
CBC TECHNOLOGY REVIEW

Issue 2 - June 2006

www.cbc.radio-canada.ca

Inclusion of Foreign Bureaus in the CBC/Radio-Canada Wide-Area Network (WAN)

By Daniel Guimond
Senior Analyst
Broadcast & Telecom Networks

INTRODUCTION

If one had to name a single factor that sets CBC/Radio-Canada's journalistic coverage apart from that provided by other Canadian media outlets, it would surely be our superior international presence, assured by several foreign bureaus strategically located around the globe. Paradoxically though, despite their significant presence, until very recently these overseas bureaus have not been able to benefit from the latest technology when it comes to communications with any of the Corporation's bureaus in Canada. Solutions for sending reports to the network centres in Montreal and Toronto have until now been initiated locally (that is, at the foreign bureau end); while these have sometimes shown originality, they have never met the standards for quality and stability that these bureaus, given their status, deserve.

In response to several connectivity issues with some overseas CBC/Radio-Canada bureaus, managers from Broadcast & Telecom Networks (BTN) have agreed to support the author's initiative: namely, to proceed with standardization of foreign bureau network connectivity within the Corporation.

This article begins with a discussion of the criteria that were used to draw up the list of CBC/Radio-Canada foreign bureaus that should be included in connectivity standardization (i.e., connection to the CBC/Radio-Canada Wide Area Network [WAN]). This is followed by a description of the chosen technology solution, known as the "Beijing model." The author then discusses some issues specific to certain regions, as well as the vagaries of working in foreign countries and the accompanying challenges, which are many and often unexpected. The article concludes with a description of the technical benefits of including foreign bureaus in the Wide-Area Network (WAN), and an analysis of some statistics.

SELECTION CRITERIA

The initial phase of the project, in early 2004, involved gaining an understanding of the existing network infrastructure in all of our bureaus outside Canada, so as to determine the scope of the task ahead.

It was immediately evident that network connectivity in the United States bureaus— the three New York City bureaus and the one in Washington, D.C.—was compliant with Broadcast & Telecom Networks (BTN) standards. At the time of our survey, the New York bureaus were (and are still) using VPN¹ technology to connect to the CBC/Radio-Canada corporate WAN via the Internet. The Washington bureau, meanwhile, was reliant on ATM² technology, and has since migrated to the same VPN technology used by the New York offices. The bureaus in Dakar, Senegal, and Rio de Janeiro, Brazil, with their reduced staffs, continued to use simple VPN clients installed on notebook computers to connect to the WAN. That left six foreign bureaus that, for various reasons, made the list of foreign bureaus that should be included in CBC's connectivity standardization.

The Paris and London bureaus were chosen in consideration of technical and (especially) budget criteria: as of spring 2004, these two bureaus were still reliant on the ATM protocol, and conversion to the Beijing model since then has ensured greater bandwidth while saving the Corporation some \$100,000 annually in telecommunications costs.

A second group of bureaus—Beijing, Moscow, Beirut and Jerusalem—was selected because of connectivity that was deficient, non-standard and extremely difficult to troubleshoot when issues arose. There was, therefore, a most urgent need for telecommunications standardization sites, which are so crucial to our newsroom operations.

THE BEIJING MODEL

By far, the situation in Beijing required our most immediate attention, and led to development of what BTN now calls the Beijing model. Chosen as the standard for ensuring acceptable connectivity of foreign bureaus to the corporate WAN, this model consists of an internet connection established via a Nortel VPN Router 1000 Series (formerly Nortel Contivity 1000 Series³) using so-called split tunneling technology.

Before a technology solution for the foreign bureaus could be rolled out, we had to define a model that would be functional regardless of the site in question. When testing was conducted in spring 2004, it quickly became clear that VPN Branch Office was the only cost-effective technology that would suit the budget. The VPN Branch Office uses encrypted tunneling to connect to the internet, and at the time was already deployed within Canada for some fifty sites outside major centres.

¹ Virtual Private Network: Private communications network carried on the Internet using encryption protocols.

² Asynchronous Transfer Mode: A telecommunications protocol for transmission of data over providers' private networks.

