Proceedings of CECNet 2022
A.J. Tallón-Ballesteros (Ed.)

doi:10.3233/FAIA220567

Emulation of the Updated CANARIE Backbone Network Topology Under IPv6 Up to 2022

Jose-Ignacio Castillo-Velazquez[1] and Nelly-Guadalupe Velazquez-Cruz
Autonomous University of Mexico City, Mexico City, Mexico

Abstract. The National Research and Education Networks or Advanced Networks implemented in all countries in the world are the alternative Internet to the commercial Internet which was developed for education and experimental purposes beginning with the Internet 2. Our interest is to study the CANARIE topology after 27 years of the foundation of the pan-Canadian advanced network which now interconnects all the thirteen provinces and territories in the country. In this work a connectivity and management emulation for the updated 2022 backbone topology of CANARIE was developed under IPv6 protocols. So, emulator GNS3, Wireshark, iReasoning MIB browser, Virtual Box and Kali Linux were required to emulated CANARIE backbone infrastructure using the best possible approximation with the available resources, considering that real infrastructure is overly expensive and just supported by internet service providers. Results were successful for connectivity and management tests, showing no significative changes when Canada expanded its advanced network. Emulation uses a lot of CPU and RAM resources, but it also shows some limitations for GNS3 when comparing to real bandwidth scenarios. CANARIE maintains important connections to support international projects with other advanced networks GEANT in Europe, APAN in Asia, AFRICACONNECT through GEANT and CLARA in Latin America through Internet2 in USA. Emulating is the alternative for backbone networks for characterizing advanced networks around the world which uses expensive equipment only available by the Internet Service Provider companies.

Keywords. Advanced networks, backbone, Internet, network management.

1. Introduction

Last august 2020, Nunavut Territory joined to the Canadian Network for the Advancement of Research, Industry, and Education (CANARIE), or the National Research and Education Network (NREN) for Canada, fulfilling all thirteen provincial and territorial partners. This way, the dream of offering a pan-Canadian NREN when the Canadian Federal Government announced the born of CA*NET project in 1993 was completed. The Canadian NREN and Internet2 its equivalent in USA were interconnected in 1998, since then CANARIE has been evolving, and covering a broader area till interconnecting all the country. CANARIE members are also members of the Canadian Access Federation (CAF) which lets them access to “Edu roam” a secure Wi-Fi global roaming service and the Federated Identity Management service for researchers

[1] Corresponding Author, Jose Ignacio Castillo Velazquez, ADVNETLAB, UACM, Mexico City, Mexico; E-mail: ignacio.castillo@uacm.edu.mx.

and students. CANARIE is clue for the innovation, science, and economic development in Canada, from 2019 to 2020 data traffic grew around 26%, the highest rate in the 27 years of existence, maybe accelerated by the new normality imposed by COVID-19. Nowadays CANARIE supports national projects such as the research software program, research data management program, CAF, Digital Accelerator for Innovation and Research (DAIR) cloud platform, Ouranos for climate research, cybersecurity program and network development working as a team with the Centre of Excellence in Next Generation Networks (CENGN). CANARIE also maintains participation in worldwide projects such as International Cancer Genome Consortium (ICGC), ATLAS experiment for LHC at CERN and Square Kilometer Array (SKA) for cosmos study. The thirteen regional networks ACORN-NL, ACORN-NS, AURORA COLLEGE, BCNET, CYBERIA, MRNET, ECN, ORION, RISQ, SRNET, YUKON COLLEGE. CANARIE infrastructure supports nowadays more than 400 PB by year interconnecting their 770 national institutions to 125 NRENs in 100 countries [1-6]. Because GNS3 supports backbone routers, in previous works this emulator was used to study other backbone topologies but specifically the CANARIE for Canada one under IPv4, when all the thirteen provinces and territories were not covered, just only 12 of them, using 25 backbone routers in its topology [7]. It was in august 2020 when Nunavut Territory was included adding the first corresponding infrastructure to make reality the Canadian dream of offering a pan-Canadian advanced network after 27 years it was founded [8]. In this work GNS3 is used to emulate the full connectivity and management for the 2022 CANARIE topology under IPv6 protocols, using c7200 backbone routers [9-14]. For the most updated topology in 2022 CANARIE maintains connection to Internet2 in USA through routers from Toronto, Victoria, Windsor, Halifax, and Winnipeg. CANARIE maintains important connections to support international projects with other advanced networks GEANT in Europe, APAN in Asia, AFRICACONNECT through GEANT and CLARA in Latin America through Internet2 in USA.

