Avaya Solution & Interoperability Test Lab

Application Notes for Network General Sniffer Voice with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Network General Sniffer Voice to capture and analyze H.323 Voice over IP (VoIP) packets generated by Avaya Media Servers, Avaya Media Gateways, and Avaya IP Telephones. During compliance testing, Sniffer Voice successfully captured, decoded, and reported H.225 RAS messages and RTP/RTCP media streams at an Avaya IP Telephone, as well as H.225 signaling messages and RTP/RTCP media streams traversing an IP trunk between two independent Avaya Media Servers. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a compliance-tested configuration comprised of Avaya IP Telephony products, such as Avaya Media Servers running Avaya Communication Manager, Avaya Media Gateways, and Avaya IP Telephones, and Network General Sniffer Voice. Sniffer Voice is an add-on package for the Network General Sniffer Distributed, Sniffer Portable, and Netasyst network analysis products. Sniffer Voice monitors and captures H.323 Voice over IP (VoIP) packets, provides real-time analysis of Registration, Admission, and Status (RAS) messages, signaling exchanges, and media streams, and measures media stream quality (jitter, packet sequencing, packet loss, etc.).

Figure 1 illustrates a sample configuration consisting of an Avaya S8500 Media Server, an Avaya S8300 Media Server residing in an Avaya G350 Media Gateway, an Avaya G650 Media Gateway, an Avaya C364T-PWR Layer 2/3 Switch, Avaya 4600 Series IP Telephones, Avaya 6400 and 8400 Series Digital Telephones, analog telephones, and a Network General Sniffer Distributed s4000. Avaya Communication Manager runs on the S8500 and S8300 Media Servers. The solution described herein is also extensible to other Avaya Media Servers and Media Gateways.

In **Figure 1**, the S8500 Media Server/G650 Media Gateway and S8300 Media Server/G350 Media Gateway are independent systems at the main and branch sites, respectively. An IP trunk connects the two systems to support H.323 VoIP calls between the two sites. The G650 Media Gateway and G350 Media Gateway also provide the TDM-IP conversion necessary for transporting calls to and from non-IP devices over the IP network. On the C364T-PWR Layer 2/3 switch, the IP network traffic transmitted and received on an Ethernet port connected to an IP telephone or IP trunk is mirrored to an Ethernet port connected to a Sniffer Distributed s4000.