³ See http://products.nortel.com/go/product_content.jsp?segId=0&parId=0&prod_id=34721&locale=en-US

The standards in effect at the time, however, demanded that all traffic be captive of the VPN tunnel; in other words, users had to proceed via Toronto for all communications—including, for example, accessing the website of a regional unit whose “brick-and-mortar” physical location might be only two blocks away. Given the speed of internet connections across Canada, the latency cost incurred by having every query routed through the Toronto firewall remained relatively viable. In contrast, however, one can well imagine the response time for a query from an employee of the Beijing bureau wishing to access the website of CCTV (China Central Television) that requires routing through Toronto before being delivered. Fortunately, the Nortel Contivity 1000 Series router supports configuration of an encrypted tunnel for key networks, with local access for others. Secure local access is guaranteed by the Nortel router’s internal “stateful firewall”. In the case of CBC/Radio-Canada, only IP networks 1.x.x.x, 10.x.x.x and 192.168.x.x are routed through the tunnel; all others enjoy direct local access (see Figure 1).

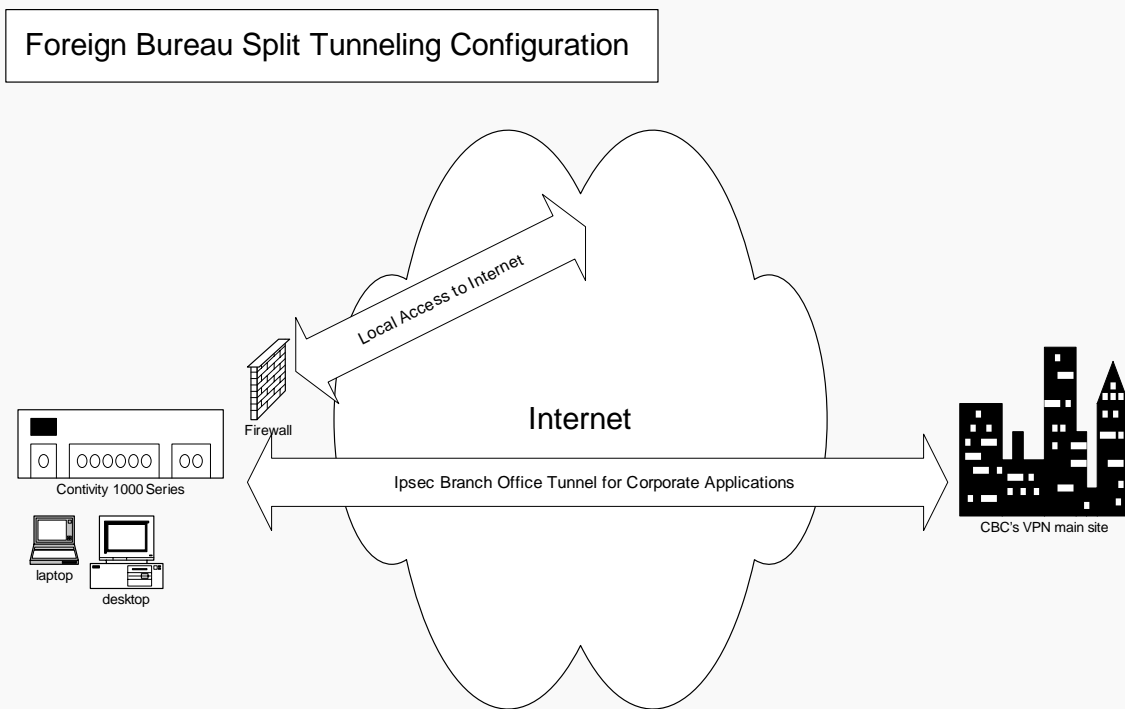


Figure 1. Split Tunneling Configuration

REGION-SPECIFIC ISSUES

During the project to migrate the various bureaus to WAN access, certain issues cropped up that were related specifically to those bureaus’ locations. Negotiating business requirements with local authorities is not always easy; CBC/Radio-Canada does not enjoy the same name recognition everywhere as it does within Canada. Obviously, that observation is not directed at the London and Paris bureaus—the only issues faced there were the normal technical challenges inherent to this type of project.

