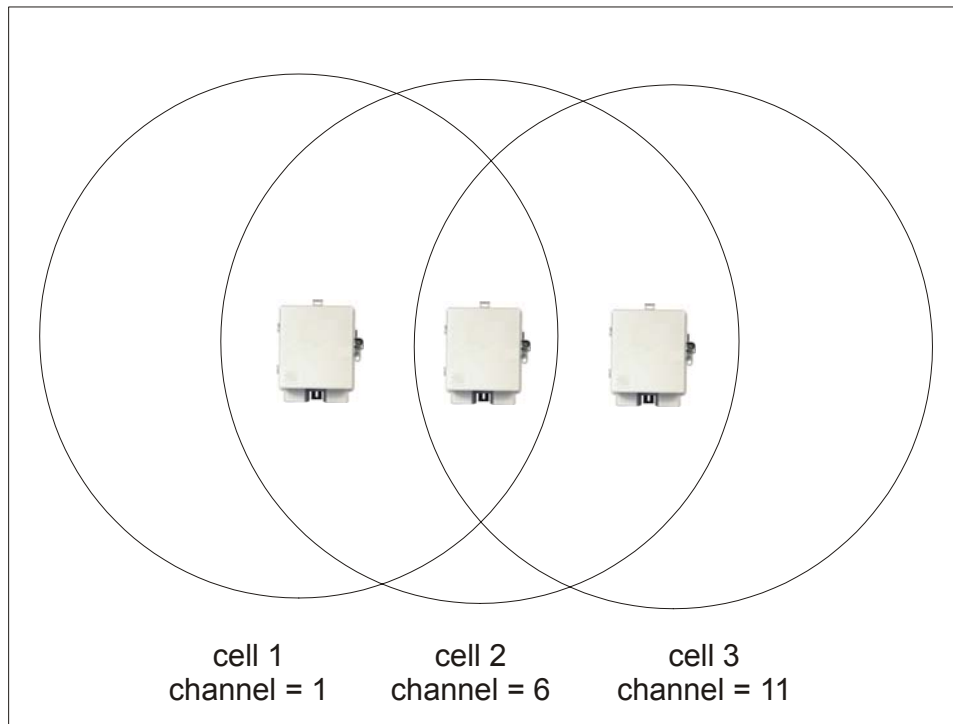


In North America, you would create the following installation (Figure 18).



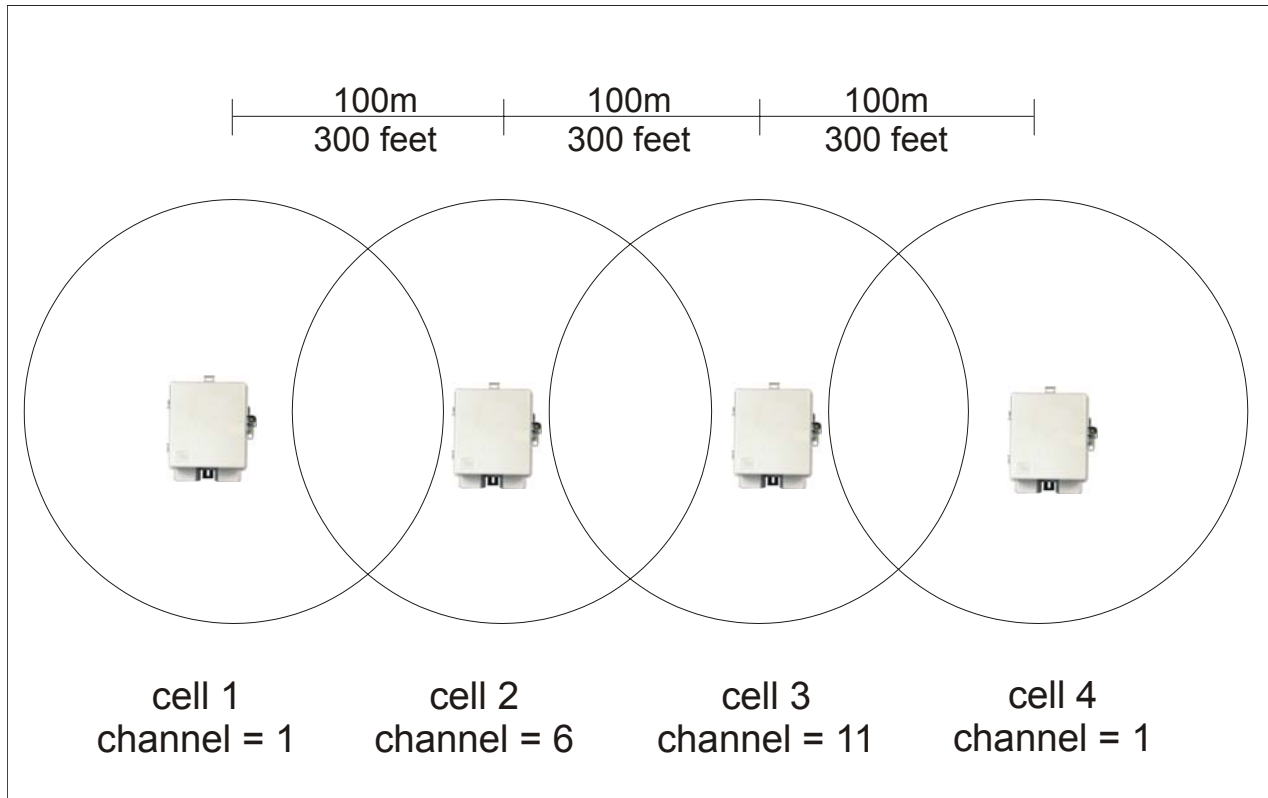
06-LPS20xR1

**Figure 18. North America Installation**



Transmission delays are reduced by using different operating frequencies.

However, it is possible to stagger your cells to reduce overlap and increase channel separation (Figure 19).



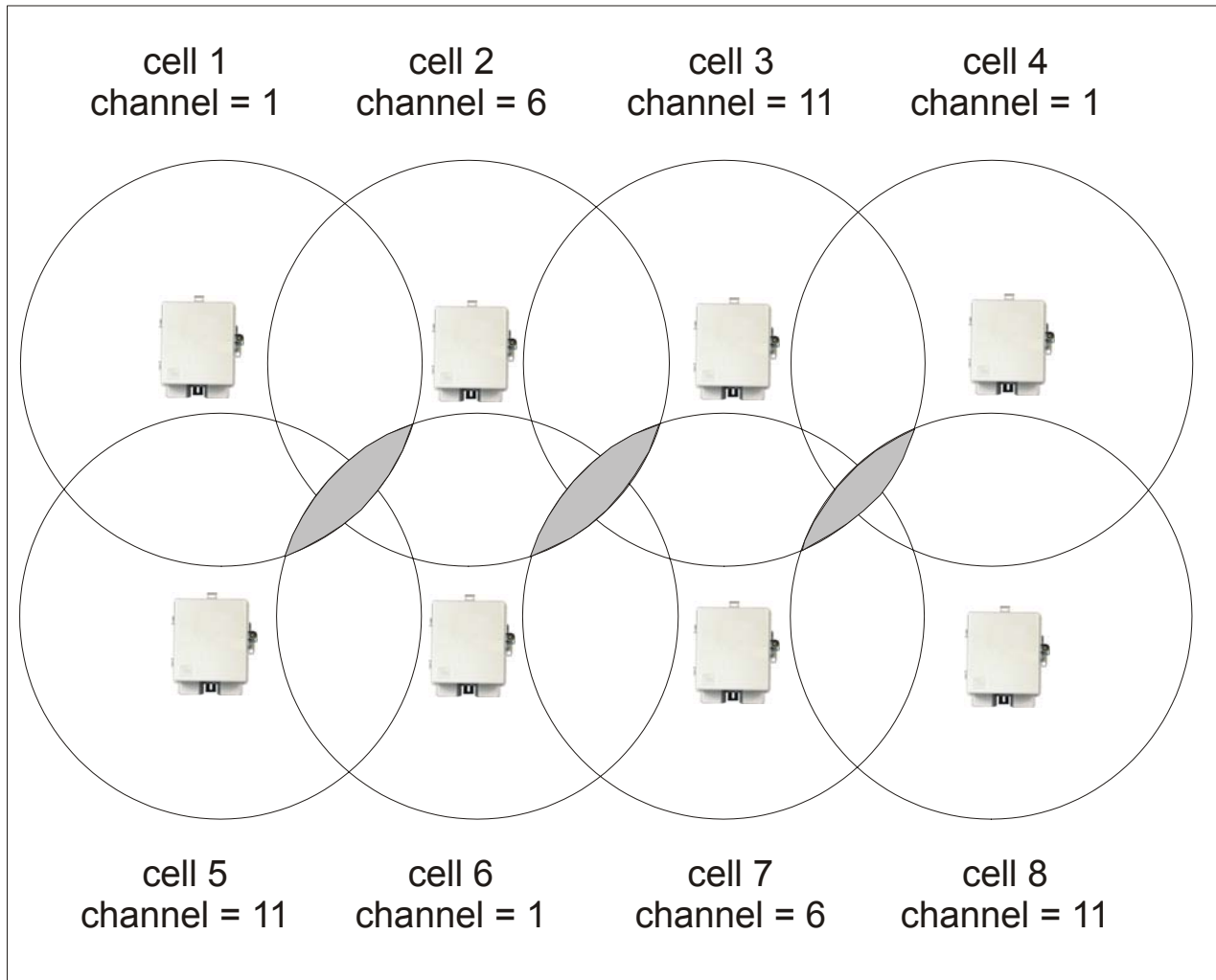
07-LPS20xR1

**Figure 19. Stagger Cells**



Figure 19 uses only three frequencies across multiple cells (North America).

This strategy can be expanded to cover an even larger area using three channels (Figure 20).



08-LPS20xR1

**Figure 20. Expanded Coverage using Three Channels**



The areas in gray indicate where two cells overlap that are using the same frequency.

## DISTANCE BETWEEN ACCESS POINTS

In environments where the number of wireless frequencies are limited, it can be beneficial to adjust the receiver sensitivity of the LPS-20x. To make the adjustment, open the **Wi-Fi** page on the **Wireless** menu.

For most installations, the **Large** setting should be used. However, if you are installing multiple LPS-20xs and the channels available to you do not provide enough separation, then reducing the receiver sensitivity can help you reduce the amount of crosstalk between the LPS-20xs.

Another benefit to using reduced settings is that it will improve roaming performance. Client stations will switch between LPS-20xs more frequently.



The **Distance Between Access Points** option provides the best performance benefit when client stations are equipped with wireless adapters that are configured with the same setting. However, not all manufacturers support this setting.

## CONFIGURING THE CONNECTION TO THE ACCESS CONTROLLER

The LPS-20x uses the services of an access controller to manage access to the public access network.

Unlike a traditional bridge which automatically forwards all traffic between ports, the LPS-20x features an intelligent bridge which can apply filters to maintain the security of the network. When the security filters are active, the LPS-20x only allows traffic to flow between itself and the access controller. This prevents wireless customers from accessing resources on the backbone LAN that interconnects the LPS-20x and the access controller.

### SECURITY FILTERS

To configure the connection to the access controller and enable the intelligent bridge, do the following:

1. On the main menu, click **Security** and then click **Access controller**. The *Access controller* configuration page opens.

2. By default, the LPS-20x uses the default gateway as the access controller.
  - If you are using static IP addressing, make sure that you set the default gateway on the LPS-20x to be the access controller.
  - If you are using a DHCP server on your network, make sure that it is configured to return the IP address of the access controller as the default gateway. (The access controller is configured to do this by default.) Alternately, you can specify the MAC address of the access controller.
3. Clear the security filters check box if you are connecting to a wired LAN (refer to [Connecting to a wired LAN on page 92](#)).
4. Click **Save**.

### ACCESS CONTROLLER SHARED SECRET

To maintain the security of network logins, the ADC access controller will only accept location-aware information from a LPS-20x that has a matching shared secret to its own.

## INTELLIGENT BRIDGE

The intelligent bridge uses filters to only allow traffic to flow between itself and an access controller. Traffic is filtered as it is received by the upstream, downstream, or wireless ports. Each port has its own specific set of filters. Filters apply only to data being received by the port (incoming traffic).

### Upstream Port Filter (incoming traffic)

#### Accepted

- Any traffic from the access controller.
- Certain address management protocols (ARP, DHCP) regardless of their source address.
- HTTPS traffic regardless of its source address. (This permits local or remote management stations to access the LPS-20x management tool.)
- Any traffic addressed to the LPS-20x.
- All broadcast traffic.

#### Blocked

- All other traffic is blocked. This includes NetBIOS traffic regardless of its source/destination address.

### Downstream Port Filter (incoming traffic)

#### Accepted

- Any traffic addressed to the access controller. If you are using multiple daisy-chained LPS-20xs, all should forward traffic to the same access controller.
- HTTPS traffic regardless of its source address. (This permits local or remote management stations to access to the LPS-20x management tool.)
- Any traffic addressed to the LPS-20x.
- Certain address management protocols (ARP, DHCP) regardless of their source address.
- All broadcast traffic.

#### Blocked

- All other traffic is blocked. This includes NetBIOS traffic regardless of its source/destination address.

### Wireless Port Filter (incoming traffic)

#### Accepted

- Any traffic addressed to the access controller.
- Any traffic addressed to the LPS-20x. Note that to access the management tool wirelessly, the appropriate security setting must be enabled on the Management tool page. Wireless client stations should have the LPS-20x configured as their default gateway. This ensures that outgoing traffic will be sent to the LPS-20x which will then forward it to the access controller.
- Certain address management protocols (ARP, DHCP) regardless of their source address.
- All broadcast traffic.

#### Blocked

- All other traffic is blocked. This includes NetBIOS traffic regardless of its source/destination address. HTTPS traffic not addressed to the LPS-20x is also blocked which means wireless client stations cannot access the management tool on other LPS-20xs.

## NETWORK PORT CONFIGURATION

The LPS-20x has three communication ports: upstream, downstream and wireless:

- Upstream - Used to connect the LPS-20x to the downstream port on another LPS-20x, to an access controller, or to a wired LAN.
- Downstream - Used to connect the LPS-20x to the upstream port on another LPS-20x or to a wired network.
- Wireless - Used to connect with wireless client stations.

All three ports are bridged and share the same IP address. By default, they are statically assigned to 192.168.1.1.

### SETTING UP DHCP CLIENT SERVICES

To set up for DHCP services, do the following:

1. On the main menu, click **Network**.
2. Click **Ports**. The *Network configuration* page opens.

The screenshot shows the 'Network configuration' page in the LPS-202 Management Tool. The page has a red header with the ADC logo and 'LPS-202 Management Tool'. Below the header is a navigation menu with 'Home' and 'Logout' on the left and right, and 'Wireless', 'Network', 'Security', 'Management', 'Status', 'Tools', and 'Maintenance' in the center. Under 'Network', there are sub-menus for 'Ports', 'Bandwidth control', and 'DNS'. The main content area is titled 'Network configuration' and contains several sections: 'Assign IP address via' with radio buttons for 'DHCP Client' (selected) and 'Static', and a 'VLAN' field set to '0'; 'Downstream port link settings' with a 'Duplex' dropdown set to 'AUTO' and a note '(Currently: 10 Mbps Half duplex)'; 'Discovery protocol' with radio buttons for 'enabled' and 'disabled' (selected); 'Current settings' showing 'IP Address: 192.168.1.1', 'Mask: 255.255.255.0', and 'MAC Address: 00:02:6F:06:13:0B'; 'ATM settings' and 'ADSL settings', each with a 'Configure' button. A 'Save' button is located at the bottom right of the configuration area.

3. Select **DHCP Client** and click the **Configure** button.

4. Set optional AP ID.
5. Click **Save** when you are done.

## ASSIGN IP ADDRESS VIA PARAMETERS

### DHCP client

Dynamic host configuration protocol. Your ISP's DHCP server will automatically assign an address to the LPS-20x which functions as a DHCP client.

### Static

This option enables you to manually assign an IP address to the LPS-20x.

### VLAN

Defines the default VLAN. All outgoing traffic that does not have a VLAN already assigned to it is sent on this VLAN.

### Restrict VLAN to management traffic only

The default VLAN can be restricted to carry management traffic only. Management traffic includes:

- all traffic that is exchanged by the LPS-20x and the access controller (login authentication requests/replies)
- all communications with RADIUS servers
- HTTPS sessions to the management tool
- SNMP traffic



## DOWNSTREAM PORT LINK SETTINGS

### Duplex

- Auto: Allows the LPS-20x to automatically set duplex mode based on the type of equipment it is connected to
- Full: Forces the port to operate in full duplex mode
- Half: Forces the port to operate in half duplex mode

## SETTING PARAMETER

### DHCP Client ID

Specify an ID to identify the LPS-20x to the DHCP server. This parameter is not required by all ISPs.

## ASSIGNED BY DHCP SERVER PARAMETERS

These settings are assigned to the LPS-20x by your ISP's DHCP server. The Internet connection is not active until this occurs.

### IP address

Identifies the IP address assigned to the LPS-20x by the ISP.

### Mask

Identifies the subnet mask that corresponds to the assigned IP address.

### Primary DNS address

Identifies the IP address of the main DNS server the LPS-20x will use to resolve DNS requests.

### Secondary DNS address

Identifies the IP address of the backup DNS server the LPS-20x will use to resolve DNS requests.

### Default gateway

Identifies the IP address of the gateway the LPS-20x will forward all outbound traffic to.

### Expiration time

Indicates how long the address is valid.

### Release

Click to release the LPS-20x's IP address.

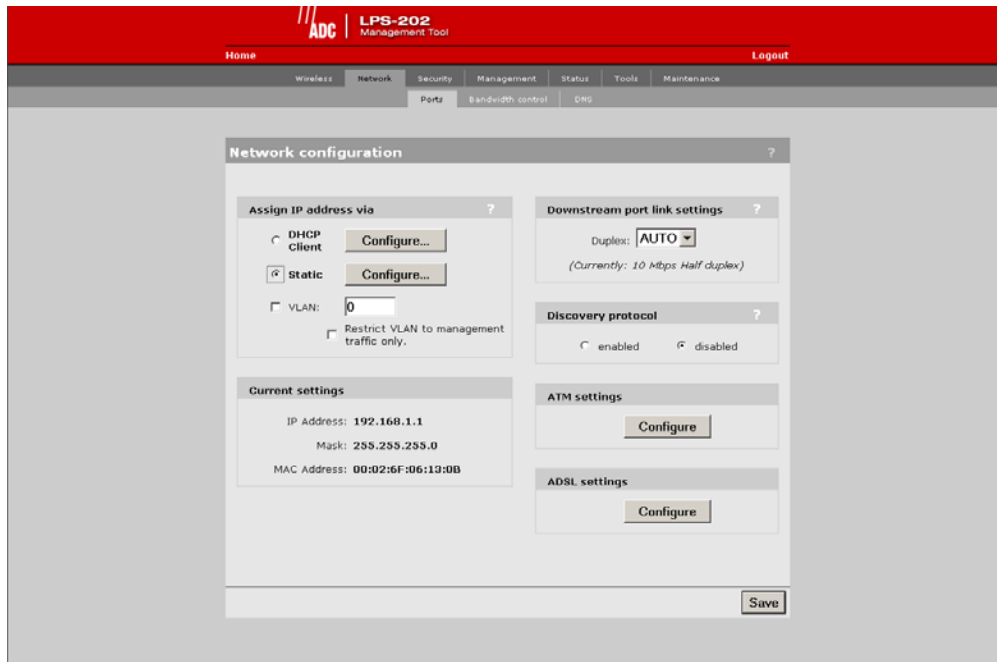
### Renew

Click to renew the LPS-20x's IP address.

## SETTING A STATIC IP ADDRESS

To set a static IP address, do the following:

1. On the main menu, click **Network**.
2. Click **Ports**. The *Network configuration* page opens.



3. Select **Static** and click the **Configure** button.



4. Set the IP address, mask and default gateway.

**IMPORTANT**

***The default gateway must be set to the IP address of the access controller.***

5. Click **Save** when you are done.

## **SETTINGS PARAMETERS**

### **IP Address**

Specify the static IP address you want to assign to the port.

### **Address Mask**

Select the appropriate mask for the IP address you specified.

### **Default Gateway**

Identifies the IP address of the gateway the LPS-20x will forward all outbound traffic to.

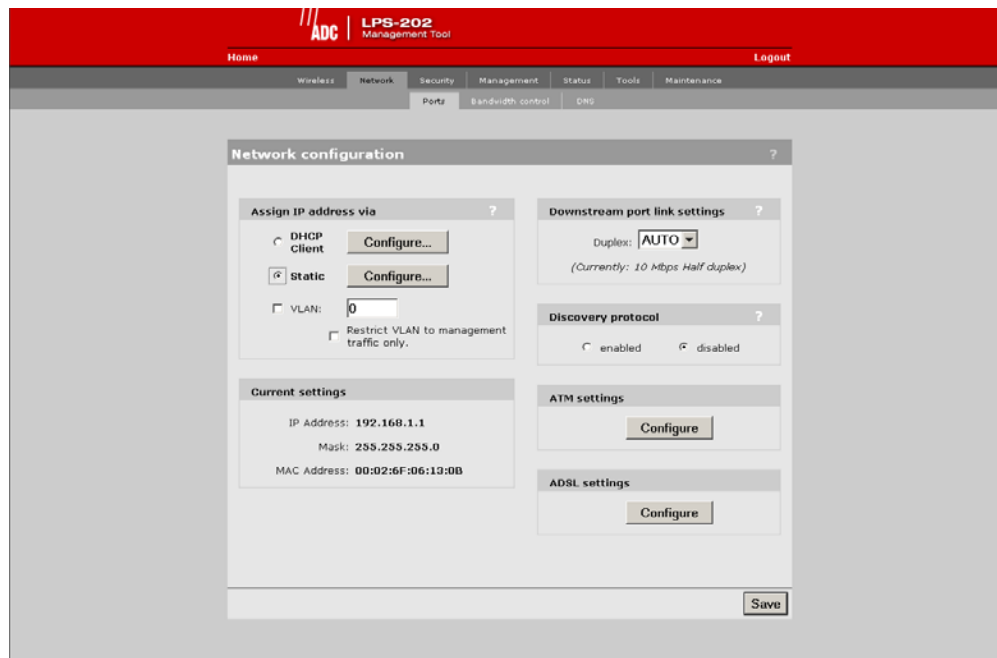
## CONFIGURE ATM SETTINGS

This option allows you to specify the VPI, VCI and encapsulation methods to use for the User and Management PVCs.



The LPS-202 screens are shown for setting the ATM settings; however, the LPS-200 screens work the same way.

1. On the main menu, click **Network**.
2. Click **Ports**. The *Network configuration* page opens.
3. Click the ATM settings **Configure** button.



4. Configure the ATM settings.

5. Click **Save** when you are done.

### USER PVC PARAMETERS

The User PVC is the ATM PVC to use for all user (non-management) traffic.

#### VPI

The ATM VP Index to use as configured upstream or on the network.

#### VCI

The ATM VC Index to use as configured upstream.

#### Encapsulation

The ATM Encapsulation to use as configured upstream.

### INBAND MANAGEMENT PVC PARAMETERS

The Inband Management PVC is the ATM PVC to use specifically for Inband Management traffic.

#### VPI

The ATM VP Index to use as configured upstream or on the network.

