Ethernet Card Testing

- Ethernet Cards for Silent Monitor, on page 1
- Test Procedure, on page 1

Ethernet Cards for Silent Monitor

On a site with IP telephony, the Unified CM and the IP Phones generally use a Virtual Local Area Network (VLAN) that logically separates voice from data. Although both traffic types are on the same physical channel, they are sent on different VLANs, one for voice and other for data. This configuration enables you to send voice with higher priority than data.

In a call center with silent monitoring, the agent desktop system uses one single physical channel to interact with two different VLANs. You connect the agent desktop system to the PC port on the back of the IP phone. Then, the silent monitor subsystem can collect the voice packets reaching the phone and forward the packets to the supervisor workstation.

The agent desktop system accesses the physical channel through an Ethernet Network Interface Controller (NIC). The NIC monitors the channel and collects Ethernet frames addressed to the agent's computer. The NIC runs a preprocessing step to extract IP packets from the Ethernet frames and deliver them to the TCP/IP stack on the operating system.

During internal testing, Cisco identified that some Ethernet NIC card drivers cannot preprocess Ethernet frames that have an IP packet encapsulated in a VLAN frame. The NIC card driver discards the Ethernet frame if the IP packet is encapsulated in an 802.1Q frame. Some vendors can provide a configuration setting that allows their NIC card driver to forward VLAN traffic to the TCP/IP stack.

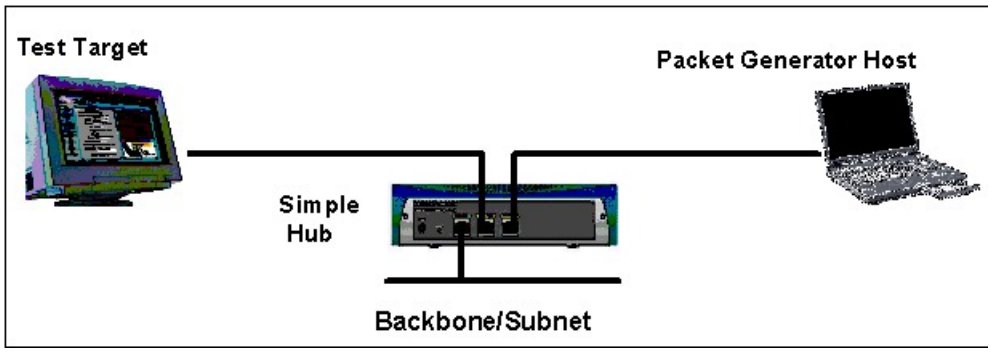
If an agent desktop's NIC card driver discards VLAN traffic, then the silent monitor subsystem on that desktop cannot collect and forward voice packets. Silent monitor cannot function properly on such a NIC. Cisco developed a procedure to determine if a particular Ethernet NIC card driver works with the CTI OS silent monitor. The procedure is described in the following sections.

Test Procedure

The test involves sending sample VLAN packets to a *Test Target NIC* card and verifying that the packets are not discarded by the pre-processing step but are passed onto the TCP/IP stack on the operating system at the computer hosting the NIC card.

The test requires a configuration as shown in the following diagram.

Figure 1: Silent Monitor Ethernet Card Test Configuration



The Test Target NIC is connected to one port of a simple Hub. The Hub is connected to the network backbone or subnet. You also need a *Packet Generator Host* capable of generating Ethernet traffic. You must connect the *Packet Generator Host* to another port on the Hub.

The *Packet Generator Host* equipment can be either a dedicated packet analyzer or a computer with a software-based packet analyzer with capabilities to generate Ethernet traffic.

You can use several available software packet analyzers that can be used for this purpose. For more information about reliable analyzers, visit the *Cooperative Association for Internet Data Analysis* website at http://www.caida.org/tools/taxonomy/workload.xml.

The following sections demonstrate the use of Sniffer Pro.

After you set up the environment as described above you must load the software tools on the *Test Target and Packet Generator Host* as follows.

Prepare Test Target

Procedure

Step 1 Install the *WinPcap* utility. The WinPcap installation program is located at the root directory on the Cisco Computer Telephony Integration CTI Object Server CD.

Step 2 Create a directory on the *Test Target* computer named "VLANTest".

Step 3 From the Cisco Computer Telephony Integration CTI Object Server CD, copy WinDump.exe and place it in the directory you created in Step 2. (*WinDump is located on the CD under CtiOS\Tools\VLANTest\WinDump*.)

Step 4 Open a console window. Go to the directory where you copied WinDump.exe.

Step 5 Determine the MAC address of the *Test Target NIC* by running *ipconfig /all* at the command prompt. Write down the number that appears for the Physical Address. For example, the "Intel Pro/100" NIC card has a MAC address of **00D059d8f7d9**.

