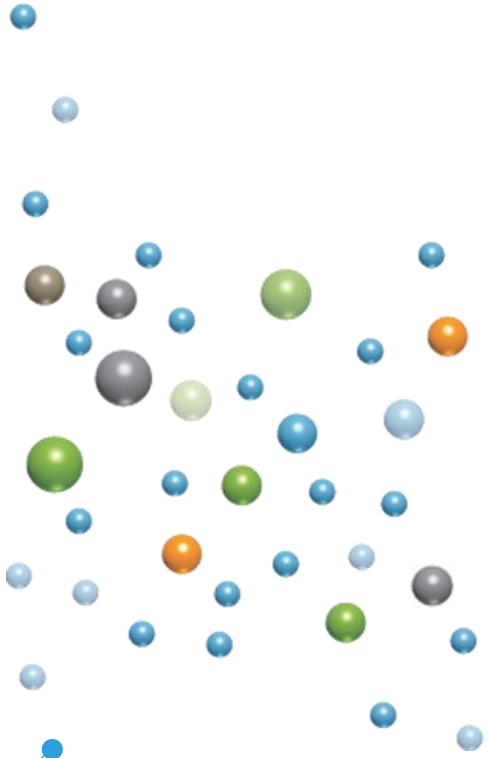
ORION Net Flow and OPNET-2013



ORION Engineering Team

March 7 2013

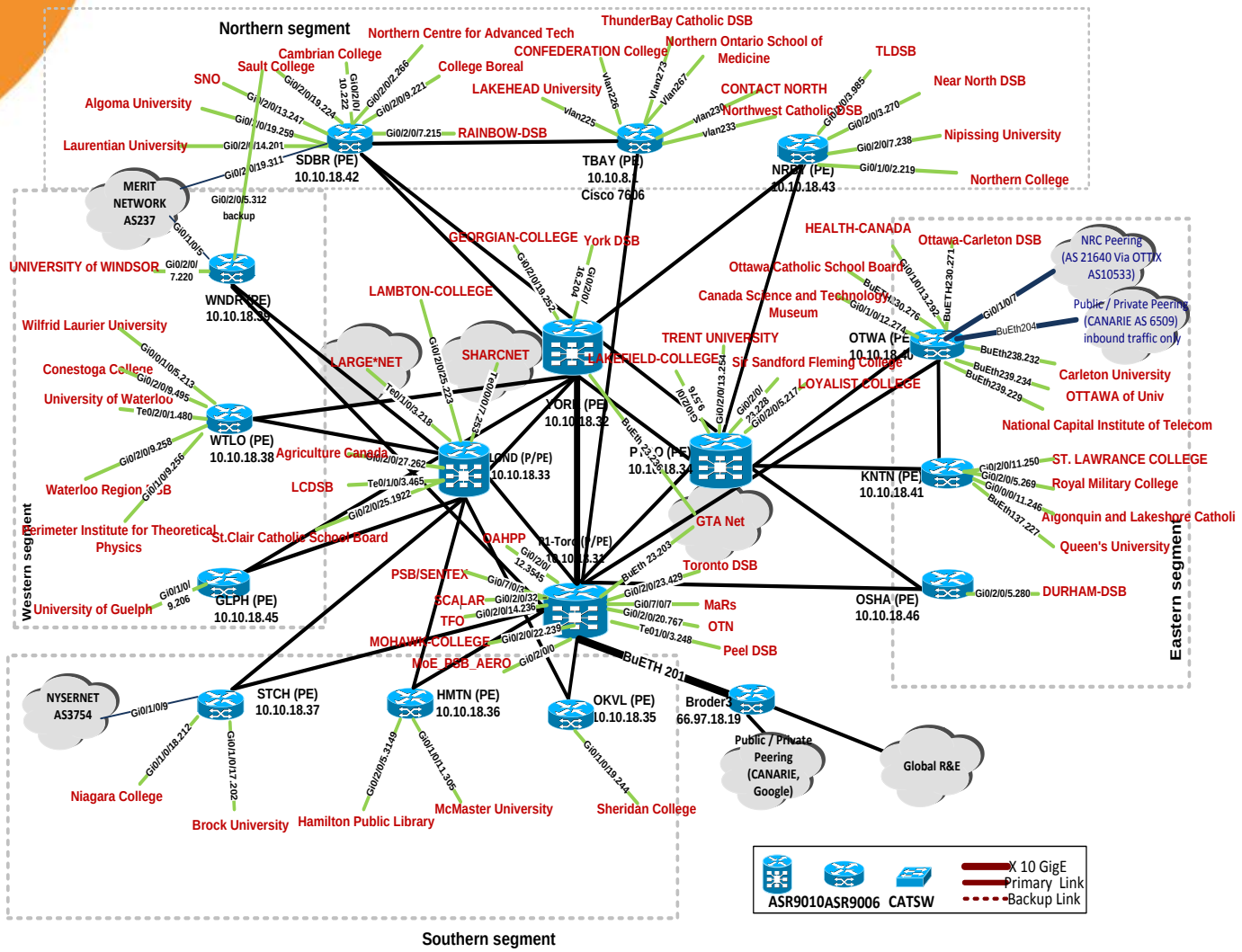
orion
Ontario's backbone of innovation

Content

- ORION Member Connection Diagram
- NetFlow Introduction and Setup @ ORION Network
- OPNET ARX Deployment
- OPNET Data Analysis
- OPNET Data Report
- OPNET ARX Alert Manager
- OPNET Deployment Advance

orion
Ontario's backbone of innovation

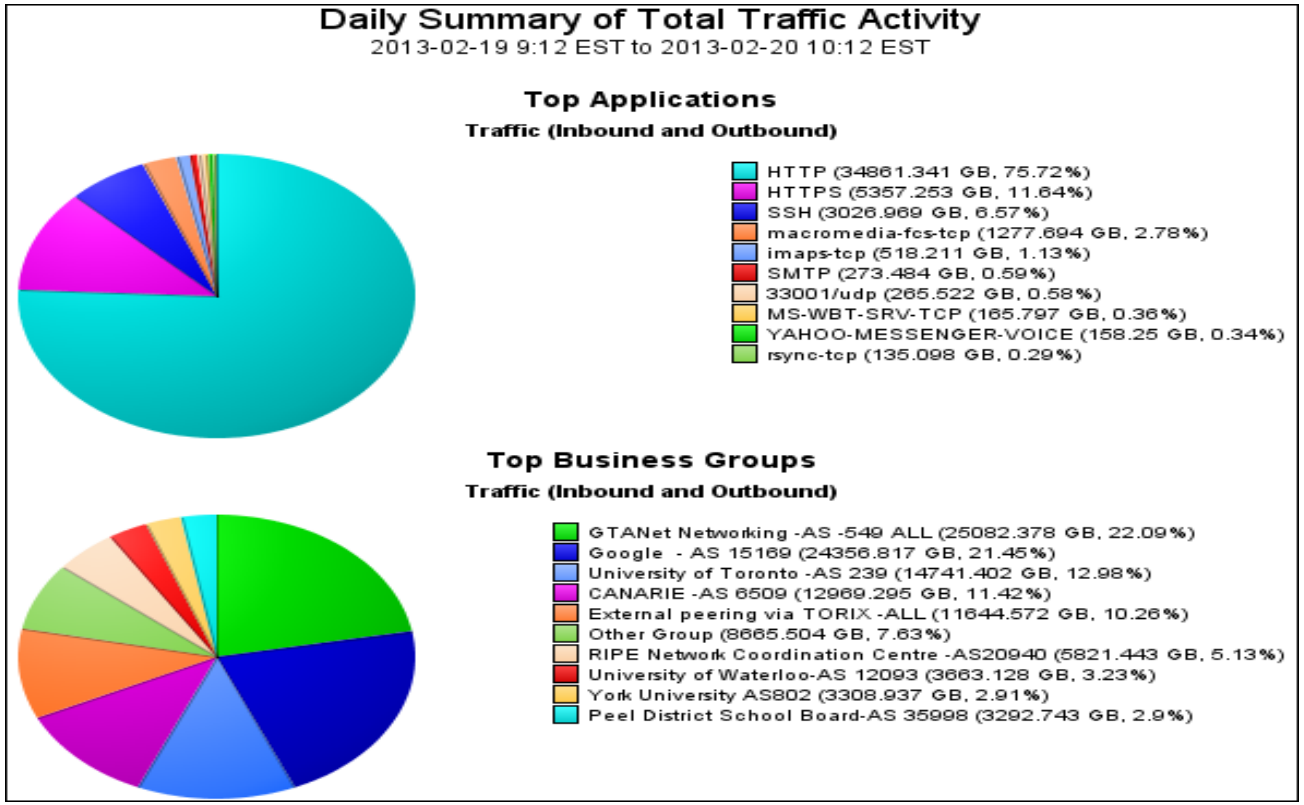
ORION Member Connection



orion
Ontario's backbone of innovation

ORION Member Connection Cont'd

BGP Setup number	Orion adversited BGP entires	AS number @Orion
66	285	Public 56 / Private 23

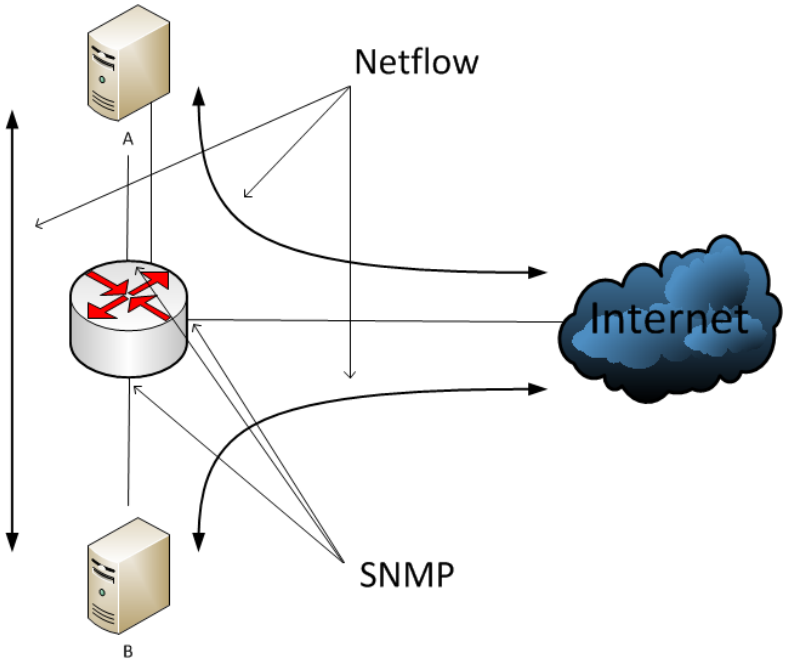


orion
Ontario's backbone of innovation

NetFlow Introduction and Setup @ ORION Network

What is Netflow?

