

White Paper

How to capture packets with Wireshark

Tim Chung

Version 1.0 (AUG, 2009)

QSAN Technology, Inc. http://www.qsan.com.tw White Paper# QWP200913-P200C



White Paper

Introduction

This document describes how to use the **Wireshark** – a network protocal analyzer – to capture the packets of iSCSI communication over the ethernet.

Environment

Windows XP
Wireshark 1.2.1
192.168.11.87/24
HP Procurve Switch 1800-24G
QSAN P200C
1GB DDR2-533
1.1.6 (20090625_1800)
192.168.11.200/24

Diagram



QSAN P200C





Installation

1. Please download the **Wireshark** first from the website: <u>www.wireshark.org</u>. The **Wireshark** version of this example is **1.2.1**.



2. Run the Setup program and follow the instructions to install the Wireshark.



3. Be sure to select the install option of **WinPcap** which is the library for capturing the packets in Windows platform.



White Paper

🕼 Wireshark 1.2.1 (32-bit) Setup	×
Install WinPcap? WinPcap is required to capture live network data. Should WinPcap be installed?	
Currently installed WinPcap version WinPcap is currently not installed	
Install ✓ Install WinPcap 4.1 beta5 (Use Add/Remove Programs first to uninstall any undetected old WinPcap versions)	
Services Start WinPcap service "NPF" at startup (so users without Administrator privileges can capture)	
What is WinPcap?	
<pre>Cancel</pre>]

4. The **WinPcap** will be installed first if it has been selected, follow the instructions to finish the setup.

😽 WinPcap 4.1 beta5 Setup	
WinPcap 4.1 beta5 Installer Welcome to the WinPcap 4.1 beta5 Installation Wizar	ď
Packet Capturing and Network Analysis Solution	•
Nullsoft Install System v2.39 Next > (Cancel

5. After the installation of **WinPcap**, it continues the setup of **Wireshark**.







6. The setup of **Wireshark** is completed now.

🕢 Wireshark 1.2.1 (32-bit) Setup		
Installation Complete Setup was completed successfully.		1
Completed		
Output folder: C:\Program Files\Wireshark Extract: mergecap.exe Extract: mergecap.html Output folder: C:\Program Files\Wireshark Extract: capinfos.exe Extract: capinfos.html Output folder: C:\Program Files\Wireshark Extract: rawshark.exe Extract: rawshark.exe Extract: rawshark.html Output folder: C:\Program Files\Wireshark Extract: user-guide.chm Completed		
Nullsoft Install System v2.44	< Back Next >	Cancel



White Paper

Operation

Capture the network packets with **Wireshark** is very easy, please follow the procedure on the following.

1. Run **Wireshark** program and click the **List the available capture interfaces** icon which is circled in red-circled.

🗖 The Wireshark Network Analyzer		
Eile Edit View Go Capture Analyze Statistics	Telephony <u>T</u> ools <u>H</u> elp	
■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	<	🛛 🖉 🔀 🔹 »
Filter:	▼ Expression Clear Apply	
WIRESHARK The World	's Most Popular Network Protocol Analyzer	
Capture	Files	(
Live list of the capture interfaces (counts incoming pack	ets) Open a previously captured file	Website Visit the proje
Start capture on interface:	Open Recent:	😝 User's (
Adapter for generic dialup and VPN capture	🗪 Sample Captures 🗟	🐸 The User's G
 Intel(R) PRO/1000 EB Network Connection with Intel(R) PRO/1000 EB Network Connection with Intel(R) PRO/1000 PT Dual Port Server Adapter Intel(R) PRO/1000 PT Dual Port Server Adapter 	A rich assortment of example capture files on the wiki	Securit Work with Wi
Capture Options		
Start a capture with detailed options		
Capture Help		
How to Capture		_
Ready to load or capture No	Packets Profile: Default	2 .:

2. All the network interfaces will be listed. Choose the one which is used to connect to the iSCSI target, and then click **Start** button. The **Wireshark** starts to capture the entire packets which pass through this interface.