#### VCI

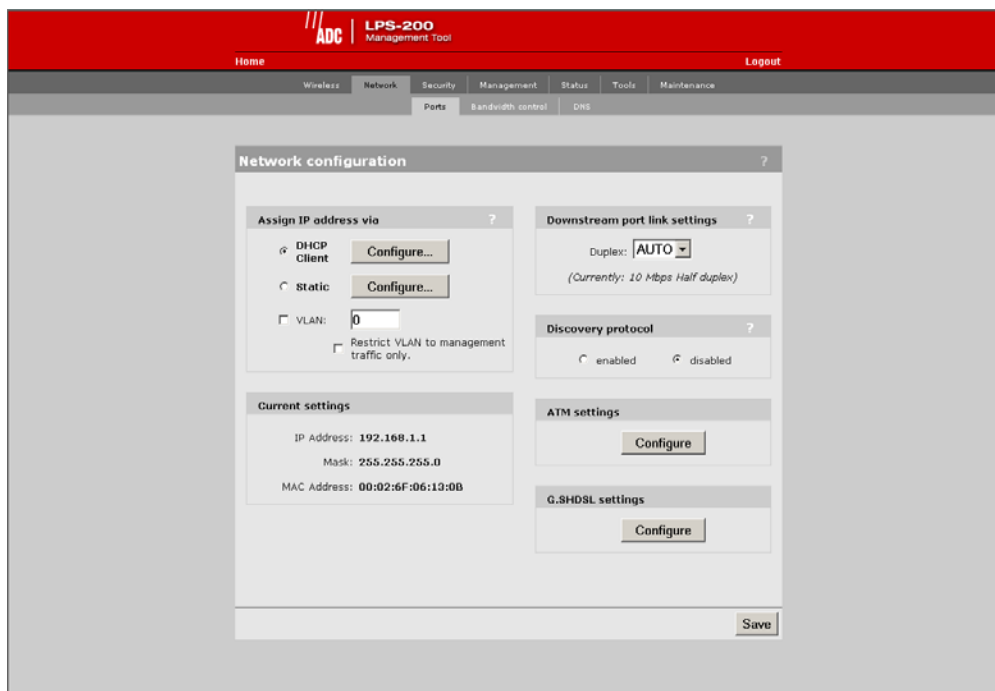
The ATM VC Index to use as configured upstream.

#### Encapsulation

The ATM Encapsulation to use as configured upstream.

## CONFIGURE G.SHDSL SETTINGS (LPS-200 ONLY)

1. On the main menu, click **Network**.
2. Click **Ports**.The *Network configuration* page opens.
3. Click the G.SHDSL settings **Configure** button.



4. Configure the G.SHDSL settings.



5. Click **Save** when you are done.

## **G.SHDSL SETTING PARAMETERS**

### **Standard Annex**

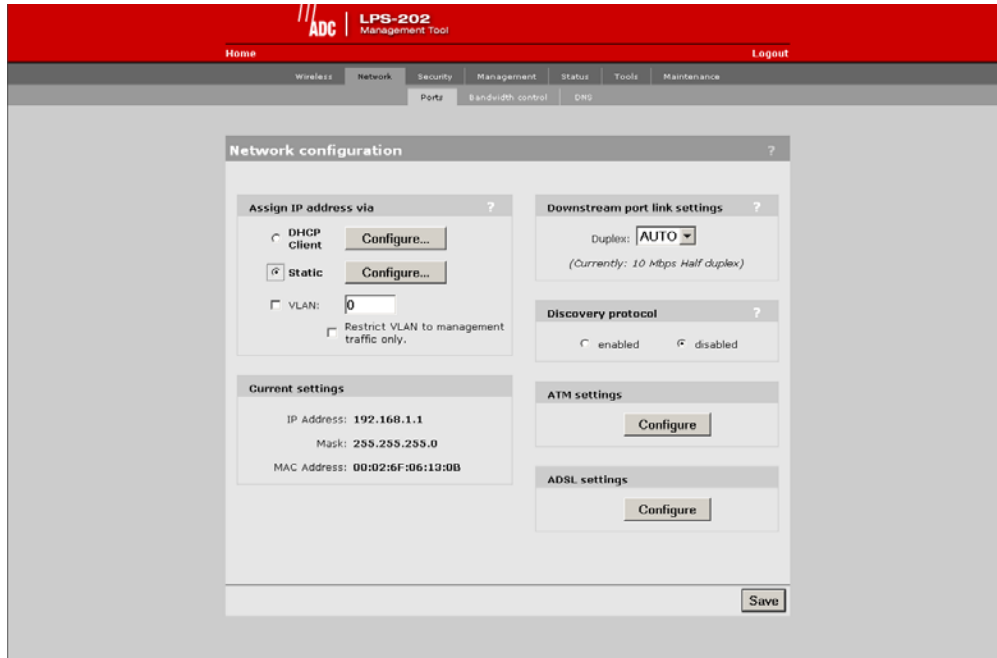
You may provision which Annex mode the access point will operate in. By default, the access point is configured to support both A and B Annex standards and will automatically detect which standard is in use. Annex type must match the setting at the STU-C.

### **Startup SNR Margin**

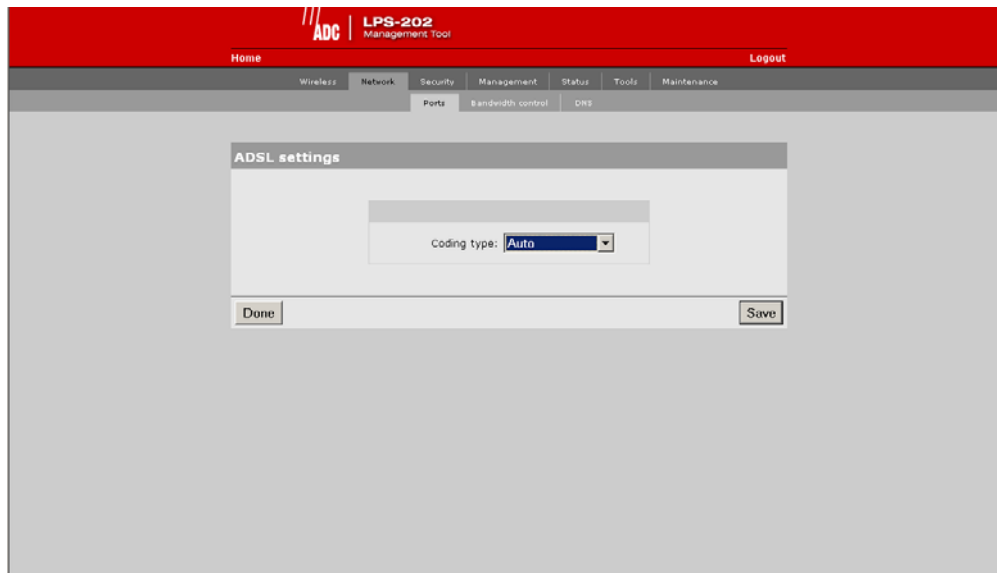
Specifies the downstream target SNR margin for a SHDSL line. The SNR Margin is the difference between the desired SNR and the actual SNR. Startup SNR Margin is the desired SNR margin for a unit.

## CONFIGURE ADSL SETTINGS (LPS-202 ONLY)

1. On the main menu, click **Network**.
2. Click **Ports**. The *Network configuration* page opens.
3. Click the ADSL settings **Configure** button.



4. Configure the ADSL settings.



5. Click Save when you are done.



## **ADSL SETTINGS (CODING TYPE) PARAMETER**

The Coding Type determines the ADSL modulation the LPS-20x will use on the ADSL line. Selections other than "Auto" require the Coding Type to match the Coding Type configured at the ATU-C. Selecting "Auto" allows the LPS-20x to negotiate the Coding Type with the "ATU-C".

## CONNECTING TO A WIRED LAN

By attaching the LPS-20x to an Ethernet hub, you can connect wired computers to the public access network (Figure 21). These computers will need to login, just as computers on the WLAN do.

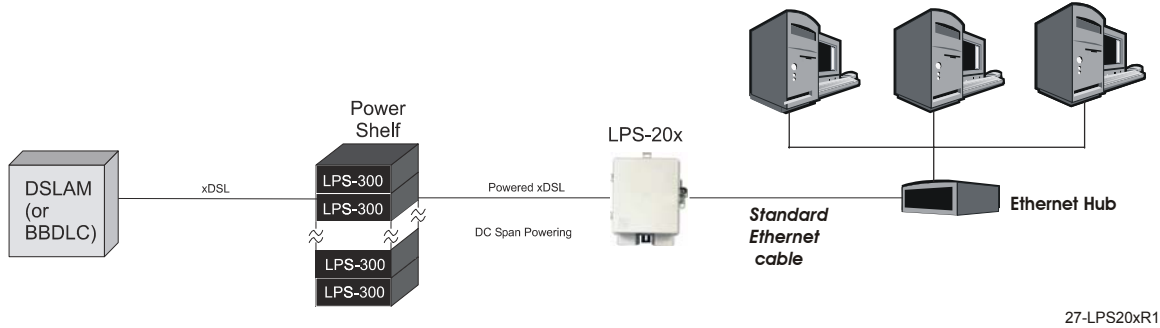


Figure 21. Connecting to a Wired LAN

## BRIDGE

The LPS-20x acts as a bridge between the wireless LAN and the wired LAN. By default, for security reasons, all traffic forwarding between the two LANs is blocked. This means that although the wired LAN and the WLAN are on the same segment, client stations cannot communicate with each other. You can enable communications by disabling the intelligent bridge security filters. See [Configuring the Connection to the Access Controller on page 79](#) and [Disabling the Security Filters on page 93](#) for more details.

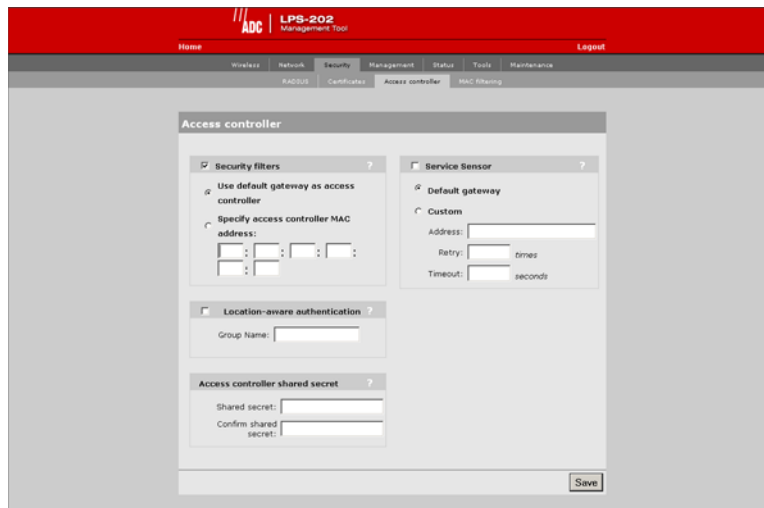
## IP ADDRESSING

The LPS-20x makes the connection to the wired LAN via its downstream (LAN/Craft) port. The downstream port shares the same IP address as the wireless port. This means that the wireless LAN and the wired LAN must always be on the same subnet.

## DISABLING THE SECURITY FILTERS

The intelligent bridge is enabled by default. To disable it, do the following:

1. On the main menu, click **Security** and then click **Access controller**. The *Access controller* configuration page opens.



The screenshot shows the 'Access controller' configuration page in the LPS-202 Management Tool. The page has a red header with 'ADC | LPS-202 Management Tool' and a navigation bar with 'Home', 'Logout', 'Wireless', 'Network', 'Security', 'Management', 'Status', 'Tools', and 'Maintenance'. Below the navigation bar, there are tabs for 'Access controller' and 'MAC filtering'. The main content area is titled 'Access controller' and contains several sections:

- Security filters** (checked):
  - Use default gateway as access controller (radio button selected)
  - Specify access controller MAC address: [ ] : [ ] : [ ] : [ ] : [ ]
- Service Sensor** (unchecked):
  - Default gateway (radio button selected)
  - Custom (radio button unselected)
  - Address: [ ]
  - Retry: [ ] times
  - Timeout: [ ] seconds
- Location-aware authentication** (unchecked):
  - Group Name: [ ]
- Access controller shared secret** (unchecked):
  - Shared secret: [ ]
  - Confirm shared secret: [ ]

A 'Save' button is located at the bottom right of the form.

2. Clear the **Security filters** check box.
3. Click **Save**.

## SERVICE SENSOR

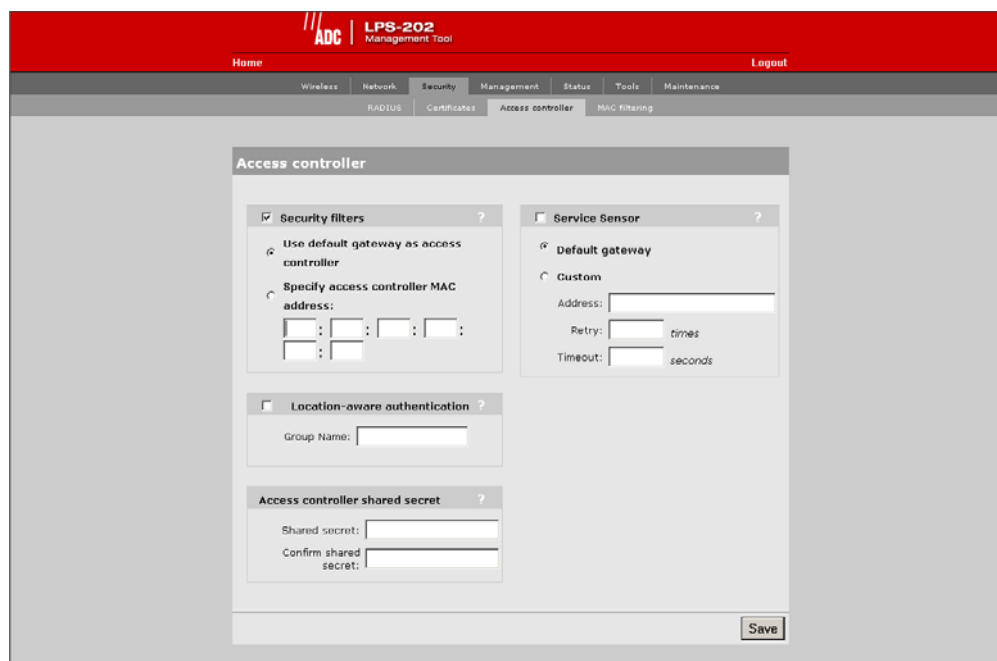
The service sensor enables the LPS-20x to determine if access to the network or a particular server is available. If not, the LPS-20x automatically shuts off its radio transmitter taking down the wireless cell.

This feature can be used to create backup operation of the network in case of equipment failure. For example, you could install two LPS-20xs, each operating on a different channel within close proximity of one another. Each LPS-20x would communicate with a different access controller. If one of the controllers goes down, the service sensor will detect it and shut down the radio on the affected LPS-20x. Client stations connected to this LPS-20x will automatically be transferred to the other LPS-20x with no interruption in service. This only works if both LPS-20xs have the same SSID or are both configured to accept any network name (default setting).

The service sensor polls the target device approximately every half second.

## CONFIGURATION PROCEDURE

1. On the main menu, click **Security** and then click **Access controller**. The *Access controller* configuration page opens.



2. Configure the parameters as described in the section that follows.
3. Click **Save** when you are done.

## SERVICE SENSOR PARAMETERS

### Default Gateway

Select this option to poll the default gateway. If the gateway does not respond to the poll within 1 second, the radio is turned off. This setting is not configurable. If **Security filters** are enabled, the default gateway must be the address of the access controller.

### Custom

Select this option to manually specify the IP address or domain name of the device to poll, the retry limit and timeout. If you are using an ADC access controller, you can use the MAC authentication option to allow the LPS-20x to log into the RADIUS server. This enables you to define an access list specifically for the LPS-20x that allows for access to the required device.

### Retry

Specify how many retries the LPS-20x will attempt when polling. When the retry limit is reached, the radio on the LPS-20x is turned off. For example, if you set retry to 4, then the LPS-20x will make 5 attempts to poll the device at the specified address. After the fifth failed poll, the radio will be turned off.

### Timeout

Specify how long the LPS-20x will wait for a response to the poll before timing out.

## MAC-LEVEL FILTERING

MAC-level filtering enables you to control access to the LPS-20x based on the MAC addresses of client stations. You can either block access or allow access depending on your requirements.

### CONFIGURATION PROCEDURE

1. On the main menu, click **Wireless** and then click **MAC filtering**. The *MAC filtering* configuration page opens.



2. Configure the parameters as described in the section that follows.
3. Click **Save** when you are done.

### MAC FILTERING PARAMETERS

When enabled, this option enables you to control access to the LPS-20x based on the MAC address of client stations. You can either block access or allow access depending on your requirements.

#### Filter Behavior

##### *Allow MAC Address List*

- Only client stations whose MAC addresses appear in the MAC address list can connect to the wireless network.

##### *Block MAC Address List*

- All client stations whose MAC addresses appear in the MAC address list are blocked from accessing the wireless network.

### MAC ADDRESS LIST

Use this box to manage the addresses in the list. To add an address, enter it and click **Add**. To remove an address, select it in the list and click **Remove**.

## LOCATION-AWARE AUTHENTICATION

This feature enables you to control logins to the public access network based on the wireless access point a customer is connected to.

**IMPORTANT** *This feature can only be used when the LPS-20x is installed in conjunction with an access controller.*



*This feature does not support 802.1x customers and devices using MAC-based authentication.*

### HOW IT WORKS

When a customer attempts to login to the public access network, the access controller sets the Called-Station-ID in the RADIUS access request to the MAC address of the LPS-20x wireless port the customer is associated with. For more information, see the Administrator's Guide for the access controller.

### CONFIGURATION PROCEDURE

1. On the main menu, click **Security** and then click **Access controller**. The *Access controller* configuration page opens.

2. Enable the **Location-aware authentication** option.
3. Specify the **Group Name** for the Access Point.
4. Specify the same shared secret configured on the access controller.
5. Click **Save**.

## **LOCATION-AWARE AUTHENTICATION PARAMETERS**

This feature enables you to control logins to the public access network based on the wireless access point a customer is connected to. When enabled, the LPS-20x will return the value you specify in the Called-Station-ID when it generates a RADIUS access request for a customer login.

### **Group Name**

Specify a group name for the access point. This name is used to identify customer logins via the Called-Station-ID. You can assign the same group name to more than one access point.

### **Shared Secret**

To maintain the security of the network logins, the LPS-21x will only accept location-aware information from an LPS-20x that has a matching shared secret to its own.



# WIRELESS BRIDGING

## OVERVIEW

The wireless bridging feature enables you to use the wireless radio to create point-to-point wireless links to other access points (Figure 22). Each LPS-20x can support up to six wireless bridges, which can operate at the same time as the network serving wireless customers. Wireless bridging provides an effective solution for extending wireless coverage in situations where it may be impractical or expensive to install cabling to a wireless access point.

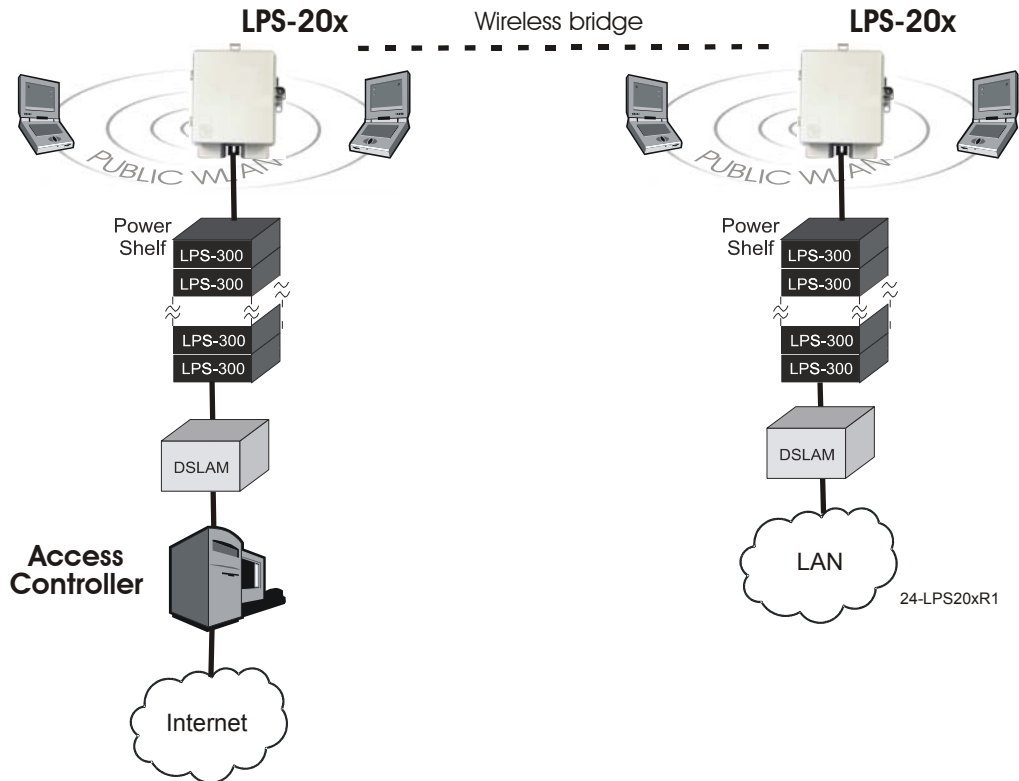


Figure 22. Wireless Bridging

In this scenario, the two LPS-20xs are used to expand the coverage of the wireless network controlled by the access controller. The first LPS-20x is connected to the access controller via the backbone LAN. The other LPS-20x uses the wireless bridging function to link to the first LPS-20x.

## SETTING UP A WIRELESS LINK

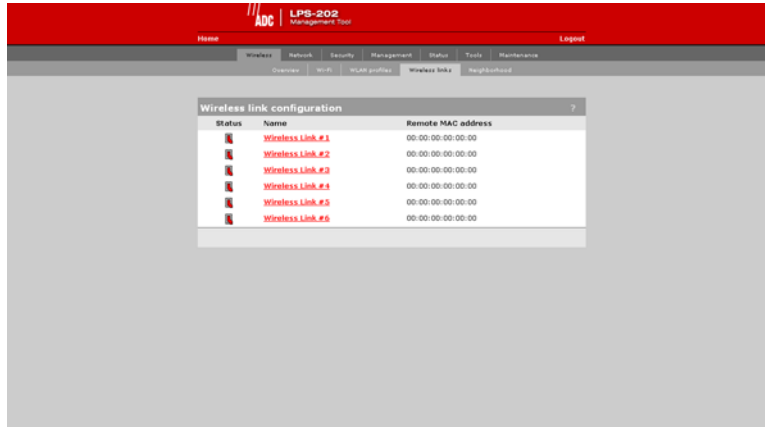
This screen shows the status of the wireless links to remote LPS-20xs.

