IEICE TRANS. COMMUN., VOL.E97–B, NO.11 NOVEMBER 2014

INVITED PAPER *Special Section on Network Virtualization, and Fusion Platform of Computing and Networking*

Network Virtualization Idealizations for Applications

Glenn RICART[†a)], ***Nonmember and*** **Akihiro NAKAO**[††], ***Member***

SUMMARY Due to limitations of today's widely-deployed commercial networks, some end-user applications are only possible through, or greatly improved by execution on virtualized networks that have been enhanced or idealized in a way which specifically supports the application. This paper describes US Ignite and the advantages provided to US Ignite end-user applications running on virtual networks which variously: (a) minimize latency, (b) minimize jitter, (c) minimize or eliminate packet drops, (d) optimize branch points for multicast packet duplication, (e) provide isolation for sensitive information flows, and/or (f) bundle network billing with application use. Examples of US Ignite applications in these categories are provided.

key words: *US Ignite, network virtualization, Internet of things, software-defined networking software-defined infrastructure*

1. Introduction

Network virtualization to date predominately has been utilized to solve issues which face network providers including managing link usage, routing around failures, network multi-tenancy, etc. Network virtualization is also valuable to solve issues which face end-user applications. End-user applications which are sensitive to network properties such as latency, jitter, packet dropping, multicast performance, and flowspace isolation are most efficiently executed upon a virtual network which manifests these network properties on behalf of the application in a way which provides a virtual network tuned to or customized to that specific application. Since this is done in software, the customized virtual network and any supporting compute or storage components is sometimes collectively referred to as software-defined infrastructure.

2. Virtualization and Idealization

Virtualization has a long history of being used to idealize a resource. Virtual memory could have a much larger capacity than the underlying physical memory. And the virtual memory hardware could provide separate and isolated address spaces for each application. Virtualized CPUs often could execute instructions never physically present using software emulation. In many virtualization environments, virtual servers could have their "hardware" augmented via software command, and in many cases while they were in full operation. Virtual disks could have larger capacities than the corresponding physical disks, and/or have higher throughput (through striping) and/or have higher reliability (through redundant recording of data on multiple disks).

All of these have analogs in the virtualized network world. In many cases, the capabilities have been available to physical networks via manual and static network configuration.

- Additional capacity can be obtained by load-sharing (or load-balancing) across multiple links
- Separate address spaces and multi-tenancy could be provided for disjoint networks, or by using VLANs or by configuring tunnels
- High priority flows recognizable to the switches could be programmed to have priority processing

All of the above can be realized just as easily and be more dynamically managed using network virtualization layers that implement these strategies within the virtualization layer.

But there are also additional capabilities possible in virtualization.

- Software-defined networking controllers can examine the entire global networking state and make direct optimizations to improve flows on an end-to-end basis.
- Cross-layer communication can be made explicit to reduce adaptation time and optimize outcomes.
- Reliability controllers can add both additional forward error correction and also add duplicated or check-sum-like packets over alternate paths to provide RAID-like reliability.

This paper will discuss US Ignite and network virtualization idealization techniques central to a new class of end-user applications being encouraged by US Ignite.

3. Internet Shortcomings

The Internet has been a wondrous success in the variety and scale of applications it has been able to support. However, it's not true that every possible application can easily be run on today's commercially-available Internet. Sometimes the capability is not present in a meaningful way. In other cases, it is theoretically possible, but carriers are not providing it due to the difficulty in implementation or the perceived lack of viable applications that need the capability.

Manuscript received July 8, 2014.

[†]The author is with US Ignite, Washington, DC 20036, USA.
[††]The author is with The University of Tokyo, Tokyo, 113-8654 Japan.
a) E-mail: glenn.ricart@us-ignite.org

DOI: 10.1587/transcom.E97.B.2252

The most fundamental is the Internet Protocol's inherent notion of dropping packets to indicate congestion. A higher layer protocol, TCP, overcomes the dropped packets by re-transmitting them and by scaling back the rate of transmission. While effective, this fundamental building block introduces variable and uncertain delays in transmission. For most applications, like web page applications, this delay is acceptable. However, for real-time applications, augmented reality, or closed control-loops, this delay can go from mildly irritating to unacceptable.

