snom m9

Unleashed VoIP!!

Ahmar Ghaffar, snom

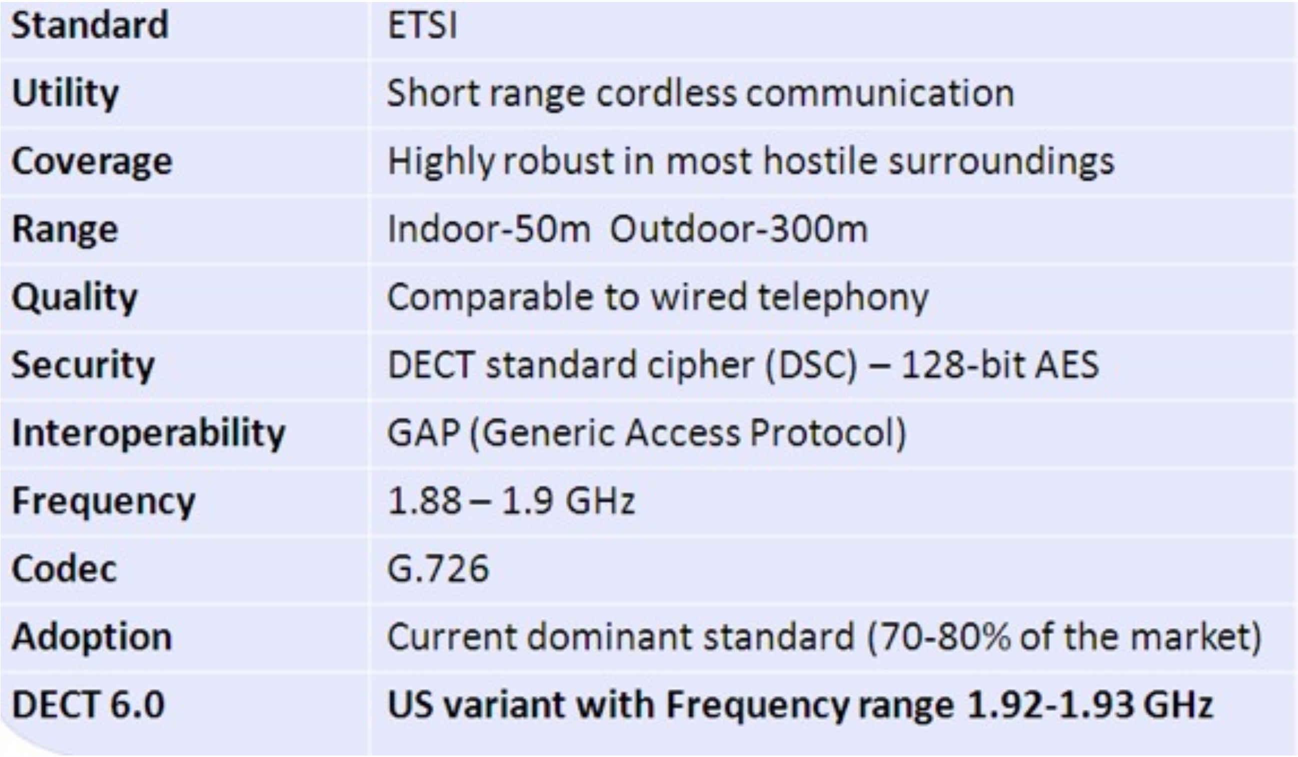
Jan 20th, 2011

Table of Contents

- DECT/DECT 6.0
- Product Overview
- Server Profiles
- CTI with Action URLs
- Caller-ID with Picture
- LDAP
- IPv6
- Security
- Auto Configuration
- Lync 2010 Setup
- Diagnostics

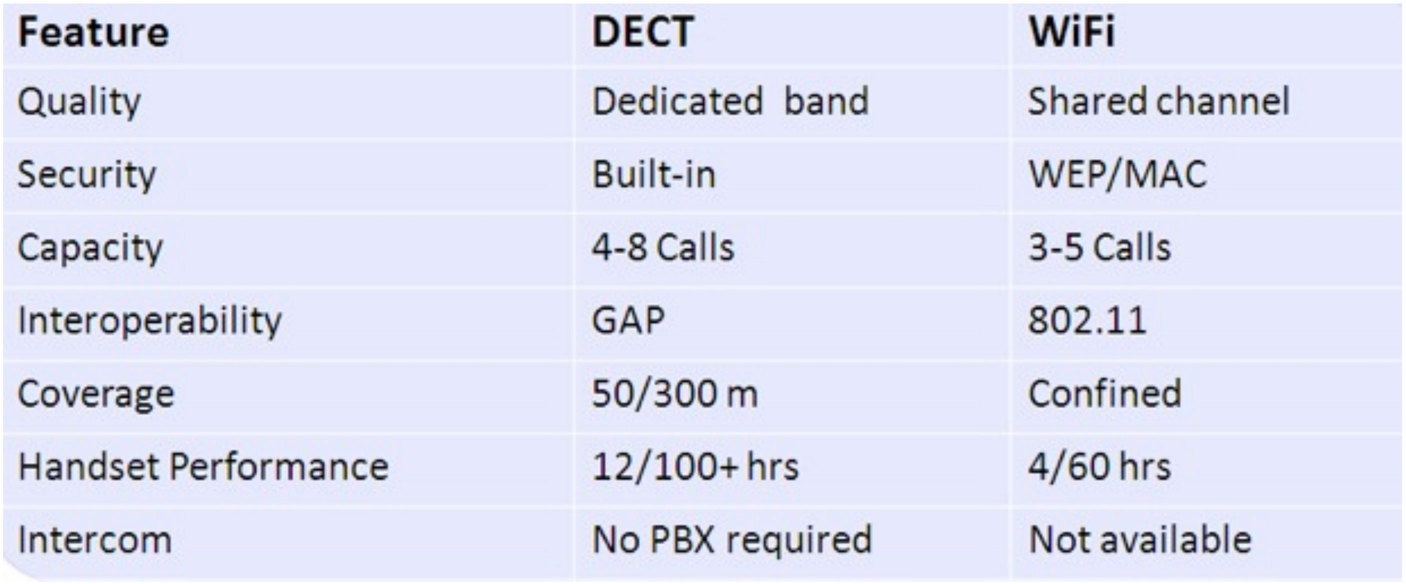
DECT/DECT 6.0

What is DECT?



Standard	ETSI
Utility	Short range cordless communication
Coverage	Highly robust in most hostile surroundings
Range	Indoor-50m Outdoor-300m
Quality	Comparable to wired telephony
Security	DECT standard cipher (DSC) – 128-bit AES
Interoperability	GAP (Generic Access Protocol)
Frequency	1.88 – 1.9 GHz
Codec	G.726
Adoption	Current dominant standard (70-80% of the market)
DECT 6.0	**US variant with Frequency range 1.92-1.93 GHz**

DECT or WiFi?

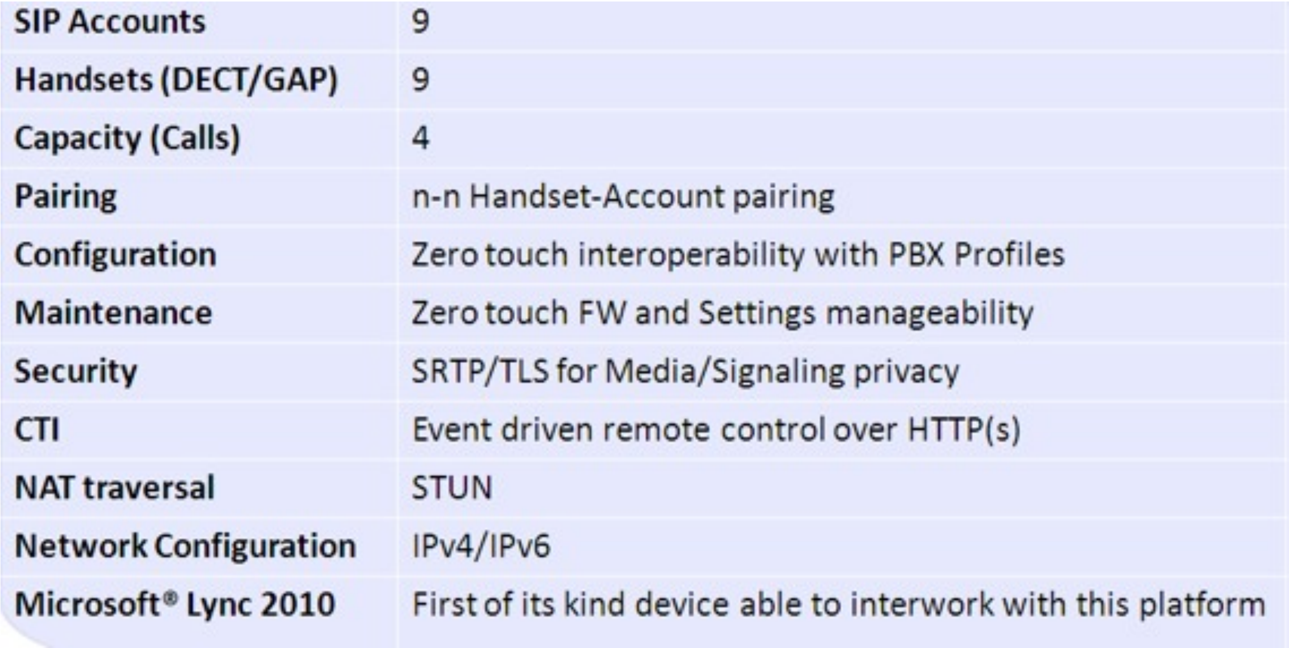


Feature	DECT	WiFi
Quality	Dedicated band	Shared channel
Security	Built-in	WEP/MAC
Capacity	4-8 Calls	3-5 Calls
Interoperability	GAP	802.11
Coverage	50/300 m	Confined
Handset Performance	12/100+ hrs	4/60 hrs
Intercom	No PBX required	Not available

