NOKIA
A032

Wireless LAN Access Point Addendum

NOKIA
CONNECTING PEOPLE

Copyright notices

We reserve the right to make changes and improvements to any of the products described in this guide without prior notice. Nokia is not responsible for any loss of data, income or any consequential damage howsoever caused.

ISSUE 1

Table of contents

1. Introduction

Purpose

This document has been written to serve as an addendum to the existing A032 user manuals. It does not attempt to replace any existing user manual, and is focussed on correcting errors and omissions from those manuals, and documenting features added in recent firmware updates.

Scope

This document describes the configuration and operation of the Access Point (AP) and, where appropriate, the format of external services used by the AP. It does not cover the setting up of a network, or the detailed configuration of any external equipment.

Terms, acronyms and abbreviations

Term	Meaning
WLAN	Wireless LAN IEEE 802.11
AP	Access Point
NAS	Network Access Server
UDP	User-Datagram-Protocol
RFC	Request For Comments
MT	Mobile Terminal (WLAN client)
LAN	Local Area Network
WEP	Wire-Equivalent Privacy
WLAN	Wireless LAN IEEE 802.11

2. Access point parameters

This section describes the changes to AP parameters, and the use of newly added parameters.

Table of parameters

Refer to the A032 user guide for descriptions of how to use the management interfaces.

Name (command line)	Config Web page	Factory default	Valid range	Description
channel	Access Point			Radio channel and domain are linked: The domain parameter selects the regulatory domain governing channel assignment, and is used to constrain the choice of channels. For domain:
		10	1–13	ETSI
		10	1–11	USA and Canada
		10	10–13	France
		14	14	Japan
frag_threshold	n/a	2346	256–2346 (even only)	Fragmentation threshold for 802.11 packets. Frames larger than this value will be broken into multiple smaller packets.

Name (command line)	Config Web page	Factory default	Valid range	Description
beacon_interval	n/a	100	1–65535	Beacon interval in mS
dtim_interval	n/a	5	1–255	Number of beacons between DTIMs
tx_power	n/a	"high"	"low", "low1", "low2", "high"	Access points transmit power level. By default, this is set to maximum, but may be reduced to suit applications with multiple APs.
cca_mode	n/a	"cs_only"	"ed_only", "cs_only", "ed_and_cs", "ed_or_cs"	This setting determines which clear channel assessment (CCA) mode should be used.
ed_threshold	n/a	17	10–127	Energy detection threshold used in CCA.
ed_absolute	n/a	TRUE	TRUE or FALSE	Use Absolute energy detection threshold, or relative to noise floor

Name (command line)	Config Web page	Factory default	Valid range	Description
wep_mode	WEP Advanced WEP	"wep"		This parameter determines the authentication policy of the AP:
			"open"	Accept either WEP or open system
			"wep"	MUST use WEP
			"wifi"	Relaxed form of WEP setting allowing use of shared keys with open system authentication
			"personal"	MUST use specific key WEP (default key not accepted for authentication)
		"local"	"local"	Per-node data stored in the NID list
			"radius"	Per-node data stored by a radius server
			"either"	Make both local and radius checks
wep_key_active	WEP	1	1–4	Select which of the four stored default keys is active.
wep_key_range	Advanced WEP	40,40	40–128, 40–128	Sets the *minimum*, *maximum* WEP key length (in bits) which will be accepted for authentication

Name (command line)	Config Web page	Factory default	Valid range	Description
wep_key	WEP	none	1–4, hex string	Set default key *1–4* to the value *hex string*. Hex string is from 10 to 32 characters in length, according to the strength of wep key being entered. Web interface also allows keys to be entered in ASCII.
radius_server	Advanced WEP	none	1–2, IP address	IP address of primary (1) and secondary (2) Radius servers.
shared_secret	Advanced WEP	none, "NokiaWLAN"	up to 16 characters each	A pair of ASCII strings: shared secret and dummy password for Radius server.
password	Advanced Access Point	"default"	up to 16 characters	Password for management access to AP
ap_name	Access Point	"LocalAP"	Up to 15 characters	Access point name (equivalent to hostname)
protocols	Advanced Access Point	"all"	"all", "tcp/ip"	Enables packet filtering, which discards all non-TCP/ IP traffic
lock	Advanced Access Point	"off"	"on" or "off"	Prevents any changes being made to the AP without using the password. This means that learn mode and restoring system defaults are impossible.