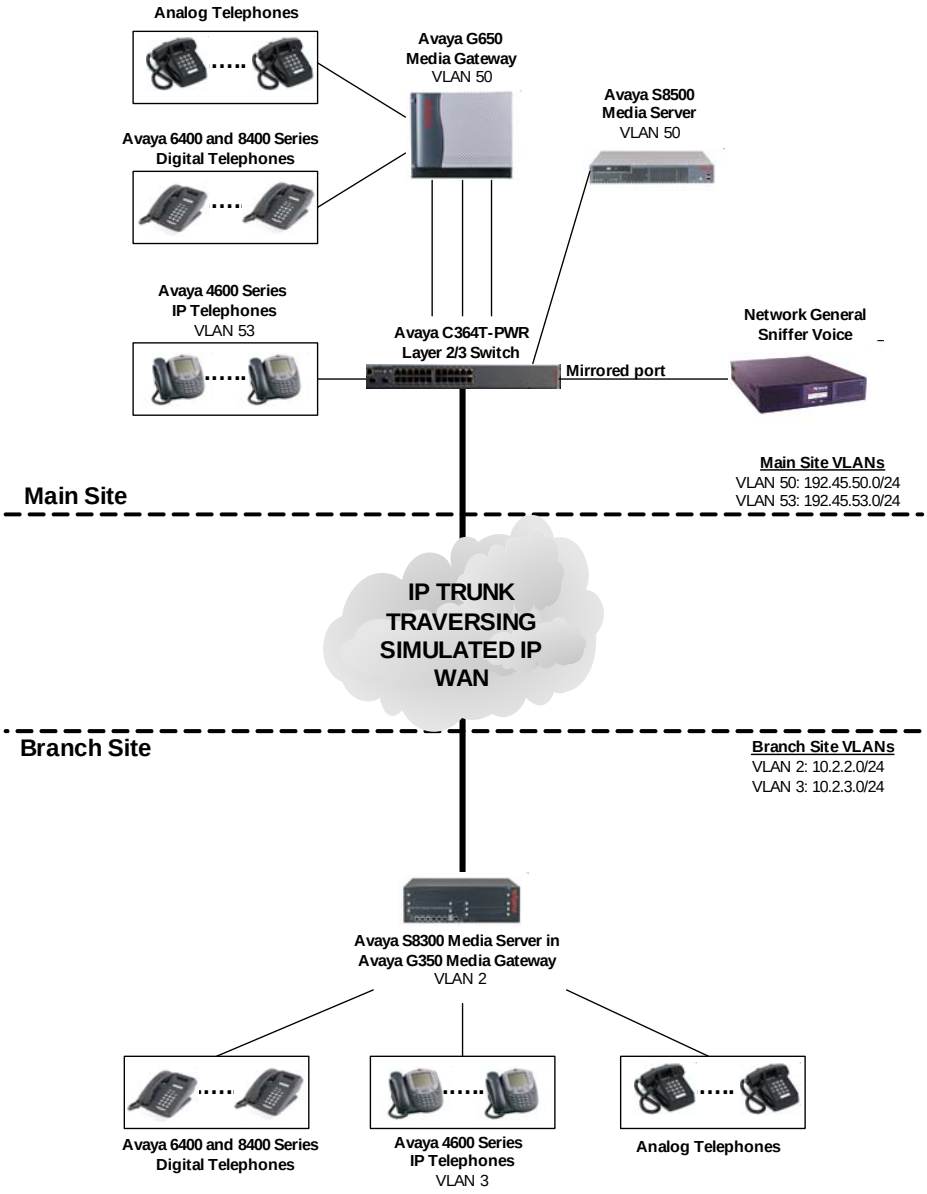


Figure 1: Sample configuration

2. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Equipment	Version
Avaya S8500 Media Server	Avaya Communication Manager 2.2
Avaya G650 Media Gateway	-
TN2312BP IP Server Interface	HW version 36 – FW version 12
TN799DP C-LAN Interface	HW version 1 – FW version 12
TN2302AP IP Media Processor	HW version 11 – FW version 95
Avaya S8300 Media Server	Avaya Communication Manager 2.2
Avaya G350 Media Gateway	23.17.0
Avaya 4600 Series IP Telephones	1.8.3 (4606) 1.8.3 (4612) 1.8.3 (4624) 1.8.2 (4602SW) 2.1.3 (4610SW) 2.1.3 (4620SW) 2.0.1 (4630SW)
Avaya 6400 Series Digital Telephones	-
Avaya 8400 Series Digital Telephones	-
Analog Telephones	-
Avaya C364T-PWR Layer 2/3 Switch	4.3.12
Network Sniffer Distributed s4000	Sniffer Distributed 4.50.118 (SP 1) Sniffer Voice 2.5 (See Note below)
Note: In Sniffer Distributed 4.5 Service Pack 1, the Sniffer Distributed console displays 2.10.505 rather than 2.5 as the Sniffer Voice version. Network General expects to resolve this in a future release.	

3. Configure Avaya Communication Manager

This section describes the steps for specifying IP codecs, and configuring IP network regions, H.323 IP trunks and signaling groups. The steps are performed from the System Access Terminal (SAT) interface and are generally applicable to both the S8500/G650 and S8300/G350 in the sample configuration; any differences are noted accordingly.

3.1. IP Codec Sets and IP Network Regions

Enter the **change ip-codec-set m** command, where "m" is a number between 1 and 7, inclusive, and enter one or more codecs for the IP codec set. IP codec sets will be selected later in the IP network region form to define which codecs may be used within an IP network region and between IP network regions. In the examples below, IP codec set 1 contains G.711MU and G.729, while IP codec set 2 contains only G.729.

```
change ip-codec-set 1                                          Page   1 of   2

                         IP Codec Set

   Codec Set: 1

   Audio      Silence      Frames   Packet
   Codec      Suppression  Per Pkt  Size(ms)
 1: G.711MU         n         2        20
 2: G.729           n         2        20
 3:
```

```
change ip-codec-set 2                                          Page   1 of   2

                         IP Codec Set

   Codec Set: 2

   Audio      Silence      Frames   Packet
   Codec      Suppression  Per Pkt  Size(ms)
 1: G.729           n         2        20
 2:
 3:
```

Enter the **change ip-network-region n** command, where "n" is a number between 1 and 250, inclusive. Note that the configurations of IP network regions are locally significant only. The S8300/G350 is unaware of how IP network regions are configured on the S8500/G650, and vice versa.

On page 1 of the **ip-network-region** form, configure the following:

- **Codec Set** – Enter the number of a configured IP codec set.

- **Intra-region IP-IP Direct Audio** ("shuffling") – if set to **yes**, RTP audio paths may be established directly between IP endpoints within this region, without using IP Media Processor (MedPro) board resources.
- **Inter-region IP-IP Direct Audio** ("shuffling") – if set to **yes**, RTP audio paths may be established directly between an IP endpoint within this region and an IP endpoint or Media Gateway in another region, without using local MedPro board resources.

```
change ip-network-region 1                                    Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location:                  Home Domain:
    Name:
                                Intra-region IP-IP Direct Audio: yes
AUDIO PARAMETERS                Inter-region IP-IP Direct Audio: yes
   Codec Set: 1                           IP Audio Hairpinning? y
UDP Port Min: 2048
UDP Port Max: 3028                        RTCP Reporting Enabled? y
                              RTCP MONITOR SERVER PARAMETERS
DIFFSERV/TOS PARAMETERS        Use Default Server Parameters? y
 Call Control PHB Value: 48
        Audio PHB Value: 48
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

On Page 3 of the form, specify the IP **codec set** for every pair of source and destination IP network regions. In the example below, IP calls from IP network region 1 to IP network region 2 may use the codecs defined in IP codec set 2.

```
change ip-network-region 1                                    Page   3 of  19

                   Inter Network Region Connection Management

 src dst  codec  direct                                    Dynamic CAC
 rgn rgn   set    WAN    WAN-BW-limits  Intervening-regions    Gateway
 1   1     1
 1   2     2       y           :NoLimit
 1   3
```

3.2. H.323 IP Trunks and Signaling Groups

On the S8300/G350, enter the **change node-names ip** command, specify a node name for the C-LAN board of the S8500/G650, and enter its IP address. The node name and IP address for **procr** (Processor Ethernet) is automatically set when the S8300 is configured with an IP address.

```
change node-names ip                                          Page   1 of   1
                                  IP NODE NAMES
    Name                 IP Address          Name             IP Address
G650-CLAN1A02         192.45 .50 .7                            .   .   .
default               0  .0  .0  .0                           .   .   .
procr                 10 .2  .2  .5                           .   .   .
```

On the S8500/G650, enter the **change node-names ip** command, specify node names and IP addresses for the Processor Ethernet of the S8300 and the C-LAN board, and enter their respective IP addresses.

```
change node-names ip                                          Page   1 of   1
                                  IP NODE NAMES
    Name                 IP Address          Name             IP Address
CLAN-1A02             192.45 .50 .7                            .   .   .
S8300-G350-ICC        10 .2  .2  .5                           .   .   .
MEDPRO-1A03           192.45 .50 .8                           .   .   .
MEDPRO-1A13           192.45 .50 .9                           .   .   .
MEDPRO-1B03           192.45 .50 .10                          .   .   .
MEDPRO-1B13           192.45 .50 .11                          .   .   .
default               0  .0  .0  .0                           .   .   .
procr                    .   .   .                            .   .   .
```

Enter the **add trunk-group p** command, where "p" is an available trunk group number. On Page 1 of the **trunk-group** form, configure the following:

- **Group Type** – set to "**isdn**".
- **Group Name** – enter a meaningful name/description.
- **Carrier Medium** – set to "**IP**".
- **Service Type** – set to "**tie**".

The following example shows the configuration of the IP trunk group on the S8500/G650. The IP configuration of the IP trunk group on the S8300/G350 is the same, except possibly the **Group Name**.

