AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for the SecureLogix Enterprise Telephony Management System with Avaya Communication Manager – Issue 1.0

Abstract

These Application Notes describe the steps for configuring the SecureLogix Enterprise Telephony Management (ETM) System to monitor and control inbound and outbound telecom activity on Avaya Communication Manager T1 and H.323 trunks. During compliance testing, the ETM System successfully detected and monitored inbound and outbound calls placed across Avaya Communication Manager T1 and H.323 trunks, and allowed or terminated calls when certain configurable conditions were met. 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.

RL; Reviewed:
SPOC 12/15/2005
Solution & Interoperability Test Lab Application Notes
©2005 Avaya Inc. All Rights Reserved.
1 of 49
SecureLogixETM.doc

1. Introduction

These Application Notes describe a compliance-tested configuration comprised of Avaya Communication Manager and the SecureLogix Enterprise Telephony Management (ETM) System. Placed on the edge of the enterprise telephony network, the ETM System monitors, controls, and logs inbound and outbound telecom activity on public and/or private trunks based on user-defined ETM security policies. The ETM System also protects enterprise telecom resources against external attacks, unauthorized access or abusive use by internal and external callers, toll fraud, and other forms of telephony line abuse.

ETM security policies are configured as sets of Voice Firewall or Voice Intrusion Protection System (IPS) rules. The Voice Firewall rules apply on a per-call basis, and allow the ETM System to permit or terminate calls based on the detected call type (voice, FAX, and modem for example), call direction (inbound or outbound), calling/called party numbers, call duration, or any combination thereof. For example, a Voice Firewall policy can be configured with one or more rules that permit outbound international calls, but terminate the calls if the calls last longer than one hour. The Voice IPS rules apply on an interval basis, and allow the ETM System to track activity over time and take action if necessary. For example, a Voice IPS policy can be configured with one or more rules that monitor for unusually large numbers of short duration inbound calls (which may indicate war-dialing attacks) over one-hour intervals.

Figure 1 illustrates a sample configuration consisting of an Avaya S8710 Media Server, an Avaya G650 Media Gateway, an Avaya S8300 Media Server residing in an Avaya G350 Media Gateway, a SecureLogix ETM 1090 Hybrid Appliance, a SecureLogix ETM Management Server, and a SecureLogix ETM System Console. Avaya Communication Manager runs on the S8710 Media Server and S8300 Media Server, and the S8710 Media Server with G650 Media Gateway and S8300 Media Server in G350 Media Gateway are independent Avaya Communication Manager systems. The solution described herein is also extensible to other Avaya Media Servers and Media Gateways. The ETM System software runs on the ETM 1090 Hybrid Appliance. The Avaya IP Telephones, FAX machine, and modem in **Figure 1** support the illustration and verification of the solution and are not discussed in these Application Notes.

Note in **Figure 1** that for monitoring and controlling the T1 line between the PSTN and the Avaya G650 Media Gateway, the ETM appliance resides inline on the T1 path. Further note that for monitoring the inbound and outbound H.323 VoIP signaling traffic to and from the G650 Media Gateway, the ETM appliance connects to a mirror port that mirrors either the C-LAN or uplink ports. To terminate H.323 VoIP trunk calls on the G650 Media Gateway, however, the ETM appliance must be placed inline[1] in the path between the C-LAN and the far-end Avaya Communication Manager system (the S8300 Media Server in G350 Media Gateway).

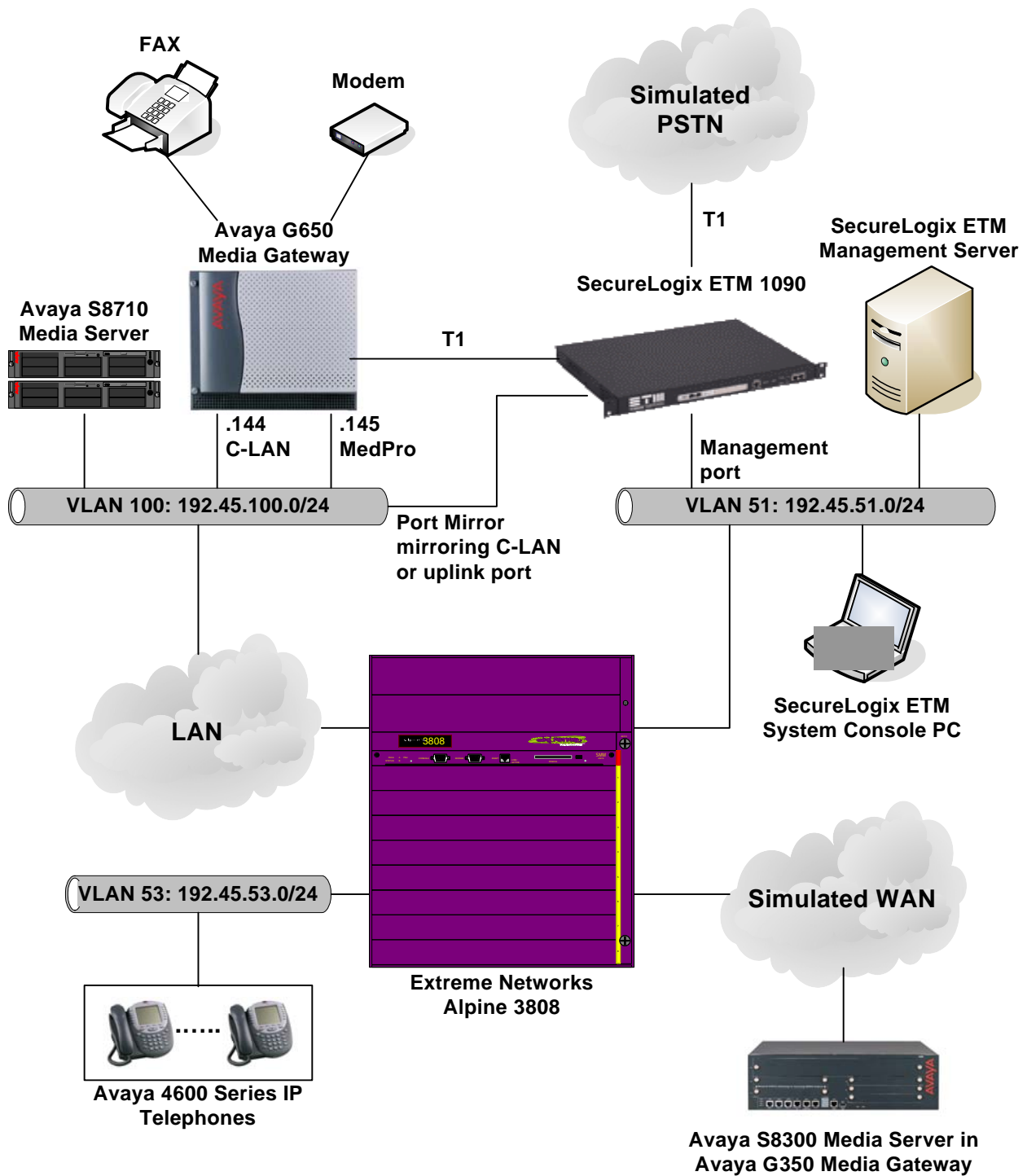[1] Not shown in **Figure 1** but tested during compliance testing.

Figure 1: Sample configuration.

RL; Reviewed:
SPOC 12/15/2005

Solution & Interoperability Test Lab Application Notes
©2005 Avaya Inc. All Rights Reserved.

3 of 49
SecureLogixETM.doc

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8710 Media Server	3.0 (R013x.00.0.340.3)
Avaya G650 Media Gateway	-
TN2312BP IP Server Interface	21
TN799DP C-LAN Interface	15
TN2302AP IP Media Processor	104
TN464GP DS1 Interface	17
Avaya S8300 Media Server	3.0 (R013x.00.0.340.3)
Avaya G350 Media Gateway	24.21.1
Avaya 4600 Series IP Telephones	1.8.2 (4602SW)
	2.2.3 (4610SW)
	2.2.3 (4620SW)
	2.0.2 (4630SW)
Extreme Networks Alpine 3808	7.3.2.3
Fax machine	-
Modem	-
SecureLogix ETM 1090 Hybrid Communications Appliance	5.1.12
SecureLogix ETM Management Server	5.1.0 Build 14
SecureLogix ETM System Console	5.1.0 Build 14

3. Configure Avaya Communication Manager

This section describes the steps for configuring DS1 circuit packs, trunk groups, and signaling groups on Avaya Communication Manager. The steps are performed from the System Access Terminal (SAT) interface.

3.1. DS1 Circuit Pack Configuration

This section describes the steps for configuring the T1 line on Avaya Communication Manager in the sample configuration of **Figure 1**.

Step	Description

1.	Enter the **list configuration all** command and note the **Board Number**(s) of the DS1 circuit pack(s) to be configured.
	
	<pre>list configuration all Page 2
	
	                        SYSTEM CONFIGURATION
	
	Board Assigned Ports
	Number Board Type Code Vintage u=unassigned t=tti p=psa
	
	01A06 CONTROL-LAN TN799DP HW00 FW015 u u u u u u u u
	                                                 u u u u u u u u
	                                                 17
	01A07 DS1 INTERFACE TN464GP HW02 FW017 u u u u u u u u
	                                                 u u u u u u u u
	                                                 u u u u u u u u
	                                                 u u u u u u u u
	01A08 DS1 INTERFACE TN464GP HW02 FW017 u u u u u u u u
	                                                 u u u u u u u u
	                                                 u u u u u u u u
	                                                 u u u u u u u u
	01A10 ANALOG LINE TN793B 000005 01 02 03 04 05 06 07 08
	                                                 09 10 11 12 13 14 15 16
	                                                 17 18 19 20 21 22 23 24</pre>

Step	Description
2.	Enter the **add ds1 xxxxx** command, where xxxxx is the board number of a DS1 circuit pack noted in Step 1. On Page 1 of the **ds1** form, enter a meaningful/description for **Name**, and set **Line Coding** to "**b8zs**" and **Framing Mode** to "**esf**". Ensure that the line coding and framing mode are consistent with the corresponding settings on the other end of the T1 line.

