WIRELESS LAN SERIAL PORT ADAPTER AT COMMANDS

Document Revision
Published: Oct 13, 2011 11:13
Document version: 4

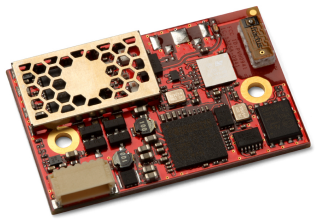
1 Table of contents

2 Abstract

The wireless LAN serial port adapter modules from connectBlue are industrial strength, low power modules, for IEEE 802.11 networks aimed at embedded, mobile, security, and industrial applications. They contains all necessary functions for a complete and efficient Wireless LAN integration; TCP/IP stack, supplicant, MAC/base-band, dual-band radio front-end, amplifiers, and antenna switches.

The modules are radio type approved* for Europe and has an unlicensed modular transmitter approval for US (FCC) and Canada (IC).

This document is applicable the following wireless LAN serial port adapter modules from connectBlue:

	
cB-OWS451-06 *(IEEE 802.11abgn)*	*cB-OWSPA311g-06* *(IEEE 802.11bg)*

**) cB-OWS451 radio and modular approvals are in progress.*

3 Key features

- Dual-band operation: IEEE 802.11-2007, abg, incl. single stream IEEE 802.11n
- WEP, AES, and CRC-32 hardware accelerators
- WPA and WPA2 support
- LEAP support
- PEAP support
- High speed UART host interface
- Ad-hoc and infrastructure mode
- Radio type approved for Europe.
- Unlicensed Modular Transmitter Approval for US (FCC) and Canada (IC).
- Compliant with EMC standards.
- Industrial temperature range.
- Support for low power modes.
- Compatible with connectBlue Bluetooth and IEEE 802.15.4 modules
- Internal antenna or dual external U.FL. antenna connectors
- Receive diversity

4 Related documents

Documents related to the wireless LAN serial port adapters:

- The Wireless LAN serial port adapter AT command set contains information on how to use the serial port adapter module.
- The Electrical & mechanical data sheets contains important information about the serial port adapter modules on how to design and implement.

5 References

- cB-OWS451 Electrical and mechanical data sheet
- cB-OWSPA311g Electrical and mechanical data sheet
- RFC1738 Uniform Resource Locators

6 Compatibility

This section describes software compatibility issues. In the table below, the firmware version in *which the compatibility issue appeared* and a description of the issue is listed. Thus, this is not a list of firmware releases and new features. For this please look at the release notes distributed with each new firmware release.

Firmware version in which the compatibility issue appeared	Description of compatibility issue
1.4.0	AT*AMMP Max output power range has changed. See AT*AMMP Max output power for new valid range.
1.3.6	AT*AGFP Encryption/Authentication Key command removed due to security reasons.
1.3.6	AT*AGFPRI command removed due to security reasons.
1.3.6	AT*AMRFM Read Feature Mask/AT*AMWFM Write Feature Mask deprecated. Commands for modifying the feature mask is now deprecated but all existing feature mask settings are kept for compatibility reasons. For more information, see the ATS General Settings S Register Manipulation command.
1.3.6	AT*AGLN included for compatibility reasons. AT*ANHN Hostname is the preferred way to manipulate this setting.
1.3.6	AT*AGRSS RSSI Value returns error when module is not connected.
1.3.6	Stop-mode will not work properly with the engineering samples with green PCB.

7 Data mode and AT mode

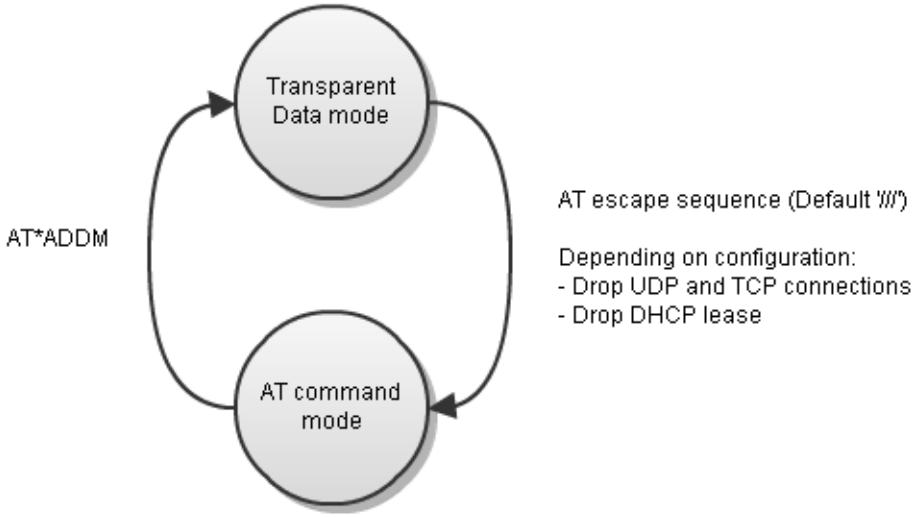
The Serial Port Adapter operates in two different modes, AT mode and data mode. The module starts up in data mode and can be requested to move to AT mode by sending an escape sequence. The default escape sequence consists of three consecutive forward slash characters '/'. The escape sequence character can be changed using the ATS2 command. See chapter 4 for information on how to restore settings to the default escape character.

The following criteria must be met for the module to interpret the sequence as a valid escape sequence:

- Before the escape sequence there must be no data for 1 second. This time can be changed using the AT*AMET Escape Sequence Timing Settings command.
- After the escape sequence there must be no data for 1 second. This time can be changed using the AT*AMET Escape Sequence Timing Settings command.
- The entire escape sequence must be sent within 200 ms.

It is also possible to configure the serial port adapter to enter AT command mode automatically at startup. S-register 4007 configures if the module should start in data mode (S4007=0) or in AT command mode (S4007=1). The default behavior is to start in AT command mode (S4007=0).

To move from AT mode to data mode, use the AT*ADDM Enter Data Mode command.



Any connection that you have with the serial port adapter module, be it serial, TCP or UDP can be used to enter AT mode. The procedure is the same as described above.

> By default, it is only possible to enter AT mode from the serial connection. This behavior can be changed using the AT command AT*ACCB Configuration over WLAN.

7.1 Handling of remote peers in AT mode

Per default the serial port adapter will disconnect all remote peers, UDP or TCP connections, when entering AT command mode. This means, among others, that if the serial port adapter is configured to use dynamic IP address (DHCP client) the address lease will be dropped. This in turn gives that AT*ANIP? will return the value of the static IP address and not the previous used dynamic one.
To let remote peers be left in connected state when entering AT command mode, set S-register 4006 = 1. (Keep remote peers connected) If this S-register is set then also the DHCP lease will be kept and AT*ANIP? will return correct values for the acquired dynamic IP.

7.2 Baud rate

The default serial connection settings are 57600 bits/s, 8 data bits, no parity, 1 stop bit and hardware flow control. See Restoring default configuration for information on how to restore the default serial settings.

The module does not support auto baud rate. The baud rate is set using the AT*AMRS RS-232 Settings AT command.

> Default serial settings are 57600 bits/s, 8 data bits, no parity, 1 stop bit and hardware flow control.

8 Restoring default configuration

8.1 Serial settings

In some situations it is necessary to restore all settings to their default values. Default values for all settings are listed in the AT Command Reference chapter. The default values of the most important settings are:

- Serial settings: 57600 baud, 8 data bits, no parity, 1 stop bit, hardware flow control.
- Serial interface type: RS232.
- AT escape sequence: "`///`" (three forward slashes).
- Escape sequence timing: 1 second of no data transmission required before and after the escape sequence for the escape sequence to be valid.
- Escape character (S2): '/' ASCII value of 47
- Command Line Termination Character (S3): ASCII value of 13
- Response Formatting Character (S4): ASCII value of 10
- Backspace Character (S5): ASCII value of 8

The default settings can be restored in two ways.

One way is to apply a logic low signal on the Switch-1 input on the module during startup.

If the module is mounted on the *OEM RS232 Module Adapter* (cB-ACC-24), this is done in the following way:

1. Disconnect power from the Module Adapter
2. Press and hold the *Restore* / *S1* button input (the one closest to the RS232 connector)
3. Connect power to the Module Adapter
4. When the module powers up, all settings will be restored to their default values
5. Release the *Restore* / *S1* button

If the module is mounted on the *OEM USB Module Adapter* (cB-ACC-34), this is done in the following way:

1. Connect the Module Adapter to a USB port
2. Press and hold the *Restore* button input (the one closest to the *RGB LED* at the short side)
3. Press the *Reset* button input (the small button at the long side, next to the *Yellow LED* for UART RxD)
4. When the module powers up, all settings will be restored to their default values
5. Release the *Restore* button

The other way is to enter AT mode on the module and use the AT command AT&F Restore to Factory Settings.

Another alternative to restore UART settings is to enable *UART fallback mode* (ATS4014=1). Firmware will then check switch-0 (see electrical and mechanical data sheets for details about pin-outs) every second when UART fallback mode is enabled. If switch-0 is activated UART settings are temporarily changed to 57600 baud, 8n1, and hardware flow control. Settings are restored when button is de-activated.

9 Configuration and operation

This chapter gives guidelines on how to perform basic configuration and operation.

There are several request packets (AT commands) that can be used to configure the serial port adapter. Many of these request packets take an integer parameter called <store>. If this parameter is set to 1 the setting will be stored in persistent memory and by active also after a power off/on cycle. If this parameter is set to 0 the setting will be applied but not stored in persistent memory. Such settings will not be applied when the module starts up in the next power cycle.

There is constraints on some AT commands which means that the module must be restarted before the commands takes effect. For those commands the <store> parameter must always be set 1 otherwise they will be reset at restart.

9.1 LED indication

LED indication is built up using three signals; Red, Blue, and Green. See the Electrical and mechanical data sheets for detailed information and pinouts of the three LED signals.

9.1.1 Color scheme

The LED indicates what mode is currently active and what activity that is currently in progress. The following color indications are used:

Red	Blue	Green	Color	Description

		X	Green	Current mode is data mode and no connection attempts are in progress
X			Red	Module could not boot properly, or is in rescue mode
X		X	Orange	Current mode is AT mode
X	X		Purple	A connection attempt is in progress
	X			A connection is currently active
	(X)		Blue blinking	A connection is active and data is transmitted or received over air
(X)			Red blinking	Buffer overflow, parity or framing error detected on the UART.

A connection is identified as a connection to an access point. A blue led does not mean that any peer connections have been established. To detect remote peer connections use the DTR pin.

9.2 Creating serial connections and sending data

See chapter User Guide for examples on how to create connections and transfer data.

9.3 WLAN security

The serial port adapter module supports different authentication and encryption methods. The following authentication methods are supported:

- Open connection
- Shared secret
- WPA and WPA2 Pre-shared key (PSK)
- LEAP
- PEAP

The following encryption methods are supported:

- No encryption
- WEP64
- WEP128
- TKIP
- AES/CCMP

The following matrix shows valid combinations of authentication and encryption methods ("x" means valid combination):

	Open connection	Shared secret	WPA/WPA2 PSK	LEAP	PEAP
No encryption	X				
WEP64	X	X		X	
WEP128	X	X		X	
TKIP			X	X	X
AES/CCMP			X	X	X

The serial port adapter will not indicate any errors if you enter an invalid combination.

