

Enabling Infrastructure as a Service (IaaS) on IP Networks: From Distributed to Virtualized Control Plane

Kim-Khoa Nguyen and Mohamed Cheriet, *École de Technologie Supérieure, University of Quebec*
Mathieu Lemay, *Inocybe Technologies*

ABSTRACT

Infrastructure as a Service (IaaS) is considered a prominent model for IP based service delivery. As grid and cloud computing have become a stringent demand for today's Internet services, IaaS is required for providing services, particularly "private cloud," regardless of physical infrastructure locations. However, enabling IaaS on traditional Internet Service Provider (ISP) network infrastructures is challenging because IaaS requires a high abstraction level of network architectures, protocols, and devices. Network control plane architecture plays therefore an essential role in this transition, particularly with respect to new requirements of scalability, reliability, and flexibility. In this article we review the evolutionary trend of network element control planes from monolithic to distributed architectures according to network growth, and then present a new virtualization oriented architecture that allows infrastructure providers and service providers to achieve service delivery independently and transparently to end users based on virtualized network control planes. As a result, current ISP infrastructures will be able to support new services, such as heavy resource consuming data center applications. We also show how to use network virtualization for providing cloud computing and data center services in a flexible manner on the nationwide CANARIE network infrastructure.

INTRODUCTION

Nowadays, converged communications is considered the main evolutionary stream in the telecommunications industry, allowing underlying infrastructure to run multiple services and accessible over multiple devices. As more services are enabled on communication equipments, the line between software applications and communications applications is blurring. Traditional communications applications such as point-to-point conference or multi-cast are now requirements of business or entertainment software [1].

The aforementioned situation has an important impact on network and software solutions. Architectures of network solutions will be required to

understand the underlying network architectures, devices, and protocols that will be used to access services. Additional frameworks and tools will be required to abstract details of the network environment. Application developers will also need to understand the protocols that will be used within their applications. These requirements will eventually lead to a convergence of network control plane architectures and software solutions.

In addition, the deployment of new services entailed the introduction of new protocols, and link bandwidth has upgraded from megabit to gigabit rates on the Internet. New devices and protocols also increase the number of interfaces in network elements. Additional overhead resulting from more control traffic among an increasing number of peers results in difficulty of scalability, highly availability, and robustness to the control plane. It appears that traditional network elements (e.g. IP routers) with centralized control plane architectures will not be able to meet new control requirements. Distributed control plane (DCP) architectures [2] are emerging solutions and have been widely used in core networks. However, the complexity and flexibility of new services, such as cloud computing and smart grids, impose new challenges on the design of network control plane architectures.

In order to satisfy tremendous demands of resources from new applications, cloud computing is used to power next generation data centers and to enable service providers to lease data center capabilities for deploying applications depending on user requirements. As cloud applications have various configurations, deployment requirements, description and finding, quantifying and allocating resources are essential in order to deliver on-demand services, particularly in large scale systems.

Today, ISPs are faced with an increased competition in the "bit-pipe" [1], a business model based purely on connectivity as a utility, with both lower revenue and lower margins. The bit-pipe model, rather than emphasizing content and services, is driven by operational excellence. Infrastructure consolidation, process automation, and operational outsourcing are key mechanisms to reduce ISPs' operating costs, driven by IP technology. New services, such as cloud computing with a huge number of resources to be managed, have placed the ISPs on the path of a new

control plane evolution from current distributed architectures [3].

We witnessed that virtualization, a new paradigm being explored by the research and education community dealing with highly complex distributed environments, is an emerging technology for next generation network control plane architectures. Regarding current trends of virtualizing practically every aspect of computing (e.g. operating systems, servers, and data centers), it is necessary to have a virtualized network to interconnect all other virtualized appliances to give each of the virtual entities a complete semblance of their counterparts. The main characteristics of a network virtualization technique include:

- A warping of network elements, such as connectivity resources and traffic processing resources.
- Dynamic establishment capability, such as flexible and efficient mechanisms to trigger and tear down service.
- End-to-end across multiple domains.
- Control by the end-user, e.g. the end-user is able to operate the virtual infrastructure as if it was a dedicated physical infrastructure.

This article discusses the need for a transition from current network elements' DCP architectures to network virtualization techniques in order to support new services. The rest of the article is organized as follows. In the next section, we review network control plane architectures and focus on the currently used distributed architecture. We next investigate a paradigm of IaaS based on network virtualization. Network virtualization tools are then presented with a proposed integrated control plane architecture and business and deployment models. A case study shows the deployment of network virtualization to provide cloud computing and data center services in a nationwide network. Finally, we conclude the article and present future work.

NETWORK CONTROL PLANE ARCHITECTURES

One of the key factors that enable the extraordinary growth of the Internet is the evolution of network element architectures. As an essential element of the Internet, the IP router has developed from simplistic packet manipulating software implemented on a general purpose computer to sophisticated network equipment that fully utilizes the capabilities of specialized hardware and integrates a set of functionalities, ranging from raw packet forwarding through traffic shaping, packet queuing, and access control, with connection tracking all the way to distributed network protocols. Lately, it has been proposed to modularize these interspersed functions and organize them into administratively and physically distinct modules, yielding what is called the distributed router. Such distributed routers are expected to improve scalability of IP routers, open up new markets for device vendors, and foster rapid innovation in the area.

CONTROL PLANE EVOLUTION

The first IP networks were made with first generation routers (Fig. 1a) which contain a single central processor (CPU) and multiple interface cards interconnected through a shared bus. The CPU runs a

commodity real-time operating system and implements the functional modules, including the forwarding engine, the queue manager, the traffic manager, and some parts of the network interface, especially Layer 2/Layer 3 processing logic in software. The central CPU capacity is shared among packet forwarding, running routing protocols, updating routing tables, and achieving management functions.

