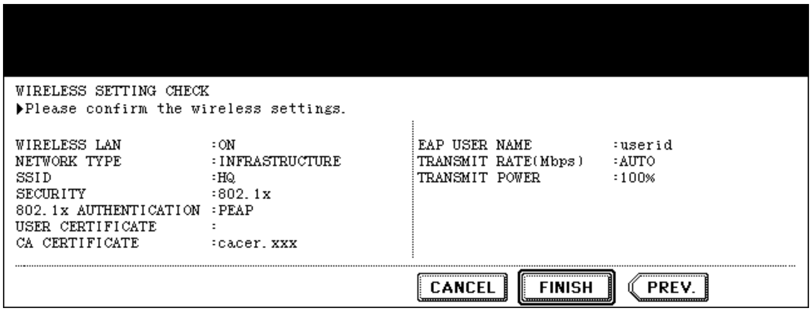
7. Specify the following items and press the [NEXT] button.



- **TRANSMIT POWER**
  Select the low transmit power if you want to limit the area that the wireless communication is enabled. If you do not have to limit the area, select [100%].

- **TRANSMIT RATE**
  Select the transmit data capacity for wireless communication. If you do not have to specify the fixed rate, select [AUTO]. When [AUTO] is selected, this equipment will use appropriate rate depending on the condition.
  Generally select [AUTO]. The communication may fail unexpectedly if you select a static transmit rate.

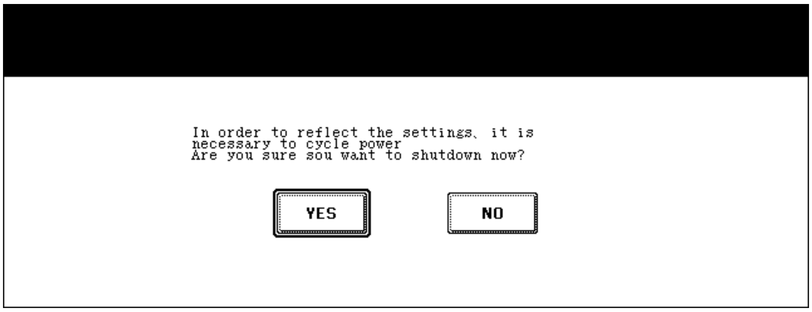
8. Confirm the settings and press the [FINISH] button.



- The shut down screen is displayed.

SUPPLEMENT: If you want to change the settings, press the [PREV] button to move back to the screen that you want to change and then repeat the operation.

9. Press the [YES] button to shut down the equipment.

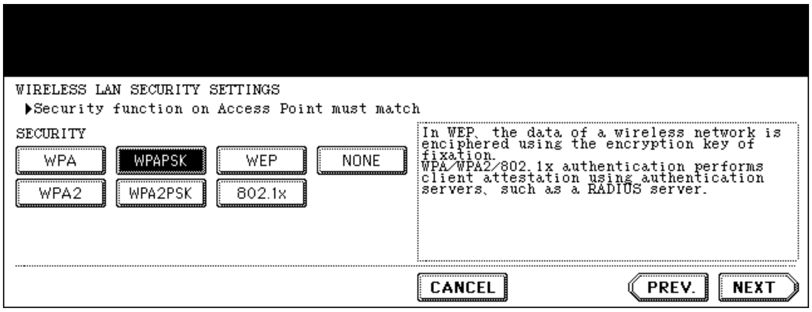


- The wireless settings apply after restarting the equipment.

Selecting WPAPSK/WPA2PSK security mode

The WPAPSK/WPA2PSK is an authentication method using the PSK (Pre-Shared Key) between the Access Point and other wireless devices.
To access the wireless network using the WPAPSK/WPA2PSK authentication, the same PSK Path Phrase must be assigned in both the Access Point and other wireless devices. If the PSKs are same between the Access Point and other wireless devices, the Access Point allows them to access the wireless network through the Access Point.

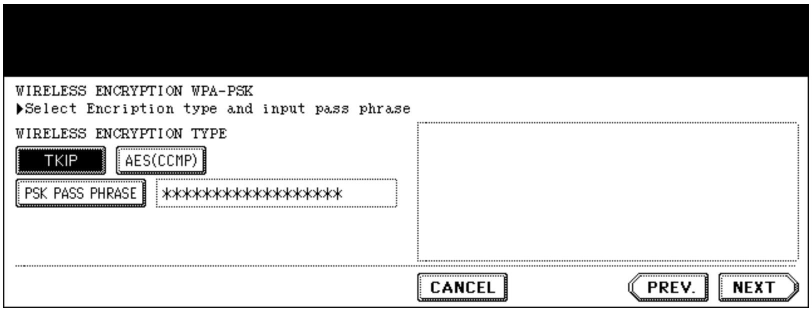
1. Press the [WPAPSK] or [WPA2PSK] button and press the [NEXT] button.



- The WIRELESS ENCRYPTION WPA-PSK screen is displayed.

NOTE: When GN-1040 is connected, the [WPA], [WPA2], and [WPA2PSK] buttons cannot be selected.

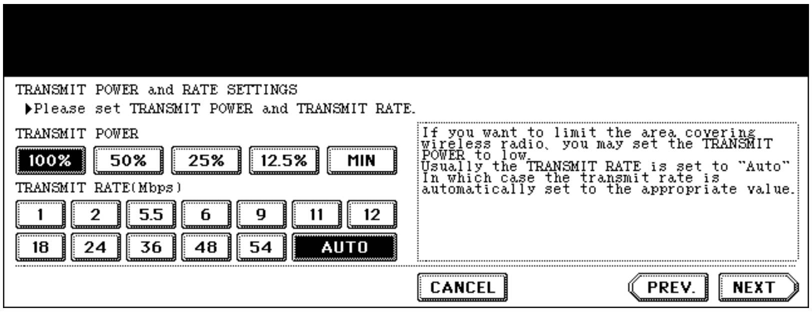
2. Enter the following items and press the [NEXT] button.



- **WIRELESS ENCRYPTION TYPE**
  Select the encryption type for the PSK.
  [TKIP] — Select this to use TKIP encryption. The TKIP provides a different key for per packet with a message integrity check. This key will be changed for every fixed interval.
  [AES(CCMP)] — Select this to use AES encryption. The AES is the next-generation cryptography algorithm that the U.S. government improves to replace the DES and 3DES.
- **[PSK PASS PHRASE]**
  Press this to enter the PSK Pass Phrase. The PSK is created by using the this pass phrase. You must enter the same pass phrase that is set in the Access Point. The PSK Pass Phrase must be between 8 to 63 characters long.

