Winter / Hiver 2002
No. 39

IEEE

Previous issues also available on-line at: www.ieee.ca

http://www.ieee.ca

Canadian Review

La revue canadienne de l'IEEE

- Canadian Newslog / *Coupures de Presse Canadienne*
- Multi-Service Computing Platform for Telecom Applications
- IEEE Canada Awards
- Region 7 Director Report, Fall 2001
- Securing your Network: Protecting Valuable Corporate & Intellectual Property
- Mainframe Computing Architecture Re-Invented - Open for Business
- Letters to the Editor / *Lettres envoyées au rédacteur en chef*
- Connecting Continents
- On Managing Virtual Private Networks
- Modeling Flow & Congestion in Packet Switching Networks
- The Engineering Institute of Canada, it's History & Import
- IEEE Canada, CCGEI 2002
- IEEE Canada, CCECE 2002

IEEE Canada

The Institute of Electrical and Electronics Engineers Inc.

Canada Post - Canadian Publications Mail Sales Product Agreement # 1804308

IEEE Canadian Review General Information

The ***IEEE Canadian Review*** is published 3 times/year as follows: Spring (to appear in April); Summer (to appear in August); Fall (to appear in December). Its principal objective is to project an image of the Canadian electrical, electronics, communications and computer engineering professions and their associated academic and business communities to:

(i) Canadian members of IEEE;
(ii) Canadian members of the profession and community who are non-members of IEEE;
(iii) The associated Canadian academic (i.e. universities, colleges, secondary schools), government and business communities.

To ensure that the ***IEEE Canadian Review*** has the desired breadth and depth, editors are responsible for screening articles submitted according to the following general themes:

1 - National Affairs	4 - Education	7 - Computers
2 - International Affairs	5 - Power	8 - Electronics
3 - Industry	6 - Communications	

Advertising Policy

Organizations are invited to place corporate advertising in the ***IEEE Canadian Review***. For information regarding rates and copy requirements, please contact the Managing Editor.

Circulation

The circulation of the ***IEEE Canadian Review*** is the entire membership of IEEE Canada, representing over 12,000 subscribers.

Information for Authors

Authors are invited to contribute submissions in electronic form to the ***IEEE Canadian Review***. Please contact one of the editors. Responsibility for the content rests upon the authors and not the IEEE, or its members.

Annual Subscription Price

Free of charge to all IEEE members in Canada. For IEEE members outside Canada: $20.00/year. Price for non-members: $30.00/year. Corporations and libraries: $37.50/year. Additional copies may be ordered at a cost of $7.50 each from the Managing Editor.

Reprint Permission

Abstracting is permitted with credit to the source. Libraries are permitted to photocopy for private use of patrons. Instructors are permitted to photocopy isolated articles for non-commercial classroom use without fee. For other copying, reprint or republication, please write to the Managing Editor. The ***IEEE Canadian Review*** is printed in Canada, postage paid at Toronto, (Ontario).

Change of address

Please send change of address notice directly to:

IEEE Service Center,
445 Hoes Lane, Box 1331,
Piscataway (New Jersey) 0885, USA
or by email at “member.services.7@ieee.org”
or address.change@ieee.org

IEEE Electronic Newsletter

IEEE related events and news of a topical nature may be published in the **IEEE Canada** email/fax Newsletter. Submissions should be emailed to the Editor Aby Gupta (a.gupta@ieee.ca). The Internet home page address of **IEEE Canada** is:

“http://www.ieee.ca”

Member Society of the Engineering Institute of Canada

The National Library of Canada
ISSN 1481-2002

Quelques mots du rédacteur en chef

Vijay K. Sood, Hydro-Québec, Varennes, QC

L'es derniers quelques mois ont été très intenses en évènements mondiaux. Ceci a résulté en une baisse marquée des soumissions de publication; maintenant les choses semblent revenir à la normale. Ce numéro arrive donc avec environ un mois en retard dû aux réponses tardives ou inexistantes des auteurs potentiels.

Une annonce importante: IEEE Canada a pris position et La revue canadienne de l'IEEE sera un journal en-ligne dès 2002. Ceci aura les bénéfices suivants:

- Coûts réduits de par l'élimination des publications papiers et des
- frais de poste (ces deux coûts étaient très importants)
- Récupération améliorée et plus rapide des informations en-ligne et
- Interaction plus rapide avec vous, les membres.

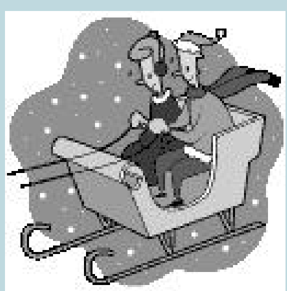
Finalement, une autre année est terminée! J'ai apprécié grandement ce défi et je peux seulement espérer que vous, les lecteurs, en avez apprécié le contenu.

Il est maintenant venu le temps de remercier plusieurs personnes, malheureusement je ne peux les nommer tous à l'intérieur de ces lignes. Toutefois, je désire spécialement remercier mon épouse Vinay pour son dévouement à réaliser ce magazine; sans son effort soutenu, ce travail n'aurait jamais été possible. Je remercie mes éditeurs associés pour leur aide, je suis fier d'eux. Également, un gros merci à IEEE Canada pour l'opportunité qui m'a été donnée (ainsi que pour le prix, voir page 8) d'essayer de nouvelles idées innovatrices avec ce journal. C'était vraiment agréable.

Finalement, je vous souhaite une merveilleuse année 2002.

Bonne Année!

Happy New Year!



A few words from the Managing Editor

The past few months were very hard in terms of world events. This resulted in a marked decrease in paper submissions; but now things seem to be returning to normal. This issue is, therefore, about a month late due to either unkept or delayed responses from potential authors and some other reasons.

An important announcement: IEEE Canada has finally made up its mind that the IEEE Canadian Review is now going to be an on-line journal in 2002. This will have the following benefits:

- Reduced costs due to elimination of the hardcopy version and no mailing costs (both costs were quite significant),
- Improved and timely retrieval of on-line data, and
- Faster turn around time to reach you, the membership.

Finally, another year is over! I enjoyed this challenge thoroughly, and I can only hope that you the member-readers got some value out of it.

It is time for me to say thanks to a lot of people; I cannot name them all in this space. However, I do thank my wife Vinay for all her dedication in putting this magazine together; without her efforts, this job could never have been done. I thank my Associate Editors for their assistance. Also, thank you IEEE Canada for the opportunity (and award, see page 8) to try out some new creative ideas with this journal. It was a lot of fun. And, of course, thank you all for your input and letters.

Finally, have a great New Year 2002!

Cover picture / *Photo de couverture*

Multi-Service Computing Platforms for Telecom Applications

Convergence of voice, data and multimedia applications onto telecom networks has involved deployment of access devices to support the next-generation telecom applications being built at the edge of the network - SS7 gateways, media/VoIP gateways, media gateway controllers and edge routers. Motorola Computer Group of Canada, a part of Motorola, Inc., which provides embedded boards and system-level platforms for nine of the world's top 10 telecommunications original equipment manufacturers (OEMs), recently launched the MXP -- a multi service platform combining open standards for switching IP and ATM packets. It also offers the speed, high bandwidth, performance flexibility and data storage capacity required for development and deployment of advanced applications. Such solutions protect the industry-wide investment in circuit-switched technology and provide telecom OEMs and third-party vendors with an easier path to the newer all packet network.

Contents / *Sommaire*

Newslog Editor

Rédacteur des coupures de Presse

Alexandre Abecassis is a patent agent trainee at Swabey Ogilvy Renault, patent and trademark agents in Montreal.

Alexandre Abecassis travaille à Montréal chez Swabey Ogilvy Renault, agents de brevets et de marques de commerce, comme agent de brevets en formation.

Send any news clippings you would like to contribute via e-mail to alexandre.abecassis@ieee.org

Veuillez faire parvenir les coupures de presse proposées par e-mail à alexandre.abecassis@ieee.org

TORONTO, ON, AUSTIN, TX, Nov. 26, 2001. 724 Solutions which provides secure mobile Internet infrastructure software and application has been chosen as one of the top emerging companies for 2002 by US based Computerworld, Inc. The company has been chosen for its innovation as well as for its ability to develop its strategy.

LAVAL, QC, le 15 nov. 2001. Le centre de cardiologie de Lavalette à Montpellier (France) a choisi la compagnie québécoise Electromed Inc pour fournir une solution en imagerie médicale. Le système développé par Electromed Inc permet notamment l'acquisition de données provenant de salles d'angiographie cardiaque et périphérique ainsi que d'échographie cardiaque, l'archivage et la transmission de dossiers médicaux complets.

MONTRÉAL, QC, Nov. 9, 2001. For the first time, a distributive violin duet was performed in real-time over a wide area in full-screen video. The two performers, separated by several kilometers, were able to see each other using the RISQ (Quebec Scientific Information Network) network. The software was developed by Stephen Spackman from McGill University. The system does not use any signal compression.

LONDON, ON and ROCKVILLE, MD, Nov. 7, 2001. Celera Genomics and Compaq Canada Corp form an exclusive marketing distribution agreement. Compaq Canada will be the preferred distributor of access to the Celera Discovery System (CDS) which is Celera's proprietary bioinformatics platform to provide access to its data. Celera announced last year the first assembly of the human genome.

TORONTO, ON, Nov. 5, 2001. The Department of Computing and Information Science of Queens University announced that it is using Avaya's collaborative technology to create the first the first integrated operation room with Kingston General Hospital enabling more than 30 graduate students to use their laptop to monitor orthopedic surgeries.

MAGOG, QC, le 30 oct. 2001. La ville de Magog qui produit 10% de sa consommation électrique a signé une entente de 12 mois avec Captech Multicom inc. pour un projet de télémétrie de la consommation électrique. 100 participants de type "résidentiel" et 100 participants de type "commercial" pourront avoir accès de façon intéractive aux données concernant leur consommation électrique respective. Une alarme pourra même éventuellement être activée par les utilisateurs si des consommations excessives sont détectées.

WATERLOO, ON, Oct. 22, 2001. Research in Motion (RIM) and Informatica Corporation announced an agreement to integrate Informatica's product within the Blackberry wireless system. This agreement will enable corporate users to receive alerts through their wireless system. Furthermore, this will allow the users to receive indicators, enterprise communication details, etc. With such informations, nomadic users may be able to perform wise decisions according to critical data. The solution is provided using a secure connection.

TORONTO, ON, Sep. 25, 2001. AirIQ which was formed in 1997 as a partnership between Bell Mobility, Lenbrook Inc. and Veridian engineering announced a contract with Dunkin' Donuts for fleet management service. AirIQ solution uses Internet through wireless solution, Global Positioning System (GPS) technology and digitized mapping.

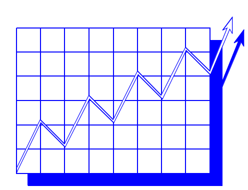
SAN DIEGO, CA, le 11 sep. 2001. Sirific, société crée par un professeur de l'Université de Waterloo (Ontario), a dévoilé une technologie permettant la conversion des radiofréquences au sein d'un seul composant électronique. L'architecture logicielle développée permet le support des standards AMPS, TDMA, EDGE, CDMA2000, GSM, GPRS et W-CDMA ainsi que les technologies Bluetooth et IEEE802.11.

LAVAL, QC, le 10 sep. 2001. L'École de Technologie Supérieure (ÉTS) a adopté les produits de Colubris Networks comme la norme de formation pour les cours de télécommunication concernant la technologie IEEE 802.11b. Colubris Networks développe des solutions d'accès sans fil sécurisées. Les routeurs offrent par exemple des accès sans fil sécurisés à d'autres réseaux, locaux ou étendus. Les produits de Colubris Networks intègrent notamment des fonctionnalités de réseau privé virtuel (VPN), de coupe-feu (Firewall).

HALIFAX, NS, Aug. 27, 2001. An home telehealth service was launched by March Networks and We Care Health Services Inc. The goal of the service is to evaluate a telehealth service involving 140 clients. The solution will enable remote nursing visits and vital sign monitoring through the deployment of interactive video, audio and data transmission over a IP network. The solution should reduce the cost of the health care system according to one of the CEO of We Care Health Services Inc.

MONTRÉAL, QC, Aug. 21, 2001. Andromed has received a Canadian patent for its electronic stethoscope. Andromed has created the first fully electronic stethoscope. The electronic stethoscope comprises filtering circuits to filter for instance low frequency rumble which originate from the patient or the practitioner movements in order to provide cardiac and the pulmonary sounds. Furthermore, this electronic stethoscope allows the practitioner to auscultate heart valve prostheses.

TORONTO, ON, le 7 nov. 2001. Telus Mobilité a réalisé une démonstration de son accès Internet haute vitesse, grâce à l'utilisation de la téléphonie de type troisième génération (3G), au congrès annuel et salon des télécommunications Communications 2001. Le réseau 3G de Telus Mobilité utilise la norme CDMA2000 et permettra des taux de transfert minimum de 144kbps. La majeure partie du réseau 3G de Telus Mobilité au Canada sera réalisée d'ici le début 2002.



Multi-Service Computing Platforms for Telecom Applications

by Robert G. Pettigrew, P.Eng,
Motorola Computer Group, Ottawa, ON

Abstract

The next-generation telecom applications being built at the edge of the network - SS7 gateways, media/VoIP gateways, media gateway controllers and edge routers - rely on multi-service computing platforms with powerful processing and storage capabilities that support multiple protocols such as IP, ATM and Frame Relay packet data. The flexibility inherent in the architecture of multi-service computing platforms protects the industry-wide investment in circuit-switched technology and provides telecom OEMs and third-party vendors with an easier path to the newer all packet network. Where time-to-market was once the primary motivator for outsourcing of platform solutions, in today's more volatile market telecommunications environment OEM's are relying on outsourcing to stay focused on leveraging their resources and unique expertise. The name of the game is ensuring they are well positioned to address the challenges and opportunities of the converged telecommunications network when the market rebounds.

Sommaire

Les applications en télécommunication de la nouvelle génération, construites à l'extrémité du réseau (passerelles SS7, passerelles media/VoIP, les contrôleurs de passerelles media et les routeurs d'extrémité), dépendent d'unités de traitement possédant de grandes capacités de traitement et de stockage et qui permettent une compatibilité avec des protocoles de communication de type "paquet" tels que l'IP, l'ATM et le "frame relay". La flexibilité inhérente dans l'architecture des unités de traitement multi-service protège les investissements dans les technologies orientées "circuit" et fournit des OEMs dans le domaine et des vendeurs tiers possédant une meilleure flexibilité vers les nouveaux réseaux de type "paquet". Dans le passé, le temps de commercialisation était la première motivation pour sous-traiter les unités de traitement ; dans le monde actuel, plus instable, la sous-traitance est utilisée par les constructeurs d'OEMs afin de pouvoir conserver leur ressources ainsi que leur expérience unique. L'objectif est de s'assurer qu'ils restent bien positionnés pour aborder les défis et les opportunités de la convergence des données lorsque la situation économique repartira.

1.0 Introduction

The explosive growth in outsourcing platform design to standards-compliant systems in the telecommunications equipment infrastructure industry was originally driven by incredible time-to-market pressures faced by the industry. Rather than design everything from the ground up, telecommunications equipment vendors concentrated on their key differentiating technologies, and outsourced as much of their systems as possible.

Recent industry volatility has not alleviated pressures to outsource. Engineering design teams are now focussed on ensuring they are well positioned to take advantage of the inevitable resurgence of the market. Today, shrinking development budgets have replaced time-to-market as the primary motivator for outsourcing.

As the telecommunications market evolves, the increasing convergence of voice, data and multimedia applications onto telecom networks has involved deployment of various access devices to the edge of the network to provide new applications or services. The proliferation of these devices has lead to interoperability and configuration management issues at the network edge. These issues have escalated the need for a platform that can provide powerful processing and storage capabilities for control applications and a high throughput bearer architecture that supports multiple services on circuit-switched and packet networks. The ability to accommodate different protocols such as Internet Protocol (IP), asynchronous transfer mode (ATM), and Frame Relay without unnecessary conversion and overhead represents a significant step forward in network convergence.

2.0 Standardization of Platform Architectures

Technologies such as CompactPCI® have been adopted by telecommunications OEM's to provide standards-based platforms. Governed by PICMG, CompactPCI systems adapt PCI technology ubiquitous in desktop computers to something suitable for deployment in industrial and telecommunications applications. Specifically, CompactPCI offers a rugged form factor, with gas-tight pin-in-socket connectors, support for hot-swap of boards, rear access for cabling, and excellent shock and vibration characteristics.

CompactPCI systems suitable for deployment in telecommunications central office environments must also meet stringent survivability (earthquake and fire) and Five Nines availability requirements. Systems that meet these requirements have been available for several years, from companies such as Motorola. These systems adhere to PICMG standards such as PICMG 2.0, the core CompactPCI specification, PICMG 2.1, which adds hot-swap of I/O boards, PICMG 2.5 (H.110), which adds a data path for Time Domain Multiplexed (TDM) voice channels, and PICMG 2.9, which defines shelf management.

PICMG 2.16 for Compact PCI, introduced by Performance Technologies Inc. and ratified in September 2001, overlays an embedded Ethernet switching fabric on the backplane in CompactPCI systems. It complements standards such as PICMG 2.0 and 2.5, making it possible to implement systems that incorporate CompactPCI bus, H.110 and Ethernet fabric communication mechanisms.

PICMG 2.16 could provide an all-packet infrastructure with IP as the core packet transport. The architecture provides up to 1Gb/s per board of bandwidth for a system capacity approaching 20Gb/s in large systems. However, this architecture only supports IP transport, limiting its scope largely to Metropolitan Area Networks and Local Area Networks. Although there is movement towards Gigabit IP transport, generally the core of the network uses TDM and ATM for public switching.

3.0 Meeting the Needs of the New Network

A flexible platform capable of accommodating a variety of protocols and services integrated into a base platform represents an optimum solution for the ever-changing needs of the telecom industry. The infrastructure of the platform requires sufficient bandwidth to meet current and future needs at the network edge where the industry will experience significant growth in the foreseeable future.

To meet the high bandwidth and speed requirements of the edge and access portions of the network, telecom OEMs must efficiently process large amounts and different types of traffic. A key strategy to meeting these high bandwidth and speed requirements - while also leveraging the move toward open standards - is to add a high-speed mesh data fabric to augment the PICMG 2.16 Ethernet packet switching backplane standard. This fabric could be used for distributed processing and storage, as well as for bearer plane applications. The high-speed mesh data fabric fills a void for bandwidth, protocols and Quality of Service (QoS) that are not supported by IP, creating a multi-computing environment that can compete with higher-end symmetric multiprocessing systems.

Combining these features in a single data transport platform allows the entire spectrum of edge applications to be addressed. The resulting multi-service platform delivers optimum performance in data plane, control plane or integrated data and control applications.

Motorola Computer Group recently introduced a system that incorporates this full mesh fabric to address the evolving needs of the packet world. The highly flexible Multi-Service Packet Transport Platform (MXP) is built to adhere to open industry standards regulated by PICMG, provides fast throughput (more than 700Gb/s aggregate bandwidth), and the flexibility and scalability to deliver multiple services that can connect different networks - IP and ATM.

Motorola's packet transport platform addresses the critical areas OEM's face when considering the packet-based network:

- Leveraging open standards,
- Addressing multiple protocols,
- Meeting increasing speed and throughput requirements, and
- Connecting to traditional circuit networks.

3.1 Leveraging Open Standards

Standards-based systems provide access to compatible products from a broad range of vendors, maximizing OEM choice. Standards can only be generated from existing technology and in fast-evolving markets need to be augmented with forward-looking new ideas and technologies. The MXP design approach offers a desirable combination of standards-based design and forward-looking innovation.