**IMPORTANT**

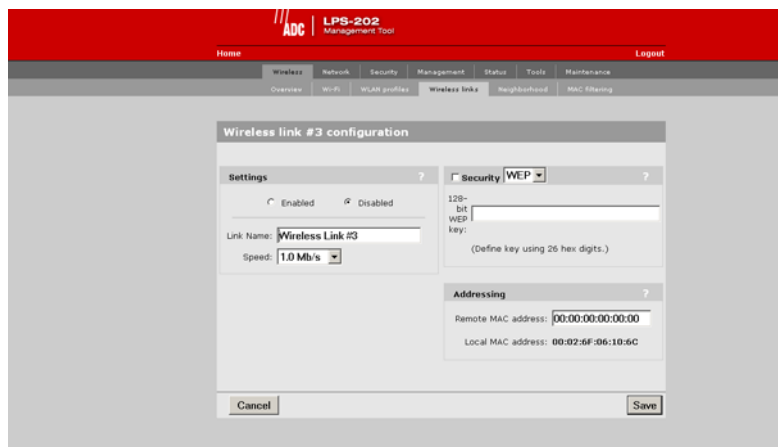


**Both ends of the wireless link will need to be provisioned for this function to work properly.**

1. On the Wireless menu, click **Wireless links**. The *Wireless links* page opens.



2. Click the wireless link you want to configure. The configuration page for the link opens.



3. In the **Settings** box, select **Enabled**.
4. In the **Security** box, select **Security**. Specify the encryption key (128 bits long - specified as 26 hexadecimal digits).
5. In the **Addressing** box, specify the **MAC address** of the other access point.
6. Click **Save**.

## WIRELESS LINK CONFIGURATION PARAMETERS

### Status

Indicates if the link is enabled or disabled.

### Name

Name of the link. Click to configure it.

### Remote MAC Address

MAC address of the remote LPS-20x.

## SETTING PARAMETERS

When the link is enabled, it is ready to establish a connection with the remote LPS-20x.

### Link Name

Identifies the link.

### Speed

Sets the speed the link will operate at. Choose auto to always use the fastest speed. For load balancing, you may want to limit the speed of a link when connecting to multiple destinations.

## SECURITY PARAMETERS

When the link is enabled, it is ready to set WEP security.

### None

No encryption.

### WEP

Specify the encryption key the LPS-20x will use to encrypt/decrypt all data it sends and receives. The key is 128 bits long and must be specified as 26 hexadecimal digits.

## ADDRESSING PARAMETERS

### Remote MAC Address

MAC address of the remote access point.

### Local MAC Address

MAC address of the remote access point.

## WIRELESS LINK STATUS

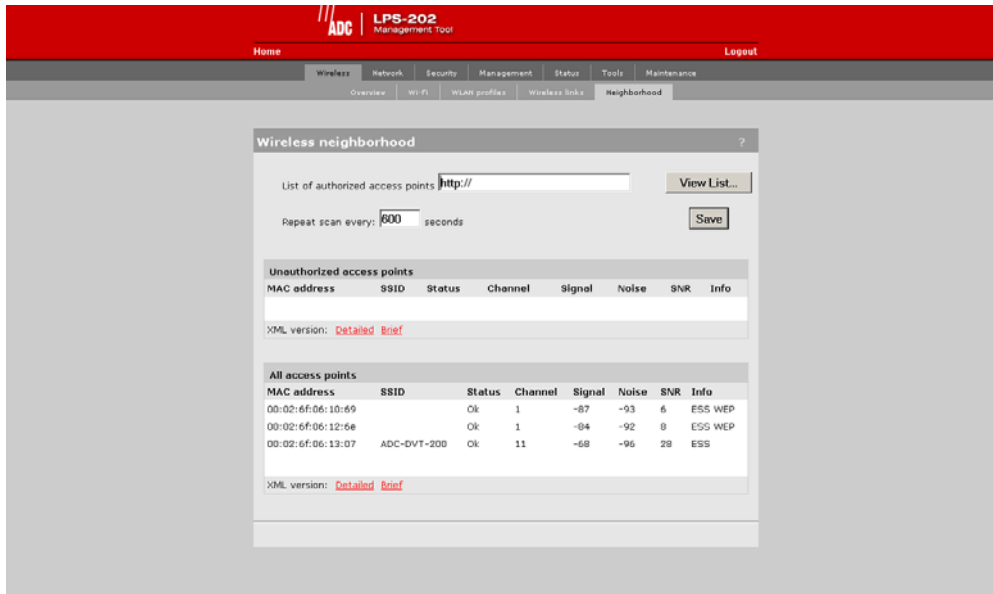
To view the status of the wireless links, open the **Status > Wireless** page.

## WIRELESS NEIGHBORHOOD

The wireless neighborhood feature enables you to view a list of all authorized and unauthorized access points that are operating nearby. At a preset interval, the LPS-20x automatically scans all operating frequencies to identify active access points. The result of this scan is presented in the All access points list.

To identify unauthorized access points, the LPS-20x compares the MAC address of each discovered access point against the list of authorized access points (which you must define). If the discovered access point does not appear in the list, it is displayed in the Unauthorized access points list.

1. On the Wireless menu, click **Neighborhood**. The *Neighborhood* page opens.



## WIRELESS NEIGHBORHOOD PARAMETERS

### List of authorized access points

Specify the URL of the file that contains a list of all authorized access points. The format of this file is XML. Each entry in the file is composed of two items: MAC Address and SSID. Each entry should appear on a new line.

The easiest way to create this file is to wait for a scan to complete, then open the list of access points in Brief format. Edit this list so that it contains only authorized access points and save it. Then specify its address for the list of authorized access point parameters.

### Field Descriptions

- MAC Address: MAC Address of the access point
- SSID: SSID assigned to the access point
- Status: Indicates if the unit is functioning properly
- Channel: Channel the access point is operating on
- Signal: Signal Strength
- Noise: Amount of noise
- SNP: Signal to noise ratio
- Info: Additional information about the access point, such as:
  - WEP: Some type of security (like WEP) is enabled on the access point
  - ESS: Operating in access point mode
  - IBSS: Operating in Ad-Hoc mode

## VLAN SUPPORT

The LPS-20x provides a robust and flexible VLAN implementation. VLANs can be assigned in one of three ways:

- Default VLAN
- Per-SSID VLAN
- Per-User VLAN

### DEFAULT VLAN

The LAN port can be configured with a default VLAN setting. Any outgoing traffic on the LAN port that is not tagged with a VLAN ID will receive the default ID. The default VLAN can be restricted to carry management traffic only. This includes:

- all traffic that is exchanged with the access controller
- all traffic exchanged with external RADIUS servers
- HTTPS sessions established by administrators to the management tool
- incoming/outgoing SNMP traffic
- DNS requests/replies

## PER-SSID VLAN

Each wireless profile can be mapped to its own VLAN. Wireless clients that connect to a profile with VLAN support are bridged to the appropriate VLAN via the LPS-20x's LAN port. Address allocation and security measures are the responsibility of the target network.

### IMPORTANT



*Per-SSID VLANs cannot have the same VLAN ID as the default VLAN ID assigned to the LAN port.*

## PER-USER VLAN

VLANs can also be assigned on a per-customer basis by setting a special ADC attribute in a customer's RADIUS account. The only restriction is that a customer cannot be assigned to a VLAN that is already mapped to the LAN port.

To use this feature, the LPS-20x must be connected to a ADC access controller. Consult the administrator guide for more information.

## VLAN PRIORITY

The VLAN assigned by RADIUS on a per-user basis always overrides the VLAN assigned by an SSID and the default VLAN. For example, a wireless station could be associated with an SSID that is configured for VLAN 30, but after logging in, RADIUS could override this setting by assigning VLAN 40.

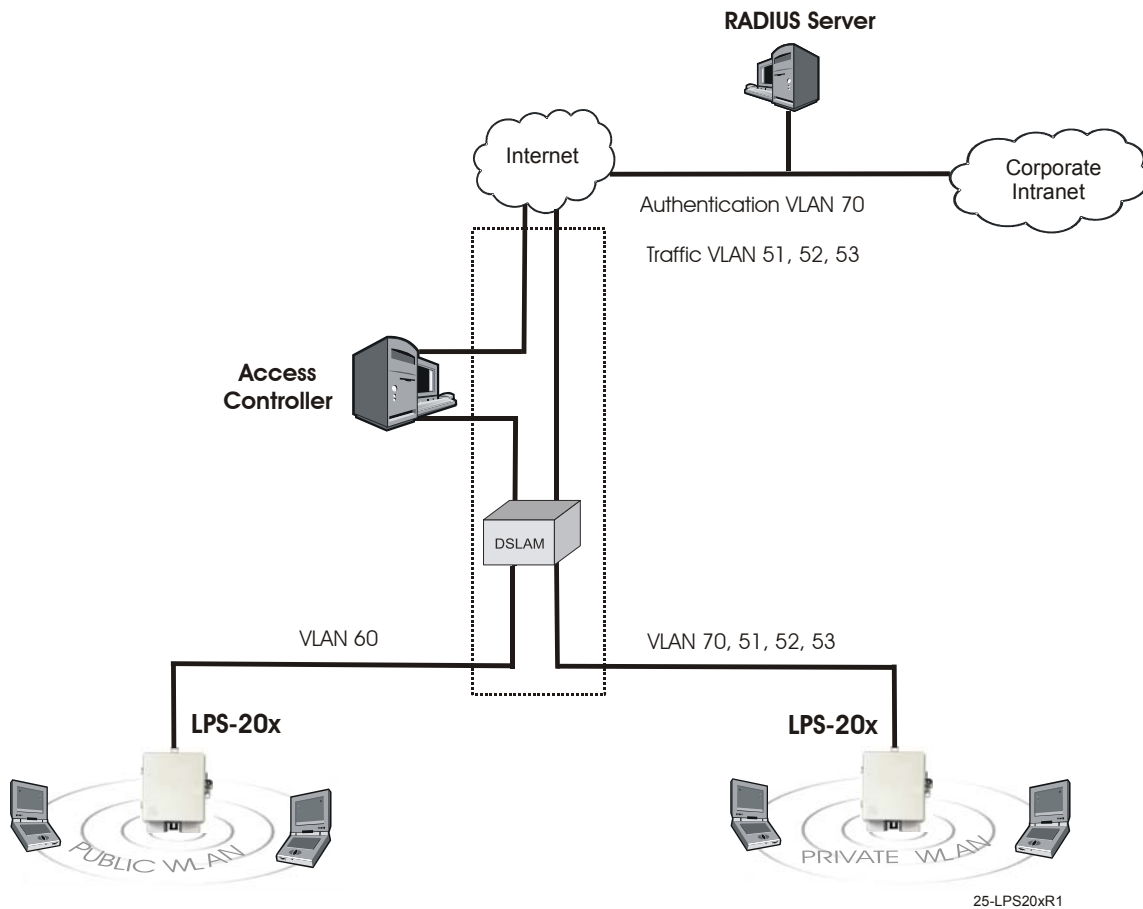
## SCENARIO

In this scenario, VLANs and multiple SSIDs are used to enable public and private users to share the same infrastructure with complete security.

### How it works

The wireless network is split into two WLANs: public and private (Figure 23).

- Wireless users on the public WLAN are mapped to the access controller via VLAN 60.
- Wireless users on the private WLAN are mapped to one of the VLANs on the corporate intranet based on a setting in their RADIUS account.



**Figure 23. WLANS - Public and Private**

## CONFIGURATION ROADMAP

The following configuration steps provide an overview on how to set up this scenario.

### On the Access Controller

1. Open the **Security > RADIUS** page.
  - Add a RADIUS profile that connects to the corporate RADIUS server.
2. Open the **Security > Authentication** page.
  - In access controller authentication, define settings to connect to the corporate RADIUS server via the profile you just added.
3. Open the **Wireless > WLAN profiles** page.
  - Add a profile named **Public**.
  - Do not assign a VLAN to this profile.
  - Enable **HTML-based user logins** and assign them to **RADIUS authentication**.
4. Open the **Security > Authentication > Advanced** page and set the **Access controller shared secret**.
5. Customize the public access interface as required. For details, see the Administrator's Guide of the access controller.
6. Define access lists to restrict the resources guests can reach. For details, see the Administrator's Guide of the access controller.

### On the LPS-20xs

1. Open the **Wireless > WLAN profiles** page. Add two profiles: **Private** and **Public**.
  - Private profile: in the **Wireless protection** box, enable either **WPA** or **802.1x**.
2. Open the **Network > Ports** page.
  - Enable **DHCP client**.
  - Set **VLAN** to **60**.
  - Disable **Restrict VLAN to management traffic only**.
3. Open the **Security > Access controller** page.
  - Set the **Access controller shared secret** to the same value as on the access controller.
  - Disable **Location-aware authentication**.

### On the RADIUS server

Define the following:

1. Define accounts for the access controller, guests, and employees.
2. In the employee account, set up support for VLAN mapping by defining the following RADIUS attributes:
  - Tunnel-type: Set to "VLAN".
  - Tunnel-medium-type: Set to "802".
  - Tunnel-private-group: Set to the appropriate VLAN number.

See the Administrator's Guide of the access controller for more information.



## VLAN STATUS

Use the **VLAN** option on the Status menu to determine the status of the virtual LAN.



## WIRELESS CLIENT STATION PARAMETERS

### Mac address

The Ethernet address of client station(s) that are associated to the AP.

### SSID

The SSID that the client station(s) is associated with.

### Association time

Indicates how long the client station has been associated with the LPS-20x.

### Authorized

Applies to client stations using 802.1x only. A value of “Yes” indicates that 802.1x authentication was successful. A value of “No” indicates that 802.1x authentication was unsuccessful. If 802.1x support is not enabled on the LPS-20x, this field shows “yes”.

### Signal

Indicates the strength of the radio signal received from the client stations. Signal strength is expressed in dBm. The higher the number, the stronger the signal.

### Noise

Indicates how much background noise exists in the signal path between client stations and the LPS-20x. Noise is expressed in dBm. The lower (more negative) the value, the weaker the noise.

### SNR

Indicates the relative strength of client station radio signals versus the radio interference (noise) in the radio signal path. In most environments, SNR is a good indicator for the quality of the radio link between the client stations and the LPS-20x. A higher SNR value means a better quality radio link.

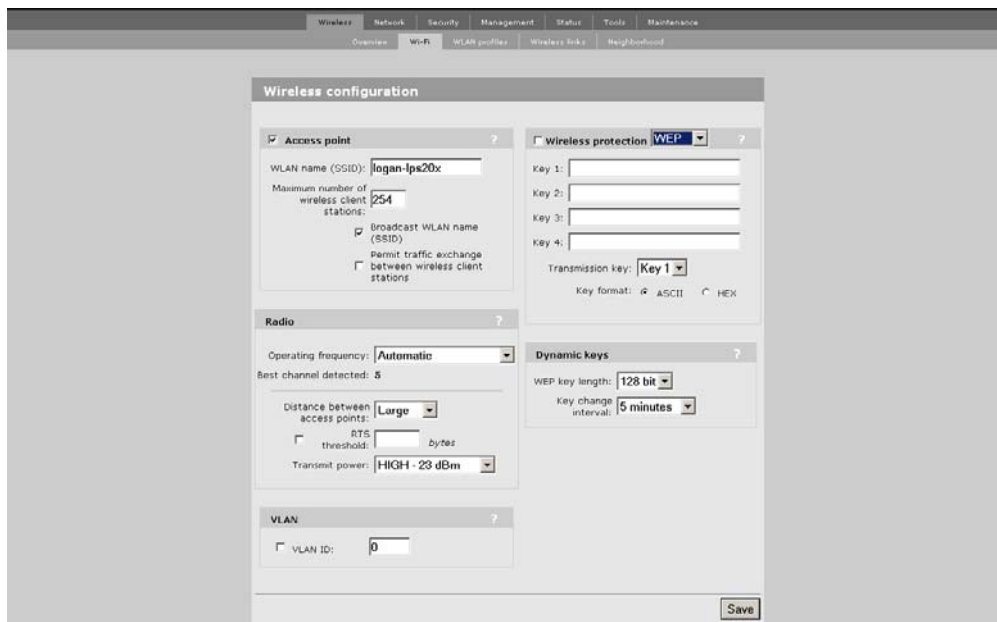
## WEP SECURITY

Wired equivalent privacy (WEP) provides protection for wireless traffic by encrypting all transmissions. Multiple keys can be defined allowing stations to rotate key usage for enhanced security.

**WARNING** *ADC does not recommend the use of WEP alone for the creation of secure wireless networks.*

### CONFIGURATION PROCEDURE

1. On the main menu, click **Wireless**. The *Wireless configuration* page opens.
2. Check the wireless protection box.
3. In the **Wireless protection** box, choose **WEP**. The following parameters are displayed:



4. Configure the parameters as described in the section that follows.
5. Click **Save** when you are done.

## WIRELESS PROTECTION PARAMETER

The parameters that are visible depend on the settings you make for the **Use dynamic key rotation**.

### Keys 1, 2, 3, 4

The number of characters you specify for a key determines the level of encryption the LPS-20x will provide.

- For 40-bit encryption, specify 5 ASCII characters or 10 HEX digits.
- For 128-bit encryption, specify 13 ASCII characters or 26 HEX digits.

When encryption is enabled, wireless stations that do not support encryption cannot communicate with the LPS-20x. The definition for each encryption key must be the same on the LPS-20x and all client stations. Keys must also be in the same position. For example, if you are using key 3 to encrypt transmissions, then each client station must also use key 3 to communicate with the LPS-20x.

### Transmission Key

Select the key the LPS-20x will use to encrypt transmitted data. All four keys are used to decrypt received data.

### Key Format

Select the following format you use to specify the encryption keys:

#### *ASCII*

ASCII keys are much weaker than carefully chosen HEX keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client station support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.

#### *HEX*

Your keys should only include the following digits: 0-9; A, B, C, D, E, F (not case sensitive)

## WPA SECURITY

Wi-Fi Protected Access (WPA) provides protection for users with WPA client software.

### CONFIGURATION PROCEDURE

1. On the main menu, click **Wireless**. The *Wireless configuration* page opens.
2. Check the wireless protection box.
3. In the **Wireless protection** box, choose **WPA**. The following parameters are displayed:

The screenshot displays the 'Wireless configuration' page with the following settings:

- Access point:**  **Access point** (checked). WLAN name (SSID): ADC. Maximum number of wireless client stations: 254.  Broadcast WLAN name (SSID).  Permit traffic exchange between wireless client stations.
- Wireless protection:** WPA (selected). Key source: RADIUS. RADIUS Profile: [Access Controller].
- Dynamic keys:** WEP key length: 128 bit. Key change interval: 5 minutes.
- Radio:** Operating frequency: Channel 10, 2.457GHz. Distance between access points: Large.  RTS threshold: bytes. Maximum transmit power: HIGH - 23 dBm.
- VLAN:**  VLAN ID: 0.

A 'Save' button is located at the bottom right of the configuration area.

4. Configure the parameters as described in the section that follows.
5. Click **Save** when you are done.

## WIRELESS PROTECTION PARAMETER

The parameters that are visible depend on the settings you make for the **Use dynamic key rotation**.

### Key Source

This option determines how the TKIP keys are generated.

**RADIUS:** The LPS-20x obtains the MPPE key from the RADIUS server. This is a dynamic key that changes each time the user logs in and is authenticated. The MPPE key is used to generate the TKIP keys that encrypt the wireless data stream. Select the appropriate RADIUS server.

WPA sessions are terminated by the LPS-20x. This means that the LPS-20x handles all authentication tasks and must communicate with the RADIUS server or access controller to validate login credentials. The LPS-20x sends this authentication traffic on the downstream port. Therefore, the RADIUS server or access controller must be reachable via this port.

**Preshared Key:** The LPS-20x uses the key you specify in the Key field to generate the TKIP keys that encrypt the wireless data stream. Since this is a static key, it is not as secure as the RADIUS option. Specify a key that is between 8 and 64 characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers.

### RADIUS Profile

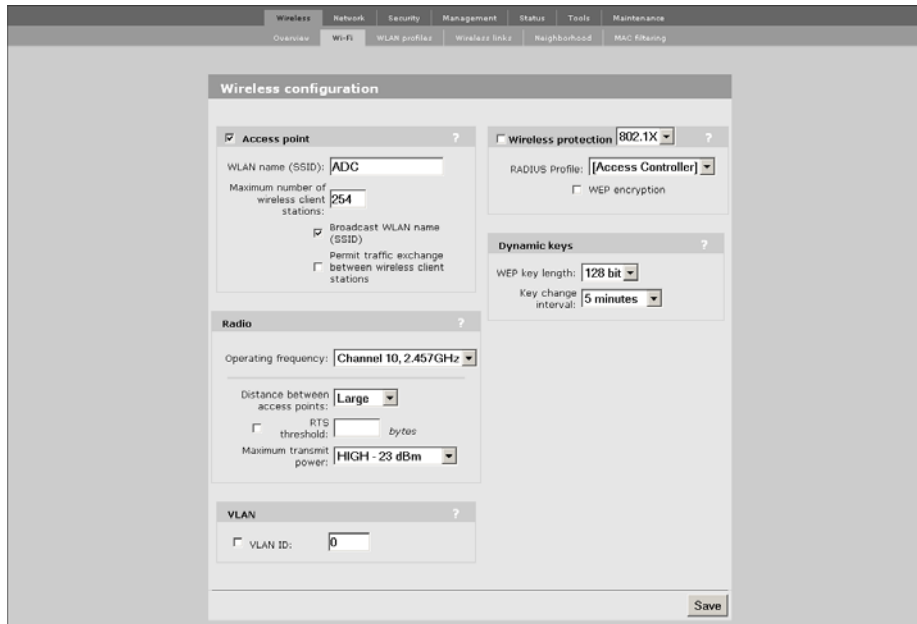
Only valid value is Access Controller.

## 802.1X SECURITY

802.1x provides protection for users with 802.1x client software.

### CONFIGURATION PROCEDURE

1. On the main menu, click **Wireless**. The *Wireless configuration* page opens.
2. Check the wireless protection box.
3. In the **Wireless protection** box, choose **802.1x**. The following parameters are displayed:



4. Configure the parameters as described in the section that follows.
5. Click **Save** when you are done.

## WIRELESS PROTECTION PARAMETER

This option enables support for users with 802.1x client software. The LPS-20x supports 802.1x client software that uses EAP-TLS, EAP-TTLS, and PEAP.

Note that all authentication tasks are handled by the LPS-20x and not the wireless client station. This means that the RADIUS server must be reachable via the downstream port.

**IMPORTANT** *802.1x sessions are terminated by the LPS-20x. This means that the LPS-20x handles all authentication tasks and must communicate with the RADIUS server to validate login credentials. The LPS-20x sends this authentication traffic on the internet port. Therefore, the RADIUS server or access controller must be reachable via this port.*



### RADIUS profile

Communications with the RADIUS server is handled via the access controller. This setting cannot be changed.

