Smart High-Performance Networks

Towards New Generation Intelligent Networking Infrastructure for Distributed Science Environments

Smart High-Performance Networks Workshop
Rockville, Maryland
December 8-9, 2016

Sponsored by
U.S. Department of Energy
Office of Advanced Scientific Computing Research

Smart High-Performance Networks

Towards New Generation Intelligent Networking Infrastructure for Distributed Science Environments

DOE Workshop Report

December 8-9, 2016
Rockville, Maryland

Workshop Organizing Committee:
Ian Foster, Argonne National Laboratory
Tom Lehman, University of Maryland/Mid-Atlantic Crossroads
Nagi Rao, Oak Ridge National Laboratory
Bryan Lyles, Oak Ridge National Laboratory
Inder Monga, Lawrence Berkeley National Laboratory/ESnet
Prasanna Balaprakash, Argonne National Laboratory
Kalyan Perumalla, Oak Ridge National Laboratory
Stacy Prowell, Oak Ridge National Laboratory
Raju Vatsavai, North Carolina State University

DOE ASCR Point of Contact:
Thomas Ndousse-Fetter

Workshop Report Author List:
Provided in Appendix B

Executive Summary

Smart systems constitute a key emerging technology trend with applications spanning a wide variety of industries and user domains, as reflected in the advances in smart cities, grids, cars, buildings, roads, and many other systems. This focus on smart is based on innovations in several information technology areas including big data availability, widespread device connectivity, computational power, and artificial intelligence (AI). Smart systems are currently in an early development phase, which we expect will be followed by decades of intense innovation and restructuring of societal systems and technology areas. The network is a critical component of these smart systems but often it is considered as basic infrastructure, whose only function is simply to transport packets. There has been little discussion of how the network may act as an active participant within a smart system. As a result, we are motivated to think about an ecosystem of smart networked systems, wherein the network infrastructure is a peer component with respect to programmatic control and real time tailoring to applications specific needs.

A smart science ecosystem is of particular interest to the DOE community, because scientists increasingly depend on highly reliable and secure high-performance networks to access critical science facilities, collaborate, and share massive volumes of data. Furthermore, the volume and variety of science data and the complexity of workflows continue to explode as newer science instruments and computing capabilities are being developed. As this trend continues, networks will need to provide more sophisticated, easy to use, secure, and more predictable services. These expectations translate to a need for a new generation of high-performance networks with intelligent capabilities delivered to scientists in the form of just-in-time network as a service.

Network designs are evolving at a rapid pace toward programmatic control, driven in large part by Software Defined Networking (SDN) concepts and technologies. This SDN innovation cycle is important as it includes a vision and promise for greatly improved automated control and configuration in comparison to the labor-intensive network deployments of today. However, even the most optimistic projections of SDN adoption and deployment do not put science ecosystems on a path to the truly smart or intelligent network infrastructures envisioned. The vision for a "smart network" combines the programmability and ease of automation enabled by SDN technologies with AI technologies to realize network infrastructures that are self-aware, self-managing, and self-healing. The ultimate goal is a smart network infrastructure that can monitor itself, diagnose and resolve problems, defend itself from cyber-attacks, and provide intelligent services to scientists. To address these issues the DOE Advanced Scientific Computing Research (ASCR) Smart High-Performance Networks workshop brought together network researchers and operators from national laboratories, academia, and industry. The core of the workshop discussions were organized around four key technical topic areas; Smart Network Infrastructures, Smart Applications, AI-Based Technology for Smart Networked Systems, and Smart Cyber Security Sub-systems.

The following key findings and observations are noted:

- *Networks are at a technology inflection point where the next phase is a transformation from a passive infrastructure to a smart system that forms the core of the smart networked ecosystem.* This inflection point is being driven by the convergence and maturation of several technologies that have been largely disjoint to date with

regard to their individual development. The integration of SDN, AI and big data analytics will enable a smart networked ecosystem to evolve such that the network becomes an interactive component for use by similarly smart applications, security systems, and other domain-specific use cases.

- *Smart Networked Ecosystems will be critical to enable future innovations across the core DOE mission domain science communities.* Current static, non-interactive network infrastructures do not have a path forward to assist domain science application innovations. The recommended way is to form multi-disciplinary teams that can employ an iterative design in steps to form a basis for more detailed and comprehensive designs and visions.
- *The DOE community should be proactive in defining future smart network functions and designs.* A typical workflow includes resources across DOE Laboratories, wide area networks, regional networks, and university campuses. Smart network functionality must thus be considered and developed in a federated and multi-domain context. Experience suggests that commercial development efforts are likely to focus on operational and cost reduction issues in individual networks. The DOE R&E community needs to be proactive in defining requirements and developing prototypes for smart networked infrastructures early in this development phase. This approach will provide the best opportunity to influence and leverage commercial and open source activities that can then be tailored and applied to the DOE environment.
- *Prototyping on at-scale testbeds will be critical to the development of complex systems such as a smart networked ecosystem.* Complex systems that include multi-technology integration will require an iterative prototype build-and-test loop, which will in turn require access to experimental infrastructure where component and system level functions can be prototyped. This experimental infrastructure needs to include realistic hardware and software systems across multiple network layers, have sufficient scale to evaluate solutions, and be breakable in order to allow robust prototype evaluation and testing.
- *Network Infrastructures are changing and the people that build and operate them will have to change as well.* Networks are evolving from manually configured infrastructures with static services, to software-driven systems with programmatic control to build, operate, and interact with clients. For smart networked ecosystems, there will be a need for personnel who can understand and debug issues from both smart application and smart network infrastructure perspectives.
- Multi-disciplinary teams should be formed to keep the focus on the enhancement of domain science and related DOE facilities.
  All of this work will require the formulation of multi-disciplinary teams with experts from the network research, domain science, and DOE facilities communities. A formal process should be identified to define the user driven requirements from the domain science and facilities communities. A continuous dialogue between these multi-disciplinary team members should occur as part of the design, build, test iterative process. These teams can also provide a mechanism for smart system knowledge transfer within the DOE and general R&E community.

Table of Contents

Smart High-Performance Science Networks

Towards New Generation Intelligent Networking Infrastructure for Distributed Science Environments

1 Introduction

Scientists increasingly depend on complex workflows that span instruments and computing facilities, which in turn require highly reliable and secure high-performance networks to access the facilities, collaborate, and share massive volumes of data. In particular within Department of Energy (DOE) science environments, the volume and variety of science data and the complexity of workflows continue to explode as the next generation science instruments and computing capabilities are being brought online. As this trend continues, networks are expected to provide more sophisticated, easy to use, secure, and predictable intelligent services. These expectations translate to requirements for a new generation of high-performance networks with intelligent capabilities delivered to scientists in the form of just-in-time network as a service.

Network designs and infrastructures are evolving at a rapid pace in this direction, driven in large part by Software Defined Networking (SDN) and related virtualization concepts and technologies. This SDN innovation cycle is important and includes a vision and promise for greatly improved automated control and configuration in comparison to the extremely labor intensive network deployments of today. Indeed, for the first time it seems possible to fully exploit the power of programmability, powerful software and virtual systems real realize the network as a service vision. However, even the most optimistic projections of SDN adoption and deployment do not put DOE science ecosystems on a path to the truly smart or intelligent network infrastructures envisioned or desired.

These developments inspire the concept of a **smart networks for science** that combines the programmability and ease of automation enabled by SDN technologies, on the one hand, with AI technologies on the other to realize network infrastructures that are "self-aware". The ultimate goal is a network infrastructure that can monitor itself, continually optimize its performance, diagnose and resolve problems, defend itself from cyber-attacks, and provide intelligent services to scientists. Figure 1 provides a capability comparison between current networks and future self-aware networks. The transformation to self-aware networks should also include an increase in value, particularly to science, which is strongly correlated to the increase in knowledge intensity. The value quantification will likely be reflected in an ability to contribute to scientific discovery by providing new network services and enabling innovation for the networked systems. Figure 2 depicts this increase in value and knowledge intensity as the networks evolve from current fixed infrastructures to smart networks.

A smart network vision has been addressed from a conceptual perspective in various forms in the past, most notably autonomic networking. This was derived from the more general concept of autonomic systems described by IBM in the early 2000s [1]. There are now efforts within the Internet Engineering Task Force (IETF) to define autonomic networking requirements and designs [2] [3] [4]. Many of the smart network concepts described here are similar to those described for autonomic networking. For this report, we consider

smart networks to be a vision which leverages autonomic networking concepts in the context of the emerging technologies of SDN, artificial intelligence (AI), and big data analytics.

Area	Current capabilities	Self-aware capabilities
Self-Configuration	Network are statically provisioned and incapable of responding dynamically to changing traffic conditions and network dynamics	Automated configuration of components and subsystems through high-level policies followed by dynamic adaption of the changes by all system components
Self-Optimization	Networks and network-intensive applications have hundreds of manually set, non-linear tuning parameters, and their number will increase exponentially.	Continually monitor and adjust resource utilization; continuously attempts to improve performance and QoS through proactive, self-optimization and automated decision making
Self-Healing	Network fault diagnosis and repairs in complex multi-layers and multi-domains can take network operators several hours and sometimes days	Network can protect itself before, during and after both malicious attacks and user/operator errors, via automatic initiation of self-repairing, self-regenerating, and self-immunity
Self-Protection	Detection and recovery from attacks and cascading failure is manual and can take hours and weeks. No attack prediction mechanisms.	Network automatically defends against malicious attacks or cascading failures. It may identify early warning indicators and adjust monitoring and defense actions.

Figure 1 Self-aware network capabilities [1]

The Research and Education (R&E) community in general and DOE science users in particular represent a unique environment from the perspectives of smart network use and development. While commercial smart network deployments are likely to focus on individual enterprises, R&E science application workflows are generally distributed and multi-domain, often spanning DOE Laboratories, wide area networks, regional networks, and university campuses. They, thus require smart networks that can function in a federated and multi-domain context. In this environment, multiple autonomous smart network domains will need mechanisms to interact with each other, and/or with higher-level workflow agents, in order to coordinate their operations. From a development perspective, no community is better positioned than DOE to realize these types of end-to-end smart network functions. The combination of advanced network infrastructure, unique science application drivers, and pervasive multi-domain cooperation that characterize DOE R&E environments can allow DOE to drive unique innovations in this space. Experience suggests that commercial development efforts are likely to focus on operational and cost reductions in individual networks rather than on optimizing user Quality of Experience

(QoE) in the end-to-end, multi-domain contexts that characterize R&E environments. (QoE is a measurement of all subjective and objective experiences arising from the interaction of a person with technology, englobing areas such as social psychology, cognitive science, economics, and engineering science.) The R&E community will need to leverage technologies being developed in the commercial space, but must extend and tailor those technologies to meet unique R&E requirements.

