Security Considerations for Avaya ESS Implementation

GIAC Gold Certification

Author: Thomas McDermott, jus330@optonline.net

Adviser: Carlos Cid

Accepted: February 15, 2008

Abstract

This paper addresses the security requirements of an enterprise PBX. The sample PBX architecture is an Avaya Enterprise Survivable Server (ESS) environment supporting an enterprise with multiple call centers. The primary objective is to define the environment, explore it, identify weaknesses and finally mitigate the weaknesses. It is not intended as a white paper on Avaya ESS or VOIP design.

Table of Contents

Introduction

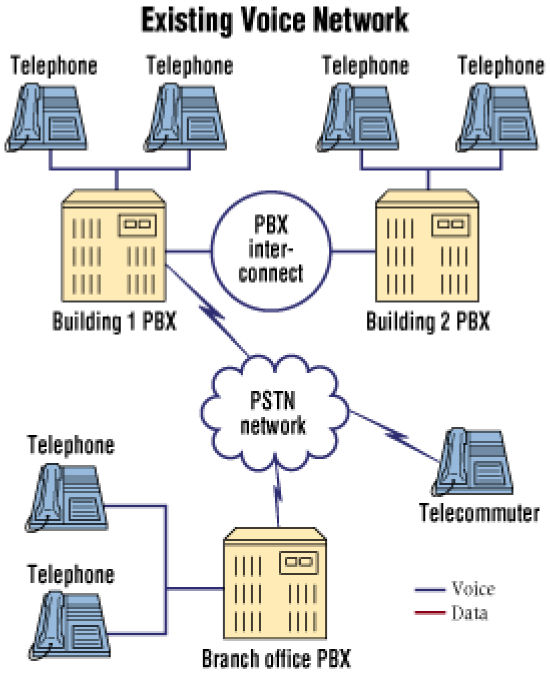
The primary focus of the paper is security revolving around the implementation of Avaya's ESS solution in a corporation. The implementation of ESS extends the backplane of the PBX (private branch exchange) across the wide area network. It is possible to implement the extended backplane described without ESS; however without it, the enterprise would be unrecoverable in the event of a disaster at the main location. If an enterprise were to run off a single set of servers that would be a single point of failure, ESS provides a second set of servers that have the configuration of the primary in a second location. This paper will utilize many acronyms, a list of these is provided in appendix B at the end of the paper.

The building blocks of the Avaya design utilize VOIP and IP Telephony. These are defined well by Kelly (2005), "VOIP for Dummies Avaya Limited Edition" (p. 5) when he states 'Basically, VoIP means "voice transmitted over a digital network"' and "IP Telephony enables voice communication over Internet Protocol (IP) networks". Essentially, VOIP is the voice traffic, while the IP telephony is the call control and all the applications (screenpops, call accounting, etc..) that add value to the voice.

In the traditional PBX (VOIP or TDM), there is a private network or backplane that is isolated from the data network where control information is exchanged. This is the "control" network, where the components of the PBX can communicate to each other. The private nature of the control network limits the ability of a single PBX to extend across geographically diverse locations, unless there is a dedicated private WAN connecting the private control networks. The ESS solution allows all the corporate PBX assets to share components (including telco services), regardless of location. The use of this PBX "extended backplane" allows the corporation to have an extremely flexible environment where phones can attach to any PBX resource and truly become virtualized. This allows the call center agents to be anywhere in the world and attach to the same skill sets / adjuncts (voice recording, IVR, telco services…). ESS allows calls to be seamless routed across the data network saving significant toll charges for interoffice calling (calls become intra office and do not require dedicated Tie Lines). Why should someone read this paper? I believe this is the next big security concern. It may surface as eavesdropping, DOS, Phreaking or a yet to be discovered attack. Corporations will rush to leverage their converged networks as Avaya and Cisco continue to push the VOIP world. Even if companies stay with TDM (Time Division Multiplexed or traditional digital hardwired phones) phones, most of the vulnerabilities will still be there on the back end control networks. Currently, there appears to be a significant disconnect between the roles of voice and data engineers. I have seen numerous corporate PBXs with public as the R/O snmp string. When asked if this is required the senior voice engineer could not tell me and was not very happy about changing it.

Overview of PBX Technology

The traditional PBX environment was a self contained system that provided all phone service to the organization. If there were multiple PBXs in the enterprise they would be tied together with Tie lines (dedicated telco links) or use the public telephone network to connect calls . The diagram below was taken from Hall (1998), " Voice-over-IP Across the Enterprise Network" (http://www.ehsco.com/reading/19981001ncf1.html).



The call routing would be seamless to the dialer, because the system would use an internal routing table (udp table) to translate the call to use the appropriate dialing sequence.

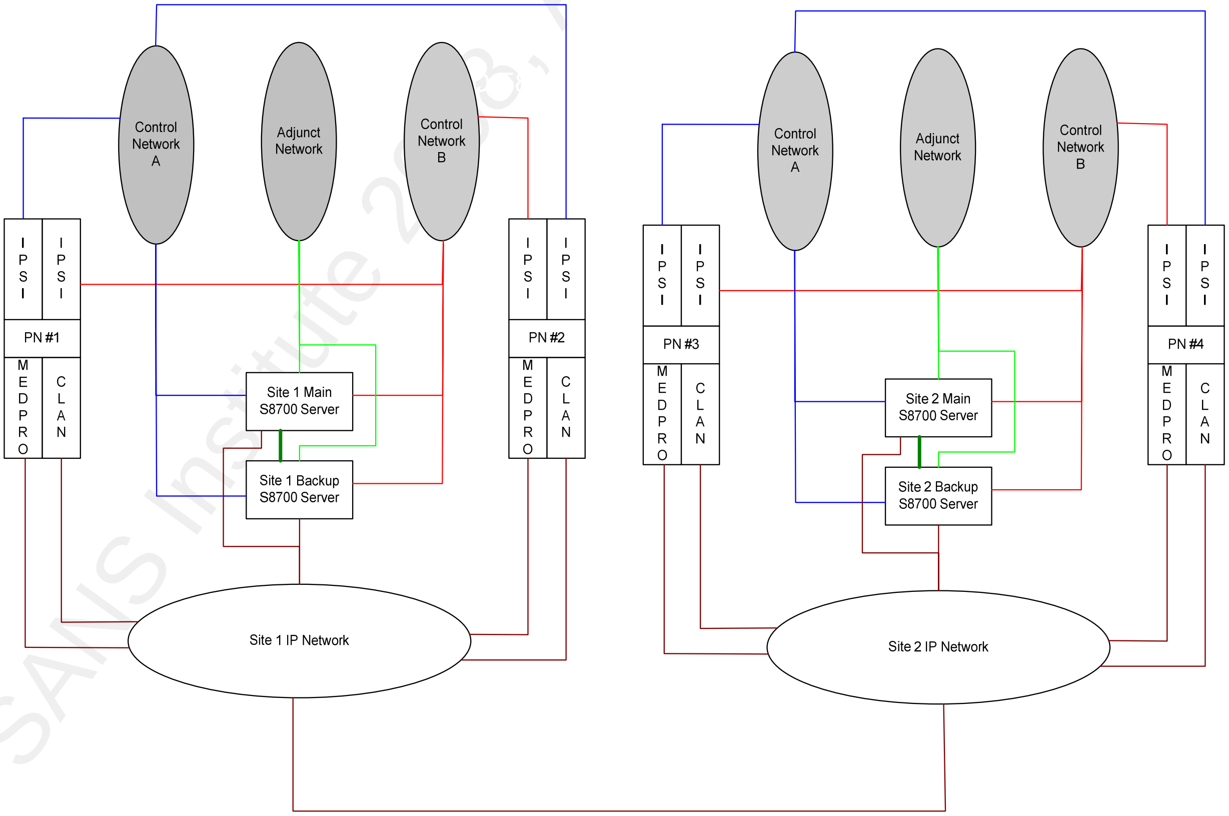
The connection of multiple corporate PBXs often required a separate parallel network, causing additional fixed cost or worse a variable cost based on usage.   The only security threat to this closed system was a Phreaker (i.e. toll fraud). This was deemed a limited exposure and thus this created a very comfortable environment for the business.   The Avaya platform of the day was Definity G3 based on a proprietary operating system called Oryx/Pecos. When Avaya moved into the IP world they made a strategic decision to go open source, so they committed to a hardened Linux based OS.   This allowed Avaya to leverage the vast UNIX and Linux resources available to secure their environment.

Enterprises have become very complicated, with call centers all over the world. The traditional enterprise pbx environment had limitations that had to be overcome by complex routing, remote shelves (a card in a remote location tied back to a home pbx) and more TIE lines. The call centers had to sign into their home PBX and skills. The ability to share agents across the PBXs was very limited and had to be handled manually.   The traditional PBX world was a series of standalone systems.

The next generation of the Avaya PBX relied on an IP based backplane. This PBX is now a Hardened Linux server (at the core) which speaks to the components via an Ethernet network based on IP. This allowed the PBX to be more modular and flexible. Each PBX had multiple Ethernet interfaces.

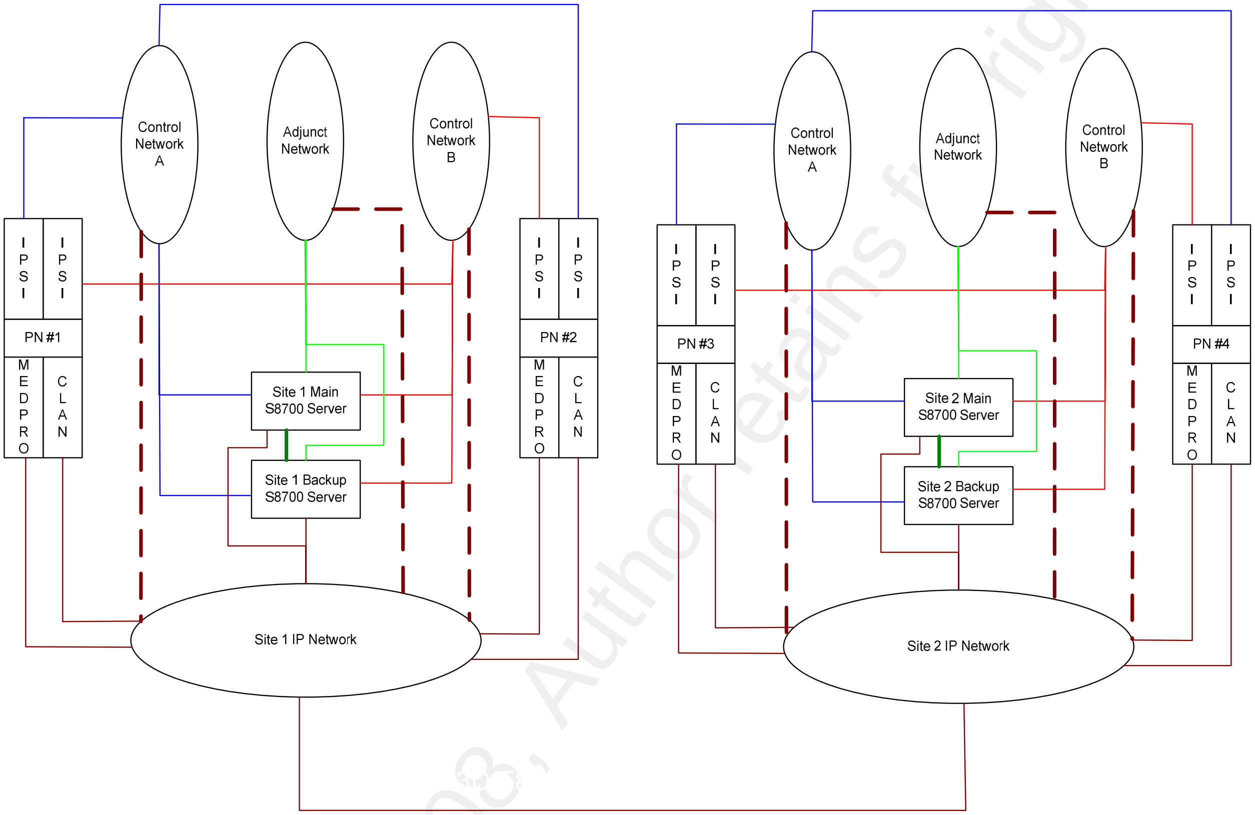
- Segment 0 and 3 are redundant Control networks where control of information is passed between the PBX and the backend cabinets
- Segment 1 – Local admin network for a laptop connection (30 bit network mask)
- Segment 2 – A duplication network used for replication / memory shadowing
- Segment 4 – Enterprise Network serving as an admin point and a registration point for port networks. This is the only routable network in this architecture.

Each location would have their own PBX, with its own control network, configuration files and local resources (T1s, announcement boards…). Usually each site would be locally administered and controlled by local staff.

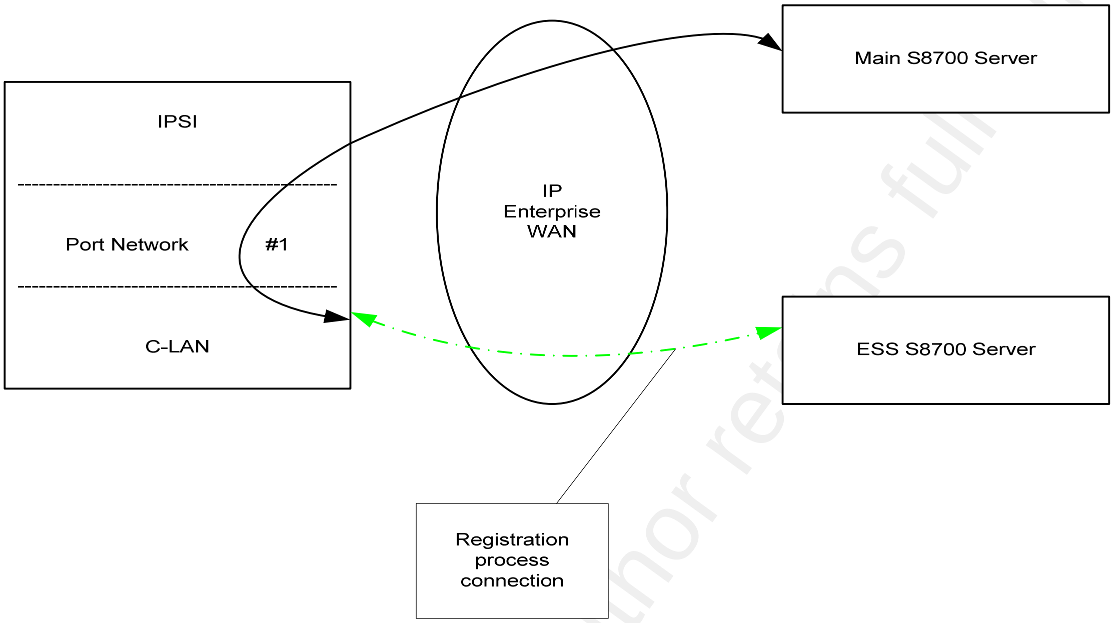


In the diagram above you can see there is no connection between the control networks in the different sites (the shaded networks are non routed). In this scenario the PBX's would need to have IP Trunks configured between the PBXs to support VOIP between sites. This helps reduce the cost but does nothing to allow the sharing of resources in each site.

In the current generation, the PBX goes global. The private control networks are connected to the data network (bold dashed lines in the diagram below) and now all components in all locations can share a configuration. The backup servers (or as they are called ESS servers) can be in a remote location, the configuration files are shared across the WAN.



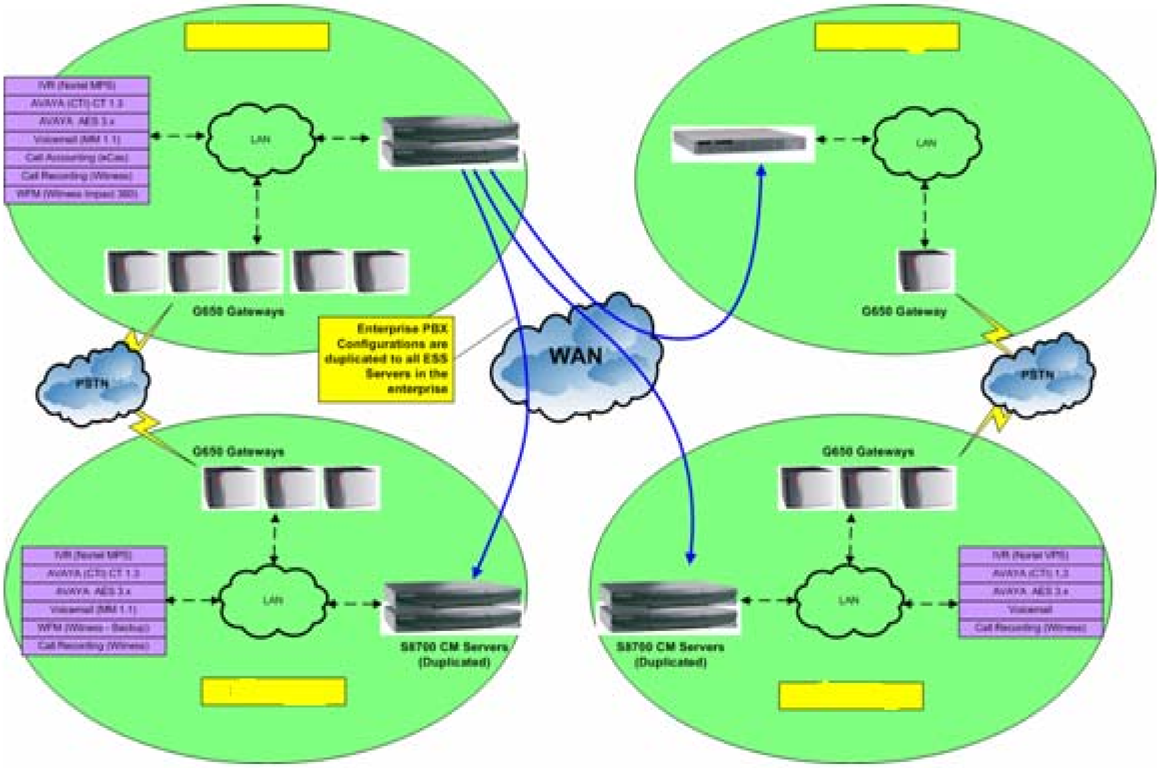
All the components of the network are aware of the primary (site 1) and backup (site2) media servers and constantly check for connectivity to the primary. The main server is actually a cluster of 2 servers with memory shadowing enabled, protecting the environment against a single server failure. The backup media servers register with the primary server via a C-LAN card (as shown below).



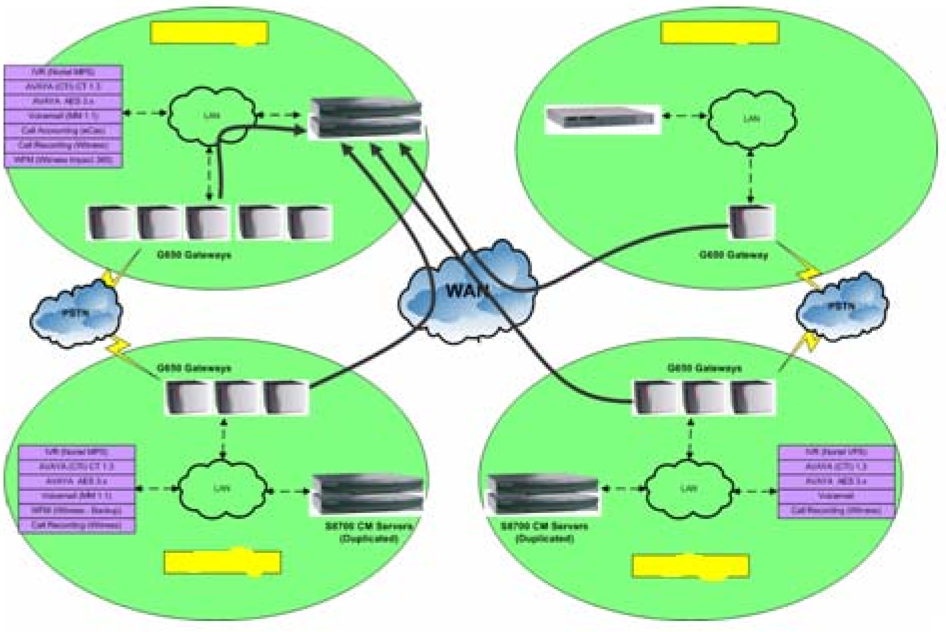
This process gives the primary server the addresses of the backup media servers which are required for the synchronization of the configuration. This process occurs once a day. The configuration synchronization only takes place once a day because ESS is designed to protect against catastrophic failure, so the loss of a minor change would be insignificant. The synchronization of the files can be configured to happen as often as desired but the default is once a day. If significant changes are made to the primary configuration, manual configuration synchronization could be forced.

