OPERATIONALIZING SOFTWARE-DEFINED NETWORKS

Summary of Large Scale Networking Workshop September 18-20, 2017

Report of the

LARGE SCALE NETWORKING INTERAGENCY WORKING GROUP

NETWORKING & INFORMATION TECHNOLOGY
RESEARCH & DEVELOPMENT SUBCOMMITTEE

COMMITTEE ON SCIENCE & TECHNOLOGY ENTERPRISE

of the

NATIONAL SCIENCE & TECHNOLOGY COUNCIL

SEPTEMBER 2018

About the National Science and Technology Council

The National Science and Technology Council (NSTC) is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the Federal research and development enterprise. A primary objective of the NSTC is to ensure science and technology policy decisions and programs are consistent with the President's stated goals. The NSTC prepares research and development strategies that are coordinated across Federal agencies aimed at accomplishing multiple national goals. The work of the NSTC is organized under committees that oversee subcommittees and working groups focused on different aspects of science and technology. More information is available at http://www.whitehouse.gov/ostp/nstc.

About the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 to provide the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics. OSTP leads interagency science and technology policy coordination efforts, assists the Office of Management and Budget with an annual review and analysis of Federal research and development in budgets, and serves as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government. More information is available at https://www.whitehouse.gov/ostp.

About the Large Scale Networking Interagency Working Group

The Large Scale Networking (LSN) Interagency Working Group (IWG) coordinates Federal R&D in leading-edge networking technologies, services, and enhanced performance under the auspices of the Networking and Information Technology Research and Development (NITRD) Subcommittee of the NSTC's Committee on Science and Technology Enterprise. The advanced Federal research network infrastructure supports national security, commercial industry, and scientific research, and enables the robust transfer of data from systems on the ground, on the sea, in the air, and in space. This coordinated R&D aims to ensure that the next generation of the Internet will be scalable, flexible, and trustworthy. More information is available at https://www.nitrd.gov/groups/lsn.

Acknowledgments

This workshop report was developed through the contributions of the workshop committee represented by members from government, industry, and academia, NITRD Federal agency representatives and members of the LSN IWG, and the staff of the NITRD National Coordination Office. Sincere thanks and appreciation go out to all who contributed.

Copyright Information

Key Takeaways

The Large Scale Networking (LSN) Interagency Working Group (IWG) held an *Operationalizing Software-Defined Networks Workshop* on September 18–20, 2017, in Washington, DC. At this workshop, Federal, private, and academic stakeholders discussed the current state-of-the-art and path forward to realize an open (nonproprietary), innovative, multidomain, and interoperable software-defined network (SDN) as an operational infrastructure that can rapidly adjust to the evolving communication and computing needs of science, engineering, and commerce, while simultaneously enhancing the economics, security, evolution, and manageability of the network. Workshop participants explored the following key needs for "operationalizing" SDNs in this context:

- Enhanced SDN processes and architecture, including control- and data-plane separation, automatic configuration, operating models for network operators and end users, single-domain and multidomain control, security, needs-driven implementation strategies, diversity of network functions, and orchestration.
- Comprehensive SDN tools for verifying, debugging, monitoring performance, and testing.
- Management and operations support, including provisioning, integration, balancing, open application programming interfaces (APIs), network operations, authentication, monitoring, self-healing, resilience, reliability, high availability, and data analytics.
- Policies for interoperability, trust and verification, and authentication.
- Forums for collaboration, progress assessment, tool sharing, test suite development, and workforce development and training.

Background

Whereas conventional data networks rely on distributed protocols among individually configured devices, SDN-enabled networks operate through centralized controllers. By decoupling control and data planes, software-defined networking enables broad flexibility in network programming and operation, including one or more of the following characteristics:

1. Separation of the control and data planes of the network (i.e., control is implemented in the software rather than the hardware)
2. Software-driven automated provisioning of network services
3. Centralized visibility and control of the network
4. Dynamic, flexible, real-time network programmability
5. Disaggregated network functions

Historically, the primary SDN research focus has been on controlling data flow forwarding and policy. Early SDN solutions for university campuses and regional and national research and education (R&E) networks offered researchers and network operators a close approximation of the far-reaching potential of SDN technologies to break down barriers to innovation. As a result, in recent years, there has been significant interest and effort across academia, industry, and government in expanding the research and development of SDN technologies.

