5 Troubleshooting

I cannot access the Web-based configuration utility from the Ethernet computer used to configure the router.

- Check that the LAN LED is on. If the LED is not on, check that the cable for the LAN connection is securely connected.
- Check that your computer resides on the same subnet with the router's LAN IP address.
- If your computer act as a DHCP client, check that your computer has been assigned an IP address from the DHCP server. If not, you will need to renew the IP address. See the check/renew IP address section under '3.2 Setting up TCP/IP' for instructions.
- Use the ping command to ping the router's LAN IP address to verify the connection.
- Make sure your browser is not configured to use a proxy server.
- Check that the IP address you entered is correct. If the router's LAN IP address has been changed, you should enter the reassigned IP address instead.

I can browse the router's Web-based configuration but cannot access the Internet.

- Check the WAN LED is illuminated. If not, check the physical connection between the router and the DSL/Cable modem is OK.
- If WAN LED is illuminated, open the WAN page of the Web configuration utility and check the status group to see if the router's WAN port has successfully obtained an IP address.
- Make sure you are use the correction method (DHCP client, PPPoE client, PPTP client or Manual) as required by your ISP. Also ensure you have entered correct

settings provided by your ISP.

- For cable users, if you ISP required a fixed Ethernet card MAC address, make sure you have cloned the network adapter's MAC address to the WAN port of the router. (See the MAC Address field in WAN page.)

My wireless client cannot communicate with another Ethernet computer.

- Ensure your wireless adapter functions properly. You may open the **Device Manager** in Windows to see if the adapter is proper installed.
- Make sure your wireless client is configured to use Infrastructure mode. Also make sure the client uses the same SSID and security settings (if enabled) with the AP.
- Ensure that the wireless adapter's TCP/IP settings are correct as required by your network administrator.
- Check that the wireless adapter's MAC address is not in the MAC address list if Access Control is enabled to use a deny list. (See Wireless LAN page in Web configuration utility.)
- If you are using a 802.11b wireless adapter, check that the Operational Mode item (in Wireless LAN page) is not limited to use 802.11g. On the other hand, if you are using an 802.11g draft adapter, check the Operational Mode item is not configured to use 802.11b only.
- Use the ping command to verify the wireless client's communication.with the router's LAN port and with the opposite computer. If the wireless client can successfully ping the router's LAN port but fails to ping the opposite computer, then verify the TCP/IP settings of the opposite computer.

After I retrieved my saved configuration file, the retrieved settings do not take effect.

- After you retrieved the desired file, you must reboot the router to have retrieved settings take effect.

A Implementing 802.1x

A.1 Overview

In a typical 802.11-based wireless network, the security is often established by the proper settings of SSID broadcast, security mode, WEP keys and MAC-address-based access control. However, for a network carrying sensitive information, a more enhanced and effective security mechanism might be needed to further protect the network against eavesdroppers. In this circumstance, 802.1x would be a better choice to offer a higher-level security solution.

Compared with the WEP encryption as defined by IEEE 802.11, 802.1x function offers the following advantages:

- **Security:** When a station requests access to a network, it is required to be authenticated by a central authentication server. Only an authenticated user is granted the network acccess and thererby unauthorized access is blocked.
- **Centralized user administration:** The WEP key does not need to be set at each station. Instead, centralized user authentication, authorization and accounting are used in 802.1x.
- **Dynamic key distribution:** 802.1x can provides WEP keys on a per-user, per-session basis. It's more secure in that even an eavesdropper obtains a WEP key, it is no longer valid after a user session terminates. It is also more effective than fixed WEP keys since it spares system administrators the tasks of updating the fixed WEP keys. * Whether the WEP key can be dynamically distributed depends on the authentication method used.

A.2 802.1x Function

This section explains the 802.1x function more specifically to help you better understand how the 802.1x operates.