The MXP platform has an open, extensible network architecture that adheres to all relevant PICMG CompactPCI standards - PICMG 2.0 Core Specification, PICMG 2.1 Hot Swap Specification and PICMG 2.16 Packet Backplane Specification for packet switching architectures. In addition, the MXP adheres to PICMG 2.9 Intelligent Packet Management Initiatiative for optimal system resource management.

IPMI is an industry standard used in Intel® based enterprise computers for management of peripherals by a PC. The IPMI protocol defines the data structure of the messages passed over the IPMI bus (IPMB) and Inter-Chassis Management Bus (ICMB), based on the I2C serial bus standard.

The IPMI Peripheral Management (PM) chip on each board in the system provides device discovery and control of power to the rest of the board. PICMG adopted IPMI for use in CompactPCI shelves or chassis as the PICMG 2.9 standard. Many telecom equipment suppliers have developed support for the PICMG 2.9 standard in both CompactPCI chassis and boards.

3.2 Addressing Multiple Protocols

Defined as a true multi-service platform, the MXP provides the flexibility and scalability needed to deliver multiple services that can connect to different networks. The platform architecture adds new features, such as a high-speed mesh data fabric and packet processor, which provides much higher data throughput and also supports multiple packet protocols. This feature removes the need for protocol conversion and opens the way for much higher data throughput rates. It also enables upgrade paths to users whose evolving needs cannot be met by architecture based entirely on existing standards.

3.3 Meeting Speed, Throughput and Application Requirements

Three key features of the MXP series architecture enable it to achieve the high speeds and throughput necessary to support applications both on the control and data plane:

- Non-shared, multi-gigabit fully meshed data fabric enabling a high-speed data environment,
- Fibre Channel fabric to support distributed storage applications,
- IPMI interconnection for combined system and resource management that increases the available payload by eliminating the need for PCI bridging and PCI system slots.

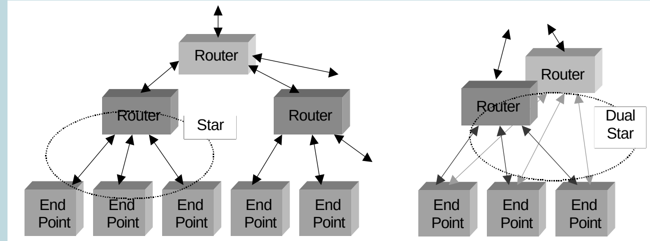


Figure 1: Star and Dual Star Topologies

Star topologies use a 'point to point' configuration where each device uses a dedicated link to send and receive data from a central resource. This resource provides the data distribution for the system. Ethernet networks are a hierarchy of star networks. Each sub-network is a leg on a star of the next layer in the hierarchy. Because reliance on a single central resource can result in a loss of all elements below a failure point, star topologies require redundancy for reliability. The PICMG 2.16 specification topology is a dual star configuration.

There are many topologies for wiring boards and systems to transport information. They differ in factors like cost (pins to connect, speed, logic costs, etc.), reliability and complexity. Motorola's MXP Multi-service Packet Transport Platform combines the advantages of star and full mesh technologies giving OEMs flexibility to use the topology most suited for various network applications and services.

In the MXP architecture, all the slots follow the core specification (PICMG 2.0) for power distribution and form factor and use the physical connection layer protection for hot swap (PICMG 2.1). The traditional CompactPCI bus has been eliminated, removing the extra complexity of dedicated system slots and PCI bridges. The slots are connected with three different networks: IPMI for shelf management; switched Ethernet; and the full mesh fabric.

The PICMG 2.9 standard defines the IPMI network, which is controlled by an alarm board resident in a dedicated alarm slot containing the IPMI Bus Management Controller. The PICMG 2.16 standard defines the dual-star switched Ethernet network. Each slot in the system includes two Ethernet interfaces, each capable of speeds up to 1Gb/s, routed to one of two dedicated switch slots. Ethernet traffic injected onto these

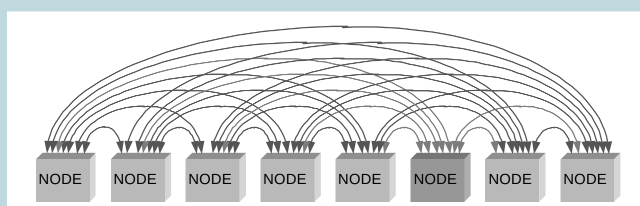


Figure 2: Mesh Topologies

Mesh Topologies are a superset of star topologies and also use 'point to point' connections. As networks add interconnects to eliminate 'dead branches' in a star topology, they reach a point where all nodes have connections to all other nodes. At this point, the hierarchy disappears. Each node can be an endpoint, a router or both. This figure illustrates how a node can act as a star point for all other nodes in the system.

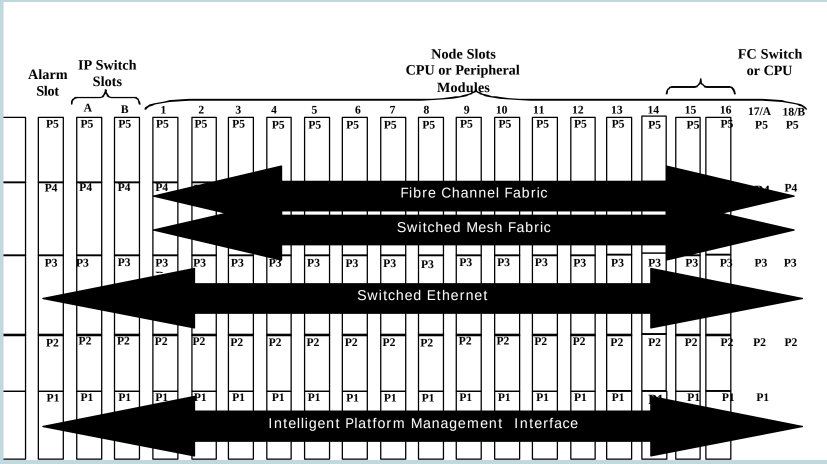


Figure 3: MXP MESH Architecture

The MXP multi-service architecture takes advantage of the mesh topology to offer a more resilient solution that needs no dependence on a central resource. The mesh architecture, which is being submitted to PICMG for consideration as an open industry standard, enables a more scalable solution than that presented merely by a star network. The backplane architecture is depicted here.

interfaces can be switched to any other slot, or out external interfaces on the switch boards.

The third infrastructure is a high-speed mesh data fabric that provides connectivity for every slot to every other slot in a 17 x 18 way interconnect. These connections, implemented with a four-wire interface capable of speeds up to 2Gb/s, are ideal for high-bandwidth bearer data applications. Because each interface is a point-to-point connection, they can be used independently of each another, making possible heterogeneous architectures supporting a variety of protocols.

Offering this mesh fabric technology to the industry as a candidate for an open standard should also ensure a full spectrum of boards will be available for a variety of other applications and interfaces. OEMs could also choose to implement their own interfaces for custom applications and product differentiation.

Motorola provides a distributed, flexible storage mechanism by implementing a dual-star Fibre Channel network topology, by dedicating two nodes in the mesh as hub slots for Fibre Channel aggregation modules.

Fibre Channel offers lower overhead, strict network determinism and higher throughput for networking and data distribution. In addition, the Fibre Channel network can connect CPUs with external HA Storage systems. A single HA Storage system can support multiple chassis. For systems with smaller storage needs, the MXP architecture supports plug-in disk modules. They are connected to the same networks as the CPUs and are served by the same Fibre Channel aggregation boards.

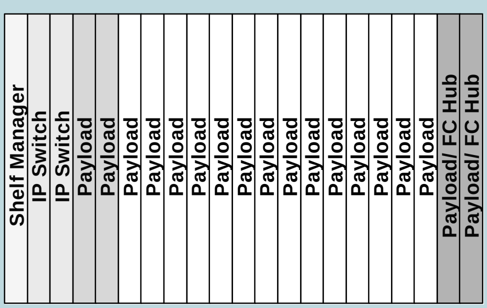


Figure 4: Flexible Chassis Configurations

The MXP topology can be applied to any chassis configuration. In a 21-slot configuration targeted for high availability applications, the system consists of an alarm slot, two fabric switches and 18 slots for task processors, network processors or storage elements. All 18 payload slots can be used for payload resources. If the Fibre Channel network is needed, two of the slots are used for the Fibre Channel aggregation hubs. The processors and disks interface to two predefined channels in the mesh.

4.0 Application Examples

The carrier-grade, high availability MXP series offers a flexible platform that can address next-generation applications such as SS7 gateways, media gateways, voice over IP (VoIP) gateways, media gateway controllers, edge routers, soft switches and access gateways. The MXP series can be scaled up or down for performance and throughput depending on the application and number of users. These options make the platform suitable for applications built at the edge of the network involving both control and bearer plane traffic. MXP support of high availability storage area networks (HA SAN) and distributed Fibre Channel storage also enables the MXP to support storage-and server-based applications including home location registers (HLR), billing servers and feature servers.

OEMs can configure the MXP with powerful combinations of distributed task processors, network processors, digital signal processors or storage elements to address many different applications and provide common development and deployment solutions.

5.0 Conclusion: Satisfying Solution to Manage Network Evolution

Highly flexible, multi-service architectures are strategic levers for reusing and driving down development and deployment costs in the telecommunications industry. Open standards and use of off-the-shelf standard products enable OEMs to more quickly develop applications that can leverage a multitude of third-party content and software. A single platform that achieves the highest levels of performance while also being flexible enough to be easily configured for a variety of applications anywhere in the network can help to ensure OEMs are well equipped to meet the needs of a changing marketplace. The packet transport platforms offer the necessary open architectures, speed and flexibility requirements to satisfy the needs of today's network while also providing the foundation to evolve into next-generation solutions.

About the author

Robert G. Pettigrew is Canadian Engineering Manager with Motorola Computer Group (MCG), and is responsible for ensuring the requirements of Canadian customers are reflected through innovative product design. To a large degree, Mr. Pettigrew's role involves managing partnerships with original equipment manufacturers (OEMs) such as Nortel, Newbridge, and Glenayre that reduce development time and result in breakthrough products for the telecommunications sector. Mr. Pettigrew manages teams of engineers across Canada who ensure OEMs in the telecommunications sector succeed in the intensely competitive global telecom market.

IEEE Canada Awards

2001 IEEE Meritorious Engineering Award

Shoaib A. Khan

Shoaib Khan was born in Jaunpur, India on May 4, 1936. He received a B.Sc. in Electrical Engineering from Benaras Hindu University, in Varanasi, India, in 1957.

Shoaib worked from 1957 to 1965 in India with Kaiser Engineers and M.N. Dastur & Co. His experience included engineering, construction and operation of steel, aluminum and power plants. He moved to Canada in 1965.

Shoaib has over forty years of experience in power systems engineering, application, and protective relaying for power (hydro, thermal, nuclear), pulp & paper, mining & metals, and chemical plants in N. America and overseas. He has worked with Bechtel Corp., SNC Lavalin, and Sandwell as a specialist in Power Systems and Protection. With Sandwell EPC Inc., he currently holds the position of a Specialist in Power Systems and Protection. He is also engaged in organizing, developing, and teaching courses in power systems and protection. He has authored numerous technical papers on power systems, applications engineering and protection, some of which have been published in IAS/PES transactions and Pulp & Paper Canada.

Shoaib is a senior member of IEEE, a registered engineer in Quebec and Ontario. He is also an active member of IEEE/IAS - PPIC PDS subcommittee. He is a recipient of the IEEE Centennial and Third Millennium Medals for achievements in education.

Shoaib has been active with IEEE Education Committee, Montreal Section for over thirty years and was Committee Chairman from 1974 to 1994. Shoaib was also an Auxiliary Professor with the Department of Electrical Engineering and a guest lecturer with the Department of Chemical Engineering at McGill University, Montreal.

Shoaib and his wife Shamim have three children, Sheema, Sheeba and Shakeeb. They also have two grandchildren, Sara and Zeyad.

IEEE REGIONAL ACTIVITIES BOARD ACHIEVEMENT AWARD 2001 - sponsored by IEEE Canada to

Vijay K. Sood (SM'IEEE), - Researcher,
Hydro-Quebec (IREQ), Varennes, QC

"For sustained outstanding contributions and service to Region 7 (IEEE Canada) by publishing and promoting the *IEEE Canadian Review* as a national journal for Region 7 members."

IEEE HARADEN PRATT AWARD 2002 - sponsored by the IEEE Foundation to:

Robert T.H. Alden (SM'IEEE) - Professor,
Department of Electrical & Computer Engineering,
McMaster University, Hamilton, ON

"For outstanding and sustained leadership in many areas of the IEEE especially in the use of electronic communication."

IEEE GRADUATE TEACHING AWARD 2002 - sponsored by the IEEE Foundation to:

Vijay K. Bhargava (F'IEEE) - Professor,
Department of Electrical and Computer Engineering,
University of Victoria, Victoria, BC

"For excellence in graduate teaching, curriculum development, and inspirational research guidance of graduate students in the area of wireless communications."

LIFE MEMBER CHAPTER FORMATION

From an initial start of a Life Member Chapter in Region 7 in May this year, it was decided at the Fall meeting in September, 2001 in Fredericton to expand to three chapters: Western, Central and Eastern Canada. Each Chapter is to include all the Sections in each Council.

An executive to co-ordinate the life member activities in R7 will have:

- Chair and Chair of Central Canada LM Chapter - Ron Potts
- Vice Chair & Chair of Western Canada LM Chapter - Mohindar Sachdev
- Secretary/Treasurer and Chair of Eastern Canada LM Chapter - Wally Read
- R7 Director - Dave Kemp, and
- EIC Life Member liaison - Len Bateman

The first activity of the Chapters will be to update and maintain a Life Member register with email, mailing address information in order to establish contact with all Life Members.

Currently there are over 1000 Life Members in R7 covering Member, Senior Member and Fellow grades. To qualify for life membership, the number of years of IEEE membership plus age must equal 100. IEEE guidelines for LM Chapters require at least 6 volunteer representatives to form a chapter and to meet at least twice a year. We now have volunteer representatives from Toronto, Hamilton, Kitchener-Waterloo and London Sections in Central Canada, with Winnipeg Section in Western Canada and Ottawa Section in Eastern Canada represented.

LM Chapter Chairs will attend future Section meetings to outline the Life Member Chapter objectives.

For further information, contact:

Ron Potts,

Life Member Chapter Co-ordinator for R7.

Email: potts@caninet.com.

Region 7 Director Report, Fall 2001

by Celia Desmond
IEEE Canada, Toronto, ON

For a number of years the Region has provided leading edge electronic services to our volunteers and members. A local company has managed our facilities, equipment and content. This year it was decided that we should relocate our services to Piscataway. The Board was to vote a motion of thanks to Jacek Chrostowski, to thank him for his vision and leadership in setting up Regional services which were at the leading edge of technology world-wide, and also to thank Hanna for her tireless efforts and contributions over the years. The move is currently underway, with plans for completion by year end. Meanwhile new service potentials have continued to appear. The Region site will be linked to two career databases:

- One is the IEEE database, which currently has mainly US postings, but their intention is to expand internationally.
- The other in a Canadian site, which has been joined by the organizations belonging to the Engineering Institute of Canada. It is provided by Brainhunter, and promises some small revenues to IEEE Canada along with the job potentials for our members. Also under investigation is the electronic distribution of our newsletter, already underway to those members we have email id's for, and possible electronic publication of our other publications in the near future.

A Canada-wide Life Members Chapter of IEEE Canada was established, and this fall the Region is working on splitting the chapter into three, one in each of our Councils. We hope to see more life members out to local meetings as a result, and also to be able to offer support to the Sections from the life members (see also the item on page 8).

The Canadian Journal ran into a small snag, which has been resolved. As a result of the budget restructures at IEEE, a pay-by-the-drink model was adopted for services provided by staff. Their staff has had some involvement with the fulfilment of the Journal orders. However, our editor, Om Malik, already did much of the work. The charge IEEE assessed to us for this item was far above the cost of doing the work internally, so for the moment Om has taken over the total fulfilment. Cathie Lowell, of the Region office, may assist future editors as well.

Another item, which has been addressed this year, is that of IEEE staff signatures on all bank account signature cards. All section, conferences, chapters or other units which have a bank account must get a staff signature on the card, to meet IEEE audit requirements. This has proved to be somewhat of a challenge due to the reluctance of the banks to send original signature cards out of the country. However, we are progressing with this to meet the IEEE auditor requirements. All account owners are currently either in compliance or actively working in this direction.

Two people have been trained to give the IEEE seminars on Leadership and Project Management.The sessions have already been given three times, and we are planning to give these presentations in as many areas as possible in the future, hopefully with more trainers trained as well.

Celia Desmond was president of IEEE Canada for the two-year term 2000-01, and is now past-director of Region 7 (IEEE Canada). She can be contacted at c.desmond@ieee.org

Summary of IEEE Meetings Attended in 2001 by IEEE Canada President

Conference Calls:

Excom:

February 5	July 3	April 12	September 7
May 9	October 19		

Nominations:	February 22	September 10

Date	Meeting	Location
Jan.13-15	RAB Strategic Planning	Newark
Jan.20-21	Leadership/PM Train the Trainer	Atlanta
Jan.26-28	RARAC	Fort Lauderdale
Feb.7-11	Comsoc Retreat	Cancun
Feb.13-18	IEEE Organizational Units	Albuquerque
Mar.3-4	EIC	Ottawa
Mar.9-11	Board of Directors	Phoenix
Apr.19-21	Comsoc OpCom	Salt Lake
Apr.22-25	Infocom	Anchorage
May 5-6	RAB Directors	Philadelphia
May 11-14	Region 7 & Excom	Toronto
May 14	Audit Committee	New Jersey
May 22	Comsoc	New York
May 29	Quebec Section	Quebec
June 8-9	EIC	Kingston
June-9-16	ICC/Comsoc BoG/RCCC	Helsinki, Finland
June 20-24	IEEE OU Series	Newark
July 11-15	BOD	Beijing
Sept. 29	Student Workshop	Calgary
Oct. 3-4	ComSoc Opcom NY	New York
Oct.13-14	RAB SPC	San Diego
Oct.19-21	Region 7 Mtg	Fredericton
Oct.27	Women in Science Convention	Calgary
Nov.3	EIC Mtg	Ottawa
Nov. 14-18	BOD Series	Mexico City
Nov.22	AGM, Northern Canada Section	Edmonton
Nov.25-29	ComSoc BOG	San Antonio
Dec. 7-9	R10 Excom	Cairnes, Australia
Dec 18	Halifax Section Visit	Halifax

Securing Your Network: Protecting Valuable Corporate and Intellectual Property in an e-nabled World

by Ajay K. Sood,
Nokia Internet Communications, Toronto, ON

Abstract

This document provides an introduction to the basic components of an Internet perimeter defense system. Security technologies such as Firewalls and Intrusion Detection Systems (IDS) are discussed, as well as the basic concepts of network security as well as the premise of risk assessment. A case study pertaining to the proliferation of the Code Red virus is detailed, as well as a brief look at future security technologies.

Sommaire

Ce document sert comme introduction aux composantes des systèmes de sécurité Internet. La discussion se centre autour des pare-feux (firewalls), ainsi que des systèmes de détection d'intrusion. En sus, les concepts fondamentaux par rapport a la securité informatique sont discutés. Finalement, une étude de l'epédimie informatique << Code Red >> est fournie, ainsi qu'un regard vers le futur de la sécurité informatique.

1.0 Introduction

The Internet has ceased to become an optional component to any company's business strategy. Rather, the Internet has risen to become an enabler for business, whether that business consists of effectuating commerce, business development, research and development, or other contemporary practices.

An emerging reality, however, is that there is a risk associated with this notion of integrating the Internet as part of one's business or research practices. Conventional as well as electronic media have been peppered with items recounting incidences of revenue losses, data theft, and more recently, 'cyber-terrorism', as politically minded hackers use their skills to make a statement.

