FORUM NOKIA

Nokia Series 40 VoIP v81 Configuration Tutorial

Version 1.1; March 4, 2009

VoIP

Contents

Change history

November 28, 2008	Version 1.0	Initial document release.
March 4, 2009	Version 1.1	Added TIMER-T1 and TIMER-T2 SIP settings.

1 Introduction

This tutorial describes the configuration of Nokia Series 40 Voice over IP (VoIP) v81.

The Nokia Series 40 VoIP v81 configuration consists of the following setting groups:

1. VoIP profile settings (Section 2.1, 'Profile-specific VoIP settings')
   a. Speech codec settings (Section 2.2, 'Speech codec settings')
   b. Profile-specific VoIP settings (Section 2.3, 'SIP profile–specific VoIP settings')
2. SIP (Session Initiation Protocol) profile settings (Chapter 3, 'SIP profile settings')
3. Network address translation (NAT)/Firewall traversal settings (Chapter 4, 'NAT/Firewall traversal settings')
4. Access point settings (IAP WLAN, Chapter 5, 'IAP settings')

The VoIP profile includes settings for one or more speech codecs. The VoIP profile may also have SIP profile-specific VoIP settings defined for each SIP profile. Series 40 VoIP v81 supports only SIP protocol.

Each VoIP profile can refer to one SIP profile, and each SIP profile can refer to one or more Internet Access Points (IAPs). The VoIP profile and the related SIP profile must refer to the same IAPs.

The NAT/Firewall traversal settings refer to a SIP domain and optionally to an access point.

References between the setting groups are handled using the following parameters:

- `APPREF` — The `APPREF` parameter uniquely names the `APPLICATION` characteristic, that is, the part of the provisioning message that provides the terminal with a set of settings (parameters). `APPREF` must be unique within its enclosed structure, that is, within the configuration context [2].
- `TO-APPREF` — The `TO-APPREF` parameter links the `APPLICATION` characteristics to another secondary `APPLICATION` characteristic with a matching `APPREF` parameter [2]`NAPID` — Network Access Point Identifier (a parameter of the NAPDEF characteristics). The NAPID must be unique within its enclosed structure, that is, within the configuration context [1].
- `TO-NAPID` — This parameter refers to a network access point with a matching `NAPID` parameter [1].

These parameters are defined in the setting groups as follows. Example values are used to illustrate the linking in practice.

VoIP settings

In the VoIP Profile settings, at least one `TO-NAPID` reference has to be included but several `TO-NAPID`s are supported as well:

```
<parm name="TO-NAPID" value="Open_VoIP_WLAN_settings"/>
<parm name="TO-NAPID" value="WPA_VoIP_WLAN_settings"/>
<parm name="TO-NAPID" value="WEP_VoIP_WLAN_settings"/>
<parm name="TO-NAPID" value="INTERNET"/>
```

Note: The `TO-NAPID` definitions here must be the same as the `TO-NAPID` references in the SIP settings.

SIP settings are referred to using the `TO-APPREF` parameter:

```
<parm name="TO-APPREF" value="VoIP_SIP_settings"/>
```

SIP profile settings

In SIP profile settings, the SIP setting must include the `APPREF` parameter, which defines a string that is referred by the `TO-APPREF` parameter:

```
<parm name="APPREF" value="VoIP_SIP_settings"/>
```

`TO-NAPID` references must be exactly the same as in the VoIP settings:

```
<parm name="TO-NAPID" value="Open_VoIP_WLAN_settings"/>
<parm name="TO-NAPID" value="WPA_VoIP_WLAN_settings"/>
<parm name="TO-NAPID" value="WEP_VoIP_WLAN_settings"/>
```

Reference is to the preferred access point defined in the same provisioning document with the VoIP settings. If this is the only `TO-NAPID` reference, no other NAPs can be used for VoIP.

```
<parm name="TO-NAPID" value="INTERNET"/>
```

For example, an additional `TO-NAPID` could refer to "`INTERNET`". This implies that any network access point can be selected with the attribute `INTERNET` defined, if the preferred access point could not been reached. If this is the only `TO-NAPID` reference, none of the network access points have a predefined preference.

At least one `TO-NAPID` must be defined. These definitions must always be in line with the `TO-NAPID` definitions in the VoIP settings.

> **Note:** Having the `INTERNET` reference only is the recommended setting. Other examples are for the cases where certain APs are more preferred, that is, the preference is predefined and cannot be changed by the user.

NAT/FW settings

NAT/FW settings must have a `APPREF` parameter that defines a string that is referred by the `TO-APPREF` parameter:

```
<parm name="APPREF" value="Example_NAT_FW_settings"/>
```

Reference to SIP settings:

```
<parm name="DOMAIN" value="example.com"/>
```

Domain links the NAT/FW settings to SIP settings. Domain here must be the same as the domain in the Public User ID (PUID) of the SIP settings.

References to access points:

```
<parm name="TO-NAPID" value="Open_VoIP_WLAN_settings"/>
<parm name="TO-NAPID" value="WPA_VoIP_WLAN_settings"/>
<parm name="TO-NAPID" value="WEP_VoIP_WLAN_settings"/>
<parm name="TO-NAPID" value="INTERNET"/>
```

`TO-NAPID` must refer to a specific NAP using the value of the `NAPID` defined in the same provisioning document or it can refer to "`INTERNET`" when any network access point can be selected with the attribute `INTERNET` defined.

Access point settings

Access point definitions must have a `NAPID` parameter that defines a string that is referred to by the TO-`NAPID` parameter:

```
<parm name="NAPID" value="Open_VoIP_WLAN_settings"/>
```

Figure 1 illustrates the relationships between the setting groups. Chapter 1, 'Introduction', offers a description of the subsequent chapters and sections in this document that explore setting parameters and their relations.