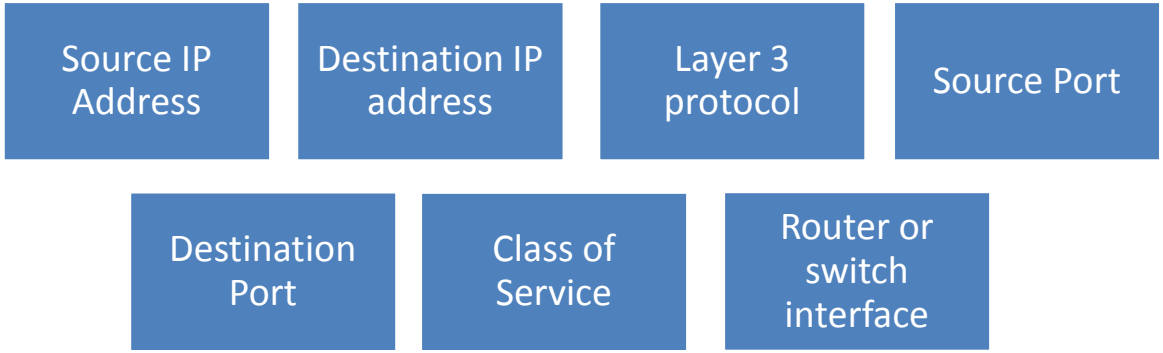
Instead of capturing counters at physical interface like SNMP, it captures the flow of information



orion
Ontario's backbone of innovation

NetFlow Introduction and Setup @ ORION Network

Different from SNMP, it samples packets and gathering the following information:



Source address tells who is originating the traffic
Destination address tells where the traffic is going to
Ports characterize the application
Class of service examines the priority of the sampled flow
The device interface tells how traffic is being routed by the networking device
Tallied packets and bytes show the amount of traffic
Timestamps are collected to calculating packets and bytes per second
Next hop IP addresses including BGP routing Autonomous Systems (AS)
Subnet mask for the source and destination addresses to calculate prefixes
TCP flags to examine TCP handshakes

orion
Ontario's backbone of innovation

NetFlow Introduction and Setup @ ORION Network

Netflow Exporter-map:

```
flow exporter-map fem1
version v9
 options interface-table
 options sampler-table
 template data timeout 60
!
transport udp 9996
source Loopback0
destination 66.97.19.7
!
```

Netflow Monitor-map:

```
flow monitor-map fmm1
 record ipv4
 exporter fem1
 cache entries 65535
 cache timeout active 60
 cache timeout inactive 15
```

Netflow Sampler map:

```
sampler-map fsm1
 random 1 out-of 100
!
```

Netflow interface setup:

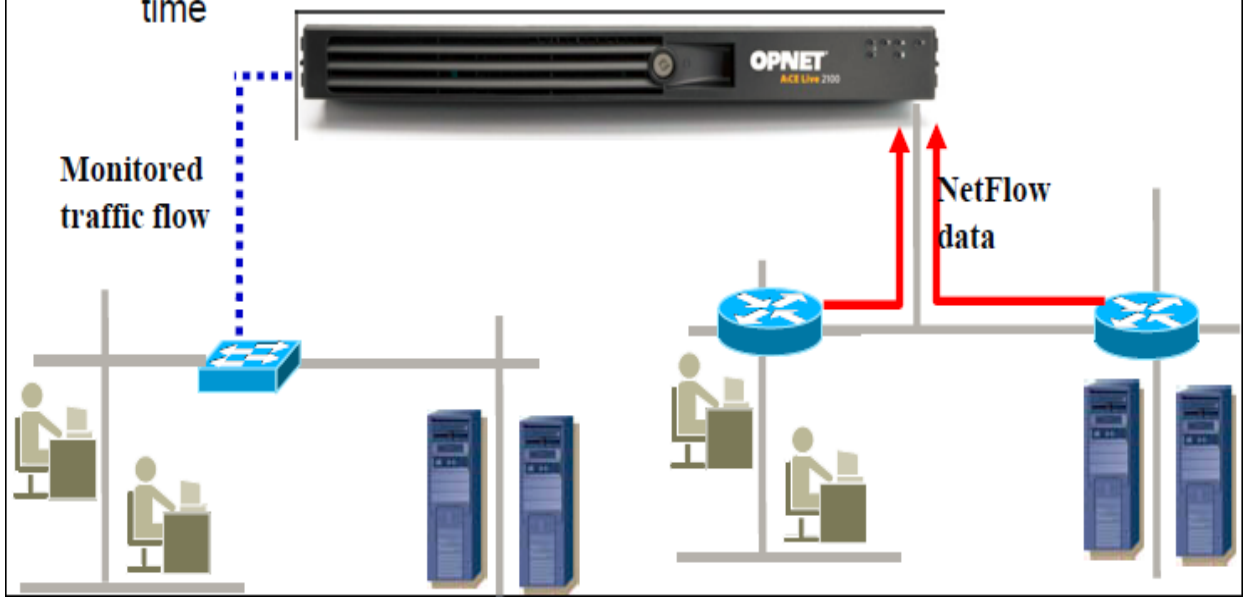
```
 flow ipv4 monitor fmm1 sampler fsm1 ingress
 flow ipv4 monitor fmm1 sampler fsm1 egress
```

orion
Ontario's backbone of innovation

OPNET ARX Deployment

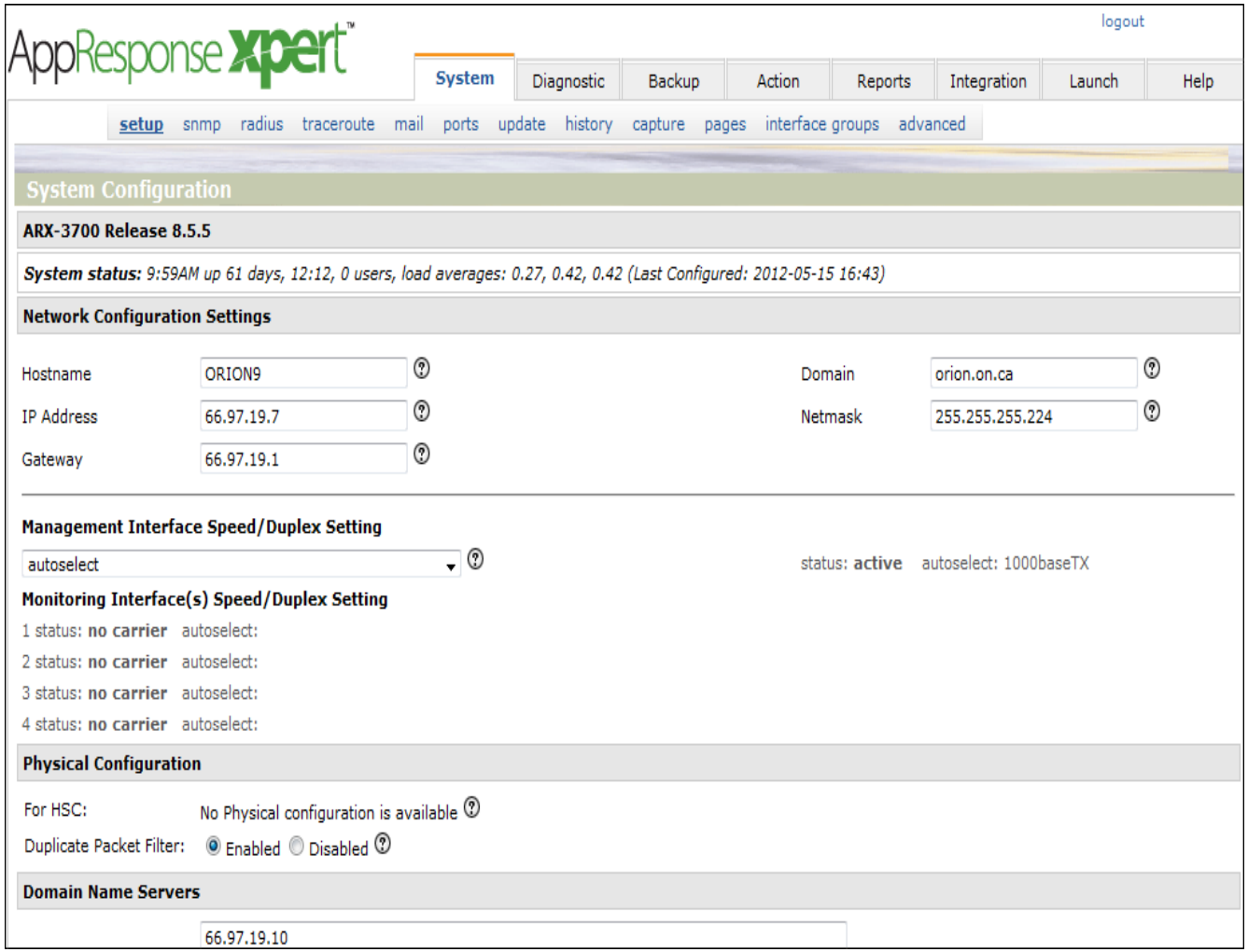
Traffic

- Packet Monitoring
  - Passive data collection via SPAN or Network TAP
  - Data is extracted from TCP/UDP/IP headers in real-time
- NetFlow Collection
  - Sent from NetFlow-enabled devices
  - Stand-alone or combined with monitoring