The Large Scale Networking Interagency Working Group co-organized this workshop[1] as part of a series of SDN-focused workshops. It follows prior workshops that promoted SDN technology adoption (2013)[2]

[1] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1747856

[2] https://www.nitrd.gov/nitrdgroups/index.php?title=SDNProgramReview

and research and development to extend SDN capabilities for end users (2015).[3] This 2017 workshop focused on the current state of software-defined networking and possible R&D efforts that could advance technology development and innovation in support of American leadership in science and technology. The overall goals of the workshop were to engage members from stakeholder communities to discuss the definition(s) of SDN; the expectations, current state, and gaps for operational SDN; and the metrics to assess available commercial and open source solutions for operationalizing SDN. Workshop attendees included representatives from academia, network operators (for universities and regional and national R&E networks), network providers, technology vendors, open source developers, commercial developers, and Federal agencies. The webpage https://www.nitrd.gov/nitrdgroups/index.php?title=OperationalizingSDN provides additional information about the workshop.

Session Summaries

The workshop was organized into seven sessions, including expert panels and discussions, which are summarized below.

Current State and Issues Regarding SDN: Users' Perspectives

As new SDN application ideas emerge, clarity and maturity in operational infrastructure and practices are critical to realizing the envisioned utilization of such technologies. Noting that the solutions share common integration and troubleshooting processes and attributes, stakeholders made a range of observations regarding SDN solutions:

- Existing commercial SDN solutions have focused on point solutions for specific use cases, with significant variation and rigor in specifications and implementations.
- Generic SDN platforms based on open protocols (e.g., OpenFlow, one of the first SDN standards) appeal to the academic, government, and R&E networks, but not to large companies due to the small immediate market demand.
- SDN customers must currently perform their own solution integration, which SDN solution providers should address in the future.

Campus Network Operators

University campus network operators primarily focus on creating Science DMZ networks[4] adjacent to existing legacy campus networks. By avoiding institutional firewalls, Science DMZs provide a fast path to connect campus computing facilities and instruments to other institutions, thereby bringing significant value to academic campuses. This panel explored critical issues that must be addressed before SDN can deliver production services. Operators from five universities that have adopted SDN networks discussed deploying SDN in specific locations or applications where it works well instead of deploying SDN across entire campuses.

Workshop discussions identified the following key issues for SDN solutions:

- *Single-domain vs. multidomain*. Current SDN solutions only address an SDN controller's single-domain control of its own network, not multidomain orchestration that requests resources or functions from individual SDN controllers from different networks. Existing tools for R&E network

[3] https://www.nitrd.gov/nitrdgroups/index.php?title=SDN_Operational_Issues_WS

[4] A science "demilitarized zone" network allows separation of a public-facing server from private, trusted networks; this separation helps protect the security of nonpublic data shared in private institutional networks without use of firewalls.

provisioning have been used to coordinate SDN and legacy networks that involve manual processes. Science DMZs need to address the interfaces between SDN and legacy networks, and between campus and regional and national R&E networks (e.g., the Department of Energy's dedicated Energy Sciences network [ESnet]).

- *Basic hardware and software problems*. Operators are experiencing serious problems that include limited hardware support for OpenFlow features, inconsistent hardware and software compatibility across vendors, firmware bugs, debugging difficulties, and a lengthy timeframe for bug fixes.
- *Protocol abstraction*. OpenFlow offers a convenient low-level programming abstraction across vendor switching devices, but higher-level interfaces are needed for operational management. Operators also discussed their experiences with higher-level abstractions (e.g., intent-based networking), but none has emerged as the most suitable solution.
- *Developer mindset*. Current SDN solutions have focused on network operator and engineering needs but not on application end users, e.g., SDN tools are designed for network operators, so end users cannot dynamically configure their services via SDN. SDN solutions today often become mere VLAN (virtual local area network) "provisioning tools".
- *Workforce development*. There is high demand for a workforce with knowledge of both software and networking. However, a majority of the emerging workforce, which is comprised of university graduates with both software and networking training, has been entering private industry instead of advanced network operations at universities and R&D networks.