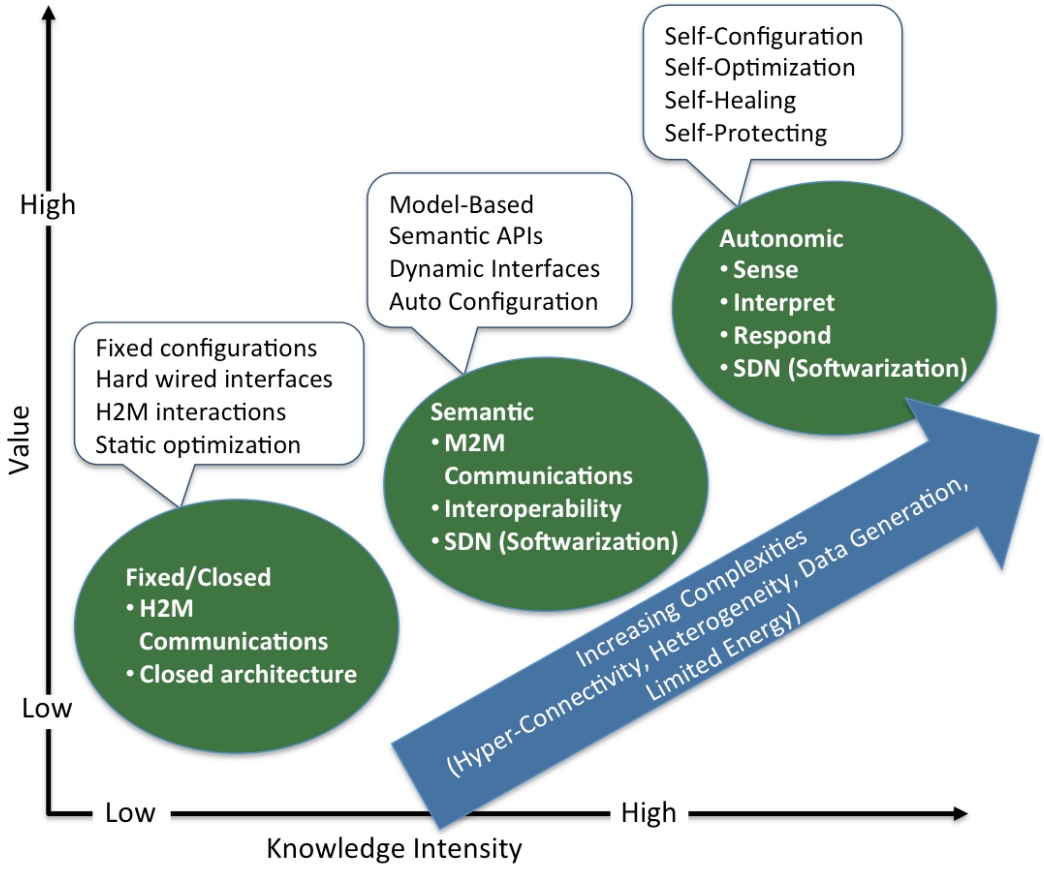

Figure 2 Smart Networks Value Progression

To address these issues, the DOE Advanced Scientific Computing Research (ASCR) Smart High-Performance Networks workshop brought together network researchers and operators from national laboratories, academia, and industry to identify and discuss emerging opportunities and challenges in the design and development of a new generation of smart high-performance network infrastructures to support distributed extreme-scale science. This document provides a summary of these workshop discussions. The remainder of this document is organized as follows: Section 2 summarizes the workshop topics and discussions; Section 3 discusses challenges and opportunities; Section 4 presents key findings; and Section 5 summarizes the overall workshop conclusions. The workshop agenda is provided in Appendix A. The workshop attendee and report author list is provided in Appendix B. Specific terms as they relate to smart networked systems are

defined in Appendix C. A summary of the key classes of network-intensive science applications is listed in Appendix D.

2 Smart Networks for Distributed Science

Smart systems are a key emerging technology trend that is being applied across a wide variety of industries and user domains, with efforts to develop, for example, smart cities, smart grids, smart cars, smart buildings, and smart roads. Recent advances in smart systems are due to the culmination of innovations in several information technology areas, including big data availability and analytics, widespread device connectivity, increased computational power, and AI. Smart systems are currently in an early development phase, which we expect will be followed by a multi-decade period of intense innovation and restructuring of societal systems and technologies. Advances in AI merit special notice as a driving force behind this innovation cycle. The National Science and Technology Council's recent National AI R&D Strategic Plan [5]outlines an ambitious research plan for these technologies, with the expectation of considerable impacts across many domains.

The network is a critical component in these smart systems and its capabilities constitute the building blocks over which broader system capabilities are built upon. And yet, it is often considered as basic infrastructure whose only function is to transport packets. There has been much less discussion of how the network may be an active participant within the smart system. As a result, we are motivated to think about an ecosystem of smart networked systems, wherein the network infrastructure is a peer component with respect to programmatic control and real time tailoring to applications specific needs.

This need for truly smart networks for science is motivated by three major factors. First, domain science applications and workflow processes are currently forced to view the network as an opaque infrastructure into which they inject data and hope that it emerges at the destination with an acceptable QoE. There is little ability for applications to interact with network to exchange information, negotiate performance parameters, discover expected performance metrics, or receive status/troubleshooting information in real time. Indeed, the ability for a science application to interact and negotiate with a network infrastructure of a science ecosystem, should be a hallmark of a truly smart network.

A second concern is that today's network infrastructures are notoriously time consuming and labor intensive to build, configure, and maintain. Workshop participants argued that a combination of SDN and AI technologies can be used to enable infrastructures that reduce required human effort by multiple orders of magnitude. This approach of course does not imply that humans will no longer be in control of these infrastructures but on the contrary they will be empowered with advanced capabilities to control more effectively. Indeed, a key research question is how to balance human-in-the-loop features with self-aware automation in order to optimize efficiency, safety, and confidence with regards to network use and function.

A third motivation for smart networks is to enable the development of new and innovative services geared toward both science users and network operators. The extreme complexity of today's network infrastructures is beyond human ability to manage in a proactive and deterministic fashion. In many areas, such as cyber security, the degree of human expertise often becomes the determining factor with regard to network performance and event

response quality. The base technologies seem to be available to develop a new class of cognitive networks that combine machine learning, knowledge representation, and SDN control. Such networks could provide human operators with summarized higher-level information that would allow them to focus on addressing more complex problems that the smart network cannot handle.

The *Smart High-Performance Networks - Towards a New Generation of Intelligent Networking Infrastructure for Distributed Science Environment* Workshop was held in Rockville, Maryland on December 8-9, 2016. The initial plenary session included a statement of the workshop topics and goals by the sponsoring agency. This statement was followed by a talk that presented a forward-looking vision for how smart networks and smart applications can enable innovations in the domain sciences. The remainder of the workshop was organized around the following four technical focus areas, with a separate breakout group discussing key issues, concepts, and findings in each area.

Smart Network Infrastructures
This group focused on defining the key requirements, characteristics, services, and technologies needed to create future smart network infrastructures. It addressed how networks may evolve into an intelligent, self-aware infrastructure that participates as an adaptable and programmable component within an ecosystem of domain science-specific end-to-end services. Discussion revolved around identifying novel research directions in smart network design, operation, and domain science-focused service provisioning.

Smart Network-Intensive Science Applications
This group focused on defining the key requirements, characteristics, and functions that identify an application as a *smart application*. Discussions covered both smart application needs from a smart network, and mechanisms for dynamic interaction between application and network.

AI-Based Technology for Smart Networked Systems
This group focused on how AI technologies can be applied in a smart network context. It identified a broad set of AI technologies, including machine learning, heuristic planning and search, bio-inspired computation, natural language interfaces, knowledge representation and reasoning, and other. Areas were then identified that can potentially contribute to smart networks in terms of both improved infrastructures by enabling operators and support for scientific discovery by enabling the science users.

Smart Cyber Defense for Open Science
This group focused on how to leverage the other smart areas to build innovative and more robust cyber security defenses and systems.

The discussion in each breakout group was placed in the context of smart networks. For example, the smart applications discussions focused on how smart applications and smart networks should interact and what services a smart network needs to provide to applications. Likewise, the AI technology discussions focused on how these technologies could be applied in a smart network context, and the smart cyber security system discussions focused on how to leverage the other smart areas to build innovative and more robust cyber security defenses and systems.

The discussions also addressed the question of what capabilities a smart network needs to provide to other smart system components, and vice versa. The time frames considered included both near term (2-4 years) and longer term (5-10 years). Each breakout group included talks by technical area experts. Each workshop attendee was pre-assigned to one of the technical focus area breakout groups.

We summarize the discussions in each of these areas in the following subsections.

2.1 Smart Network Infrastructures

Today's state-of-the-art commercial production networks leverage a variety of different networking technologies, but are fundamentally constructed using two network layers: an optical transport layer and a packet switching/routing layer. The optical transport layer is often comprised of dense wavelength division multiplexed (DWDM) signals ranging from 10 Gb/s to nx100G coherent sub-carrier multiplexed 'super channels' and a photonic reconfigurable optical add drop multiplexed (ROADM)-based switching function with an optical transport network (OTN) electronic switching function that is integrated with the optical transport. These technologies can support multiple Terabits of transmission capacity over dark fiber and a broad set of fixed circuit-oriented wavelength services. Transparent optical transport layer implementations deliver provisioned optical wavelength granular services (100G and 10G), whereas OTN-switched implementations can deliver a broader set of circuit-oriented services through OTN grooming and multiplexing on to optical carriers, including 1/10/40/100Gb Ethernet services, storage protocols, InfiniBand, OTN, and other time division multiplexed (TDM) services.

Overlaid on this optical transport substrate is generally a separate packet switching/routing layer to provide packet-oriented services and packet transport functions. Often this layer comprises off-the-shelf one-size-fits-all IP routers—frequently with multi-protocol label switched (MPLS) Provider-Edge (PE) and Provider (P) routers—with embedded distributed routing protocols designed for the service provider market and Internet. Consequently, packet-oriented services supported in this layer are often defined by pre-existing IP protocols (e.g., IGP/BGP) used in carrier IP/MPLS backbones and cloud networks. Provisioning of services and resources in current network architectures is typically done independently within the packet and optical layers in a non-coordinated fashion, leveraging either vendor-supplied network management systems with domain-centric service provisioning functionality, or vendor-implemented control plane technologies. For example, IGP/BGP on routers is typically used to establish L2/L3 services, while GMPLS for optical transport systems is used to establish L0/L1 services.

Commercial networks are generally designed to support specific commercial business objectives, and thus have matching control capabilities. Service provider networks, for example, are designed as a walled garden and optimized for huge volumes of commercial services for the consumer and enterprise markets, with little (but emerging) end-user control and visibility. They rely on the law of large numbers and take advantage of statistical multiplexing to help in network planning. Cloud networks are similarly closed and are generally treated as an internal resource, optimized for the cloud operator's specific applications.

R&E networks have typically adopted this commercial-based architecture and then built value added services on top of the packet switching/routing layer in order to provide advanced value-added services for science users. The OSCARS [6] system built by DOE ESnet is an example of such as system. It represents a pioneering Software Defined Network (SDN) technology prior to that term of art being defined.

SDN technologies are now the driving force behind a new class of network architectures. SDN concepts and technologies originated within the R&E community and hold the promise of revolutionizing network designs, operations, and services. A key component of SDN is the decoupling of the network control plane from the underlying hardware or data plane layer. This separation allows adaptable programmability to be introduced to the network control, and reduces the dependency on specific hardware technologies and vendors. Initial SDN deployments have been concentrated in data center environments where there was a clear need to automate those network infrastructures and implementation was facilitated by the wholly owned infrastructure in a common location.