Wireshark: Capture Interfaces						
Description	IP	Packets	Packets/s		Stop	
🖀 Adapter for generic dialup and VPN capture	unknown	0	0	Start O	ptions	Details
Intel(R) PRO/1000 EB Network Connection with I/O Acceleration (Microsoft's Packet Scheduler)	192.168.10.79	111	0	Start O	ptions	Details
TINTER INTER INTERIOR IN THE INTERNATION OF THE INTERNATION INTERNATIO	192.168.11.87	6	0	Stark O	ptions	Details
Intel(R) PRO/1000 PT Dual Port Server Adapter (Microsoft's Packet Scheduler)	169.254.125.88	1	0 Imm	ediately sta	art a capt	ure from this
The Intel(R) PRO/1000 PT Dual Port Server Adapter (Microsoft's Packet Scheduler) Help	169.254.174.166	5 1	0 Devi E2B4 Desc O Ac IP: 1	ce: \Device 1-4F0E-908 cription: Int celeration 192,168,11	e\NPF_{Ff 35-1A0909 tel(R) PRC (Microsof 87	8798061- 9A687E0} D/1000 EB Ne t's Packet Sch



White Paper

 After Wireshark starts to capture the network packets, we can do the regular operation of iSCSI. For example, login the iSCSi target and have some IO with iSCSI disk. All the packets of the communication between the initiator and the iSCSI target will be captured completely.

iSCSI Initiator Pro	perties			×
General Discovery	Targets	Persistent Targets	Bound Volumes/Device	es
Select a target and target. Click details devices for that targ	click Log (to see infor et.	In to access the stor mation about the ses	age devices for that ssions, connections and	
Log On to Target				
Target name: node1				
Automatically res	tore this c	onnection when the	system boots	
Only select this on your comput	option if iS er.	iCSI multi-path softw	vare is already installed	
Advanced		Цок	Cancel	
				Γ
	De	tails Log O	n Refresh	
	(ОК	Cancel Apply	

4. Click **Stop** button to stop the running capture.

📶 test.pcap - Wireshark				
<u>File Edit View Go Capture Analyze</u>	<u>Statistics</u> Telephony <u>T</u> ools <u>H</u> elp			
	28 9 7 :		- 🖉 🕅	🐻 »
Filter: Stop the running live ca	pture .	▼ Expression Clear Apply		
No Time	Source	Destination	Protocol	Info 🔷
1 0.000000	192.168.11.87	192.168.11.200	İSCSI	LOC
2 0.000250	192.168.11.200	192.168.11.87	iscsi	Log
3 0.000388	192.168.11.87	192.168.11.200	iscsi	Log
4 0.000471	192.168.11.200	192.168.11.87	iscsi	Log
5 0.000724	192.168.11.87	192.168.11.200	iscsi	тех
6 0.000810	192.168.11.200	192.168.11.87	iscsi	тех
7 0.000954	192.168.11.87	192.168.11.200	iscsi	Log
8 0.001023	192.168.11.200	192.168.11.87	iscsi	Log
9 27.413080	192.168.11.87	192.168.11.200	iscsi	Log
10 27.413183	192.168.11.200	192.168.11.87	iscsi	Log
11 27.413246	192.168.11.87	192.168.11.200	iscsi	Log
12 27.413394	192.168.11.200	192.168.11.87	iscsi	Log
13 27.425998	192.168.11.87	192.168.11.200	iscsi	SCS
14 27.426132	192.168.11.200	192.168.11.87	iscsi	SCS
15 27.426203	192.168.11.87	192.168.11.200	iscsi	SCS
16 27.426298	192.168.11.200	192.168.11.87	iscsi	SCS
17 27.426348	192.168.11.87	192.168.11.200	iscsi	SCS
18 27.426412	192.168.11.200	192.168.11.87	iscsi	SCS
19 27.426447	192.168.11.87	192.168.11.200	iscsi	SCS
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	107 169 11 700	107 160 11 07	iccer	ere 🎽
<u> </u>				
🗄 Frame 1 (190 bytes on wire	, 190 bytes captured)			
🕀 Ethernet II. Src: Asusteko	00:9c:81 (00:1f:c6:00:90	c:81). Dst: OsanTech a6	:04:7c (00	:13:78:2
Toternet Protocol Src: 10	2 168 11 87 (102 168 11 1	87) Det. 197 168 11 70	0 (102 168	11 200
		(1500) 5-+ 5+	· (192.108.	.11.200,
Iransmission Control Proto	col, Src Port: robcad-Im	(1509), DST PORT: ISCS	i-target (:	s260), S
🗄 iSCSI (Login Command)				



White Paper

5. Because **Wireshark** will capture the entire packets pass through the specified network interface, you may get a lot of packets which you don't need. The **Filter** function can filter out the unnecessary packets.