2. Methodology

For the emulation of the 2022 CANARIE's backbone topology, the 28 backbone routers interconnecting the thirteen provinces and territories were configured using IPv6 addresses for all the 1Gbps optical fiber interfaces as shown in figure 1. Check that the new infrastructure at Nunavut was connected to CANARIE through the Yellowknife router. The physical equipment used for emulation was an icore 7 CPU and 16 GB, where the GNS3 2.2.20 was installed.

2.1. Connectivity configuration

All the 28 C7200 backbone routers were configured using IPv6 addresses and OSPFv3 under the IOS v12, for providing connectivity as shown in figure 2 as an example for the Whitehorse router. Then connectivity can be tested for all the 28 backbone routers in the advanced network, using ping and traceroute commands, but also by other tools as Wireshark.

2.2. Management configuration

For management emulation, first SNMPv3 was configured for each of the 28 backbone routers as indicated in figure 3, including the SHA security and parameters.

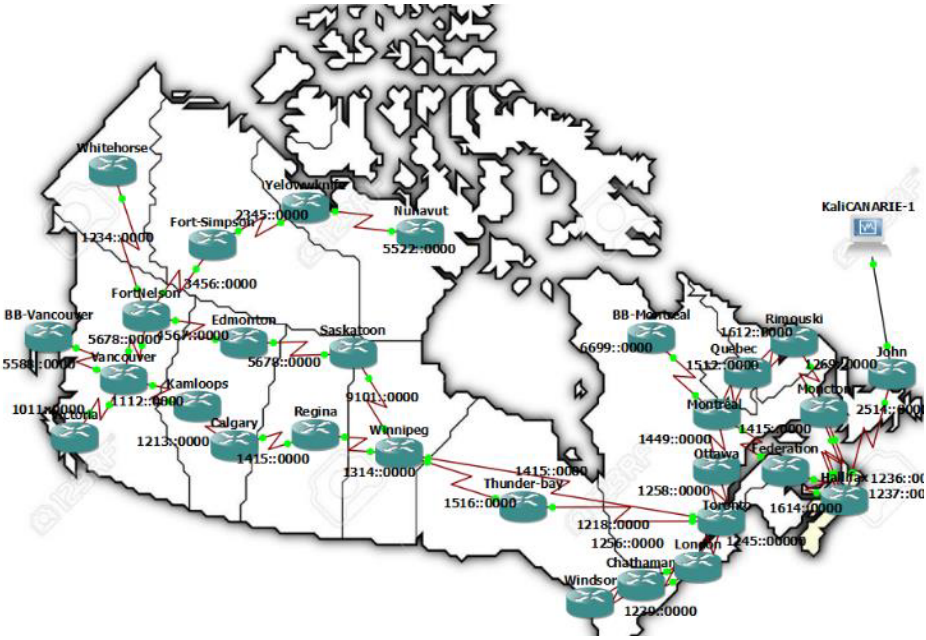

Figure 1. The backbone topology for CANARIE in 2022, using 28 backbone C7200 in GNS3 under IPv6 including the new infrastructure.

```
Whitehorse(config)#ipv6 router ospf 100
Whitehorse(config-rtr)#
*May  3 21:51:06.499: %OSPFv3-4-NORTRID: OSPFv3 process 100 could not pick a router
-id,
please configure manually
Whitehorse(config-rtr)#router-id 1.1.1.1
Whitehorse(config-rtr)#exit
Whitehorse(config)#int p1/0
Whitehorse(config-if)#ipv6 ospf 100 area 0
```

Figure 2. IPv6 and OSPFv3 configuration for one of the 28 backbone routers

```
Victoria(config)#snmp-server group adv v3 auth read 123 write 456
Victoria(config)#snmp-server user nelly adv v3 auth sha amigo
```

Figure 3. The SNMPv3 configuration for BB router at Victoria Island.