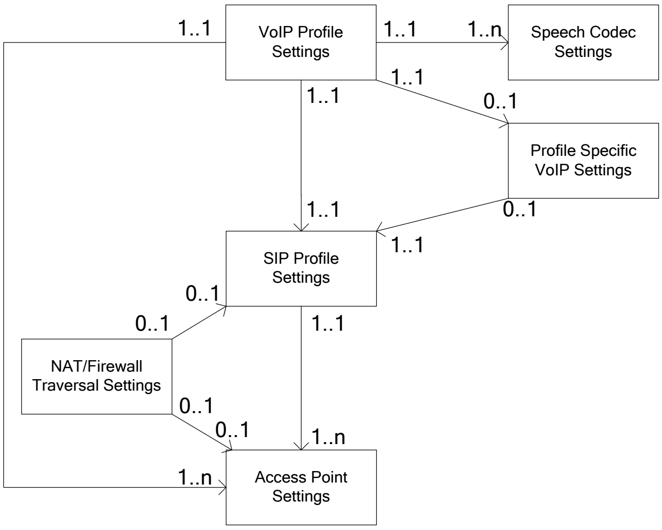

Figure 1: Relations between the VoIP settings

WLAN AP settings can be entered by the user. Other settings cannot be edited from the UI but must either be provisioned by the service provider as an Over the Air (OTA) service, or edited by using the browser of the mobile device (see Chapter 6, 'VoIP connectivity and accounts').

2 VoIP profile settings

The VoIP profile includes VoIP service-specific settings, such as:

- VoIP service name
- VoIP service parameters
- Speech codec settings
- SIP profiles used

The VoIP profile name is the same as the VoIP service name shown on the terminal UI. If a VoIP service provider also configures the access networks used that have, for example, a different billing or connectivity mode, the VoIP service can be divided into one or more VoIP profiles. The following is an example of a VoIP service divided into two different VoIP profiles:

- 'ServiceName Home'
- 'ServiceName City WLAN'

If the service provider does not set up the access networks, only one VoIP and one SIP profile are needed. The VoIP profile settings are linked to the access point selected when the user is successfully registered to the service from the *Internet telephone menu*.

The VoIP services work in automatic or manual mode:

- In automatic mode, the VoIP service is automatically registered if a network is available. WLAN network availability is detected when the WLAN scan is triggered.
- In manual mode, the user connects by an active idle shortcut or from the *Internet telephone menu*. It is also possible to register when making an Internet call from the phonebook logs or idle view.

Figure 2 shows the VoIP profile settings, including the speech codec settings and SIP profile-specific VoIP settings.

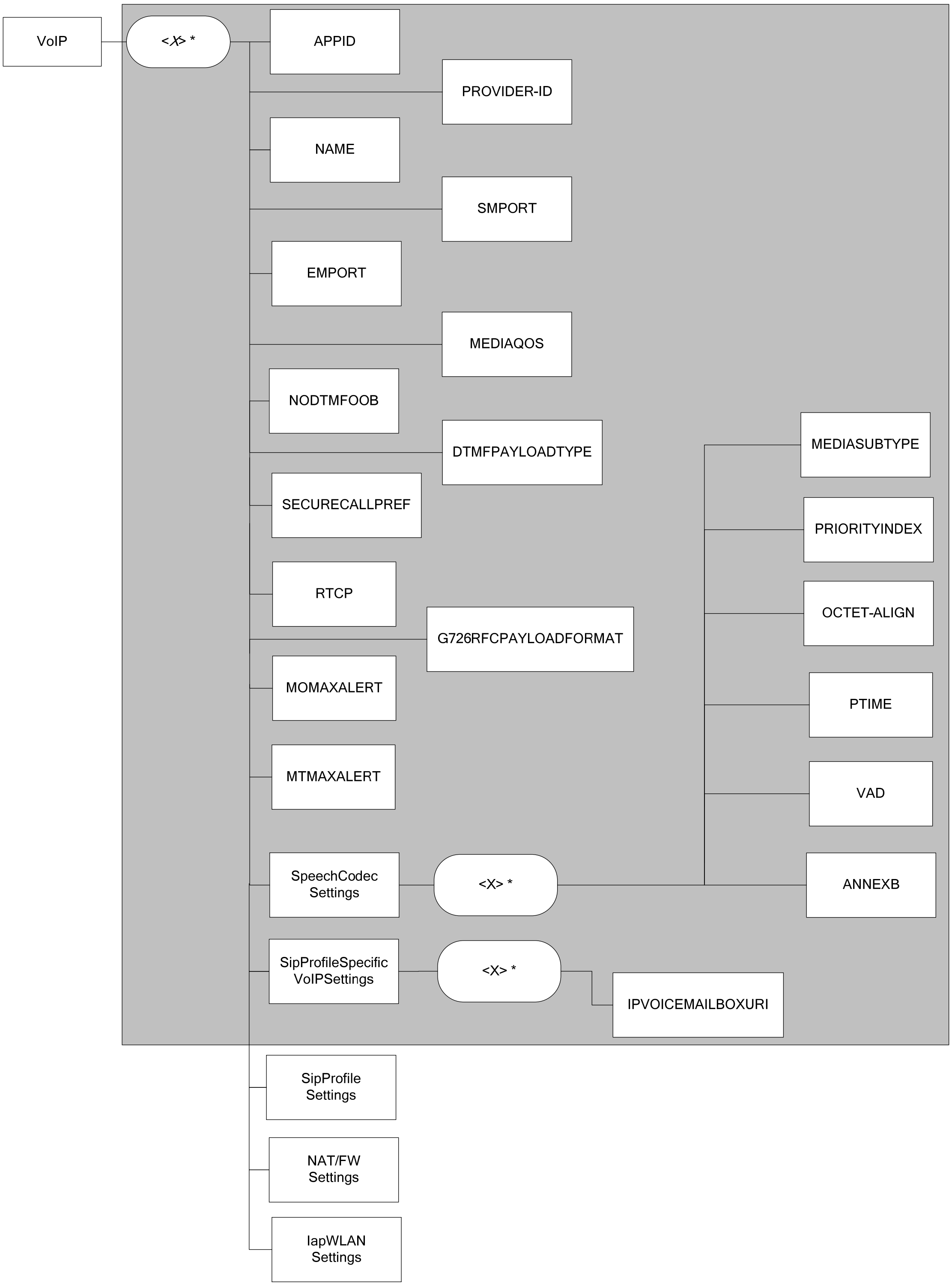

Figure 2: VoIP profile settings

2.1 Profile-specific VoIP settings

ID of the VoIP settings (APPID):