Name (command line)	Config Web page	Factory default	Valid range	Description
zone_privacy	Advanced Access Point	“off”	“on” or “off”	If set to “on”, the AP blocks traffic from being passed directly between radio clients (this has the effect of blocking peer-peer networking)
snmp_contact	SNMP	“Contact”	up to 32 characters	SNMP contact name (from the RFC1213 MIB)
snmp_sys_name	SNMP	“Sys Name”	up to 32 characters	SNMP system name (from the RFC1213 MIB)
snmp_location	SNMP	“Location”	up to 64 characters	SNMP location data (from the RFC1213 MIB)
dhcp_mode	DHCP	“disabled”	“off”, “disabled”, “client”, “server”	Used to select DHCP operation for the AP. By default, this will be disabled, but server and client operation can be selected.
dhcp_base	DHCP	192.168.5.100	IP address	The base address of the IP pool for DHCP server operation.
dhcp_pool	DHCP	16	1–64	The number of entries in the pool for the DHCP server.
dhcp_gateway	DHCP	none	IP address	The gateway address for DHCP clients.

Radio parameters

A number of new radio parameters have been added for the AP. As with all AP radio settings, they are only accessible via the command line interface. The new parameters and their functions are described in the following subsections.

Path delay

This parameter is designed for use on systems where an AP is being used in specialized bridging links covering large distances. In these cases, the round trip time for a radio signal and its reply can be significant and the path delay parameter can be set to allow the AP to compensate for it. In normal use, the path delay should be at its default setting (0).

The path delay is set in microseconds – a radio signal will travel approximately 300m per microsecond, so this parameter should be set to the distance between the bridging points in metres, divided by 150 (to account for the round-trip time). Path delay can be disabled by setting back to zero.

Beacon interval

Sets the time interval between beacons in milliseconds. This defaults to 100ms – longer intervals reduce the amount of idle load on the radio interface, but may increase the time taken to join a network or roam.

The beacon interval can be changed with the command

```
set beacon_interval <n>
```

DTIM interval

The number of beacons to count between DTIMs. The default value is 5 – larger values will reduce network load, but at the cost of reduced performance, particularly where clients are using power saving.

The DTIM interval can be changed using the command

```
set dtim_interval <n>
```

TX power

Allows the AP power level to be fine-tuned. In a large installation, using multiple APs, it may be helpful to reduce the power level to prevent distant APs from interfering – the default setting uses the highest power level, which minimizes the effect of interference and maximizes range.

The tx power level may be trimmed by entering the command

```
set tx_power <level>
```

CCA mode

This setting determines which CCA mode should be used. The modes are:

Term	Meaning
ed_only	Energy detect only
cs_only	Carrier sense only
ed_and_cs	Energy detect and carrier sense
ed_or_cs	Energy detect or carrier sense

Use caution when altering this setting, as an inappropriate CCA mode can prevent reliable reception. The default setting is to use Carrier sense only – this can be changed with the command

```
    set cca_mode <New_Mode>
```

ED Threshold

This value contains the signal level at which the ED part of the CCA checking is triggered. Whether or not the Energy Detect forms part of the CCA signal is determined by cca_mode; this variable merely sets the threshold.

Use caution when altering this setting, as in combination with certain CCA modes it can prevent reliable reception. The default value for ED threshold is 17, which can be changed with the command

```
    set ed_threshold <n>
```

ED Absolute

If set, this variable causes the ED threshold set by ‘set ed_threshold’ to be regarded as an absolute value. Otherwise the value is taken to be relative to the noise floor.

Use caution when altering this setting, as in combination with certain CCA modes it can prevent reliable reception. By default, ED absolute is set to TRUE, which can be changed using the command

```
set ed_absolute <TRUE or FALSE>
```

3. Minor functional changes

Learn mode

In this mode, only one of the interfaces is operational (either LAN or radio) – if the unit is started up with both a radio card and LAN connection, then the active interface will be radio, and the LAN connection ignored; otherwise, the connected interface will be used.

In LAN learn mode, the unit will attempt to learn an IP address – if three successive ARP requests are passed through the unit without a reply, it will adopt the IP address in the ARP request for itself. This would normally be used by plugging the unit into a network, and accessing it (e.g. pinging the desired IP address). Once the address is learnt this way, any one of the configuration methods listed the user manual can be used to configure the unit.

In radio learn mode, the unit automatically becomes a limited DHCP server, assigning itself the first address in the pool (however, it will respond to any incoming packet with a valid IP address). This can be used to provide a permanent configuration, as above.

