DRBAP as an AP cannot see each other, and wireless-to-wireless traffic between the STAs is blocked. When the setting is set to **All APs in This Subnet**, traffic among wireless users of different APs in the same IP subnet is blocked. The behaviors are illustrated in the following figures.

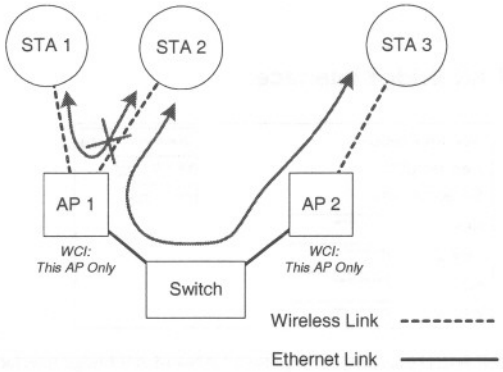

Fig. 50. Behavior of the "This AP Only" wireless client isolation option.

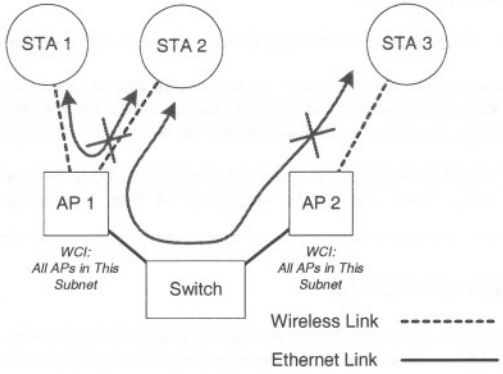

Fig. 51. Behavior of the "All APs on This Subnet" wireless client isolation option.

As illustrated in Fig. 50 when AP 1 and AP 2 are using the "This AP Only" option, wireless traffic between STA 1 and STA 2 is blocked by AP 1, while wireless traffic between STA 2 and STA 3, which are associated with different APs, is still allowed. If the "All APs in This Subnet" option is used as shown in Fig. 51, AP 1 and AP 2 communicates with each other via an inter-AP protocol to share their STA association information to block wireless traffic among all the STAs.

There are up to 7 security modes depending on AP model variations:

- **Open System.** No authentication, no data encryption.

- **Static WEP.** WEP (Wired Equivalent Privacy) keys must be manually configured.
- **Static TKIP (WPA-PSK).** Only TKIP (Temporal Key Integrity Protocol) mechanism of WPA (Wi-Fi Protected Access) is enabled. In this mode, you have to specify the **Pre-shared key**, which will be used by the TKIP engine as a *master key* to generate keys that actually encrypt outgoing packets and decrypt incoming packets.

NOTE: The number of characters of the **Pre-shared key** setting must be at least 8 and can be up to 63.

- **IEEE 802.1x EAP without Encryption (EAP-MD5).** The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. No data encryption.
- **IEEE 802.1x EAP with Static WEP (EAP-MD5).** The IEEE 802.1x functionality is enabled and the user-name/password-based EAP-MD5 authentication is used. Data encryption is achieved by static WEP.
- **IEEE 802.1x EAP with Dynamic WEP (EAP-TLS, EAP-TTLS, PEAP).** The IEEE 802.1x functionality is enabled and dynamic WEP key distribution authentication (EAP-TLS, EAP-TTLS, or PEAP) is used. Data encryption is achieved by dynamic WEP.
- **IEEE 802.1x EAP with Dynamic TKIP (WPA).** This is a full WPA mode, in which both the TKIP and IEEE 802.1x dynamic key exchange mechanisms are enabled. The AP is highly secured in this mode.

In the above security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1x functionality is enabled. See Section 3.5.3 for more information about IEEE 802.1x and RADIUS.

When WEP is enabled by a security mode, the **Key length** can be specified to be **64 Bits** or **128 Bits**. The **Selected key** setting specifies the key to be used as a *send-key* for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the AP side.

NOTE: Each field of a WEP key setting is a *hex-decimal* number from 00 to FF. For example, when the security mode is **Static WEP** and the key length is **64 Bits**, you could set Key 1 to "00012E3ADF".

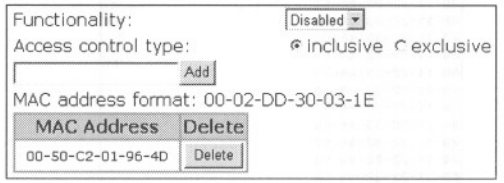

Fig. 52. MAC-address-based access control settings for an AP interface.