In addition, today's commercial Internet has multiple cooperating carriers whose interconnecting routing topologies are driven more by inter-carrier agreements and policies than any kind of designed backbone strategy. It's a testament to the Internet that these collections of networks effectively interconnect any two endpoints. In the meantime, any given packet may have to navigate a multi-dozen number of hops to get to its destination. Needless to say, network performance depends entirely on the sizes and latencies of the paths selected. For latency and bandwidth insensitive applications such as informational web pages, these issues are relatively unimportant. But for high performance applications such as those frequently used at the University of Tokyo and at US Ignite, special high-performance networks like JGN-X and Internet2 have been put in place to bypass the limitations of the commercial networks.

An area of considerable interest is video conferencing because it has the possibility of reducing the environmental impact of travel. The marketplace for videoconferencing software has come to be dominated by companies that have found ways of producing "acceptable" video quality in the face of packet drops, high jitter, etc. The price paid is often delay in the video. Redundant video information is sent in multiple packets to avoid having to re-transmit any one missed packet. However, the video cannot be displayed until all of the subsequent packets have been received. This adds delay. Variable packet arrival times require the use of a large jitter buffer. That also adds delay. So, the acceptable video comes at the cost of what is often multi-hundred millisecond delays and the consequent awkwardness of multiple people replying at once because they can't tell that others also have begun talking.

In short, today's typical commercial Internet has bandwidth limitations (and sometimes even bandwidth caps), variable and often high latency, high amounts of jitter, and unpredictable packet drops. While it's true that upper layer protocols compensate for some of these deficits, the price is often significant delays which can be costly to certain applications.

Many applications to be described later cannot tolerate the current Internet shortcomings.

4. US Ignite

The US Ignite Partnership [1] is a public-private nonprofit venture to encourage and coordinate efforts toward developing and deploying applications and services for ultra-fast broadband and software-defined networks that have the potential to transform areas of international priority such as advanced manufacturing, clean energy (including advanced vehicle technologies), education and workforce technologies, emergency preparedness and public safety, and health information technologies (Fig. 1).

Fig. 1 Public private partnership.

The public sector has a significant interest in the possibility of new applications and services addressing these areas. In addition, U.S. federal agencies such as the National Science Foundation and Japanese national agencies such as the National Institute of Information and Communications Technologies (NICT) have an interest in bringing promising new technologies out of the research laboratory and into public service. There is also a public interest in the economic growth that investment in the new technologies and their applications will bring.

The private sector has a significant interest as well in the new markets that such technologies and applications will open. Forward-looking companies will want to establish their credentials by being able to serve these markets and their new revenue opportunities. Since the opportunity is so new, it makes sense for the first several years to have close collaboration between the public and private sectors to better define the technologies and their applications.

Foundations are interested in pursuing their missions, and there are two strong reasons for foundations to join the US Ignite Partnership. First, they may share an interest in the public benefit applications the US Ignite Partnership will stimulate and help disseminate. Second, they may want to encourage the economic development that will arise around new business and government activities enabled by the new applications and technologies, sometimes in a specific geographic area.

US Ignite focuses on encouraging and coordinating efforts aimed at applications and services enabled by the new technologies. This is in contrast to other complementary efforts intended to deploy the new technologies. The US Ignite partnership believes it will be more scalable to "pull" the new infrastructure using compelling new applications than to "push" new infrastructure into place and hope that the applications will then happen. But both approaches are valid and complementary. The US Ignite Partnership will help attract and coordinate the "pull" efforts based on applications (Fig. 2).

Fig. 2 US ignite partners.

US Ignite is collaborating with NEC, NTT, and the University of Tokyo to coordinate US and Japanese efforts to promote these new applications.

The National Science Foundation is the lead federal agency in the United States and has a continuously open call for proposals that will support the US Ignite mission. This open call has been renewed in August of past years, and the current call is NSF 13-121 [2].