There are now significant efforts within both the commercial and R&E communities to evolve current production wide-area and regional networks into native SDN-based infrastructures. On the commercial side, we see efforts like AT&T Domain 2 [7], which defines a next generation network architecture firmly rooted in the use of SDN network infrastructure and Network Functions Virtualization (NFV) [8] based edge systems to provide customer services. This strategy extends throughout the network stack, including optical systems through their OpenROADM multi-source agreement to enable SDN-controlled optical systems [9]. SDN-focused open source development projects such as the Open Network Operating System (ONOS) [10] and OpenDaylight platform (ODL) [11] include significant contributions and product incorporation from many commercial network providers and vendors.

Optical layer systems have historically been designed to enable growth in static capacity (the 'big pipe' model) between end nodes. They do not support the cross-layer programmability that would be needed for a fully autonomous multi-layer network infrastructure. Service providers have recently begun to develop specifications and semantic models [9,12] to enable programmability. Machine learning is being applied to extend the ability of current systems to support this new dimension [13]. However, the application performance levels and capabilities that can be supported by these approaches are limited by available hardware capabilities, and commercial vendors are not looking far enough ahead to overcome these limitations. Progress will require not only new software capabilities in optical equipment, but also an entirely new architecture to support a highly dynamic, flexible, and programmable optical layer amenable to autonomic control.

R&E networks including ESnet [14] and Internet2 [15] are now designing their next generation network architectures, which are anticipated to provide a rich set of SDN based services. There are many emerging technologies that may contribute to, or be necessary to the realization of, this next generation of SDN networks, including:

- Broader utilization of programmable, lean Layer 2 devices with SDN IP control plane functionality to replace or offload certain application or traffic types from existing routers.

- Packet and optical function convergence, for example by the deployment of pluggable coherent optics into packet switches/routers or of packet fabric modes into existing optical transport systems to enable native L2 transport and aggregation functions, so as to offload routers from performing these functions.
- Emerging open APIs on vendor systems and the maturation of SDN controller platforms create new opportunities to develop network control platforms that can facilitate near-term smart networks with the flexibility to support smart applications.
- Photonic component technology evolution towards larger-scale Sliceable Bandwidth Variable Transponder (SBVT) technologies that support multiple dimensions of flexibility, including arbitrarily sliceable spectrum, programmable modulation schemes, and tunability over broader spectral ranges.
- Enabled by the American Institute for Manufacturing (AIM) Photonics consortium and other initiatives, integrated photonic devices manufactured at high volumes through platforms such as silicon photonics will dramatically change the cost structure and capabilities available for optical systems. This integration of optical components into the electronic chip eco-system and markets will enable new intelligent functionality from optics.
- Advances in merchant silicon packet switching technologies, which will mitigate the need for custom ASIC/FPGA, and enable the creation of converged, open, and programmable packet/optical systems.
- NFV is a rapidly evolving trend that will have substantial impact on future networks. As compute technologies scale, and NFV orchestration and lifecycle management technologies evolve, it will become possible to instantiate functions once performed by dedicated routers on general compute platforms.

We do not review all of these emerging technologies here. From a smart network perspective, we expect the current R&E and commercial networks to evolve into networks with programmatic control. A previous DOE workshop held in the 2014, Software Defined Networking for Extreme-Scale Science [16], addressed issues associated with applying SDN principles and technologies to R&E networks. The current workshop, Smart High-Performance Networks, discussions focused on how to leverage these emerging SDN infrastructures to build the smart network infrastructures of the future. Current SDN efforts will likely not evolve into truly smart network systems without careful architecture and design efforts to determine how to leverage these technologies toward that goal. This observation is especially true in the R&E world, in which user and network requirements and infrastructure are significantly different than those found in the general commercial internet. In particular, we expect a truly smart network-capable infrastructure to exhibit the following properties:

Self-Configuration: An ability to automatically configure network elements, or policy, based on its self-aware state or other authorized inputs.

Self-Optimization: An ability to understand current and expected traffic profiles and use self-aware conditions, and defining configuration or policy optimizations for the benefit of the network infrastructure utilization or user quality of experience.

Self-Healing: An ability to identify failures and anomalies and then leverage self-awareness and self-configuration properties to take corrective action.

Self-Protection: An ability to recognize malicious activity on or directed against the network and initiate defensive measure to mitigate or stop the threat.

Realization of these properties will require more than simply leveraging the emerging SDN technologies. For some feature sets, there may be a need to influence these SDN systems to ensure that they have the degree of state awareness and real-time response capabilities needed. Toward this goal, we identify the following characteristics of an SDN network infrastructure that should be present to allow realization of the smart network related Self-X properties described in this document.

Real-time programmability: Programmability and moving to a DevOps ("software DEVelopment" and "information technology OPerationS") paradigm are two key motivations for the transition to SDN-based infrastructures. These new capabilities require well-defined Application Program Interfaces (APIs) for discovering capabilities, providing resource descriptions, and requesting services. However, smart network use cases will likely require a higher degree of real-time responsiveness than may be typically imagined for standard DevOps scenarios. The SDN hardware and software systems will need to be designed to support real-time levels of dynamic state discovery, service provisioning, transaction based negotiations, and configuration adjustments, all across multiple network layers. Optical systems, in particular, are severely limited in their programmability and their ability to interface through software with other layers.

Fine-grained resource control: Smart networks will need to make fine-grained decisions and adjustments regarding network functions, often at the flow and user levels. As a result, the SDN infrastructure will need to support fine-grained identification and control of resources and flows. This granularity will need to be reflected in the API and in other systems responsible for overall network monitoring and control. These systems will also need to include fine-grained policy and security mechanisms to ensure that only authorized users have access to appropriate resources and services.

State awareness (topology, configuration, and utilization): Emerging SDN technologies and systems already provide a significant degree of state awareness, including an understanding of the underlying network topology, configurations, and provisioned services instantiated upon the topology. This state awareness is discovered and maintained in a variety of ways, but typically includes discovery protocols and mechanisms for maintaining provisioning state in a centralized SDN controller. Smart networks will require merging of this infrastructure state with real-time data on network utilization and traffic profiles. This merging will in turn require inputs from sophisticated and scalable instrumentation/telemetry systems, with implications for the design of network state acquisition and maintenance systems.

Network instrumentation and telemetry: There are multiple network instrumentation and measurement mechanisms available today, such as perfSONAR [17], sFlow [18], and IPFIX [19]. The R&E community uses perfSONAR for active measurement of end-to-end performance. However, perfSONAR does not provide the utilization information that will be needed for smart network functions and use

cases. Many vendors support sFlow and IPFIX, which provide data at the individual network element level. However, these mechanisms are often limited to specific technology layers and require tradeoffs between network element performance impacts and data collection granularity. Smart network implementations will require a more holistic, comprehensive, and flexible approach to network instrumentation and telemetry, to include scalable, non-performance impacting designs for data collection and sharing, plus methods for integrating with the general state management systems of the SDN network.

Computation services: Significant amounts of computation will be needed to process real-time state and instrumentation data in order to service user requests and support other smart network functions, including the use of machine learning. This capability may be realized via tightly coupled or embedded compute resources that will effectively form part of the network. Another alternative is for high speed and programmable interconnects to compute facilities external to the network infrastructure. Smart networks may thus be another motivation for the development of edge computing mechanisms [20], with specialized requirements.

Propagation of information across smart network protocol layers: In classical telecommunications networks, information on faults is propagated across layers via well-defined Operations and Maintenance (OAM) messaging. This information allows fault repair and adaption within both networks and end systems. These systems worked because OAM data was statically defined, networks were rigidly engineered with tightly proscribed deployment architectures, and time scales were defined by standards committees. Within current Internet-based systems there are no equivalent architectural OAM mechanisms. Instead, applications are responsible for inferring the correct response to unknown and unannounced changes in the network. Information flow and control capabilities need to penetrate all layers of the network stack, including the optical layer.

The re-imagined OAM of smart network messaging ties deeply into the network's measurement capabilities, and enables new capabilities for system responses to changing infrastructure conditions and user load. Providing the needed information flows will require research on architectural changes supporting mechanisms for passing information and its attribution, mechanisms for supporting the evolution and addition of new information, and mechanisms for supporting varying time-scales.

Protocol changes induced by changes to network architecture: Envisioned changes to network architecture and new network capabilities may allow for fundamental improvements in basic protocols such as TCP, with the potential for substantial gains in performance and reliability. In addition, fine-grained awareness of network status may allow for the construction of end-to-end services via the composition of piecewise protocol choices based on network operating conditions, rather than as a single protocol that works end to end.

Network modeling for prediction and control: Smart networks will need modeling mechanisms that can be used to predict the result of changes in network and application configurations. To enable effective use in control loops, these models will need to be simple and computationally efficient while also being

accurate. The problem of modeling R&E networks differs radically from that of modeling commercial Internets because the former systems are characterized by small numbers of extremely large flows, flow correlation resulting from scientific workflows, and a desire to run networks at high utilization. As a result, models cannot rely on the statistical properties of many flows. The community currently lacks adequate modeling methodologies for networks in which a small number of flows consume nearly the entire network for extended periods of time.

2.2 Smart Network-Intensive Science Applications

A modern networked system dynamically couples users, applications, and infrastructures. In smart systems, applications and infrastructures are assumed to have built-in intelligence, including the instrumentation and software entities needed to express and satisfy user intents, whether simple or complex. The behavior and properties of each such entity may vary over time, both for internal reasons (e.g., user goes to lunch, router fails,) and in response to changes in other coupled entities. Each type of entity may, if smart, adapt to changes observed in entities of the other types in order to optimize metrics of interest.

Smart applications acting on behalf of users (in the form of autonomous or semi-autonomous agent subsystems for example) may interact both with the underlying infrastructure and with their users. Applications and network infrastructures may each consist of sets of entities that can interact and cooperate in order to effectively carry out tasks that involve the use of resources at many sites.

We define a smart X (whether user, application, or network) as one that understands, interacts with, and adapts to the capabilities and needs of the other elements of this coupled system. Thus, for example, a smart user working with a classic application and network may know how to configure the frame rate and resolution on her videoconferencing application to make it work in a particular situation. Or, she may realize that at a moment of high load she should turn video off altogether to retain good audio quality. A smart videoconferencing application working with a classic network might perform similar configuration changes automatically, given implicit or explicit understanding of user desires for communication quality. A smart network might recognize that a classic videoconferencing application is running and reconfigure itself to avoid the need for changes at the application or user levels. ***A smarter network can thus also enable and improve classic applications*** (and, presumably, also, classic—i.e., less engaged—users). The combination of a smart application and smart network can allow for optimal use of resources on both sides, for example in situations in which a computation is allocated resources to match the expected speed that data will arrive.

Smart users, applications, and infrastructures thus depend on mechanisms for exchanging information about capabilities and needs. They need to be able to:

- ***Discover*** the identities and properties of other elements. (Note that this step requires establishment of common terminology.)
- ***Negotiate*** requirements and actions, for example by the user communicating an intent and an application and/or network agreeing to support that intent.
- ***Agree*** to some actions, for the time being.

This process may be repeated periodically, in which case the different entities participate in an ongoing dynamic decision process.

It is recognized that network-intensive science applications are not typically a single entity. They are often comprised of complex distributed workflows which coordinate actions across many sub-components of instrument, storage, and compute infrastructures. A purpose of this workshop was to focus on how the smart applications, or related workflow agents, should interact with a smart network. For this reason we do not discuss the details of smart application architectures, but consider them in the context of how they will interact with future smart networks.

Given this context, we now discuss requirements that applications (see Appendix D for a representative list) may place on networks. We consider not only smart applications, but also classic applications that can, with a sufficiently smart network, function effectively without built-in smarts.