```
change trunk-group 11                                          Page   1 of  22
                                TRUNK GROUP

Group Number: 11                    Group Type: isdn          CDR Reports: y
  Group Name: H.323 Calls to S8300/G350   COR: 1        TN: 1        TAC: 111
   Direction: two-way        Outgoing Display? n         Carrier Medium: IP
 Dial Access? y                Busy Threshold: 255       Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n           TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
TRUNK PARAMETERS
         Codeset to Send Display: 6    Codeset to Send National IEs: 6
        Max Message Size to Send: 260  Charge Advice: none
  Supplementary Service Protocol: a    Digit Handling (in/out): enbloc/enbloc

            Trunk Hunt: cyclical
                                                  Digital Loss Group: 18
Incoming Calling Number - Delete:     Insert:                 Format:
              Bit Rate: 1200         Synchronization: async    Duplex: full
 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 0
```

Enter the **add signaling-group q** command, where "q" is an available signaling group number. On Page 1 of the **signaling-group** form, configure the following:

- **Group Type** – set to "**h.323**".
- **Trunk Group for Channel Selection** – enter the number of the trunk group (configured above) to be associated with this signaling group.
- **Near-end Node Name** – enter the node name of a local C-LAN board, or "**procr**" if the local node is an S8300.
- **Near-end Listen Port** – specify the local listen port, typically 1720.
- **Far-end Node Name** – enter the node name of a C-LAN board or processor Ethernet on the remote Avaya system.
- **Far-end Listen Port** – specify the remote listen port, typically 1720.
- **Far-end Network Region** – (optional) assign a network region to the remote system.
- **Direct IP-IP Audio Connections** – if set to "**yes**", then RTP audio paths may be established directly between IP endpoints that use the associated IP trunk.

The example below shows the configuration of the H.323 signaling group on the S8500/G650. Note that the **Far-end Network Region** is set to **2**. This means that from the perspective of the near-end system (S8500/G650), the entire system at the far end (S8300/G350) of the IP trunk is considered to be in IP network region 2, **as defined on the near-end system**. The configuration of the H.323 signaling group on the S8300/G350 is similar, with the node names and **Far-end Network Region** set to locally configured and significant values.

```
add signaling-group 11                                        Page   1 of   5
                              SIGNALING GROUP

 Group Number: 11             Group Type: h.323
                            Remote Office? n        Max number of NCA TSC: 0
                                      SBS? n         Max number of CA TSC: 0
                                                  Trunk Group for NCA TSC:
      Trunk Group for Channel Selection: 11
         Supplementary Service Protocol: a
                        T303 Timer(sec): 10

       Near-end Node Name: CLAN-1A02     Far-end Node Name: S8300-G350-ICC
     Near-end Listen Port: 1720         Far-end Listen Port: 1720
                                      Far-end Network Region: 2
             LRQ Required? n          Calls Share IP Signaling Connection? n
             RRQ Required? n
                                          Bypass If IP Threshold Exceeded? n

             DTMF over IP: out-of-band     Direct IP-IP Audio Connections? y
                                                   IP Audio Hairpinning? y
                                           Interworking Message: PROGress
```

Enter the **change trunk-group p** command, where "p" is the number of the trunk group configured earlier. On Page 6 of the **trunk-group** form, add one or more trunk members by entering "**IP**" for **Port** and the number of the signaling group configured earlier for **Sig Grp**.

```
add trunk-group 11                                            Page   6 of  22
                                TRUNK GROUP
                                     Administered Members (min/max):   0/0
GROUP MEMBER ASSIGNMENTS                 Total Administered Members:   0