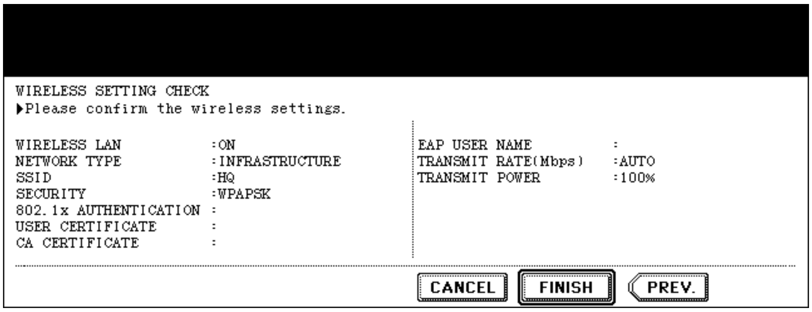
SUPPLEMENT: When pressing the [PSK PASS PHRASE] button, the letter entry screen is displayed. Enter the value using the keyboard and digital keys, and press the [ENTER] button to set the entry.

3. Specify the following items and press the [NEXT] button.



- **TRANSMIT POWER**
  Select the low transmit power if you want to limit the area that the wireless communication is enabled. If you do not have to limit the area, select [100%].
- **TRANSMIT RATE**
  Select the transmit data capacity for wireless communication. If you do not have to specify the fixed rate, select [AUTO]. When [AUTO] is selected, this equipment will use appropriate rate depending on the condition.
  Generally select [AUTO]. The communication may fail unexpectedly if you select a static transmit rate.

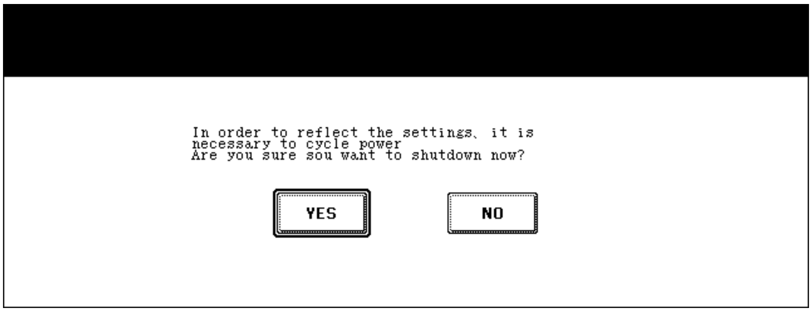
4. Confirm the settings and press the [FINISH] button.



- The shut down screen is displayed.

SUPPLEMENT: If you want to change the settings, press the [PREV] button to move back to the screen that you want to change and then repeat the operation.

5. Press the [YES] button to shut down the equipment.

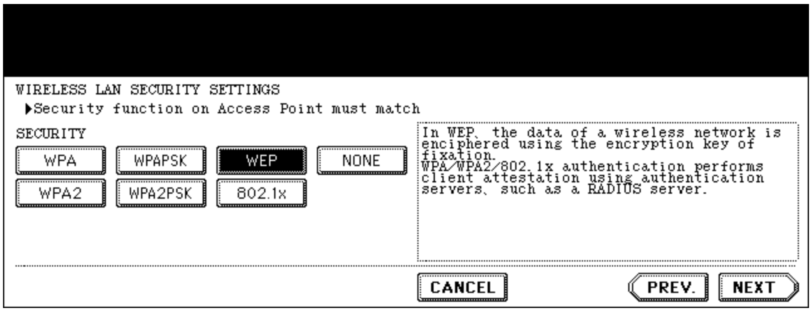


- The wireless settings apply after restarting the equipment.

Selecting WEP security mode

The WEP is a data encryption method using the WEP key between the Access Point and other wireless devices. Compared with WPA/WPA2/802.1x and WPAPSK/WPA2PSK, the WEP is less security. If the wireless network is configured in the Infrastructure Mode and the Access Point supports WPA/WPA2/802.1x or WPAPSK/WPA2PSK, it is recommended to use WPA/WPA2/802.1x or WPAPSK/WPA2PSK rather than WEP.

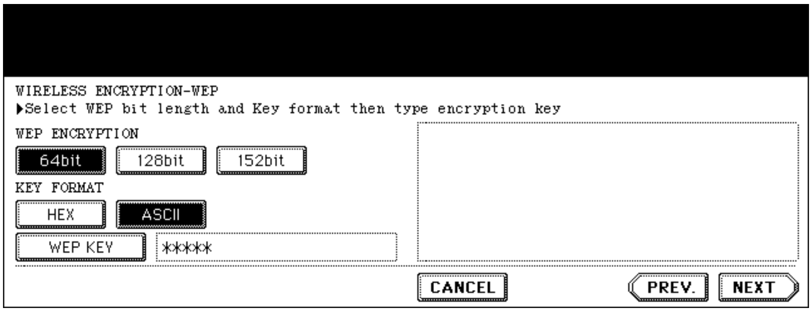
1. Press the [WEP] button and press the [NEXT] button.



- The WIRELESS ENCRYPTION - WEP screen is displayed.

NOTE: When GN-1040 is connected, the [WPA], [WPA2], and [WPA2PSK] buttons cannot be selected.

2. Enter the following items and press the [NEXT] button.

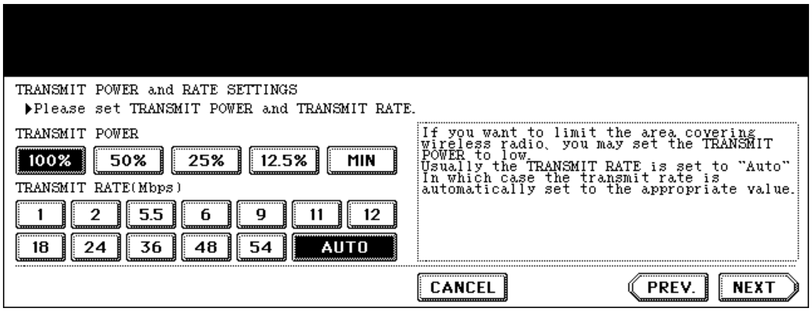


- **WEP ENCRYPTION**
  Select the bit length of the WEP key.
- **KEY ENTRY METHOD**
  Select the character code for the WEP key.
- **[WEP KEY]**
  Press this to enter the WEP key.
  The maximum length of WEP key varies depending on the WEP Encryption and Key Entry Method.

	64bit	**128bit**	**152bit**
HEX :	10	26	32
ASCII :	5	13	16

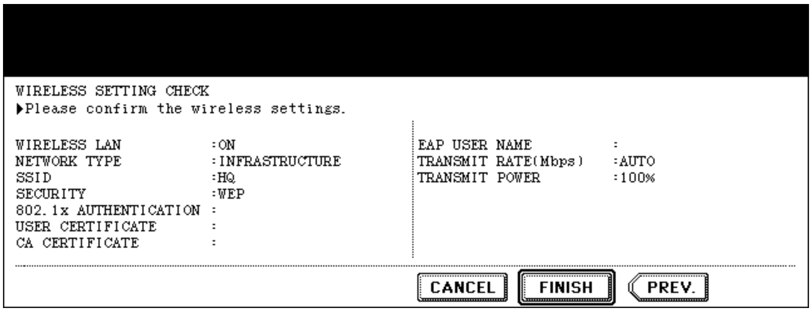
SUPPLEMENT: When pressing the [WEP KEY button, the letter entry screen is displayed. Enter the value using the keyboard and digital keys, and press the [ENTER] button to set the entry.