When routers are upgraded to the second generation (Fig. 1b), more intelligence is added to the line cards, with processor, memory, and forwarding caches, allowing them to perform locally some packet forwarding operations. However, control and forwarding planes still remain on the same processing unit.

The third generation routers (Fig. 1c) were introduced with the concept of strict separation of control plane (software based) and data plane (hardware based), allowing the growth of service provider networks. As the shared bus is replaced by a switch fabric, which allows multiple packets to be simultaneously transferred across, data forwarding performance is significantly increased.

DISTRIBUTED CONTROL PLANE ARCHITECTURE

Due to the growing expansion of ISP networks, a network element may have to exchange control messages with hundreds of peers. Such growth in bandwidth, network traffic, and network element density imposes several challenges when designing a network control plane. Particularly, the evolution of traditional communication networks into multi-service networks requires control planes to be highly scalable, reliable and flexible. The monolithic architecture, where software and hardware are intertwined into a single, complex system, has many limitations, which made it difficult to meet new requirements, and which has held back the introduction of new services and applications. For example, a change in one of its subsystems may affect many other subsystems; flexibility and performance are also limited due to its inherent complexity.

Although third generation routers are still used in many of today's core networks, large ISPs are transforming their network equipments into optical based, where the data plane will include optical cross-connects that provide services for the IP layer through MPLS or similar technologies. This results in the development of DCP architectures, which are entirely separated from the data plane (Fig. 2).

A DCP architecture [3, 4] is based on the physical separation between control functions and forwarding functions. Control functions are reduced to the minimum in line cards, such as Hello protocols, neighbor discovery, and switch-over in case of failures. Control elements (CE) and forwarding elements (FE) are interconnected using an internal network, which carries control and data traffic between the elements. The internal network can be designed in various ways, often using high-speed optical network or high performance switches. Such an architecture involves three types of communications: CE-CE, CE-FE, and FE-FE. ForCES [5] was introduced by IETF as a protocol for communications between elements. However, many network operators and equipment providers developed their own version of internal protocols, which seem similar to ForCES with specific features [3]. The separation of control elements from

Due to the growing expansion of ISP networks, a network element may have to exchange control messages with hundreds of peers. Such growth in bandwidth, network traffic, and network element density imposes several challenges when designing a network control plane.

forwarding elements enables the control plane to handle complex tasks such as traffic engineering, QoS, and VPN, in large scale networks. The challenges of a distributed architecture include determining the function to be distributed and the network element that will host that function. Solutions result in two ways of distributing control

plane functionalities: functional and layered distribution [2].

Today, most network operators have upgraded their control planes to distributed architectures, composed of multiple separate elements communicating through open, well-defined interfaces. The control plane and data plane are completely decoupled, running on two different devices, with a 1:N relationship, a control plane handling multiple forwarding planes. Several distributed schemes have been proposed in order to significantly increase scalability, flexibility, and availability [3].

However, regarding the rapid growth of the number of network devices and VPNs needed for new cloud computing services, DCP will unlikely meet new requirements, particularly as it is related to high flexibility. Since the control plane is linked to the data plane by an internal network, handling change is difficult because each change to the physical infrastructure requires a corresponding modification to the control plane, such as reconfiguring the tunable parameters in the routing protocols.

INFRASTRUCTURE AS A SERVICE (IAAS) FOR INTERNET PROVIDERS

The growing utilization of real-time services such as network telephony and video conferencing, has resulted in a higher need for constant connectivity, which requires more scalable management. Infrastructure as a Service (IaaS) has been introduced to meet new management requirements. Offered by Amazon, BlueLock, and other companies as a renting hardware service using proprietary solutions, IaaS scales service delivery as the physical location of the infrastructure can be determined in a flexible way. This is the base of cloud architecture, where complex underlying services remain hidden inside the infrastructure provider. Resources are allocated according to user need, hence the highest utilization and optimization levels can be achieved. During the duration of the service, the user owns and controls the infrastructure as if he was the owner.

From the ISP's perspective, an IaaS solution allows:

Scaling cloud service. Since the network is extensively used in cloud-based services, IaaS allows organizations to build a separate network dedicated to services they provide, given the flexibility and expected easy way of creating virtual infrastructures. IaaS opens new ways of building a backbone, particularly for "private cloud" customers, leading to converge routing capabilities in more centralized locations.

Slicing packet-based infrastructure: If a physical device is sliced into virtual elements, it might be desirable to run different software versions on each slice. This concept, already implemented in computers, is now being deployed in routing systems. The virtualization also allows the upgradability of a software version to be achieved without disruption of services.

Programmable network systems: A trend we observe in the industry is to integrate in the infrastructure new services up to the application level, increasing the value of the network that can be exposed to end-users. It requires more flexible