There are a few important considerations that need to be addressed as well. If you choose WPA/WPA2 PSK and TKIP, this is considered a WPA connection. If you choose WPA/WPA2 PSK and AES/CCMP, a WPA2 connection is assumed. It is not possible to have WPA with AES/CCMP encryption nor WPA2 with TKIP.

If you wish to use LEAP or PEAP as the authentication algorithm, make sure that your access point supports it. Not all access points support LEAP and PEAP.
Neither LEAP, PEAP nor WPA/WPA2 PSK will work in ad-hoc mode.

9.3.1 Key management

For WEP64 and WEP128 shared keys can be entered into all four possible slots made available by the AT*AGFPWI Write Encryption/Authentication Key (with Index) command. However, for LEAP and WPA/WPA2 PSK the password or PSK must be entered into key slot with index 1 (one). This key must also be the one currently set active by the AT*AGAFP Active Encryption/Authentication Key command.

If you are using LEAP, the username for the Radius server should be entered with the command AT*AGUN Username.

If you are using WPA/WPA2 PSK you can enter either the pre-shared key (i.e. the hexadecimal string) or the password (plain-text), commonly referred to as "WPA-PSK" and "WPA-PWD". Each time you change the password you need to reboot the serial port adapter for the settings to take effect. If you choose to enter a password (not a hexadecimal string) the serial port adapter will take slightly longer during the first boot after this change, in order to deduce the real key from the password. When the serial port adapter is calculating the real key it will be unresponsive.

Hexadecimal strings are given byte-by-byte. Each hexadecimal coded byte is prepended with the string escape character '\'. Example: "\AF\11\12\4C\00\FF\0A\6D".

9.4 Important behavior

9.4.1 Cache

When a module is not connected to any remote peers it cannot transfer any incoming data on the UART to any remote devices. Instead it tries to cache the data. This will happen in any of these cases: if there are no remote peers configured, if the module is trying to connect to a remote peer or if a single remote peer uses the "Connect on data" connection scheme. The data is cached until a connection to a remote peer is established. The cache is implemented as 256 bytes FIFO. If the FIFO gets full before the module has established a connection, the oldest data is silently discarded.

9.4.2 Ad-hoc and roaming

Ad-hoc networks operate without any access point. This makes them versatile and well suited for small and improvised networks setup on the fly. However, since there is no access point in the network, one of the devices in the ad-hoc network will assume the role of a basic access point.

Therefore, if a module wanting to connect to an ad-hoc network cannot find an existing network with the correct SSID, it will take the role of the access point. Any devices looking for the network after this will find the network and can properly connect to it.

If the module that has the role of the access point for some reason leaves the network (due to power failure or moving out of range) another device in the network will automatically assume the role of the access point and this will keep the network going.

This introduces a roaming issue. If the module that left the network returns (returns into range), it will still believe it is the access point of the network. Suddenly we have two modules acting as access point. These modules effectively operate on different networks and will not be able to communicate.

To try to remedy this issue connectBlue has introduced a trigger setting into the module. This trigger will activate if one module has been alone in a network for too long. It will then try to scan for present network and connect to it if possible. This timeout period is adjustable via an S register.

However, this only solves the most basic of roaming cases for ad-hoc. Imagine an ad-hoc network with four modules. If two modules leave at the same time and leaves the two other modules behind. There is little chance of the four modules reconnecting again without interaction.

Therefore, if roaming if desired, please look into planning a proper network with access points spread out over the desired area.

9.4.3 Background scan

TODO

9.4.4 Improving roaming in infrastructure networks

If you are using the module in an infrastructure network there is one way to improve roaming times radically. By using the command AT*AGCL you can define the channel list the module should use. By default, this channel list includes all legal channels but since it is unlikely that one network is using all channels available you can narrow it down. This means that instead of scanning 11 to 14 channels you can set it to scan only the ones in your network, which should be very few.

So, for instance, if your network only uses 3 channels, say 1, 6 and 11. When a connection is to be established the module will only scan the three channels instead of 11 or 14, which takes a lot shorter time. When a module later moves out of the range of one AP, it will only have to scan these three channels again to find an appropriate access point.

9.4.5 CPU idle, improving response times and throughput

By default, the modules CPU is put into a mode where it will try to sleep as often as possible, thus conserving power. Setting the Power Save mode to Online does not affect this specific setting. To adjust this you need to use the S-register 4005.

At low speeds, the cpu idle setting will not make a difference in response times or throughput. However, at higher uart speeds, from 230 Kbit/s and up throughput will be affected. If you desire maximum throughput at these speeds, you should look into changing this setting.

9.5 Pin diagrams

These diagrams show the pin behaviour for different configurations.

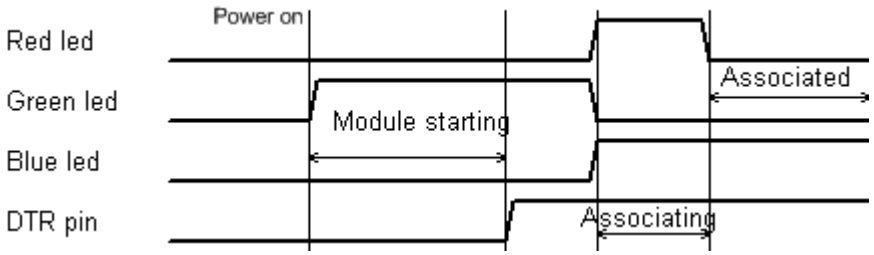


Figure 1 Default configuration, DTR mode = at startup

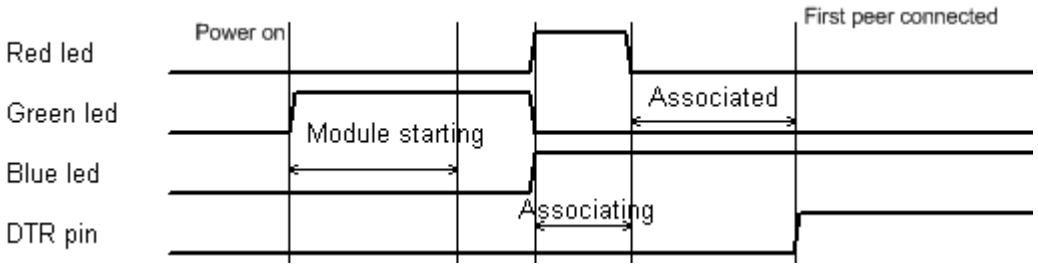


Figure 2 DTR mode = at connection

10 Power save

It is possible to lower the module power consumption by configuring different power save modes. Generally, lowering the overall power consumption leads to higher system response times. It is hard to find a configuration to fit all needs and it might be a good idea to experiment with different configurations to find one that fits the application.

To understand the power settings it's important to understand that the serial port adapter has two independent chips that have individual power saving features. The two chips are the wlan radio chip and the processor.

Independently of what power save mode is configured, the processor can be configured to enter its idle mode when idle. This is configured using the ATS4005 AT command. By default, the processor enters idle mode. Turning off the idle mode feature will increase the throughput slightly.

10.1 Power modes

The serial port adapter has three different power saving modes.

1. Online mode
2. Sleep mode
3. Stop mode

10.1.1 Online mode

The online mode does not have any power save features. Latency is the lowest possible. Wireless LAN do not do any power saving unless the serial port adapter is in a disassociated state.

10.1.2 Sleep mode

This mode is the default. In this mode the radio chip will utilize power save in both connected and disconnected mode. Wake up latency in connected mode is determined by how often the access point sends out beacons. The amount of power saved is also determined by how often the access point sends out beacons as well as the DTIM values.

In Ad-hoc mode the radio cannot perform any power saving whilst associated. Power saving in disassociated mode is still possible though.

10.1.3 Stop mode

In Stop mode the radio chip behaves exactly as in Sleep mode. The module will keep its connection to the access point. The difference here is the processor.

The processor will try to power down itself into a state where it is completely shut off except for a few interrupts. There are only two things that can wake up the processor from this state. The first one is automated and is activated by the radio chip when new data is available. The other one is the DSR pin of the UART. If the DSR pin is disabled the module will try to enter Stop mode. If this pin is enabled, the serial port adapter will wake up from Stop mode.

After the DSR pin has been disabled there is an adjustable timer setting that the serial port adapter waits until it tries to enter Stop mode. The serial port adapter will not enter Stop mode if it still has things to do. It will enter it as soon as it deems possible after the timer has elapsed.

If the DSR pin is enabled the processor will of course idle if there is nothing to do. A module in Stop mode with the DSR pin enabled therefore behaves the same way as a module in Sleep mode.

10.2 Optimization

To optimize the power consumption further the WLAN beacon listening interval can be reduced. By doing so, the time the WLAN chipset is active is reduced. This setting is configured with the ATS3001 AT command.

11 Syntax

11.1 Command line format

Each command line sent from the DTE to the DCE is made up of a prefix, body and terminator. As prefix for the serial port adapter AT commands, only "AT" (ASCII 65, 84) and "at" (ASCII 97, 116) can be used. There is no distinction between upper and lower case characters. The body is a string of characters in the range ASCII 032-255. Control characters other than <CR> (carriage return; ASCII 13) and <BS> (back space; ASCII 8) in a command line are ignored.

The terminator is <CR>. Commands denoted with a "*" character are extended AT commands, i.e. serial port adapter specific AT commands.
Multiple commands in the same command line are not supported. Each command has to be terminated by a <CR> before a new command can be sent. A command must not be longer than 300 characters.

A command can either be:

- Read commands without parameters: AT<command>?<CR>
- Write commands without parameters: AT<command><CR>
- Read and write commands with parameters: AT<command>=<parameter1>, parameter2>, ...<parameterN><CR>

Responses are sent back to the host and can be any of the following:

- Successful final message: <CR><LF>OK<CR><LF>
- A read command will precede the OK response with the read parameters. The form is <CR><LF><command>:<param1>,<param2>,...,<paramN><CR><LF> String results will have "" around them.
- Successful intermediate/final message with parameters follows an OK message in some commands. In these cases the OK message works as a confirm message only. <CR><LF><result_response>:<parameter1>, parameter2>, ...<parameterN>
- Error message: <CR><LF>ERROR<CR><LF>

11.2 Data Types

The definition of each command specifies the data types used for values associated with the command. There are four different data types:

- String
- Integer
- IP_Addr
- MAC_Addr

These are described below:

11.2.1 String

A string shall consist of a sequence of displayable characters from the ISO 8859-1 (8-bit ASCII) character set, except for characters "\", """ and characters below 32 (space). A string constant shall be delimited by two double-quote (""") characters, e.g. "Donald Duck". If the double-quote character (""") is to be used within a string, e.g. "My friend "Bono" is a singer", they have to be represented as "\22". If the back-slash character ("\") is to be used within a string constant, it has to be represented as "\5C". An empty string is represented by two adjacent delimiters, "".

11.2.2 Integer

An integer value consists of a sequence of characters all in the range {0..9}. Numeric constants are expressed in decimal format only.