🗖 (Untitled) - Wireshark	
<u>File Edit View Go Capture Analyze Statistics</u>	Telephony <u>T</u> ools <u>H</u> elp
	🔍 🗢 🗢 🖓 🛧 🛛
Filter	▼ E <u>x</u> j
No. Popen the "Display Filter" dialog, to edit/apply filters	ource
RA 20122T	L92.168.11.200
90 50.501573 1	L92.168.11.87
91 50.501641 1	L92.168.11.200
92 50.501840 1	L92.168.11.87
93 50.501908 1	L92.168.11.200
94 50.501946 1	192.168.11.87
95 50.502014 1	192.168.11.200
96 50.742477 1	92.168.11.87
97 53, 780213	0.0.0.0
98 55, 507245	92.168.11.200
99 55 507279 1	92.168.11.87
100 55, 517238	192.168.11.200
101 60 288927	HewlettP 60:a2:80
102 60.517449 1	192.168.11.200

6. Click **Filter** button to pop up a dialog window. Here I use the condition of IP address which will matches the IP address of iSCSI target. Remember to change **Filter string** column with the IP address of iSCSI target.

🗖 Wiresh	nark: Display Filter - Profile: Default 📃 🗖 🔀
Edit	Display Filter
	No ARP
	IP only
New	IP address 192.168.0.1
	IP address isn't 192.168.0.1, don't use != for this!
	IPX only
	TCP only
	UDP only
	UDP port isn't 53 (not DNS), don't use != for this!
Delete	TCP or UDP port is 80 (HTTP)
Euro	нттр
	No ARP and no DNS
	Non-HTTP and non-SMTP to/from 192.168.0.1
Properties	
Filter name	: IP address 192.168.0.1
Filter string	: ip.addr == 192.168.11.200
Help	OK Apply Cancel



White Paper

7. Now, only the packets which match the IP are kept.

er: ip.addr == 192.168.11.200		Expression Clear Apply		
Time	Source	Destination	Protocol	Info
55 48.886842	192.168.11.200	192.168.11.87	iscsi	SCS
56 48.886876	192.168.11.87	192.168.11.200	iscsi	SCS
57 48.886961	192.168.11.200	192.168.11.87	iscsi	SCS
58 48.887002	192.168.11.87	192.168.11.200	iscsi	SCS
59 48.887078	192.168.11.200	192.168.11.87	iscsi	SCS
60 48.887114	192.168.11.87	192.168.11.200	iscsi	SCS
61 48.887194	192.168.11.200	192.168.11.87	iscsi	SCS
62 48.887391	192.168.11.87	192.168.11.200	iscsi	SCS
63 48.887462	192.168.11.200	192.168.11.87	iscsi	SCS
64 48.887519	192.168.11.87	° 192.168.11.200	iscsi	SCS
65 48.887579	192.168.11.200	192.168.11.87	iscsi	SCS
66 49.102706	192.168.11.87	192.168.11.200	TCP	win
67 50.472595	192.168.11.87	192.168.11.200	iscsi	SCS
68 50.472704	192.168.11.200	192.168.11.87	iscsi	SCS
69 50.472780	192.168.11.87	192.168.11.200	iscsi	SCS
70 50.472896	192.168.11.200	192.168.11.87	iscsi	SCS
71 50.472942	192.168.11.87	192.168.11.200	iscsi	SCS
72 50.477047	192.168.11.200	192.168.11.87	TCP	isc
73 50.500358	192.168.11.200	192.168.11.87	iscsi	SCS
74 50 500405	100 160 11 07	107 160 11 700	Accer	eee l
				>

8. If you want to filter out the packets which do not belong to iSCSI protocol, you can use the filter again. Input the string "**iSCSI**" in **Filter** column and click **Apply**. Then all packets which do not belong to iSCSI protocol will be filter out.

