



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Mirage Networks Endpoint Controller in an Avaya IP Telephony Infrastructure – Issue 1.0**

### **Abstract**

These Application Notes describe a configuration where the Mirage Networks Endpoint Controller protects the subnets where an Avaya Servers, an Avaya Media Gateway, and Avaya IP Telephones reside against rapidly propagating threats. During compliance testing, the Mirage Networks Endpoint Controller detected basic ping and port scans that often precede threats on the protected subnets, and mitigated basic Denial of Service (DoS) attacks.

Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

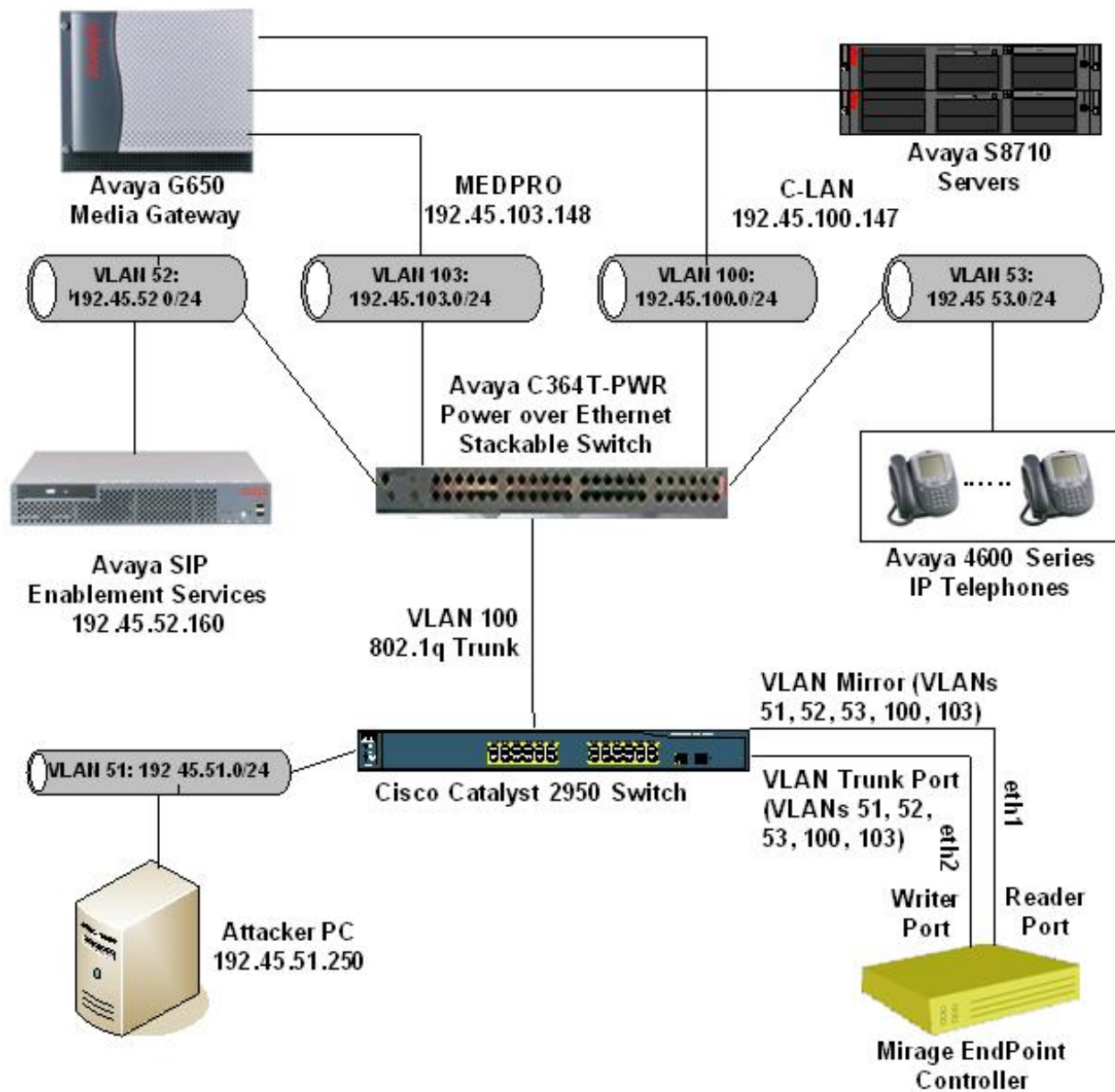
# 1. Introduction

These Application Notes describe a configuration where the Mirage Networks Endpoint Controller protects the subnets against rapidly propagating threats where Avaya Servers, Avaya Media Gateways, and Avaya IP Telephones reside. During compliance testing, the Mirage Endpoint Controller detected basic ping and port scans that often precede threats on the protected subnets, and mitigated basic Denial of Service (DoS) attacks. Mirage Endpoint Controller operates within the network interior, and is complementary to perimeter security solutions.

Mirage Endpoint Controller is a suite of purpose-built full-cycle Network Access Control appliances. The product enforces both pre-admission and post-admission policy controls to ensure secure network access for all network endpoints. The Mirage Endpoint Controller provides native (in-box) policy enforcement via Address Resolution Protocol (ARP) management techniques. The Mirage Endpoint Controller also provides a collection of post-admission content targeted specifically at protecting IP Telephony environments.

**Figure 1** illustrates a sample configuration consisting of Avaya S8710 Servers running Avaya Communication Manager, an Avaya G650 Media Gateway, an Avaya SIP Enablement Services (SES) server, Avaya IP Telephones, an Avaya C364T-PWR Power over Ethernet Stackable Switch, a Cisco Catalyst 2950 Series switch, an Attacker PC, and a Mirage Endpoint Controller. Avaya Communication Manager runs on the S8710 Servers, though the solution described herein is also extensible to other Avaya Servers and Media Gateways. The Avaya S8710 Server, Avaya SES, Avaya IP Telephones and G650 Media Gateway are connected to the C364T-PWR, which in turn connects to the Catalyst 2950 via an 802.1q trunk. The Avaya S8710 servers and the C-LAN cards are on VLAN 100, Avaya SES is on VLAN 52 and the Avaya Medpro boards are on VLAN 103. The IP Telephones reside on VLAN 53 and the Attacker PC resides on VLAN 51.

The Mirage Endpoint Controller connects to two ports on the Catalyst 2950. The VLANs to be protected (51, 52, 53, 100 and 103) are also configured on these two ports. The protected VLANs are mirrored to one of the two Catalyst 2950 ports called the Reader Port. Reader port allows the Mirage Endpoint Controller to monitor unicast and broadcast traffic on the protected VLANs. The Writer port allows the Mirage Endpoint Controller to transmit ARP messages onto the protected VLANs and perform quarantining.