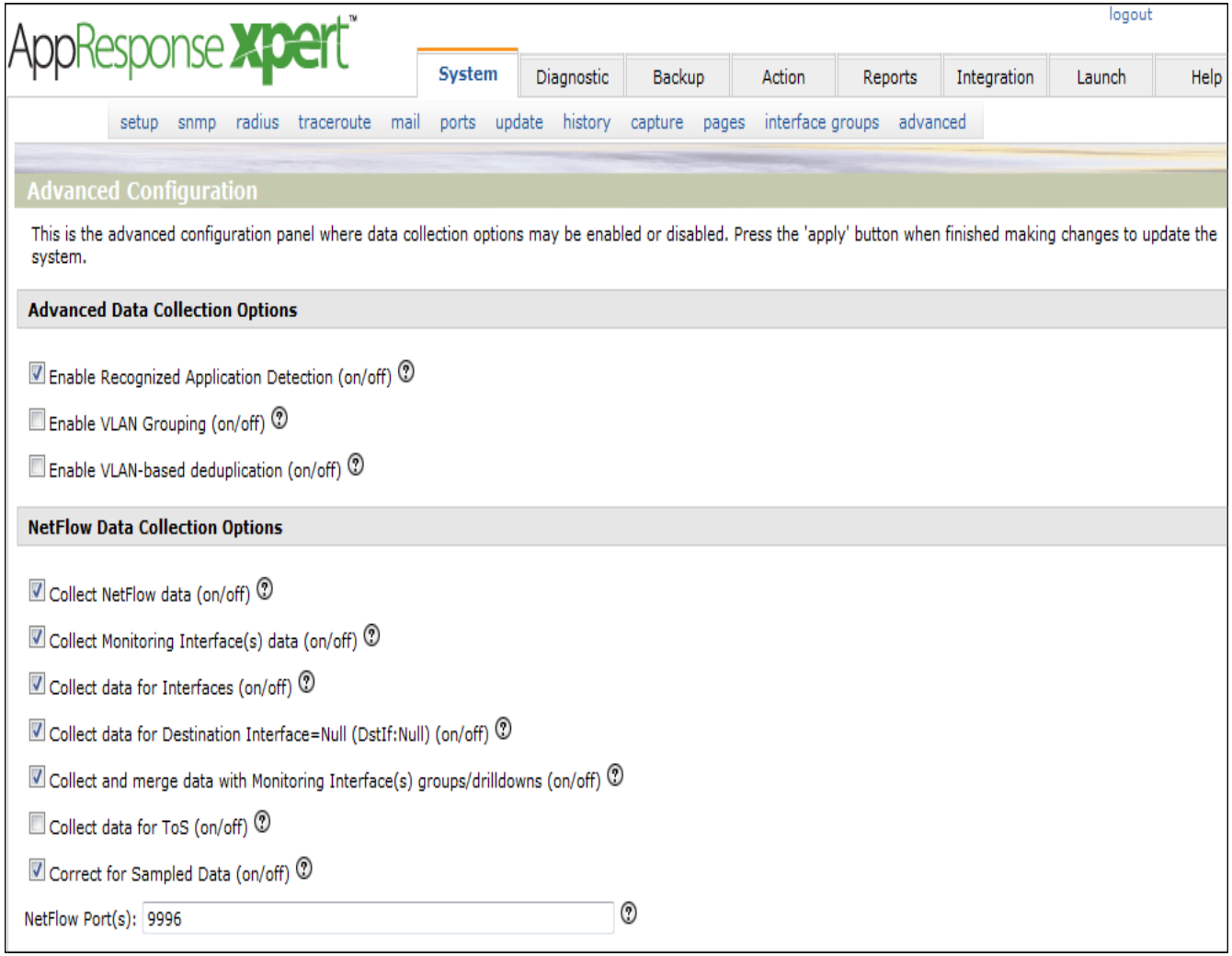
orion
Ontario's backbone of innovation

OPNET ARX Deployment Cont'd



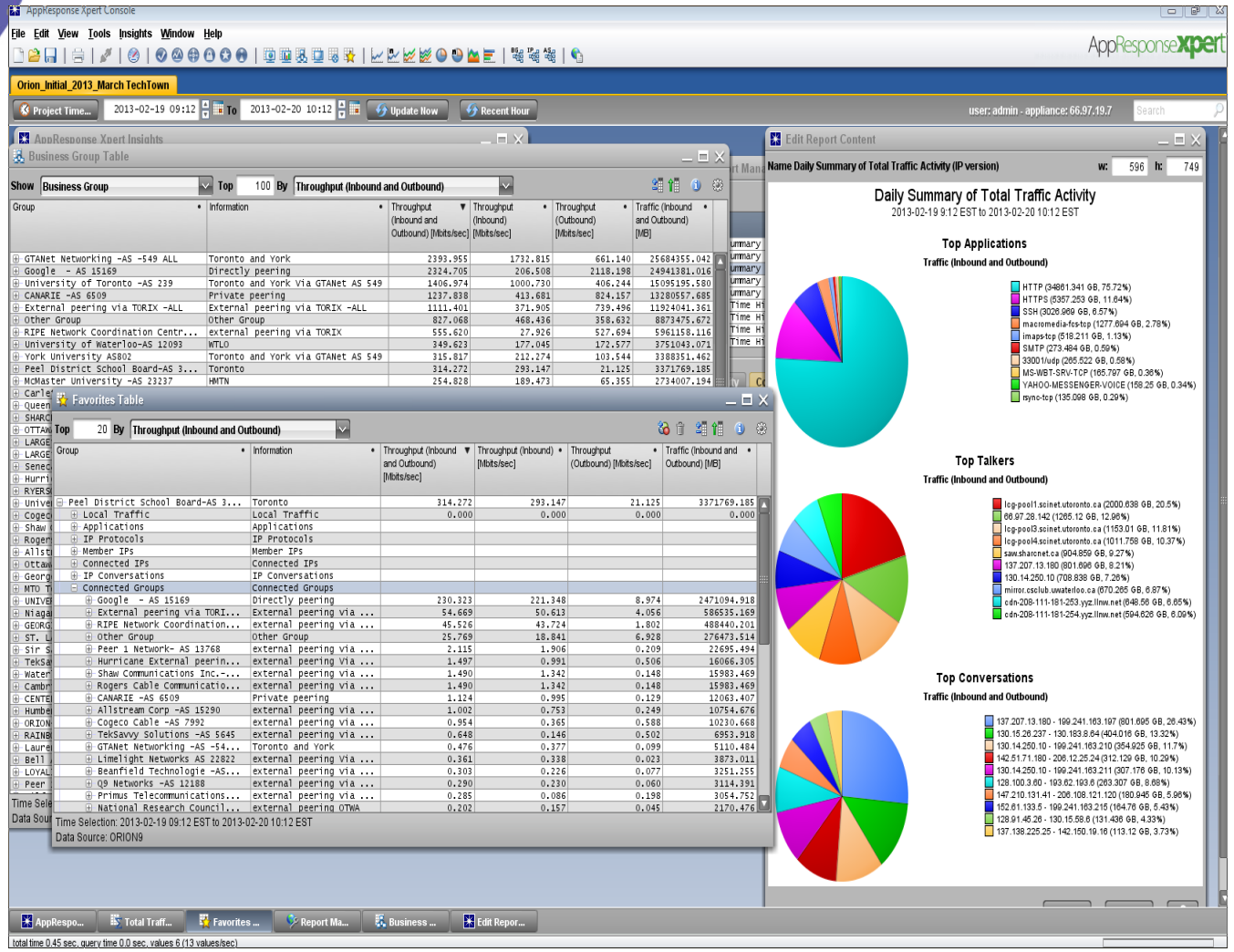
orion
Ontario's backbone of innovation

OPNET ARX deployment Cont'd



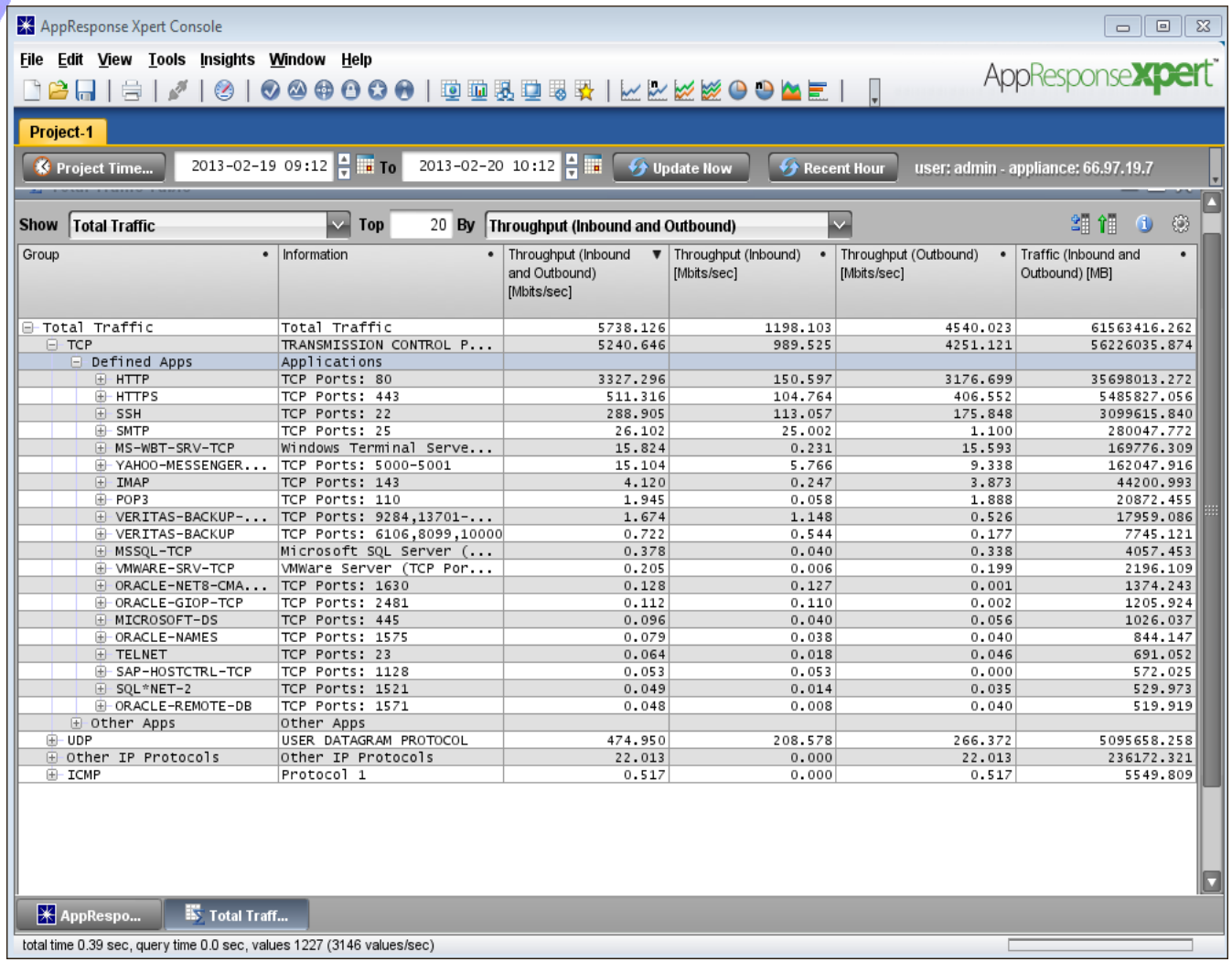
orion
Ontario's backbone of innovation

OPNET ARX Deployment Cont'd



orion
Ontario's backbone of innovation

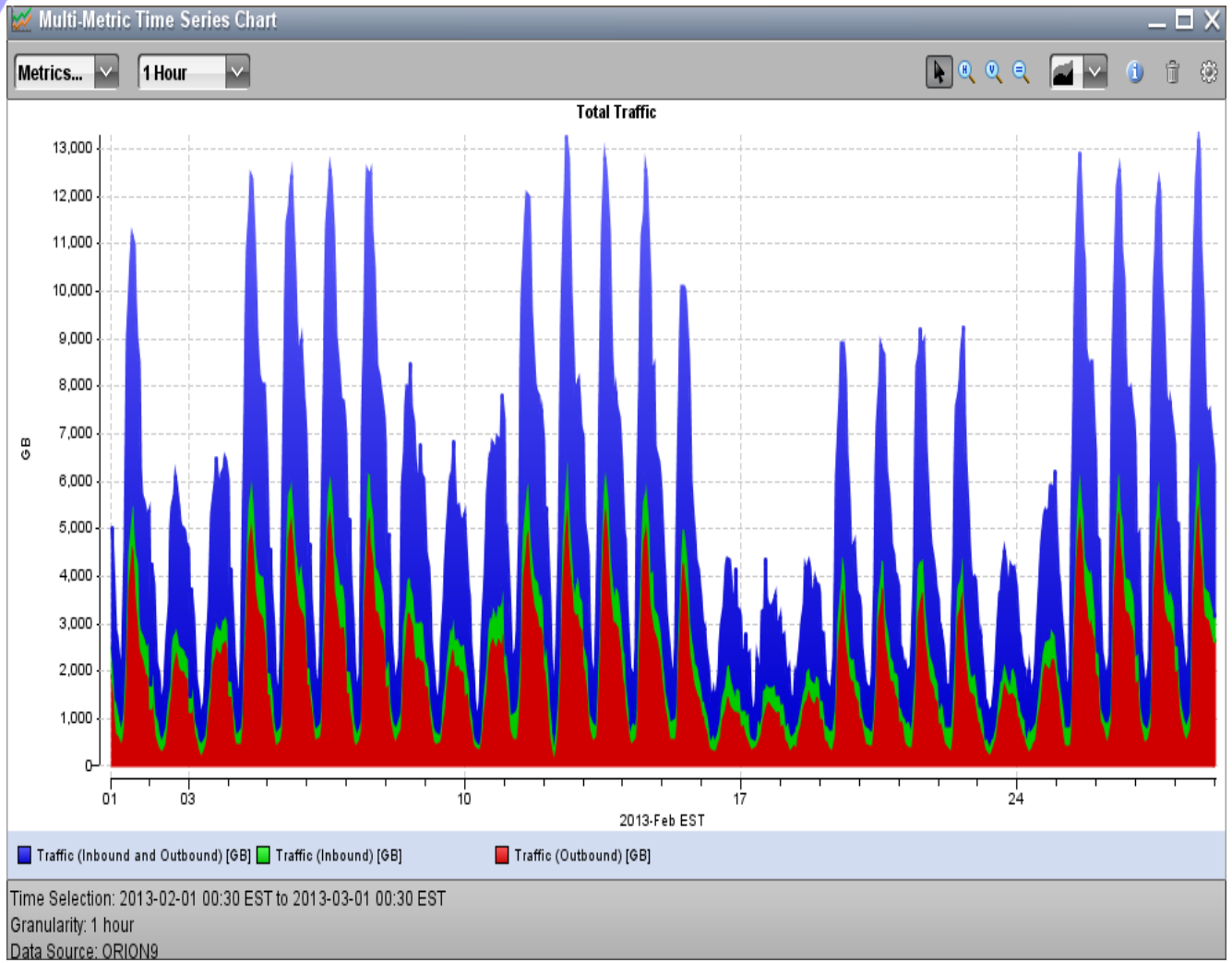
OPNET ARX Data Analysis



Group	Information	Throughput (Inbound and Outbound) [Mbits/sec]	Throughput (Inbound) [Mbits/sec]	Throughput (Outbound) [Mbits/sec]	Traffic (Inbound and Outbound) [MB]
Total Traffic	Total Traffic	5738.126	1198.103	4540.023	61563416.262
TCP	TRANSMISSION CONTROL P...	5240.646	989.525	4251.121	56226035.874
Defined Apps	Applications				
HTTP	TCP Ports: 80	3327.296	150.597	3176.699	35698013.272
HTTPS	TCP Ports: 443	511.316	104.764	406.552	5485827.056
SSH	TCP Ports: 22	288.905	113.057	175.848	3099615.840
SMTP	TCP Ports: 25	26.102	25.002	1.100	280047.772
MS-WBT-SRV-TCP	Windows Terminal Serve...	15.824	0.231	15.593	169776.309
