

How to configure an Advanced Expert Probe as NetFlow Collector

created by: Rainer Bemsel - Version 1.0 - Dated: Jan/31/2012

There are two types of NetFlow collectors in Observer. In most cases, it will likely be the NetFlow Trending collector being configured. The Trending Collector supports up to 512 NetFlow devices, whereas the NetFlow Collector only supports one NetFlow Device. That means you must add and configure a NetFlow Collector for each NetFlow device in your environment.

The purpose of this document is to outline the required steps to configure Network Instruments Advanced Expert Probe to run as a NetFlow Collector.

Configure Network Instruments Advanced Expert Probe as a NetFlow Collector

If you are not already connected to a NetFlow Trending collector, redirect on to your local Observer by choosing Actions -> Redirect Probe

After the probe is connected, select the NetFlow collector and right-click. Choose Administer Selected Probe. Log in to the probe



Click the New Instance button

Probe Administration: Rainer's Advanced Expert	Probe (192.168.10.79)			in the second	23
🎦 New Instance 🛛 Configure Memory 🖉	Rename 🗙 Delete			900 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100 - 100	
ID Probe Instance Name	Instance Type	Packet Capture Buffer	Statistics Queue	Statistics Configuration	Description
1 Instance 1	Probe	16 MB	16 MB	Medium (default)	



DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consu each Vendor for further information or support.

Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or atherwise charge the information contained within for any reaso and without notice. This technate has been created after studying the material and / or practical evaluation by myself. All liability for use of the information presented here remains with the user Choose NetFlow Trending collector - Type a name and a description for the collector, and click Next

Edit Probe Instance Select instance ID, edit name and description.	
Probe instance ID: 2	
Instance Type:	
O Probe	
NetFlow collector (single flow)	
SFlow collector	
MPLS Probe	
NetFlow Trending collector (multiple flows)	<u> </u>
Probe instance name:	2
Probe instance name: Netflow Trending Description:	2
Probe instance name: Netflow Trending Description:	2
Probe instance name: Netflow Trending Description:	2
Probe instance name: Netflow Trending 2 Description:	2
Probe instance name: Netflow Trending Description:	2

Choose a statistics memory configuration. For most users, the default should be sufficient,

Select the memory allocation and config Observer Statistics. Edit the size of Pac	uration for ket Capture Buffer.
Probe instance name:	etflow Trending
Packet capture and GigaStor buffer (MB):	0 MB
Statistics queue buffer (MB):	16 MB
Free Observer reserved memory:	968 MB
Note: Parallel processing in Observer require for the statistics queue and packet capture b If a Probe instance function is to collect statis should be allocated to statistics queue buffer Capture or GigaStor, most of the memory sh nay need to reserve 1GB or more for either extractions and the statistic of the statistics is a statistic of the statistic of the statistic of the statistics is a statistic of the statistic of the statistic of the statistics is a statistic of the statistic of the statistic of the statistic of the statistic is a statistic of the statistic	s that you allocate sufficient amount of memory uffers. sites, treading or analysis, most of the memory . If a Probe instence is collecting data for Packet ould be allocated to packet capture buffer. You or both of the buffers on a heavily loaded
Note: Parallel processing in Observer require for the statistics quue and packet capture b ff a Probe instance function is to collect statist found be allocated to statistics que buffer Capture or GigaStor, most of the memory sh may need to reserve 1GB or more for either of network. Statistics memory configuration: #§ Medium (default)	s that you allocate sufficient amount of memory uffers. sites, treading or analysis, most of the memory . If a Probe instence is collecting data for Packet ould be allocated to packet capture buffer. You or both of the buffers on a heavily loaded
Note: Parallel processing in Observer require for the statistics queue and packet capture b If a Probe instance function is to collect status foculd be allocated to statistics queue buffer Capture or GigaStor, most of the memory sha may need to reserve 1GB or more for either network. Statistics memory configuration: BM Medum (default) View	s that you allocate sufficient amount of memory uffers. Joba, trending or analysis, most of the memory I. Ta Probe instance is collecting data for Packet puld be allocated to packet capture buffer. You or both of the buffers on a heavily loaded
Vote: Parallel processing in Observer require fr a Probe instance function is to collect stabut fr a Probe instance function is to collect stabut house be allocated to stabistics queue buffer Capture or GigaStor, most of the memory sha may need to reserve 1GB or more for either network. Stabistics memory configuration: ES Medum (default) View	s that you allocate sufficient amount of memory uffers. Joba, trading or analysis, most of the memory I. Ta Probe instance is collecting data for Packet suid be allocated to packet capture buffer. You or both of the buffers on a heavily loaded

