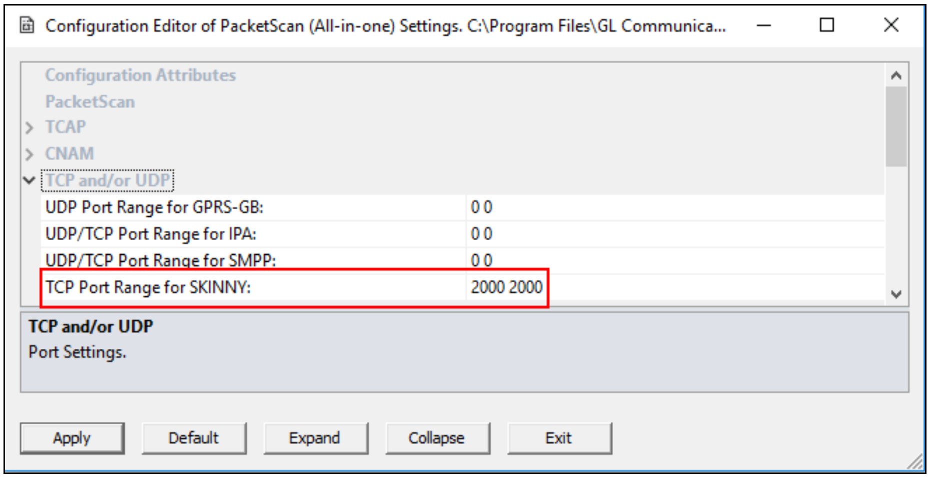
It is assumed that the PacketScan™ Analyzer Software and License installations (PKV100) are already performed referring to the Software Quick Installation Guide (PacketScan-Quick-Install-Guide.pdf). Now proceed with the verification steps below for capturing and analyzing Skinny protocol.

Verification

- Double click on the **PacketScan™** shortcut icon PacketScan 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**.
- Expand **TCP and/or UDP** option and for **TCP Port Range for SKINNY** enter port range as **2000**. Click on **Apply** and **Exit**. Refer to the below screenshot.



Configuration Editor of PacketScan (All-in-one) Settings. C:\Program Files\GL Communica...

Configuration Attributes
PacketScan
TCAP
CNAM
TCP and/or UDP

UDP Port Range for GPRS-GB:	0 0
UDP/TCP Port Range for IPA:	0 0
UDP/TCP Port Range for SMPP:	0 0
TCP Port Range for SKINNY:	2000 2000

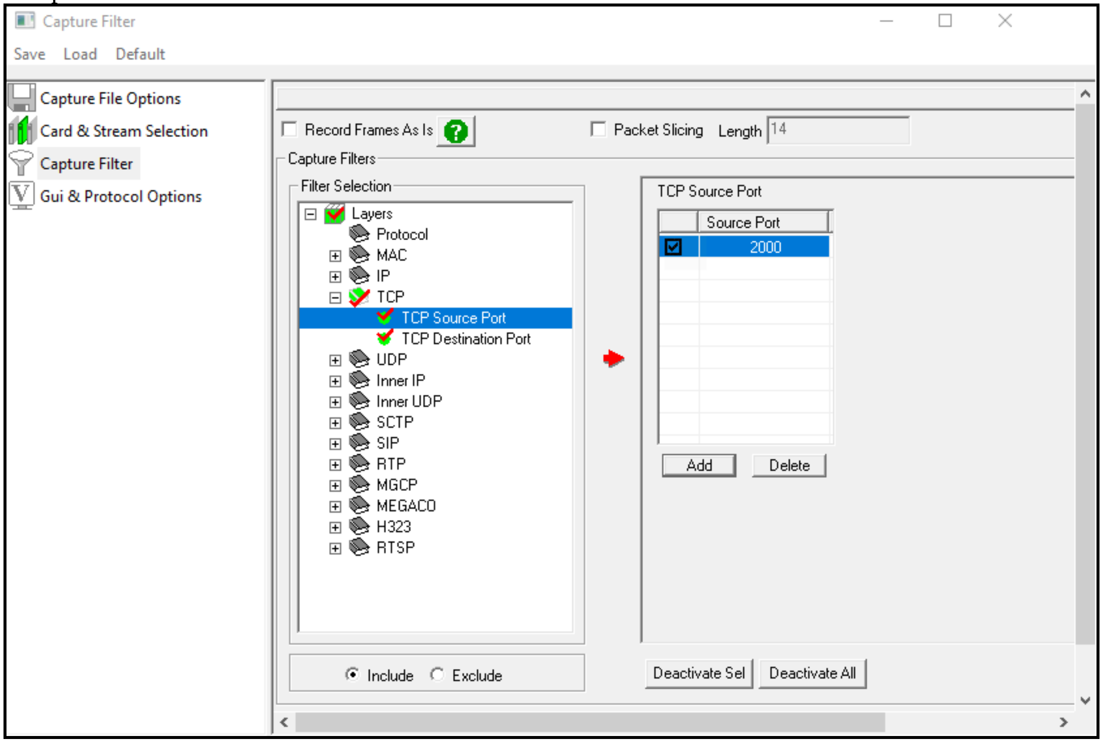
TCP and/or UDP
Port Settings.