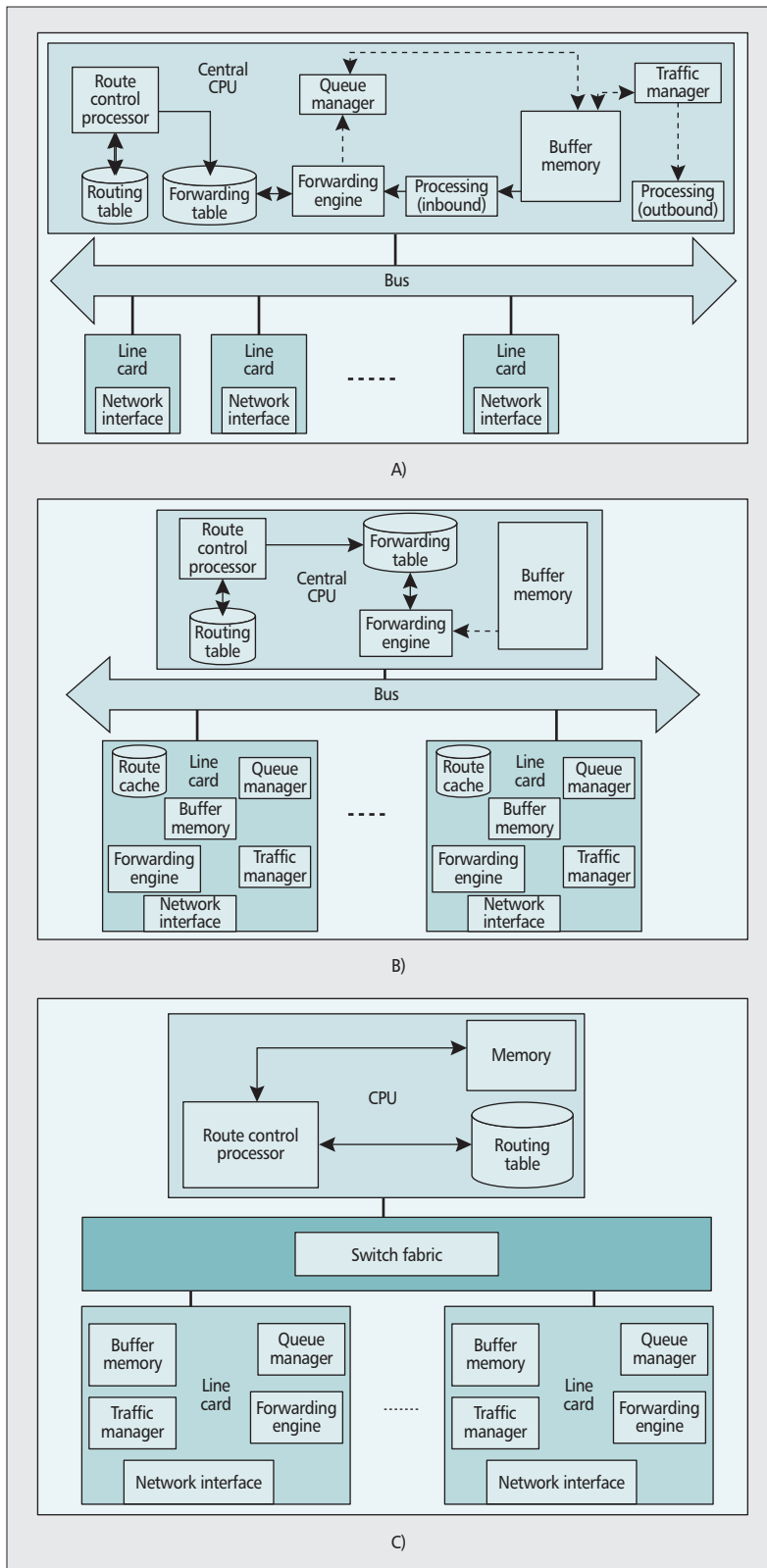


Figure 1. Router generations.

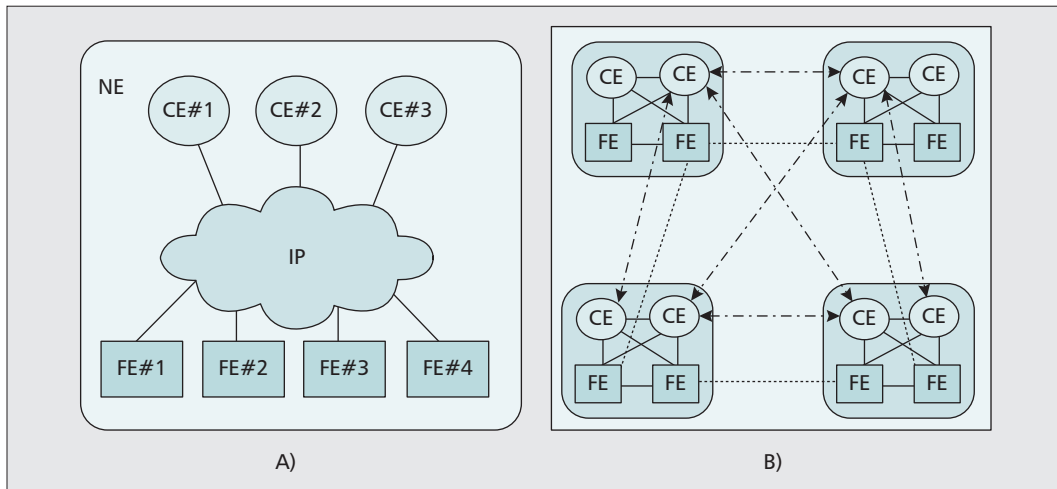


Figure 2. Distributed control plane.

ways of implementing extensions of network device software, facilitating third party development and partnerships. This approach of programmable infrastructure systems, such as via an operating system SDK on routers, or a standard protocol such as OpenFlow [6], will open a new dimension of innovation in communications industry.

Scaling the management and service delivery:

This is undoubtedly the most important concern for ISPs, in particular related to mobility in a multi-domain environment. The service delivery model used by current ISPs, which tightly couples services to the underlying transport network, fails to deliver the flexibility needed by ISPs for service innovations. ISPs need an IaaS framework that deals with service and transport independently. In addition, they want to reduce costs through service automation and streamlining of regulatory compliance.

NETWORK VIRTUALIZATION

The deployment of the IaaS model on current networks requires involving multiple network solutions and architectures and enables multiple networks to function as a whole. The DCP approach, which links control planes to data planes within a network element, is unable to meet this requirement. Virtualization is therefore a natural evolution from DCP architectures, since it allows the coexistence of different network architectures, including legacy systems.

Network virtualization divides traditional Internet Service Providers (ISPs) into two independent entities: Infrastructure Provider, who manages the physical infrastructure, and Service Provider, who creates virtual networks by aggregating resources from multiple infrastructure providers and offers end-to-end services [7]. Each service provider leases resources from one or more infrastructure providers to create virtual networks and deploys customized protocols and services, taking into account performance, topology, and cost of each infrastructure.