SNMP changes

The A032 enterprise traps have been updated since the previous issue of the user manual. The following are now generated:

Trap	Name	Description
1	A032 Authenticate fail	Generated in the event that a station tries to associate but is refused due to the fact that the NID Name security feature is enabled. Note that this trap is limited to being generated no more than once every 30 seconds to prevent flooding due to denial of service attack.
2	A032 Bridge Down	If the bridge/repeater function is active, this trap is generated when a bridge link is lost.
3	A032 Management login	Generated whenever the Management password is successfully entered in one of the management utilities.
4	A032 TFTP Access	Generated whenever a TFTP transfer is initiated to or from the unit.
5	WEP Authenticate fail	Generated in the same way as Trap 1, but when the authentication is rejected because of WEP rather than the NID name feature.

WEP key lengths

The A032 now has explicit support for 104 bit WEP keys. Some manufacturers have produced 802.11b clients using 104-bit WEP keys (usually marketed as being 128 bit). Creating a 104-bit key in the A032 should allow these clients to be used with their maximum key strength.

4. Radius operation

Introduction

This section describes the Nokia Radius client implementation. It provides sufficient detail to get third-party Radius servers to operate with the A032 Access Point. It describes frame formats and details of interactions between the AP and a Radius server. It does not cover how a particular Radius server implementation is configured to operate with an AP.

This section documents both new and previously existing behavior.

Technical information

Radius overview

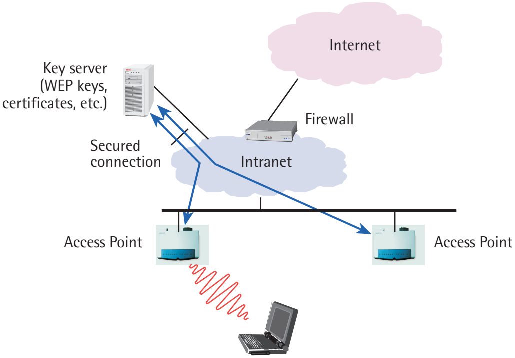
Radius is a simple authentication protocol for remote clients. The name Radius comes from the words Remote Authentication Dial In User Service. The Radius protocol has traditionally been used in modem pools but nowadays its use has been expanded to include firewall authentication, amongst other things. The AP implementation of Radius widens the scope of the protocol to include Wireless LAN clients and the provision the key exchange as part of authentication scheme.

The basic characteristics and assumptions are following:

- Radius is simple protocol where all messages are encoded on protocol specific way using a byte a smallest single field so no ASN.1 or any other kind bit-based message coding scheme is used.
- Radius is stateless protocol that uses UDP for sending protocol packet. In practice this means that Radius is fairly simple to implement on the server side but client needs to have some short of retransmission capabilities for lost packets.
- There is no encryption of the messages (except the password) so Radius assumes that authentication is performed inside a trusted network (for example, intranet).

The traditional Radius system is meant to operate within a secure network, such as intranet, because it does not require much skill to capture radius packets and use faked packets to provide false authentication information. That's why the WEP keys received from Radius server are encrypted.

Radius security scheme has three to four components. The network architecture of the system can be seen in the figure below. The first component is the client trying to perform the authentication. Traditionally, this is a laptop trying to set up a connection to corporate modem pool via a dial-in connection from the PSTN. On the WLAN scenario the client is a laptop, or a wired PC using an adapter, trying to set up a WLAN connection to an Access Point.



The second component is the modem-pool server that tries to find out if the user is valid or not. The modem pool server tries to authenticate the user against the central user database by using the Radius protocol so modem pool server is a Radius client described on the protocol specification. The protocol specification uses name Network Access Server (NAS) for the client of the Radius server. On our WLAN radius security scheme, the AP is equivalent to the NAS on the protocol specification so the AP is a client of the Radius server (in other words, the NAS functionality is build into the AP).

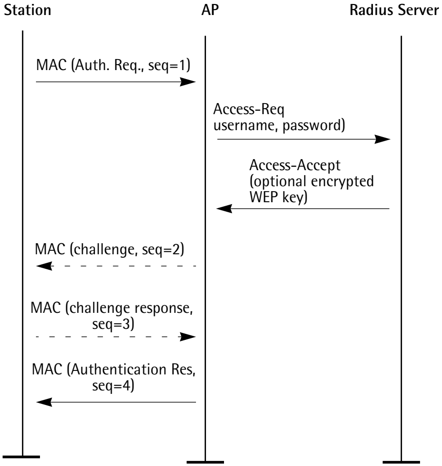
The third component is the Radius server, which takes care of deciding if the clients should be granted access to the network. Usually, there is a database attached to the Radius server implementation, which holds the list of the authorized clients. Radius server is a stateless system that receives packets and responds to them right away. If state information is needed, it is included in the response. When clients receive the state information, this includes the state of its response packet.