If the primary servers go offline, the components will all re-register to the backup and within 4 minutes the entire organization will be re-converged. Most likely calls outside the failing component would stay connected during the initial failure, however once the new main server is elected, there is a disruptive re-convergence.

The following diagram illustrates how the configuration files for the single image switch (one shared configuration) are copied from the master to the secondary servers. The following three diagrams were originally created by KC Miller, VOIP Architect (personal communication, May 2007).

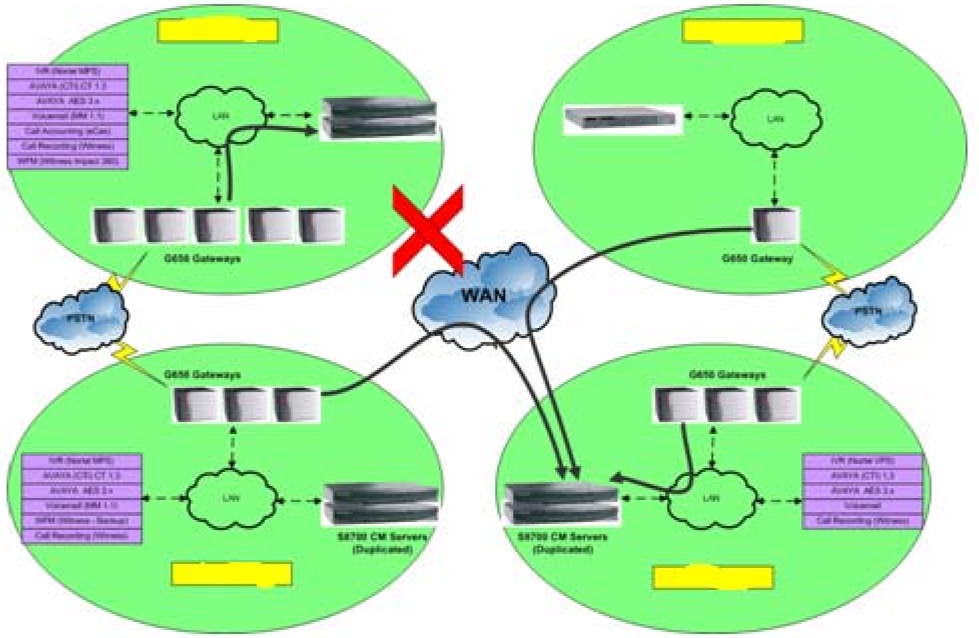


The actual components of the PBX, the gateways and such would communicate back to the primary central processor. You can see this in the diagram below.



The registration process consists of the port networks registering (via IPSIs) with all media servers in the enterprise by selecting the primary from the list. The IPSIs calculate a formula to track who the main server is in the configuration. This formula consists of a number of factors that contribute to a base score including local preference, system preference and main cluster designation. Essentially you can control how it converges by setting these values. The higher the score, the higher in the list of successors the server will be placed. This priority list is dynamic and is maintained as changes occur in the network.

If the primary location goes off line completely, all the components in all locations have a list of candidates to be the new central server. The remote components will now re-register with the new central server. The following diagram shows this re-registration process.



Review of Avaya Architectural Components

This section of the document will attempt to give the reader an overview of the terms and technologies used in the document specific to Avaya's technology. It is accurate as of this writing but Avaya is continually updating the technology available. I have defined some of the components in further detail in appendix A.

Media Server

The media server is the brains of the PBX. In the Avaya world, there are several types of media servers, sometimes called an SPE (Switch Processing Engine). The enterprise class media server is the S87XX server. These are hardened Linux servers running the communications manager software (define below).

Media Gateways

Media gateways are modular backplanes that allow for expansion in the PBX. These are the cabinets that contain all the individual components of the PBX that will be described below. There are several flavors of the Media Gateway : G250, G350, G450, G650 and G700. The G650 is the enterprise class gateway and is the one used in this PBX. The G650 gateway is a chassis that has 14 slots available for cards.

Internet Protocol Server Interface (IPSI)

The IPSI circuit pack provides signaling between the G650 gateway and the S87xx media servers (over IP). The IPSI is a card that is inserted in the G650 chassis. These devices compose the new backplane or control network. All devices in the Media Gateway that are not IP based utilizes the IPSI to speak to the processor. Things like T1 / Digital phone boards cards are examples of this type of device.

Control Local Area Network (C-LAN)

The C-LAN card is an IP gatekeeper that provides a registration point for IP-connected devices, including phone sets, Call Management System (CMS), messaging etc.   This card is inserted into the G650 chassis. The ESS backup processors also register to a C-LAN. In addition to registration, the C-LAN is the interface for call control for all IP endpoint devices.

Media Processor (MedPro)

The MedPro is an IP gateway device that converts TDM to IP and IP to TDM. It also applies compression algorithms (G.711, G.722, G.729) to packetized voice traffic prior to the traversal of the IP network. This device is a card that is inserted into a G650 chassis.

Communications Manager Software

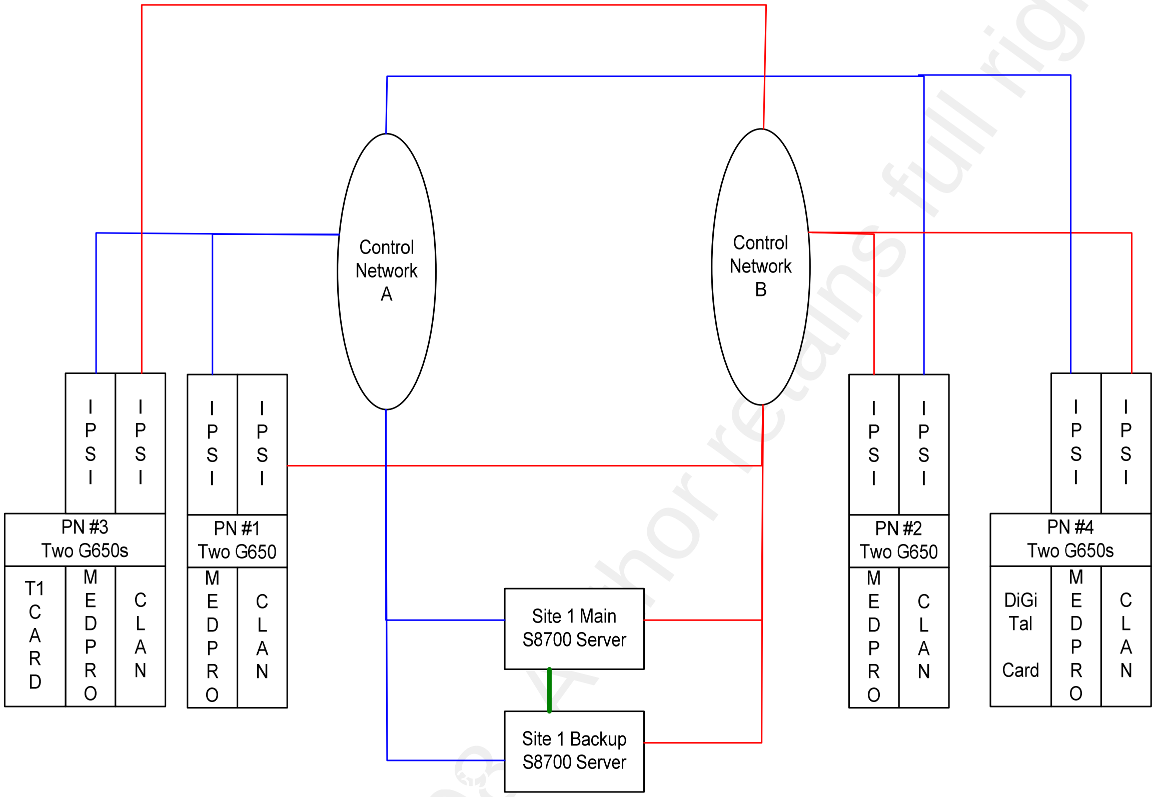
The communications manager software runs on the media servers and is the brains of the PBX. This code runs on the PBX and provides the intelligence to the phone system. The version referenced in this paper is version 3.X, the most recent version is 4.X with 5.X due out shortly, as of this writing.   The versions of the CM does not impact this architecture greatly, there are more configurable options but the architecture described is very much the same.

Port Networks

A port network is a grouping of components. In this example we will consider a port network consisting of 2 G650 gateways. Each G650 gateway has 2 backplanes, a TDM bus (supporting the traditional cards) and a packet bus (supporting the newer architecture). Each port network is connected to the main processor via IPSI boards.

Architecture Summary

ESS takes the conventional architecture of a PBX and extends it to the WAN. The Server's control networks are now connected across the network. This represents a few challenges, especially when converting an existing environment. When converting an existing environment to ESS, there are lots of adjuncts that require continued support. These adjuncts might not be optimized for ESS and represent exposure to the enterprise network. One more thing to consider, the adjunct system might not have the best documentation supporting the migration. I need to secure the environment but allow communications across the WAN. The control networks are made up of IPSI boards (which connect the entire G650 cabinet into the control network). The diagram below illustrates this.



Each of the port network checks in with the primary server by sending a heartbeat once a second. This heartbeat also contains the status of all the boards in the port network. Each port network should have 2 IPSI boards (an A and a B network). In the event there is a failure on the A control network, the server would try to reconnect via the B side. This is called an IPSI Interchange. Each port network has software acting as a primary controller (called an archangel). This controller coordinates with the rest of the PBX. The archangel runs in the IPSI board, by convention on the A side IPSI when both IPSIs are available. If the path to the primary server is unavailable on both the IPSIs, the port network will restart. There are multiple layers of restarts, each one starting an escalating amount of the port network. If this does not fix the problem ESS will begin to come into play and the port network will try to connect to the next server in its priority list. The IPSIs control the failover to avoid multiple ESS servers trying to take control simultaneously.

The architecture of the PBX is very complex; each of the components plays a distinct role in the process. I have attached 2 examples explaining how a call proceeds through the various components of the PBX. The following examples of call control process were created by Brain Adelson, Senior Converged Engineer of SPS communications (personnel communication, Jan 2008). The call sequencing detail is also available in the Avaya IP Telephony Implementation Guide on page 49 (http://support.avaya.com/elmodocs2/comm_mgr/r3_1/avaya-iptel-imp-guide3.1.pdf)

Call Flow IP to IP phone (Very Busy Diagram Below)

1) Phone A is picked up and dials Phone B's Extension. At this time, Phone A initiates an admission request (ARQ)/admission confirmation (ACF) exchange with the CLAN board it has already registered to.

2) The CLAN Board takes the information, and aggregates the information through the G650 Bus, and sends it to the IPSI card.

3) The IPSI card takes the information and utilizes a CCMS to communicate to the S87xx Servers.

4) The S87xx server receives the information request, and determines the location of the called party, whether it be an IP station or a Digital Station.

5) The S87xx server sends the information back to the IPSI which is then returned back to the CLAN, which is then returned back to the IP station as an ACF message. Step 5a also setups up an audio stream with a medpro resource

6) Media Server then sends a setup message directly to the extension (Phone B) via the CLAN it is registered to.

7) At this point, Phone A plays ringback to the caller, and the call goes into a call proceeding status

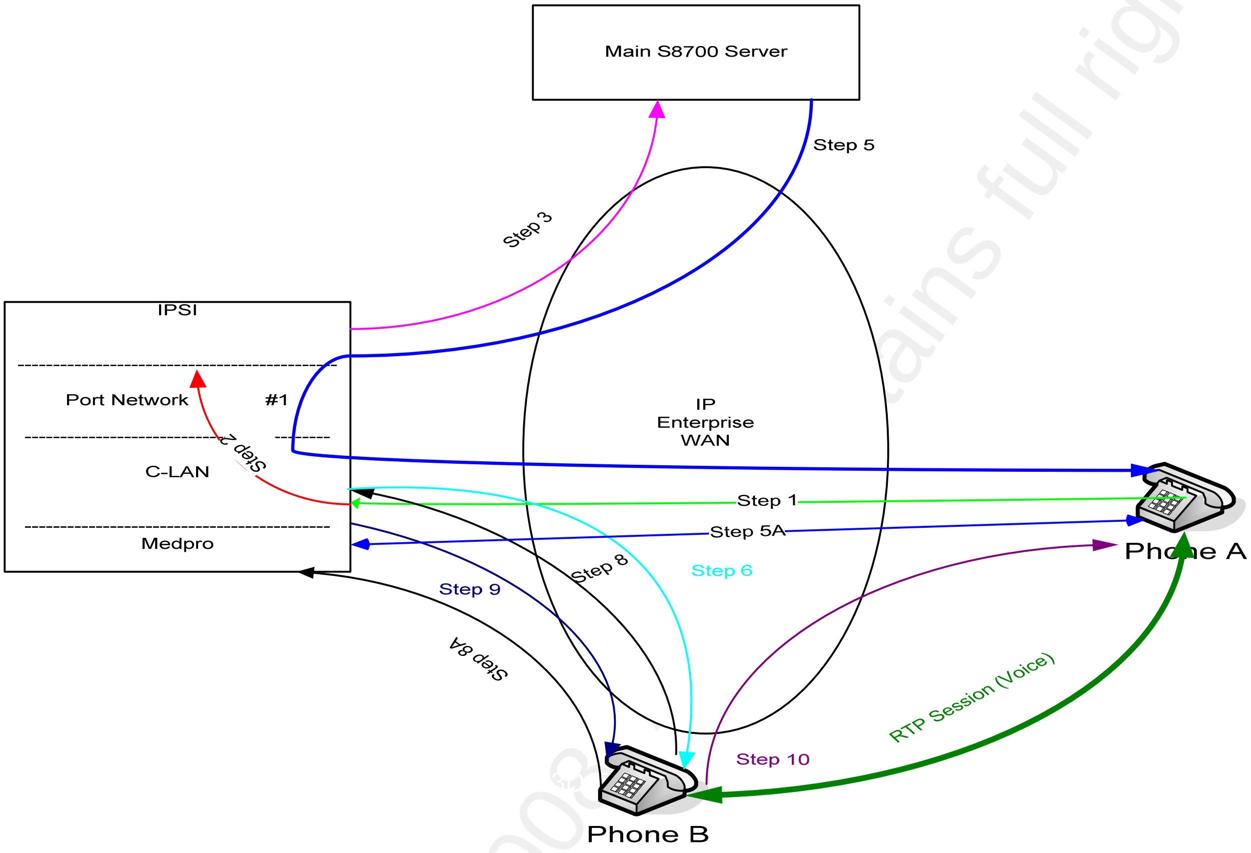
8) If Phone B is in service and able to accept the call, it initiates an ARQ/ACF exchange with the CLAN board and waits for a response back to verify the call. At this point, a one way audio stream is established to the Medpro. (step 8A)

9) The CLAN board sends back an ACF/ARJ message depending on if the phone is allowed to take the call.

10) Phone B then sends an alerting message back to Phone A if it receives a ACF message, otherwise it will send a release complete and disconnect the call.

11) CLANs then instruct the phones to direct their media streams to each other

12) Phone B and Phone A establish a RTP Stream and utilize RTCP to keep track of the order of packets for the audio portion of the call.



IP to IP Call Flow

Call Flow IP to TDM Phone (Diagram Below)

1) Phone A is picked up and dials Phone B's Extension. At this time, phone A initiates an admission request (ARQ)/admission confirmation (ACF) exchange with the CLAN board it is registered to.

2) The CLAN Board takes the information, and aggregates the information through the G650 Bus, and sends it to the IPSI card.

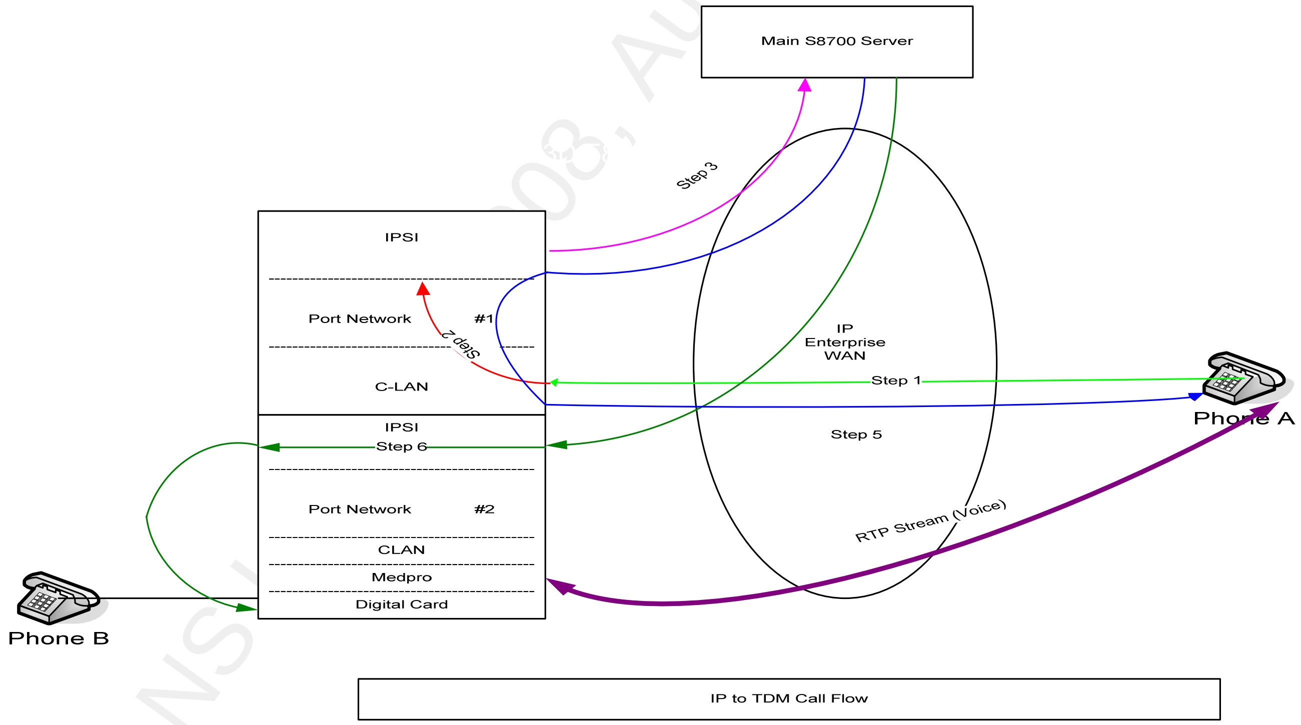
3) The IPSI card takes the information and utilizes a CCMS to communicate to the S87xx Servers.

4) The S87xx server receives the information request, and determines the location of the called party a Digital Station (Phone B).

5) The S87xx gives the address of the medpro in the port network which sends it to my CLAN who sends it to my phone. (the medpro resource is known to the server via the IPSI Heartbeat communication)

6) The S87XX server also contacts the IPSI (2) and it sends a request via CCMS to the TDM bus on the G650 to alert the phone of the call.

7) Phone A sets up the RTP path with the medpro which converts IP Packets onto the TDM bus (and vice versa) and it is sent to the digital phone.



Benefits of the New Architecture

The Avaya ESS environment is complex and exposes the enterprise to risks that a traditional PBX does not have. Why would anyone do this?

1. Cost savings – Leveraging the data network for intersite calls leads to significant savings because the data network has a fixed cost. In a sample install, 95% of all intersite calls were routed over the Data network, reducing the phone bill by 120K per month.

2. Flexibility – People can use their phone number anywhere in the network. Agents can log into the skills anywhere in the organization allowing for significant reduction in agent idle time and customer wait time.

3. Recoverability – The ability to quickly have the PBX environment recover in the event of a significant asset loss is essential in this day and age. The Avaya ESS environment has a redundant pair of processors in another location with an exact copy of the configuration in the event of a disaster.

The risks associated with the Avaya ESS design can be mitigated easily with some thought and careful planning.