US Ignite annually sponsors an open Applications Summit at which new applications are demonstrated. The most recent Summit was held in Silicon Valley June 24-27, 2014 and examples in this paper are largely taken from demonstrations given at the Summit [3].

US Ignite also allies itself with testbed cities or communities with advanced networking capabilities. Thirty-one cities or communities are currently allied with US Ignite, and they are committed to develop applications and deploying US Ignite applications in their communities.

5. End-User Application Idealizations

In this section, we examine a number of idealizations possible with virtualization that enable various US Ignite applications.

5.1 Minimize Latency

Some latency is inherent in the speed of light in fiber optics and, if Albert Einstein is correct, cannot be reduced except by moving the source and destination physically closer to each other.

However, most Internet applications encounter far higher latency from potentially controllable sources.

- Carrier interconnect points are often chosen based on policy, cost, and sometimes limitations in the Border Gateway Protocol (BGP) [4] instead of minimal latency.
- Routes in use often have more routers in the path than necessary. Each router in the path requires packets to be received, examined, and queued for re-transmission, adding to latency.
- Congestion can leave packets sitting in router queues awaiting their turn.
- When servers and routers are implemented in individual boxes, there is additional latency from sending packets from the router to the server to the router.
- WiFi links can add significant latency when they detect a collision and "back off" or wait before attempting a retransmission. Tens to hundreds of milliseconds can be added in retransmission in crowded WiFi environments.
- When end-user Internet access is limited by clock rate to the user (common in DSL situations), latency is added in last-link packet transmission time. For example, a 1 Mbps last-mile link introduces a 12 millisecond delay on a 1500 byte packet even before speed of light considerations.
- Deep packet inspection, when implemented by carriers, requires the entire packet to be completely received and to undergo computationally-intensive analysis before being released for retransmission.

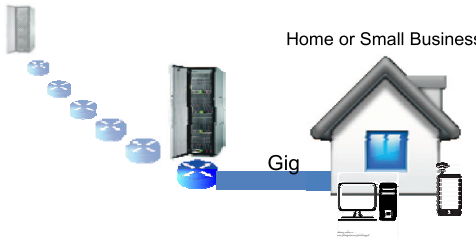

Fig. 3 Low latency architecture.

Virtualized networks can be implemented using specific techniques to reduce these delays. Virtual networks implemented by software-defined networking can use controllers to observe global state and choose paths which:

- are physically shorter (to minimize speed of light delays)
- have fewer hops (to minimize router delays)
- operate over less congested links (to minimize queuing delays)
- give latency-sensitive flows priority treatment
- reduce the variance in transit times

In addition, US Ignite applications try to avoid low-speed links which can add latency and often operate in cities where gigabit last-mile links are available (Fig. 3).

In congested WiFi areas, the ARCCN in Russia has developed Chandelle, a technique for coordinating WiFi access points to reduce latency [5].

The approach of the Nakao lab to combine server and router (FLARE [6]) eliminates router-to-server-to-router latency.

The sum of these actions is that latency can be substantially reduced.

Many US Ignite applications that depend on reduced

latency were demonstrated at the 2014 US Ignite Applications Summit and included the following:

Dr. Cruz performed simulated orthopedic surgery between surgeons in El Paso, Texas, and Sunnyvale, California, using a simulator provided at the University of Wisconsin. The scenario for the surgery was for an unusual operation for which the experienced surgeon is remote. Low latency was required to allow the surgeons to accurately move remote virtual instruments and conduct the virtual surgery successfully. A track record of success in virtual surgery should lead the way to actual physical remote surgery.

The FITNET Health Application showed simultaneous exercise routines between participants in Blacksburg, Virginia and Sunnyvale California. Gigabit wireless (802.11ac) was used in both locations to provide low last-mile latency while allowing the participants to see and watch each other. This simulates an exercise studio environment in which exercise is a social affair and participants can see each other and compare their performance but without having the travel time and cost to an exercise studio.

In both of these situations, a software-defined network was created over Internet2's Advanced Layer 2 Service (AL2S) [7] which minimized hops and delays. A special circuit was run to the Application Summit facility (the Juniper Aspiration Dome) to avoid a clump of local routers. The result was the ability to do human-mediated tasks in apparent simultaneity over thousands of kilometers.