YAHOO-MESSENGER...	TCP Ports: 5000-5001	15.104	5.766	9.338	162047.916
IMAP	TCP Ports: 143	4.120	0.247	3.873	44200.993
POP3	TCP Ports: 110	1.945	0.058	1.888	20872.455
VERITAS-BACKUP-...	TCP Ports: 9284,13701-...	1.674	1.148	0.526	17959.086
VERITAS-BACKUP	TCP Ports: 6106,8099,10000	0.722	0.544	0.177	7745.121
MSSQL-TCP	Microsoft SQL Server (...	0.378	0.040	0.338	4057.453
VMWARE-SRV-TCP	VMWare Server (TCP Por...	0.205	0.006	0.199	2196.109
ORACLE-NET8-CMA...	TCP Ports: 1630	0.128	0.127	0.001	1374.243
ORACLE-GIOP-TCP	TCP Ports: 2481	0.112	0.110	0.002	1205.924
MICROSOFT-DS	TCP Ports: 445	0.096	0.040	0.056	1026.037
ORACLE-NAMES	TCP Ports: 1575	0.079	0.038	0.040	844.147
TELNET	TCP Ports: 23	0.064	0.018	0.046	691.052
SAP-HOSTCTRL-TCP	TCP Ports: 1128	0.053	0.053	0.000	572.025
SQL*NET-2	TCP Ports: 1521	0.049	0.014	0.035	529.973
ORACLE-REMOTE-DB	TCP Ports: 1571	0.048	0.008	0.040	519.919
Other Apps	Other Apps				
UDP	USER DATAGRAM PROTOCOL	474.950	208.578	266.372	5095658.258
Other IP Protocols	Other IP Protocols	22.013	0.000	22.013	236172.321
ICMP	Protocol 1	0.517	0.000	0.517	5549.809