3. Specify the following items and press the [NEXT] button.



- **TRANSMIT POWER**
  Select the low transmit power if you want to limit the area that the wireless communication is enabled. If you do not have to limit the area, select [100%].
- **TRANSMIT RATE**
  Select the transmit data capacity for wireless communication. If you do not have to specify the fixed rate, select [AUTO]. When [AUTO] is selected, this equipment will use appropriate rate depending on the condition.
  Generally select [AUTO]. The communication may fail unexpectedly if you select a static transmit rate.

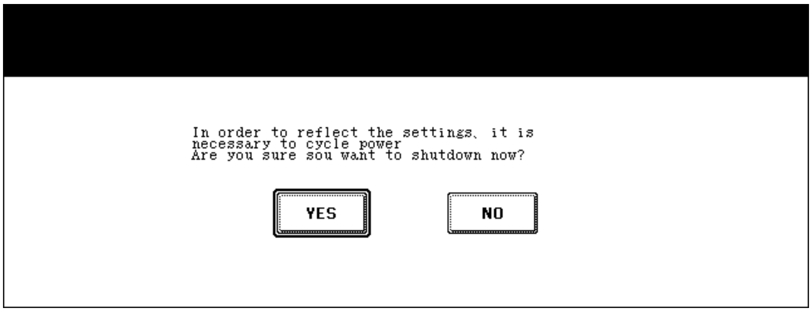
4. Confirm the settings and press the [FINISH] button.



- The shut down screen is displayed.

SUPPLEMENT: If you want to change the settings, press the [PREV] button to move back to the screen that you want to change and then repeat the operation.

5. Press the [YES] button to shut down the equipment.



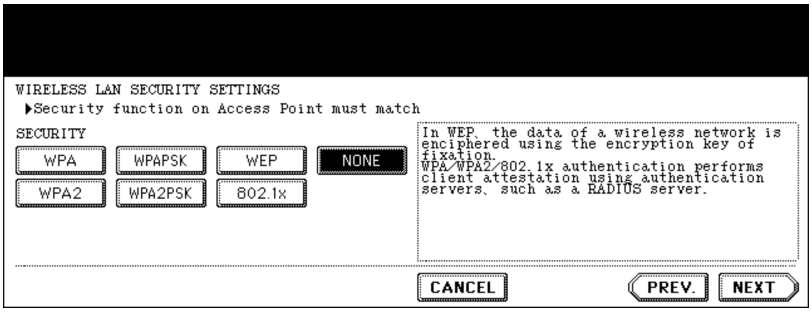
- The wireless settings apply after restarting the equipment.

Selecting no security mode

You can also set no security for wireless access.

NOTE: If you do not set no security, anyone how knows the SSID can connect to the wireless network. Therefore, it is recommended to set the security if it is possible.

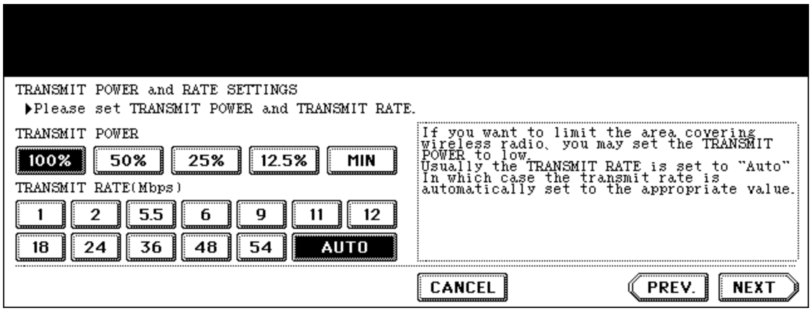
1. Press the [NONE] button and press the [NEXT] button.



- The TRANSMIT POWER and RATE SETTING screen is displayed.

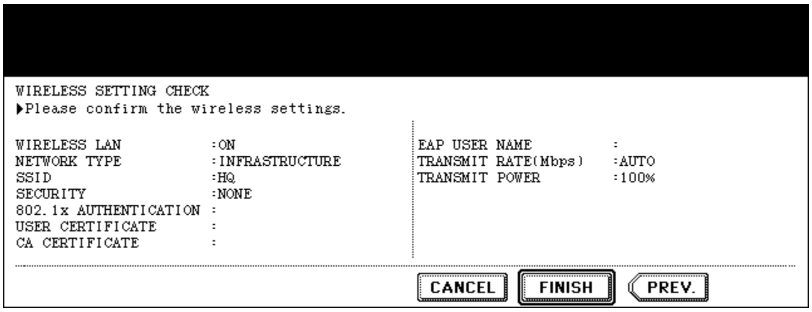
NOTE: When GN-1040 is connected, the [WPA], [WPA2], and [WPA2PSK] buttons cannot be selected.

2. Specify the following items and press the [NEXT] button.



- **TRANSMIT POWER**
  Select the low transmit power if you want to limit the area that the wireless communication is enabled. If you do not have to limit the area, select [100%].
- **TRANSMIT RATE**
  Select the transmit data capacity for wireless communication. If you do not have to specify the fixed rate, select [AUTO]. When [AUTO] is selected, this equipment will use appropriate rate depending on the condition.
  Generally select [AUTO]. The communication may fail unexpectedly if you select a static transmit rate.

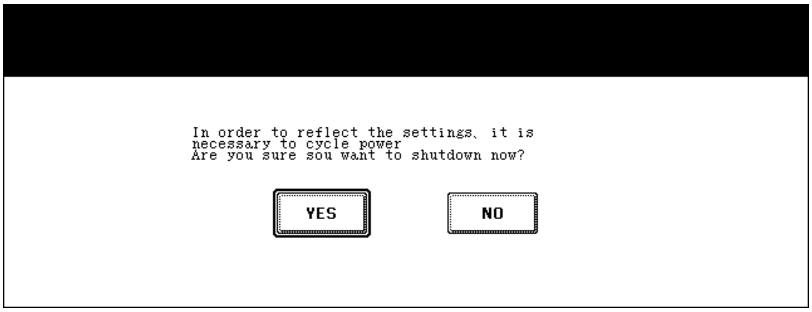
3. Confirm the settings and press the [FINISH] button.



- The shut down screen is displayed.

SUPPLEMENT: If you want to change the settings, press the [PREV] button to move back to the screen that you want to change and then repeat the operation.

4. Press the [YES] button to shut down the equipment.



- The wireless settings apply after restarting the equipment.