       Port    Code Sfx Name        Night           Sig Grp
  1: IP                                              11
  2: IP                                              11
  3: IP                                              11
  4: IP                                              11
  5: IP                                              11
  6: IP                                              11
  7: IP                                              11
  8: IP                                              11
```

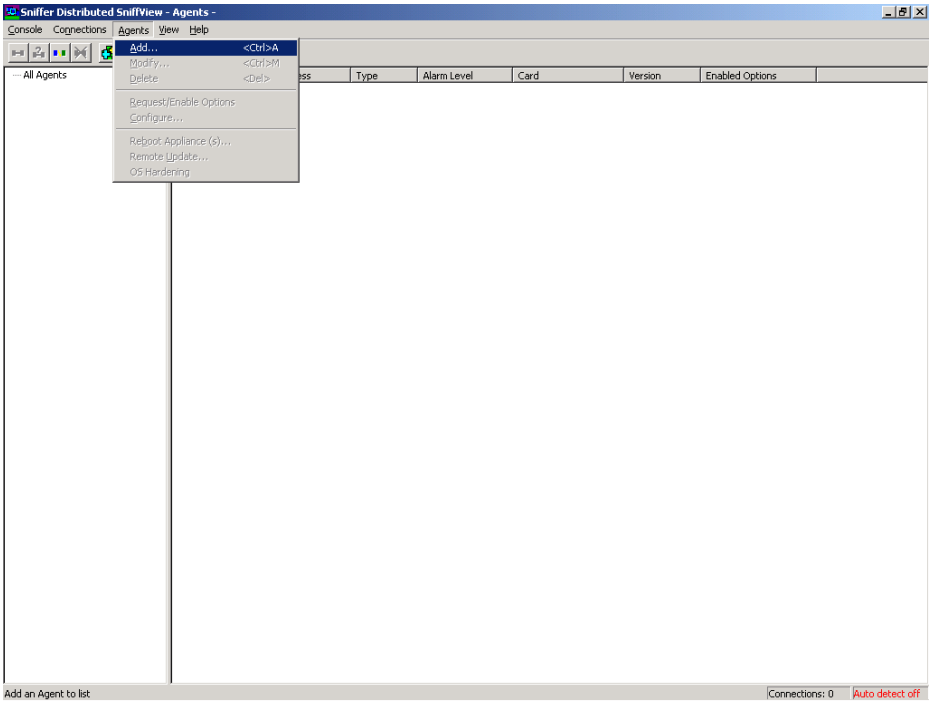
4. Configure Port Mirroring on Avaya C364T-PWR

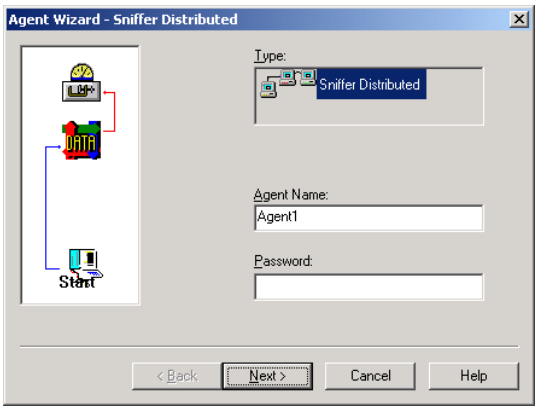
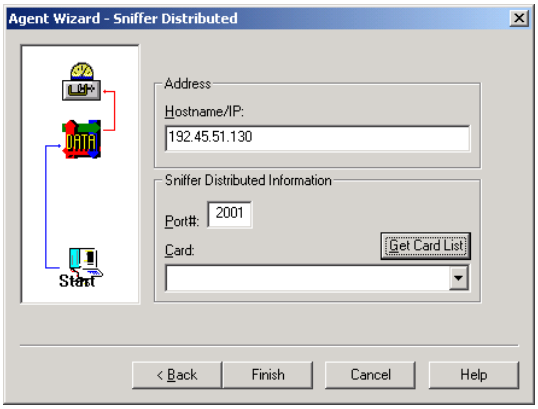
Enter the **set port mirror** command in the command line interface of the Avaya C364T-PWR to copy all bi-directional traffic from a source port to a mirror port. The source port is connected to an Avaya IP telephone or IP trunk, and the mirror port is connected to the Sniffer Distributed appliance.

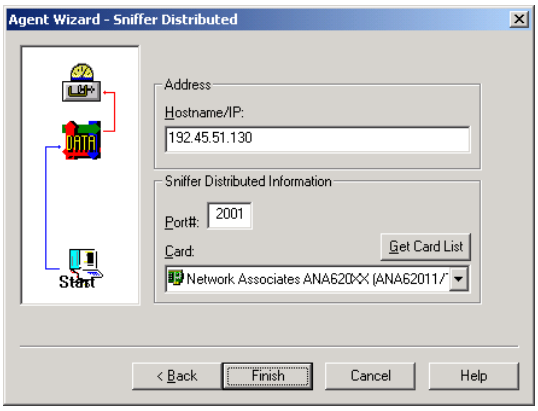
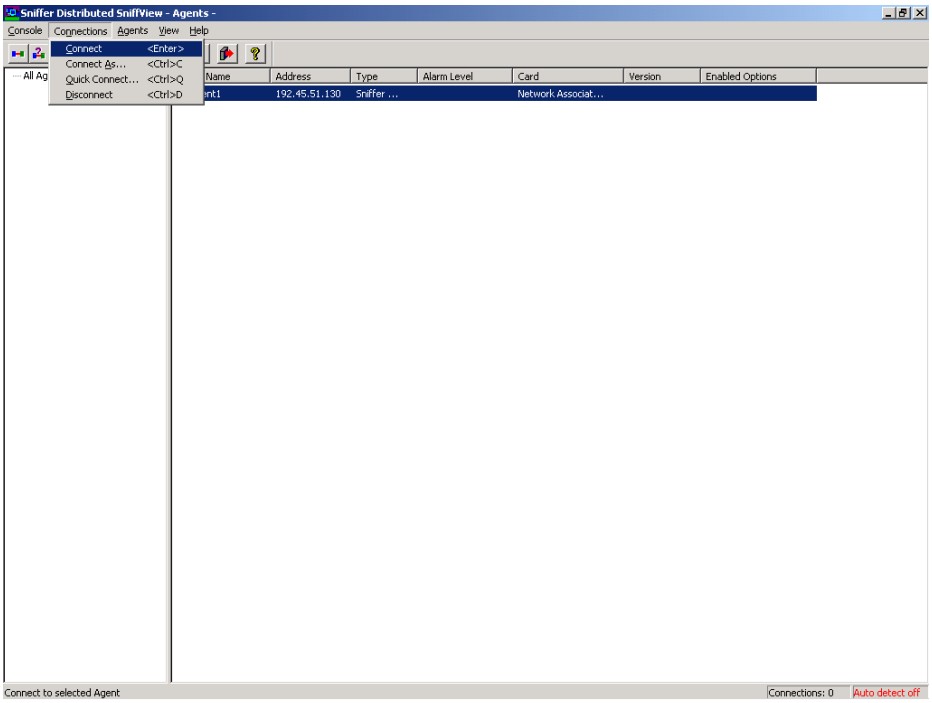
```
C360-1(super)# set port mirror source-port 1/47 mirror-port 1/45 sampling
always direction both
Mirroring both Rx and Tx packets from port 1/47 to port 1/45 is enabled
```

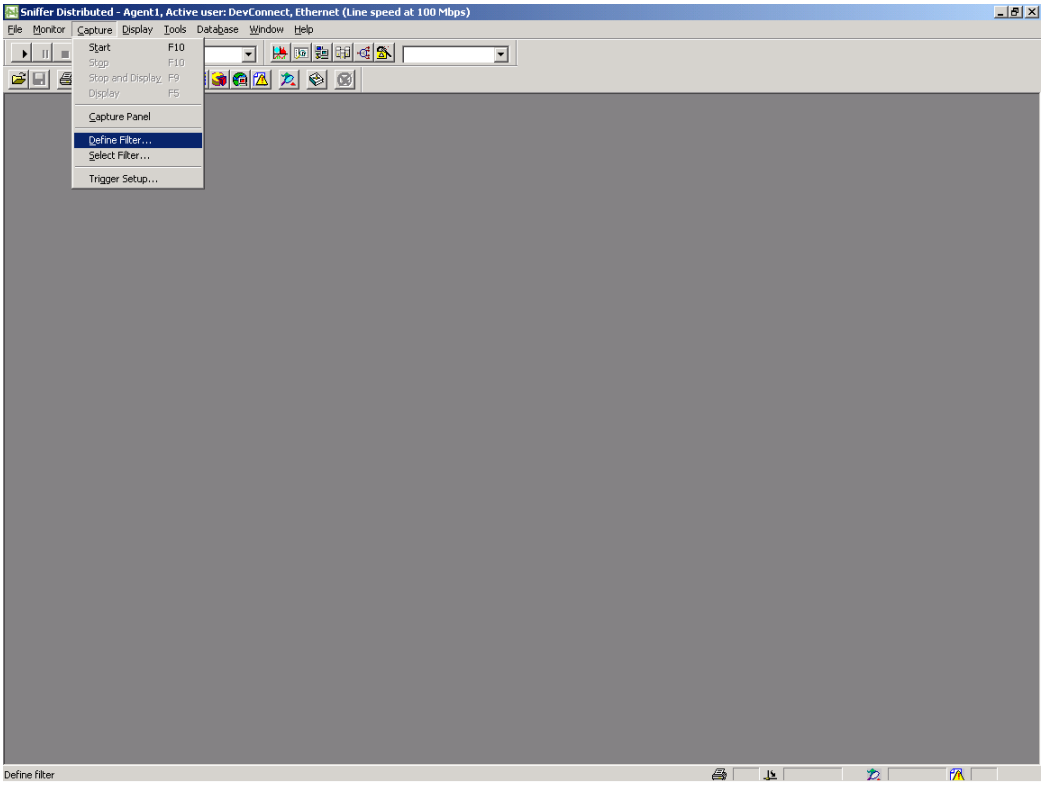
5. Configure Network General Sniffer Voice

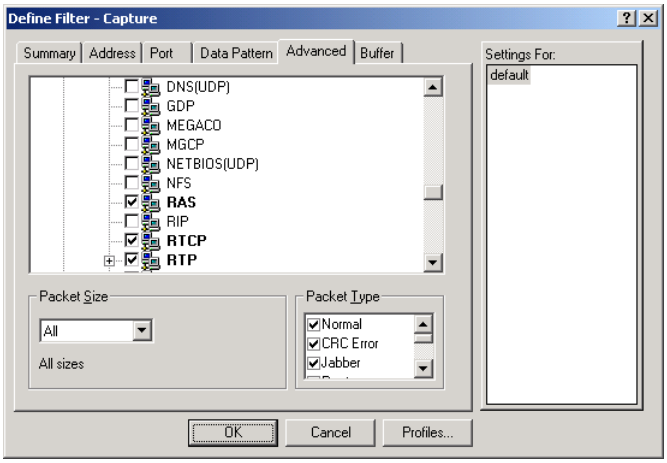
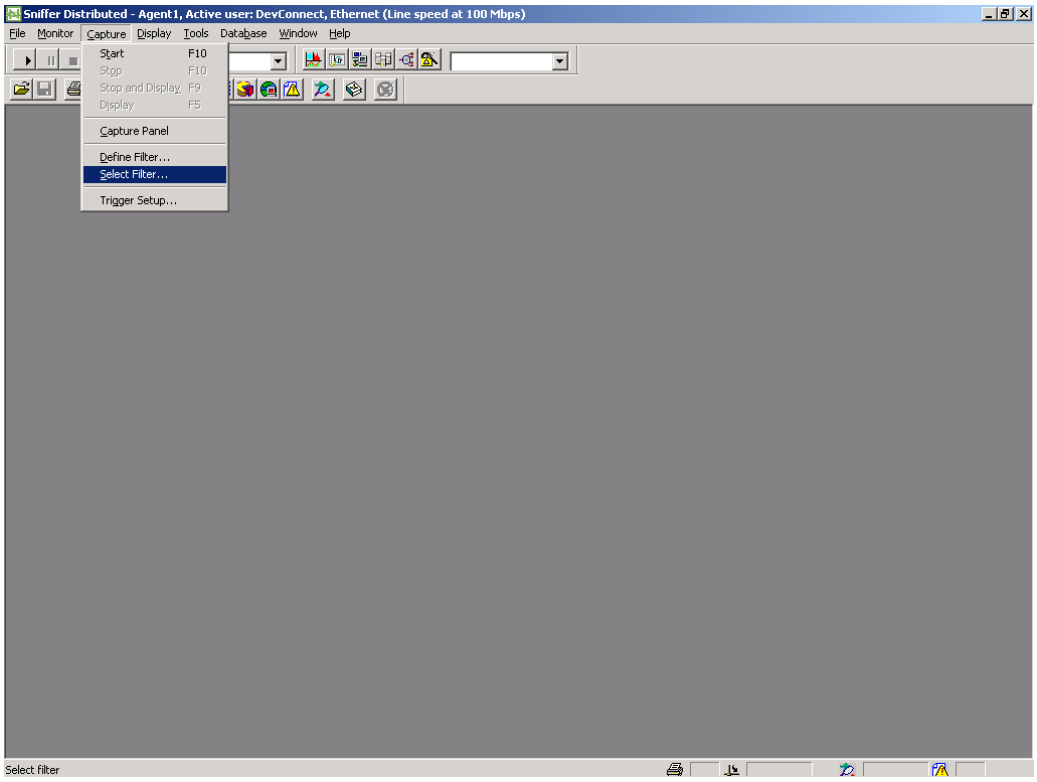
This section describes the steps for adding and defining Sniffer Distributed Agents to the Sniffer Distributed SniffView console and defining capture filters on the Sniffer Distributed appliances. The following assumes that Agents have been properly installed and configured on the Sniffer Distributed appliances.

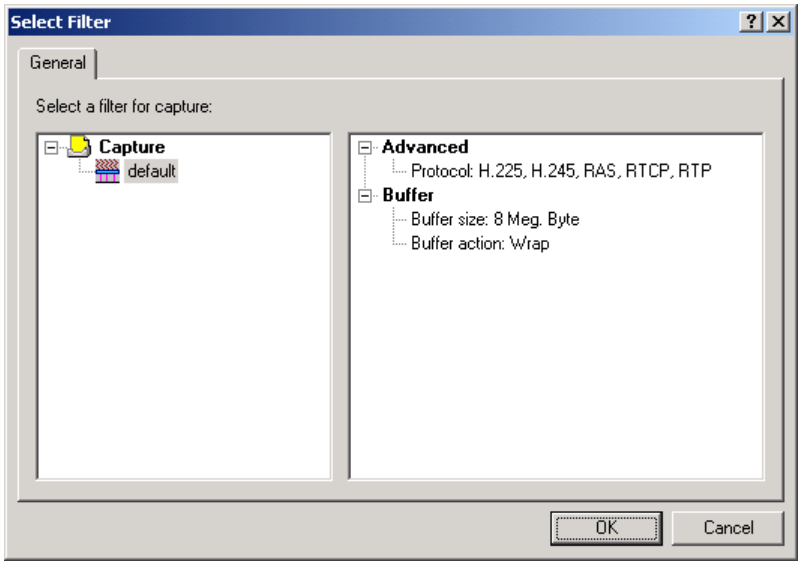
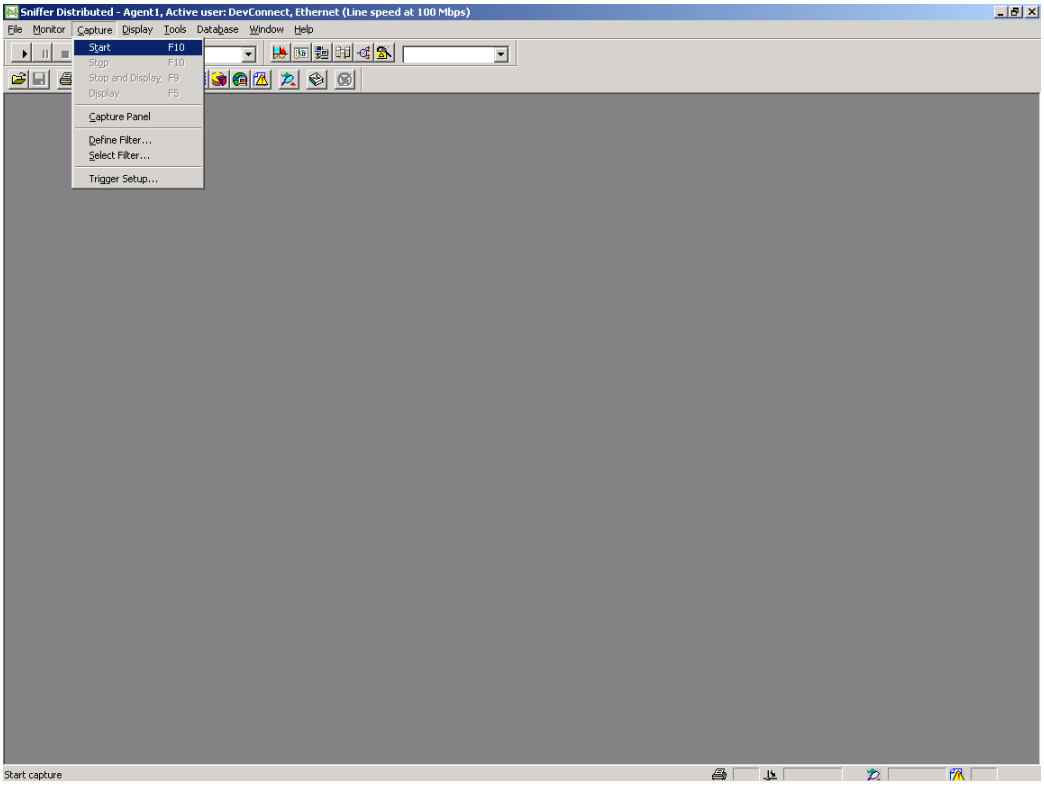
Step	Description
1.	Launch the Network General Sniffer Distributed SniffView application and log in with the appropriate credentials.
