

# Welkom

*bij de Televersal Group*



*The Netherlands*

**televersal BV**

Nedervonder 19  
Oisterwijk

*Belgium*

**televersal**  
**TopTel BVBA**

Z3. Doornveld 154  
B-1731 Zellik

[www.televersalgroup.com](http://www.televersalgroup.com)



# Content

## Connecting Gigaset N510 IP Pro

- General Information
- Hipath 3000 Configuration
  - Settings Hipath 3000
- OSO MX V3 configuration
  - Settings OSO MX V3
- Gigaset N510 IP Pro configuration
  - Settings Gigaset N510 IP Pro
- Troubleshooting
  - Making a wireshark capture



# General information

- Components used
  - Hipath 3000 v8
  - Hipath HG1500 V8
  - Hipath Comscendo licenses
  - Gigaset N510 IP Pro base station
  - Gigaset Handset devices
- Maximum configuration:
  - Max. 6 handsets connected to the N510 IP Pro
  - Max. 6 configured SIP accounts in the N510 IP Pro (6 Hipath comscendo client licenses needed)
  - Max. 4 simultaneous calls (4 Hipath HG1500 B-channel licenses needed)



# General information

- Overview of the supported features
  - Compatible with Gigaset's wide range of DECT handsets
  - Desktop or wall mountable
  - Integrated power over Ethernet (POE class 1)
  - Caller ID for incoming and outgoing calls
  - Missed and dialled call lists
  - Call transfer using the "R" button
  - Vlan tagging supported
- Recommended handsets
  - C59H, C610H, SL78H, S79H, SL400H and S810H



# Hipath 3000 configuration

- Create the extension numbers
- Configure one of the HG1500 modules as gatekeeper
- Set the flag "enable gateway resources" for at least one of the HG1500 modules
- Define the SIP users
- Setup user security
- Check the number of available comscendo licenses

# Create the extension numbers

- Create extension numbers on ports where no hardware is assigned to.

3.13.10

Station	Key programming	Endpoint hw sw version	Fax / Modem	Emergency	Gatekeeper		
Gateway	Mobility Entry	OSD Ports					
Call no.	DID	Name	Status	Type	Type	Access	
91			⊗ *	No Port	Standard		
92			⊗ *	No Port	Standard		
93			⊗ *	No Port	Standard		
94			⊗ *	No Port	Standard		
95			⊗ *	No Port	Standard		
96			⊗ *	No Port	Standard		
97			⊗ *	No Port	Standard		
98			⊗ *	No Port	Standard		
99			⊗ *	No Port	Standard		
100	150	N510 - 1	⊗ *	No Port	Standard		
101	151	N510 - 2	⊗ *	No Port	Standard		
102	152	N510 - 3	⊗ *	No Port	Standard		
103	153	N510 - 4	⊗ *	No Port	Standard		
104			⊗ *	No Port	Standard		
105			⊗ *	No Port	Standard		
106			⊗ *	No Port	Standard		
107			⊗ *	No Port	Standard		
108			⊗ *	No Port	Standard		

This fields MUST NOT contain any hardware port.



# Setup user Security

- Always setup user security
- Make sure you choose strong passwords

Station selection

Call no.	Name
100	Asterix
101	Obelix
102	Idefix
134	Sippox
150	N510 -1
151	N510 - 2
152	N510 - 3
153	N510 - 4
160	N300 - 1
161	N300 - 2
170	
171	DX800A
190	Basenix
199	

Name: N510 -1 | Call number: 150 | CLIP/LIN: | Direct inward: | Type: SO Extension | Access: HXGS3 8 - SIP | Mobile code: ...

System Client

Flags:  Status message

Authentication active:

Type:  Mobile,  Non mobile,  Mobile blocked

Redundancy Destination: IP Address:

SIP Client

Security:  Authentication active

Password: [masked]

Validate password: [masked]

UserID: user\_150

Realm: 150

IP Address: 195 . 0 . 0 . 3

Fixed IP address

SMG register

Analog adapter connected

Annotations:

- choose a strong password to prevent unauthorised access (points to Password field)
- do not use the extension number as UserID (points to UserID field)
- Realm MUST be the extension number (points to Realm field)