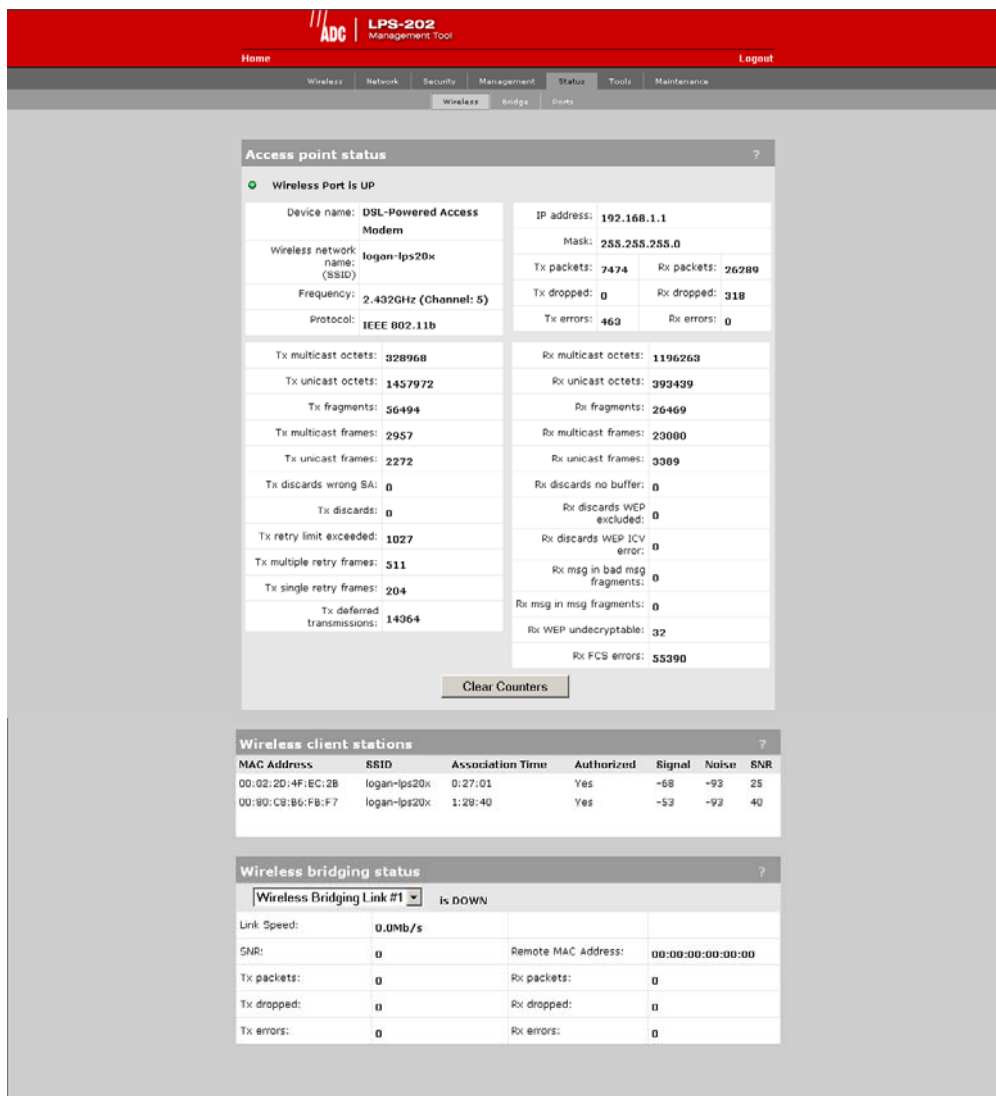
### WEP encryption

Enable the use of dynamic WEP keys for all 802.1x sessions. Dynamic key rotation occurs on key 1, which is the broadcast key. Key 0 is the pairwise key. It is automatically generated by the LPS-20x.

Key length and key change interval are set in the **Dynamic keys** box.

# WIRELESS STATUS

1. On **Status** menu, click **Wireless**. The *Access Point status* page opens.



## ACCESS POINT STATUS PARAMETERS

### Wireless Port

- UP: Port is operating normally
- DOWN: Port is not operating normally

### Device Name

The name that identifies the LPS-20x on your wireless network (for information only).

### Wireless Network Name (SSID)

The name assigned to the LPS-20x wireless network.



**Frequency**

The current operating frequency.

**Protocol**

Identifies the wireless protocol (802.11b) used by the LPS-20x to communicate with client stations.

**Tx Packets**

The total number of packets transmitted.

**Tx Dropped**

The number of packets that could not be transmitted. This can occur when the wireless configuration is being changed.

**Tx Errors**

The total number of packets that could not be sent to the following errors: Rx retry limit exceeded and Tx discards wrong SA.

**Rx Packets**

The total number of packets received.

**Rx Dropped**

The number of received packets that were dropped due to lack of resources on the LPS-20x. This should not occur under normal circumstances. A possible cause could be if many client stations are continuously transmitting small packets at a high data rate.

**Rx Errors**

The total number of packets received with the following errors: Rx discards WEP excluded, Rx discards WEP ICV error, Rx msg in bad MSG fragments, Rx MSG in MSG fragments, Rx WEP undecryptable, Rx FCS errors.

**Tx Multicast Octets**

The number of octets transmitted successfully as part of successfully transmitted multicast MSDUs. These octets include MAC Header and Frame Body of all associated fragments.

**Tx Unicast Octets**

The number of octets transmitted successfully as part of successfully transmitted unicast MSDUs. These octets include MAC Header and Frame Body of all associated fragments.

**Tx Fragments**

The number of MPDUs of type Data or Management delivered successfully (i.e., directed MPDUs transmitted and being acknowledged, as well as non-directed MPDUs transmitted).

**Tx Multicast Frames**

The number of MSDUs of which the Destination Address is a multicast MAC address (including broadcast MAC address) transmitted successfully.

**Tx Unicast Frames**

The number of MSDUs of which the Destination Address is a unicast MAC address transmitted successfully. This implies having received an acknowledged to all associated MPDUs.

**Tx Discards Wrong SA**

The number of transmit requests that were discarded because the source address is not equal to the MAC address.

**Tx Discards**

The number of transmitted requests that were discarded to free up buffer space on the LPS-20x. This can be caused by packets being queued too long in one of the transmit queues or because too many retries and defers occurred or otherwise not being able to transmit (e.g., when scanning).

**Tx Retry Limit Exceeded**

The number of times an MSDU is not transmitted successfully because the retry limit is reached due to no acknowledge or no CTS received.

**Tx Multiple Retry Frames**

The number of MSDUs successfully transmitted after more than one retransmission (on the total of all associated fragments). May be due to collisions, noise, or interference.

**Tx Single Retry Frames**

The number of packets successfully transmitted after one (and only one) retransmission (on the total of all associated fragments). May be due to collisions, noise, or interference.

**Tx Deferred Transmissions**

The number of packets for which (one of) the (fragment) transmission attempt(s) was deferred one or more times to avoid a collision.

**Rx Multicast Octets**

The number of octets received successfully as part of multicast (including broadcast) MSDUs. These octets indicate MAC Header and Frame Body of all associated fragments.

**Rx Unicast Octets**

The number of octets received successfully as part of unicast MSDUs. These octets indicate MAC Header and Frame Body of all associated fragments.

**Rx Fragments**

The number of MPDUs of type Data or Management delivered successfully.

**Rx Multicast Frames**

The number of MSDUs with a multicast MAC address (including broadcast MAC address) as the Destination Address received successfully.

**Rx Unicast Frames**

The number of MSDUs with a unicast MAC as the Destination Address received successfully.

**Rx Discards no Buffer**

The number of received MPDUs that were discarded because of lack of buffer space.

**Rx Discards WEP Excluded**

The number of discarded packets, excluding WEP-related errors.

**Rx Discards WEP ICV Error**

The number of discarded MPDUs that were discarded due to malformed WEP packets.

**Rx MSG in Bad MSG Fragments**

The number of MPDUs of type Data or Management received successfully while there was another reception going on above the carrier detect threshold but with bad or incomplete PLCP Preamble and Header (the message-in-message path #2 in the modem).

**Rx MSG in MSG Fragments**

The number of MPDUs of type Data or Management received successfully while there was another good reception going on above the carrier detect threshold (the message-in-message path #2 in the modem).

**Rx WEP Undecryptable**

The number of received MPDUs with the WEP sub-field in the Frame Control field set to one that was discarded because it should not have been encrypted or due to the receiving station not implementing the privacy option.

**Rx FCS Error**

The number of MPDUs considered to be destined for this station (Address matches) received with an FCS error. Note that this does not include data received with an incorrect CRC in the PLCP header. These are not considered to be MPDUs.

## **WIRELESS CLIENT STATION PARAMETERS**

### **MAC Address**

The hard coded media access number of the client station.

### **VLAN**

Indicates the virtual LAN associated with the LPS-20x.

### **SSID**

Indicates the name of the client station associated with the LPS-20x.

### **Association Time**

Indicates how long the client station has been associated with the LPS-20x.

### **Signal**

Indicates the strength of the radio signal received from client stations. Signal strength is expressed in dBm. The higher the number, the stronger the signal.

### **Noise**

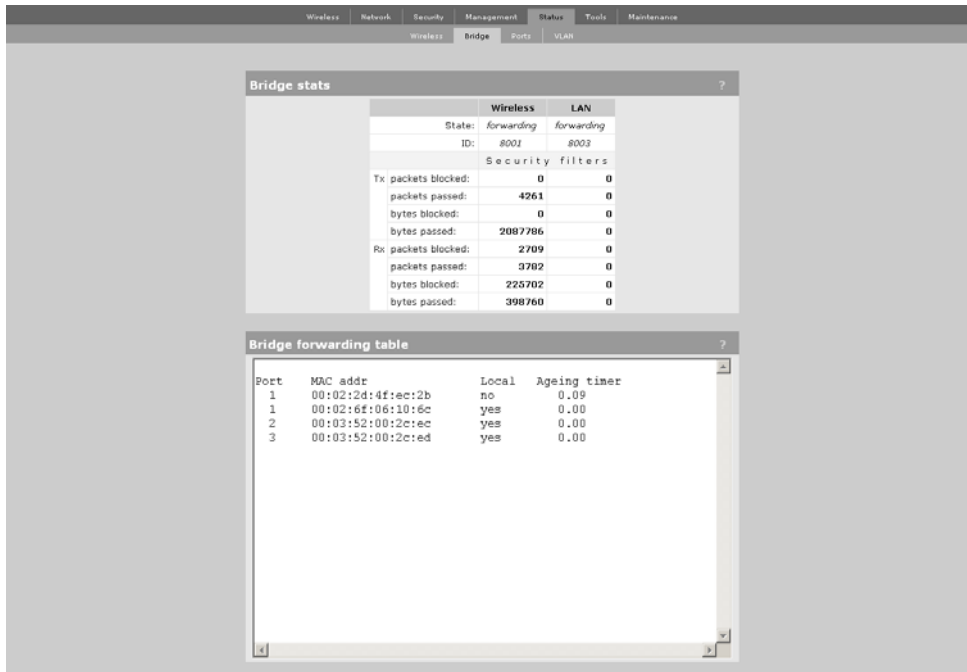
Indicates how much background noise exists in the signal path between client stations and the LPS-20x. Noise is expressed in dBm. The lower (more negative) the value, the weaker the noise.

### **SNR**

Indicates the relative strength of client station radio signals versus the radio interference (noise) in the radio signal path. In most environments, SNR is a good indicator for the quality of the radio link between the client stations and the LPS-20x. A higher SNR value means a better quality radio link.

# BRIDGE STATUS

1. On **Status** menu, click **Bridge**. The *Bridge stats* page opens.



## BRIDGE STAT PARAMETERS

### State

Current state of the bridge.

- Listening: Initial state. Port is not forwarding packets but listens for other bridges.
- Learning: Bridge learns about other bridges on that port. Port is not forwarding packets.
- Forwarding: Port is forwarding packets. Bridge is operational on the port.
- Blocking: Port is not forwarding. A loop was detected in the bridging network.

### ID

Unique ID assigned to a port. This ID cannot be changed. The last digit in the ID corresponds to the port number used in the Bridge forwarding table.

### *Packets Blocked*

Number of packets blocked by the Security filters. To activate the filters, click **Security > Access controller**.

### *Packets Passed*

Number of packets forwarded by the bridge.

### *Bytes Blocked*

Number of bytes blocked by the Security filters. To activate the filters, click **Security > Access controller**.

### *Bytes Passed*

Number of bytes forwarded by the bridge.

## Spanning Tree Protocol

For complete definitions of these fields, refer to the following document which is available in a number of locations on the Internet.

- ANSI/IEEE Std 802.1D, 1998 Edition - Part 3: Media Access Control (MAC) Bridges

## BRIDGE FORWARDING TABLE PARAMETERS

This table lists the forwarding entries learned by the bridge.

### Port

Identifies the port on the LPS-20x that traffic is forwarded on. The interface number corresponds to the last digit of the port ID in the Bridge stats box.

### MAC Address

Identifies the MAC address to be matched. Traffic addressed to this address is forwarded on the corresponding port.

### Local?

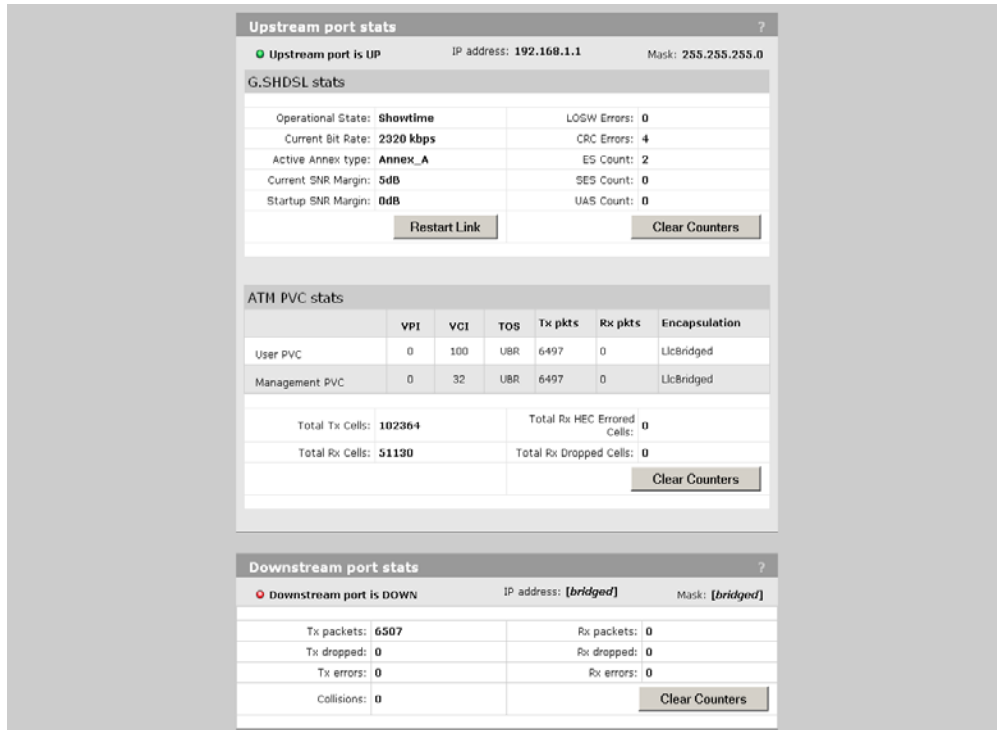
- Yes: Indicates that the MAC address identifies an interface on the LPS-20x.
- No: Indicates that the MAC address is learned.

### Aging Timer

Indicates how long (in seconds) until the entry is deleted from the table. Once deleted, the entry must be relearned.

## G.SHDSL PORTS STATUS (LPS-200 ONLY)

1. On **Status** menu, click **Ports**. The *Port stats* page opens.



## G.SHDSL STAT PARAMETERS

### Operational State

#### Showtime

Indicates an active G.SHDSL link.

#### Idle

Indicates the link is down and no attempt is being made to initialize the link.

#### Handshake

Indicates the ATU\_C and ATU\_R are negotiating the link speed.

#### Framer

Framer is synchronizing with far end Framer.

### Current Bit Rate

Shows current bit rate in Kbps.

### Annex Type

Shows what annex type the LPS-20x is configured to support.

### Current SNR Margin/Startup SNR Margin

Specifies the downstream target SNR margin for a SHDSL line. The SNR Margin is the difference between the desired SNR and the actual SNR. Startup SNR Margin is the desired SNR Margin for a unit.

**LOSW Errors**

A LOSW occurs when at least three consecutive received frames contain one or more errors in the framing bits.

**CRC Errors**

A CRC error is declared when the CRC bits generated locally on the data in the received xDSL frame do not match the CRC bits received from the transmitter.

**ES Count**

An ES count is incremented when one or more CRC errors and/or one or more LOSW errors are declared.

**SES Count**

A SES count is incremented when 50 CRC errors or one or more LOSW errors are declared.

**UAS Count**

A UAS count is incremented for each second in which the xDSL line is unavailable. The xDSL line becomes unavailable at the onset of 10 contiguous SESs. The 10 SESs are included in the unavailable time. Once unavailable, the xDSL line becomes available at the onset of 10 contiguous seconds with no SESs. The 10 seconds with no SESs are not included in the unavailable time.

**ATM PVC STAT PARAMETERS****User PVC**

Indicates the user VPI, VCI, Type of service, and encapsulation method. Also shows the total transmitted and received packets since start up or the last time the counters were cleared.

**Management PVC**

Indicates the management VPI, VCI, Type of service, and encapsulation method. Also shows the total transmitted and received packets since start up or the last time the counters were cleared.

**Total Tx Cells**

Indicates the total amount of transmitted cells for the user and management PVC since startup or the last time the counters were cleared.

**Total Rx Cells**

Indicates the total amount of received cells for the user and management PVC since startup or the last time the counters were cleared.

**Total Rx HEC Errored Cells**

Indicates the total amount of received cells that have HEC errors.

**Total Rx Dropped Cells**

Indicates the total amount of dropped cells in the receive direction.



## **DOWNSTREAM PORT STATS**

### **IP Address**

The IP address assigned to the port.

### **Mask**

The mask assigned to the port.

### **Tx Packets**

Number of packets transmitted.

### **Tx Dropped**

Number of transmitted packets dropped.

### **Tx Errors**

Number of packets with transmission errors. This can be caused by: loss of carrier, no heartbeat, late collision, too many retransmits (too many collisions when transmitting a packet).

### **Rx Packets**

Number of packets received.

### **Rx Dropped**

Number of received packets dropped.

### **Rx Errors**

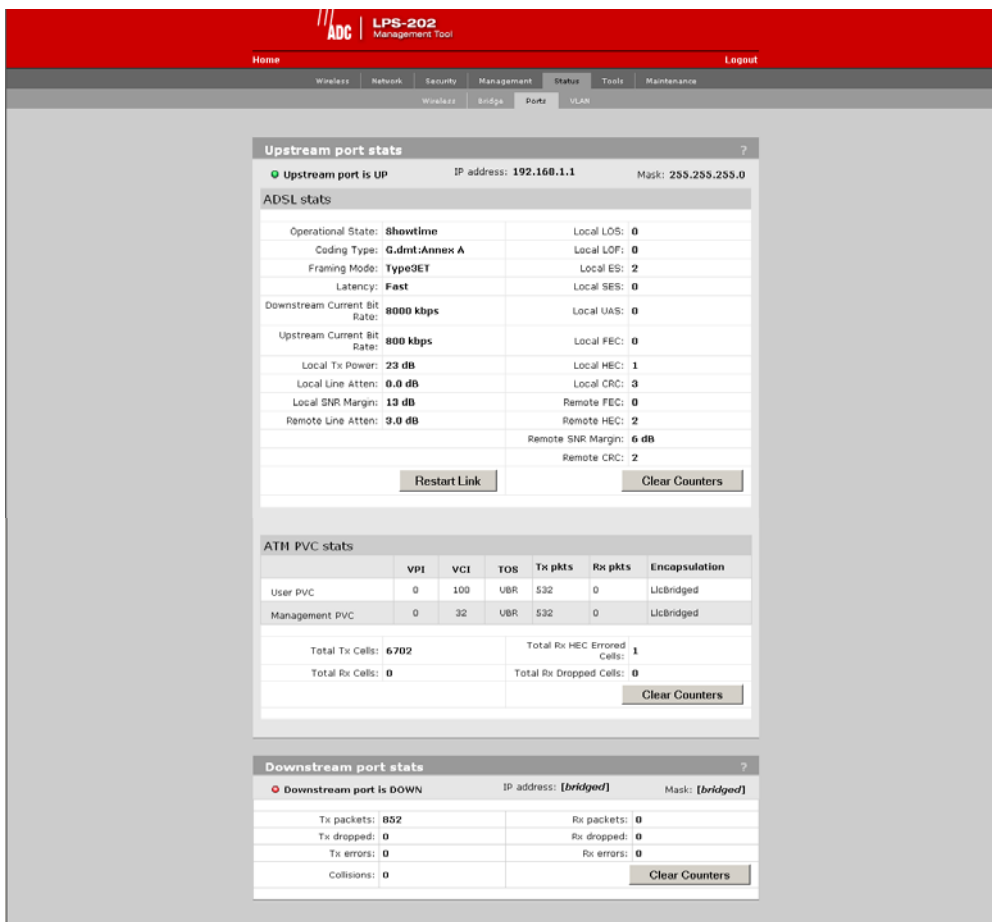
Number of packets received with errors. This can be caused by: overruns, unaligned frames, bad CRCs, frame length violations, or late collisions.

### **Collisions**

Collisions indicate how many times two stations tried to use the network simultaneously. A small number of collisions is normal. A large number of collisions indicates that not enough bandwidth exists to support the traffic on the network. This may be caused by connecting too many client stations to the network or by one or more client stations performing continuous large data transfers. Either reduce the number of client stations or reduce the amount of traffic being carried by the network. You could also define customer quotas to limit the amount of traffic.

## ADSL PORTS STATUS (LPS-202 ONLY)

1. On **Status** menu, click **Ports**. The *Port stats* page opens.



### ADSL STAT PARAMETERS

#### Operational State

##### Showtime

Indicates an active ADSL link.

##### Idle

Indicates link is down and no attempt is being made to initialize the link.

##### Handshake

Indicates the ATU-C and ATU-R are in the process of synchronizing over the link.

##### Training

Indicates the ATU-C and ATU-R are negotiating link speed.

##### Framer

Indicates Framer is synchronizing with far end framer.

**Coding type**

The active ADSL line-encoding type configured at the CO. Supported coding types are: Inactive, G.dmt-Annex A, Alcatel 1.4, Alcatel, ADI, and ANSI T1.413i2

**Framing Mode**

The active ADSL framing mode configured at the CO. Supported framing modes are: Type0, Type1, Type2, Type3, and Type3ET

**Latency**

The ADSL latency mode configured at the CO. Supported latency modes are: Fixed and Interleaved

**Downstream Current Bit Rate**

Receive rate in bits per second of the device.

**Upstream Current Bit Rate**

Transmit rate in bits per second of the device.

**Local Tx Power**

The sum of all data-carrying DMT subcarrier powers averaged over a 1-second period.

**Local Line Atten**

The difference in dB between the power received at the near-end (ATU-R) and that transmitted from the far-end (ATU-C).

**Local SNR Margin**

The amount of communication signal in relation to the amount of interference, or noise, on the medium, measured at the ATU-R.

**Remote Line Atten**

The difference in dB between the power received at the far-end (ATU-C) and that transmitted from the near-end (ATU-R).

**Local LOS**

Loss of Signal error counts since power-up, measured at the ATU-R.

**Local LOF**

Loss of Frame error counts since power-up, measured at the ATU-R.

**Local ES**

Errored Second counts since power-up, measured at the ATU-R.

**Local SES**

Severely Errored Second counts since power-up, measured at the ATU-R.

**Local UAS**

Unavailable Second counts since power-up, measured at the ATU-R.

**Local FEC**

Forward Error Correction counts since power-up, measured at the ATU-R.

**Local HEC**

ATM over ADSL cell header error checksum counts since power-up, measured at the ATU-R.

**Local CRC**

Cyclical Redundancy Check counts since power-up, measured at the ATU-R.

**Remote FEC**

Forward Error Correction counts since power-up, measured at the ATU-C.

**Remote HEC**

ATM over ADSL cell header error checksum counts since power-up, measured at the ATU-C.

**Remote SNR Margin**

The amount of communication signal in relation to the amount of interference, or noise, on the medium, measured at the ATU-C.

**Remote CRC**

Cyclical Redundancy Check counts since power-up, measured at the ATU-C.

**ATM PVC STAT PARAMETERS****User PVC**

Indicates the user VPI, VCI, Type of service, and encapsulation method. Also shows the total transmitted and received packets since start up or the last time the counters were cleared.

