Use this screen to:

- Activate a wireless profile from the pull-down menu, or
- Add, Edit or Delete a user-defined wireless profile.

You can add up to 99 different profiles, which will be stored in alphabetical order. To view a profile, use the Edit button.

See also:

- Using Configuration Profiles

Use this screen to:

- Assign a name to your wireless profile.
- Select the Network Type to identify the type of wireless connection for this profile.
  - Peer-to-Peer Group
  - Access Point I
  - Residential Gateway

Use this screen to identify the Network Name of the wireless network to which you wish to connect your computer.

- When connecting to a Base Station, consult the LAN Administrator of the network for the correct value, or use the Scan button to retrieve a list of open wireless networks.
- When connecting to a Peer-to-Peer Group, consult one of the workgroup participants for the correct value.

Valid value is a case-sensitive string of ASCII printable characters with a maximum of 32 characters. The value **ANY** will allow your computer to connect to the first open Base Station network that it can find.

NOTE

In environments with third-party wireless products, this parameter is also referred to as ESSID.

Use this screen to:

- Enable or disable wireless data Network Name.
- Enter the encryption key that applies in your network.

You can enter key values in either Alphanumeric Value or Hexadecimal Value. The encryption key value is case-sensitive.

Consult your LAN Administrator for the correct value.

NOTE

When setting up a new network the defaults are:

- Disabled for Access Point I devices.
- Enabled for Residential Gateway devices, where the default key matches the last 5 characters of the Network Name printed on a label on the Residential Gateway.

Use this screen to:

- Enable Power Management for low power consumption and wireless performance.
- Disable Power Management for default power consumption and high wireless performance (default).

NOTE

Power Management is only supported in Base Station networks.

Use this screen to control the TCP/IP protocol behavior when switching from one wireless profile to another.

Enable this option when your profiles connect to networks with a different TCP/IP. For example your home network and a corporate network.

As most TCP/IP servers assign an TCP/IP lease for 24 hours, your network connection might not work due to an IP Address mismatch when moving between two different network spaces. Enabling this option will ensure your IP Address will be renewed every time you select this profile.

Use this screen to resolve hardware resource conflicts if the Windows NT operating system does not assign these resources automatically.

- I/O Base Address
- Interrupt Request (IRQ)

In normal situations, the default values 0400 and 10 will work just fine.

To allow easy recognition, you can assign your own names to each profile.

Before you can start using Configuration Profiles, you have to add a Configuration Profile for each wireless network environment that you want to participate in with your (mobile) Wireless Client Station.

If you plan to use your Wireless Client Station in multiple networking environments that require different configuration settings, you can define dedicated profiles for each environment.

For example you can create a Configuration Profile for:

- your office head quarters
- a branch-office
- your home or SOHO network

After creating configuration profiles, you can easily switch your station from one wireless network to another by selecting one of the profiles.

See also:

- Network Type.

To connect a wireless computer to a network, you will need to identify how you wish to establish the connection.

- Peer-to-Peer Group
- To connect to a Base Station Network select the type of Base Station:
  - Access Point I
  - Residential Gateway

This specifies the I/O base address to be used by the adapter.

You can select an address from the range of I/O Base addresses in the pull-down list.

Default value is 0400-0437.

IMPORTANT:

To determine which resource settings are available, run the Windows NT Diagnostics program ***prior to*** installing the Wireless Client Adapter driver. If you did not do so yet, abort the driver installation and run the Windows NT Diagnostics program now.

For more detailed information please consult the documentation that came with your Windows NT System.

This specifies the interrupt number to be used by the adapter.

You can select a IRQ value from the range of Interrupt Requests in the pull-down list.

Default value is 10.

IMPORTANT:

To determine which resource settings are available, run the Windows NT Diagnostics program ***prior to*** installing the Wireless Client Adapter driver. If you did not do so yet, abort the driver installation and run the Windows NT Diagnostics program now.

For more detailed information please consult the documentation that came with your Windows NT System.

If you cannot connect your Wireless Client Station to the network, the first troubleshooting hint is to verify LED activity of the Wireless Client Adapter. The LEDs may show the following behavior:

- Power LED on, Transmit/Receive LED off
- Power LED on, Transmit/Receive LED flickering
- Both LEDs blink once every 10 seconds
- Power LED is Flickering
- No LED Activity

If there is LED activity, run the Client Manager diagnostic tool on your station to:

- Run the **Link Test** to verify the quality of wireless network interface radio communications with the network.
- Run the **Card diagnostics** to investigate and/or resolve version mismatch of the various wireless network interface software components installed on your computer

NOTE

To isolate a potential conflict without unintentionally creating another one, you are advised to change only one value at the time.

This LED status indicates normal operation:

- The Wireless Client Adapter is powered on
- The Transmit/Receive LED indicates there is no activity on the wireless network.

The absence of activity on the Wireless Network Interface might be related to the fact that:

- You moved out of Transmit Rate of the Base Station(s) that could provide access to the selected network.
- There are no Wireless Client Stations in the Transmit Rate of your computer to participate in the selected Peer-to-Peer Group.
- The Base Station(s) that could provide access to the selected network has (have) a problem (e.g. power is off).

This LED status indicates normal operation:

- The Wireless Client Adapter is powered on
- The Transmit/Receive LED indicates activity on the wireless network.

If the radio of your Wireless Client Adapter seems to communicate with other radio devices, but does not succeed in actually connecting to the network (i.e. the power and radio LED shows normal activity), you may need to verify whether your operating system installed the correct Network Protocol Settings.

This LED indicates that the Wireless Client Adapter is powered on and working properly, but it is not able to establish a wireless connection to the wireless network.

Possible causes might be:

- Your wireless station is outside the Transmit Rate of the Base Station(s) that could provide you access to the selected network.
- The Wireless Network Interface of your station has been configured with an incorrect Network Name and/or Encryption Key settings.
- By mistake you selected a configuration profile on your wireless station, that does not belong to the wireless network that you want to connect to.
- The Base Station(s) that could provide access to the selected network has (have) been configured to deny access to stations that use the value **ANY** as their Network Name.

Contact your LAN Administrator for information about the correct values of the parameter settings that apply in your network.

If there is absolutely no LED activity on the Power LED and Receive/Transmit LED of the Wireless Client Adapter, this may be due to one of the following reasons:

- The Wireless Client Adapter device is not properly connected to your computer.
- No driver was installed to allow communication between your computer and the wireless network interface.
- You are using a wireless network interface in combination with an ISA Avaya Wireless Tools, but you did not yet "introduce" the adapter to your computer using the "Add New Hardware" option on the Control Panel.

A flickering Power LED identifies that you enabled the Card Power Management option for the Wireless Client Adapter of a Wireless Client Station (Advanced Settings).

Subject to the type and version of your Windows operating system, the correct protocol may or may not be installed automatically when installing the wireless network interface. Network protocols are for example:

- TCP/IP
- NetBEUI
- IPX/SPX

To verify your network protocol settings:

1. Click **Start**, select **Settings**, then select **Control Panel**.
2. Double-click the **Network** icon to open the Network properties window.
3. Display the list of network components installed protocols for your wireless network interface.
   - When using Windows 95/98, scroll down the list of items in the tab **Configuration**.
   - When using Windows NT, select the tab **Protocols**.
4. Contact your network administrator for information about:
   - Which protocols should be included in the list.
   - What property settings should apply for each of these protocols.
5. (Optional) Click the:
   - **Add** button to add a missing protocol.
   - **Properties** button to view/modify the protocol settings.

Unfortunately, the Windows NT Diagnostics program does not always show a 100% accuracy in displaying which resources were claimed by other hardware. In exceptional cases you may encounter difficulty installing your Wireless Client Adapter despite the fact that you ran the Windows NT Diagnostics.

In this case you might run into a Hardware Conflict even though you selected values for your wireless network interface that, according to the Windows NT Diagnostics, did not seem to be used by another device.

If you are using the wireless network adapter in combination with the ISA Adapter, but did not yet "introduce the ISA adapter" to your computer, open the Control Panel, select the item "Devices" to enable the option "Start PCMCIA device at boot" option.

See also: Another Device does no longer work.

In case another device does no longer work after you installed the Wireless Client Adapter, you may have run into a Hardware Conflict. You can verify whether this is caused by the wireless network interface, simply by removing the interface and rebooting the computer:

- When the problem persists, the problem is not caused by the wireless network interface.
- When the other device functions properly again after removing the wireless network interface, one of the following two causes may apply:
  - The resources were already claimed upon booting the device, by a resource setting in the BIOS or CMOS of your computer, or
  - The driver software of the conflicting device did not notify the Windows NT operating system of its claim upon specific resources.

