Version 4.6

Problem Description: Network cards and 802.1Q VLAN tags

Some Broadcom and Intel Network cards DO NOT show any 802.1Q VLAN tags in capture:

- Broadcom 570x Gigabit integrated adapter (Dell Laptop) Driver 8.48.0.0 Date 10/31/05
- Intel PRO/1000 MT Mobile Connection (IBM T41 Laptop) Driver 8.6.11.0 date 6/29/2005
- Broadcom NetXtreme 57xx Gigabit Controller (Dell Desktop) Driver 8.48.0.0 Date 10/31/05

The following Network cards DO show 802.1Q VLAN tags in capture:

- 3Com 10/100 mini PCI Ethernet adapter (Dell Laptop) Driver 1.21.0.1 Date 7/21/2001
- 3Com Megahertz Model 3CXFE575BT (PCMCIA Card) Driver 2.60.500.20
- 3Com EtherLink 10/100 PCI TX NIC 3C905B-TX (PCI Card) Driver 4.31.0.0 Date 8/13/2002

Other information:

http://wiki.wireshark.org/CaptureSetup/VLAN

Workaround or alternative remediation:

For Intel Cards, look at Intel Support site:
[From http://support.intel.com/support/network/sb/cs-005897.htm]

Microsoft* Windows* ---

To allow tagged frames to be passed to your packet capture software you must go into the registry and either add a registry dword and value or change the value of the registry key. Depending on the bus type of your network adapter you will either create the keyword "MonitorModeEnabled" for PCI/PCI-X Network Adapters, or "MonitorMode" for PCI-e based Network Adapters.

The new key (dword) should be placed at:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}\00xx

where xx is the instance of the network adapter that you need to see tags on. (Check by opening and viewing the name of the adapter).

Note: ControlSet001 may need to be CurrentControlSet or another 00x number.

If you are using a **PCI or PCI-X** Network Adapter the registry dword is:
MonitorModeEnabled
Set the dword value to either:
0 - disabled (Do not store bad packets, Do not store CRCs, Strip 802.1Q vlan tags)
1 - enabled (Store bad packets. Store CRCs. Do not strip 802.1Q vlan tags)

If you are using a **PCI-Express** Network Adapter the registry dword is: **MonitorMode**
Set the dword value to either:
0 - disabled (Do not store bad packets, Do not store CRCs, Strip 802.1Q vlan tags)
1 - enabled (Store bad packets. Store CRCs. Do not strip 802.1Q vlan btag)
2 - enabled strip vlan (Store bad packets. Store CRCs. Strip 802.1Q vlan tag as normal)

In most cases you should set MonitorMode=1 or MonitorModeEnabled=1.

Warning: This modification should be made very carefully and only by skilled technicians since changes to the registry may disable your machine. This change should only be made for promiscuous mode/sniffing use.

Operating System:

Windows Vista*, Windows Server* 2008, Windows* 98 SE, Windows Home Server, Windows* 2000, Windows* Me, Windows NT* 4.0, Windows* XP 64-Bit Edition, Windows* XP Professional, Windows Server* 2003

For Broadcom Cards:

There is a registry key under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet that can be set to cause the driver and chip not to strip the 802.1Q headers.
In order to set that key, you need to find the right instance of the driver in Registry Editor and set that key for it. You can do this by doing following:

1. Run the Registry Editor (regedt32).

2. Search for "TxCoalescingTicks" under "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet" and ensure this is the only instance that you have.

3. Right-click on the instance number (eg. 0008) and add a new string value.

4. Enter "PreserveVlanInfoInRxPacket" and give it the value "1".

Save and Reboot

This should set you up to be able to sniff the VLAN tag information.