2.2.1 Smart Applications - Research and Development Areas

Examination of a wide range of application examples led us to identify the following areas in which focused research and development can be expected to lead to more interesting smart applications and/or more effective classic applications.

Network status and history: A universal network status and history application programming interface is needed so that clients can obtain the information required to predict future network performance. This information could include planned network maintenance outages. As an analogy, while an advanced Waze-type application cannot feasibly store complete past traffic knowledge in order to predict how driving times will change over the course of a trip, access to summarized historical information can allow a client to make extrapolations, and information about scheduled road construction closings can increase accuracy yet further. In some cases, specific details for this type of information may need to be kept confidential, in which case information servers must abstract and anonymize what they provide.

Monitoring: Smart applications require better instrumentation and monitoring. For example, a light source data processing application wants to know which network paths support bandwidth reservations and how different paths are behaving, in order to ensure that application needs will be satisfied. Layered monitoring tools are required to allow collection of multiple attributes across network paths, to encompass various measures of quality of service (QoS) and both functional and non-functional attributes. Methods are needed for aggregating data into the information required for different purposes, and for presenting information to users and to AI systems to support informed decision making.

Networks currently are capable of collecting large amounts of data, but those data are maintained independently and often either are available only at the wrong granularity level (e.g., SNMP data) or are not available at all for legal or privacy reasons. There is a need for an advanced monitoring layer that can maintain multiple levels of data and aggregate data into meaningful information, all while controlling who is able to access which information. These aggregation and information delivery functions need to be relevant to user- and application-specific needs for real-time monitoring of network behavior.

In many cases, application flows traverse devices in different administrative domains. For example, an application flow from a national lab to a university goes through devices in the national lab, ESnet, Internet2, possibly one or more regional network providers, and the university. It is challenging for the application to gather information from all of the entities that a flow traverses. perfSONAR data provides some clues about end-to-end network performance but because perfSONAR data collection is controlled by host administrators at individual sites and occurs only for a few endpoint pairs at a coarse granularity (e.g., once every 8 hours), it is of limited utility for many purposes.

Points that indicate the need for advanced monitoring layers include inability for user or application to discover network properties; inability for user or application to request QoS from network; lack of feedback from user to application or network about what works and what does not; lack of global information (within some scope) required to diagnose problems or optimize decisions; lack of feedback from system to user, even simple feedback such as "this will take two days, do you want to continue?"; lack of access to end system log files due to security and privacy issues; information that is inaccessible for administrative or regulatory reasons.

Context-aware smart scientific assistant: Think of a lab notebook that talks back. A context-aware digital assistant would understand what you are trying to do and would use a smart network to bring relevant and useful resources from the network to help you. The realization of this capability will require a smart network that is content-, ontology-, mobile location-, and context-addressable in order to locate, retrieve, or interact with other people, agents, or content that may be relevant and useful to the scientific task at hand. A smart lab notebook would also innately understand the scientific methods being applied, associated documentation requirements, intellectual property capture (inferred when the smart network cannot locate other similar concepts), and team collaboration. A smart notebook could make a user aware of a complementary measurement or simulation being performed by other teams, allowing creation of new collaborations. Current electronic lab notebooks lack a smart network capable of locating relevant information and concepts.

Resilient applications that can interact with smart networks and infrastructure to allow for graceful degradation in cases of resource congestion, much as advanced electrical transmission grids shed or delay low priority use at times of high demand.

Smart services represent the actuator part of a smart network: they contain mechanisms that allow networks to translate and prioritize high-level objectives (such as specific performance or reliability levels) into specific actions that need to be undertaken to achieve those objectives. High-level objectives could, for example, include self-repair/self-healing, reliability, delivery by deadline, and other forms of self-management. Specific actions could include leveraging redundant connections or exploring alternate routes supported by existing topologies, compressing data prior to transmission, or dropping low-priority traffic. These actions could be reactive, i.e., tactically applied to manage a given transfer, or proactive, i.e., anticipating (potentially in a speculative manner) and providing for capacity needs, for example via prediction of failures and pre-emptive actions in response. The latter approach implies that smart services will both have access to global system state and be able participate in the management of this state, for example by employing strategies to reduce overall congestion. In addition to using infrastructure management actions to satisfy its objectives, smart services will also be equipped to negotiate and re-negotiate the high-

level objectives of their clients. The following are some anticipated smart service features and capabilities:

- Higher-level abstractions than the familiar network socket. For instance, service abstractions may include features such as redundant connections, topologies, reliable storage, content distribution networks, and other functions.
- Services which have the following qualities: self repair, self healing, reactive, proactive.
- Autonomic prediction of failures and pre-emptive actions in response.
- Overall management of QoS and QoE from a network user's perspective.
- Distributed security for purposes such as isolation of sensitive information:
    - By its very nature—distributed and connected—networking is the main source of concern when considering security issues. As more scientific applications, collaborations, and even instruments become widely distributed, every aspect of security (authentication, authorization, encryption, partitioning, etc.) becomes both more critical and simultaneously more complex to accomplish. Federated identifiers, domains of trust, encryption, filtering, sanitization—many aspects of security are relegated to points in the networks or specific layers of individual applications where global knowledge is not available.
    - Smart networks offer the opportunity to allow users and applications to request placement of trusted security functions on their behalf elsewhere in the network: for example, network function virtualization instances, traffic sanitations instances, virus filters, and BRO deep packet inspection services.
- Computing in the network, while data is in transit
    - Given an infrastructure of network devices with embedded or attached computing capabilities, certain forms of processing are possible on data streaming through the network in real/near-real time. Examples are simple transformations, such as transcoding of high-resolution video to a lower resolution format requested by a specific client; extraction of statistics from streams (e.g., to determine which files are requested more frequently from a storage infrastructure, in order to optimize the number of replicas and disk pools); and processing of sensor data from a sensor network, such as smart meter data in the power grid to forecast future loads.
- Upgrading in place: Unlike individual computers or even computing facilities, upgrades to the network must be done in place, that is, without interruption of service and without incurring large penalties on users and endpoints. Thus large changes in functionality and behavior must be performed incrementally and staged in a way to allow adaptation and minimize perturbation of the global system.

2.2.2 Further observations

The following observations are also noted regarding interactions between smart applications and smart networks:

- Many applications currently embed a priori knowledge of network configuration and state in ad hoc ways. Delegating responsibility for maintaining such knowledge to the network will allow more applications to benefit from such knowledge and will reduce fragility due to incorrect knowledge. Many other applications currently do not embed or exploit any such knowledge, either because the information is not

readily available or is hard to find. These applications can benefit from knowledge of network capabilities and current status.

- Networks continue to grow in capacity, but science demands are increasing faster than capacity can affordably be added. This evolution, plus the emergence of entirely new applications and the need to manage complex workflows efficiently, result in needs for smarter networks.
- Networks should cater to diverse needs of users for their specific applications, but at the same time optimize overall network behavior.
- We currently see a lot of sneakernet transmission of data at scientific user facilities, whereby scientists move data via physical movement of detachable devices (e.g., carrying a hard disk). Increasing use of Globus across facilities is already changing this situation. We expect users to migrate increasingly to the use of this service.
- Streaming and steering applications require greater support from networks.
- Scientific applications, workflows, and campaigns continue to grow in network awareness and dependence. Many such applications are crafted to a static view of the network and distributed compute resources that may not reflect the ground truth, leading to sub-optimal performance and/or avoidable failure modes.
- The network is in the best position to identify and connect to resources whose locations may not be already known to an application. For example, the best location of scientific data or of relevant publications may be best determined by a smart network.
- A smart network that understands the resources that are accessible through it can be a concierge to the information, applications, and services scientists need.
- Networks that inform users of changes to network state will increase user satisfaction and productivity.
- Smart applications will need an API to access information on both current network status and expected future performance based on statistical interpolations as well as on expected outages.
- Smart networks would benefit many applications and make new discoveries possible across a broad and exciting spectrum of science including physics, chemistry, biological sciences, health sciences, materials sciences, urban science, geo and climate science, engineering and energy technology, mathematics, and computer and information sciences.

2.3 AI-Based Smart Networks

The emergence of SDN-based networks, in particular their enabled programmability, combined with extensive measurements from instrumentation, provides unprecedented opportunities for the application of AI methods. Recently, AI methods have witnessed significant advances, leading to first-time solutions to a wide spectrum of complex problems ranging from natural language processing to medical diagnosis. The DOE Machine Learning and Understanding for Intelligent Extreme Scale Scientific Computing and Discovery workshop [21] evaluated machine learning in the context of high performance computation environment and application optimizations. Opportunities for the application of AI technologies has been recognized in a much broader scope in the National AI R&D Strategic Plan [5] developed by the National Science and Technology Council, Networking and Information Technology Research and Development (NITRD) Subcommittee. That document identified communications as an area that should look to leverage AI technologies. In terms of smart network systems, AI enables the application of advanced automated methods for planning, monitoring, analysis, reasoning and control of these new

network infrastructures. In particular, there is a growing interest in applying AI technologies to network design, planning, management and operations in order to enable effective use by facility operators and science users.

AI is a broad term that includes expert systems, neural networks, natural language processing, fuzzy logic, bio-inspired algorithms, knowledge representation and reasoning, machine learning, deep learning, and many other areas. Among them, machine learning, knowledge representation, automated planning and reasoning, data and information fusion, and heuristic search and optimization are among the most relevant technologies from a smart network systems perspective. In particular, future smart SDN infrastructures will entail and produce large amounts of information about network topology, traffic and other system measurements, and user behavior. Such disparate, multi-modal data must be correlated in order to realize value-added services such as optimal planning and deployment, operations and diagnosis, performance optimization, and user support. This correlation task requires that these SDN infrastructures be tightly integrated with AI processes such that (i) design and deployments are optimized using intelligent search, reasoning, and optimization methods, and (ii) operations and science workflows are supported by machine learning and other techniques for continuous and real-time performance monitoring, diagnosis, optimization, and tuning. Overall, AI techniques hold an enormous promise in realizing the vision of self-awareness, self-configuration, self-healing, and self-optimization properties in science networking infrastructures.

Potential Big Gains

AI methods have the potential to enable radical improvements in the scientific productivity of the DOE science complex from the perspectives of both infrastructure and science:

- *Improved DOE Science Complex:* The utilization, fault-tolerance, and resilience of the entire DOE science complex, including its supercomputers, storage systems, instruments, and networks, can be improved significantly by using AI-based reasoning and optimization. These approaches are expected to enable effective control, troubleshooting, continual monitoring and improvement.
- *Improved Scientific Discovery*: AI methods can enable the development of new science tools that lead to faster scientific discovery via automation of currently manual workflow configuration and optimization tasks. Indeed, the entire science infrastructure can be presented as a single unified resource that relieves scientists from network-level details through automatic intent-aware operation.