Network Providers

The Network Providers panel reflected a broad spectrum of interests due to the diverse customer bases and use cases of these participants:

- Large science data flows
- The interconnection of international optical circuits
- Dynamic Layer 1 network instantiation with monitoring and analytics services
- Customized policy realization over high degree interconnects, i.e., internet exchange points
- Support of a broad range of applications and connectivity to resources (e.g., cloud facilities)

R&E network providers discussed shared needs and experience. Shared needs include multidomain network provisioning, traffic engineering, visibility, and troubleshooting. Shared experience includes in-depth experience in developing and using automated network provisioning tools and standards, and they face the same challenges regarding SDN hardware and software issues. Before adopting multiprotocol label switching (MPLS) in 2017, one research network was using OpenFlow-based switches throughout its U.S. backbone and developed a tool for its automated VLAN switching service. ESnet has been assessing the feasibility of SDN in its upcoming infrastructure upgrade (ESnet6). An Internet research organization has been developing its own SDN controller in the form of a software-defined exchange (SDX) and has long supported automated lightpath provisioning via Network Service Interface-based tools. A regional network provider has focused on developing the northbound interface[5] for its SDN at the perimeters for connecting to the public cloud. These examples reflect the ongoing use of SDN in multiple network automation efforts. Developers are continuously building tools that are constantly evolving to support SDN automation.

[5] A northbound interface enables a specific component of a network to communicate with a higher-level component.

The panel also explored the development of DevOps integration, which network providers feel they can undertake. Workshop discussants emphasized the importance of a suitable programming abstraction, in addition to reliable hardware, as necessary for sustaining such development. A programming abstraction that promotes a scalable developers' ecosystem is necessary for deriving operational tools for use with SDN. Discussion of the data-plane and control-plane protocols included the need for management-plane protocols.

Network providers compared abstractions, specifically OpenFlow-style match/action abstraction and the Network Configuration Protocol (NETCONF)-style configuration,[6] and their roles in an operational SDN. They discussed the principle of separation of control plane and data plane is upheld if there is a central source of decision (as opposed to distributed decisions) without limiting the chosen programming abstraction, versus the fact that NETCONF-style configuration inherently limits the programmability to legacy network semantics, thereby preventing realization of the full promise of SDN programmability.

Network providers also raised the following issues:

- The need to consider heterogeneous infrastructure (both legacy and OpenFlow, and potentially others), particularly in the case of multidomain objectives.
- The role of both "green-field" (all SDN hardware) and "brown-field" (mix of SDN and non-SDN hardware) in supporting emerging applications.
- The necessary role of decision making on distributed hardware to quickly respond to operational infrastructure failures even when they cannot connect with the SDN controller.

Open Source SDN Development

The keynote speaker provided a status update on "open SDN" development. While the industry is pushing for "incremental SDN" (e.g., a NETCONF-based controller configuring networking hardware designed for distributed control), "open SDN" is still a work in progress. Some of the latest focal points of the open SDN journey are "disaggregation," "and "open source." The disaggregation trend has led to the creation of multiple disaggregated open source components, which have not been easily integrated into a complete solution. Various vendor solutions incorporate open components into their closed proprietary solutions. Contributions are encouraged to open source projects that can be incorporated into practical vendor solutions.

Open source SDN developers also presented four initiatives characterized by different community participation models: open virtual network software projects, national R&D networks, open SDN controller projects, and sharing of best-practice network control methods.

Workshop discussion identified the desired properties of SDN software:

- Modularity and microservices for network functions at various levels
- Enhanced programmability, enabling networks to keep pace with the speed of change
- Open interface for control across multiple domains

[6] The Network Configuration Protocol (NETCONF) is a standard network management protocol that provides mechanisms to install, manipulate, and delete the configuration of networked devices.

Commercial SDN Development

The Commercial SDN Developers panel focused on the current market landscape and the challenges facing commercial developers. Workshop discussions identified the following characteristics and trends of today's market landscape:

- Most controller applications address point needs with little functionality overlap.
- APIs are supported for integration with other systems.
- Open source components are combined by commercial third-party entities that provide proprietary solutions. There is no complete open source SDN solution.

Workshop discussions identified the following challenges:

- Quality assurance, which is extremely time-intensive.
- Chasing new changes in hardware and standards (i.e., OpenFlow).
- Interoperability among controllers and switches, even when claiming OpenFlow-compliance, is not guaranteed.
- A standard schema for network telemetry.
- Troubleshooting involves addressing
  - Hardware, software, issues when crossing legacy networks, etc.
  - Difficulty debugging with only low-level flow statistics
- Certification for government compliance can be a long process; a potential "on-ramp" certification strategy was suggested.