Note:

- The values shown here represent generic minimum and maximum values.
- PacketScan™ SKINNY protocol does not support Call Detail Records.

- 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, double-click on **TCP** in the Filter Selection, select TCP Source Port, click on **Add** and enter the TCP source port as **2000**. Similarly, select TCP Destination Port, click on **Add** and enter the TCP destination port as **2000**.



□ Record Frames As Is

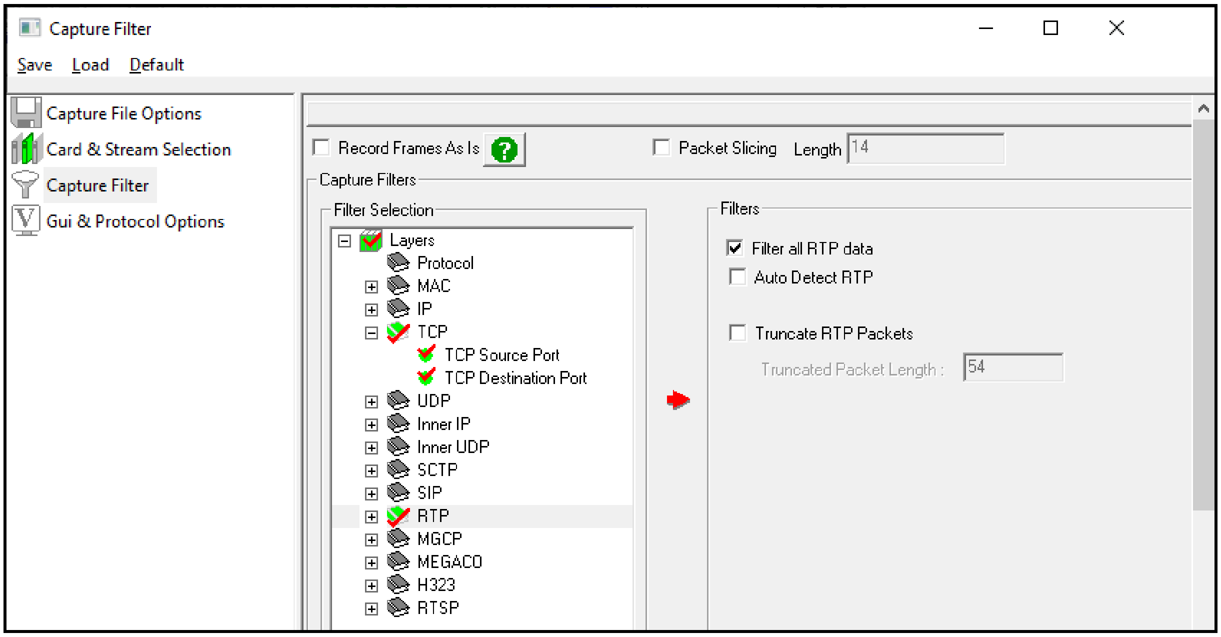
□ Packet Slicing Length 14

TCP Source Port

	Source Port
☑	2000

● Include ○ Exclude

- Similarly, in the **Capture Filter** option, select **RTP** and check **Filter all RTP data**. After Filter configuration, close the window.