Workshop participants identified two key broad functional areas in which AI methods can be applied to next generation smart networks: (a) network operations and optimization, and (b) intelligent network services. The former seeks to exploit the latest advances in AI to make networks function smarter by learning critical aspects of network operation on-the-fly. For example, we anticipate accurate forecasts of user needs, estimates of high efficiency configurations, and identification of network states that may lead to instabilities. The latter seeks to provide powerful computation and analytic capabilities to respond to complex user service requests. These functional areas can be mapped into the following more detailed technical areas:

1) *Smart Designs and Operations*: Current network designs and operations are carried out within the highly specialized constraints of network devices and tools. SDN technologies unify these diverse methods, but also require solutions at broader and larger scales as

networks expand to include virtual and physical components. These advanced capabilities require unprecedented scale and functionalities in their design and operations that can only be realized by AI technologies:

a) Failure detection and robust operations: Failures can be detected using AI approaches, particularly in early stages, using both learning and reasoning methods. These diagnosis methods may be combined with planning and reasoning methods for graceful degradation responses.
b) Subtle correlations and dependencies: Machine learning and reasoning methods can be used to extract hidden and evolving vulnerabilities by rapidly processing large system design and measurement based datasets. AI methods are particularly well suited for sifting through large datasets to map vast spaces of cyber-physical correlations and extract subtle dependencies and correlations. These findings can be combined with planning and reasoning methods to identify cost-effective performance improvement strategies.
c) Optimal allocation and scheduling of the science complex: Complex optimization problems may be solved using methods such as genetic algorithms and approximate planning algorithms for co-scheduling networks together with supercomputers, storage systems, and science instruments. These solutions promise high utilization of science-networked environments by effectively mapping science workflows to available resources, thereby contributing to improved science productivity.
d) Next generation network and science interfaces: AI methods promise significantly improved tools for both network operators and science users. Simple, intuitive interfaces can make these new tools easier to use, for example, by supporting high-level, natural language commands.

2) *Continuous Awareness and Performance Improvement*: Next generation infrastructure can offer a number of potentially game changing capabilities:
   a) Trend detection and tracking: Network infrastructures can be made self-aware via continuous processing of large quantities of monitoring data to detect and tract both current trends and subtle incipient trends. Positive trends can contribute to high utilization, for example, by enabling smaller queues and faster responses to science requests. Negative trends such as users gaming schedulers and increased cyber attack attempts can be used to trigger timely responses.
   b) Anticipation and projection of future trends: Significant advances can be made to move beyond current practices of simply reacting to increased/decreased demand by anticipating and projecting future capabilities. In a more general case, the impacts of future technologies can be assessed by using AI reasoning methods, for example by projecting the impacts of quantum and superconductor computing on science productivity.

The following tasks can be addressed in the short term so that progress can be demonstrated within the context of user-specified functionality:

i. AI analytics methods may be applied to historical data to learn user behaviors, detecting anomalies, perform troubleshooting, and identify network fault correlations.
ii. Data sets and feeds may be developed by carefully/minimally retrofitting easy instrumentation to feed into AI analytics.
iii. SDN-enabled network-aware science workflows may be optimized using AI techniques for performance improvement.

iv. New science-specific abstract interface(s) can be developed with AI-based implementation, staying above computing facilities as black boxes.
v. AI analytics can be applied to intelligently process security monitoring data to extract trends and develop input to decisions.

The long-term goal is to exploit AI methods to provide the DOE science complex with capabilities that far exceed that anticipated in current plans and their projected evolutionary trajectories:

- A Smart Super-Facility for Science: The entire science complex will appear to users as a single, simple, and ready-to-use resource, somewhat analogous to an HPC machine. This resource will span the entire DOE complex such that all components and their interactions are orchestrated by AI-based approaches. The ultimate goal is to provide the entire science infrastructure as a personal "Scientist's Watson" interfaces for both scientists and facility operators.
- Decision Support and Data/Action Interpretability: In addition to providing various capabilities to execute science workflows and operate the infrastructure, this facility supports decision making by providing critical interpretability of extracted datasets and actions executed.

We close this section with a cautionary note. One possible response to this vision of an AI-enhanced DOE science environment is to suggest that these developments may happen by themselves without DOE effort. The following are responses to such a viewpoint:

i. Industry will surely develop some relevant solutions, but their incentive/revenue model is entirely different. In general, the industry model is based on supporting many users with much smaller individual demands. The industry has little incentive to apply AI methods to the unique challenges of R&D environments, since this DOE mission is a zero-billion-dollar market.
ii. Generic AI methods need refinement/customization/adaptation to be effective for DOE science. Furthermore, the mappings from DOE network problems to AI technique are not evident from industry scenarios. Indeed, they need to be developed with intimate knowledge of DOE infrastructures and operations. For example, most of the deep learning algorithms are designed for video and image recognition task which cannot be directly applied for anomaly detection in network traffic data.
iii. AI methods may work extremely well, but it may be hard to determine why they work or if they are likely to continue to work well in future, or how to interpret and act on underlying factors. Also, trade-offs between interpretability and network-level performance may become unclear with as AI methods become increasingly sophisticated. Indeed, these solutions are essential and must be developed for specific DOE science scenarios.

2.4 Smart Cyber-Defense for Open Science

Even open science systems are subject to security risks and attack from the computer networks they are connected to. The Open Science Cyber Risk Profile [22] gives examples of these attacks, including targeted attacks on the science itself by hacktivists. The next generation of high-performance smart networks will result in more interconnectivity and fewer well-known, static network properties, complicating network protection. Much as the shift to cloud computing has introduced new threats and afforded new security

opportunities, networks based on dynamic, autonomous, hierarchical control will change the tools at our disposal and the risks we face. While the fundamental principles of security design will not change, new challenges and opportunities emerge. New research is required to articulate new threats and to identify and exploit new opportunities. Without such research, we will not be able to secure the science conducted on these new networks.

Existing cyber security solutions operate under an assumption that the network either does not, or should not, change frequently. For example, anomaly detection systems may track traffic flows between IP addresses, under the assumption that the identity of the node and the IP address are the same. Firewalls and intrusion detection and intrusion prevention systems (IDS / IPS) operate at least partly based on rules about what traffic is and is not allowed to certain internal destinations, again identified by IP address. The network is assumed to consist of well-known nodes, segmented according to criticality or purpose, with "normal" traffic passing between them. The network's "self" is well known largely in a top-down fashion and its organization is designed by network engineers based on long-term needs.

Smart networks change these assumptions by introducing dynamic reconfiguration that, while based on criteria that are known to the maintainers, arise from machine learning and AI algorithms driven by self-observation of the network state, required workloads, and other criteria. The result may well be configurations that are unexpected or unanticipated. This situations breaks existing network security approaches, but also provides an opportunity. The "self" here may be a localized set of nodes at the network edge that have become organized in response to a computational demand, self-healing due to device failure, or as a result of some AI attempting to optimize network features. This just-in-time, self-organized "self" can be said to have some expected flows and usual traffic, but it is also likely to be torn down and re-organized at the next workload.

In order to secure such dynamic networks against tampering, sabotage, misuse, and malicious insiders, and to ensure the availability and integrity of the computing platform and the credibility of the scientific enterprise, new security methods are needed that protect the software, data, physical assets, instruments, and people connected to smart networks. These new methods must be tailored to, and take advantage of, smart network properties. Because some tradeoffs during the development of smart networks may make network protection easier, while others may make network defense harder or even impractical, this effort should take place simultaneously with, and inform, other aspects of smart network research and development.

This report identifies opportunities for research to exploit properties of next generation smart networks to address the cyber security needs of these networks. Specifically, several areas are identified where one can exploit properties of smart networks to enable better security solutions.

- Monitoring of smart networks
- Coordination among different network cyber security policies
- Implementation of moving target defense
- Detection of anomalies
- Tracking of data lifecycle integrity
- Access and authentication

- Security-aware network operations

We explore each of these areas in the following sections.

Smart Network Monitoring

Multi-scale, pervasive, and dynamically tunable monitoring will be essential for the success of smart networks. The resulting measurements will provide both past history and current status of the network, and will be the main inputs for smart network management, cyber security, and various AI and machine learning algorithms employed by smart networks. Different components will have different monitoring requirements. Monitoring all traffic at the finest granularity will be neither feasible nor desirable. Instead, smart networks will need to strive to offer multi-scale, multi-location, and dynamically tunable monitoring.

Two forms of monitoring are considered here.

- Multi-scale smart network monitoring: The scale and granularity at which monitoring is conducted must reflect the needs of network components and must be flexibly tunable as requirements change.
- Multi-location distributed monitoring: In contrast to traditional middle-box-based, centralized monitoring, which is neither scalable nor cost effective, the smart network must pursue a multi-location, hierarchically distributed network monitoring approach that uses instrumented devices throughout the smart network.

A lightweight and dynamic monitoring approach would many benefits. First, it can satisfy the requirements of various smart network components without overloading the underlying networks with large volumes of monitoring traffic. Second, multi-location distributed monitoring offers a local view of each network subsystem. Security solutions can readily use the local monitoring data to conduct local cyber defense, and only propagate measurements of global importance to higher levels of the hierarchy, reducing monitoring traffic overhead. This approach enables incorporating defense-in-depth into the network design, so that security alerts are shared among all relevant security components at every level before making a final (global) decision.

While the implementation of such a smart network monitoring system is challenging, several technologies have the potential to contribute. Instrumenting the existing network devices provides a way toward implementing multi-scale, distributed monitoring. For instance, Wang et al. [23] demonstrate the possibility of instrumenting Open vSwitches to provide multi-scale monitoring at the network edge. Another possibility is to use the upcoming programmable network devices, such as P4-capable network routers [24], to provide tunable monitoring services. Finally, network monitoring can also be implemented by using a networking function virtualization (NFV) technique. Monitoring points can be dynamically triggered or eliminated as the needs of the cyber security solution and other networking components change.

Cyber Security Policy Coordination

Smart network technologies inherently imply end-to-end network services, where end-to-end nominally means NIC-to-NIC. A customized network service that is consistent across all independently-administered network domains along an end-to-end path will require an operational framework capable of providing that service within each domain. There will be

cyber security policy aspects of that operational framework. Each end site and transit network will have its own cyber security policies and procedures. Each end-to-end network service will need to conform to domain cyber policies all along the path. These requirements strongly suggests the need for a cyber security policy coordination component within that operational framework. Such a coordination component would need to not only be capable of providing approval for local network configurations and services within its domain purview, but also of negotiating acceptable service permissions, characteristics, and parameters with other domains.

Policy coordination across network domains would not be limited to application data movement. Smart networks will be instrumented to generate a wide spectrum of operational and performance measurement data. Cyber security policy coordination will be necessary to allow access to local operational and performance data in a manner consistent with local policies on that data.

Moving Target Defense

The same dynamic, software-defined configuration capabilities that will make smart networks easier to use and more responsive can also support enhanced cyber security through the "moving target" concept. Conventional static configurations mean that a vulnerability, once discovered, can be exploited at will. The uncertainty faced by attackers can be increased, and their chances of success reduced, by randomizing network implementation details in space and/or time. When such diversity is introduced, exploits that depend on those implementation details require lucky guesses by the attacker and are no longer reproducible in time or space. The semantics for intended function of the network, however, should be left unchanged in this randomization.

For example, dynamic reconfiguration involving diverse, rapidly changing routes, addresses, and protocols could frustrate attacks that depend on consistent internal responses, while maintaining functionality needed by legitimate users. Addresses (including hardware addresses) and routes would hop randomly but synchronously based on a common configuration seed. The interface would allow authorized users to access the network consistently through knowledge of this seed, which attackers would not have.

In a more comprehensive approach, redundancy in the network (which may already be needed for reliability) would also be made diverse, embedding moving target in a voting system. Multiple protocols or routes would process a given request in parallel so that, if a vulnerability were triggered in one of them, it could be detected as a discrepant response and discarded, further reducing an attacker's chances of success. While the simplest version of this approach would involve expensive triple redundancy, more efficient redundancy approaches for security analogous to error-correcting codes could be investigated.