With **MAC-Address-Based Access Control**, you can specify the wireless client computers that are permitted or not permitted to connect to the AP interface. When the table type is set to **inclusive**, entries in the table are permitted to connect to the AP interface. When the table type is set to **exclusive**, entries in the table are not permitted to connect to the AP interface.

To *deny* wireless clients' access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.
2. Set the **Access control type** to *exclusive*.
3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.
4. Repeat Steps 3 for other wireless clients.

To *grant* wireless clients' access to the wireless network:

1. Select *Enabled* from the **Functionality** drop-down list.
2. Set the **Access control type** to *inclusive*.
3. Specify the MAC address of a wireless client to be denied access, and then click **Add**.
4. Repeat Steps 3 for other wireless clients.

To delete an entry in access control table:

- Click **Delete** next to the entry.

NOTE: The size of the access control table is 64.

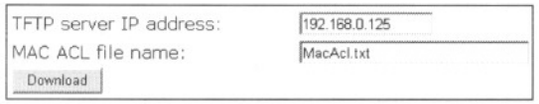

Fig. 53. MAC ACL download settings.

Instead of manually entering MAC addresses to the access control table one by one, you can prepare a text file that contains all the MAC addresses and put it on a TFTP server, and then command the AP to download the MAC ACL (Access Control List) file from the TFTP server. Fig. 54 shows the contents of a sample ACL file.

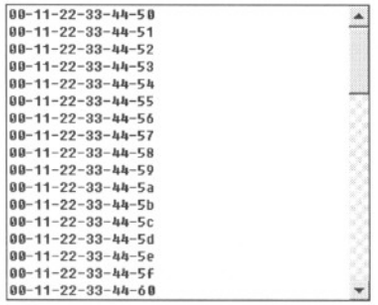

Fig. 54. Sample MAC ACL file.

To download a MAC ACL file from a TFTP server:

1. Specify the IP address of the TFTP server in the **TFTP server IP address** text box.
2. Specify the name of the MAC ACL file on the TFTP server in the **MAC ACL file name** text box.
3. Click **Download**.

3.5.2.2. LAN-to-LAN Bridge Interface

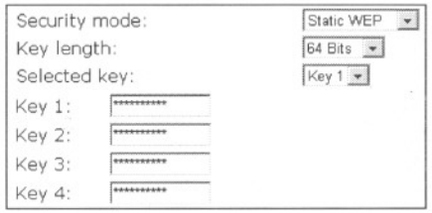

Fig. 55. IEEE 802.11g security settings for a LAN-to-LAN bridge interface.

Data transmitted over the bridge links can be encrypted by WEP (Wired Equivalent Privacy). Therefore, there are 3 security modes:

- **Open System.** No data encryption.
- **Static WEP.** WEP (Wired Equivalent Privacy) keys must be manually configured.

When Static WEP is chosen as the security mode, the **Key length** can be specified to be **64 Bits** or **128 Bits**. The **Selected key** setting specifies the key to be used as a *send-key* for encrypting outgoing WDS traffic. All 4 WEP keys are used as *receive-keys* to decrypt incoming WDS traffic.

NOTE: Each field of a WEP key setting is a *hex-decimal* number from 00 to FF. For example, when the security mode is **Static WEP** and the key length is **64 Bits**, you could set Key 1 to "00012E3ADF".

3.5.3. IEEE 802.1x/RADIUS

IEEE 802.1x *Port-Based Network Access Control* is a new standard for solving some security issues associated with IEEE 802.11, such as lack of user-based authentication and dynamic encryption key distribution. With IEEE 802.1x and the help of a RADIUS (Remote Authentication Dial-In User Service) server and a user account database, an enterprise or ISP (Internet Service Provider) can manage its mobile users' access to its wireless LANs. Before granted access to a wireless LAN supporting IEEE 802.1x, a user has to issue his or her *user name* and *password* or *digital certificate* to the backend RADIUS server by EAPOL (Extensible Authentication Protocol Over LAN). The RADIUS server can record accounting information such as when a user logs on to the wireless LAN and logs off from the wireless LAN for monitoring or billing purposes.

The IEEE 802.1x functionality of the advanced wireless access point is controlled by the *security mode* (see Section 3.5.2.1). So far, the wireless access point supports two authentication mechanisms—EAP-MD5 (Message Digest version 5) and EAP-TLS (Transport Layer Security). If EAP-MD5 is used, the user has to give his or her *user name* and *password* for authentication. If EAP-TLS is used, the wireless client computer automatically gives the user's *digital certificate* that is

stored in the computer hard disk or a smart card for authentication. And after a successful EAP-TLS authentication, a session key is automatically generated for wireless packets encryption between the wireless client computer and its associated wireless access point. To sum up, EAP-MD5 supports only user authentication, while EAP-TLS supports user authentication as well as dynamic encryption key distribution.