Workshop discussions also touched upon whether SDN brings new security challenges and the utility of open source efforts. It was also noted that some customers purchase products to meet security needs, and that the SDN capability of segmentation and central visibility of network events has facilitated its security management. One challenge is the lack of a confirmation mechanism to validate that the network carries out all commands by the controller. The desirability of having a standard for validating controller-switch executions was also discussed.

In discussing the utility of open source efforts, several attendees observed that open source projects are not the most useful for users needing an operational solution; however, they are very valuable for vendors. Open source projects also foster developer-to-developer discussions.

SDN Application Drivers and Primary Needs

The Application Drivers panel represented the following range of use cases that are driven by end user needs (services and integrated infrastructure [cloud] view) and by the need to deliver services beyond best-effort service levels:

- High-volume scientific data
- SDX for telescope data
- Interdomain SDN for South America
- SDN-based "services edge"
- SDX for traffic analysis resistant Internet
- Delivering city services via network virtualization
- Multicasting scientific data using SDN
- Multidomain SDN for K–12 video streaming in a smart city
- Multicontroller, multiprotocol, multivendor, and multiservices SDN laboratory

The panel specifically identified the following needs:

- End users need segmented services, not VLANs.
- SDN solutions are needed for end users (vs. SDN solutions for network operators).
- Operators need precise information on failures (poor debugging and diagnostics experiences are due to the lack of tools).
- Orchestrators for multidomain support are strongly needed.

Workshop participants also observed that in today's fragmented market, there is no real owner of technical issues. The issues identified above prompted further observations on SDN design perspectives:

- Sharing past experiences is critical because years of prior work on network control tools exists.
- An independent troubleshooting framework to detect failure is needed instead of relying on switches to report their own failures.
- Engineering principles can be drawn from other critical systems (e.g., car alarm systems).
- Useful data can be adopted from existing standards such as Simple Network Management Protocol and NetFlow.
- Workforce development is critical.
- Other automation approaches, such as those put forward by industry or user groups, may complement the provisioning needs across multiple domains.

Security Implications of SDN

The Security panel, consisting of both academic and industry participants, addressed the following topics:

- Security threats and opportunities for university campus networks.
- Use of machine learning and cloud resources to attain visibility and control against security risks.
- Secure authenticated federation across multiple domains via trust models and reasoned policies.
- Network original equipment manufacturers performing risk assessment and SDN controls in a standardized cybersecurity framework.

The workshop discussion identified key security concerns:

- Risk and significant damage resulting from a compromised, hacked, or spoofed (via a man-in-the-middle attack) SDN controller.
- Risk of multidomain network path control traversing network segments with unknown properties.
- The explosion of network states and configurations on SDN arising from network events and adversaries.
- Automated, natural-language translation of security policies into SDN configuration.
- SDN approaches for security provisioning, which can avoid human misconfiguration.
- The need to impose role-based resource request constraints.
- Identity management, policy management, and trust management; much current work can be leveraged.

Federal SDN Interests and Efforts

The Federal panel explored government SDN interests and activities focused on the following topics:

- Prototyping advanced global secure computing and communication capabilities using available technologies, including Level-3 MEF circuits and commercial cloud, all via their provisioning APIs.[7]
- The importance of model verification of such new SDN capabilities for millions of data flows, coupled with SDN and compute.
- The procurement challenges for such bleeding-edge technologies, pointing back to the crucial need of SDN training for soldiers and the workforce.

SDN, from Research to the Real World

A panel of academic and industry experts explored past macroscopic trends and lessons for disruptive networking technologies for the future. The first presentation included the following key points:

- Accelerated network evolution involves programmability and balancing usability, flexibility, performance, and security.
- Increasing the speed of innovation would entail standardizing the programming model, not the network nodes, so that networks evolve as fast as software gets programmed.
- Active networking involves enabling network programmability and focusing on secure and agile methods to control network behavior by software loaded onto network nodes.
- Significant research has gone into hardware security, contributing to the current broad availability of hardware secure boot capabilities.
- Programming active network applications is difficult, and insufficient time has been spent to accomplish it.
- As SDN research picks up again with OpenFlow and subsequent efforts, the following continuing challenges need to be addressed:
    - Enabling applications motivated by cost saving and attractive services
    - Diagnosis capabilities (often an afterthought)
    - Focus on theory and programming language
    - Trust: Programmability cuts both ways
    - Service needs and specifications; if these are met, the economics will follow

The second discussion focused on router economics, including the following points:

- Economics today favor pervasive compute and storage. The goals for today's network/compute racks that are based on GENI racks[8] are three orders of magnitude more compute, six orders more storage, and one-third the cost compared to earlier systems that were based on ARPANET's Interface Message Processor system.[9]

[7] The MEF is nonprofit international industry association that works to enable agile, assured, and orchestrated ethernet and cloud services for the digital economy.