    This means that if you selected resources that appeared to be available according to the Windows NT Diagnostics program, these settings were already claimed by the conflicting device.

In both cases you are encouraged to try alternative values for your wireless network interface to see whether these new values might help solving your problem. Upon doing so, you are advised to change only one parameter at a time.

A conflict of the NT Adapter Settings of your Wireless Client Adapter with another device in your computer.

If you encounter difficulty in connecting your computer using the Wireless Client Adapter in a Windows NT environment, the cause is often related to hardware device settings, which prevent the driver from loading properly. In such situations you are advised to explore the following hints, prior to contacting Technical Support.

- Verify the settings of the BIOS that is loaded when you (re)start your computer.
- Try alternative I/O Base Address values for your wireless network interface. An I/O Base address conflict is most often perceived as no LED activity on the wireless network interface. In some cases an I/O Base conflict might result in hanging the system with a "blue-screen" error.
- Try alternative Interrupt Request (IRQ) values for your wireless network interface. An IRQ conflict is most often perceived as little LED activity: Power LED on, Receive/Transmit LED off. When running the Client Manager diagnostic tool, it will display that the radio communications are good, but the Base Station is not displayed with its proper name and is identified by its MAC Address only. When you would select the Link Test diagnostics, you will see that all dynamic indicators are blank.

In most cases selecting either a different I/O Base Address or IRQ value will help you resolve the issue.

This program that is included with the Windows NT operating system, is a tool that enables you to determine which system resources are used hardware installed into your computer.

Running this program will help you to find out whether the factory-set defaults of your wireless network interface have already been claimed by other hardware devices. If so, this program will also help you to determine which alternative values supported by your wireless network interface are available.

To minimize the risk of hardware conflicts, you are advised always to run this program always *prior* to installing new hardware.

Consult the Windows documentation for more information about Windows NT Diagnostics.

The following operating systems support 'Plug and Play' for the wireless network interface:

- Microsoft Windows 95
- Microsoft Windows 95 OSR2
- Microsoft Windows 98 & 98 Second Edition (SE)
- Microsoft Windows Millennium Edition (ME)
- Microsoft Windows 2000

The following operating systems do not support 'Plug and Play' for the wireless network interface:

- Microsoft Windows NT v3.51
- Microsoft Windows NT workstation v4.0
- Microsoft Windows for Workgroups (v3.x)

These operating systems are not able to dynamically allocate system resources such as I/O Base addresses and/or Interrupt Request (IRQ) values to your new hardware.

This means that prior to installing new hardware on such systems, you will need to determine which system resources have been claimed by other devices prior to selecting the resource settings for your wireless network interface. Failing to do so might lead to an I/O Base address conflict and/or IRQ conflict which might prevent your card or the other device from operating properly.

To determine which resource settings are available:

- Run the Windows NT Diagnostics program ***prior to*** installing the wireless network interface driver.
- Verify the contents of your computer's BIOS or CMOS.

Operating Systems that support 'Plug & Play' will be able to allocate the correct values automatically. On such systems, you will not see the tab "Adapter".

On computers running these operating systems, you must identify the following parameters to allow your computer to work properly with the various devices and adapter cards installed:

- I/O Base Address
- Interrupt Request (IRQ)

Confirm the factory-set defaults or to select an alternative value using the pull-down boxes.

This specifies the I/O base address to be used by the adapter.

You can select an address from the range of I/O Base addresses in the pull-down list.

Default value is 0400-0437.

IMPORTANT:
To determine which resource settings are available, run the Windows NT Diagnostics program ***prior to*** installing the Wireless Client Adapter driver. If you did not do so yet, abort the driver installation and run the Windows NT Diagnostics program now.

For more detailed information please consult the documentation that came with your Windows NT System.

This specifies the interrupt number to be used by the adapter.

You can select a IRQ value from the range of Interrupt Requests in the pull-down list.

Default value is 10.

IMPORTANT:
To determine which resource settings are available, run the Windows NT Diagnostics program ***prior to*** installing the Wireless Client Adapter driver. If you did not do so yet, abort the driver installation and run the Windows NT Diagnostics program now.

For more detailed information please consult the documentation that came with your Windows NT System.

Unfortunately, the Windows NT Diagnostics program does not always show a 100% accuracy in displaying which resources were claimed by other hardware. In exceptional cases you may encounter difficulty installing your Wireless Client Adapter despite the fact that you ran the Windows NT Diagnostics.

In this case you might run into a Hardware Conflict even though you selected values for your wireless network interface that, according to the Windows NT Diagnostics, did not seem to be used by another device. When this is the case you may notice one of the following events:

- You are perhaps using a wireless network interface card in combination with an ISA Adapter, but you did not yet "introduce the ISA adapter" to your computer using the "Devices" option on the Control Panel to enable the "Start PCMCIA device at boot" option.
- Another Device does no longer work after the installation of your wireless network interface.

In case another device does no longer work after you installed the Wireless Client Adapter, you may have run into a Hardware Conflict. You can verify whether this is caused by the wireless network interface, simply by removing the interface and rebooting the computer:

- When the problem persists, the problem is not caused by the wireless network interface.
- When the other device functions properly again after removing the wireless network interface, one of the following two causes may apply:
  - The resources were already claimed upon booting the device, by a resource setting in the BIOS or CMOS of your computer, or
  - The driver software of the conflicting device did not notify the Windows NT operating system of its claim upon specific resources.

    This means that if you selected resources that appeared to be available according to the Windows NT Diagnostics program, these settings were already claimed by the conflicting device.

In both cases you are encouraged to try alternative values for your wireless network interface to see whether these new values might help solving your problem. Upon doing so, you are advised to change only one parameter at a time.

A conflict of the Adapter Settings of your Wireless Client Adapter with another device in your computer.

If you encounter difficulty in connecting your computer using the Wireless Client Adapter in a Windows NT environment, the cause is often related to hardware device settings, which prevent the driver from loading properly. In such situations you are advised to explore the following hints, prior to contacting Technical Support.

- Verify the settings of the BIOS that is loaded when you (re)start your computer.
- Try alternative I/O Base Address values for your wireless network interface. An I/O Base address conflict is most often perceived as no LED activity on the wireless network interface. In some cases an I/O Base conflict might result in hanging the system with a "blue-screen" error.
- Try alternative Interrupt Request (IRQ) values for your wireless network interface. An IRQ conflict is most often perceived as little LED activity: Power LED on, Receive/Transmit LED off. When running the Client Manager diagnostic tool, it will display that the radio communications are good, but the Base Station is not displayed with its proper name and is identified by its MAC Address only. When you would select the Link Test diagnostics, you will see that all dynamic indicators are blank.

In most cases selecting either a different I/O Base Address or IRQ value will help you resolve the issue.

This program that is included with the Windows NT operating system, is a tool that enables you to determine which system resources are used hardware installed into your computer.

Running this program will help you to find out whether the factory-set defaults of your wireless network interface have already been claimed by other hardware devices. If so, this program will also help you to determine which alternative values supported by your wireless network interface are available.

To minimize the risk of hardware conflicts, you are advised always to run this program always *prior* to installing new hardware.

Consult the Windows documentation for more information about Windows NT Diagnostics.

The following operating systems support 'Plug and Play' for the wireless network interface:

- Microsoft Windows 95
- Microsoft Windows 95 OSR2
- Microsoft Windows 98 & 98 Second Edition (SE)
- Microsoft Windows Millenium Edition (ME)
- Microsoft Windows 2000

The following operating systems do not support 'Plug and Play' for the wireless network interface:

- Microsoft Windows NT v3.51
- Microsoft Windows NT workstation v4.0
- Microsoft Windows for Workgroups (v3.x)

These operating systems are not able to dynamically allocate system resources such as I/O Base addresses and/or Interrupt Request (IRQ) values to your new hardware.

This means that prior to installing new hardware on such systems, you will need to determine which system resources have been claimed by other devices prior to selecting the resource settings for your wireless network interface. Failing to do so might lead to an I/O Base address conflict and/or IRQ conflict which might prevent your card or the other device from operating properly.

To determine which resource settings are available:

- Run the Windows NT Diagnostics program ***prior to*** installing the wireless network interface driver.
- Verify the contents of your computer's BIOS or CMOS.

The Network Name is a value that logically connects devices within your wireless network. This value (also referred to as SSID) is used to distinguish your wireless network from neighboring networks.

To allow communication, each wireless device within your network must use the same Network Name.