□ Record Frames As Is

□ Packet Slicing Length 14

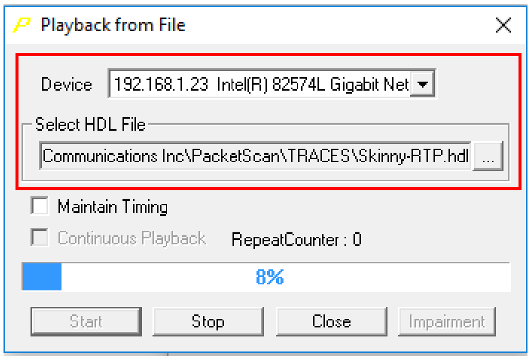
☑ Filter all RTP data

□ Auto Detect RTP

□ Truncate RTP Packets

Truncated Packet Length : 54

- From the **PacketScan™** main menu, select **File → Start Real-time** or Click **Start Real-time** icon from the toolbar.
- 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 **C:\Program Files\GL Communications Inc\PacketScan\Traces\SKINNY-RTP.hdl** file from the PacketScan installation directory.
  - Ensure that **Maintain Timing** option is Unchecked and click on **Start**.



Device: 192.168.1.23 Intel(R) 82574L Gigabit Net

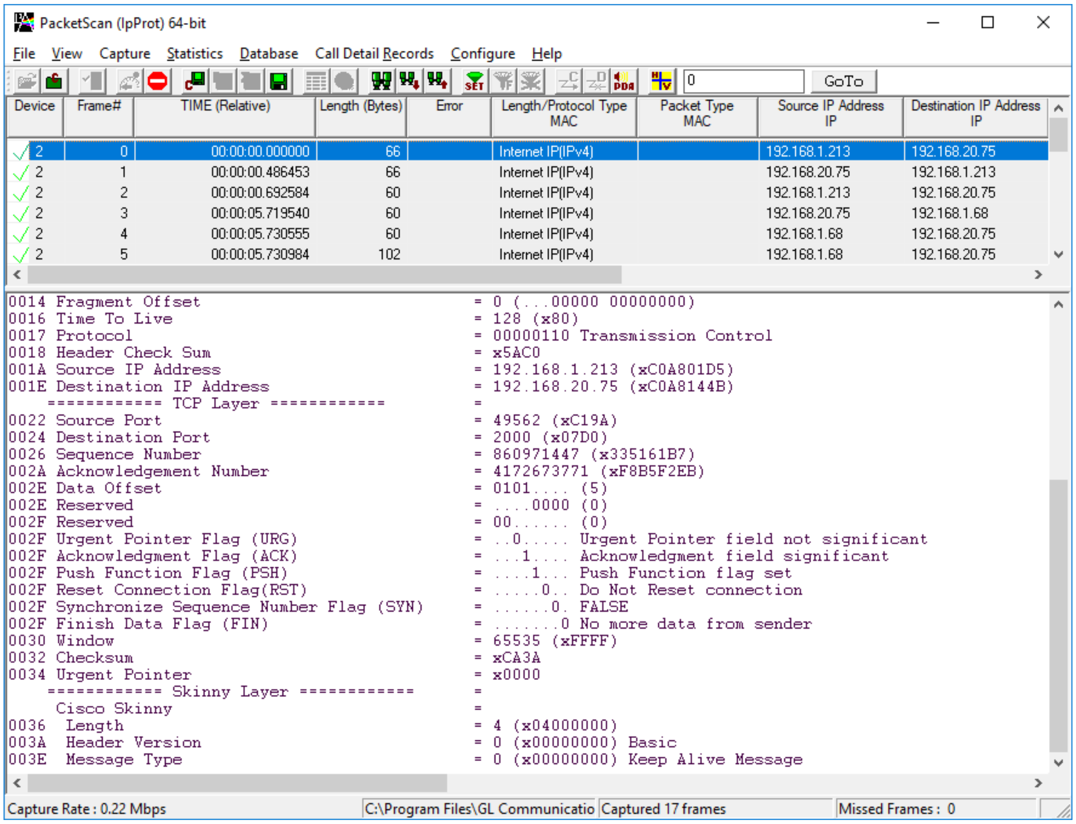
Select HDL File: Communications Inc\PacketScan\TRACES\Skinny-RTP.hdl

☐ Maintain Timing

☐ Continuous Playback   RepeatCounter : 0

8%

- observe the **Skinny** decodes displayed in PacketScan™ analyzer summary and detail views.