11.2.3 IP_Addr

A valid IP address consists of four integer values separated by dots. Valid range of each integer value is {0..255}. An example IP address is "192.168.0.1", excluding the double-quote characters.

11.2.4 MAC_Addr

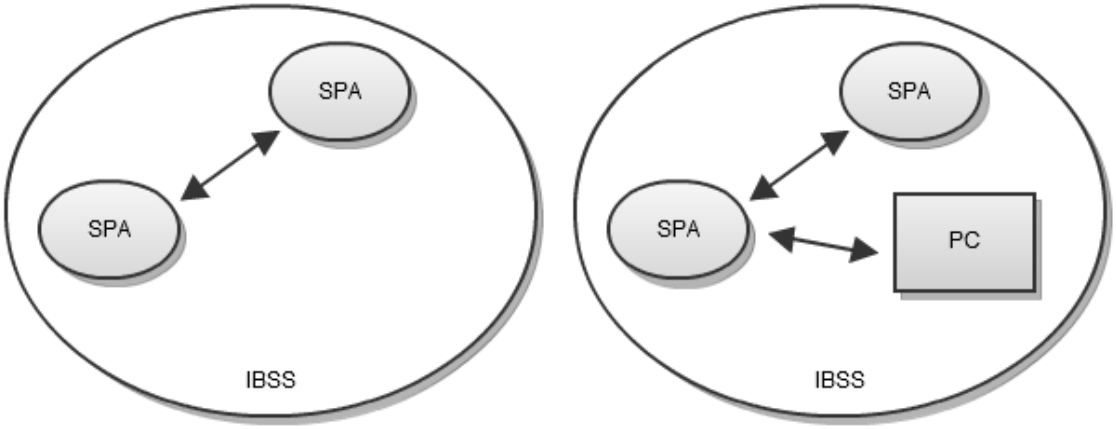
A MAC address consists of a sequence of six values, expressed in two-digit hexadecimal, in sequence. The hexadecimal values are grouped together without delimiters. An example MAC address is "01A0F7101C08", excluding the double-quote characters.

12 User guide

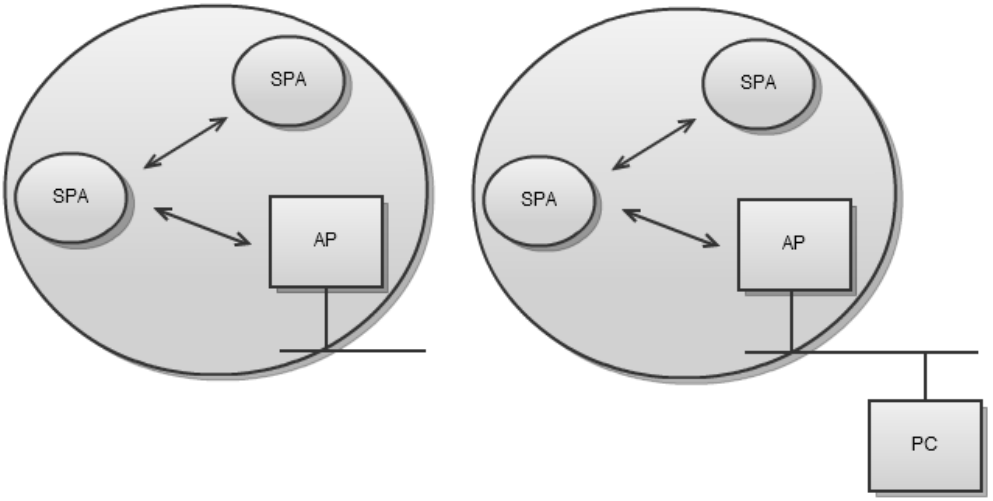
12.1 Overview

The cB-OWS451 is an 802.11abgn, and the cB-OWSPA311g is an 802.11bg based serial port adapter capable of transporting serial information across an IP network. The IP network relies on a link layer consisting of an 802.11 a/b/g/n topology that has two basic modes, ad-hoc and infrastructure. Ad-hoc does not need an access point, the participating units will create and manage the network by themselves. Infrastructure mode requires an access point to be available in the network.

12.1.1 Stand alone network (Ad-hoc)



12.1.2 Infrastructure



12.1.3 Associating to a network

Can be done using:

- The network SSID

12.1.4 Peers

A connection consists of a sender and a receiver of data. It can also consist of a sender and several receivers in the case of a broadcast data. In both cases every sender and receiver in a setup is referred to as a **peer**. Thus, a peer is capable of either receiving and/or sending data.

There are two kinds of peer classes in the serial port adapter, local peer and remote peer.

The local peer is synonymous with the UART.

In contrast to the local peer, the remote peer is another device or broadcast range on the network. Several remote peers can be defined if a multi-drop scenario is needed.

A remote peer is addressed using a Uniform Resource Locator, URL. These locators are strings representing nodes on internet or on a local net. This is the same addressing technology used in for example a web browser. For more information about URLs, read RFC 1738.

In general, URLs are written as follows:

<scheme>:<scheme-specific-part>

Where <scheme> is the scheme or protocol used when communicating and <scheme-specific-part> is normally the address and port number of the remote node.

For example, a web server on the internet can have the following address:

http://www.connectblue.com

This tells the browser to use the HTTP protocol and connect to the node at address "www.connectblue.com"

Similar addressing scheme is used by the serial port adapter to pinpoint the remote peer. The scheme is not "http", but the node addressing is identical.

Available schemes:

- tcp: TCP connection
- udp: UDP connection, broadcast capabilities

Syntax:

<scheme>://ipaddress<:portnumber>

Remarks:

- IP address can be either a numeric IP address or a host and domain name that can be resolved using the configured DNS servers.
- If scheme is not given it defaults to "tcp"
- If the port is not given it defaults to 0 (zero).

Examples

tcp://10.0.0.9:5003

tcp://www.connectblue.com:80

udp://192.168.0.42:6809

Once a remote TCP peer is connected, it can not be disconnected via any commands. The peer will have to be removed from the settings and the module rebooted. If the other end of the connection decides to close the connection the serial port adapter will close the connections gracefully. The connection will also be removed it the OWS451 detects that the remote host no longer acknowledge the sent packets.

UDP is a connection-less protocol and the peer will therefore, once activated, always remain active until a reboot of the serial port adapter is performed.

12.1.5 Listeners

The serial port adapter can also be set to listen for traffic and incoming connections on specific ports. As with the remote peers it uses TCP and UDP.

If the TCP listener is active and an incoming connection is detected on the specified port the serial port adapter will negotiate a TCP handshake and establish a TCP connection. It will also create a peer which works in the same way as a remote peer once it is connected. You can not tell the serial port adapter to disconnect peers that has been spawned in this manner.

12.1.6 Transferring data

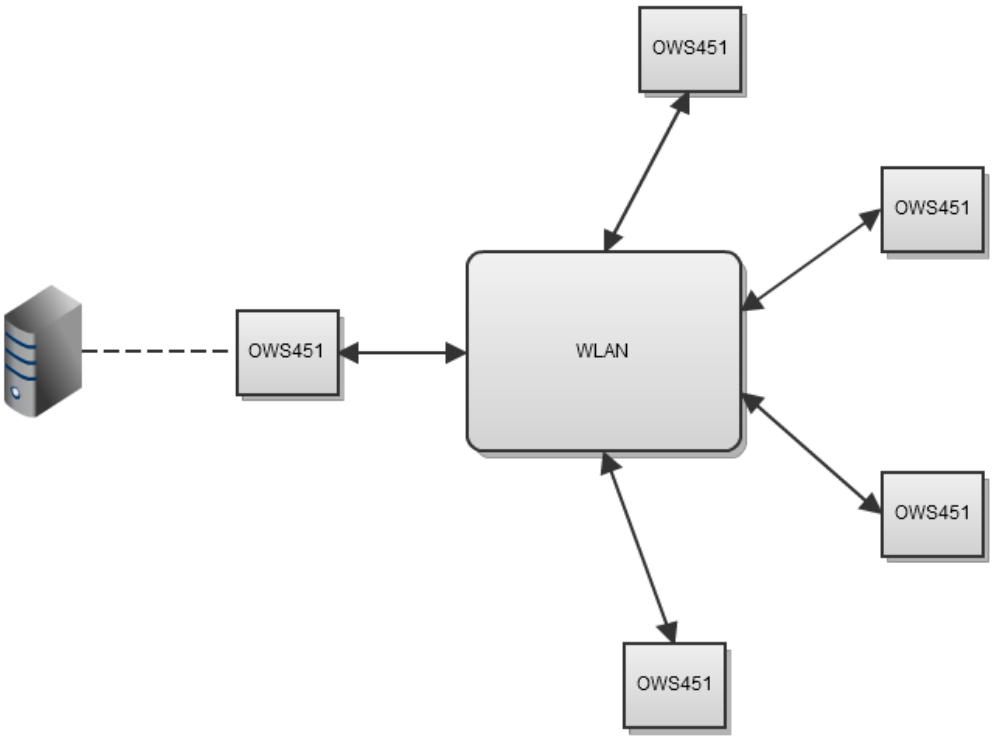
The serial port adapter only acts as an intermediary and does not produce any data itself. The serial port adapter can receive data in two different ways; the UART (local peer) and the network (remote peers). Any data received on the UART will be distributed to all the remote peers while the module is not in AT-mode. However, any data received from one remote peer will only be sent to the UART. It will not be distributed to all the remote peers.

Neither the UDP peer nor the UDP listener creates a full duplex channel peer. This means that even if you create a UDP peer to another device on a specific port, the serial port adapter will not listen on this port for incoming data; it will only send data received from the UART to this specific destination. The opposite is true for the UDP listener. The UDP listener will only listen for data on a specific port and distribute any data received to the UART. It will not try to send any data received on the UART anywhere.

There are no differences in data flow between a TCP peer and a TCP listener once the connection is established. The data channel has full duplex abilities, unlike the UDP case.

12.1.7 Physical topology

This section will demonstrate a common topology setup for the serial port adapter.



The serial port adapter on the right could be connected to some form of sensors transmitting data, which is then forwarded by the serial port adapter on the left side to the computer that monitors the process.

12.1.8 LLDP

LLDP stands for Link Layer Discover Protocol and is an IEEE standard. The serial port adapter module uses LLDP for announcing its capabilities. The default settings are to send an LLDP packet every 60 seconds. This interval can be changed with the ATS4010 command. Setting this value to zero will turn off the sending completely.

The serial port adapter has three levels of information that can add more information to the LLDP packet. The following list shows what's included in the different levels.

Level 0:

- MAC-address
- IP-address
- Time to live (the announce interval)

Level 1:

- Hostname
- System description with version information
- Capabilities (Tells the network that the serial port adapter is a station only)

Level 2:

- System services (TCP Listener on / UDP Receiver on)

Level 3 (default):

- Peer list (Sends a list of all currently connected peers including port)

The levels are additive. Level 3 will always include all lower levels. Level 2 will always include Level 0,1,2 but not 3. You adjust the levels with ATS4011.