# Check the availability of Comscendo licenses

- A Hipath Comscendo license is needed for each IP workpoint

CDB Data

License ID: 1

Type - Slot	Port	Feature	Assigned	Emergency	Expiration date
HG 1500 - 08	-	HG1500 B-channel	40	2	22.06.11
HG 1500 - 08	-	HiPath ComScendo	40	0	22.06.11
HG 1500 - 08	-	IP Sec	0	0	-
HG 1500 - 08	-	CA functionality	0	0	-
HG 1500 - 08	-	ComScendo Security	80	2	22.06.11
HG 1500 - 08	-	HG1500 B-Channel Evaluation	0	0	-

# OSO MX V3 Configuration

- SIP clients are set-up in the "IP Telephones" setup wizard

Home Administrators **Setup** Expert mode Data Backup License Management Service Center

Setup

- Wizards
- Basic Installation
- Network / Internet
  - Telephones / Subscribers**
  - Central Telephony
  - User Telephony
- Security
- OpenScope Office

**Telephones / Subscribers**

<input type="button" value="Edit"/>	<b>IP Telephones</b> Set up system-specific IP and SIP telephones as well as IP/analog adapters
<input type="button" value="Edit"/>	<b>ISDN Devices</b> Unpowered ISDN ports for ISDN cards / modems and S0 stations
<input type="button" value="Edit"/>	<b>Analog Terminals</b> Analog DTMF and CLIP-capable ports for Fax and Telephone
<input type="button" value="Edit"/>	<b>Key Programming</b> Name and function key programming for system-specific IP telephones

# Setup SIP clients

- Assign a name and number for each sip client
- Assing a license to each sip client

Take DID from changed call number

Box	Slot	Callno	Name	DID	Type	Licence Type	Licensed	Fax Callno	
	1	1	-	-	- editable	System Client	No Licence	-	-
	1	1	-	-	- editable	System Client	No Licence	-	-
	1	1	150	N510 - 1	- editable	SIP Client	Comfort User	✓	-
	1	1	151	N510 - 2	- editable	SIP Client	Comfort User	✓	-
	1	1	152	N510 - 3	- editable	SIP Client	Comfort User	✓	-
	1	1	153	N510 - 4	- editable	SIP Client	Comfort User	✓	-
	1	1	-	-	- editable	System Client	No Licence	-	-
	1	1	-	-	- editable	System Client	No Licence	-	-
	1	1	-	-	- editable	System Client	No Licence	-	-

Page 1 of 3 Edit 1 | 2 | 3 Items per page [10](#) [25](#) [50](#) [100](#)

# Set security

- Setup a strong username and password for each extension

Box	Slot	Tel.nr.	Naam	Doorkie
	1	1		- kan worden gev
	1	150	N510 - 1	- kan worden gev
	1	151	N510 - 2	- kan worden gev

click on the pencil to edit the extensions settings

Licence Type:

Licensed: Yes

Language:

Call signaling internal:   
(Ringer pitch for internal calls):

Call signaling external:   
(Ringer pitch for external calls):

**Security**

Authentication active:

Password:

Confirm password:

SIP User ID / Username:

Realm:

choose a strong password to prevent unauthorised access

do not use the extension number as UserID

Realm SHOULD be left default

Help Abort Back OK & Next

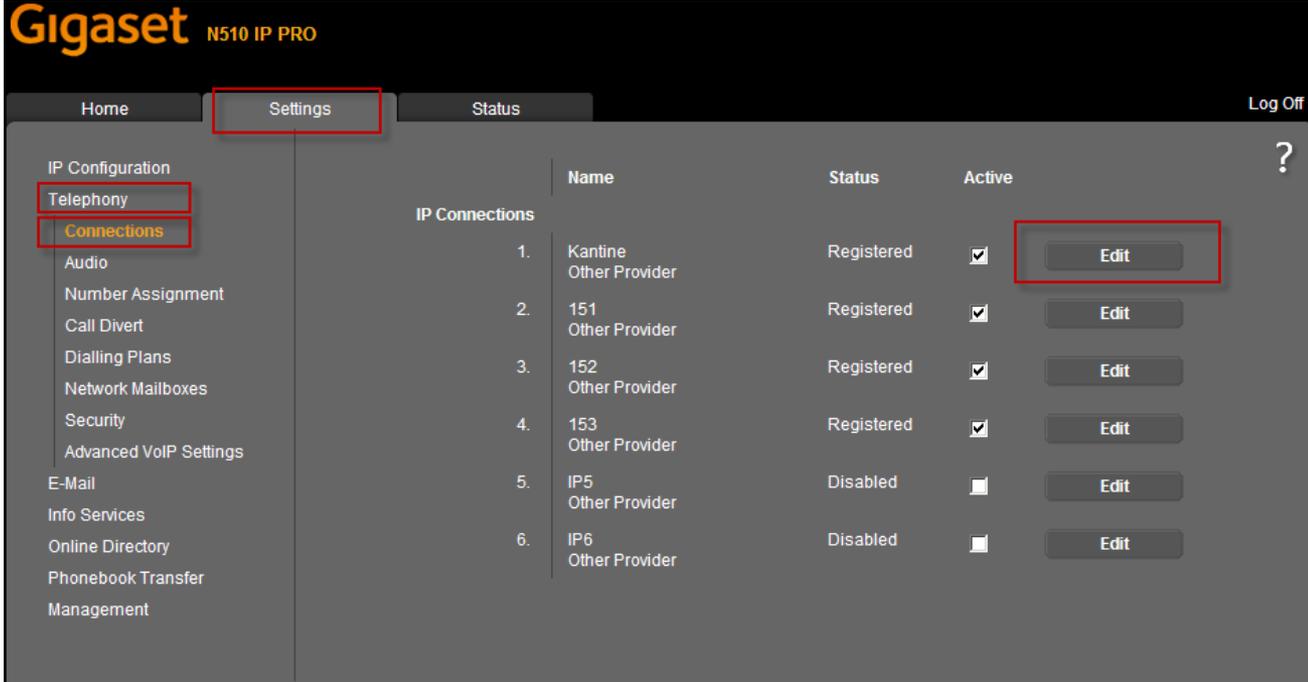


# Gigaset N510 IP Pro Configuration

- Create an IP connection for each user
- Setup the designed codecs
- Assign an extension to each handset
- Configure the advanced VOIP Settings

# Create an IP connection

- Login to the N510 IP Pro (default PIN: 0000)
  - Click "Settings"
  - Click "Telephony"
  - Click on the "Edit" button behind one of the unused IP connections



The screenshot displays the Gigaset N510 IP PRO web interface. The 'Settings' tab is selected, and the 'Connections' sub-tab is highlighted. The 'IP Connections' table lists six entries, with the 'Edit' button for the first entry (Kantine) highlighted.

Name	Status	Active	
1. Kantine Other Provider	Registered	<input checked="" type="checkbox"/>	<a href="#">Edit</a>
2. 151 Other Provider	Registered	<input checked="" type="checkbox"/>	<a href="#">Edit</a>
3. 152 Other Provider	Registered	<input checked="" type="checkbox"/>	<a href="#">Edit</a>
4. 153 Other Provider	Registered	<input checked="" type="checkbox"/>	<a href="#">Edit</a>
5. IP5 Other Provider	Disabled	<input type="checkbox"/>	<a href="#">Edit</a>
6. IP6 Other Provider	Disabled	<input type="checkbox"/>	<a href="#">Edit</a>

# IP connection settings

- First set the basic settings and click "Show Advanced Settings" for further options.

The screenshot displays the 'Gigaset N510 IP PRO' settings page, specifically the '1. IP Connection' section. The interface includes a navigation menu on the left with options like 'IP Configuration', 'Telephony', 'Connections', 'Audio', 'Number Assignment', 'Call Divert', 'Dialling Plans', 'Network Mailboxes', 'Security', 'Advanced VoIP Settings', 'E-Mail', 'Info Services', 'Online Directory', 'Phonebook Transfer', and 'Management'. The main content area is titled '1. IP Connection' and contains the following fields and options:

- Connection Name or Number:** A text input field containing 'Kantine'. A red arrow points to this field with the annotation 'just a name'.
- Profile Download:** A section with a 'Provider:' dropdown set to 'Other Provider' and a 'Select VoIP Provider' button.
- Personal Provider Data:** A section with four text input fields:
  - Authentication name:** 'user\_150'. A red arrow points to it with the annotation 'Username must match the setting in the Hpath/OSO'.
  - Authentication password:** '\*\*\*\*\*'. A red arrow points to it with the annotation 'Password must match the setting in the Hpath/OSO'.
  - Username:** '150'. A red arrow points to it with the annotation 'Must match the extension number'.
  - Display name:** 'Kantine test'. A red arrow points to it with the annotation 'Optional: Phone name can only be seen in the network traces. OpenScope Office uses the name configured in'.

At the bottom of the form, there are three buttons: 'Show Advanced Settings', 'Set', and 'Cancel'. A 'Delete Connection' button is also visible at the bottom right. A 'Log Off' link and a question mark icon are located in the top right corner of the settings area.