Valid values:

- Alphanumeric string of 1 to 32 case-sensitive ASCII printable characters
- Range of "a" to "z", "A" to "Z", "0" to "9"

- AP-I **WaveLAN Network**
- AP-II
- Residential Gateway Printed on a label on the device

Default Values

When connecting to a Base Station:

- Consult the LAN Administrator for the correct value, or
- When using the AP Manager, press the **Scan** button to retrieve a list of open wireless networks.

When connecting to a Peer-to-Peer Group:

- Consult one of the workgroup participants for the correct value.

Default value	**No default value**
Valid values for **64-bit** RC4 encryption	• 5-digit case-sensitive Alphanumeric Value.: **SECU1** • 10-digit Hexadecimal Value in the range of "a-f", "A-F" and "0-9".: **ABCD1234FE**
Valid values for **128-bit** RC4 encryption.	• 13-digit case-sensitive Alphanumeric Value.: **SECURITY12345** • 26-digit Hexadecimal Value in the range of "a-f", "A-F" and "0-9".: **ABCDEF1234567890FEDCBA4321**

Use the AP Manager whenever your Base Station allows you to configure 128-bit RC4 encryption.

See also Translating Hex & ASCII values.

Default Encryption Settings	**Base Station**
• Enabled	Residential Gateway Default key matches the last 5 characters of the Network Name printed on a label on the device
• Disabled	Access Point I Access Point II Access Point 3

The frequency channel parameter gives you the ability to select a sub-channel of the 2.4 GHz channel set. You can use this option to configure your Base Station for one of the following reasons:

- To to solve a situation where the default channel suffers from interference by an in-band interfering device (e.g. microwave ovens).
- To configure your network infrastructure to support a Multiple Channel Configuration.

Wireless Client Station devices that roam between different Base Station devices, will automatically adapt the operating frequency of their radio when required.

To extend the battery life of your (mobile) Wireless Client Station, you can use Power Management to adjust the power consumption behavior of the Wireless Client Adapter.

Subject to the type of network traffic power management may have some impact on network performance.

See also:

Power Management Enabled

To minimize power consumption, the station will go to "sleep mode" whenever activity is low. At regular intervals it will wake up to verify whether there is network traffic addressed to the wireless station. `

Power management only works in combination with Base Station products which can buffer messages for wireless computers in "sleep mode".

- Open Configuration
- Closed Configuration.

The Avaya Wireless product family is a comprehensive set of wireless network equipment based on radio technology. You can use Avaya Wireless to build a variety of wireless network topologies using client adapters and Base Stations.

The Avaya Wireless products have been designed for inter operability. This means that your Avaya Wireless hardware will communicate with other vendors' products carrying the WiFi logo.

See also:

- Wireless Client Station
- Base Station
- Wireless Configurations
- Avaya Wireless Tools

A wireless client station is a computing device equipped with a Wireless Client Adapter that can connect to a (wired) network infrastructure via a Base Station.

Alternatively, you can connect wireless clients to one another in a Peer-to-Peer Group to share files and printers.

Avaya Wireless Client Adapters are wireless network adapters that are not much different from Ethernet adapters for wired LANs. The operating system will not even notice the difference. The wireless adapters support all protocols that are supported by Ethernet adapter cards.

Like wired adapters, wireless adapters require installation of a dedicated driver, but unlike wired adapters they do not need a cable to connect them to the network. Only wireless network interfaces allow you to relocate workstations without the need to change network cabling or connections to patch panels or hubs.

Avaya Wireless offers the following types of adapters:

- Avaya Wireless PC Card
- PCI Adapter
- USB Client

The Avaya Wireless PC Card is a Wireless Client Adapter that can be used with (mobile) computers that support the PC Card Type II slot. It has two LED indicators and two integrated antennas.

The USB Client is a Wireless Client Adapter that can be connected to computers with a USB port.
The USB Client has two LED indicators and two integrated antennas

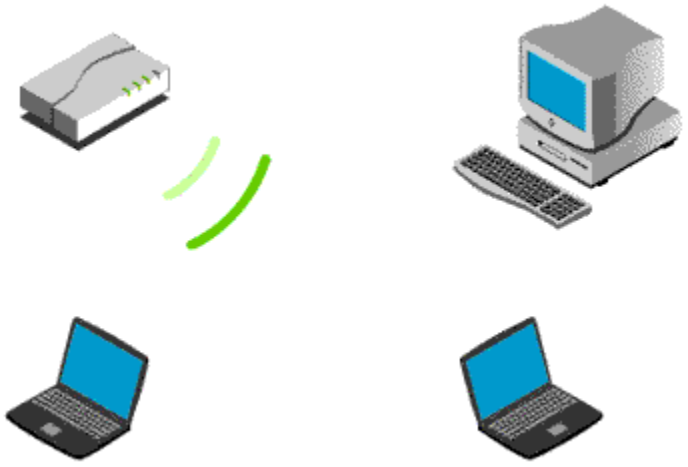
The Base Station is a transparent bridge device that you can use to connect a Wireless Client Station to a (wired) network.

Avaya Wireless offers the following types of Base Station devices, that allow for a a variety of Wireless Configurations:

- Access Point I
- Access Point II
- Access Point 3
- Residential Gateway

The Access Point I is a transparent bridge device equipped with:

- A 10Base-T Ethernet Interface to connect the unit to a wired network.
- An integrated 128-Bit RC4 Network Interface to connect wireless stations. The wireless interface allows you to specify up to 4 different encryption keys.



Optionally you can use the AP-I in combination with the Range Extender Antenna.

The Access Point II is a transparent bridge device equipped with:

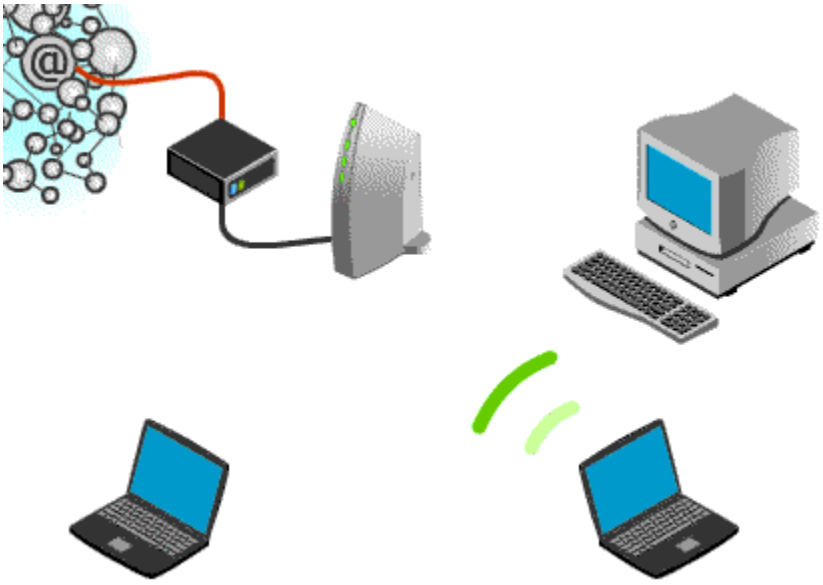
- A 10/100 Base-T Ethernet Interface to connect the unit to a wired network.
- Two wireless network interfaces via PC Card Type II slots

Optionally you can use the AP-II in combination with the Range Extender Antenna.

The Access Point 3 is a transparent bridge that supports:

- A 10/100 Base-T Ethernet Interface
- Two wireless network interfaces via PC Card Type II slots
- A Serial Port for configuration via a direct cable connection.
- Management via a web-browser and/or Command Line Interface.

The Residential Gateway is a Base Station that enables you to build various types of wireless network applications in your home or small office environment.

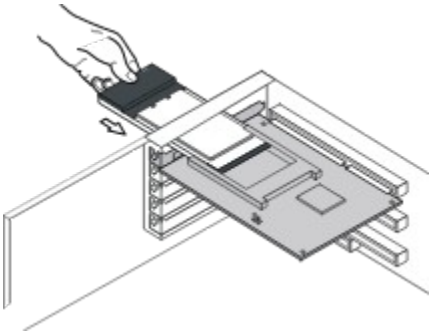


It enables you to share internet access via an external Cable or xDSL Modem, via an ISDN Router or the Ethernet port.

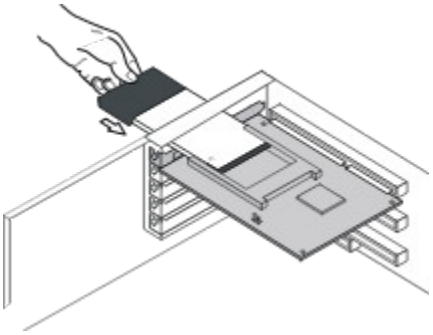
RG-I units also allow to share internet access via the built-in v90 modem.