LLDP can also be used as a keep-alive packet for the access point. If the module remains idle and in power save for longer periods some access points will try to disassociate the module. However, not all access points will wake up the module from its sleep state before sending the disassociate packet. This means that the module will never know it has been disassociated. By regularly sending out a packet, the access point will know that the module is still alive.

12.2 TCP/IP configuration

The serial port adapter has an internal IP stack. This stack needs to be configured before connecting to a network. This can be done manually via AT commands or automatically via DHCP. The serial port adapter can also act as a DHCP server, serving other devices on the net with IP configurations.

12.2.1 Manual IP Configuration

If manual configuration is required use the IP Settings command, AT*ANIP, to set address and other IP related information. Also, DHCP functionality needs to be deactivated using the DHCP Activation command, AT*ANDHCP. If DHCP is activated, this will take precedence over settings made with AT*ANIP.

It is also possible to set DNS servers. If DNS servers are set, it is then possible to address remote peers via hostnames instead of IP addresses. Use the DNS Settings command, AT*ANDNS, to set up to 2 DNS servers. E.g. An URL of tcp://192.168.0.23:5003 can then be replaced with tcp://sensor1.example.com:5003.

12.2.2 DHCP client

The serial port adapter can also retrieve IP address, netmask, gateway, and DNS servers from a DHCP server.

To activate the DHCP client use the DHCP Activation command, AT*ANDHCP. Information retrieved via DHCP takes precedence over manually configured.

Example

AT*ANDHCP=1,1

12.2.3 DHCP server

The serial port adapter can also act as a DHCP server serving other devices on the subnet with IP addresses. This is convenient setup if the OWS451 is configured as a listener waiting for other devices to connect.

When configured for DHCP server, the serial port adapter itself needs a manual configured IP address. This is set using the AT*ANIP command.

The address range managed by the DHCP server is derived from the manually set netmask and ip address. If the netmask set to a range that is less than the maximum of 7 possible clients, the manageable range is reduced accordingly.

To enable the DHCP server use the DHCP Activation command, AT*ANDHCP. Do not forget to set a valid static IP address too. (AT*ANIP)

Example

AT*ANIP=192.168.0.99,255.255.0.0,192.168.0.99,1
AT*ANDHCP=2,1

The capabilities of the serial port adapter DHCP server are limited. It can track leases for a maximum of 7 clients.

12.3 Examples

If nothing else is mentioned, all of these examples assume factory default settings for the settings that are not changed.

Many AT commands require that you reboot the module before the settings are activated.

The module will not try to associate with an access point unless a connection property on a higher layer has been defined. Please see the following examples for instructions on how to set up an outgoing and incoming connection.

12.3.1 Example 1, Configure a WLAN connection

This example describes how to configure the module to make it possible to associate with an access point. The example requires a wireless access point setup using the SSID "HailToTheKingBaby" on channel 6, not using any encryption or authentication.

1. Connect to the module and enter AT mode.
2. Set the SSID by sending the AT command `AT*AGSSID="HailToTheKingBaby",1`
3. Configure channel and save it. Usually channel number can be set to 0 to enable auto-channel but in this example we set it explicit to 6 with the AT command `AT*AGCH=6,1`
4. Restart the module with the AT command `AT*AMWS=0,0,0,0,1,0`
5. The module will now restart but will not try to associate with the access point (see the note above).

12.3.2 Example 2, Enable DHCP and configure a remote peer

This example describes how to enable IP settings using DHCP and how to configure the module to connect to a remote peer. The example requires that a DHCP server is available on the wireless network and that a host with the IP address 10.0.0.9 is listening on the TCP port 5002.

1. Connect to the module and enter AT mode.
2. Setup WLAN configuration settings (see Example 1, Configure a WLAN Connection).
3. Enable DHCP IP settings with the AT command `AT*ANDHCP=1,1`
4. Add a remote TCP peer with the AT command `AT*ADWDRP=0,tcp://10.0.0.9:5002,2,0,"peer1",1`
5. Set the number of configured remote peers to 1 with the AT command `AT*ADNRP=1,1`
6. Restart the module with the AT command `AT*AMWS=0,0,0,0,1,0`
7. The module will now restart and associate with the access point. When associated it will request an IP address from the DHCP. When it has got a DHCP lease it will try to connect to the IP address 10.0.0.9 on TCP port 5002.

12.3.3 Example 3, Static IP address and TCP listener

The serial port adapter can be configured to listen for incoming TCP and/or UDP connections on a specified port. This example shows how to configure the module for this purpose and how to make sure the connection works. It also shows how to use static IP settings instead of dynamic settings which was used in the previous example.

1. Connect to the module and enter AT mode.
2. Setup WLAN configuration settings (see Example 1, Configure a WLAN Connection).
3. Set the static IP address, netmask and gateway settings with the AT command `AT*ANIP="192.168.0.42","255.255.0.0","192.168.0.1",1`. Also make sure DHCP is disabled with the AT command `AT*ANDHCP=0,1`.
4. Turn on the TCP listener and set it to listen on port 5003 with the AT command `AT*AMTL=5003,1,1`
5. Restart the module with the AT command `AT*AMWS=0,0,0,0,1,0`
6. The module will now restart and associate with the access point. It will use the configured static IP settings.
7. Connect to the module with a terminal program (i.e. HyperTerminal in Windows) but do not enter AT mode.
8. Start a telnet session to the module from a computer that is connected to the same network as the access point to which the module is associated. In Windows, a telnet session is started by opening command prompt (Start->Run, "cmd"). In the command prompt type `telnet 192.168.0.42 5003` and press ENTER.
9. Telnet should now connect to the module. Verify the connection by typing something in the telnet window. The text should appear in the terminal window.

12.3.4 Example 4, Find the DHCP assigned address and RSSI value

This example describes how to find out what IP settings the module is assigned when configured to use DHCP IP settings. The default behavior of the serial port adapter is to disconnect all peers including the link layer (WLAN link) when AT mode is entered. Effectively this will release and flush the assigned IP settings as soon as the module enters AT mode, which makes it impossible to read out these settings. However, there is a way to change this behavior, so that the peers and link layer are kept connected when the module enters AT mode. This method also applies if you want to find out the RSSI value for the link layer connection.
The example requires the module to have valid WLAN settings (see Example 1, Configure a WLAN Connection) and at least one remote peer configured (see Example 2, Enable DHCP and configure a Remote Peer).

1. Connect to the module and enter AT mode.
2. Tell the serial port adapter to keep all connections, even when entering AT mode. This is done with the AT command `ATS4006=1`
3. Restart the module with the AT command `AT*AMWS=0,0,0,0,1,0`
4. Again enter AT mode. This time the peers and link layer will not be disconnected which makes it possible to read out IP settings and RSSI value.
5. Read the assigned IP settings with the AT command `AT*ANIP?`
6. Read the current RSSI value with the AT command `AT*AGRSS`

12.3.5 Example 5, WLAN connection with WEP encryption

This example requires an access point with WEP128 encryption enabled and the key set to "MisterFancypants".

1. Follow Example 1, Configure a WLAN Connection, but before you restart the module execute the following commands.
2. Set the authentication mode to shared secret with the AT command `AT*AGAM=1,1`
3. Set the encryption mode to WEP128 with the AT command `AT*AGEM=2,1`
4. Set the first encryption key with the AT command `AT*AGFPWI=1,"MisterFancypants",1`
5. Set the active encryption key to 1 with the AT command `AT*AGAFP=1,1`
6. Restart the module with the AT command `AT*AMWS=0,0,0,0,1,0`
7. The module will now restart but not associate with the access point because of the reason described in example 1.

> To enter hexadecimal values in the key, the value must be escaped with "\". For example, the hexadecimal value 0x42 should be entered as "\42".

12.3.6 Example 6, WLAN connection with WPA2 encryption

This example requires an access point with WPA2 encryption enabled and the key set to "MisterFancypants".

1. Follow Example 1, Configure a WLAN Connection, but before you restart the module execute the following commands.
2. Set the authentication mode to WPA/WPA2 PSK with the AT command `AT*AGAM=2,1`
3. Set the encryption mode to AES/CCMP with the AT command `AT*AGEM=4,1`
4. Set the first encryption key with the AT command `AT*AGFPWI=1,"MisterFancypants",1`
5. Make sure the module uses encryption key 1 by setting it to this with the AT command `AT*AGAFP=1,1`
6. Restart the module with the AT command `AT*AMWS=0,0,0,0,1,0`
7. The module will now restart but not associate with the access point because of the reason described in example 1.

12.3.7 Example 7, Example DNS configuration and usage

This example describes how to configure the DNS settings and connect to a remote peer using its host and domain name instead of its IP address. The example requires that a DNS server is available on the wireless network and that the name of the remote peer resolves in the DNS. In the example we use one DNS server with the address 192.168.0.5 and a remote peer with the name test.connectblue.se.

1. Configure WLAN and static IP settings (Example 3, Static IP Address and TCP Listener, step 1-3)
2. Configure DNS server with the AT command `AT*ANDNS=192.168.0.5,0.0.0.0,1`
3. Add a remote TCP peer with the AT command `AT*ADWDRP=0,tcp://test.connectblue.com:6666,2,0,"peer1",1`
4. Set the number of configured remote peers to 1 with the command `AT*ADNRP=1,1`
5. Restart the module with the AT command `AT*AMWS=0,0,0,0,1,0`
6. The module will now restart and associate with the access point and use the configured static IP settings. When associated, it will try to connect to the remote peer test.connectblue.com on TCP port 6666. The remote peer name will be resolved using the configured DNS server.

12.3.8 Example 8, Enable remote configuration

This example describes how to enable remote configuration, i.e. how to enter AT mode from a remote peer. By default this functionality is disabled because it may pose a security risk. If remote configuration is allowed, any remote peer may enter AT mode using the configured escape sequence. From there, all configuration settings are exposed. With this in mind the following steps are required to enable remote configuration.

1. Configure WLAN and IP settings.
2. Configure one or more remote TCP peers or enable the TCP listener (UDP peers don't make sense because it is a one way communication channel).
3. Enable remote configuration with the command `AT*ACCB=1,1`
4. Let the module associate with the network.
5. From any of the remote TCP peers send the escape sequence to enter AT mode (for more information, see Chapter 2). Alternatively connect to the configured TCP listener and send the escape sequence. The remote peer is now in AT mode and all AT commands are available. Several remote peers can be in AT mode at the same time without affecting the communication with the other peers.
6. When configuration is finished, leave AT mode with the command `AT*ADDM`

12.4 Use Cases

The aim of these uses cases is to describe what to configure in different scenarios.

12.4.1 Use case 1, Sensor network, infrastructure, asynchronous

12.4.1.1 Problem description

An industry needs to monitor the air quality and humidity in a large assembly hall. They have concluded that they need to place 20 sensors on different locations in the assembly hall. They want the sensors to be battery powered and report the samplings wirelessly. The assembly hall already has an access point ready. The sensors report data every 10 seconds. The data packet sent is 1kb.

Security: WPA2 PSK.
Data delivery: All values are as important.

12.4.1.2 Solution

Using an access point is preferable in this scenario since the devices will be battery powered. An infrastructure network provides a lot better power saving properties than an ad-hoc network.