# Advanced settings

- Set the IP Address of the HG1500 or OSO as "domain" "proxy-server" and "registration server"
- Leave all other settings unchanged and press "Set"

Username: 150  
Display name: Kantine test  
Hide Advanced Settings

General data of your service provider

Domain: HG1500\_OSO\_IPADDRESS  
Proxy server address: HG1500\_OSO\_IPADDRESS  
Proxy server port: 5060  
Registration server: HG1500\_OSO\_IPADDRESS  
Registration server port: 5060  
Registration refresh time: 180 sec

Network data for your service provider

STUN enabled:  Yes  No  
STUN server address:  
STUN server port: 3478  
STUN refresh time: 240 sec  
NAT refresh time: 20 sec  
Outbound proxy mode:  Always  Automatic  Never  
Outbound server address:  
Outbound proxy port: 5060

Set Cancel Delete Connection

- Repeat the last 2 steps for all the extensions you wish to register at the N510 IP Pro basestation.

# Setup the codecs

- Set the codec for each extension number according to the settings in the HG1500/OSO
- Note that codecs G.722 and G.726 are NOT supported by the HG1500 and OSO, but can be used in HG1500/OSO environments. E.g. Openstage phones do support the G.722 codec.

The screenshot displays the 'Settings' page of a televersal system. The left sidebar contains a menu with 'Audio' highlighted under the 'Connections' section. The main content area is titled 'Settings for Bandwidth' and includes a descriptive paragraph about VoIP call quality. Below this, there are radio button options for 'Allow 1 VoIP call only' (set to 'No') and 'Voice Quality' (set to 'Own Codec preference'). A 'Hide Advanced Settings' button is visible. The 'Settings for Connections' section shows 'Kantine' as the profile and 'Normal' as the volume setting. At the bottom, there are two lists: 'Selected codecs' containing 'G.729' and 'Available codecs' containing 'G.711 a law', 'G.711 µ law', 'G.726', and 'G.722'. Navigation buttons like '< Add', 'Remove >', 'Up', and 'Down' are provided between the lists.

# Assign the numbers to a handset.

The screenshot shows a web-based configuration interface for telephony. The top navigation bar includes 'Home', 'Settings', and 'Status', with 'Log Off' in the top right corner. A sidebar on the left lists various settings categories: IP Configuration, Telephony (with sub-items: Connections, Audio, **Number Assignment**, Call Divert, Dialling Plans, Network Mailboxes, Security, Advanced VoIP Settings), E-Mail, Info Services, Online Directory, Phonebook Transfer, and Management. The main content area is titled 'Handsets' and contains instructions: 'Select the line for outgoing calls and also one or more lines for incoming calls for the desk phone and each handset.' There are two handset configuration sections, 'INT 1' and 'INT 2', each with a 'Name' field set to 'HANDSET 1' and 'HANDSET 2' respectively. Each section has a table for assigning lines:

Connection	for outgoing calls	for incoming calls
Kantine	<input type="radio"/>	<input checked="" type="checkbox"/>
151	<input type="radio"/>	<input type="checkbox"/>
152	<input type="radio"/>	<input type="checkbox"/>
153	<input type="radio"/>	<input type="checkbox"/>
Select line for each outgoing call <input type="radio"/>		

Red boxes in the original image highlight the 'Kantine' row and the '151' row in both tables, indicating the selected configuration.

# Set the advanced VoIP setting as shown in the screenshot

The screenshot displays a web interface with three tabs: Home, Settings, and Status. The 'Settings' tab is active, showing a sidebar on the left with various configuration options. The 'Advanced VoIP Settings' option is highlighted in orange. The main content area is divided into several sections:

- DTMF over VoIP connections**:
  - Send settings:  Automatic  Audio  RFC 2833  SIP Info
  - When using G.722-Codecs (wide-band connection) DTMF Signals cannot be transmitted via audio.
- Call Transfer**:
  - Use the R key to initiate call transfer with the SIP Refer method:  Yes  No
  - Transfer Call by On-Hook:  Yes  No
  - You can define the choice of target address in the SIP protocol
  - Find target addr. automatically:  Yes  No
  - Derive target address:  from the SIP URL  from the SIP contact header
  - Hold on transfer target:  For attended transfer  For unattended transfer
- Hook Flash (R-key)**:
  - R key settings are disabled because the R key is being used for call transfer.
- Listen ports for VoIP connections**:
  - Use random ports:  Yes  No
  - SIP port: 5060 - 5076
  - RTP port: 5004 - 5020

At the bottom of the settings area, there are two buttons: 'Set' and 'Cancel'.