Security Assessment

The methodology followed in this paper is based on the best practice assessment methodology as defined by McNab (2004), "Network Security Assessment" (p. 4). I will try to discover the PBX environment blindly because that is how an attacker would have to attempt an attack. I have already received permission from the Director of Information Security to run a non disruptive network assessment on the PBX and all its supporting components. This network assessment will allow me to take a closer look at the full PBX environment. This assessment will not be scripted, but will follow what I find during the assessment. The end result of this assessment will be a series of counter measures to correct anything vulnerabilities identified.

SNMP is a network management protocol that relies on simple strings or passwords to control the access to specific areas of Management Information Blocks (MIB). These MIBs are blocks of information that can be used to retrieve or set values on the device. The type of access is either Read Only (R/O) or Read Write (R/W). Having access to set values is extremely powerful and should be limited as much as possible. I relied heavily on SNMP for a lot of the assessment because it is very easy to use and very informative.

Network Enumeration

The traditional approach would be to gather as much information as possible without actively probing the environment. This is an internal target, google searches and who is lookups are not going to help much. Instead, I have a much more informative portal to gather information. This portal is my VOIP phone on my desk. Here is where I start my search.

The IP phone has a nice menu feature that will give me an incredible amount of information. Following the regular menu of my new phone, 9650 phone from Avaya, I do the following:

- Hit Menu
  - Network Information
    - IP Address of the Phone – 10.32.175.242
    - Call Server – 10.32.31.102
    - File Server – 10.35.154.20
    - VLAN ID – 175
    - Boot File – ha96XXUA1_20.bin
    - QOS settings

Immediately I have a few valuable pieces of information, I have the IP address of my phone. I have also identified a “Voice VLAN” for later recon, 10.32.175.0/24. The next bit of information is the actual IP address of the PBX server – 10.32.31.102.   I also observe the boot process of a 9650 phone, I see the following occur:

1. The phones gets assigned to the VLAN supporting voice VLAN175 in this case
2. DHCP address is assigned 10.32.175.243
3. The server is contacted for the upgrade script, 96xxupgrade.scr (server is 10.35.150.15), via HTTP
4. The Script runs checking the current version of software
5. The phone then grabs its settings files from the same server 46xxsettings.txt

Counter Measure to Enumeration

There is a way to limit the amount of information the menu gives up to the user of the phone but in speaking to the support personnel of the telecommunications department I was informed that this information is very valuable in troubleshooting. Removing this information from view would require a technician to login in with powerful access permissions that would be even more dangerous. One way to mitigate the risk of exposing the C-LAN addresses would be to make each DHCP scope give out a different C-LAN as the primary registration point. This would manually load balance the access across the connections. I consider this best practice for VOIP phones.

Active Network Scanning

My first goal is to review the voice vlan to find out what devices are on the network. I ran solarwinds snmpsweep on the voice network to see what is out there. I found 75 phones on the dedicated voice vlan. Most of the phones simply reply to the ICMP Echo Request and give no other information. If these were windows PCs I would have gotten names back as well (Solarwinds SNMPSweep does a DNS lookup if requested). Interestingly there is one phone configured with public as its Read Only string. The 46XX phones, an older model of phone, had the R/O public string configured by default.

Concentrating on this older phone I ran the Solarwinds MIBWalk utility. I managed to grab some more information from this phone:

tcpConnRemAddress	10.35.160.30
endptMCIPAdd	10.32.31.103, 10.32.31.102, 10.35.160.30, 10.32.31.40
endptMCIPInUse	10.35.160.30
endptTFTPSrvr	10.35.154.20
endptBootName	b20d01b2_1_1.bin
endptAppName	a20d01b2_1_1.bin
endpt46xxupgr	46xxupgrade.scr
endptTCPmon	10.35.150.15
endptHTTPSrvr	10.35.154.20
endptNVMCIPAdd	10.35.160.30
endptNVM.26	10.35.154.20
endptAppinuse	a20d01b2_1_1.bin

I need to investigate what these values mean but right off the bat I see a few things I know will be important:

- TFTP Server address
- Software Version
- HTTP Server (on an older phone this is N/A since the 46XX phones use TFTP)
- TCP Monitor address (performance monitor?)

4600 Series IP Telephone LAN Administrator's Guide (http://support.avaya.com/elmodocs2/avayaip/555233507_1_7.pdf) has a very good breakdown of these values (p. 86). The most important piece of information is the endptMCIPAdd values.

These represent call server addresses that the phone can register with. I have just located a group of C-LAN cards. The next entry endptMCIPInUse designates what C-LAN the phone is actively registered to. The C-LAN list is supplied to the phone via the DHCP scope.

I have now identified the following networks as potential locations for voice servers and PBX components, 10.32.31.0/24 and 10.35.160.0/24 (I am making an educated guess on the net mask based on my phone and my PC's delineation on a class C network). I decide to run snmpsweep against these segments. This sweep reveals very interesting information on the 10.35.160.0/24 network, nothing of note is returned on the 10.32.31.0/24. I decide to focus on the 10.35.160.0/24 network because that is the corporate HQ (based on IP address). I see a bunch of live hosts (based on the ICMP response) but SNMP gives back some more information. I find 5 live hosts that are responding to the string of public. These appear to be adjunct machines – Voice mail, Call Accounting and recording servers. I can tell this by the DNS names that are returned. I now know the following information.

- 5 C-LAN Addresses
- TFTP Server (Older Avaya Phones use this for version control)
- HTTP Server (Newer Avaya Phones use this for version control)
- Call Monitoring Address
- Call Accounting Address
- Call Recording Address
- Voice Mail Address – Announcements (2) and Message store

I began port scans of the live hosts that I have found. There appear to be no ICMP filters in place so I limited the scans to the ones that responded to ICMP Echo Requests. If there was filtering in place, I might choose to scan non responsive hosts. I need to find out what ports PBX Components use so I can limit the noise going forward (no point in scanning for ports that we know are not used). The scanning to date has been pretty noisy, so stealth is not the objective here. I have received permission from the Director of Information Security to conduct this scan already.

The 10.35.160.30 will be the first target, because I believe this is the primary PBX's CLAN based on the phone being registered to it. I am going to use the sl.exe utility (www.foundstone.com) to do a windows based port scan on the machine. I use the following command:

```
sl –vbht 1-65535 10.35.160.30

Adding IP 10.35.160.30
Banner grabbing enabled.
Hiding systems with no open ports.
Scan of 1 IP started at Thu Jan 17 10:33:31 2008
Pinging 1 IP (ICMP Echo Request)...
Found 1 live system
Scanning 1 IP...
-----------------------------------------------------------------------------
10.35.160.30
Responded in 0 ms.
5 hops away
Responds with ICMP unreachable: No
TCP ports: 1039 1720 2945 5023
-----------------------------------------------------------------------------
Scan finished at Thu Jan 17 11:02:55 2008
```

In the above command, the following flags are used

-v Verbose mode gives more information

-b Grab the banner from open ports

-h Hide any hosts with no open ports

-t Defines the ports to scan

My PC has McAfee AV running on it so I have to be careful about false positives and negatives. I reviewed the logs to see if there is anything being flagged by the logs.

```
2/3/2007     11:31:00 AM   Blocked by port blocking rule   C:\sl.exe     Anti-virus Standard
Protection:Prevent mass mailing worms from sending mail 10.35.160.30:25

12/3/2007    11:39:56 AM   Blocked by port blocking rule   C:\sl.exe     Anti-virus Standard
Protection:Prevent mass mailing worms from sending mail 10.35.160.30:587
```

The above log entry indicates I cannot scan for ports 25 or 587 or I will get unreliable results, unless I suspend this feature on my personal firewall.

Getting back to the scan, immediately I see that the C-LAN cards listen on TCP 1720. This is the port used for call control in most h.323 implementations. I scan the other three addresses that the phone returned to me to make sure they are all the same profile. The results (not attached) confirm that I have identified the profile for the standard CLAN. Knowing that certain addresses have a set of services running unique to C-LANS helps me create a profile for identifying other C-LANs on different segments. Network administrators tend to group networks by functionality (at least the good ones try to have some sense to the IP scheme). I ran snmpscan against the 5 address ranges below the one I just scanned 10.35.155.0-10.35.159.254. Even though I have permission to do the scans, the primary monitor of our IDS systems was not informed of this scan, yet I have not triggered any alarms to date, which indicates to me that the IDS sensors may have to be redeployed to be able to see PBX bound traffic.

The results of the scan show I have discovered some live hosts but none pertaining to this document. There is a fileserver segment located at 10.35.155.0/24. Interestingly, there were a few IP KVMs that were found with SNMP and public configured but that is outside the scope of my mandate.

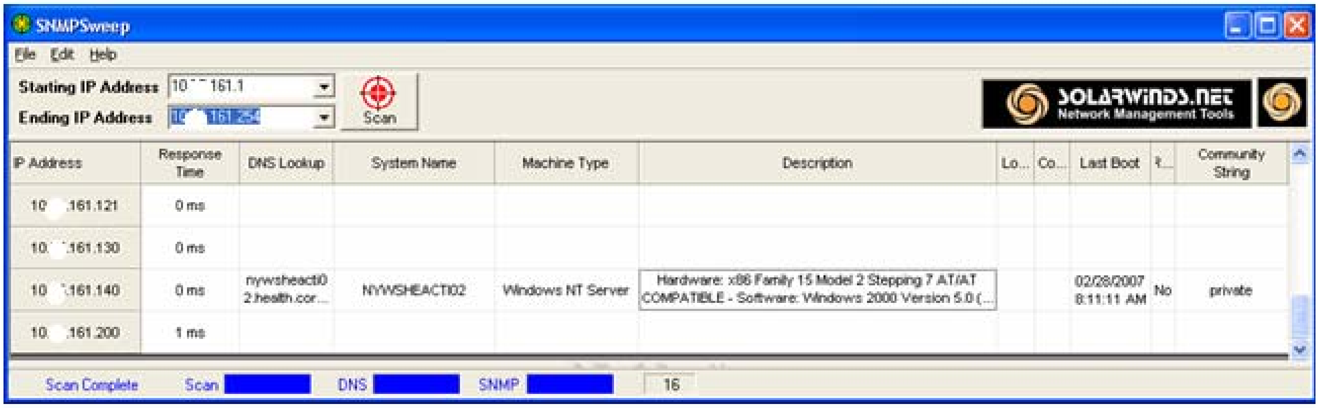
I ran a scan against 10.35.161.0-10.35.175.0.254. This produced much more interesting results. First I ran a scan looking for more C-LAN cards using the profile for the standard CLAN. I then did a global scan and looked for all the CLANs in the site and later expanded the search to all locations. I scanned 10.35.160.0/20. I used nmap with the options shown below.

```
Nmap –v –sS –p 1720 10.35.160.0/20
```

```
Starting Nmap 4.20 ( http://insecure.org ) at 2007-12-03 23:05 Eastern Standard Time
Initiating Parallel DNS resolution of 2048 hosts. at 23:05
Completed Parallel DNS resolution of 2048 hosts. at 23:05, 9.02s elapsed
Initiating Parallel DNS resolution of 2048 hosts. at 23:05
Completed Parallel DNS resolution of 2048 hosts. at 23:05, 6.50s elapsed
Initiating SYN Stealth Scan at 23:05
Scanning 159 hosts [1 port/host]
Discovered open port 1720/tcp on 10.35.160.30
Discovered open port 1720/tcp on 10.35.160.31
Discovered open port 1720/tcp on 10.35.160.32
Discovered open port 1720/tcp on 10.35.160.33
Discovered open port 1720/tcp on 10.35.161.31
Discovered open port 1720/tcp on 10.35.161.30
Discovered open port 1720/tcp on 10.35.164.20
Discovered open port 1720/tcp on 10.35.164.21
Discovered open port 1720/tcp on 10.35.164.22
Discovered open port 1720/tcp on 10.35.164.23
Discovered open port 1720/tcp on 10.35.164.142
Discovered open port 1720/tcp on 10.35.164.24
Discovered open port 1720/tcp on 10.35.164.25
Discovered open port 1720/tcp on 10.35.165.50
```

I wanted to see what is available via SNMP, so I run another SNMP sweep. I find a few high priority targets:

- We find a CTI server – this server provides integration between a computer system and the PBX. This server has Private as the R/W String. This is very interesting and will be further explored.

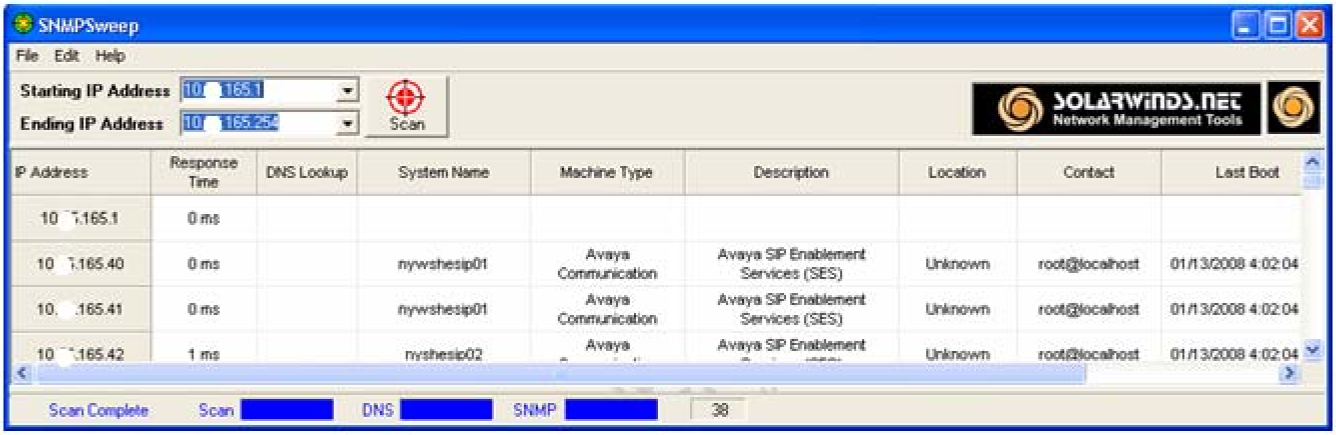


Starting IP Address 10[redacted]161.1
Ending IP Address 10[redacted]161.254

IP Address	Response Time	DNS Lookup	System Name	Machine Type	Description	Lo...	Co...	Last Boot	R...	Community String
10[redacted].161.121	0 ms									
10.[redacted].161.130	0 ms									
10[redacted].161.140	0 ms	nywsheacti02.health.cor...	NYWSHEACTI02	Windows NT Server	Hardware: x86 Family 15 Model 2 Stepping 7 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (...			02/28/2007 8:11:11 AM	No	private
10[redacted].161.200	1 ms									

Scan Complete Scan DNS SNMP 16

- We also find a SIP server cluster with public enabled as the R/O string. We will explore this first since the SIP server is an Avaya SIP server, making it likely that we will acquire PBX specific information. It is actually 2 SIP servers with a Virtual IP address and I can see both .40 and .41 have the same information.



Starting IP Address 10 [redacted] 165.1
Ending IP Address 10 [redacted] 165.254

IP Address	Response Time	DNS Lookup	System Name	Machine Type	Description	Location	Contact	Last Boot
10 [redacted].165.1	0 ms							
10 [redacted].165.40	0 ms		nywshesip01	Avaya Communication	Avaya SIP Enablement Services (SES)	Unknown	root@localhost	01/13/2008 4:02:04
10. [redacted] .165.41	0 ms		nywshesip01	Avaya Communication	Avaya SIP Enablement Services (SES)	Unknown	root@localhost	01/13/2008 4:02:04
10 [redacted].165.42	1 ms		nyshesip02	Avaya	Avaya SIP Enablement	Unknown	root@localhost	01/13/2008 4:02:04

Scan Complete Scan DNS SNMP 38

SIP Servers

The SIP servers reveal very little information other than the interfaces and network designs. I can revisit the SIP servers later as I have a very good understanding of the configuration based on the SNMP information returned.

```
# SIP Server IP Browser.txt exported on 12/03/2007 11:15:40 AM
# IP Network Browser  version 9.0.19
10.35.165.40   : nywshesip01
  Avaya Communication
  Community String: public
10.35.165.41   : nywshesip01
  Avaya Communication
  Community String: public
10.35.165.42   : nyshesip02
  Avaya Communication
  Community String: public
    System MIB
        System Name: nyshesip02
        Description: Avaya SIP Enablement Services (SES)
        Contact: root@localhost
        Location: Unknown
        sysObjectID: 1.3.6.1.4.1.6889.1.5.1
        Last Boot: 12/02/2007 4:02:05 AM
        Router (will forward IP packets ?) : No
    Interfaces
        7 interfaces
        1    lo
            softwareLoopback
 <lines Removed>
            TCP/IP Addresses
                127.0.0.1       255.0.0.0
        2    eth1
            ethernetCsmacd
 <lines Removed>
            TCP/IP Addresses
```

```
                192.11.13.6     255.255.255.252
          3   eth0
              ethernetCsmacd
     <lines Removed>
              TCP/IP Addresses
                10.35.165.42    255.255.255.0
          4   eth2
              ethernetCsmacd
     <lines Removed>
              TCP/IP Addresses
                192.11.13.1     255.255.255.252
          5   eth3
              ethernetCsmacd
    <Lines Removed>
              TCP/IP Addresses
                192.11.14.11    255.255.255.0
          6   eth4
```

CTI Server

The CTI server scan produced significant information. Using the R/W string I could essentially shut it down without a trace (see the denial of service attack on the VOIP monitor in the attack section). This would directly impact the call center as screen pops on PCs would stop working. The interesting information that we find out from this server is the existence of 10.35.164.0/24 network that is the backend of the CTI server.