A.2.1 Required Components

The following components are required to implement 802.1x on a wireless network:

- **Access Point (the Authenticator) :** It acts as a intermediary between the authentication server and the supplicant.
- **802.1x station (the supplicant):** A wireless station must use 802.1x-compliant software such as Windows XP built-in Wireless Zero Configuration Utility.
- **RADIUS Server (the authentication server):** A server providing Remote Authentication Dial In User Service. It is a central server for managing authenticaticatoin, authorization and configuration for 802.1x stations.

A.2.2 Authentication Procedure

This section briefly describes the authentication procedure. In this section, the abbreviation "STA" is used to refer to the 802.1x wireless client.

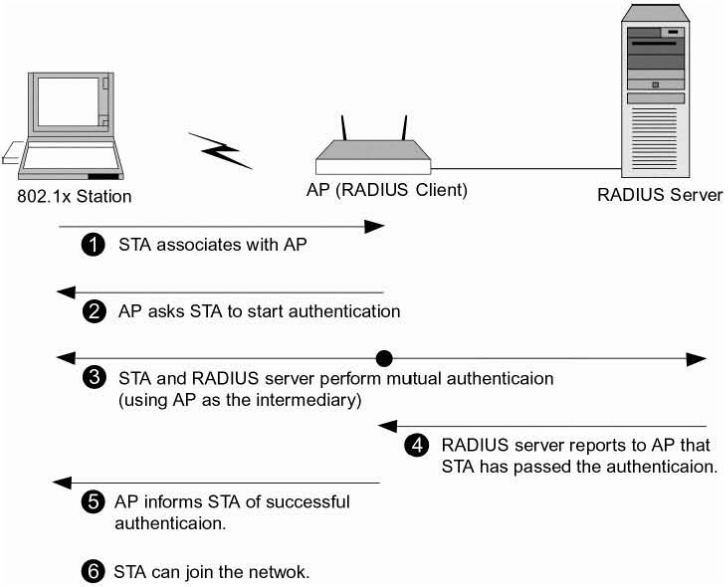
1. When an unauthenticated STA attempts to connect to the AP, the authentication starts. In this initial stage, the STA sends an EAP-start message to the AP.
2. The AP asks the STA to start the authentication. Then a series of message exchange between the AP and the STA will start:
   a. The AP replies with an EAP-request/identity message requesting the STA 's identity.
   b. The STA sends an EAP-response message containing its identity.
   c. The AP transfers all authentication-related messages to the authenticator server (the RADIUS server).
3. The STA and the RADIUS server keep changing EAP messages to perform mutual authentication. AP acts as the intermediary only.

   While the authentication procedure is performed, only EAP traffic is allowed to pass through the AP; all other traffic are blocked. That is, the STA cannot yet join the network.

   The EAP authentication mechanisms can be MD5-challenge or EAP-TLS as required.
4. When the STA passes the authentication, the RADIUS server reports to the AP.
5. The AP in turn sends an EAP-success message to the STA.

   At this point, the WEP key can be distributed. (Whether the WEP key can be distributed depends on the authentication type.)
6. The AP changes the originally controlled port state to be authorized so that other network traffic are allowed between the STA and the network.

The following figure depicts a successful authentication procedure:



A.2.3 EAP and Authentication Type

The Extensible Authentication Protocol (EAP) is a method of conducting an authentication conversation between a client and an authentication server. Intermediate devices (such as the AP) do not take part in the conversation but just relay EAP messages between the parties performing the authentication. 802.1X employs the Extensible Authentication Protocol (EAP) as an authentication framework.

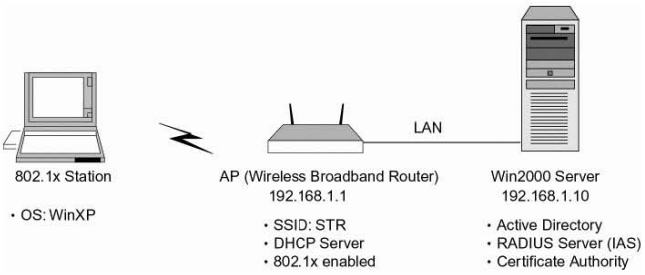
The wireless network and the RADIUS sever should use the same method to perform the authentication procedure. Two commonly used EAP authentication mechanisms are MD5-challenge and EAP-TLS, which are described as below:

- **MD5-Challenge (Message Digest version 5)**
  Using this method, the user must provide the user name and password to pass the authentication. In this type of authentication, the WEP key **cannot** be distributed.
- **EAP-TLS (Transport Layer Security).**
  Using this method, the wireless client computer has to obtain a valid digital certificate from a Central Authority (CA) or Smart Card for authentication.
  In this type of authentication, the WEP key **can be** distributed and the WEP key is created at random by the AP.