# Troubleshooting

- Activating the online RPCap daemon on the HG1500
- Activating the online RPCap daemon on the OSO
- Starting the wireshark capture
- Analyzing the wireshark capture
- Creating a problem report for expert analysis.

# HG1500 online Rpcap daemon

- Go to "maintenance" → "Traces"
- Click on the rpcap Daemon
- Press "Apply" without changing the settings
- Click "OK" in the popup message
- The rpcap Daemon is now started

The screenshot shows the web interface for the HG 1500 V9 SAPP. The top navigation bar includes 'Front panel', 'Wizard', 'Explorers', 'Maintenance' (highlighted in red), 'Help', and 'Logoff'. The main content area is titled 'Start rpcap Daemon'. On the left, a tree view under 'Traces' has 'rpcap Daemon' selected and highlighted with a red box. The main configuration area has two sections: 'Address to Bind to' and 'Client identification to allow access'. Both sections have an 'IP Address (either numeric or literal):' field set to '0.0.0.0' and a 'Port (please choose a free one):' field set to '2002'. Below these fields, there are explanatory notes: '\* ) 0.0.0.0 binds to all local IPv4 addresses' and '\* ) 0.0.0.0 allows access from all clients'. A text box provides instructions: 'This action will start the rpcap daemon and opens a server port. This allows direct remote access from applications e.g. Wireshark or Ethereal to the TCP/IP packets processed by the LAN interfaces. To capture in Wireshark (Ethereal), enter the target URI in Capture->Options (Capture->Start->Interface), e.g.: "rpcap://target-ip-address/eth2" Available interfaces on the target: [Interface Details](#) If you use eth2 interface, it is useful to add a "Capture Filter" in Wireshark e.g.: "not host PC IP address"'. At the bottom of the configuration area, there are 'Apply' and 'Undo' buttons, with 'Apply' highlighted by a red box. The bottom status bar shows system information: 'SSL on', 'IPsec off', '18140815', 'hg1500', '06/27/2011 10:50:10', and '4d 15h 58m'.

# OSO MX online rpcap Deamon

- Login as a user with expert rights
- Click on "Expert Mode"
- Go to "Maintenance" → "Traces"
- Click on the "rpcap Deamon", leave all settings unchanged and click "Apply".

The screenshot shows a web browser window titled "Traces - Windows Internet Explorer". The main content area is titled "Traces" and contains a sidebar on the left with a tree view of configuration options. The "rpcap Daemon" option is highlighted with a red box. The main content area is titled "rpcap" and contains the following configuration fields:

- Address to Bind to**
  - IP Address (either numeric or literal):  \*)
  - Port (please choose a free one):
  - Trace Internal LAN:
- Client identification to allow access**
  - IP Address (either numeric or literal):  \*)

Below the configuration fields, there is a red warning message: "\*) 0.0.0.0 binds to all local IPv4 addresses".

Below the warning, there is a section titled "Client identification to allow access" with a red warning message: "\*) 0.0.0.0 allows access from all clients".

Below the warning, there is a section titled "This action will start the rpcap daemon and opens a server port." with the following text:

This allows direct remote access from applications e.g. Wireshark or Ethereal to the TCP/IP packets processed by the LAN interfaces.

To capture in Wireshark (Ethereal), enter the target URI in Capture->Options (Capture->Start->Interface), e.g.: "rpcap://target-ip-address/eth2"

Available interfaces on the target: eth0 eth2 eth7 eth7.4091 eth7.4094 eth7.547 eth8 eth9 lo [Interface Details](#)

If you use eth2 interface, it is useful to add a "Capture Filter" in Wireshark e.g.: "not host PC IP address"

At the bottom of the page, there are three buttons: "Apply", "Undo", and "Help".