[8] Global Environment for Network Innovations (GENI) architecture provides an open infrastructure for networked research designed to allow research institutions to customize network topologies for multiple concurrent experiments, each which of which may use different protocol stacks and packet forwarding algorithms.

[9] ARPANET was the groundbreaking Department of Defense Advanced Research Projects Agency Network developed in the 1960s and operational through 1990 for sharing digital resources among geographically separated computers; it provided the technical foundation of the Internet.

- "Slices" of software-defined infrastructure based on virtualization and distributed clouds are becoming the *de facto* basis for rolling out services. Services are becoming more easily adopted through "App Store" models.

Participants also discussed research areas representing a continuum of community and industry understanding in the quest for programmable networks. Discussion focused on hardware economics (cheaper compute and storage, and abundant cloud infrastructure), and the forces demanding separation of control and data forwarding, continuing to drive SDN implementations.

Wrap-Up: Key Areas for Operational SDN

The workshop concluded with a discussion of SDN adoption and identification of key areas for further exploration, focused on flexibly enabling end-to-end paths to network, compute, and storage resources with customizable properties, using software to easily assemble such paths across hardware infrastructure, with favorable economics, security, evolution, and operation manageability.

Participants identified the following key SDN areas for further exploration:

1. **Processes and Architecture**
    - SDN's range of definitions
    - Separation of control and data planes and automatic configuration
    - The "wholesale" model (network operators) and "retail" model (end users) for operations
    - Single-domain and multidomain control
    - Level-2 and Level-3 implementation strategies as driven by actual service needs
    - Disaggregation and diversity of network functions
    - Orchestration (northbound APIs)
2. **Support**
    - More and better tools to provision, verify, debug, monitor performance, test, and provide a sandbox for experimentation
    - Security enhancement through transparency and visibility
    - Workforce development for long-term success
    - Support for training, resilience, reliability, and high availability
3. **Management and Operations**
    - Provisioning: the needs for a common base feature set, resource expression, and openness
    - Integration across vendors, hardware, software, and science
    - Balance of complexity and operability
    - Open APIs at the core of interoperability and composability
    - Open, standard authentication and authorization standards
    - Monitoring, self-healing, and data analytics
4. **Policy**
    - Interoperable hardware and software
    - Policy: fail open/close/safe mode strategies that keep the network connected or stopped when a network switch loses connection to its controller. How do we use, secure, etc., authentication and authorization?
    - Trust and verification

5. **Forums**
    - Collaboration, assessment, and workforce development for sharing tools, lessons, progress, and test suites
6. **Drivers**
    - Economics/cost
    - Security
    - Measurements
    - Virtual network containers that can be managed
    - Policy enforcement
    - Agility and speed of orchestration

Conclusion

Since the last SDN workshop in 2015, much progress has been made in developing the underlying technology and understanding the critical operational requirements for advancing SDN. While proprietary SDN solutions continue to be developed, an important trend has emerged for developing SDN systems by integrating open source components and network stack disaggregation. An increasing number of SDNs have become operational. Based on different technologies that permit different programming granularities, protocols, and features, these deployed SDNs provide important insights into a range of issues that need to further mature. High demands for improved diagnostic tools have been made, as well as crucial security and trust requirements for SDN. The definition and requirements of multidomain SDN remain open questions, as does the vision of a complete open source SDN solution. Nonetheless, the continuous evolution of tools by vibrant academic, industrial, and governmental stakeholders shows great promise for the realization of SDN automation in the near future.

Abbreviations

API	application programming interface
IWG	Interagency Working Group
LSN	Large-Scale Networking (a NITRD IWG)
NETCONF	Network Configuration Protocol
NITRD	Networking and Information Technology Research and Development Program
R&E	research and education
Science DMZ	science demilitarized zone
SDN	software-defined network(ing)
SDX	software-defined exchange
VLAN	virtual local area network