This points us to a MAPD that provides the integration point to the PBX from our customer service applications (MAPD Boards are being replaced by C-LANS). I will explore this entry point. Now I know from this output that the MAPD server is located at 10.35.164.111. The output below allows me to confirm this is a CTI server based on the Avaya CT server running (green blocked below)

```
      # 10.35.161.140.txt exported on 12/03/2007 11:22:22 AM
      # IP Network Browser  version 9.0.19
      10.35.161.140  : NYWSHEACTI02
        Windows 2000 Server
        Community String: private
          System MIB
              System Name: NYWSHEACTI02
              Description: Hardware: x86 Family 15 Model 2 Stepping 7 AT/AT
COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Multiprocessor
Free)
              Contact:
              Location:
              sysObjectID: 1.3.6.1.4.1.311.1.1.3.1.2
              Last Boot: 02/28/2007 8:11:11 AM
              Router (will forward IP packets ?) : No
          Interfaces
              3 interfaces
              1    MS TCP Loopback interface
      <lines Removed>
                      127.0.0.1       255.0.0.0
              7219 HP NC7781 Gigabit Server Adapter
      <Lines Removed>
                  TCP/IP Addresses
                      10.35.164.141   255.255.255.0
              7220 HP NC7781 Gigabit Server Adapter
      <Lines Removed>
                  TCP/IP Addresses
                      10.35.161.140   255.255.255.0
          Services
       <lines Removed>
              AVAYA ASAI Server
              AVAYA CT Logging Server
```

```
                AVAYA CT Monitor Server
                AVAYA CT Server
                AVAYA CVLAN Server
        <Lines Removed>
                DameWare Mini Remote Control
                DameWare NT Utilities 2.6
        <Lines Removed>
                McAfee Framework Service
        <Lines Removed>
                SNMP Service
        <Lines Removed
                Telephony
        <Lines Removed>
            Accounts
                CTIAdmin
                Grhiddenadmin
                Guest
                niceuser
                TsInternetUser
             TCP/IP Networks
                10.35.161.140      255.255.255.0
                10.35.164.141      255.255.255.0
                127.0.0.1          255.0.0.0

            TCP Connections
                active          127.0.0.1:2872
127.0.0.1:6139
                active          127.0.0.1:6139
127.0.0.1:2872
                active      10.35.161.140:135   (DCOM SCM)    10.1.41.190:4849
                active      10.35.161.140:139   (netbios-ssn)
10.1.41.190:2606
```

```
             active      10.35.161.140:2427  (stgcp)
10.1.41.190:2819
             active      10.35.161.140:2427  (stgcp)
10.1.41.190:2883
             active      10.35.161.140:2427  (stgcp)
10.1.41.190:2887
             active      10.35.164.141:1262
10.35.164.111:5678  (rrac)
       <Lines Removed>
             listening   10.35.164.141:139   (netbios-ssn)
             listening   10.35.164.141:7770
             listening   10.35.164.141:9999  (distinct)
```

I will change the SNMP strings on this box as the primary countermeasure. If the SNMP information was not available I would never have seen the CTI link was being made between 10.35.164.141 and 10.35.164.111. The mapd board is an interesting target now so I scan 10.35.164.111 and find the following:

```
      C:\>nmap -sT -v -sV 10.35.164.111


      Starting Nmap 4.20 ( http://insecure.org ) at 2007-12-28 17:11 Eastern
Standard Time
      Initiating Parallel DNS resolution of 1 host. at 17:11
      Completed Parallel DNS resolution of 1 host. at 17:11, 0.00s elapsed
      Initiating Connect() Scan at 17:11
      Scanning 10.35.164.111 [1697 ports]
      Discovered open port 23/tcp on 10.35.164.111
      Discovered open port 21/tcp on 10.35.164.111
      Discovered open port 7/tcp on 10.35.164.111

      Discovered open port 515/tcp on 10.35.164.111

      Discovered open port 110/tcp on 10.35.164.111

      Discovered open port 514/tcp on 10.35.164.111

      Discovered open port 513/tcp on 10.35.164.111

      Discovered open port 13/tcp on 10.35.164.111

      Discovered open port 9/tcp on 10.35.164.111

      Connect() Scan Timing: About 39.72% done; ETC: 17:12 (0:00:45
remaining)

      Discovered open port 2766/tcp on 10.35.164.111

      Discovered open port 37/tcp on 10.35.164.111

      Discovered open port 9999/tcp on 10.35.164.111

      Discovered open port 111/tcp on 10.35.164.111

      Discovered open port 512/tcp on 10.35.164.111

      Discovered open port 19/tcp on 10.35.164.111

      Completed Connect() Scan at 17:13, 84.69s elapsed (1697 total ports)

      Initiating Service scan at 17:13

      Scanning 15 services on 10.35.164.111

      Service scan Timing: About 13.33% done; ETC: 17:27 (0:12:18 remaining)

      Service scan Timing: About 86.67% done; ETC: 17:17 (0:00:34 remaining)

      Completed Service scan at 17:16, 227.13s elapsed (15 services on 1
host)

      Host 10.35.164.111 appears to be up ... good.

      Interesting ports on 10.35.164.111:

      Not shown: 1677 filtered ports
      PORT     STATE  SERVICE    VERSION

      7/tcp    open   echo?

      9/tcp    open   discard?

      13/tcp   open   daytime?

      19/tcp   open   chargen?

      21/tcp   open   ftp?

      23/tcp   open   telnet?

      37/tcp   open   time?

      110/tcp  open   pop3?

      111/tcp  open   tcpwrapped

      512/tcp  open   exec?

      513/tcp  open   login?

      514/tcp  open   shell?

      515/tcp  open   printer?

      2766/tcp open   listen?

      9999/tcp open   tcpwrapped



      Service detection performed. Please report any incorrect results at
http://insec

      ure.org/nmap/submit/ .

      Nmap finished: 1 IP address (1 host up) scanned in 312.438 seconds

                     Raw packets sent: 2 (68B) | Rcvd: 1 (46B)
```

The command executes nmap with the following options:

-sT – A full TCP connect scan, this allows the whole TCP handshake to occur. It is less stealthy but more accurate. If Stealth was required, I would have used the –sS command. This scan would not complete the TCP handshake but just drop the connection after the syn/ack was received from the target.

-v – Verbose mode allows me to see what is going on and generates more information to the user. The progress updates in the output above is the result of this option.

-sV – I requested service verification. This would give me more information on the services running. In this case it gave me nothing more than a normal scan would give but it was worth a try.

The output of this scan is very interesting because it seems to be a rich target. I attempted to connect to the common services like telnet and ftp but the server does not respond. I believe the service is listening but not configured on the box. The mapd board is older technology that was meant as an integration point between the PBX and telephony applications. This map-d is normally placed in a private network talking to the integration server in a screened environment. A technical white paper found on the Avaya Website written by Robinson, 2001 called “TN801B MAP-D circuit pack running the DEFINITY LAN Gateway (DLG) and/or CVLAN applications Security” provides this recommendation.

The next area I want to review is the web server used to distribute the software and settings to the phone. I ran a port scan on the webserver and find it is listening to SNMP. I scan it with SNMPSCAN and I find private is configured as the R/W. Using this information, I download the list of users with IP Network browser. There are 3 users on the machines; I can quickly identify the admin user. The administrator id has a weak password and I am able to guess it quickly. Using the administrative privileges, I edited this file (46XXsettings.txt – File listed in Examples section) and changed the Voicemail extension to my own number. I rebooted my phone to pick up the new settings and hit my voicemail button. It immediately lights up my second extension and goes to “cover”. This confirmed that changing this file had an effect. I quickly changed the file back and reload my phone again and the message button started working again.

The http server setting is provided to the phones via dhcp. I don’t want to attack the DHCP server because that would attract attention. I decide to see if I can override the setting on the phone. I reloaded my phone (unplug it and plug it back in) and when it boots it gives me the option to hit * to program. I hit * and the phone asks me for a code. I tried a few things like Avaya, 12345 and nothing works. I searched the internet and discover the default password for the phones, “craft”. I entered this password and the phone menus unlock. This allowed me to override the file server setting. I reloaded the phone again and saw it briefly look for the new file server setting but then it loaded down the original settings file. I assumed this was caused by a mistake in the 46xxsettings.txt but I looked at the logs on my webserver and saw no connection was ever made. I realized that the DHCP settings were overriding mine. I re-entered the password and created a static IP address. All the other settings seemed to hold when I reloaded the phone again. This time, I confirmed the “new” 46xxsettings.txt had loaded to the phone. I played with a few settings, hoping to get the phone to give me more information. I set RTCP monitor (this is a performance monitoring setting) to my machine. I started ethereal on my machine but no packets were seen. I was hoping the RTCP packets would contain PBX information, but this setting had no effect on the phone and no information was captured. I then tried to change syslog setting to report to my machine, I set the reporting level to debug but nothing showed up. I continued to investigate the settings and managed to unlock the browser on my phone. I inadvertently locked my NT account because I configured the proxy and entered my ID into the phone; however the phone would not allow me to enter in the special characters required for my password. This was amusing but I decided to see what annoying changes I could make to the phones. This attack will not scale because of the need to create static IP addresses but it would be very difficult for the telecom personnel to troubleshoot. More than likely the phone would be deemed “bad” and replaced or have the factory default settings restored. Here are the things I was able to accomplish with my own 46xxsettings files:

- Disable the redial and call log list
- Turn off the menus, including the logoff button directly impacting the call center
- Create a home page and screensaver for the phone.
- Change the message waiting button's extension

The most interesting thing for me was the home page setting. It took some doing but I figured out that I needed to create a page using wireless markup language (WML). I downloaded a sample and modified it to create a message of the day. I wanted to add a graphic so I downloaded a wbmp file of a snake. I added this to a webserver that I managed and added the wml and wbmp extensions to apache via the httpd config file. I also have to exclude this web server from the proxy list in the 46xxsettings.txt file. I reload my phone the browser now sees the new home page. I could have made this page say anything. I have in reality defaced the phone.

Here is the wml code

```
        <?xml version="1.0"?>
        <!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">
        <wml>
```

```
<template>
   <do type="accept" label="Back"><prev/></do>
</template>
<card id="home" title="HIP Phones">
<p align="center">
  <img src="snake.wbmp" alt="[Octane Logo]"/>
</p>
<p>
<big><b>T</b></big>he test worked.  This is the placeholder for the message of the day
<br/>
</p>
</card>
</wml>
```

The ability to override the DHCP on my phone allowed me to test the options in the 46xxsettings files without impacting every IP phone in the company.   This is a nice way to test the file before I put it on the server. If I put it on the phones, the next time a phone reloaded, there would be a new version of the settings file. If I wanted to have a bigger impact, I would have to force a global reload. This can be done from the media server or by reloading the IP POE switch. Phones and PBX components are segmented into port networks on the PBX. All of the phones in a port network can be reloaded from the media server (SPE).

Counter Measures to file manipulation:

The 46xxsettings file is a critical piece of the voice infrastructure. Changing this could wreak havoc on the VOIP platform. Given the value of this target, combined with the ease of locating the resource I have made the following changes to this server:

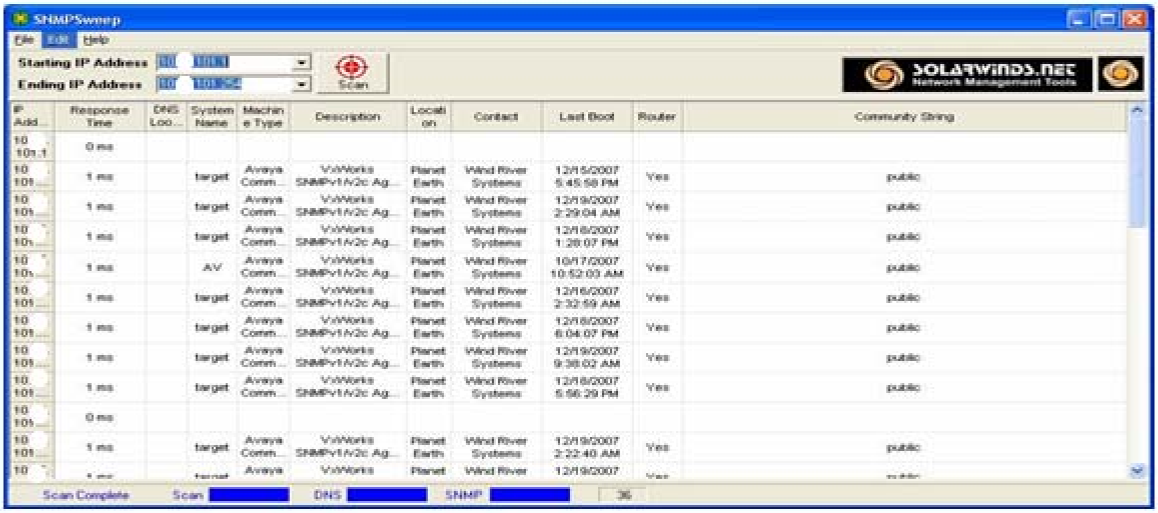
- Installed Tripwire to monitor the critical parts of this server, including the 46xxsettings.txt and 96xxupgrade.txt files.
- Installed the McAfee McHIP firewall to protect the fileserver. When I reviewed the current configuration, the signatures of the AV were 14 Months old.
- Added this server to the MS patching infrastructure so the latest patches are added on a regular basis.
- Log files will be archived to our central monitoring location. This product, Arcsight, will look for patterns and correlate the data with all our other alerts.

Counter Measures to SNMP scanning:

Block SNMP to voice networks

There are over a hundred phones on the voice vlan and there are hundreds of voice vlans in the enterprise, to rapidly remove the public string would take a lot of work because the older phones use TFTP for setting distributions. The quick counter measure to SNMP vulnerabilities is to restrict who can send SNMP queries to the phones and this can be done with an ACL on the voice vlan interface.

SNMPSweep before the ACL is applied:



Starting IP Address
Ending IP Address

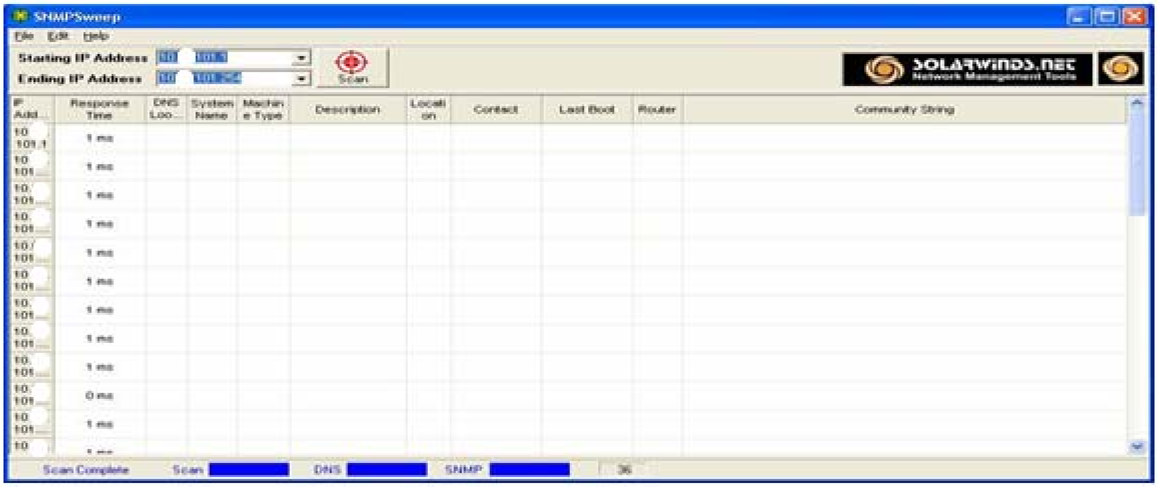
IP Add...	Response Time	DNS Loo...	System Name	Machine Type	Description	Location	Contact	Last Boot	Router	Community String
10 101.1	0 ms									
10 101...	1 ms		target	Avaya Comm...	VxWorks SNMPv1/v2c Ag...	Planet Earth	Wind River Systems	12/15/2007 5:45:58 PM	Yes	public
10 101...	1 ms		target	Avaya Comm...	VxWorks SNMPv1/v2c Ag...	Planet Earth	Wind River Systems	12/19/2007 2:29:04 AM	Yes	public
10 101...	1 ms		target	Avaya Comm...	VxWorks SNMPv1/v2c Ag...	Planet Earth	Wind River Systems	12/18/2007 1:28:07 PM	Yes	public
10 101...	1 ms		AV	Avaya Comm...	VxWorks SNMPv1/v2c Ag...	Planet Earth	Wind River Systems	10/17/2007 10:52:03 AM	Yes	public
10 101...	1 ms		target	Avaya Comm...	VxWorks SNMPv1/v2c Ag...	Planet Earth	Wind River Systems	12/16/2007 2:32:59 AM	Yes	public
10 101...	1 ms		target	Avaya Comm...	VxWorks SNMPv1/v2c Ag...	Planet Earth	Wind River Systems	12/18/2007 6:04:07 PM	Yes	public
10 101...	1 ms		target	Avaya Comm...	VxWorks SNMPv1/v2c Ag...	Planet Earth	Wind River Systems	12/19/2007 9:38:02 AM	Yes	public
10 101...	1 ms		target	Avaya Comm...	VxWorks SNMPv1/v2c Ag...	Planet Earth	Wind River Systems	12/18/2007 5:56:29 PM	Yes	public
10 101...	0 ms									
10 101...	1 ms		target	Avaya Comm...	VxWorks SNMPv1/v2c Ag...	Planet Earth	Wind River Systems	12/19/2007 2:22:40 AM	Yes	public
10	1 ms		target	Avaya	VxWorks	Planet	Wind River	12/19/2007	Yes	public

Scan Complete Scan DNS SNMP 36

We apply the following ACL as an outbound access group on the Voice VLAN Interface

```
Extended IP access list VOICE-SHIELD
    10 deny udp any any eq snmp (585 matches)
    20 permit ip any any (436 matches)
```

As a result, you can see the phones no longer respond to the SNMP requests



Starting IP Address 10 . 101.1
Ending IP Address 10 . 101.254

IP Add...	Response Time	DNS Loo...	System Name	Machine Type	Description	Location	Contact	Last Boot	Router	Community String
10. 101.1	1 ms									
10. 101....	1 ms									
10. 101....	1 ms									
10. 101....	1 ms									
10. 101....	1 ms									
10. 101....	1 ms									
10. 101....	1 ms									
10. 101....	1 ms									
10. 101....	1 ms									
10. 101....	0 ms									
10. 101....	1 ms									
10	[illegible]									

Scan Complete   Scan   DNS   SNMP   36

Change SNMP strings on all devices/ restrict access

Changing strings is a simple technique that requires little work but pays off quickly. I have to change the monitoring software but that is better than leaving all this information in the open. On Windows servers I changed the SNMP strings, removed the default (this is important) and configured the service to only accept requests from pre-approved servers like my NMS software. A sniffer could still pick up the string but the device would not respond to the string unless the source address matched the pre-approved list. I could spoof the source address but this would be very difficult if I can't map out the SNMP MIBs for each of the devices.

USE SNMP Version 3

Avaya supports SNMP version 3, which uses encryption on the all communications between the management server and the agents. This eliminates the sniffing of the strings as a potential problem. Some MGMT servers still don't support this version but it should be considered.

Enumerating the Control Networks

As previously defined, the media servers control the components of the PBX via the control networks. The control network now spans multiple sites, leveraging the WAN to allow for the PBX to service the enterprise seamlessly. If I can enumerate the control network across the enterprise I will have a very good map of the PBX. A control network will have two main components: media servers and IPSIs. These are very high priority targets in the ESS world.

I started by doing some research on the Avaya website to see if I can get clues as to how to identify these various devices. I located the information in the Avaya ESS users guide, p.66, (http://support.avaya.com/elmodocs2/comm_mgr/r3/pdfs/03_300428_1_1.pdf) under port considerations. There is a listing of ports required to make the ESS functional. It looks like the IPSIs will respond on some of the following ports:

- 20 FTP Data
- 21 FTP
- 22 SSH
- 23 Telnet
- 68 DHCP
- 514 Download translations
- 1719 UDP
- 1956 Command Server
- 2312 Telnet Firmware monitor
- 5010, 5011 and 5012 IPSI control, version and serial number channels
- 21873, 21874 Translations to LSP

I run an NMAP scan

```
Nmap –v –sS –p 20,21,22,23,68,514,1720,1956,2312,5010-5012,21873-21874
10.35.160.0/20
```

This will identify all the CLANs and IPSIs in the range. I left off the output because it was very long and the list of IPSIs will be shown below.

I know my two other main sites IP addressing scheme based on servers located in each site. The LI site is 10.15.0.0/16 and the Florida Site is 10.7.0.0. I run the same series of steps again in these sites (SNMPSweep, MIB WALK, IP Browser, NMAP). I start with my Long Island site. Running the snmpscan, I get very lucky. The main server at the LI site has the public string enabled. This reveals a lot of information. The SNMP mibwalk gets me a list of all the devices this is talking to, which is everything since this is a backup processor to the main processor in my NYC Location. Considering this is a backup processor, I have the ability to poke around at this one without attracting as much attention.

The following connections are listed in the MIB walk, the ports are listed as 5010 making them IPSI boards. These devices listed below make up the A and B control networks of the PBX.

10.15.170.115	10.15.170.116	10.15.170.124	10.15.170.125
10.15.170.126	10.15.170.127	10.15.171.115	10.15.171.116
10.15.171.124	10.15.171.125	10.15.171.126	10.15.171.127
10.32.31.20	10.32.31.21	10.35.170.101	10.35.170.102
10.35.170.103	10.35.170.104	10.35.170.105	10.35.170.106
10.35.170.107	10.35.170.108	10.35.170.109	10.35.170.110
10.35.170.111	10.35.170.112	10.35.170.113	10.35.170.114
10.35.171.101	10.35.171.102	10.35.171.103	10.35.171.104
10.35.171.105	10.35.171.106	10.35.171.107	10.35.171.108
10.35.171.109	10.35.171.110	10.35.171.111	10.35.171.112
10.35.171.113	10.35.171.114	10.7.170.117	10.7.170.118

10.7.170.119	10.7.170.120	10.7.170.121	10.7.170.122
10.7.171.117	10.7.171.118	10.7.171.119	10.7.171.120
10.7.171.121	10.7.171.122		

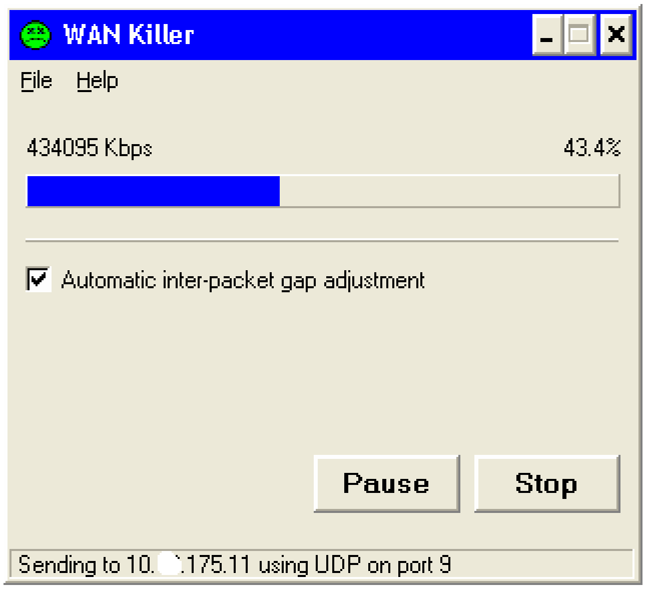
This enumerates all of the IPSIs that make up the control network for the enterprise, this was done with one tool via SNMP. There was not a lot of work involved with mapping this network out.