Children's Mercy Hospital demonstrated effective telemedicine using multiple-location broadcast-quality graphics composited and sent in real-time over gigabit-speed networks. Low latency makes the telemedicine seem natural and to come alive. SightDeck technology [8] was used for the video compositing.

A Distributed Virtual Worlds demonstration showed the ability of kids across the country to collaborate on the task of fixing a broken Mars rover. In addition to a shared simulation environment, the kids had video and audio interconnects that allowed them to work together in real-time. Such real-time distributed (multi-location) virtual world simulations can be constructed to give students experience and expertise in handling situations, and giving them a safe space in which to try out new approaches and techniques as well as reinforcing successful behaviors. Officials at the US Department of Education have also suggested it should be useful for educational assessment. This virtual worlds approach is the same one famously used for training pilots in flight simulators. The networks we need to support educational flight simulators are low-latency virtual networks.

Health-E-Me is a virtual video conference service providing 24/7 telehealth-psychological services with high resolution-low latency live video. Psychological services require very high resolution video in order to catch small and fleeting facial movements that give the psychologist insight into the patient and the context of what they are discussing.

In Visualizing Virtualized Networks, Cisco developed a US Ignite demo that is a mash-up of the Virtual Internet Routing Lab (VIRL) platform and Oculus Rift VR, so that you're able to create a network simulation of VMs running Cisco operating systems and then 'walk among/fly over' your simulated network. Low latency is required to provide an accurate sense of movement and real-time activity in the visualized network and show you the actual results of any changes you make to the simulated virtual network. This is a case of a low-latency virtual network aiding in the visualization of another virtual network.

The Gigabots project uses a distributed set of robots communicating with one another to share information and act collectively. Something sensed by one robot can cause different robots, some perhaps hundreds of kilometers away, to react to that knowledge. In one simple demonstration at the Summit, people interacting with a robot in Kansas City saw the reaction by a robot in Sunnyvale, California.

When there is a tight feedback control loop between stimuli and action which involves the real world, we have a cyberphysical system. Cyberphysical systems usually operate best with minimum latency so that they react immediately to changes in their surroundings. For example, Montgomery County, Maryland demonstrated their SCALE (Safe Community ALErt) network prototype [9] which relayed emergency smoke and fire conditions directly to county emergency management facilities and prompted coordinated alarms and responses.

Cyberphysical systems are expected to play a large role in the Internet of Things, and US Ignite-style networks will be important to support the Internet of Things.

5.2 Minimize Jitter

Jitter is the variation in inter-arrival times for packets. For example, for smooth video, you can't just display each frame when it arrives. If you did so, the jitter would result in jerky playback.

To overcome jitter, the universal solution is a jitter buffer which delays all packets by the maximum expected amount of jitter so that playback is smooth. For watching one-way video of movies or sports events, the jitter buffer delay may not be noticeable. But for interactive activities and especially video-mediated human-to-human interactions, the jitter buffer causes significant awkwardness in multi-party video situations.

Many of the techniques used to minimize jitter are very similar to those used to minimize latency. However, in addition, all sources, sinks, and intermediate routers can be given to understand that packets should be generated and received at predictable times (like clockwork) and should be handled in a consistent amount of time and dispatched on schedule (like clockwork). If there are intermediate routers which have limited capacity, slightly delaying one of the initial packets can often affect the entire stream in such a way that the routers and packet streams adjust to one another and drive jitter toward zero.

In return, the applications need to reduce their jitter buffers accordingly. US Ignite is working with the

WEBRTC project to substantially reduce jitter buffers when WEBRTC video is used over groomed links set up as part of US Ignite. Standardization is being pursued by the Internet Engineering Task Force [10].

5.3 Minimize or Eliminate Packet Drops

One of the most destructive but natural behaviors of the Internet is to drop packets under congestion. In days past, dropped packets indicated congestion and helped to give applications fair shares of the available capacity. But today, there are many reasons for dropped packets besides congestion, and dropped packets wreak havoc with the kinds of US Ignite applications already discussed.