The fourth component is the proxy server. It receives requests from the NAS and either processes them by itself or sends them to another Radius server. This makes it possible to distribute the processing of Radius requests, allowing load balancing and making the security solution more fail safe.

Radius operation

The use of a Radius server on the current AP range can be enabled using the web pages or via the command line, either through the serial port or via Telnet.

Once enabled, whenever a wireless station attempts to authenticate with the AP, the following interaction with the Radius server occurs:



The basic message flow between different external entities is shown above.

The authentication procedure is initiated by the station, which sends **Authentication Req** MAC frame to the AP. The AP builds a Radius **Access-Request** containing a Radius **user-name** and **user-password** derived as follows:

- The **user-name** is either the MAC address of the station expressed as a 12-character hexadecimal string or the unit name if this has been supplied by the station.

  The A040 adapter sends its unit name as a vendor-specific IEEE802.11 information element in the Authentication Req message.
- The **user-password** is generated from a **password**, a **shared secret** and a random Request Authenticator included in the Radius packet (see RFC2138 section 5.2 for the password generation algorithm) using the MD5 hashing function. The **password** and **shared secret** are defined via the 'set shared_secret' command on the AP CLI. Note that the password, being a value entered at into the AP configuration, is the same for all stations.

Using its copy of the **shared secret** and **password**, the Radius server can check that the **user-password** supplied is valid. The **password** for all the MAC-address entries in the Radius server configuration should be set to same value as was entered on the APs. Also, the **password** and **shared secret** must be the same in all the APs using the Radius server.

When the Radius server receives the **Access-Request**, it takes the user-name and looks up the entry for the station. It then recalculates its own copy of the **user-password** and if the supplied **user-password** and its own match it builds an **Access-Accept** message to send back to the AP. If a WEP key has been stored in the Radius database for this station, it uses the Blowfish algorithm to encrypt the WEP key and includes this as a Vendor-Specific Radius attribute. Otherwise, no Vendor-Specific attribute is included.

The WEP key is transmitted as a 32-character hexadecimal ASCII string derived as follows:

- Copy the n-byte WEP key to a 16-byte buffer.
- Fill the remainder of the buffer with 0x00.
- Encrypt the 16-byte buffer using Blowfish with the **shared secret** as the key.
- Encode the 16-byte buffer as a 32-character hexadecimal string.

The WEPkeygen utility provided with the AP can be used to generate the encrypted keys. The data can be entered as normal, and saved to a file instead of being sent to the AP. This is a simple text file, and the encrypted key values can be copied across to the Radius database.

The 32-character string representing the encrypted key is sent to the AP as a vendor-specific attribute (see RFC2138 section 5.26) with the vendor ID set to the Nokia value (94). This is shown below.

Field	Octets
Type (26)	1
Length	1
Vendor ID (94)	4
WEP key attribute (see following tables)	34 or 36

The encrypted WEP key is placed in the String field. This is formatted also like an attribute (type+length+string) but the type values are defined in this document. There are two formats for the Nokia-specific attribute:

Field	Octets
Type (2)	1
Length (34)	1
Encrypted WEP key (ASCII hex string)	32

The format above has no mechanism for determining the length of the WEP key. The first implementation of the AP Radius client measured the length by looking for the first non-0x00 byte in the decrypted key from the end of the 16-byte decrypted key. Unfortunately, this means that no key can end with bytes of 0x00 even though this would otherwise be a valid key. For backwards compatibility, the format above is still supported but should not be used for new systems.

To fix the WEP key length problem, the format below should be used:

Field	Octets
Type (3)	1
Length (36)	1
Key Length (ASCII hex)	2
Encrypted WEP key (ASCII hex string)	32

This uses a new type code and the attribute now contains the length of the WEP key in bytes expressed as a 2-character ASCII hex string in the range 05 to 10. When configuring a Radius server, the two strings shown above can be treated as a single 34-character hex string.