China, as is well known, is an emerging nation on several fronts, and is increasingly open to the rest of the world. Despite that openness, however, the Chinese authorities enforce strict rules when it comes to answering service requests from the Western media, as well as ensuring that all foreign media bureaus are housed in sites of the government's choosing. The employees of CBC/Radio-Canada's Beijing bureau, along with those of almost all foreign media, live and work in the Jianguomenwai Diplomatic Compound. The site is subject to surveillance, and the identities of anyone wishing to enter are checked (see Photo 1).

Only the BBC, in the wake of Great Britain's retrocession of Hong Kong to China, seems to enjoy any preferential treatment; its staff is more or less free to set up shop where they choose. It is important to mention, however, that the concentration of foreign media bureaus in one location by the Chinese authorities is not altogether a bad thing. Within the walls of the Jianguomenwai Diplomatic Compound, there is significant solidarity among foreign media employees, who all must deal with the same administrative constraints.



Photo 1. Entrance to the Jianguomenwai Diplomatic Compound, Beijing, photographed by the author in April 2004

The language barrier can result in the occasional awkward situation: during pre-testing prior to migration of the Beijing bureau, it soon became clear that the Internet connection provided by Beijing Telecom was causing 15% of packets to be dropped during peak periods. One can well imagine the challenge of explaining the problem through an interpreter who lacks the technical know-how and terminology to understand what needs to be translated. In the end, Beijing Telecom admitted that the problem existed, but said that nothing could be done to improve the situation. A quick check with our "neighbours" in the Compound—NBC, CBS and Australia's ABC—regarding transmission quality revealed that the missing packets problem was not unique to CBC/Radio-Canada. (The Chinese authorities designate an official ISP for the Jianguomenwai Compound, and there is no way for the foreign media bureaus to use another provider.)

Different country, different challenges: during preparations for the Russia component of our project in November 2004, employees of the Moscow bureau warned us against importing hardware into the country, as heavy taxes would be levied.⁴ Fortunately, Nortel hardware is available for sale in Russia, and the Moscow bureau was able to adopt the same technology to connect to the WAN.

Pleasant surprises can always occur . . . The old Soviet regime had left the local Internet infrastructure in such a sorry state that authorities had no choice but to build a new network from scratch. As a result, our Moscow VPN site is proving to be the most stable connection, as measured by monthly reporting.⁵

In the Middle East, the challenges are more complex. For obvious economic and geographic reasons, our Beirut and Jerusalem bureaus merited inclusion in our VPN infrastructure migration during the same trip. The extreme political tensions in the region, however, make it extremely difficult to jointly coordinate migration of the two sites.

First of all, the border between Lebanon and Israel has been closed since the withdrawal of Israeli troops from southern Lebanon in the mid-1980s, which means that to get from Beirut to Jerusalem, one must now detour through Jordan. Furthermore, anyone attempting to enter Lebanon from Israel, or to transit through the country to get to Israel, is systematically barred from entering by the Lebanese authorities. All documentation relative to the Israel component of the project was therefore sent directly to Jerusalem by mail, to avoid it falling into the hands of Lebanese customs agents during a search.