For a T1 ISDN-PRI line, configure the following:
- **Signaling Mode** – set to "**isdn-pri**".
- **Connect** – ensure that this setting is complementary to the corresponding setting on the other end of the T1 line.

```
add ds1 01A07                                                   Page   1 of   2
                              DS1 CIRCUIT PACK

            Location: 01A07                             Name: T1 PRI to G3r1
            Bit Rate: 1.544                      Line Coding: b8zs
    Line Compensation: 1                         Framing Mode: esf
        Signaling Mode: isdn-pri
              Connect: network
    TN-C7 Long Timers? n                      Country Protocol: 1
Interworking Message: PROGress                Protocol Version: a
Interface Companding: mulaw                               CRC? n
            Idle Code: 11111111
                               DCP/Analog Bearer Capability: 3.1kHz


                                         T303 Timer(sec): 4



      Slip Detection? n                     Near-end CSU Type: other
```

For a T1 E&M line, configure the following:
- **Signaling Mode** – set to "**robbed-bit**".

```
add ds1 1a08                                                   Page   1 of   2
                              DS1 CIRCUIT PACK

            Location: 01A08                             Name: T1 E&M to G3r1
            Bit Rate: 1.544                      Line Coding: b8zs
    Line Compensation: 1                         Framing Mode: esf
        Signaling Mode: robbed-bit




Interface Companding: mulaw
            Idle Code: 11111111







      Slip Detection? n                     Near-end CSU Type: other
```

3.2. IP Codec Sets and IP Network Regions

Step	Description
1.	Enter the **change ip-codec-set g** command, where "g" is a number between 1 and 7, inclusive, and enter one or more codecs for the IP codec set. IP codec sets may be selected in the IP Network Region forms to define which codecs may be used within and between IP network regions. In the examples below, IP codec set 1 contains "**G.711MU**", while IP codec set 2 contains "**G.729**" and "**G.711MU**".

```
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:
 3:
 4:
 5:
 6:
 7:
```

```
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: G.711MU           n           2          20
 3:
 4:
 5:
 6:
 7:
```

Step	Description
2.	Enter the **change ip-network-region h** command, where "h" is a number between 1 and 250, inclusive. On Page 1 of the **ip-network-region** form, set **Codec Set** to the number of a configured IP codec set. In the example below, the codecs defined in IP codec set 1 may be used for IP calls within IP network region 1.

```
change ip-network-region 1                                     Page   1 of  19
                            IP NETWORK REGION
  Region: 1
Location:           Authoritative Domain: 192.45.51.155
    Name:
                                   Intra-region IP-IP Direct Audio: yes
MEDIA 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
DIFFSERV/TOS PARAMETERS            RTCP MONITOR SERVER PARAMETERS
 Call Control PHB Value: 46         Use Default Server Parameters? y
        Audio PHB Value: 46
        Video PHB Value: 26
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 **ip-network-region** form, specify the IP **codec set** for every pair of source and destination IP network regions. In the example below, IP connections between IP network regions 1 and 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   IGAR
 1   1     1
 1   2     2      y            :NoLimit                                  n
 1   3
 1   4
 1   5
 1   6
 1   7
 1   8
 1   9
 1   10
```

3.3. Trunks and Signaling Groups

3.3.1. T1 ISDN-PRI

The steps in this section create a trunk group that will contain trunks (channels) from a T1 ISDN-PRI line.

Step	Description

1.	Enter the **add trunk-group i** command, where "i" 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.
	• **TAC** – enter a Trunk Access Code that is valid under the provisioned dial plan.
	• **Carrier Medium** – set to "**PRI/BRI**".
	• **Service Type** – was set to "**tie**" for compliance testing, but for trunks connected directly to the public network, the administrator may want to set to "public-ntwrk".
	
	<pre>add trunk-group 6 Page 1 of 19
	                              TRUNK GROUP
	
	Group Number: 6 Group Type: isdn CDR Reports: y
	  Group Name: T1 ISDN-PRI trunks COR: 1 TN: 1 TAC: 106
	    Direction: two-way Outgoing Display? n Carrier Medium: PRI/BRI
	 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: 13
	Incoming Calling Number - Delete: Insert: Format:
	             Bit Rate: 1200 Synchronization: async Duplex: full
	 Disconnect Supervision - In? y Out? n
	 Answer Supervision Timeout: 0</pre>

Step	Description
2.	Enter the **add signaling group j** command, where "j" is an available signaling group number. On Page 1 of the **signaling-group** form, configure the following: • **Group Type** – set to "**isdn-pri**". • **Associated Signaling** – set to "**y**". • **Primary D-Channel** – enter xxxxx24, where xxxxx is the board number of the DS1 circuit pack configured for T1 ISDN-PRI (24 is the D-Channel in a T1 ISDN-PRI). • **Trunk Group for Channel Selection** – enter the number of the trunk group configured in Step 1.

```
add signaling-group 6                                          Page   1 of   5
                              SIGNALING GROUP

 Group Number: 6                        Group Type: isdn-pri
                     Associated Signaling? y          Max number of NCA TSC: 0
                       Primary D-Channel: 01A0724      Max number of CA TSC: 0
                                                    Trunk Group for NCA TSC:
          Trunk Group for Channel Selection: 6
              Supplementary Service Protocol: a
```

Step	Description
3.	Enter the **change trunk-group i** command, where "i" is the number of the trunk group configured in Step 1. On Page 3 of the **trunk-group** form, add trunk members by entering: • **xxxxxzz** for **Port**, where xxxxx is the board number of the DS1 circuit pack configured for T1 ISDN-PRI, and zz is a channel in the T1 ISDN-PRI, and • the number of the signaling group associated with the trunk member (port) for **Sig Grp**. Ensure that the trunk member assignments match the assignments on the other end of the T1 line.

```
change trunk-group 6                                          Page   3 of  19
                              TRUNK GROUP
                                    Administered Members (min/max):   0/0
 GROUP MEMBER ASSIGNMENTS               Total Administered Members:   0

        Port   Code Sfx Name          Night            Sig Grp
  1: 01A0701  TN464  G                                    6
  2: 01A0702  TN464  G                                    6
  3: 01A0703  TN464  G                                    6
  4: 01A0704  TN464  G                                    6
  5: 01A0705  TN464  G                                    6
  6: 01A0706  TN464  G                                    6
  7: 01A0707  TN464  G                                    6
  8: 01A0708  TN464  G                                    6
  9: 01A0709  TN464  G                                    6
 10: 01A0710  TN464  G                                    6
 11: 01A0711  TN464  G                                    6
 12: 01A0712  TN464  G                                    6
 13: 01A0713  TN464  G                                    6
 14: 01A0714  TN464  G                                    6
 15: 01A0715  TN464  G                                    6
```

3.3.2. T1 E&M

The steps in this section create a trunk group that contains trunks (channels) from a T1 E&M line.

Step	Description
3.	Enter the **add trunk-group m** command, where "m" is an available trunk group number. On Page 1 of the **trunk-group** form, configure the following: • **Group Type** – set to "**tie**". • **Group Name** – enter a meaningful name/description. • **TAC** – enter a Trunk Access Code that is valid under the provisioned dial plan. • **Comm Type** – set to "**voice**". • **Trunk Type (in/out)** – set to "**wink/wink**". • **Outgoing Dial Type** and **Incoming Dial Type** – set to "**tone**". The **Trunk Type (in/out)**, **Outgoing Dial Type** and **Incoming Dial Type** must match the corresponding settings on the other end of the T1 line.

```
add trunk-group 8                                              Page   1 of  20
                               TRUNK GROUP

Group Number: 8                       Group Type: tie          CDR Reports: y
  Group Name: T1 E&M Trunks                 COR: 1       TN: 1         TAC: 108
   Direction: two-way         Outgoing Display? n Trunk Signaling Type:
 Dial Access? y                    Busy Threshold: 255      Night Service:
Queue Length: 0                                        Incoming Destination:
   Comm Type: voice                       Auth Code? n
                                        Trunk Flash? n


TRUNK PARAMETERS
   Trunk Type (in/out): wink/wink          Incoming Rotary Timeout(sec): 5
    Outgoing Dial Type: tone                    Incoming Dial Type: tone
      Wink Timer(msec): 300                Disconnect Timing(msec): 500
       Digit Treatment:                                      Digits:
                                              Sig Bit Inversion: none
       Analog Loss Group: 9                  Digital Loss Group: 13
      Incoming Dial Tone? y

 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 0          Receive Answer Supervision? y
```

Step	Description
4.	On Page 4 of the **trunk-group** form, add one or more trunk members by entering **xxxxxzz** for **Port**, where xxxxx is the board number of the DS1 circuit pack configured for T1 E&M, and zz is a channel in the T1 E&M. Ensure that the trunk member assignments match the assignments on the other end of the T1 line.

```
change trunk-group 8                                             Page   4 of  20
                                  TRUNK GROUP
                                       Administered Members (min/max):   0/0
GROUP MEMBER ASSIGNMENTS                    Total Administered Members:   0

         Port     Code Sfx Name         Night           Mode      Type  Ans Delay
  1: 01A0801   TN464  G
  2: 01A0802   TN464  G
  3: 01A0803   TN464  G
  4: 01A0804   TN464  G
  5: 01A0805   TN464  G
  6: 01A0806   TN464  G
  7: 01A0807   TN464  G
  8: 01A0808   TN464  G
  9: 01A0809   TN464  G
 10: 01A0810   TN464  G
 11: 01A0811   TN464  G
 12: 01A0812   TN464  G
 13: 01A0813   TN464  G
 14: 01A0814   TN464  G
 15: 01A0815   TN464  G
```

3.3.3. H.323

The steps in this section create a trunk group that contains H.323 trunks (channels) to the remote Avaya Communication Manager system (S8300 Media Server in G350 Media Gateway in **Figure 1**).