**Figure 1: Sample configuration**

## 2. Equipment and Software Validated

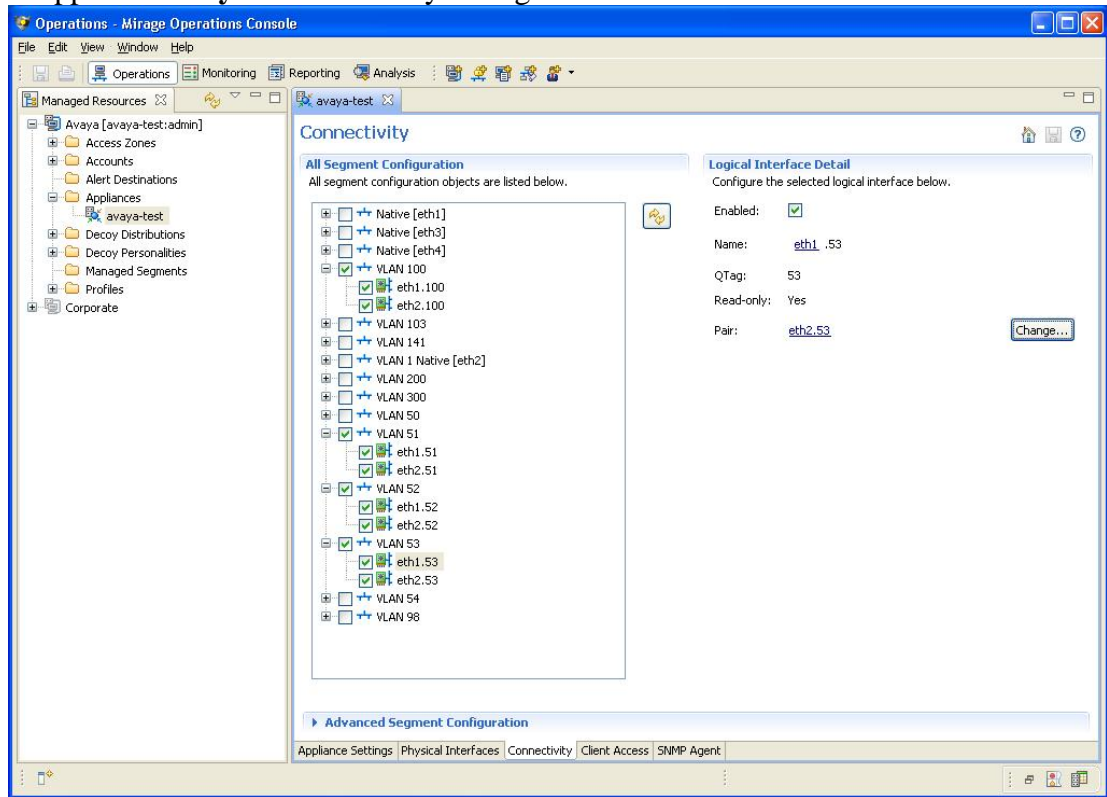
The following equipment and software/firmware were used for the sample configuration provided:

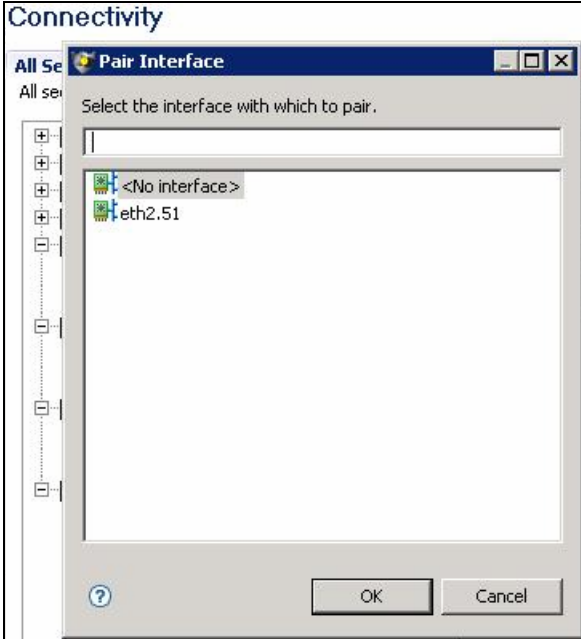
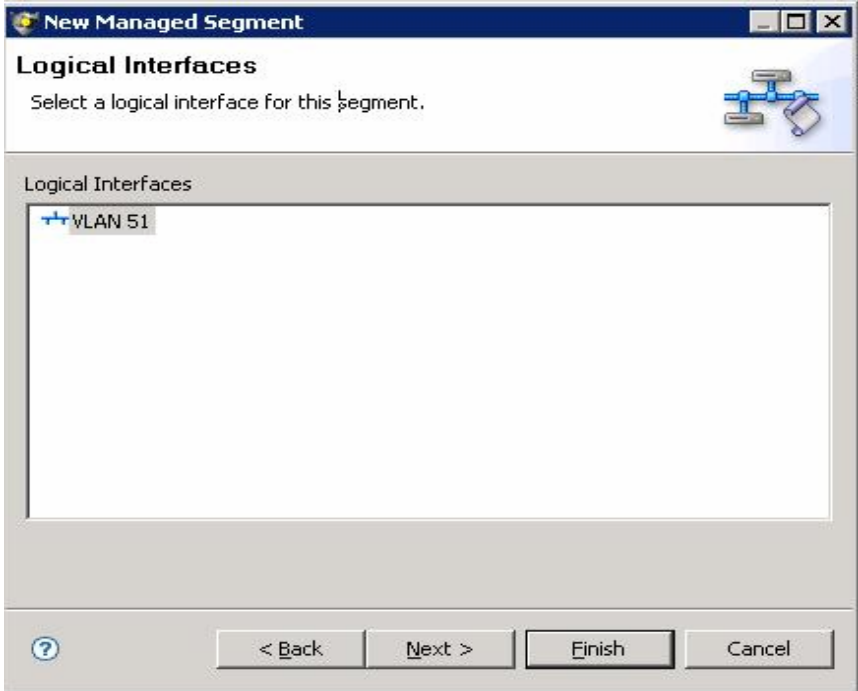
Equipment		Software/Firmware
Avaya S8710 Servers		Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya G650 Media Gateway		-
	TN2312BP IP Server Interface	HW12, FW039
	TN799DP C-LAN Interface	HW01, FW024
	TN2302AP IP Media Processor	HW18, FW117
Avaya SIP Enablement Services		4.0 (SES-4.0.0.0-033.6)
Avaya 4600 Series IP Telephones		2.3 (4602SW H.323) 2.5 (4625SW H.323) 2.2.3 (4610SW SIP)
Avaya C364T-PWR Power over Ethernet Stackable Switch		4.5.14
Mirage Networks Endpoint Controller		3.2.1 Build 18029
Cisco Catalyst 2950 Switch		12.1(12C)EA1
Attacker PC		Windows XP SP2

