

It is assumed that the PacketScan™ Analyzer Software and License installations (PKV100, PKV103) are already performed referring to the Software Quick Installation Guide ([Packetscan-Quick-Install-Guide.pdf](#)). Now proceed with the verification steps below for capturing and analyzing UMTS IuCS protocol.

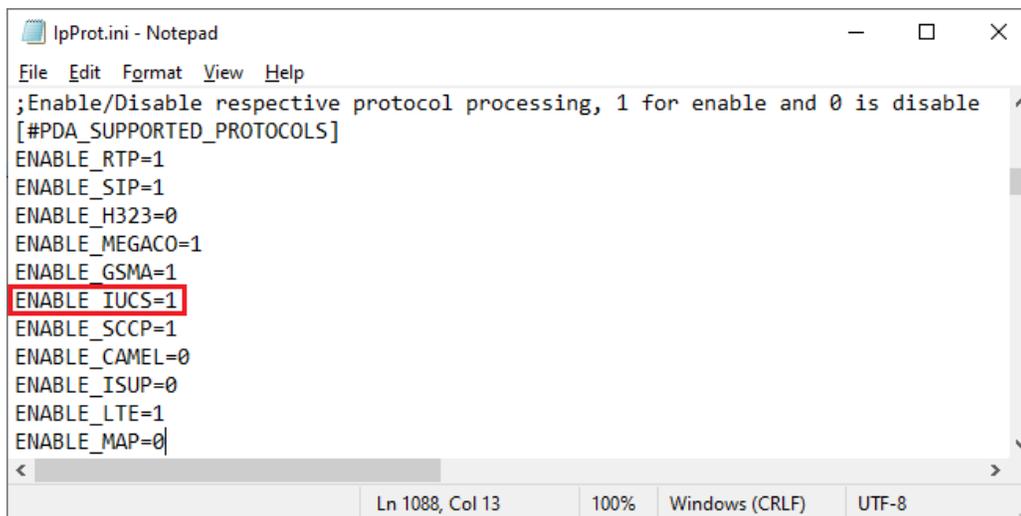


Note:

- Verify that Windows® Firewall is disabled before proceeding with the instructions given below. You should **Turn off Windows Firewall** on Windows® and on any 3rd party Anti-Virus software that may be installed on the PC to make sure that Firewall is not blocking any packets or frames.

Pre-Requirement

Users need to configure the **IpProt.ini** file from the following path “C:\Program Files\GL Communications Inc\PacketScan”. Set the **ENABLE_IUCS** parameter value to ‘1’ in the **IPProt.ini**. Save the changes and close the files. Refer to the below screenshot.



```
IpProt.ini - Notepad
File Edit Format View Help
;Enable/Disable respective protocol processing, 1 for enable and 0 is disable
[#PDA_SUPPORTED_PROTOCOLS]
ENABLE_RTP=1
ENABLE_SIP=1
ENABLE_H323=0
ENABLE_MEGACO=1
ENABLE_GSMA=1
ENABLE_IUCS=1
ENABLE_SCCP=1
ENABLE_CAMEL=0
ENABLE_ISUP=0
ENABLE_LTE=1
ENABLE_MAP=0
Ln 1088, Col 13 100% Windows (CRLF) UTF-8
```



Note:

Make sure that the PacketScan™ installation directory has full control permission to save the *.ini files. Follow the below steps to provide writing permission for the **PacketScan** directory.

- Go to " C:\Program Files\GL Communications Inc"
- Right click on the "PacketScan" folder and select **Properties**
- Click on **Security** tab and click **Edit** from explorer menu
- Click **Add** in the Permission window
- Type '**Everyone**' and click '**Check Names**'. Click **OK** to add this user group to Permissions Window
- Provide full control to the users added and click on **Apply** and **OK**.