2.0 The Role of Internet Security

The practice of Internet security is centered on the notion of risk mitigation, in that one can never be assured to the point of certitude that an Internet-enabled system is truly secured. Security consultants are frequently sought out in order to identify and classify information or assets at risk, enumerate these risks, and subsequently make recommendations to mitigate them.

The tools of the trade are numerous. Forensic tools such as scanners can be used for network discovery, and vulnerability identification, whereas customized data audits can be used to verify the security and integrity of data stores. The dichotomy of the situation is that these, and other tools are not only used by security professionals to obtain information, but also by hackers (those who make it their business to misuse, misappropriate, or corrupt information which is not theirs). What these two factions have in common is that they deal in acquiring information - it's what they do with it, which differentiates them.

The lesson then becomes, that the science of Internet security deals with the mitigation of the risk of having critical information compromised, and thus, having the cyclical processes in place to review, refine, and improve the status quo, so that critical assets and information are protected. That having been said, what are the key components of a secure network infrastructure?

3.0 Firewalls

Firewalls are a typical starting point for enforcing security policies on Internet Protocol (IP) networks. A firewall is a network traffic governor, which inspects and filters network traffic, which is incident on any one of its interfaces, much like a router with a security subsystem. The role of a firewall is to stratify a network infrastructure into domains of trust, by delineating zones, and regulating communication between them. The behaviour of a firewall should be a representation of the security policy, which it supports.

Practically, contemporary firewalls are so much more. Over and above merely filtering an IP packet based upon its OSI layer 3 parameters (source IP, destination IP, source and service ports), today's firewalls do not even live up to that name if there is not some form of state-derived inspection performed on these packet streams, which is to say that packet filtering is not enough. Packet inspection algorithms, which make decisions on whether or not to accept a given packet stream based upon previous traffic states, are now the norm.

A simple example is the establishing of a client-server TCP session through a firewall (the most common - like HTTP, FTP and SMTP), which takes place in three phases, each consisting of a single packet (Figure 1):

- The client SYN packet, which constitutes a client's proposal for communication,
- The SYN/ACK, which signals the server's readiness to transmit, and
- The client ACK, which signifies completion of session establishment - please continue.

Typical packet filtering technology (present on conventional routers, for example) would have to permit all three of the aforementioned messages in any given order, for this transaction to work, whereas a state-sensitive firewall would exercise more sophistication in this matter:

- The firewall would be configured only to accept a connection (SYN-request) to a given server (WWW server, for example), on a given service (in this case, WWW - port 80), from an arbitrary Internet client with IP address, say a.b.c.d,
- Once a qualifying SYN is received, the server would then be permitted to reply with its SYN/ACK,
- The firewall would record these occurrences in a state table, which would anticipate an ACK packet from a.b.c.d. Only this packet would be accepted, and no other packet from any other machine on the Internet would qualify,
- Once the ACK is received, the firewall will open a data channel between that particular client and the server, and record this instance in its state table,
- Exceptional cases (like a SYN without a SYN/ACK, or an order reversal) would not be passed, and
- Connection requests (SYNs) for any other service other than the ones prescribed (in this case WWW) would be blocked at the firewall.

4.0 Completing the Security Picture

So, while firewalls guarantee that only permitted IP addresses access private servers on the specified services, what is to stop the use of the inherent weaknesses in the accepted protocol? Recent events surround-

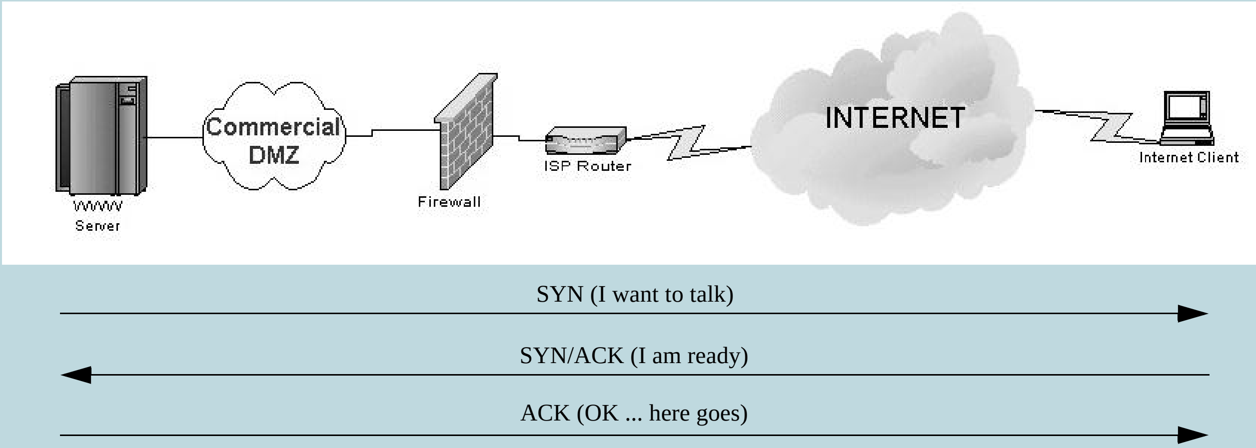


Figure 1 – The Client, the Firewall, and the Server

ing the proliferation of the Code Red worm/virus have provided a great example of firewalls being a necessary component of, but not sufficient as a complete security solution.

Code Red exploited a vulnerability in Microsoft's IIS Web server, which runs on a large number of Internet web servers. Even though a majority of these web servers were protected by firewalls limiting connections to the WWW port (port 80), the worm was able to utilize the open port to infect the host and propagate itself. The firewall never had a chance!

Enter intrusion detection systems (IDS) - a technology which, in real time, examines the traffic flow of data across a given network segment. An IDS sits on the network, and monitors for attack streams, which may be flowing on the segment, but is not an active member of the data path. Rather, an IDS passively listens and reacts in a variety of ways to attacks that it detects. Typical reactions are alerts sent by email, SNMP, or pager, and can even go as far as reconfiguring the nearest firewall to reconfigure itself to stop the attackers, or send port resets to the attacking machine to close the offending connections.

So in the case of Code Red, although the firewall could, in theory, allow the worm to infect the web server, the IDS would sense the attack pattern in the transmitted data stream, and take the prescribed action, neutralizing the threat by sending a port reset, canceling the connection, or instructing the firewall to close down all traffic from the attacking IP address for a finite or infinite period of time. In either case, some form of logging and alerting would also be a mandatory component of the IDS strategy (Figure 2).

Therefore, it can be said that a complete perimeter defense system could contain a variety of components, each complementing the overall security goals of the enterprise, with the firewall acting as the nucleus of this system. Conversely, encryption techniques for authenticating and privatizing communications can be employed in order to set up what is

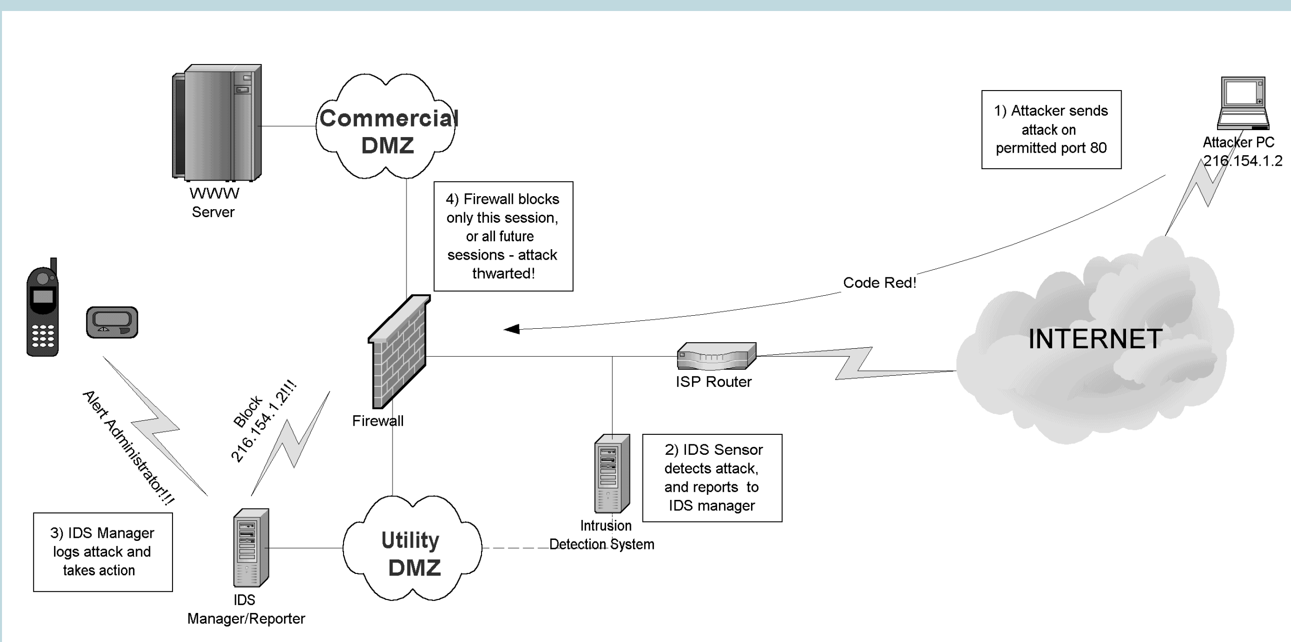


Figure 2 – Firewall with Intrusion Detection System

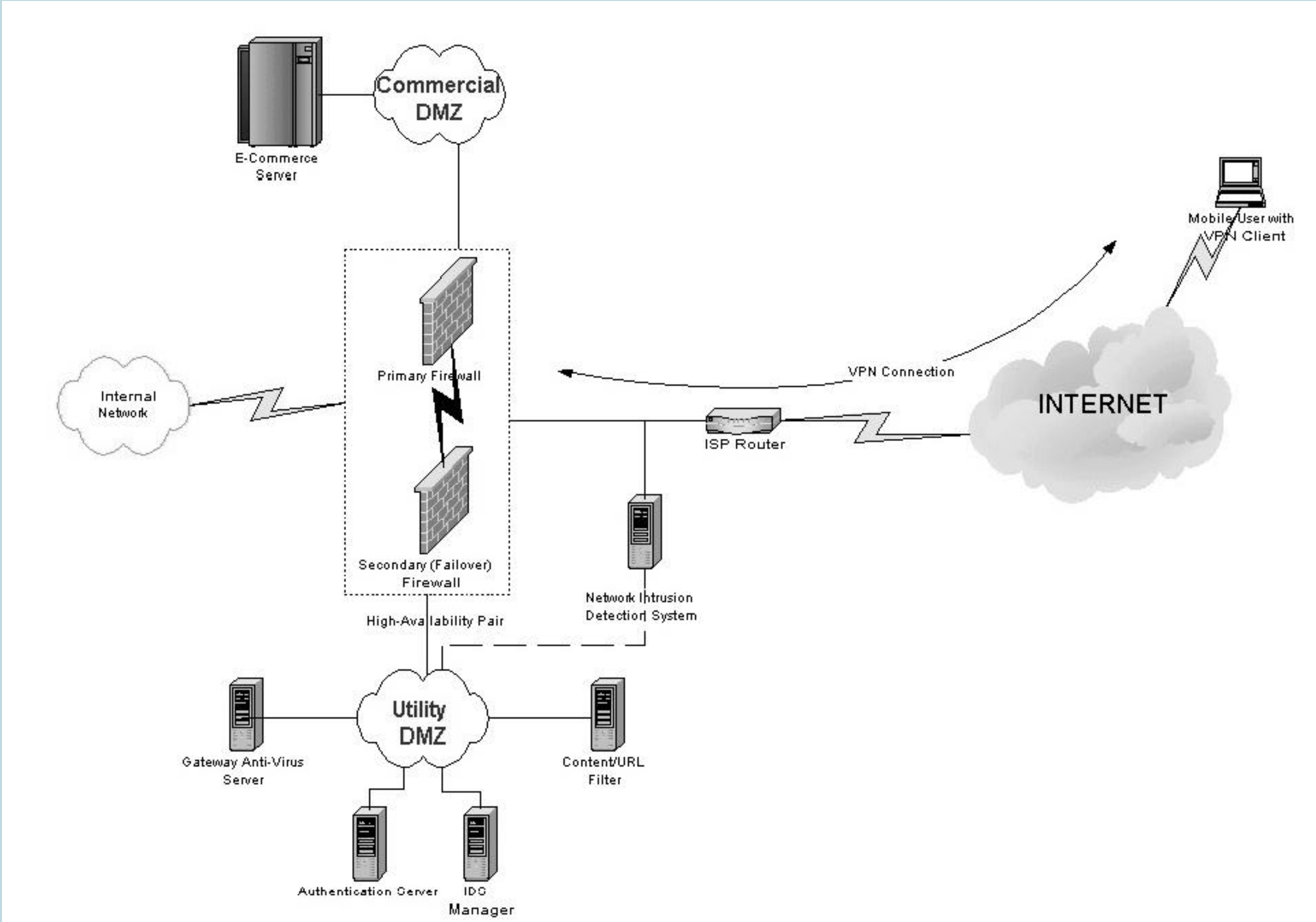


Figure 3 – Conceptual Security Infrastructure

known as a VPN (Virtual Private Network), connecting businesses across the Internet.

Additional technologies such as anti-virus gateways, or content filtering can be employed to inspect and control malicious content entering and exiting the enterprise. Authentication and non-repudiation represents again another exciting realm of security technology, with identifying technologies such as digital signatures, dual-factor authentication, and Public Key Infrastructures (PKI) all playing a role in certifying user identities (Figure 3).

5.0 Conclusion

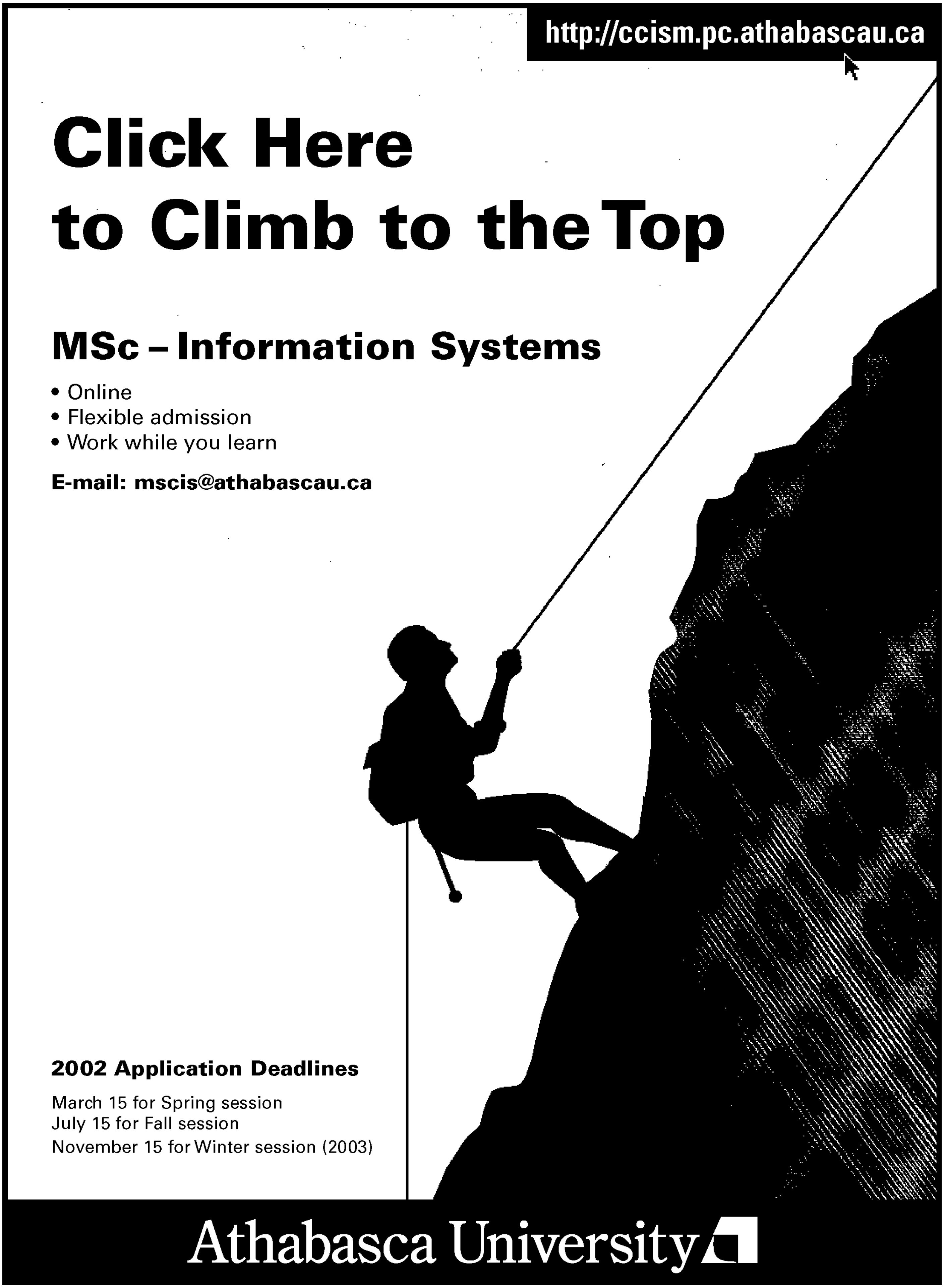
In closing, it is important to note that information security should be regarded as an iterative process, with a cyclical nature. The Internet is an evolving landscape, and technology, as a whole, must adjust and scale accordingly. The advent of new technologies, network protocols, and practices will result in new ways of doing business. Emerging technologies such as mobile-IP will further enable a mobile Internet infrastructure, as we rush towards a mobile information society, in which a cellular handset/terminal will have a real IP address, a firewall and VPN client of its own, as well as a host of protocols, applications, and vulnerabilities.

6.0 List of Acronyms

DMZ	- De-Militarized Zone
FTP	- File Transfer Protocol
HTTP	- Hyper Text Transfer Protocol
IDS	- Intrusion Detection Systems
IP	- Internet Protocol
ISP	- Internet Service Provider
OSI	- Open Systems Integration
PKI	- Public Key Infrastructures
SMTP	- Simple Mail Transfer Protocol
SNMP	- Simple Network Management Protocol
TCP	- Transmission Control Protocol
VPN	- Virtual Private Network
WWW	- World Wide Web

About the author

Ajay Sood is a Sales/Systems Engineer at Nokia Internet Communications, and works with a variety of security technologies, such as firewalls, intrusion detection systems, virtual private Networks (VPNs), as well as authentication and anti-virus products. He has also served as a network security, design, and vulnerability assessment consultant for many organizations. Ajay holds a B. Eng. degree in Electrical/Computer Engineering from Concordia University. He can be reached at Ajay.Sood@Nokia.com


http://ccism.pc.athabascau.ca
Click Here
to Climb to the Top
MSc – Information Systems
• Online
• Flexible admission
• Work while you learn
E-mail: mscis@athabascau.ca
2002 Application Deadlines
March 15 for Spring session
July 15 for Fall session
November 15 for Winter session (2003)
Athabasca University

Mainframe Computing Architecture Re-Invented – Open for Business

by Jim Bowman
GE Capital IT Solutions, Calgary, AB

Abstract

The IT industry has re-invented itself several times over the past 20 years, as a result of major changes in computer architecture. We have witnessed the era of mainframe computing, PC's for individuals, midrange clusters for departmental systems, standalone systems for small business, the internet, explosive growth in storage systems and a new growing class of high performance servers. As each shift was introduced to the marketplace, the business community reacted with changing business models. The first wave of dot.coms and e-business is today analyzing the more secure, high performance architectures similar to centralized mainframes. In many ways, we have come full circle.