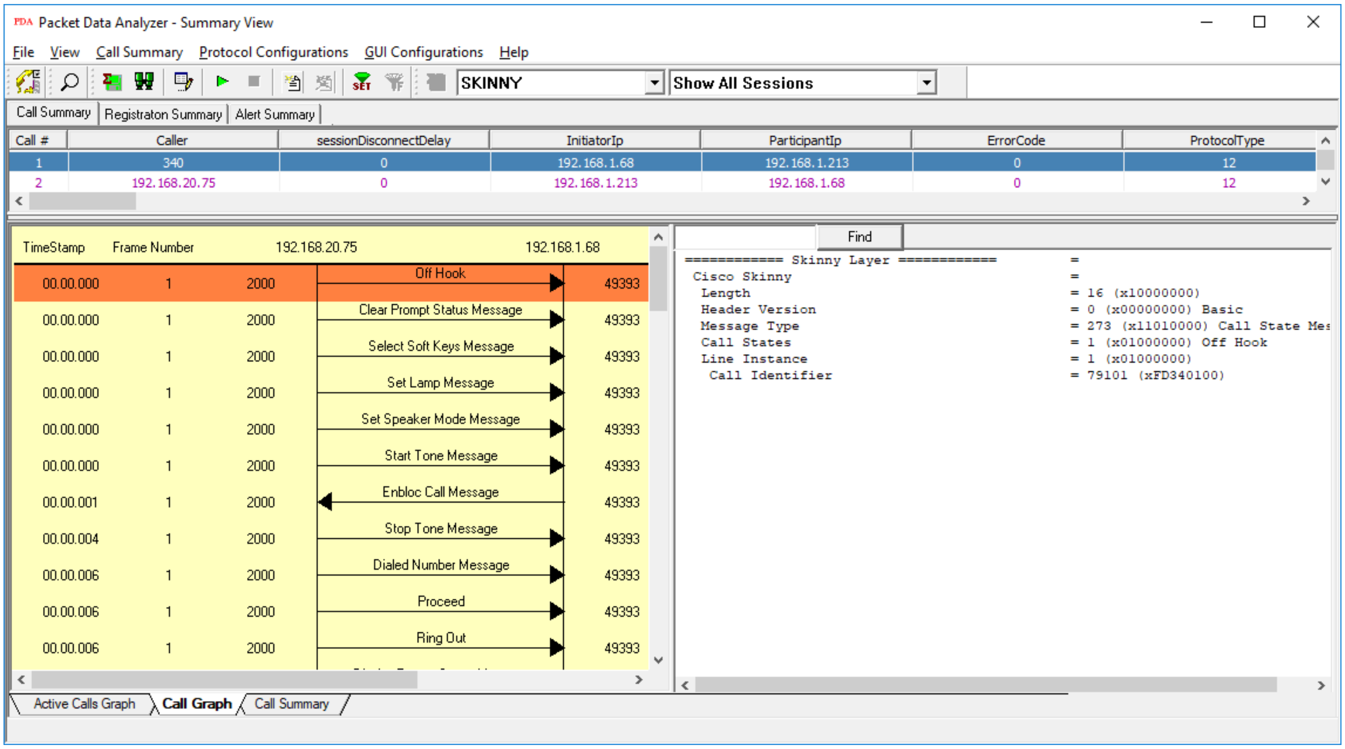
PacketScan (IpProt) 64-bit
File View Capture Statistics Database Call Detail Records Configure Help
0
GoTo