2.	In the **Sniffer Distributed SniffView** main window, select "**Add…**" from the **Agents** menu to add and define a Sniffer Distributed Agent to SniffView. 

Step	Description
3.	In the **Agent Wizard** window, assign an **Agent Name** and enter a **Password** if a password was configured on the Agent. **Password** may be left blank if no password is required to access the Agent. Click on "**Next**". 
4.	Continuing in the **Agent Wizard**, enter the hostname or IP address of the Sniffer Distributed Appliance for **Hostname/IP** and click on "**Get Card List**". 

Step	Description
5.	Continuing in the **Agent Wizard**, select one of the network cards on the Sniffer Distributed appliance from the card list and click on "**Finish**". The selected network card should be connected to a mirror port configured in Section 4. 
6.	Repeat Steps 2 through 5 to add and define additional Agents within SniffView. Note that since a Sniffer Distributed appliance may have multiple network cards, an Agent must be added and defined for each network card used to capture network traffic.
7.	In the **Sniffer Distributed SniffView** main window, select an Agent and select "**Connect**" from the **Connections** menu. 

Step	Description
8.	By default, the Sniffer Distributed Agent captures all packets received on its associated network interface. If capturing all packets is desired, then skip to Step 12. To capture packets meeting specific criteria, select "**Define Filter…**" from the **Capture** menu of the **Sniffer Distributed Agent** console main window. 

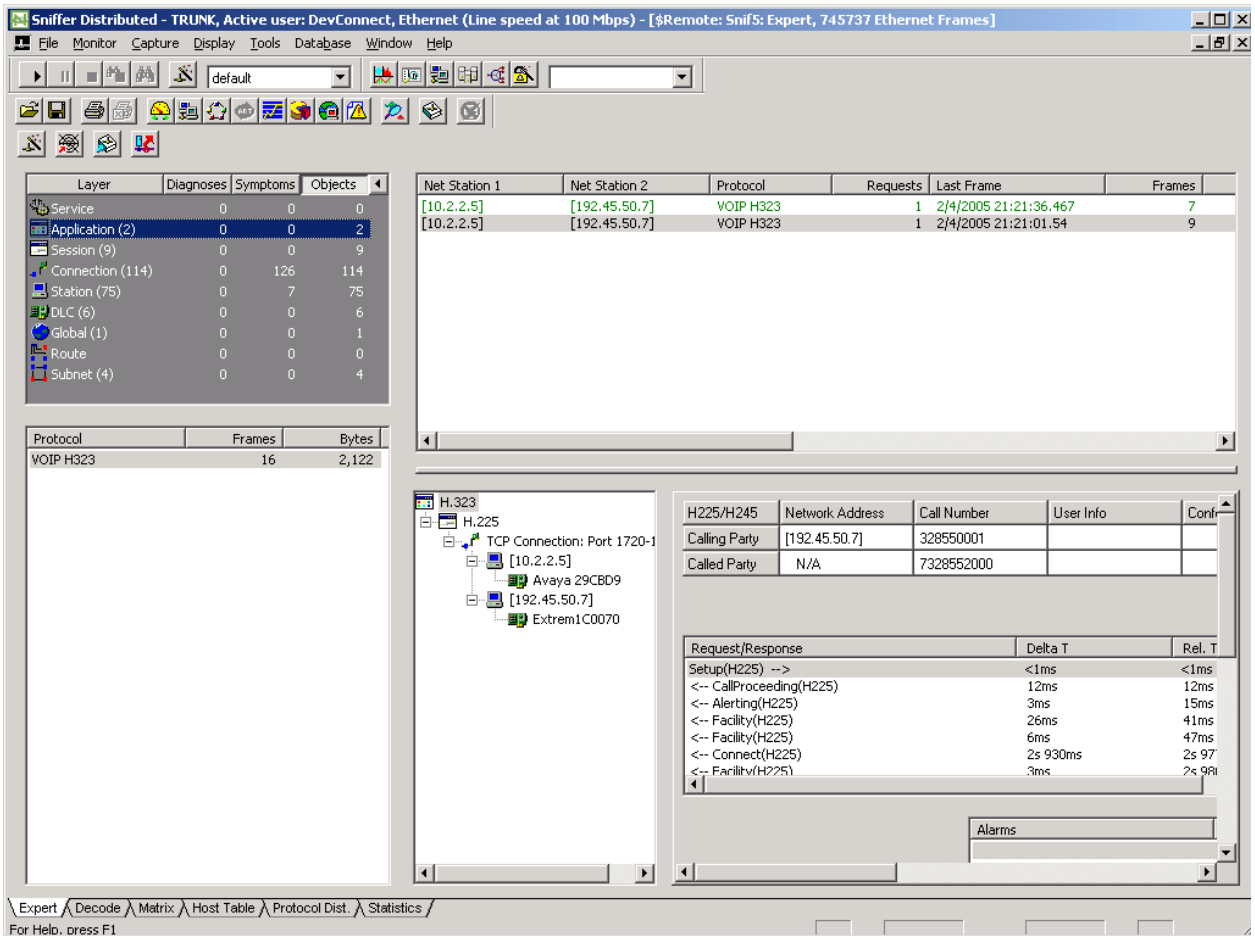
Step	Description
9.	In the **Define Filter – Capture** window, select the **Advanced** tab and check the checkboxes for "**IP**", "**TCP**", "**UDP**", "**H.225**", "**H.245**", "**RAS**", "**RTCP**", and "**RTP**". Note that the checkboxes are hierarchical, i.e. "**RAS**", "**RTCP**", and "**RTP**" are under "**UDP**", which in turn is under "**IP**". Click on **"OK"**. 
10.	In the **Sniffer Distributed Agent** console main window, click on "**Select Filter…**" from the **Capture** menu. 