Choose a network adapter to use to monitor the NetFlow device.



Select a network Adapt collected Probe instar	er and Redirection ter from the list. You may redirect ce statistics to a remote Observer.	
Probe instance name:	Netflow Trending	
Data Source(s):		
Note: Please	define Data Source(s) in Network Trending - Settin	gs.
Selected network adapter 1 Management [Intel(R) PRO Monitor [Intel 8255x-base	or incoming Flow data: /100 VE Network Connection] I PCI Ethernet Adapter (10/100)]	
Selected network adapter Management [Intel(R) PRC Monitor [Intel 8255x-base	or Incoming Flow data: /100 VE Network Connection] PCI Ethernet Adapter (10/100)] Auto-Sele	ect Adapter
Selected network adapter (Management [Intel(R) PR(Monitor [Intel 8255x-base Probe Instance Redirect	or incoming Flow data: /100 VE Network Connection) IPCI Ethernet Adapter (10/100)) Auto-Sele	ect Adapter
Selected network adapter i Management [Intel(8) PRG Monitor [Intel 8255x-base Probe Instance Redirect © Connect remote Prob	or incoming Flow data: /100 VE Network Connection] IPCI Ethernet Adapter (10/100)] Auto-Sele on: e instance to this Observer (192.168.10.231)	ect Adapter
Selected network adapter 1 Management [Intel(R) PRO Monitor [Intel 8255x-base Probe Instance Redirect © Connect remote Prob © Disconnect	or incoming Flow data: /100 VE Network Connection) I PCI Ethernet Adapter (10/100)] Auto-Sele on: E instance to this Observer (192, 168, 10, 231)	sct Adapter
Selected network adapter Management [Intel(8)] PRO Monitor [Intel 8255x-base Probe Instance Redirect © Donnect remote Prob © Disconnect remote Prob © Disconnect a specifie Redirect to a specifie	or Incoming Flow data: //100 VE Network Connection) I PCI Ethernet Adapter (10/100)] an: e instance to this Observer (192.168.10.231) d IP address or DNS name 0.0.0.1 0/ved to IP address):	sct Adapter
Selected network adapter Management (Intel(2) PRO Monitor (Intel 8255x-base Probe Instance Redirect © Connect remote Prob © Disconnect Redirect to a specific (DNS name will be ret © Redirect to Probe's o	or Incoming Flow data: //100 VE Network Connection) IPCI Ethernet Adapter (10/100)] a unit of the second	er Observer)

Click Finish

Step 4 - Configure Network Trending Settings

Ensure your NetFlow Trending collector is selected in the list of probes and choose Trending/Analysis -> Network Trending.



The Network Trending window opens.



🛃 Network Trending - Netflow Trending	/ Rainer's Advanced Exper	t Probe					
🕞 Start 📵 Stop 🗉 Settings 🔶	Ánalysis 🔍 Tools						
Current time:::- Filter: Not usi	ng filters Schedule: No	scheduling CPU (per core	%): 0.00 Fifo (%):	0.00			
Start time:::- End time:::-	Interval (min):						
IP Pair (Port)	Data Source Source ID	Collect Data by	Status	Count	IP Pairs	Packets	Bytes
	1	·	1				

Click the Settings button

13E	General Schedule Data Tran	sfer					
General	Data Sources:						- H
	Source IP Address A	Target IP Address	Source ID	UDP Port	Collect Data by	Description	
				NetFlow Flow A	Trending Data Sc gent:	ource	
				Source	IP address:	192 . 168 . 1	0.25
	<			- Sour	ce ID:	0	
	Add Edit	. Delete		Destina	tion IP address:	192 . 168 . 1	0.79
	Collection Settings:			Destina	tion port:	9995	
	Statistics collection interva	1: 10 minutes	•	Descript	tion:		
				Collect © Ir © A	: Data by: nterface Index utonomous System	0	

Click on Add

Enter your Router IP Address as Source. I don't use a Source ID. Enter the IP Address of your Collector Because Reporter Analyzer is sending data on port 9995, I had to change the default 9996 to 9995.