When AP receives the **Access-Accept** message, if a vendor-specific attribute is present the WEP-key is extracted from the Radius and the AP continues its normal IEEE802.11 authentication procedure using the supplied WEP key for communication with the station. If no key is provided, the AP will continue to use the keys existing on the AP – normally the current default key. IEEE802.11 authentication is not described in this document.

If the Radius server cannot identify the station, it will send an **Access-Reject** message to the AP. The AP will terminate the IEEE802.11 authentication and return an error code to the wireless station.

Configuration

To configure the A032 to use Radius authentication, carry out the following steps (the items within <> are user-specified, the other text must be typed as shown):

1 Set the Radius secret and the password common to all APs:

```
set shared_secret
<shared_secret> <password>
```

2 Set the IP addresses of the primary and secondary radius servers (if only one server is present, set the primary and secondary addresses to be the same):

```
set radius_server 1
<xxx.xxx.xxx.xxx>
set radius_server 2
<yyy.yyy.yyy.yyy>
```

3 Set the WEP mode and specify that a Radius server is to be used for key lookup:

```
set wep_mode <mode> radius
```

4 Set the admission policy to only permitted stations:

```
set admission named
```

5 Restart the AP:

```
restart
```

Because there are many different radius servers available, no specific configuration details can be given. However, the following general procedure can be used:

1. Set the Radius secret and the password common to all APs:

   ```
   set shared_secret
   <shared_secret> <password>
   ```

2. For each station, create an entry where the username is the station MAC address expressed as a 12-character hexadecimal string, and the password is the password used in step 1 of the AP configuration
3. If per-station WEP keys are required, define the WEP key for the station. How this is done will depend on how the server handles vendor-specific attributes.

Because the use of a per-station WEP key is optional, Radius can still be used to authenticate wireless station access.

5. DHCP operation

Introduction

This document describes the operation and configuration of DHCP on the AP. Server operation is essentially unchanged, other than the effects of revisions to the user interface to cater for client operation.

The AP can be configured for either server or client operation (this is an exclusive choice – choosing both simultaneously is not accepted). Server operation is described in more detail below, while client operation is described on page 33. The AP DHCP implementations **do not** support BOOTP interoperability.

Server operation

The Server implementation is targeted at small installations (such as home use), and includes only a minimal feature set. It is anticipated that larger networks would have a pre-existing system administration policy – either precluding the use of DHCP, or having a more fully featured DHCP server under central control. The AP DHCP server provides for the following:

- Dynamic address assignment on a 1-hour lease.
- Provides subnet mask, DNS server and default gateway to clients (note that if DNS and gateway information is not explicitly set up, the AP provides its own address for these).
- The DHCPINFORM message is not supported.
- Address assignment is only performed on the local subnet.
- The server can be assigned an address pool ranging from 1 to 64 addresses, which are assigned contiguously from a configured base address. When the AP initializes, it will probe the network for address conflicts, removing these and invalid addresses from the pool (for example, if pool addresses stray outside the AP subnet, they will simply be marked invalid).

- If the AP does not have a fixed IP address assigned to it, then it will claim one from the DHCP address pool during startup.
- If the AP is put into radio learn mode, the DHCP server is automatically enabled, using either the default pool address or (if present) its own IP address as the pool base address.
- The DHCP server will always assign an IP address, subnet mask, gateway and DNS server. The subnet mask assigned is the one set for the AP, while the gateway and DNS addresses are configurable. The default setting causes the DHCP server to instruct the clients to use the A032 as their gateway and (proxy) DNS server - this is required for normal Internet access via the AP. Explicit IP addresses can be configured if these defaults are inappropriate.

Client operation

The DHCP client has been designed to ease integration of the AP into larger networks, and as such has a larger feature set than the server. The intention is to allow the DHCP protocol to be used to download a working configuration, enabling the management of all APs on a network to be handled centrally. In order to support this, the client implementation draws configuration information from the following:

- Standard DHCP options.
- Custom (Vendor class) options.
- The DHCP *boot file* option (identifies a resource to be obtained later using TFTP).

The standard options cover only a small part of the AP configuration, and by themselves are insufficient to meet the target of central management, so it is anticipated that one or both of the remaining configuration methods would also be required. However, it is possible to devise a workable scheme, using DHCP to assign addresses backed up by, for example, a script using TFTP to update parameters.

When the AP is configured to run in DHCP client mode, the *dhcp* command in the CLM reports on the current lease within the AP.