- ISA Adapter
- PCI Adapter
- Range Extender Antenna

To use the Avaya Wireless PC Card in a (desktop) computer that does not have a PC Card slot Avaya provides the ISA Adapter.



To use the Avaya Wireless PC Card in a (desktop) computer that does not have a PC Card slot Avaya provides the PCI Adapter and the ISA Adapter.

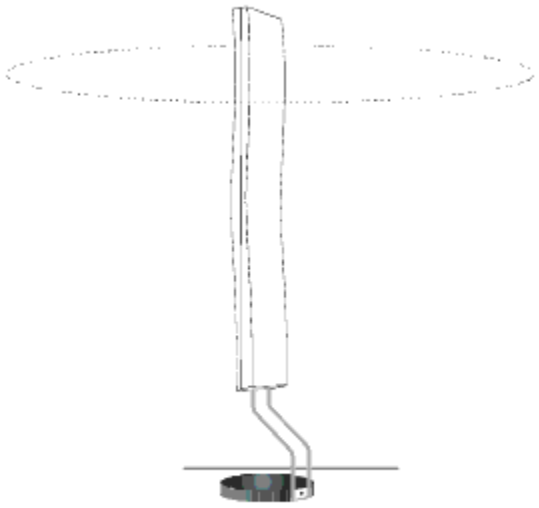


You can use the Range Extender Antenna to extend the Transmit Rate of your Avaya Wireless PC Card with approximately 15%.

Use of the Range Extender Antenna is recommended in situations where the integrated antenna of your PC Card is shielded. For example:

- Objects, such as thick stacks of books (or other objects) shield the integrated antenna.
- Your computer is installed in a cabinet or underneath a table.

Use of the Range Extender Antenna is especially recommended for the Avaya Wireless PC Card that is installed into a desktop computer, or in a Base Station.



The Avaya Wireless software suite consists of a set of Windows based management tools that enables you to configure your Base Station devices, and diagnose wireless network performance.

The Avaya Wireless software suite consists of the following tools:

- Client Manager
- Base Station Management Tool

To view and modify the configuration of your Base Station, or monitor its performance, you can use one or more of the following tools:

Management Tool	**Base Station Type**
Residential Gateway Setup Utility	Residential Gateway (easy install)
AP Manager	AP-I, AP-II, Residential Gateway (expert install)
Web-Browser Management	AP-3
Commnand Line Interface	AP-II, AP-3

To monitor the wireless performance of your Wireless Client Station, the Client Manager provides:

- Card Diagnostics to investigate the operation of the Wireless Client Adapter hardware.
- Link Test to measure wireless communication with a single Link Test partner in a Peer-to-Peer Group or a single Base Station.
- Site Monitor to verify and optimize placement of your Base Station devices.

You can install the program on any Windows computer equipped with one Avaya Wireless adapter.

The AP Manager program is a tool for LAN administrators or system supervisors to configure and monitor the performance of:

- AP-I
- AP-II
- Residential Gateway

You can install the program on any wired or wireless computer in your network that:

- runs the Microsoft windows operating system
- has the TCP/IP protocol installed.

The Residential Gateway Setup Utility is a software tool for setting up Residential Gateway Network Scenarios.

Subject to the size and requirements, a wireless network can be identified by either one of the following configuration types:

- Stand Alone Network
- Wireless Access to Ethernet Networks
- Multiple Base Station Network
- Multiple Channel Configuration

A Base Station network is a wireless network where all wireless computers connect to one another or a larger network infrastructure via a dedicated Base Station.

Base Station Networks allow for larger wireless coverage, and more flexibility in network design, as they can bridge data between:

- wireless stations, and
- wireless and wired infrastructures.

Base Stations exist in different versions, allowing for a variety of network connections:

Stand Alone Network

Wireless Access to Ethernet Networks

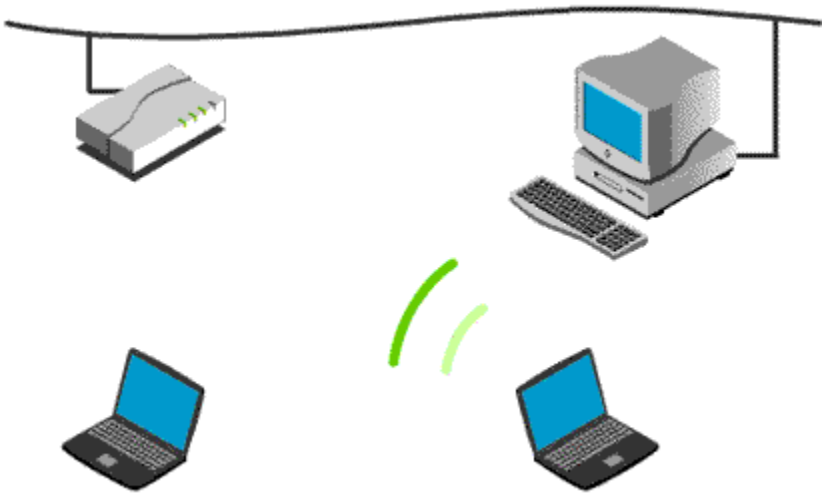
Multiple Base Station Network

A stand-alone configuration is the quickest and easiest way to set up a small wireless network. In this configuration only one Base Station is used, functioning as a relay that will forward the data communication from one Wireless Client Station to another within the same wireless cell. A server is not required, wireless stations can communicate like in a Peer-to-Peer Group, but in this configuration via a Base Station.

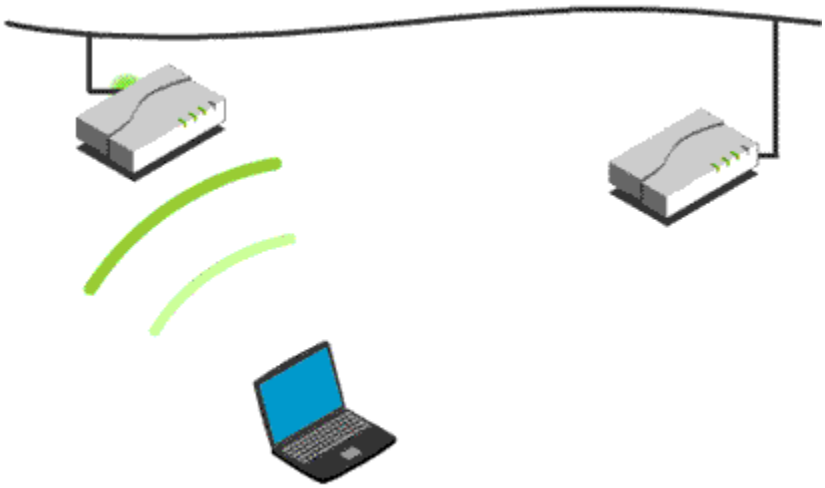
The wireless infrastructure is identified by a unique Network Name. All equipped devices that wish to connect to this network, must be configured with an identical Network Name.

Mobile wireless stations will maintain communication with the infrastructure as long as they remain within the Transmit Rate of the Base Station in their network.

Connecting the Base Station to an Ethernet network, allows you to connect a number of Wireless Client Station devices (mobile and/or desktop) to an existing Ethernet infrastructure, creating a larger coverage area.



To extend the total wireless coverage area, you can setup a wireless network with multiple Base Station devices. To create multiple cell networks, the Base Station devices must be connected via a wired backbone.



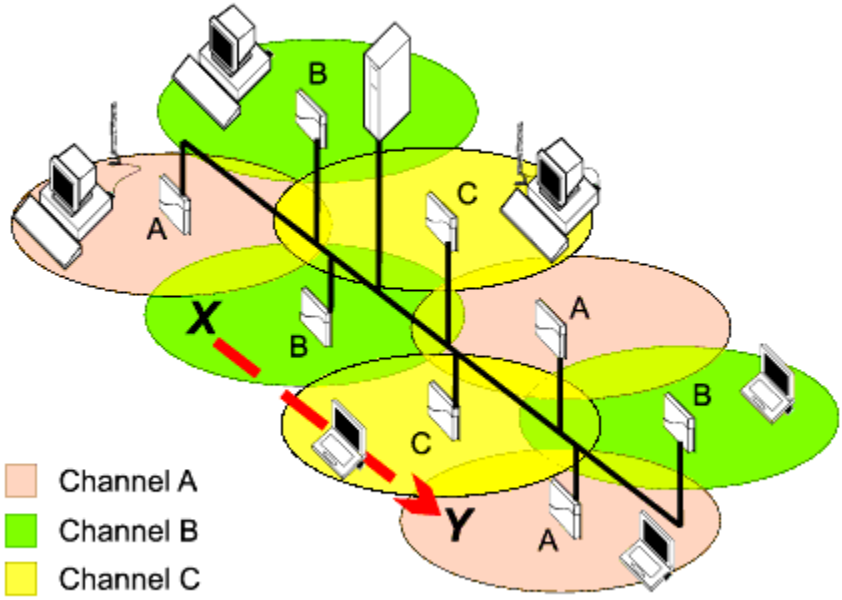
The Base Station devices can serve mobile Wireless Client Stations SOHO between various locations within a network premises. Roaming wireless stations in a multiple Base Station configuration will:

- automatically switch between Base Station devices, when required, thus maintaining the wireless connection to the network.
- communicate with the infrastructure as long as they remain within the Transmit Rate of the Base Station devices in their network.