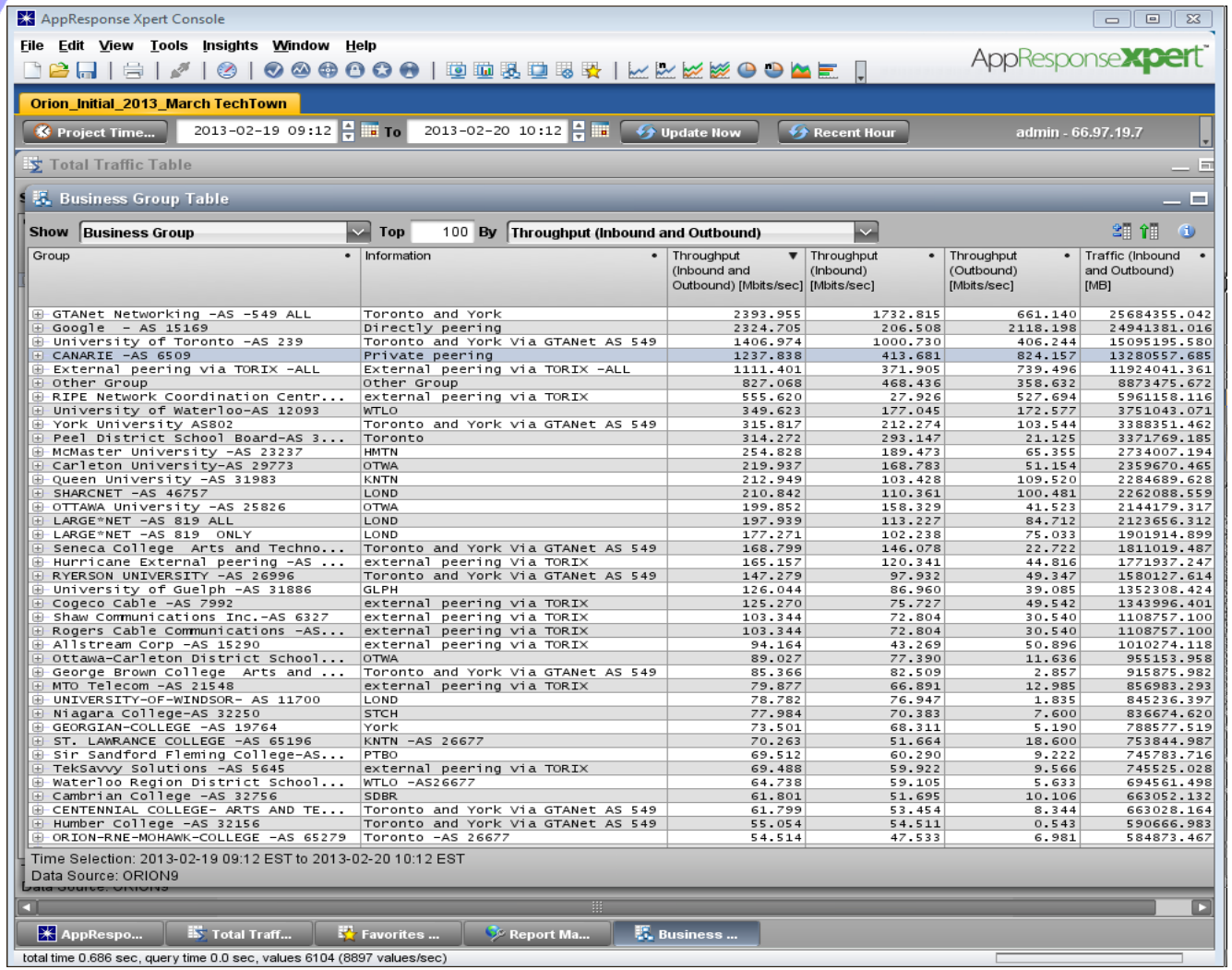
orion
Ontario's backbone of innovation

OPNET ARX Data Analysis



orion
Ontario's backbone of innovation

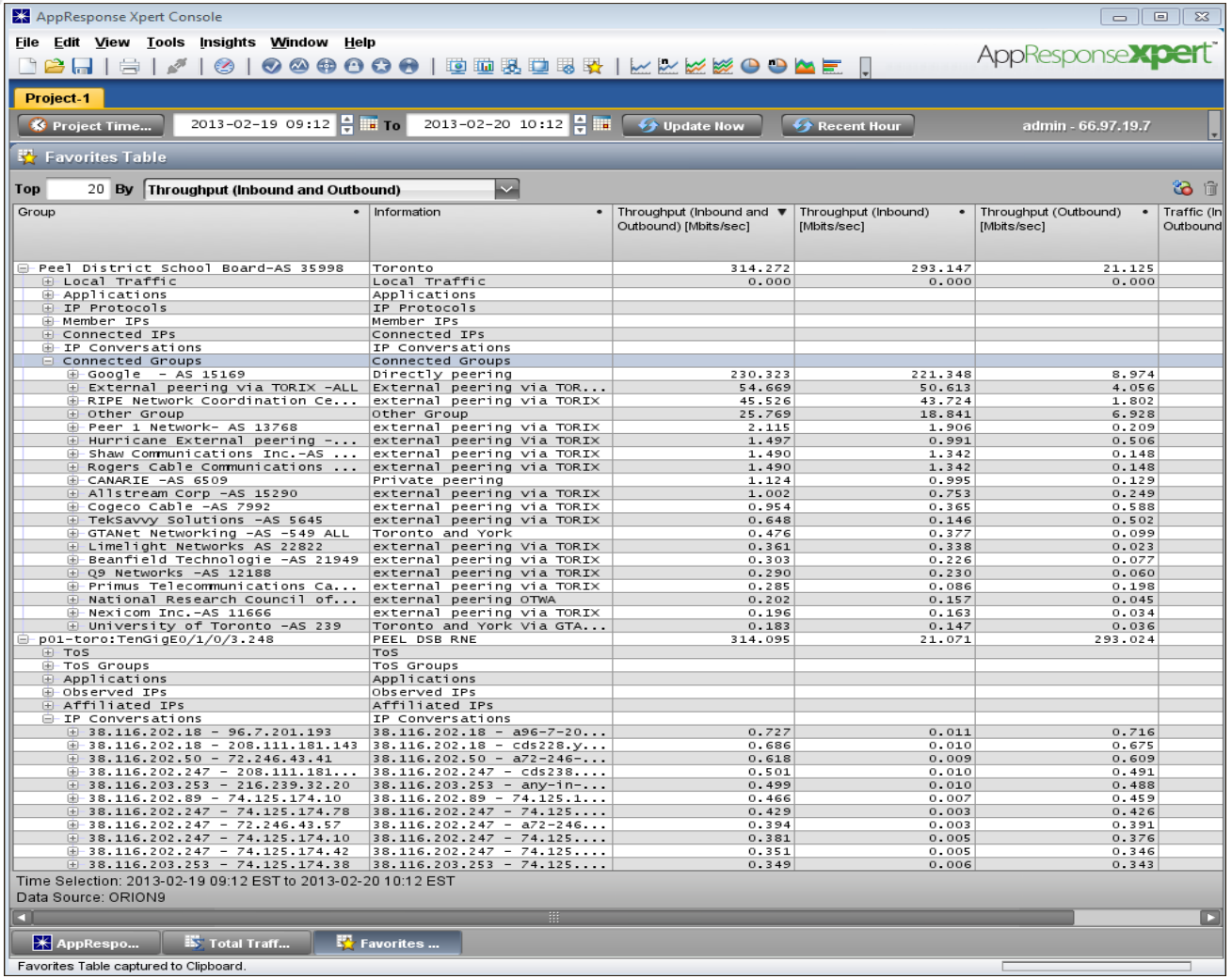
OPNET ARX Data Analysis Cont'd



Group	Information	Throughput (Inbound and Outbound) [Mbits/sec]	Throughput (Inbound) [Mbits/sec]	Throughput (Outbound) [Mbits/sec]	Traffic (Inbound and Outbound) [MB]
GTANet Networking -AS -549 ALL	Toronto and York	2393.955	1732.815	661.140	25684355.042
Google - AS 15169	Directly peering	2324.705	206.508	2118.198	24941381.016
University of Toronto -AS 239	Toronto and York Via GTANet AS 549	1406.974	1000.730	406.244	15095195.580
CANARIE -AS 6509	Private peering	1237.838	413.681	824.157	13280557.685
External peering via TORIX -ALL	External peering via TORIX -ALL	1111.401	371.905	739.496	11924041.361
Other Group	Other Group	827.068	468.436	358.632	8873475.672
RIPE Network Coordination Centr...	external peering via TORIX	555.620	27.926	527.694	5961158.116
University of Waterloo-AS 12093	WTLO	349.623	177.045	172.577	3751043.071
York University AS802	Toronto and York via GTANet AS 549	315.817	212.274	103.544	3388351.462
Peel District School Board-AS 3...	Toronto	314.272	293.147	21.125	3371769.185
McMaster University -AS 23237	HMTN	254.828	189.473	65.355	2734007.194
Carleton University-AS 29773	OTWA	219.937	168.783	51.154	2359670.465
Queen University -AS 31983	KNTN	212.949	103.428	109.520	2284689.628
SHARCNET -AS 46757	LOND	210.842	110.361	100.481	2262088.559
OTTAWA University -AS 25826	OTWA	199.852	158.329	41.523	2144179.317
LARGE*NET -AS 819 ALL	LOND	197.939	113.227	84.712	2123656.312
LARGE*NET -AS 819 ONLY	LOND	177.271	102.238	75.033	1901914.899
Seneca College Arts and Techno...	Toronto and York Via GTANet AS 549	168.799	146.078	22.722	1811019.487
Hurricane External peering -AS ...	external peering via TORIX	165.157	120.341	44.816	1771937.247
RYERSON UNIVERSITY -AS 26996	Toronto and York Via GTANet AS 549	147.279	97.932	49.347	1580127.614
University of Guelph -AS 31886	GLPH	126.044	86.960	39.085	1352308.424
Cogeco Cable -AS 7992	external peering via TORIX	125.270	75.727	49.542	1343996.401
Shaw Communications Inc.-AS 6327	external peering via TORIX	103.344	72.804	30.540	1108757.100
Rogers Cable Communications -AS...	external peering via TORIX	103.344	72.804	30.540	1108757.100
Allstream Corp -AS 15290	external peering via TORIX	94.164	43.269	50.896	1010274.118
Ottawa-Carleton District School...	OTWA	89.027	77.390	11.636	955153.958
George Brown College Arts and ...	Toronto and York Via GTANet AS 549	85.366	82.509	2.857	915875.982
MTO Telecom -AS 21548	external peering via TORIX	79.877	66.891	12.985	856983.293
UNIVERSITY-OF-WINDSOR- AS 11700	LOND	78.782	76.947	1.835	845236.397
Niagara College-AS 32250	STCH	77.984	70.383	7.600	836674.620
GEORGIAN-COLLEGE -AS 19764	York	73.501	68.311	5.190	788577.519
ST. LAWRANCE COLLEGE -AS 65196	KNTN -AS 26677	70.263	51.664	18.600	753844.987
Sir Sandford Fleming College-AS...	PTBO	69.512	60.290	9.222	745783.716
TekSavvy Solutions -AS 5645	external peering via TORIX	69.488	59.922	9.566	745525.028
Waterloo Region District School...	WTLO -AS26677	64.738	59.105	5.633	694561.498
Cambrian College -AS 32756	SDBR	61.801	51.695	10.106	663052.132
CENTENNIAL COLLEGE- ARTS AND TE...	Toronto and York Via GTANet AS 549	61.799	53.454	8.344	663028.164
Humber College -AS 32156	Toronto and York Via GTANet AS 549	55.054	54.511	0.543	590666.983
ORION-RNE-MOHAWK-COLLEGE -AS 65279	Toronto -AS 26677	54.514	47.533	6.981	584873.467