Operational sequence

When the DHCP client is enabled, the AP will first boot up into a limited operation mode, connected to LAN only, and begin the DHCP negotiation. During this phase, the AP will signal *no radio* operation on the LEDs. Only when a DHCP offer is received (and accepted), or the process is abandoned (no response is received from a server after three retries) will the AP complete booting and run management and radio interfaces. If a dynamic lease expires, the AP will return to this limited operational mode (by rebooting). Note that all radio clients will be forcibly disconnected.

The AP will always perform a full DHCP initialization (that is, it begins with a DISCOVER frame), even if it has a configured IP address. Neither an init-reboot or DHCPINFORM process are ever used. If the AP does have a configured management IP address, it will request assignment of it via the DHCP procedure, but make use of whatever IP address it is given. This process can be tracked using the DHCP status screen on the web interface.

Depending on the success of DHCP negotiation, one of the following will occur:

- No DHCP server found – AP will operate as far as possible using its stored configuration, including making use its management IP address if configured with one. If no IP address was configured for the AP, then this will limit its functionality accordingly.

- DHCP response with no option string – AP will operate using its stored configuration, but with the IP address provided by DHCP.
- DHCP response with option string and/or a configuration file reference – AP will accept the parameters given, and fill in the remainder from its stored configuration. The AP gives precedence to such an offer, and will select it in preference to a simple IP address offer.

The options received via DHCP do **not** become permanently stored by the AP, and will lapse at the next restart of the AP (which will immediately re-request parameters via DHCP). The existing methods of configuring the AP (command line and web) were not designed to cope with this, but the command line interface has no trouble – it has commands to show both current and pending configuration (in his case, pending effectively means stored settings that have been overridden by the temporary DHCP configuration). The web interface works throughout on pending configuration, and generally overlooks the DHCP modifications. However, using **restore active settings** in the web interface will have the effect of making the DHCP configuration permanent.

If a DHCP frame is received containing a *file* reference, the AP will use TFTP to download and store it. See page 42 for details of the TFTP download, but note that, in this case, there is a hierarchy of configuration data:

1. The standard DHCP options (IP address and network parameters, including host (AP) name) are fetched and applied.
2. TFTP is used to fetch the specified configuration, which is itself applied, and finally, the vendor options fields are parsed. If any configuration details clash, the following precedence applies:
   - Vendor Options (highest)
   - DHCP Options
   - TFTP Download (existing stored settings)

If the AP is run in learn mode, the DHCP client is automatically disabled.

Accepting dynamic IP addresses

Using a DHCP client implementation allows the AP to be offered an IP address according to one of the following schemes:

- Automatic addressing – the server allocates the address, but offers it indefinitely.
- Dynamic addressing – the server allocates an address for a time-limited period.
- Manual allocation – a system administrator selects addresses, but uses DHCP to distribute them.

Acceptance of an automatically selected IP address makes management of the AP difficult, as its IP address will be unknown, but doesn't directly affect its operation. The AP will accept such offers regardless. Administrators are advised to allocate IP addresses manually for APs if this is an issue.

A dynamic address which expires (i.e. if lease renewal and rebind both fail) causes the AP to reboot. This ensures that the expired IP address will not be used, and forces a fresh negotiation. In this case, the log records the reboot and the reason as DHCP lease expiry.

DHCP standard options

The following tables list AP parameters and their availability via DHCP. These are the standard DHCP options and their option codes:

Parameter	DHCP option code	Default value
Default gateway	3	none
Subnet mask	1	255.0.0.0
IP address	n/a	none
AP name	12	"LocalAP"

DHCP Vendor class options

All other AP configuration items require private option codes for vendor-specific option processing. These are packaged into DHCP option 43, using the encapsulated option format described there. The following table lists the remaining AP configuration items and their option code and format within DHCP. Options are stored in the standard DHCP format, and packaged as shown below:

Parameter	Option code	Size (octets)	Default value	Data
Zone Privacy	1	1	n/a	Experimental option, do not use
Radio channel	2	1	10	channel #
Domain	3	1	varies	coded value (see 802.11 MIB)
802.11 net name	4	max. 32	"Nokia WLAN"	ASCII
Password	5	max. 16	"default"	ASCII
RTS Threshold	10	2	2301	value (2 octets)
Fragmentation Threshold	11	2	2346	value (2 octets)
Basic Rates	12	max. 8	1000 2000	array of 2 octet values
Beacon interval	13	2	100 (mS)	value (2 octets)
DTIM interval	14	1	5	value
Tx power level	15	1	1	value
CCA mode	16	1	2	value
ED threshold	17	1	17	value
ED absolute	18	1	1	1 or 0
Path delay	19	2	0	value (2 octets)
Short retry	21	1	15	value