Setting up the Ad Hoc Mode

The wireless settings can be operated from the Control Panel of this equipment.
When setting up the equipment for the wireless network in the Infrastructure Mode, follow the steps below.

1. Select the Network Type
   P.35 "Select Network Type"
2. Specify the SSID
   P.38 "Specify SSID"
3. Select the Security Mode
   P.40 "Select Security Mode"

Select Network Type

First access the WIRELESS SETTING screen from the ADMIN menu from the Touch Panel Display to select the network type for the wireless network.

NOTE: If you are not sure what network type to select, see the following section to determine the network type first.
P.10 "1. Determine the Network Type"

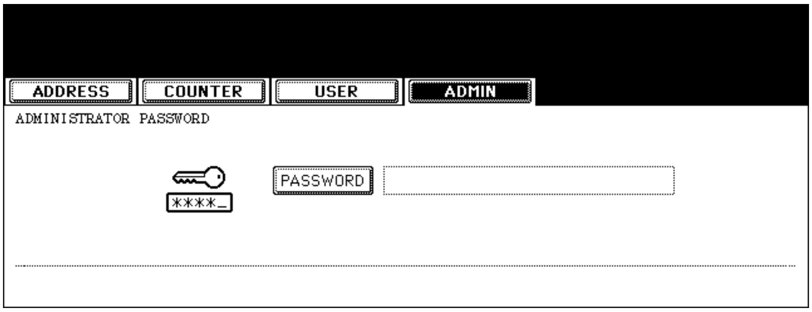
Selecting the network type

1. Press the [USER FUNCTIONS] button on the control panel to enter the User Functions menu.

2. Press the [ADMIN] button.

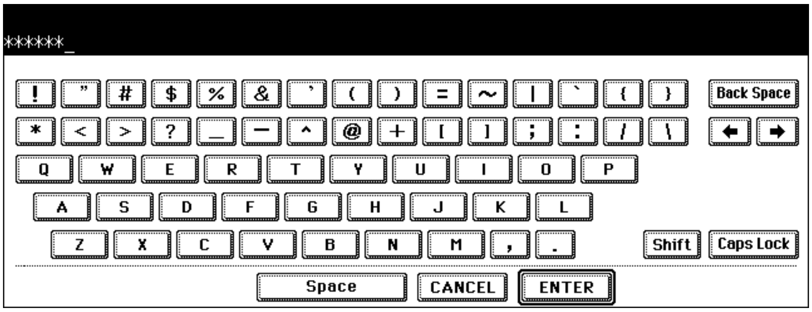
- The ADMINISTRATOR PASSWORD screen is displayed.

3. Press the [PASSWORD] button.



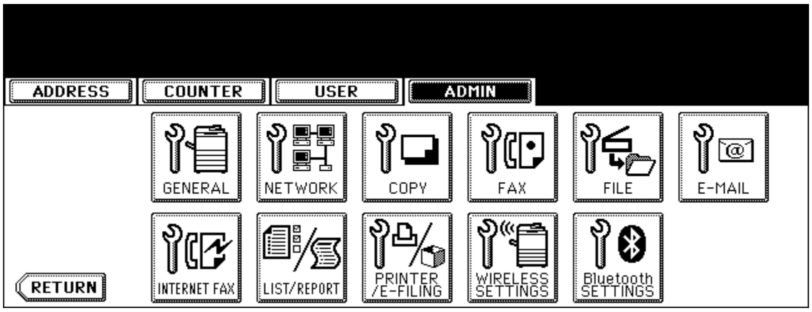
- The input screen is displayed.

4. **Enter the administrator password and press the [ENTER] button.**



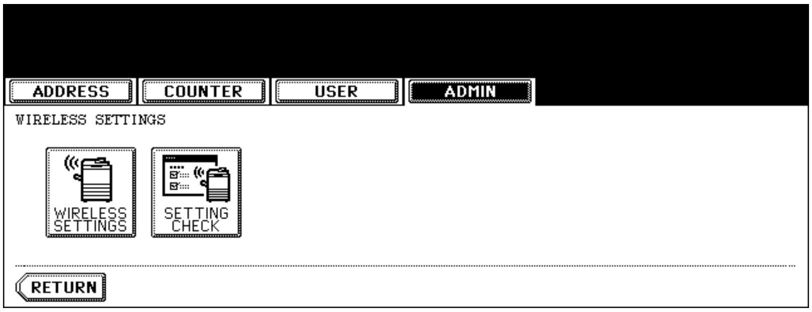
- The ADMIN menu is displayed.

5. **Press the [WIRELESS SETTINGS] button.**



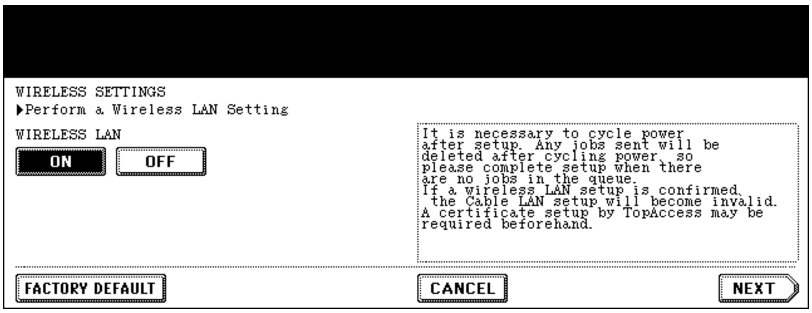
- The WIRELESS SETTINGS menu is displayed.

6. **Press the [WIRELESS SETTINGS] button.**



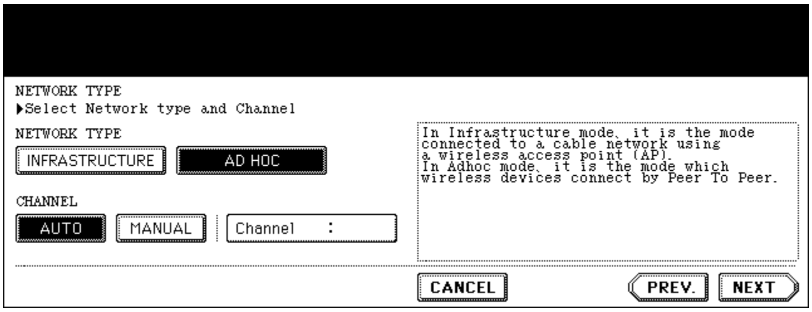
- The WIRELESS SETTINGS screen is displayed.

7. **Press the [ON] button and press the [NEXT] button.**



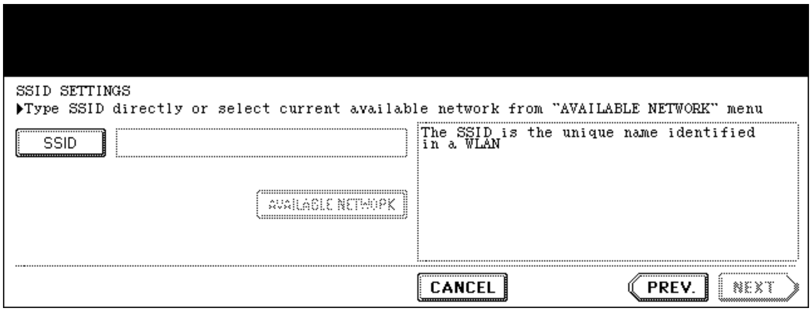
- The NETWORK TYPE screen is displayed.