**Management PVC**

Indicates the management VPI, VCI, Type of service, and encapsulation method. Also shows the total transmitted and received packets since start up or the last time the counters were cleared.

**Total Tx Cells**

Indicates the total amount of transmitted cells for the user and management PVC since startup or the last time the counters were cleared.

**Total Rx Cells**

Indicates the total amount of received cells for the user and management PVC since startup or the last time the counters were cleared.

**Total Rx HEC Errored Cells**

Indicates the total amount of received cells that have HEC errors.

**Total Rx Dropped Cells**

Indicates the total amount of dropped cells in the receive direction.

## DOWNSTREAM PORT STATS

### IP Address

The IP address assigned to the port.

### Mask

The mask assigned to the port.

### Tx Packets

Number of packets transmitted.

### Tx Dropped

Number of transmitted packets dropped.

### Tx Errors

Number of packets with transmission errors. This can be caused by: loss of carrier, no heartbeat, late collision, too many retransmits (too many collisions when transmitting a packet).

### Rx Packets

Number of packets received.

### Rx Dropped

Number of received packets dropped.

### Rx Errors

Number of packets received with errors. This can be caused by: overruns, unaligned frames, bad CRCs, frame length violations, or late collisions.

### Collisions

Collisions indicate how many times two stations tried to use the network simultaneously. A small number of collisions is normal. A large number of collisions indicates that not enough bandwidth exists to support the traffic on the network. This may be caused by connecting too many client stations to the network or by one or more client stations performing continuous large data transfers. Either reduce the number of client stations or reduce the amount of traffic being carried by the network. You could also define customer quotas to limit the amount of traffic.

## SECURITY RADIUS – ADD NEW PROFILE

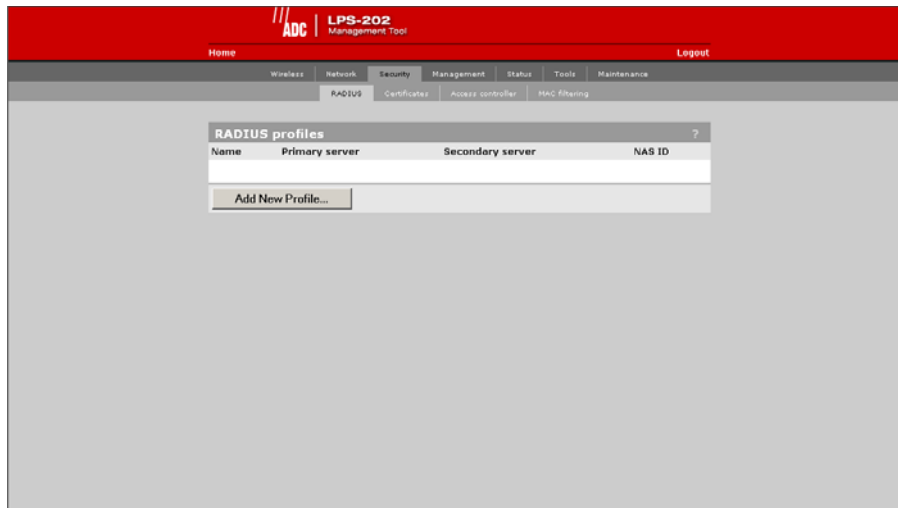
Each RADIUS profile defines the settings for a RADIUS client connection. To support a client connection, you must create a client account (e.g., RAS account) on the RADIUS server. The settings for the account must match the profile settings you define on the LPS-20x.

For backup redundancy, each profile supports a primary and secondary server. The LPS-20x will function with any RADIUS server that supports RFC 2865 and RFC 2866. Authentication occurs via EAP-MDS, CHAP, MSCHAP v1/ v2 or PAP. To edit a profile, click on its name.

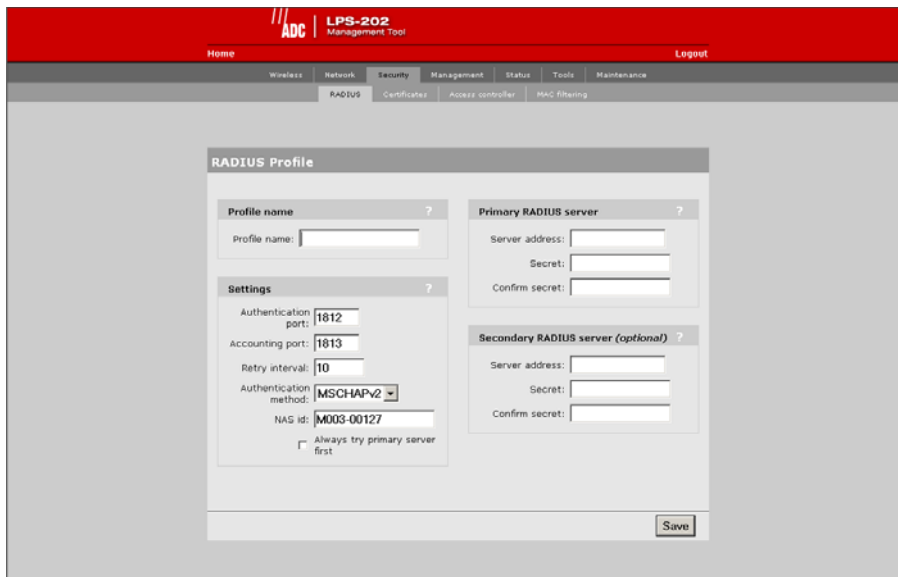


Only management users can be authenticated directly with RADIUS servers. For clients to be authenticated, the LPS-20x must have security filters enabled and an access controller (e.g., LPX-21x) must be accessible.

1. On the main menu, click **Security**.
2. Click **RADIUS**. The *RADIUS profiles* page opens.



3. Select **Add New Profile**. The *RADIUS configuration* page opens.



## PROFILE NAME PARAMETER

Specify the name to identify the profile.

## SETTING PARAMETERS

### Authentication Port

Specify the port to use for authentication. By default, RADIUS servers use port 1812.

### Accounting Port

Specify the port to use for accounting. By default, RADIUS servers use port 1813.

### Retry Interval

Controls the retry interval (in seconds) for access and accounting requests that time-out. If no reply is received within this interval, the LPS-20x switches between the primary and secondary RADIUS servers (if defined). If a reply is received after the interval expires, it is ignored. This parameter applies to access and accounting requests generated by the following:

- administrator logins to the management tool
- customer logins via HTML
- MAC-based authentication of devices
- authentication of the LPS-20x

The maximum number of retries can be determined as follows:

- HTML-based Logins: The number of retries is calculated by taking the setting for HTML-based logins Authentication Timeout parameter and dividing it by the value of this parameter. The default settings result in four retries (40/10).
- MAC-based and LPS-20x authentication: Number of retries is infinite.
- 802.1x authentication: Retries are controlled by the 802.1x client software.

### Authentication Method

Choose the default authentication method the LPS-20x will use when exchanging authentication packets with the primary/secondary RADIUS server defined for this profile.

For 802.1x users, the authentication method is always determined by the 802.1x client software and is not controlled by the setting.

If traffic between the LPS-20x and the RADIUS server is not protected by a VPN, it is recommended that you use EAP-MD5 or MSCHAP V2 if supported by your RADIUS server. (PAP, MSCHAP V1 and CHAP are less secure protocols.)

### NAS Id

Specify the network access server ID you want to use for the LPS-20x. By default, the serial number of the LPS-20x is used. The LPS-20x includes the NAS-ID attribute in all packets that it sends to the RADIUS server.

**Always Try Primary Server First**

Set this option to force the LPS-20x to contact the primary server first. Otherwise, the LPS-20x sends the first RADIUS access request to the last known RADIUS server that replied to any previous RADIUS access request. If the request times out, the next request is sent to the other RADIUS server (if defined).

For example, assume that the primary RADIUS server was not reachable and that the secondary server responded to the last RADIUS access request. When a new authentication request is received, the LPS-20x sends the first RADIUS access request to the secondary RADIUS server. If it does not reply, the RADIUS access request is retransmitted to the primary RADIUS server. The LPS-20x always alternate between the two servers (when configured).

**PRIMARY RADIUS SERVER****Server Address**

Specify the IP address of the RADIUS server.

**Secret/Confirm Secret**

Specify the secret (password) that the LPS-20x will use when communicating with the RADIUS server. The shared secrets is used to authenticate all packets exchanged with the server to prove that they originate from a valid/trusted source.

**SECONDARY RADIUS SERVER (OPTIONAL)****Server Address**

Specify the IP address of the RADIUS server.

**Secret/Confirm Secret**

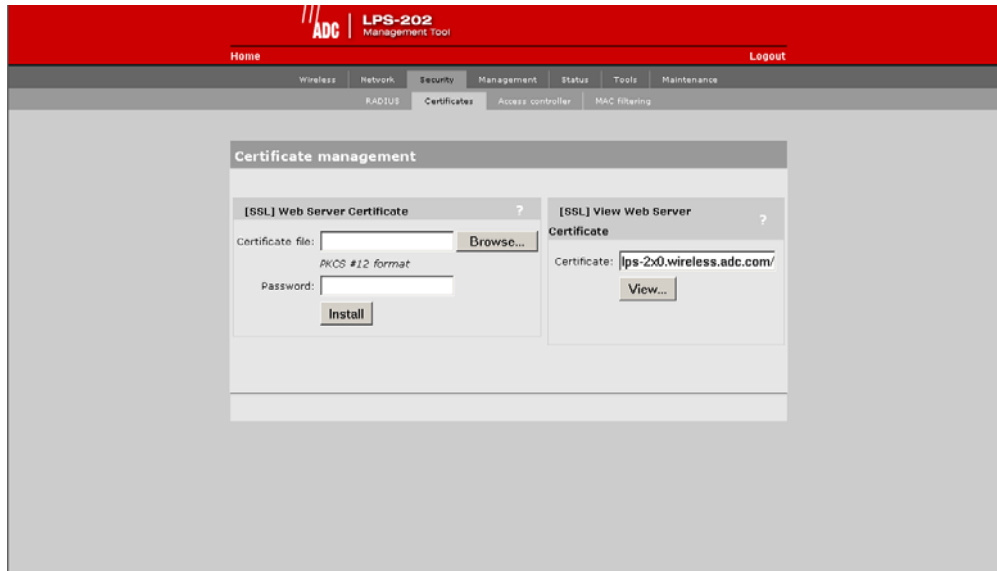
Specify the secret (password) that the LPS-20x will use when communicating with the RADIUS server. The shared secrets is used to authenticate all packets exchanged with the server to prove that they originate from a valid/trusted source.



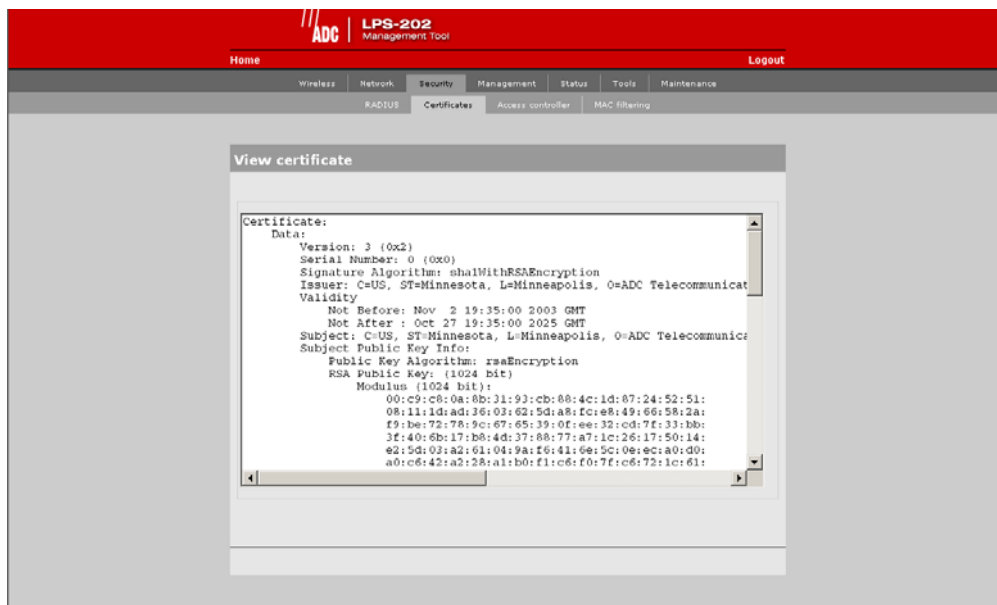
## SECURITY CERTIFICATES

Use this option to replace the SSL certificate that ships with the LPS-20x with one of your own. This certificate is used when validating user logins to the management tool via SSL.

1. On the main menu, click **Security**.
2. Click **Certificates**. The *Certificate Management* page opens.



3. Select **View** to see the contents of the certificate. The *View Certificate* page opens.



The certificate field shows the contents of the CN field in the certificate. This is the domain name of the certificate.

## CONFIGURING THE SNMP INTERFACE

This section provides an overview of the SNMP interface and the MIBs supported by the LPS-20x. The LPS-20x SNMP interface can be reached both locally and remotely for complete flexibility.

### TO CONFIGURE SNMP OPTIONS

1. On the main menu, click **Management**, then click **SNMP**. The *SNMP configuration* page opens.

2. Enable the options that you require. The options are described in the sections that follow.
3. Click **Save**.

### ATTRIBUTES

#### System Name

Specify the name to identify the LPS-20x.

#### Contact

Contact information for the LPS-20x.

#### Community Name

This is the password that controls access to the SNMP information. A network management program must supply this password when attempting to set or get SNMP information from the LPS-20x.

#### Read-only community name

This is the password that controls read-only access to the SNMP information. A network management program must supply this password when attempting to get SNMP information from the LPS-20x. The default is public.

## AGENT

Enables/disables support for SNMP.

### Port

Specify the port and protocol the LPS-20x will use to respond to SNMP requests. The default port is 161.

### SNMP Protocol

Specify the SNMP version.

## TRAPS

Enables/disables support for SNMP traps. The LPS-20x supports the following MIB II traps:

- coldStart
- linkUp
- linkDown
- authenticationFailure

In addition, the LPS-20x supports a number of ADC-specific traps as described in the MIBs. The MIBs are available from ADC.

### Community Name

Specify the password required by the remote host that will receive the trap.

### Host

Specify the IP address or domain name of the host that the LPS-20x will send traps to.

### Port

Specify the port that the LPS-20x will send traps on. By default, port 162 is used.

### Configure Traps

Click this button to customize certain traps.

## SECURITY

### Allowed Addresses

Lets you define a list of IP addresses from which access to the SNMP interface is permitted. To add an entry, specify the IP address and appropriate mask and click **Add**.

When the list is empty, access is permitted from any IP address.

### Active Interfaces

Choose the interfaces through which client stations will be able to access the SNMP interface.

## STANDARD MIBs

The LPS-20x supports the following MIBs:

- IEEE8021-PAE-MIB
- RFC1213-MIB – Full read support. Write support as defined below.
- 802.11b

The MIB defined in "IEEE Std 802.11b/D8.0, September 2001 Annex D" has been moved under the MIB (COLUBRIS-IEEE802DOT11).

- Colubris MIB

## MANAGEMENT CONSOLES

- To manage the LPS-20x, third-party SNMP management consoles must support the SNMPV2c protocol.

## MIB II SUPPORT DETAILS

The LPS-20x provides complete read support of MIB II objects 1.10. Table 14 lists all MIB II objects defined as read/write and indicates the objects that can be "set" on the LPS-20x.

**Table 14. MIB II Read/Write Objects**

Set	Group	OID	Notes
Y	system	sysContact	
Y		SysName	
Y		sysLocation	
Y	interfaces	ifAdminStatus(1)	Can be up(1), down(2), or testing(3)
N	At	AtIfIndex	
N		atPhysAddress	
N		atNetAddress	
N	Ip	ipForwarding	
N		ipDefaultTLL	
N		ipRouteDest	
N		ipRouteIfIndex	
N		ipRouteMetric1	
N		ipRouteMetric2	
N		ipRouteMetric3	
N		ipRouteMetric4	
N		ipRouteNextHop	
N		ipRouteType (3)	Can be other(1), invalid(2), direct(3), or indirect(4)
N		ipRouteAge	
N		ipRouteMask	

<b>Set</b>	<b>Group</b>	<b>OID</b>	<b>Notes</b>
N		ipRouteMetric5	
N		ipNetToMediaIflIndex	
N		ipNetToMediaNetAddress	
N		ipNetToMediaType(4)	Can be other(1), invalid (2), dynamic(3), or static(4)
N	Tcp	tcpConnState(5)	Can be closed(1), listen(2), synSent(3), synReceived(4), established(5), finWait1(6), finWait2(7), closeWait(8), lastAck(9), closing(10), timeWait(11), or deleteTCB(12)

## COLUBRIS ENTERPRISE MIB

The Colubris Enterprise MIB is available (refer to [Product Support on page 177](#)). It is organized as follows:

- COLUBRIS-802DOT1X-MIB.my
- COLUBRIS-CDP-MIB.my
- COLUBRIS-IEEE802DOT11.my
- COLUBRIS-MAINTENANCE-MIB.my
- COLUBRIS-PRODUCTS-MIB.my
- COLUBRIS-PUBLIC-ACCESS-MIB.my
- COLUBRIS-SMI.my
- COLUBRIS-SYSLOG-MIB.my
- COLUBRIS-SYSTEM-MIB.my
- COLUBRIS-TC.my

**Table 15. MIB II Read/Write Objects**

Group	OID	Get	Set
dot11StationConfig	dot11StationId	N	N
	dot11MediumOccupancyLimit	N	N
	dot11CFPPeriod	N	N
	dot11CFPMaxDuration	N	N
	dot11AuthenticationResponseTimeOut	N	N
	dot11PowerManagementMode	N	N
	dot11DesiredSSID	N	N
	dot11DesiredBSSType	N	N
	dot11OperationalRateSet	N	N
	dot11BeaconPeriod	Y	N
	dot11DTIMPeriod	Y	N
	dot11AssociationResponseTimeOut	N	N
dot11PrivacyOptionImplemented	Y	N	
dot11AuthenticationAlgorithms	dot11AuthenticationAlgorithmsEnable	Y	N
dot11WEPDefaultKeys	dot11WEPDefaultKeyValue	Y	Y
dot11WEPKeyMappings	dot11WEPKeyMappingAddress	N	N
	dot11WEPKeyMappingWEPOn	N	N
	dot11WEPKeyMappingValue	N	N
	dot11WEPKeyMappingStatus	N	N

<b>Group</b>	<b>OID</b>	<b>Get</b>	<b>Set</b>
dot11Privacy	dot11PrivacyInvoked	Y	Y
	dot11WEPDefaultKeyID	Y	Y
	dot11WEPKeyMappingLength	N	N
	dot11ExcludeUnencrypted	Y	Y
dot11SMTnotification		N	N
dot11Operation	Dot11RTSThreshold	Y	N
	Dot11ShortRetryLimit	Y	N
	Dot11LongRetryLimit	Y	N
	Dot11FragmentationThreshold	Y	N
	Dot11MaxTransmitMSDULifetime	Y	N
	Dot11MaxReceiveLifetime	Y	N
dot11Counters		Y	N
Group OID			
dot11GroupAddresses	Dot11Address	N	N
	Dot11GroupAddressesStatus	N	N
dot11PhyOperation	Dot11CurrentRegDomain	Y	N
dot11PhyAntenna	Dot11CurrentTxAntenna	Y	N
	Dot11CurrentRxAntenna	Y	N
dot11PhyTxPower	Dot11CurrentTxPowerLevel	Y	N
dot11PhyFHSS	Dot11CurrentChannelNumber	N	N
	Dot11CurrentDwellTime	N	N
	Dot11CurrentSet	N	N
	Dot11CurrentPattern	N	N
	Dot11CurrentIndex	N	N
dot11PhyDSSS	Dot11CurrentChannel	Y	Y
	Dot11CurrentCCAMode	Y	N
	Dot11EDThreshold	Y	N

Group	OID	Get	Set
dot11PhyIR	Dot11CCAWatchdogTimerMax	N	N
	Dot11CCAWatchdogCountMax	N	N
	Dot11CCAWatchdogTimerMin	N	N
	Dot11CCAWatchdogCountMin	N	N
dot11RegDomainsSupported		Y	N
dot11AntennasList	Dot11SupportedTxAntenna	Y	N
	Dot11SupportedRxAntenna	Y	N
	Dot11DiversitySelectionRx	Y	N
SupportedDataRatesTx		Y	N
SupportedDataRatesRx		Y	N

**Traps**

Not applicable.



## SSL CERTIFICATES

This section explains how to create and install SSL certificates to secure communications with the LPS-20x.

### OVERVIEW OF SSL CERTIFICATES

The only way to securely access a web server is to encrypt the data stream that is exchanged between the browser and the web server. This ensures that if data is intercepted by a malicious third-party using a network analyzer on the LAN or the Internet, it will be difficult or impossible for the data to be deciphered.

However, encryption does not solve another important security issue, namely how the identity of a web server can be validated before a connection to it is established. The solution to this problem is provided by digital certificates.

A digital certificate is a collection of information about a web server digitally signed by a certificate authority. A certificate authority is by definition an entity that can be trusted. It may be an entity in your organization responsible for issuing certificates, a commercial certificate authority such as Thawte, Entrust or even yourself.

SSL is the standard for creating a secure encrypted connection between a web browser and a web server. SSL relies on the exchange of digital certificates which provide the means for the web server and browser to authenticate each other.

### SSL AUTHENTICATION

The following sequence of steps illustrates how an SSL session is established.

1. A web browser attempts to open a web page via HTTPS.
2. The web server sends its digital certificate (as well as information needed to establish the SSL connection) to the web browser. The certificate is signed using the private key of a certificate authority (CA). This is usually a well known commercial entity.
3. The web browser attempts to validate the web server's certificate. This happens as follows:
  - The web browser checks that the server's certificate has not expired. The certificate will contain the certificate's validity period which can be compared to the current date.
  - The web browser may be configured to check that the certificate is not in a Certificate Revocation List maintained by the entity that issued the certificate.
  - The web browser checks its internal list of trusted CAs to find the one that signed the web server's certificate. Using the public key of this CA (which is also stored in the web browser), the web browser validates the authenticity of the web server's digital signature. This is possible because the web server's certificate is signed using the CA's private key.
  - The web browser extracts the domain name of the web server from the certificate. (When the certificate was registered, this domain name was associated with the IP address of the LPS-20x's Internet port.) It then compares this against the domain name of the web server.
4. The web browser and the web server agree on a symmetric key to encrypt the SSL connection.
5. The SSL connection is started.

The host name in the currently installed SSL certificate is automatically assigned as the domain name of the LPS-20x. The factory default SSL certificate that is installed on the LPS-20x has the host name **wireless.adc.com**. You do not have to add this name to your DNS server for it to be resolved. The LPS-20x intercepts all DNS requests it receives on the wireless or LAN ports. It resolves any request that matches the certificate host name by returning the IP address assigned to the wireless port. All other DNS requests are forwarded to the appropriate DNS servers as configured on the **Network > DNS** page. To summarize, this means that by default, any DNS request by a client station on the wireless or LAN ports that matches **wireless.adc.com** will return the IP address of the LPS-20x's wireless port.

## ABOUT CERTIFICATE WARNING MESSAGES

The default certificate installed on the LPS-20x is not registered with an authority certificate. It is a self-signed certificate which is attached to the default IP address (192.168.1.1) for the LPS-20x.

This results in the following warning message each time a web browser attempts to validate the certificate.