A.3 Configuration Example

This section gives a specific example to explain how to establish an 802.1x environment. The following components will be used in our example network:

- **Windows 2000 Server**
  - Active Directory is installed.
  - RADIUS server is installed using "Internet Authentication Service."
  - Certificate Services is installed (due to EAP-TLS is be used as the authentication method in our example.)
- **AP (Wireless Broadband Router)**
  - Connects to Windows 2000 Advanced Server through its LAN port.
  - The Wireless Broadband Router's DHCP server is used (192.168.1.100~192.168.1.150).
  - 802.1x and WEP Key distribution is enabled.
  - The SSID is set to "STR".
- **802.1x Station**
  - A WLAN card supporting 128-bit WEP is used.
  - Windows XP built-in Wireless Zero Configuration Utility is used for 802.1x function.
- **Authentication Mechanism**
  - EAP-TLS is used so that a session key is automatically generated for wireless packets encryption between the wireless client and the AP.



Part 1. Windows 2000 Server

Assumptions:

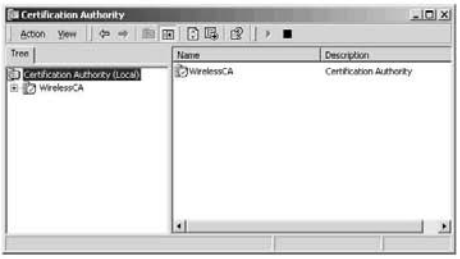
The following description assumes that Active Directory and a RADIUS server using Internet Authentication Service are already installed on the Windows 2000 server. For details on these services, refer to the online Help of Windows 2000.

In Active Directory Users and Computers, a domain user "Ian" was created and will be used in our example.

Step 1: Install Certificate Authority.

Select **Control Panel > Add/Remove Programs > Add/Remove Windows Components > Certificate Services** and then follow the on-screen prompts to proceed. For details on installing Certificate Service, refer to the online help of Windows 2000.

As this is the first CA in our example Active Directory domain, we create an **Enterprise Root CA** named **WirelessCA**.



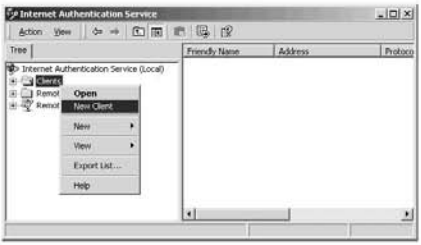
Step 2: Create a Radius client for the RADIUS server.

Install Internet Authentication Service (IAS) in Windows 2000 Server. For details on IAS, refer to the online Help of Windows 2000.

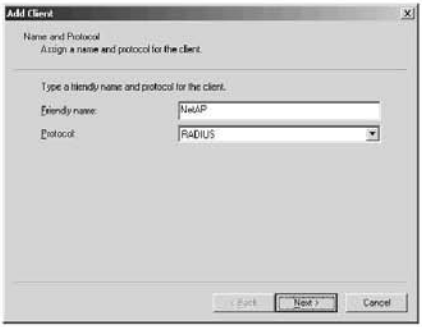
Then take the following procedures to create a RADISU client.

1. Start **Internet authentication service** in **Administrative Tools**.

2. Right-click **Client** in the **Tree** window and select **New Client** from the menu.



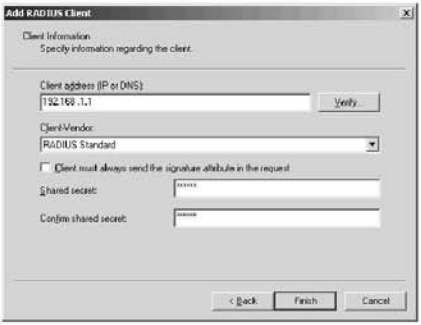
3. Set **Friendly name**. In this example, **NetAP** is set. Leave the other items in the default setting and click **Next**.