Neighboring Base Station devices alternate between three or more sub-channels (depends on local radio regulations).

Any Wireless Client Station roaming in a Multiple Base Station Network will automatically change the operating radio frequency when required.

Figuur: Multiple Channel Configuration



A Peer-to-Peer group is a group of Wireless Client Station communicate directly to one another, without intervention of a Base Station or network infrastructure.

Peer-to-Peer networks are typically small networks where:

- Wireless computers use for example Microsoft file and printer sharing to exchange data directly.
- Co-workers can quickly set up an ad-hoc workgroup while on the road or in a temporary workplace.

See also: Base Station Network

Transparent bridge device to connect Wireless Client Adapter units to a (wired) network.

See also:

- Access Point I
- Access Point II

Authorized stations are identified by the MAC Address of the Wireless Client Adapter in a so called Access Control Table file that is loaded into the Base Stations as part of the configuration.

With this security feature enabled, the Base Station ignores all requests to forward data to/from the wireless devices that are not identified in the Access Control Table. You can create or edit the Access Control Table files with:

- Base Station Management Tool
- Client Manager

Typically a task for the LAN Administrator, and part of the configuration upload.

The Access Control Table can be used as a security mechanism to restrict access to the wireless network with a list containing the unique MAC Address of the network interface:

- On each individual Base Station in your network, or
- On a central database, stored in a dedicated RADIUS Server or third party server.

Asymmetric **D**igital **S**ubscriber **L**ine

Technology for broadband computer communication via standard telephone lines. Unlike regular dialup phone service, ADSL provides continuously-available, "always on" connection. ADSL is asymmetric because it uses most of the channel to transmit downstream to the user and only a small part to receive information from the user. ADSL simultaneously accommodates analog (voice) information on the same line.

An alphanumeric value is a value that can include both:

- Numeric values in the range of '0-9' and
- Alphabetical characters in the range of 'a-z'.

For example: AP2on2ndfloor.

Usually alphanumeric values are applied to specify a name or password, where the use of both alphabetical and numerical characters expands the flexibility to enter a name or value of your choice.

When used for passwords, alphanumerical characters expand the number of possible code-combinations for each single character.

For example:

- Numerical values would allow you to select from 10 different values per character only, in the range of '0-9'.
- Alphabetical values would allow you to select from 26 different values per character only, in the range of 'a-z'. or maximum 52 when the characters would be case-sensitive: 'a-z', and 'A-Z'.
- Alphanumerical characters enable you to select from 36 different values per character, in the range of '0-9' and 'a-z'. When the field value would be case-sensitive, the number of values per character would be 62:

  Per character you could select from a value in the range of '0-9', 'a-z', and 'A-Z'.

See also: Translating Hex & ASCII values

Association refers to the process where a Wireless Client Station establishes a connection to a Base Station that provides access to IEEE 802.11 infrastructures. This connection applies to the "physical" networking layer only: i.e., it involves nothing more than for example pulling a cable between a wired computer and the wiring closet.

To access networking data, the end-user would still need a login name and login password as implemented by most of today's network operating systems.

Control interaction role where an entity enforces authentication before allowing user access(Supplicant).

Control interaction role where an entity requests access to the services that can be accessed through the Authenticator.

A basic access network consists of a small sized wireless LAN, with no connections via gateways or routers. The number of Base Stations in this network typically varies between 1 and 5. The administrator stations need to have the TCP/IP protocol stack loaded and use IP addressing to configure and monitor the Base Stations. IP addressing and the TCP/IP protocol are not strictly necessary for client stations.

Beacon messages are management frames transmitted by a Base Station at regular intervals. The purpose of Beacon messages is to support Roaming wireless devices.

A beacon message contains information that:

- Identifies the wireless network, and
- Informs the wireless computing device about the quality of its radio connection with the various Base Station devices throughout the wireless network.

Wireless devices that roam between different physical locations, will use the Beacon information to determine if and when they should (try to) connect to another Base Station. This will avoid that wireless devices moving away from the Base Station might lose their network connection.

To receive and interpret a Beacon message, the Wireless Client Station must be configured with identical identification parameters as the Base Station interface that transmitted the Beacon message. Wireless devices equipped with the PC Card must be configured with an identical Network Name.

Base Station devices transmit Beacon Messages at an interval of approximately 10 beacons/second.

Basic I/O System (sometimes also referred to as CMOS)

This system is loaded first each time you (re)start your computer. It usually contains basic information about devices and ports installed into your computer. Examples of such settings are:

- System clock, which determines the date and time settings on your computer
- Type and number of Hard Disk Drives
- Type and device settings of Parallel and Serial ports
- Type and device settings of "on-board" audio cards and/or Ethernet interfaces

The number of settings defined in the BIOS and/or the ability to view or modify these settings may differ from one computer to another.

To access the BIOS or CMOS you typically need to press a specific key when (re)starting your computer. For most computer systems this is either the F1 function key, or the "Delete" key, other systems may use a custom key. Consult the user documentation that came with your computer for more information about accessing the BIOS, and instructions for viewing/modifying settings for your computer.

Unshielded Twisted Pair Cable

Standard cable for wired Ethernet networks, equipped with RJ-45 connectors. This cable is also referred to as 10Base-T or 100Base-T cable.

This cable is typically used to connect a computer or Base Station to:

- A LAN hub or Switch in a corporate or SOHO network with wired infrastructure.
- An external device such as a Cable Modem, xDSL modem or ISDN Router to allow computers in a SOHO network to access the internet via an ISP.

Unshielded Twisted Pair Cable

Special cable for wired Ethernet networks, equipped with RJ-45 connectors. This cable is also referred to as 10Base-T or 100Base-T cable.

This cable is typically used to connect a Base Station directly to a computer.

Avaya Wireless proprietary mode where the Base Station denies access to:

- any Wireless Client Station with the incorrect Network Name
- any Wireless Client Station with the Network Name set to **ANY**

This mode is not compliant with the IEEE 802.11 Standard.

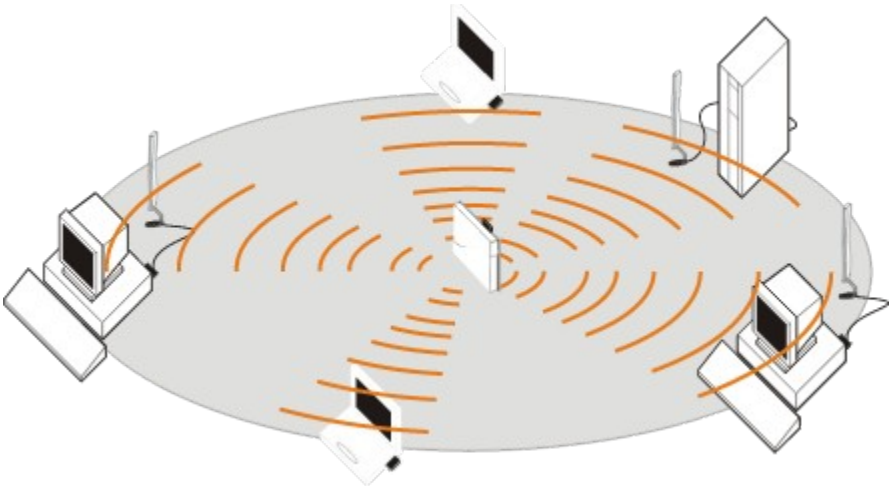
Carrier **S**ense **M**ultiple **A**ccess with **C**ollision **A**voidance.

Pro-active mechanism used by wireless network devices to avoid collisions of wireless transmissions. The CSMA/CA mechanism is based on sensing whether the medium is free prior to starting transmissions. If the medium is not free, the wireless device will defer its transmission using a random time-out counter until the medium becomes available again.