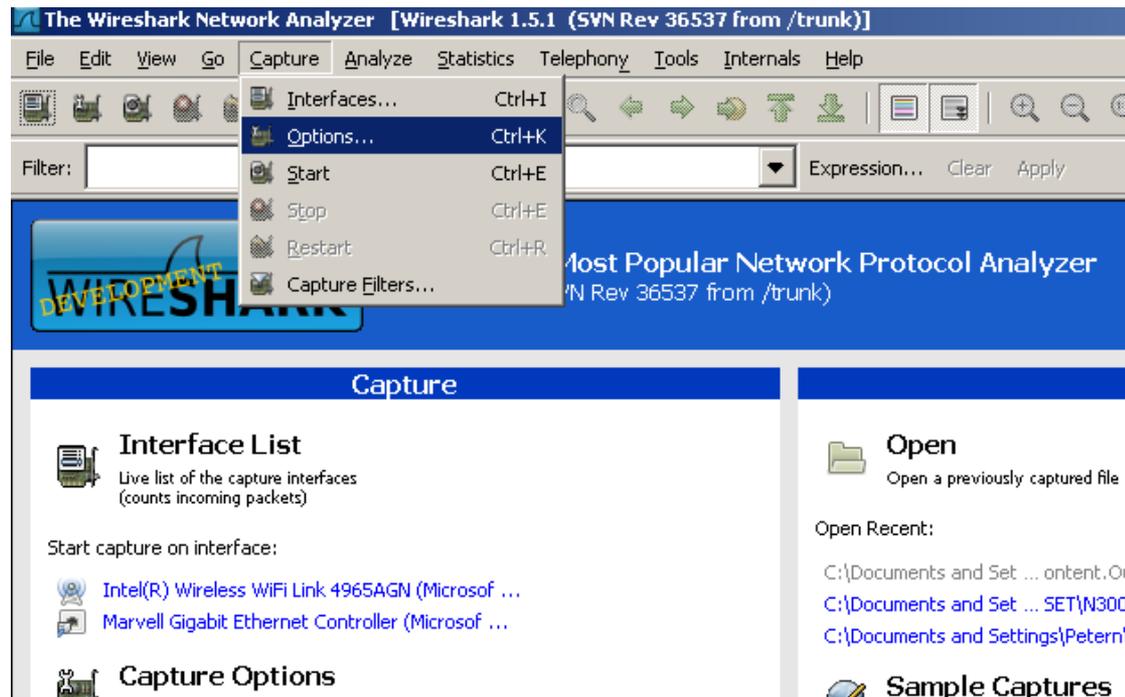
# Settings in Wireshark



- Wireshark is a free network protocol analyzer that can be downloaded from <http://www.wireshark.org>
- Wireshark uses WinPcap as the driver to capture network traffic. This WinPcap driver is included in the installer package
- In Wireshark you must define the rpcap daemon interface of the HG1500/OSO as capture interface
- The interface format for the HG1500 is always
  - Rpcap://IP-ADDRESS/emac0
  - IP-ADDRESS must be the ipadress of the HG1500's LAN1 port
  - EMAC0 is the LAN1 port of the HG1500
- The interface format for the OSO is
  - Rpcap://IP-ADDRESS/INT-NAME
  - IP-ADDRESS must be the LAN ipadress of the OSO
  - INT-NAME is the name of the interface you wish to capture packages from
    - ETH1 is the OSO's WAN port
    - ETH2 is the OSO's LAN port