Then also traps were enabled as shown in figure 4, in this example, configuration under another router is shown.

```
Fort-Simpson(config)#snmp-server view 123 iso included
Fort-Simpson(config)#snmp-server view 456 iso included
Fort-Simpson(config)#snmp-server host AAAA::1 version 3 auth nelly
Fort-Simpson(config)#snmp-server host 3456::1 v3
Fort-Simpson(config)#snmp-server host 2345::2 v3
Fort-Simpson(config)#snmp-server enable traps
```

Figure 4. The SNMPv3 configuration for enabling traps on Fort Simpson router.

Finally, the IReasoning MIB Browser was installed on the Kali Linux virtual machine attached to Victoria´s router, which does the function as the Network Management System (NMS). For testing management activities, five managed variables were tested: “sysname”, “syslocation”, “ifnumber”, “IfTable”, “ipAddrTable” and “ipRouteTable” for monitoring the network at distance or changing the configuration just in case of read and write variables. SNMPv3 included the SHA secure algorithm at the configuration.

3. Results

3.1. Connectivity emulation

After configuring the 28 c7200 backbone routers using OSPFv3, the connectivity of the network was tested using ping among all routers but also using traceroute as shown in figure 5 as evidence when testing connectivity from the St John´s router to the new infrastructure in Nunavut, using just 12 hops to get from east to Nunavut.

```
John#traceroute 5522::1

Type escape sequence to abort.
Tracing the route to 5522::1

  1 2514::1 184 msec 144 msec 100 msec
  2 1614::2 36 msec 8 msec 28 msec
  3 1415::1 60 msec 36 msec 36 msec
  4 1449::1 64 msec 52 msec 60 msec
  5 1258::1 92 msec 68 msec 68 msec
  6 1415::1 68 msec 72 msec 72 msec
  7 9101::2 76 msec 88 msec 84 msec
  8 5678::1 84 msec 104 msec 112 msec
  9 4567::1 108 msec 124 msec 108 msec
 10 3456::1 144 msec 144 msec 136 msec
 11 2345::1 140 msec 124 msec 156 msec
 12 5522::1 148 msec 152 msec 140 msec
```

Figure 5. Connectivity test using traceroute from ST John´s to the new infrastructure in Nunavut.

Also, for testing connectivity its was used Wireshark in GNS3 for analyzing ICMPv3 and OSPFv3 packets, but not shown for extension.

3.2. Management emulation

Figure 6 shows the result from sending SNMP packets after a get request for the name of the router for Nunavut from the NMS next to ST John´s routers, using the IReasoning MIB Browser at the virtual machine. The “sysname” variable content was obtained through the entity or agent enabled at the router, this is a read and write variable, so changing the router´s name also was tested.

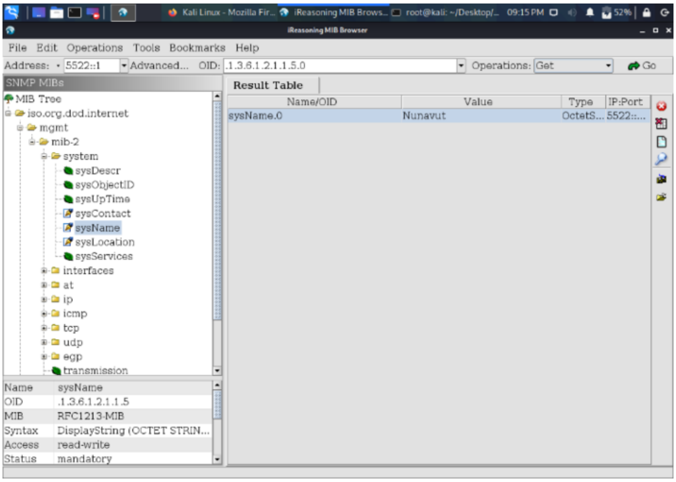

Figure 6. Management test SNMPv3 for getting the routers name for Nunavut.