Traditional IP routers use dropped packets to try to control application traffic to fit their capabilities. In SDN and virtual networks, the reverse approach is used. Applications control the creation of virtual networks to meet their needs.

If network capacity is exceeded, new virtual networks which require unavailable capacity are told in advance that they cannot be handled with the quality they expect. As a fallback, they can request a lower level of service that still may be available. Conversely, pre-emption can be used to stop a lower priority application if there is urgent need for the surgical application, for example.

Note that optimizing latency may result in different routes than optimizing for available bandwidth. In addition, if cost is a consideration, yet other routes may be optimal. In general, the multi-application optimization is a multivariate linear programming problem (assuming there are linear benefit/cost functions).

US Ignite is currently moving away from the use of routers and their habit of dropping packets in favor of software-defined networking layer 2 OpenFlow [11] switches operating over the least congested infrastructure available. In Kansas City and Chattanooga, for example, gigabit metro networks minimize congestion in the city and regional research and education networks and Internet2 layer 2 switching minimizes any packet drops over the longer haul circuits.

The ubiquitous use of layer 2 OpenFlow switching under SDN control is critical to minimize packet drops. Traditional routers are avoided.

However, if true reliability and very-high probability of packet delivery are needed, US Ignite applications show some pathways for further solutions. Douglas Comer and George Adams have a US Ignite funded project for *Reliable Packet Delivery with Open Flow for Advanced Manufacturing and More*. They are developing techniques for an SDN controller to find N diverse paths through a network and duplicate critical packets over all paths. A redundancy controller duplicates the packets and checks-in all received packets to make sure all have eventually arrived. If any given path stops delivering packets, the controller attempts to find a replacement diverse path to maintain the redundancy. A side effect of this ultra-high-reliability approach is that the first packet to arrive can be delivered with a lower average latency and lower average jitter than any single path, in agreement with queuing theory.

The US Ignite application demonstrated at the 2014 Application Summit involved the control of a remote 3D printer which must lay down continuous material and which cannot be paused for packet re-transmissions. Real-time control of the remote printer simplifies policy considerations which can be enforced by the network server such as prohibitions against printing out forbidden objects and accurate billing for use.

5.4 Optimize Branch Points for Multicast Packet Duplication

Some distributed collaborative applications want to share state or video with as low latency as possible to support collaborative efforts. Traditionally this is handled with a Multipoint Control Unit (MCU). However, sending all packets to an MCU and then out to the other parties introduces hundreds of milliseconds of latency, making the application less valuable.

Marvin Schwartz of Cleveland's OneCommunity has pointed out that each of a total of N cooperating sites is sending (N-1) streams to the other cooperating sites. If each of those streams is handled as an independent OpenFlow SDN stream, its path through the network can be latency and jitter optimized as discussed above. Furthermore, OpenFlow includes a native operator to duplicate packets. This permits each site to send a single copy of their state or video and have it duplicated at the optimal point in the network to minimize backbone traffic and avoid traffic on heavily-used links.

In this way, virtual networks can provide an idealization of multicast that doesn't require the execution of the IETF Multicast [12] algorithms and the class D group addresses which must be handled by intervening routers. Another reason to avoid IETF multicast is that the capability if often disabled in production routers due to its potential impact on router performance.

The OpenFlow-based multicast can provide a virtual network idealization tuned to the application requirements and which can be executed in inexpensive and fast OpenFlow switches with nearly zero additional packet forwarding complication.

The National Science Foundation has funded OneCommunity to develop a virtualized network implementation of multipoint low latency video with layer 2 packet forwarding and duplication. We are expecting to see a demonstration of this technology at the 2015 US Ignite Application Summit.

5.5 Isolation for Sensitive Flows

Virtual networks are widely used in datacenters for multitenancy isolation. There are many end-user applications that also are receiving benefits from isolation including those which process sensitive financial or public safety or medical information.