Investigation / Exploitation Phase:

DOS Attack on phones:

I have configured QOS on all the phones and components. Each of the phones is trusted by the Cisco switch. This allows the phone to withstand the average denial of service attack. The book Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions has an excellent section about the different DOS attacks that can be run. I was not able to replicate the attacks for this paper. Avaya feels they have addressed these issues and that may be why I cannot replicate them.

I used WAN Killer from Solarwinds to generate random traffic to the phone. Watching the phone and statistics I see minor changes in the statistics. QOS is working quite well and all call functions stay up.



434095 Kbps 43.4%

☑ Automatic inter-packet gap adjustment

Sending to 10.[redacted].175.11 using UDP on port 9

DOS Attack on the VOIP manager:

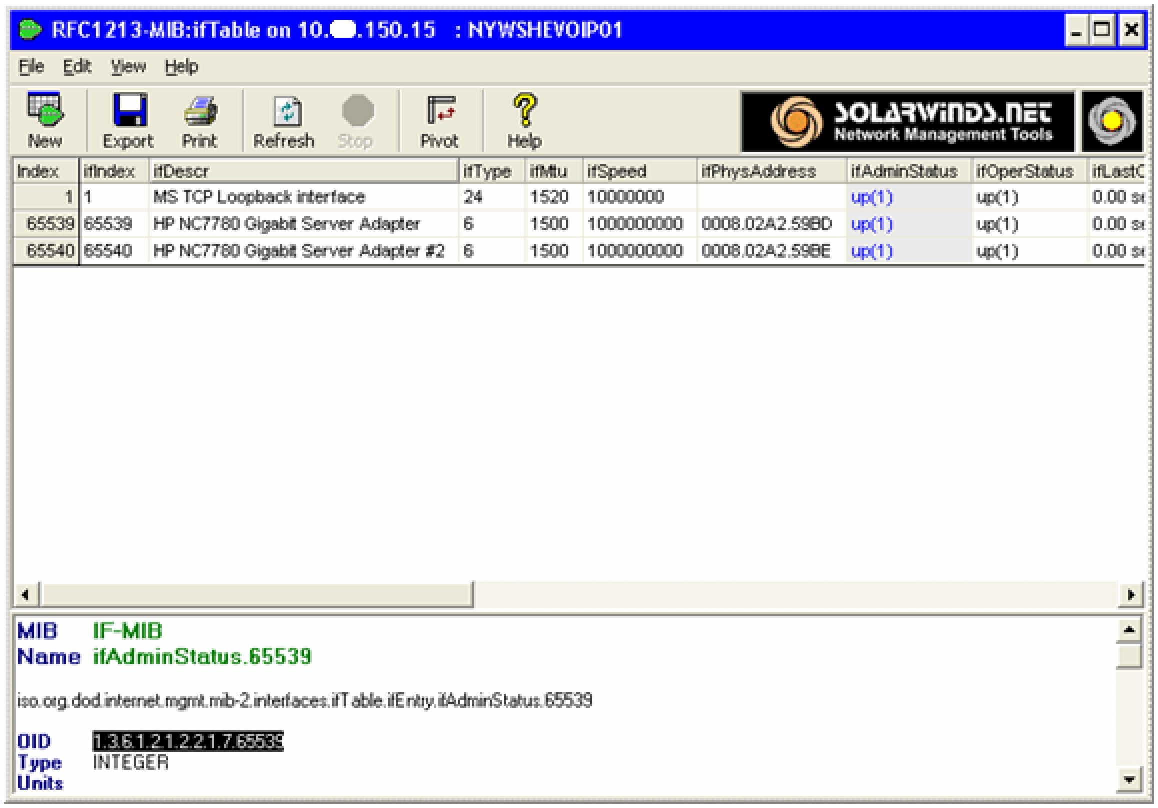
All the phones currently report statistics back to a central manager that will allow the administrators to see the performance of the VOIP phones. This manager is located at 10.35.150.15. We begin this attack by doing a scan of the box.

I found the following major services available:

- 139 – Netbios Name Service
- 80 – Apache
- 3389 – Terminal Services
- 6139 - Dameware

In a previous scan I had already noted that this host was running the R/W string of “private”. In this section I ran an Solarwinds IP browse on the machine and this provides a bunch of good information. I record the users that are defined on the machine, one of which is the admin account. I also tested to see if I have the R/W string (private is a clue but I wanted to make sure). I set the contact information of the MIB to ME and re-scanned it to confirm the change. The scan showed the change so this confirms the string is the R/W string.

There are a lot of vectors to attack now that we have a list of users. While I would like to "own" this box, I am more interested in blinding it so we can look around the PBX and try to do things. I decide to use the R/W string to knock the box off the network. I reset the NIC to admin state of down.


RFC1213-MIB:ifTable on 10.[redacted].150.15 : NYWSHEVOIP01
File Edit View Help
New Export Print Refresh Stop Pivot Help
SOLARWINDS.NET Network Management Tools

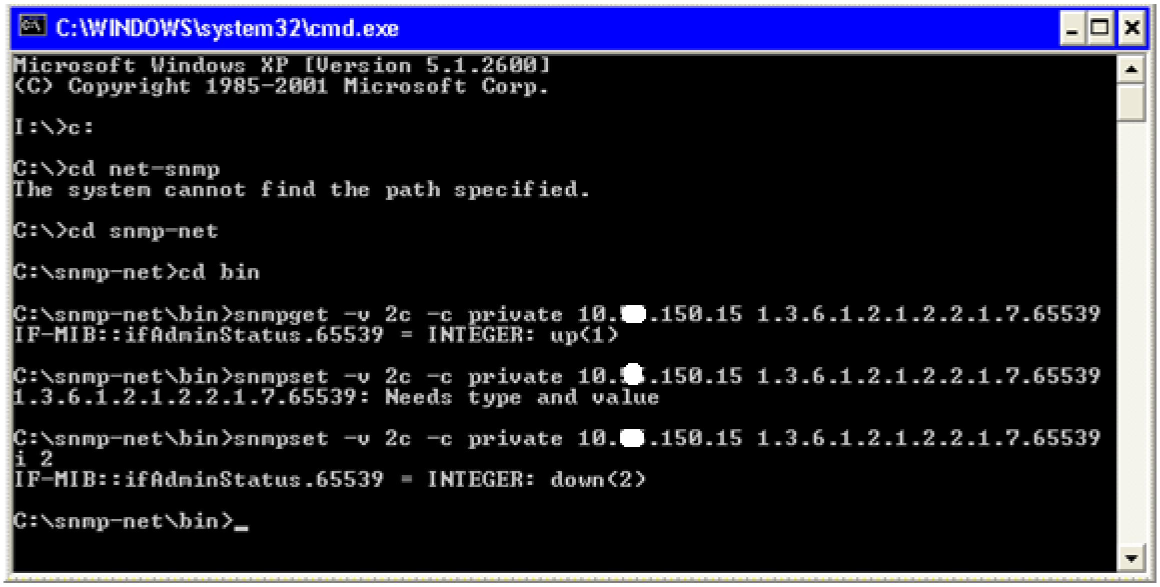
Index	ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastC
1	1	MS TCP Loopback interface	24	1520	10000000		up(1)	up(1)	0.00 se
65539	65539	HP NC7780 Gigabit Server Adapter	6	1500	1000000000	0008.02A2.59BD	up(1)	up(1)	0.00 se
65540	65540	HP NC7780 Gigabit Server Adapter #2	6	1500	1000000000	0008.02A2.59BE	up(1)	up(1)	0.00 se

MIB IF-MIB
Name ifAdminStatus.65539

iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifAdminStatus.65539

OID 1.3.6.1.2.1.2.2.1.7.65539
Type INTEGER
Units

In the frame below you will see the command I used to set this OID'd value to down, first I validated I have the right OID by doing a get. I then issue a set to change it to admin down. I tell the command that it is Version 2c of SNMP, the community string to use is private and the value is an integer and I want to set it to 2 (down). I use the snmp-net toolset, found on sourceforge at the following location: http://net-snmp.sourceforge.net/, to manipulate the OID values.

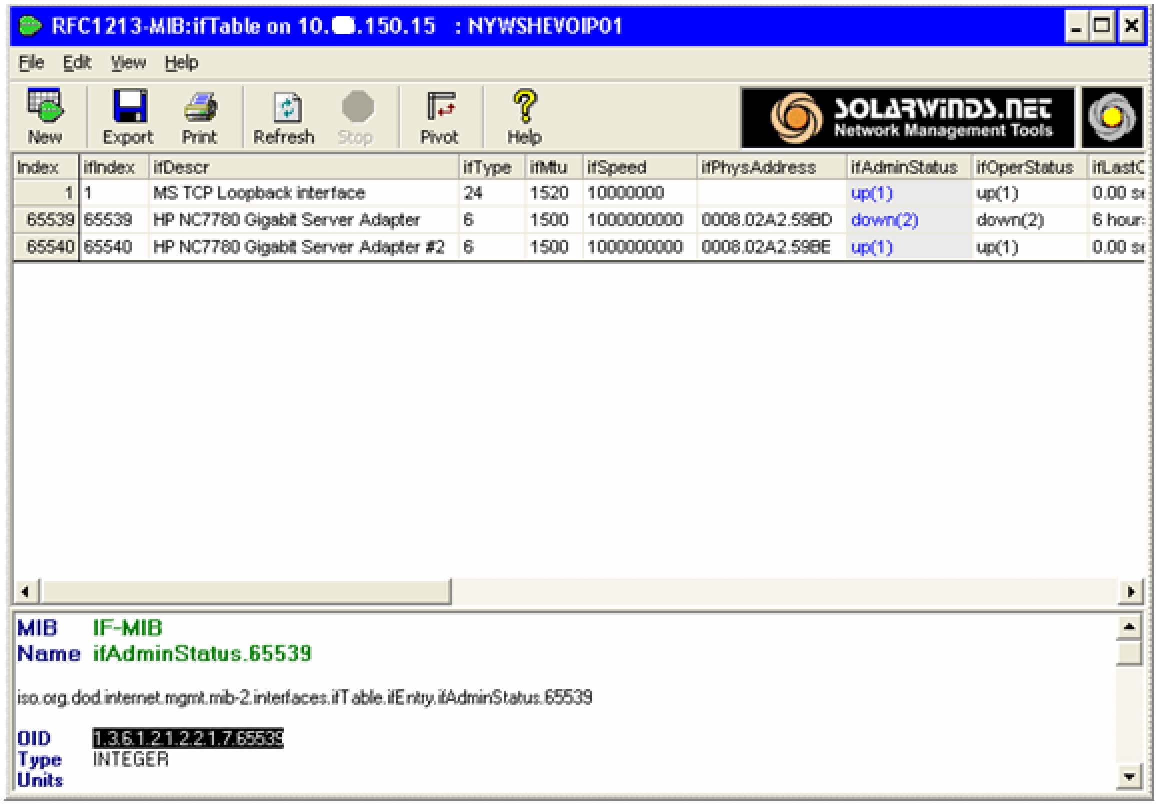


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

I:\>c:

C:\>cd net-snmp
The system cannot find the path specified.

C:\>cd snmp-net

C:\snmp-net>cd bin

C:\snmp-net\bin>snmpget -v 2c -c private 10.[redacted].150.15 1.3.6.1.2.1.2.2.1.7.65539
IF-MIB::ifAdminStatus.65539 = INTEGER: up(1)

C:\snmp-net\bin>snmpset -v 2c -c private 10.[redacted].150.15 1.3.6.1.2.1.2.2.1.7.65539
1.3.6.1.2.1.2.2.1.7.65539: Needs type and value

C:\snmp-net\bin>snmpset -v 2c -c private 10.[redacted].150.15 1.3.6.1.2.1.2.2.1.7.65539
i 2
IF-MIB::ifAdminStatus.65539 = INTEGER: down(2)

C:\snmp-net\bin>_
```

The above commands are run from the command line issuing SNMP commands directly against the OID of the MIBs supported on the device. You need to provide a R/W string to do a set and a R/W or R/O string to issue a get. If you don't have the OID from a MIB walk or another tool, this would be a difficult to thing to do. The MIB's are published but the entry can be dependent on the specific machine / configuration.

The –v flag indicates the version (1, 2c or 3), -c indicates the community string. The OID follows; this is the long number that indicates the hierarchy in the standard. The next field indicates the type of setting, in this case "I" indicates integer, followed by the value 2 for down

(Value and string are dependent on OID).



Index	ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastC
1	1	MS TCP Loopback interface	24	1520	10000000		up(1)	up(1)	0.00 s
65539	65539	HP NC7780 Gigabit Server Adapter	6	1500	1000000000	0008.02A2.59BD	down(2)	down(2)	6 hour
65540	65540	HP NC7780 Gigabit Server Adapter #2	6	1500	1000000000	0008.02A2.59BE	up(1)	up(1)	0.00 s

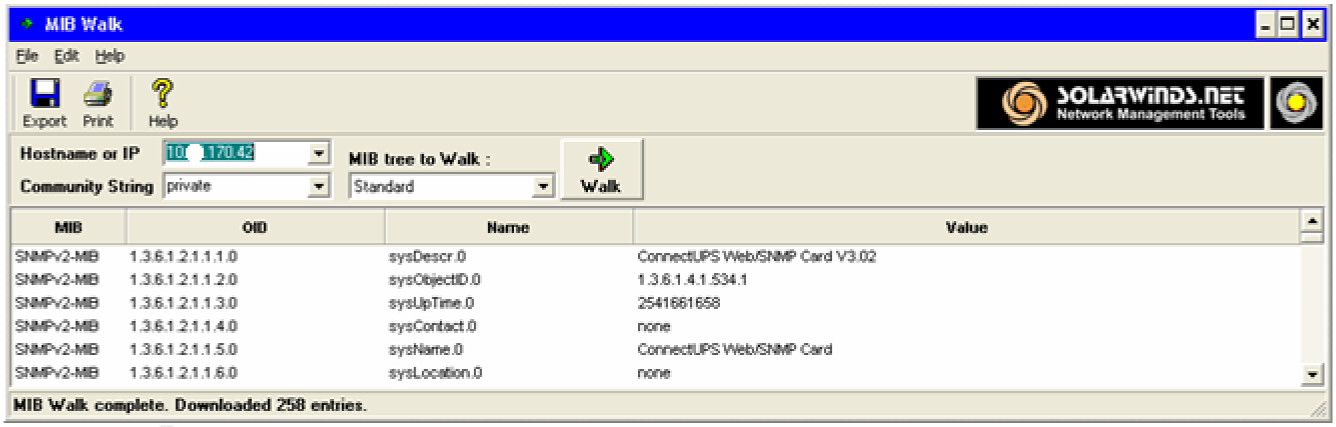
MIB IF-MIB
Name ifAdminStatus.65539

iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifAdminStatus.65539

OID 1.3.6.1.2.1.2.2.1.7.65539
Type INTEGER
Units

This sets the NIC to down but there is no evidence on the box that the NIC is down except I cannot ping it. The links are blinking on the back of the machine, the NICs show as up and enabled in the OS. There is no evidence of anything happening to the box in any of the logs. The box simply drops off the network. I spent sometime with the NT admin of this box as he tried to figure out what happened. The admin could not find any reason for it being down, he even opened a ticket with the network group to see what happened. The eventlogs showed no evidence of the box being off net, except the inability to get to a domain controller. The OS seemed to think the NICs were up and running.   With this box out of the picture I can now try DOS attacks on the calls without triggering alarms. If I were to attack the phones they would report to the VOIP manager that they were seeing degraded performance on calls. This might trigger additional interest in the environment that I don’t want right now.

The next portion of the PBX that needs attention is the UPS, each Avaya media server comes with a UPS that it is plugged into. If we were able to disable the UPS we could bring the server down (essentially unplugging the PBX remotely). The UPS is located on the control network but could be on any of the screened networks. It only needs to talk to the media server. The UPS ship with SNMP enabled and the R/W string set to private.   I run a MIB walk on the UPS and find the following:

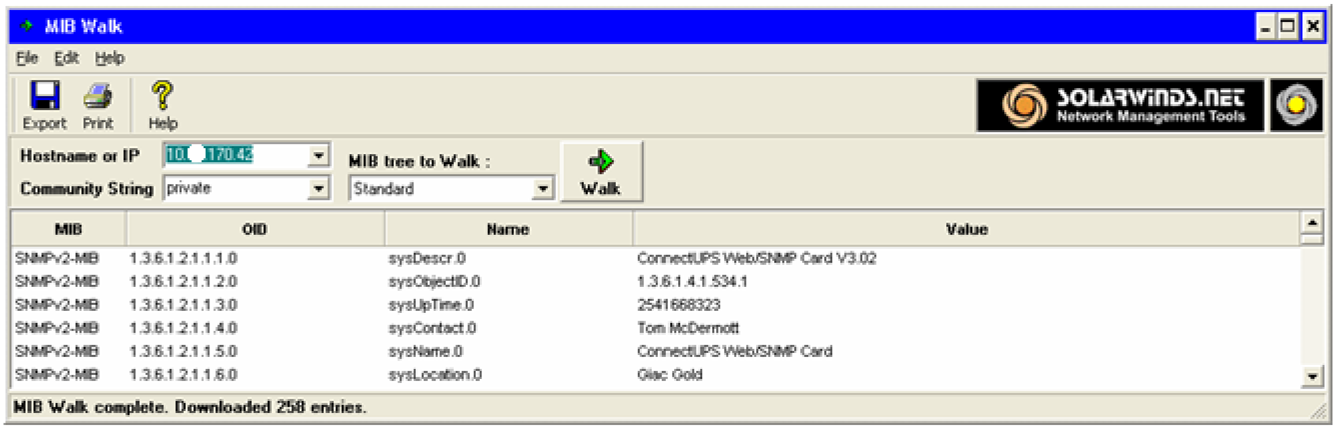


Hostname or IP: 10[redacted]170.42
Community String: private
MIB tree to Walk : Standard

MIB	OID	Name	Value
SNMPv2-MIB	1.3.6.1.2.1.1.1.0	sysDescr.0	ConnectUPS Web/SNMP Card V3.02
SNMPv2-MIB	1.3.6.1.2.1.1.2.0	sysObjectID.0	1.3.6.1.4.1.534.1
SNMPv2-MIB	1.3.6.1.2.1.1.3.0	sysUpTime.0	2541661658
SNMPv2-MIB	1.3.6.1.2.1.1.4.0	sysContact.0	none
SNMPv2-MIB	1.3.6.1.2.1.1.5.0	sysName.0	ConnectUPS Web/SNMP Card
SNMPv2-MIB	1.3.6.1.2.1.1.6.0	sysLocation.0	none

MIB Walk complete. Downloaded 258 entries.

I decide to validate this is the R/W string by doing an “update system MIB” from Solarwinds on this device. I change the system MIB to have my name as the contact and the location as giac gold. This change takes effect, I re-run the MIB walk and get the following results:



Hostname or IP: 10.[redacted]170.42
Community String: private
MIB tree to Walk : Standard

MIB	OID	Name	Value
SNMPv2-MIB	1.3.6.1.2.1.1.1.0	sysDescr.0	ConnectUPS Web/SNMP Card V3.02
SNMPv2-MIB	1.3.6.1.2.1.1.2.0	sysObjectID.0	1.3.6.1.4.1.534.1
SNMPv2-MIB	1.3.6.1.2.1.1.3.0	sysUpTime.0	2541668323
SNMPv2-MIB	1.3.6.1.2.1.1.4.0	sysContact.0	Tom McDermott
SNMPv2-MIB	1.3.6.1.2.1.1.5.0	sysName.0	ConnectUPS Web/SNMP Card
SNMPv2-MIB	1.3.6.1.2.1.1.6.0	sysLocation.0	Giac Gold

MIB Walk complete. Downloaded 258 entries.

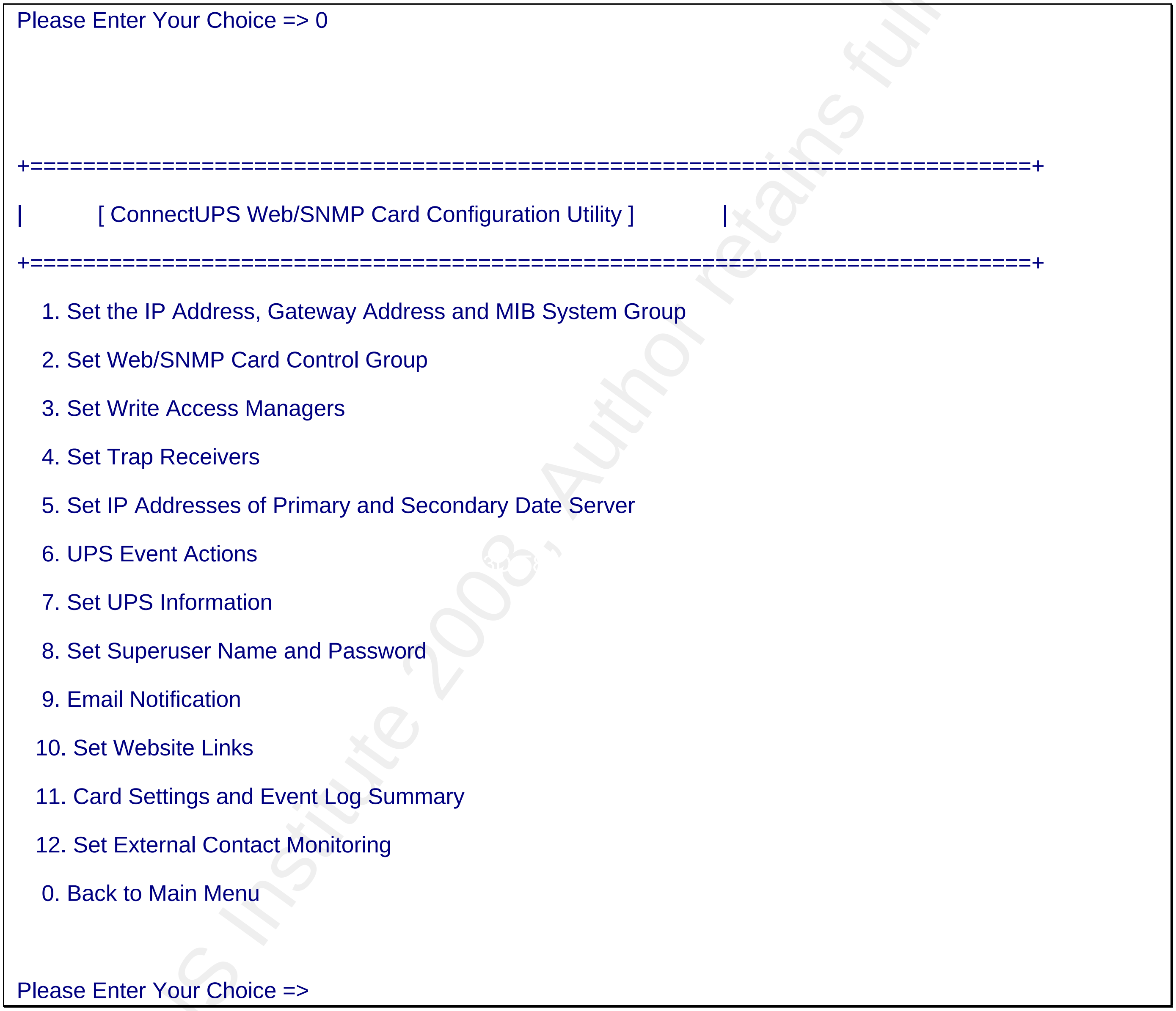
I could probably use the read-write string to shut down the UPS and bring down the servers but I cannot find the right OID to force the UPS down. I run a scan and see what other services are running.