There are three types of possible warnings in the Security Alert:

1. The security certificate was issued by a company you have not chosen to trust. This indicates that your browser has no knowledge of the certificate and treats it as if it cannot be trusted. The warning is caused by not having a CA certificate in the browser that can validate the certificate provided by the LPs-20x. To eliminate this warning message, you can install a new certificate as described in [Installing a new SSL certificate on page 141](#).
2. The Security certificate date is valid. Signifies that the operating system's date is within the range of beginning and end dates specified in the security certificate. Certificates have a limited lifetime and must be renewed and replaced before they expire or else warnings will appear in the browser.
3. The security certificate has a valid name. This refers to the domain name listed in the "subject" field of the security certificate that matches the domain name of the URL that you're attempting to go to. By default, the name in the "subject" field of the certificate installed in the LPs-20x also becomes the domain name of the LPs-20x and is resolved by the LPs-20x itself.



Once you comply with all three criteria, client stations will no longer get a certificate warning in their browser.

## INSTALLING A NEW SSL CERTIFICATE

Do the following to create and install a new certificate on the LPS-20x.

1. **Obtain or create a new SSL certificate.** For instructions, see [Step 1: Creating SSL Certificates on page 142.](#)
2. **Prepare the certificate chain.** For instructions, see [Step 2: Preparing the certificate chain on page 155.](#)
3. **Convert the Certificate.** For instructions, see [Step 3: Converting a Certificate to PKCS #12 Format on page 156.](#)
4. **Install the certificate on the LPS-20x.** For instructions, see [Step 4: Installing a New SSL Certificate on page 157.](#)
5. **Install certificates on the client stations.** For instructions, see [Step 5: Installing Certificates in a Browser on page 158.](#)

## STEP 1: CREATING SSL CERTIFICATES

There are three ways to create a digital certificate:

1. Obtain a certificate from a recognized certificate authority: This is the best option, since it ensures that your certificate can be validated by any web browser. A number of companies offer this service for a nominal charge. These include: Thawte, Verisign, and Entrust.
2. Become a CA and issue your own certificate: You can become your own CA and create as many certificates as you require. However, since your CA will not be included in the internal list of trusted CAs maintained by most browsers, customers will get a security alert until they add your CA to their browser.
3. Create a self-signed certificate: This is the least secure method since the certificate is signed using the private key of the server rather than a CA. Self-signed certificates should generally be used for testing purposes only.

### CERTIFICATE TOOLS

Digital certificates can be created/managed with a variety of tools. The examples in this section use the OpenSSL tools and components included with the ADC Backend archive. You should download and install these items as follows:

1. Download the Backend sample archive (refer to [Product Support on page 177](#)).
2. Download **openssl-0.9.7c-win32-bin.zip** from <http://curl.haxx.se/download.html> > **OpenSSL Library Packages**.
3. Open a command prompt and create the following folder on your computer:  
**c:\certificates** and **c:\certificates\ca\newcerts**
4. Extract **openssl-0.9.7c-win32-bin.zip** into **c:\certificates**.
5. Extract the contents of the **certificates** folder in the Backend archive into **c:\certificates**.

You are now ready to execute the following examples.

### OBTAINING A REGISTERED CERTIFICATE

This example illustrates how to create a certificate request and send it to a certificate authority to obtain a registered public certificate.

The benefit of using a registered certificate is that the public key for these CAs is included by default in most web browsers and eliminates warning message pop-ups.

For the purpose of this example:

- the certificate will be requested for the domain name: **www.company.com**.
  - the secret password used to protect the key is **your\_password**.
1. Open a Windows command-line session.
  2. Go to the directory where you installed the certificate tools. This example assumes **c:\certificates**.
  3. Execute the command: **newreq domain\_name**

For example:

```
C:\certificates\>newreq www.company.com
You will now be prompted for a password
that will protect the new private key.
Loading 'screen' into random state - done
0 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
```

```
.....+++++
.....+++++
e is 65537 (0x10001)
Enter PEM pass phrase: your_password
```

At this stage, the private key has been generated and you are prompted to specify the secret password that will protect the key. Do not forget this password, otherwise you will lose access to the private key. From this point on, this password will be referred to as the key password.

When prompted, enter the password again to confirm it.  
Verifying password - Enter PEM pass phrase: **your\_password**  
Re-enter the password for your new private key  
(The same you just entered)  
Enter pass phrase for www.company.com.key: **your\_password**

You are about to be asked to enter information that will be incorporated into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank.  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.

```
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [Minnesota]:
Locality Name (eg, city) [Minneapolis]:
Organization Name (eg, company) [ADC Inc.]:Company Inc.
Organizational Unit Name (eg, section) [Research &
Development]:Department
Your Name []:www.company.com
Email Address [wsd.support@adc.com]:support@company.com
Generated certificate request:
Using configuration from openssl.conf
```

```
Certificate Request:
Data:
Version: 0 (0x0)
Subject: C=US, ST=Minnesota, L=Minneapolis, O=Company Inc.,
OU=Department, CN=www
.company.com/Email=support@company.com
Subject Public Key Info:
```

```
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:cb:bb:24:82:9d:f6:24:ee:8f:f4:ec:39:5c:88:
a2:c3:08:96:68:1b:0b:c8:a8:48:09:db:6f:01:c2:
45:41:d0:a4:eb:b0:11:78:3d:55:ea:49:26:e1:dc:
9a:02:79:ae:fc:2c:4a:8a:d7:d7:eb:50:49:ec:08:
d3:7b:fe:66:52:fd:74:0a:9d:f4:e1:79:95:3a:7f:
46:d6:79:ea:04:7c:63:1b:36:9c:c2:28:4f:1a:01:
9a:90:90:6f:7c:f3:b4:d7:0d:d5:9d:e0:bf:b3:af:
b9:8a:95:6a:87:20:0b:e8:28:29:03:cb:1d:54:9f:
6d:c5:67:d6:1d:6b:9a:08:4b
Exponent: 65537 (0x10001)
Attributes:
a0:00
Signature Algorithm: md5WithRSAEncryption
a5:53:2d:91:95:1f:9c:75:ac:0e:92:1d:b9:7f:b2:c3:ce:59:
ca:aa:fc:1c:e2:f2:09:a9:bf:1d:34:ae:a9:ac:44:6a:d8:7e:
ac:de:9e:ed:00:d9:57:e0:bf:c9:c1:a6:25:ba:d6:68:a8:24:
d5:05:94:03:c8:54:49:cd:db:a6:d4:87:29:c5:ab:0e:59:30:
01:f9:d0:f8:0e:75:c5:39:38:0c:77:e3:87:ab:6d:25:3f:fd:
d5:a6:08:0a:02:0c:67:6d:84:bb:2b:3e:d8:b3:2c:08:1d:38:
53:a7:61:00:7a:91:67:16:03:6a:51:0b:67:db:73:4c:4d:96:
bf:80
-----BEGIN CERTIFICATE REQUEST-----
MIIB2TCCAUICAQAwwZgxCzAJBgNVBAYTAkNBMQ8wDQYDVQQIEwZRdWViZWMyDjAM
BgNVBAcTBUXhdmFsMRUwEwYDVQQKEwxD21wYW55IEluYy4xEzARBgNVBAcTckRl
cGFydG11bnQxGDAwBgNVBAMTD3d3dy5jb21wYW55LmNvbTEiMCAGCSqGSIb3DQEJ
ARYTc3VwcG9ydEBjb21wYW55LmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAy7skgp32JO6P9Ow5XIiwwiWaBsLyKhICdtvAcJFQdCk67ARed1V6kkm4dya
Anmu/CxKitfX61BJ7AjTe/5mUv10Cp304XmVOn9G1nnqBHxjGzacwihPGgGakJBv
fPO01w3VneC/s6+5ipVqhyAL6CgpA8sdVJ9txWfWHWuaCEsCAwEAAaAAMA0GCSqG
SIb3DQEBBAAUAA4GBAKVTLZGVH5x1rA6SHbl/ssPOWcqq/Bzi8gmpvx00rqmsRGrY
fqzenu0A2Vfgv8nBpiW61mioJNUFlAPIVEN26bUhyNFqw5ZMAH50PgOdcU5OAx3
44erbSU//dWmCAoCDGdthLsrPtizLAgdOFOnYQB6kWCWA2pRC2fbc0xNlr+A
-----END CERTIFICATE REQUEST-----
```

At this stage, two files have been created in C:\certificates:

- **www.company.com.key**: This file contains the private key for the server.
- **www.company.com.req**: This file contains the certificate request.

Next, send the certificate request to a Trusted Certificate Authority to obtain a public key certificate from the CA. The certificate file will be protected by the password you specified.

## BECOMING A PRIVATE CA

This procedure enables you to sign your web server certificates using your own private key. Users who trust you will be able to trust the certificates you have signed, providing that they have your public key certificate.

### Creating the CA certificates

You will be asked for a password to protect the new private key, which will be the private key for your own Certificate Authority.

#### IMPORTANT



*This password will be required when signing subsequent certificates.*

Ideally, the private key should be handled as one of your corporate secrets and should be in a safe location accessible to the person responsible for signing the certificates.

For the purposes of this example:

- the certificate will be requested for the domain name: **CompanyCA**
  - the secret password used to protect the key is **CA\_key\_password**
1. Open a Windows command-line session.
  2. Go to the directory where you installed the certificate tools. This example assumes **c:\certificates**.
  3. Execute the command: **newca CompanyCA**

```
C:\certificates\>newca CompanyCA
You will be asked for a password protecting your
Certificate Authority Private Key
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....++++++
..++++++
writing new private key to 'CA\private\CAkey.pem'
Enter PEM pass phrase: CA_key_password
Verifying password - Enter PEM pass phrase: CA_key_password
```

-----  
You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,  
If you enter '.', the field will be left blank.

-----

```
Country Name (2 letter code) [US]:
State or Province Name (full name) [Minnesota]:
Locality Name (eg, city) [Minneapolis]:
Organization Name (eg, company) [ADC Inc.]:Company Inc.
Organizational Unit Name (eg, section) [Research &
Development]:Department
Your Name []:Test-Only Certificate Authority
Email Address [wsd.support@adc.com]:ca@company.com
The certificate for your CA will then be displayed.
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=Minnesota, L=Minneapolis, O=ADC Inc., OU=Department,
CN=Test
-Only Certificate Authority/Email=ca@company.com
Validity
Not Before: Feb 27 21:46:40 2002 GMT
Not After : Feb 27 21:46:40 2003 GMT
Subject: C=US, ST=Minnesota, L=Minneapolis, O=ADC Inc.,
OU=Department, CN=Test
t-Only Certificate Authority/Email=ca@company.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:c5:b8:ff:2b:82:cf:93:39:eb:90:ff:fe:21:a0:
de:d4:38:0c:ae:08:f3:dc:d5:52:59:80:9d:72:5a:
9b:2d:cf:22:e3:84:c9:f7:e1:99:67:7b:08:74:71:
25:14:24:93:00:f5:4f:c2:ee:6c:88:35:96:df:20:
80:69:4c:c8:13:df:7c:cc:06:86:c2:bc:30:4a:97:
41:b0:2d:23:33:60:bb:ba:68:5f:26:87:4b:22:14:
f6:3e:99:15:c6:ca:29:0d:c6:20:23:97:78:ae:94:
bb:13:02:ed:96:66:06:40:8a:60:7a:c8:ac:18:5b:
8c:4b:95:26:c2:84:04:e9:a9
Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
12:4c:98:8d:ed:da:42:5f:d4:d4:83:14:b1:2b:8a:28:a4:90:
30:8f:09:22:47:f5:3c:8d:e2:ae:8d:f6:4e:e9:14:0c:89:26:
f6:0a:92:dc:5a:9b:fc:77:e7:94:33:db:86:93:98:1b:34:37:
3d:5e:06:9e:4d:d9:50:4f:57:b5:3f:d8:06:ad:27:26:a8:5c:
b7:36:e0:10:ae:a2:b3:5a:ed:90:5a:90:85:0f:94:8e:01:55:
7d:e5:69:b1:60:19:9c:68:3b:4c:1c:4b:b7:0b:b5:47:9d:a5:
92:d6:45:df:e4:6a:db:96:af:58:13:88:c2:c2:f9:66:3b:32:
1d:bc
```



```

-----BEGIN CERTIFICATE-----
MIICvDCCAiWgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBoczELMAkGA1UEBhMCQ0Ex
DzANBgNVBAGTB1F1ZWJlYzEOMAwGA1UEBxMFTGF2YWVwFTATBgNVBAoTDENvbXBh
bnkgSW5jLjJlETMBEGA1UECzMKRGVwYXJ0bWVudDEoMCYGA1UEAxMfVGVzdC1Pbm5
IENlcnRpZmljYXR1IEF1dGhvcml0eTEdMBsGCSqGSIb3DQEJARYOY2FAY29tcGFu
eS5jb20wHhcNMDIwMjI3MjE0NjQwWWhcNMDMwMjI3MjE0NjQwWjCBoczELMAkGA1UE
BhMCQ0ExDzANBgNVBAGTB1F1ZWJlYzEOMAwGA1UEBxMFTGF2YWVwFTATBgNVBAoT
DENvbXBhbnkgSW5jLjJlETMBEGA1UECzMKRGVwYXJ0bWVudDEoMCYGA1UEAxMfVGVz
dC1Pbm5IENlcnRpZmljYXR1IEF1dGhvcml0eTEdMBsGCSqGSIb3DQEJARYOY2FA
Y29tcGFueS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMW4/yuCz5M5
65D//iGg3tQ4DK4I89zVUlmAnXJamy3PIuOEyffhmWd7CHRxJRQkkwD1T8LubIgl
lt8ggG1MyBPffMwGhsK8MEqXQbAtIzNgu7poXyaHSyIU9j6ZFcbKKQ3GICOXeK6U
uxMC7ZzZmBkCKYHrIrBhbJeuVJsKEBOmpAgMBAAEwDQYJKoZIhvcNAQEBBQADgYEA
EkyYje3aQ1/U1IMUsSuKKKSQMI8Jikf1PI3iro32TukUDIkM9gqS3Fqb/HfnlDPb
hpOYGzQ3PV4Gnk3ZUE9XtT/YBq0nJqhctzbGek6is1rtkFqQhQ+UjgFVfeVpsWAZ
nGg7TBxLtwu1R521ktZF3+Rq25avWBOIwsL5ZjsyHbw=
-----END CERTIFICATE-----

```

At this stage, two files have been created in c:\certificates:

- **CompanyCA.key**, which contains the private key for your new Certificate Authority.
- **CompanyCA.pem**, which contains the X.509 certificate for your Certificate Authority's public key.

These two files have been respectively copied into:

```

C:\certificates\CA\private\CAkey.pem
and
C:\certificates\CA\private\CAcert.pem

```

### Creating the web server certificates

Once you have created the CA certificates, you can use them to create certificates for your LPS-20x or web server.

1. Open a Windows command-line session.
2. Go to the directory where you installed the certificate tools. This example assumes **c:\certificates**.
3. Execute the command: **newcert domain\_name**

```

C:\certificates\>newcert www.company.com
*** You will now be prompted for a password ***
*** that will protect the new private key. ***
Loading 'screen' into random state - done
0 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....++++++
....++++++
e is 65537 (0x10001)
Enter PEM pass phrase: your_password
Verifying password - Enter PEM pass phrase: your_password
*** Re-enter the password for your new private key ***
*** (The same you just entered) ***
Using configuration from openssl.conf

```

Enter PEM pass phrase:

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [US]:

State or Province Name (full name) [Minnesota]:

Locality Name (eg, city) [Minneapolis]:

Organization Name (eg, company) [ADC Inc.]:Company Inc.

Organizational Unit Name (eg, section) [Research & Development]:Department

Your Name []:www.company.com

Email Address [wsd.support@adc.com]:webmaster@company.com

Generated certificate request:

Using configuration from openssl.conf

Certificate Request:

Data:

Version: 0 (0x0)

Subject: C=US, ST=Minnesota, L=Minneapolis, O=ADC Inc.,  
OU=Department, CN=www

.company.com/Email=webmaster@company.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:f6:93:52:3b:6b:da:7c:f2:dc:4b:5f:93:2c:9a:

0c:50:52:ac:3d:5a:a4:43:d2:ef:7d:36:b5:54:9c:

7a:df:b2:bd:9b:82:41:3b:ae:07:8a:45:26:a3:37:

eb:c1:c4:e7:04:d2:67:32:ca:08:33:9f:ac:ec:23:

89:e2:36:60:63:61:5c:2d:60:9a:92:48:ed:b3:7c:

0f:60:94:6d:a4:74:d5:eb:a9:7f:40:cc:cd:24:ae:

13:f0:a7:ea:db:81:a5:d0:1b:dc:26:f8:8f:89:c6:

27:1d:5c:d5:ae:a4:94:76:e8:d6:14:37:ac:aa:95:

62:26:d8:22:b1:5f:fb:19:d5

Exponent: 65537 (0x10001)

Attributes:

a0:00

```
Signature Algorithm: md5WithRSAEncryption
35:04:94:33:7e:13:86:05:9e:dd:49:4d:eb:d7:cb:21:6c:8b:
aa:84:2a:6b:9b:ff:49:7d:6f:06:49:c8:ba:18:8b:b7:ad:4b:
ab:3d:2d:91:79:1f:c3:48:a1:83:7b:d4:38:b6:10:1c:87:bd:
e6:46:41:69:b1:1a:ec:31:19:cc:05:44:46:24:7b:3b:b4:e2:
f3:54:94:36:90:f3:5f:f8:94:23:95:e6:26:0f:c7:36:39:44:
5d:94:85:e6:64:10:ae:b5:4e:a0:3b:ca:bd:e0:ae:eb:ad:af:
44:bf:20:a2:f8:30:cc:14:f1:0a:0e:3b:b5:32:a3:c9:2a:14:
05:25
```

-----BEGIN CERTIFICATE REQUEST-----

```
MIIB2zCCAUAQAQAwgZoxCzAJBgNVBAYTAKNBMQ8wDQYDVQQIEwZRdWVizWmxDjAM
BgNVBActBUxhdmFsMRUwEwYDVQQKEwxD21wYW55IEluYy4xEzARBgNVBAsTCkRl
cGFydG1lbnQxGDAWBgNVBAMTD3d3dy5jb21wYW55LmNvbTEkMCIIGCSqGSIB3DQEJ
ARYVd2VibWFzdGVyQGNvbXBhbnkuY29tMIGfMA0GCSqGSIB3DQEBQUAA4GNADCB
iQKBgQD2k1I7a9p88txLX5MsmgxQUqw9WqRD0u99NrVUnHrfsr2bgkE7rgeKRSaj
N+vBxOce0mcyggzn6zSI4niNmBjYVwtYJqSSO2zfA9glG2kdNXrqX9AzM0krhPw
p+rbgaXQG9wm+I+JxicdXNWupJR26NYUN6yqlWIm2CKxX/sZ1QIDAQABoAAwDQYJ
KoZIHvcNAQEEBQADgYEANQSUM34ThgWe3U1N69fLIWyLqoQqa5v/SX1vBknIuhiL
t61Lqz0tkXkfw0ihg3vUOLYQHie95kzBabEa7DEZzAVERiR7O7Ti81SUNpDzX/iU
I5XmJg/HNjleXZSF5mQQrrVOoDvKveCu662vRL8govgwzBTxCg47tTKjySoUBSU=
```

-----END CERTIFICATE REQUEST-----

\*\*\* You will now be prompted for the password for your \*\*\*

\*\*\* Certificate Authority private key. \*\*\*

Using configuration from openssl.conf

Loading 'screen' into random state - done

Enter PEM pass phrase:

Check that the request matches the signature

Signature ok

The Subjects Distinguished Name is as follows

```
countryName          :PRINTABLE:'US'
stateOrProvinceName  :PRINTABLE:'Minnesota'
localityName         :PRINTABLE:'Minneapolis'
organizationName     :PRINTABLE:'ADC Inc.'
organizationalUnitName :PRINTABLE:'Department'
commonName           :PRINTABLE:'www.company.com'
emailAddress         :IA5STRING:'webmaster@company.com'
```

Certificate is to be certified until Feb 28 16:31:17 2003 GMT (365 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

At this stage, two files have been created:

- **www.company.com.pem**, which contains the X.509 certificate for the web
- **www.company.com.key**, which contains the private key for the server. server's public key.

A copy of www.company.com.pem has been created as:

C:\certificates\DemoCA\CA\newcerts\01.pem

The file containing the next serial number that will be used for the next certificate to be signed has been updated:

C:\certificates\DemoCA\CA\serial

The previous version of this file is in:

C:\certificates\DemoCA\CA\serial.old

The file containing the serial numbers and descriptions of all certificates issued by the certificate authority has been updated with a description of the certificate just issued to www.company.com:

C:\certificates\DemoCA\CA\index.txt

The previous version of this file is in:

C:\certificates\DemoCA\CA\index.txt.old

## CREATING A SELF-SIGNED CERTIFICATE

If you decide to use this option, there is no need for a certificate authority. This limits the effectiveness of the certificate since it is signed using the private key of the server.