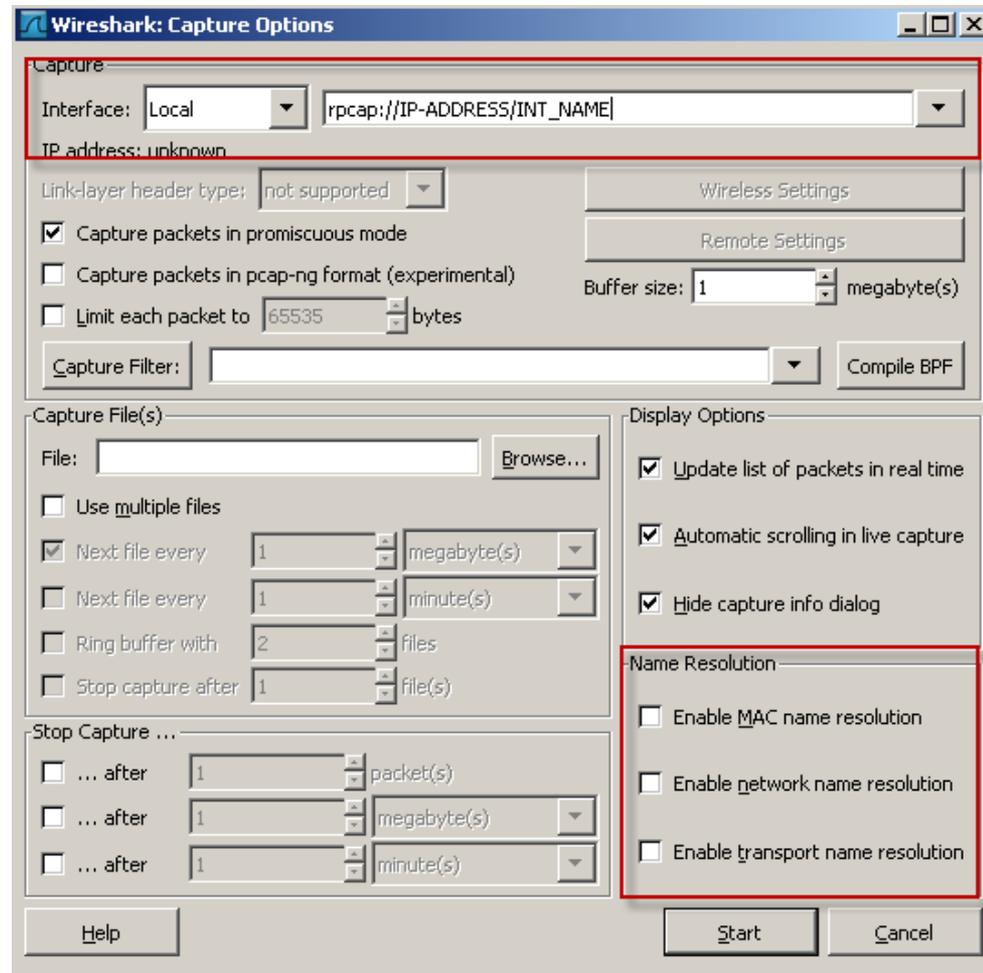
# Starting wireshark

- Start wireshark
- In the "capture" menu select "options"



# Setting capture options

- Set the rpcap interface of the HG1500/OSO as local capture interface
- Disable the “name resolution” flags
- Press “start” to start the capture



The image shows the 'Wireshark: Capture Options' dialog box. The 'Capture' section is highlighted with a red box, showing the 'Interface' set to 'Local' and the 'IP address' set to 'unknown'. The 'Name Resolution' section is also highlighted with a red box, showing three checkboxes: 'Enable MAC name resolution', 'Enable network name resolution', and 'Enable transport name resolution', all of which are unchecked. Other options include 'Capture packets in promiscuous mode' (checked), 'Buffer size' (1 megabyte(s)), and 'Capture Filter' (empty). The 'Display Options' section includes 'Update list of packets in real time' (checked), 'Automatic scrolling in live capture' (checked), and 'Hide capture info dialog' (checked). The 'Stop Capture ...' section has three options, all with '1' selected in the dropdowns.

Wireshark: Capture Options

Capture

Interface: Local | rpcap://IP-ADDRESS/INT\_NAME |

IP address: unknown

Link-layer header type: not supported | Wireless Settings

Capture packets in promiscuous mode | Remote Settings

Capture packets in pcap-ng format (experimental) | Buffer size: 1 | megabyte(s)

Limit each packet to 65535 | bytes

Capture Filter: | Compile BPF

Capture File(s)

File: | Browse...

Use multiple files

Next file every 1 | megabyte(s)

Next file every 1 | minute(s)

Ring buffer with 2 | files

Stop capture after 1 | file(s)

Display Options

Update list of packets in real time

Automatic scrolling in live capture

Hide capture info dialog

Name Resolution

Enable MAC name resolution

Enable network name resolution

Enable transport name resolution

Stop Capture ...

... after 1 | packet(s)

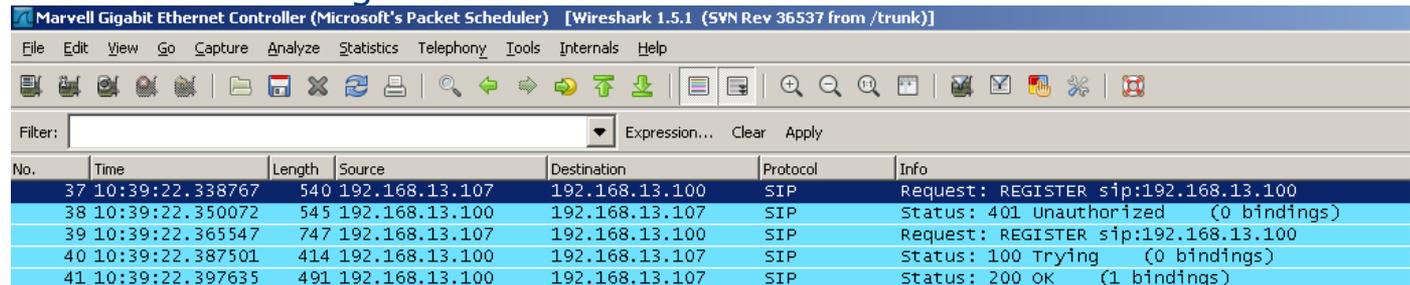
... after 1 | megabyte(s)