Anomaly Detection

Smart, dynamic networks may provide an opportunity to create new, basic security mechanisms or to improve existing mechanisms. Network anomaly detection is one example. The goal here is to subject observable features like traffic volume, mix of applications, or communications profiles of individual hosts to a test that categorizes them as normal or deviant. Events are selected such that deviance indicates a security failure that can then be diagnosed and corrected.

Unfortunately, network anomaly detection, as it is most often implemented today, has a significant drawback rooted in what is termed the *base rate fallacy*. The fallacy describes the false belief that a process that can correctly classify an individual event as normal or anomalous a large fraction of the time will necessarily make a good filter for a large population of events in which anomalies are rare. Even highly accurate tests can result in large numbers of false positive responses in such situations, which are furthermore typical of most network traffic. Frequent false positives waste resources and destroy confidence in a filter, rendering it useless.

There is some chance that the combination of HPC applications and clean-slate smart networks could combine to overcome the worst effects of the base rate fallacy. To be an effective filter for exceptionally rare events, the detector on which it is based must be nearly perfect. HPC workloads already exhibit less diversity, have more regular patterns of network behavior, and afford malicious software much less noise in which to hide than do general enterprise or Internet applications. That combination should, in principle, allow more accurate detectors. Further, an SDN application, running on a suite of hierarchical, distributed controllers, could establish single purpose virtual circuits, on demand, for specific network use cases like file transfer, interactive login, or even application-specific halo exchange. If the custom application protocols allowed within such a circuit were designed to be extremely constrained and transparent, then lightweight controller-deployed monitors would be more likely to distinguish acceptable from anomalous network traffic correctly. Selectively trading protocol flexibility and diversity for analytic tractability is one example of a larger engineering pattern that smart dynamic networks may enable in the service of security.

Data Lifecycle Integrity Tracking

Smart networks allow significantly higher levels of instrumentation, data gathering, and monitoring than are possible in traditional networks. The versatility of these systems allows for approaches to protecting data integrity that are unprecedented in current networks. Scientific data has a particular need for data integrity protection and tracking throughout its lifetime from data gathering / creation to model completion or publishing. Smart networks will allow us more flexibility in offering cyber subsystems to provide these types of features transparently to the science user. These features will also allow security analysts and network security operators forensic capabilities currently unavailable in traditional networks.

One possible implementation of such an audit system would involve the use of blockchain, as used in bitcoin and other emerging areas in the tech and financial worlds. Blockchain offers a novel approach to tracking data assets through multiple transactions. A smart network could offer a blockchain ledger as a cyber subsystem to an open science network. This ledger would allow a data user (scientist), security analyst, or auditor to see changes to data correlated to a user, a date/timestamp, and a network location. The cryptographic properties in blockchain would prevent tampering with the ledger itself and would allow any tampering of the actual data to be traced to a time/location, or at minimum, a time between check-ins.

There would immediate benefits to this type of audit trail for both the scientist and the security analyst, if it could be realized. It would allow the scientist to track and verifiably show the chain of custody, development, and changes for her data from creation to publishing (or any other lifecycle the data may go through). It would provide the security

analyst with a closer audit trail and forensic path to attempt attribution or discovery of potentially compromised nodes in the event of data tampering.

There are a number of potential implementation locations for this type of audit trail. Implementing it within the network stack, as an extension to a transport layer protocol, for instance, is attractive, but seems likely to be prohibitively difficult. Implementing it at the file system layer is much more approachable but requires knowledge and/or enforcement of the environment in which the scientist works, which is undesirable. Further investigation is definitely required, but one solution may be to implement it as part of the network monitoring infrastructure. This approach has some obvious drawbacks, most notably that it would limit the full chain of custody benefit to the scientist, who would have audit trails only for data that flowed across the network. This approach also places infection of the working host deliberately out of scope. Nevertheless, the potential benefits are numerous:

1. Much of the needed logistics already exists, thanks to existing support for full packet capture of individual flows at sender and receiver. The data portion of the packet capture should be cryptographically verifiable on both ends of the flow.
2. This approach could be implemented transparently to the scientist.
3. Network and security teams could work with scientists to determine how much data should be archived for a given mission space, problem set, workflow, etc.

While a number of unanswered questions remain, this approach has a great deal of potential to improve security in an open science network.

Access and Authentication

It is essential to maintain flexible controls that can prevent damage to, or theft of, data by unauthorized users, while also enabling access to systems by legitimate users. However, there is no one system or method of user/group authentication; the myriad of current methods of access and authentication for national resources such as supercomputers, instruments, and data sets are uncoordinated, difficult to use, and hard to manage. This situation complicates auditing and makes it also impossible to create a baseline profile of normal use, as would be required to identify rogue users or misuse.

Some of the challenges to maintaining such access and authentication systems are that users of computing systems and instruments are widely dispersed and frequently include international collaborators or students. One area to consider improving is a more robust framework around federated identity, such that users from disparate organizations can seamlessly access resources. Several barriers currently exist to federated identity becoming a solution for access to instruments, resources, and virtual organizations. For example, national level scientific resources often have their own identity provider service for users who are not affiliated with a campus or organization.

Future smart networks may enable improved access and authentication due to the potential ease of identifying user behavioral patterns within and across networks as well as user activity while on a network. The ability to create user profiles that constitute normal activity (e.g., expected patterns of behavior for a scientific researcher versus a sysadmin), and thus to detect anomalous actions, would make it easier to identify rogue users, misuse of assets, and exfiltration of sensitive data.

Some of the benefits of more fine-grained access control that is integrated into and more tightly coupled with networks are the following.

1. *It is easier to identify users engaging in malicious activity within and across systems.* The granting of highly privileged access to authorized users is particularly dangerous if intentionally misused. Smart networks enable the rapid identification, isolation, and containment of such behavior, avoiding further damage to systems.
2. *Provides for more seamless administration of systems.* Currently there are several layers of network access, application access, and data access in addition to multiple (often federated) software systems for credentialing which must be updated and administered. Building a more seamless administrative framework across DOE labs and national resources, which are contingent on interconnected high speed networking and integrated with network administration, can ease administrative burdens.
3. *Provides integration with networking, scientific workflows, and data provenance.*
4. *Enables data integrity*. Users can collaborate on their data without anyone getting access to their data unless they authorize it.

Continuous multi-factor authentication is an emerging trend of modern authentication research. A one-time validation of a user's identity is inadequate to secure their credentials for a long workflow. The user of both active and passive authentication modalities is essential to continuously authenticate users with the help of behavioral and cognitive traits. Ideally, such an authentication system should be fast in execution, non-intrusive, and application and hardware independent, and it should use different behavioral attributes at different times.

Security-Aware Network Operations

One objective of smart networks is to enable intelligent network operations without humans in the loop. They can thus allow networks to react promptly to changing conditions and to achieve higher regimes of performance, improving overall user QoE. One important component of QoE is security, understood as the degree to which a user's interactions with the network are safe. In order to ensure the QoE of smart networks, traffic engineering decisions will need to take into account the intelligence provided by the security systems.

Through the separation of the application, control, and data planes, smart networks enable real-time modifications of the parameters and tables that control data plane network elements, changing the routes and policies that such elements apply to data packets. In smart networks, these real-time changes will be orchestrated through a system of inputs that will incorporate both data sensed from the network itself and the processing of such data via AI applications. Such intelligent applications will need to incorporate information from the security layer.

The interactions between traffic engineering and the smart cyber security systems will need to identify optimal trade-offs between the amount of information that can be processed to ensure proper network visibility and the cost of such processing. A classic example of interactions between the two domains involves a two-layered approach. The first layer collects data at a coarser granularity level with the goal of reducing the size of the search space (the number of false positives) without affecting data plane performance. Upon detection of potentially malicious activity, traffic engineering in smart networks can be used to reroute the suspicious traffic to another path involving a second layer of deeper, finer

granularity analysis. This second layer is responsible for discarding false negatives. Upon detection of an attack, further traffic engineering rules can be applied to block the traffic.

Intelligent security analytics for smart networks will necessary involve their cooperation with the network operations sub-system to protect them from cyber threats.

3 Opportunities, Challenges, and Actions

Realization of a smart network that reflects autonomic characteristics is an ambitious vision, which necessarily requires multi-disciplinary research and development. The communications and Internet industry is now at a unique inflection point due to the convergence of multiple technologies that have matured to the point where integration and cross-disciplinary adaptation can lead to building such smart systems, which were not previously possible. This workshop reflected this need for integration, with discussion spanning the network infrastructure, application, AI, and security areas.

The opportunities identified for smart networks innovation are significant. This is an ideal time for the R&E community to define its vision for these smart network systems, as the commercial industry is moving rapidly in complementary directions. The R&E community should leverage technologies being developed in the commercial space, and take those technologies beyond commercial horizons and extend or tailor them to meet unique science community requirements. This early phase of technological transition also presents an opportunity for the R&E community to drive the direction of smart network systems evolution, and to influence commercial vendors to include feature sets needed for domain science applications.

While the component technologies are maturing to the point where integration can be imagined in the form of smart networks, the challenges of realizing this integration are equally significant. As the component technologies continue to mature, there will be many options, features, and implementations that need to be evaluated for possible use or extension. The work of integrating the component technologies into a smart network system will be complex. Different use cases will need to be approached in unique ways. The DOE environment will be driven by emerging systems such as superfacilities, exascale computing, science instruments/experiments, and big data analytics, each with unique requirements as compared to commercial activities.

Based on the vision for future smart networked systems, and the discussions held during this workshop, the following key focus areas and activities are identified to address the many opportunities and challenges.

Short-term opportunities for action (2-5 years):

- Establish a study group to define an architecture and associated requirements for a smart networked ecosystem that encompasses network infrastructure, applications, AI technologies, and security functions. This study group should identify suggested development timeframes for the various requirements and technology areas. The output of this group should be of sufficient detail to guide prototype development. For a complex system such as a smart network ecosystem, the recommended approach is design, prototype, test, evaluate, modify design, and then iterate

through this cycle until a satisfactory solution is developed. This task is the initial prototype design phase.

- Provide an experimental infrastructure where component and system level functions can be prototyped. This experimental infrastructure needs to include realistic hardware and software systems across multiple network layers, have sufficient scale to evaluate solutions, and be breakable in order to allow robust prototype evaluation and testing.
- Establish R&D programs to support the design, prototyping, and evaluation of various elements of a smart network system ecosystem.
- Define three to five initial smart application experiments that leverage smart network testbeds.
- Form a multi-disciplinary team across DOE facilities, networks, and laboratories as the basis for this work and to enable knowledge transfer more widely within the DOE and general R&E community.
- Train application developers and develop best practices regarding use of new methods associated with the smart networked ecosystem.

Longer-term opportunities for action (6-10 years):

- Include capabilities within the near-term experimental testbeds and support longer-term experimental testbeds that enable experimentation on the next evolutionary steps of the hardware—beyond what can be done with commercial hardware
- Take successes from the first phase and establish partnerships (e.g., with industry and R&E networks) to enable broad deployment across DOE and other networks.
- Transform networking research via the research, development, and deployment of a new generation of smart networks.
- In so doing, increase productivity of DOE science and engineering programs through engagement with smart network systems and development of corresponding smart applications.

4 Findings

The following key findings and observations are noted. These are drawn from the discussions across all of the workshop technical focus groups and plenary sessions.