- ID for the VoIP settings.
- Default: ‘w9013’.

Provider of the settings (PROVIDER-ID):

- Text, the maximum length is 32 characters.
- Provider of the VoIP profile settings as described in [1] 'Open Mobile Alliance, Provisioning Content, OMA-WAP-ProvCont-v1_1-20050428-C'.
- This text is displayed on the terminal UI as the sender of the settings. If the VoIP service has a customer brand name, put it here.

Name of the settings (NAME):

- Text, the maximum length is 32 characters.
- Based on the provisioning parameter NAME as described in [1] 'Open Mobile Alliance, Provisioning Content, OMA-WAP-ProvCont-v1_1-20050428-C'.
- This text is displayed on the terminal UI as the service name.
- Default: 'VoIP settings'.

Start media port number (SMPORT):

- A number in the range of 1024–65535.
- The lower limit of the RTP port range.
- Default value: '16384'.

End media port number (EMPORT):

- A number in the range of 1028–65535.
- The upper limit for the allocated RTP ports. The value must be at least 4 over the 'Start media port number' to guarantee two simultaneous calls.
- Default value: '32766'.

Media QoS (MEDIAQOS):

- A number in the range of 0–63.
- Quality of Service for VoIP media. DiffServ Code Point (Diffserv, DSCP bits) QoS values to be used in IP headers (IPv4 TOS and IPv6 TC).
- Default value: '46'.

No DTMF out-of-band signaling (NODTMFOOB):

- When this parameter is defined, DTMF out-of-band is disabled.
- Default: Parameter is not defined.

Predefined payload type for DTMF (DTMFPAYLOADTYPE):

- A number in the range of 96-127 (dynamic payload type range).
- With this parameter the payload type for DTMF (telephone-event) can be predefined to a certain value.
- If this parameter is not defined, codecs with dynamic payload types will get numbers starting from 96 according to the order of codecs in the provisioned settings with the exception that the DTMF (telephone-event) gets the last value.
- Default: Parameter is not defined.

Secure call preference (SECURECALLPREF):

- ‘0’, Nonsecure call is preferred.
- ‘1’, Secure call is preferred in MO (Mobile Originated) calls.
- ‘2’, Security is mandatory for call establishment in MO calls.
- Default value: ‘0’.

RTCP reporting (RTCP):

- This setting enables the Real-Time Transport Control Protocol (RTCP) reports defined in IETF RFC 3550.
- ‘0’: RTCP reporting is disabled.
- ‘1’: RTCP reporting is enabled.
- Default value: ‘0’.

G.726 RFC Payload Format (G726RFCPAYLOADFORMAT):

- When this parameter is defined, the RTP payload format used for the G.726 codecs is according to RFC 3551, and when not defined, the RTP payload format is according to ITU-T I.366.2.
- Default: Parameter is not defined.

MO maximum alerting time (MOMAXALERT):

- Maximum time waited in an MO call if the alerting call is not answered by the Mobile Terminated (MT) end. Call is released after the time has expired.
- Value in seconds: 0 ... 255 (‘0’ indicates that the feature is disabled).
- Default: ‘45’.

MT maximum alerting time (MTMAXALERT):

- Maximum time waited if an MT call is not answered. Call is released after the time has expired.
- Value in seconds: 0 ... 255 (‘0’ indicates that feature is disabled).
- Default: ‘30’.

2.2 Speech codec settings

The following parameters are defined for the supported speech codecs (CODEC):

Media subtype name (MEDIASUBTYPE):

- Number range 0 – 10.

Priority index (PRIORITYINDEX):

- Number range 0 – XX.

Octet-align (OCTET-ALIGN):

- When this parameter is defined, octet-aligned framing is used according to RFC 3267, and when not defined, bandwidth efficient framing is employed. Relevant only for the AMR-NB codec.
- Default: Parameter is defined.

Ptime (PTIME):

The length of time in milliseconds represented by the media in a packet. The ptime may have values up to maxptime. Possible values are multiples of the sampling intervals. 10 ms, 20 ms, and 30 ms sampling intervals are supported. This parameter has an affect only for the encoding (uplink media).

- Default: Parameter is not defined. Table 1 shows the default ptime values when not defined with this parameter.

Voice Activation Detection (VAD):

When this parameter is defined, VoIP Discontinuous Transmission (DTX) is enabled.

This means that RTP packets are not sent during silent periods but

- AMR generates Silence Description (SID) packets also during inactivity with reduced packet frequency, and
- iLBC, G.711, and G.726 codecs generate Comfort Noise (CN) frames. For that, the CN codec needs to be defined.

This maximises the number of concurrent VoIP calls per WLAN AP. This parameter is not relevant for the G.729 codec that uses a built-in mechanism to reduce packets during the silent periods (Annex b).

- Default: Parameter is defined.

Annex b (ANNEXB):

When this parameter is defined, annex-b enhancements of IETF RFC 3555 are enabled. Relevant only for the G.729 codec.