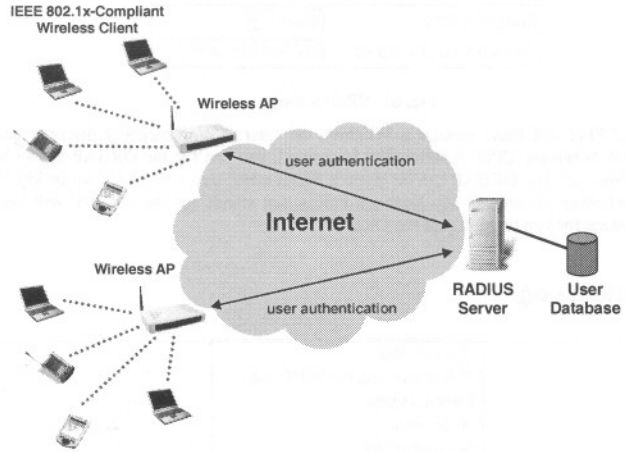

Fig. 56. IEEE 802.1x and RADIUS.

A wireless access point supporting IEEE 802.1x can be configured to communicate with two RADIUS servers. When the primary RADIUS server fails to respond, the wireless access point will try to communicate with the secondary RADIUS server. The administrator can specify the length of timeout and the number of retries before communicating with the *secondary* RADIUS server after failing to communicate with the primary RADIUS server.

An IEEE 802.1x-capable wireless access point and its RADIUS server(s) share a secret key so that they can authenticate each other. In addition to its IP address, a wireless access point can identify itself by an NAS (Network Access Server) identifier. Each IEEE 802.1x-capable wireless access point must have a *unique* NAS identifier.

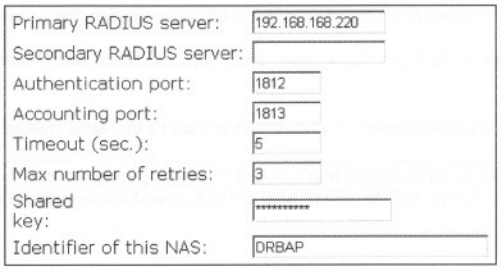

Fig. 57. IEEE 802.1x/RADIUS settings.

NOTE: This feature is only available for AP interfaces. If the DRBAP is set to be in **Bridge Repeater** mode, the **IEEE 802.11, IEEE 802.1x/RADIUS** section of the management UI will be hidden from accessing.

TIP: Refer to the IEEE 802.1x-related white papers on the accompanying CD-ROM for more information about deploying secure WLANs with IEEE 802.1x support.

3.6. Configuring Advanced Settings

3.6.1. Packet Filters

The DRBAP provides layer 2 (Ethernet Type Filters), layer 3 (IP Protocol Filters), and layer 4 (TCP/UDP Port Filters) filtering capabilities. The configuration processes for the filters are similar.

Functionality: whether this filtering capability is *enabled* or *disabled*.

Policy for matched packets: how a matched packet is processed—*discard* or *pass*.

To enable a filtering rule: select the check box to the left of the rule.

3.6.1.1. Ethernet Type Filters

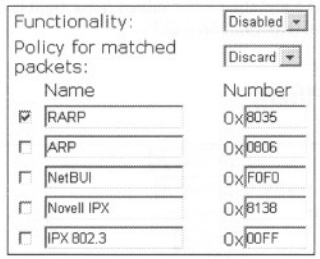

Fig. 58. Ethernet type filters settings.

The *Ethernet type* filed of the MAC (Media Access Control) header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the hex-decimal Ethernet type number and give the rule a name.

3.6.1.2. IP Protocol Filters

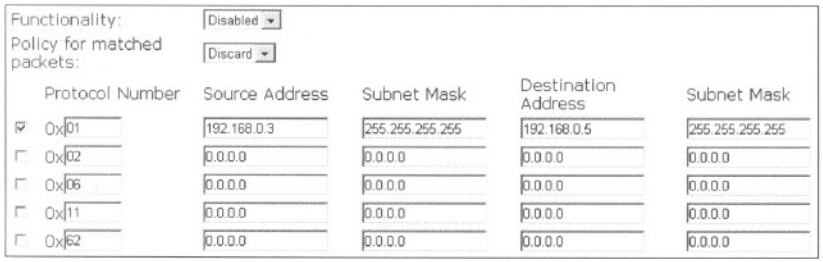

Fig. 59. IP protocol filters settings.