- *Networks are at a technology inflection point, with the next phase being a transformation from a passive infrastructure to a smart system that forms the core of the smart networked ecosystem.*

  We are now at the early stages of a networked systems technology and infrastructure inflection point. We use term network systems here to refers to the network infrastructure and the things that connect to and rely on the network. This inflection point is being driven by the convergence and maturation of several technologies that have been largely disjoint to date with regard to their individual development. Network designs are evolving at a rapid pace toward automation and programmatic control, driven in large part by SDN concepts and technologies. AI technologies and systems are also evolving rapidly and are being applied to a wide variety of use cases. Big data systems and analytics technologies are readily available and being used across many domains. These and other technologies will be integrated in unique way to create truly autonomic, self-aware, smart networks. This development will enable a smart networked ecosystem to evolve such that the

network becomes an interactive component for use by similarly smart applications, security systems, and other domain specific use cases.

- *Smart Networked Ecosystems will be critical to enable future innovations across the core DOE mission domain science communities.*
  It seems clear that current static, non-interactive network infrastructures do not have a path forward to assist the domain science application innovations. There is a somewhat of a chicken and egg issue where the application developers need a smart network with which to interact, and the networks builders need some requirements from the applications people to build the smart network. The best way to bootstrap this process is to form multi-disciplinary teams that can employ an iterative design a little, build a little, test a little strategy. This approach will provide a basis for more detailed and comprehensive designs and visions.

- *The DOE R&E community should be proactive in defining future smart networks functions and designs.*
  The smart networked ecosystem transformation is an emerging activity that will be of interest to both the commercial and R&E communities. The R&E community represents a unique environment from the perspectives of both smart network use and development. R&E science workflows are generally distributed and multi-domain, often spanning DOE Laboratories, wide area networks, regional networks, and university campuses. As a result, smart network functionality has to be considered and developed in a federated and multi-domain context. In this environment, autonomous smart network domains will need mechanisms to interact with each other, or with higher-level workflow agents, in order to coordinate operations that cross multiple domains. In contrast, commercial smart network activities are likely to focus more on operations and cost reduction issues within individual networks. The R&E community will need to leverage technologies being developed in the commercial space, but must take those technologies and extend and tailor them to meet the unique requirements of science. The R&E community should be proactive in defining requirements and developing prototypes for smart networked infrastructures early in this development phase. This approach will provide the best opportunity to influence and leverage commercial activities which can then be tailored and applied to the DOE environment.

- *Prototyping on at-scale testbeds will be critical to the development of complex systems such as a smart networked ecosystem.*
  The iterative build-and-test prototyping of complex systems that include multi-technology integration will require access to an experimental infrastructure where component and system level functions can be deployed and evaluated. This experimental infrastructure needs to include realistic hardware and software systems across multiple network layers, have sufficient scale to evaluate solutions, and be breakable in order to allow robust prototype evaluation and testing.

- *Network Infrastructures are changing and the people that build and operate them will have to change as well.*
  Networks are evolving from manually configured infrastructures providing a relatively static set of services, to software-driven systems that rely on programmatic control to build, operate, and interact with clients. As a result, the

skill sets of network builders and operators will also have to evolve. As detailed network configurations will increasingly be handled by software, operators will need the requisite software skills to operate and control the network. In addition, as the level of interaction increases between the network and the things that attach to, or use, the network, there will be a great need for technical staff who can understand and operate across boundaries between disciplines and infrastructures. For example, there will be a need for personnel who can understand and debug issues from both the smart applications and smart network infrastructure perspectives.

- Multi-disciplinary teams should be formed to keep the focus on the enhancement of domain science and related DOE facilities.
  All of this work will require the formulation of multi-disciplinary teams with experts from the network research, domain science, and DOE facilities communities. A formal process should be identified to define the user driven requirements from the domain science and facilities communities. These requirements should then drive the smart networks research and development activities which include experts from the network infrastructure, applications, AI, security, facilities, and other component technology areas. A continuous dialogue between these multi-disciplinary team members should occur as part of the design, build, test iterative process. These teams can also provide a mechanism for smart system knowledge transfer within the DOE and general R&E community.

References

[1] Kephart, J.O.; Chess, D.M. (2003), "The vision of autonomic computing", Computer, 36: 41–52, doi:10.1109/MC.2003.1160055

[2] Autonomic Networking: Definitions and Design Goals, https://datatracker.ietf.org/doc/rfc7575/

[3] A Reference Model for Autonomic Networking, https://datatracker.ietf.org/doc/html/draft-ietf-anima-reference-model-02

[4] An Autonomic Control Plane, https://datatracker.ietf.org/doc/html/draft-ietf-anima-autonomic-control-plane-05

[5] National Science and Technology Council, National Artificial Intelligence R&D Strategic Plan, October 2016, https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf

[6] On-Demand Secure Circuits and Advance Reservation System (OSCARS), https://www.es.net/engineering-services/oscars/

[7] ATT Domain 2.0 Vision White Paper, November 13, 2013, http://www.att.com/Common/about_us/pdf/AT&T Domain 2.0 Vision White Paper.pdf

[8] "Network Functions Virtualization-Introductory White Paper" (PDF). ETSI. 22 October 2012, 20 June 2013, http://portal.etsi.org/NFV/NFV_White_Paper.pdf

[9] OpenROADM multi-source agreement, http://openroadm.org

[10] ONOS: Open Network Operating System, http://onosproject.org

[11] OpenDaylight, Open Source Software Defined Network (SDN) Controller, https://www.opendaylight.org

[12] OpenConfig, vendor neutral, model driven network management designed by users, http://openconfig.net

[13] WaveLogic AI, machine learning based network management product feature, http://www.ciena.com/products/wavelogic/wavelogic-Ai/

[14] Energy Sciences Network (ESnet), www.es.net

[15], Internet2, www.internet2.edu

[16] ASCR, *Software Defined Networking for Extreme-Scale Science: Data, Compute, and Instrument Facilities*, Report of the DOE ASCR Intelligent Network Infrastructure Workshop, August 5–6, 2014, http://www.orau.gov/ioninfrastructure2014/default.htm.

[17], perfSONAR network test and measurement infrastructure, http://www.perfsonar.net

[18], Sampled Flow, http://www.sflow.org/sflow_version_5.txt, https://www.ietf.org/rfc/rfc3176.txt

[19], IP Flow Information Export (IPFIX), https://tools.ietf.org/html/rfc7011

[20] Satyanarayanan, Mahadev. "The Emergence of Edge Computing." *Computer*50, no. 1 (2017): 30-39.

[21] Machine Learning and Understanding for Intelligent Extreme Scale Scientific Computing and Discovery, DOE Workshop Report, January 7–9, 2015 Rockville, MD, https://www.orau.gov/machinelearning2015/Machine_Learning_DOE_Workshop_Report_6.pdf

[22] "OSCRP: The Open Science Cyber Risk Profile," CTSC and ESnet, on web: https://trustedci.github.io/OSCRP/ (retrieved on December 9, 2016).

[23] An Wang, etc. "UMON: Flexible and Fine Grained Traffic Monitoring in Open vSwitch", ACM CoNEXT 2015.

[24] "P4: High-level Language for Programming Protocol-Independent Packet Processor", http://onrc.standford.edu (retrieved on December 9, 2016).

Appendix A Workshop Agenda

Smart High-Performance Networks
Toward a New Generation of Intelligent Networking Infrastructure for Distributed Science Environment
Workshop

Rockville, Maryland
December 8-9, 2016

Sponsored by the U.S. Department of Energy
Office of Advanced Scientific Computing Research
Agenda

Thursday, December 8, 2016

7:30 am Registration, Continental Breakfast
8:30 am Workshop Topics, Goals, and Report Schedule
9:00 am Plenary Talk, Cees de Laat (University of Amsterdam)

9:45 am Technical Focus Area Overview and Charter
The leads from each technical focus areas provide an overview of the area, emphasizing the smart network context, setting the expectation for the level of discussion detail, and breakout group outputs
1) Smart Networks (Tom Lehman, Inder Monga, Bryan Lyles)
2) Smart Applications (Ian Foster, Raju Vatsavai)
3) AI-Based Technology for Smart Networked Systems (Prasanna Balaprakash, Kalyan Perumalla, Nagi Rao)
4) Smart Cyber Security Sub-systems (Stacy Prowell)

10:45 am Break, Refreshments
11:00 am Focus Area Breakout Groups
Parallel breakout groups for each technical focus areas:
1) Smart Networks
2) Smart Applications
3) AI-Based Technology for Smart Networked Systems
4) Smart Cyber Security Systems
Each breakout group may start with one or more talks by a technical area expert

12:30 pm Lunch
1:30 pm Focus Area Breakout Groups
3:30 pm Breakout Group Summary Reports
5:00 pm Discussion about the workshop process and activities,

	Review plan for next day
5:30 pm	Dinner: on your own

Friday, December 9, 2016

7:30 am	Continental Breakfast
8:30 am	Welcome and Plan for the day
8:45 am	Focus Area Breakout Groups
10:45 am	Break, Refreshments
11:00 am	Focus Area Breakout Groups
12:30 pm	Lunch
1:30 pm	Breakout Group Summary Reports
2:30 pm	Group Discussion and Workshop Summary
3:00 pm	Workshop End

3-4:00 pm Workshop Report Writing Group

Appendix B Smart Networks Workshop Attendee and Report Author List

DOE/ASCR Smart Networks Workshop – Attendees and Report Authors		
Last Name	**First Name**	**Institution**
Anitescu	Mihai	Argonne National Laboratory
Balaprakash	Prasanna	Argonne National Laboratory
Berry	Michael	University of Tennessee
Calyam	Prasad	University of Missouri-Columbia
Cole-Rhodes	Arlene	Morgan State University
Dasari	Venkat	U.S Army Research Laboratory
Dasgupta	Dipankar	The University of Memphis
Delaat	Cees	University of Amsterdam
DeMar	Phil	Fermi National Accelerator Laboratory
Dumitraș	Tudor	University of Maryland, College Park
Foster	Ian	Argonne National Laboratory
Guo	Yang	National Institute of Standards and Technology
Hess	Bryan	Thomas Jefferson National Accelerator Facility
Hicks	Susan	Oak Ridge National Laboratory
Jones	Todd	Sandia National Laboratories
Jukan	Admela	Braunschweig University of Technology
Katramatos	Dimitri	Brookhaven National Laboratory
Keahey	Kate	Argonne National Laboratory
Kettimuthu	Raj	Argonne National Laboratory
Kilper	Dan	University of Arizona
Kiran	Mariam	Esnet/Lawrence Berkeley National Laboratory
Lake	Andrew	Esnet/Lawrence Berkeley National Laboratory
Lehman	Thomas	University of Maryland/MAX
Liou	Chris	Infinera
Lyles	Bryan	Oak Ridge National Laboratory
Mack-Crane	Ben	Corsa Technology
Mayo	Jackson	Sandia National Laboratories
Medard	Muriel	Massachusetts Institute of Technology
Monga	Inder	Esnet/Lawrence Berkeley National Laboratory
Newman	Harvey	California Institute of Technology
Nikolich	Anita	National Science Foundation
Perumalla	Kalyan	Oak Ridge National Laboratory
Prete	Luca	Open Networking Laboratory
Prowell	Stacy	Oak Ridge National Laboratory
Ramamurthy	Byrav	University of Nebraska-Lincoln

Rao	Nagi	Oak Ridge National Laboratory
Ricart	Glenn	US Ignite
Ros-Giralt	Jordi	Reservoir Labs
Russell	John	AAAS/National Science Foundation
Samadi	Payman	Columbia University
Spentzouris	Panagiotis	Fermi National Accelerator Laboratory
Thompson	Michael	Argonne National Laboratory
Toby	Brian	Argonne National Laboratory
Tull	Craig	Lawrence Berkeley National Laboratory
Vatsavai	Raju	North Carolina State University
Vokkarane	Vinod	University of Massachusetts, Lowell
Wu	John	Lawrence Berkeley National Laboratory
Yang	Xi	University of Maryland/MAX
Yoginath	Srikanth	Oak Ridge National Laboratory
Yoo	Ben	University of California, Davis

Appendix C Smart Networked Systems Terms Definition

We define the following terms to facilitate the smart network and related systems discussions.