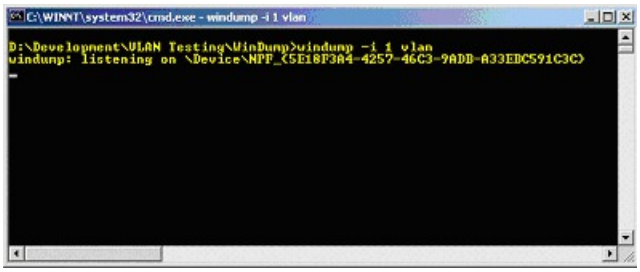
Figure 2: Determining the Test Target NIC MAC Address

Step 6 Determine the device interface number of the *Test Target NIC*. Run **windump –D** and write down the number of the NIC you want to test. In this example, you would choose interface number 1, which corresponds to the "Intel Pro/100" NIC card.

Note If you are not sure which number to pick, repeat the test for each card until the test succeeds for one (sufficient to pass) or this fails for all cards.

Step 7 Start WinDump to monitor the *Test Target NIC* for incoming VLAN packets. To do this, run **windump –i <device_number> vlan**. In the following example the *device_number* is 1.

Figure 3: Monitoring the Test Target NIC for Incoming VLAN Packets



Prepare Packet Generator Host

Perform the following steps to prepare the packet generator host.

Procedure

Step 1 Load the packet analyzer software onto your *Packet Generator Host.*

Step 2 Load the sample capture file provided in the Cisco Computer Telephony Integration CTI Object Server CD (Ctios\Tools\VLANTest\VLANCapture\VLANSamplePackets.cap). The capture file was generated in a format that is used by most dedicated and software packet analyzers.

Step 3 Select the Decode view from the tab at the bottom of the screen.

Running a Test

The test involves sending sample VLAN packets to a *Test Target NIC* card and verifying that the packet is not discarded by the pre-processing step but is passed onto the TCP/IP stack on the computer hosting the NIC card.

The test case to determine whether or not the *Test Target NIC* is qualified to work with CTI OS silent monitor is as follows. (In the test case nomenclature, PA stands for Packet Analyzer and WD stands for WinDump.)

Table 1: SMNIC- 1 Send Sample VLAN Packets to Test Target NIC Card

Objective	Verify that the Test Target NIC can pre-process VLAN packets and forward them to the TCP/IP stack on the Test Target Host.	
Steps	**Party**	**Action**
1	PA	Select one of the loaded sample VLAN Packets.
2	PA	Select or right-click “Send Current Frame”.
3	PA	Modify the destination MAC address to use the MAC address of the Test target NIC (for more information, see the figure “Modifying the destination MAC address” below).
4	PA	Send the new frame to the Test Target NIC five times.
5	WD	Verify that there is activity reported on the Test Target NIC.
Expected Result	At the *Test Target* computer *windump* displays five packets for VLAN ID = 85 (for more information, see the figure “Sample output showing successful packet capture” below). If the test fails, no packets appear.	

Figure 4: Modifying the Destination MAC Address

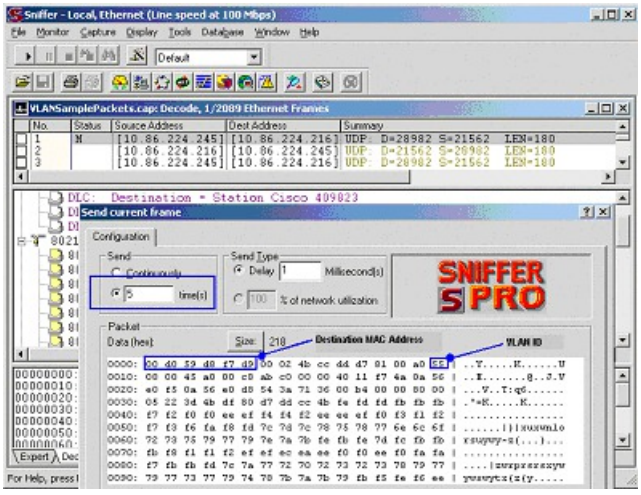
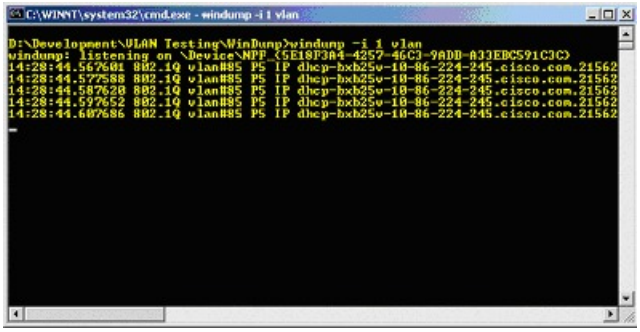


Figure 5: Sample Output Showing Successful Packet Capture



If the outcome of this test is successful, then your *Test Target NIC* works with the CTI OS silent monitor. Otherwise, contact your NIC card provider and ask what settings are necessary to allow your NIC card driver to forward all packets including VLAN packets to the TCP/IP stack on the computer so that your packet analyzer tool can capture and display them. Then apply the appropriate adjustments and rerun this test procedure.

Ethernet Card Testing