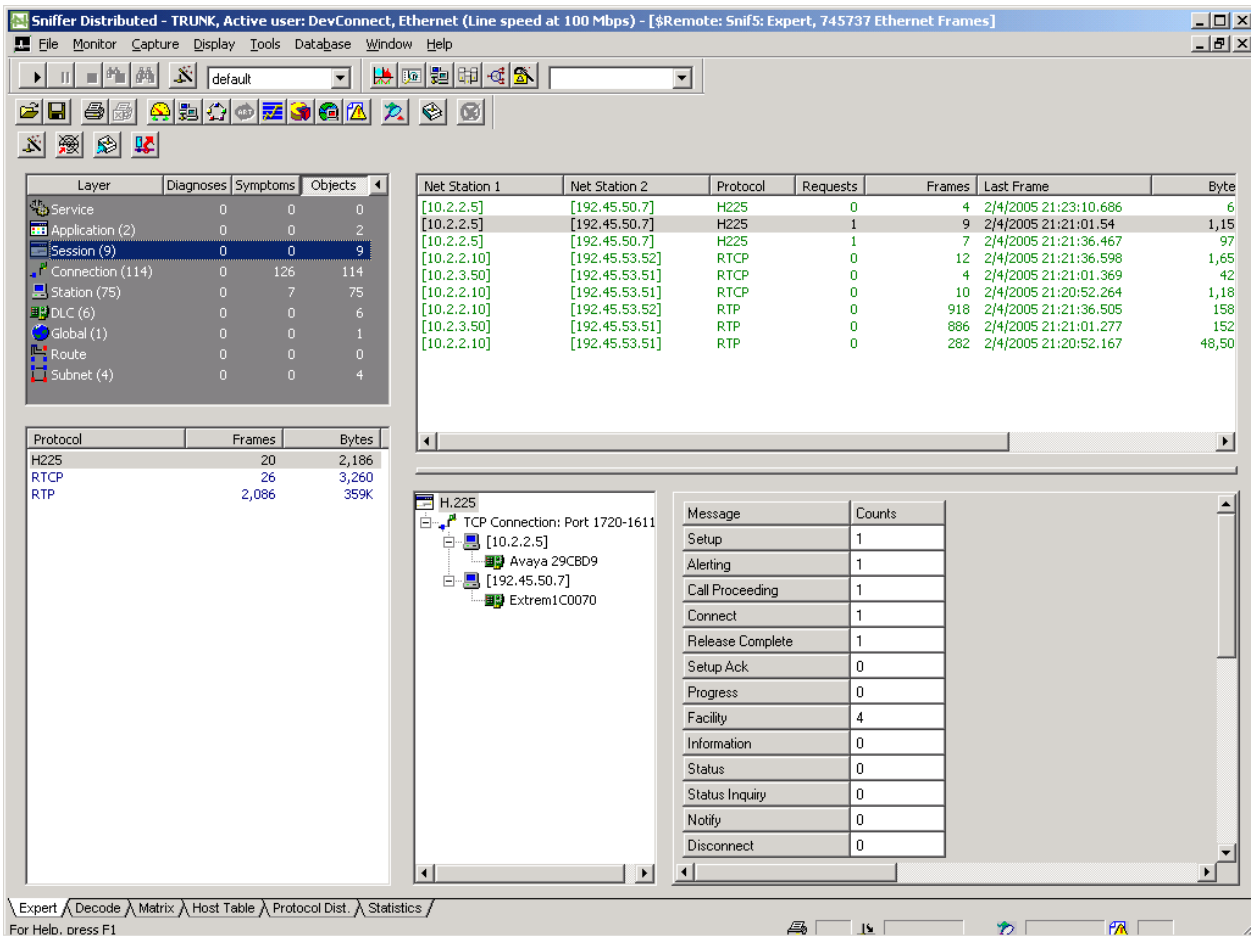
Step	Description
11.	In the **Select Filter** window, select the capture filter defined in the previous steps and click on "**OK**". 
12.	In the **Sniffer Distributed Agent** console main window, select "**Start**" from the **Capture** menu. 

6. Network General Sniffer Voice Capture Analysis

Sniffer Voice presents captured traffic in various views, including the Expert and Decode views. The Expert view provides analysis at several layers, such as the Application, Session, and Connection layers, summarizing information such as network addresses, calling and called party numbers, and codecs. The Decode view presents raw packet data along with interpretations of fields and values. Consult the Network General documentation for further details.

The following sample screenshots show the Expert view at the Application and Session layers. Each H.323 call is classified as an Application Object, and each set of H.225 signaling messages associated with a single call flow between two IP ports is classified as a Session Object. Each bi-directional RTP or RTCP media stream between two IP ports is also classified as a Session Object.





7. Interoperability Compliance Testing

The interoperability compliance testing included feature, serviceability, and performance testing. The feature testing evaluated the ability of Sniffer Voice to capture H.225 RAS and RTP/RTCP media streams inbound and outbound from Avaya IP telephones, and H.225 signaling and RTP/RTCP media streams going across Avaya IP trunks. The serviceability testing introduced failure scenarios to see if Sniffer Voice can resume packet capture after failure recovery. The performance testing stressed Sniffer Voice by continuously placing H.323 VoIP calls across an Avaya IP trunk over extended periods of time.

7.1. General Test Approach