Sommaire

L'industrie TI a dû se renouveler à plusieurs reprises depuis les 20 dernières années étant donnés les changements majeurs de l'architecture des ordinateurs. On a observé l'évolution des époques de la programmation centrale « mainframe », des ordinateurs PC personnels, des « clusters » mi-niveau pour les systèmes de département, les systèmes autonomes pour la petite entreprise, l'internet, la croissance explosive des systèmes de stockage et la croissance nouvelle des serveurs à haute performance. Au fur à mesure de l'avènement de ces nouvelles technologies, le milieu des affaires a réagi en ajustant son mode de fonctionnement. La première vague des entreprises « dot.coms » et « e-business » analyse maintenant les architectures les plus sécuritaires et performantes similaires au systèmes « mainframe » centralisés. De plusieurs façon, on peut conclure que le cycle d'évolution se referme.

Over the past 20 years, the computer industry has re-invented itself several times. In the late 1970's most business in North America was using a form of mainframe computer architecture which was created by IBM engineers in the 1960's and refined by technology inventors including Honeywell, Burroughs, Digital Equipment, Hitachi Data Systems, and others. These systems used simple operating systems to run a single version of an application to handle mostly accounting applications.

As new technology for chip design was patented, developed for mass manufacturing, it was packaged in small computers for use by small business. This provided an explosive opportunity for more people to become introduced to the benefits of automated accounting, which saved people time and increased the accuracy of information. During the early 1980's, the industry thrived with the creation of new business applications for use in municipal governments, hospitals, classroom education, building construction, and engineering.

The pace of new technology increased again as the Personal Computer model was invented by Apple Computers and IBM. With Microsoft software for Operating Systems, Spreadsheets and Word Processing, individuals could use a computer for daily information. People in all walks of life began creating applications to simplify cooking, writing, homework and any task imaginable.

With the use of 3 different methods of computing: mainframe, distributed and personal systems, many organizations changed their methods of business to achieve more efficiencies, growth and profit. This was also fueled by the business trend to decentralize operations, outsource processing and empower people to run their own piece of the organization.

In the late 1980's, the computer industry created another major advancement with the introduction of UNIX. The concept was to allow application developers a common operating system with which to deliver applications. Using the University of Berkeley kernel, several manufacturer's including SUN, Digital, IBM, HP, and SCO packaged additional support function into this kernel to provide higher levels of reliability, availability and security. During the 1990's, this evolved into common, but unique operating systems that minimized the ability for applications to become portable across different hardware vendors. Many would argue that UNIX has failed to deliver the true heterogeneous model it was intended for. The newest attempt is seen in the LINUX operating system.

The next major breakthrough in computing has been the development of the Internet as a delivery mechanism for computing. As we have seen, the Internet has changed everything, and is evolving rapidly as the main architecture for global communications.

One of the major impacts of Internet usage has been the massive amount of information that is being gathered and created, i.e. DNA and Genome mapping and stored on computers. Industry estimates have stated that the total amount of information in the world will double every 2-3 years. The effect of this is being seen in the business world with introductions of Enterprise Resource Management (ERP), Supply Chain Management (SCM), Customer Relationship Management (CRM), Business Intelligence (BI), E-Commerce and many other major applications that are connecting suppliers and customers together.

The cumulative effect of this explosion of computing demand has caused business and government organizations to begin thinking about centralization of information technology. IT managers are struggling with support, costs are increasing and a general feeling that IT is falling behind, resulting in potential disasters such as the Year 2000 situation and more recently, Sept. 11 in New York.

There are several bright spots in the technology sector which are just now being refined and delivered to the marketplace. These include Copper Chip Technology, Silicon on Insulator (SOI) and Logical Partitioning (LPAR). Each of these technologies offers substantial potential in creating the computing architecture that is required to manage the demand for computing.

IBM has lead the way with the patents and manufacturing development of Copper and SOI. In 1997, fulfilling a dream of several decades, IBM introduced a technology that allows chipmakers to use copper wires, rather than the traditional aluminum interconnects, to link transistors in chips.

Every chip has a base layer of transistors, with layers of wiring stacked above to connect the transistors to each other and, ultimately, to the rest of the computer. The transistors as the first level of a chip are a complex construction of silicon, metal, and impurities precisely located to create the millions of minuscule on-or-off switches that make up the brains of a microprocessor. Aluminum has long been the conductor of choice, but it will soon reach technological and physical limits of existing technology. Pushing electrons through smaller and smaller conduits becomes harder to do – aluminum just isn't fast enough for these new, smaller sizes.

Scientists had seen this problem coming for years and tried to find a way to replace aluminum with the three metals that conduct electricity better: copper, silver, or gold. Of course, if that was simple, it would have been done a long time ago. None of those metals is as easy to work with as aluminum in decreasing amounts. Any new material presents fresh challenges, and reliably filling submicron channels is a bit like filling the holes of a golf course from an airplane.

IBM had to develop a diffusion barrier that could buffer silicon wafers along with the copper. The company has now announced the first commercially viable implementation of Silicon-on-Wafer (SOI) and the ability to apply it in building fully functional microprocessors. SOI refers to the process of implanting oxygen into a silicon wafer to create an insulating layer and using an annealing process until a thin layer of SOI is formed. The transistors are then built on top of this thin layer. SOI technology improves performance over bulk CMOS by 25-35%. It also brings power usage advantages of 1.7 to 3 times, creates higher performance and reliability per processor.

In the past, IBM would spend billions of dollars of R&D, create their own patents and determine what inventions to manufacture based on market dynamics. In 1995, this changed. Today, IBM creates it's own products and also sells the patented technology to it's competitors like, Dell, EMC and Compaq, who use this technology in their products. The result is that the larger computer marketplace is benefiting from these technologies. This allows IT customers to actively plan for systems consolidation of servers and storage that address the processing requirements, reduce IT budgets and improve utilization of scarce human resources.

These technologies were joined by many other advancements in programming, disk storage, software, telecommunications and operations over the past few years. I believe that we are set to achieve a significant improvement in computer performance and will outdistance the mainframe architectures of the past. Mainframes have traditionally been the most powerful, largest capacity and most reliable systems for mission critical computing.

The third major advancement lies in the creation of Logical Partitioning (LPAR) for the new architectures based on copper and SOI.

Why Partition:

The mainframe world has been able to implement partitioning for many years using MVS and Virtual Machine (VM) concepts. These operating systems have not been able to keep up with Windows or open UNIX or the exciting Linux environments. Today, we see a new class of system partitioning available for open systems.

From a marketplace perspective, there is a demand for high end systems to provide greater flexibility, in particular, the ability to subdivide them into smaller partitions that are capable of running a version of the operating system or a specific set of applications.

The main reasons for partitioning a large system are as follows:

- Server Consolidation: Running multiple applications that previously resided on separate physical systems and provide benefits of lower costs, space savings and reduced operation management,
- Production / Test Environments: Partitioning means setting aside a portion of the system resources to be used for testing new versions of applications while the production system continues to run. This avoids buying computers for test applications and provides higher confidence that the test system will migrate to production,
- Increased hardware utilization: Partitioning is a means of achieving better hardware utilization when software does not scale well across large numbers of processors. In such circumstances, running multiple instances of an application on separate smaller partitions can provide better throughput than running a single large instance of an application,
- Application Isolation: Running applications in separate partitions ensure that they cannot interfere with one another in the event of a software failure in one partition. Also, applications are prevented from consuming excessive amounts of resources, which could starve other applications of the resources that they require, and
- Increased flexibility of resource allocation: A workload that has resource requirements that change over a period of time can be managed more easily within a partition that can be altered to meet the varying demands of the workload.

There are several different ways in which server resources may be partitioned. Some vendors distinguish between hard and soft partitions, while others distinguish between physical partitioning, logical partitioning and software resource management.

Physical Partitioning: PPAR - PPAR is used to describe a method of dividing an SMP server into smaller processing units. These units can be considered small servers. It is called PPAR due to the fact that the partitions have to conform to the physical boundaries of the building blocks used to construct the server.

Logical Partitioning: LPAR – LPAR differs from PPAR in the way resources are grouped to form a partition. Instead of grouping using physical building blocks, LPAR adds more flexibility and freedom to select components from the entire pool of available system resources. LPAR works from within a single memory coherence domain, so it can be used within a simple SMP with no single building block structure. All the operating system images run within the same memory map, but are protected from each other by special address access control mechanisms in the hardware, and special firmware added to support the operating system. Several key advantages can be achieved:

- Resource re-allocation for performance,
- Configuration flexibility,
- Full Isolation protection, and
- Fault Isolation.

Resource Management: Many operating systems provide resource management capabilities that can be applied even when the operating system is running within a physical or logical partition. This provides more control over the allocation of computational resources (CPU, memory, I/O) to applications. The allocation of resources can be dictated by different classification rules (users, application, and names). In this way, workloads can be prevented from consuming all the resources. Also, it provides a mechanism to balance the use of system resources optimally. By grouping applications by resource usage behavior, the workloads can be managed together to maximize the utilization of the server.

Now that we have a new class of chip technology available and a good choice of partitioning from the major vendors, it is re-assuring to also see major improvements in the hardware tools for problem management. For years, the mainframe class computers where the only ones which could self diagnose their own problems, providing online reporting back to support staff and even fix themselves. It is exciting to see this same functionality has been brought down to midrange open systems.

Major vendors have introduced concepts of Self-Configuration, Self-Protection, Self-Healing and Self-Optimizing. These sound more like medical terms that computer systems terms, but the concepts are similar. New servers have millions of lines of software code built into the hardware that provides a level of intelligence. Recent functionality in self healing systems include:

- Chipkill ECC memory,
- Cache de-allocation,
- Processor de-allocation,
- Soft memory scrubbing,
- First Failure Data Capture, and
- Redundant bit steering.

When you add all this up, it looks like a new class of mainframe architecture has arrived. Now, the IT staff can seriously examine alternatives for consolidating business applications onto smaller, cheaper, powerful servers, which are easier to manage.

We have witnessed an increased pace of hardware and software announcements being delivered every 12-18 months. It is hard to imagine how much faster the industry will be able to invent new technology for the market, but we will certainly find out.

Stay tuned.

About the author

Jim Bowman began his career with a Marketing / Finance Degree from Northeastern University in Boston. During a decade with IBM, Jim's experience covered sales, marketing, management, training and education, and channel management. Building on a technical background, Jim's focus changed to ERP software with JDA Software in retail and distribution, Labor Management and Shop Floor Data Collection with Kronos and Wireless Integration for SCM. Jim's current role with GE Capital IT Solutions focuses on Infrastructure Consulting for large accounts and e-business implementations. Jim has a fabulous wife, 4 children and enjoys an exciting life in Calgary, Canada.

Letters to the Managing Editor / *Lettres envoyéers au rédacteur en chef*

IT Mania

Five cannibals get appointed as programmers in an IT company. During the welcoming ceremony the boss says: “You're all part of our team now. You can earn good money here, and you can go to the company canteen for something to eat. So don't trouble the other employees”. The cannibals promise not to trouble the other employees.

Four weeks later the boss returns and says: “You're all working very hard, and I'm very satisfied with all of you. One of our cleaners has disappeared, however. Do any of you know what happened to her?” The cannibals disavow all knowledge of the missing cleaner.

After the boss has left, the leader of the cannibals says to the others: “Which of you idiots ate the cleaner?” A hand raises hesitantly, to which the leader of the cannibals says: “You fool! For four weeks we've been eating Team Leaders, Managers, and Project Managers so no-one would notice anything, and you have to go and eat the cleaner!”

Bob McLoud

Markham, ON

Thought for the Day

A bus station is where .... a bus stops.
A train station is where .... a train stops.
On my desk, I have a work station where ....

what more can I say.

Anonymous

IEEE

Université du Québec
École de technologie supérieure

New IEEE Senior members

Johnny W. Wong	- Kitchener-Waterloo
Marvan Abboud	- Montreal
Gerard Dunphy	- Newfoundland-Labrador
Jose N. Amaral	- Northern Canada
Voicu Z. Groza	- Ottawa
Xavier P. V. Maldague	- Quebec
Vern L. Buccholz	- Vancouver
Veera R. Vinnakota	- Vancouver
Dale John Shpak	- Victoria

En réponse aux besoins de l’industrie, l’ÉTS présente son nouveau programme de baccalauréat en génie logiciel

Montréal, le 21 novembre 2001 – « Le nouveau baccalauréat en génie logiciel de l’École de technologie supérieure (ÉTS) constitue une voie privilégiée pour accéder à la profession naissante d’ingénieur logiciel ». C’est ce qu’a déclaré M. Michel Lavoie, directeur du programme, à l’occasion de l’inauguration du nouveau baccalauréat qui a eu lieu à l’ÉTS, le 24 octobre dernier.

Cet événement s’est déroulé dans le cadre des journées-conférences de l’École sur le génie logiciel, où l’on a notamment entendu des membres du conseil consultatif international du guide du Software Engineering Body of Knowledge (SWEBOK), un guide présentant le corpus des connaissances dans le domaine. Selon le directeur général de l’ÉTS, M. Robert L. Papineau, « La participation de ces sommités mondiales à l’événement constitue un gage de la reconnaissance du programme et de l’École, à laquelle sont d’ailleurs rattachés deux membres du conseil du guide SWEBOK. »

Le génie logiciel, c’est cette nouvelle profession qui intègre les principes de l’ingénierie à la conception de logiciels utilisés dans tous les domaines de l’ingénierie et plus spécifiquement dans les technologies de l’information. L’ingénieur logiciel est donc celui qui assure la cohérence et l’intégrité des informations à travers toutes les phases de réalisation d’un projet. L’ÉTS offre le seul programme de baccalauréat en génie entièrement composé de cours sur le développement, l’opération et la maintenance des logiciels. Comportant plusieurs mois de stages et nombre de travaux pratiques, ce programme unique a été conçu en réponse aux attentes des diplômés des cégeps et aux besoins exprimés par l’industrie.

Pour obtenir plus d’information sur le programme, contactez Michel Lavoie, mlavoie@etsmtl.ca

Connecting Continents

by Wally Read
IEEE Canada, St.John's, NF

Abstract

The author engages in a lighthearted discussion about the history of the migration of humankind on this planet and the difficulties associated with establishing and improving communications links between the migrants. Those captivated by the progress of our telecommunications technology in the 19th and 20th centuries will read about some of Canada's unique contributions and of its "unsung heros".

Sommaire

Les auteurs se sont engagés dans une discussion de fond sur l'histoire de la migration des humains sur cette planète et sur les difficultés associées à l'établissement des liens de communication entre les immigrants. Ceux qui sont captivés par le développement des technologies de télécommunication du 19 et 20e siècle pourront découvrir quelque unes des contributions canadiennes majeures ainsi que ses héros obscurs.

As many of you are aware, my career background has been with electric power utilities, or what I like to refer to as the "muscle" end of our electro-technologies. But, since my retirement I have become fascinated with the story of the migration of peoples on this planet and the role that communications played in establishing and maintaining contact between them.

Winston Churchill is purported to have once said "the further back one looks, the further forward one is able to see." In preparing this paper I have taken him at his word and consequently I have titled it "Connecting Continents". In its broadest interpretation, that means I have to cover 100 millenniums of history to tell the real story - no mean chore, even for an engineer.

It all began for us 100,000 years ago when the human race migrated out of Africa. Some tribes turned west, others east. After a few hundred generations, those who'd turned left reached the uncrossable Atlantic Ocean. But the descendants of those who turned right found a larger world at their feet, across Asia. Some crossed the narrow Bering Strait 16,000 years ago, spreading across North America. Some continued on to the Strait of Belle Isle 8,000 years later and then on to the island of Newfoundland. Once again the uncrossable Atlantic Ocean confronted humankind, this time having been reached from the west.

It was the Vikings, driven by ambition and a desire to claim new lands, who finally closed the formidable gap. Aboard sturdy ocean-going knarrs, without compass or astrolabe, they ventured farther and farther from mainland Europe, to the Orkneys, the Faeros, Iceland and Greenland. Then in the early summer of 1000 AD, Leif Ericson and his crew, left Greenland and sailed west for unknown lands. Months later Leif sailed ashore on the northern tip of Newfoundland, a vast area where the Viking visitors encountered the aboriginal people they called "Starlings". Here was the end of a 99,000-year voyage - descendants of those who turned east were met by the descendants of those who turned west. Humanity had come full circle.

The explorer instinct continued in the east but it was not until some 500 years later that the Atlantic Ocean was challenged again, this time by Christo Colombo and Giovanni Caboto and some say the Portuguese before them. Columbus and Cabot had a lot in common. Both were Italians, both went abroad to have their expeditions financed by foreign countries, and both their voyages terminated on islands, not on mainland North America. Although they are written up in the text books as discoverers of North America, that is a bit of a stretch because technically what they discovered were only the islands of Puerto Rico and Newfoundland.

I made a quick reference to a belief that Portuguese navigators may have preceded these two Italians by a few years, but there is no hard evidence on this. Typically, when hard facts do not exist we humans are not beyond inventing supporting stories.

One such story involves the naming of our country, Canada. The official version is that the name "Canada" is of aboriginal derivation but some say it was indeed the Portuguese that were responsible. It seems the driving force behind Portugal's early exploration ventures was to find a land more hospitable than their own. When they came upon my country they called it "ca" meaning "here" and "nada" meaning "nothing" - "here is nothing". So with that they made no claim and headed further south for warmer climes.

Why have I dwelt on this background of migration and exploration? Really it was to make the point that, just as the Atlantic Ocean was the barrier and challenge to the free movement of peoples in those years, so it would be for the transportation and communication links needed between the Old World and the New World in the future.

The roles of the sailing ships and later the ocean-going steamships have been well documented and for the next 350 years they remained the primary means for contact between the east and west. It was not until the last 150 years of this 100,000 year journey that we would see technological developments which would truly "connect continents" through communications by instantaneous electronic means. Many are the stories that surround these remarkable engineering achievements and many are the numbers of unsung heroes that contributed to their success. Let me just touch on a few of these.

With the invention of the telegraph in 1832 and subsequently the opening of the first telegraph system twelve years later, a new era of telecommunications had begun that brought all people of the world into contact. As telegraph lines sprung up in Europe and in North America, the uncrossable Atlantic reared its ugly head again. Visionaries on both sides were planning to meet this challenge.

On our side of the "big pond" a gentleman from Lancashire by the name of Frederick Newton Gisbourne, appeared on the scene. Gisbourne was taught mathematics and civil engineering by the local vicar in Broughton. At the early age of eighteen years he toured Australia, New Zealand, Mexico and Guatemala and ended up in Canada where he took up positions with telegraph companies while still in his twenties.

Gisbourne saw the commercial value of undersea communications cables connecting continents and set about the first steps of building the infrastructure needed on the North American side of the Atlantic. The initial plan was to intercept ocean-going vessels off the coast of Newfoundland and telegraph the news of Europe to New York two days in advance of its arrival by ship.

The proposal included constructing a 600-Km telegraph line across the island of Newfoundland, using carrier pigeons for the 170-Km sea crossing to mainland Canada and utilizing the existing circuits to New York. Difficult construction conditions forced a withdrawal of his financial backing and the plan was only salvaged by the intervention of Cyrus Field an American entrepreneur. The carrier pigeon proposal was replaced with an undersea cable and Field's company completed the project. This was the communications system that was in place when the Civil War broke out in the United States and thereby by hangs another tale.

When there was some question as to whether England was going to enter the war on the side of the South to protect its cotton supply, Parliament met, debated and decided it would not. That important news was dispatched by ship to the United States. Off of Newfoundland the canister containing the headlines was thrown overboard at Cape Race and picked up by the "Newsboat". However the telegraph operator was unable to transmit the message due to ice buildup on the lines.