A virtual control plane (VCP) contains a network slice formed by virtual instances hosted by the physical networks. As virtualization instances are managed on a different system, the control plane scaling and resource allocation can evolve

considerably and independently of the data plane. Adopting a hybrid optical/packet based approach for the transport layer, the lightpath paradigm is a key technology. However, we have also recognized a trend in the communications industry, away from point-to-point deterministic pipes into the packet based transport infrastructure, such as MPLS over Ethernet. This move, from circuit oriented technologies to packet based technologies, also requires better cooperation between the packet based systems and optical cross connect systems. When the coexistence between these two trends remains, an integrated control solution based on virtualization is needed.

A traditional ISP network will therefore be virtualized as shown in Fig. 3. The Physical layer includes forwarding elements, which can be optical switches or IP routers. Each forwarding element, or a set of forwarding elements of the same kind, is managed by a VCP instance. For IP routers, the VCP contacts the routers' control plane in order to set up entries in routing tables. Networking services are provided to users through the Service layer of VCPs.

The challenges for a virtualization solution include:

- Virtualization of network devices, such as physical equipments from different vendors, routing software, multiple configuration protocols, APIs, etc.
- Virtualization of routing policies, in order to provide users with the ability to express potentially complex requests in a simple way.
- Federation of user-defined autonomous systems, which allows users to create their own IP domains and choose which other IP domains they want to peer with.
- Integrate lower layer resources in a converged management fashion.

A virtual network solution by its nature gives the full advantages of cloud-based systems. Although most known VCP products are still developed in research projects [7, 8], some commercial cloud systems, e.g. Flexiscale [9], are seen having virtual network features allowing users to rent VPNs together with virtual servers regardless of the locations of their physical servers. Nevertheless, large-scale providers, e.g.

The move from circuit oriented technologies to packet based technologies requires better cooperation between the packet based systems and optical cross connect systems. When the coexistence between these two trends remains, an integrated control solution based on virtualization is needed.

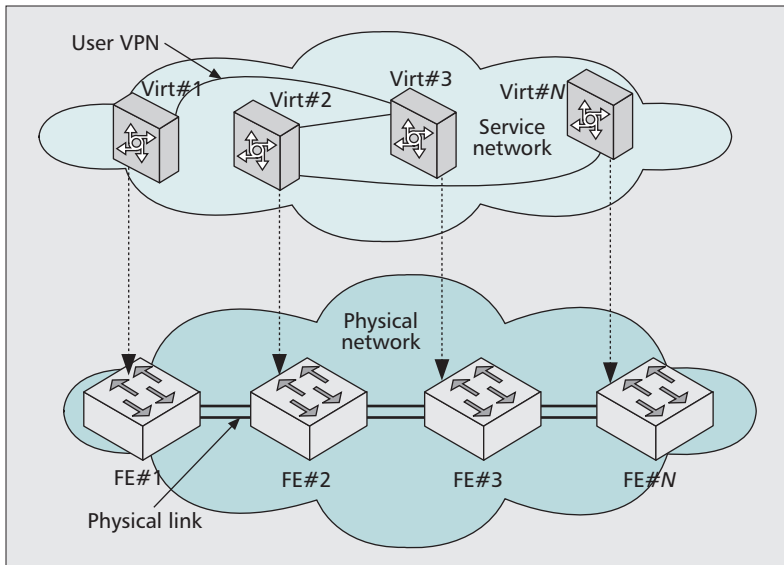


Figure 3. Virtualized control plane network.

Amazon or Google, might still be concerned about performance issues when expanding their services to public utilization. As a result, no network virtualization feature has yet been implemented in their public cloud products. Thus, we believe that for the time being, a virtual network is more appropriate for medium-and-small enterprise customers. Incoming products from hardware providers, such as Juniper Networks' Control System (JSC1200) or Cisco' IOS XR, fully support virtualization features. However, they focus on hardware virtualization of the point of presence (POP), while a cloud-based system needs a more flexible solution at the software level.

In addition, there is a difference between public cloud and private cloud services. Public cloud services, e.g. Amazon EC2, do not allow users to reconfigure their networks of virtual servers because of performance and security issues. However, private cloud services will potentially be provided with virtual network solutions. For example, Amazon Virtual Private Cloud will allow users to have complete control over their virtual networking environment [10].

VIRTUALIZED NETWORK CONTROL PLANE ARCHITECTURE

A VCP architecture for a network element is shown in Fig. 4. It is built on top of network elements (e.g. optical cross-connect) used as the data plane. The proposed architecture has been used to develop a set of VCP software, including UCLP (User-Controlled LightPaths) [11]. The Lookup Service is used to find the different instances of network elements in the network. Network Service Access Point (NSAP) advertises its service instantiation through a well-known process described by an OSGi implementation such as a Web Services Description Language (WSDL) pointer or Universal Description, Discovery and Integration (UDDI) database. When a client application wants to use a NSAP service, it sends user requests to the NSAP using the

Simple Object Access Protocol (SOAP) adopted for Web Services. The requests are then converted into procedure calls within the NSAP which then performs the calls on its local Service Access Point, where commands are executed with the help of the other components within the system. The Traffic Engineering Service implements a set of methods to create end-to-end connections. It supports concatenating, partitioning, receiving requests, and using and releasing paths. There are two types of users. Normal users may invoke a connection request to create a new end-to-end connection, and the administrator may perform administrative functions, such as adding new paths, deleting paths according to changes in the physical layer, and the allocating new resources (i.e. network elements). Finally, the Network Element Service encapsulates the communication protocol required to communicate with the managed network device.