4. Set **Client address**. Enter the IP address of the AP. In this example, **192.168.1.1** is set.

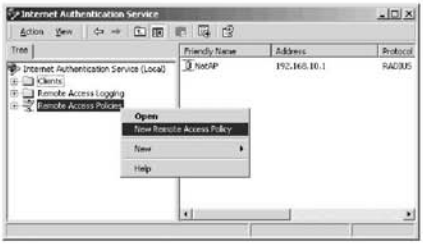
   Set **Shared secret**. Enter the password for communication between the AP and the RADIUS server. In this example, **secret** is set.

   Leave the other items in the default setting and click **Finish**.

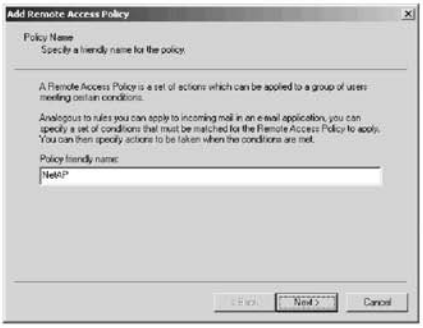


Step 3: Create Remote Access Policies.

1. In the **Tree** window, right-click **Remote Access Policies** and select **New Remote Access Policy** from the menu.



2. Enter a friendly name for this policy and click **Next**.



3. Click **Add** to add a condition. This example defines that this policy should be used when **Client-Friendly-Name** is **NetAP**.

   Various conditions are available. For details, refer to Windows 2000 online Help. Click **Next**.

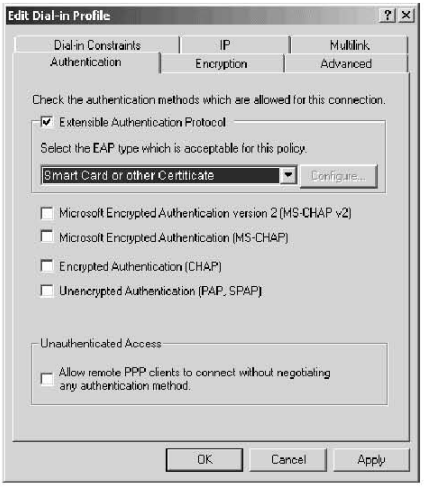
4. Select **Grant remote access permission**. Click **Next**.

5. Click the **Edit Profile** button and select the **Authentication** tab.

   Place a check mark in the **Extensible Authentication Protocol** check box.

   Select **Smart Card or other Certificate** for the EAP type.

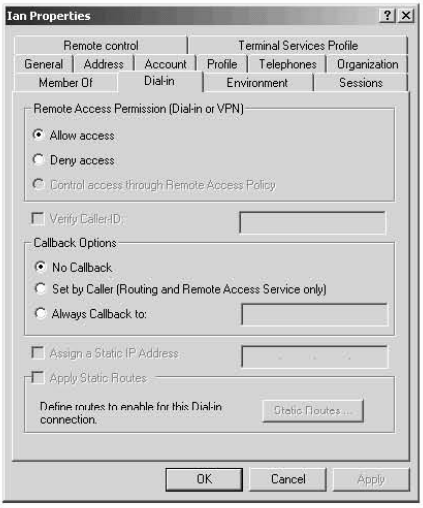
   Click **OK** and then **Finish**.



Step 4: Enable remote access login for the user.

1. Go to **Active Directory Users and Computers** and double-click on the user ("lan" in our example) to bring up its properties window.

2. Select the **Dial-in** tab and select **Allow access**. Click **OK**.



Part 2: Access Point

The following is the setting procedure for the AP.

Step 1: Setting the 802.1x function at the AP.

The following procedure is to enable the 802.1x function. The other settings of the **Wireless LAN** page are omitted.