Using WPA2 PSK is no problem and we can follow Example 6, WLAN Connection with WPA2 Encryption to enter the correct parameters.

Since all values are important we choose a TCP connection for sending the data. This means that somewhere on the network there has to be a computer with an open port accepting the connections from the modules. We set up the connection parameters by following Example 2, Enable DHCP and configure a Remote Peer.

The short interval of 10 seconds for every new packet means that we should not make the module disconnect after a period of idle since booting up and scanning uses a lot of energy as well as takes time.

12.4.2 Use case 2 Sensor network, infrastructure, polled

12.4.2.1 Problem description

The same company as in Use case 1 has a number of other sensors that they want to request data from at certain times. For instance, when the humidity rises above a certain level based on the values from Use case 1, the server starts to request a number of other properties from sensors rigged around the assembly hall.

Security: WPA2 PSK
Data delivery: Current values the most important.

12.4.2.2 Solution

The serial port adapter have their UDP Receiver activated and a UDP peer set to send data to the server.

The server will request data from a specific sensor with a data packet that includes the sensor id and the register of the sensor it wants data from. The data will be sent to all sensors with UDP but only the sensor with the targeted id will respond.

12.4.3 Use case 3, Service access, ac-hoc

12.4.3.1 Problem description

A series of weather stations are established to continuously gather data. The stations have access to the power grid but the sensors needs to be placed on high poles for best data input. Every second week a maintenance guy will stop by every station to download the gathered data. To save the maintenance guy from having to climb up to the sensors for every station a wireless network is setup so that the data can be read from the ground via a PDA.

Security: None
Data delivery: All values are important

12.4.3.2 Solution

The weather station will use the serial port adapter in an ac-hoc mode. The serial port adapter will have an ac-hoc network running and a TCP Listener active for incoming connections. When the values need to be read, the PDA will connect to the ad-hoc network. The PDA will get an ip-address via the built-in DHCP server in the serial port adapter. Once the PDA has its ip-address it will connect to the TCP port and send a request for data to the system controlling the serial port adapter. The underlying system will respond by sending the last week's stored data.

12.5 Serial Connection

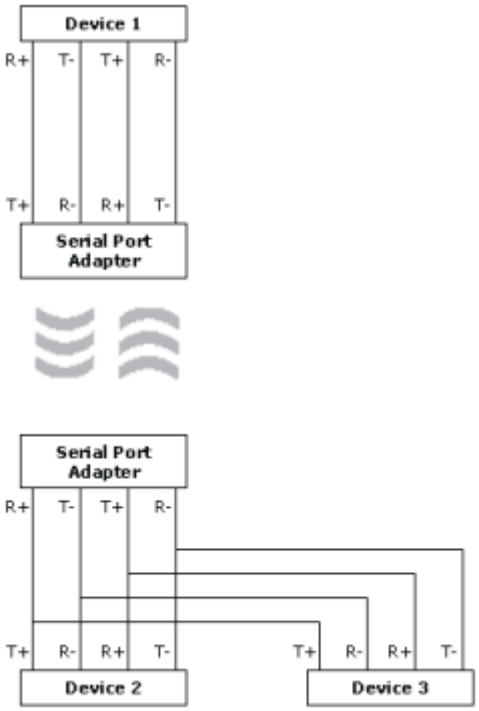
For details on how to set the specific serial communications protocol please see the specific serial settings AT commands: AT*AMSIT Serial Interface Type and AT*AMRS RS-232 Settings.

12.5.1 RS232

The serial port adapter can be used with an RS232 connection.

12.5.2 RS422

The OWSP451 can be used with an RS422 connection.
For four-wire RS422 multi-drop, the following connection setup shall be used:

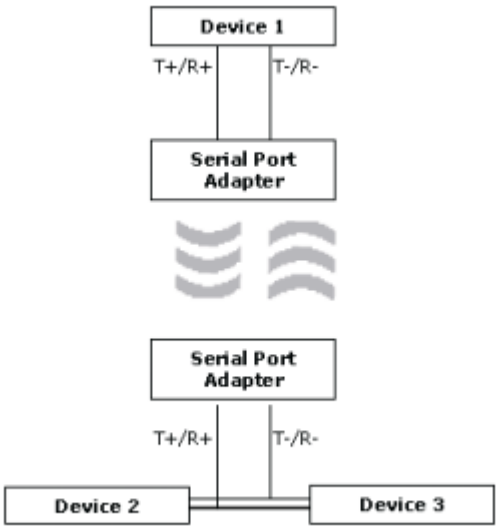


> ⚠ The definition of R+/R-,T+/T- may vary between manufacturers.

12.5.3 RS485

The OWSP451 can be used with an RS485 connection.

For two-wire RS485 the following connection setup shall be used:



> ⚠ The definition of R+/R-,T+/T- may vary between manufacturers.

13 AT Command Reference

The "store" variable that is used in some commands will not be returned when performing a read.

13.1 Standard AT Commands

13.1.1 AT Attention Command

Syntax	Description
AT<CR>	Attention command determining the presence of a DCE, i.e. the serial port adapter.

Responses	Description
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.2 AT* List Available Commands

Syntax	Description
AT*<CR>	List available commands

Responses	Description
<CR><LF><cmd1><CR><LF><cmd2><CR><LF>...<CR><LF>OK<CR><LF>	List of available commands
<CR><LF>ERROR<CR><LF>	Error response

13.1.3 ATZ

Syntax	Description
ATZ<CR>	This command does nothing. For backwards compatibility only

Responses	Description
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error Response

13.1.4 AT&F Restore to Factory Settings

Syntax	Description
AT&F<CR>	This command instructs the unit to set all parameters to their defaults as specified by the manufacturer. Factory settings can be specialized during production.

Responses	Description
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.5 AT&F0 Restore to Factory Settings

Syntax	Description
AT&F0<CR>	See description of the AT&F command.

Responses	Description
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.6 AT&F1 Restore to Static Default Settings

Syntax	Description
AT&F1<CR>	This command instructs the unit to set all parameters to their hardcoded static defaults as specified by connectBlue.

Responses	Description
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.7 ATE Echo Off

Syntax	Description
ATE<CR>	This command turns off character echoing from the DTE when in AT mode.

Responses	Description
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.8 ATE Echo On/Off

Syntax	Description
ATE<echo_on><CR>	This command configures whether or not the unit echoes characters received from the DTE when in AT mode.
ATE?	Read current echo setting.

Parameters	Type	Description
echo_on	integer	0 = Unit does not echo characters during command state and online command state.1 = Unit echoes characters during command state and online command state.

Responses	Description
<CR><LF>echo_on<CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.9 ATQ Result Codes On/Off

Syntax	Description
ATQ<result_off><CR>	The setting of this parameter determines whether or not the unit transmits result codes to the DTE. When result codes are being suppressed, no portion of any intermediate, final, or unsolicited result code – header, result text, line terminator, or trailer – is transmitted. Information text transmitted in response to commands is not affected by the setting of this parameter.
ATQ?	Read current result code setting.

Parameters	Type	Description
result_off	integer	0 = Unit transmits result codes. 1 = Result codes are suppressed and not transmitted

Responses	Description
<CR><LF>result_off<CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.10 ATS2 Escape Character

Syntax	Description
ATS2=<esc_char><CR>	Configure the escape character used to switch the unit from data mode to AT mode.
ATS2?	Read escape character

Parameters	Type	Description
esc_char	integer	0...255 (Note: The escape sequence will be the value repeated three times. I.e. "///".)

Responses	Description
<CR>>LF>esc_char<CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.11 ATS3 Command Line Termination Character

Syntax	Description
ATS3=<line_term><CR>	Write command line termination character. This setting changes the decimal value of the character recognized by the DCE from the DTE to terminate an incoming command line. It is also generated by the DCE as part of the header, trailer, and terminator for result codes and information text along with the S4 parameter. The previous value of S3 is used to determine the command line termination character for entry of the command line containing the S3 setting command. However, the result code issued shall use the value of S3 as set during the processing of the command line. For example, if S3 was previously set to 13 and the command line "ATS3=30" is issued, the command line shall be terminated with a CR, character (13), but the result code issued will use the character with the ordinal value 30 in place of the CR.
ATS3?<CR>	Read command line termination character.

Parameters	Type	Description
line_term	integer	0...127 (13, CR is default)

Responses	Description
<CR><LF>line_term<CR><LF>OK<CR><LF>	Successful read response
<line_term><LF>OK<line_term><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.12 ATS4 Response Formatting Character

Syntax	Description
ATS4=<term><CR>	Write response formatting character. This setting changes the decimal value of the character generated by the DCE as part of the header, trailer, and terminator for result codes and information text, along with the S3 parameter. If the value of S4 is changed in a command line, the result code issued in response to that command line will use the new value of S4.
ATS4?	Read response formatting character.

Parameters	Type	Description
term	integer	0...127 (10, LF is default)

Responses	Description
<CR><LF>term<CR><LF>OK<CR><LF>	Successful read response
<CR><term>OK<CR><term>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.13 ATS5 Backspace Character

Syntax	Description
ATS5=<backspace><CR>	Write backspace character. This setting changes the decimal value of the character recognized by the DCE as a request to delete from the command line the immediately preceding character.
ATS5?	Read backspace character.

Parameters	Type	Description
backspace	integer	0...127 (8, BS is default)

Responses	Description
<CR><LF>backspace<CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.14 ATS General Settings S Register Manipulation

Syntax	Description
ATS<register>=<value><CR>	Write to a general settings S register.
ATS<register>?	Read from a general settings S register.

Parameters	Type	Description
register	integer	Any of the registers described below.
value	Interger	-2147483648...2147483647. Valid values for each register is listed below.