In a traditional networking environment, routing protocols assemble routing tables used to find available resources for routing a new connection through a given network. However, no standard is available for inter-domain routing in optical networks and full knowledge of network topology as normally used for intra-domain routing is not appropriate for customer-managed networking. Therefore, when the control plane is implemented for an optical network, an ad-hoc path searching mechanism can be used based on a static database, which is updated by the Lookup Service.

In order to provide interfaces to upper layers, the NSAP defines management services in the context of Web Services standards, based on XML and SOAP. The XML-based SOAP protocol is used for remote method invocation. There is also a service directory where VCPs can register their list of services specified in terms of XML schemas. Client applications search this directory to find desired services and corresponding VCPs.

Such a VCP can be hosted by a server separately from the network element it manages. This allows the control plane to be implemented using robust software platforms, e.g. J2EE/OSGi.

COMPARISON OF DISTRIBUTED AND VIRTUAL CONTROL PLANE

Regarding the complexity in the management of DCP due to command line interfaces, VCP offers a clear advantage as it allows both end-user and administrator to configure the network through a user-friendly GUI interface with different access levels, thus reducing the risk of errors committed by users. The scalability of the distributed model depends on the capacity of devices, while a VCP running on a dedicated server is able to manage many devices or even multiple networks. This significantly reduces the capital and operational expenditures (CAPEX/OPEX) of network providers. In addition, a DCP based on hardware components is more costly than a VCP, which is software-based.

As VCP is programmable, drivers can easily be added in order to control a wide range of devices and support traffic engineering features, which is inextensible in the DCP model. Similarly, security mechanisms can be implemented in a VCP for authentication, access control, and user

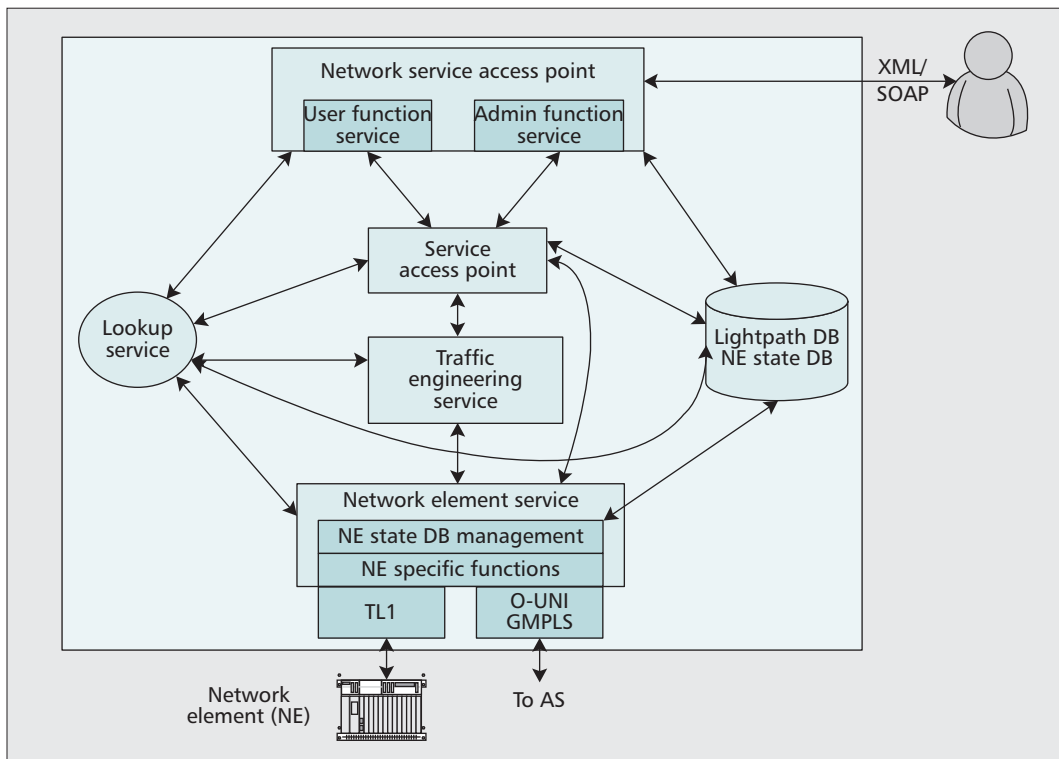


Figure 4. Virtual control plane architecture.

The scalability of the distributed model depends on the capacity of devices, while a VCP running on a dedicated server is able to manage many devices or even multiple networks. This significantly reduces the capital and operational expenditures of network providers.

management, while security features in DCP focus mainly on the protocol level. Another advantage of the virtual control model is that it is by nature very flexible and easily customized.

However, while DCPs have widely been adopted and standardized by many equipment providers, most VCPs are still in the research and finalizing phases. The aforementioned discussions are summarized in Table 1.

SERVICE DELIVERY MODEL

The proposed IaaS service delivery model based on VCPs, as shown in Fig. 5, consists of four layers. The Infrastructure layer includes physical network devices owned by infrastructure providers. These devices are usually linked within provider networks. The Virtualization layer includes servers running VCP software used to control the physical devices, such as setup and tear down on-demand paths. The Bandwidth Broker is also implemented in this layer to enable traffic engineering services. The Service layer provides VCP service capabilities based on IaaS-Framework components [12]. It also authenticates and handles access authorization to VCPs, enforces policy, and generates a usage record. The top Management plane or User level focuses on application services by making use of services provided by the lower-layer services.

In such a model, the Resource Lists Service provides the means of exchanging resources between services providers (SPs). Each SP has a resource list populated with VCPs that represent the physical network elements that the SP can access. The list of SP (A) will be sent to SP (B) when A wants to give B permission to access some of A's resources. B may then assign the network

resources it receives to the network application services that B is deploying. A resource broker site, such as V-Infrastructures [12], can be used to provide SPs with resource listing, defining, browsing, and bargaining functionalities. In a typical system configuration, each SP has a set of services supported by the V-Infrastructure, including web service bundles. Although the sharing of resources among different SPs is enabled, it is important to keep administrative boundaries between SPs to avoid confusion about the ownership of assets and administrative privileges.