Then “syslocation” and “ifnumber” were evaluated, not shown for extension and because they can be obtained using the get operation, but those kinds of test can be plotted just exemplified as the evidence shown in figure 5. So, to test *get bulk* operations, the “ifTable” was request, results are shown in figure 7, where index and descriptions are displayed.

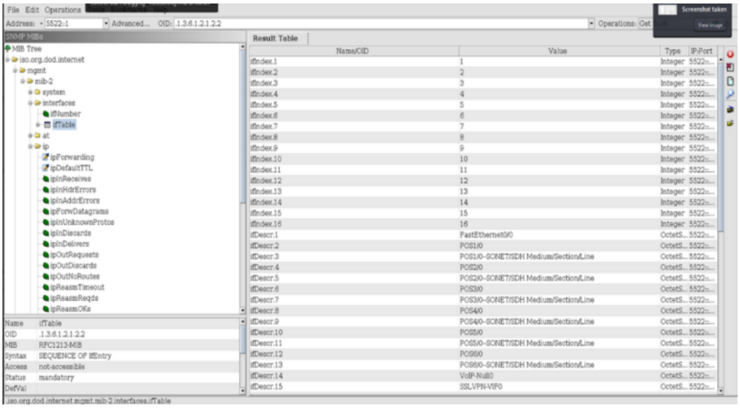

Figure 7. Management test for getting the table of interfaces for Nunavut router.

Also, for testing the *getbulk* operation a larger table was requested, the "ipAddrTable" as shown in figure 8, where some of the details are indicated. For all cases Wireshark was used to check SNMP packets sent and coming from the NMS.

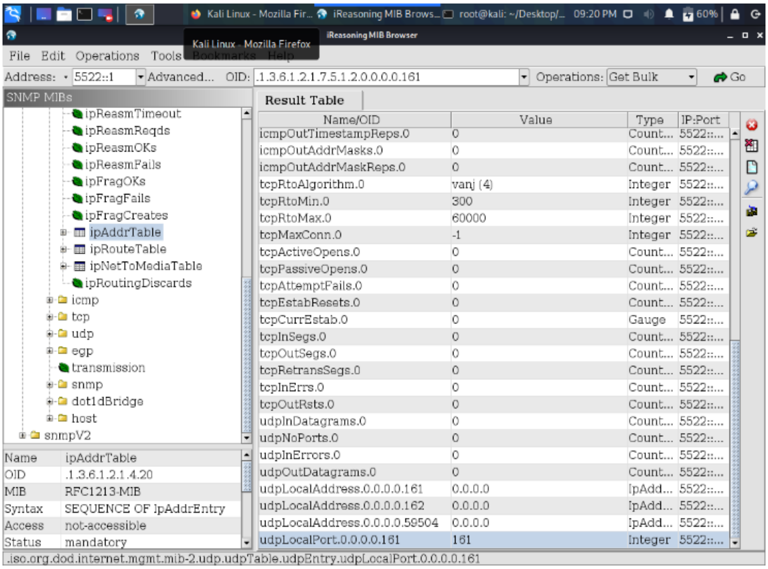

Figure 8. Management test for getting the addresses table for interfaces for Nunavut router.

3.3. Emulation resources consumption

Finally, table 1 shows the consumption of CPU and RAM by the different groups of processes when emulating tests for all the routers in the CANARIE backbone network. The average latency measured for all the connectivity tests was around 10 ms.