Responses	Description
<CR><LF>value<CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.1.14.1 Wireless LAN registers

Register	Module	Default	Description
3000	All	0	WLAN preamble. 0 = Long preamble 1 = Short preamble
3001	All	0	WLAN beacon listen interval in units of beacon interval. 0...16 (default 0, listen on all beacons)
3002	All	50	WLAN minimum scan time in milliseconds on each channel. 0...65535
3003	All	200	WLAN maximum scan time in milliseconds on each channel. 0...65535
3004	All	0	WLAN scan type. 0 = Active scan 1 = Passive scan
3005	All	38	WLAN lower RSSI trigger value to trigger a rescan. In dBm + offset 128 38...113 (-90 dBm ...-15 dBm)
3006	All	16	Averaging depth for the RSSI trigger 0...16 (default 16, 0 means no depth)
3007	All	30	WLAN lower lost beacon value to trigger a rescan. The maximum number of lost beacons before a rescan happens. 1...32
3008	All	32	Averaging depth for the lost beacon trigger 1...32
3009		0	Deprecated, do not modify.
3010		0	Deprecated, do not modify.
3011	All	100	Beacon Period of the BSS Descriptor of the ESS to Join or Start a network in IBSS. Value in milliseconds.
3012	All	600	The time limit, in units of beacon intervals, after which the Join procedure will be terminated. 1...65535
3013	All	1	Turns DTPA (Dynamic Transmit Power Adaptation) On and off. 0...1
3014	All	145	Max power (See also AT*AMMP Max output power). Valid range 111...145
3015	All	145	Max association power. The maximum transmit power used during the association phase. This value is interpreted just as the AT*AMMP Max output power AT command. 111...145
3016	All	0	Enable Bluetooth co-existence pins on module. 0 = Pins disabled 1 = Pins enabled
3017	OWSPA311g	0	Enable internal pull-down resistors on Bluetooth coexistence pins on module. Only used if S3016=1. 0 = Pull-downs disabled (default) 1 = Pull-downs enabled
3018-3021			Reserved, do not modify.
3022	All	1	Enable DTIM in power save. If DTIM is enabled and module in power save, the access point sends an indication when new data is available. If disabled the module polls for data every beacon listen interval (beacon listen interval is configured in S register 3001). 0 = DTIM disabled 1 = DTIM enabled
3023	All	0	QoS enable. 0 = Disabled 1 = Enabled
3024	OWS451	2347	RTS (Request to send) Threshold. 0...2347

3025	OWS451	2346	Fragmentation Threshold. 0...2346
3026	OWS451	0	PS Listen Interval. Listen interval in beacons. 0...100
3027	OWS451	50	PS Fast PSP Timeout. Timeout in ms before the baseband enters Power Save. 0...500
3028	OWS451	0	Antenna Receive Diversity. If two antennas are used, this should be enabled. 0 = Disabled 1 = Enable receive antenna diversity

13.1.14.2 SPA registers

Register	Module	Default	Description
4000	All	600	Number of milliseconds to wait before stop mode is entered after a valid stop mode condition is detected. Lowering this value will minimize power consumption but affect system responsiveness in a negative way. 0...360000000
4001			Reserved, do not modify.
4002			Reserved, do not modify.
4003	All	0	WPA key input mode. Controls how the WPA key is parsed and interpreted. 0 = Auto 1 = ASCII 2 = Hexadecimal Auto mode will try to determine if it the input is an ASCII key or a HEX key by looking at the contents.
4004	All	0	LED scheme. Can be used to disable the status LED output pins to save power. 0 = LED status always on 1 = LED status disabled when module is in stop mode. 2 = LED status always off If the module is mounted on a Module Adapter, the always off setting will result in the LED being red which is the default LED color when the LEDs are not driven by the module.
4005	All	1	Put CPU in idle mode. This will conserve power but will but affect system responsiveness and data throughput in a negative way, especially at baud rates over 230400 bps. 0 = Idle mode off 1 = Idle mode on
4006	All	0	Keep remote peers connected when entering AT mode. 0 = Disconnect remote peers 1 = Keep remote peers connected
4007	All	0	Configure module to automatically put local peer (UART) in AT mode at startup. 0 = Local peer in data mode at startup 1 = Local peer in AT mode at startup
4008	All	6000	Ad-hoc timeout. Time before a single unit in an ad-hoc network tries a rescan to find an existing network. Value in milliseconds. 6000...2147483647
4009	All	0	Delayed association. Time to wait before an association attempt is initiated. Value in milliseconds. 0 = no delay 0...2147483647
4010	All	60	LLDP send interval. The module will per default send information in LLDP frames with its current setup and peers. This can also be used to stay alive on access points that do not properly wake the module before a disassociation. Value in seconds. 0 = Do not send. 0...2147483647
4011	All	3	LLDP information level. The levels are additive. I.e. level 2 include level 0 and 1 as well as level 2. 0...3 0 = Send MAC address and IP address 1 = Send system name (user defined hostname), system description (version information) and announce station capability. 2 = Send services (Announce tcp listener and udp receiver ip and port). 3 = Send peer information (information regarding the currently connected peers).
4012	All	58	RSSI threshold value for activation of background scans. When associated access point signal strength drops below specified value the system starts to do backgrounds scans. Roaming is done if another access point with better signal strength is found. 38...113 (0dBm is 128. 58 – 128 = --70dBm)
4013		0	LED scheme (reserved) 0..1
4014	All	0	Enable UART fallback mode. As long as switch 0 is pressed/activated UART settings are temporarily changed to 57600 baud, 8n1, and hardware flow control. Settings are restored when button is released. Switch 0 status is sampled every second. 0 = off 1 = on

4015	OWS451	0	Disable Ad-Hoc network creation. Only allow the module to scan and join existing networks. 0 = off - create an Ad-Hoc network if no existing is found, this is the default behavior. 1 = on - scan once, never create an Ad-Hoc network, only join existing ones, scan only channel selected by AT*AGCH. 2 = on - scan every Ad-hoc timeout (ATS4008, typical 10 seconds), will never create an Ad-Hoc network only join existing ones, scan only channel selected by AT*AGCH. 3 = on - scan every Ad-hoc timeout (ATS4008, typical 10 seconds), will never create an Ad-Hoc network only join existing ones, scan all channels defined by AT*AGCL. 4 = on - do not scan and connect, only allow others to join the network created by the module.
4016	OWS451	30000	Max Connection Retry Delay. Delays the re-connections in managed mode if the access point can't be found. The delay have a default value of 30000 ms. By setting it to 0 the delay will be disabled. The behavior is like this: 1,1,1,1,2,2,2,4,4,8,16...MAX_TIMER. 0 = no delay (re-connect as fast as possible) 1...2147483647
4017	OWS451	7	Max number of remote peers. 0...7
4018	OWS451	0	Reserved, do not modify.

13.1.14.3 Network registers

Register	Module	Default	Description
5000	All	0	Turn on/off TCP keepalive packets. It is important to understand that sending frequent keepalive packets usually isn't a good solution to detect dropped connections. Detecting dead links should be done on a higher level, i.e. in the user application protocol. There is a lot of information available on the subject on the web. 0 = TCP keepalive packets turned off 1 = TCP keepalive packets turned on
5001	All	7200000	Time in milliseconds for a TCP connection to be idle before a keepalive packet is sent. 0...2147483647 (default 7200000 = 2 hours)
5002	All	75000	Time in milliseconds between keepalive packets after a keepalive packet has been lost. 0...2147483647 (default 75000 = 75 seconds)
5003	All	9	Number of lost keepalive packets to wait before a TCP connection is resetted. 1...255
5004	OWS451	0	Specify UDP sender source port. Normally the source port is random. 0 = random port 1...65535 use this port number
5005	OWS451	5000	Delay in milliseconds before sending GARP (gratuitous ARP) message. 0...2147483647

13.2 Link Layer Commands

13.2.1 AT*AGAM Authentication Mode

Syntax	Description
AT*AGAM=<amode>,<store><CR>	Write authentication mode.
AT*AGAM?	Read authentication mode

Parameters	Type	Description
amode	integer	0 = Open (default) 1 = Shared secret 2 = WPA/WPA2 PSK 3 = LEAP 4 = PEAP
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AGAM:<amode><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

Model	Constraint
cB-OWSPA311g	PEAP is not supported

13.2.2 AT*AGEM Encryption Mode

Syntax	Description
AT*AGEM=<emode>,<store><CR>	Write encryption mode
AT*AGEM?	Read encryption mode

Parameters	Type	Description
emode	integer	0 = None (default) 1 = WEP64 2 = WEP128 3 = TKIP 4 = AES/CCMP
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AGEM:<emode><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.3 AT*AGSM Security Mode

Syntax	Description
AT*AGSM=<smode>,<store><CR>	Write security mode. Security mode is a shortcut for setting a combination of the authentication and encryption modes. Sending a "AT*AGSM=3" command is therefore the equivalent of sending the commands: "AT*AGAM=2" and "AT*AGEM=3". If a "AT*AGSM?" command is sent the DCE will return 255 if the current settings does not match any of the predefined values.
AT*AGSM?	Read security mode

Parameters	Type	Description
smode	integer	0 = No security (default) (AM=0,EM=0) 1 = Shared-WEP64 (AM=1,EM=1) 2 = Shared-WEP128 (AM=1,EM=2) 3 = WPA-PSK-TKIP (AM=2,EM=3) 4 = WPA2-PSK-AES/CCMP (AM=2,EM=4) 5 = LEAP-WPA2 (AM=3,EM=4) 6 = LEAP-WEP128 (AM=3,EM=2)
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AGSM:<smode><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.4 AT*AGOM Operational Mode

Syntax	Description
AT*AGOM=<omode>,<store><CR>	Write operational mode, i.e. if the device is operating in an ad-hoc environment or a predetermined infrastructure with access points.
AT*AGOM?	Read operational mode.

Parameters	Type	Description
omode	integer	1 = Managed (infrastructure) (default) 2 = Ad-Hoc
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AGOM:<omode><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.5 AT*AGFP Encryption/Authentication Key

Syntax	Description
AT*AGFP=<key>,<store><CR>	Write encryption/authentication key at index 1. This command is a shortcut for AT*AGFPWI=1,<key>,<store>.

Parameters	Type	Description
key	string	Any string value
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.6 AT*AGFPWI Write Encryption/Authentication Key (with Index)

Syntax	Description
AT*AGFPWI=<keyindex>,<key>,<store><CR>	Write encryption/authentication key.

Parameters	Type	Description
keyindex	integer	1...4
key	string	Any string value
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.7 AT*AGAFP Active Encryption/Authentication Key

Syntax	Description
AT*AGAFP=<keyindex>,<store><CR>	Write active encryption/authentication key.
AT*AGAFP?	Read active encryption/authentication key.

Parameters	Type	Description
keyindex	integer	1...4 (1 default)
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AGAFP:<keyindex><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.8 AT*AGUN Username

Syntax	Description
AT*AGUN=<username>,<store><CR>	Write the username.
AT*AGUN?	Read the username.

Parameters	Type	Description
username	string	The username to use with authentication servers. Used when LEAP or PEAP is enabled. See AT*AGAM Authentication Mode.
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AGUN:<username><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.9 AT*AGDN Domain Name

*Syntax	Description
AT*AGDN=<domain name>,<store><CR>	Write the domain name.
AT*AGDN?	Read the domain name.

Parameters	Type	Description
domain name	string	The username to use with authentication servers. Used when LEAP or PEAP is enabled. See AT*AGAM Authentication Mode.
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	*Description
<CR><LF>*AGDN:<domain name><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.10 AT*AGSSID SSID

Syntax	Description
AT*AGSSID=<ssid>,<store><CR>	Write SSID of the access point.
AT*AGSSID?	Read SSID of the access point.

Parameters	Type	Description
ssid	string	Any string value (max length 32 bytes)
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AGSSID:<ssid><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.11 AT*AGBSSID BSSID

Syntax	Description
AT*AGBSSID?	Read BSSID of the connected access point. Note; module has to be configured to remain connected when in AT-mode to read out BSSID. See S-register 4006.

Responses	Description
<CR><LF>*AGBSSID:<bssid><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.12 AT*AGRSS RSSI Value

Syntax	Description
AT*AGRSS?	Read RSSI value of the connection. ERROR is returned if the module is not connected.

Parameters	Type	Description
rssi	integer	RSSI value. 28...138 where value is dBm value + 128, i.e. 128 = 0dBm. If no connection is established, the response is an error response.