```
C:\>nmap -sT -F  -v -sV 10.35.170.42



Starting Nmap 4.20 ( http://insecure.org ) at 2008-01-07 23:57 Eastern
Standard

Time

Initiating Parallel DNS resolution of 1 host. at 23:57

Completed Parallel DNS resolution of 1 host. at 23:57, 0.02s elapsed

Initiating Connect() Scan at 23:57

Scanning 10.35.170.42 [1256 ports]
```

```
Discovered open port 80/tcp on 10.35.170.42
Discovered open port 23/tcp on 10.35.170.42
Completed Connect() Scan at 23:59, 65.86s elapsed (1256 total ports)
Initiating Service scan at 23:59
Scanning 2 services on 10.35.170.42
Completed Service scan at 23:59, 6.03s elapsed (2 services on 1 host)
Host 10.35.170.42 appears to be up ... good.
Interesting ports on 10.35.170.42:
Not shown: 1249 filtered ports
PORT     STATE  SERVICE    VERSION
23/tcp   open   telnet     ConnectUPS Web/SNMP Card telnetd
80/tcp   open   http       Powerware ConnectUPS WEB/SNMP Card http config
(UPS_S
erver httpd 1.0)
Service Info: Device: power-device
Service detection performed. Please report any incorrect results at
http://insec
ure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 72.684 seconds
               Raw packets sent: 2 (68B) | Rcvd: 1 (46B)
```

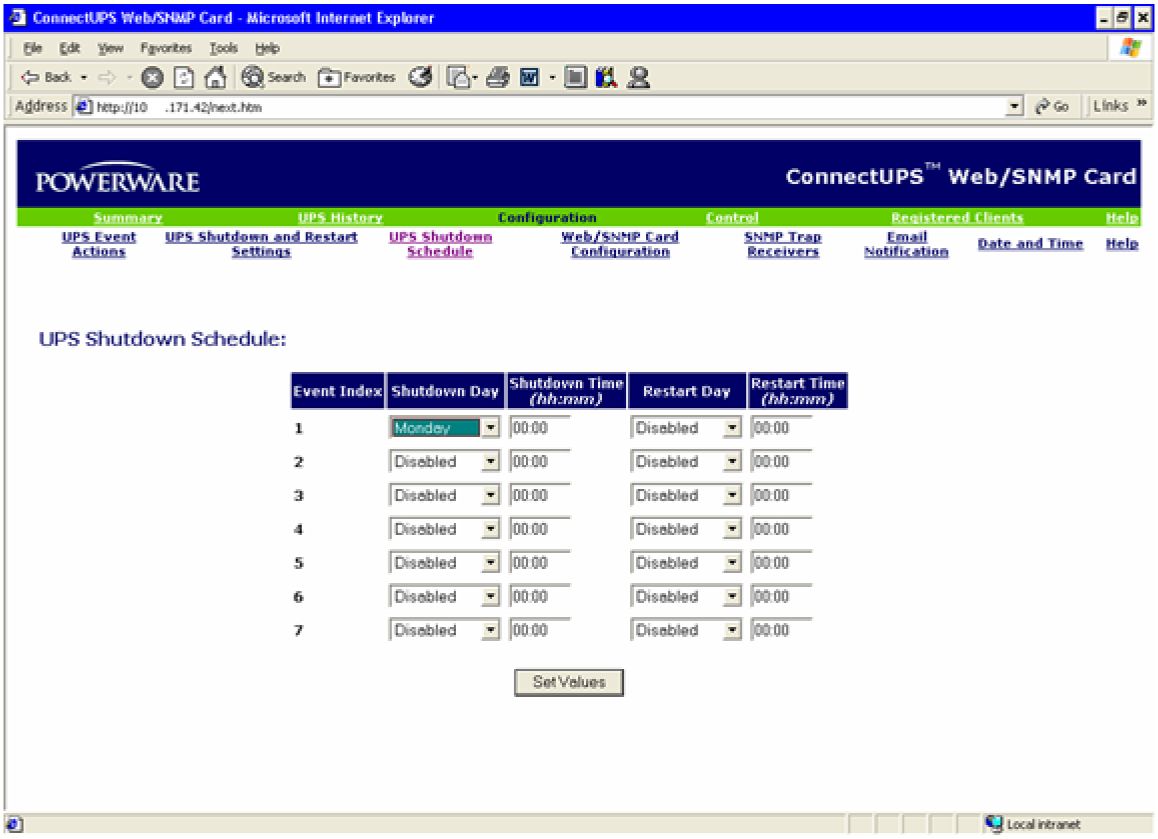
The scan reveals that there is a web server and telnet service running. The webserver displays a status and option to log in as super-user. I tried a few logins but cannot get into the device. I try telnet and I am curiously only asked for a password. I found the ConnectUPS Web/SNMP card user's guide on Google. In the install guide, the default password is “admin”.

I try this and it works. I am given the following menu:



```
Please Enter Your Choice => 0



+============================================================================+
|          [ ConnectUPS Web/SNMP Card Configuration Utility ]          |
+============================================================================+
   1. Set the IP Address, Gateway Address and MIB System Group
   2. Set Web/SNMP Card Control Group
   3. Set Write Access Managers
   4. Set Trap Receivers
   5. Set IP Addresses of Primary and Secondary Date Server
   6. UPS Event Actions
   7. Set UPS Information
   8. Set Superuser Name and Password
   9. Email Notification
  10. Set Website Links
  11. Card Settings and Event Log Summary
  12. Set External Contact Monitoring
   0. Back to Main Menu

Please Enter Your Choice =>
```

Immediately I setup the superuser name and password to get rid of the default password. This UPS is on the control network so the ACL implemented above would prevent this. However I am going to change the default strings for R/O and R/W strings. Additionally, I restrict the hosts that are allowed to communicate with these devices to the local network and the NMS station assigned to manage this device. Looking at the attached screenshot below you will see I can schedule a shutdown of the UPS, this would take down the primary brains of the PBX, I could even schedule it to come back up if I wanted to play mind games on the support staff. This is a critical vulnerability and needs to be immediately fixed. This will be fixed by changing the SNMP strings, creating a unique super user and screening the subnet this UPS resides on.


ConnectUPS Web/SNMP Card - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://10 .171.42/next.htm
Go Links
POWERWARE
ConnectUPS™ Web/SNMP Card
Summary UPS History Configuration Control Registered Clients Help
UPS Event Actions
UPS Shutdown and Restart Settings
UPS Shutdown Schedule
Web/SNMP Card Configuration
SNMP Trap Receivers
Email Notification
Date and Time
Help
Local intranet

UPS Shutdown Schedule:

Event Index	Shutdown Day	Shutdown Time (hh:mm)	Restart Day	Restart Time (hh:mm)
1	Monday	00:00	Disabled	00:00
2	Disabled	00:00	Disabled	00:00
3	Disabled	00:00	Disabled	00:00
4	Disabled	00:00	Disabled	00:00
5	Disabled	00:00	Disabled	00:00
6	Disabled	00:00	Disabled	00:00
7	Disabled	00:00	Disabled	00:00

Set Values

Security Recommendations for the ESS world

This portion of the document will attempt to list some of the architectural considerations for the deployment of ESS. It is important for an enterprise to properly secure any technology going through a transition from an isolated secure system to a fully distributed enterprise class computer system. All major PBX vendors are pushing this architecture moving forward. These systems process significant amounts of personal data. Think about the last time you called a credit card company, the IVR collected your phone number and account number at a minimum, prior to live transfer. This information will now be passed across the enterprise network and must be secured.

The Avaya components of the PBX are very secure. Each of the devices has significant safeguards to prevent hacking. The original Medpro boards were relatively easy to overwhelm with traffic. The current iteration, the crossfire boards, can withstand very aggressive DOS attacks. I was not able to even make a dent in the ability of the crossfire medpro to do it s job, with SYN attacks or straight packet attacks. Similar safeguards are built into the C-LANs and the IPSIs. The newer PBX components are very secure. I have outlined these components below.

Media Servers (SPE)

The media servers based on Linux use the built-in firewall ability to restrict access to the appropriate partitions and services. Additionally, it is very resistant to Denial of Service attacks. The servers also have the following features:

- One time password for Avaya support personnel
- Shell access is severely restricted
- Root access is not allowed directly for any account
- Secure services are provided for support, FTP is available but off by default and must be enabled each time it is used (it times out after 15 minutes of inactivity)
- Tripwire and account logging are active for audit putposes
- No file shares or mail services are available on the media server so virus and worm issues are non existent.

The circuit packs that make up the primary components of the PBX also have significant protections against attacks. The three main components are IPSI, C-LAN and Medpro.

IPSI

- FTP is enabled for firmware upgrades but is controlled via the communications manager software. It is enabled only when required. If there is no activity the service times out and is shutdown.
- Control traffic is encrypted between IPSI and Media Servers

Medpros

- Medpros will only establish audio streams if they have received a corresponding control stream
- The Medpro is a proprietary OS and is not connected directly to the Media Servers
- The Medpros are very resilient and are not susceptible to DOS attacks

C-LANS

- Independent of the Media Gateway
- No IP link back to the admin process of the Media Servers

- Built-in DOS attack safeguards that are built to repel most Synfloods tools

The PBX components are not the only portions of the IP telephony architecture. These may be secure but they depend other resources to provide full functionality to the enterprise. The overall design of the IP telephony solution extends past the edge of the PBX and into the adjuncts that support it. This is where the risk to the organization lies. The possible weaknesses are in the following areas:

1. Design Mistakes

2. Adjunct server weaknesses

3. Legacy hardware

I will discuss each of these in the context of the GCFW certification. Each area will be discussed include recommended countermeasures.

Design Mistakes

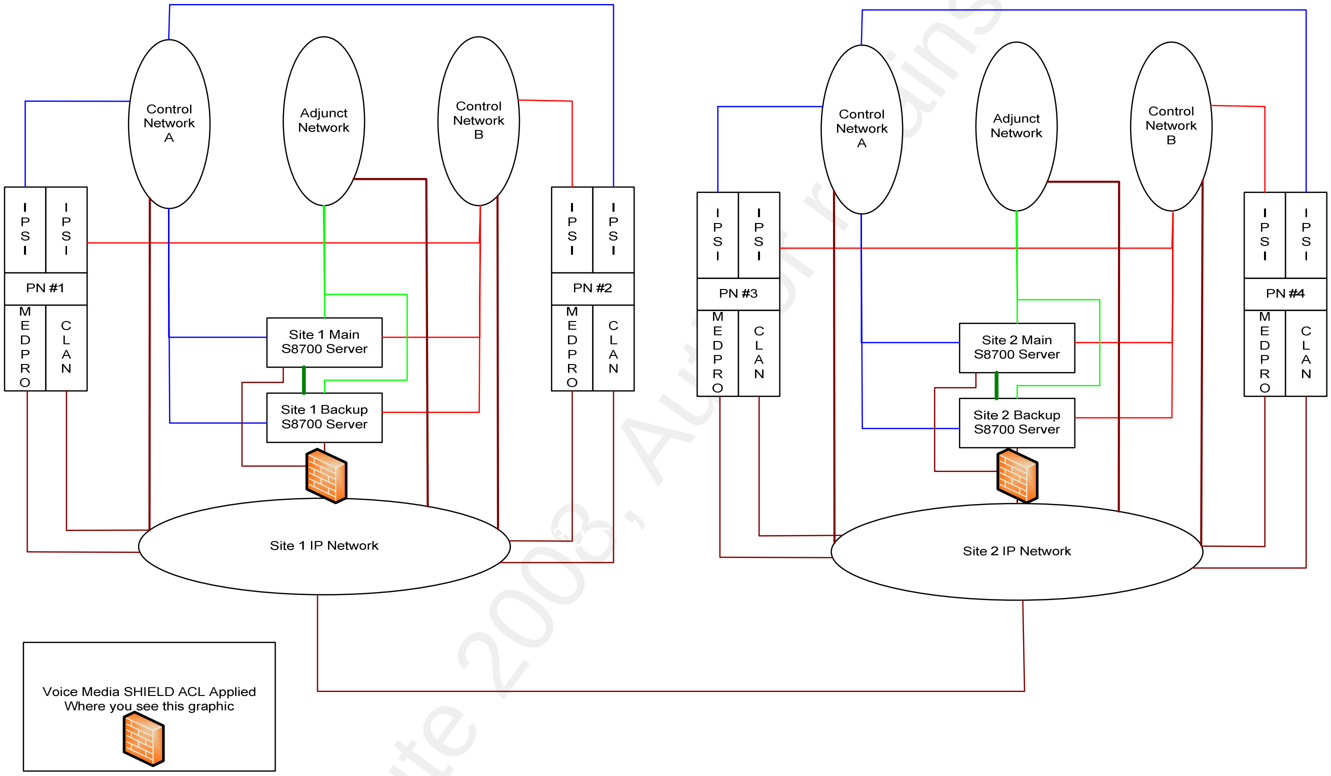
The primary objective of the ESS environment is to allow the enterprise to share a common configuration file and shared adjuncts. Allowing full "IP any" access will allow this to be accomplished; however is not best practice for this configuration. I want to restrict the access to the various supporting networks as much as possible. This would eliminate the ability to easily map the entire PBX. as well as make planning an attack against the PBX very difficult.

Recommendation #1 - The media servers should be screened from the IP network, allowing only required traffic to pass

All of the components in the PBX validate that the primary servers are available every minute. If malicious traffic were able to reach the server and take it down, the entire enterprise would be impacted as the entire PBX would reconverge. This is the single most important component of the PBX and must be protected. Avaya has built in many layers of defense: Hardened OS and Tripwire are the most important. To supplement this I will add IDS (covered below), and screen the IP address of the Media servers in the network to allow only the following communication:

- all the media servers and media gateways to communicate with the each other
- administrative access from support personnel (Via FTP, FTP Data, SSH and port 5022)
- all IPSIs in the enterprise must be able to communicate with all media servers

- deny any other access to the media servers



ip access-list extended Voice Media Shield

```
Permit  IP host 10.32.31.40  host 10.35.160.211

Permit  IP host 10.15.160.211 host 10.35.160.211

Permit  IP host 10.15.160.212  host 10.35.160.211
```

```
 Permit  IP host 10.7.160.211 host 10.35.160.211

 Permit  IP host 10.7.160.212 host 10.35.160.211

Permit  IP host 10.32.31.40  host 10.35.160.2112

 Permit  IP host 10.15.160.211 host 10.35.160.212

 Permit  IP host 10.15.160.212  host 10.35.160.212

 Permit  IP host 10.7.160.211 host 10.35.160.212

 Permit  IP host 10.7.160.212 host 10.35.160.212

# The above are media servers, there would be one entry for each ESS / LSP server

Permit IP 10.X.170.0 255.255.255.0 host 10.35.160.211

Permit IP 10.X.171.0 255.255.255.0 host 10.35.160.212

# there would be one for each control network as well

Permit TCP any host 10.35.160.212 eq 80

Permit TCP any host 10.35.160.212 range 20-22
Permit TCP any host 10.35.160.212 5022

deny   ip any  host 10.35.160.211 log-input

deny   ip any host 10.35.160.212 log-input

# This denies anything not allowed to the media servers

permit ip any any

# The final permit is because the media server is not alone on the segment
```

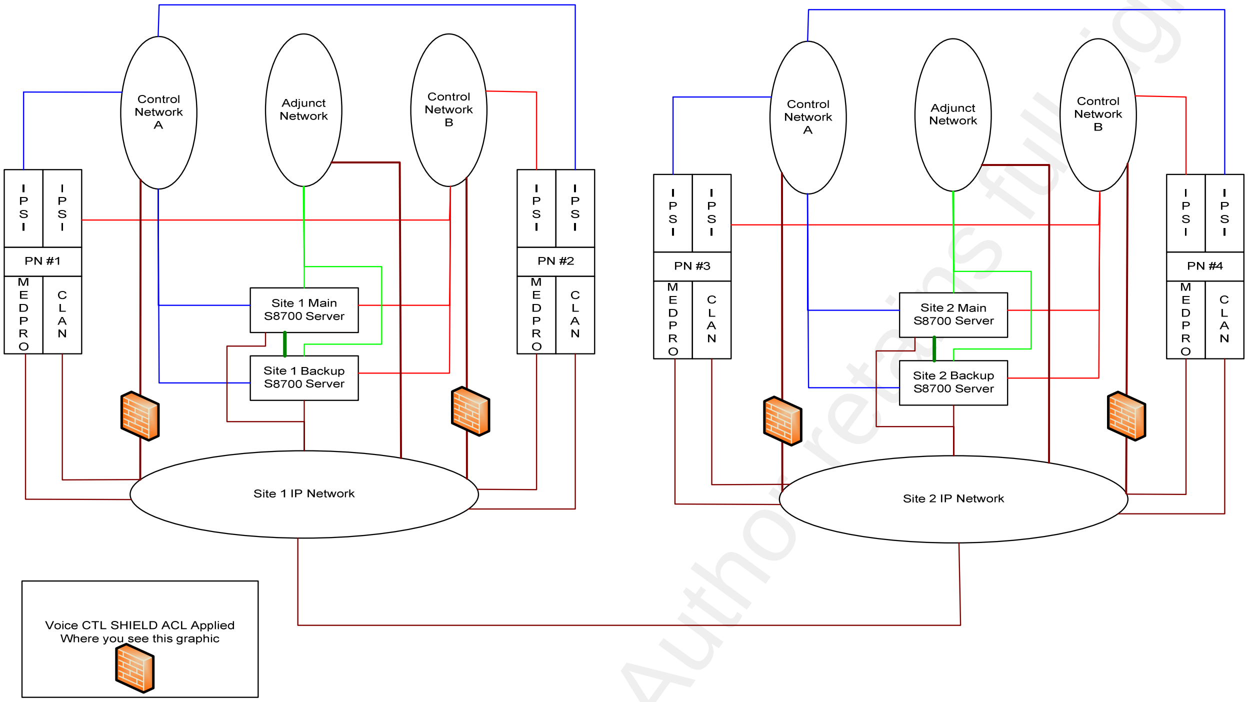
Recommendation #2 - The control networks should be screened to allow only the Media Servers (SPE) to see the control networks.

I will only allow the media servers to have access to the IPSIs in any site.   This permits the call control to flow across the enterprise without interruption from denial of service attacks and prevent enumeration.

The following ACL will be applied to all control networks in the organization. There is a finite list of media servers in the enterprise so this will remain a short list.