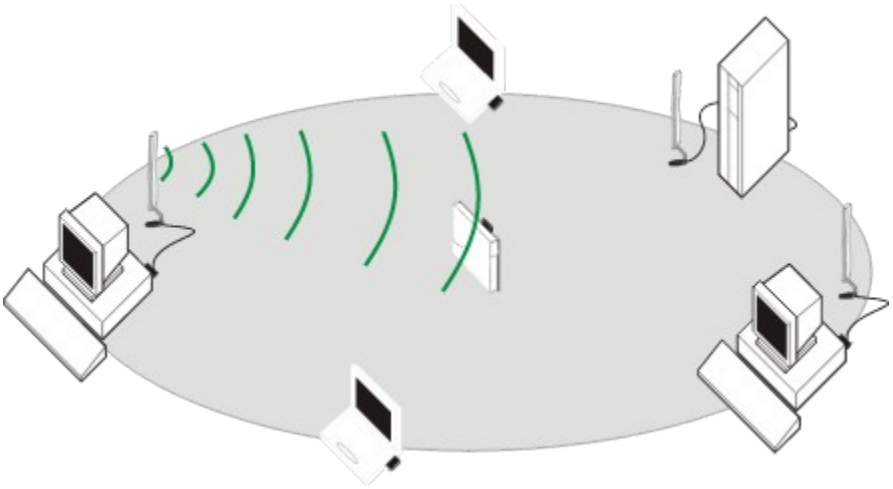
Carrier **S**ense **M**ultiple **A**ccess **C**ontrol, **C**ollision **D**etect.

Reactive mechanism used by wired network devices to detect collisions of transmitted frames. The CSMA/CD mechanism is based on starting transmissions without sensing whether the medium is free, and only detect frames that failed as a result of a collision.

Clear To Send.



Request To Send.



Basic operating software for the Avaya Wireless hardware that determines basic functionality and features. This software is already loaded into the hardware at the factory, so does not require user installation.

When new features or functions become available for your hardware, these will be released as updates on the website at http://www.avaya.com/.

Subject to the type of hardware, the embedded software may also referred to as:

- Firmware for wireless your wireless Client Station.
- Kernel for your Base Station.

Alphanumeric Value or Hexadecimal Value used to validate the access to the network.

Given that each wireless device on the network must be configured with the same security settings, encryption keys provide a basic mechanism to prevent any unauthorized access to the network.

Extended Service Set.

Definition in the IEEE 802.11 Standard for wireless LANs to identify a wireless network consisting of Base Stations and Clients.

European Telecommunications Standards Institute (Europe).

Federal Communications Commission (USA).

Industry Canada.

The Frame Check Sequence is a cyclic redundancy check (CRC), calculated on all fields from the Destination Address on.

It is used to detect corrupted packets on the network.

Embedded software of the Avaya Wireless PC Card and PCI Adapter.

This basic operating software for wireless devices hardware is factory-installed. You will only need to update this software when new functions or features have been developed for your hardware.

Embedded software of the Base Station.

This software is a binary file of the format "XXXXyyy.bin", where XX identifies the type of Base Station, and yyy identifies the version of the software.

- wpntxxxx.bin for AP-II
- ap05xxxxx.bin for AP-I
- rg10xxxxxx.bin for Residential Gateway

Security system designed to prevent unauthorized access to a private or local network.
It can either be a hardware firewall or a software firewall, or a combination of both.

When transmitting data via the wireless network, your Wireless Network Interface will automatically split up the file or message in a number of different packets, that are re-assembled again by the communication partner.

Avaya Wireless Products use standard IEEE 802.11 compatible frame lengths, where different lengths apply for each Transmit Rate. Fragmentation will apply alternative (usually shorter) frame lengths to split and reassemble the wireless data frames.

Numeric value that can include both numeric and a limited number of alphabetical characters:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Where 0 identifies the lowest value, and F the highest value of the hexadecimal range.

In most occurrences where hexadecimal values apply, you will be able to distinguish the hexadecimal values from standard numerical values.

For example:

- 3F2C will identify a four-digit hexadecimal value
- 1234 will most probably identify a four-digit numerical value.

Usually hexadecimal values are identified by a leading 0x, or trailing 'h', to allow you to distinguish a hexadecimal value from a numerical value. For example:

- 1234 'h or 0x1234 will identify a four-digit hexadecimal value, where.
- 1234 will identify a four-digit numerical value.

In case of doubt, consult the user documentation or online help of your product, to find out which type of value applies in a specific situation.

See also: Translating Hex & ASCII values

When your network includes computers equipped with wireless adapters from different manufacturers, you may encounter difficulty entering the encryption keys because one system might require you to enter a Hexadecimal Value where the other system prompts you to specify an Alphanumeric Value.

You can use the table below to translate such values to a valid equivalent for the other system.

NOTE

Encryption Key strings are case-sensitive!

Example: If your Encryption Key reads: "Key2Z" the hexadecimal equivalent would be: "4B657932A"

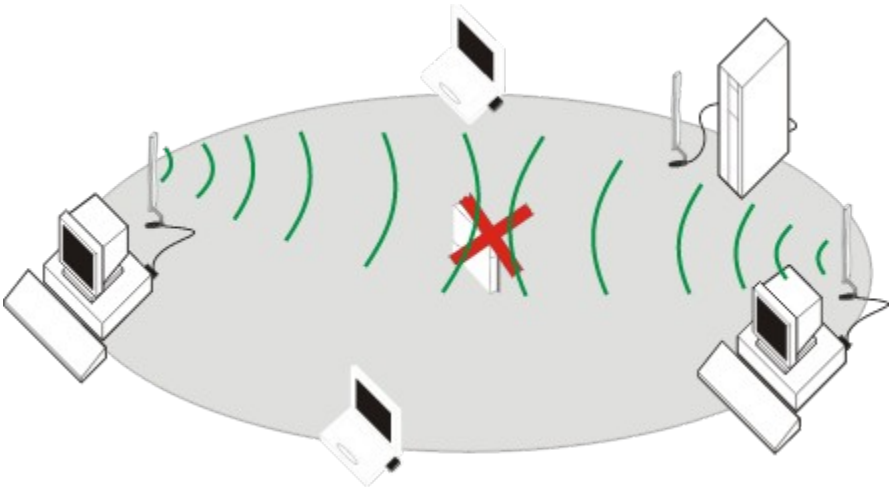
Alphanumeric	Hex	Alphanumeric	Hex
A	41	a	61
B	42	b	62
C	43	c	63
D	44	d	64
E	45	e	65
F	46	f	66
G	47	g	67
H	48	h	68
I	49	i	69
J	4A	j	6A
K	4B	k	6B
L	4C	l	6C
M	4D	m	6D
N	4E	n	6E
O	4F	o	6F
P	50	p	70
Q	51	q	71
R	52	r	72
S	53	s	73
T	54	t	74
U	55	u	75
V	56	v	76
W	57	w	77
X	58	x	78
Y	59	y	79
Z	A	z	7A
Spacebar	20	0	30
!	21	1	31
"	22	2	32
#	23	3	33
$	24	4	34
%	25	5	35
&	26	6	36
'	27	7	37
(	28	8	38
)	29	9	39
*	2A	:	3A
+	2B	;	3B
,	2C	<	3C
-	2D	=	3D
.	2E	>	3E
/	2F	?	3F
[	5B	@	40
	5C		
]	5D		
^	5E		
_	5F		
`	60		
	7B		
|	7C		

	7D
~	7E
Del.	7F

A hidden station is a situation in which two Client Stations are within range of the same Base Station, but are not within range of each other.

The Hidden Station Problem illustrates an example of the "hidden station" problem. Both station A and station B are within range of the Base Station however, station B cannot "hear" station A, therefore station A is a "hidden station" for station B.

Figuur: The Hidden Station Problem



When station B starts to communicate with the Base Station, it might not notice that station A is already using the wireless medium. When station A and station B send messages at the same time, they might collide when arriving simultaneously at the Base Station. The collision will most certainly result in a loss of messages for both stations.

A situation in a wireless network, where communication fails despite the CSMA/CA mechanism. This problem may typically occur in networks where Base Station devices are located at large distances from one another, and/or multiple wireless stations are located at the periphery of a wireless cell.

In such situations wireless stations are not able to adequately sense whether the medium is free, and might start transmissions simultaneously, resulting in a frame collision.

Institute of Electrical & Electronics Engineers, Inc.

The IEEE is an organization that develops Standards for electrical and electronic equipment. IEEE Standards documents are developed within the Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board.

For more information, contact IEEE Customer Service at:

E-mail/Internet:	Customer.service@ieee.org
	http://standards.ieee.org
Phone:	1.732.981.0060 (outside of the US and Canada)
Fax:	1.800.701.IEEE (within the US and Canada)
	1.732.981-9667
Mail:	IEEE Customer Service
	445 Hoes Lane, PO Box 1331
	Piscataway, NJ 08855-1331 USA

IEEE 802.xx Standards define the access technologies for local and metropolitan area networks. IEEE Standards are developed and defined by the IEEE.