- Default: Parameter is defined.

Default values of the parameters for the codecs are presented in Table 1. The G.726 codec has a Media Subtype Name reserved for each of its data rates, that is, for 40, 32, 24, and 16 kbit/s.

Codec/ Param.	AMR NB	iLBC	G711 A-law PCMA	G711 μ-law PCMU	G726-40	G726-32	G726-24	G726-16	CN	G729
Media Subtype Name	0	1	3	4	5	6	7	8	9	10
Default Priority Index	0	1	3	4	5	6	7	8	9	2
Octet-align	Defined	-	-	-	-	-	-	-	-	-
Ptime	20	20	20	20	20	20	20	20	-	10
VAD	Defined	Defined	Defined	Defined	Defined	Defined	Defined	Defined	-	-
Annex b	-	-	-	-	-	-	-	-	-	Defined

Table 1: Table of codecs

2.3 SIP profile-specific VoIP settings

IP voice mailbox URI (IPVOICEMAILBOXURI):

- A SIP or TEL URI defining the IP voice mailbox address (IETF RFC 3842-compliant server) of the user. For example, robert@ipvoicemailbox.example.com.

3 SIP profile settings

Session Initiation Protocol (SIP) profile settings include items such as:

- Public user name (SIP AOR)
- SIP registrar server address and authentication credentials
- Proxy server address and authentication credentials

Figure 3 shows the SIP profile settings.

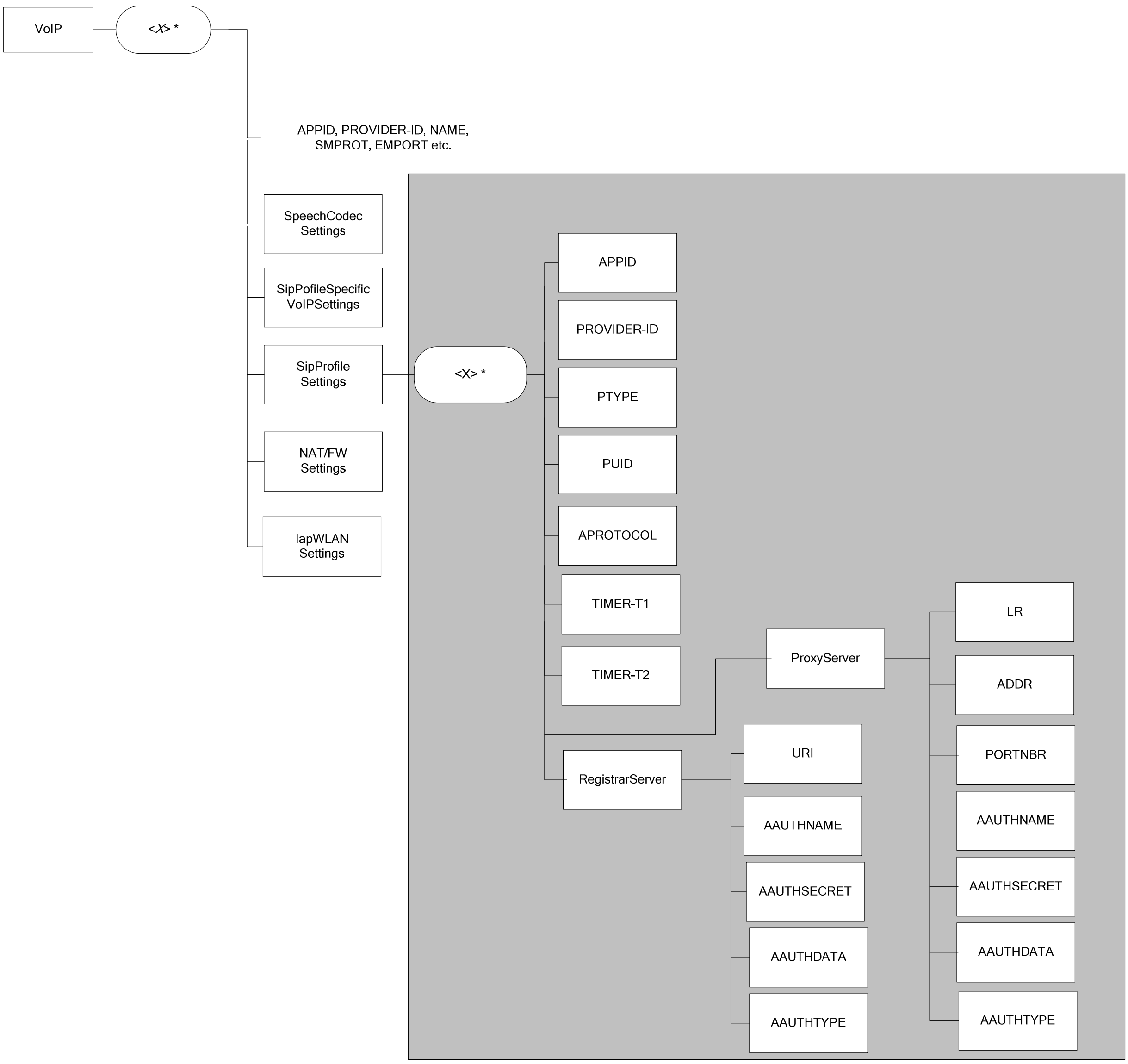

Figure 3: SIP profile settings

3.1 Creating a SIP profile

To create a SIP profile for VoIP use, the following SIP settings are needed:

Profile name (PROVIDER-ID):

- Give a name to describe the settings, identify this particular set of parameters. Using the same name as for the VoIP profile settings is recommended.

Service profile type (PTYPE):

- Service profile type indicates the supported SIP dialect. The only possible value for Series 40 VoIP v81 is 'IETF'.