Device	Frame#	TIME (Relative)	Length (Bytes)	Error	Length/Protocol Type MAC	Packet Type MAC	Source IP Address IP	Destination IP Address IP
✓ 2	0	00:00:00.000000	66		Internet IP(IPv4)		192.168.1.213	192.168.20.75
✓ 2	1	00:00:00.486453	66		Internet IP(IPv4)		192.168.20.75	192.168.1.213
✓ 2	2	00:00:00.692584	60		Internet IP(IPv4)		192.168.1.213	192.168.20.75
✓ 2	3	00:00:05.719540	60		Internet IP(IPv4)		192.168.20.75	192.168.1.68
✓ 2	4	00:00:05.730555	60		Internet IP(IPv4)		192.168.1.68	192.168.20.75
✓ 2	5	00:00:05.730984	102		Internet IP(IPv4)		192.168.1.68	192.168.20.75

```
0014 Fragment Offset                          = 0 (...00000 00000000)
0016 Time To Live                             = 128 (x80)
0017 Protocol                                 = 00000110 Transmission Control
0018 Header Check Sum                         = x5AC0
001A Source IP Address                        = 192.168.1.213 (xC0A801D5)
001E Destination IP Address                   = 192.168.20.75 (xC0A8144B)
    ============ TCP Layer ============       =
0022 Source Port                              = 49562 (xC19A)
0024 Destination Port                         = 2000 (x07D0)
0026 Sequence Number                          = 860971447 (x335161B7)
002A Acknowledgement Number                   = 4172673771 (xF8B5F2EB)
002E Data Offset                              = 0101.... (5)
002E Reserved                                 = ....0000 (0)
002F Reserved                                 = 00...... (0)
002F Urgent Pointer Flag (URG)                = ..0..... Urgent Pointer field not significant
002F Acknowledgment Flag (ACK)                = ...1.... Acknowledgment field significant
002F Push Function Flag (PSH)                 = ....1... Push Function flag set
002F Reset Connection Flag(RST)               = .....0.. Do Not Reset connection
002F Synchronize Sequence Number Flag (SYN)   = ......0. FALSE
002F Finish Data Flag (FIN)                   = .......0 No more data from sender
0030 Window                                   = 65535 (xFFFF)
0032 Checksum                                 = xCA3A
0034 Urgent Pointer                           = x0000
    ============ Skinny Layer ============    =
     Cisco Skinny                             =
0036  Length                                  = 4 (x04000000)
003A  Header Version                          = 0 (x00000000) Basic
003E  Message Type                            = 0 (x00000000) Keep Alive Message
```

Capture Rate : 0.22 Mbps | C:\Program Files\GL Communicatio | Captured 17 frames | Missed Frames : 0

- From the **PacketScan™** main toolbar, click on the PDA icon PDA to invoke PDA (Packet Data Analyzer), from the drop-down protocol list select **SKINNY** to view detail analysis of each session, call graphs and quality scores for the captured **SKINNY** Traffic.



SKINNY

Show All Sessions

Call #	Caller	sessionDisconnectDelay	InitiatorIp	ParticipantIp	ErrorCode	ProtocolType
1	340	0	192.168.1.68	192.168.1.213	0	12
2	192.168.20.75	0	192.168.1.213	192.168.1.68	0	12

TimeStamp	Frame Number	192.168.20.75		192.168.1.68
00.00.000	1	2000	Off Hook →	49393
00.00.000	1	2000	Clear Prompt Status Message →	49393
00.00.000	1	2000	Select Soft Keys Message →	49393
00.00.000	1	2000	Set Lamp Message →	49393
00.00.000	1	2000	Set Speaker Mode Message →	49393
00.00.000	1	2000	Start Tone Message →	49393
00.00.001	1	2000	← Enbloc Call Message	49393
00.00.004	1	2000	Stop Tone Message →	49393
00.00.006	1	2000	Dialed Number Message →	49393
00.00.006	1	2000	Proceed →	49393
00.00.006	1	2000	Ring Out →	49393

```
============ Skinny Layer ============          =
 Cisco Skinny                                   =
  Length                                        = 16 (x10000000)
  Header Version                                = 0 (x00000000) Basic
  Message Type                                  = 273 (x11010000) Call State Mes
  Call States                                   = 1 (x01000000) Off Hook
  Line Instance                                 = 1 (x01000000)
   Call Identifier                              = 79101 (xFD340100)
```

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.