Parameter	Option code	Size (octets)	Default value	Data
Long retry	22	1	15	value
Telnet port	30	2	23	value (2 octets)
HTTP port	31	2	80	value (2 octets)
Protocol filter	32	1	0	1 (discard all non-TCP/ IP frames) or 0 (no filtering)
Management access	40	max. 8	“any”	ASCII text: “any”, “specific” or “none”
Manager IP list	41	max 16	none	between 1 and 4 IP addresses
WEP mode	50	max. 8	“wep”	ASCII text: “open”, “wep”, “wifi” or “personal”
Lookup mode	51	max. 8	“local”	ASCII text: “local”, “radius” or “either”
Radius server IPs	52	max. 8	none	1 or 2 IP addresses
Radius shared secret	53	max. 16	none	ASCII
Radius dummy password	54	max. 16	none	ASCII
NID list encryption	55	1	off	1 or 0
WEP key length policy	56	2	40,40	2 lengths in bits
WEP key active	60	1	1	1–4
WEP key 1	61	max. 16	none	WEP key
WEP key 2	62	max. 16	none	WEP key
WEP key 3	63	max. 16	none	WEP key
WEP key 4	64	max. 16	none	WEP key
DHCP server	no	n/a	n/a	Automatically disabled

Parameter	Option code	Size (octets)	Default value	Data
SNMP community get	70	max. 16	"public"	ASCII
SNMP community set	71	max. 16	"private"	ASCII

The AP requests this parameter list by sending a Vendor class identifier (DHCP option) with the DHCPREQUEST/DISCOVER frames. This will comprise the option code (60), length (10), and the ASCII text “Nokia A03x”.

The AP does **not** expect to receive values for every parameter in the table above; they are subject to the same principle as standard options (included if only if needed). In fact, the total length of the option field is limited to 255 octets (and each option requires its length + 2 octets overhead), so including all of the options runs the risk of overrunning the maximum size. Some of the larger or more specialized AP parameters are not supported via DHCP options: if DHCP configuration is required for them, the TFTP configuration file method must be used.

Operational sequence on page 34 describes the implications of not including certain options.

TFTP download

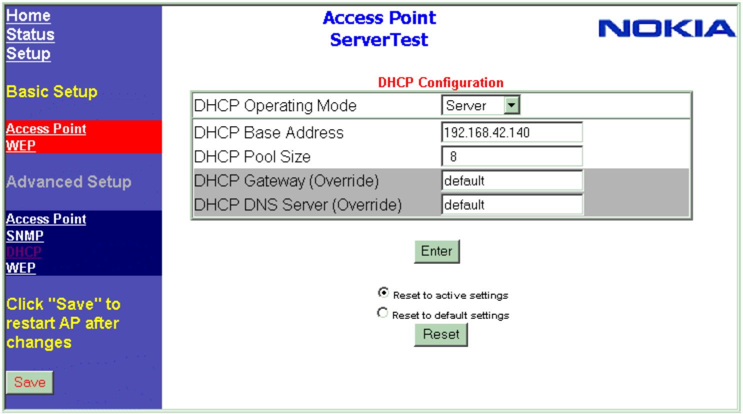
DHCP may also be used to notify the AP of a filename to use for a download. The AP will parse this, if present, and use TFTP to request the file specified. This file is structured like a normal AP TFTP config.txt file (although it may optionally be augmented with WEP keys and passwords, and should not contain parameters which clash with the standard DHCP options: IP address, subnet mask, gateway and AP name). In this case, the AP downloads the new configuration, then moves onto normal operation.

See *Operational sequence* on page 34 for a description of the whole configuration process.

DHCP Web pages

DHCP configuration page

The configuration page simply displays (and allows changes to) the five DHCP configuration entries.