Product Overview

Product Overview

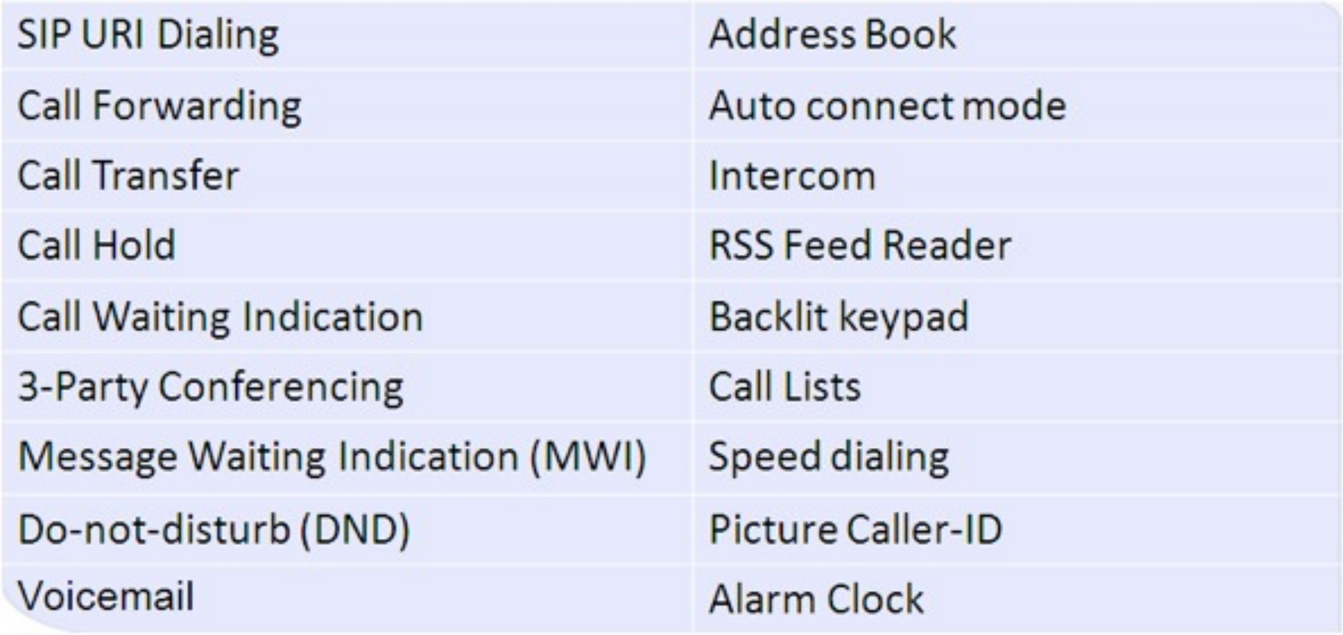
snom m9 – At a Glance:



SIP Accounts	9
Handsets (DECT/GAP)	9
Capacity (Calls)	4
Pairing	n-n Handset-Account pairing
Configuration	Zero touch interoperability with PBX Profiles
Maintenance	Zero touch FW and Settings manageability
Security	SRTP/TLS for Media/Signaling privacy
CTI	Event driven remote control over HTTP(s)
NAT traversal	STUN
Network Configuration	IPv4/IPv6
Microsoft® Lync 2010	First of its kind device able to interwork with this platform

Product Overview

snom m9 Handset Features:



SIP URI Dialing	Address Book
Call Forwarding	Auto connect mode
Call Transfer	Intercom
Call Hold	RSS Feed Reader
Call Waiting Indication	Backlit keypad
3-Party Conferencing	Call Lists
Message Waiting Indication (MWI)	Speed dialing
Do-not-disturb (DND)	Picture Caller-ID
Voicemail	Alarm Clock

Server Profiles

Server Profiles

The Motivation:

- To increase snom m9 product ease of use and integration with 3rd party iPBXs
- To provide support for non-standard functionality of some of the most popular VoIP platforms in the market
- To limit tailored FW builds by providing a single FW release interoperable with a number of VoIP platforms

Server Profiles

Interoperability:

- Support for non-standard functionality may include any parameters relating to:
  - **SIP** (Implemented standards for Registration, Call Setup/Teardown, Call hold, Call transfer, Caller-id display, Music-on-hold, Mailbox, Conferencing, Presence)
  - **RTP** (Codec packetization, Payload length, Media encryption)

Server Profiles

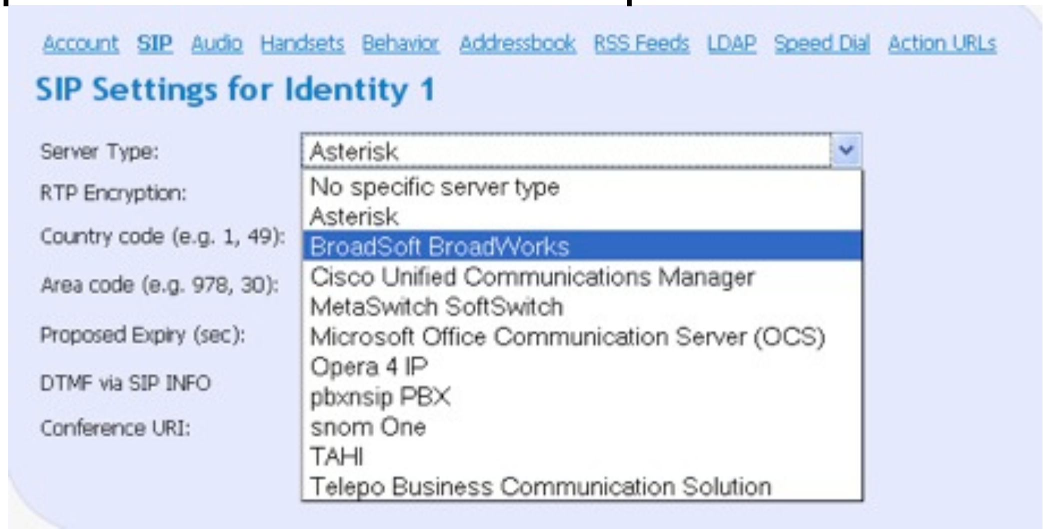
Supported Platforms:

- Microsoft Lync 2010
- Cisco Call Manager
- Broadsoft
- Asterisk
- snom ONE
- Metaswitch
- Telepo BCS
- Advoco NetPBX
- Avaya CM

Server Profiles

Setup:

- Located under the “SIP” tab of each Identity, the “Server Type” provides a convenient drop-down for server selection



Account SIP Audio Handsets Behavior Addressbook RSS Feeds LDAP Speed Dial Action URLs

SIP Settings for Identity 1

Server Type: Asterisk

RTP Encryption:

Country code (e.g. 1, 49):

Area code (e.g. 978, 30):

Proposed Expiry (sec):

DTMF via SIP INFO

Conference URI:

No specific server type
Asterisk
BroadSoft BroadWorks
Cisco Unified Communications Manager
MetaSwitch SoftSwitch
Microsoft Office Communication Server (OCS)
Opera 4 IP
pbxnsip PBX
snom One
TAHI
Telepo Business Communication Solution

Identity → SIP

CTI with Action URLs

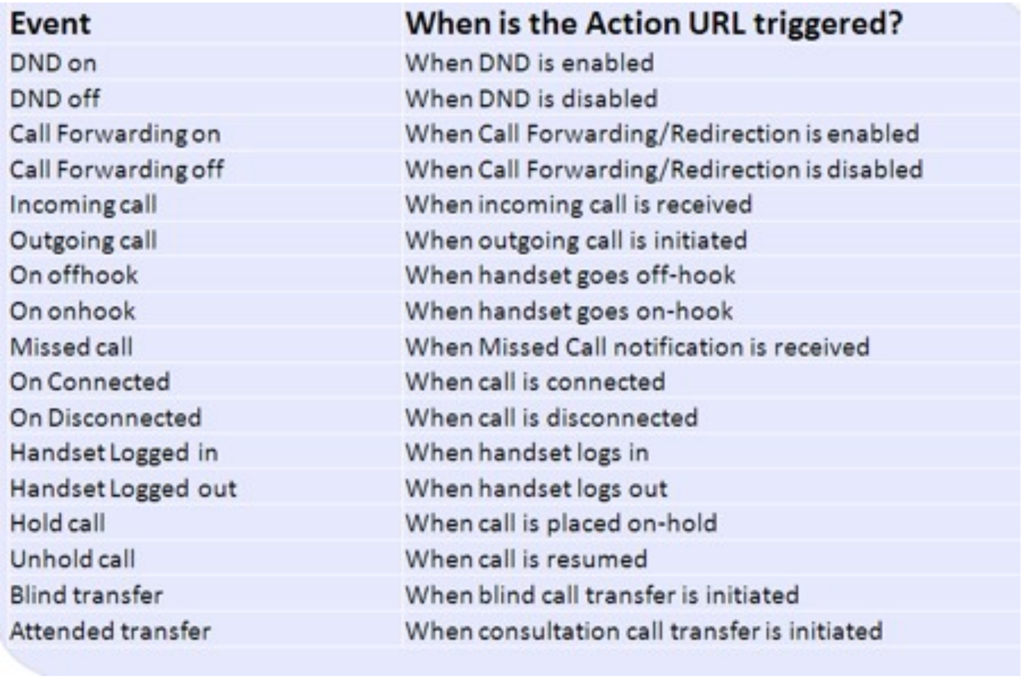
CTI with Action URLs

What are Action URLs:

- Action URLs are HTTP GET Requests allowing the phone to interact with web server applications for CTI and remote notification
- Action URLs can be triggered on the snom m9 by predefined events of each connected handset

CTI with Action URLs

What events are available:



Event	When is the Action URL triggered?
DND on	When DND is enabled
DND off	When DND is disabled
Call Forwarding on	When Call Forwarding/Redirection is enabled
Call Forwarding off	When Call Forwarding/Redirection is disabled
Incoming call	When incoming call is received
Outgoing call	When outgoing call is initiated
On offhook	When handset goes off-hook
On onhook	When handset goes on-hook
Missed call	When Missed Call notification is received
On Connected	When call is connected
On Disconnected	When call is disconnected
Handset Logged in	When handset logs in
Handset Logged out	When handset logs out
Hold call	When call is placed on-hold
Unhold call	When call is resumed
Blind transfer	When blind call transfer is initiated
Attended transfer	When consultation call transfer is initiated

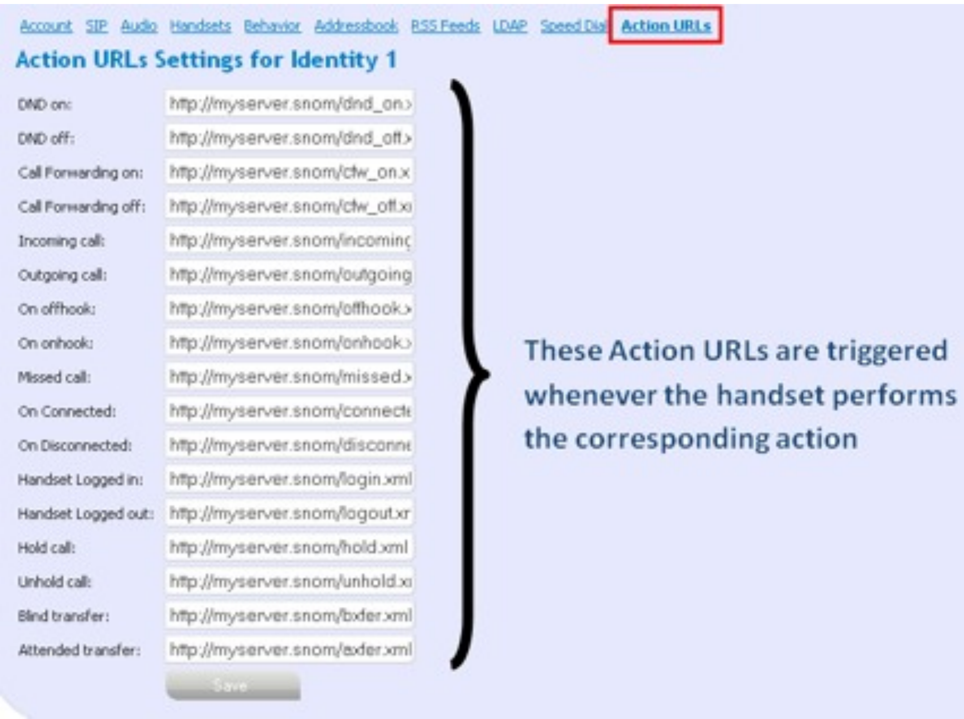
CTI with Action URLs

Setup:

- Each SIP Identity on the snom m9 base station provides this sets of Action URLs
- These Action URLs are triggered whenever a handset assigned to that Identity performs a particular action
- These Action URLs can either be configured manually for each Identity or can be automatically configured with a configuration server

CTI with Action URLs

Setup:



Action URLs Settings for Identity 1

DND on:	http://myserver.snom/dnd_on.
DND off:	http://myserver.snom/dnd_off.
Call Forwarding on:	http://myserver.snom/cfw_on.x
Call Forwarding off:	http://myserver.snom/cfw_off.x
Incoming call:	http://myserver.snom/incoming
Outgoing call:	http://myserver.snom/outgoing
On offhook:	http://myserver.snom/offhook.
On onhook:	http://myserver.snom/onhook.
Missed call:	http://myserver.snom/missed.
On Connected:	http://myserver.snom/connecte
On Disconnected:	http://myserver.snom/disconne
Handset Logged in:	http://myserver.snom/login.xml
Handset Logged out:	http://myserver.snom/logout.x
Hold call:	http://myserver.snom/hold.xml
Unhold call:	http://myserver.snom/unhold.x
Blind transfer:	http://myserver.snom/bxfer.xml
Attended transfer:	http://myserver.snom/axfer.xml

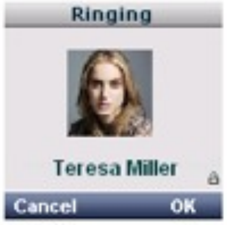
These Action URLs are triggered whenever the handset performs the corresponding action

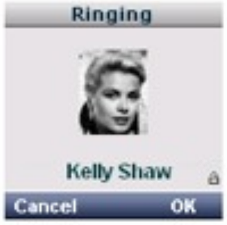
Picture Caller-ID

Picture Caller-ID

Overview:

- The caller picture feature allows the snom m9 Handset to display the picture of the calling party
- All photo pictures provided to the snom m9 Base Station must be in **40 × 50 Pixels JPEG** format





Picture Caller-ID

Mechanisms:

- **VCARDs:** Caller picture is displayed when the snom m9 has a VCARD with picture available for the calling party in the Address book
- **SIP “Call-Info”:** Alternatively, picture of the caller can also be sent to the snom m9 Handset, if the calling-party provides a SIP "Call-Info" header in the incoming call

Picture Caller-ID

VCARDs:

- The feature allows the snom m9 Handset to display the calling party picture via VCARDs
- In order to use this feature, the user need to create a 40x50 Pixel JPEG and assign it the contact’s VCARD
- The VCARD then needs to be uploaded to the snom m9 Base station
- The snom m9 Base station would then relay the contact’s picture to the handset when a call is received from the contact

Picture Caller-ID

Creating a VCARD with picture:

▪Select a Contact Card from “Contacts” or create a new Contact under File→New→Contact

▪Click on “Add Contact Picture” and upload the picture of the contact in **40 × 50 Pixels JPEG format**

▪Click on “Save and Close” to save the contact

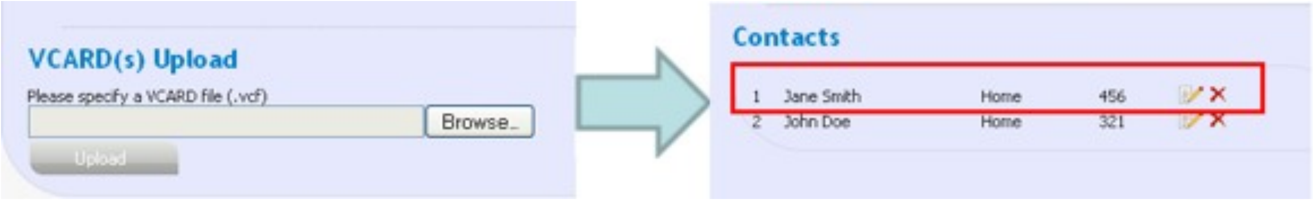
▪Right click on the contact and click on “Send as Business Card”

▪Right click on the **.vcf** file and Copy Paste the file on your computer

Picture Caller-ID

Uploading the VCARD to snom m9:

- ▪Select the Identity for which you want to add the VCARD
- ▪Upload the VCARD through the “VCARD(s) Upload” section
- ▪The newly added VCARD should be visible under “Contacts”
- ▪The picture of “Contact” will be displayed on the associated handset whenever a call is received from the “Contact”



Please specify a VCARD file (.vcf)

1	Jane Smith	Home	456
2	John Doe	Home	321

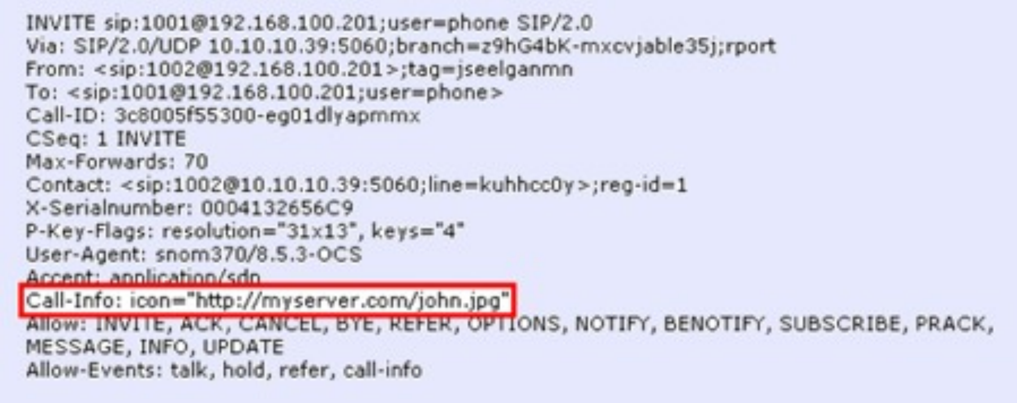
Picture Caller-ID

SIP “Call-Info”:

- The snom m9 is also able to display the calling party picture on the handset, via HTTP links
- For this purpose, the snom m9 Base station support the “icon” parameter of the SIP “Call-Info” header
- HTTP(s) links received in the “**icon**” parameter are processed and the photo is downloaded for display on the handset

Picture Caller-ID

- The Calling-party provides his picture in the “Call-Info” header of the SIP INVITE
- The “icon” parameter is used to specify the picture URL
- The snom m9 downloads the picture from the link and displays it on the handset



```
INVITE sip:1001@192.168.100.201;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.10.10.39:5060;branch=z9hG4bK-mxcvjable35j;rport
From: <sip:1002@192.168.100.201>;tag=jseelganmn
To: <sip:1001@192.168.100.201;user=phone>
Call-ID: 3c8005f55300-eg01dlyapmmx
CSeq: 1 INVITE
Max-Forwards: 70
Contact: <sip:1002@10.10.10.39:5060;line=kuhhcc0y>;reg-id=1
X-Serialnumber: 0004132656C9
P-Key-Flags: resolution="31x13", keys="4"
User-Agent: snom370/8.5.3-OCS
Accept: application/sdp
Call-Info: icon="http://myserver.com/john.jpg"
Allow: INVITE, ACK, CANCEL, BYE, REFER, OPTIONS, NOTIFY, BENOTIFY, SUBSCRIBE, PRACK,
MESSAGE, INFO, UPDATE
Allow-Events: talk, hold, refer, call-info
```

LDAP

LDAP

Overview:

- Lightweight Directory Access Protocol (LDAP), is an Internet protocol that a device can use to look up contact information from a server
- Information retrieved from an LDAP server may include a contact's:
  - Name
  - Email Address
  - Telephone number(s)
  - Address
  - Photo(s)

LDAP

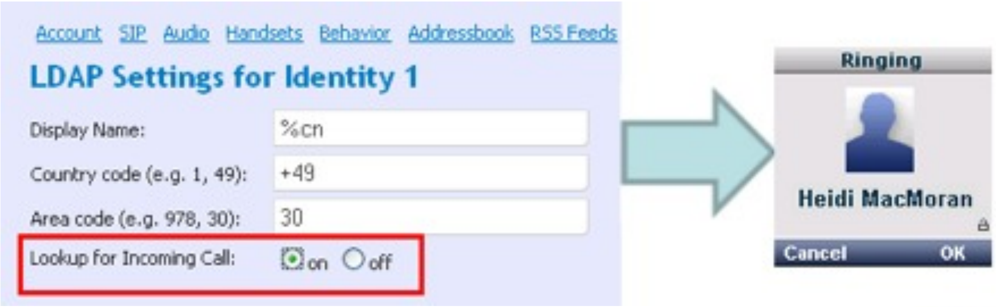
What LDAP features are available on the snom m9?

- LDAP can be used to retrieve Caller-ID related information from an LDAP server for incoming calls
- LDAP may also be used to view corporate address book (s) on the snom m9 Handset, and subsequently calling the contacts from the LDAP address book

LDAP

Caller-ID lookup with LDAP:

- This feature allows the snom m9 base station to retrieve the calling-party name from the LDAP server when an incoming call is received
- If the server returns a valid name for the calling number, the snom m9 base relays the calling party name to the associated handset



LDAP Settings for Identity 1

Display Name: %cn

Country code (e.g. 1, 49): +49

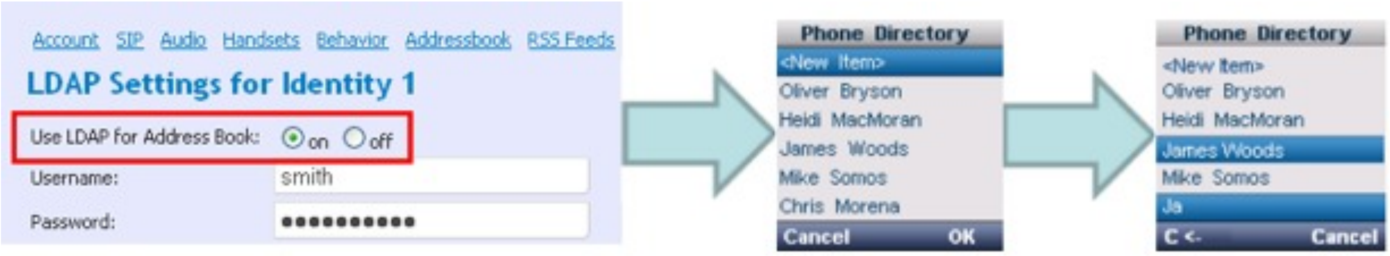
Area code (e.g. 978, 30): 30

Lookup for Incoming Call: ● on ○ off

LDAP

Address book searching:

- On the snom m9, LDAP can also be used to view the corporate address book and subsequently place telephone calls to the contacts
- The snom m9 handset further allows the user to search through the LDAP address book returned from the server



LDAP Settings for Identity 1

Use LDAP for Address Book: ● on ○ off

Username: smith

Password: ●●●●●●●●●●●

Phone Directory

<New Item>
Oliver Bryson
Heidi MacMoran
James Woods
Mike Somos
Chris Morena

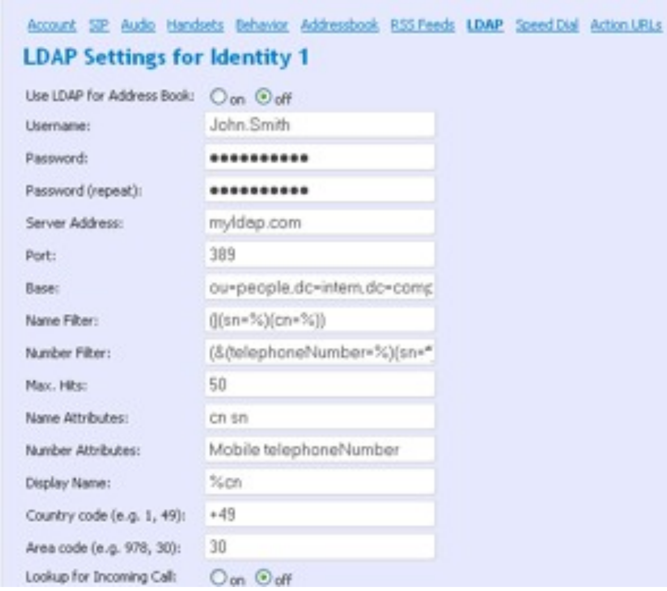
Phone Directory

<New Item>
Oliver Bryson
Heidi MacMoran
James Woods
Mike Somos
Ja

LDAP

Setup:

- Located under the “LDAP” tab of each Identity, the “LDAP” settings allow a fully customizable setup



LDAP Settings for Identity 1

Use LDAP for Address Book:	○ on ● off
Username:	John.Smith
Password:	●●●●●●●●●●●
Password (repeat):	●●●●●●●●●●●
Server Address:	myldap.com
Port:	389
Base:	ou=people.dc=intern.dc=comp
Name Filter:	(|(sn=%)(cn=%))
Number Filter:	(&(telephoneNumber=%)(sn=*
Max. Hits:	50
Name Attributes:	cn sn
Number Attributes:	Mobile telephoneNumber
Display Name:	%cn
Country code (e.g. 1, 49):	+49
Area code (e.g. 978, 30):	30
Lookup for Incoming Call:	○ on ● off

IPv6

IPv6

IPv4 Issues:

- Internet is running out of Internet addresses
- Insufficient internet routing leading NAT usage
- Network security is optional and no single standard exists for security (IPSEC, SSL etc.)
- New applications are becoming more demanding and will require guaranteed bandwidth and security
- Mobility in IPv4 Networks (Mobile IP) is unclear and difficult to manage

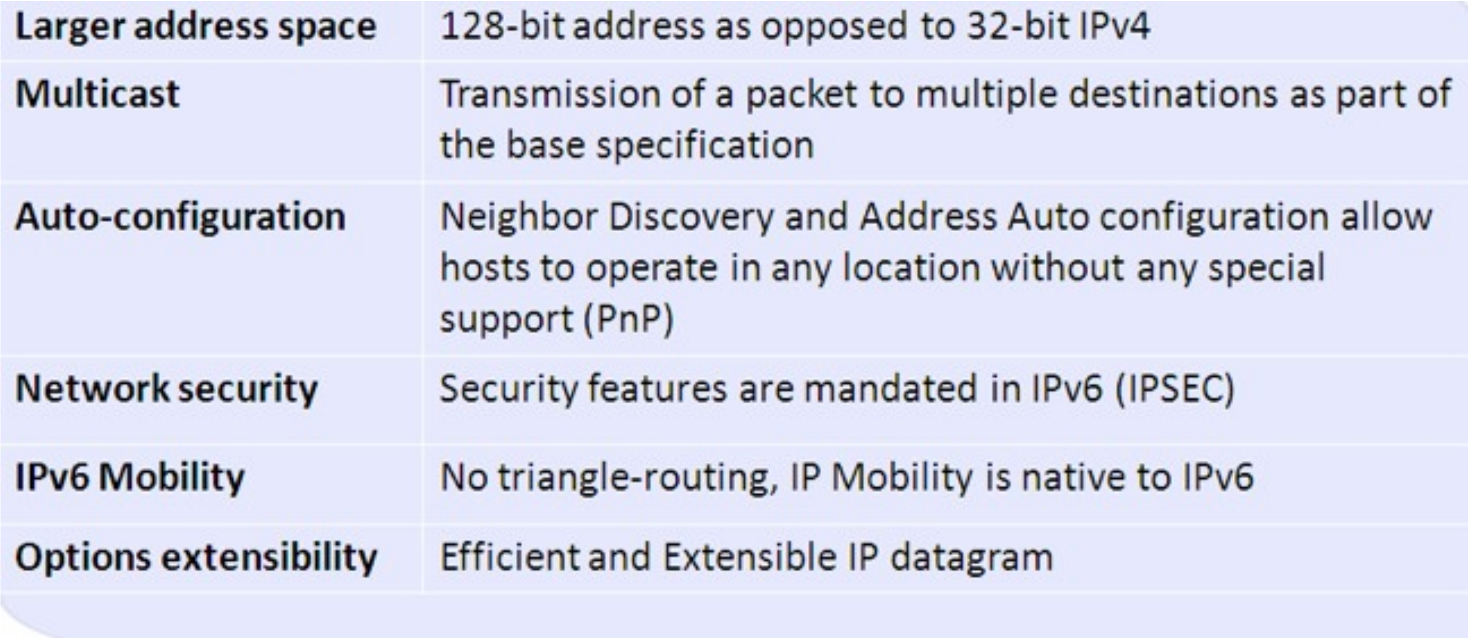
IPv6

What is IPv6?

- **Internet Protocol Version 6** (IPv6) is a version of the Internet Protocol that is the successor of Internet Protocol version 4 (IPv4) which is the current Internet Protocol in operation since 1981
- Mainly introduced to expand the internet address space available (128-bit addresses compared to 32-bit addresses of IPv6)

IPv6

Primary Advantages:



Larger address space	128-bit address as opposed to 32-bit IPv4
Multicast	Transmission of a packet to multiple destinations as part of the base specification
Auto-configuration	Neighbor Discovery and Address Auto configuration allow hosts to operate in any location without any special support (PnP)
Network security	Security features are mandated in IPv6 (IPSEC)
IPv6 Mobility	No triangle-routing, IP Mobility is native to IPv6
Options extensibility	Efficient and Extensible IP datagram

IPv6 on snom m9

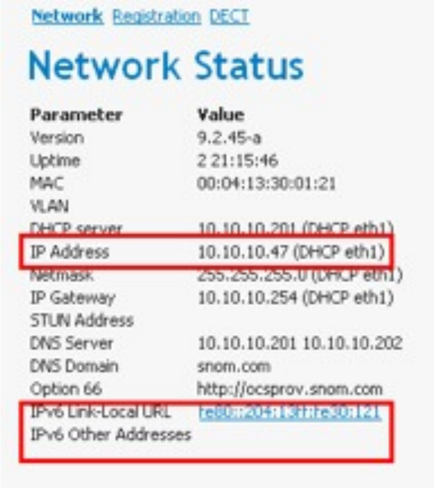
Address assignment and auto configuration

- The snom m9 is able to automatically assign an IPv6 address to the device over DHCPv6
- Further more, when connected to an IPv6 network, the snom m9 can configure itself automatically using Internet Control Message Protocol version 6 (ICMPv6) router discovery messages
- The Dual-IP-Stack allows snom m9 to maintain IPv4 and IPv6 interfaces in parallel

IPv6 on snom m9

Dual IP Stack

- The ability to perform DHCPv6/ICMPv6 queries in addition to the IPv4 DHCP queries simultaneously, allows the snom m9 to maintain multiple IPv4 and IPv6 interfaces in parallel



Network Registration DECT

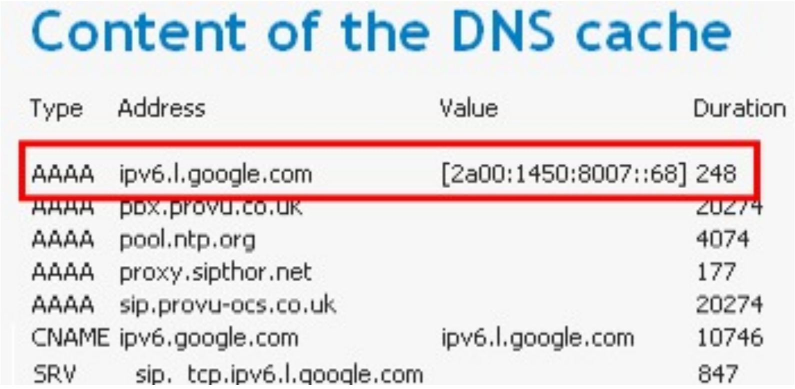
Network Status

Parameter	Value
Version	9.2.45-a
Uptime	2 21:15:46
MAC	00:04:13:30:01:21
VLAN	
DHCP server	10.10.10.201 (DHCP eth1)
IP Address	10.10.10.47 (DHCP eth1)
Netmask	255.255.255.0 (DHCP eth1)
IP Gateway	10.10.10.254 (DHCP eth1)
STUN Address	
DNS Server	10.10.10.201 10.10.10.202
DNS Domain	snom.com
Option 66	http://ocsprov.snom.com
IPv6 Link-Local URL	fe80::204:13ff:fe30:121
IPv6 Other Addresses	

IPv6 on snom m9

DNS

- Support for IPv6 naturally allows the snom m9 to perform AAAA queries for IPv6 address lookup
- For routing packets to IPv6 destinations, snom m9 uses its local IPv6 interface, if available



Content of the DNS cache

Type	Address	Value	Duration
AAAA	ipv6.l.google.com	[2a00:1450:8007::68]	248
AAAA	pbx.provu.co.uk		20274
AAAA	pool.ntp.org		4074
AAAA	proxy.sipthor.net		177
AAAA	sip.provu-ocs.co.uk		20274
CNAME	ipv6.google.com	ipv6.l.google.com	10746
SRV	sip. tcp.ipv6.l.google.com		847