Responses	Description
<CR><LF>*AGRSS:<rssi><CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.13 AT*AGCH Channel Number

Syntax	Description
AT*AGCH=<ch_no>,<store><CR>	Write channel number to use.
AT*AGCH?	Read channel number in use

Parameters	Type	Description
ch_no	integer	0 = Auto (default)1...11, 1...14 or 36...48 depending on regulatory domain setting
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AGCH:<ch_no><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.14 AT*AGSCAN

Syntax	Description
AT*AGSCAN?	Scan the surroundings for networks. The command will return 0...48 networks in the immediate surroundings, then return OK.

Parameters	Type	Description
bssid	mac_addr	The MAC address of the access point
op_mode	integer	1 = Infrastructure 2 = Ad-hoc
ssid	string	The SSID name of network
channel	integer	The channel the network uses
rssi	integer	Signal strength value for the network

encryption	integer	0 = No encryption 1 = WEP 2 = WPA 3 = WPA2/RSN
information_element	string	Hexadecimal string with the information element for WPA and RSN networks. Will not be present with WEP networks or networks without encryption.

Responses	De
<CR><LF>*AGSCAN:<bssid>,<op_mode>,<ssid>,<channel>,<rssi>,<encryption>,<information_element><CR><LF>OK<CR><LF>	Su rea res
<CR><LF>ERROR<CR><LF>	Err res

Note: AT*AGSCAN will return ERROR if channel list set by AT*AGCL is empty.

13.2.15 AT*AGRTE Data Rate and Link Adaptation

Syntax	Description
AT*AGRTE=<data_rate >,<link_adaptation>,<store><CR>	Write data rate and link adaptation settings.
AT*AGRTE?	Read current data rate and link adaptation settings.

Parameters	Type	Description
data_rate	integer	1 = 1 Mbit 2 = 2 Mbit 3 = 5.5 Mbit 4 = 6 Mbit 5 = 9 Mbit 6 = 11 Mbit 7 = 12 Mbit 8 = 18 Mbit 9 = 24 Mbit (default) 10 = 36 Mbit 11 = 48 Mbit 12 = 54 Mbit N-rates (using 20 MHz and 800 ns Guard Interval) is only supported by cB-OWS451 13 = 6.5 Mbit (MCS0) 14 = 13 Mbit (MCS1) 15 = 19.5 Mbit (MCS2) 16 = 26 Mbit (MCS3) 17 = 39 Mbit (MCS4) 18 = 52 Mbit (MCS5) 19 = 58.5 Mbit (MCS6) 20 = 65 Mbit (MCS7)
link_adaptation	integer	0 = Link adaptation off. The set data_rate will always be used. 1 = Link adaptation on. The data_rate used will automatically be adjusted depending on the operation environment. Maximum rate used will be data_rate (default). If link adaptation is turned off, the configured data rate will be used for data transmissions. If data has to be retransmitted, the module will decrease the data rate in steps until the remote side receives it.
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AGRTE:<data_rate>,<link_adaption><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.2.16 AT*AGCL Channel List

Syntax	Description

AT*AGCL=<ch1>,<ch2>,...,<chN>,<store><CR>	Write the channel list to use. This list also specifies the scan order.
	The number of channels to specify is dependent on the regulatory domain set. See below for channel list lengths.
	If you don't want to use all positions, pad list with zeros.
	
	Channel list length for the regulatory domains:
	
	• World = 11
	• FCC = 11
	• ETSI = 13
	• TELEC = 14
	• U-NII band 1 = 4
	
	Example 1: If regulatory domain is set to World + U-NII band 1, then the number of channels to specify is 11 + 4 = 15.
	
	`AT*AGCL:6,1,11,2,7,4,9,3,8,5,10,36,40,44,48,1`
	
	Example 2: To use only channel 1,6, and 11 in regulatory domain 'World'.
	
	`AT*AGCL=1,6,11,0,0,0,0,0,0,0,0,0,0,1`

AT*AGCL?	Read channel number in use

Parameters	Type	Description
ch#	integer	0 = No more channels 1...11, 1...14 or 36...48 depending on regulatory domain setting
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AGCL:<ch1>,<ch2>,...,<chN><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

Note: The channels will be scanned in the order they are listed by this command.

13.2.17 AT*AGLN Local Name

AT*AGLN manipulates the same setting as AT*ANHN Hostname. This command is included for compatibility reasons, see AT*ANHN Hostname for description.

13.3 Network Layer Commands

13.3.1 AT*ANIP IP Settings

Syntax	Description
AT*ANIP=<ip_addr>,<netmask>,<gw>,<store><CR>	Write IP address and related information. The information set by this command will not be valid until after the module is restarted. The AT*ANIP? Command will therefore return the old IP settings until you restart the module.
AT*ANIP?	Read IP address and related information currently in use.

Parameters	Type	Description

ip_addr	ip_addr	IP address for the device (default 192.168.0.99)
netmask	ip_addr	Netmask for the device (default 255.255.0.0)
gw	ip_addr	The IP address of the gateway (default 192.168.0.1)
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*ANIP<ip_addr>,<netmask>,<gw><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.3.2 AT*ANDHCP DCHP Activation

Syntax	Description
AT*ANDHCP=<on>,<store><CR>	Activate/deactivate DHCP. If activated, this will take precedence over settings made with AT*ANIP.
AT*ANDHCP?	Read the current DHCP setting

Parameters	Type	Description
on	integer	0 = Use static IP address (default) 1 = Acquire an IP address using DHCP 2 = DHCP Server. Use static IP address + act as DHCP server.
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*ANDHCP:<on><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.3.3 AT*ANHN Hostname

Syntax	Description
AT*ANHN=<hostname>,<store><CR>	Write the hostname used with dynamic DNS.
AT*ANHN?	Read the hostname used with dynamic DNS.

Parameters	Type	Description
hostname	string	Any string (default is "cB-OWS451" for the cB-OWS451)
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*ANHN:<hostname><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response

<CR><LF>ERROR<CR><LF>	Error response

13.3.4 AT*ANDNS DNS Settings

Syntax	Description
AT*ANDNS=<dns1>,<dns2>,<store><CR>	Write the name server information.
AT*ANDNS?	Read the name server information.

Parameters	Type	Description
dns1	ip_addr	Primary DNS server. If DNS is not used, set this parameter to 0.0.0.0 (default 0.0.0.0).
dns2	ip_addr	Secondary DNS server. If DNS is not used or if only one server is used, set this parameter to 0.0.0.0 (default 0.0.0.0).
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*ANDNS:<dns1>,<dns2><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.4 Data Mode Commands

13.4.1 AT*ADDM Enter Data Mode

Syntax	Description
AT*ADDM<CR>	Enter data mode.

Responses	Description
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.4.2 AT*ADMRP Read Maximum Number of Remote Peers

Syntax	Description
AT*ADMRP?<CR>	Read max number of remote peers. This is a static value and the maximum sum of all TCP and UDP connections.

Parameters	Type	Description
nr_of_peers	integer	1...7 (default 7)

Responses	Description
<CR><LF>*ADMRP:<nr_of_peers><CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.4.3 AT*ADNRP Number of Remote Peers

Syntax	Description
AT*ADNRP=<nr_of_peers>,<store><CR>	Write preferred number of remote peers.
AT*ADNRP?	Read the number of remote peers.

Parameters	Type	Description
nr_of_peers	integer	Any value between 0 and the response from AT*ADMRP
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*ADMRP:<nr_of_peers><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.4.4 AT*ADRDRP Read Default Peer

Syntax	Description
AT*ADRDRP=<peer_id><CR>	Read the default peer

Parameters	Type	Description
peer_id	integer	Any value between 0 and the response from AT*ADMRP - 1
address	string	Address to the service on the remote peer. On the form of <protocol>://ipaddr:port. I.e. tcp://192.169.0.1:5130
conn_scheme	integer	0 = Unused 1 = Connect on data (Connects when there is something to send, then remains connected) 2 = Always connected (Connects right after power on)
update_on_incoming	integer	Reserved for future use.
name	string	A string with a user defined name of the peer.

Responses	Description
<CR><LF>*ADRDRP:<address>,<conn_scheme>,<update_on_incoming>,<name>,<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.4.5 AT*ADWDRP Write Remote Peer Information

Syntax	Description
AT*ADWDRP=<peer_id>,<address>,<conn_scheme>,<reserved>,<name>,<store>	Write information for a remote peer.

Parameters	Type	Description
peer_id	integer	Any value between 0 and the response from AT*ADMRP - 1
address	string	Address to the service on the remote peer. On the form of <protocol>://ipaddr:port. I.e. tcp://192.169.0.1:5130

conn_scheme	integer	0 = Unused 1 = Connect on data (Connects on first incoming UART data, then remains connected). Also see chapter Cache. 2 = Always connected (Connects right after power on)
reserved	integer	Reserved for future use. Use 0
name	string	A string with a user defined name of the peer.
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.5 Informational Commands

13.5.1 AT*AILBA Read MAC address

Syntax	Description
AT*AILBA?<CR>	Read the MAC address of the device.

Parameters	Type	Description
mac_address	mac_addr	The MAC address of the device

Responses	Description
<CR><LF>*AILBA:<mac_address><CR><LF>OK<CR><LF>	Successful response. <mac_address> not enclosed in " ".
<CR><LF>ERROR<CR><LF>	Error response

13.5.2 AT*AILVI Local Version Information

Syntax	Description
AT*AILVI?<CR>	Read local version information

Parameters	Type	Description
manufacturer	string	Serial port adapter manufacturer, example "connectBlue"
spa_sw_version	string	Serial port adapter software version, example "2.2.5 [11:32:15,Sep 14 2010]"
wlan_driver_version	string	WLAN host driver version, example "2.4"
wlan_fw_version	string	WLAN firmware version, example "2.1.9.100"
wlan_hw_manufacturer	string	WLAN hardware manufacturer, example "RPS"

Responses
<CR><LF>*AILVI:<manufacturer>,<spa_sw_version>,<wlan_driver_version>,<wlan_fw_version>,<wlan_hw_manufacturer><CR><LF>O

<CR><LF>OK<CR><LF>
<CR><LF>ERROR<CR><LF>

13.5.3 AT*AILTI Read Type Information

Syntax	Description
AT*AILTI?<CR>	Read the type information for the device

Parameters	Type	Description
major	integer	The major number of the type information. 1 = Bluetooth product 2 = WLAN product 3 = 802.15.4 product This product should return 2 as the major number.
minor	integer	The minor number of the type information. 0 = cB-OWSPA311g 1 = cB-OWS451

Responses	Description
<CR><LF>*AILBA:<major>,<minor><CR><LF>OK<CR><LF>	Successful response.
<CR><LF>ERROR<CR><LF>	Error response

13.6 Miscellaneous Commands

13.6.1 AT*AMRS RS-232 Settings

Syntax	Description
AT*AMRS=<baud_rate>,<data_bits>,<stop_bits>,<parity>,<flow_control>,<reserved>,<store><CR>	Write the RS-232 settings. Automatically stores the settings.
AT*AMRS?	Read the RS-232 settings.