The general approach was to configure Sniffer Voice to monitor network traffic for H.323 VoIP traffic at Avaya IP telephones and Avaya IP trunks. For feature testing, successful and unsuccessful Avaya IP telephone registration and un-registration scenarios were exercised, and calls with various characteristics (shuffling on/off, different codecs, transfers, conferences, hold, busy) were placed across Avaya IP trunks. For performance testing, a call generator continuously placed calls across an Avaya IP trunk monitored by Sniffer Voice. For

serviceability testing, failures such as cable pulls, traffic impairments (jitter, packet loss, and out of sequence packets), and resets were applied.

7.2. Test Results

Sniffer Voice successfully captured and decoded RAS messages and RTP/RTCP packets at an Avaya IP telephone, as well as H.225 call signaling messages (i.e., Setup, Call Proceeding, Alerting, Connect, Facility, and Release Complete) and RTP/RTCP packets going across an Avaya IP trunk. For serviceability testing, Sniffer Voice was able to resume capturing and decoding H.323 VoIP packets after failure recovery, provide measurements of jitter, packet loss, and out of sequence packets, and generate alarms for excessive traffic impairments and call volume. For performance testing, Sniffer Voice captured a continuous, low to moderate call volume for over 15 hours, and continued to successfully capture and decode H.323 VoIP packets afterwards.

The following observations were made during testing:

- In Sniffer Distributed 4.5 Service Pack 1, the Sniffer Distributed console displays 2.10.505 rather than 2.5 as the Sniffer Voice version. Network General expects to resolve this in a future release.
- The first digit of the Calling Party Number is missing in the Expert view of an H.323 call (the entire number is visible in the Decode view however). Network General plans to resolve this in a future release.
- The RTP/RTCP media streams and call signaling messages of a call were presented independently in the Expert view. Network General plans to present RTP media streams together with their associated call signaling messages in a future release.