8. Press the [AD HOC] button and press the [NEXT] button.



NOTE: You can specify the between 1 to 11 for the channel. However, if there is a channel that has already been used for Ad Hoc network, use the same channel.

9. The SSID SETTINGS screen displayed.



- Continue to the procedure for specifying the SSID.
P.16 "Specify SSID"

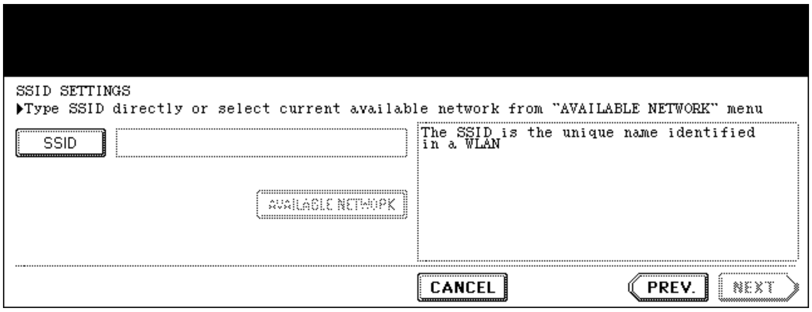
Specify SSID

When you select the Ad Hoc Mode for the Network Type, you can specify the SSID by entering the SSID manually.

NOTE: If you are not sure how the SSID must be specified, see the following section to determine the SSID.
📖 P.11 "2. Determine the SSID"

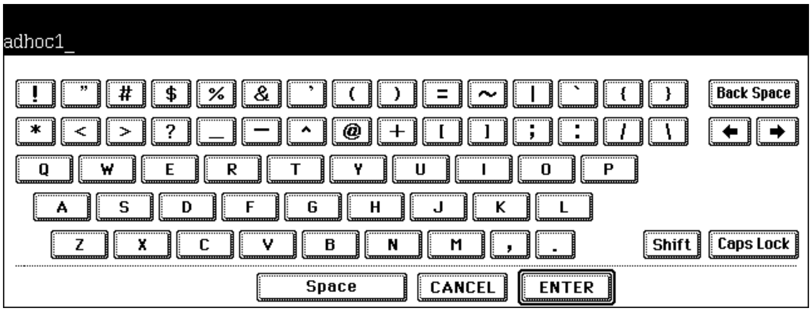
Entering the SSID manually

1. Press the [SSID] button.



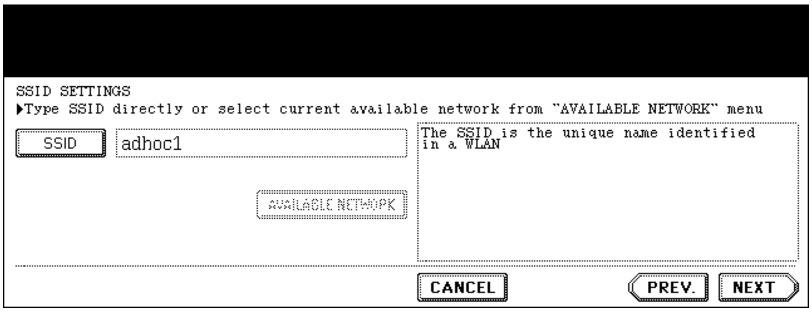
- The letter entry screen is displayed.

2. Enter the SSID using the keyboard and digital keys and press the [ENTER] button.

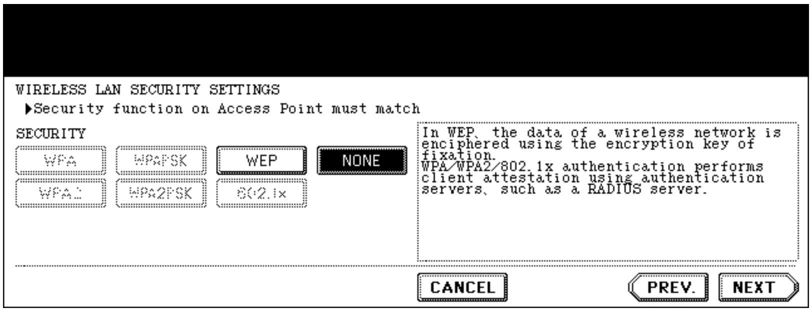


- The screen returns to the SSID SETTINGS screen.

3. Press the [NEXT] button.



4. The WIRELESS LAN SECURITY SETTINGS screen is displayed.



- Continue to the procedure for specifying the Security Mode.
  P.19 "Select Security Mode"

Select Security Mode

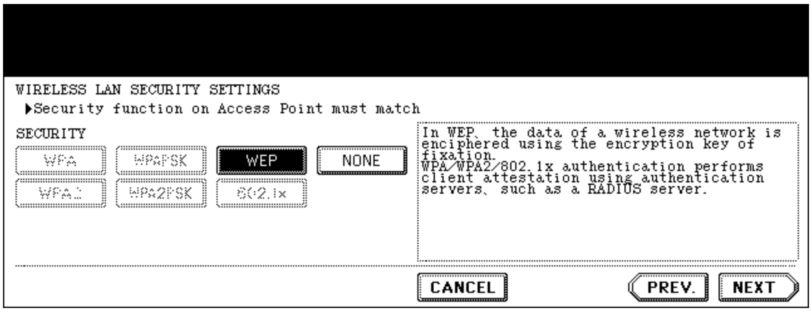
After specifying the SSID, you must select the security mode for your wireless network. The procedure to configure the security mode varies depending on the security mode that you select.
📖 P.31 "Selecting WEP security mode"
📖 P.33 "Selecting no security mode"

NOTES:
- If the Ad Hoc Mode, only WEP or NONE can be selected for the security mode.
- If you are not sure what security mode to select, see the following section to determine the security mode.
  📖 P.11 "3. Determine the Security Mode"

Selecting WEP security mode

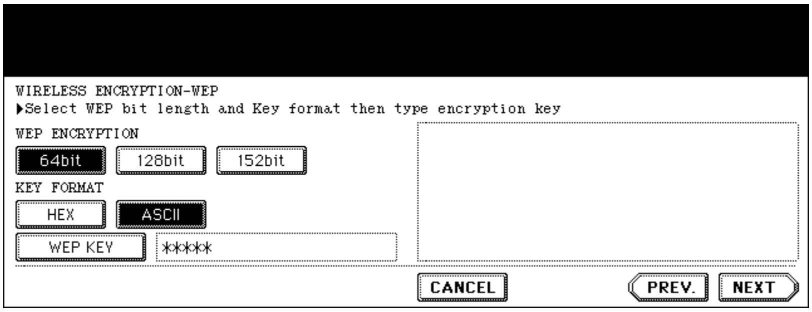
The WEP is a data encryption method using the WEP key between the Access Point and other wireless devices.