... after 1 | minute(s)

Help | Start | Cancel

# Analyzing the capture

- In the capture there should be a "REGISTER" message visible
- The first "REGISTER" is without the authentication header so the response from the HG1500/OSO is "401 UNAUTHORIZED"
- The second "REGISTER" should contain the authentication information
- If the username and password are configured right the HG1500/OSO should respond with "200 OK"
- The extension is now registered



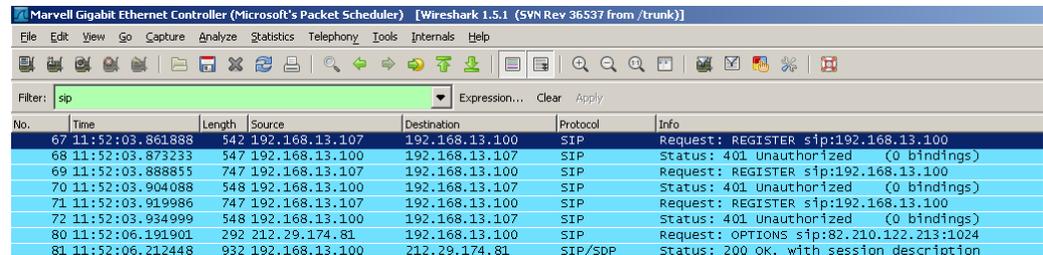
Marvell Gigabit Ethernet Controller (Microsoft's Packet Scheduler) [Wireshark 1.5.1 (SVN Rev 36537 from /trunk)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Length	Source	Destination	Protocol	Info
37	10:39:22.338767	540	192.168.13.107	192.168.13.100	SIP	Request: REGISTER sip:192.168.13.100
38	10:39:22.350072	545	192.168.13.100	192.168.13.107	SIP	Status: 401 Unauthorized (0 bindings)
39	10:39:22.365547	747	192.168.13.107	192.168.13.100	SIP	Request: REGISTER sip:192.168.13.100
40	10:39:22.387501	414	192.168.13.100	192.168.13.107	SIP	Status: 100 Trying (0 bindings)
41	10:39:22.397635	491	192.168.13.100	192.168.13.107	SIP	Status: 200 OK (1 bindings)

- If the username or password is incorrect, the N510 will try to register for 3 times



Marvell Gigabit Ethernet Controller (Microsoft's Packet Scheduler) [Wireshark 1.5.1 (SVN Rev 36537 from /trunk)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: sip Expression... Clear Apply

No.	Time	Length	Source	Destination	Protocol	Info
67	11:52:03.861888	542	192.168.13.107	192.168.13.100	SIP	Request: REGISTER sip:192.168.13.100
68	11:52:03.873233	547	192.168.13.100	192.168.13.107	SIP	Status: 401 Unauthorized (0 bindings)
69	11:52:03.888855	747	192.168.13.107	192.168.13.100	SIP	Request: REGISTER sip:192.168.13.100
70	11:52:03.904088	548	192.168.13.100	192.168.13.107	SIP	Status: 401 Unauthorized (0 bindings)
71	11:52:03.919986	747	192.168.13.107	192.168.13.100	SIP	Request: REGISTER sip:192.168.13.100
72	11:52:03.934999	548	192.168.13.100	192.168.13.107	SIP	Status: 401 Unauthorized (0 bindings)
80	11:52:06.191901	292	212.29.174.81	192.168.13.100	SIP	Request: OPTIONS sip:82.210.122.213:1024
81	11:52:06.212448	932	192.168.13.100	212.29.174.81	SIP/SDP	Status: 200 OK, with session description



## If all else fails.....

- We'll be available to help you out
- If you cannot get it working with this manual, contact us at
  - Televersal Support Center  
0900-2020173  
[TSC@Televersalgroup.com](mailto:TSC@Televersalgroup.com)
- Make sure before contacting us
  - The latest software versions are used in all components
  - Traces are available
  - Remote access is possible via Teamviewer