EXAMPLE: CLOUD COMPUTING SERVICE PROVISIONING ON CANARIE NETWORK

We now investigate an example of using virtualization techniques for providing cloud computing and data center services on top of a nationwide optical network infrastructure.

Figure 6a shows CANARIE (previously named CA*net 4), a shared network used by all the provincial Optical Regional Advanced Networks (ORANs) across Canada. It links each provincial ORAN by a set of wavelengths that can be shared among them. CANARIE provides 10Gb/s optical lightpaths for research and education through multiple optical cross-connects.

Based on CANARIE infrastructures, the GreenStar Network (GSN) project aims at reducing greenhouse gas emissions (GHG) arising from ICT services [13]. The GSN is made of a set of data centers linked by CANARIE, and connected to the United States, Europe, and Asia Pacific. The data centers are powered

Control	Distributed control plane	Virtual control plane
Management role	Hard and error prone Administrator only	Easy and user friendly with GUI End-user/Administrator
Scalability	Scale with device capacity	Scale with network and server capacity One control plane can manage multiple devices
Price	Expensive, due to hardware components	"Cheap," as software-based component
Traffic engineering/QoS	Limited by operators and device features. QoS is based on routing protocol extensions (e.g., RSVP-TE or NSIS)	Very flexible and easily compatible with a wide range of devices. QoS is based on bandwidth broker and load balancing
Security	Protocol level	Cover from underlying protocol level to application level
Flexibility	Hardware can be changed or upgraded	Very flexible, customizable by end-users
Standardization	Standardized by many equipment providers	No standard has yet been defined

Table 1. A comparison of distributed and virtual control planes.

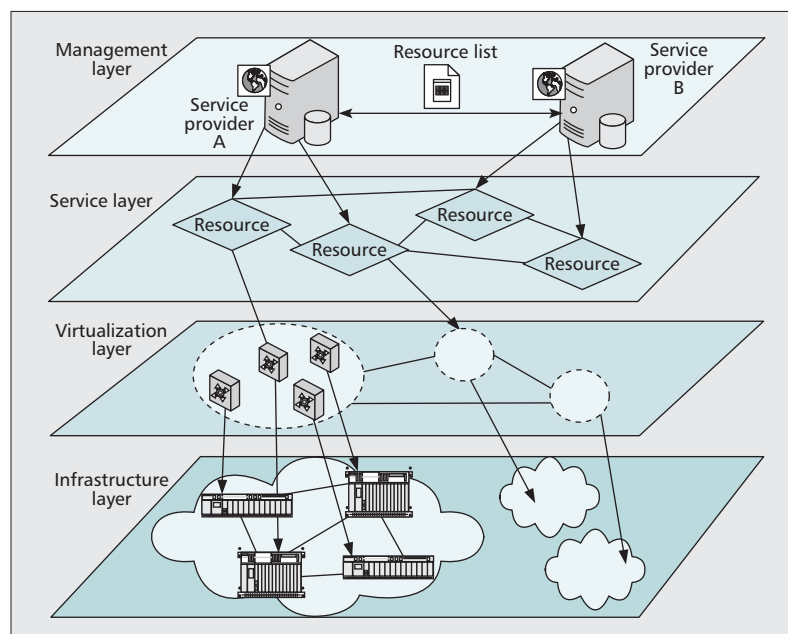


Figure 5. Layers of IaaS service delivery model.

entirely by green energy sources, such as sun, wind, geothermal, and hydroelectricity. The idea behind the GSN project is that a zero carbon network must consist of data centers built in proximity to green power sources, and user applications will be moved to be executed in data centers, assuming that losses incurred in energy transmission over power utility infrastructures are much higher than those caused by data transmission [14]. Such a network must be highly flexible in order to migrate an entire virtual data center (including virtual routers and servers) to alternate locations because green energy sources, like solar and wind, are intermittent. Thus, the key challenge of the GSN is that the network has to move virtual servers around its nodes according to green power availability. Unfortunately, hypervisors (e.g KVM, XEN) running vir-

tual servers can only migrate virtual servers within a flat network. As the GSN spans multiple domains, VPNs must dynamically be reconfigured when a migration is triggered. Without VCPs, this task is very costly in terms of management as migration events are not predictable.

In such a network model, CANARIE is the infrastructure layer. The Virtualization layer consists of VCP software. The Service layer is a middleware we have implemented based on IaaSFramework, which brings services offered by VCPs to GSN users. Each VCP is considered as a resource in the middleware. The Management layer handles user policies of network slices. The Service provider is a GSN operator, and end-users are data center service consumers.

Service delivery is achieved in the GSN by VCPs for network elements at three layers. At the physical layer, we use Argia [8], a commercial version of UCLP [11]. Argia is a VCP that allows end-users (humans or applications) to treat optical cross-connects as software objects, and provision and reconfigure optical lightpaths within a single domain or across multiple, independently managed domains. Users can join or divide lightpaths, as well as hand off control and management of their private sub-networks to other users or organizations. With a focus on optical switches, Argia enables the virtualization of a network element that can be reconfigured by the end-user without any interaction by the optical network manager.

In order to establish Layer 2 VLAN, a network virtualization tool, named Ether [8], is used. Ether is similar in concept to Argia, except that it is designed for LAN environments. With a focus on Ethernet and MPLS networks, Ether allows users to acquire ports on an Enterprise Switch and manage VLANs or MPLS configurations on their own. At the network layer, a VCP created by the MANTICORE project [15] is deployed. MANTICORE is specifically designed for IP networks with an ability to define and configure physical and/or logical IP networks. It allows infrastructure owners to manage their physical as well as logical routers and to enable third parties to control the routers. MANTICORE also provides tools to assist infra-

As the GSN spans multiple domains, VPNs must dynamically be reconfigured when a migration is triggered. Without VCPs, this task is very costly in terms of management as migration events are not predictable.