For the purposes of this example:

- the certificate will be requested for the domain name: **www.yourserver.com**
  - the secret password used to protect the key is **your\_password**
1. Open a Windows command-line session.
  2. Go to the directory where you installed the certificate tools. This example assumes **c:\certificates**.
  3. Execute the command: **newselfcert domain\_name**.

```
C:\certificates>newselfcert www.company.com
You will now be prompted for a password
that will protect the new private key.
Loading 'screen' into random state - done
0 semi-random bytes loaded
Generating RSA private key, 1024 bit long modulus
.....+++++
+
.....+++++
e is 65537 (0x10001)
Enter pass phrase: your_password
Verifying password - Enter pass phrase: your_password
Re-enter the password for your new private key
(The same you just entered)
Enter pass phrase for www.company.com.key: your_password
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [US]:

State or Province Name (full name) [Minnesota]:

Locality Name (eg, city) [Minneapolis]:

Organization Name (eg, company) [ADC Inc.]:Company Inc.

Organizational Unit Name (eg, section) [Research & Development]:Department

Your Name []:www.company.com

Email Address [wsd.support@adc.com]:webmaster@company.com

The resulting self-signed certificate will then be displayed:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=US, ST=Minnesota, L=Minneapolis, O=Company Inc., OU=Department, CN=www.

company.com/Email=webmaster@company.com

Validity

Not Before: Feb 27 21:34:38 2002 GMT

Not After : Mar 29 21:34:38 2002 GMT

Subject: C=US, ST=Minnesota, L=Minneapolis, O=Company Inc., OU=Department, CN=www

.company.com/Email=webmaster@company.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

```

00:d7:63:8f:5f:ee:29:99:6e:6a:c5:06:61:30:e7:
87:3e:5b:d5:04:af:ba:92:cd:f1:cc:f4:19:4a:95:
ec:79:76:47:b5:5a:0d:4d:aa:7d:27:c2:d5:1c:bf:
4a:04:3a:34:6e:86:6d:34:40:1a:15:1b:21:4c:44:
eb:50:f4:27:19:bd:59:0f:80:a9:85:a7:0b:4e:5d:
1e:c8:b8:ff:1a:c4:d9:18:2a:9d:a9:c9:1c:0f:17:
92:38:58:89:ac:1e:b6:d4:b0:97:5d:47:41:28:ea:
ef:f5:cf:ac:c1:cc:0e:d9:9f:71:d6:74:ec:32:af:
a9:26:5b:11:cf:96:be:09:c9
Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
38:f2:ee:90:38:fc:23:ce:0c:e2:50:5b:86:a9:f0:7e:2e:b6:
dd:d9:4a:d1:ad:6a:78:b0:44:f8:44:dd:4c:8b:93:49:44:35:
a8:ae:77:b1:ae:be:bb:0b:27:28:7d:69:f5:6e:9a:51:88:82:
32:a6:2d:21:16:ea:81:11:c8:6e:b2:f3:c8:4b:4b:72:1e:7d:
55:7e:5f:86:0f:f0:63:96:a9:08:e3:d0:f5:3b:f6:b5:a8:ed:
8f:65:56:7d:7c:b8:a3:09:50:39:39:fe:e1:f7:fc:82:6f:7b:
da:07:8d:09:9c:a0:a1:c2:09:b0:9e:24:4d:20:d5:95:0b:bd:
08:8b

```

-----BEGIN CERTIFICATE-----

```

MIICqjCCAhOgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBmjELMAkGA1UEBhMCQ0Ex
DzANBgNVBAGTB1F1ZWJlYzEOMAwGA1UEBxMFTGF2YWwxFTATBgNVBAoTDENvbXBh
bnkgSW5jLjJlETMBEGA1UECxMKRGVwYXJ0bWVudDEYMBYGA1UEAxMPd3d3LmNvbXBh
bnkuY29tMSQwIgwYJKoZIhvcNAQkBFhV3ZWJtYXN0ZXJAY29tcGFueS5jb20wHhcN
MDIwMjI3MjEzNDM4WmcNMDIwMjI3MjEzNDM4WjCBmjELMAkGA1UEBhMCQ0ExDzAN
BgNVBAGTB1F1ZWJlYzEOMAwGA1UEBxMFTGF2YWwxFTATBgNVBAoTDENvbXBhbnkg
SW5jLjJlETMBEGA1UECxMKRGVwYXJ0bWVudDEYMBYGA1UEAxMPd3d3LmNvbXBhbnku
Y29tMSQwIgwYJKoZIhvcNAQkBFhV3ZWJtYXN0ZXJAY29tcGFueS5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBANdj1/uKZluasUGYTDnhz5b1QsvupLN8cz0
GUqV7H12R7VaDU2qfSfC1Ry/SgQ6NG6GbTRAGhUbIUxE61D0Jxm9WQ+AqYWnC05d
Hsi4/xrE2RgqnanJHA8XkjhYiawettSw111HQSjq7/XPrMHMDtmfcdZ07DKvqSZb
Ec+WvgnJAgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAOPLukDj8I84M41Bbhqnfwi62
3dlK0a1qeLBE+ETdTIuTSUQ1qK53sa6+uwsnKH1p9W6aUYiCMqYtIRbqgRHibrLz
yEtLch59VX5fhg/wY5apCOPQ9Tv2tajtj2VWfXy4owlQOTn+4ff8gm972geNCZyg
ocIJsJ4kTSDVlQu9CIs=

```

-----END CERTIFICATE-----

At this stage, two files have been created:

- **www.company.com.key**, which contains the private key for the server.
- **www.company.com.pem**, which contains the X.509 certificate for the web server's public key.

## VIEWING THE CERTIFICATE

It is important to confirm that the company details are correct and in this case, you will see that the Issuer and the Subject are different. The content of the certificate CA be displayed using **viewcert**.

```
C:\certificates\DemoCA>viewcert www.company.com
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, ST=Minnesota, L=Minneapolis, O=ADC Inc.,
OU=Department, CN=Test
-Only Certificate Authority/Email=ca@company.com
Validity
Not Before: Feb 28 16:31:17 2002 GMT
Not After : Feb 28 16:31:17 2003 GMT
Subject: C=US, ST=Minnesota, L=Minneapolis, O=ADC Inc.,
OU=Department, CN=www
.company.com/Email=webmaster@company.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:f6:93:52:3b:6b:da:7c:f2:dc:4b:5f:93:2c:9a:
0c:50:52:ac:3d:5a:a4:43:d2:ef:7d:36:b5:54:9c:
7a:df:b2:bd:9b:82:41:3b:ae:07:8a:45:26:a3:37:
eb:c1:c4:e7:04:d2:67:32:ca:08:33:9f:ac:ec:23:
89:e2:36:60:63:61:5c:2d:60:9a:92:48:ed:b3:7c:
0f:60:94:6d:a4:74:d5:eb:a9:7f:40:cc:cd:24:ae:
13:f0:a7:ea:db:81:a5:d0:1b:dc:26:f8:8f:89:c6:
27:1d:5c:d5:ae:a4:94:76:e8:d6:14:37:ac:aa:95:
62:26:d8:22:b1:5f:fb:19:d5
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
E3:5A:38:77:E4:0C:B9:16:98:BF:A8:D5:A4:5D:A8:81:A2:C2:72:B6
X509v3 Authority Key Identifier:
DirName:/C=CA/ST=Minneapolis/L=Minnesota/O=Company Inc./
OU=Department/CN=
Test-Only Certificate Authority/Email=ca@company.com
serial:00
Signature Algorithm: md5WithRSAEncryption
37:2b:ad:c2:18:9a:dc:ab:14:b9:de:f4:dd:d4:b8:21:84:59:
2a:8a:af:5f:ea:a5:33:1b:90:0e:56:ff:f5:34:5c:1b:8c:1b:
```

```

ba:bd:64:1b:f0:6b:f4:a8:b8:14:dc:8b:1f:25:f9:04:25:85:
82:d5:07:8b:26:90:7d:c7:c8:71:ba:37:e0:a8:42:91:31:30:
2b:56:4a:34:70:14:22:38:7c:3f:99:5d:a5:5c:2c:a0:52:58:
cc:b0:87:5d:14:ff:c3:7e:c8:ed:4e:a8:7b:ca:f3:d3:e3:85:
99:88:a4:7f:26:15:a1:14:61:01:87:18:53:ab:48:d4:f8:f9:
aa:2d
-----BEGIN CERTIFICATE-----
MIID0DCCAzmGAWIBAgIBATANBgkqhkiG9w0BAQQFADCBozELMAkGA1UEBhMCQ0Ex
DzANBgNVBAGTB1F1ZWJlYzEOMAwGA1UEBxMFTGF2YWVwFTATBgNVBAoTDENvbXBh
bnkgSW5jLjETMBEGA1UECXMKRGVwYXJ0bWVudDEoMCIYGA1UEAxMfVGVzdC1Pbmx5
IENlcnRpZmljYXR1IEF1dGhvcml0eTEdMBSGCSqGSIB3DQEJARYOY2FAY29tcGFu
eS5jb20wHhcNMDIwMjI4MTEyMTEzMTUzMTUzMTUzMTUzMTUzMTUzMTUzMTUzMTUz
BhMCAQExDzANBgNVBAGTB1F1ZWJlYzEOMAwGA1UEBxMFTGF2YWVwFTATBgNVBAoT
DENvbXBhbnkgSW5jLjETMBEGA1UECXMKRGVwYXJ0bWVudDEoMCIYGA1UEAxMfVGVz
dC1Pbmx5IENlcnRpZmljYXR1IEF1dGhvcml0eTEdMBSGCSqGSIB3DQEJARYO
Y2FAY29tcGFueS5jb20wHhcNMDIwMjI4MTEyMTEzMTUzMTUzMTUzMTUzMTUzMTUz
b20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAPaTUjtr2nzy3EtfkyyaDFBS
rD1apEPS7302tVScet+yvZuCQTuuB4pFJqM368HE5wTSzLKCDOfrOwjieI2YGNh
XC1gmpJI7bN8D2CUbaR01eupf0DMzSSuE/Cn6tuBpdAb3Cb4j4nGJx1c1a6klHbo
1hQ3rKqVYibYIrFf+xnVAgMBAAGjggEZMIIBFTAJBgNVHRMEAjAAMCwGCWCGSAGG
+EIBDQOQfFh1PcGVuU1NMIEdlbmVyYXR1ZCBBDZXJ0aWZpY2F0ZTAAdBgNVHQ4EFgQU
41o4d+QMuRaYv6jVpF2ogaLCCrYwgboGA1UdIwSBsjCBR6GBqaSBpjCBozELMAkG
A1UEBhMCQ0ExDzANBgNVBAGTB1F1ZWJlYzEOMAwGA1UEBxMFTGF2YWVwFTATBgNV
BAoTDENvbXBhbnkgSW5jLjETMBEGA1UECXMKRGVwYXJ0bWVudDEoMCIYGA1UEAxMf
VGVzdC1Pbmx5IENlcnRpZmljYXR1IEF1dGhvcml0eTEdMBSGCSqGSIB3DQEJARYO
Y2FAY29tcGFueS5jb22CAQAwDQYJKoZIhvcNAQEEBQADgYEANYutwhia3KsUud70
3dS4IYRZKoaqX+qlMxuQDlb/9TRcG4wbur1kG/Br9Ki4FNyLHyX5BCWFgtUHiyaQ
fcfIcbo34KhCkTEwK1ZKNHAUIjh8P5ldpVwsoFJYzLCHXRT/w37I7U6oe8rz0+OF
mYikfyYVORRhAYcYU6tI1Pj5qi0=
-----END CERTIFICATE-----

```

This time, the issuer and subject fields of the certificate are different.

### VERIFYING THE CERTIFICATE

You can check that a certificate has been issued by your Certificate Authority using the command **verifycert**:

```

C:\certificates\DemoCA>verifycert CompanyCA www.company.com
www.company.com.pem: OK

```



## STEP 2: PREPARING THE CERTIFICATE CHAIN

When a web browser connects to the LPS-20x using SSL, the LPS-20x only sends its own SSL certificate to the browser. This means that if the certificate has been signed by an intermediate certificate authority, and if the web browser only knows about the root certificate authority that signed the Public Key Certificate of the Intermediate certificate authority, the web browser will not get the whole certificate chain it needs to validate the identity of the LPS-20x.



This does not apply when using self-signed certificates, since these certificates implicitly contain the whole chain.

To resolve this problem, all the public key certificates must be appended to the certificate (`www.company.com.pem` file, for example) in base64 format.

For example, if the LPS-20x certificate has been signed by an intermediate CA (CA2), and if the public key certificate for CA2 was signed by CA1 root CA, the following certificates should be appended to the file `www.company.com.pem`.

```
-----BEGIN CERTIFICATE-----
this is CA1 certificate
in BASE64/PEM encoding
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
this is CA2 certificate
in BASE64/PEM encoding
-----END CERTIFICATE-----
```

When done, the `www.company.com.pem` file should look like this:

```
-----BEGIN CERTIFICATE-----
insert the www.company.com certificate in BASE64/PEM encoding
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
insert the CA1 certificate in BASE64/PEM encoding
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
insert the CA2 certificate in BASE64/PEM encoding
-----END CERTIFICATE-----
```

## STEP 3: CONVERTING A CERTIFICATE TO PKCS #12 FORMAT

Before you can install a certificate on the LPS-20x, you need to convert it to PKCS #12 format. This can be done with the openssl program **pemtopkcs12**. Execute the command:

### **pemtopkcs12 certificate**

Replace **certificate** with the name of the certificate file.

Make sure that the .PEM and .KEY file are in the same folder and have the same name (with a different extension).

You will be prompted for two passwords:

- PEM pass phrase: Password used to protect the private key
- Export password: Password that will lock the PKCS#12 file. You will specify this password when you load the certificate onto the LPS-20x.

For example:

```
pemtopkcs12 hotspot.adc.com
Loading 'screen' into random state - done
Enter PEM pass phrase:
Enter Export Password:
Verifying password - Enter Export Password:
```

This procedure will generate a file named **.pcs12** file that contains both the private key and public key certificate. This file can now be installed on the LPS-20x.

## STEP 4: INSTALLING A NEW SSL CERTIFICATE

Use this procedure to replace the SSL certificate that ships with the LPS-20x with one of your own. This certificate is used when validating user logins to the management tool via SSL.

Before you can install a new SSL certificate, make sure that it conforms to the following:

- It must be in PKCS #12 format. Refer to [Step 3: Converting a Certificate to PKCS #12 Format on page 156](#) for instructions on how to do this.
- It must contain a private key. (The password is used to access the private key.)
- It must not have a name that is an IP address. The name should be a domain name containing at least one dot. If you try to add a certificate with an invalid name, the default certificate is restored.
- It must contain the entire certificate chain if signed by an intermediate certificate authority.
- It must not have a “\_” in its name.

The name in the certificate is automatically assigned as the domain name of the LPS-20x. The default certificate has the name wireless.adc.com.

### MANUAL INSTALLATION

To install a new SSL certificate, do the following:

1. Use your web browser to open the management tool.
2. On the **Security** menu, click **Certificates**.
3. In the **Web server - SSL certificate** box, specify the location of the new certificate and its password. If you are using the certificate created by the example in this section:
  - The certificate is located in: **c:\certificates\www.company.com.pkcs12**.
  - The password is **your\_export\_password**.
4. Click **install**.

## STEP 5: INSTALLING CERTIFICATES IN A BROWSER

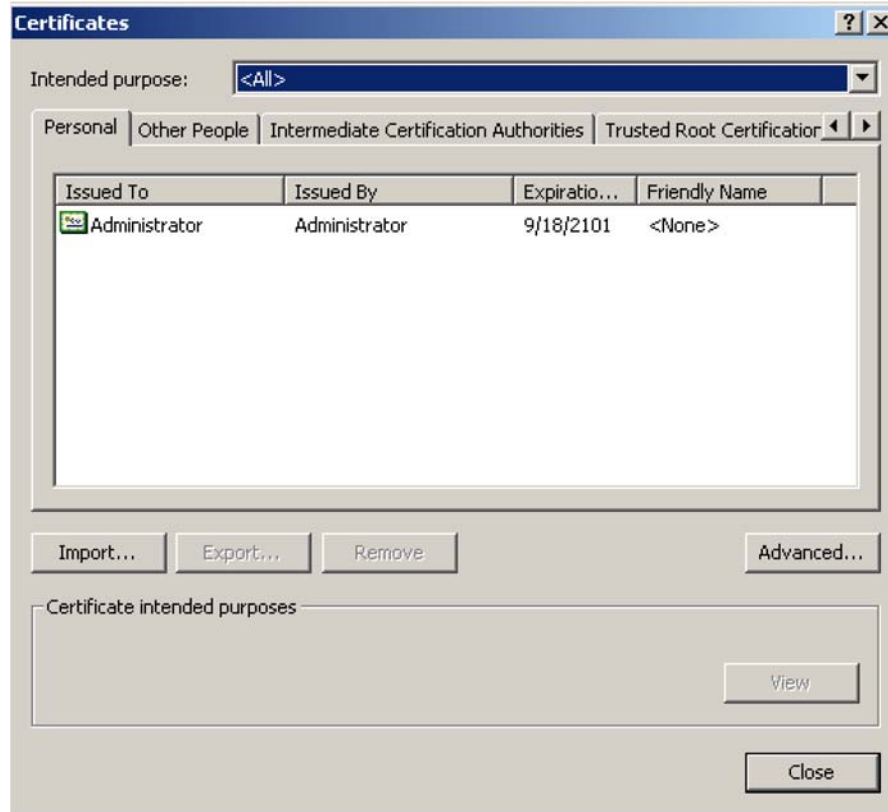
If you are operating as your own certificate authority, installing a certificate signed by your own CA will still cause a security warning to appear when customers open the LPS-20x's Login page. This occurs because your CA is not part of the group of well-known certificate authorities included with most browsers. This means customers will get a security warning when establishing the SSL connection with the Login page.

To eliminate this warning message, customers must add the public key certificate for your CA to the list maintained by their browsers.

### INTERNET EXPLORER

To eliminate the certificate warning message in Internet Explorer 6.0, do the following:

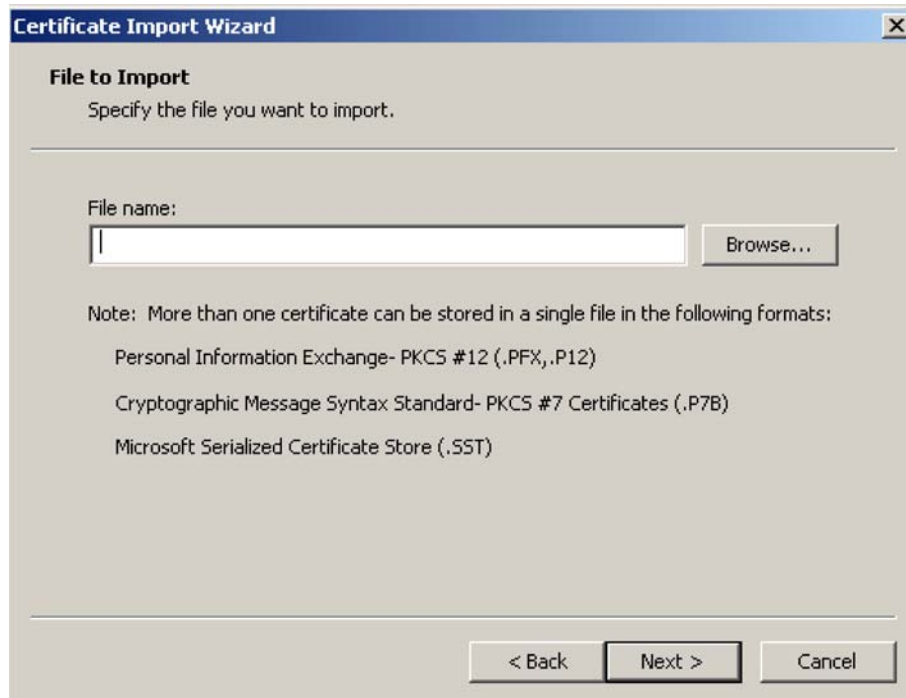
1. On the **Tools** menu, click **Internet Options**.
2. Click the **Content** tab.
3. Click **Certificates**. The *Certificates* window opens.



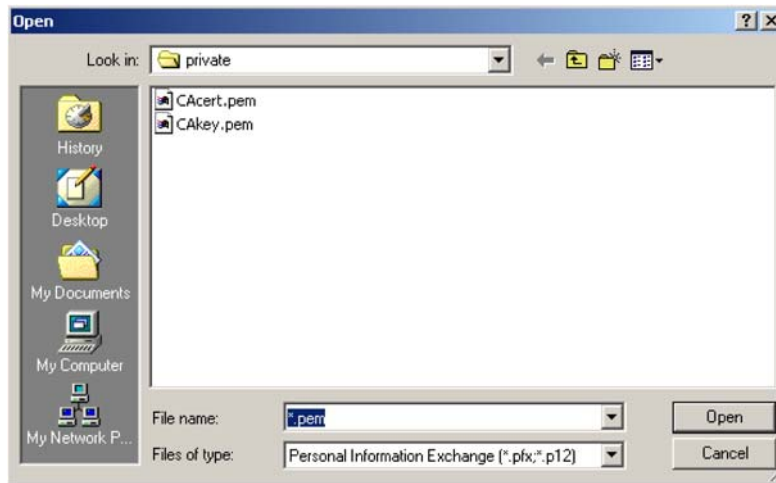
4. Click **Import**. The *Certificate Import Wizard* starts. Click **Next**.



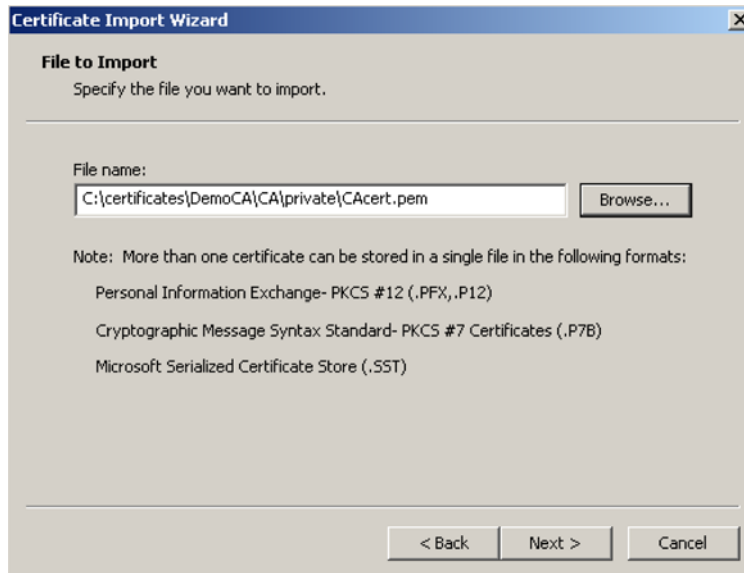
5. Click **Browse**.



- 6. Specify \*.pem in the **File name** box, and press the **Enter** key, then select **CAcert.pem** and click **Open**.



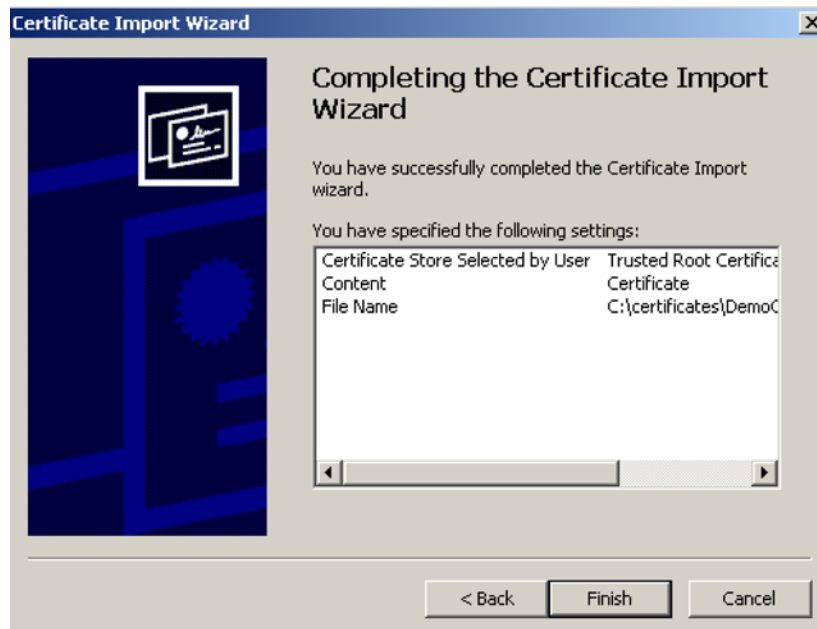
- 7. Click **Next**.



8. Click **Next**.



9. Click **Finish**.



10. Click **Yes**.



Customers who do this will no longer see any security warnings.

## NETSCAPE NAVIGATOR

To eliminate the certificate warning message in Netscape Navigator 7.1, do the following:

1. On the **Edit** menu, click **Preferences**.
2. Click **Privacy & Security**.
3. Click **Certificates**.
4. Click **Manage Certificates**.
5. Click **Authorities**.
6. Click **Import**.
7. Select your Public Key certificate. (If you are using the examples in this section, select **C:\certificates\ca\private\CAcert.pem**.)
8. Click **Open**.
9. Select **Trust this CA to identify web sites**.
10. Optional: Click **View** to verify the certificate details.
11. Click **Ok, Ok**.



## THE CONFIGURATION FILE

This section provides an overview of the configuration file and explains how to edit it.

### MANUALLY EDITING THE CONFIG FILE

The configuration file contains the settings for all customizable parameters on the LPS-20x. Almost all of these parameters can be set using the web-based management tool. However, certain infrequently-used parameters can only be set by manually editing the configuration file.

### RETRIEVING/RESTORING THE CONFIGURATION FILE

To edit the configuration file, you must first retrieve it from the LPS-20x. Once edited, it then needs to be restored. There are several ways to do this:

- The easiest way to accomplish both tasks is via the management tool. Use the **Config file management** page on the **Maintenance** menu to download/upload the configuration file.
- HTTPS: The configuration file can be downloaded and uploaded via HTTPS. Use a tool like cURL to make this easy. Refer to **Configuration File Management on page 56** for details.
- Many configuration file parameters are also accessible via SNMP. For details, see the comments inside the Colubris-Maintenance-MIB (refer to **Product Support on page 177**).

#### **IMPORTANT**



***The local username and password for the administrator is not saved when you use the Backup Configuration option. If you upload a configuration file, the old username and password are therefore not updated.***

***If you upload a configuration file with an invalid structure, it is possible to put the LPS-20x into an unstable state. To return to normal operation, do a factory reset.***

## CONFIGURATION FILE STRUCTURE

The configuration file is an ASCII file and can be edited in a standard text editor. Key components in the file are:

- **Block:** A block contains sections, sub-sections, and parameters. Blocks start with:  
`%begin block_name`  
and end with:  
`%end block_name`
- **Section:** A section contains sub-sections and parameters. Sections start with:  
`[SECTION_NAME]`  
and end with another block or section name. Section names are not case-sensitive.
- **Sub-section:** A sub-section contains parameters. Sub-sections start with:  
`<SUB-SECTION_NAME>`  
and end with another block, section, or sub-section name. Sub-section names are not case-sensitive.
- **Parameter:** A parameter takes the form: *parameter = value*  
Each parameter and value pair must appear on its own line. Parameter names are not case-sensitive. Parameter values **are** case-sensitive.
- **Comments:** Comments begin with the pound sign (#) and continue until the end of the line.
- Dash (-) and underscore (\_) characters can be used in section names, subsection names, and parameter names, and are strictly equivalent.
- Blank lines are ignored and may be added in to make the file easier to read.
- Strings containing spaces must be contained in double-quotes.

# TROUBLESHOOTING

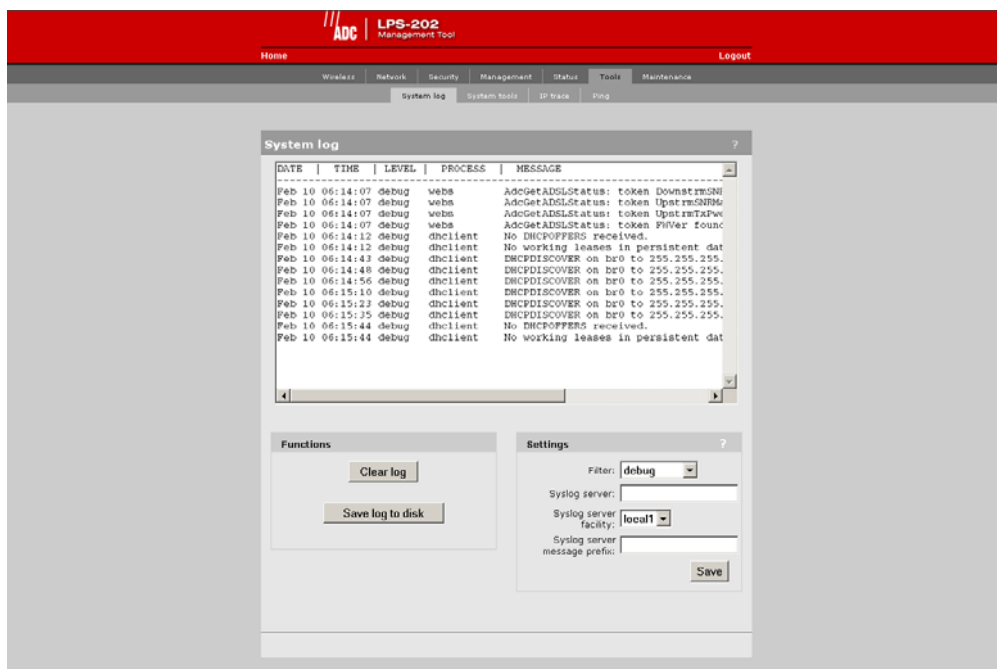
## SYSTEM LOG

The system log maintains a record of the last 400 events that occurred on the LPS-20x.



The log file is reset if the LPS-20x loses power or is restarted abnormally.

1. On the main menu, click **Tools**.
2. Click **System Log**. The *System log* page opens.



## SETTING PARAMETERS

### Filter

Specify the type of messages that will be recorded in the log. Each message level includes all those below it. For example, if you select “notice,” then all messages under it in the list are included. This means that selecting “debugs” logs all messages. Messages are classified as follows:

- Debug: Debug-level messages
- Info: Informational messages
- Notice: Normal, but significant condition
- Warning: Warning condition
- Error: Error condition
- Critical: Critical condition
- Alert: Action must be taken immediately
- Emergency: System is unusable

### Syslog Server

Specify the address of the device to send log entries to.

### Syslog Server Facility

The facility that will be used when logging messages to a syslog server. Available facilities are local0-local7.

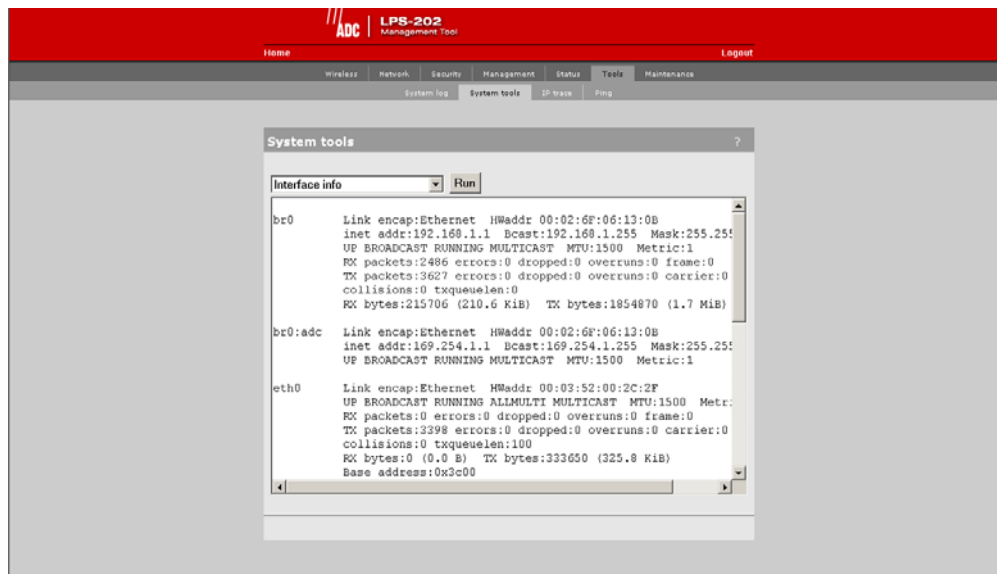
## SYSTEM TOOLS

The system tools enables you to obtain detailed information on the internal operation of the LPS-20x.

1. On the main menu, click **Tools**.
2. Click **System Tools**. The *System tools* page opens.



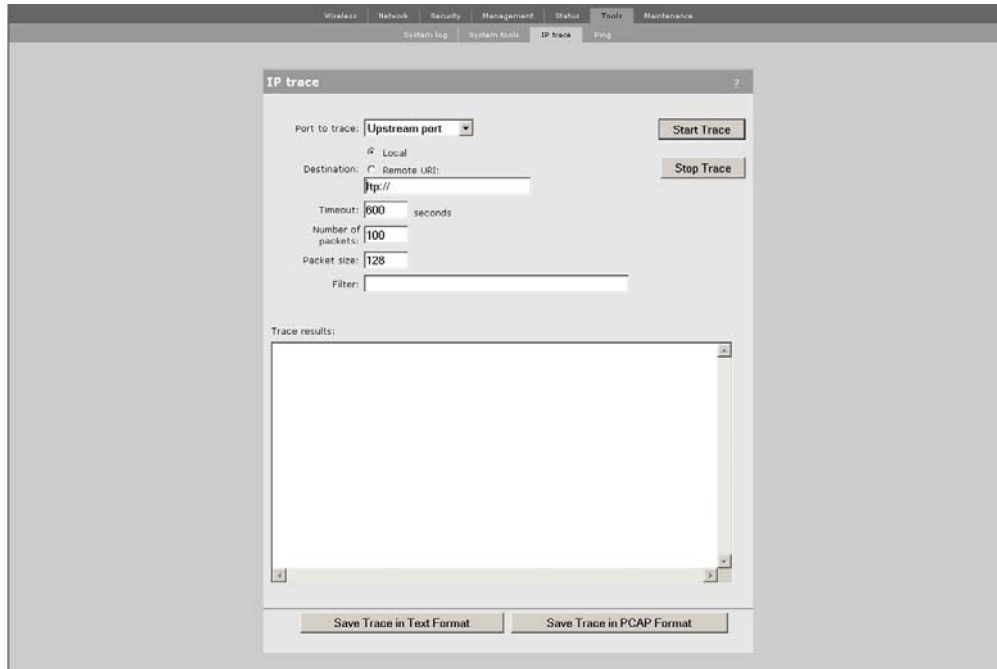
3. Select the desired tool in the pull-down window.
4. Click on **Run**. The detailed information screen opens.



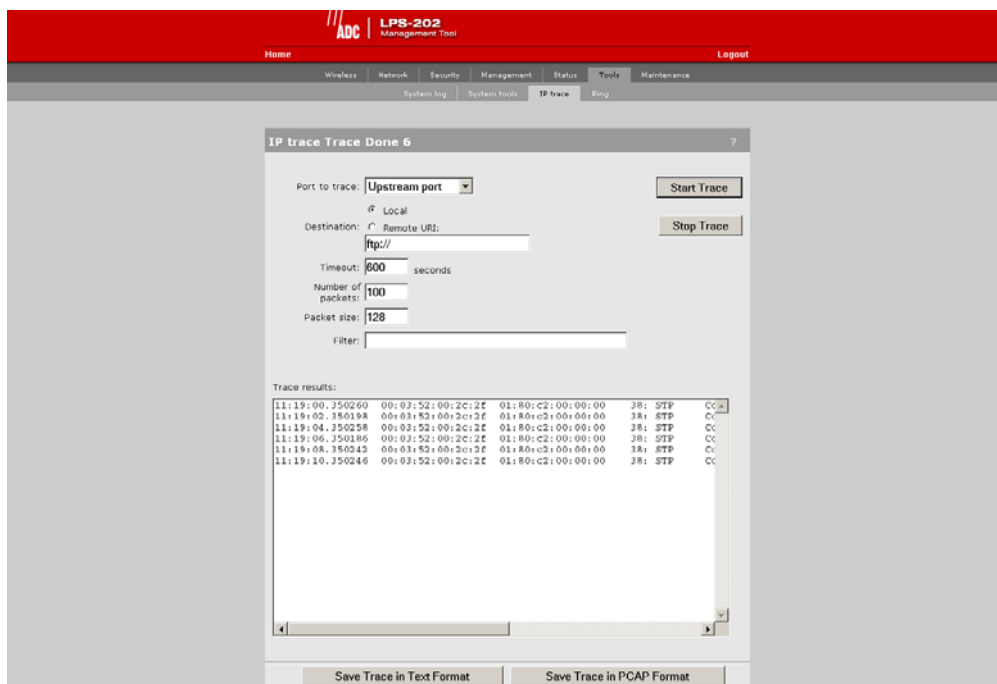
# IP TRACE

The IP trace enables you to capture detailed information on the data streaming through the LPS-20x.

1. On the main menu, click **Tools**.
2. Click **IP Trace**. The *IP trace* page opens.



3. Click on **Start Trace**.
4. Click on **Stop Trace** to review the results.



## IP TRACE PARAMETERS

### Port to Trace

Choose the port to apply the trace to.

### Destination

Select where the trace file will be stored/sent:

- Local: Trace file is stored on the LPS-20x. Size of the trace file is limited by available memory. When space is exhausted, the trace is truncated.
- Remote URL: Specify the URL of the remote device to send the trace file to. Trace data is automatically sent as it is gathered; therefore, there is no size limit to the trace. To avoid unnecessary bandwidth usage, a filter should be used to restrict the trace.
- When using FTP://, the trace is saved in Etherneal PCAP format.
- When using HTTP://, the target server must be able to receive and save the file correctly. Server-side scripts may be required to support this.

### Timeout

Specify the amount of time the trace will capture data (in seconds). Once this limit is reached, the trace automatically stops.

### Number of Packets

Specify the maximum number of packets (IP datagrams) the trace should capture. Once this limit is reached, the trace automatically stops.

### Packet Size

Specify the maximum number of bytes to capture for each packet. The rest of the data is discarded.

**Filter**

Lets you specify a filter expression which controls which packets will be captured by the trace. Leave the filter blank to trace all packets. The filter expression has the same format and behavior as the expression parameter used by the well-known TCPDUMP command. **Table 16** is a summary of syntax of this command. For more detailed information, consult one of the many TCPDUMP pages available on the Internet. The filter consists of one or more primitives. Primitives usually consist of a qualifier followed by an id (number or name).

**Table 16. Syntax**

Qualifier	Description
type	Possible values are: host, net, port. If you do not specify a type qualifier, then host is assumed.  Examples: host 192.168.30.57 net 128.3 port 20
dir	Identifies transfer direction. Possible values are: src, dst, src or dst, src and dst If you do not specify a dir qualifier, then src or dst is assumed.  Examples: src 192.168.30.57 dst net 128.3 src or dst port ftp-data
proto	Restricts the trace to a particular protocol. Possible values are: ether, ip, arp, rarp, tcp, udp. If you do not specify a proto qualifier, then all protocols consistent with the supplied type are assumed.  Examples: src 192.168.30.57 (implies ip, arp or rarp) net yahoo.com (implies ip, arp or rarp) net yahoo.com and port 53 (implies tcp or udp on port 53)



In addition to [Table 16](#), there are some special “primitive” keywords that do not follow the pattern: gateway, broadcast, less, greater and arithmetic expressions. For more detailed information, consult one of the many TCPDUMP pages available on the Internet. More complex filter expressions are built up by using the words: “and”, “or”, and “not” to combine primitives.

For Example:

```
host 192.168.30.57 and not port ftp and not port ftp-data
```

To save typing, identical qualifier lists can be omitted.

For Example:

```
tcp dst port ftp or ftp-data or domain
```

is exactly the same as

```
tcp dst port ftp or tcp dst port ftp-data or tcp dst port domain
```

The following examples show how to construct some basic trace filters.

```
src 192.168.30.57
```

```
src not 192.168.130.57
```

```
src or dst 192.168.30.57
```

```
src or dst net 192.168.130
```

```
tcp port 21 or tcp port 20 which is the same as tcp port 21 or 20
```

```
dst port 21 and tcp
```

```
tcp port 21 and src or dst 192.168.130.57
```

```
icmp
```

```
broadcast
```

### Trace Results

Displays the results of the trace after it stops.

### Start Trace

Starts the trace. Data captured by the trace is not displayed until the trace has stopped.

### Stop Trace

Stops the trace and displays the captured data in the Trace results box.

### Save Trace in Text Format

Click this button to save the captured data to an ASCII file.

### Save Trace in PCAP Format

Click this button to save the captured data to a PCAP file, which is the format used by the Ethereal Network Protocol Analyzer. Ethereal is free and is available for both Unix and Windows. It allows you to interactively browse the trace data, viewing summary and detailed information for each packet to a much greater level of detail than is provided by the text version of the trace.

## PING

1. On the main menu, click **Tools**.
2. Click **Ping**. The *Ping* page opens.



## PING PARAMETERS

### Address/URL to Ping

Specify the IP address of the network device you want to ping.

### Timeout

Specify how long the LPS-20x will wait for a reply to the ping before timing out.

## **REGULATORY, WIRELESS INTEROPERABILITY, AND HEALTH INFORMATION**

### **REGULATORY INFORMATION**

The LPS-20x complies with the following radio frequency and safety standards.

#### **CANADA - INDUSTRY CANADA (IC)**

This device complies with RSS 210 of Industry Canada. Cet appareil numérique de la classe B est conforme à la norme NMB-003 et CNR 210 d'Industrie Canada.

#### **EUROPE - EU DECLARATION OF CONFORMITY**

This device is for indoor use only.

**IMPORTANT** *Users must select the proper country of operation when ordering to ensure wireless operational settings conform to local regulations.*



*If more than one unit is deployed, users must ensure that the operating frequencies are spread among different channels (according to channel availability).*

#### **USA - FEDERAL COMMUNICATIONS COMMISSION (FCC)**

The LPS-20x complies with Part 15 of FCC Rules. Operation of the LPS-20x in a system is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference that may cause undesired operation.

#### **Caution: Exposure to Radio Frequency Radiation**

The radiated output power of the LPS-20x is far below the FCC radio frequency exposure limits. Nevertheless, the LPS-20x should be used in such a manner as to minimize the potential for human contact during normal operation. When using this device in combination with ADC antenna products, a certain separation distance between the antenna and nearby persons has to be kept to ensure RF exposure compliance.

Refer to the Regulatory Statements as identified in the documentation that comes with those products for additional information.

When an external antenna is connected to the LPS-20x, it shall be placed in such a manner as to minimize the potential for human contact during normal operation. To avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

When no external antenna is connected, the RF output power of the LPS-20x is far below the FCC radio frequency exposure limits. Nevertheless, it is advised to use the LPS-20x in such a manner that human contact during normal operation is minimized.

### Interference Statement

The LPS-20x has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

The LPS-20x generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If the LPS-20x causes harmful interference to radio or television reception which can be determined by turning the LPS-20x on and off, the user is encouraged to try and correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the distance between the LPS-20x and the receiver.
- Connect the LPS-20x to an outlet on a circuit different from that which the receiver is connected (if locally powered).
- Consult your dealer or an experienced radio/TV technician for help.

ADC is not responsible for any radio or television interference caused by unauthorized modification of the LPS-20x, or the substitution or attachment of connecting cables and equipment other than that specified by ADC.

The correction of interference caused by such unauthorized modification, substitution or attachment is the responsibility of the user.

## HEALTH INFORMATION

The LPS-20x, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by the LPS-20x is much less than the electromagnetic energy emitted by other wireless devices, such as mobile phones.

Because the LPS-20x operates within the guidelines found in radio frequency safety standards and recommendations, ADC believes that the LPS-20x 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 the LPS-20x may be restricted by the proprietor of the building or responsible representatives of the organization. These situations may, for example, include:

- Using the LPS-20x

In any 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 to the use of wireless devices in a specific organization or environment (e.g. airports), you are encouraged to ask for authorization to use the LPS-20x prior to turning it on.

## **ACRONYMS**

### **A**

**ADSL** – Asymmetric Digital Subscriber Line

**AP** – Span-Powered Access Point

**ATM** – Asynchronous Transfer Mode

**AWG** – American Wire Gauge

### **C**

**CA** – Certificate Authority

**CO** – Central Office

**CTS** – Clear To Send

### **D**

**DHCP** – Dynamic Host Configuration Protocol

**DLC** – Digital Loop Carrier

**DN** – Distinguished Name

**DNS** – Domain Naming System

**DSL** – Digital Subscriber Loop

**DSLAM** – Digital Subscriber Line Access Multiplexer

**DSSS** – Direct Sequence Spread Spectrum

### **E**

**ES** – Errored Seconds

### **G**

**G.SHDSL** – Single-pair High-speed Digital Subscriber Line

**GUI** – Graphical User Interface

### **H**

**HTTP** – Hypertext Transfer Protocol

**HTTPS** – Hypertext Transfer Protocol Secure

### **L**

**LAN** – Local Area Network

**LED** – Light Emitting Diode

**LLC** – Logical Link Control

### **M**

**MIB** – Management Information Base

**MLT** – Mechanized Loop Testing

**MPPE** – Microsoft Point-to-Point Encryption Protocol

**MUX** – Multiplexer

### **N**

**NEBS** – Network Equipment Building System

**NIC** – Network Interface Card

**NT1** – Network Termination Type-1

### **O**

**OSP** – Outside Plant

**P****POTS** – Plain Old Telephone Service**Q****QoS** – Quality of Service**R****RADIUS** – Remote Authentication Dial-In Service**RAM** – Remote Access Multiplexer**RMA** – Return Material Authorization**RTS** – Request To Send**S****SCB** – Serial Communication Bus**SES** – Severely Errored Seconds**SNMP** – Simple Network Management Protocol**SSID** – Service Set Identifier (Wireless Network Name)**SSL** – Secure Sockets Layer**T****TC-PAM** – Trellis Coded Pulse Amplitude Modulation**TKIP** – Temporary Key Integrity Protocol**TTL** – Time To Live**U****UAS** – Unavailable Seconds**UBR** – Unspecified Bit Rate**V****VC** – Virtual Circuit**VCI** – Virtual Circuit Identifier**VLAN** – Virtual Local Area Network**VPI** – Virtual Path Identifier**W****WAN** – Wide Area Network**WECA** – Wireless Ethernet Compatibility Alliance**WEP** – Wired Equivalent Privacy**WLAN** – Wireless Local Area Network**WPA** – WiFi Protected Access

## PRODUCT SUPPORT

### TECHNICAL SUPPORT

Technical Assistance is available 24 hours a day, 7 days a week by contacting the Customer Service Engineering group at:

Telephone: 800.366.3891

The 800 telephone support line is toll-free in the U.S. and Canada.

Email: [wsd.support@adc.com](mailto:wsd.support@adc.com)

Knowledge Base: [www.adc.com/Knowledge\\_Base/index.jsp](http://www.adc.com/Knowledge_Base/index.jsp)

Web: [www.adc.com](http://www.adc.com)

### LIMITED WARRANTY

Product warranty is determined by your service agreement. Refer to the ADC Warranty/Software Handbook for additional information, or contact your sales representative or Customer Service for details.

### RETURNS

To return equipment to ADC:

1. Locate the number of the purchase order under which the equipment was purchased. To obtain a return authorization number, you need to provide the original purchase order number to ADC's Return Material Authorization (RMA) Department.

If you cannot locate the purchase order, find the equipment serial number and contact ADC's RMA Department.

2. Call or write ADC's RMA Department to ask for an RMA number and any additional instructions. Use the telephone number, fax number or email address listed below:

- Telephone: 800.366.3891

- Email Address: [repair.return@ADC.com](mailto:repair.return@ADC.com)

3. Include the following information, in writing, along with the equipment you are returning:

- Company name and address
- Contact name and telephone number
- Shipping address to which ADC should return the repaired equipment
- Original purchase order number
- Description of the equipment that includes the model and part number of each unit being returned, as well as the number of units that you are returning.
- Reason for the return. For example:
  - The equipment needs an ECO/ECN upgrade.
  - The equipment is defective.



If the equipment is defective, please tell us what you observed just before the equipment malfunctioned. Be as detailed in your description as possible.

If there is any other reason for returning the equipment, please let us know so we can determine how best to help you.

4. Pack the equipment in a shipping carton.
5. Write ADC's address and the RMA Number you received from the RMA Department clearly on the outside of the carton.



All shipments are to be returned prepaid. ADC will not accept any collect shipments.

## FCC CLASS B COMPLIANCE

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- \* Reorient or relocate the receiving antenna.
- \* Increase the separation between the equipment and receiver.
- \* Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- \* Consult the dealer or an experienced radio/TV technician for help.

## MODIFICATIONS

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by ADC voids the user's warranty.

All wiring external to the product(s) should follow the provisions of the current edition of the National Electrical Code.





---

**World Headquarters:**

ADC Telecommunications, Inc.  
PO Box 1101  
Minneapolis, Minnesota USA 55440-1101

**For Technical Assistance:**

800.366.3891



1259075

---