Public user name (PUID):

- A SIP URI for the user including the host-name part, that is, the SIP domain name provided by the service provider. For example, sip:robert@example.com or sip:+12345678@example.com.
- Value may be given without the "sip:" or "sips:" prefix, in which case "sip:" is automatically added.

Transport type (APROTOCOL):

- 'UDP': UDP transport forced to be used.
- 'TCP': TCP transport forced to be used.
- Parameter is not defined. Transport is selected according to RFC 3261, that is, UDP is used for <1300 bytes, and TCP for >1300 bytes long initial requests.
- Default: 'UDP'.

Timer T1 (TIMER-T1):

- SIP timer T1: The RTT estimate. An estimate for the round-trip time in the system (terminal – proxy). See RFC 3261 for reference.
- A timer value in milliseconds: 500 ... 5000.
- If this parameter is not defined, the default value of 800 ms is used.
- Default: Parameter is not defined.

Timer T2 (TIMER-T2):

- SIP timer T2: The maximum retransmit interval for non-INVITE requests and INVITE responses. See RFC 3261 for reference.
- A timer value in milliseconds: 1000 ... 40000.
- If this parameter is not defined, the default value of 6400 ms is used.
- Default: Parameter is not defined.

3.1.1 Proxy server

Allow loose routing (LR):

- Parameter is defined for RFC 3261-compliant SIP proxy.
- Parameter is not defined for SIP 1.0 specification-compatible strict routing mode.
- It is recommended that this parameter is defined.

Proxy server address (ADDR):

- The address of the SIP outbound proxy; leave empty if the outbound proxy is not used.
- Value can be given without the “sip:” or “sips:” prefix, in which case “sip:” is automatically added.

If the proxy server is defined as a Fully Qualified Domain Name (FQDN), resolving the related IP address is done with the procedures specified within RFC 3263. A short summary follows:

- If the FQDN is supplied without port and transport parameters, the terminal will try to resolve it using the DNS NAPTR, SRV, and finally the A and AAAA queries.
- If the FQDN is supplied without the port but with the transport parameter, the terminal will try to resolve it using the DNS SRV, and finally the A and AAAA queries.
- If the FQDN is supplied with the port parameter, the terminal will try to resolve it using only the A and AAAA queries.
- This setting creates a preroute set according to RFC 3261; the Route header is inserted in the initial request.
- The proxy has to insert Record-Route headers to keep itself in the route set on later requests inside a SIP session.

Port (PORTNBR):

- The TCP and/or UDP port the SIP proxy is listening to; the default value of 5060 is typically used.

User name (AAUTHNAME):

- Needed for proxy authentication (not necessarily the same as the public user name). The authentication user name may simply be the user name part of the public SIP URI, but it may also contain the SIP domain or the SIP scheme as a prefix, that is:

  robert

  robert@example.com

  sip: robert@example.com

- Depends on the proxy vendor and configuration.

Password (AAUTHSECRET):

- Needed if proxy authentication is used (provided by the service provider).

Realm (AAUTHDATA):

- The realm parameter sent by the proxy in the authentication challenge in the 407 response. The recommended value is the SIP domain. The value must be exactly the same as the proxy is configured to use, case sensitive.
- If no value is given for this parameter in the settings, it is read from the 407 response.

Authentication method (AAUTHTYPE):

- This parameter indicates the used authentication method. The only possible value is ‘`HTTP-DIGEST`’.

3.1.2 Registrar server

Registrar server address (URI):

- FQDN of the registrar server or the SIP domain, that is, the host-name part of the user's SIP URI. Port number and transport protocol may be included if needed, for example, "registrar.example.com:5068;transport=UDP".
- Value can be given without the 'sip:' or 'sips:' prefix, in which case 'sip:' is automatically added.

User name (AAUTHNAME):

- Needed for user authentication. Often, but not necessarily always the same as the public user name. This parameter is often called a private user ID. Normally the same value as for the proxy authentication (see Section 3.1.1, 'Proxy server'.)

Password (AAUTHSECRET):

- Needed for registrar authentication. Typically the same as for the proxy authentication.

Realm (AAUTHDATA):

- The realm parameter sent by the registrar in the authentication challenge in the 401 response. The recommended value is the SIP domain. The value must be exactly the same as the registrar is configured to use (case sensitive.)
- If no value is given for this parameter in the settings, it is read from the 401 response.

Authentication method (AAUTHTYPE):

This parameter indicates the authentication method that is being used. The only possible value is '`HTTP-DIGEST`'.

4 NAT/Firewall traversal settings

Nokia Series 40 VoIP v81 has STUN protocol support for NAT traversal and NAT binding refresh features following the IETF RFC 3489. The NAT/Firewall traversal features enable the VoIP functionality behind NATs of a certain type.

The STUN/Firewall settings cannot be edited from the terminal UI, but must be provisioned by the service provider.

If the STUN server address is not configured, the terminal tries to find one with a SIP SRV query, using the Public User Identity domain of the used SIP profile.

Additional dummy packet (CRLF) refresh cannot be enabled by provisioning. The CRLF refresh is enabled automatically if the STUN server is situated in a different address from the SIP proxy/registrar. The CRLF refresh is also enabled if there is no STUN server configured and the user's own IP address is in a private address space, since the terminal is then presumably behind a NAT.