orion
Ontario's backbone of innovation

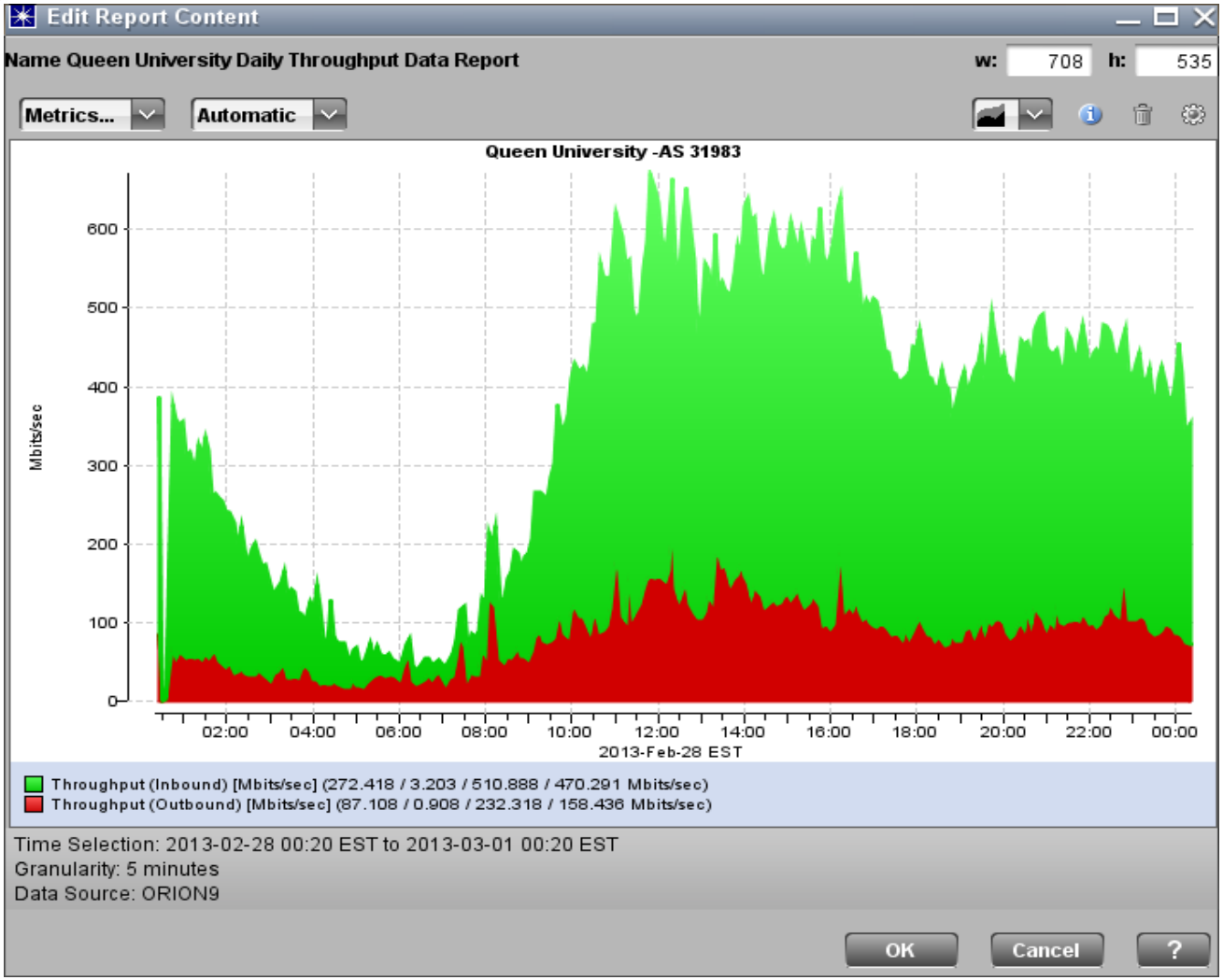
OPNET ARX Data Analysis Cont'd



Group	Information	Throughput (Inbound and Outbound) [Mbits/sec]	Throughput (Inbound) [Mbits/sec]	Throughput (Outbound) [Mbits/sec]	Traffic (In Outbound
Peel District School Board-AS 35998	Toronto	314.272	293.147	21.125	
Local Traffic	Local Traffic	0.000	0.000	0.000	
Applications	Applications				
IP Protocols	IP Protocols				
Member IPs	Member IPs				
Connected IPs	Connected IPs				
IP Conversations	IP Conversations				
Connected Groups	Connected Groups				
Google - AS 15169	Directly peering	230.323	221.348	8.974	
External peering via TORIX -ALL	External peering via TOR...	54.669	50.613	4.056	
RIPE Network Coordination Ce...	external peering via TORIX	45.526	43.724	1.802	
Other Group	Other Group	25.769	18.841	6.928	
Peer 1 Network- AS 13768	external peering via TORIX	2.115	1.906	0.209	
Hurricane External peering -...	external peering via TORIX	1.497	0.991	0.506	
Shaw Communications Inc.-AS ...	external peering via TORIX	1.490	1.342	0.148	
Rogers Cable Communications ...	external peering via TORIX	1.490	1.342	0.148	
CANARIE -AS 6509	Private peering	1.124	0.995	0.129	
Allstream Corp -AS 15290	external peering via TORIX	1.002	0.753	0.249	
Cogeco Cable -AS 7992	external peering via TORIX	0.954	0.365	0.588	
TekSavvy Solutions -AS 5645	external peering via TORIX	0.648	0.146	0.502	
GTANet Networking -AS -549 ALL	Toronto and York	0.476	0.377	0.099	
Limelight Networks AS 22822	external peering via TORIX	0.361	0.338	0.023	
Beanfield Technologie -AS 21949	external peering via TORIX	0.303	0.226	0.077	
Q9 Networks -AS 12188	external peering via TORIX	0.290	0.230	0.060	
Primus Telecommunications Ca...	external peering via TORIX	0.285	0.086	0.198	
National Research Council of...	external peering OTWA	0.202	0.157	0.045	
Nexicom Inc.-AS 11666	external peering via TORIX	0.196	0.163	0.034	
University of Toronto -AS 239	Toronto and York via GTA...	0.183	0.147	0.036	
p01-toro:TenGigE0/1/0/3.248	PEEL DSB RNE	314.095	21.071	293.024	
ToS	ToS				
ToS Groups	ToS Groups				
Applications	Applications				
Observed IPs	Observed IPs				
Affiliated IPs	Affiliated IPs				
IP Conversations	IP Conversations				
38.116.202.18 - 96.7.201.193	38.116.202.18 - a96-7-20...	0.727	0.011	0.716	
38.116.202.18 - 208.111.181.143	38.116.202.18 - cds228.y...	0.686	0.010	0.675	
38.116.202.50 - 72.246.43.41	38.116.202.50 - a72-246-...	0.618	0.009	0.609	
38.116.202.247 - 208.111.181...	38.116.202.247 - cds238....	0.501	0.010	0.491	
38.116.203.253 - 216.239.32.20	38.116.203.253 - any-in-...	0.499	0.010	0.488	
38.116.202.89 - 74.125.174.10	38.116.202.89 - 74.125.1...	0.466	0.007	0.459	
38.116.202.247 - 74.125.174.78	38.116.202.247 - 74.125....	0.429	0.003	0.426	
38.116.202.247 - 72.246.43.57	38.116.202.247 - a72-246...	0.394	0.003	0.391	
38.116.202.247 - 74.125.174.10	38.116.202.247 - 74.125....	0.381	0.005	0.376	
38.116.202.247 - 74.125.174.42	38.116.202.247 - 74.125....	0.351	0.005	0.346	
38.116.203.253 - 74.125.174.38	38.116.203.253 - 74.125....	0.349	0.006	0.343	