```
ip access-list extended Voice CTL Shield

 Permit  tcp host 10.32.31.40 any range 5010-5012

 Permit  tcp host 10.15.160.211 any range 5010-5012

 Permit  tcp host 10.15.160.212 any range 5010-5012

 Permit  tcp host 10.15.160.212 any range 5010-5012

 Permit  tcp host 10.7.160.211 any range 5010-5012

 Permit  tcp host 10.7.160.212 any range 5010-5012

 deny   ip any any log-input
```

This acl should be applied as an outbound access group on the control VLANs. This will eliminate all non-essential traffic to the control network. When new ESS servers are added this list will have to be adjusted to include those servers.



Recommendation #3- The adjunct networks should be restricted to only speak to other adjunct networks in each location. .

This will allow a private network for CTI integration, call recording and other adjuncts that need to communicate to the servers. In this case, the CTI servers have a public network interface card (nic) used to speak to the IP telephony applications while communicating on a nic attached to a private network connecting the integration points of the PBX.

The following ACL should be applied

```
ip access-list extended Adjunct CTL Shield

Permit  IP 10.32.31.0 255.255.255.0 any

Permit  IP 10.35.160 255.255.250.0 any

Permit  IP 10.7.160 255.255.250.0 any

Permit  IP 10.15.160 255.255.250.0 any

# this allows anything on the Voice range to get to the adjunct network

# there would be one entry for each site’s voice networks

deny   ip any any log-input
```

Recommendation #4 -C-LAN registration points should be segmented by function. IP endpoints should not register with C-LANs that do Back-end communications

The registration points to the network should be separated into 2 zones. This will allow the PBX to keep primary communications with critical system separate. The C-LANS for adjunct support would be hidden from the enterprise network users. This would enable crucial back-end communications to remain invisible and secure from the general public. I must publish the registration points for the IP phones but I do not have to allow access to the other C-LANs. For Example, the primary PBX location has 12 C-LAN cards and should be segmented in the following zones:

IP Phone registration Zone (Enterprise IP Network):
10.35.160.30, 10.35.160.31, 10.35.160.32, 10.35.160.33 10.35.161.30, 10.35.161.31

Adjunct support Zone (10.X.164.0/24 network):
10.35.164.20, 10.35.164.21, 10.35.164.22, 10.35.164.23, 10.35.164.142, 10.35.164.24, 10.35.164.25

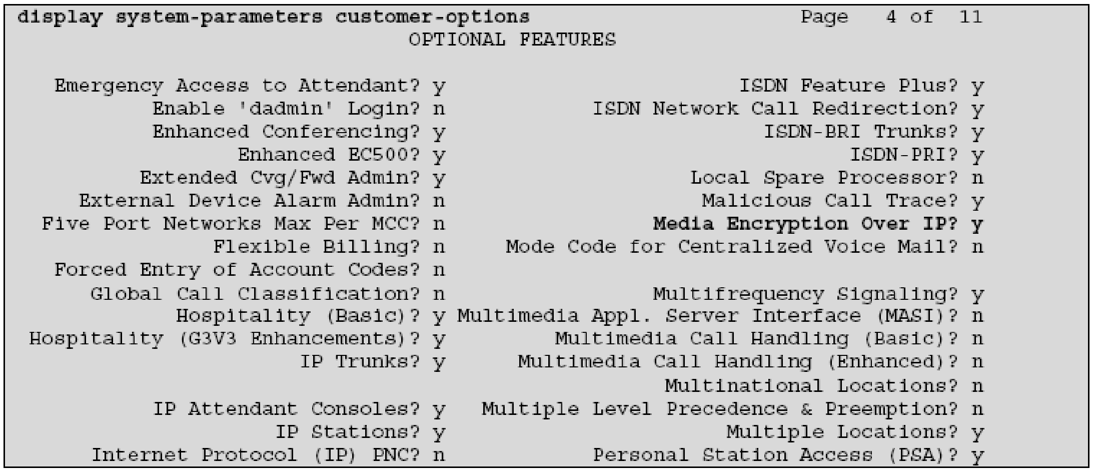
Recommendation #5 - Encryption should be enabled on all functions to limit the capabilities to eavesdrop on the network.

If the communication across the enterprise network is not encrypted a simple sniffer could become a recording / eavesdropping device as unencrypted media streams can be replayed. The function of encryption is enforced by a codec set (defined communication parameters). The definition of a codec set is done at the Media server level (S87XX).

Depending on how the call will route and what the end-point will support determines the selection of the codec.   I also must consider the backend control network and whether or not to encrypt the traffic between server and IPSI. My recommendation is that the PBX encrypts all control and voice traffic. Without encryption on an audio stream it is relatively easy to eavesdrop on the phones. A simple sniffer trace will be enough to listen to the call if you capture the RTP stream. Encryption is enabled on a network region (group of pbx assets that share a common network region number) basis. This is done via the following steps in the PBX.

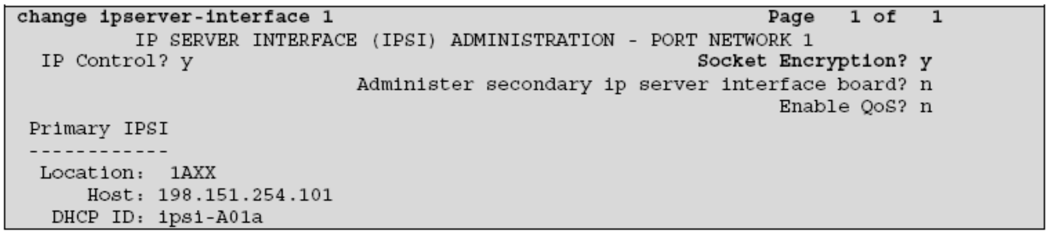
The IP Encryption license must be installed and active. The screen shots in the following section were taken from an Avaya Solution & Interoperability Test Lab Application Note - Configuring Avaya Communication Manager for Media Encryption – Issue 1.0 (http://www.Avaya.com/master-usa/en-us/resource/assets/applicationnotes/media-encrypt.pdf) and do not use the same configuration as the model PBX in this paper. This section is meant as a tutorial on how to setup the encryption.

The following screen shows an example of turning on the IP Encryption:



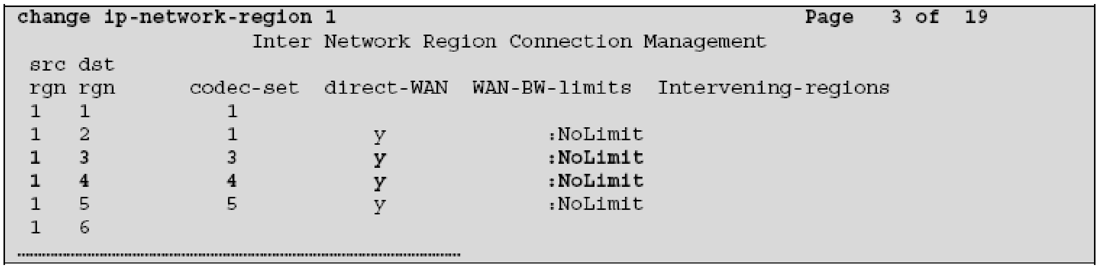
```
display system-parameters customer-options                         Page   4 of  11
                                 OPTIONAL FEATURES

   Emergency Access to Attendant? y                      ISDN Feature Plus? y
           Enable 'dadmin' Login? n            ISDN Network Call Redirection? y
           Enhanced Conferencing? y                         ISDN-BRI Trunks? y
                  Enhanced EC500? y                                ISDN-PRI? y
          Extended Cvg/Fwd Admin? y                   Local Spare Processor? n
     External Device Alarm Admin? n                     Malicious Call Trace? y
  Five Port Networks Max Per MCC? n                 Media Encryption Over IP? y
                Flexible Billing? n     Mode Code for Centralized Voice Mail? n
   Forced Entry of Account Codes? n
      Global Call Classification? n                 Multifrequency Signaling? y
             Hospitality (Basic)? y Multimedia Appl. Server Interface (MASI)? n
 Hospitality (G3V3 Enhancements)? y        Multimedia Call Handling (Basic)? n
                     IP Trunks? y      Multimedia Call Handling (Enhanced)? n
                                                 Multinational Locations? n
           IP Attendant Consoles? y   Multiple Level Precedence & Preemption? n
                     IP Stations? y                      Multiple Locations? y
      Internet Protocol (IP) PNC? n            Personal Station Access (PSA)? y
```

Once the IP encryption is turned on, I need to get into each IPSI's configuration and turn on the encryption for the IP traffic back to the Media Server (S87XX). The menu option below is where I turn this on:



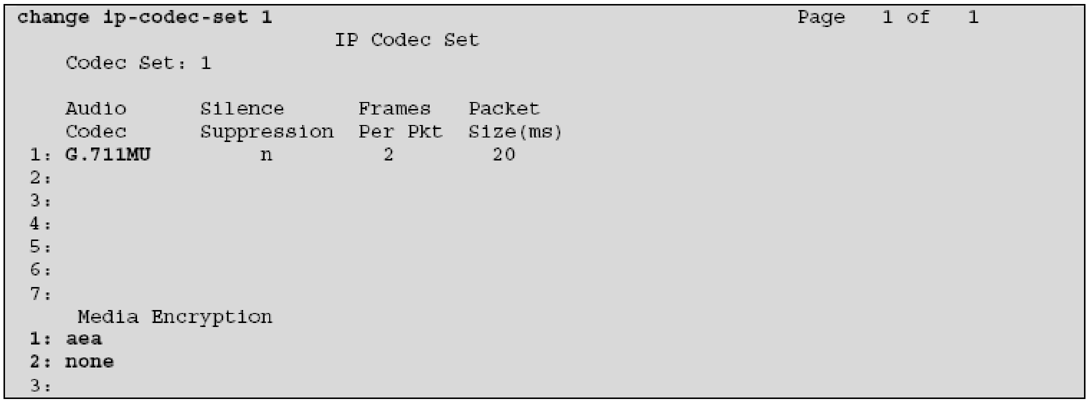
```
change ipserver-interface 1                                   Page   1 of   1
         IP SERVER INTERFACE (IPSI) ADMINISTRATION - PORT NETWORK 1
  IP Control? y                                         Socket Encryption? y
                            Administer secondary ip server interface board? n
                                                                Enable QoS? n
 Primary IPSI
 ------------
  Location:  1AXX
      Host: 198.151.254.101
   DHCP ID: ipsi-A01a
```

This completes the implementation of encryption on the control networks within my PBX. Now I need to move onto the codec sets for the voice traffic. There are several current codecs that Avaya supports G.711, G729 and G722 (96XX phones only). Avaya also supports AES encryption on each of these codecs. The selection of the codec set is made based upon the endpoints capabilities, the available options defined, the route of the call and the preference of the system. When setting the codec in a port network region on the PBX I must define this.



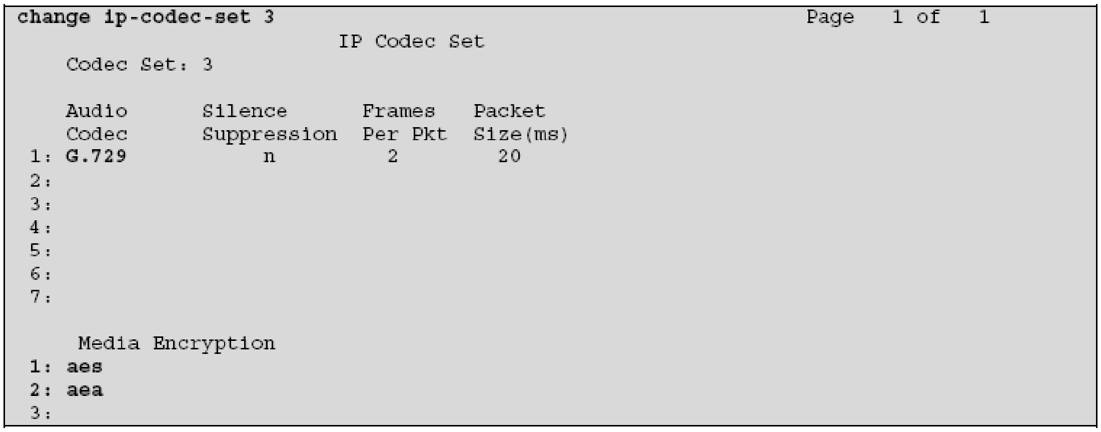
```
change ip-network-region 1                                      Page   3 of  19
                    Inter Network Region Connection Management
 src dst
 rgn rgn      codec-set  direct-WAN  WAN-BW-limits  Intervening-regions
 1   1          1
 1   2          1           y             :NoLimit
 1   3          3           y             :NoLimit
 1   4          4           y             :NoLimit
 1   5          5           y             :NoLimit
 1   6
```

In the table above I see the Source (SRC) Region and the Destination (DST) Regions listed with applicable Codec-Set defined. This will define what are the available codecs to use in this path. Intra network region calls are also defined here. The next graphic represents the first codec set – 1.



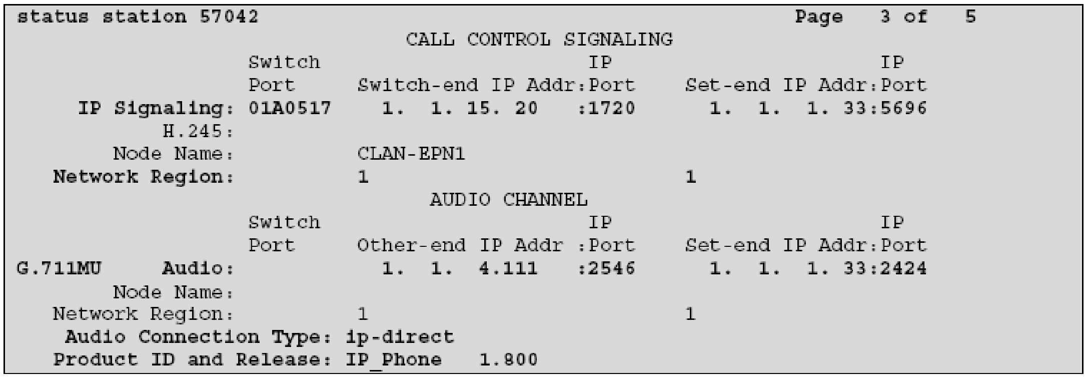
```
change ip-codec-set 1                                           Page   1 of   1
                              IP Codec Set
    Codec Set: 1

    Audio      Silence      Frames   Packet
    Codec      Suppression  Per Pkt  Size(ms)
 1: G.711MU         n          2        20
 2:
 3:
 4:
 5:
 6:
 7:
     Media Encryption
 1: aea
 2: none
 3:
```

In this case the codec used is G.711MU. The G.711 codec is a less compressed codec used on local networks. There are 2 options defined for encryption, AEA and none. The phone allows a call to complete if the other endpoint is unable to encrypt. AEA is Avaya Encryption Algorithm AEA uses a 104-bit key, and has the attractive characteristic that using AEA has no effect on the capacity of the various resources.   AEA is a pre-standard encryption algorithm that Avaya utilized in older installations. The next Codec to review is Codec-Set 3. This codec is used when a call goes from network region 1 to network region 3 (or vice versa).



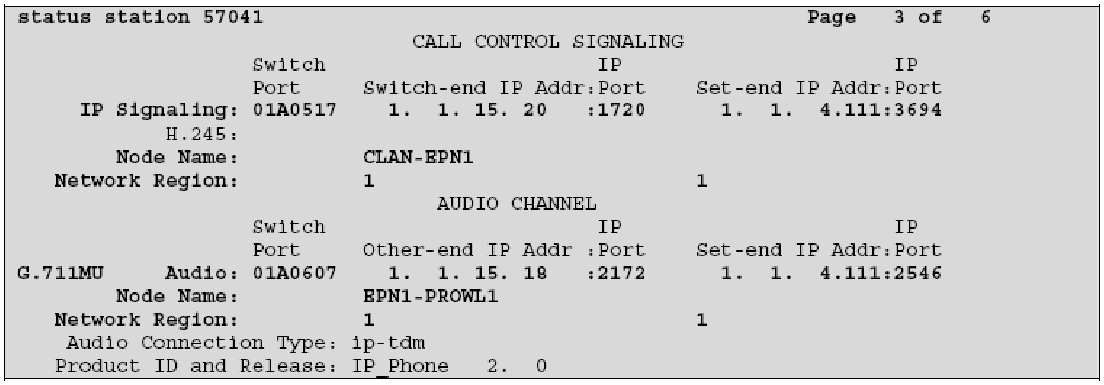
```
change ip-codec-set 3                                          Page   1 of   1
                          IP Codec Set
    Codec Set: 3

    Audio      Silence      Frames   Packet
    Codec      Suppression  Per Pkt  Size(ms)
 1: G.729           n         2        20
 2:
 3:
 4:
 5:
 6:
 7:

     Media Encryption
 1: aes
 2: aea
 3:
```

In this case the system requires encryption; there is no option for none. This is because this call will cross a WAN link and the system designers chose to require encryption. The first choice is AES encryption, the second being AEA if the devices are not AES capable.



```
status station 57042                                      Page   3 of   5
                                   CALL CONTROL SIGNALING
                   Switch                    IP                      IP
                   Port     Switch-end IP Addr:Port    Set-end IP Addr:Port
     IP Signaling: 01A0517    1.  1. 15. 20   :1720      1.  1.  1. 33:5696
            H.245:
        Node Name:          CLAN-EPN1
   Network Region:          1                          1
                                     AUDIO CHANNEL
                   Switch                    IP                      IP
                   Port     Other-end IP Addr :Port    Set-end IP Addr:Port
G.711MU     Audio:            1.  1.  4.111   :2546      1.  1.  1. 33:2424
        Node Name:
   Network Region:          1                          1
    Audio Connection Type: ip-direct
   Product ID and Release: IP_Phone    1.800
```

The above graphic shows a call in progress with the G.711 MU codec in use. This call is an intra network region call so Codec-set 1 is used. The graphic below shows an intra network region call that goes to a TDM phone, again you see it is using the proper codec but the second endpoint of the call is a TDM phone (audio connection type) so a medpro resource is doing the IP to TDM conversion. The IP stream is encrypted.