1. Press the [WEP] button and press the [NEXT] button.



- The WIRELESS ENCRYPTION - WEP screen is displayed.

2. Enter the following items and press the [NEXT] button.



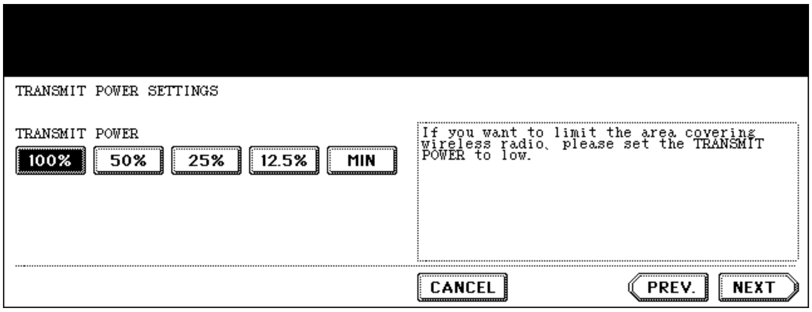
- **WEP ENCRYPTION**
  Select the bit length of the WEP key.
- **KEY ENTRY METHOD**
  Select the character code for the WEP key.

- **[WEP KEY]**
  Press this to enter the WEP key.
  The maximum length of WEP key varies depending on the WEP Encryption and Key Entry Method.

	64bit	128bit	152bit
HEX :	10	26	32
ASCII :	5	13	16

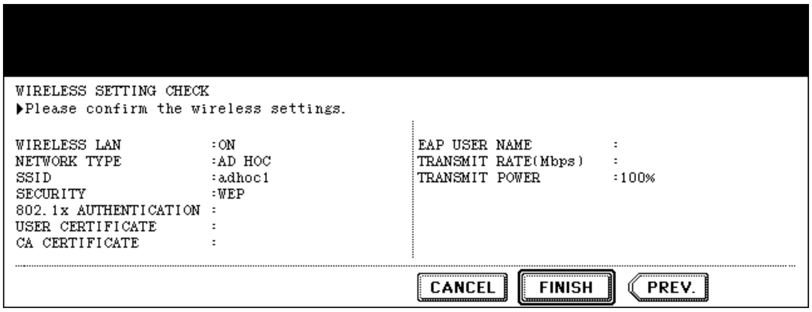
SUPPLEMENT: When pressing the [WEP KEY button, the letter entry screen is displayed. Enter the value using the keyboard and digital keys, and press the [ENTER] button to set the entry.

3. Select the transmit power and press the [NEXT] button.



- Select the low transmit power if you want to limit the area that the wireless communication is enabled. If you do not have to limit the area, select [100%].

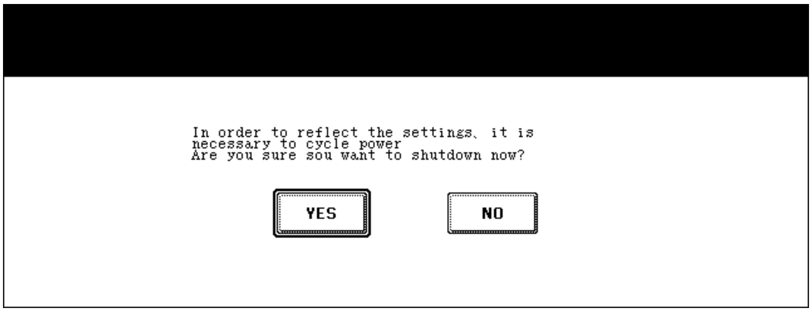
4. Confirm the settings and press the [FINISH] button.



- The shut down screen is displayed.

SUPPLEMENT: If you want to change the settings, press the [PREV] button to move back to the screen that you want to change and then repeat the operation.

5. **Press the [YES] button to shut down the equipment.**



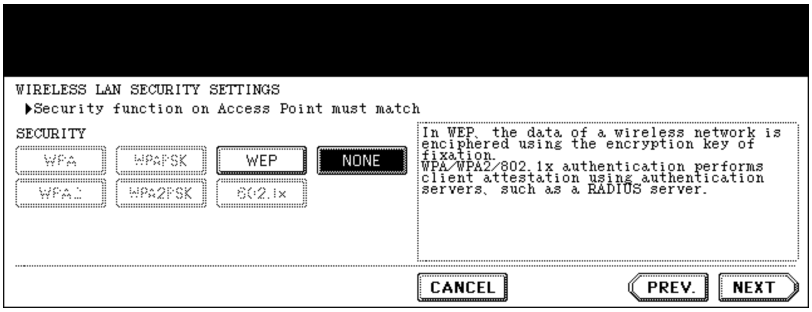
- The wireless settings apply after restarting the equipment.

Selecting no security mode

You can also set no security for wireless access.

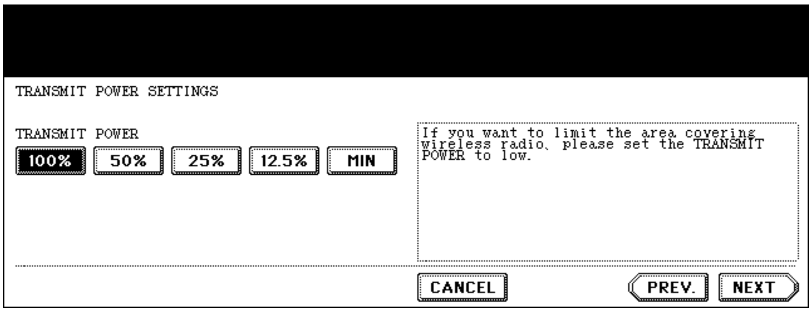
NOTE: If you do not set no security, anyone how knows the SSID can connect to the wireless network. Therefore, it is recommended to set the security if it is possible.

1. **Press the [NONE] button and press the [NEXT] button.**



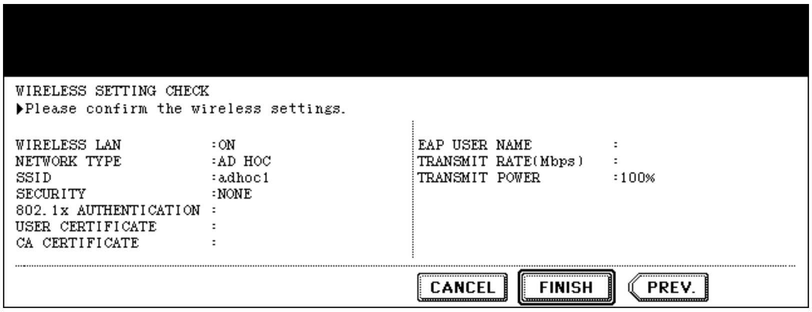
- The TRANSMIT POWER and RATE SETTING screen is displayed.