- Network: A computer network or data network is a telecommunications network which allows computers to exchange data.
- Smart network: A network that is enhanced with AI features to observe, interact, negotiate and enhance the quality of the supported applications.
- Workflow: A composable directed acyclic graph of executable components that define and perform a task [on data].
- Application: (Webster) a program that performs one of the major tasks for which a computer is used. In our context, an application is the collection of tasks for which the network and connected data processing resources are used to drive science. The application is typically developed by the scientist based on libraries and APIs that interact with the underlying operating system and the advanced resources.
- Smart application: An application that is enriched with code to interact on behalf of the user/scientist with the underlying infrastructure to accomplish application goals. The extra code can either be coded in the science code or be located in an agent placed next to the scientist's application to act on behalf of the scientist. John: A smart application allows for the reduction of complexity to allow a user to manage an overarching process rather than individual tasks.
- Classic application: an application that is not enhanced in any way to interact with a smart infrastructure, beyond its use of the classic system interfaces.
- User: An interactive client of the system, which may be a human being, process, thread, or autonomous agent. Users as a whole should be able to respond, in turn, to requests or feedback from the system.
- User intent: What the user wants from the network as requirements: can be a high-level goal such as *analyze this set of data* or a technical goal such as *move a given dataset from A to B*. Given the achievability of the goal, the response can be either simple or complex, and the actions taken on behalf of the user can be deterministic or conditional, depending on state changes of the system while the response to the user's request continues.
- Application intent: Is the expected behavior from the network: includes effects of the application interacting with other components in the system (user, network, data, compute resources).
- Network intent: Is the expected response or predicted behavior to a request for a network capability (e.g., QoS reservation request, route for requested transfer), or a prediction of future behavior or status (e.g., future changes, degradations, or outages of paths or capabilities due to planned HW changes or extant-promised QoS commitments).
- Network-intensive applications: Applications that place unusual demands on networks, e.g., substantial fraction of available bandwidth, real-time QoS. Better than best effort; or Applications that rely for critical application capabilities or behavior on interaction with the network or explicitly with network-connected resources.

- Security: Methods of preserving confidentiality, integrity, and availability of information. Certain classes of information, such as HIPAA or export controlled, may require encryption or other precautions due to regulation.

Appendix D: Classes of Network-Intensive Science Applications

Network-intensive applications can be categorized along the two axes of communication volume (from low to high) and required response time (from days to milliseconds). These simple linear scales can encompass complexities such as latency, jitter, and burstiness. We can easily add further axes, such as scalability (number of concurrent users, flows, activities, sensors, etc.) and security (degree of concern about illicit access). Group discussions identified many compelling applications along these axes, such as the following.

Real-time processing of data from BES experimental facilities. There are numerous exciting opportunities for real-time processing of data from Basic Energy Sciences (BES) experimental facilities that would benefit from smart network capabilities. For example, at the Linac Coherent Light Source (LCLS) and upgraded Advanced Photon Source (APS), high data rate streams are to be transferred to high performance computing (HPC) systems and processed within seconds of acquisition in order to permit experimental modalities based on computer-in-the-loop automated control of experiments. Such configurations are either entirely impossible or impractically complex to realize today, due to lack of global information about network capabilities and inability to obtain dedicated, reliable network connectivity, and a consequent need for extensive human effort for discovery and control. Not all cases are related to large volume data transmission. Some applications may need to negotiate for low-latency or highly robust connections, for example when remote feedback is needed to operate an experiment (instrument, robotics, data acquisition) or when scheduled or streaming data transfers must keep up with remote data reduction processes, in which case packets must always arrive with a known maximum delay. Similarly, only if the expected data transfer rate is known does it become possible to anticipate the optimal parallelization scaling for a remote data reduction process.

Real-time steered simulations are an emerging theory and modeling methodology of interest to BES and Biological and Environmental Research (BER). For example, steered molecular dynamics simulations allow scientists to manipulate structures during a simulation by pushing or pulling along desired degrees of freedom, thus reducing the range of configurations to be sampled through expert guidance. A scientist can thus start to explore how a structure may or may not fit together, providing a physical understanding of stochastic processes that would otherwise take a long time to occur in simulation time. This methodology has many applications, including protein folding, drug delivery, docking, and protein-protein binding. Such simulations require advanced visualization capabilities and a smart, fast, and reliable network.

Fusion: A major challenge in fusion research is to identify and avoid or reliably mitigate large-scale disruptions within the tokamak. Recent research is geared towards analyzing big data consisting of multi-dimensional observations such as electron temperature profiles from electron-cyclotron emission measurements from tokamak systems such as the Joint European Torus. A key requirement is to predict these disruptions in real-time in order to avoid costly damage to the machine.

High Energy Physics (HEP) workflows involve hundreds to millions of tasks processing petabytes of data distributed among tens to hundreds of sites. Key steps in the workflow include the production and distribution of real and simulated input datasets, processing of datasets at sites, and delivering output datasets to groups of users for further analysis.

Small and large production workflows may be re-executed on the same data following software releases that provide improved methods and/or calibrations. In each case, researchers want to improve time to solution, resource utilization, and runtime predictability via dynamic and elastic resource provisioning. A key required capability is then to provide access to data at the right time to the right computational resources, and eventually to users for further analysis and possibly for additional code development.

Computational resources are multi-architecture, multi-platform, and heterogeneous, provided by traditional grid, commercial, and academic cloud and HPC providers. Data are not necessarily collocated with computational resources. For example, in the HEPCloud superfacility, which aims to provide solutions for High Luminosity (HL) Large Hadron Collider (LHC) and the international Neutrino program, workflows may burst to either HPC systems or to commercial clouds. However, orchestrating and optimizing this bursting currently involves a lot of complexity. Moving key functionality to the network layer (e.g., security policy, monitoring, and decision making on which resources to use for bursts) will be of great value. Realizing such use cases will require that the application be able to first communicate intent and high-level metadata to the network layer and then adapt (or not) its intent based on information provided by the network layer.

Large-scale machine learning for cancer: Pilot projects involving DOE, the National Cancer Institute, and Veterans Administration are using DOE supercomputers for large machine learning computations on various cancer-relevant data. As the data considered extend to clinical records, confidentiality is a big concern. Labs are creating secure enclaves to hold and process personal health information, but such enclaves are expensive and inflexible. A smart network that could ensure that designated data did not leak outside designated boundaries would be far more flexible.

Analysis of large distributed data: Scientific communities are increasingly storing data in distributed repositories and databases, rather than within monolithic single sources. Biological data such as genomic or proteomic data of relevance to biomedical research, climate data in the Earth Systems Grid Federation (ESGF), and materials information of relevance to the Materials Genome Initiative are stored in distributed databases. A smart network would simplify access to, and transfer of data from, these repositories, for example by allowing applications to determine the best copy to access at a particular time, based on current and expected future network and storage system state. Users might impose timing and location constraints on when and where to move data.

Correlation and interferometry in digital astronomy. The Square Kilometer Array (SKA) and similar astronomical observatories generate high data rate flows from multiple sources that then need to be combined at a single site for correlation or interferometry. Such systems need specialized network configurations at different times for different physics modes. In the absence of smart networks that can provide for such configurations, SKA will not work; indeed, for SKA the wide area network is seen as part of the instrument. Real-time control will be needed to steer the immense data streams in round robin mode to available processing power to implement load balancing among back-end data processing resources.

Distributed sensor systems are being deployed to provide detailed scientific data for urban systems (EERE), the electrical grid, transportation networks, and in other domains such as seismology. As the price of sensors declines and the quality and intensity of detectors improves, new scientific opportunities are driving requirements for smarter and more

capable networks in data-intensive fields such as climate and weather science, geoscience, and environmental science. This need to aggregate data from widely distributed and heterogeneous sources is a feature of an emerging category of scientific research that cuts across many domains of interest to basic and applied research offices. As data rates increase, needs grow for networks that can process streaming data while in transit, placing analysis/transformation operations optimally given potentially dynamically changing data rates, data analysis needs, and network characteristics.

Network operator internal applications: As network operators work to optimize costs and performance, they depend on intelligence in the network to be able to capture such operational data as fine-grained utilization data on specific links, ports, internal services; fine-grained latency and response-time data; indications of abnormal usage patterns that may require shifting resources; indications of abnormal usage patterns that may indicate a distributed denial of service (DDoS) attack that should be abated; and billable events, flows, and allocations.

A smart network needs to be able to associate this data with specific flows and network operator actions. In addition, in some networks there are internal network NFV applications for such things as subscriber authentication; subscriber or flow resource reservation or priority; Communications Assistance for Law Enforcement Act (CALEA) enforcement; packet inspection for various purposes; multicast (sometimes with transcoding); network test and/or synthetic loads (e.g., Perfmon); alternate configurations for power saving or maintenance; reverting to a "dumb" mode when there is an attack on one or more of the "smart" features; implementing mobility, caching, content addressing, or DNS; capturing (and sometimes anonymizing) network loads for later analysis and simulation; implementing network virtualization (e.g., VLANs, MPLS); automated problem detection, diagnosis, and healing; locating information accessible to the network by content rather than by host addressing; and performance optimization.

Network operators might also choose to act as the local data center for subscriber-driven edge applications requiring low and deterministic response times. This smart edge applications services paradigm will be increasingly important as the Internet of Things, machine-to-machine communications, and the Industrial Internet grow in scale.

Smart grid: Emerging smart grid architectures aim to monitor electric power grid operations with the goal of responding in real time to perturbations so as to prevent large-scale instabilities. They thus seek to use existing assets but with smarter analytics and operation regimes. In these environments, both the network traffic used to communicate data about the state of individual system components and the network traffic used to control those components need to be controlled and optimized. For example, network delays may change the spot price for demand response, an important smart grid function, or delayed voltage recovery post contingencies, putting additional stress on the network. The ability to manage communication delays is thus important for optimizing smart grid functions. The priority of a node or connection, measured by delay consequences, may change depending on grid state. A smart network that can manage such prioritizations and also provide higher-level service guarantees (e.g., to ensure reliable delivery and/or in-network processing) is expected to be particularly important for smart grids.

Low-latency and deterministic response applications require smart network handling to expedite their packets. Examples of applications that would have transformative impact

include telemedicine applications, such as observation of wound progression, remote surgery for delicate but rare surgeries, deep brain stimulation tuning, and stroke imaging in the ambulance; continuous high frame-rate video for lip reading, psychiatry, and other highly interactive uses; defense applications in which response time matters, such as remote drone control, interception of enemy missiles, and high scan-rate reconnaissance; and digital assistants that can catch errors in progress and provide just-in-time information.