Realizing the importance of the news he rode on horseback into St. John's and met with the Governor who immediately sent him to the next repeater station to try there. After another lengthy horseback and open boat ride he arrived at Rantem where he found the circuit solid all the way down to New York. The news got there Sunday night ready for the

Monday morning headlines and President Lincoln got at least a couple of good nights rest before the details arrived some two days later.

As for Gisbourne, he did not benefit from the vast enterprise which was established afterwards by the laying of the transatlantic cable and in some cases he was never given the recognition he deserved. Thank you, Frederick Newton Gisbourne and, on behalf of President Lincoln, a special thanks to the telegraph operator of Cape Race.

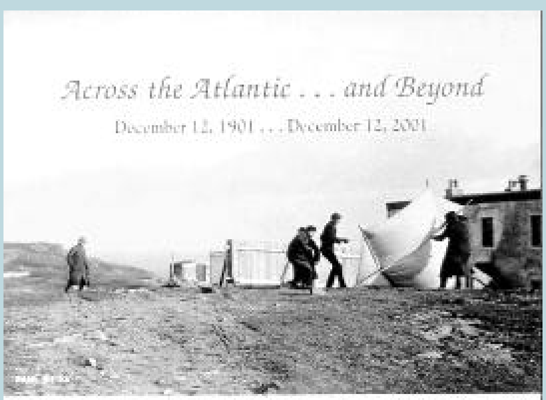
Space does not permit my repeating the tale of the various attempts to lay a communications cable across the Atlantic and the success of the Great Eastern in 1866 in doing just that. Nor is there a need for me to do so. It is well documented. I will tell you though, that a long overdue dedication of an IEEE Engineering Milestone took place in Valentia Bay in County Kerry, Ireland in 2000. The IEEE UKRI Section sponsored the event and it marked the 134th anniversary of the sailing of the Great Eastern with her precious cargo.

Nor does space permit mention the many wizards who worked in the field of voice communication over wires epitomized by that great Scot, Alexander Graham Bell who perfected his inventions in Canada and the United States towards the end of the 19th century. It is enough to say all of these events signaled a new era for us all. Just as the Vikings made people-contact early in the second millennium, just as further exploration and advances in sea transport maintained and improved that contact for the next 850 years, so did the transatlantic cable provide a fast communications link for peoples on either side of Ocean.

By 1900, the question was being asked whether we had achieved all that we wanted to in transatlantic communications? Could even greater accomplishments be envisaged?

Enter the wireless age and the magic of another Italian, Guglielmo Marconi who made history by transmitting the letter “S” in Morse code from Poldu, Cornwall, England to a receiving station on Signal Hill, overlooking St. John's Harbour in Newfoundland on December 12, 1901. Without question this was a startling discovery and a wonderful gift to humankind at the start of a new millennium.

However I want to talk about another one of those “unsung heroes” I spoke about earlier. His name was Reginald Aubrey Fessenden, a Canadian, who was working in the wireless communication field in those days. Stimulated by the work going on in wireless telegraphy he wanted to go one step beyond that and have voices and music carried over high frequency waves. Unable to obtain funding in Canada he went to work for the United States Weather Bureau where he was able to convince the powers that be to support his work.



Gugliemo Marconi raises an antenna on Signal Hill, St. John's NF, 1901.

On December 23, 1900, from his new laboratory at Cobb Island on the Potomac River, Fessenden was experimenting with Morse transmissions to a receiving station in Arlington, Virginia, some 50 miles away, where his assistant, Thiessen was located. He hooked up a microphone to his improved system and spoke into it the words “One, two, three, four. Is it snowing where you are Mr. Thiessen? If so telegraph back and let me know”. Thiessen replied by telegraph in Morse code that it was indeed snowing. In great excitement Fessenden wrote at his desk, “This afternoon here at Cobb Island, intelligible speech by electromagnetic waves has, for the first time in the world's history, been transmitted.” This was almost one year before Marconi's transatlantic signal was received in Newfoundland on December 12, 1901.

Obsessed with increasing the range of his long distance voice transmission he experimented successfully with messages from Brant Rock, just outside of Boston, Massachusetts and a receiving station in Armour in Scotland. The Atlantic Ocean had fallen victim to yet another challenger.

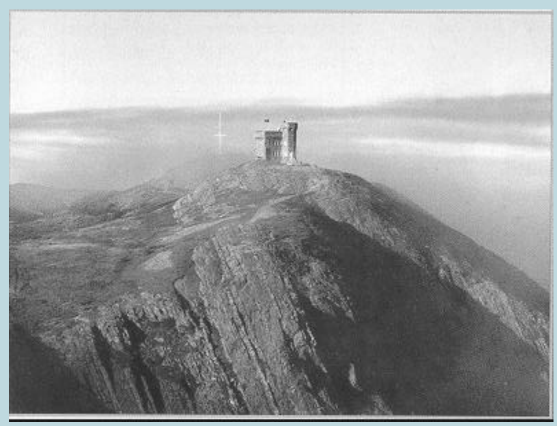
Perhaps Fessenden's most satisfying moment came on December 24, 1906 at 9pm when he orchestrated a broadcast to several ships at sea owned by the United Fruit Company. This company had installed wireless systems on their boats so as to control the harvesting and marketing of bananas in Puerto Rico. Fessenden held a contract with them and wanted to give a Christmas present to his customers on the dozen or so ships at sea.

On that cold December night he played a recording of Handle's “Largo” on an Ediphone. Following that he dazzled his listeners with his talent as a violinist by playing “Oh Holy Night”. After several readings from the Bible he signed off by extending Christmas greetings and a request to have them write and report to him on the reception of the broadcast wherever they were. The mail response confirmed that Fessenden had successfully invented radio, as we know it today.

In spite of this, the rest of Fessenden's life was a constant struggle for recognition of his inventions and for compensation from his rich partners who had sold his patents out from under him to large American companies. He died relatively unknown, in Bermuda.

Thank you Reginald Fessenden. On the 100th anniversary of your great discovery, we the Canadian members of the IEEE have honoured your contribution to society by establishing the IEEE Canada Reginald Fessenden Medal in 2000. Sorry we were so late.

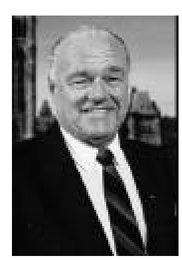
Well I am going to stop there, The story of the advances in the communications industry since the start of the 20th century is well documented. From radio to television, from wired to wireless, from copper to fiber optics, from earth to satellites and beyond, the progress has been outstanding and worthy of your research. There are lots of “Atlantic Oceans” out there to be challenged and I urge you to tackle them by following Churchill's advice, “to look back occasionally so that you can see further into the future.”



St. John's NF site selected by Gugliemo Marconi to receive the first wireless transatlantic signal.

About the author

Wally Read is a former Region 7 Director (1984-85), and a Past President of the IEEE (1996). Currently he is Chair of the 2002 IEEE History Committee and takes particular delight in identifying Canadian achievements in our technologies and honouring those responsible. Wally can be reached at w.read@ieee.org



On Managing Virtual Private Networks

by Raouf Boutaba
Computer Science Dept., University of Waterloo, ON

Abstract

Network operators and value added service provider offer VPN services to corporations that wish to tie together their geographically dispersed offices and to provide their mobile workforce with access to the company resources. Currently, the management of the VPN resources is mainly ensured by the provider of the bearer telecommunication services, while the VPN customers have no direct control over these resources. The increasing importance of the broadband communication infrastructure in corporate operations and transactions is stressing the requirement for a customizable design, operation and management of VPN services. This article discusses the trend towards customer management of VPNs.

Sommaire

Le réseau privé virtuel (RPV) est un service offert par les opérateurs de réseaux et les fournisseurs de services à valeur ajoutée. Il est utilisé par les corporations qui ont besoin de relier ensemble leurs bureaux géographiquement répartis et pour fournir à leurs employés mobiles un accès à distance aux ressources. Actuellement, la gestion des ressources du RPV est assurée par l'opérateur du service de télécommunication de base, alors que les clients du service RPV n'ont aucun contrôle directe sur ces ressources. L'importance grandissante de l'infrastructure réseau pour les activités et les transactions des corporations suscite de plus en plus le besoin d'une conception et une gestion personalisées du service RPV. Cet article analyse la tendance vers une gestion client des RPVs.

1.0 Introduction

Virtual Private Network (VPN) is one of the major trends in the integrated broadband communications environment. There is a myriad of definitions of a VPN used in the networking community to describe a broad set of problems and solutions. In [1], Ferguson et al. define a VPN as a communications environment in which access is controlled to permit peer connections only within a defined community of interest. A VPN is constructed through some form of partitioning of a common underlying communications medium, where this underlying communications medium provides services to the network on a non-exclusive basis".

A VPN service is primarily useful for organizations that wish to use public networks to connect their various LAN's for private purposes. This is typically the case of large corporations that need to connect a set of geographically separated offices while preserving the private character of their communications. Therefore, the VPN concept has to respond to two conflicting requirements:

1. Allow for a cost-effective communications infrastructure through resource sharing. Compared to the dedicated leased circuit approach, organizations reduce the cost of connecting geographically dispersed sites by establishing VPNs across a shared public network.
2. Allow for communications privacy. Although several organizations share a common communications infrastructure (public backbone network), they want their communications services to be within one closed environment isolated from all other environments that share the common underlying communication infrastructure.

VPN services are commonly offered by a value added service provider to a number of service subscribers referred to as the VPN customers. The VPN provider sets up the VPN connectivity for a customer using the services of multiple Public Network Operators (PNOs). The VPN provider may be a separate organization or it may be part of one of the PNOs. The advantage of the VPN provider as an intermediate level between the customer and the involved PNO(s) is that of one-stop shopping which provides a single interface to the customer for accepting requests, queries and complaints, and also to provide a single bill to the customer.

The initial target of the VPN concept was to successfully replace the leased lines-based private data networks and PBX interconnection. The evolution of VPN is motivated by the reduction of the high cost due to the dedication of equipment. Most of existing VPN services are based on conventional Public Switched Telephone Networks (PSTN) or on Public Switched Packet data Networks (PSPDN). Second generation VPNs use technologies such as ATM cross connect, and support semi-permanent pipes such as ATM end-to-end Virtual Path Connections (VPCs).

In such VPNs, management services include configuration and static bandwidth management, in which bandwidth is not altered after VPC set up. Similar VPNs are implemented using Frame Relay (FR) networks. New generation VPNs are evolving to support full open network provisioning. They use B-ISDN based on switched ATM and IP routing capabilities as well as encryption techniques. There is a powerful logic to the shift towards Internet VPNs. *Economic of communications* is the most predominant factor: a corporation's expenses are only the cost of the short loop between its offices and the Point Of Presence (POP) of the local ISP. *Flexibility* in setting up a VPN using the public Internet is another factor. This can be as simple as adding a gateway and the necessary software for establishing a secure VPN connection. The Internet provides *worldwide connectivity*. Indeed, a VPN node can be added wherever there is an Internet POP, which are available worldwide. Last but not the least worldwide availability of cheap Internet access increases *mobile workforce productivity* through remote access. In turn Internet VPN face significant challenges such as security, quality of service and reliability. These issues are currently subject to large research and development efforts.

This article starts with a comprehensive analysis of existing VPN models. Then, it describes current VPN operation and management practices. Finally, it discusses future trends in VPN management.

2.0 VPN Models

The models to construct VPNs can be categorized into two main models: "peer" and "overlay" VPN models [1]. In the peer VPN model, the network layer forwarding path computation is done on a hop-by-hop basis. Traditional routed networks are examples of peer models, where each router in the network path is a peer with its next hop adjacencies. In the overlay VPN model, the intermediate link layer network is used as a "cut-through" to another edge node on the other side of a large cloud. Examples of overlay VPN models are ATM, Frame Relay, and tunneling implementations. Orthogonal to the previous models is the security requirement in a VPN, including confidentiality, data integrity, authentication, and access control. Encryption is what makes VPNs private. It is a key component used to respond to most of these requirements.

In general, the VPN architecture depends on the layer of the protocol suite that is used to implement the VPN service. Also, the complexity of implementation and maintenance of the VPN depend on the type of VPN as well as on scalability and security requirements. The remaining of this section overviews the different types of VPNs and presents their respective features.

2.1 Overlay VPN Models

Overlay VPN models are more naturally implemented at the link-layer of the protocol stack. A link-layer VPN attempts to provide a functionality similar to conventional private data networks while achieving economies of scale and operation through multiplexing (using virtual circuits instead of dedicated transmission paths). In this scenario, VPNs share a common switched public network infrastructure for connectivity (i.e., the same switching elements within the public network), while the VPNs have no visibility of one another. Usually, such infrastructure consists of Frame Relay or ATM networks. The major advantage of utilizing virtual circuits in the public switched network is their flexibility and cost-effectiveness. However, the disadvantage is the scaling limitation and the complexity of configuration management.

Multi Protocol Over ATM [2] (*MPOA*) is an “overlay” model of constructing VPNs similar to the “cut-through” mechanisms where the switched ATM network enables egress nodes to be one “Layer-3” hop away from one another, using dynamically controlled edge-to-edge ATM Virtual Connections (VC’s). However, MPOA approach assumes a homogeneous ATM environment, and relies on external address resolution servers to support the Address Resolution Protocol (ARP).

Tunneling is one increasingly popular method of constructing VPNs by sending specific portions of network traffic across tunnels. It is considered as an overlay model. The most common mechanisms are GRE (Generic Routing Encapsulation) [3] tunneling between a source and destination router, router-to-router or host-to-host tunneling protocols such as L2TP [4] (Layer 2 Tunneling Protocol) and PPTP [5] (Point-to-Point Tunneling Protocol), and DVMRP [6] (Distance Vector Multicast Routing Protocol) tunnels.

2.2 Peer VPN Models

Controlled Route Leaking is one implementation of the peer VPN model. It consists of controlling route propagation to the point that only certain client networks receive routes for other networks which are within their own community of interest. The routes associated with a set of clients are filtered such that they are not announced to any other set of connected clients, and that all other non-VPN routes are not announced to the clients of the VPN. The controlled route leaking technique is considered to be prone to administrative errors, and admit an undue level of insecurity and network inflexibility. In addition, this technique does not possess the scaling properties desirable to allow the number of VPNs to grow beyond the bounds of a few hundreds, using today’s routing technologies. An alternative technique uses *BGP community attribute* [7, 8] to control route propagation. This method is less prone to human misconfiguration and allows for a better scalability. It allows a VPN provider to “tag” BGP NLRI’s (Network Layer Reachability Information) with a community attribute, such that configuration control allows route information to be propagated in accordance with a community profile. The BGP communities technique allows flexible construction of network layer VPNs by preventing VPN service subscribers to detect the fact that there are other subscribers to the service. However, it does not guarantee data privacy in the core of the service provider’s network (i.e., the portion of the network where traffic from multiple communities of interest share the infrastructure).

Multi-Protocol Label Switching [9] (*MPLS*) is a hybrid architecture which combines the use of network layer routing structures and per-packet switching, and the use of link-layer circuits and per-flow switching. In the case of IP over ATM, each ATM bearer link becomes visible as an IP link, and the ATM switches are augmented with IP routing functionality. The latter is used to select a transit path across the network, and those transit paths are marked with a sequence of locally defined forwarding path indicators or labels. A generic MPLS architecture for the support of VPN structures is that of a label switched common host network and a collection of VPN environments that use label-defined virtual circuits on an edge-to-edge basis across the MPLS domain. The label applied to a packet on ingress to the MPLS environment effectively determines the selection of the egress router, as the sequence of label switches defines an edge-to-edge virtual path. MPLS itself and MPLS-based VPNs are still under active research and present great potential particularly for supporting VPNs with Quality-of-Service (QoS) over the Internet.

2.3 Encryption-based VPNs

Encryption technologies are effective in providing the virtualization required for VPN connectivity, and can be deployed at almost any layer of the protocol stack. The implementation of VPNs at the transport and application layers is mostly based on the use of encryption services. Application layer encryption, for example, is the most pervasive method of constructing VPNs in multiprotocol networks. Transport layer encryption aims at providing privacy and data integrity between two communicating applications. For this purpose the Transport Layer Security Protocol or TLS [10] is being defined within the Internet Engineering Task Force (IETF). Network layer encryption is implemented according to two modes: the end-to-end mode where encryption is performed between participating hosts; and the tunnel mode where encryption is performed between intermediate routers. The first mode allows for a higher level of security and implements VPN granularity at the level of the individual end system. The second mode is less secure in that it leaves the tunnel ingress and egress points vulnerable, since these points are logically part of the host network as well as being part of the unencrypted VPN network. In the Internet, the network layer encryption standard being defined within the IETF is IPSec (IP Security) [11]. Encryption at the link layer is supported by special encryption hardware generally vendor specific and hence poses interoperability problems in multi-vendor environments. It is worth noting that as one moves down through the protocol stack, the implementation of VPN tunnels become easier, while securing them becomes more challenging.

3.0 VPN Operation and Management

3.1 Current Practice

The VPN is mainly viewed from two distinct viewpoints: the VPN customer and the VPN provider. The VPN customer represents the closed user group of the VPN. It is responsible for negotiating the VPN services with the VPN provider. The negotiation includes the type of services required, the offered quality and the price. If the VPN fails to provide the contracted quality of service, the customer complains to the VPN provider. The VPN provider is the party offering the VPN service to the VPN customer. Commonly, each VPN has one provider, which can be either a private company or a public network operator. The most important task of the VPN provider is to coordinate the various sub-networks over which the VPN is built and to make this inter-working transparent to the VPN customer and user. The VPN provider predicts the traffic generated by its customers and plans the capacity of its network resources. In case the VPN service provider is the public network operator, then the VPN provider is also responsible for operating the network over which the VPN is implemented.

VPN provisioning may involve several levels of providers and customers. The visibility of network resources is not the same in these distinct administrative domains and the operation and management functions are not applied the same way. Efficient operation of the network necessitates the management of the available resources in order to maximize their utilization and to ensure the expected QoS. The provision of VPN imposes further requirements on the management of network resources (physical and logical) which has to be performed in a cooperative way between VPN providers and VPN customers. The configuration of the VPN commonly leads to the reservation of a set of resources in order to accommodate the VPN traffic.

3.2 Operation and Management Functions

The estimation of traffic expected to be generated by VPN users (traffic matrix) is a prerequisite to determine the transmission and switching capabilities needed to support the VPN operation. This estimation, referred to as user traffic characterization, is initially used by the VPN customer to select which VPN service to subscribe to. It is then continuously adjusted to reflect the real utilization of the subscribed services (e.g., frequency and duration of service utilization) possibly leading to service re-negotiation. The VPN provider has also to continuously estimate the expected traffic to accommodate changing VPN customers needs. The provision of the VPN service consists of network resources reservation according to the specified performance and bandwidth requirements. The service may be of the following types:

- Fixed bandwidth is provided for the lifetime of a VPN;
- Pre-booked bandwidth variations where the customer may specify in advance how the bandwidth reserved on a VPN should vary over time (throughout the working day for example);
- Bandwidth on demand where the customer may change the bandwidth reserved on an already existing VPN.

To configure a VPN, the VPN provider takes into account the location of the VPN customer sites and the associated traffic needs as estimated in the traffic characterization phase. The VPN customers provide the VPN provider with a private addressing scheme (if applicable), an estimate of traffic requirements and the requested QoS. Based on the previous information, the VPN provider plans his network by determining the type and amount of transmission and switching resources. The objective of the VPN provider is usually to minimize the amount of network resources in order to reduce the cost and hence maximize the revenue while satisfying the QoS contracted to VPN customers. VPN reconfigurations may also occur during the VPN lifetime to take into account changes of user-traffic requirements (e.g., service upgrade);

faults occurrence at the network level; QoS degradation; customer's complaints; and others.