```
status station 57041                                      Page   3 of   6
                                   CALL CONTROL SIGNALING
                   Switch                    IP                      IP
                   Port     Switch-end IP Addr:Port    Set-end IP Addr:Port
     IP Signaling: 01A0517    1.  1. 15. 20   :1720      1.  1.  4.111:3694
            H.245:
        Node Name:          CLAN-EPN1
   Network Region:          1                          1
                                     AUDIO CHANNEL
                   Switch                    IP                      IP
                   Port     Other-end IP Addr :Port    Set-end IP Addr:Port
G.711MU     Audio: 01A0607    1.  1. 15. 18   :2172      1.  1.  4.111:2546
        Node Name:          EPN1-PROWL1
   Network Region:          1                          1
    Audio Connection Type: ip-tdm
   Product ID and Release: IP_Phone    2.  0
```

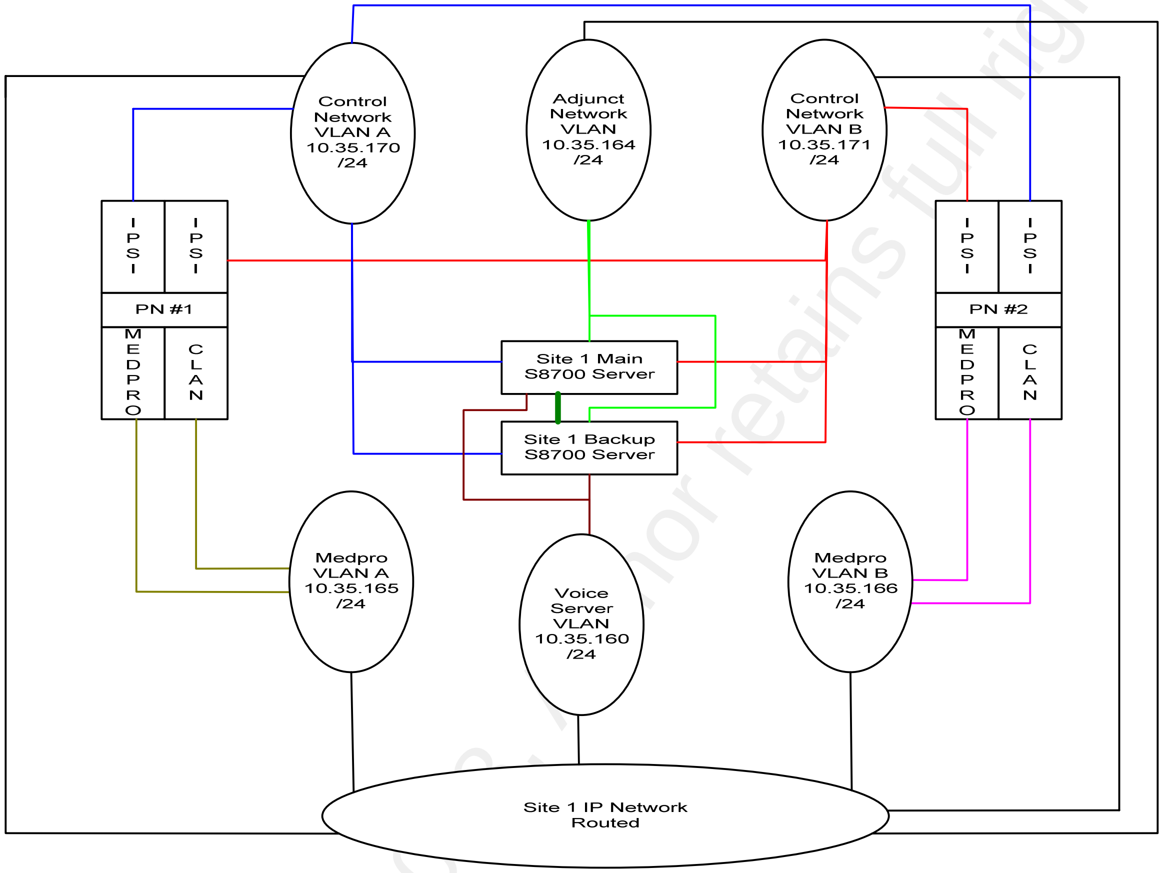
Recommendation #6 - Unnecessary services should be disabled on all devices, where disabling the service is not an option network screening should be implemented

Server comes with TELNET, SSH, HTTP, HTTPS enabled as administrative options. The use of telnet should be eliminated and replaced with SSH. This can be accomplished quickly with an ACL on the VLAN with the administrative interface. I can also turn this off at the media switch (SPE). The most common administrative option for an Avaya PBX is Avaya Site Administrator. This tool puts a GUI on the administration tool. It connects using telnet (port 5023) or SSH (port 5022) on the back side. The recommendation is that all administration be done via SSH or SSL as the other protocols are clear text and subject to sniffer attacks.

SNMP should be highly restricted and should be actively scanned to make sure no information leakage occurs. This can be enforced by ACL but it is best practice to change the default strings as well. This is an example of a defense in depth strategy.

Recommendation #7- IDS Technology should be deployed in front of the PBX and all adjuncts

The deployment of IDS probes in front of the PBX would allow an enterprise to monitor any probe of the VOIP network. The introduction of softphones (phones that run as an application on a computer) has reduced the ability to firewall the PBX from everything that is not on the voice vlans. The IDS will need to be tuned to filter out the expected traffic. The IDS sensors should be placed behind the ACLs (when applicable) so false positives will not be generated. As the company moves to SIP as a solution, we will have to closely monitor these servers as well. In the diagram below we see that there are six critical VLANs that require IDS monitoring. We have one Cisco 4260 IDS available for implementation; this device has 4 monitoring ports available. These VLANs reside on 3 different Cisco switches so we are going to have to monitor this with multiple VLANs span into some ports. Port 1 will monitor VLANs 164, 165, and 170 as they are one Cisco Switch. We do not anticipate much traffic on 164 and 170 because they will be protected by a very restrictive ACL. Port 2 will monitor VLAN 166 and 171. VLAN 171 should not see a lot of traffic because the ACL recommended above will be in place. Port 3 will monitor VLAN 160 which is the public nic of the PBX. This VLAN will see a lot of traffic.


Control Network VLAN A 10.35.170 /24
Adjunct Network VLAN 10.35.164 /24
Control Network VLAN B 10.35.171 /24
IPSI
IPSI
PN #1
MEDPRO
CLAN
IPSI
IPSI
PN #2
MEDPRO
CLAN
Site 1 Main S8700 Server
Site 1 Backup S8700 Server
Medpro VLAN A 10.35.165 /24
Voice Server VLAN 10.35.160 /24
Medpro VLAN B 10.35.166 /24
Site 1 IP Network Routed

Adjunct server weaknesses

The biggest weaknesses discovered were in the servers that support the IP telephony environment. This is because traditionally, these servers were treated differently. They may have even been supplied and/or installed by the vendor. If I ever want to disrupt the PBX, this would be my first attack vector. These servers must be treated with the same techniques as any high priority server in the enterprise. They must be hardened and secured.

Recommendation #8 - Remove any unneeded service

In Avaya's default implementation of Modular messaging (voice mail) there is a default webserver running, with an under construction page as the index. I found VNC running on another machine for remote support. Each adjunct server must be reviewed with port scans and a vulnerability scanner to ensure it is locked down. This review must be repeated for all servers in the PBX environment.

Recommendation #9 - SNMP must be removed or restricted

SNMP is a very powerful network management tool. Used properly, I can manage and support a VOIP environment very well. In my experience, SNMP is rarely used properly in the VOIP world. I have found default read/only and read/write strings installed and responsive on the central components of the PBX. Avaya does a good job limiting the damage you can do with this information but if it is not being used it should be removed, if it is being used it should be restricted by changing the strings, implementing ACLs (network and host) and finally using Version 3 for encryption.

Recommendation #10 - Host based firewalls / tripwire must be installed on all critical servers

The VOIP environment is still relatively immature. Avaya just stopped using tftp to distribute the phone settings and software upgrades to the phones. It now uses HTTP to do this. This is a step in the right direction but I must secure these files from tampering. As seen in the previous section, the 46xxsettings file is a high value target.

The first server that will be targeted for tripwire is the distribution server for the phone settings file. We monitor the home directory of the Avaya home page of the apache server. In this case, e:\program files\Avaya\home page\html. Any change to this directory will result in an alert sent to tripwire's management console as seen below

```
Modified:
E:\Program Files\Avaya\Home Page\html\96xxupgrade.txt
```

The next step in protecting this server will be the installation of a host based intrusion prevention package. The enterprise standard is McAfee McHIP software. We need to protect the web server on this machine against any web based attacks because of the presence of the webserver for software distribution.

The servers needs to be audited for MS patch levels and virus dat file levels.

Recommendation #11 - Default Password must be changed on all devices on the PBX.

This is illustrated by the section above where the UPS was mis-configured and I was able to shut it down. A good vulnerability scanning tool like Retina from e-eye digital should be used on all PBX components.

Legacy hardware

Recommendation #12 - Each of the components of the PBX has a software component that requires revisions that must be kept up to date.

The traditional PBX was isolated and the support mentality was “if it isn’t broke why fix it?”. The opening of the PBX to the enterprise makes this notion obsolete and dangerous. A company must implement an aggressive patch schedule. Avaya now offers this as part of the support contracts. If you call in a ticket, you are always told to upgrade to the latest rev anyway. I have implemented an aggressive upgrade program to update all components of the PBX, including the phones. Before this upgrade program was implemented, some phones were running code that was 5 years old. I currently require the PBX components to be upgraded once a quarter.

Recommendation #13 - Older technology should be replaced as significant technical and security advances have been made in the PBX world. If we can’t replace them we should protect them with ACLs.

There are some older technologies that are in place in most PBXs that have evolved over time. A Greenfield install (new install from scratch) might not have this exposure but PBXs with a longer history will probably have some equipment that is older. Avaya made the wise business and marketing decision to make the new S87XX technology backwards compatible with the older G3 cabinet technology. This means some of the older interfaces to the IP network are still supported. Here are a couple of examples:

Crossfire Medpros are significantly more resilient in the face of a DOS attack than thier older counterparts. I was able to take one of the older ones offline with about 45Mb of traffic from a single source. The investment in an upgrade is significant but in the long run it has a short ROI. One Crossfire can replace 4 older Medpros, so the maintenance bill will be reduced and you cabinet space significantly reduced.

MAP-D boards – these were the bolt on interface to the G3 series of PBXs to support interfaces to the IP telephony world. CTI technology is a prime example of this but recording is another. If you needed to provide the information collected in the IVR (Interactive Voice Response) to a customer service rep so they could be ready to service the caller, you need to feed this information out to the systems via the mapd boards. The MAP-D boards are technically being replaced by C-LANs, the AES server will be replacing the CTI server function. The map-d board was designed to sit on the old private network and never be exposed to the outside world. When our PBX was moved to the ESS world, this was exposed. There are many services listening on the box. These are not configured to respond but they do accept connections which may make it still vulnerable to attack. This needs to be replaced with the hardened AES servers and C-LANs. Replacing an older piece of equipment is never an easy task, especially in the Telephony world where you may have a situation where no one understands it so no one wants to touch it. In this case we need to place an ACL in front of it to only allow it to speak to what is supposed to speak to.

Conclusion

The security concerns associated with an ESS installation are manageable. Planning security upfront is very important as with any project, however even if this step is skipped, it can be managed. Understanding the architecture of any enterprise solution is extremely important. The biggest concern with VOIP in general and ESS specifically is the cross discipline nature of the solution. The backend architecture of the solution is more IP than telephony so the knowledge of a traditional PBX engineer is not really applicable. Avaya also takes a lead role in the installation of the PBX. This can be very advantageous for the speed of install, but for long term supportability this can result in significant gaps in knowledge. Additionally, Avaya does not take responsibility for the support of the adjunct applications like CTI based call center applications. The lesson here is the technology has converged; the design, engineering and support organizations must converge as well.

Examples:

46xxsettings.txt Changes

```
##############  APPLICATION ACCESS SETTINGS  ###############
## These settings restrict access to certain applications.
## APPSTAT is not supported on 96xx SIP phones.
##   When APPSTAT is set to 0, Call Log and Redial are
##   suppressed and changes to Speed Dial/Contacts are not allowed.
##
##   When APPSTAT is set to 1, Call Log, Redial and,
##   Speed Dial/Contacts work without restrictions.
##
##   When APPSTAT is set to 2, Call Log is suppressed.
##   For Redial the Last-6-numbers option is suppressed
##   and changes to Speed Dial/Contacts are not allowed.
##
##   When APPSTAT is set to 3, changes to Speed Dial/Contacts
##   are not allowed.
##
SET APPSTAT 1

#################  OPTION ACCESS SETTINGS  #################
##
## This setting restricts access to certain user options.
## OPSTAT is not supported on 96xx SIP phones.
##
```

```
##   When OPSTAT is set to 000, the user options  are not accessible.
##   When OPSTAT is set to 001, the user can only access the Log-Off Option.
##   When OPSTAT is set to 010, the user can only access  view-only options. The
##   user cannot change any setting.
##   When OPSTAT is set to 011, the user can only access
##   view-only options and the Log-Off Option.
##   When OPSTAT is set to 100, the user can access
##   all options except the view-only options and the Log-Off option.
##  When OPSTAT is set to 101, the user can access
##   all options except the view-only options.
##   When OPSTAT is set to 110, the user can access
##   all the options except the Log-Off option.
##  When OPSTAT is set to 111, the user can invoke any or all of the user options.
SET OPSTAT 111

##   A list of one or more HTTP proxy server exception
##   domains separated by commas without any spaces.
##   Accesses to these addresses will not go through the
##   proxy server.
SET WMLEXCEPT 10.32.100.107

## SNMP community name string
##   This value must be set to enable viewing of the phone's
##   MIB. This value must match the community string name
##   used in the SNMP query (up to 32 ASCII characters, no
##   spaces).
SET SNMPSTRING testread
```

```
## LOGLOCAL is not supported on 96xx SIP phones.
##     0 for disabled
##     1 for emergencies
##     2 for alerts
##     3 for critical
##     4 for errors
##     5 for warnings
##     6 for notices
##     7 for information
##     8 for debug
SET LOGLOCAL 7
##
## Syslog Server address
##   One syslog server IP address in dotted-decimal or DNS
##   name format (0 to 255 ASCII characters).
SET LOGSRVR 10.32.75.199

##
SET WMLHOME http://10.32.100.107/hello.wml
SET WMLIDLEURI http://10.32.100.107/helloscr.wml
```

Appendix A – Avaya Component Details

Media Servers

S8300

The S8300 Media Server can be configured in two modes: Internal Call Control (ICC) where the S8300 acts as a standalone PBX or in Local Survivable Processor (LSP) mode where it is subtended to another server. The S8300 runs the Linux operating system and can support up to 450 stations and 450 trunks.

S8500

The S8500 can be configured in three modes: Internal Call Control (ICC) where the S8500 acts as a standalone PBX, in Local Survivable Processor (LSP) mode where it is subtended to another server or as an Enterprise Survivable Server (ESS). The S8500 is one rack unit high and runs the Linux operating system. The S8500 can support up to 2,400 stations.

S87XX

The S8700, S8710 and S8720 media servers are redundant server pairs that run on the Linux operating system and host the Avaya Communication Manager software. Through memory shadowing, the secondary server in the pair is able to support all features in the event the primary server fails. The S87xx servers are able to support up to 36,000 stations and 12,000 trunks.

Media Gateways

G350 Gateway

The G350 Media Gateway is designed for branch offices. It can support up to 72 stations. It can be configured with an S8300 in ICC mode or LSP mode. The G350 includes a Standard Local Survivability (SLS) mode that provides basic functionality in case connectivity to a primary server fails.

G700 Gateway

The G700 is a stackable gateway that can support up to 450 stations and 450 trunks. The G700 supports the S8300 Media Server, either in standalone (ICC) mode or Local Survivable Processor (LSP) mode.

G650 Gateway

The G650 has 14 slots to accommodate trunk circuit packs, station circuit packs, CLAN, MedPro, IPSI and other circuit packs. The G650 can be supported by the S87xx servers. The G650 is 8 rack units high. This is the primary gateway used in the sample PBX.

Appendix B – Glossary (wikipedia is primary source)

H.323 - an umbrella recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network

CM – Avaya's Communications Manager Software

Computer telephony integration (**CTI**) allows interactions on a telephone and a computer to be integrated

Enterprise Survivable Server (ESS) This is the implementation of a hot spare media server located in a separate location with a fully copy of the main configuration files

Intrusion Detection System (IDS) – Probes around the network scanning traffic for anomalies or signatures of attacks

Host Intrusion Prevention System (HIPS) – Software running on the host system that actively prevents intrusions and attacks from succeeding

Local Survivable Processor (**LSP**) is the ability for the local processor to run the communications manager software. This allows the processor to run the local site as a standalone pbx should it be cutoff from the main processor

Network Management Systems (NMS) – CA Spectrum or HP Openview are examples of this type of system and are used to monitor network devices.

Phreaking Manipulating a telephone system illicitly to allow one to make calls without charges

Private Branch Exchange (PBX) – A dedicated corporate phone system servicing an enterprise

Real-time Transport Control Protocol (RTCP) is a sister protocol of the Real-time Transport Protocol (RTP) and provides out of band management of the RTP session.

Real-time Transport Protocol (RTP) defines a standardized packet format for delivering audio and video over the Internet

Session Initiation Protocol (SIP) is a signaling protocol for creating, modifying, and terminating sessions with one or more participants

Simple Network Management Protocol (SNMP) – This is used to manage IP based devices, it used by most Network Management Systems

Tie line-A connection between systems communications systems.

Time-Division Multiplexing (**TDM**) is digital signaling technique, but in this paper it refers to traditional telephony services. It includesTelco services like T1s or digital / hardwired phone sets

TFTP – Trivial File Transfer Protocol Utilizes UDP port 69 and is generally insecure

Wireless Application Protocol (WAP) is an open international standard for applications that use wireless communication

Wireless Markup Language (WML) - a content format for devices that implement the Wireless Application Protocol (WAP) specification

References

Robinson, Rick (2001) *TN801B MAP-D circuit pack running the DEFINITY LAN Gateway (DLG) and/or CVLAN applications Security*

McNab, Chris (2004) *Network Security Assessment* Sebastopol, CA: O'Reilly

Endler, David & Collier, Mark (2006) *Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions (Hacking Exposed)* United States:McGraw-Hill Osborne Media

Kelly (2005), *VOIP for Dummies Avaya Limited Edition* : Avaya

Avaya Communications (2006), *Avaya Application Solutions: IP Telephony Deployment Guide 555-245-600 Issue 4.3 February 2006* United States: Avaya

Avaya Communications (2006) *4600 Series IP Telephone LAN Administrator's Guide* http://support.avaya.com/elmodocs2/avayaip/555233507_1_7.pdf United States:Avaya

Avaya Communications (2006) *Avaya ESS users guide,* (http://support.avaya.com/elmodocs2/comm_mgr/r3/pdfs/03_300428_1_1.pdf) United States: Avaya

Hall (1998), *Voice-over-IP Across the Enterprise Network* (http://www.ehsco.com/reading/19981001ncf1.html

Avaya Solution & Interoperability Test Lab Application Note - *Configuring Avaya Communication Manager for Media Encryption – Issue 1.0* (http://www.Avaya.com/master-usa/en-us/resource/assets/applicationnotes/media-encrypt.pdf) United States: Avaya

Connect UPS *Connect UPS WEB/SNMP Card User's Guide* http://www.armspower.com/Products/Powerware/Software/ConnectUPS%20Multiview/ConnectUPS%20Web_SNMP%20User's%20Manual.pdf United States:Powerware.com

Solarwinds Engineering Toolkit mibwalk, *wan killer, IP network browser and other utilities* found at http://www.solarwinds.com/products/toolsets/engineer.aspx Solarwinds Inc

Foundstone free tools *Scanline sl.exe* http://www.foundstone.com/us/resources/proddesc/scanline.htm Foundstone Inc

Sourceforge *net-snmp v5.4.1* http://net-snmp.sourceforge.net/

HPING authors and Contributers http://www.hping.org/authors.php *hping* hping2.win32.tar.gz

Wikipedia http://www.wikipedia.org/

Nmap - http://nmap.org/

WML Examples http://www.w3schools.com/wap/wml_examples.asp