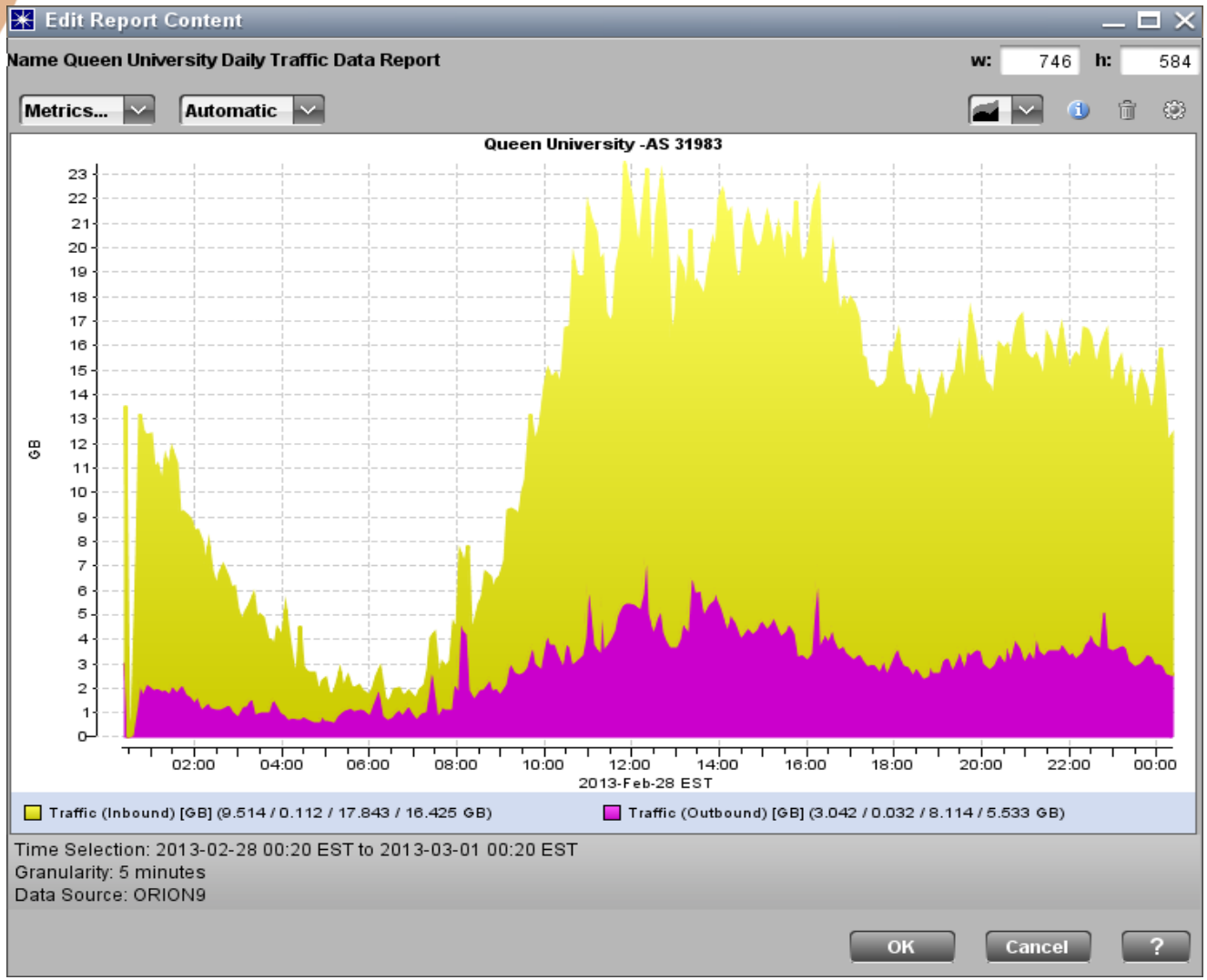
orion
Ontario's backbone of innovation

OPNET ARX Data Report



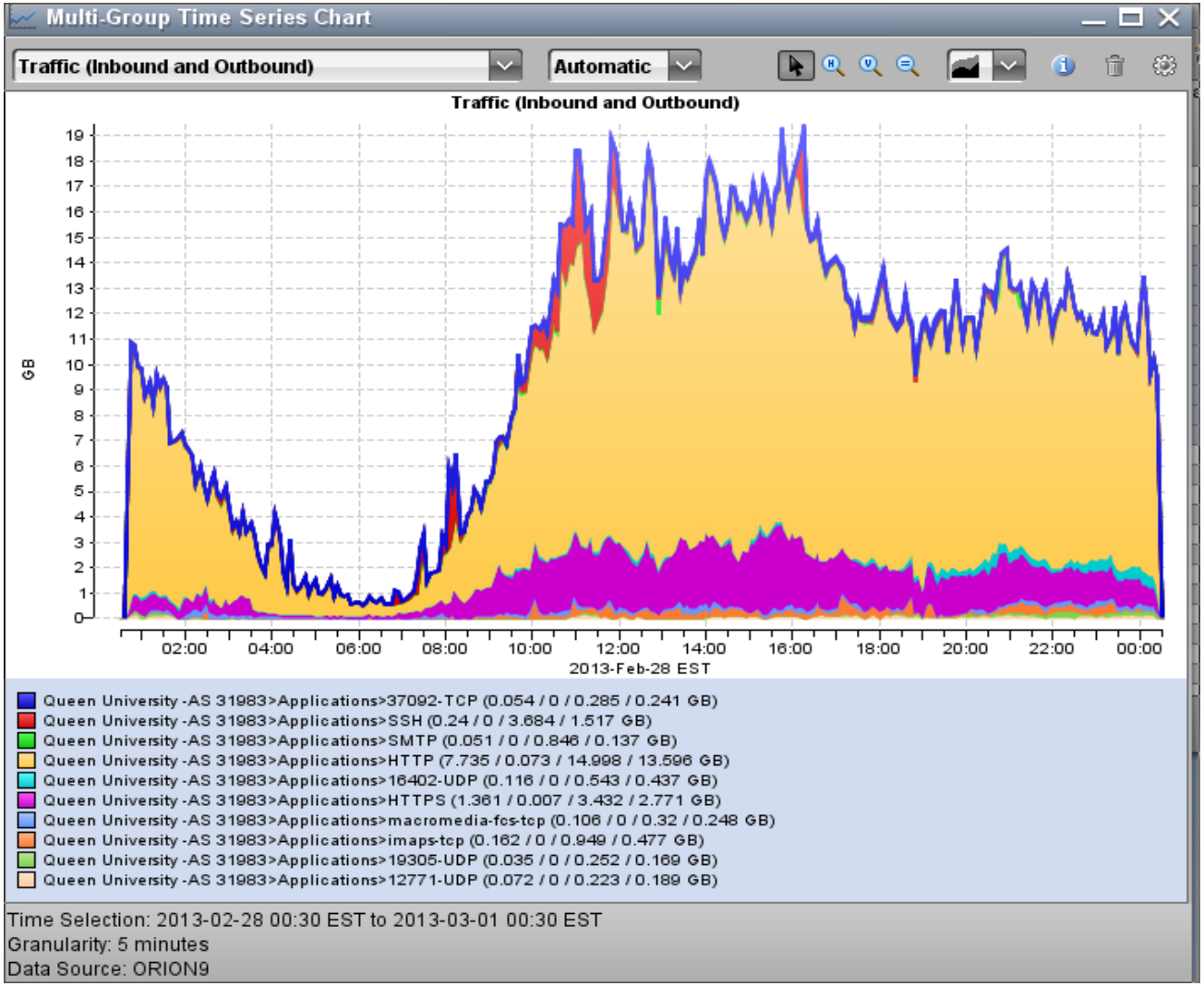
orion
Ontario's backbone of innovation

OPNET ARX Data Report Cont'd



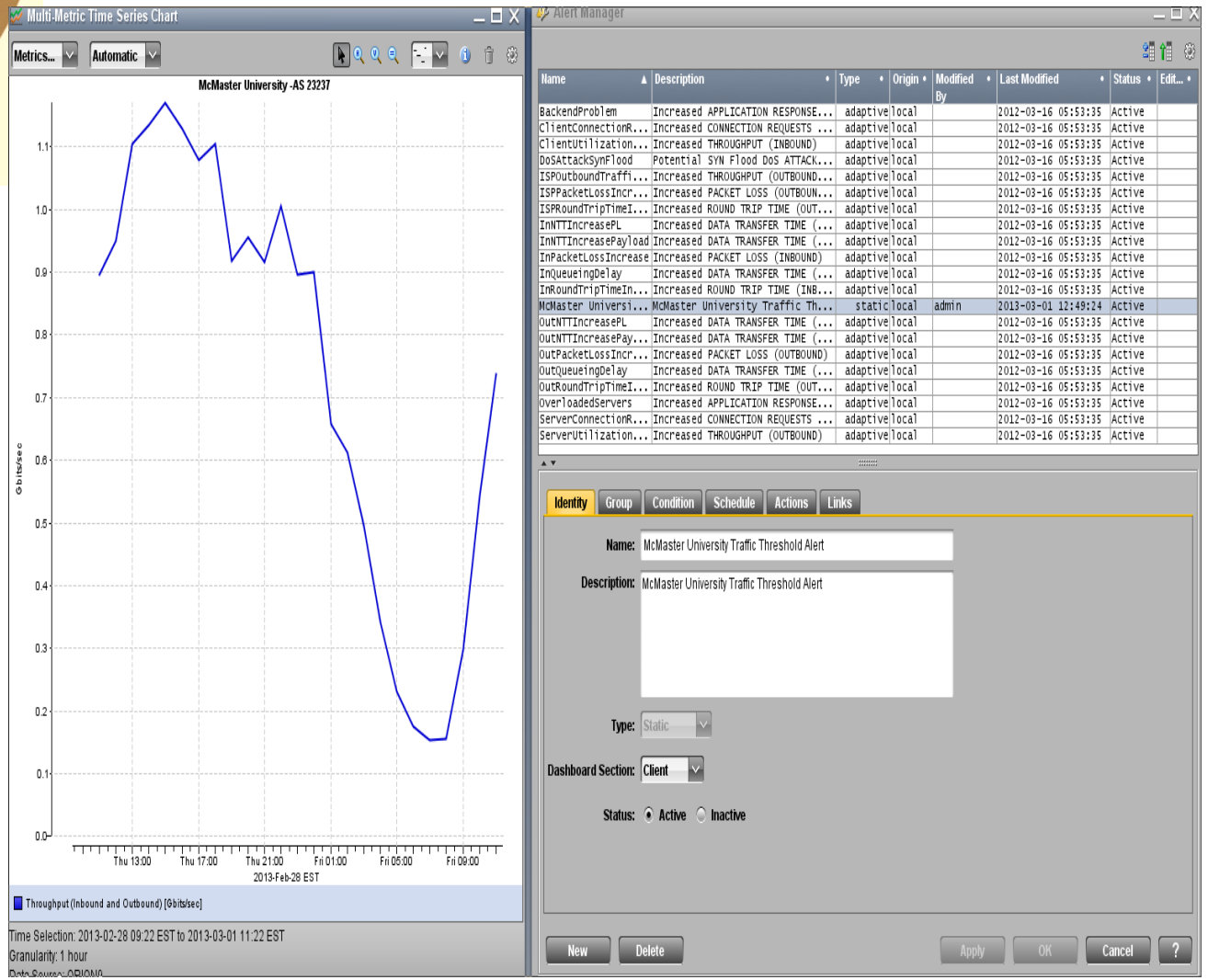
orion
Ontario's backbone of innovation

OPNET ARX Data Report Cont'd



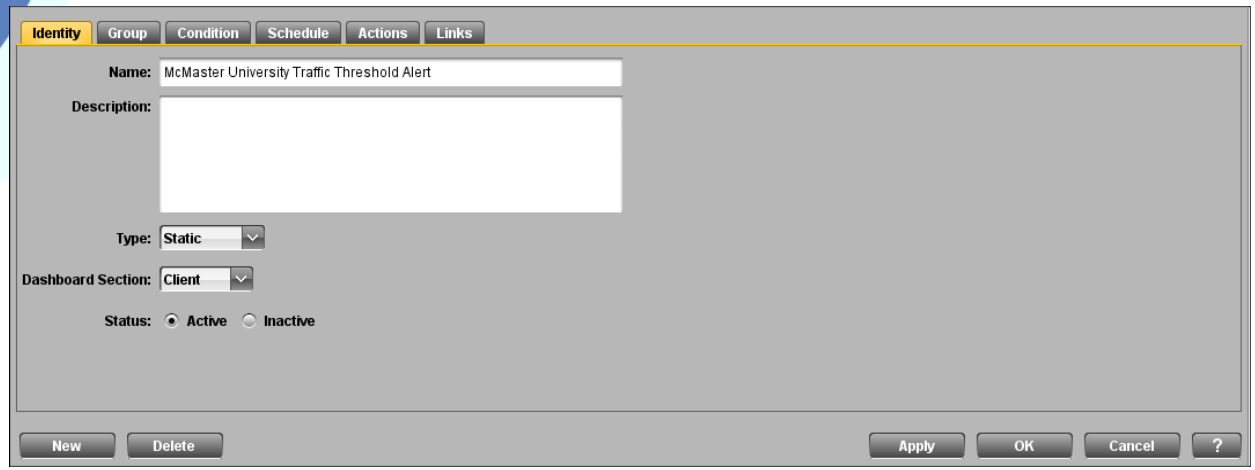
orion
Ontario's backbone of innovation

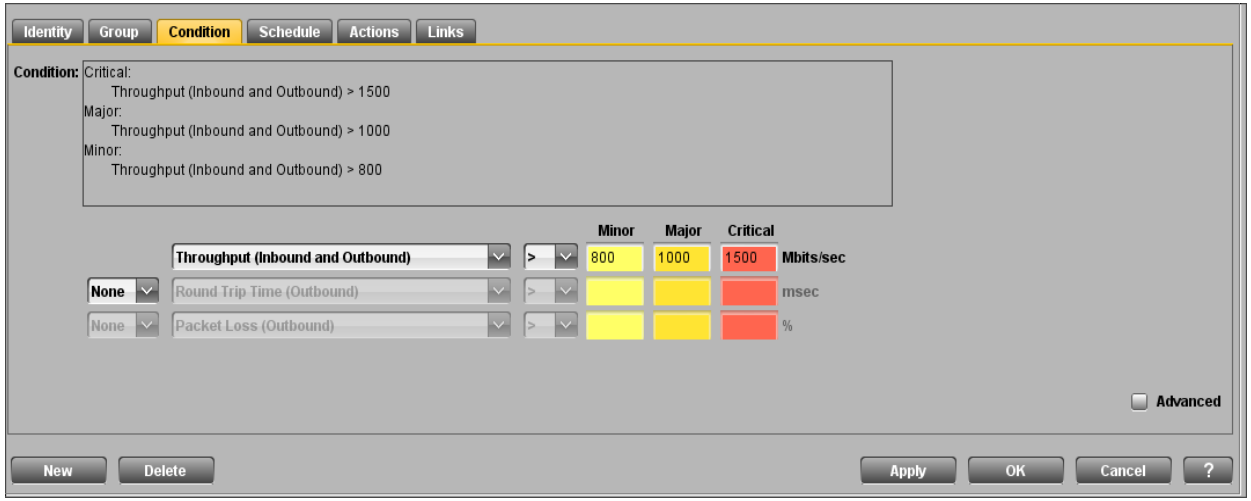
OPNET ARX Alert Manager



orion
Ontario's backbone of innovation

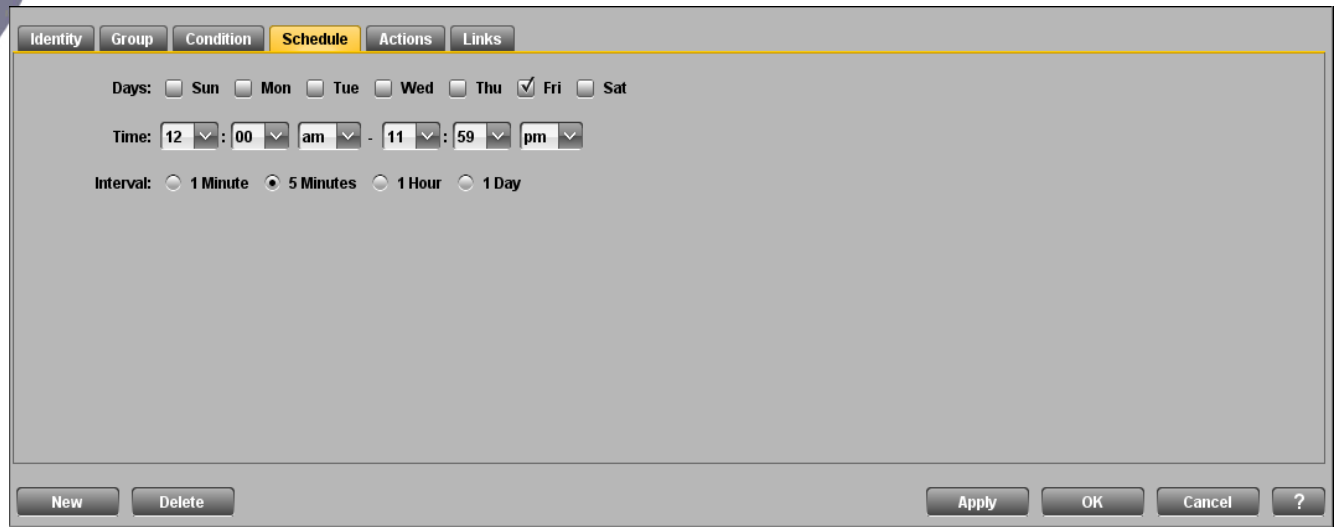
OPNET ARX Alert Manager Cont'd

