Collection of BCNET BGP Traffic

Tanjila Farah, Sukhchandan Lally, Rajvir Gill, Nabil Al-Rousan, Ravinder Paul, Don Xu, and Ljiljana Trajkovic
Simon Fraser University
Vancouver, British Columbia
{tfarah, lally, rajvirg, nalrousa, rpa28, donx, ljilja}@sfu.ca

***Abstract*—This poster paper describes testbed for collection of BCNET Border Gateway Protocol (BGP) traffic. The BGP traffic was collected using special purpose hardware and software. Preliminary data collection was illustrated using the Wireshark and Walrus graph visualization tools.**

Keywords—Communications technology; communication networks; communication system traffic; communication system traffic control; protocols; routing protocols

I. INTRODUCTION

Measuring and monitoring traffic in deployed communication networks is necessary for effective network operations. Such measurements are essential for developing traffic models, evaluating performance of network protocols and applications, and planning network development. Analysis of collected traffic enables network operators to understand the behavior of network users and ensure quality of service.

II. MEASUREMENT TESTBED

BCNET provides high-speed optical advanced network to British Columbia's higher education and research institutes and operates the Optical Regional Advanced Network (ORAN) [1]. Primary BCNET backbone is a 10 Gbps Ethernet network with backup 1 Gbps links planned for rapid failover. BCNET provides IPv4 and IPv6 Internet Protocol routed services and Transparent Ethernet services (point to point and point to multipoint). The transit providers are connected to BCNET via 1 Gbps and 10 Gbps network links. Connections between BCNET and its transit providers are shown in Figure 1.

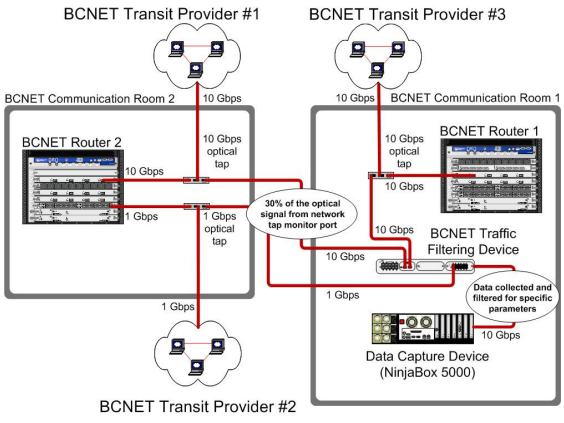

Figure 1. Physical overview of the BCNET packet capture.

This research was supported by the NSERC Discovery Grant 216844-07, the NSERC RTI Grant 330480-06, and the BCNET.

BGP provides mechanisms for supporting classless inter-domain routing [2]. BGP is the de-facto Inter-Autonomous System routing protocol. It operates over Transmission Control Protocol (TCP). The main function of BGP is to exchange reachability information among BGP systems based on policy decision, shortest *AS_path*, and closest *Next_hop* router. To select the best path, BGP employs the Best Path Selection algorithm [3].

The placement of various devices deployed to collect the BGP traffic is shown in Figure 1. Traffic received from the network links is split using an optical tap. 30% of the split is directed to traffic filtering device. *Net Optics Director 7400* shown in Figure 2 is used as the filtering device [4]. It helps to select traffic based on communication protocols, IP addresses, port numbers, and the virtual local area network (VLAN). Traffic selected by the filtering device is then directed to the data capture device *NinjaBox 5000*, which has options of specifying the type of data to be captured from the directed traffic.

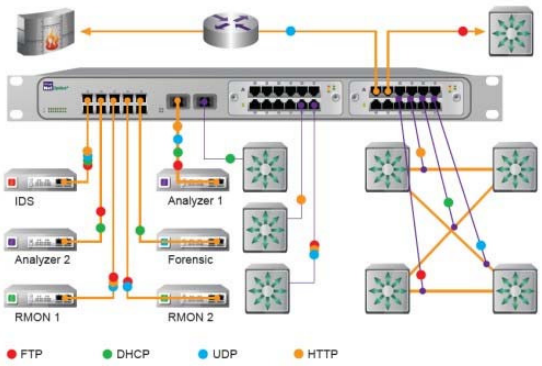

Figure 2. Net Optics Director 7400 application diagram [4].

The main component of *NinjaBox 5000* is the *Endace DAG 5.2X* card [5] shown in Figure 3. This card enables 100 % packet capture at full line rates even on high-speed links operating at full line utilization.

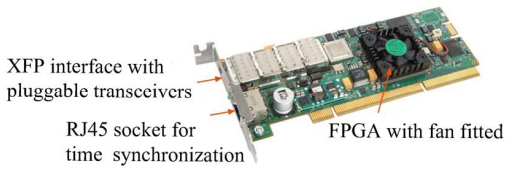

Figure 3. ENDACE card is used for network monitoring and analyzing [5].

978-0-9836283-0-9

This paper was peer reviewed by subject matter experts for publication in the Proceedings of ITC 2011

The real-time network usage by BCNET associates is shown in Figure 4 [1]. British Columbia's network extends to 1,400 kilometers and connects cities of Kamloops, Kelowna, Prince George, Vancouver, and Victoria. The arrows in the map show the traffic bound for CANARIE (Canada's Advanced Research and Innovation Network), the commercial Internet (Transits), and peering traffic at the Seattle Internet Exchange (Seattle IX).