The IEEE 802.11 Standard is an interoperability standard for wireless LAN devices, that identifies three major distribution systems for wireless data communication:

- Direct Sequence Spread Spectrum (DSSS) Radio Technology
- Frequency Hopping Spread Spectrum (FHSS) Radio Technology
- Infrared Technology

IEEE 802.11 compliant networking products that are based on the same type of distribution system are interoperable with one another, regardless of the device's manufacturer.

Draft standard for port-based network access control, which provides authenticated network access for IEEE 802.11 wireless networks and to wired Ethernet networks.

- IEEE 802.1x Authentication

Authentication and Dynamic key distribution prior to LAN access.

- Zero-Configuration IEEE 802.11

Media sense wireless aware in the Wireless Client Adapter detects changes for IEEE 802.11 LANs and triggers updates in clients, applications, and network. This means that the operating system manages Driver installation and Client Station configuration.

Requirements:

- IEEE 802.1x compliant TCP/IP
- Disabled Closed Configuration.

Extensible Authentication Protocol.

IP Security, developed for per packet integrity and encryption.

The Base Station that you selected to initiate the AP Manager Remote Link Test.

A networking protocol that is commonly used in networking environments that use the Novell Netware network operating system.

Internet Protocol version 6, which uses a 128-bit addressing scheme to support system identification on the public network.

Internet Service Provider

Company or organization that provides you access to the Internet via one of the following means:

- v90 telephone line
- ISDN telephone line
- xDSL Modem line.
- TV Cable network via Cable Modem

As a computer user you can not connect directly to the internet. The ISP acts as an intermediary between you and the internet.

Local Area Network

The LAN Administrator Station is the computer used for managing your Local Area Network

A logical area within a network that is connected with other areas via a bridge.
For Base Station devices these areas can either be an Ethernet or wireless segment.

Light Emitting Diode

Indicator light on that you can find on most Avaya Wireless devices.

LED lights up at regular intervals.

LED lights up quickly at irregular intervals.

Medium Access Control.
See also: MAC Address.

12-digit hexadecimal identification number for networking products.

Every networking device is identified by a unique factory-set number that can not be changed, also referred to as the 'Universal MAC Address'.

- The MAC Address of a Wireless Client Station is printed on a label on the backside of the hardware.
- Base Station type devices may have more than one MAC Address:
  - One MAC Address for the wired Ethernet interface of the device, printed on a label on the Base Station, and
  - A MAC Address for the Wireless Network Interface of the Base Station.
  - The wireless MAC Address corresponds with the value printed on a label on the backside of the card inside the Base Station.

Management Information Base.

A database of objects that can be monitored by network management systems. Both SNMP and remote monitoring tools (RMON) use standardized MIB formats to monitor any device defined by a MIB.

Ministry of Post and Telecommunication (Japan)

MAC Protocol Data Unit

MAC Service Data Unit

Messages transmitted by a single station (typically a server) to a select group of recipients on the network. This type of traffic is also referred to as Non-Unicast messages.

A Microsoft proprietary protocol that is often used in small networking environments. It allows end-users to share resources on their computers by providing 'peer-to-peer' access. This protocol is required to use 'disk-sharing' or allow other users to print files on a printer connected directly to your computer.

Typical radio environment where antennas can "see" each other, i.e. there are no physical obstructions between them.

Standard IEEE 802.11 mode where the Base Station bridges data for:

- every Client Station with the correct Network Name
- every Client Station with the Network Name set to **ANY**.

Typical radio environment where work space is divided by shoulder-height, hollow wall elements; antennas are at desktop level.

Typical radio environment where work space is separated by floor-to-ceiling brick walls: antennas can not "see" each other.

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to an Internet server. Essentially, it packages your computer's TCP/IP packets and forwards them to the (Internet) server, where they can actually be put on the Internet. PPP can handle synchronous as well as asynchronous communication.

PPPoE (Point-to-Point Protocol over Ethernet) is a specification for connecting multiple computer users on an Ethernet to a remote site through a modem. PPPoE combines PPP with the Ethernet protocol, where the PPP protocol information is encapsulated within the Ethernet frames.

In a Residential Gateway network, PPPoE can be used to let multiple wireless users share a common Digital Subscriber Line, by connecting an ADSL modem to the gateway.

Layer **T**wo **T**unneling **P**rotocol
Extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPN).
L2TP requires that the ISP's routers support the protocol.

Remote Authentication Dial In User Interface.

RADIUS Server Access Control is a security mechanism based on a protocol exchange between Base Station devices and a dedicated server that contains a central database of computer stations that are allowed to access the network.

Authorized stations are identified by the unique Universal MAC Address of their network adapter.

The movement by a mobile Wireless Client Station among multiple wireless cells. The wireless network can locate the wireless station as it `roams', and provides continuing service to that station.

When moving away from its current Base Station, your network interface will automatically connect to another Base Station when the quality of radio communications require it do so, in order to maintain the network connection.

Every Avaya Wireless card has a unique identification number of the format:
YYUTxxxxxxxx, where

- YY identify the year of manufacturing
- xx identifies the unique item number.

This number is printed on a label that you can find on your product.

The Signal-to-Noise Ratio (SNR) is the primary diagnostic counter to diagnose wireless performance. SNR indicates the relative strength of the received Signal Level compared to the Local Noise Level.

In most environments, SNR is a good indicator for the quality of the radio link between transmitter and receiver. A higher SNR value means a better quality radio link. The color coding of the SNR-bar indicates the link quality.

Signal Level indicates the strength of the wireless signal as received at the Wireless Client Adapter. As the wireless system may perform quite well even when the signal level is low, the primary indicator to diagnose the communications quality is the level of SNR.

Use the Client Manager or AP Manager Link Test to investigate the communications quality.

Noise Level reflects the level of local background noise as measured at the Wireless Client Adapter.

Noise can be indicated as Local Noise (close to the monitoring station) or Remote Noise (close to the Link Test partner)

Possible sources of interference can be:

- Theft Protection Devices
- Cordless Phones
- Microwave Ovens
- Pager Systems

This counter reflects only the Noise Level value (in%) of the latest frame that was received on this interface.

When the value displayed changes dynamically, the likely cause will be that there are multiple wireless stations communicating to this wireless interface, where the communications path of one or more stations to Base Station suffers from interference, and the communications path of the other stations is 'clean'.

Use the Client Manager Link Test to investigate the communications quality between each Wireless Client Station and this Base Station.

The Noise Level, as well as the Signal Level, is expressed in decibel milliwatt (dBm) and has a negative value. The lower (= more negative) the value, the weaker the Noise.

When the source of interference is identified, eliminate the source of interference, or use this indicator to optimize station or antenna placement for optimal wireless performance.

The level of radio interference as measured in the vicinity of your wireless computer.

The level of radio interference as measured in the vicinity of the remote station (for example your `Link Test Partner' or the current).

Small Office / Home Office

Relatively small network that comprises up to 10 wireless and/or wired computers.

Occasionally a SOHO network uses a shared connection to an Internet Service Provider to provide internet access to individual workstations.

Simple Network Management Protocol. A network protocol that can be used to manage networks locally, or world-wide via the internet.

Advanced Security option that enables you to authorize SNMP management to a restricted group of SNMP Management stations.

You can authorize one or multiple LAN Administrator Stations to access the Base Station configuration or diagnostic information.

SNMP Trap Messages is part of the Trap Host mechanism.
It sends information on actions such as:
Reset procedures on the Base Station,
Upload of new configuration in to the Base Station,
Forced Reload so that the network administrator can verify whether the action was authorized or not.

The station name is an optional parameter that may be used to designate wireless devices in the network. The name can help to identify a device in one of the Avaya Wireless diagnostic utilities. A station name can consist of up to 31 alphanumeric characters.

Station in an SNMP managed network, where SNMP Trap Messages are collected.

User **D**atagram **P**rotocol.

Connection less protocol, like TCP, that runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive data grams over IP networks. It is used primarily to broadcast messages over a network.

Protocol **D**ata **U**nit

Retransmission time-out algorithm as defined by the UK **R**oyal **S**ignals and **R**adar **E**stablishment.

Extension to the **I**nternet **C**ontrol **M**essage **P**rotocol (IP).

It supports packets that contain error, control, and informational messages. The PING command, for example, uses ICMP to test the Internet connection.

Bridge **P**rotocol **D**ata **U**nit (also referred to as Configuration BPDU).