Although isolation does not provide ironclad security by itself, it can provide a significant layer of protection against:

- Man-in-the-middle attacks where an attacker pretends to be the legitimate collaborator or server
- DNS attacks which re-direct intended traffic to a sham or simply disrupt legitimate traffic
- Distributed denial of service attacks attempting to overwhelm a publicly available network server or node
- Impersonation attacks in which a malicious code impersonates a legitimate collaborator
- Scanning attacks which are looking for open ports which may lead an attacker to valuable information

In all of these cases, the use of a virtual network in a separate addressing space provides isolation protection against these attacks. The attacker literally cannot address or force packets onto the sensitive virtual network if the layer 2 switches are working correctly and there are no mistakes in the forwarding rules.

An existence proof of the assumptions in the previous paragraph is being conducted by Internet2 with its Flowspace Firewall [13]. The Flowspace Firewall checks OpenFlow commands to make sure they only affect packets in the correct virtual network and keep those packets in the same virtual network.

At the US Ignite Application Summit in June of 2014, there were three demonstrations of virtualizations for isolation and protection.

Idaho State University in conjunction with the city of Ammon, Idaho and Albion Telephone Company and Entrey-Point Systems showed a virtualization of the last mile service provider network to the home. At the home, a carrier-provided device split out multiple virtual networks. Similarly, in Chattanooga, Tennessee, VLANs are used for layer 2 separation of multiple data paths to the home.

At the end-user's home, both Suman Banerjee of the University of Wisconsin and Nick Feamster of Georgia Tech have devised SDN-capable home routers that also act as access points. Both are capable of using SDN to create multiple virtual networks in the home and connecting them to carrier virtual networks.

In the case of the Banerjee project called Paradrop [14], Linux containers [15] are used to contain the on-board compute and storage apps which are specific to a virtual network.

At the University of Utah, Jacobus van der Merwe has a US Ignite grant from the National Science Foundation to develop a containerized Linux and Android add-in which securely links sandboxes/containers in mobile devices to virtual networks for sensitive information. The US Ignite use case is mobile secure access to medical records. Linked virtual networks provide the security and isolation desired. Van der Merwe provided a demonstration of the Linux version at the 2014 US Ignite Applications Summit.

5.6 Bundle Network Billing with Application Use

Carriers typically receive a flat rate for providing a physical network channel with certain characteristics. End-users can fill the channel generally as desired, although some carriers are imposing usage caps above which there are extra charges. Commercial users may be billed at the 95% percentile of usage.

US Ignite applications are, by definition, those which don't run well on a shared physical network. Instead, the idealizations of network virtualization enable them. Since the services required can be provided on a per-virtual-network basis, the carrier can also bill on the basis of the virtual network.

In the US Ignite model, applications requiring these virtual network capabilities instantiate a virtual network designed to provide the characteristics they require on an as-needed basis. This allows for a simple billing mechanism by the carrier — billing per virtual network — that can be incorporated by the application into an overall application use charge.

Therefore, we would expect that use of certain US Ignite applications will carry charges that might include the use of an appropriate virtual network. Other models are possible, but bundling the entire required infrastructure into the application cost would seem to be attractive to both users and providers. Users would appreciate a single all-in price, and providers would appreciate incremental revenue streams depending upon scope and use. The result should be more attractive US Ignite applications and incentives for providers to support them.

6. Virtualization Elegance

Many knowledgeable readers will note correctly that many of the capabilities of idealized virtual networks could also have been provided by techniques that can be programmed into IP routers today. Why do we need idealized virtualizations for applications?

The same can be said for Software-defined Networks. It's hard to find things that SDN networks can do that could not have been managed in some way, shape, or fashion by today's networking techniques. After all, latency-sensitive apps like Voice over IP (VoIP) have been conquered by specific ad hoc programming on vendor switches and IETF standards approved.

Our response is in four parts:

1. Configurating the corresponding IP network capabilities is too static and can't be feasibly done for many of the US Ignite applications. Static things like VoIP telephone ports can be statically configured, but many applications want to be instantiated as needed.
2. The virtualized idealization provides a much simpler and more elegant solution. The complexity is hidden from the application writer and end-user.

3. The costs for hardware and software for SDN-implemented layer 2 virtualized networks are often much lower than for the complex IP-based hardware needed for physical network solutions.
4. Virtualization solutions using SDN can be more vendor independent allowing for wider use across multi-vendor and heterogeneous networks.