- On occasion, RTP packets were identified as SSL packets. Network General plans to resolve this in a future release.

8. Verification Steps

The following steps may be used to verify the configuration:

- Configure Sniffer to capture network traffic at an Avaya IP telephone and across an Avaya IP trunk. Verify that Sniffer captures ping messages to the IP telephone and across the IP trunk.
- Using the SAT, enter the command **list trace ras ip-address ip**, where "ip" is the IP address of a registered (or unregistered) IP telephone. Unregister (or register) the IP telephone, and verify that the RAS messages captured by Sniffer Voice are consistent with the trace provided by the SAT.
- Place a call to or from the IP telephone and verify that Sniffer Voice captures the inbound and outbound RTP/RTCP streams.
- Place a call across the IP trunk and verify that Sniffer Voice captures the signaling and RTP/RTCP streams in both directions.

9. Support

For technical support on Network General products, contact Network General at:

- Phone: 1-800-SNIFFER (1-800-764-3337)
- Email: support@networkgeneral.com

10. Conclusion

These Application Notes illustrate the procedures for configuring Network General Sniffer Voice to capture and analyze H.323 Voice over IP (VoIP) packets generated by Avaya Media Servers, Avaya Media Gateways, and Avaya IP Telephones. During compliance testing, Sniffer Voice successfully captured, decoded, and reported H.225 RAS messages and RTP/RTCP media streams at an Avaya IP Telephone, as well as H.225 signaling messages and RTP/RTCP media streams traversing an IP trunk between two independent Avaya Media Servers. Sniffer Voice was also able to capture VoIP packets going across the IP trunk under continuous call volumes over extended periods of time.

11. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.

Product information for Network General products may be found at http://www.networkgeneral.com/Product_Home.aspx.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.