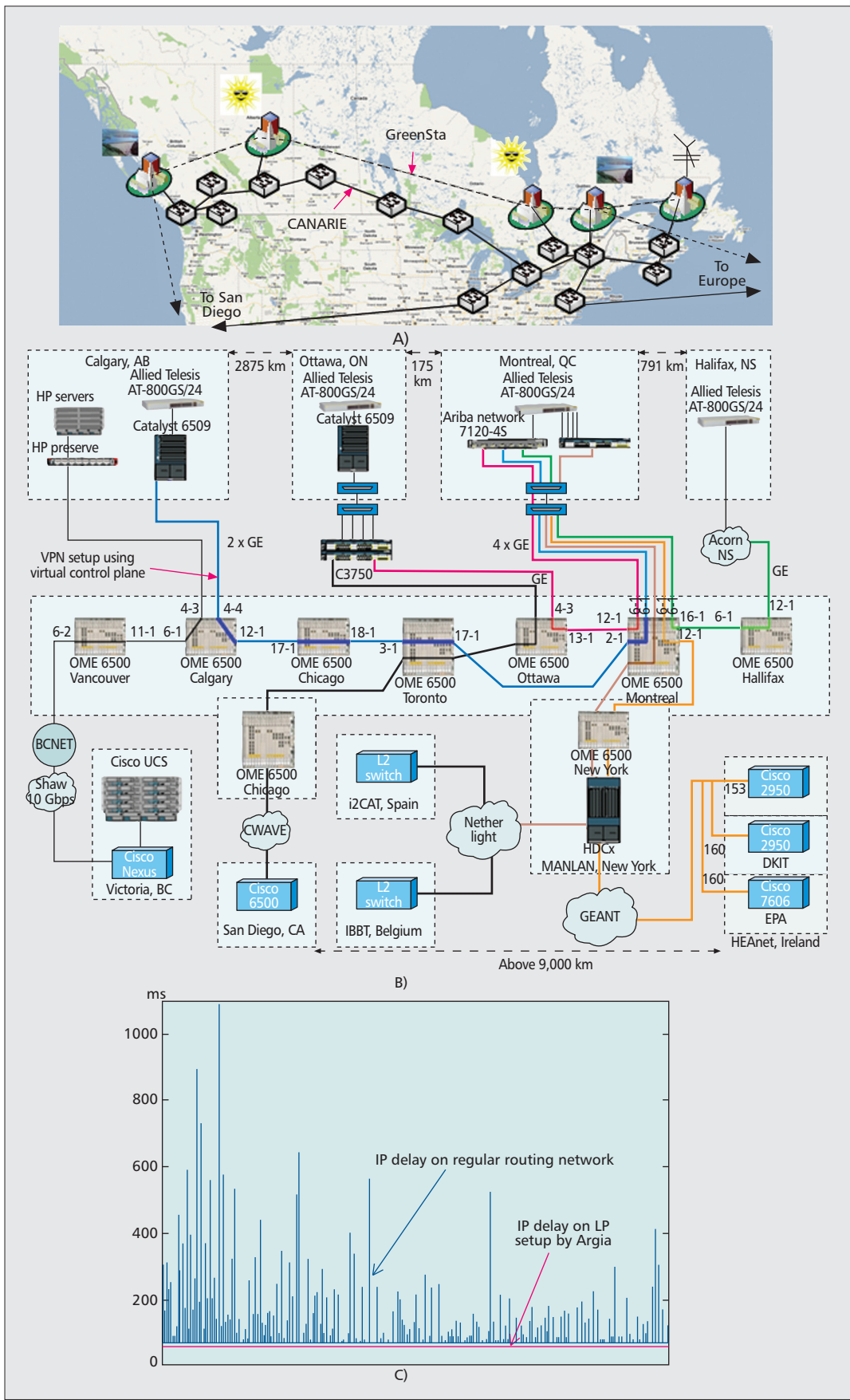


Figure 6. The Green Star Network and traffic characteristics: a) GreenStar Network (Canadian portion) built on top of CANARIE; b) physical connection of the GreenStar Network with VPNs established at 10AM, Feb. 22, 2011; and c) delay (IP traffic) between Montreal and Calgary measured during 24 hours in a regular IP routing network and on a GSN lightpath setup by a Layer 1 virtual control plane.

Distributed control plane architectures are being widely used. However, they are facing issues of scalability and the flexibility requirements of new cloud computing services. Therefore, we believe that network virtualization is a more appropriate solution.

structure users in the creation and management of IP networks using router resources of one or more infrastructure owners.

As shown in Fig. 6b, data centers of the GSN are linked by several types of equipments, including optical cross-connects in the core CANARIE network, Layer 2 switch of local networks, and IP routers. Therefore, reconfiguring and setting up a VPN within such a network is very challenging. In addition, the VPN needs to be flexible, i.e. its topology can be changed dynamically. VCPs allow GSN operators to enable user-controlled traffic engineering. Thus, networks within a single domain or across multiple independent domains can be self-provisioned and dynamically reconfigured. For example, an optical connection is set up as follows. When a path is requested between Montreal and Calgary, as shown in Fig. 6b, resource objects representing ports on each switch are defined. Next, a VCP (i.e. Argia) creates a link object representing an optical connection between two switches. Then a path is allocated. When the path is required on a SONET network (e.g. CANARIE core network), VCP deals with the 10GE WAN PHY protocol. After the 10GE WAN PHY signal is converted to a 10GW LAN PHY signal in Calgary, it goes to the Allied Telesis switch. The path allows virtual servers to be migrated from Calgary to Montreal as on the same LAN environment.