The protocol, source address, and destination address fields of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the hex-decimal protocol number, source IP address range (Source IP Address AND Source Subnet Mask), and destination IP address range (Destination IP Address AND Destination Subnet Mask).

A source (destination) IP address range is determined by performing an AND operation on the source (destination) IP address field and the source (destination) subnet mask field. For example, if the source IP address field is 192.168.0.1 and the source subnet mask field is 255.255.255.0, the resultant source IP address range is 192.168.0.0 to 192.168.0.255.

3.6.1.3. TCP/UDP Port Filters

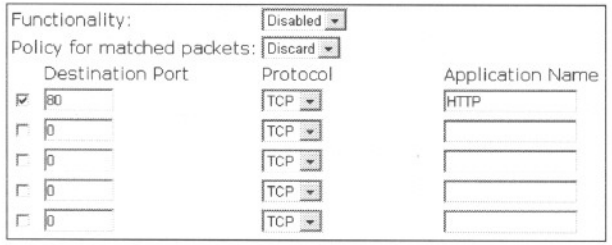

Fig. 60. TCP/UDP port filters settings.

The *destination port* field the TCP or UDP header of a packet incoming from the WLAN or Ethernet interface is inspected for filtering. In a rule, specify the decimal **Destination Port**, **Protocol** type (TCP/UDP), and the name of the higher-level protocol (**Application Name**).

3.6.2. Management

3.6.2.1. UPnP

Fig. 61. UPnP settings.

UPnP (Universal Plug and Play) enables a Windows XP user to automatically discover peripheral devices by HTTP. When the UPnP functionality is enabled, you can see the DRBAP in My Network Places of Windows XP. The DRBAP can be given a *friend name* that will be shown in My Network Places. *Double-clicking* the icon in My Network Places that stands for the DRBAP will launch the default Web browser for you to configure the DRBAP.

3.6.2.2. System Log

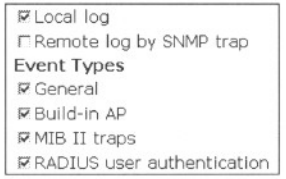

Fig. 62. System log settings.

System events can be logged to the on-board RAM of the DRBAP (**Local log**) or sent to a remote computer on which an SNMP trap monitor program runs (**Remote log by SNMP trap**). See the next subsection for more information about SNMP trap settings.

The system events are divided into the following categories:

- **General**: system and network connectivity status changes.
- **Built-in AP**: wireless client association and WEP authentication status changes.
- **MIB II traps**: *Cold Start*, *Warm Start*, *Link Up*, *Link Down* and *SNMP Authentication Failure*.
- **RADIUS user authentication**: RADIUS user authentication status changes.

NOTE: The *SNMP Authentication Failure* trap is issued when using an incorrect community string to manage the DRBAP via SNMP and the SNMP MIB II OID, **snmpEnableAuthenTraps**, is enabled (*disabled* by default).

3.6.2.3. SNMP

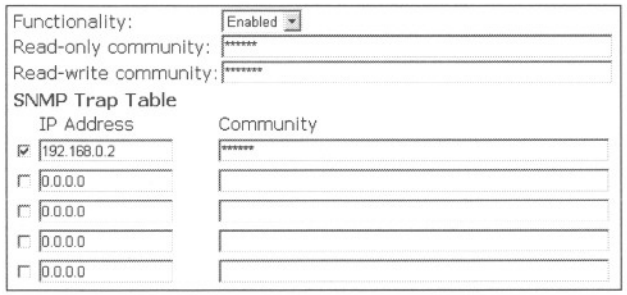

Fig. 63. SNMP settings.

The SNMP (Simple Network Management Protocol) functionality can be disabled, and you can specify the name (used as a *password*) of the read-only and read-write community. In addition, up to 5 SNMP trap targets can be set in the **SNMP Trap Table**.

To specify a trap target:

1. Type the IP address of the target host.
2. Type the **Community** for the host.
3. Select the corresponding check box next to the IP address text box.

Appendix A: Default Settings

TIP: Press the **SF-Reset** switch on the housing of a *powered-on* DRBAP to reset the configuration settings to factory-default values.