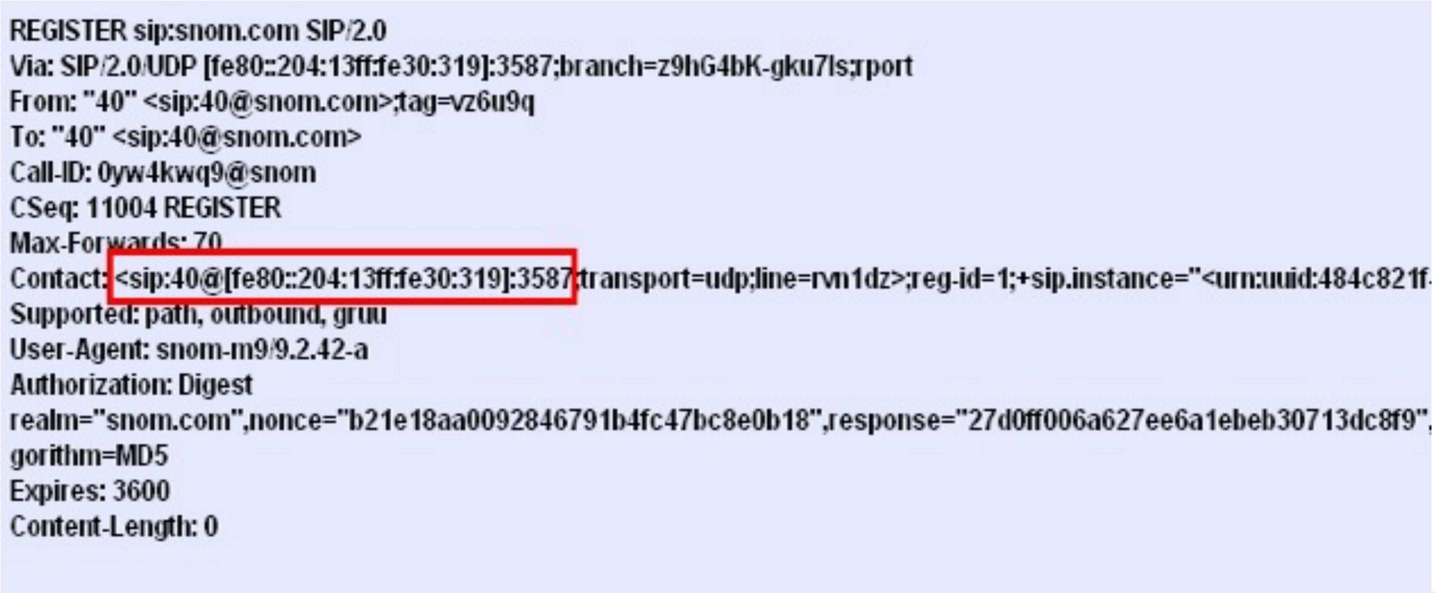
IPv6 on snom m9

SIP

- Depending on the type of address returned (IPv4 or IPv6) for a SIP server, the snom m9 automatically selects the corresponding IP interface for registration
- SIP packet addresses and headers are also automatically substituted with the appropriate IP interface

IPv6 on snom m9

Registration sample



```
REGISTER sip:snom.com SIP/2.0
Via: SIP/2.0/UDP [fe80::204:13ff:fe30:319]:3587;branch=z9hG4bK-gku7ls;rport
From: "40" <sip:40@snom.com>;tag=vz6u9q
To: "40" <sip:40@snom.com>
Call-ID: 0yw4kwq9@snom
CSeq: 11004 REGISTER
Max-Forwards: 70
Contact: <sip:40@[fe80::204:13ff:fe30:319]:3587;transport=udp;line=rvn1dz>;reg-id=1;+sip.instance="<urn:uuid:484c821f-
Supported: path, outbound, gruu
User-Agent: snom-m9/9.2.42-a
Authorization: Digest
realm="snom.com",nonce="b21e18aa0092846791b4fc47bc8e0b18",response="27d0ff006a627ee6a1ebeb30713dc8f9",
gorithm=MD5
Expires: 3600
Content-Length: 0
```

Security

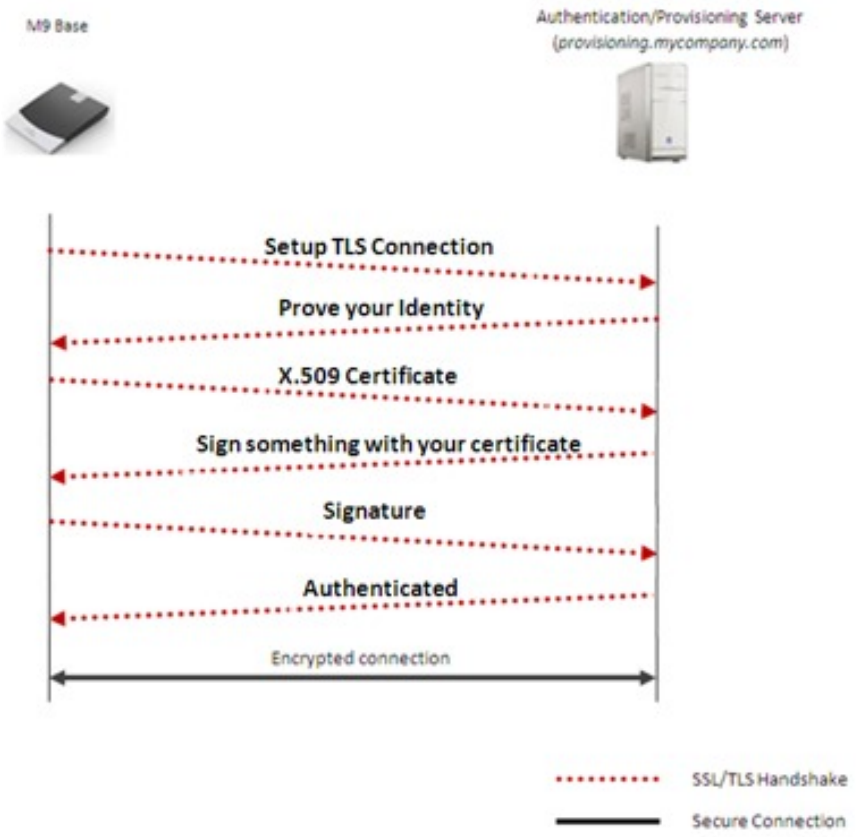
Certificates

- Each snom m9 base station comes equipped with a unique **X.509 certificate** signed by **“snom CA”** as default
- These **“Client Certificates”** allow the SIP server or Configuration server to verify the snom m9 base as an authentic device on the network
- The m9 base station is also able to perform **“Server Identity Verification”** based on trusted X.509 chains when SSL/TLS is used

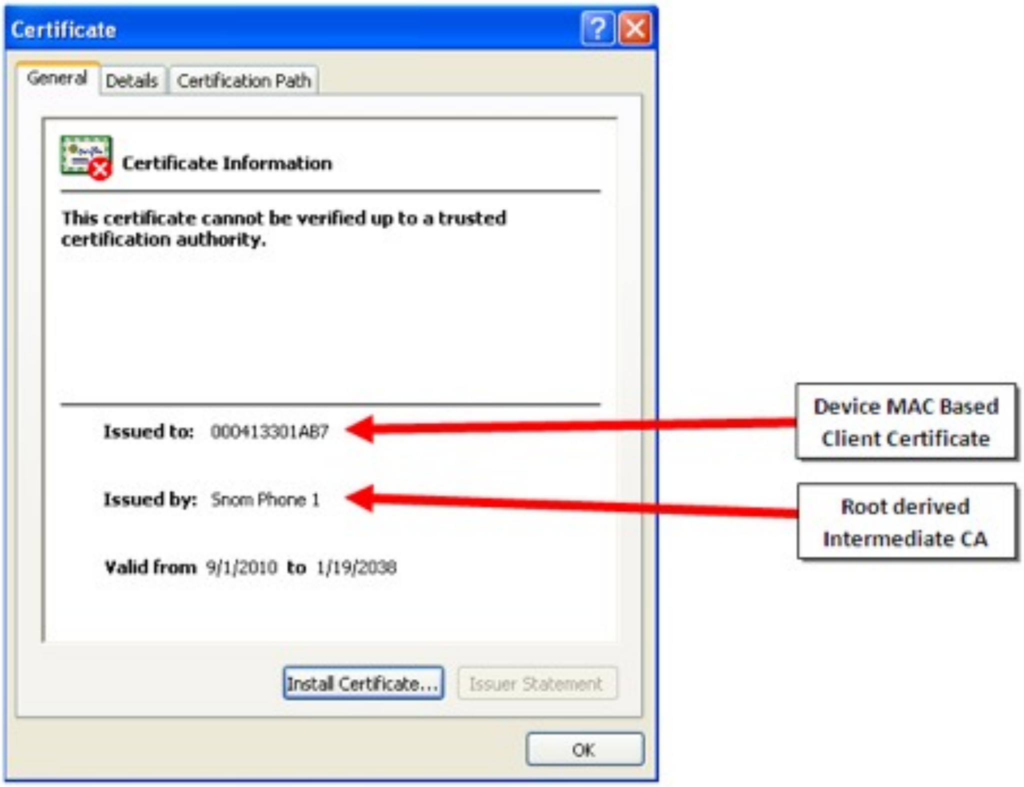
Client Certificates

- Client Certificates allow an SSL/TLS server to verify the identity of a connecting client
- The verifying server can be co-located within a SIP server, a configuration server or can be an independent network entity
- This mechanism of identity verification also eliminates the need for standard authentication mechanisms such as Username/Password authentication

Client Verification



Certificate Format



Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: 000413301AB7

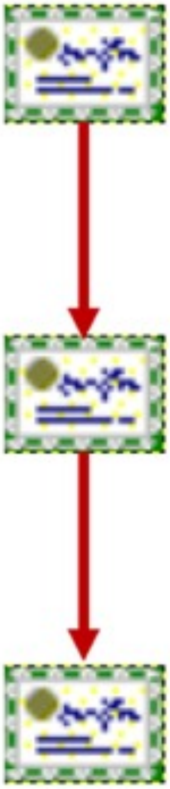
Issued by: Snom Phone 1

Valid from 9/1/2010 to 1/19/2038

Device MAC Based Client Certificate

Root derived Intermediate CA

Default Chain-of-Trust



snom AG
(Root CA)

The default snom root CA
“Snom Technology AG CA”