1. Enter the Web-Based Configuration Utility of the Wireless Broadband Router and go to the **Wireless LAN Security** page.
2. In 802.1x group:

   802.1x: Select **Used**.

   WEP Key Distribution: Select **Enable**.

   If WEP key distribution is disabled, you will need to manually set the WEP keys instead.

   Re-authentication: Select **Enable**. This enables periodic 802.1x client re-authentication. When authentication times out, the authenticator (AP) will request the stations to be reinitiate the authentication process.

Interval: Specify how often the re-authentication occurs.

Key Length: Set **5byte** in this example.

3. In RADIUS group:

RADIUS Server1: Select **Enable**.

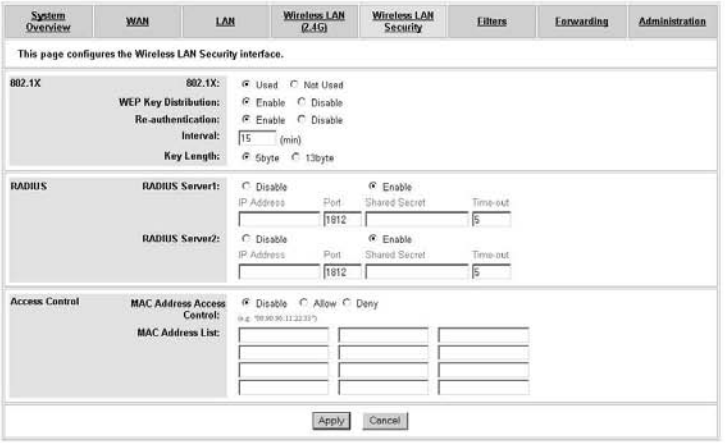
IP Address: Enter the IP address of the RADIUS server. In this example, set **192.168.1.10**.

Port: Use the default **1812**. The RADISU server uses this port for authentication.

Shared Secret: This is a password shared between the AP and the RADIUS server. In this example, set **secret**.

Time-out: Enter a response time-out value. In this example, set 5.

RADIUS Server2: Select **Disabled** unless you have a backup RADIUS server.



Part 3: 802.1x Station

The following provides the setting procedure for the 802.1x station.

Step 1. Install Certificate.

1. Temporarily, have the station join the wired network. Then open the Web browser and connect to the following URL:

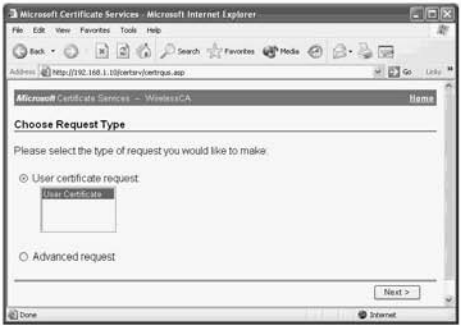
   http://<the CA's IP address>/certsrv

   In this example, type **http://192.168.1.10/certsrv** in the URL field.

2. Log on to the domain using the user account "lan" that has been allowed remote access dial-in.

3. Select **Request a certificate** and click **Next**.

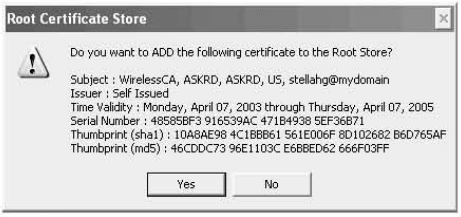
4. Select **User certificate request: User Certificate** and click **Next**.



5. Click **Submit** and then waiting for server response.

6. Click **Install this certificate**.

7. You'll receive a confirmation message about accepting the certificate, click **Yes**



Notes:

1. To issue a certificate from the certificate authority and install it, [Certificate Service Web Enrollment Support] needs to have been installed in the certificate authority.
2. The above example issues and installs a certificate through the network. You can also export the certificate into a file and then import it to another wireless client. For more information, refer to the online Help of the certificate authority.

Step 2. Setting the 802.1x function in the Wireless LAN station

Next, set the 802.1x function.