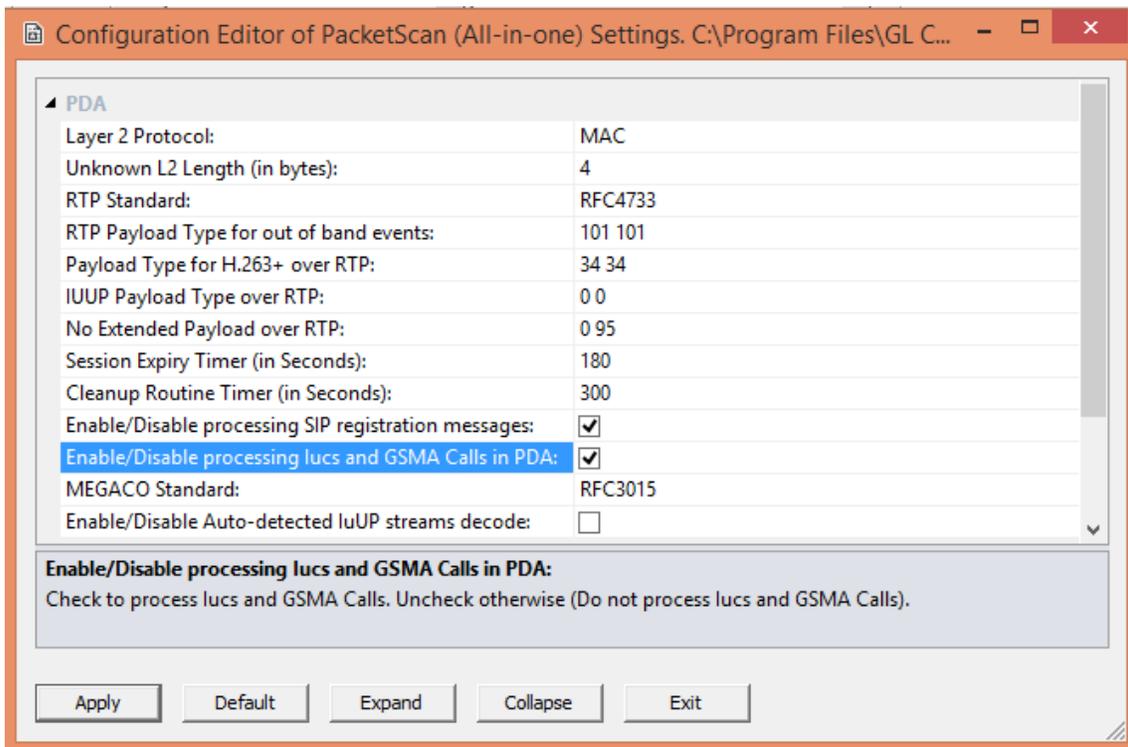
Verification



- Double click on the **PacketScan™** shortcut icon created on the desktop to launch the application.

Follow the steps below for functional verification of **PacketScan™ Real-time** analysis feature.

- From the **PacketScan™** main menu, select **Configure** → **Settings**. This will invoke **Configure Editor of PacketScan Settings window**.
- Check the **Enable/Disable processing luCS and GSMA Calls in PDA** to enable **IuCS** and **GSMA** calls in PDA. Click on **Apply** and **Exit**. Refer to the below figure.

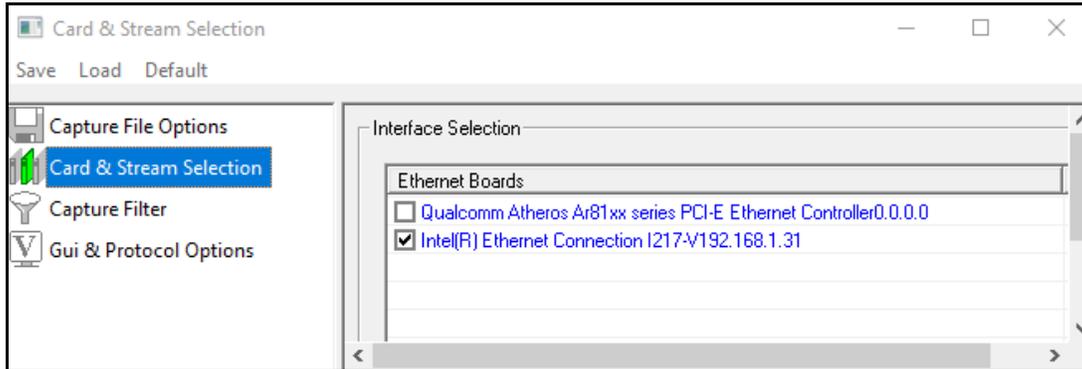


Note:

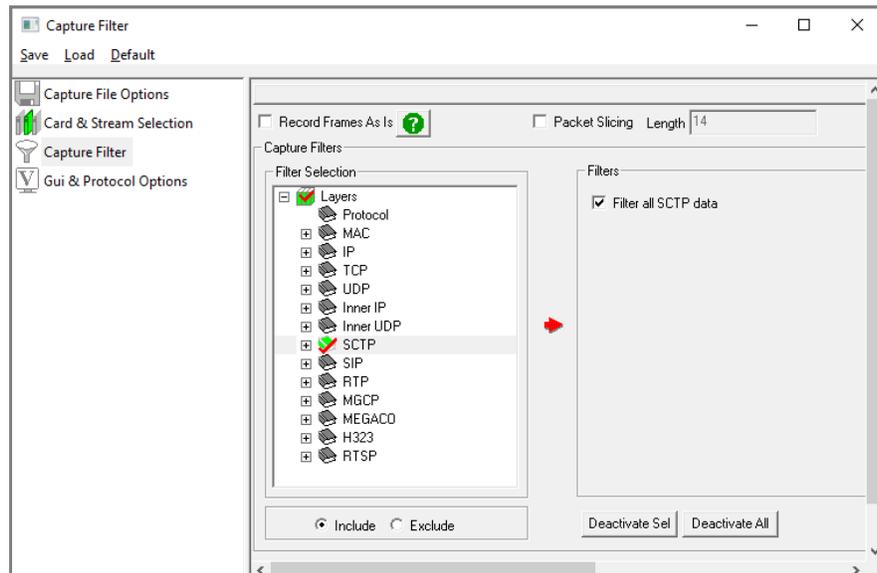
- The values shown here represent generic minimum and maximum values.
- Users can enter the exact minimum and maximum port number range as required. If the user doesn't know the port number, configure minimum and maximum port range as given above.

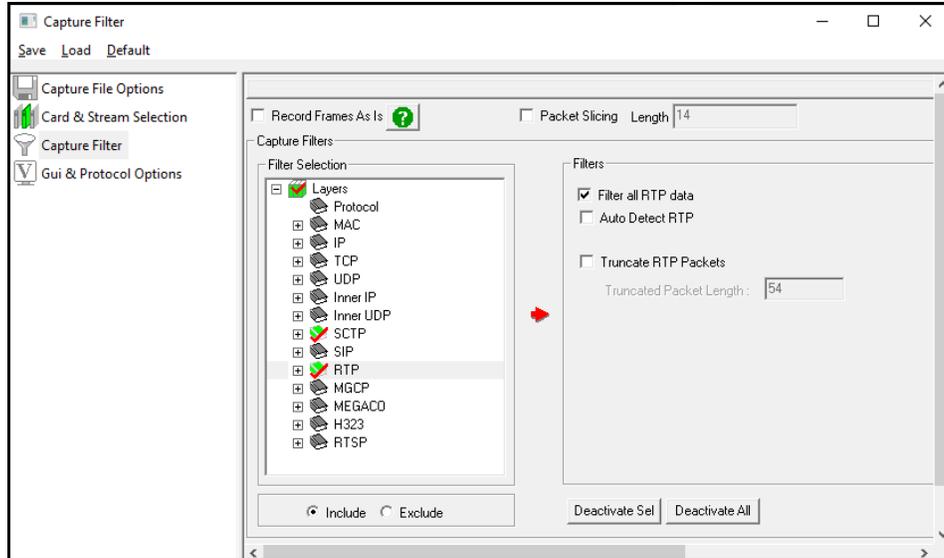
- A warning message will appear to restart the PacketScan Analyzer. Click on **OK**.
- Close the **PacketScan™** application and invoke again to apply the changes as per configuration settings.

- Select **Capture** → **Stream/Interface Selection** and enable the Ethernet card on which packet needs to be captured.