Figure 6c compares the delay of IP traffic between Montreal and Calgary nodes in the GSN when regular IP routing and VCP are used to establish a connection. Data is collected during a period of 24 hours. In the regular IP routing service, data packets going through each intermediate switch need to be processed and sometimes converted by OEO (optical-electrical-optical) modules. This results in high delay that, in peak load periods, does not meet requirements for live migrations. VCP offers a more stable lightpath between two nodes compared to regular IP routing.

As the CANARIE network is composed of multiple federated domains, each domain includes a set of network devices, and VCPs are implemented on each domain to export available Resource Lists. Since the VCPs cover three underlying layers, GSN users get full control of all network elements. Network topology can therefore be reconfigured according to user requirements in a very flexible manner (e.g. changed at least two times a day) in order to move data centers following green power availabilities.

CONCLUSION

Along with the growing demand for new services on the Internet, the network control plane has evolved in ISP networks through many generations. Distributed control plane architectures are being widely used. However, they are facing issues of scalability and the flexibility requirements of new cloud computing services. Therefore, we believe that network virtualization is a more appropriate solution, particularly in cases of very elastic networks as shown in this article. The virtualized control plane architecture we presented has been used in a number of research and educational projects and proven to be a flexible and efficient tool.

Our future work will address evolving such network virtualization tools, driven by the needs of

new complex networks, and implementing advanced optimization techniques for traffic management.

REFERENCES

- [1] A. Cuevas *et al.*, "The IMS Service Platform: A Solution for Next Generation Network Operators to Be More Than Bit Pipes," *IEEE Commun. Mag.*, vol. 44, no. 8, 2006, pp. 75–81.
- [2] K.-K. Nguyen *et al.*, "Towards A Distributed Control Plane Architecture for Next Generation Routers," *Proc. ECUMN'07*, 2007, pp. 173–82.
- [3] K.-K. Nguyen, B. Jaumard, and A. Agarwal, "A Distributed and Scalable Routing Table Manager for Next Generation IP Router," *IEEE Network*, vol. 22, no. 2, Mar. 2008, pp. 6–14.
- [4] Császár *et al.*, "Converging the Evolution of Router Architectures and IP Networks," *IEEE Network Mag.*, vol. 21, no. 4, 2007, pp. 8–14.
- [5] A. Doria *et al.*, "RFC 5810: Forwarding and Control Element Separation (ForCES) Protocol Specification," IETF Draft, IETF — Network Working Group, 2010.
- [6] N. McKeown *et al.*, "OpenFlow: Enabling Innovation in Campus Networks," *ACM SIGCOMM Comp. Commun. Review*, vol. 38, issue 2, 2008, pp. 69–74.
- [7] N. M. Mosharaf Kabir Chowdhury and R. Boutaba, "Network Virtualization: State of the Art and Research Challenges," *IEEE Commun. Mag.*, vol. 47, no. 7, 2009, pp. 20–26.
- [8] S. Figuerola and M. Lemay, "Infrastructure Services for Optical Networks [Invited]," *J. Opt. Commun. and Networking*, vol. 1, no. 2, 2009, pp. A247–A257.
- [9] FlexiScale Inc., "Flexiscale Cloud Computing," <http://www.flexiscale.com>.
- [10] Amazon Inc., "Amazon Virtual Private Cloud (Amazon VPC)," <http://aws.amazon.com/vpc/>.
- [11] E. Grasa *et al.*, "UCLPv2: A Network Virtualization Framework Built on Web Services," *IEEE Commun. Mag.*, vol. 46, no. 3, 2008, pp. 126–34.
- [12] M. Lemay, "An Introduction to IaaS Framework," 8/2008. <http://www.iaasframework.com/>.
- [13] The GreenStar Network Project. <http://greenstarnetwork.com>.
- [14] S. Figuerola *et al.*, "Converged Optical Network Infrastructures in Support of Future Internet and Grid Services Using IaaS to Reduce GHG Emissions," *J. Lightwave Tech.*, vol. 27, no. 12, 2009, pp. 1941–46.
- [15] E. Grasa *et al.*, "The MANTICORE Project: Providing users with a Logical IP Network Service," *Proc. TERENA Net. Conf.*, 5/2008.

BIOGRAPHIES

KIM-KHOA NGUYEN (knguyen@synchronmedia.ca) is a Research Fellow in the Automation Engineering Department at the École de Technologie Supérieure (University of Quebec). He is key architect of the GreenStar Network project and a member of the Synchronmedia Consortium. Since 2008 he has been with the Optimization of Communication Networks Research Laboratory at Concordia University. His research includes green ICT, cloud computing, smart grid, router architectures and wireless networks. He holds a Ph.D. in Electrical and Computer Engineering from Concordia University.

MATHIEU LEMAY holds a degree in electrical engineering from the École de Technologies Supérieure (2005) and a master's in optical networks (2007). He is currently a Ph.D. candidate at the Synchronmedia Consortium of ETS. He is the Founder, President, and CEO of Inocybe Technologies Inc. He is currently involved in Green IT and he is leading the IaaS Framework Open Source initiative. His main research themes are virtualization, network segmentation, service-oriented architectures and distributed systems.

MOHAMED CHERIET is a Full Professor in the Automation Engineering Department at the École de Technologie Supérieure (University of Quebec). He is co-founder of the Laboratory for Imagery, Vision and Artificial Intelligence (LIVIA), and founder and director of the Synchronmedia Consortium since 1998. He serves on the editorial boards of Pattern Recognition (PR), the International Journal of Document Analysis and Recognition (IJRAR), and the International Journal of Pattern Recognition and Artificial Intelligence (IJPRAI). He is a member of IAPR, a senior member of the IEEE and the Founder and Premier Chair of the IEEE Montreal Chapter of Computational Intelligent Systems (CIS).