Click on OK



Gene	eral Schedule Data Tra	ansfer				
	Data Sources:	1		1		
	Source IP Address A	Target IP Address	Source ID	UDP Port	Collect Data by	Descript
	192.168.10.254	192.168.10.79		9995	Interface Index	
	<					
	Add Edit	Delete	m			
	Add Edit Collection Settings:	Delete	m			
~	Add Edit Collection Settings: Statistics collection interv	Delete				

Change the Collection interval to 1 minute. Click on OK to close the Network Trending Settings window

🛃 Network Trending - Netflow Trending	/ Rainer's Advanced	Expert Probe						×
🜔 Start 🔳 Stop 🗉 Settings 🔍	Analysis 🛛 🔻 Too	ls						
Current time: 17:24:10 Eilter: Net u	eing filtere – Cohod	ula: No ochoduling	CPU (per core %): 0	00 56	(%)- 0.00			
Start time: 17:24:00 End time: 17:2	5:00 Interval (min	ale. No schedaling	CFU (per core %). U	Filo	(%). 0.00			
Data	Source		Chabur	Count	ID Doite	Dealers	Dutas	
IP Pair (Port) 🔺	Source ID	Collect Data by	Status	Lount	IF Pairs	Packets	Bytes	
192.168.10.254->192.168.10.79 (9995)		Interface Index	30%	3 Interfaces	62	2677	1.92e6	

Click on Start to begin monitoring the NetFlow Device

After you have collected some data, click the Analysis button. The View Network Trending data dialog opens. Choose "Transfer and view current day statistics" and click OK. This opens the Network Trending Viewer in a new tab.



In the Network Trending Viewer you can see for your NetFlow Devices:



- Station Activity Time
- Top Talkers
- Packet Size Distribution
- Bandwidth Size Utilization