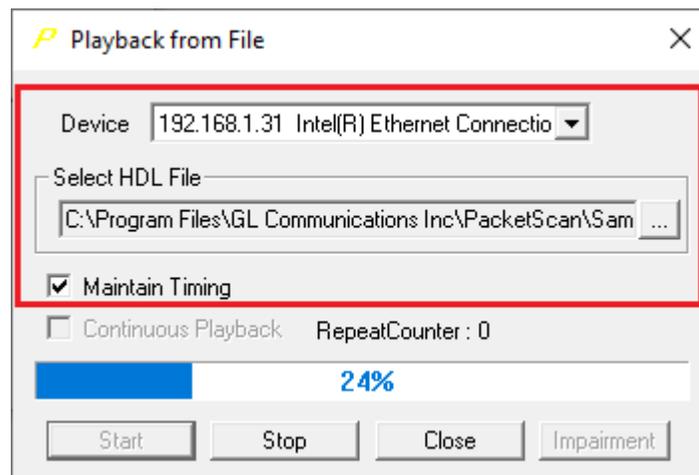


- On the left pane, select **Capture File Options** and verify that **Circular Capture Buffer** is checked.
- Now, on the left pane, select **Capture Filter** option, click on **SCTP** in the Filter Selection and check **Filter all SCTP data**. Similarly, click on **RTP** in the Filter Selection, check **Filter all RTP data**. After Filter configuration, close the window.