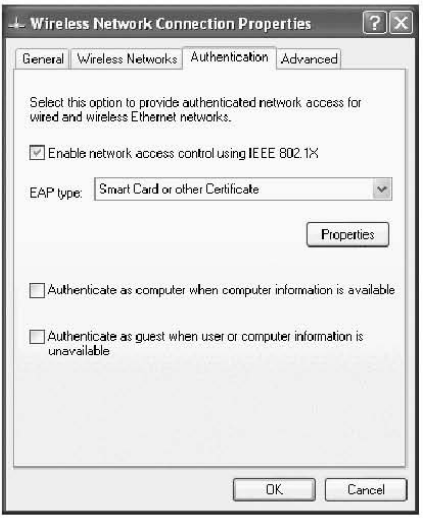
1. Launch Windows XP built-in Wireless Zero Configuration Utility and then select the **Wireless Networks** tab.

   Make sure the **Use Windows to configure my wireless network settings** check box is ticked.

2. Select the **Authentication** tab.

   Select the **Enable network access control using IEEE 802.1x** check box.

   Select **Smart Card or other Certificate** from the **EAP type** list. Then click **Properties**.

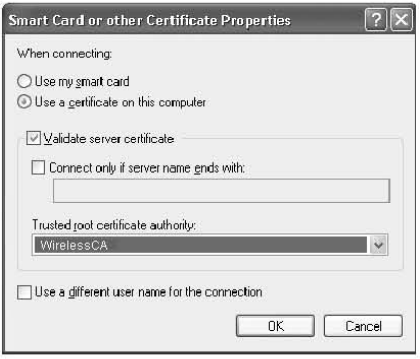


3. Select the **Use a certificate on this computer** radio button.

   Select the **Validate server certificate** check box.

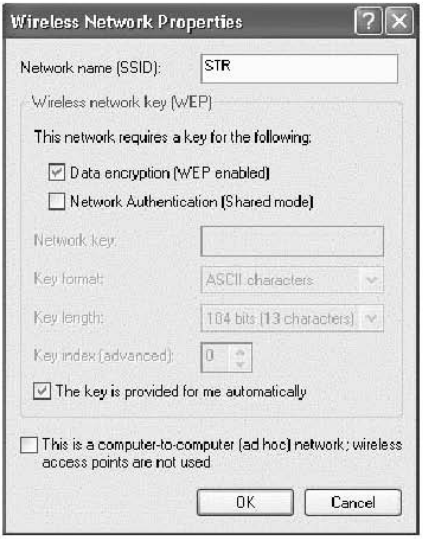
   Select a reliable certificate authority from the **Trusted root certificate authority** list.

   In this example, select the certificate authority, WirelessCA, which was installed in Windows 2000 Server.

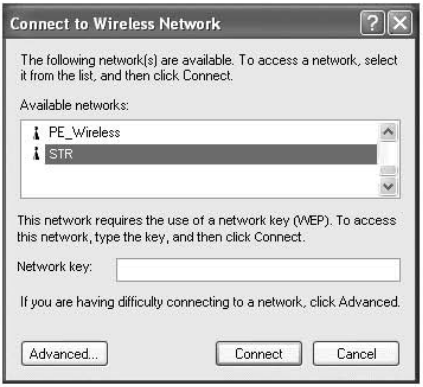


Step 3. Connect to the Wireless Network

1. Make sure the properties of the target wireless network (STR) are set to use **Data encryption (WEP enabled)**, and ensure **The key is provided for me automatically** is also selected