A continuous monitoring of the VPN customer traffic and the underlying network is performed by the VPN provider to ensure that service is provided to customers according to the contracted QoS. The VPN customer computes statistics on the VPN service performance (e.g., the number of (un)successful accesses). The measured and the expected VPN performance are then compared which may lead, in case the VPN users are not satisfied with the experienced QoS, to issuing complaints to the VPN provider or to a re-negotiation of QoS parameters.

The VPN service can be used by VPN customers only. Therefore, access control mechanisms are required to protect VPN users/services from unauthorized access. Encryption mechanisms are used to guarantee privacy and data integrity. These mechanisms are usually defined on a per closed user group (i.e. customer) basis. Accounting management uses the information collected by the VPN provider monitoring function to establish the service usage bills and charge the VPN customer.

3.3 Inter-domain VPN Management

The provision of a VPN service may involve several network providers. For example, setting up an Internet VPN between a company's headquarters and its branch offices abroad typically requires services from several local Internet Service Providers (ISPs) and backbone network providers. The management of such VPN involves several administrative domains (the customer domain and the various providers' domains).

VPN end-to-end management requires interactions between VPN customer and VPN provider(s) management domains. These interactions are based on a client/server model, and mainly correspond to negotiating the VPN configuration and the VPN service provision according to the agreed contract. Contracts specify equipment rental and service-level agreements (SLA). During the lifetime of the VPN, the management domains interact to ensure proper operation of the VPN or to renegotiate their contracts. The customer is responsible for identifying the end points, the performance (delay, jitter, packet loss ratio), and the bandwidth (peak bandwidth and variations in bandwidth over time) requirements. According to traffic characteristics and QoS parameters agreed with the customer, the VPN Provider establishes the VPN with the negotiated QoS. In addition to the regular VPN, the customer may require exceptional traffic demands such as setting up high bandwidth calls at given times or changing backup schedule leading to changes in bandwidth requirements. The customer complaints to the provider whenever the offered QoS is below the negotiated one. The customer may also request for re-configuration of the VPN. Ultimately, VPN Provider management is required to provide a single interface to the customer for accepting requests, queries and complaints and also to provide a single bill to the customer. In case the VPN provider is a value added service provider distinct from the public network operator, the VPN provider determines which public network operators should be involved in the provision of the VPN. The VPN provider identifies the end points in each public network domain, the performance and bandwidth requirements, and rents network resources from the involved public network operators. In turn network operators interact with each other, most likely in a peer-to-peer fashion, to negotiate which network resources between their gateway nodes will be used for the VPN.

Service level agreement (SLA) or service contract, mainly consisting of the *traffic contract*, is the basis for the peer-to-peer negotiations involved in a VPN service provision. A traffic contract can be defined for every connection. It consists of connection traffic descriptors and QoS parameters. Each customer is expected to generate traffic that conforms to these parameters. The VPN service provider monitors the offered load and enforces the traffic contract. The VPN service provider is committed to meet the requested QoS, as long as the customer complies with the traffic contract. In addition to the traffic contract, a service contract, for example between the customer and the VPN provider, may include time intervals information for the connections (e.g., days of the week, times during the day, duration etc.) and which customer sites should be connected.

4.0 Future trends

In traditional VPN environments, the customer has the view of the configuration of its CPN (Customer Premises Network) and a view of the VPN resources dedicated to interconnect its sites. The customer is also aware of the capacity of these connections. The VPN provider has a view of the access and transit nodes (VPN switching/routing nodes in the public network domain) and the interconnection between them. If the VPN service provider is also the public network provider then it has also an explicit view of the physical and logical configuration of its own network including the transit and access nodes constituting the public network as well as the links interconnecting these nodes.

In this scenario, the VPN provider hides the network topology as far as the customer was not interested in the way the connections between the customer sites are realized. The main reason for that is the assumption that customers do not have the appropriate skills to control and manage the public network resources that are rented to them. In this case, the customer only controls its CPN including the equipment used to access the public network. The customer also performs the modifications in the CPN when requested (e.g., updates the route selection tables or the private addressing scheme, etc.). The VPN service provider, as a value added service provider, plays an intermediate role between the customers and the involved providers of bearer communication services. It operates the network links rented from the network providers and allocates the contracted bandwidth to customers. In this case, the VPN service provider has a limited access to the network infrastructure and performs management such as the reconfiguration of the links indirectly by requesting the appropriate network provider.

Customers ranging from large to small enterprises are relying more than ever on the networks to conduct their businesses. For that reason, they are either acquiring the appropriate management tools and qualified personnel to administrate and maintain their growing customer premises networks or outsourcing the management of their network resources to third parties. Moreover, customers are seeking to control and manage the VPN services they are subscribing to. There are several reasons for that. Above all is the possibility for customers to control and manage their VPNs according to their own policies reflecting their business goals. A VPN service provider cannot easily accommodate a large variety of service requirements of the various customers. Customers may have different traffic requirements (data, voice, and video) with different priority schemes and performance characteristics. They often require different levels of security. Another important reason for customers to control and manage their VPN is to perform the necessary partitioning of the VPN resources among the different end-users and applications they support, and to implement their own policing mechanisms. Last but not the least is the ability of customers to introduce new communication services if they have full control over the resources allocated to them in the internal network nodes and hence the possibility to introduce their proper resource control algorithms. This trend has been recently strengthened by the emergence and wide acceptance of network programmability as the networking paradigm of the future.

Indeed, effort is currently spend in both academia and industry to open the core network infrastructure and facilitate its programmability by providing the appropriate *network programming interfaces.* Among the undergoing works in this area, there are: the definition of open switching architectures [12], the specification of open signaling protocols [13], the development of programmable and active networks [14]. This trend will bring new challenges to the control and management of network resources. One of the most critical problems that need to be addressed is the shared control and management of the network resources between several domains, which may lead to conflicts. In general, the functions of each domain and the interactions between the different domains have to be re-engineered.

These advances will ultimately enable customer management of VPNs and thereby customizable configuration and goal-driven management of these VPNs. A demonstration of such capabilities is presented in [15].

5.0 References

[1]. Paul Ferguson and Geoff Huston, *What is a VPN?,* White paper, http://www.employees.org/~ferguson/, April 1998.

[2]. ATM Forum, *Multi-Protocol Over ATM*, Specification v1.0, af-mpoa-0087.000, July 1997.

[3]. Hanks, T. Li, D. Farinacci, P. Traina, *Generic Routing Encapsulation,* RFC1701, October 1994.

[4]. A. Valencia, K. Hamzeh, A. Rubens, T. Kolar, M. Littlewood, W. M. Townsley, J. Taarud, G. S. Pall, B. Palter, W. Verthein,, *Layer Two Tunneling Protocol 'L2TP'*, draft-ietf-pppext-l2tp-10.txt, March 1998.

[5]. K. Hamzeh, G. Singh Pall, W. Verthein, J. Taarud, W. A. Little, *Point-to-Point Tunneling Protocol – PPTP*, draft-ietf-pppext-pptp-02.txt, July 1997.

[6]. D. Waitzman, C. Partridge, S. Deering, *Distance Vector Multicast Routing Protocol*, RFC1075, November 1988.

[7]. R. Chandra, P. Traina, T, Li, *BGP Communities Attribute*, RFC1997, August 1996.

[8]. E. Chen, T. Bates, *An Application of the BGP Community Attribute in Multi-home Routing*, RFC1998, August 1996.

[9]. Callon, P. Doolan, N. Feldman, A. Fredette, G. Swallow, A. Viswanathan, *A Framework for Multiprotocol Label Switching*, draft-ietf-mpls-framework-02.txt, November 1997.

[10]. T. Dierks, C. Allen, *The TLS Protocol – Version 1.0*, draft-ietf-tls-protocol-05.txt, November 1997.

[11]. S. Kent, R. Atkinson, *Security Architecture for the Internet Protocol*, draft-ietf-ipsec-arch-sec-04.txt, March 1998.

[12]. Proceedings of OPENARCH'99, N.Y., March 1999.

[13]. Proceedings of OPENSIG'98, Toronto, October 1998.

[14]. D. Tennenhouse, J. Smith, W. Sincoskie, D. Wetherall, and G. Minden, *A Survey of Active Network Research*, IEEE Communications Magazine, January 1997.

[15]. R. Boutaba, W. Ng., A. Leon-Garcia, *Web-based Customer Management of VPNs*, Journal of Network and Systems Management, Vol. 9, No. 1, 2001.

6.0 List of Acronyms

ARP	- Address Resolution Protocol
ATM	- Asynchrous Transfer Mode
BGP	- Boarder Gateway Protocol
CPN	- Customer Premises Network
DVMRP	- Distance Vector Milticast Routing Protocol
FR	- Frame Relay
GRE	- Generic Routing Encapsulation
IETF	- Internet Engineering Task Force
ISP	- Internet Service Provider
LAN	- Local Area Network
L2TP	- Layer 2 Tunneling Protocol
MPLS	- Multi-Protocol Label Switching
MPOA	- Multi Protocol Over ATM
NLRI	- Network Layer Reachability Information
PBX	- Private Branch Exchange
PNO	- Public Network Operators
POP	- Point of Presence
PSPDN	- Public Switched Packet Data Networks
PSTN	- Public Switched Telephone Networks
QoS	- Quality-of-Service
SLA	- Service Level Agreement
TLS	- Transport Layer Security
VC	- Virtual Connection
VPC	- Virtual Path Connections
VPN	- Virtual Private Network

About the author

Prof. Raouf Boutaba teaches networks and distributed systems in the Department of Computer Science of the University of Waterloo and conducts research in integrated network and systems management, wired and wireless multimedia networks, and quality of service control in the Internet. He is the program chair of the technical committee on information infrastructure of the IEEE Communications Society and the chairman of the IFIP working group on network and distributed systems management Dr. Boutaba is a member of the advisory editorial board of the International Journal on Networks and Systems Management. He is the recipient of the Province of Ontario Premier's Research Excellence Award in 2000.

Newly Elected IEEE Fellows 2002

Majid Ahmadi University of Windsor Windsor, ON	For contributions to the design of digital filters, and to pattern recognition and image restoration.
Jens Bornemann University of Victoria Victoria, BC	For contributions to the modeling of design of waveguide components and planar structures.
Terrence Michael Caelli University of Alberta Edmonton, AB	For contributions to machine vision and pattern recognition.
James Kennedy Cavers Simon Fraser University Burnaby, BC	For contributions to the theory and practice of digital transmission over wireless channels.
Henrietta L. Galiana McGill University Montreal, QC	For leadership in understanding biological control systems and for the development of transient identification methods in the modeling of ocular reflexes.
Wayne Davy Grover University of Alberta Edmonton, AB	For contributions to survivable and self-organizing broadband transport networks.
James W. Haslett University of Calgary Calgary, AB	For contributions to high temperature instrumentation and noise in solid-state electronics.
Praveen K. Jain Queen's University Kingston, ON	For contributions to efficient high frequency power converter systems.
Wenyuan Li BC Hydro Burnaby, BC	For contributions to power system reliability theory, calculation methods and algorithms, and applications.
Jose Ramon Marti University of British Columbia Vancouver, BC	For contributions to the development of electromagnetic transients programs for transmission line modeling and real-time simulation.
Andrew Ng University of British Columbia Vancouver, BC	For contributions to plasma science concerning warm dense matter, femtosecond-laser matter interactions, and laser-driven shock waves.
Graham John Rogers Cherry Tree Scientific Software Colbourne, ON	For contributions to the modelling, analysis and control of dynamic phenomena in power systems.
Magdy M.A. Salama University of Waterloo Waterloo, ON	For contributions to the advancement of distribution system performance.
Kon Max Wong McMaster University Hamilton, ON	For contributions to sensor array and multi-channel signal processing.

Modeling Flow and Congestion in Packet Switching Networks

by *Anna Lawniczak[1,2], Peng Zhao[1], Alf Gerisch[1,2], Bruno Di Stefano[3]*

[1]University of Guelph, Guelph, ON

[2]The Fields Institute for Research in Mathematical Sciences, Toronto, ON

[3] Nuptek Systems Ltd., Toronto, ON

Abstract

We investigate simplified models of packet switching networks and examine how an introduction of additional randomly generated links influences the performance of these networks. In general, the impact of additional randomly generated links on the performance of a network depends on a routing algorithm used in the network and on a "cost" assigned to each network link. With the shortest path full table routing, where the cost of each link is one, i.e. with the "minimum-hop full table routing", degradation of performance of a network is observed. However, if the cost of each link is equal to the queue size of the node from which the link originates or to the queue size plus one then an improvement in the network performance is observed.

Sommaire

Nous étudions les modèles simplifiés des réseaux de commutation par paquets et examinons comment l'introduction de liens générés aléatoirement influence la performance de ces réseaux. En général, l'impact de l'addition des liens générés aléatoirement sur la performance d'un réseau dépend de l'algorithme de « routing » utilisé dans le réseau et du « coût » assigné à chaque lien du réseau. Avec la table complète du « routing » du chemin le plus court, où le coût de chaque lien est égal à 1, c'est-à-dire avec le « minimum-hop full table routing », on observe une dégradation de la performance du réseau. Toutefois, si le coût de chaque lien est égal à la grandeur de la queue du noeud à partir duquel le lien origine (ou égal à la grandeur de la queue plus 1) alors une amélioration dans la performance du réseau est constatée.

1.0 Introduction

Understanding the dynamics of flow and congestion in data communication networks is of vital importance. Some of the aspects of this dynamics can be captured and investigated by studying simplified models of data communication networks. Often these models assume either regular topology of a network, in the form of a square or a hexagonal lattice, or a binary Cayley tree, or a random graph topology. The purpose of our work is to study how additional randomly generated links affect the dynamics of flow and congestion in packet switching networks. We investigate the performance of such networks for various routing algorithms and network topologies. In order to simulate simplified models of packet switching networks we developed a software tool called DataNetwork.exe. In this article we highlight only the developed methodology and present some selected results. This work is the continuation of the research commenced by one of the authors in [1,2], and it can be easily extended to simulate dynamics of more complex networks. The proposed methodology can be extended to model dynamics of flow of data in wireless networks.

2.0 Packet Switching Network Models

The purpose of a packet switching network is to transmit messages from points of origin to destination points. In our model, we assume that the entire message is contained in a single "capsule" of information, which, by analogy to packet-switching networks, is simply called a packet. In a real packet-switching network, a single packet carries the information "payload", and some additional information related to the internal structure of the network. Since our aim is to understand, for various routing algorithms, the effects of additional randomly generated links on network flow and congestion, we ignore the information "payload" entirely. Hence, in the considered models we assume that each packet carries only two pieces of information: time of its creation and its destination address.

Our simulated networks consist of a number of interconnected nodes. Each node can perform two functions: of a hosts, meaning that it can generate and receive packets, and of a router (message processor), meaning that it can store and forward packets. Packets are stored in queues and buffers which are maintained by the nodes. We assume that each queue can be of unlimited length and that each buffer stores temporarily only one packet which is ready for routing. Packets are created and moved according to a discrete time parallel algorithm. The structure of the considered networks and their routing algorithms are described in subsections which follow.

2.1 Connection Topologies

A packet-switching network topology can be viewed in an obvious way as a digraph, where each network node corresponds to a vertex, and each communication link between two nodes corresponds to a pair of parallel edges, each carrying data in one direction. With each direction of a link is associated a cost of transmission of a packet.

We consider the following network connection topologies: regular periodic (non-periodic) two-dimensional lattices L; and regular periodic (non-periodic) lattices L_l with "l" additional randomly generated links added to them. In particular, our software tool, DataNetwork.exe has been developed for square and hexagonal lattices.

The network hosts and routers are located at the nodes of the lattice L. The communication links between nodes are represented by the lattice L edges. The extra links are constructed using the following procedure. First, we select randomly a node n_1 on a lattice L. Next, we select randomly another node n_2 on the lattice L, different from the node n_1. We connect these two nodes with a direct communication link. By repeating this procedure independently l times we obtain the lattice L_l having l additional randomly generated links. In the described model it can happen that the nodes n_1 and n_2 can be selected again to form a new link. Hence, in the network the same nodes can be connected directly by several links. However, this procedure can be easily modified. We want to emphasise that all the connections in our model are static, they do not change during the simulation period. Randomly generated links are added before the simulation starts and remain unchanged. This property can be easily modified.

2.2 Routing Decisions

In the network models under discussion, each packet is transmitted from its source node through various links and packet switches to a destination node according to some routing decision. This is equivalent to finding a path (route) through the graph. Depending on the costs assigned to network links we consider routing decisions based on the following least-cost criterion: minimum path distance and minimum path length.

We consider three types of link cost functions called "One", "QueueSize" and "QueueSizePlusOne". In the case of the link cost function "One" all links in the network are assigned a cost equal to one. Using the minimum path distance criterion for this link cost function, the number of hops from source to destination is minimized for each packet. The routing based on this criterion is called the minimum-hop routing. In the case of the link cost function "QueueSize" all links in the network are assigned a cost equal to the number of packets awaiting transmission in

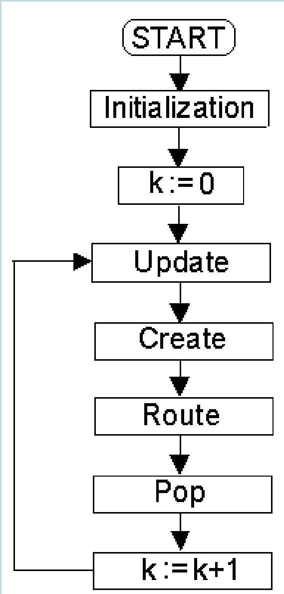


Figure 1: Simplified flow chart of the discrete time network algorithm.

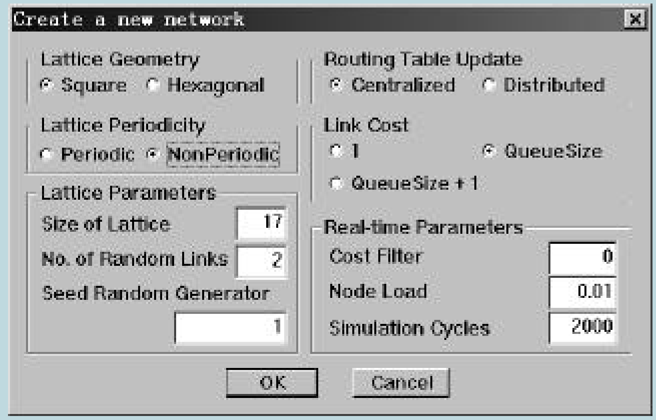


Figure 3: The dialog box of DataNetwork.exe tool.

the node from which the link originates. In the case of the link cost function "QueueSizePlusOne" all links in the network are assigned a cost equal to the number of packets awaiting transmission in the node from which the link originates plus the cost of a single hop (which is equal to one). For these two types of link cost functions the minimum path length criterion selects for a packet in a buffer the next node on its path to its destination. This node is on a path with a minimum sum of queue sizes or with the smallest sum of queue sizes plus the number of hops, respectively, from the packet's node to its destination, depending on the current state of the network.

2.3 Discrete Time Network Algorithm

For all three link cost functions discussed in the previous section the routing decisions can be expressed in terms of routing tables. Here we consider only full routing tables, i.e. each node has a routing table with entries for all nodes in the network. Based on these tables we employ two types of full table routing algorithms, the centralized full table routing algorithm and the distributed one.

In the centralized full table routing algorithm at any discrete time each node knows what are the costs of the least-cost paths to all other nodes in the network. This case corresponds to the situation where a central site is in charge of updating routing tables. Nodes provide their link costs to the central site, which in turn provides new routing tables to all the nodes. At each discrete time new routing tables are calculated based on the criterion of least-cost routing for link cost functions "One", "Queue-Size", or "QueueSizePlusOne", respectively. However, for the link cost function "One" the routing table can be computed *a priori* any simulation. We use the shortest path backward tree algorithm to calculate the new routing tables [3].