Ketwork Trending Viewer - Rainer's	Advanced Expert Probe\J	nstance02\192.168.10.254->	192.168.10.79,Port	9995\IP\2012-0:	30											C		8
IIS Go to Previous Day IIS Go to N	ext Day 🔲 Settings	▼ View ▼ Tools	Refresh Report	t														
	Show data for all time in																	
🛓 🧔 Rainer's Advanced Expert Probe	Select statistic ty	pe:																
inst Netflow Trending	All Connections		-															
in 192.168.10.254->192.168.	Stations: 1695 Pa	ckets: 287292 Bytes: 1	28e6															
🕀 🖵 Interface Index	Interface	T 11 1 1 10 100	Packets	Butes		0.1.1.0							Time Sp	ban				
₽- ₽ ₽ 2010 1	Index	Talking to (by IP)	Total	Total	Packets I -> 2	Packets I <- 2	Bytes I -> 2	Bytes I <- 2	0	2 4	6	8 1	0 12	14 1	6 18	20 27	2 24	
2012 January	26	p578e2a78.dip.t-dialin.net	67036	30.6e6	39150	27886	25.5e6	5.14e6 📃										
	23	130.119.250.4	56695	17.7e6 🔜	24817	31878	5.48e6 📕	12.2e6								<u> </u>		
H. CAN	26	192.168.10.5	29157	9.10e6 📕	16116	13041	6.23e6	2.87e6										
	26	cupertino.bemsel.home	14994 📕	9.21e6 📕	8784 📕	6210 🔳	8.39e6 📕	829104										
	23	192.221.126.254	10371 📕	9.17e6 📕	3455	6916 🔳	583248	8.58e6							h			
	26	reddell.bemsel.home	9558	5.00e6	4894	4664	4.16e6	838698							- M.			
	26	SNUSER-PC	8838 🛔	6.56e6	5263	3575	6.01e6 📕	547849										
	23	mta.superchat.at	4610	573762	2404	2206	180352	393410							- b			
	0	cupertino.bemsel.home	3782	296269	0	3782 🚦	0	296269						1		4		
	23	173.194.6.102	3465	3.37e6	1229	2236	51220	3.32e6 📕								i		
	23	csco-2802-dsl.bemsel.home	3146	2.21e6	1422	1724	367980	1.84e6							il in the second se			
	23	ra2.bemsel.home	2894	2.10e6	2894	0	2.10e6	0										
	23	mail.spamarrest.com	2450	2.21e6	844	1606	34610	2.17e6							- i(h			
	23	*.13.san.plaxo.com	2238	97954	1120	1118	49120	48834							i de la composition	4		
	0	BEMRA01-W7	2001	144962	0	2001	0	144962							-			
	23	www-10-01-pm1.facebook	1944	1.46e6	816	1128	209456	1.25e6								1		
	23	myaccount.flukenetworks.c	1880	1.48e6	764	1116	151718	1.32e6							1			
	23	194.25.94.179	1844	1.25e6	886	958	175988	1.07e6								1		
	23	95.142.109.92	1687	1.44e6	653	1034	31550	1.41e6							- E			
	23	213.95.79.75	1664	737658	898	766	148854	588804							- In			
	23	www.spin.de	1492	730884	738	754	120964	609920							1			
	23	a92-122-24-124.deploy.aka	1426	1.26e6	562	864	78696	1.18e6							1			
	23	cds19.lon9.msecn.net	1370	1.34e6	476	894	36262	1.30e6							1			
	23	87.252.216.126	1362	1.87e6	12	1350	2272	1.87e6								1		
4 III >>	23	cds294.lon9.msecn.net	1358	1.29e6	474	884	37488	1.26e6						j.	1			-
Refresh Tree	Internet Patro	IP to IP Pairs (Matrix)	/															







Configure Network Single NetFlow Collector for live statistics

Live statistics are details about the flow that appear in Observer in as few as five seconds. The kind of NetFlow collector provides the same trending data as above, but it also includes NetFlow statistical data. However, you must configured one NetFlow collector for each NetFlow device you wish to monitor.

If you are not already connected to a NetFlow Trending collector, redirect on to your local Observer by choosing Actions -> Redirect Probe

After the probe is connected, select the NetFlow collector and right-click. Choose Administer Selected Probe. Log in to the probe

Click the New Instance button

Probe Administration: Rainer's Advanced Expert	Probe (192.168.10.79)			is from the	23
🐴 New Instance 🛛 Configure Memory 📲	Rename 🗙 Delete				
ID Probe Instance Name	Instance Type	Packet Capture Buffer	Statistics Queue	Statistics Configuration	Description
1 Instance 1	Probe	16 MB	16 MB	Medium (default)	

Choose NetFlow collector (single flow) and give it a name.

•]		
•]		
	J		
ow) 🖌			1
(multiple flows))		
•			2
	· (multiple flows)	r (multiple flows)	· (multiple flows)

Click on Next



Edit Probe Instance	23
Configure Observer/Probe Instance M Select the memory allocation and configu Observer Statistics. Edit the size of Pack	emory aration for et Capture Buffer.
Probe instance name: Net	Flow Live Statistics
Packet capture and GigaStor buffer (MB):	0 MB
Statistics queue buffer (MB):	16 MB
Free Observer reserved memory:	952 MB
If a Probe instance function is to collect statis should be allocated to statistics queue buffer. Capture or GigaStor, most of the memory sho may need to reserve 1GB or more for either o network. Statistics memory configuration:	cc, trenuing or analysis, most of the memory If a Probe instance is collecting data for Packet uld be allocated to packet capture buffer. You r both of the buffers on a heavily loaded
Hedium (default)	•
View	
< Back	Next > Cancel Help

Choose a statistics memory configuration. For most users, the default should be sufficient. Click on Next