Setting Name	Default Value
Global	
User Name	root
Password	root
Operational Mode	AP Repeater
IEEE 802.11g	
Regulatory Domain	FCC (U.S.)
Channel Number for WLAN 1	11
Channel Number for WLAN 2	6
SSID for WLAN 1	wireless1
SSID for WLAN 2	wireless2
Transmission Rate for WLAN 1	Auto
Transmission Rate for WLAN 2	11Mbps
MAC Address of WLAN 1 and of WLAN 2	See the label on the housing of the DRBAP.
WDS Links	None
Security Mode	Open System
Selected WEP Key	Key #1
WEP Key #1	00-00-00-00-00
WEP Key #2	00-00-00-00-00
WEP Key #3	00-00-00-00-00
WEP Key #4	00-00-00-00-00
LAN Interface	
Method of obtaining an IP Address	Set manually
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Management	
UPnP	Enabled
System Log	Local Log
SNMP	Enabled
SNMP read community	public
SNMP write community	private

Appendix B: Troubleshooting

- **Check the following first:**
  - Make sure that the power of the DRBAP is on and the Ethernet cables are connected firmly to the RJ-45 jacks of the DRBAP.
  - Make sure that the LED ALV of the DRBAP is blinking to indicate the DRBAP is working.
  - Make sure the types of the Ethernet cables are correct. Recall that there are two types—*normal* and *crossover*.
- **The DRBAP has been set to obtain an IP address automatically by DHCP. How can I know its acquired IP address so that I can manage it using a Web browser?**
  - Use the utility, Wireless Router/AP Browser (**WLBrwsr.exe**), in the "**Utilities**" folder on the companion CD-ROM disc. This utility can discover nearby DRBAPs and show their MAC addresses and IP addresses. In addition, it can launch the default Web browser on your computer.

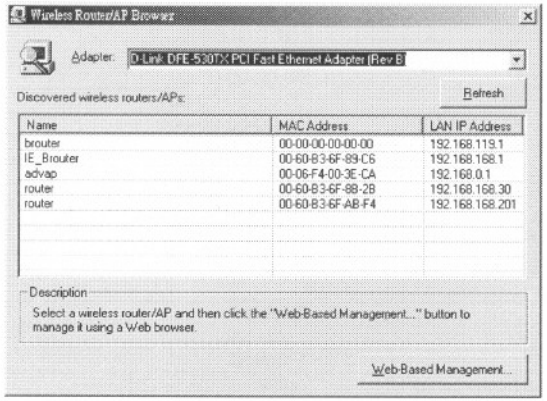

Fig. 64. Wireless Router/AP Browser.

- **The DRBAP stops working and does not respond to Web management requests.**
  - The firmware of the DRBAP may be stuck in an incorrect state.
    - Unplug the power connector from the power jack, and then re-plug the connector to restart the DRBAP.
    - Contact our technical support representatives to report this problem, so that the bugs can be static in future firmware versions.
  - If the DRBAP still does not work after restarting, there may be hardware component failures in the DRBAP.

- Contact our technical support representatives for repair.

Appendix C: Additional Information

C-1: Firmware Upgrade Using Xmodem Upgrade

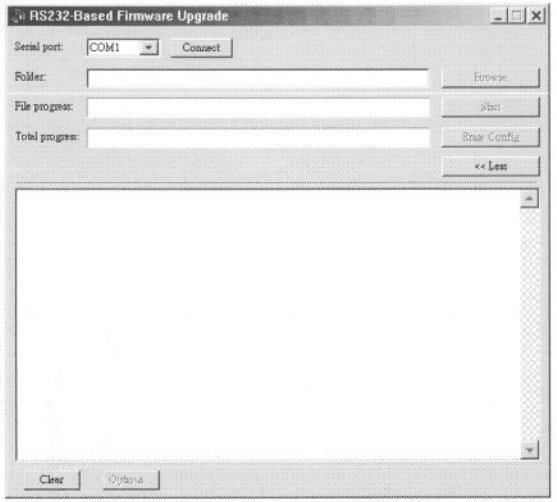

Fig. 65. Xmodem Upgrade.

To upgrade the firmware of DRBAP using Xmodem Upgrade over RS232:

1. Power off the DRBAP whose firmware will be upgraded.
2. Connect the managing PC and the DRBAP with an *RS232 Null Modem* cable.
3. Select the serial port (COM1 or COM2) you use for connecting the device from the **Serial port** drop-down list and click **Connect**.
4. Chose the folder in which the firmware files reside by click **Browse**.
5. Power on the DRBAP and you'll see bootup information.
6. Click **Start** to begin upgrade the firmware of the DRBAP.
7. You will be prompted when the upgrade process completes.

Click **Erase Config** to reset the configuration settings of the DRBAP to default values.