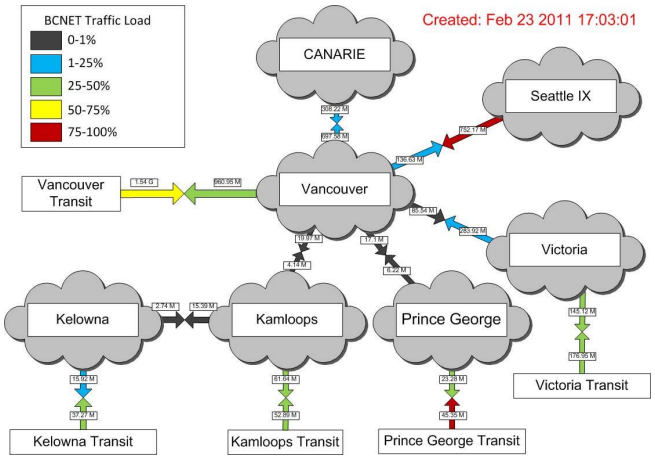

Figure 4. Real-time network usage by BCNET members. Shown are traffic loads for individual transits [1].

III. Traffic Collection

Samples of BCNET Border Gateway Protocol (BGP) traffic traces were collected over a continuous period of 48 hours between December 20, 2010 and December 22, 2010. Collected BGP traffic is displayed using the Wireshark packet analyzer [6]. The Walrus graph visualization tool [7] is used to display network topology on the Autonomous System (AS) level.

Wireshark provides wide range of statistics such as the number of packets captured, statistics about specific protocols, and general statistics such as traffic summary, protocol hierarchy, conversations, end-points, and input/output graphs. Wireshark enables detailed analysis of the collected traffic. For each BGP update message, it displays path attributes and network layer reachability information (prefixes). A sample of the collected data is shown in Figure 5.

The Walrus 3D hyperbolic display of the BCNET AS topology is shown in Figure 6. The graph consists of 982 nodes, 981 tree-links, and 441 non tree-links. It is created using the value of the BGP *AS_path* attribute in BGP *update* messages. The *AS_path* attribute is generated by the Best Path Selection algorithm and contains a list of ASs. The local AS number is added to the head of the list by a BGP peer when it advertises its prefixes to the next external BGP (eBGP) peer. Three visible clusters of ASs corresponding to BCNET transit providers Telus Advanced Communications (AS 852), Shaw Communications (AS 6327), and Peer 1 Network Inc. (AS 13768) are shown in Figure 6. The graph links reflect a policy relationship between BCNET transit providers. (They do not necessarily indicate the actual data traffic flow.)

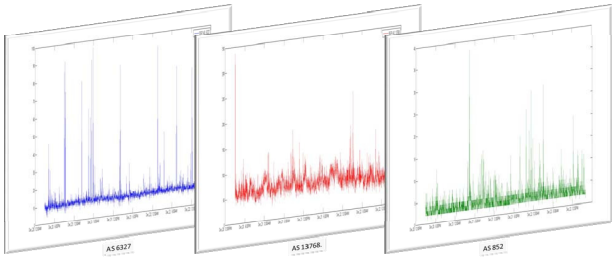

Figure 5. The traffic generated by the BGP update messages for the three BCNET transit providers. Total of 230,424 BGP update messages were identified.

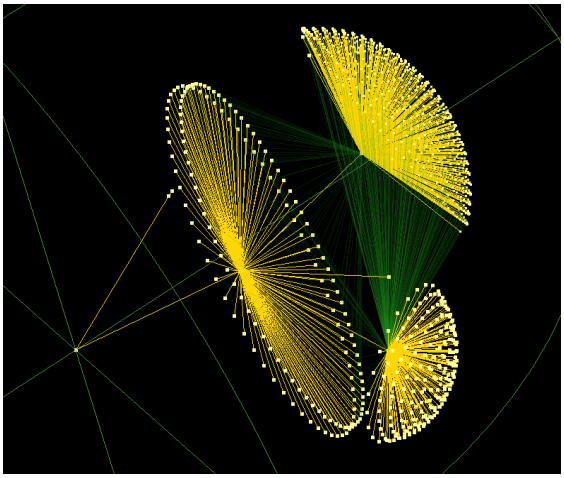

Figure 6. Walrus AS topology graph of the collected BCNET traffic. The centers of the three clusters correspond to BCNET transit providers with AS numbers 852, 6,327, and 13,768. Clusters consist of 683, 588, and 155 AS nodes, respectively.

IV. Conclusions

This poster paper illustrates collection of traffic from a deployed network and reports preliminary traffic measurements. The ultimate goal is to analyze BGP protocol performance and its dependence on various algorithms and parameters such as route flap damping and minimal route advertisement interval. Collected BGP traffic data will be used to infer the Internet topologies and their historical development on AS level [8].

References

[1] BCNET [Online]. Available: http://www.bc.net.

[2] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," *IETF RFC 1771*.

[3] BGP Best Path Selection Algorithm [Online]. Available: http://www.cisco.com/en/US/tech/tk365.

[4] Data Monitoring Switch [Online]. Available: http://www.netoptics.com/pdf/datasheet/PUBDIRD.pdf.

[5] Welcome to DAG [Online]. Available: http://www.endace.com.

[6] Wireshark [Online]. Available: http://www.wireshark.org.

[7] Walrus - Graph Visualization Tool [Online]. Available: http://www.caida.org/tools/visualization/walrus.

[8] Lj. Trajković, "Analysis of Internet topologies," *IEEE Circuits and Systems Magazine*, vol. 10, no. 3, pp. 48–54, Third Quarter 2010.