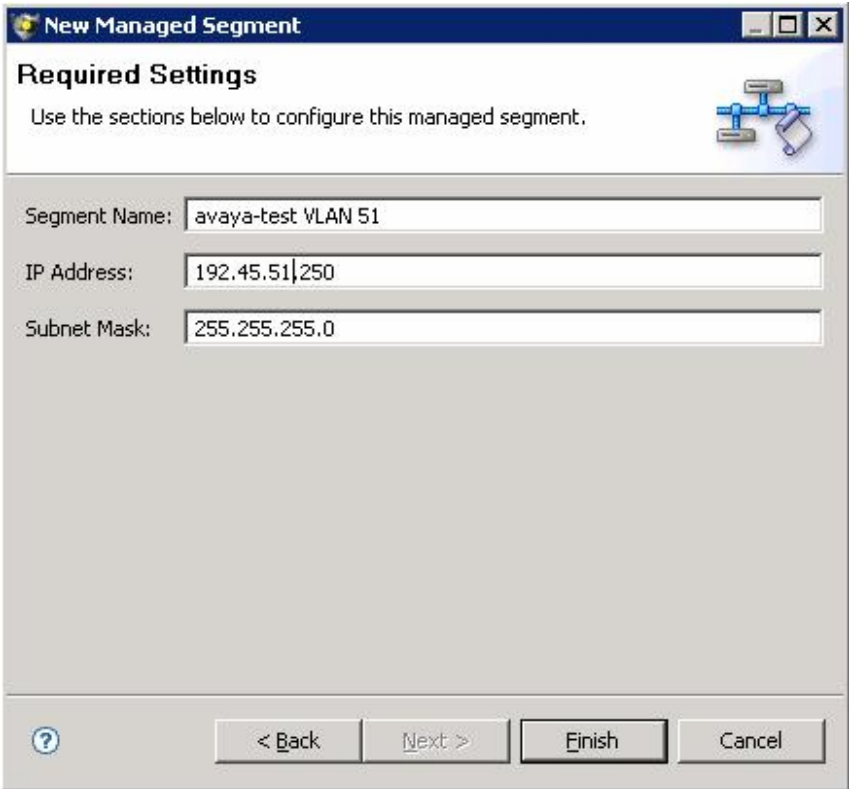
### 3. Configure Mirage Endpoint Controller