Step	Description
1.	Enter the **change node-names ip** command. Specify node names and IP addresses for the C-LAN and MedPro boards, as well as the remote Avaya Communication Manager system.

```
change node-names ip                                            Page   1 of   1
                               IP NODE NAMES
    Name              IP Address            Name            IP Address
 CLAN-1A02         192.45 .100.144                        .   .   .
 MEDPRO-1A03       192.45 .100.145                        .   .   .
 Ext-H323-Node1    192.45 .60 .5                          .   .   .
 default           0  .0   .0   .0                        .   .   .
 procr             192.45 .100.141                        .   .   .
```

Step	Description
2.	For the C-LAN and MedPro boards, enter the command **add ip-interface xxxxx**, where xxxxx is a board number. In the **add ip-interface** form, specify the **Node Name** (from Step 1), **Subnet Mask**, and **Gateway Address**, set **Enable Ethernet Port** to **y**, and set **Network Region** to the IP network region configured in Section 3.2 Step 2. The board numbers of the C-LAN and MedPro boards can be obtained from the **list configuration all** form.

```
add ip-interface 1a02                                        Page   1 of   1
                             IP INTERFACES


                    Type: C-LAN
                    Slot: 01A02
             Code/Suffix: TN799  D
               Node Name: CLAN-1A02
              IP Address: 192.45 .100.144
             Subnet Mask: 255.255.255.0
         Gateway Address: 192.45 .100.1
     Enable Ethernet Port? y
          Network Region: 1
                    VLAN: n

Number of CLAN Sockets Before Warning: 400

                             ETHERNET OPTIONS
                    Auto? y
```

```
add ip-interface 1a03                                        Page   1 of   1
                             IP INTERFACES


                    Type: MEDPRO
                    Slot: 01A03
             Code/Suffix: TN2302
               Node Name: MEDPRO-1A03
              IP Address: 192.45 .100.145
             Subnet Mask: 255.255.255.0
         Gateway Address: 192.45 .100.1
     Enable Ethernet Port? y
          Network Region: 1
                    VLAN: n




                             ETHERNET OPTIONS
                    Auto? y
```

Step	Description
3.	For each C-LAN board, enter the command **add data-module nnnn**, where **nnnn** is an extension whose length and value depends on the provisioned dial plan. In the add data-module form, set **Type** to **ethernet**, **Port** to the C-LAN board number appended with "**17**", and **Link** to a number between 1 and 99.

```
add data-module 2999                                          Page   1 of   1
                              DATA MODULE


  Data Extension: 2999              Name: clan-1a02
            Type: ethernet
            Port: 01A0217
            Link: 1




Network uses 1's for Broadcast Addresses? y
```

Step	Description
4.	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. • **TAC** – enter a Trunk Access Code that is valid under the provisioned dial plan. • **Carrier Medium** – set to "**IP**". • **Service Type** – set to "**tie**".

```
add trunk-group 31                                            Page   1 of  19
                              TRUNK GROUP


Group Number: 31                    Group Type: isdn       CDR Reports: y
  Group Name: Trunks to External H.323    COR: 1     TN: 1        TAC: 131
   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: 13
Incoming Calling Number - Delete:     Insert:                   Format:
            Bit Rate: 1200         Synchronization: async     Duplex: full
 Disconnect Supervision - In? y  Out? n
 Answer Supervision Timeout: 0
```

Step	Description
5.	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 "**h323**". • **Trunk Group for Channel Selection** – enter the number of the trunk group configured in Step 4. • **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 the remote H.323 system configured in Step 1. • **Far-end Listen Port** – specify the remote listen port, typically 1720. • **Far-end Network Region** – (optional) associate the remote H.323 system with a network region. • **Calls Share IP Signaling Connection** – set to "**n**" if the remote H.323 system is not an Avaya Communication Manager system or if ETM termination of H.323 calls is to be allowed.

```
change signaling-group 31                                        Page   1 of   5
                            SIGNALING GROUP

 Group Number: 31                  Group Type: h.323
                               Remote Office? n          Max number of NCA TSC: 0
                                        SBS? n           Max number of CA TSC: 0
                                   IP Video? n        Trunk Group for NCA TSC:
        Trunk Group for Channel Selection: 31
            Supplementary Service Protocol: a
                          T303 Timer(sec): 10


   Near-end Node Name: CLAN-1A02               Far-end Node Name: Ext-H323-Node1
  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
                                                 H.235 Annex H Required? n
          DTMF over IP: out-of-band          Direct IP-IP Audio Connections? y
                                                     IP Audio Hairpinning? y
                                             Interworking Message: PROGress
                                         DCP/Analog Bearer Capability: 3.1kHz
```

Step	Description
6.	Enter the **change trunk-group p** command, where "p" is the number of the trunk group configured in Step 4. On Page 3 of the **trunk-group** form, add one or more trunk members by entering: • "**IP**" for **Port**, and • the number of the signaling group configured in Step 5 for **Sig Grp**. Ensure that the number of trunk members match the other end of the H.323 trunk.

```
change trunk-group 31                                           Page   3 of  19
                              TRUNK GROUP
                                     Administered Members (min/max):    0/0
GROUP MEMBER ASSIGNMENTS                     Total Administered Members:    0

         Port    Code Sfx Name          Night            Sig Grp
  1: IP                                                    31
  2: IP                                                    31
  3: IP                                                    31
  4: IP                                                    31
  5: IP                                                    31
  6: IP                                                    31
  7: IP                                                    31
  8: IP                                                    31
  9: IP                                                    31
 10: IP                                                    31
 11: IP                                                    31
 12: IP                                                    31
 13: IP                                                    31
 14: IP                                                    31
 15: IP                                                    31
```

4. Configure SecureLogix ETM 1090

This section describes the steps for configuring the ETM 1090.
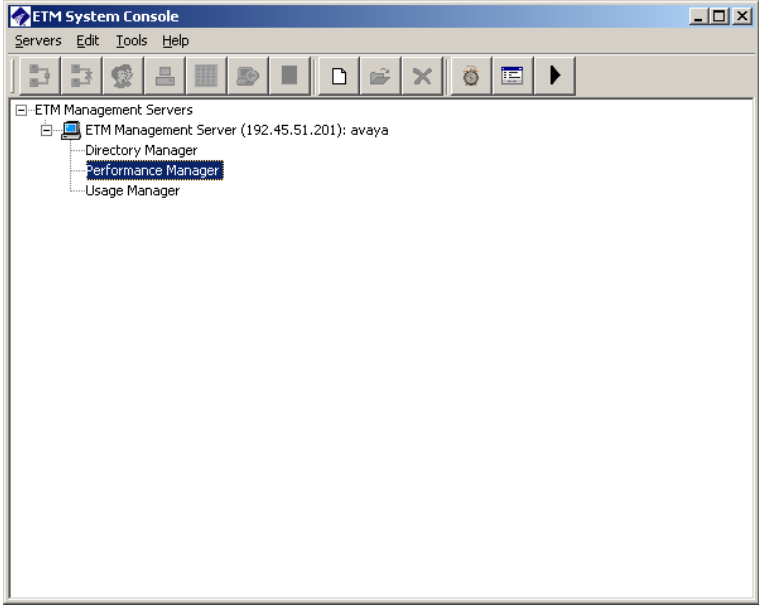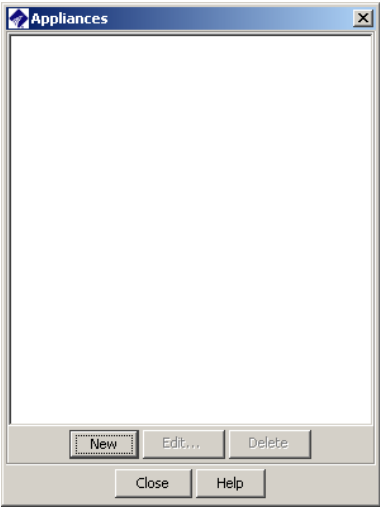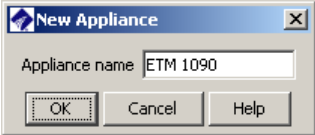
4.1. Pre-Configuration
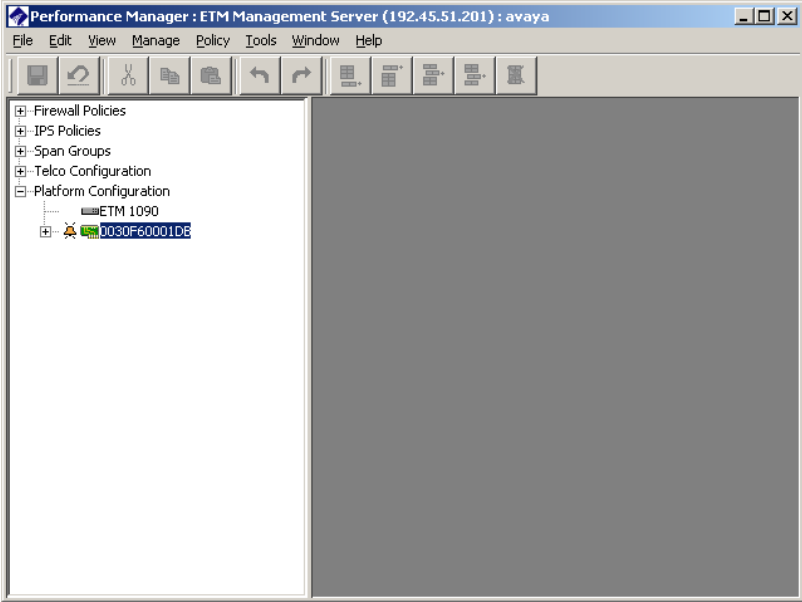
The steps in this section configure the T1 port on the ETM 1090 as an ISDN-PRI or CAS (E&M or robbed bit) interface, and place the T1 and H.323 VoIP ports in maintenance mode.
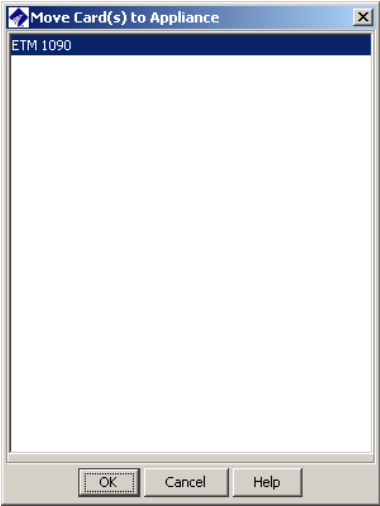
Step	Description
1.	Connect a PC to the ETM 1090 appliance console port and start a terminal session with the following settings: Bits per second: 115200 Data bits: 8 Parity: None Stop bits: 1 Flow control: None
2.	When prompted, log in with the proper credentials. Enter the command "**enable**" and provide the password to enter enabled mode.
3.	Enter the command "**RESTART FAILSAFE**".
4.	Select the option "**1 - Enter Fail Safe ETM Shell**" from the **Fail Safe Mode Menu**.
5.	Enter the command "**MAINT SPAN TYPE m PRI**" or "**MAINT SPAN TYPE m CAS**", where m is the T1 span number. Enter the command "**MAINT SPAN TYPE n VOIP**", where n is the VoIP span number.
6.	Enter the command "**REBOOT NOW**".
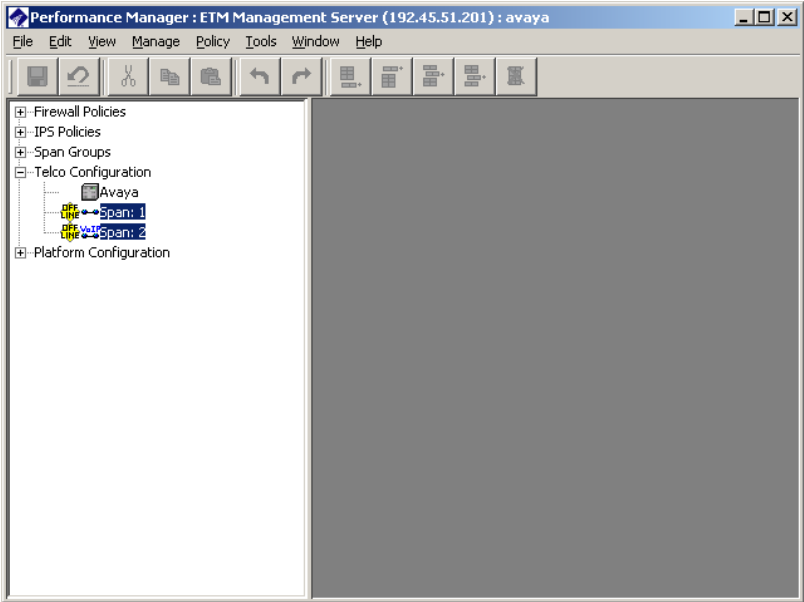
4.2. System Configuration
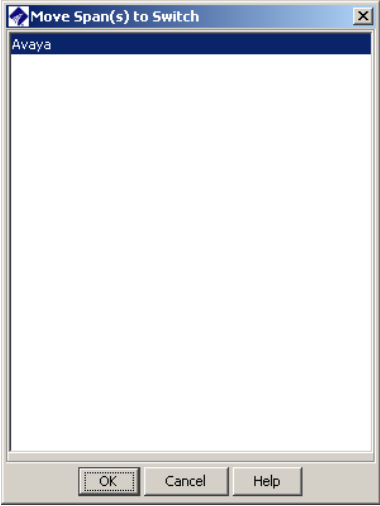
Step	Description
1.	Launch the ETM System Console application on the ETM System Console PC. Right-click on an ETM Management Server and select "**Connect**". Log in with the appropriate credentials.
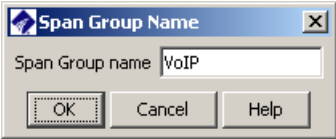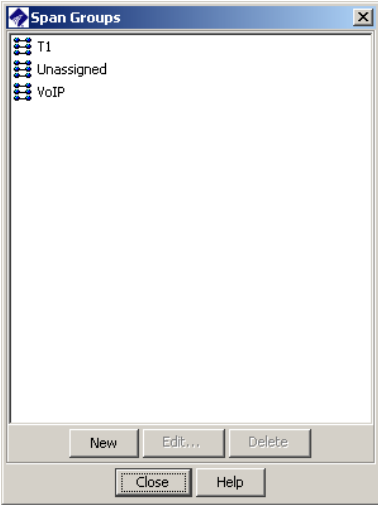
Step	Description
2.	In the ETM System Console, double-click on "**Performance Manager**".
3.	In the Performance Manager main window, select "**Appliance**" from the "**Manage**" menu.
4.	Click on "**New**" in the **Appliances** window.
5.	Enter a descriptive **Appliance name** and click on "**OK**".
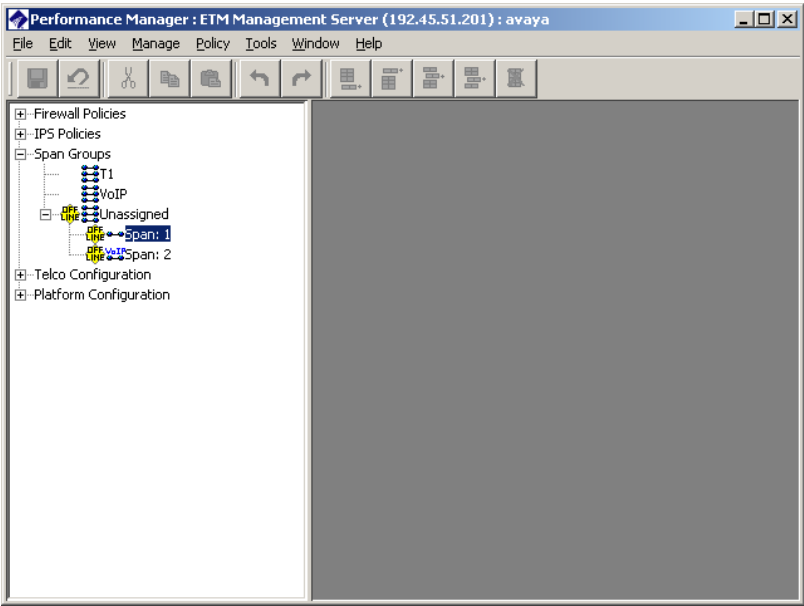
Step	Description
6.	Click on "**Close**" in the **Appliances** window.
7.	In the Performance Manager main window, expand the **Platform Configuration** tree. Select a card (the ETM 1090 has one card, other ETM Platform appliances may have multiple cards), right-click, and select "**Move Card**".