Parameters	Type	Description
baud_rate	integer	Sets the baud rate. 1 = 300 2 = 1200 3 = 2400 4 = 4800 5 = 9600 6 = 19200 7 = 38400 8 = 57600 (default) 9 = 115200 10 = 230400 11 = 460800 12 = 921600 13 = 1382400 14 = 2764800 > 300 = set to this baud rate
data_bits	integer	Sets the data bits. 1 = 8 bits (default) 2 = 7 bits 3 = 6 bits 4 = 5 bits

stop_bits	integer	Sets stop bit. 1 = 1 bit (default) 2 = 2 bits
parity	integer	Sets parity. 1 = None (default) 2 = Odd 3 = Even
flow_control	integer	Flow control settings 1 = cts/rts (default) 2 = None
reserved	integer	Reserved for future use. Use 0.
store	integer	0 = Do not store 1 = Store (will store between reboots)

Model	Constraint
cB-OWS451	5-7 data bits not supported. Baud rate of 300 bits/s not supported.
For standard baud rates an accuracy of 0.06% or better is achieved. For non-standard baud rates an accuracy of 0.18% or better is achieved	

Note: If you do not set one of the predefined baud rates the serial port adapter will try to use the value you set. It calculates a "true baud rate" that it can use, taking into account the UART clock. If the original value that you tried to set is within 2% of this "true baud rate", the module will return OK. Otherwise it will return ERROR and no baud rate change will take place after reboot.

Responses	Description
<CR><LF>*AMRS<baud_rate>,<data_bits>,<stop_bits>,<parity>,<flow_control><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.2 AT*AMSIT Serial Interface Type

Syntax	Description
AT*AMSIT=<type>,<store><CR>	Write the serial interface type.
AT*AMET?	Read the serial interface type.

Parameters	Type	Description
type	integer	The serial interface type. Possible values: 1 = RS232 (default) 2 = RS422 3 = RS485
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMSIT:<type><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.3 AT*AMET Escape Sequence Timing Settings

Syntax	Description
AT*AMET=<min_time_before>,<min_time_after>,<store><CR>	Write the escape sequence timing settings. For an escape sequence to be valid, a period of no data activity is required before and after the escape sequence. This command reads the minimum time of no data activity required before and after the escape sequence.
AT*AMET?	Read the escape sequence timing settings.

Parameters	Type	Description
min_time_before	integer	50...5000ms (1000 default)
min_time_after	integer	50...5000ms (1000 default)
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMET:<min_time_before>,<min_time_after><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.4 AT*AMWS Watchdog Settings

Syntax	Description
AT*AMWS=<reserved1>,<inactivity_timeout>,<reserved3>,<reserved4>,<reset>,<store><CR>	Write the watchdog settings. The watchdog functionality will disconnect from a remote peer if one of the given conditions are met.
AT*AMWS?	Read the watchdog settings

Parameters	Type	Description
reserved1	integer	Reserved for future use. Use 0.
inactivity_timeout	integer	Disconnect WLAN after this long idle time in seconds (default 0, i.e. inactivated)
reserved3	integer	Reserved for future use. Use 0.
disconnect_reset	integer	Will reset the module if all peers are disconnected. 1 = On, 0 = Off, Default = 0
reset	integer	1 Will reset the unit immediately. (Will not store nor return any response)
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMWS:<reserved1>,<inactivity_timeout>,<reserved3>,<disconnect_reset>,<reset><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response

<CR><LF>ERROR<CR><LF>	Error response

13.6.5 AT*AMPM Power Mode

Syntax	Description
AT*AMPM=<power_mode>,<store><CR>	Write the operational power mode
AT*AMPM?	Read the operational power mode

Parameters	Type	Description
power_mode	integer	1 = Online 2 = Sleep mode (default) 3 = Stop mode
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMPM:<power_mode><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.6 AT*AMMP Max output power

Syntax	Description
AT*AMMP=<max_power>,<store><CR>	Write the max power settings. This will set both the power used during association and when associated. See also S-register 3014 and 3015.
AT*AMMP?	Read max power setting. Reads the power used in associated mode.

Parameters	Type	Description
max_power	integer	Actual dBm + 128. Valid range is between 128...145 (0dBm...17dBm). Default 145.
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMPM:<max_power><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.7 AT*AMTU MTU Size

Syntax	Description
AT*AMTU=<mtu_length>,<store><CR>	Write the network MTU size.
AT*AMTU?	Read the network MTU size.

Parameters	Type	Description

mtu_length	integer	Valid range is 64...1472 (1472 default)
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMTU:<mtu_length><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.8 AT*AMGD General Purpose Data

Syntax	Description
AT*AMGD=<data>,<store><CR>	Write general-purpose data.
AT*AMGD?	Read general-purpose data

Parameters	Type	Description
data	string	Any kind of data. Maximum size is 32 bytes.
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMGD:"<data>"<CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.9 AT*AMTL TCP Listener Activation

Syntax	Description
AT*AMTL=<port>,<tl_on>,<store><CR>	Enable or disable the TCP listener.
AT*AMTL?	Read TCP listener activation status.

Parameters	Type	Description
port	integer	A port number, 0...65535
tl_on	integer	0 = Disabled (default) 1 = Enabled
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMTL:<port>,<tl_on><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.10 AT*AMUR UDP Receiver Activation

Syntax	Description
AT*AMUR=<port>,<ul_on>,<store><CR>	Enable or disable the UDP receiver.
AT*AMUR?	Read UDP receiver activation status.

Parameters	Type	Description
port	integer	A port number, 0...65535
ul_on	integer	0 = Disabled (default) 1 = Enabled
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMUR:<port>,<ul_on><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.11 AT*AMES Echo server

Syntax	Description
AT*AMES=<enable>,<store><CR>	Control activation of echo server on TCP port 7 and UDP port 7. In case of UDP packages are returned to the port number of sender.
AT*AMES?	Read status of echo server.

Parameters	Type	Description
enable	integer	Status of echo server. Possible values: 0 = off (default) 1 = on
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMES:<enable><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.12 AT*AMDS DSR/DTR Control

Syntax	Description
AT*AMDS=<DTR_on>,<DSR_on>,<store><CR>	Controls how the system utilizes the DSR and DTR pins.
AT*AMDS?	Read the current settings

Parameters	Type	Description
DTR_on	integer	1 = DTR is activated when the module is started (default). 2 = DTR is active if there are one or more active remote peers.
DSR_on	integer	1 = DSR is ignored (default) 2 = Connect and disconnect remote peers. Connects all remote peers when DSR changes from inactive to active. Disconnect all when DSR changes from active to inactive.
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMDS:<DRT_on>,<DSR_on><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.13 AT*AMRD Regulatory Domain Control

Syntax	Description
AT*AMRD=<domain>,<store><CR>	Write regulatory domain
AT*AMRD?	Read the current setting

Parameters	Type	Description
domain	integer	1 = World (2,4 GHz) - default 2 = FCC (2,4 GHz) 3 = ETSI (2,4 GHz) 4 = TELEC (2,4 GHz) 10 = U-NII-1 (5 GHz) The regulatory domain value is built using two parts X + Y. Where Y is the value for 2.4GHz and X is for 5GHz. To build the regularly domain value combine 2.4 and 5GHz channel values like this: Only FCC on 2.4GHz: 0 + 2 = 2 U-NII band 1 + TELEC: 10 + 4 = 14 U-NII band 1 (no 2.4GHz channels): 10 + 0 = 10 All channels for ETSI (both 2.4GHz and 5GHz): 10 + 3 = 13 'World' contains channels: 6, 1, 11, 2, 7, 4, 9, 3, 8, 5, 10 'FCC' contains channels: 6, 1, 11, 2, 7, 4, 9, 3, 8, 5, 10 'ETSI' contains channels: 7, 1, 13, 6, 11, 2, 4, 12, 3, 8, 5, 9, 10 'TELEC' contains channels: 1, 6, 11, 14, 2, 7, 12, 3, 8, 13, 4, 9, 5, 10 'U-NII-1' contains channels: 36, 40, 44, 48
store	integer	0 = Do not store 1 = Store (will store between reboots)

Responses	Description
<CR><LF>*AMRD:<domain><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

Model	Constraint
cB-OWSPA311g	U-NII-1 (5 GHz) Regulatory domain and channels is not supported.

13.6.14 AT*ACCB Configuration over WLAN

Syntax	Description
AT*ACCB=<allow>,<store><CR>	Write allow configuration over WLAN setting.
AT*ACCB?	Read allow configuration over WLAN setting.

Parameters	Type	Description
allow	integer	0 = AT mode can only be entered from the UART (default) 1 = AT mode can be entered from both UART and any connected remote peer

Responses	Description
<CR><LF>*ACCB:<allow><CR><LF>OK<CR><LF>	Successful read response
<CR><LF>OK<CR><LF>	Successful response
<CR><LF>ERROR<CR><LF>	Error response

13.6.15 AT*AMCIO / AT*AMRIO / AT*AMWIO Read/Write IO

Some of the IO pins can be configured and set using AT commands.

In reset the IO pins are input floating. About 1 ms after start, the boot will configure the IO pins for input pull-up which is the Serial Port Adapter default configuration.

AT Command	Description
AT*AMCIO=<io_pin>,<cfg><CR>	Configure IO for input or output.
AT*AMRIO=<io_pin><CR>	Read IO.
AT*AMWIO=<io_pin>,<value>,<CR>	Write IO.

Responses	Description
<CR><LF>OK<CR><LF>	Successful configuration or write response
<CR><LF>ERROR<CR><LF>	Error message.
<CR><LF>*AMRIO: <value><CR><LF>OK<CR><LF>	Successful read response.

Parameters	Type	Value

io_pin	integer	IO pin to configure, read or write. The following pins are available only for reading. 0: UART-DTR 1: SW0 2: Red 3: Green/SW1 4: Blue 5: UART-CTS 6: UART-Tx 7: UART-RTS 8: UART-Rx 9: UART-DSR 19: I2C-Clock/SS1 20: I2C-Data/SS0 The following pins are available for both reading and writing. 10: SPI-Irq 11: SPI-Miso 12: SPI-Clock 13: SPI-Mosi 14: SPI-SS 15: ADC-IN0 16: ADC-IN1 17: ADC-IN2 18: ADC-IN3 See Electrical Mechanical data sheet for details on pins.
Cfg	integer	IO pin configuration 0: Output Push-Pull 1: Input pull-up 2: Input pull-down 3: Input floating
Value	integer	IO pin value to read or write. 0: Inactive 1: Active See Electrical and Mechanical data sheet for details.

Model	Constraint
cB-OWSPA311g	Not supported.
cB-OWS451	Supported in version 2.3.0 or later.

14 Licenses

This product contains software under the following licenses:

```
/*
 * Copyright (c) 2001, 2002 Swedish Institute of Computer Science.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without modification,
 * are permitted provided that the following conditions are met:
 *
 * 1. Redistributions of source code must retain the above copyright notice,
 *    this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright notice,
 *    this list of conditions and the following disclaimer in the documentation
 *    and/or other materials provided with the distribution.
 * 3. The name of the author may not be used to endorse or promote products
 *    derived from this software without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED
 * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
 * MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT
 * SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
 * EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT
 * OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING
 * IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
 * OF SUCH DAMAGE.
 *
 * This file is part of the lwIP TCP/IP stack.
 *
 * Author: Adam Dunkels <adam@sics.se>
 *
 */
```