Select Network Adapter a Select a network adapter collected Probe instance	and Redirection r from the list. You may redired statistics to a remote Observe	ct er.
robe instance name:	NetFlow Live Statis	tics
Data Source (DNS names will	be resolved to IP addresses):	
Flow source IP address or DNS name:	192.168.10.254	SNMP Settings
Source ID:	0	Collect Data by:
Flow destination IP address or DNS name:	192.168.10.79	Interface Index Autonomous System
Flow destination port:	9995	
elected network adapter for i Management [Intel(R) PRO/1(Monitor [Intel 8255x-based Po	ncoming Flow data: 00 VE Network Connection] CI Ethernet Adapter (10/100)]	
elected network adapter for i Management [Intel(R) PRO/11 Monitor (Intel 8255x-based Pr	ncoming Flow data: 00 VE Network Connection] CI Ethernet Adapter (10/100))	
elected network adapter for Janagement [Intel(R) PRO/11 Jonitor [Intel 8255x-based Pr	ncoming Flow data: 20 VE Network Connection] CI Ethernet Adapter (10/100)]	Auto-Select Adapter
elected network adapter for i danagement [Intel(R) PRO/11 frontor [Intel 8255x-based Pl Probe Instance Redirection: © Connect remote Probe in	ncoming Flow data: 10 VE Network Connection] CI Ethernet Adapter (10/100) Istance to this Observer (192	Auto-Select Adapter
elected network adapter for i danagement [Intel(R) PRO/11 frontor [Intel 8255x-based Pl Probe Instance Redirection: © Connect remote Probe in © Disconnect	ncoming Flow data: 10 VE Network Connection] CI Ethernet Adapter (10/100) Istance to this Observer (192.	Auto-Select Adapter 168. 10. 231)
elected network adapter for i lanagement [Intel(R) PRO/II forntar [Intel 8255x-based Pl Probe Instance Redirection: © Connect remote Probe in © Disconnect © Redirect to a specified IF (DNS name ville persol)	ncoming Flow data: 10 VE Network Connection] c1 Ethernet Adapter (10/100) istance to this Observer (192. 2 address or DNS name ed to IP address):	Auto-Select Adapter 168.10.231) 0.0.0.1
elected network adapter for i Management [Intel(R) PRO/1(Monitor [Intel 8255x-based P Probe Instance Redirection: © Connect remote Probe in © Disconnect © Disconnect © Redirect to a specified IF (DNS name will be resolv © Redirect to Probe's own	ncoming Flow data: 20 VE Network Connection] CI Ethernet Adapter (10/100) astance to this Observer (192. P address or DNS name ed to IP address): Observer (if redirecting an Ins	Auto-Select Adapter 168. 10. 231) 0.0.0.1 itance from another Observer)

IN the Data Source section, type the IP Address of the NetFlow device you want to monitor. Choose a UDP ports. The default is 9996. If necessary, set the Source ID. The Source ID guarantee uniqueness for all flows exported from a particular device. The format of this field is vendor specific. Collector devices should us the combination of the source IP address plus the Source ID field to associate an incoming NetFlow export packet with a unique collector of NetFlow on a particular device.



Click the SNMP Settings button to tell Observer how SNMP is configured on your devices.

SNMP settings will be about NetFlow device	used to get information ports in the Discovery Mode window.	
IP address:	192 . 168 . 10 . 254	
Timeout:	5 econds	
Retries:	3 🚔 times	
SNMP version:	SNMPv2	
Security user name:		
Auto-discover Context	Engine ID	
Context engine ID:	HEX	
Community string:	public	
SNMPv3 Security		
Apply USM key localized	ation to passwords	
Authentication protocol:	noAuth (none) 👻	
Authentication password	(key):	
Privacy protocol:	noPriv (none)	
Privacy password (key):		
Authentication time wind	ow (seconds):	

SNMPv1, v2 & v3 are supported. Click on OK to return to previous window. Finally, choose the network adapter to use to monitor the NetFlow device and click finish. It's now OK to close the Probe Administration window.