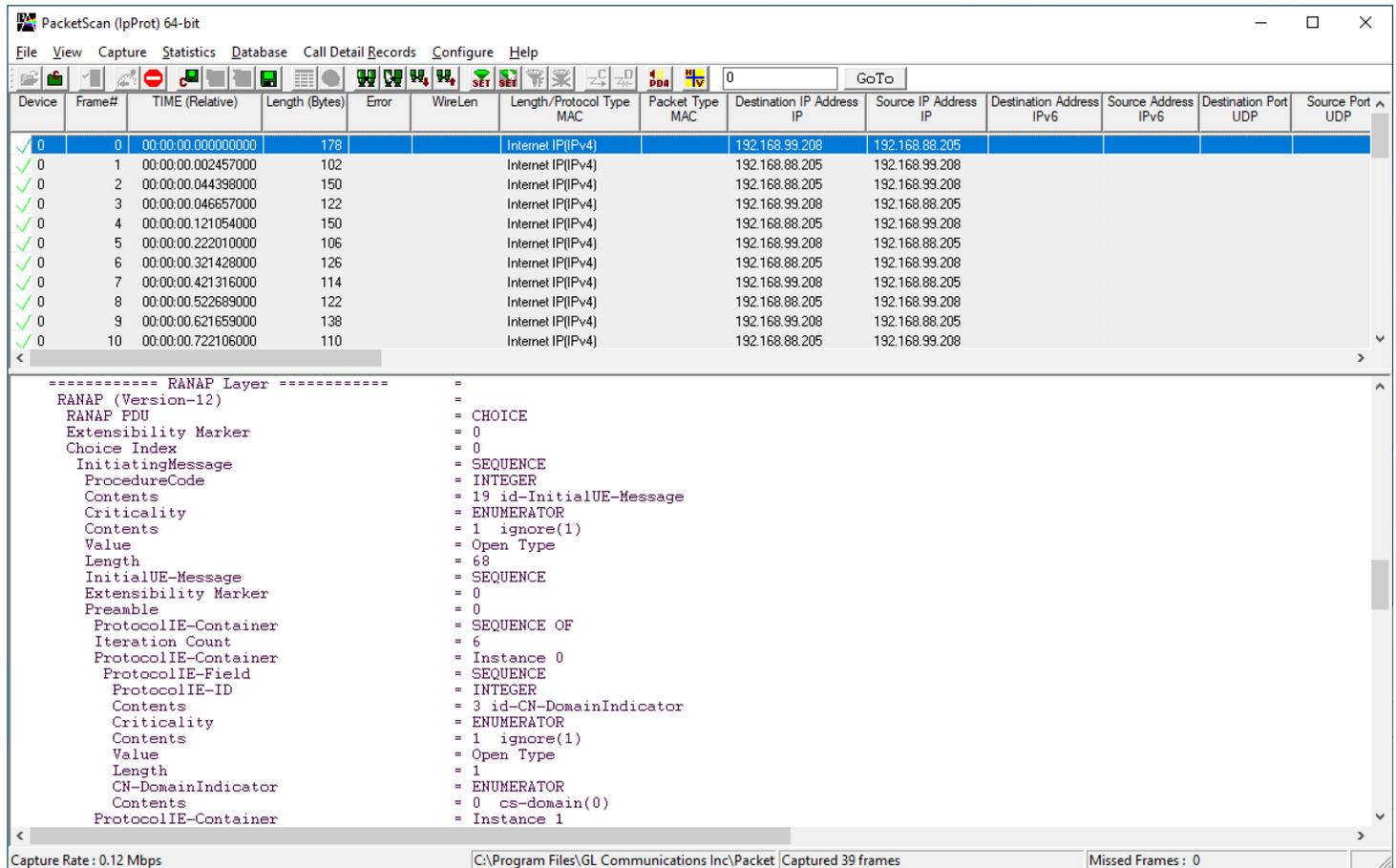




- From the **PacketScan™** main menu, select **File → Start Real-time** or Click **Start Real-time**  icon from the toolbar.
- If the **Temp.hdl** file already exists in the PacketScan installation directory, a warning message will popup to replace Temp.hdl file, click **Yes** to overwrite the file.
- Generate traffic by playing HDL file using **PacketScanUtilities** application. From the PacketScan installation directory (**C:\Program Files\GL Communications Inc\PacketScan**) double-click on  **PacketScanUtilities** application. This will invoke PacketScan Utility application.
 - Select **Utilities → HDL Playback** from the menu.
 - In the **Device** option, from the drop-down list, select NIC card on which PacketScan™ Real-time capture is configured. **Note:** Ensure that selected NIC card is enabled in PacketScan™ under **Capture → Stream/Interface Selection**.
 - In the **Select HDL File** option click on browse button to browse and select **CC:\Program Files\GL Communications Inc\PacketScan\SampleTraces\IuCS\IuCS-RTP.hdl** file from the PacketScan installation directory.
 - Enable **Maintain Timing** option and click **Start**.



- Observe the **UMTS protocol** decodes displayed in PacketScan™ analyzer. The detail view should display all the UMTS protocol layers - **MAC, IP, SCTP, M3UA, SCCP, and RANAP** layers.



The screenshot shows the PacketScan (IpProt) 64-bit interface. The top pane displays a list of captured packets. The bottom pane shows a detailed decode of the selected packet, highlighting the RANAP layer structure.

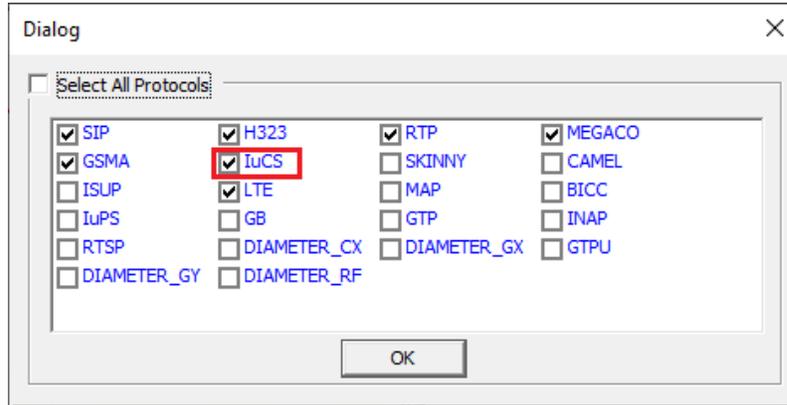
Device	Frame#	TIME (Relative)	Length (Bytes)	Error	WireLen	Length/Protocol Type MAC	Packet Type MAC	Destination IP Address IP	Source IP Address IP	Destination Address IPv6	Source Address IPv6	Destination Port UDP	Source Port UDP
✓ 0	0	00:00:00.000000000	178			Internet IP(IPv4)		192.168.99.208	192.168.88.205				
✓ 0	1	00:00:00.002457000	102			Internet IP(IPv4)		192.168.88.205	192.168.99.208				
✓ 0	2	00:00:00.044398000	150			Internet IP(IPv4)		192.168.88.205	192.168.99.208				
✓ 0	3	00:00:00.046857000	122			Internet IP(IPv4)		192.168.99.208	192.168.88.205				
✓ 0	4	00:00:00.121054000	150			Internet IP(IPv4)		192.168.88.205	192.168.99.208				
✓ 0	5	00:00:00.222010000	106			Internet IP(IPv4)		192.168.99.208	192.168.88.205				
✓ 0	6	00:00:00.321428000	126			Internet IP(IPv4)		192.168.88.205	192.168.99.208				
✓ 0	7	00:00:00.421316000	114			Internet IP(IPv4)		192.168.99.208	192.168.88.205				
✓ 0	8	00:00:00.522689000	122			Internet IP(IPv4)		192.168.88.205	192.168.99.208				
✓ 0	9	00:00:00.621659000	138			Internet IP(IPv4)		192.168.99.208	192.168.88.205				
✓ 0	10	00:00:00.722106000	110			Internet IP(IPv4)		192.168.88.205	192.168.99.208				

```

===== RANAP Layer =====
RANAP (Version-12)
RANAP PDU
Extensibility Marker
Choice Index
InitiatingMessage
ProcedureCode
Contents
Criticality
Contents
Value
Length
InitialUE-Message
Extensibility Marker
Preamble
ProtocolIE-Container
Iteration Count
ProtocolIE-Container
ProtocolIE-Field
ProtocolIE-ID
Contents
Criticality
Contents
Value
Length
CN-DomainIndicator
Contents
ProtocolIE-Container
  