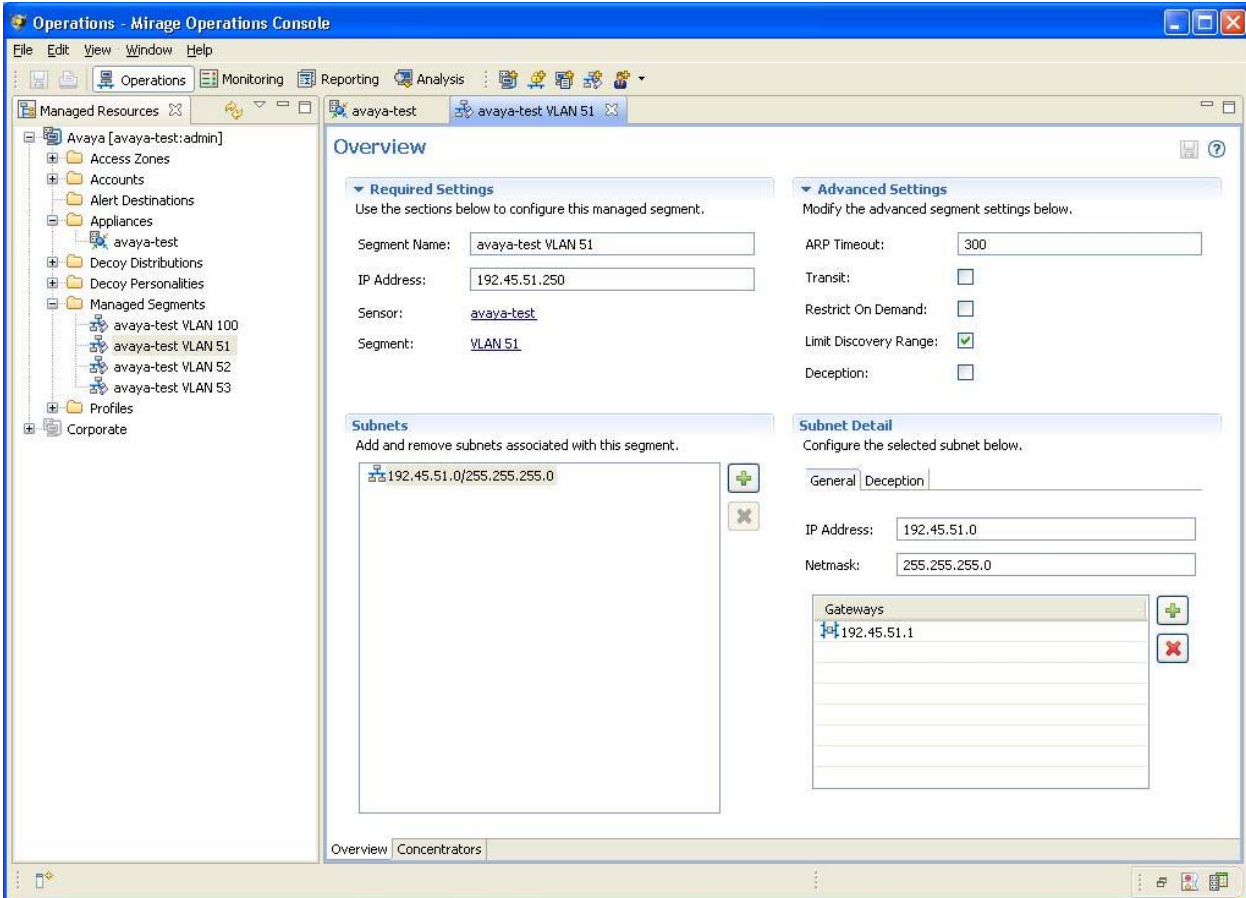
This section describes the steps for configuring the Mirage Endpoint Controller to protect the subnets (VLANs 51, 52, 53, 100 and 103 in the sample configuration) where the Avaya S8710 Server, Avaya SES, G650 Media Gateway, and IP telephones reside on. For Mirage Endpoint Controller configuration rules, contact Mirage Networks.