TECHNICAL BENEFITS, STATISTICS

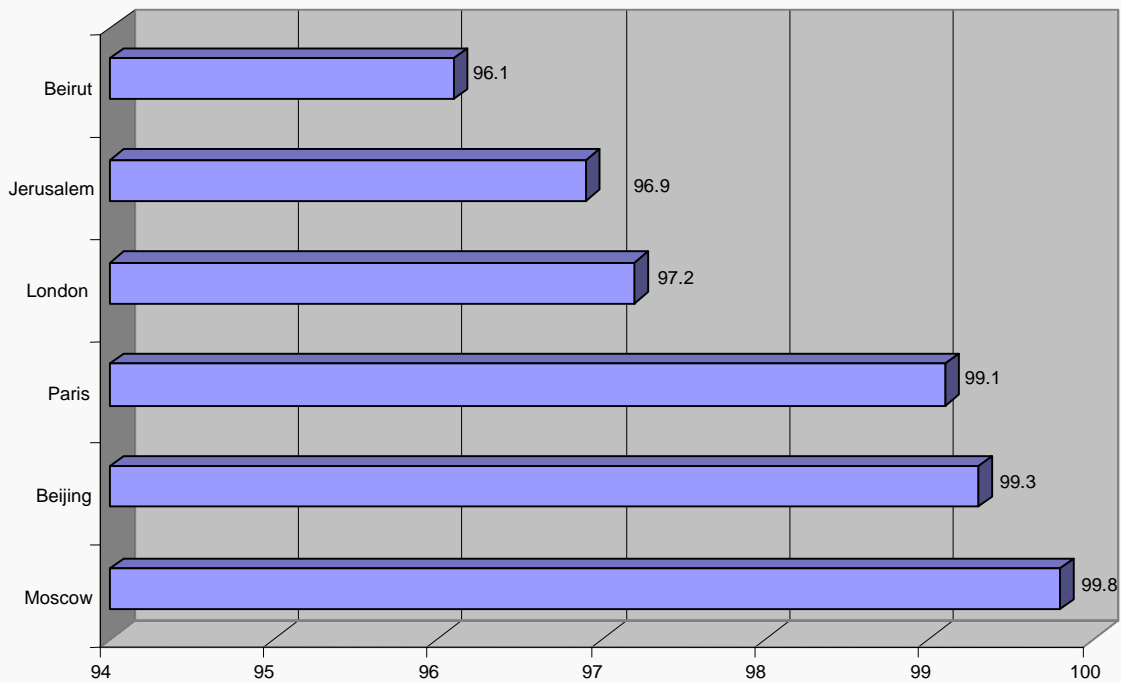
The six foreign bureaus covered by the project now included in our VPN infrastructure also benefit from full technical support from CBC's home base in Canada. Telecommunications standardization at these sites now enables BTN to track network traffic trends for the bureaus and recommend increased bandwidth assignments as needed. Monitoring and statistics, meanwhile, enable detection of any suspicious behaviour (such as viruses) and use of a proactive approach to network stability and security. In many cases it is now possible to take advantage of the time difference to detect and resolve a problem before the employees of a given bureau show up for their shift. All traffic from foreign bureaus is now captured, and all problems reported can now be efficiently analyzed. Stability is another benefit of connectivity standardization: when major events occur, the foreign bureaus can now welcome special teams without causing chaos. The Jerusalem bureau, for instance, was able to provide quality connectivity to extra personnel during coverage of Prime Minister Ariel Sharon's emergency hospitalization, and during the most recent Israeli legislative elections.

Looking at the statistics, it is surprising to note that locations at the mercy of the vagaries of the internet fare quite well overall. Graph 1 shows figures for the month of January 2006, which reveal more-than-acceptable network availability in Moscow (99.8% availability) as well as Beirut (96.1% availability).⁶ Graph 2 details average round-trip response times as calculated from Montreal.

⁴ The rate can go as high as 50% of the item's value the first year and 30% of its value for subsequent years of use.

⁵ See statistics in the following section.

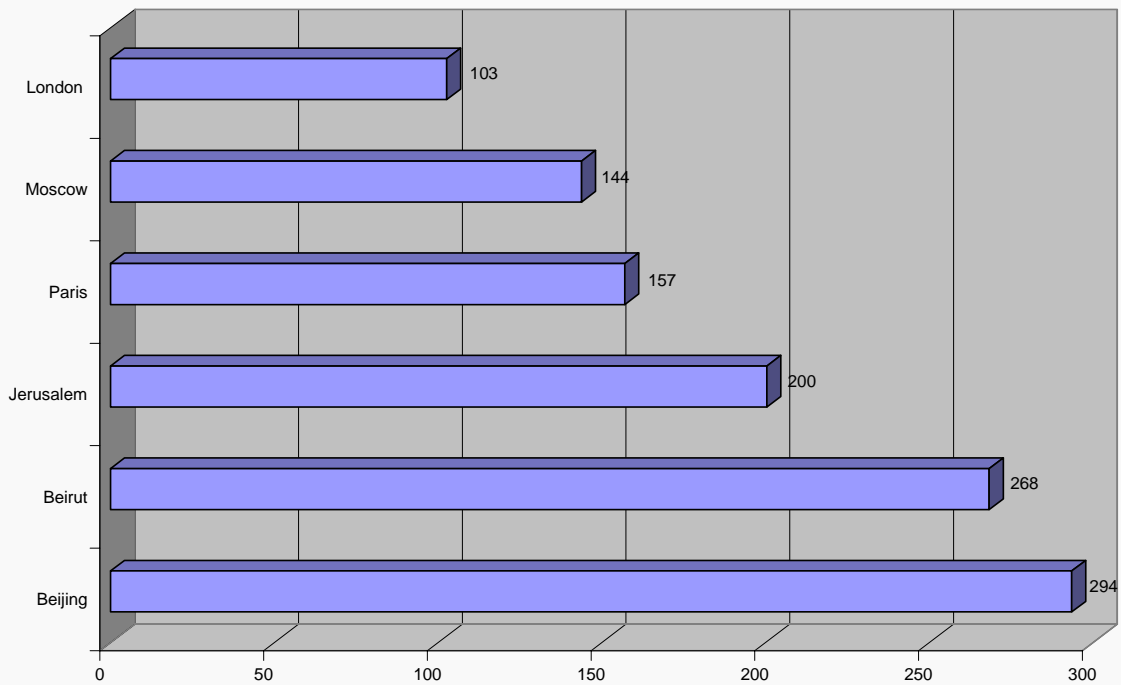
Availability in % (Jan. 2006)