In the case of the distributed full table routing algorithms nodes exchange information about their link costs in time in order to determine the least-cost paths from one node to another one. The routing tables are not built up in one cycle as in the case of the centralized full table routing algorithm. They are build up gradually in time. To calculate the routing tables we use the distributed version of the shortest path backward tree algorithm [3].

For the networks with centralized full table routing algorithms or distributed full table routing algorithms the dynamics are governed by the discrete time algorithms as described by the simplified flow chart in Figure 1. The implementation of the modules in the main loop is in parallel over the network nodes.

For each type of the considered routing algorithm we start the network simulation with all queues empty and with discrete time clock "k" set to zero. Then the following operations are repeated in sequence:

1. **Update:** at each node the routing table for centralized or distributed full table routing algorithm is calculated.
2. **Create:** at each node independently of the other nodes, a packet is created with probability p, called the presented node load. Its destination address is randomly selected among all other nodes in the network with uniform probability distribution. The newly created packet is placed at the end of the queue.
3. **Route:** at each node the packet from the buffer is forwarded, if there is one, to the next node along the least-cost path to its destina-

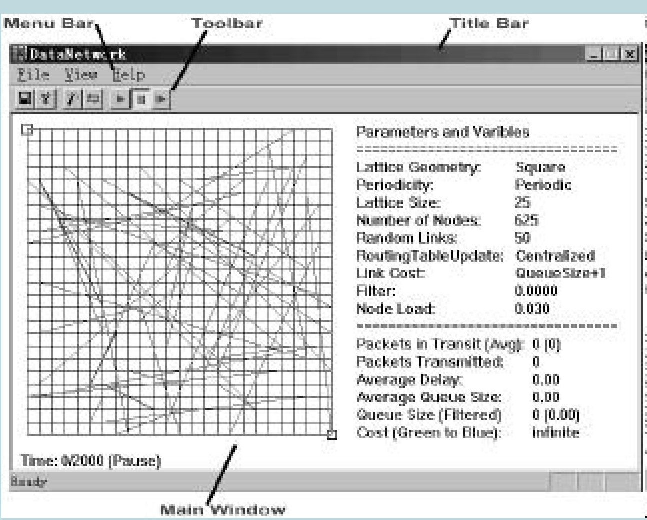


Figure 2: The main window of the DataNetwork.exe tool.

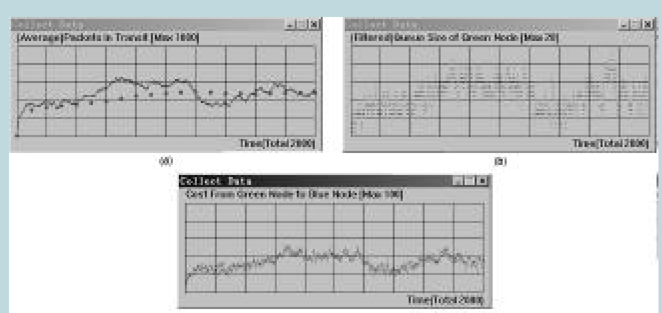


Figure 4: Real-time output data windows of DataNetwork.exe

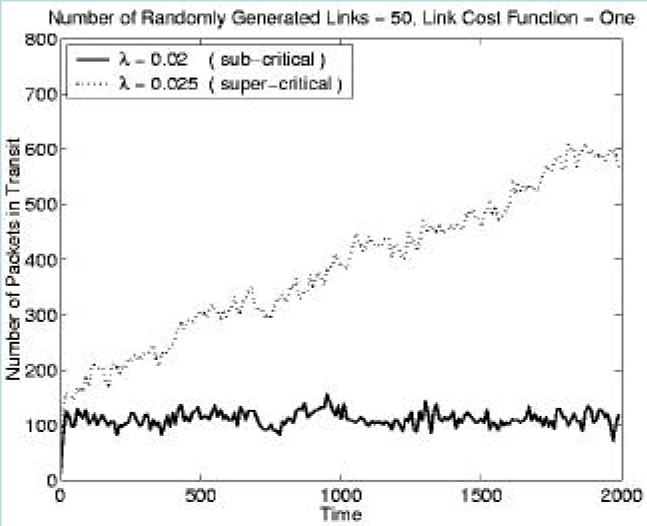


Figure 5: Time evolution of the Number of Packets in Transit for a sub- and a super-critical value of presented node load.

tion. If there are several least-cost paths, then one of them is selected randomly with uniform probability. If the next node is the packet destination, then the packet is destroyed immediately. Otherwise, it is placed at the end of the queue of the next node.

4. **Pop:** at each node, if the queue is not empty then the first packet from the queue is picked up and stored in the node's buffer.
5. Time k is incremented by 1.

The above described sequence of events constitutes a single time step update. It can be repeated an arbitrary number of times. The state of the network is observed after sub-step 5 (clock increase).

3.0 DataNetwork.exe

In order to simulate our models of networks we developed a program called DataNetwork.exe. The program has been developed using the Microsoft Visual C++ 5.0 compiler and is capable of running under

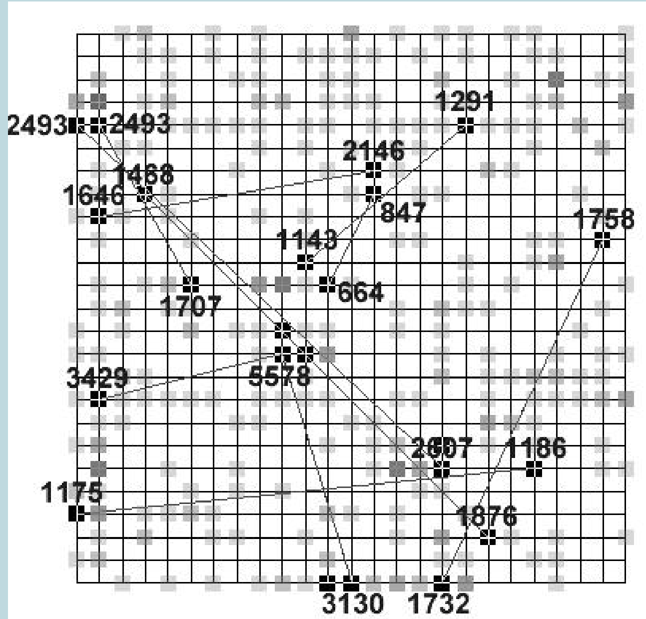


Figure 7: Colour coded queue sizes (from black corresponding to a large queue size to white corresponding to a small queue size) at time 2000 at the nodes a 25 by 25 periodic square lattice network with 10 additional randomly generated links under a presented node load of 0.065. The link cost function is "One". There are approximately 98% of all undelivered packets concentrated in nodes from which extra links originate (queue sizes given there).

Microsoft Windows 95 and 98. Figure 2 depicts the main window of the tool with its various components. The dialog box used to create a new network configuration is given in Figure 3.

DataNetwork.exe allows for real-time output of several network characteristics. These can be displayed during the simulation in special data windows, see Figure 4.

The source code of DataNetwork.exe is currently being ported to UNIX/Linux operating systems. We also plan to incorporate some new features and improvements.

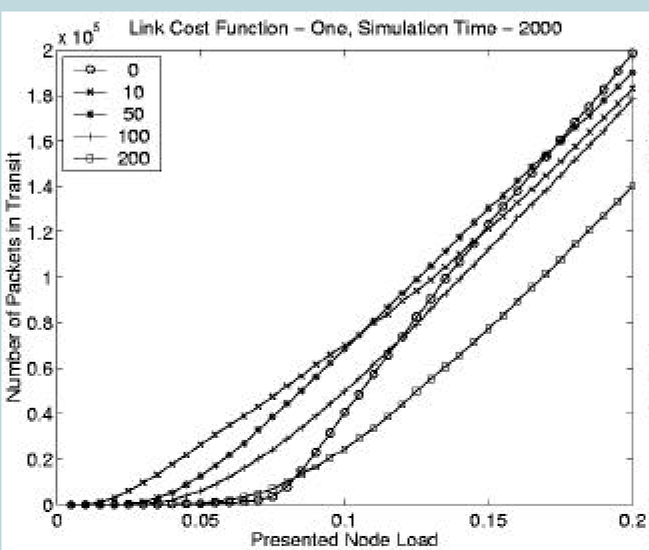


Figure 6: Number of Packets in Transit as a function of presented node load for different numbers of added randomly generated links.

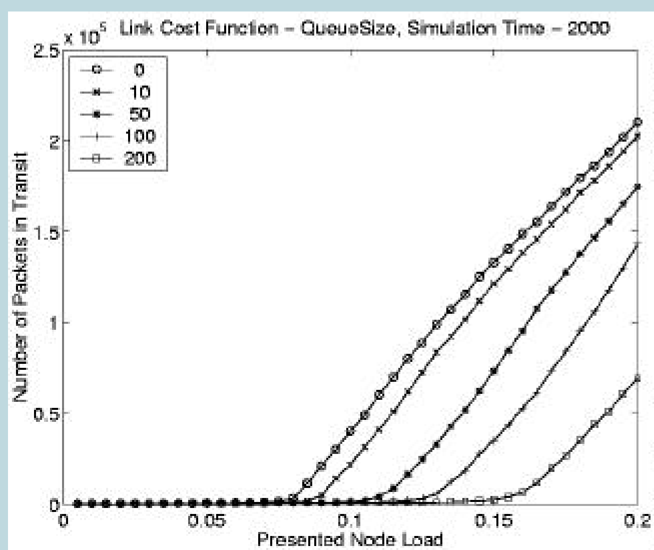


Figure 8: Number of Packets in Transit as a function of presented node load for different numbers of added randomly generated links.

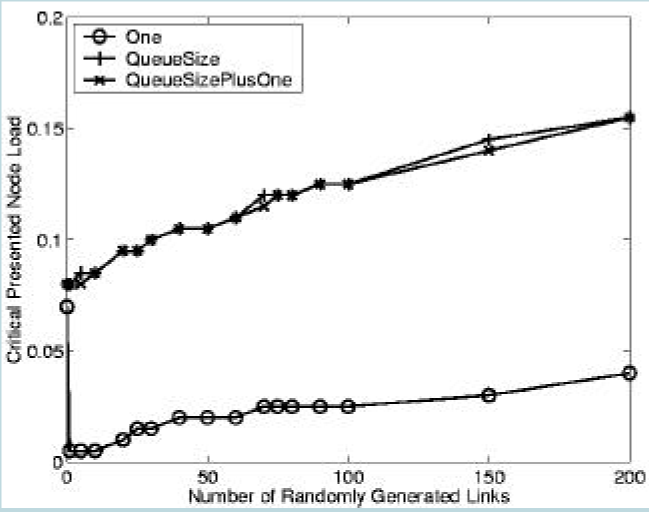


Figure 9: Estimated values of critical presented node load as a function of the number of randomly generated links for the three link cost functions considered.

4.0 Selected Simulation Results

We conducted a large variety of data network simulation experiments with the DataNetwork.exe tool. We first want to stress that the dynamics of a simulated network using the centralized full table routing algorithm turned out to be very similar to the behavior of the network with the same network topology which instead employs the distributed full table routing algorithm.

However, in terms of simulation costs (CPU time) the distributed algorithm is much more cost effective. In this presentation we describe only some of the results obtained in the simulations with the centralized full table routing algorithm. All simulations are performed for 2000 discrete time steps on a periodic square lattice with 25 nodes in each spatial direction. We add randomly generated links to this regular network in a manner such that the set of links of a network with l_1 randomly generated links is a subset of the set of links of the network with l_2 randomly generated links for all $l_2 \geq l_1$. We study the influence of the addition of randomly generated links on the performance the network. To this end, we monitor some characteristic network quantities during the time of simulation. These are, beside some others, the Number of Packets in Transit (i.e., the number of all packets in the network which have not yet arrived at their respective destination node) and the Average Delay Time (i.e., for all packets, which have reached their destination since the simulation was started, we form the sum of their delay times and divide by the number of those packets; the delay time of a packet is the simulation time elapsed between creation of the packet at its source node and arrival at its destination node).

Our main interest is to determine the maximum admissible presented node load (the critical presented node load) for a network configuration such that the flow in the network does not become congested. We decide on this critical node load value by considering the time evolution of the Number of Packets in Transit in the network. A value of the presented node load is called sub-critical if the Number of Packets in Transit is constant (beside some fluctuations caused by the randomness in the network) after a transient phase at the beginning of the simulation. If the Number of Packets in Transit increases with time then the presented node load value is called super-critical. The typical behavior of the Number of Packets in Transit as a function of simulation time for a sub- and a super-critical presented node load value is shown in Figure 5.

We now consider the Number of Packets in Transit at final simulation time as a function of the presented node load. Figure 6 gives the resulting graphs for the simulations with link cost function "One" for 0, 10, 50, 100, and 200 added randomly generated links. We clearly observe degradation of the networks performance if less than 200 additional randomly generated links are added. The reason for this behavior is that the additional randomly generated links provide short-cuts which lead to reduced path costs if packets utilize these links. Hence, many packets are attracted to nodes from which extra links originate and subsequently these nodes become congested (only one packet can be dealt with at any time step), leading to the increase of the number of undelivered packets in the network. It is important to note that not the whole network is congested but only areas around the origins of additional randomly generated links.

This can be deduced by looking at the Average Delay Time instead of the Number of Packets in Transit (not presented here) and more clearly seen by looking at the actual queue sizes at the nodes, see Figure 7. A consequence of the described behavior is that the critical presented node load for networks with cost function "One" drops sharply as soon as the first extra link is added and grows only slowly as we add more and more randomly generated links, see Figure 9.

The situation is improved if we change the link cost function to "QueueSize". Now the queue size is taken into account when making the routing decision and packets can circumvent possible congested areas of the network. The result is that the additional links are now utilized by the packets but they do not attract more packets than can be transmitted. This results in a network behavior which is "monotone" in the number of additional randomly generated links, see Figure 8 for plots of the Number of Packets in Transit as a function of the presented node load. Also, we see from Figure 9 that we can present a much higher node load to a network with link cost function "QueueSize" (compared to link cost function "One") without causing congestion.

However, there is one drawback with this kind of link cost function: the packets have no "incentive" at all to reach their destination; they just try to avoid congestion. This results in increased delay times for the packets. This shortcoming, which is especially notable for small values of presented node load, is overcome by the third link cost function "QueueSizePlusOne".

If the link costs of a network are assigned according to the link cost function "QueueSizePlusOne" then both, the number of hops of a path in the network and the queue sizes of the path nodes, contribute to the cost of this path. Therefore, for low presented node load path costs are dominated by the number of hops, and consequently packets travel along paths with a minimum number of hops to their destination. This leads to small delay times of the packets. Otherwise, as the presented node load increases, the sizes of the queues are growing and therefore the cost of a path is dominated by these queue sizes. The result is that packets avoid congested areas (as it is the case with link cost function "QueueSize") and travel around them. This avoids over utilization of the randomly generated links (short cuts). The graphs of the Number of Packets in Transit as a function of the presented node load for networks with link cost function "QueueSizePlusOne" are very similar to those in Figure 8.

Therefore we do not give these plots here. Further, from Figure 9, we see that the critical presented node load for networks with link cost functions "QueueSizePlusOne" and "QueueSize" are almost identical. The advantage of "QueueSizePlusOne" is the improved performance of the network for low values of presented node load.

5.0 Final Remarks

This paper has presented a methodology to model flow and congestion in packet switching networks. DataNetwork.exe is the software tool developed to conduct this work and is the most recent of a series of software tools developed by Dr. Lawniczak's research team. Further research is being conducted to study various aspects of packet switching networks such as data traffic type (short message text (SMS), video, etc.) and network behavior under various levels of degradation. Extensions to wireless networks are being planned. The software tool is being improved to handle more complex models.

Also, we remark that significant performance gains can be observed for the shortest path reduced table routing (where each node holds routing information for a part of the network's nodes only), even when the cost of each link is one, or for the routing based on "geometrical distance" [1,2].

Interested readers wishing to know more and to be kept informed about future work should email to alawnicz@uoguelph.ca.

6.0 Acknowledgement

A.T. Lawniczak, Peng Zhao and Alf Gerisch acknowledge partial support from the University of Guelph. A.T. Lawniczak acknowledges additionally partial support from the Natural Science and Engineering Research Council (NSERC) of Canada and The Fields Institute for Research in Mathematical Sciences. Alf Gerisch acknowledges additionally partial support from The Fields Institute for Research in Mathematical Sciences. Bruno Di Stefano acknowledges total financial support from Nuptek Systems Ltd. The authors acknowledge the use of the SHARCNET computational resources at the University of Guelph. The authors thank Dr. H. Fuks for helpful discussions.

7.0 References

[1]. H. Fuks and A.T. Lawniczak, "Performance of data networks with random links", Mathematics and Computers in Simulation, 51, 1999, pp. 101-117.

[2]. H. Fuks, A.T. Lawniczak, and S. Volkov, "Packet Delay in Models of Data Networks", ACM-Transactions on Modeling and Computer Simulation, Vol. 11, No. 3, July 2001, pp. 1-18.

[3]. W. Stallings, "High-speed networks: TCP/IP and ATM design principles", Prentice Hall, New Jersey, 1998.

About the authors

Prof. Anna T. Lawniczak holds a PhD in Mathematics from Southern Illinois University (USA) and a M.Sc.Eng. from Wroclaw Technical University, Poland.

Since 1989 she is an associate professor at the University of Guelph. Dr. Lawniczak has held a number of visiting positions at various institutions (i.e. Los Alamos National Laboratory, and The Fields Institute for Research in Mathematical Sciences, University of N. Carolina, Bartol Research Institute at the University of Delaware, the University of Roma, etc).

She conducts research in the areas of Mathematical Modelling and Simulation of Dynamics & Complex Systems.

Peng Zhao holds a M.Eng. from the Xi'an University of Technology (PRC), specializing in Automatic Control. He is currently completing a M.Sc. in mathematics at the University of Guelph and will soon defend a thesis on flow and congestion in data communication networks. His advisor is Prof. Lawniczak. Peng intends to continue his studies with a Ph.D.

Alf Gerisch holds a Ph.D. in mathematics from the University of Halle-Wittenberg (Germany), a M.Sc. (Numerical Analysis & Programming) from the University of Dundee (UK). He holds a post-doctoral fellowship, jointly at the University of Guelph and at The Fields Institute. He collaborates with Prof. Lawniczak, conducting research to model flow and congestion of data communication networks and the dynamics of semiconductor nanostructures.

Alf has several papers on numerical methods and their applications to the simulation of tumor angiogenesis and taxis-diffusion-reaction systems.

Bruno Di Stefano, P.Eng., is president of Nuptek Systems Ltd., a consulting company specialising in real-time embedded systems, fuzzy logic, OOA/OOD, C/C++. Previously, he was a senior design engineer for AES Data Ltd. and Delphax Systems.

His professional activities include teaching within the Professional Development Program of Engineering at the University of Toronto since 1986 and previously with Ryerson Polytechnic University. Bruno is also active with the IEEE and with PEO, holding various positions since 1979 and 1992 respectively.

IEEE Canada

Guidelines for submitting an article to the IEEE Canadian Review

Contact any one of the Associate Editors (address information is available on page 2 of this journal). A short abstract should be sent in and will be reviewed before approvals are given for a full paper submission.