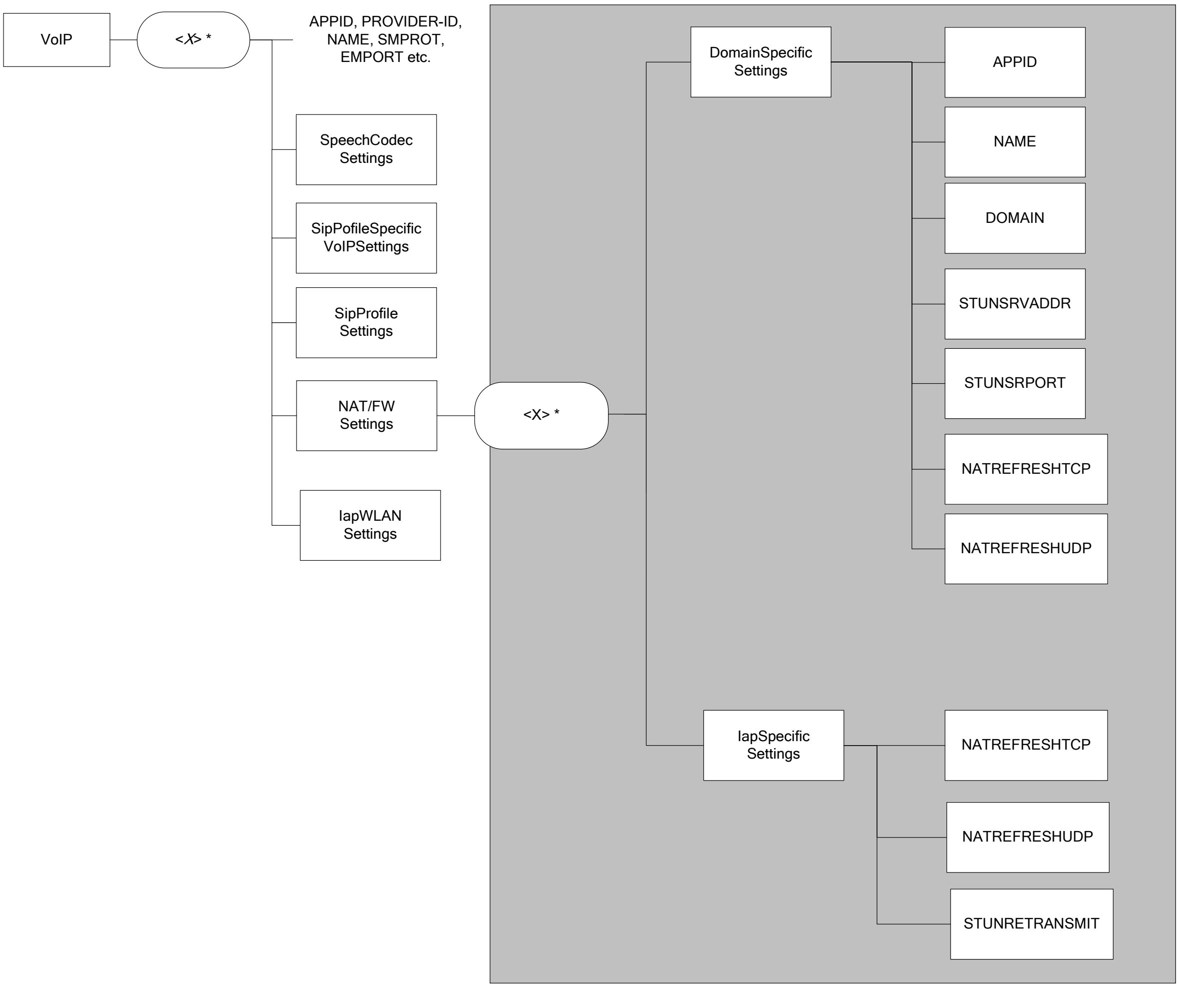

Figure 4: NAT/FW settings

4.1 Domain-specific settings

Domain (DOMAIN):

- SIP domain to specify domain-specific NAT/FW traversal values.

STUN server address (STUNSRVADDR):

- This parameter defines the STUN server address in the domain-specific NAT-FW settings. Optional. By default, the DNS SRV query tries to find the STUN server.
- Apply value 0.0.0.0 to disable the STUN server, for example if an SBC is taking care of the NAT traversal.

STUN server port (STUNSRVPORT):

- This parameter defines the STUN server port in the domain-specific NAT-FW settings. Optional.
- Default value: '3478'.

NAT refresh TCP (NATREFRESHTCP):

- This parameter defines the NAT refresh interval for TCP in the domain-specific NAT-FW settings. The unit of the refresh interval is seconds. If an IAP-specific value for this interval is defined, it overrides this value. Optional.
- Minimum value: '30'.
- Default value: '1200'.

NAT refresh UDP (NATREFRESHUDP):

- This parameter defines the NAT refresh interval for UDP in the domain-specific NAT-FW settings. The unit of the refresh interval is seconds. If an IAP-specific value for this interval is defined, it overrides this value. Optional.
- Minimum value: '15'.
- Default value: '28'.

4.2 IAP-specific settings

NAT refresh TCP (REFRESHTCP):

- This parameter defines the NAT refresh interval for TCP in the IAP-specific NAT-FW settings. The unit of the refresh interval is seconds. The value overrides the domain-specific NAT Refresh TCP value, if it is defined. Optional.
- Minimum value: '30'.
- Default value: '1200'.

NAT refresh UDP (REFRESHUDP):

- This parameter defines the NAT refresh interval for UDP in the IAP-specific NAT-FW settings. The unit of the refresh interval is seconds. The value overrides the domain-specific NAT Refresh UDP value, if it is defined. Optional.
- Minimum value: '15'.
- Default value: '28'.

STUN retransmit (STUNRETRANSMIT):

- This parameter defines the STUN request retransmit timer (time in milliseconds) in the IAP-specific NAT-FW settings. Optional.
- Default value: '250'.

5 IAP settings

IAP settings are graphically presented in Figure 5.