RL; Reviewed:
SPOC 12/15/2005

Solution & Interoperability Test Lab Application Notes
©2005 Avaya Inc. All Rights Reserved.

19 of 49
SecureLogixETM.doc

Step	Description
8.	Select the appliance configured in Steps 3 – 6, and click on "**OK**".
9.	In the Performance Manager main window, select "**Switches**" from the **Manage** menu.
10.	Click on "**New**" in the **Switches** window.
11.	Enter a descriptive **Switch name** and click on "**OK**".
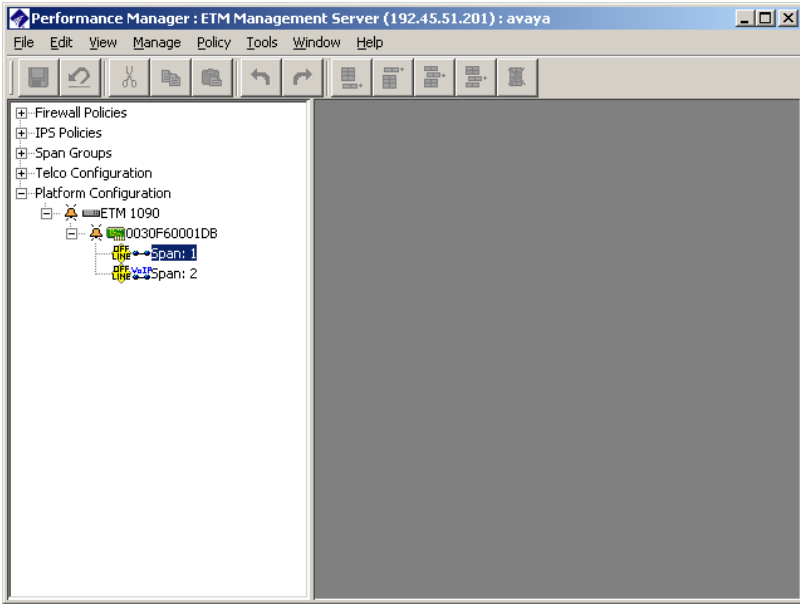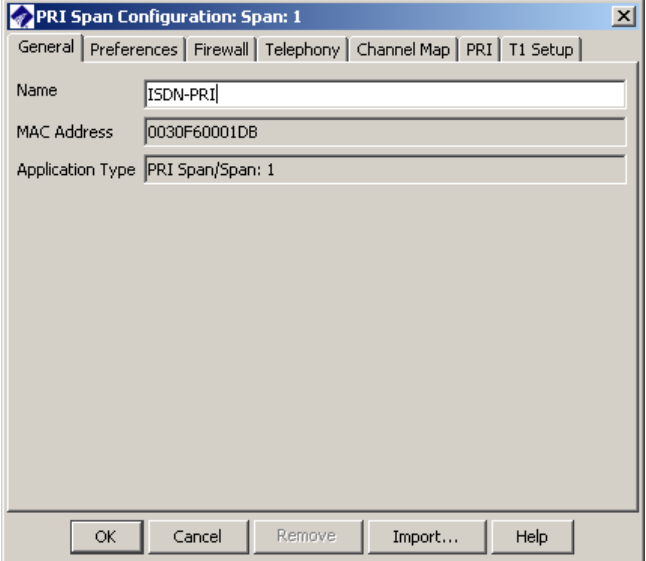
Step	Description
12.	Click on "**Close**" in the **Switches** window.
13.	In the Performance Manager main window, expand the **Telco Configuration** tree. Select one or more spans, right-click, and select "**Move Span(s)->To Switch**".
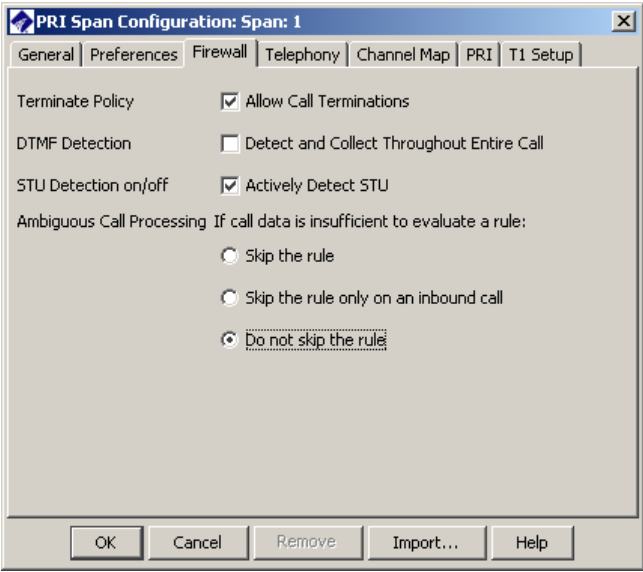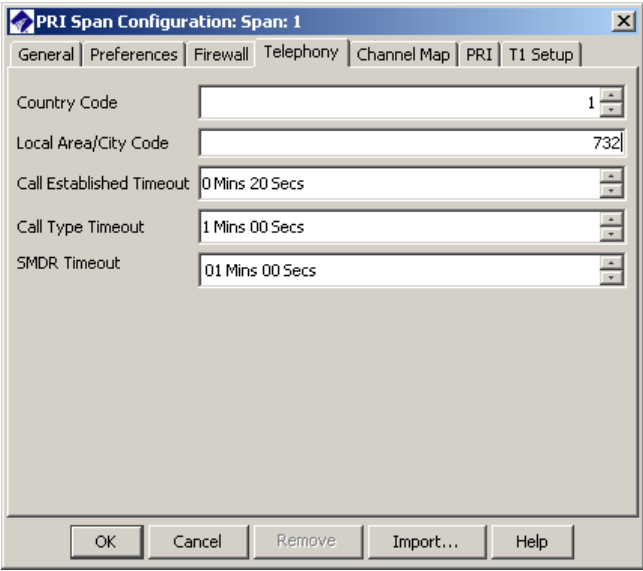
Step	Description
14.	Select the switch configured in Steps 9 – 12, and click on "**OK**".
15.	In the Performance Manager main window, select "**Span Groups**" from the **Manage** menu.
16.	Click on "**New**" in the **Span Groups** window.

Step	Description
17.	Enter a descriptive **Span Group name** and click on "**OK**".
18.	Click on "**Close**" in the **Span Groups** window.