Step	Description
1.	Launch the Mirage Operations Console (MOC) application by following Start->All Programs->Mirage Operations Console->Mirage Operations Console and log in with the appropriate credentials.
2.	<p>The following steps need to be performed to get access to the <b>Connectivity</b> screen and change the pairing characteristics for the interfaces in each segment:</p> <ul style="list-style-type: none"> <li>• Select <b>Operations</b> from the top tab.</li> <li>• Expand the <b>Appliances</b> container.</li> <li>• Double-click the appliance (<b>avaya-test</b> in this example) to open its Properties panel on the right.</li> <li>• Select <b>Connectivity</b> from the bottom tab.</li> <li>• Select the segment to be configured and click <b>Change</b>.</li> </ul> <p>Notes:</p> <ol style="list-style-type: none"> <li>1. <b>eth1</b> is the reader port that takes the mirror feed and <b>eth2</b> is the writer port that is responsible for interacting with the devices on each segment.</li> <li>2. Appliance <b>avaya-test</b> is already configured.</li> </ol>



Step	Description
3.	<p>Enter the interface to pair with and click <b>OK</b>.</p> 
4.	<p>Right-click on the <b>Managed Segments</b> container at the screen shown in <b>Step 2</b>, and choose <b>Add Managed Segment</b> at the pop-up screen [not shown]. Select the logical interface (<b>VLAN51</b> in this example) at the <b>New Managed Segment-&gt;Logical Interfaces</b> screen and click <b>Next</b>.</p> 

Step	Description
5.	<p>At the <b>New Managed Segment-&gt;Required Settings</b> screen, configure as follows:</p> <ul style="list-style-type: none"> <li>• <b>Segment Name</b> – Any descriptive name</li> <li>• <b>IP Address</b> – Any IP address not to be used on this segment.</li> <li>• <b>Subnet Mask</b> – A valid subnet mask.</li> <li>• Click <b>Finish</b>.</li> </ul> 

Step	Description
6.	<p>Enter the default gateway of the subnet and click on the <b>Save</b> icon on the top right corner.</p> 
7.	Repeat <b>Steps 2 – 6</b> for each subnet to be configured.



## 4. Configure Cisco Catalyst 2950

This section describes the steps on the Cisco Catalyst 2950 for configuring the VLAN mirror, the two ports connected to the Mirage Endpoint Controller, and the port connected to the Avaya C364T-PWR. These steps assume that the VLANs and routing between VLANs have already been configured on the Catalyst 2950.

Step	Description
1.	From the Catalyst 2950 Command Line Interface (CLI), assign the protected VLANs (51, 52, 53, 100 and 103 in the sample configuration) to the two ports connected to the Mirage, and configure the ports as trunk ports with 802.1q encapsulation.
	<pre>interface FastEthernet0/1     description To-Mirage-Read ! interface FastEthernet0/2     description To-Mirage-Write     switchport trunk encapsulation dot1q     switchport trunk allowed vlan 51,52,53,100,103     switchport mode trunk     no ip address     no mdix auto</pre>
2.	Configure a monitor session to mirror all VLAN traffic from the protected VLANs to the port in Step 1 connected to the “Reader” port on the Mirage.
	<pre>monitor session 1 source interface FastEthernet0/2 - 12 monitor session 1 destination interface Fa0/1 encapsulation replicate</pre>
3.	Configure the port connected to the Avaya C364T-PWR as a trunk, with 802.1q encapsulation, carrying VLAN’s 51, 52, 53, 100 and 103.
	<pre>interface FastEthernet0/12     description To-Avaya-P33T     switchport trunk encapsulation dot1q     switchport trunk allowed vlan 51,52,53,100, 103     switchport mode trunk     no ip address     no mdix auto</pre>

## 5. Configure Avaya C364T-PWR

From the Avaya C364T-PWR CLI, assign VLAN 100 to the port connected to the Cisco Catalyst 2950, and configure the port as an 802.1q trunk port.

```
set port vlan 100 1/24
set trunk 1/24 dot1q
```

## 6. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying that the Mirage Networks Mirage detected basic ping and port scans, and mitigated basic Denial of Service (DoS) attacks.