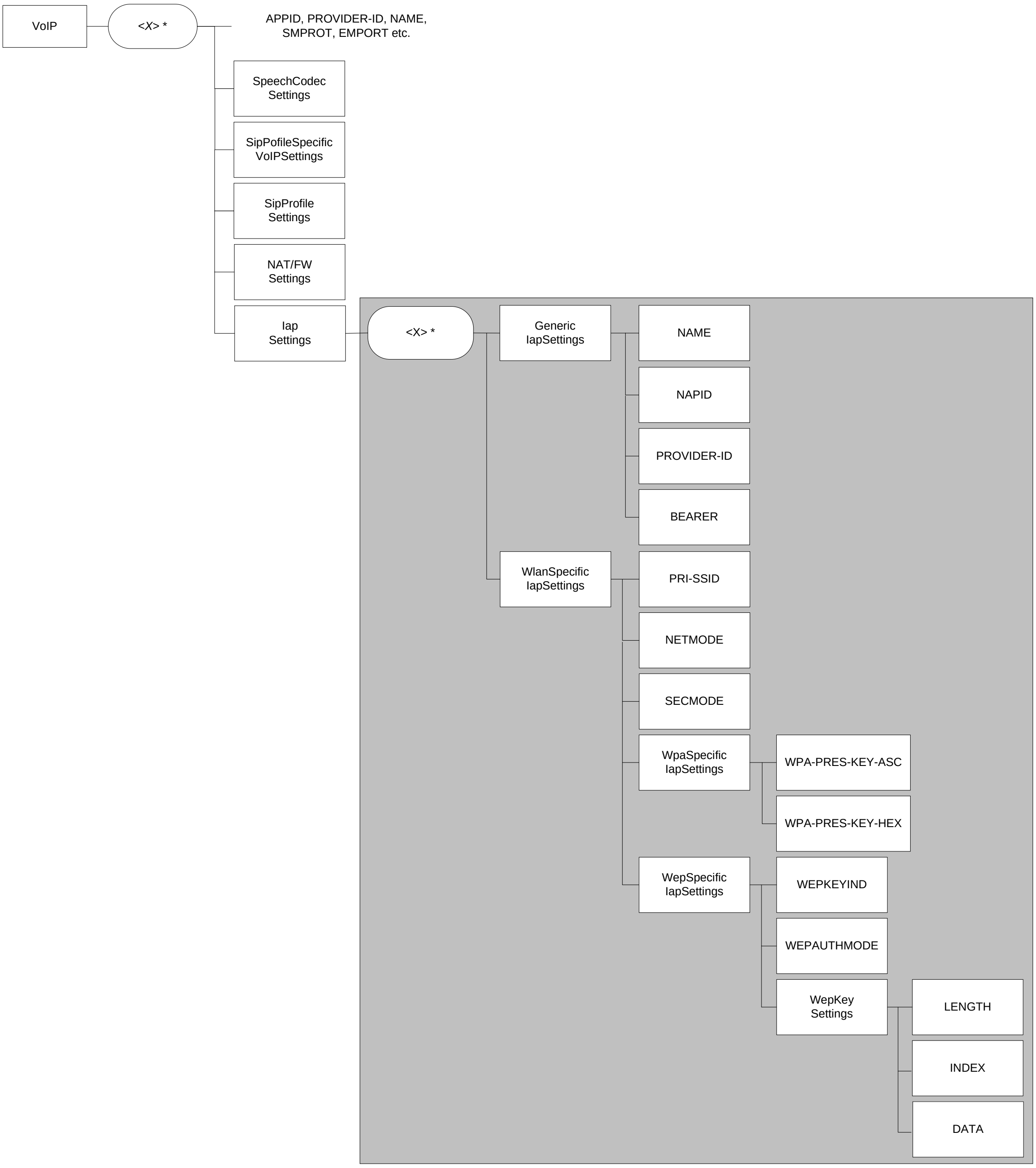

Figure 5: IAP settings

5.1 Generic IAP settings

Name for the IAP settings (NAME):

- The NAME indicates a logical, user-readable identity (property) of the configuration context.

Network Access Point ID (NAPID):

- Unique ID for the defined NAP. The `TO-NAPID` parameter must match the value of `NAPID` when referring to this NAP.

Service Provider ID (PROVIDER-ID):

- The identifier for the network service.

Bearer Type (BEARER):

- Bearer supported in this network access point. `NAPDEF` -> `BEARER` can be used if direction information is not needed. The `BEARER` indicates which network type (in addition to address type) the definition is valid for.
- Default: "`WLAN`".

5.2 WLAN-specific IAP settings

Primary SSID (PRI-SSID):

- The primary name (SSID) of the WLAN network.
- Character string.

Network Mode (NETMODE):

- Network Mode indicates the operation mode for the WLAN network.
- Only possible value for Series 40 VoIP v81 is 'INFRA' — infrastructure network.

Security Mode (SECMODE):

- Security mode for the WLAN network.
- Possible values are:
  - 'WEP': WEP security in use.
  - 'WPA-PRESHARED-KEY': Wi-Fi Protected Access security using preshared key in use. This mode also supports WPA2 with preshared key.
  - 'WPA2-PRESHARED-KEY': Wi-Fi Protected Access 2 security using preshared key in use. In this mode only AES (CCMP) cipher is allowed.
  - Parameter is not defined: No security is applied.
- Default: Parameter is not defined.

5.2.1 WPA-specific IAP settings

ASCII form preshared key (WPA-PRES-KEY-ASC):

- This parameter defines the ASCII form preshared key.
- Value must be 8 – 63 characters long.
- Valid only if SECMODE value is WPA-PRESHARED-KEY or WPA2-PRESHARED-KEY.

Hexadecimal form preshared key (WPA-PRES-KEY-HEX)

- This parameter defines the hexadecimal form preshared key.
- Value must be 32 bytes long (64 hexadecimal digits) when decoded back to binary.