RL; Reviewed:
SPOC 12/15/2005

Solution & Interoperability Test Lab Application Notes
©2005 Avaya Inc. All Rights Reserved.

23 of 49
SecureLogixETM.doc

Step	Description
19.	In the Performance Manager main window, expand the **Span Groups** tree. In the **Unassigned** sub-tree, right-click on a span, and select "**Move Span(s)**". On the ETM 1090, Span 1 is a T1 span and Span 2 is a VoIP span.
20.	Select an appropriate span group and click on "**OK**".
21.	Repeat Steps 19 – 20 for the remaining unassigned spans.

4.3. T1 ISDN-PRI Span Configuration
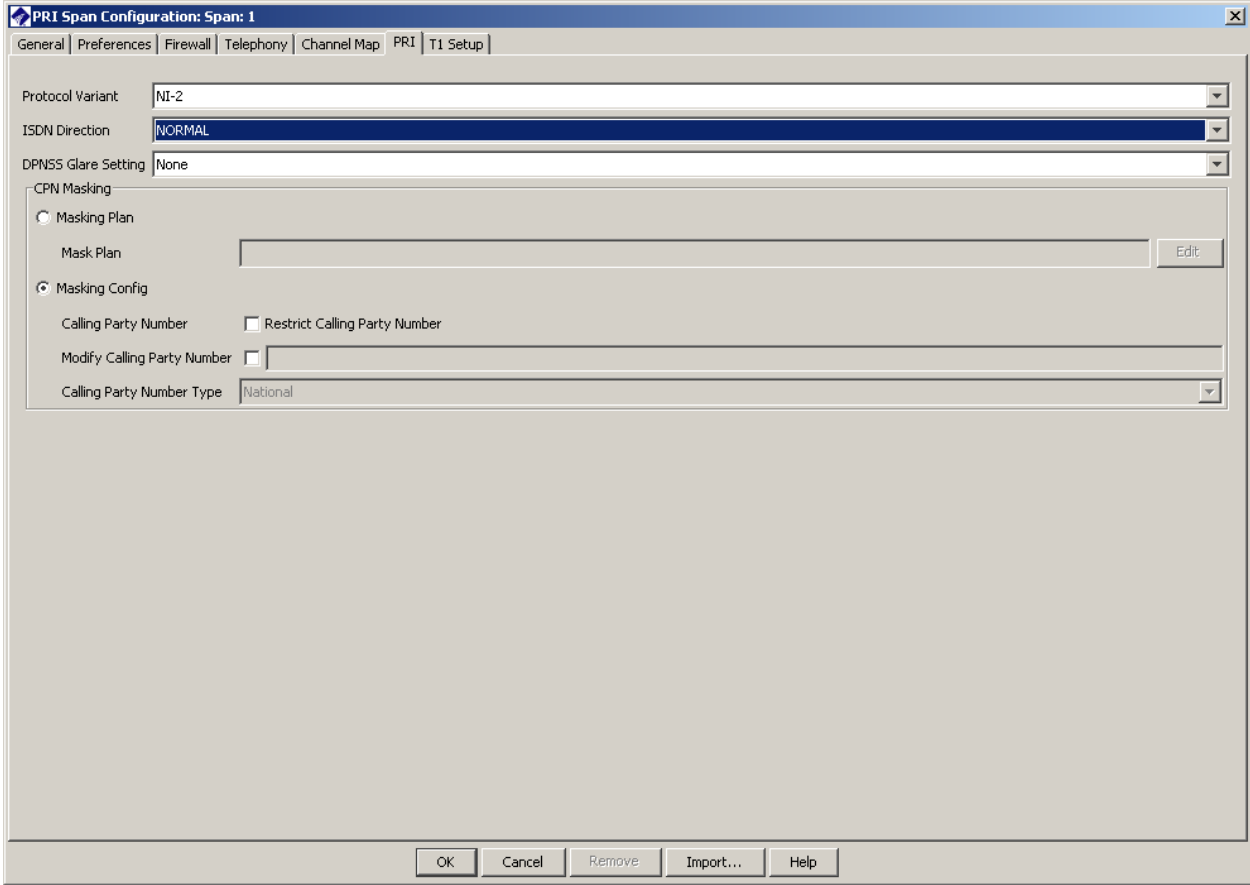
Step	Description
1.	In the Performance Manager main window, expand the **Platform Configuration** tree to the Span level. Right-click on the T1 span and select "**Edit Span(s)**".
2.	In the **General** tab, enter a descriptive **Name**.
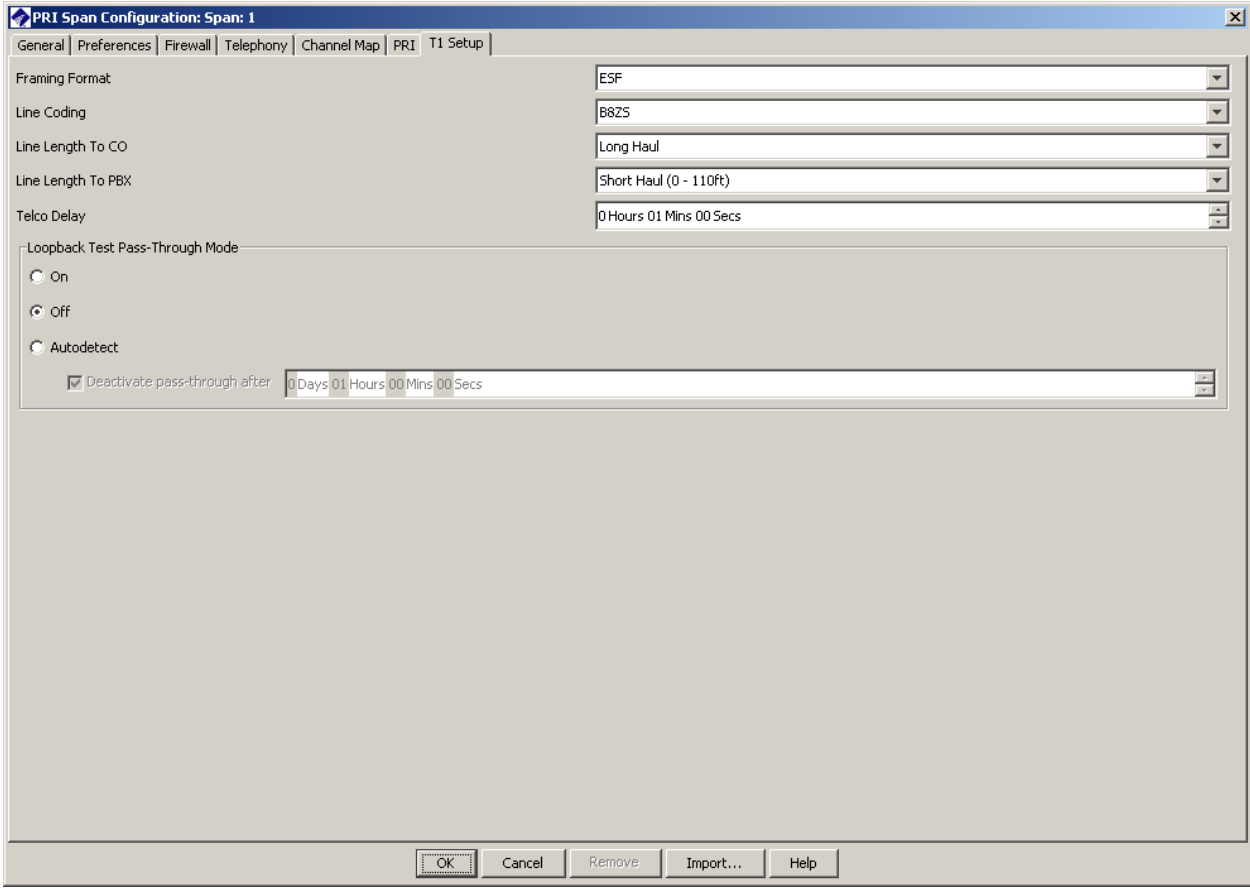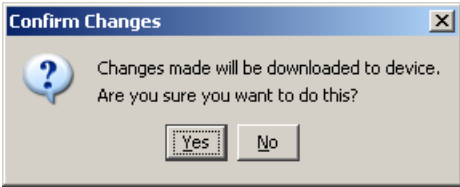
Step	Description
3.	Click on the **Firewall** tab. Check the **Allow Call Terminations** checkbox if the call termination by the ETM System is to be allowed.
4.	Click on the **Telephony** tab. Enter the **Local Area/City Code**.
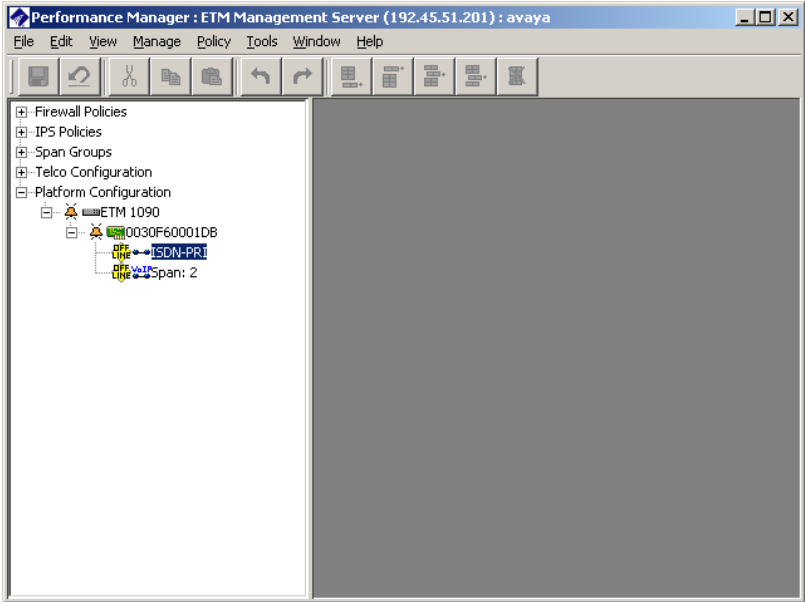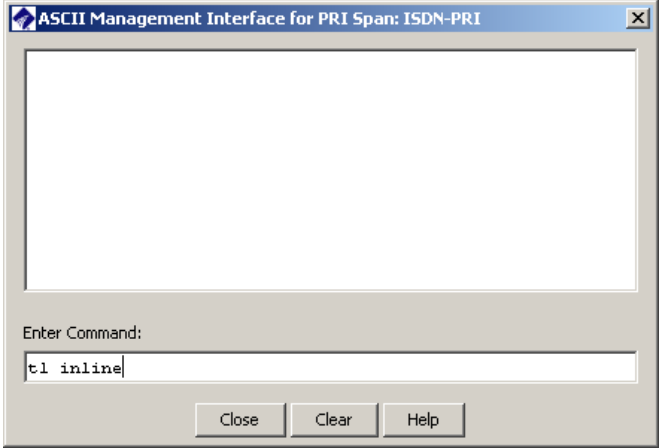
Step	Description
5.	Click on the **Channel Map** tab. Set **Incoming Numbering Format** and **Format Precedence** to "**DID**" for all channels if the span receives inbound DID calls from the network*. * The Dialing Plan file in the ETM System must be configured with the DID numbers/ranges. Consult SecureLogix for guidance.