Data message that is exchanged between switches within large networks where the Spanning Tree protocol has been enabled. This message includes information about ports, addresses, priorities and path costs and it is used to detect loops in the network.

When a loop is detected, the Spanning Tree protocol will shut down selected bridge interfaces, and place redundant switch ports in a back-up or blocked state.

The Bridge that has the lowest Bridge priority level in a Spanning Tree topology.

In a Spanning Tree configuration, the LAN is usually split up into multiple LAN segments. The Designated Bridge is the bridge that will forward all packets from bridges residing on the same LAN segment to the Root Bridge or bridges residing in other LAN segments and vice versa.

The Designated Bridge is usually the one closest to the Root Bridge.

Retransmission is a standard IEEE 802.11 method of dealing with lost messages. In case a transmitting wireless computer does not receive the acknowledgment that a transmitted message was received, the station will try to transmit the message again. When the retransmission fails as well, your wireless computer will switch to a lower Transmit Rate, using the Auto Fallback mechanism.

In a Spanning Tree configuration, each bridge unit will identify which bridge port provides the shortest path to the Designated Bridge on the LAN segment and the Designated Bridge on the LAN.

In complex network topologies, the Spanning Tree option enables you to enhance data traffic efficiency, and eliminate the possibility of data loops.

With the spanning tree algorithm, all bridges on the LAN exchange special configuration messages (PDU's) that allow them to:

- Select a single bridge among all bridges in the connected LAN segments to be the Root Bridge
- Calculate the distance of the shortest path from them-selves to the root bridge.
- select a Designated Bridge in each LAN segment that will forward packets between that LAN segment and the root bridge.
- Select a Root Port among all ports of the bridge unit.

This way bridges will dynamically discover a loop-free subset of the LAN topology (a tree), that provides the most efficient level of connectivity between every pair of physically connected Local Area Network segments.

If the 'shortest data path' fails, (for example as a result of a physical breakdown), the Spanning Tree will automatically rebuild the topology within the confines of the available bridged LAN components.

The total number of data packets arriving at the Base Station from the LAN segment served by the selected wireless network interface.

This number reflects the sum of Unicast and Non-Unicast packets.

Messages transmitted by a single station (typically a server) to all stations on the network. This type of traffic is also referred to as Non-Unicast messages.

The number of bytes (octets) received at the Base Station from the LAN segment served by the selected wireless network interface, including framing characters.

The number of packets requested by higher level protocols, to be transmitted to a subnetwork-unicast address, typically Multicast or Broadcast messages. This number includes the frames that were discarded or not sent.

The name of the Base Station. The Base Station name is defined in the SNMP parameter settings in the Base Station configuration.

You can display or modify these settings using the AP Manager.

An advanced Bridge setup option that you can use to protect the network against data overload by:

- Specifying a maximum number of frames per second as received from a single network device (identified by its MAC Address).
- Specifying an absolute maximum number of messages per port.

The `Storm Threshold' parameters allow you to specify a set of thresholds for each port of the Base Station, identifying separate values for the number of broadcast messages/second and Multicast messages/second.

When the number of frames for a port or identified station exceeds the maximum value per second, the Base Station will ignore all subsequent messages issued by the particular network device, or ignore all messages of that type.

Time-**T**o-**L**ive

An advanced IP Parameter Setup counter that you can you use to maintain network efficiency. The purpose of the Time To Live counter (TTL) is to avoid endless forwarding of message frames with an incorrect address that pollute the network medium.

The TTL defines a maximum number of passes per hop. Each time the frame is forwarded by a router, the TTL counter decreases by one. When the TTL = 0, the frame is rejected.

Ultra **H**igh **D**ensity

The number of bytes (octets) transmitted out to the interface.
This is `true data' from station to station.

Universal **S**erial **B**us

In a network with multiple Residential Gateway devices, you will typically assign one Residential Gateway to act as the **primary** station that will distribute IP addresses to all clients and other Base Station units.

In a network with multiple Residential Gateway devices, this term refers to the Base Station units that have the DHCP functionality disabled, and will receive their IP Address of the Primary Base Station.

The Variant level identifies the type of Avaya Wireless adapter.

As different variant types may support different functionality and features, you can only use firmware upgrades that are identified by the same Variant type as the one of your card.

The Version number identifies the type of Avaya Wireless adapter. This number increments with each new firmware release.

The format of the version identification designator is typically X.xx, where:

X	identifies a major version upgrade
xx	identifies a minor version upgrade

You are advised not to 'downgrade' the firmware of your Avaya Wireless card, by loading firmware with a version level that is less than the one currently installed on your card.

In some exceptional cases, typically upon advice of Avaya Wireless technical Support you may need to downgrade. Doing so the WSU tool will prompt you to confirm that you wish to overwrite the card's firmware with an older version.

The basic operating software of the Avaya Wireless adapter, required to interface with standard PC Card sockets and services.

Usually, this software does not need any update. In the exceptional case where an upgrade of your card's Station Functions Firmware requires upgrade of the Primary Functions Firmware as well, this upgrade will be executed automatically, provided that the variant of the firmware upgrade is the same type as the variant of your PC Card's hardware.

See also:

- Variant
- Version

This card software controls the features of your Wireless Client Adapter. It allows the adapter to operate as a Station (STA) in an IEEE 802.11 LAN, when inserted into the computer.

The STA functions firmware includes features such as:

- 'Auto-connect' to IEEE 802.11 networks
- Option to select the data transmission speed
- Option to assign a Network Name

See also:

- Variant
- Version

This type refers to the standard Avaya Wireless PC Card.

This is a network adapter card that fits into any standard PC Card Type II slot.

This type of card has a small extended part containing the radio antennas. The extended part protrudes slightly from the host device to allow the antennas to transmit/receive wireless signals with as little obstructions as possible.

This is a special adapter that has been designed for use in 'Fixed Wireless Systems' to connect LAN via wireless outdoor antenna links.

This type of card is identified by a distinct (green) color of the extended antenna part of the PC Card.

Local Radio regulations may require you to apply this type of Avaya Wireless adapter when setting up wireless outdoor antenna links.

In combination with the IP address, this number will identify which network your computer is on. If the *IP Address Mask* was assigned to you by your Script file (ISP), this is a required value to fill in.

Domain **N**ame **S**ystem

Distributed database used by computers on the Internet to look up each other's addresses.

When any site needs to add or remove computers, it simply updates the correspondent portion of the database and, after a short period, everyone on the net can see the change.

A script file contains scripting commands, parameters, and expressions that provide and retrieve information to and from the remote computer you are connecting to. This information can include your user name and password, port information, carriage returns, line feeds, and pauses.

Wireless **E**thernet **C**ompatibility **A**lliance

Group of leading equipment and software providers, aiming at inter operability among a wide variety of wireless systems.

http://www.wirelessethernet.org

Wireless **Fi**delity

Inter operability standard of wireless network systems as defined by the WECA organization.

The WiFi logo on your wireless products ensures IEEE 802.11 High Rate quality and certified inter operability with an expanding range of WiFi certified product and solutions.

Wired **E**quivalent **P**rivacy

IEEE 802.11 compliant encryption scheme based on the RC4 algorithm that is used to secure wireless data.

WEP encryption is a method of encrypting data that is transmitted over your wireless network to insure data security. In a wired network, data security is maintained through the physical wire. WEP encryption provides the same level of security for your wireless data as if it were being transmitted over standard network cabling. In order to duplicate wired network security levels, wireless data is encrypted at its point of transmission. The receiving device decodes the data. This allows users to have the same amount of security over their wireless network as they would over a wired network.

Wireless Station Update tool.

Windows-based tool to update the firmware of the Avaya Wireless PC Card and PCI Adapter.

The WSU tool runs on any desktop or laptop computer that:

- Runs the Microsoft Windows 9x, ME, 2000 and NT4.0
- Has the Avaya Wireless Driver installed.

Wireless Client Adapter that supports 64-bit WEP data encryption.

This type of interface allows you to enter:

- 5-digit keys in Alphanumeric Value or
- 10-digit keys in Hexadecimal Value.

Wireless Client Adapter that supports both 64-bit WEP and 128-Bit data encryption based on the RC4 algorithm. This type of interface allows you to enter:

- 5 or 13-digit keys in Alphanumeric Value or
- 10 or 26-digit keys in Hexadecimal Value.

Network **A**ddress **T**ranslation

Translation of an IP address used within one network to a different IP address known within another network.

A NAT-enabled device translates a set of local IP addresses to one or more IP addresses on the Internet. NAT translates the IP address of incoming packets back to local IP addresses.

Automatically enables IPSec.