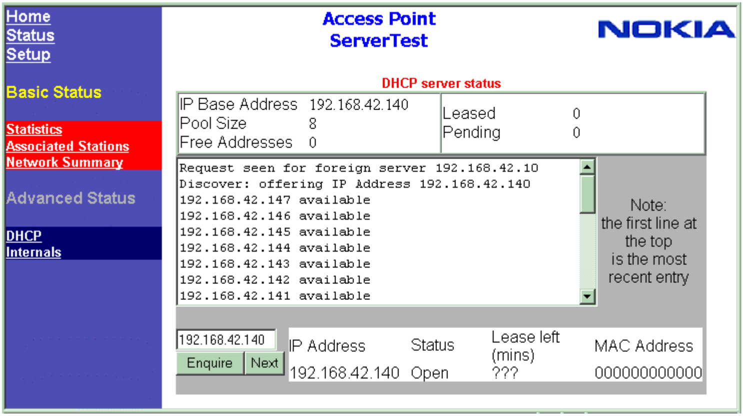


DHCP Configuration

DHCP Operating Mode	Server
DHCP Base Address	192.168.42.140
DHCP Pool Size	8
DHCP Gateway (Override)	default
DHCP DNS Server (Override)	default

● Reset to active settings
○ Reset to default settings

DHCP status page (server)



Access Point
ServerTest

DHCP server status

IP Base Address	192.168.42.140	Leased	0
Pool Size	8	Pending	0
Free Addresses	0		

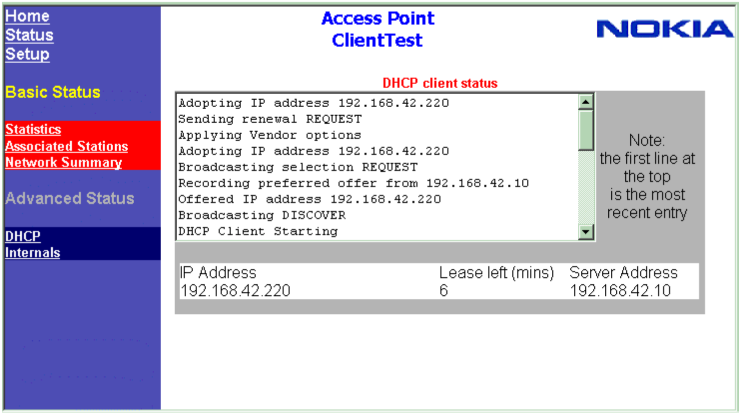
```
Request seen for foreign server 192.168.42.10
Discover: offering IP Address 192.168.42.140
192.168.42.147 available
192.168.42.146 available
192.168.42.145 available
192.168.42.144 available
192.168.42.143 available
192.168.42.142 available
192.168.42.141 available
```

Note: the first line at the top is the most recent entry

192.168.42.140

IP Address	Status	Lease left (mins)	MAC Address
192.168.42.140	Open	???	000000000000

DHCP status page (client)



Access Point
ClientTest

DHCP client status

```
Adopting IP address 192.168.42.220
Sending renewal REQUEST
Applying Vendor options
Adopting IP address 192.168.42.220
Broadcasting selection REQUEST
Recording preferred offer from 192.168.42.10
Offered IP address 192.168.42.220
Broadcasting DISCOVER
DHCP Client Starting
```

Note: the first line at the top is the most recent entry

IP Address	Lease left (mins)	Server Address
192.168.42.220	6	192.168.42.10

6. TFTP config.txt file

The TFTP config.txt file has been restructured in line with the changes to configuration. The following example illustrates the current format:

```
/Config.txt for AP(Example) on Wed, 27 Jun 2001 09:55:06
%channel: 11
%net_name: "ExampleNet"
/*%rts_threshold: 2301
/*%frag_threshold: 2346
/*%short_retry: 15
/*%long_retry: 15
/*%gateway: 0.0.0.0
/*%subnet_mask: 255.255.255.0
%ip_address: 192.168.84.76
%ap_name: "Example"
/*%lan: "10baseT"
%domain: ETSI
/*%telnet: 23
/*%web: 80
%wep_mode: open either
/*%protocols: all
%admission: all
%manager: any 0 0 1
%basic_rate:  1000 2000
%wep_key_range: 40 128
%use_encrypted_nid: false
%dhcp_pool: 16
%dhcp_base: 192.168.84.140
%isp_num: "0123456789"
%isp_user: "test"
%mdm_speed: 57600
%mdm_holdtime: 3
```

```
/*%nat_port: off
%community_get: "public"
%community_set: "private"
/*%radius_server: 1 0.0.0.0
/*%radius_server: 2 0.0.0.0
%snmp_contact: "Contact"
%snmp_sys_name: "Sys Name"
%snmp_location: "Location"
%path_delay: 0
%zone_privacy: off
%beacon_interval: 100
%dtim_interval: 5
%tx_power: high
%cca_mode: cs_only
%ed_threshold: 17
%ed_absolute: true
%dhcp_mode: server
/*default setting
```