7. Conclusion

Due to limitations of the currently available commercial Internet, it is attractive for a new class of applications to use idealized capabilities of virtual networks.

This adds new constituencies to the groups interested in virtual networks — applications writers and end-users. Their goals are generally to gain access to a network which is more in-line with their application and to do so simply and without complex network configuration.

Japan and the United States are two of the countries doing the most work on network virtualization. We can learn much from the work on server and storage virtualization.

However, there remain special challenges to network virtualization, and our work there should be guided by not only the needs of carriers but also those of the next generation of end-user applications that will usher in the next transformative chapter of the Internet.

Acknowledgments

Much of the work described has been performed by the principal investigators of US Ignite and related projects. We'd also like to thank the staff and investigators of US Ignite and Nakao Labs.

References

[1] US Ignite official web page, http://www.us-ignite.org, accessed on 6 July 2014.
[2] NSF US Ignite Dear Colleague Letter, http://www.nsf.gov/pubs/2013/nsf13121/nsf13121.jsp?WT.mc_id=USNSF_25&WT.mc_ev=click, accessed on 6 July 2014.
[3] US Ignite Applications Summit, http://us-ignite.org/applicationsummit, accessed on 6 July 2014.
[4] Y. Rekhter, T. Li, and S. Hares, "RFC 4271," Internet Engineering Task Force, http://www.rfc-editor.org/rfc/rfc4271.txt, access on 6 July 2014.
[5] S. Monin, A. Shalimov, and R. Smeliansky, "Chandelle: Smooth and fast WiFi roaming with SDN/OpenFlow," A Poster Presented at the US Ignite 2014 Applications Summit, June 2014.
[6] A. Nakao, "FLARE: Open deeply programmable switch," 16th GENI Engineering Conference, 2012.
[7] Internet2, "Advanced layer 2 services," http://www.internet2.edu/products-services/advanced-networking/layer-2-services/, accessed 6 July 2014.
[8] SightDeck, Information page at http://sightdeckkc.com/, accessed 6 July 2014.
[9] Montgomery County, Maryland, "SCALE — Safe community alert network," http://smartamerica.org/teams/scale-safe-community-alert-network-a-k-a-public-safety-for-smart-communities/, accessed on 6 July 2014.
[10] Internet Engineering Task Force, "RTCWEB," https://datatracker.ietf.org/wg/rtcweb/documents/, accessed on 6 July 2014.
[11] Open Networking Foundation, "OpenFlow," https://www.opennetworking.org/sdn-resources/onf-specifications/openflow, accessed 6 July 2014.
[12] Wikipedia, "Multicast," http://en.wikipedia.org/wiki/Multicast, accessed on 6 July 2014.
[13] GlobalNOC, "Flowspace Firewall," http://globalnoc.iu.edu/sdn/fsfw.html, accessed 6 July 2014.
[14] S. Banerjee, "Paradrop," http://www.paradrop.org/, accessed on 6 July 2014.
[15] Linux container community, "LXC- Linux Containers," https://linuxcontainers.org/, accessed 6 July 2014.

Glenn Ricart is founder and CTO of US Ignite, a US public-private partnership whose goal is to show that the next generation of the Internet will enable transformative applications in public benefit areas such as education, healthcare, public safety, transportation, advanced manufacturing, and clean energy. Dr. Ricart has also been recognized for his early work on the Internet and inducted into the Internet Hall of Fame Pioneer's Circle.

Akihiro Nakao received B.S. (1991) in Physics, M.E. (1994) in Information Engineering from the University of Tokyo. He was at IBM Yamato Laboratory, Tokyo Research Laboratory, and IBM Texas Austin from 1994 till 2005. He received M.S. (2001) and Ph.D. (2005) in Computer Science from Princeton University. He has been teaching as an associate professor (2005–2014) and as a professor (2014-present) in Applied Computer Science, at Interfaculty Initiative in Information Studies, Graduate School of Interdisciplinary Information Studies, The University of Tokyo.