⁶ SNMP polling every 10 minutes; percentage denotes number of successful pollings.

Graph 1. Percent availability of sites

Response Time in ms (roundtrip) (Jan. 2006)



Graph 2. Roundtrip response times to/from Montreal (milliseconds)

CONCLUSION

While explaining the technologies in use and describing the performance of the various sites that have been migrated to our VPN infrastructure is a useful exercise, there is one fact that we must keep in mind when providing support to staff in our foreign bureaus: More often than they should need to, these people risk their lives in the course of their duties. Whether in danger zones like Chechnya, the Gaza Strip or Baghdad, or simply sitting in their offices (see Photo 2), our overseas personnel often work in very tense situations, and they deserve the unconditional assistance of our support teams. Under no circumstances should the foreign bureaus be viewed as “normal” bureaus. They have specific needs, and it is up to us—the support teams—to adjust to their realities, not vice versa.



Photo 2. Reception area of the Beirut bureau after a car-bomb attack.⁷

Improvements in intercontinental connectivity represent a key factor in rapid transmission of news reports (e.g., via on-site Telestream equipment⁸), as do corporate applications such as iNews and GroupWise, when used effectively. Unfortunately, there are many extant issues. The LANs in our foreign bureaus are often improvised and obsolete, while the computers are aging in general. Furthermore, there is no standard procedure for analyzing technology requirements when opening new bureaus. With better coordination, we could target needs more effectively to avoid these and similar pitfalls.

⁷ View full article by Nahlah Aayed at <http://www.cbc.ca/news/reportsfromabroad/ayed/20050228.html>

⁸ ClipMail Pro and ClipRemote; see <http://www.telestream.net/>

With connectivity now standardized in these foreign bureaus, now may well be the time to look a bit further down the road (or, rather, aim a little higher) to see whether the latest advances in satellite technology⁹ might provide the capability to create mobile VPNs from the ground up when major events occur on the other side of the world (e.g., the recent natural disasters in Asia and the Southern U.S., feature reports from Afghanistan). Several feasibility tests are to be conducted in the near future, and our analysis of those tests will tell us whether that avenue is worth exploring. This will represent another noble challenge for the Broadcast & Telecom Networks group.

To Daniel Morin, Gilles Plante, Patrick Brown, Zhu Tao, Michael Kearns, Charles Dubois, Yvon Corre, Jon Anderson, Marie-Ève Bédard, Alexei Sergueev, Irina Melnikova, Tatiana Stukalova, Nahlah Ayed, Zouhair, Hussein, Adrienne Arsenault, Ian Kalushner, Azur and Helena—each, in his or her own way, an unsung hero of CBC/Radio-Canada.

Daniel Guimond
Senior Analyst
Broadcast & Telecom Networks



After starting his career at CBC/Radio-Canada Montreal in 1977, Daniel Guimond held a variety of positions in the computer operations unit until 1986, when he began working in the various telecommunications units as an expert in network protocols and standards such as X.25, Ethernet, FDDI, ATM, MPLS and VPN. He is currently senior analyst, Broadcast & Telecom Networks. He is also part of the Wide Area Network (WAN) team, and responsible for national election coverage team telecommunications needs.

⁹ See <http://broadband.inmarsat.com/>