2. **Select the transmit power and press the [NEXT] button.**



- Select the low transmit power if you want to limit the area that the wireless communication is enabled. If you do not have to limit the area, select [100%].

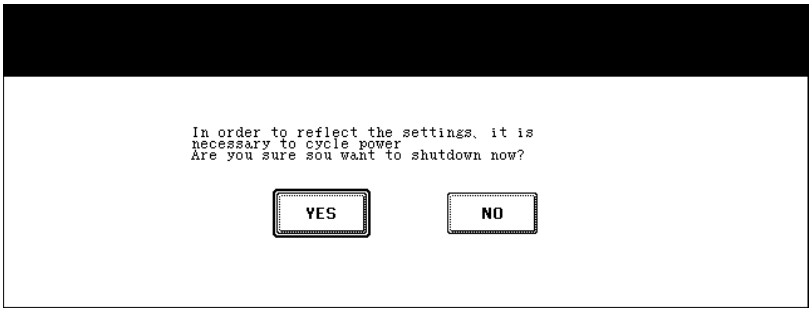
3. Confirm the settings and press the [FINISH] button.



- The shut down screen is displayed.

SUPPLEMENT: If you want to change the settings, press the [PREV] button to move back to the screen that you want to change and then repeat the operation.

4. Press the [YES] button to shut down the equipment.



- The wireless settings apply after restarting the equipment.

Disabling Wireless Network

When you enable the wireless network, the on-board NIC will be disabled.
If you want to connect the equipment to wired network via the on-board NIC, you must disable the wireless network.

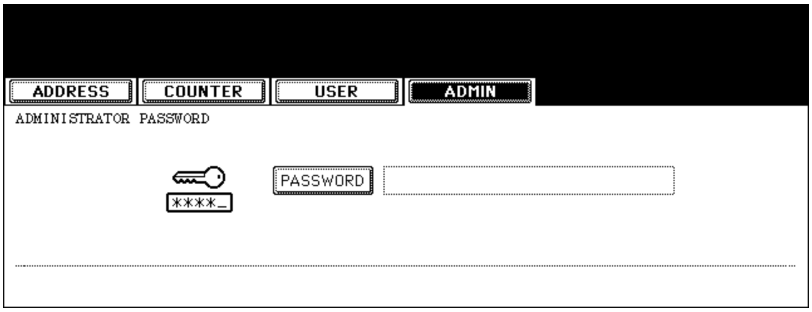
Disabling the wireless network

1. Press the [USER FUNCTIONS] button on the control panel to enter the User Functions menu.

2. Press the [ADMIN] button.

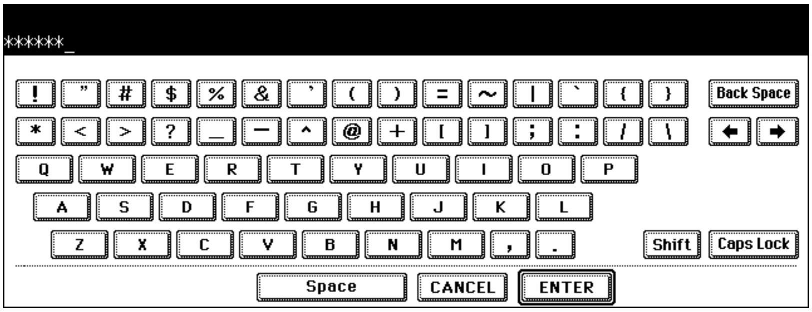
- The ADMINISTRATOR PASSWORD screen is displayed.

3. Press the [PASSWORD] button.



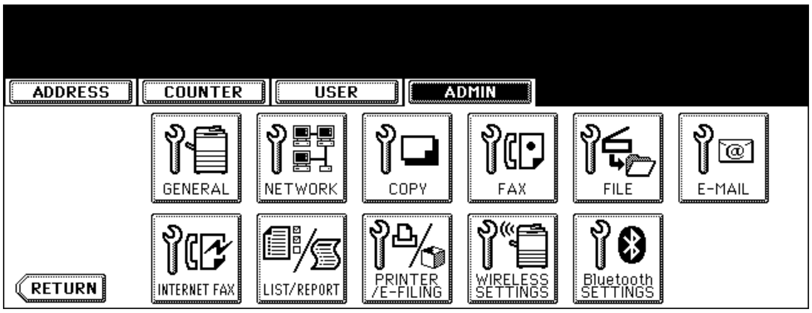
- The input screen is displayed.

4. Enter the administrator password and press the [ENTER] button.



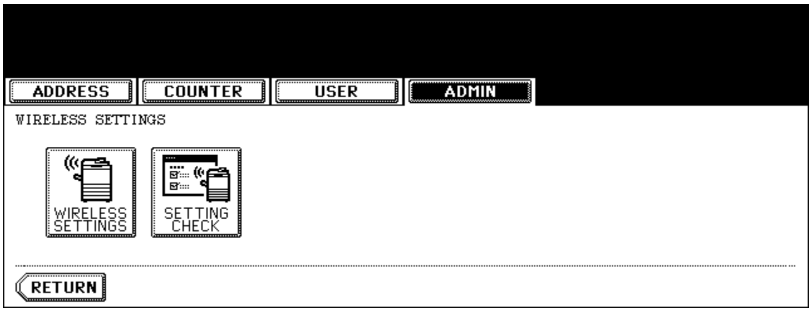
- The ADMIN menu is displayed.

5. Press the [WIRELESS SETTINGS] button.



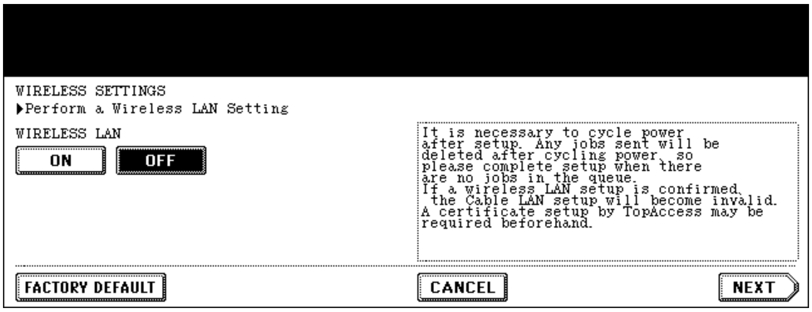
- The WIRELESS SETTINGS menu is displayed.