Step	Description
6.	Click on the **PRI** tab. Set **Protocol Variant** to "**NI-2**" and **ISDN Direction** to "**NORMAL**".

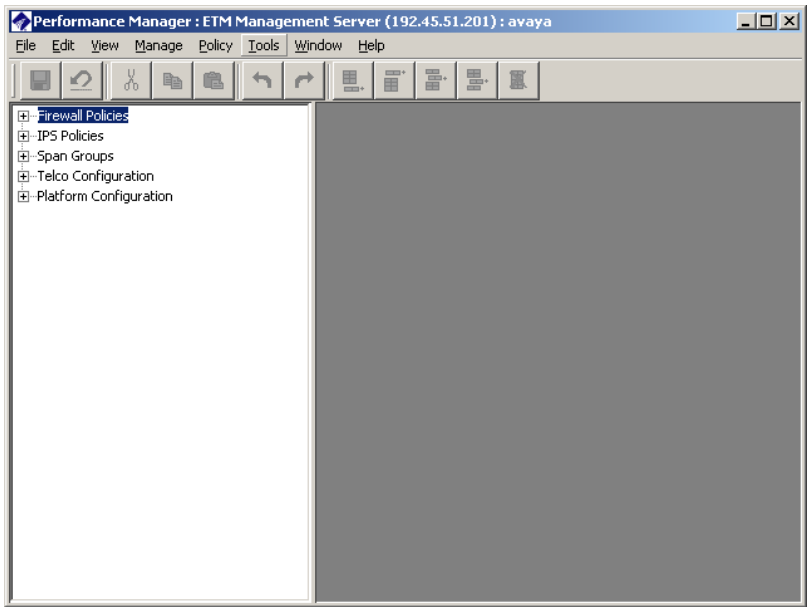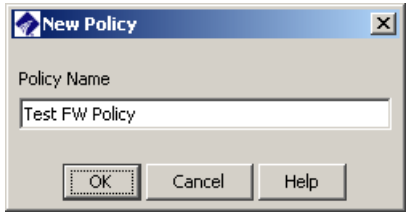| Step	Description
7.	Click on the **T1 Setup** tab. Set **Framing Format** and **Line Coding** to match settings on Avaya Communication Manager in Section 3.1 Step 2. Click on "**OK**".
8.	Click on "**Yes**" to confirm and download the changes.
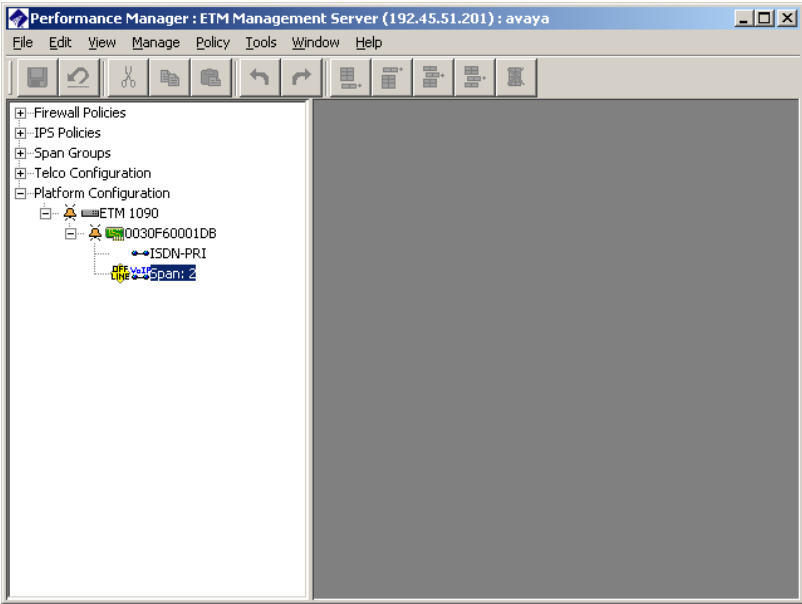
Step	Description
9.	In the Performance Manager main window, expand the **Platform Configuration** tree to the Span level. Right-click on the T1 span and select "**ASCII Management**".
10.	Enter the command "**t1 inline**" and press Enter.
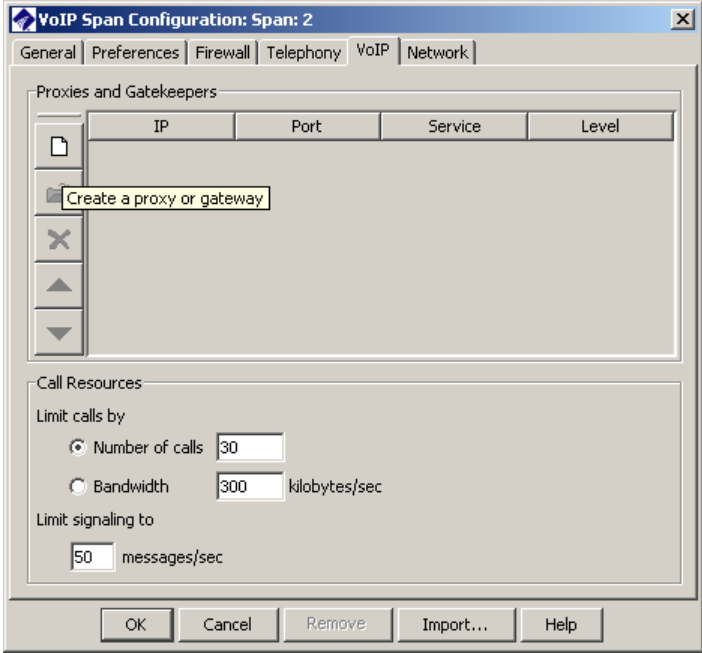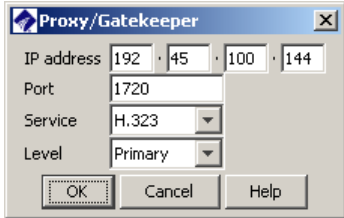
Step	Description
11.	Enter the command "**restart**" and press Enter.

ASCII Management Interface for PRI Span: ISDN-PRI

```
t1 inline
Please RESTART the span to place the T1/E1 inline
```

Enter Command:

```
restart
```

Close   Clear   Help
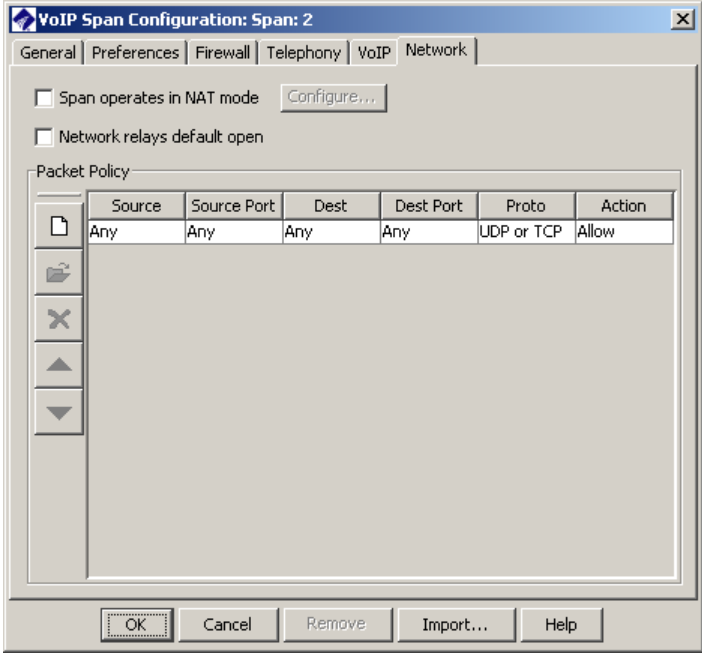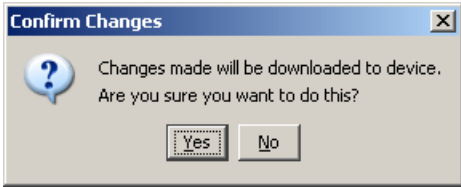
4.4. T1 CAS Span Configuration
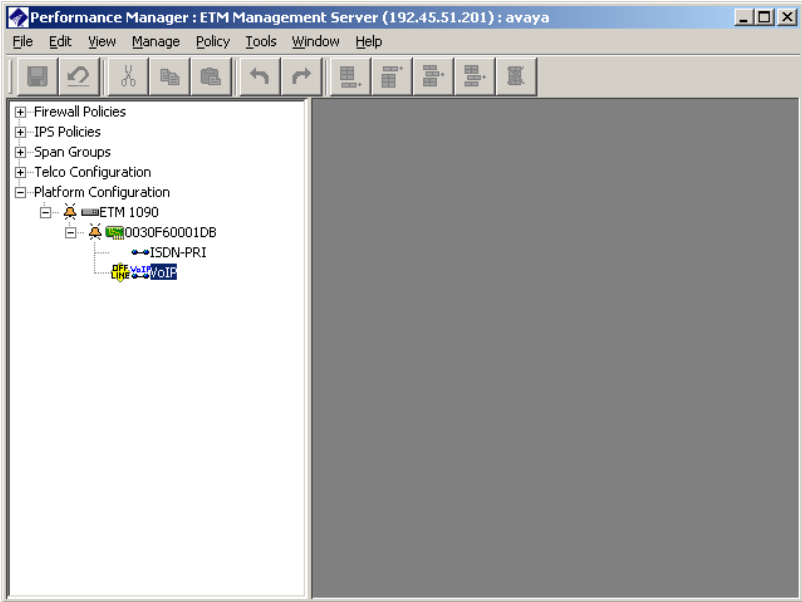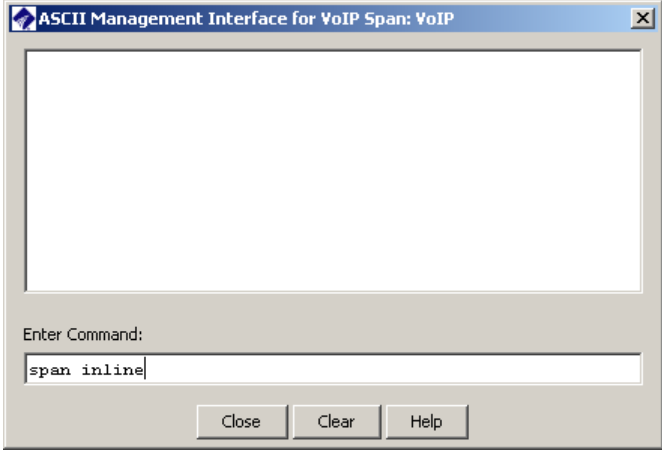
Step	Description
1.	Repeat Steps 1 – 4 of Section 4.3.
2.	Click on the **Channel Map** tab. Set **Incoming Numbering Format** and **Format Precedence** to "**DID**" for all channels if the span receives inbound DID calls from the network*. For all channels, set **Signal Type** to "**Wink**" and **Tone Type** to "**DTMF**" to match the trunk settings in Avaya Communication Manager (see Section 3.3.2). * The Dialing Plan file in the ETM System must be configured with the DID numbers/ranges. Consult SecureLogix for guidance.
3.	Repeat Steps 7 – 11 of Section 4.3.