Table 1. CPU and RAM consumption for the CANARIE Emulation

Process	CPU % (Average)	RAM% (Average)
Connectivity	30.4+-0.1	90.2+-0.1
Management GET/SET	35.9+-0.1	90.5+-0.2
Management GET/BULK	42.4+-0.2	90.1+-0.1

4. Conclusions

This work shows the full connectivity and management of CANARIE as in 2022, including 28 backbone routers, where the OSPFv3 routing protocol, the IPv6 protocol and SNMPv3 were configured and tested. When configuring and testing connectivity, all tests were successfully, using 90.2% of RAM and 30.4% of CPU, but limited to 1Gbps links, far from real infrastructure links which support 100 to 300 Gbps. When configuring and testing management, by monitoring for GET and SET operations iReasoning MIB browser functioned correctly using 35.9% of CPU and 90.5% of RAM. While when testing GET BULK operations the computational resources usage for RAM was 90.1%, but the CPU usage rises to 42.4%. The average latency was about 10 ms. On the other hand, it is important to mention that authors had a problem when asking for the entire IP Routing Table, due to the command “go”, must be used several times to get the entire routing table. This problem, which was solved at the indicated way, could be caused by the iReasoning MIB browser free version, but that must be proved. The main trouble authors faced was the activation of traps, for that test links among routers were evaluated making link down and link up tests, but problems persisted, the possible cause could be the iReasoning MIB browser free version, but that must be proved. So, in general, the connectivity and management for CANARIE topology as in 2022 was successful, although GNS3 still has two disadvantages, first, the limit of 1Gbps Bandwidth links and second, the only Cisco backbone router supported image is for c7200, this way emulating the full CANARIE´s function as advanced network is still a challenge for ISP companies. This updated work shows that when comparing to the previous analysis developed some years ago, no significative changes impacted the update of the CANARIE topology when Canada expanded its advanced network. Emulating is the alternative for backbone networks for characterizing advanced networks around the world which uses expensive equipment only available by the Internet Service Provider companies.

References

[1] Petitti DB, Crooks VC, Buckwalter JG, Chiu V. Blood pressure levels before dementia. Arch Neurol. 2005 Jan;62(1):112-6.

[2] Rice AS, Farquhar-Smith WP, Bridges D, Brooks JW. Canabinoids and pain. In: Dostorovsky JO, Carr DB, Koltzenburg M, editors. Proceedings of the 10th World Congress on Pain; 2002 Aug 17-22; San Diego, CA. Seattle (WA): IASP Press; c2003. p. 437-68.

[3] Leslie Regan S., *Computer Networking in Canada: from CA*net to CANARIE,* Canadian Journal of Communication, Vol 19, N1, 1994.

[4] Howard C. Clark, *Formal Knowledge Networks: A syudy of candian experiences*, 1998 Ed Int. Inst. for Sust. Dev., Canada, 1998: pp. 60-61.

[5] CANARIE, *Scientific Research,* [online], 2022, [May 2022], Availiable: https://www.canarie.ca/scientific-research/

[6] Canadian ICFA, Canadian Networks for Particle Physics Research, [online];2021[May 2021] Available:http://hepnetcanada.ca/assets/themes/hepnet/documents/Canadian-ICFA-SCIC-Network

[7] J. -I. Castillo-Velazquez and A. Delgado-Villegas, "GNS3 Limitations when Emulating Connectivity and Management for Backbone Networks: A Case Study of CANARIE," 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2020: pp. 1-4

[8] CANARIE, NREN, Annual Report 2020:pp. 3-10.

[9] S. Deering, Xerox PARC, R. Hinden, Ipsilon Networks. “Internet Protocol, Version 6 (IPv6) Specification”, RFC 1883, December 1995.

[10] S. Deering, Cisco, R. Hinden, Nokia. “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460, December 1998.

[11] R.Coltun, D.Ferguson, J. Moy, OSPF for IPv6, RFC 2740, December 1999.

[12] R.Coltun, D.Ferguson, J. Moy, A.Lindem, OSPF for IPv6, RFC 5340, July 2009.

[13] J. Case et al, Introduction to Version 3 of the Internet-standard Network Management Framework, RFC 2570, April 1999.

[14] S. U. Masruroh, A. Fiade, M. F. Iman and Amelia, "Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP," 2017 International Conference on Innovative and Creative Information Technology (ICITech), 2017: pp. 1-7.