Follow these broad-based guidelines for paper preparation:

- Papers (in English or French) must be on topical subjects of interest to the vast majority of our members across Canada,
- Papers selected for the CR are not the type that would normally be submitted to a Conference or Transactions/Journal type of publication. Any mathematical material must be kept to a minimum,
- Papers are normally about 4 pages long (about 2000 words), but articles can be as short as 1 page or as long as 6 pages,
- Submit text in ascii (or WORD) format, as well as a typeset version in pdf format,
- Graphics and images must only be in two colors (Black and Reflex Blue) or Grayscale; Graphics should be scanned at 300 dpi, in 8 bit grayscale, and submitted electronically in either jpeg or gif formats,
- A short Abstract (about 200 words) in English and French (we can provide assistance in translation) is required,
- A short biographical note (about 150 words) about the author(s) is also required, together with a passport size photo,
- For samples of previously published articles, see our website at www.ieee.ca, and follow the links to the *IEEE Canadian Review.*
- Items are normally submitted on-line directly to the Editor.
- We particularly encourage articles from small businesses on topics in electrical, electronic, computer or telecommunications related industries etc.
- We encourage academic institutions to present their new programs so that the community is aware of recent program changes,
- Newsworthy items such as senior appointments in academia and industry are also welcome.

For further information, contact Vijay Sood, Managing Editor, at:

v.sood@ieee.org

Phone: 450-652-8089

Canadian Journal of Electrical and Computer Engineering

Revue canadienne de genie electrique et informatique

For 26 years, the **Canadian Journal of Electrical and Computer Engineering** has been publishing high-quality refereed scientific papers highlighting:

- The results of original research in the field,
- New Technical Achievements,
- Applications related to novel realizations and major systems implementations, and
- Synthesis and tutorial papers on state-of-the-art technology.

Published quarterly, the ***Journal*** also covers particular interests:

- ATM Networks,
- Personal Communications system,
- Visual Computing & Communications,
- and more.

The Canadian journal complements international Journals in the field, as well as the activities in electrical and computer engineering in Canada.

IEEE Canada sponsors the ***Journal*** as a part of its role to promote scientific and professional activities for its members in Canada.

The Canadian Journal of Electrical and Computer Engineering will be of particular interest to anyone active in research and development activities.

IEEE Canada

Subscribe today for $15.00. **All applicable Canadian taxes included**

CANADIAN JOURNAL SUBSCRIPTION FORM

YES! I would like to receive the Canadian Journal of Electrical and Computer Engineering for the low IEEE Canada member price of only CDN $15.00 for the year 2002.

☐ **New subscriber** ☐ **Renewal**

☐ **Cheque or money order enclosed.** (Payable in Canadian dollars, made out to CCECE).

☐ **Charge my** ☐ **Visa**

☐ **MasterCard**

Credit Card No. Exp Date

Signature

Name ____________________

____

Member No. ____________________

Address ____________________

____

____

____

Phone No. ____________________

Fax No. ____________________

Email Address ____________________

GST: R108102864

Mail to:

Canadian Journal of Electrical and Computer Engineering

Attention: Professor O.P.Malik

Dept. of Electrical and Computer Engineering

The University of Calgary

2500 University Drive N.W.

Calgary AB T2N 1N4

Visit our web sites:

www.enel.ucalgary.ca/CJECE

www.ieee.ca

For Fast Service . Fax + 1 403 282 6855 . Tel + 1 403 220 6178 . Email: maliko@ieee.org

The Engineering Institute of Canada, Its History and Importance in 2002

by B. John Plant,
Executive Director EIC, Ottawa, ON

1.0 Historical Background

Once the largest and best-known engineering association in Canada, the Engineering Institute is striving - with some success - to regain a prominent niche in the affairs of a diversely organized Canadian engineering community.

Founded by Royal Charter in Montreal in 1887 as the Canadian Society of Civil Engineers, its objective was the dissemination of technical information and experience.

A quarter century later, membership had grown from 300 to 3000. Although the majority of the founding members were civil engineers, the Society embraced all disciplines of the time with mechanical, electrical, mining and general (civil) engineering sections and branches in Quebec City, Ottawa, Toronto, Winnipeg and Vancouver. During World War I the number of non-civil members increased and the dominance by members from Montreal declined as activities spread across the country. The Society's Charter was appropriately amended by Parliament in April 1918, to the Engineering Institute of Canada. The EIC prospered during the 1920s, survived the Depression and gained strength during World War II. By the early 1960s membership in all grades exceeded 22,000 and there were over 50 branches. However, by the mid-1960s, membership fell as more specialized Canadian engineering societies were formed, the influence of the larger American-based societies grew, the smaller branches were having difficulty surviving and the provision of services to the increasingly diverse membership became more difficult and expensive.

A solution was found in the establishment of semi-autonomous member societies within the Institute, based on technical divisions that had been established earlier. The first, the Canadian Society for Mechanical Engineering, was formed in 1970, followed by the Canadian Society for Civil Engineering and the Canadian Geotechnical Society in 1972 and the Canadian Society for Electrical Engineering in 1973. Those EIC members who declined to join one of these societies became members of the General Members' Group that in the late 1980s was re-formed as the Canadian Society for Engineering Management. By this time, these societies had become fully autonomous through incorporation. With EIC by-law changes these societies replaced individuals as members of the Institute and the Institute became a federation of societies.

In the late 1980s, the Electrical Society added Computer Engineering to its title. Then in 1993 it merged with Region 7 of IEEE to become IEEE Canada, replacing the Civil Society as the largest within the EIC. New member societies have since been added - the Canadian Society for Chemical Engineering in 1998, the Canadian Medical and Biological Engineering Society in 1999, and the Canadian Nuclear Society in 2001. Currently, the membership in all classes within the eight member societies exceeds 30,000. The Institute remains open to the inclusion of additional member societies.

The EIC Mission

- Promote cooperation between the technical societies and their commitment to the vision.
- Collaborate with member societies, universities, educational institutions, industry, to make continuing education and professional development available to all engineers and engineering technology practitioners.
- Assist other national engineering bodies in promoting the good image of the profession particularly in relation to maintaining engineering competency.
- Maintain a national electronic registry of continuing education and professional development activities for engineering professionals ensuring convenience and privacy.
- Promote the maintenance and portability of professional and continuing education credentials.
- Promote the awareness of engineering history in Canada.

The Institute's Life Members Organization, founded in 1954 and incorporated as a charitable organization in 1967, provides an opportunity for retired engineers of varied backgrounds to interact. Members are invited to make voluntary contributions in support of the organizations efforts to advance science and engineering in Canada and support certain benevolent activities.

In 1987 the Institute joined with the Canadian Council of Professional Engineers and the Association of Consulting Engineers of Canada to celebrate the Centennial of the founding of the original Civil Engineer's Society.

Today, the fundamental mandate of the EIC federation includes service to the member societies and the enhancement of the value of membership in those societies by providing services to their members.

2.0 The EIC Objectives

- Membership of all engineering technical societies in the EIC,
- Use of the EIC registry by all engineering professionals (engineers, engineering technologists and technicians),
- Development of the EIC Website as the primary location for communicating opportunities for continuing education and professional development,
- Recognition of EIC Honors and Awards as symbols of Canadian engineering excellence,
- Provide benchmark standards for the delivery of continuing engineering education,
- Establish a system for quality assurance checks on continuing education and professional development experiences,
- Growth in membership of our technical societies,
- Publish Institute documents in both official languages (Note: French version of this document will be available on the website:www.ieee.ca),
- Standardization of Professional Development in Canada.

3.0 EIC Services

- **A forum** for the exchange of experience and other information between member societies. The Institute is governed by a council comprising members from each member society and an executive. Meetings of the Council and workshops provide such a forum.
- **Representation** of all member societies at meetings with the other national engineering bodies such as the Canadian Council of Professional Engineers, the Engineering Academy and the Association of Consulting Engineers of Canada and the Partnership Group on Science and Engineering. For example, the EIC represents the societies at regular meetings of the National Engineering Week Committee and recently at a PEO forum on the future of engineering and has been invited to be a founding member of Registered Engi-

neers for Disaster Relief (Canada).

- The **EIC website** serves the societies by containing links not only to all of the societies but to practically all Canadian engineering organizational sites.
- **Director's Insurance** is purchased as a group for all member societies significantly decreasing the cost to each.
- **Professional development services** are provided to the member societies and their members alike.

1. Recognized standards for the delivery of continuing education and training have been adapted to meet Canadian Engineering needs (see http://www.eic-ici.ca/english/cont_ed/standards1.html) and agreements have been entered into with a number of providers (see http://www.eic-ici.ca/english/cont_ed/pp2.html). These providers commit to the standards and award the EIC Continuing Education Unit to participants in their programs. Compliance with the standards by these providers is monitored using a questionnaire that is sent by the EIC to individuals selected by random sampling. The EIC offers individual engineering professionals the opportunity to record these high quality professional development experiences in a registry maintained by the EIC. To take advantage of the opportunity the individual needs only to indicate to the provider that this is desired. The provider sends the information to the EIC and the EIC protects its privacy and its existence. The advantage to individuals is the ability to store professional development records that may have been obtained over space and time in such a manner that they can be readily retrieved. This activity is paid for with dues collected from the "participating provider partners".

2. Much recognized professional development cannot be awarded CEUs and many licensing bodies recognize the Professional Development Hour. As there appears to be a growing trend to have engineer professionals record their professional development, the EIC is maintaining a professional development registry (see http://www.eic-ici.ca/english/pda/) as a service to the engineering community. Think of it as a personal professional development diary. Use is available to all, a simple matter of registering and establishing your own file by defining an identity and a password. It is organized for the convenient entry of professional development records and the individual user can retrieve personal data simply by printing it at their own computer. In time it is intended to link the CEU and PDH registries. At present, information in the CEU registry will be supplied to the individual to whom it applies in the form of a transcript upon request.

- A new **Career Site** provides a service to the members of the member societies. (http://www.eic-ici.ca/english/career.htm). As a collectivity, the EIC group has the potential to attract the interest of a large number of companies and head hunters seeking to employ engineering professionals. Many job posters are looking for more than one type of engineer. Individuals who are actively or passively seeking a position can easily post their resumes by simply cutting and pasting once they register at the site. They can also indicate any restrictions that they may feel they have on salary, location etc. These users can surf the jobs that have been posted by employers. The qualifications and employment restrictions of job seekers are matched with employer needs by computer. The job posters pay a fee to post jobs or search the resume database. The revenue from this activity is shared with the member societies.
- The **Honours, Awards and Fellowships** program of the EIC represents the top in the hierarchy of the recognition programs of its member societies (see http://www.eic-ici.ca/english/tour/haf1.htm) Twenty engineers are recognized as Fellows each year and up to six medal winners at a banquet held in their honor. Employers etc. are advised of these awards.
- The **History and Archives** committee serves the entire Canadian engineering community by collecting information, publishing papers (see http://www.eic-ici.ca/english/tour/ha1.html), lobbying for public recognition of great Canadian engineers and ensuring that historical plaques are installed at sites appropriate to the engineering history of Canada.

Member Societies of the EIC

The Canadian Geotechnical Society

The Canadian Medical and Biological Engineering Society

The Canadian Nuclear Society

The Canadian Society for Civil Engineering

The Canadian Society for Chemical Engineering

The Canadian Society for Engineering Management

The Canadian Society for Mechanical Engineering

IEEE Canada

THE ENGINEERING INSTITUTE OF CANADA

1100-180 Elgin Street, Ottawa ON K2P 2K3

Admin. Office: 1295 Hwy 2 E, Kingston ON K7L 4V1

Tel: (613) 547 5989 / Fax: 547 0195
E-Mail: info@eic-ici.ca / URL: http://www.eic-ici.ca

About the Author

John Plant, a retired naval officer, received his Ph.D. in Electrical Engineering (M.I.T.) in 1965 and began an academic career which culminated in his being Principal of the Royal Military College from 1984 to 1999. He was President of the Canadian Society for Electrical and Computer Engineering and a key participant in its merger with IEEE Canada. He is a Fellow and Life Member of IEEE and EIC and a recipient of the IEEE Centennial and A.G.L. McNaughton Medals, the EIC John B. Stirling Medal and the PEO Citizenship Award.

Dr. Plant is currently President of the Advanced Technology Education Consortium, Executive Director of the Engineering Institute of Canada and Treasurer of the International Association of Continuing Education and Training.

Président du congrès
Dr. Witold Kinser
University of Manitoba

Président du programme technique
Dr. Doug Chapman
Manitoba Hydro

Dr. Abdel Sebak
University of Manitoba

Trésorier
Dr. Hilmi Turnali
Manitoba Hydro

Secrétaire
Ms. Grace McCaskill
University of Manitoba

Président du programme
Dr. Ken Ferens
Norsat, Winnipeg

Publicité
Mr. Jeffrey Anderson
Internet Innov. Centre

Arrangements locaux
Mr. Alan Pollard
LSM

Expositions
Mr. Doug Strang
NRC

Tutoriaux et sessions spéciales
Dr. Udaya Annakkage

Représentante des étudiants
Dr. Zahra Moussavi
Industry/Government

Mr. George Ortega

Secrétariat du congrès
CCECE 2002
Dept. Electrical & Computer Eng.
15 Gillson St.
University of Manitoba
Winnipeg, MB R3T 5V6
Phone: (204) 474-8097
Fax: (204) 474-7522
E-Mail: ccece02@ieee.org

Visitez notre site Internet:
ewh.ieee.org/soc/ccece02

Commanditaires:
IEEE Canada
IEEE WCC
IEEE Sections du Winnipeg

IEEE Canada

CCGEI 2002

Congrés Canadien en génie électrique et informatique

Technologie pour le Millénaire

Du 12 au 15 mai, 2002

L'Hôtel Fort Garry, Winnipeg, Manitoba, Canada

La Conférence Canadienne en Génie Électrique et Informatique IEEE 2002 aura lieu à l'hôtel Fort Garry, Winnipeg, Manitoba, du 12 au 15 Mai 2002. Cette

conférence est la plus importante conférence Canadienne dans les domaines du Génie Électrique et Informatique, rassemblant des chercheurs et développeurs d'universités et autres instituts de recherche, aussi bien de l'industrie que du gouvernement.

Dans le passé, cette conférence s'est concentrée sur 3 domaines: communications, puissance et calcul. Le sous-titre de la conférence 2002, "Communication, Puissance et Calcul pour le Nouveau Millénaire" reflète un thème de convergence et interdépendance entre ces domaines qui se retrouvera dans le programme technique.

Les principaux sujets de la conférence incluent:

- Modélisation, Planification et Opération des Systèmes de Puissance
- Électronique de Puissance et Machines
- Informatique et Numérique
- Systèmes Embarqués temps-réel
- Logiciels / Technologie de l'Information
- Calcul Intelligent
- Réseaux de Neurones
- Algorithmes Génétiques, Logique Floue et Logiciels et Calcul
- Reconnaissance de Formes et Analyse d'Images
- Traitement de Signal et Design de Filtres
- Circuits et Systèmes
- Microélectronique et VLSI
- Nanotechnologies et Micromachines
- Communications et Systèmes sans fil
- Électromagnétique et Optique
- Théorie des Antennes, Design et Applications
- Réseaux Informatiques
- Génie Biomédical
- Robotique et Mécatronique
- Contrôle des Procédés / Automatique Industrielle
- Télédétection
- Instrumentation et Capteurs
- Théorie de Contrôle et Applications
- Aérospatiale et Aéronautique
- Applications Industrielles
- Génie de la Sûreté
- Systèmes de Transport Intelligents

La conférence a lieu chaque année, traditionnellement à la mi-Mai, durant trois jours et demi, et comprend 5 sessions parallèles, environ 500 articles, des cours préalables, des séances pleinières, des expositions, et de 400 à 500 participants. Les 3 conférences précédentes étaient organisées par IEEE Alberta (Edmonton, 9-12 Mai 1999), Nouvelle-Écosse (Halifax, 7-10 Mai 2000), et Ontario (Toronto, 13-16 Mai 2001).

Quelques dates importantes de CCECE'02 incluent:

- 7 Décembre 2001 (Soumission de résumés, de sessions spéciales et de cours)
- 15 Janvier 2002 (Notification des résultats)
- 15 Mars 2002 (Version finale des articles et premières inscriptions)

L'hébergement peut être arrangé directement avec l'hôtel Fort Garry (1-800-665-8088) en demandant une réservation de groupe CCECE'02 à prix réduit (code UMENG).

Nous espérons vous voir à la conference CCECE'02 à Winnipeg.

IEEE Canada

CCECE 2002

Canadian Conference on Electrical & Computer Engineering

Technology in the New Mellennium

May 12 to 15, 2002

Hotel Fort Garry, Winnipeg, Manitoba, Canada

The 2002 IEEE Canadian Conference on Electrical and Computer Engineering, CCECE'02, will take place at the Fort Garry Hotel, Winnipeg, Manitoba, May 12 to 15, 2002. This is the most comprehensive Canadian conference in the fields of electrical and computer engineering, bringing together researchers and developers from the universities and other research institutions, as well as industry and governments.

In the past, the conference has focused on three areas: communications, power, and computers. The subtitle for the 2002 conference, "Communications, Power and Computing in the New Millennium" reflects a theme of convergence and interdependence of these areas that will be reflected in the technical program.

The main conference topics include:

- Modelling, Planning and Operation of Power Systems
- Power Electronics and Machines
- Computers and Digital Hardware
- Real-Time Embedded Systems
- Software / Information Technology
- Computational Intelligence
- Neural Networks
- Genetic Algorithms, Fuzzy Logic and Soft Computing
- Pattern Recognition and Image Analysis
- Signal Processing and Filter Design
- Circuits and Systems
- Microelectronics and VLSI
- Nanotechnology and Micromachining
- Communications and Wireless Systems
- Electromagnetics and Optics
- Antenna Theory, Design and Applications
- Computer Networks
- Biomedical Engineering
- Robotics and Mechatronics
- Process Control / Industrial Automation
- Remote Sensing
- Instrumentation and Sensors
- Control Theory and Applications
- Aerospace and Avionics
- Industrial Applications
- Reliability Engineering
- Intelligent Transportation Systems

The conference takes place every year, traditionally in mid May, for three and half days, with five parallel sessions, approximately 500 papers, pre-conference tutorials, plenary speakers, exhibits, and 400 to 500 attendees. The previous three conferences were organized by IEEE Alberta (Edmonton; May 9-12, 1999), Nova Scotia (Halifax; May 7-10, 2000), and Ontario (Toronto; May 13-16, 2001).

Several CCECE'02 important dates include:

- December 7, 2001 (abstracts, special session and tutorial proposals)
- January 15, 2002 (notification of acceptance)
- March 15, 2002 (final papers and early registration)

Accommodation can be arranged directly with the Hotel Fort Garry (1-800-665-8088) by asking for a CCECE'02 discount group reservation (code UMENG).

We are looking forward to seeing you at the CCECE'02 in Winnipeg.

Conference Chair
Dr. Witold Kinsner
University of Manitoba

Tech. Program Chairs
Dr. Doug Chapman
Manitoba Hydro

Dr. Abdel Sebak
University of Manitoba

Treasurer
Dr. Hilmi Turnali
Manitoba Hydro

Secretary
Ms. Grace McCaskill
University of Manitoba

Publications
Dr. Ken Ferens
Norsat, Winnipeg

Publicity Chair
Mr. Jeffrey Anderson
Internet Innov. Centre

Local Arrangements
Mr. Alan Pollard
LSM

Exhibit
Mr. Doug Strang
NRC

Tutorials and Special
Dr. Udaya Annakkage

Student Activities
Dr. Zahra Moussavi
Industry/Government

Mr. George Ortega

Conference Secretariat
CCECE 2002
Dept. Electrical & Computer Eng.
15 Gillson St.
University of Manitoba
Winnipeg, MB R3T 5V6
Phone: (204) 474-8097
Fax: (204) 474-7522
E-Mail: ccece02@ieee.org

Visit our Web Site:
ewh.ieee.org/soc/ccece02

Sponsors:

IEEE Canada
IEEE WCC
IEEE Winnipeg Section