4.5. H.323 VoIP Span Configuration

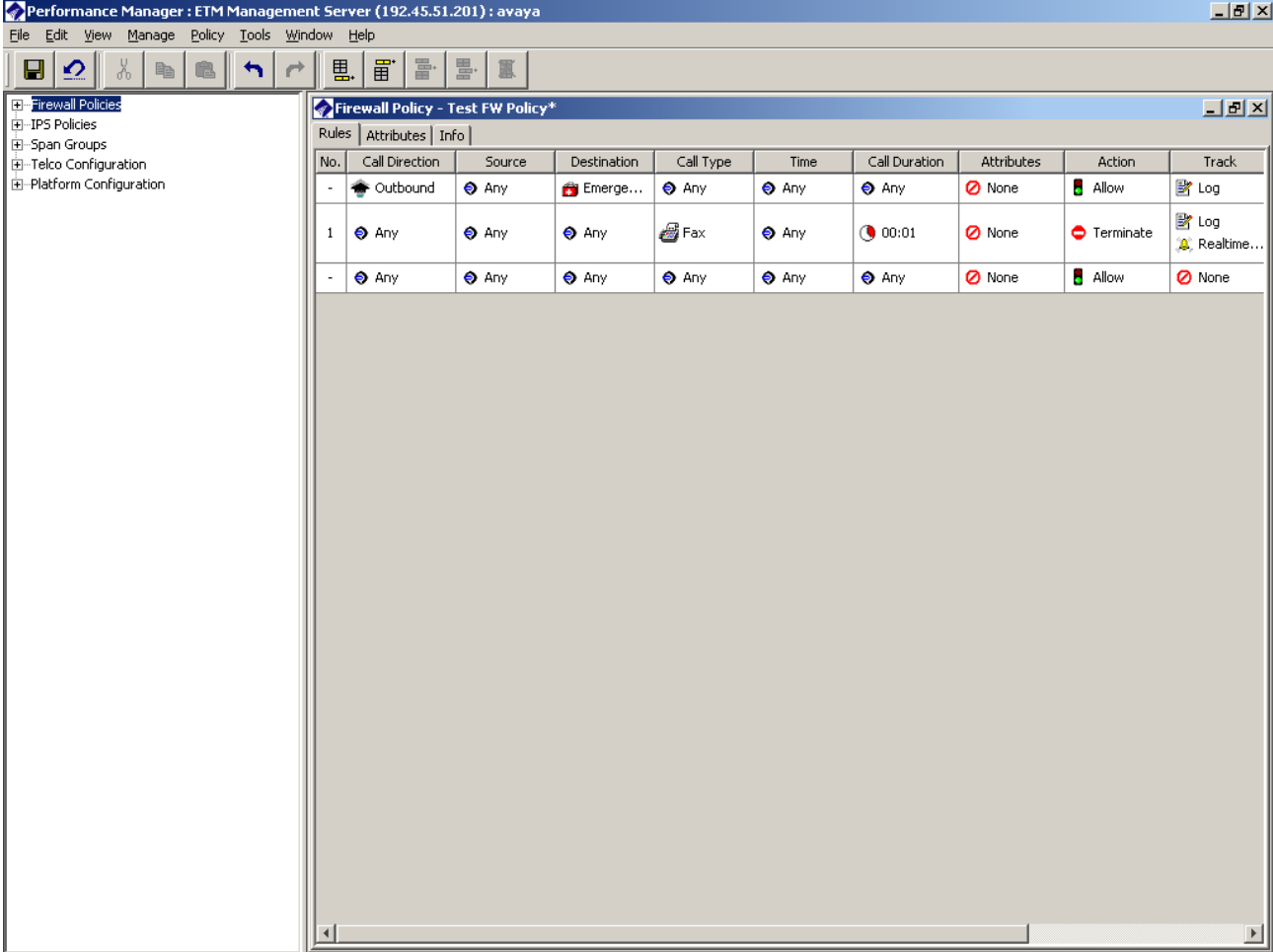| Step	Description
1.	In the Performance Manager main window, expand the **Platform Configuration** tree to the Span level. Right-click on an H.323 VoIP span and select "**Edit Span(s)**".
2.	Repeat Steps 2 – 4 of Section 4.3.
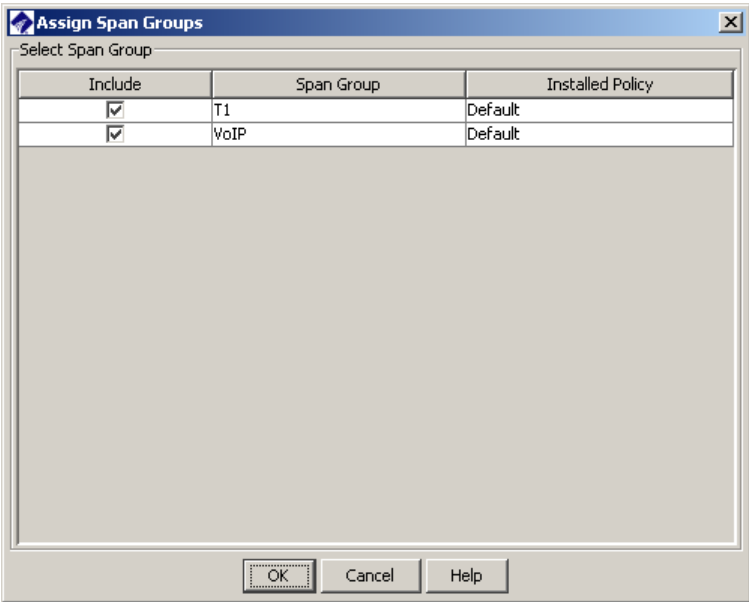
Step	Description
3.	Click on the **VoIP** tab. Click on the "**Create a proxy or gateway**" icon.
4.	Enter the IP address and near-end listen port (see Section 3.3.3 Step 5) of the C-LAN board for **IP address** and **Port**, respectively, and set **Service** to "**H.323**". Click on "**OK**".

Solution & Interoperability Test Lab Application Notes
©2005 Avaya Inc. All Rights Reserved.

Step	Description
5.	Click on the **Network** tab. Uncheck the **Network relays default open** checkbox. VoIP Span Configuration: Span: 2 General | Preferences | Firewall | Telephony | VoIP | Network ☐ Span operates in NAT mode Configure... ☐ Network relays default open Packet Policy |	Source	Source Port	Dest	Dest Port	Proto	Action
---	---	---	---	---	---	---
	Any	Any	Any	Any	UDP or TCP	Allow	 OK Cancel Remove Import... Help
6.	Click on "**Yes**" to confirm and download the changes. Confirm Changes Changes made will be downloaded to device. Are you sure you want to do this? Yes No

RL; Reviewed:
SPOC 12/15/2005

Solution & Interoperability Test Lab Application Notes
©2005 Avaya Inc. All Rights Reserved.

35 of 49
SecureLogixETM.doc

Step	Description
7.	In the Performance Manager main window, expand the **Platform Configuration** tree to the Span level. Right-click on the VoIP span and select "**ASCII Management**".
8.	Enter the command "**span inline**" and press Enter.
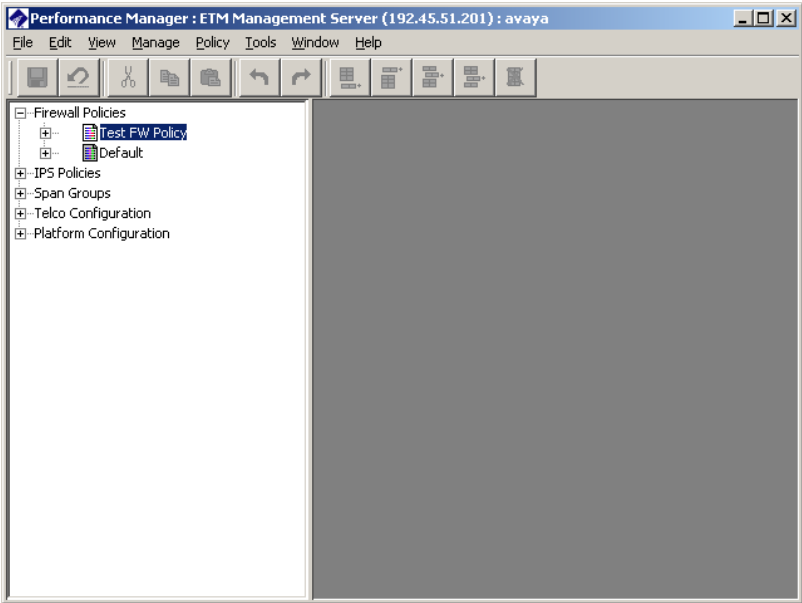
4.6. Voice Firewall Policy

Step	Description
1.	In the Performance Manager main window, right-click on **Firewall Policies** and select "**New**".
2.	Enter a descriptive **Policy Name** and click on "**OK**".