Snom Phone 1
(Intermediary CA)

snom Intermediary CA derived from the snom root CA

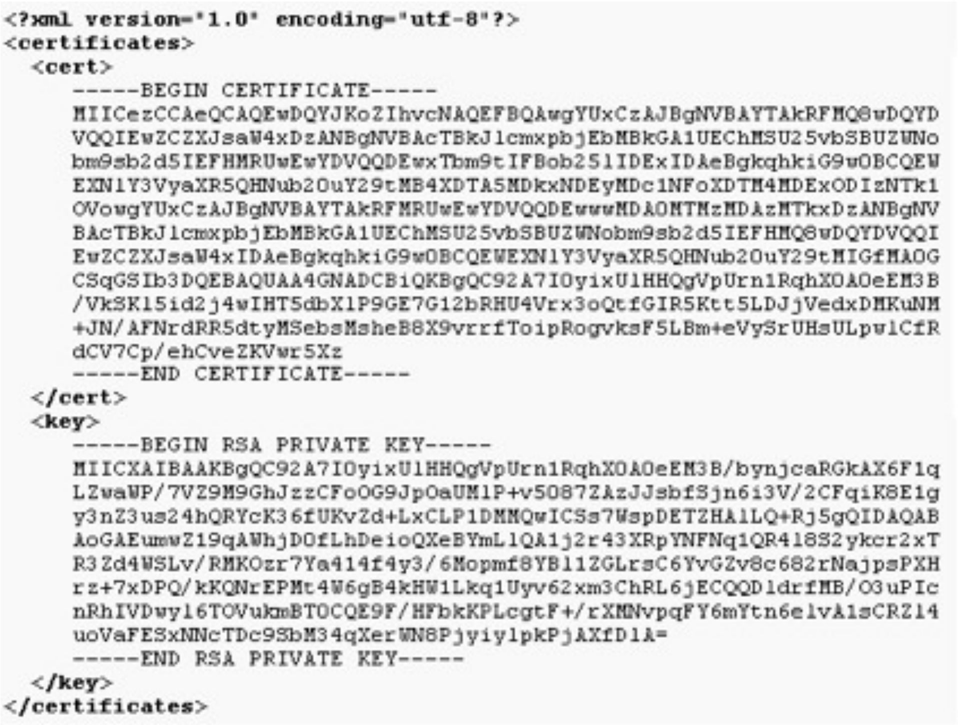
000413301AB7
(m9 Base Certificate)

MAC based device client certificate derived from the intermediary CA

Custom Client Certificates

- The client certificate of the snom m9 can also be customized by loading custom client certificate/private key pairs to the device
- Embedded within an XML file with **<cert>** and **<key>** tags, the snom m9 can be auto configured to customize the client Identity of snom m9
- Both these **<cert>** and **<key>** tags need to be encapsulated within a **<certificates>** XML tag

Example XML



```
<?xml version='1.0' encoding='utf-8'?>
<certificates>
  <cert>
     -----BEGIN CERTIFICATE-----
     MIICezCCAeQCAQEwDQYJKoZIhvcNAQEFBQAwgYUxCzAJBgNVBAYTAkRFMQ8wDQYD
     VQQIEwZCZXJsaW4xDzANBgNVBAcTBkJlcmxpbjEbMBkGA1UEChMSU25vbSBUZWNo
     bm9sb2d5IEFHMRUwEwYDVQQDEwxTbm9tIFBob25lIDExIDAeBgkqhkiG9w0BCQEW
     EXN1Y3VyaXR5QHNub20uY29tMB4XDTA5MDkxNDEyMDc1NFoXDTM4MDExODIzNTk1
     OVowgYUxCzAJBgNVBAYTAkRFMRUwEwYDVQQDEwwwMDA0MTMzMDAzMTkxDzANBgNV
     BAcTBkJlcmxpbjEbMBkGA1UEChMSU25vbSBUZWNobm9sb2d5IEFHMQ8wDQYDVQQI
     EwZCZXJsaW4xIDAeBgkqhkiG9w0BCQEWEXN1Y3VyaXR5QHNub20uY29tMIGfMA0G
     CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC92A7IOyixUlHHQgVpUrn1RqhX0A0eEM3B
     /VkSKl5id2j4wIHT5dbX1P9GE7G12bRHU4Vrx3oQtfGIR5Ktt5LDJjVedxDMKuNM
     +JN/AFNrdRR5dtyMSebsMsheB8X9vrrfToipRogvksF5LBm+eVySrUHsULpwlCfR
     dCV7Cp/ehCveZKVwr5Xz
     -----END CERTIFICATE-----
  </cert>
  <key>
     -----BEGIN RSA PRIVATE KEY-----
     MIICXAIBAAKBgQC92A7IOyixUlHHQgVpUrn1RqhX0A0eEM3B/bynjcaRGkAX6F1q
     LZwaWP/7VZ9M9GhJzzCFoOG9JpOaUMlP+v5087ZAzJJsbfSjn6i3V/2CFqiK8E1g
     y3nZ3us24hQRYcK36fUKvZd+LxCLP1DMMQwICSs7WspDETZHAlLQ+Rj5gQIDAQAB
     AoGAEumwZ19qAWhjD0fLhDeioQXeBYmLlQA1j2r43XRpYNFNq1QR418S2ykcr2xT
     R3Zd4WSLv/RMKOzr7Ya414f4y3/6Mopmf8YB11ZGLrsC6YvGZv8c682rNajpsPXH
     rz+7xDPQ/kKQNrEPMt4W6gB4kHW1Lkq1Uyv62xm3ChRL6jECQQDldrfMB/O3uPIc
     nRhIVDwyl6TOVukmBTOCQE9F/HFbkKPLcgtF+/rXMNvpqFY6mYtn6elvA1sCRZl4
     uoVaFESxNNcTDc9SbM34qXerWN8PjyiylpkPjAXfDlA=
     -----END RSA PRIVATE KEY-----
  </key>
</certificates>
```

Custom Client Certificate

Custom Private Key

Server Identity Verification

- The snom m9 base station is able to perform **“Server Identity Verification”** based on trusted X.509 chains when SSL/TLS is used
- Servers which present certificates signed by CAs unknown to the base are rejected
- By default, the snom m9 is designed to authenticate all SSL servers based on a chain-of-trust

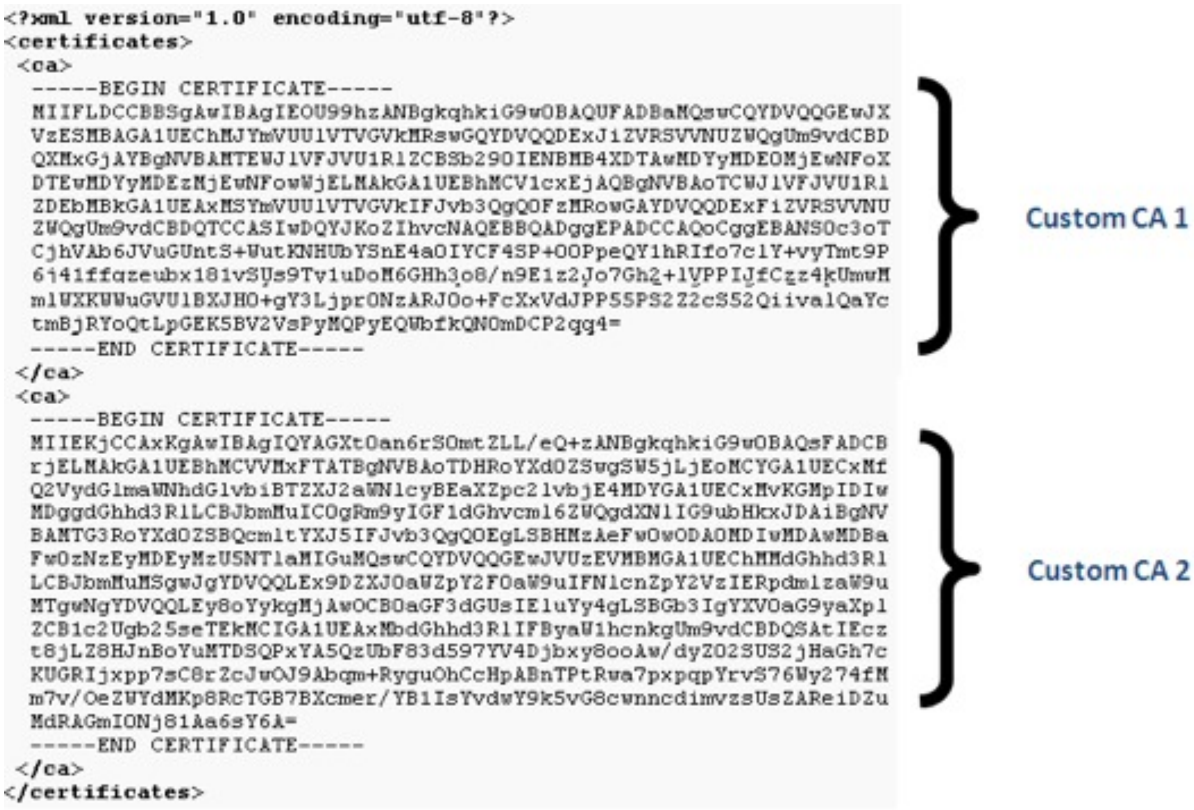
Certification Authorities (CA)

- A Certificate authority or Certification authority (CA) is an entity that issues digital certificates
- In cyber world, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate

Custom CA Setup

- Trusted Root CAs can also be customized on the snom m9 to tailor **“Server Identity Verification”**
- With **<certificates>** as the top XML tag, each trusted root CA can be enclosed within a **<ca>** tag