🗖 (Untitled) - Wireshark				. 🗆 🛛
<u>File Edit View Go Capture Analyza</u>	e <u>S</u> tatistics Telephony <u>T</u> ools <u>H</u> elp			
				5 »
Filter: iscsi		▼ Expression Clear Apply		
No Time	Source	Destination	Protocol	Info 🔷
46 48.886244	192.168.11.87	192.168.11.200	iscsi	SCS
47 48.886332	192.168.11.200	192.168.11.87	iscsi	SCS
48 48.886360	192.168.11.87	192.168.11.200	iscsi	SCS
49 48.886443	192.168.11.200	192.168.11.87	iscsi	SCS
50 48.886523	192.168.11.87	192.168.11.200	iscsi	SCS
51 48.886586	192.168.11.200	192.168.11.87	iscsi	SCS
52 48.886648	192.168.11.87	192.168.11.200	iscsi	SCS
53 48.886726	192.168.11.200	192.168.11.87	iscsi	SCS
54 48.886756	192.168.11.87	192.168.11.200	iscsi	SCS
55 48.886842	192.168.11.200	192.168.11.87	iscsi	SCS
56 48.886876	192.168.11.87	192.168.11.200	iscsi	SCS
57 48.886961	192.168.11.200	192.168.11.87	iscsi	SCS
58 48.887002	192.168.11.87	192.168.11.200	iscsi	SCS
59 48.887078	192.168.11.200	192.168.11.87	iscsi	SCS
60 48.887114	192.168.11.87	192.168.11.200	iscsi	SCS
61 48.887194	192.168.11.200	192.168.11.87	iscsi	SCS
62 48.887391	192.16 11.87	192.168.11.200	iscsi	SCS
63 48.887462	192.168.11.200	192.168.11.87	iscsi	SCS
64 48.887519	192.168.11.87	192.168.11.200	iscsi	SCS
65 40 007570	107 160 11 700	107 160 11 07	iccet	ere 🞽
<				>
Frame 5 (190 bytes on wir	e. 190 bytes cantured)			
Ethorpot II Spc: Acustok	(0, 1) $(0, 1)$ $(0, 1)$	c.91) Det. Occuptoch of	.04.76 (00	.12.70.
	92.168.11.87 (192.168.11.6	87). Dst: 192.168.11.20	0 (192.168	.11.200
Transmission Control Drot	ocol Src Port: robcod lm	(1509) Det Port: jece	i_target (2260)
in ansin's ston control Prot	ocor, sic Porc. robcad-im	(1909), DSC POLC: ISCS	i-carget (5200), 1
H ISCSI (LUGIN COmmand)				
<				>



White Paper

 You can save the capture result to a file, remember to choose the radio button of Displayed in the Packet Range. This will save the packets which have been filtered.

Wireshark: Save file as							
Save in:	📋 My Documents			•			
My Recent Documents Desktop My Documents My Documents	My Music My Pictures SnagIt Catalog						
S	File name: test		-	Save			
My Network Places	Save as type: Wires	hark/topdump/ li	ibpcap (*.pcap;*.cap) 💌	Eancel			
Packet Range All packets Selected packet Marked packets First to last I Range:	C Captured 105 acket 1 skets 0 marked 0 0	Displayed 83 1 0 0		Help			

Special case

How can I capture the packets of the communication between **QSAN P series** controller and the surveillance device? In this case, you could not install **Wireshark** program in iSCSI target or surveillance device. The solution is to use the **Port Mirror** function which can mirror the network traffic from one port to another in a specified network switch. Setup a mirror port to iSCSI target or surveillance device, and then connect this port to a host with **Wireshark**. When the traffic begins, the host with **Wireshark** can do the good job.

Here I use the HP Procurve switch as an example. In the picture below, port 6 is connected to **P200C** iSCSI data port and port 1 is connected to a host with **Wireshark** installed. After setup port mirror, all packets which pass through to port 1 will mirror a copy to port 6. So I can capture the entire packets between the iSCSI target and any other network device.



White Paper

ProCurve Networking HP Innovation	Profession Barrier and Barrier	ProCurve 1800-24G			 Link Status: Up Down 	
▶ SYSTEM	Port Mirroring	1				
✓ PORTS	This page enables you	to set up the port mirroring	features of the switch	to enable traffic monitoring.		
Configuration	Port to Mirror to					
Statistics		Port to Mirror to	1 💌			
▶ TRUNKS	Ports to Mirror					
▶ VLANS	Port	Mirroring Enabled	Port	Mirroring Enabled		
► LLDP	1		13			
▶ SNMP	2		14			
► DIAGNOSTICS	3		15			
SUPPORT	4		16			
▶ LOGOUT	5		17			
	6		18			
	7		19			
	8		20			
	9		21			
	10		22			
	11		23			
	12		24			
			HELP	APPLY CANCEL		

Summary

In case of iSCSI initiator can not work with the iSCSI target properly, you can use the **Wireshark** to capture the packets and send them to **QSAN** Support Team. We will find out the problem by analyzing the packets. The ability of capturing the network packets will be helpful when you meet problem with the connection between the IP SAN.

Applies to

All QSAN P series controllers

References

Wireshark http://www.wireshark.org/