```

Capture Rate: 0.12 Mbps | C:\Program Files\GL Communications Inc\Packet | Captured 39 frames | Missed Frames: 0

- From the **PacketScan™** main toolbar, click on the PDA icon  to invoke PDA (Packet Data Analyzer), from the drop-down protocol list select IuCS to view detail analysis of each session, call graphs and quality scores for the captured IuCS calls.
- Select **GUI Configurations** → **Protocol Statistics Display Configuration** this will display **Dialog** window. Check the **IuCS** option to view the **IuCS** counters on PDA. Refer to the below screenshots.

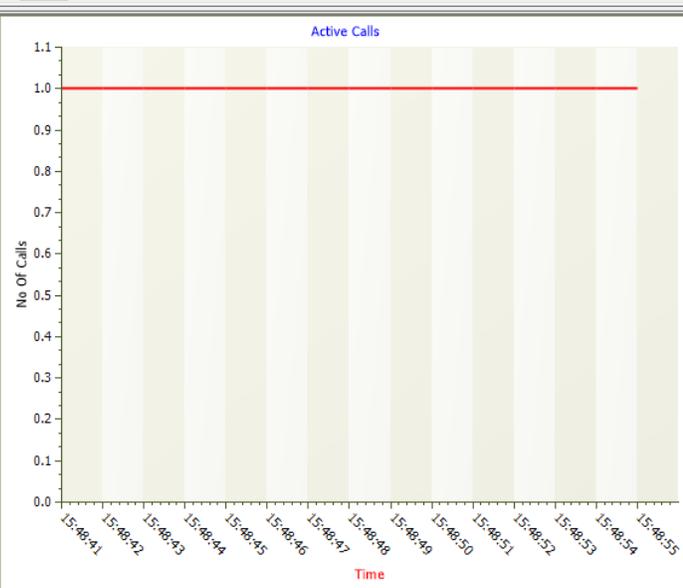


PDA Packet Data Analyzer - Summary View

File View Call Summary Protocol Configurations GUI Configurations Help

Call Summary | Registrar Summary | Alert Summary

Call #	CallType	IMSI	Caller	Callee	PresentationIndicator	Duration	Result	FailureCause
1	MO Speech Call			919655359818		00:01:01.372	Success	
2	MO Speech Call			919655359818		00:01:01.378	Success	



Active Calls Graph

Counter Type	Counters
Total IuCS(RANAP)Messages	36
IuCS Calls	2
IuCS Active Calls	0
IuCS Completed Calls	2
IuCS Purged Calls	0
IuCS Failed Calls	0
IuCS Timed Out Calls	0
IuCS ForceClosed Calls	0
Header CRC Pass Count	0
Header CRC Fail Count	0
Payload CRC Pass Count	0
Payload CRC Fail Count	0
Voice Calls	2
SMS Calls	0
Location Update Calls	0
Setup Messages	2
Connect Messages	2
Disconnect Messages	2

OverAll \ SIP \ H323 \ RTP \ MEGACO \ GSM \ IuCS \ LTE \ ED137 /



Note:

- You should **Turn off Windows Firewall** on Windows® and on any 3rd party Anti-Virus software that may be installed on the PC to make sure that Firewall is not blocking any packets or frames.