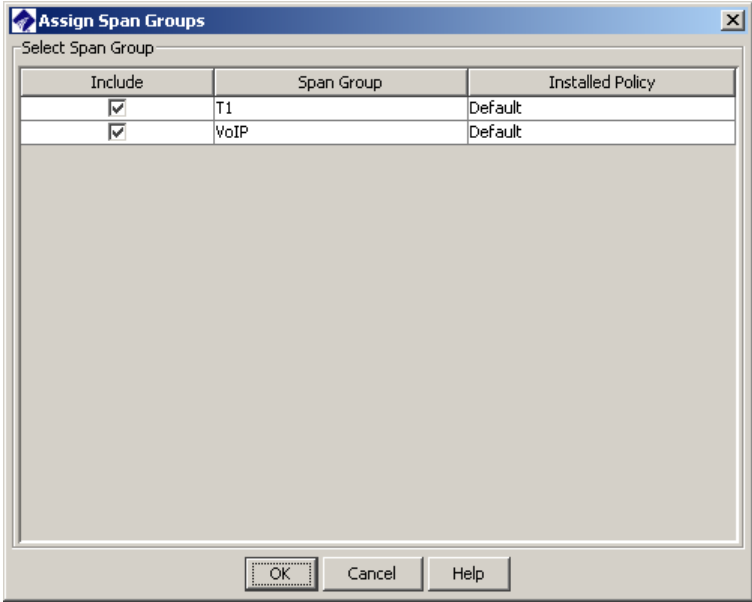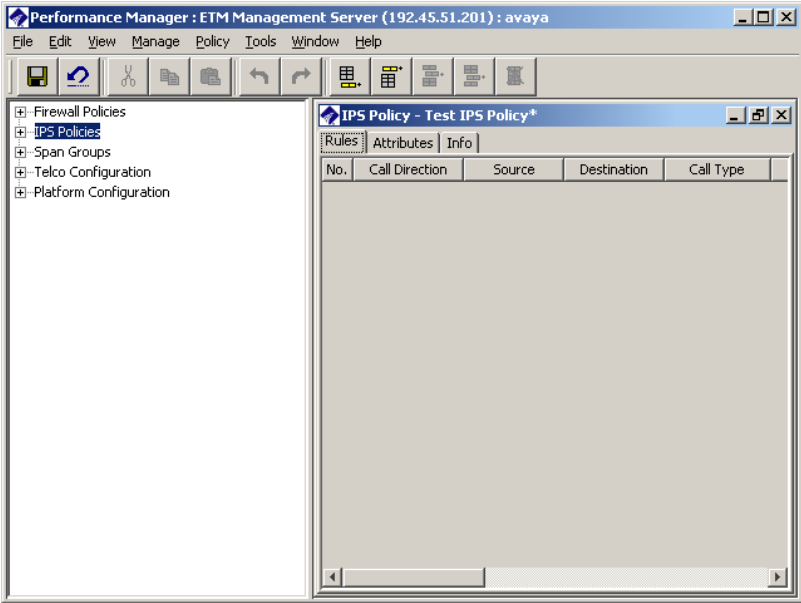| Step	Description
3.	Assign the new Voice Firewall policy to one or more span groups by checking the corresponding checkboxes and click on "**OK**".

Step	Description
4.	The new Voice Firewall policy appears in the right pane of the Performance Manager main window. Select "**Implied Rules**" from the **View** menu to view the default rules. The default rules cannot be deleted. The first default rule is always checked first and the other default rule is always checked last.

Right-click in the **Firewall Policy** sub-window and select "**Add Rule**".

Step	Description
5.	Configure a rule according to **Call Direction**, **Source**, **Destination**, **Call Type**, **Time**, **Call Duration**, and **Attributes**. When the rule is triggered, the **Action** taken may be "**Allow**" or "**Terminate**". The example rule No. 1 below terminates inbound FAX calls that are longer than one minute in duration, and logs and sends real-time alerts whenever the rule is breached. Repeat as necessary to add additional rules. Note that the order of the firewall rules matters. In other words, the firewall rules are checked in order from top to bottom until a rule is matched, and no further checking is performed once a rule is matched.
6.	After finishing adding rules, click on the "**Save**" icon or select "**Save**" from the **File** menu. If the policy is not saved, there is an asterisk next to the policy name.
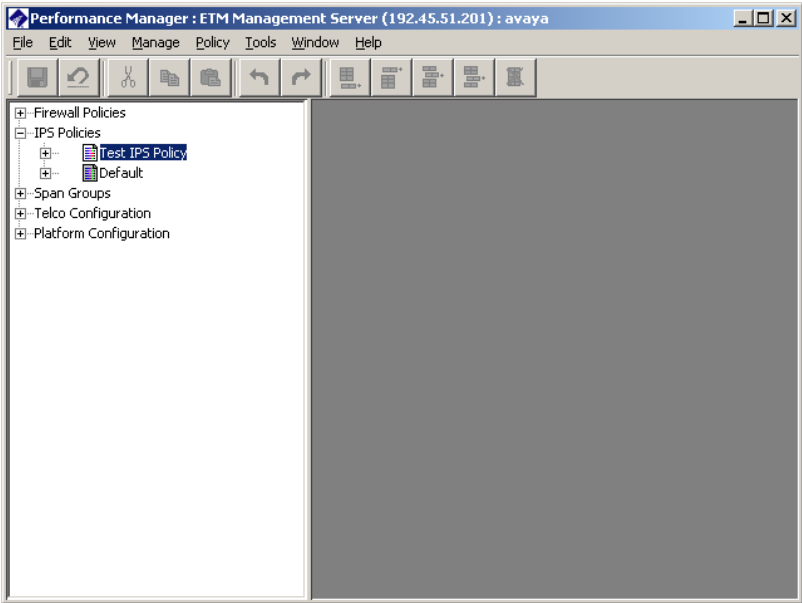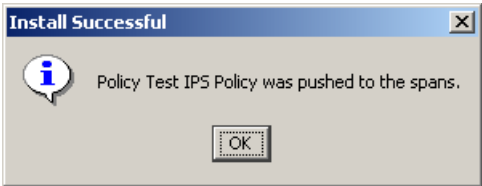
Step	Description
7.	In the Performance Manager main window, expand the **Firewall Policies** tree. Right-click on the Voice Firewall policy created in Steps 1 – 6 and select "**Install**".
8.	Click on "**OK**".

4.7. Voice Intrusion Protection System (IPS) Policy

Step	Description
1.	In the Performance Manager main window, right-click on **IPS Policies** and select "**New**".
2.	Enter a descriptive **Policy Name** and click on "**OK**".

Step	Description
3.	Assign the new Voice IPS policy to one or more span groups by checking the corresponding checkboxes and click on "**OK**".
4.	The new Voice IPS policy appears in the right pane of the Performance Manager main window. Right-click in the **IPS Policy** sub-window and select "**Add Rule**".

Step	Description
5.	Configure a rule according to **Call Direction**, **Source**, **Destination**, **Call Type**, **Time**, **Call Duration**, and **Service Types**. When the rule is triggered, the **Action** taken may be "**Allow**", "**Terminate Current and Future**" or "**Terminate Future**". The example rule below triggers if three 30-minute long distance calls are placed during a weeknight 1-hour interval. The rule terminates current and future long distance calls that last longer than thirty minutes for the rest of the 1-hour interval. Repeat as necessary to add additional rules.
6.	After finishing adding rules, click on the "**Save**" icon or select "**Save**" from the **File** menu. If the policy is not saved, there is an asterisk next to the policy name.

RL; Reviewed:
SPOC 12/15/2005

Solution & Interoperability Test Lab Application Notes
©2005 Avaya Inc. All Rights Reserved.

44 of 49
SecureLogixETM.doc

Step	Description
7.	In the Performance Manager main window, expand the **IPS Policies** tree. Right-click on the Voice IPS policy created in Steps 1 – 6 and select "**Install**".
8.	Click on "**OK**".

5. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying ETM System monitoring, detection, and policy enforcement.

5.1. General Test Approach

The general approach was to place calls inbound and outbound on Avaya Communication Manager T1 ISDN-PRI, T1 E&M, and H.323 trunks connected to the simulated PSTN and remote Avaya Communication Manager system, respectively, and to verify that the ETM System correctly monitors and controls telecom activity on those trunks. The main objectives were to verify that:

- The ETM System correctly detects voice calls on the T1 and H.323 trunks, as well as fax and modem calls on the T1 trunks.
- The ETM System allows or denies calls on the trunks in accordance with configured policies.
- The ETM System administrator is able to manually terminate calls on the trunks.
- The ETM System Firewall and IPS policies are correctly triggered and enforced.
- When the ETM Platform Appliance is shut down, trunk calls can still be successfully completed.

For serviceability testing, failures such as cable pulls and hardware resets were applied. For performance testing, a call generator continuously placed calls over T1 ISDN-PRI and H.323 trunks[2] and the ETM System was configured to terminate calls over a configured threshold each hour.

5.2. Test Results

The test objectives of Section 5.1 were verified. For serviceability testing, the ETM System operated properly after recovering from failures such as T1 and Ethernet cable disconnects, and resets of Avaya Communication Manager, the ETM Platform Appliance, and the DS1 and MedPro circuit packs on the G650 Media Gateway. For performance testing, the ETM System was subjected to call volumes of 16 inbound trunk calls per minute for over 14 hours; the ETM System correctly counted the number of inbound trunk calls and correctly terminated calls above the configured threshold.

---

[2] For H.323 trunk performance testing, the ETM appliance was placed inline in the path of the H.323 trunk.

6. Verification Steps

The following steps may be used to verify the configuration:

- For T1 ISDN-PRI and H.323 trunks, from the SAT, enter the command **status signaling-group s**, where s is the number of a signaling group configured in Section 3.2, and verify that the Group State is "in service".
- For T1 ISDN-PRI and H.323 trunks, from the SAT, enter the command **status trunk-group t**, where t is the number of a trunk group configured in Section 3.2, and verify that the Service States of all trunks are "in-service/idle" or "in-service/active".
- Place inbound and outbound calls across the trunks and verify that the calls are monitored in ETM. Disconnect the calls and verify that the ETM System correctly reports the call type, the origination and disconnect times, the calling and called party numbers if applicable, trunk IDs, and the call duration.
- Configure one or more rules that restrict inbound/outbound telecom access on the trunks and place calls across the trunks that would violate those rules. Verify that such restricted calls do not complete.
- Place inbound and outbound calls across the trunks and verify that the calls may be terminated from the ETM System Console.

7. Support

For technical support on SecureLogix Enterprise Telephony Management, consult the support pages at http://support.securelogix.com/index.htm or contact SecureLogix customer support at:

- Phone: 1-877-752-4435
- E-mail: support@securelogix.com

8. Conclusion

These Application Notes described the steps for configuring the SecureLogix Enterprise Telephony Management (ETM) System to monitor and control inbound and outbound telecom activity on Avaya Communication Manager T1 and H.323 trunks. During compliance testing, the ETM System successfully detected and monitored inbound and outbound calls placed across Avaya Communication Manager T1 and H.323 trunks, and allowed or terminated calls when certain configurable conditions were met. 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.

9. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.
[1] *Administration for Network Connectivity for Avaya Communication Manager*, Issue 10, June 2005, Document Number 555-233-504

Product documentation for SecureLogix products may be found at http://support.securelogix.com/manuals/index.htm.
[2] *ETM System User Guide Release 5.0*

RL; Reviewed:
SPOC 12/15/2005

Solution & Interoperability Test Lab Application Notes
©2005 Avaya Inc. All Rights Reserved.

49 of 49
SecureLogixETM.doc