### 6.1. General Test Approach

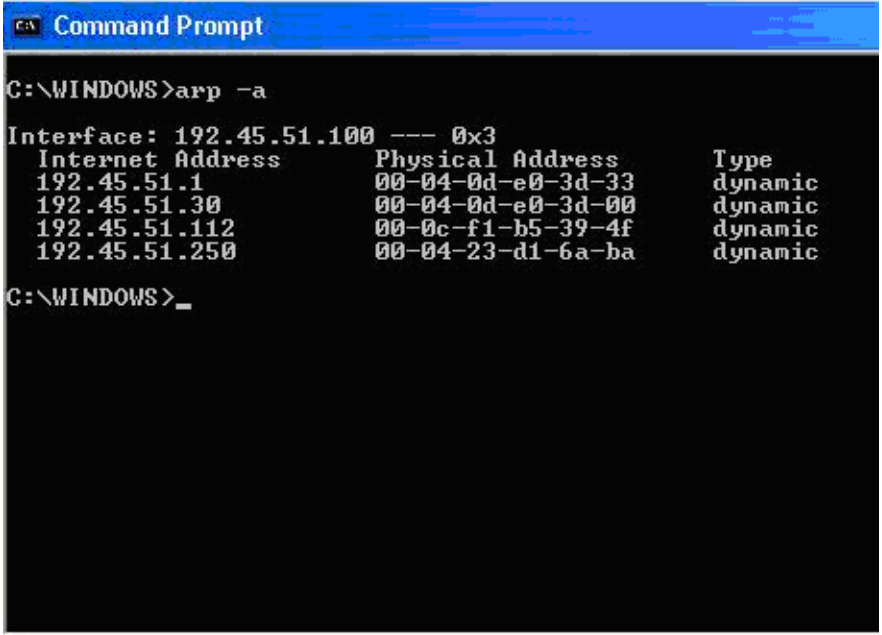
The general approach was to launch ping scans on the protected VLANs, and port scans and basic DoS attacks on the C-LAN and Media Processor boards on the Avaya G650 Media Gateway, as well as the Avaya IP Telephones. The main objectives were to verify that:

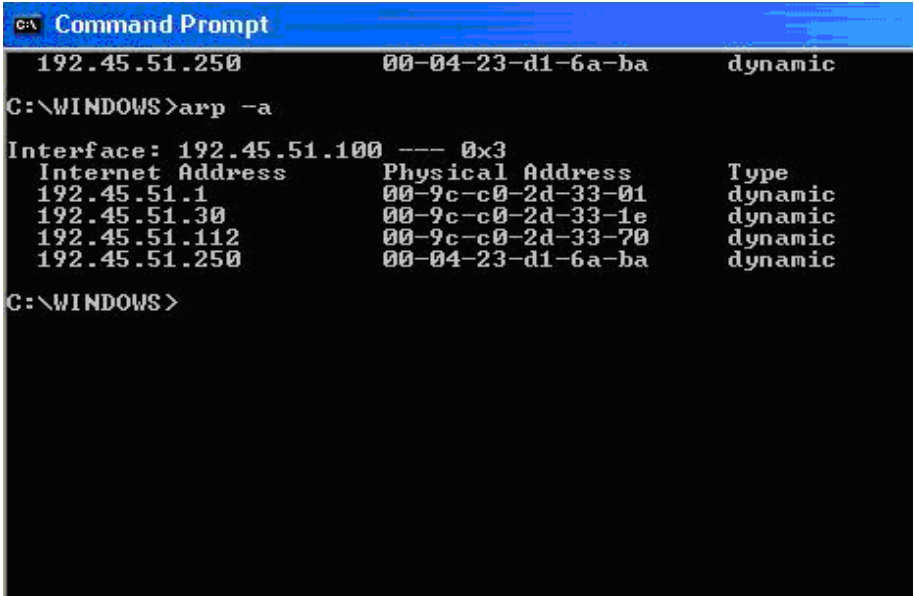
- The Mirage Endpoint Controller correctly detects basic ping, TCP SYN, and UDP scans on protected subnets.
- The Mirage Endpoint Controller correctly detects basic DoS attacks, such as ping, TCP SYN/FIN, UDP floods and smurf attacks against the C-LAN and Media Processor boards on the Avaya G650 Media Gateway, and the Avaya IP Telephones.
- The Mirage Endpoint Controller correctly detects H.323 GRQ DoS attacks on the Avaya IP Telephony network.
- The Mirage Endpoint Controller correctly detects SIP Invite and Registration DoS attack on Avaya SES.
- The Mirage Endpoint Controller correctly detects IP Telephony unauthorized use such as unauthorized hosts, routers and servers.
- The Mirage Endpoint Controller quarantines the DoS attacks.
- Avaya IP Telephones on the protected subnets successfully establish and maintain calls during the basic scan and DoS attack activity.
- Avaya IP Telephones on the protected subnets successfully establish and maintain calls when there is no scan or DoS attack activity.