6. Press the [WIRELESS SETTINGS] button.



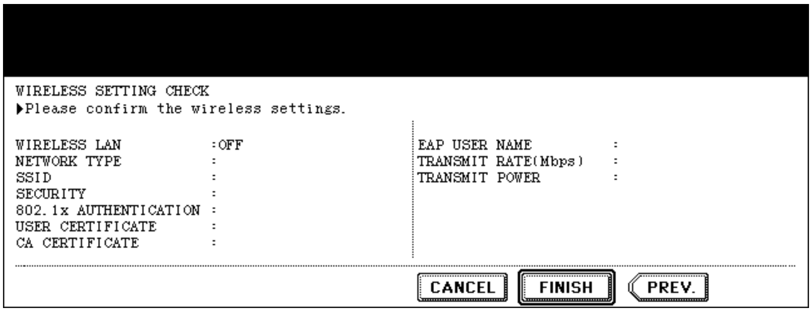
- The WIRELESS SETTINGS screen is displayed.

7. Press the [OFF] button and press the [NEXT] button.



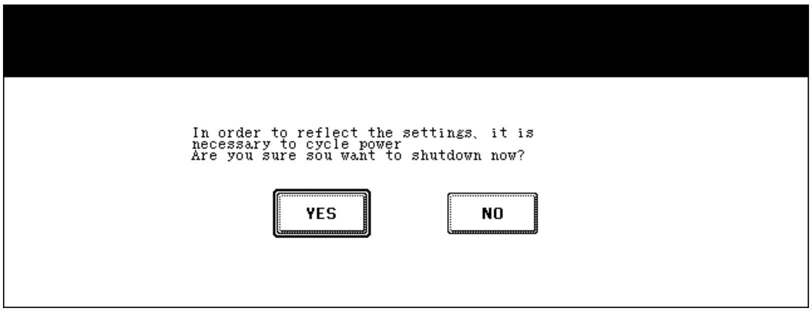
- The NETWORK TYPE screen is displayed.

8. Press the [FINISH] button.



- The shut down screen is displayed.

9. Press the [YES] button to shut down the equipment.



- The wireless settings apply after restarting the equipment.

2

APPENDIX

This section describes the specification and glossary of terms.

Specification

Physical Specification

Item	Description
Transmission Format	IEEE 1802.11g standard Direct Sequence Spread Spectrum (DSSS) Orthogonal Frequency Division Multiplexing (OFDM)
Data Transmission Speed	54, 24, 11, 5.5, 2, 1Mbps (fixed/automatic)
Access Method	CSMA/CA
Transmission Packet	IEEE 802.11g frame
Wireless Category	Low-power data transmission system (2400 to 2472MHz)
Aerial Power	10mW/MHz or below
Security	Static WEP Key Length: 40bit (WiFi Standard), 104bit, 128bit Dynamic WEP Authentication Method: TLS*1, PEAP*2 Key Exchange Method: 802.1x WPA/WPA2: PSK (TKIP, AES(CCMP)) WPA/WPA2: TLS (TKIP, AES(CCMP)) *1 Supported RADIUS server Funk Odyssey Server (WiFi Standard) Microsoft Windows 2000/2003 Server (WiFi Standard) *2 Supported RADIUS server Microsoft Windows 2000/2003 Server (WiFi Standard)
Operation Mode	Infrastructure Mode, Ad Hoc Mode
Wireless ON/OFF	Available
Wired LAN/Wireless LAN Simultaneous Operation	Not Available
Wireless LAN/Bluetooth Simultaneous Operation	Available

Troubleshooting

If any error messages are displayed on the touch panel, see the following table to troubleshoot the problems for the Wireless LAN.

Error Message	Troubleshooting
Bad certificate	Unsupported certificate is installed. Reinstall the appropriate certificate. This equipment supports md5RSA and sha1RSA certificate only.
Bad record mac	SSL Key exchange failed. Turn the power OFF and then ON to restart the equipment.
Certificate expired	The certificate has been expired. Make sure that the time is set correctly or whether the certificate is expired.
Certificate revoke	The certificate has been revoked. Ask your network administrator.
Certificate unknown	The installed CA certificate cannot work as server certificate. Make sure to install a correct CA certificate.
Decompression failure	This equipment does not support the SSL compression. Please disable the SSL compression on the RADIUS server.
Handshake failure	Unsupported encryption may be set on the server. Make sure to use the supported encryption method.
Illegal parameter	Unsupported version of the TLS protocol may be used. Make sure to use the supported version of the TLS protocol.
No certificate	No certificate is installed or you do not specify the certificate file name. Make sure to install the certificate and specify the certificate file name correctly.
Peer error certificate	Installed CA certificate cannot verify the server certificate in the RADIUS server. Make sure to install a correct CA certificate.
Peer error no certificate	The RADIUS server operates the communication with the certificate using the TLS protocol.
Peer no cipher	The RADIUS server requests the unsupported encryption for this equipment.
Peer error unsupported certificate type	This equipment uses the certificate that the RADIUS server does not support.
Peer unexpected message	The RADIUS server sends the message that is not TLS standard. Confirm the settings on the RADIUS server.
Unknown remote error type	The RADIUS server sends the alert message of illegal TLS.
Unsupported certificate	This equipment uses the certificate that the RADIUS server does not support.
Unknown ca	Installed CA certificate cannot verify the server certificate in the RADIUS server. Make sure to install a correct CA certificate.
Unable to connect	

Glossary

Ad Hoc
System to communicate directly between each wireless device without an Access Point.

AP (Access Point)
Access points serve as the bridge between wired networks and wireless networks, as well as providing bridge functions between segments and IP tunnel functions indispensable to the building of versatile, large-scale networks.

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

Channel
This term has the same meaning as a television or radio channel. In the 2.400 to 2.472GHz ISM band used by this product, the IEEE 802.11 standard provides for division into 11 channels numbered 1 to 11. Even on the same network, wireless devices operating on different channels cannot communicate with each other.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
CSMA is a method of avoiding collision by which wireless terminals listen before transmitting and do not transmit if they can hear transmissions from other wireless terminals. CSMA/CA is CSMA plus additional collision avoidance functions.

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

ESS ID (Extended Service Set ID)
The ESS ID is similar to a name assigned to the wireless LAN network to which a unit belongs. Communication between wireless terminals which have different names cannot be performed.
Wireless network can be partitioned by using different ESS ID names.

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

IEEE 802.11b/IEEE 802.11g
The wireless LAN standard established by the IEEE.

Infrastructure
System to integrate wireless LAN with wired LAN

LAN (Local Area Network)
A network configured from mutual connections between computers within a limited area.
Also called an "intranet" or "business or regional data communications network."

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

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

RSSI (Receive Signal Strength Indication)
A numeric indicator of incoming signal strength.

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

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

INDEX

INDEX

MULTIFUNCTIONAL DIGITAL SYSTEMS
Operator's Manual for Wireless LAN Module

GN-1041

TOSHIBA TEC CORPORATION
2-17-2, HIGASHIGOTANDA, SHINAGAWA-KU, TOKYO, 141-8664, JAPAN

R05082091200-TTEC
2005-09