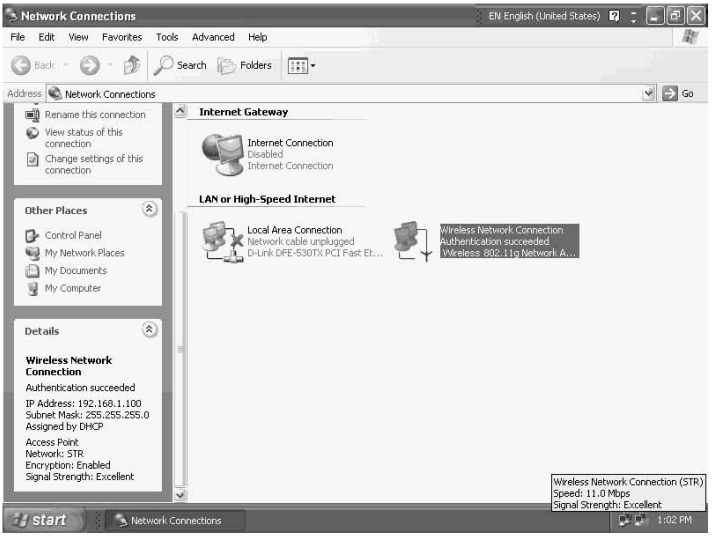


2. Open the **Connect to Wireless Network**. Select the target 802.1x wireless network and click **Connect**.



Step 4. Check the connection status.

A successful wireless connection is shown as the figure below. Highlighting the icon of the wireless adapter displays the connection details. The wireless client has been successfully authenticated and obtained an IP address (192.168.1.100) from the DHCP server of the Wireless Broadband Router.



Re-authentication

When re-authentication interval passes (15 minute is set in our example), the re-authentication will be performed.

B Specification

B.1 Hardware

- 125MHz MIPS CPU
- 16MB SDRAM
- 4MB Flash Memory
- Wireless: 802.11g draft MiniPCI module
- One external and one built-in antennas for wireless technology

Interface

- One 10/100 Base-TX RJ-45 auto sensing and crossover Ethernet WAN port for Broadband connection (Cable/DSL or direct Ethernet)
- Four RJ-45 LAN ports for 10/100Base-TX auto sensing & crossover Ethernet Switch LAN connection
- 802.11g draft wireless LAN
- One external and one built-in antennas for wireless technology

Physical

- Front Panel: 7 LEDs (Power x 1, LAN x 4, WAN x 1, Wireless x 1)
- Back Panel: Reset / Load Default button, Power Jack, RJ-45 LAN Port x 4, RJ-45 WAN Port x 1
- Dimensions
  170mm (L) x 135mm (W) x 45mm (H)
- Case types:
  Stand up / Lay down

Power Adapter and Environmental Requirement

- Power Adapter:
  Input AC110V, Output 12V AC, 1A
- Temperature: 0 to 40°C (operation), -20 to 70 °C (storage)
- Relative Humidity: 5% to 90% (non-condensing)

Electromagnetic Compliance

- FCC Part 15 Class B
- CE
- EMI/Immunity: VCCI class B
- PTT: JATE

B.2 Software

WAN Port Features

- PPPoE (PPP over Ethernet) Client with Keep Alive/Connect On Demand Support
- PAP and CHAP Authentication
- DHCP Client
- MAC Address Cloning
- Settable and Changeable IP Address

LAN Port Features

- DHCP Server
- Settable and Changeable IP Address

Router Features

- NAT
- Firewall Support
- Bridge Mode Support
- 802.1D Spanning Tree Bridging
- IP Filtering, IP Forwarding

- DMZ Hosting
- DNS Forwarding
- UPNP Support
- Microsoft NetMeeting Passthrough Support
- Microsoft XP Messenger Passthrough Support

Security Features

- PAP and CHAP Authentication
- ASCII/HEX Format 64/128 Bit WEP Key for Wireless LAN
- Allow/Deny List for Wireless LAN
- 802.1x Security for Wireless LAN
- Supports IP packets filtering based on IP address, port number, and protocol
- VPN Support (IPSec Passthrough, and PPTP Passthrough)

Wireless LAN Features

- Fully compatible to 802.11g draft standard
- Direct Sequence Spread Spectrum (DSSS) technology exploitation
- Seamless roaming within wireless LAN infrastructure
- Low power consumption via efficient power management

Configuration and Management Features

- Configurable through Web Browser via WAN/LAN
- Software Upgrade
- DHCP Server function for IP distribution to local network users
- NTP/Manual System Clock
- Configuration Saving/Retrieving
- Event Log