### 6.2. Test Results

The test objectives of Section 6.1 were verified. The Mirage Endpoint Controller was able to detect the basic ping, port scans, and mitigate spoofed DoS attacks generated by the Attacker PC. Mirage Endpoint Controller was able to detect and mitigate SIP Invite and Registration DoS attacks on Avaya SES and IP Telephony network. The Mirage Endpoint Controller detected and quarantined the unauthorized use of the Avaya IP Telephony network. Avaya IP Telephones continued to function normally before the Attacker PC was identified and after it was quarantined.

## 7. Verification Steps

Step	Description
1.	<p>Verify the ARP table of the Attacker PC for the MAC addresses prior to attack as shown in the picture.</p>  <pre>Command Prompt C:\WINDOWS&gt;arp -a  Interface: 192.45.51.100 --- 0x3 Internet Address      Physical Address      Type 192.45.51.1           00-04-0d-e0-3d-33    dynamic 192.45.51.30          00-04-0d-e0-3d-00    dynamic 192.45.51.112         00-0c-f1-b5-39-4f    dynamic 192.45.51.250         00-04-23-d1-6a-ba    dynamic  C:\WINDOWS&gt;_</pre>

Step	Description
2.	<p>From the Attacker PC, send a basic ping and port scan to specific targets in the protected subnets.</p> <ul style="list-style-type: none"> <li>• Verify that one or more Mirage rules are triggered.</li> <li>• Verify the Attacker PC is quarantined and is not available to any other network element.</li> <li>• Verify the ARP table of the Attacker PC and target after the attack. In the example below the ARP table has modified MAC addresses indicating that the source of attack is quarantined.</li> </ul>  <pre> C:\&gt;arp -a  Interface: 192.45.51.100 --- 0x3 Internet Address      Physical Address      Type 192.45.51.1           00-9c-c0-2d-33-01     dynamic 192.45.51.30          00-9c-c0-2d-33-1e     dynamic 192.45.51.112         00-9c-c0-2d-33-70     dynamic 192.45.51.250         00-04-23-d1-6a-ba     dynamic C:\WINDOWS&gt; </pre>

## 8. Support

For technical support on the Mirage Networks Endpoint Controller, consult the support pages at <http://miragenetworks.com/support.html> or contact Mirage Networks customer support at:

- Phone: 866.869.6767
- E-mail: [support@miragenetworks.com](mailto:support@miragenetworks.com)

## 9. Conclusion

These Application Notes describe a configuration where the Mirage Networks Endpoint Controller protects the subnets where an Avaya Server, an Avaya Media Gateway, and Avaya IP Telephones reside against rapidly propagating threats. During compliance testing, the Mirage Networks Endpoint Controller detected basic ping and port scans that often precede threats on the protected subnets, mitigated basic Denial of Service (DoS) attacks, and enforced segment-specific compliance policies.

## 10. Additional References

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

Product information for Mirage Networks products may be found at <http://miragenetworks.com>.

---

**©2008 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).