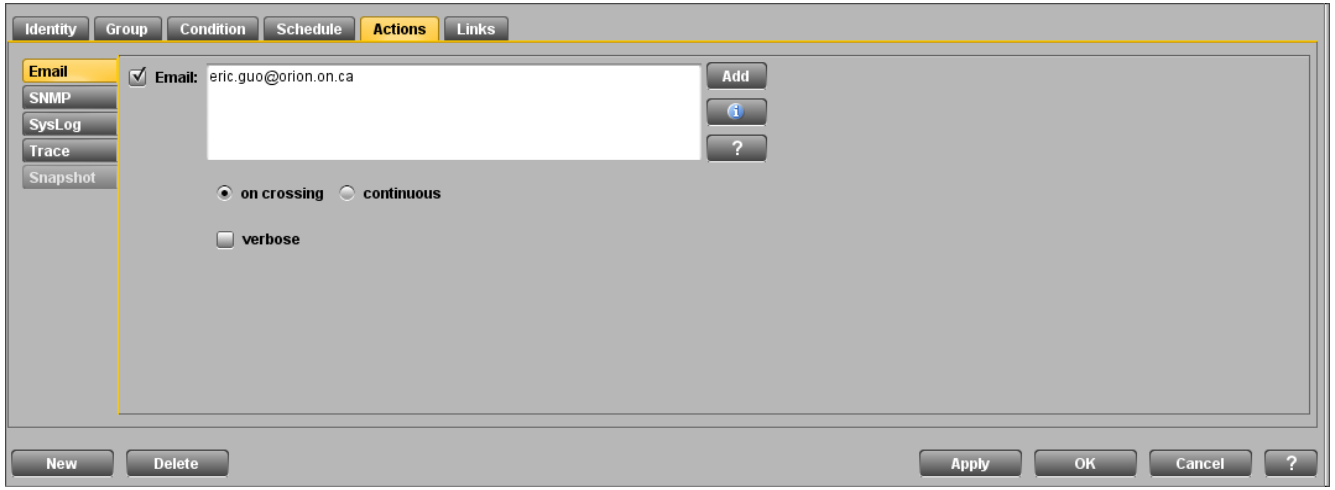




orion
Ontario's backbone of innovation

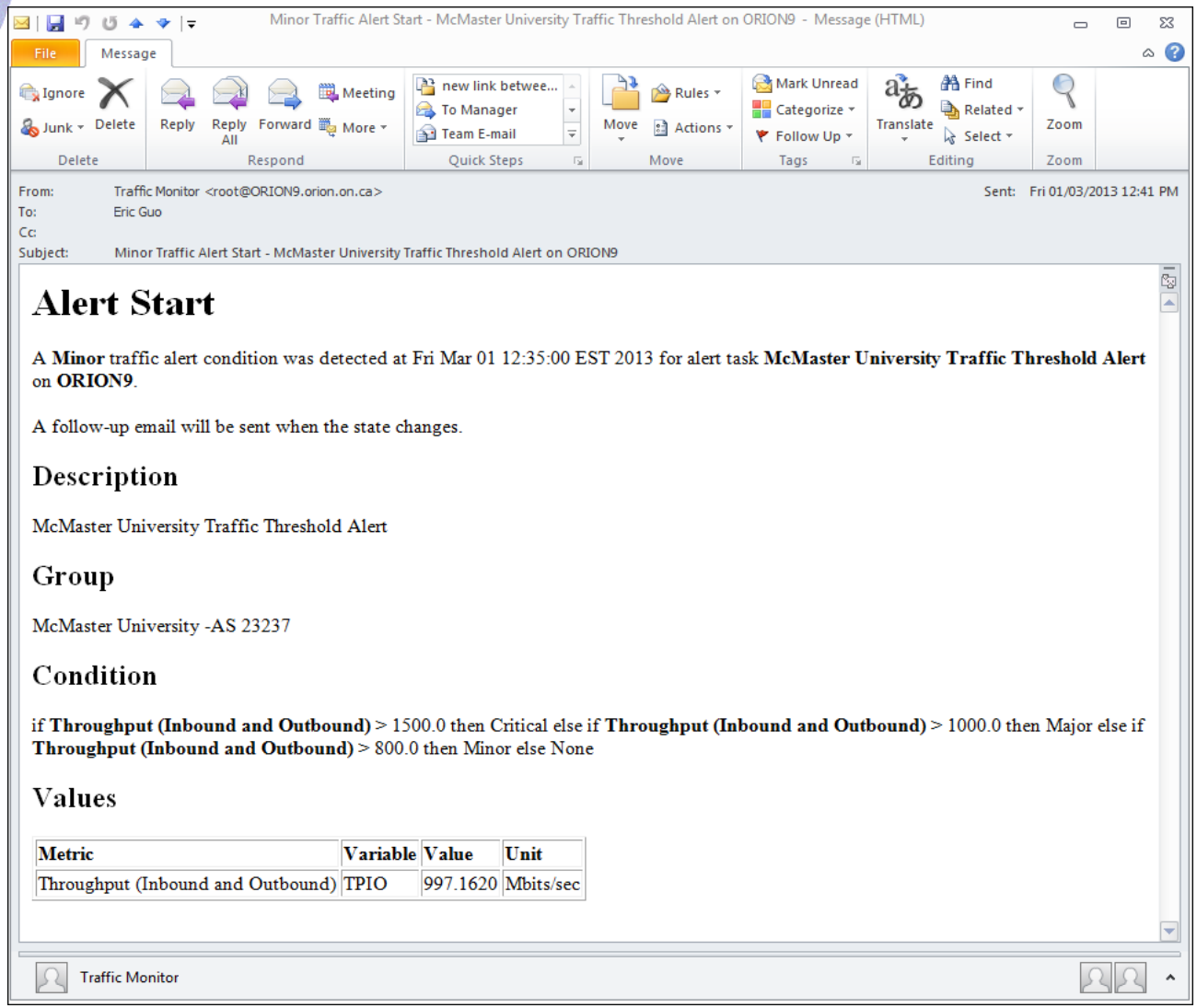
OPNET ARX Alert Manager Cont'd





orion
Ontario's backbone of innovation

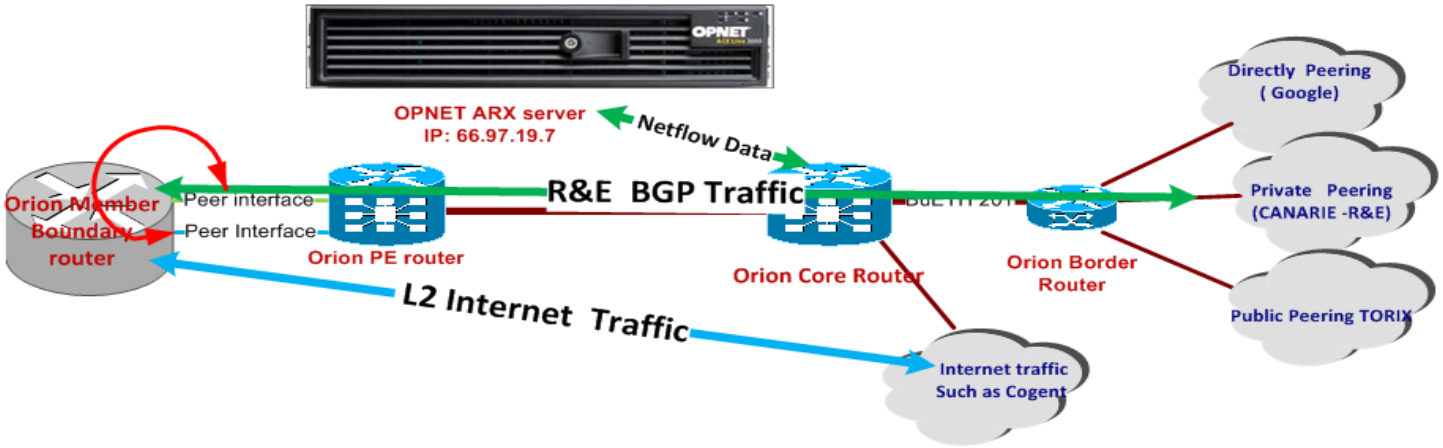
OPNET ARX Alert Manager Cont'd



orion
Ontario's backbone of innovation

OPNET Deployment Advance

L2 Internet Traffic Net Flow Data Collecting by ORION Appliance



Network Requirement from Member side:

- Support Net Flow Version 9
- IP Reachable with Orion OPNET Server 66.97.19.7

orion
Ontario's backbone of innovation

Thank You ! ☺

orion
Ontario's backbone of innovation