- Value must be either Base64 encoded or hexadecimal text (64 characters). Encoding is determined from the length of the value.
- Valid only if SECMODE value is WPA-PRESHARED-KEY or WPA2-PRESHARED-KEY.

5.2.2 WEP-specific IAP settings

Default key index (WEPKEYIND):

- This parameter defines which of the WEPKEYs should be the default key.
- A number in the range of 0 – 3.
- If the parameter is not defined, the first WEP key is the default.
- Valid only if SECMODE value is WEP.

Authentication mode (WEPAUTHMODE):

- Authentication mode for WEP.
- Possible values are:
  - ‘OPEN’: Open authentication mode in use.
  - ‘SHARED’: Shared authentication mode in use.
- Valid only if SECMODE value is WEP.

5.2.2.1 WEPKEY settings

These parameters define the length and the data for the WEPKEY. The maximum amount of keys is limited to 4. The first defined WEP key is the default unless WEPKEYIND is included.

WEP key length (LENGTH):

- This parameter defines the length of the WEP key in bits.
- Possible values are 64 and 128.

WEP key index (INDEX):

- This parameter defines the index of the WEP key.
- A number in the range of 0 – 3.

WEP key data (DATA):

- This parameter defines the WEP key data.
- The value can be in any of the following formats. Encoding is determined from the length of the value.
  - Base64 encoded.
  - Plain text (if all characters are printable).
  - Hexadecimal text.
- The following examples contain the same 64-bit WEP key in different formats:
  - Base64 encoded: `ZXhhbXBsZXNlY3JldA==`
  - Plain text: `examplesecret`
  - Hexadecimal text: `6578616D706C657365637265 74`

6 VoIP connectivity and accounts

VoIP Connectivity handles the user's VoIP (Internet phone) calling profiles. A VoIP calling profile (VoIP Account) contains all the necessary information to register to a VoIP service, for example the log-in name and password, and server address. The user can have several profiles, but can be registered to only one at a time.

VoIP Connectivity can be accessed from the **Internet telephone menu** item (by default under **Settings > Connectivity**; menu structure may vary between products). It has the following structure:

My accounts

- A list of the user's VoIP accounts.

Registration tone

- When enabled, a tone is played when registering to and reregistering from a VoIP account. The tone is disabled by default. This is product configurable.

If the mobile device has a default (selected) VoIP account, and a saved WLAN network profile is defected, the mobile device will attempt to register to the account automatically if WLAN scanning is on. Registration will take place in the background, unless initiated from the menu. A VoIP status indicator is displayed and a tone is played (if enabled) when the connection is made to the account.

It is not possible to add VoIP accounts manually; this is set as an OTA service.

In flight mode, the WLAN radio is disabled. The user has access to the menu and can operate the existing accounts, but does not have the option to connect.

7 Usage

A Nokia Series 40 VoIP v81 terminal may be registered simultaneously to a cellular service (CS domain) and a VoIP service (IP domain). The user can choose the domain in which the mobile device should attempt to place outgoing calls — in the CS domain, in the IP domain, or both — and in which order of preference. This selection can be done through the menu item **Call Settings > Call type setting** (see Figure 6).

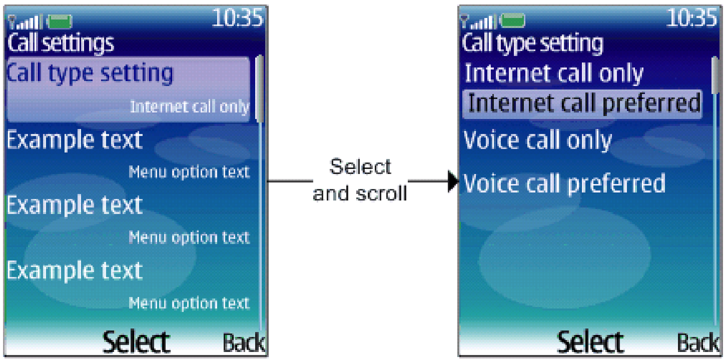

Figure 6: Call preferences

Taking these preferences into account, the mobile originated (MO) calls are made according to the following rules:

- Preferred telephone switch:
    - Cellular call mode — Prefers cellular network.
    - Internet call mode — Prefers VoIP.

  The preferred telephone switch first determines the call preference: cellular or Internet.
- If the user specifically selects the Internet or Voice call from the phonebook or log, the call is made as VoIP or cellular, respectively.
- If the user calls to a SIP URI, the call is made as VoIP.
- If the user tries to make an Internet call without an active VoIP service registration, the registration is performed if a known VoIP-capable access point is available.

8 Abbreviations

Abbreviations	Meaning
AOR	Address of record
DNS	Domain name server
DTMF	Dial-tone multi-frequency
FQDN	Fully qualified domain name
FW	Firewall
IAP	Internet access point
IETF	Internet Engineering Task Force (www.ietf.org)
MO	Mobile originated
MT	Mobile terminated
NAT	Network address translation
OMA	Open Mobile Alliance
OTA	Over the air
QoS	Quality of service
RTP	Real-time protocol
RTCP	Real-time control protocol
SBC	Session border controller
SDP	Session description protocol
SIP	Session initiation protocol
SRV	Server
SSID	Service set identifier
STUN	Simple traversal of user datagram protocol (UDP) through network address translators (NATs)
TCP	Transport control protocol
UDP	User datagram protocol
UI	User interface
VoIP	Voice over IP
WLAN	Wireless LAN, wireless local area network

9 References

[1] Open Mobile Alliance, Provisioning Content, OMA-WAP-ProvCont-v1_1-20050428-C, available at Candidate Version 1.1 – 28 Apr 2005.

[2] Open Mobile Alliance, Change Request, OMA-DM-2004-0211R01-CR_AC.doc, available at OMA-DM-2004-0211R01-CR_AC.