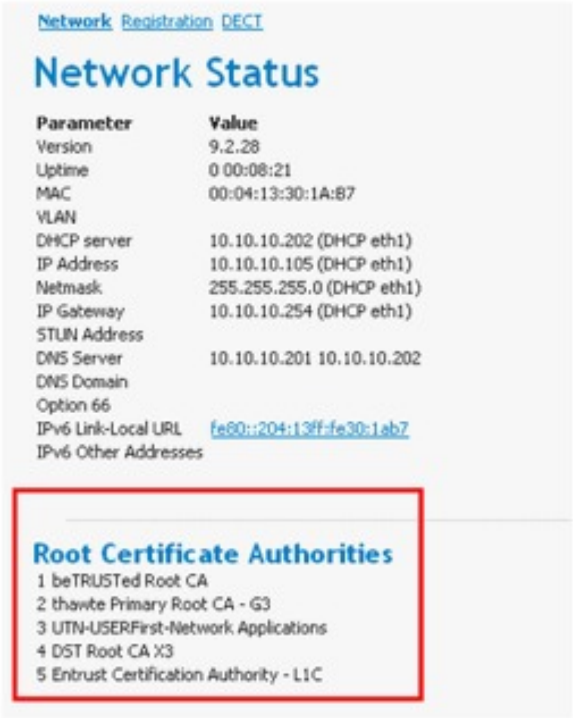
Example XML



```
<?xml version="1.0" encoding="utf-8"?>
<certificates>
 <ca>
  -----BEGIN CERTIFICATE-----
  MIIFLDCCBBSgAwIBAgIEOU99hzANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQGEwJX
  VzESMBAGA1UEChMJYmVUU1VTVGVkMRswGQYDVQQDExJ1ZVRSVVNUZWQgUm9vdCBD
  QXMxGjAYBgNVBAMTEWJ1VFJVU1R1ZCBSb290IENBMB4XDTAwMDYyMDE0MjEwNFoX
  DTEwMDYyMDEzMjEwNFowWjELMAkGA1UEBhMCV1cxEjAQBgNVBAoTCWJ1VFJVU1R1
  ZDEbMBkGA1UEAxMSYmVUU1VTVGVkIFJvb3QgQ0FzMRowGAYDVQQDExF1ZVRSVVNU
  ZWQgUm9vdCBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANS0c3oT
  CjhVAb6JVuGUntS+WutKNHUbYSnE4a0IYCF4SP+00PpeQY1hRIfo7c1Y+vyTmt9P
  6j41ffqzeubx181vSUs9Tv1uDoM6GHh3o8/n9E1z2Jo7Gh2+1VPPIJfCzz4kUmwM
  m1WXKWWuGVU1BXJHO+gY3LjprONzARJOo+FcXxVdJPP55PS2Z2cS52QiivalQaYc
  tmBjRYoQtLpGEK5BV2VsPyMQPyEQWbfkQNOmDCP2qq4=
  -----END CERTIFICATE-----
 </ca>
 <ca>
  -----BEGIN CERTIFICATE-----
  MIIEKjCCAxKgAwIBAgIQYAGXt0an6rS0mtZLL/eQ+zANBgkqhkiG9w0BAQsFADCB
  rjELMAkGA1UEBhMCVVMxFTATBgNVBAoTDHRoYXd0ZSwgSW5jLjEoMCYGA1UECxMf
  Q2VydGlmaWNhdGlvbiBTZXJ2aWNlcyBEaXZpc2lvbjE4MDYGA1UECxMvKGMpIDIw
  MDggdGhhd3R1LCBJbmMuIC0gRm9yIGF1dGhvcml6ZWQgdXNlIG9ubHkxJDAiBgNV
  BAMTG3RoYXd0ZSBQcmltYXJ5IFJvb3QgQ0EgLSBHMzAeFw0wODA0MDIwMDAwMDBa
  Fw0zNzEyMDEyMzU5NTlaMIGuMQswCQYDVQQGEwJVUzEVMBMGA1UEChMMdGhhd3R1
  LCBJbmMuMSgwJgYDVQQLEx9DZXJ0aWZpY2F0aW9uIFN1cnZpY2VzIERpdmlzaW9u
  MTgwNgYDVQQLEy8oYykgMjAwOCB0aGF3dGUsIE1uYy4gLSBGb3IgYXV0aG9yaXp1
  ZCB1c2Ugb25seTEkMCIGA1UEAxMbdGhhd3R1IFByaW1hcnkgUm9vdCBDQSAtIEcz
  t8jLZ8HJnBoYuMTDSQPxYA5QzUbF83d597YV4Djbxy8ooAw/dyZ02SUS2jHaGh7c
  KUGRIjxpp7sC8rZcJwOJ9Abqm+RyguOhCcHpABnTPtRwa7pxpqpYrvS76Wy274fM
  m7v/OeZWYdMKp8RcTGB7BXcmer/YB1IsYvdwY9k5vG8cwnncdimvzsUsZAReiDZu
  MdRAGmIONj81Aa6sY6A=
  -----END CERTIFICATE-----
 </ca>
</certificates>
```

CA Overview

Status → Network → Root Certificate Authorities



Network Registration DECT

Network Status

Parameter	Value
Version	9.2.28
Uptime	0 00:08:21
MAC	00:04:13:30:1A:B7
VLAN	
DHCP server	10.10.10.202 (DHCP eth1)
IP Address	10.10.10.105 (DHCP eth1)
Netmask	255.255.255.0 (DHCP eth1)
IP Gateway	10.10.10.254 (DHCP eth1)
STUN Address	
DNS Server	10.10.10.201 10.10.10.202
DNS Domain	
Option 66	
IPv6 Link-Local URL	fe80::204:13ff:fe30:1ab7
IPv6 Other Addresses	

Root Certificate Authorities

1 beTRUSTed Root CA
2 thawte Primary Root CA - G3
3 UTN-USERFirst-Network Applications
4 DST Root CA X3
5 Entrust Certification Authority - L1C

Auto Configuration

Auto Configuration

- To administer a large pool of snom m9 devices, the device provides the possibility to configure settings and upgrade device Firmware with zero-touch interaction from the user
- These mechanisms allow the administrator to manage and monitor all snom m9 devices in the network remotely

Note: All auto configuration mechanisms discussed in this section can also be provided in a secure manner as discussed in the “**Security**” section

Auto Configuration

Automatic Setup

- The most convenient way of auto configuring a snom m9 is via DHCP options 66 and 67
- DHCP option 66 and 67 provide an HTTP(S) or TFTP configuration server's address and a boot file-name for download
- Upon receiving the said DHCP options, the snom m9 connects to the configuration server and downloads its configuration file

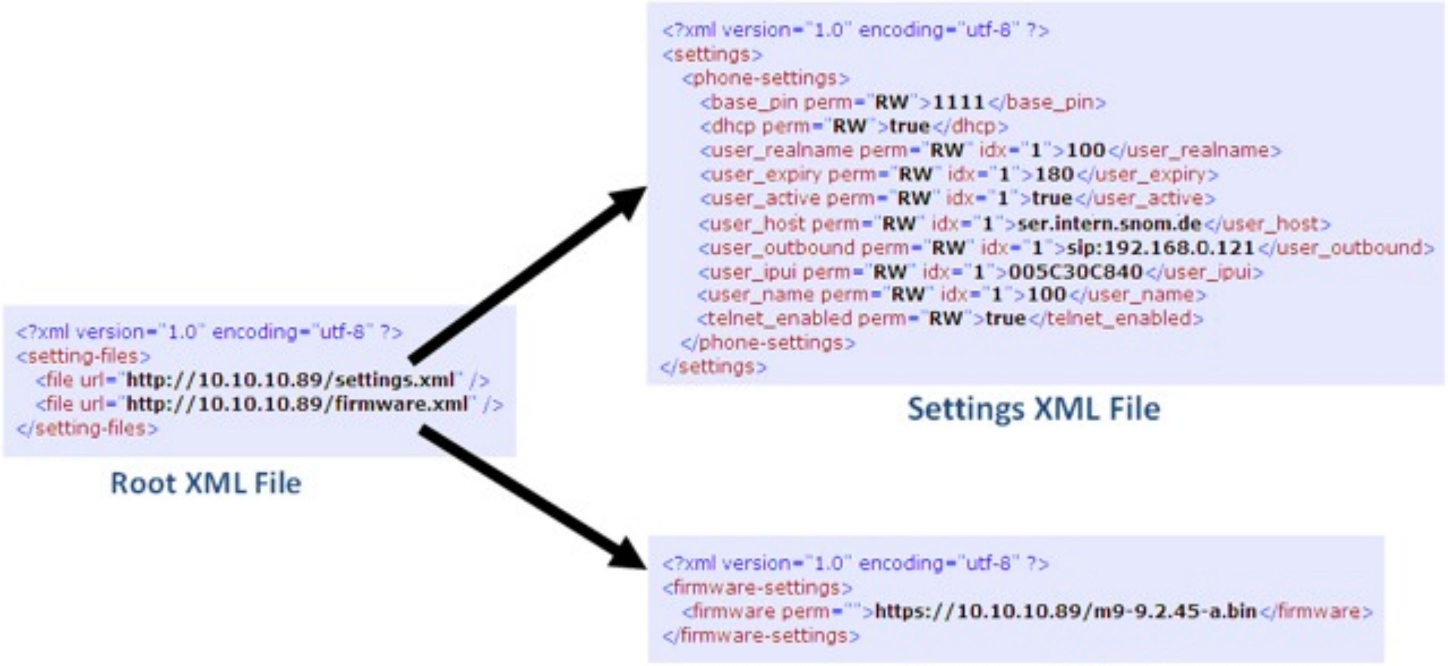
Auto Configuration

Automatic Firmware Upgrade

- The boot-file provided by the DHCP server may also contain a link to a newer version of the snom m9 Firmware
- In case a new Firmware is provided in the configuration file, the snom m9 downloads the Firmware and performs an automatic reboot
- This automatic Firmware upgrade mechanism makes the maintenance of device very convenient

Auto Configuration

XML Structures



```xml
<?xml version="1.0" encoding="utf-8" ?>
<setting-files>
  <file url="http://10.10.10.89/settings.xml" />
  <file url="http://10.10.10.89/firmware.xml" />
</setting-files>
```

Root XML File

```xml
<?xml version="1.0" encoding="utf-8" ?>
<settings>
  <phone-settings>
    <base_pin perm="RW">1111</base_pin>
    <dhcp perm="RW">true</dhcp>
    <user_realname perm="RW" idx="1">100</user_realname>
    <user_expiry perm="RW" idx="1">180</user_expiry>
    <user_active perm="RW" idx="1">true</user_active>
    <user_host perm="RW" idx="1">ser.intern.snom.de</user_host>
    <user_outbound perm="RW" idx="1">sip:192.168.0.121</user_outbound>
    <user_ipui perm="RW" idx="1">005C30C840</user_ipui>
    <user_name perm="RW" idx="1">100</user_name>
    <telnet_enabled perm="RW">true</telnet_enabled>
  </phone-settings>
</settings>
```

Settings XML File

```xml
<?xml version="1.0" encoding="utf-8" ?>
<firmware-settings>
  <firmware perm="">https://10.10.10.89/m9-9.2.45-a.bin</firmware>
</firmware-settings>
```

Firmware XML File

Microsoft® Lync 2010 Setup

Microsoft® Lync 2010 Setup

- snom m9 provides native Microsoft Lync® 2010 support in its Firmware
- The “Microsoft Office Communications Server” profile provides a one-click integration possibility with this popular telephony platform

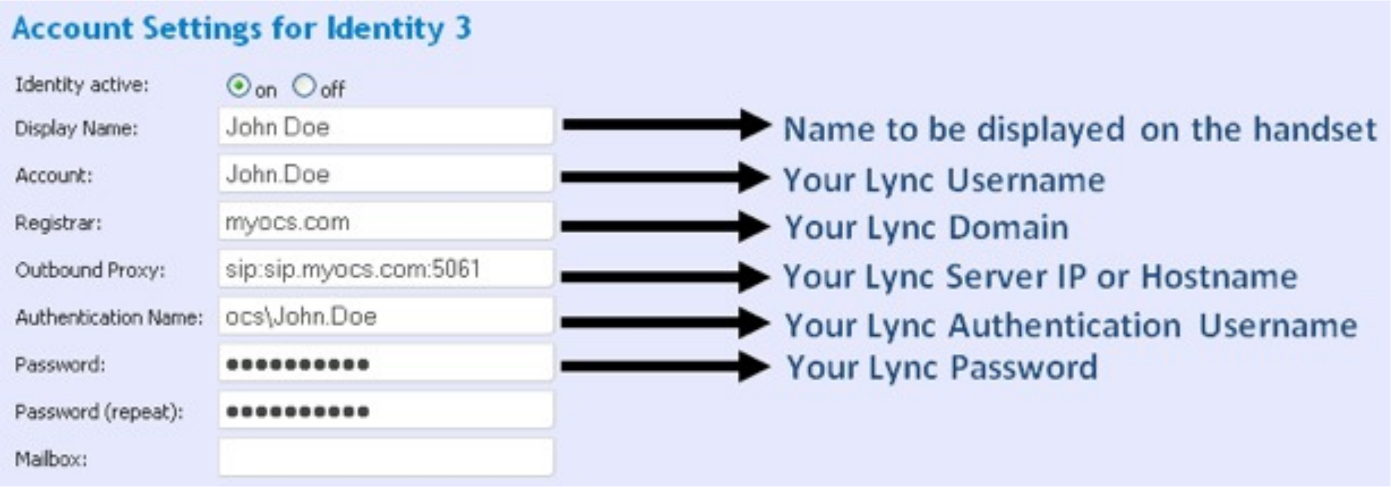
Microsoft® Lync 2010 Setup

Supported Features on snom m9:

- Basic calling
- Call Hold
- Call Transfer
- 3-party Conference
- Play-on-phone (MS Exchange Server)
- Voicemail (MS Exchange Server)
- Presence state notification

Microsoft® Lync 2010 Setup

Setup:



Account Settings for Identity 3

Identity active:	● on ○ off
Display Name:	John Doe
Account:	John.Doe
Registrar:	myocs.com
Outbound Proxy:	sip:sip.myocs.com:5061
Authentication Name:	ocs\John.Doe
Password:	●●●●●●●●●●●
Password (repeat):	●●●●●●●●●●●
Mailbox:	

Name to be displayed on the handset

Your Lync Username

Your Lync Domain

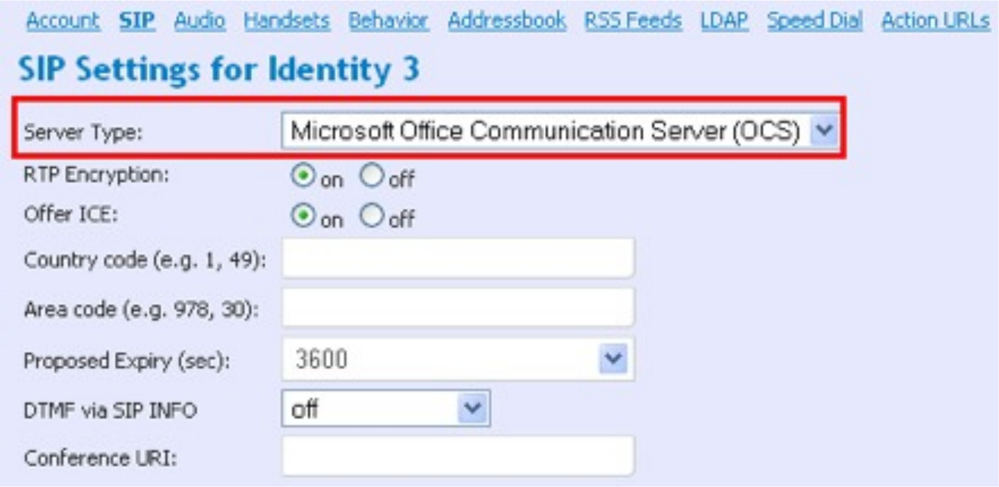
Your Lync Server IP or Hostname

Your Lync Authentication Username

Your Lync Password

Microsoft® Lync 2010 Setup

Setup:



Account SIP Audio Handsets Behavior Addressbook RSS Feeds LDAP Speed Dial Action URLs

SIP Settings for Identity 3

Server Type:	Microsoft Office Communication Server (OCS)
RTP Encryption:	● on ○ off
Offer ICE:	● on ○ off
Country code (e.g. 1, 49):	
Area code (e.g. 978, 30):	
Proposed Expiry (sec):	3600
DTMF via SIP INFO	off
Conference URI:	

Microsoft® Lync 2010 Setup

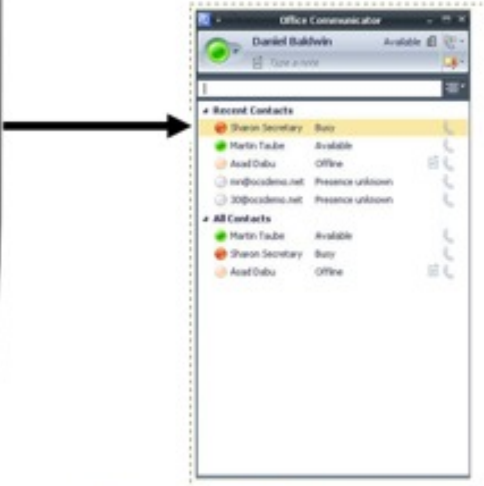
Presence:

- snom m9 also supports the Presence Protocol used by Microsoft® Lync 2010 and Microsoft Office Communicator
- Depending on the activity, the snom m9 publishes its presence state to the server reflecting states such as Online, Offline, In-call, Away, Busy and Do-not-disturb
- The presence activity of the snom m9 user can be viewed on the Microsoft Office Communicator or on other Lync 2010 compatible device

Microsoft® Lync 2010 Setup

Presence:

snom m9 Handset


Office Communicator

Daniel Baldwin Available

Type a note

Recent Contacts

Sharon Secretary	Busy
Martin Taube	Available
Asad Dabu	Offline
nn@ocsdemo.net	Presence unknown
30@ocsdemo.net	Presence unknown

All Contacts

Martin Taube	Available
Sharon Secretary	Busy
Asad Dabu	Offline

Microsoft® Office Communicator 2007 R2

Diagnostics

Diagnostics

- To increase responsiveness toward customers and reduce customer support overhead, the snom m9 provides a number of mechanisms for device diagnostics
- Such tools allow snom's to provide a solution to customer reported issues in an efficient manner, even in the absence of physical access to the device

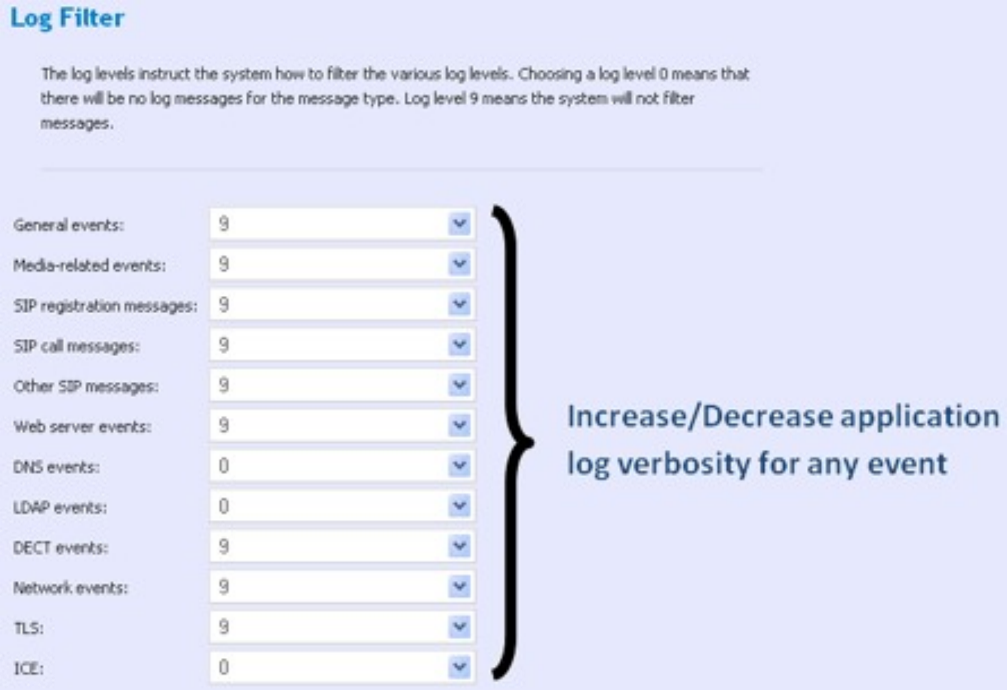
Diagnostics

Application Log:

- The snom m9 software provides an event driven application event logging interface
- Events which may trigger device logging may include SIP, TLS, Media, DECT or LDAP
- Further more, the device provides a “**Log Filter**” to increase the verbosity of the application log

Diagnostics

Log Filter:



Log Filter

The log levels instruct the system how to filter the various log levels. Choosing a log level 0 means that there will be no log messages for the message type. Log level 9 means the system will not filter messages.

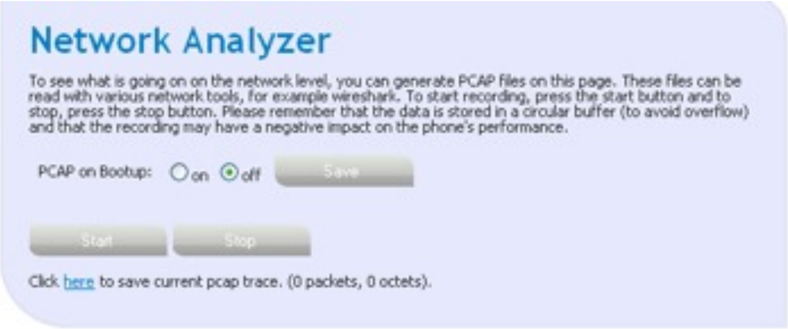
General events:	9
Media-related events:	9
SIP registration messages:	9
SIP call messages:	9
Other SIP messages:	9
Web server events:	9
DNS events:	0
LDAP events:	0
DECT events:	9
Network events:	9
TLS:	9
ICE:	0

Increase/Decrease application log verbosity for any event

Diagnostics

Packet Capture:

- As a further diagnostics tool, the snom m9 provides an on-device packet capture tool “**Network Analyzer**”
- Such packet captures provide an efficient way for snom to analyze and respond to any customer reported device issues



Network Analyzer

To see what is going on on the network level, you can generate PCAP files on this page. These files can be read with various network tools, for example wireshark. To start recording, press the start button and to stop, press the stop button. Please remember that the data is stored in a circular buffer (to avoid overflow) and that the recording may have a negative impact on the phone's performance.

PCAP on Bootup: ○ on ● off

Click here to save current pcap trace. (0 packets, 0 octets).

References

Product Page:
http://www.snom.com/en/products/voip-dect-phones/snom-m9-sip-dect-ip-phone/

Online Admin Manual:
http://wiki.snom.com/Snom_m9/Documentation/Online_Manual

Wiki Resources:
http://wiki.snom.com/Snom_m9

Company Profile | Contact

We would like to get talking to you!

snom technology AG
Charlottenstraße 68–71
10117 Berlin
Germany

Tel: +49 30 39833-0
Fax: +49 30 39833-111

snom technology, Inc.
18 Commerce Way
Suite 6000
Woburn, MA 01801,
U.S.A.
Tel: +1 978-998-7882
Fax: +1 978-998-7883

snom UK Ltd
Aspect Court
47 Park Square East
Leeds LS1 2NL
United Kingdom
Tel: +44 1133 503 111
Fax: +44 1133 503 110

snom technology SRL
Via A. Lusardi 10
20122 Milano
Italy

Tel: +39 02 00611212
Fax: +39 02 93661864

snom France SARL
1er Etage Gauche
6 Parc des fontenelles
78870 Bailly
France
Tel: +33 1 80 87 64 87
Fax: +33 1 80 87 62 88