Software-Defined Networking and Security for Utilities

Hakki C. Cankaya, PhD
Solutions Architect
Fujitsu Network Communications, Inc.
hakki.cankaya@us.fujitsu.com
Overview

Software-Defined Networking (SDN) open source technology can virtualize and manage complex utility networks.

SDN simplifies configuration and control of network elements, plus their connection to each other and the cloud.

SDN addresses most utility network challenges today, and provides a solid technology foundation moving forward.
What is Software-Defined Networking (SDN)?
What is SDN?
Approach to Designing, Building & Managing Networks

• Virtualized network command and control
  – SDN decouples control plane from forwarding plane and offloads its functions to centralized controller
  – Control plane is now executed via software
  – Centralized, simplified configuration and management of network components
  – Facilitates customization, optimization and innovation
SDN is Next-Generation Software-Centric Approach to Networking

- **Today's Network**
  - Complex, costly and cumbersome
  - Manual configuration at device level

- **SDN Network**
  - Simple, flexible, programmatic control of network infrastructure
  - Configuration and control via software
SDN Offers Simplicity, Programmability and Flexibility

• Simplicity
  – Eliminates manual configuration at device level
  – Simplifies machine-to-machine (M2M) and cloud connectivity

• Programmability
  – Logically centralized controllers provide global network view and help avoid vendor lock-in

• Flexibility
  – Mix/match solutions from different vendors
  – Create unified control that is easier to re-shape traffic and deploy services
# Driving Forces for SDN

<table>
<thead>
<tr>
<th>Complexity of networks</th>
<th>• Increased M2M communication, new applications and services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Big Data</td>
<td>• Massive amounts must be stored and analyzed</td>
</tr>
<tr>
<td>Public/private data centers and clouds</td>
<td>• Becoming important pieces of the energy, oil and gas companies' IT infrastructure</td>
</tr>
<tr>
<td>On-demand network services</td>
<td>• Adding more services such as video surveillance, Internet access, power automation and context-aware security</td>
</tr>
<tr>
<td>Virtualization of hardware</td>
<td>• Already ongoing in server and storage spaces, now SDN for network virtualization, management and control</td>
</tr>
</tbody>
</table>
A Historical Review

Invention
- 2007: Creation of SDN Concept – Professor Nick McKeown, Stanford University

Platform Development
- 2007: Ethane
- 2008: Network Operating Systems, OpenFlow
- 2009: FlowVisor, Mininet
- 2010: Beacon
- 2013: OpenDaylight

Deployments
- 2009: Stanford
- 2010: GENI started and grew to 20 universities
- 2013: 20 more campuses to be added

Demonstrations
- 2008-2011: SIGCOMM
- 2011: Open Networking Summit, Interop
- 2013: radware Adaptive SDN-based DDoS Solution

Moving Forward
- 2012: Defining SDN research agenda for the coming years
- 2013: China SDN Conference, Beijing, China

Source: Open Networking Lab (ON.LAB) from Stanford University and US Berkeley
### Who is Working on SDN?

<table>
<thead>
<tr>
<th>Organization</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Open Networking Foundation**    | - Non-profit trade organization dedicated to improve network via SDN  
                                    - Board: Google, Yahoo, Deutsche Telekom, Microsoft, Facebook, Goldman Sachs, Verizon, NTT Communications  
                                    - Members include: Fujitsu, Juniper Networks, Cisco, Big Switch Networks, VMware  |
| **ETSI (European Telecommunications Standards)** | - Telecommunications standards that will be used throughout Europe  
                                    - NFV Working group  
                                    - Members include: Fujitsu Laboratories of Europe, Juniper Networks  |
| **MEF Carrier Ethernet (Metro Ethernet Forum)** | - Non-profit international industry consortium dedicated to worldwide adoption of Carrier Ethernet networks and services  
                                    - Members include: Fujitsu, Juniper Networks, RAD Data Communications, Cisco, AT&T, Verizon, CenturyLink  |
| **IETF/IRTF (Internet Engineering Task Force)** | - IETF Deals with standards of the Internet Protocol Suite (TCP/IP)  
                                    - Internet Research Task Force (IRTF) works on topics related to the evolution of the Internet  |
What are the Benefits of SDN?
Simplification is Central to SDN Benefits

- SDN makes it easier to:
  - Mix-and-match multi-vendor solutions
  - Configure M2M communications
  - Strategically place security appliances
  - Create logically central firewalls
  - Facilitate new apps and services
  - Connect network elements to the cloud
  - Interconnect Data Centers (DCs)
SDN Offers Increased Efficiencies and Reduced Expenditures

<table>
<thead>
<tr>
<th>Current Networks</th>
<th>SDN Networks</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network provisioning complexity</td>
<td>Self provisioning</td>
<td>Additional revenue opportunity</td>
</tr>
<tr>
<td>Managed network functions</td>
<td>Automated network functions</td>
<td>Reduced OPEX</td>
</tr>
<tr>
<td>Technology-specific connections for the network</td>
<td>Technology-agnostic connections for the network</td>
<td>Reduced CAPEX and OPEX</td>
</tr>
<tr>
<td>Purpose-built hardware for each network function (routing,</td>
<td>Software-based network functionality</td>
<td>Reduced CAPEX</td>
</tr>
<tr>
<td>firewallsing, etc.)</td>
<td>Network OS with Southbound APIs</td>
<td></td>
</tr>
<tr>
<td>Multi-vendor EMSs and their orchestration</td>
<td>Network-aware applications</td>
<td>Innovative applications and increased revenue opportunity</td>
</tr>
<tr>
<td>Application-ware networks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Another SDN Benefit: Increased Agility

- SDN paradigm gives foundation to address issues proactively, faster and more effectively:

<table>
<thead>
<tr>
<th>Simplify network complexity</th>
<th>Add or move network elements with less effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deal with changing traffic patterns</td>
<td>Shape your M2M communications</td>
</tr>
<tr>
<td>Respond to Big Data demands</td>
<td>Create more bandwidth</td>
</tr>
<tr>
<td></td>
<td>Design data center requirements</td>
</tr>
<tr>
<td>Easier to scale</td>
<td>More programmability means more flexibility and less effort to change or grow/add on</td>
</tr>
<tr>
<td>Vendor independence</td>
<td>Reduce or eliminate vendor lock-in</td>
</tr>
<tr>
<td></td>
<td>Migrate or connect easier with open source technology</td>
</tr>
</tbody>
</table>
How Does SDN Impact Utility Communications Networks?
Typical Existing Utility Networks
Complex, Costly, Often in Need of Modernization

Core Networks

Access Networks – Wireless

Field Area Networks (FAN)

Access Networks – Wireless and Wireline
## Common Network Challenges for Utilities

<table>
<thead>
<tr>
<th>Complexity of communication networks</th>
<th>Multi-domain: WAN, Field Area Network, Core, Neighborhood Area Network</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Owns both network and leases network from service provider(s)</td>
</tr>
<tr>
<td>Multiple vendors and product lifecycles</td>
<td>Incompatibilities and vendor lock-in</td>
</tr>
<tr>
<td></td>
<td>Multi-vendor equipment maintenance and network upgrades</td>
</tr>
<tr>
<td>Large security coverage</td>
<td>Ability to control traffic per application</td>
</tr>
<tr>
<td>Need for flexible bandwidth</td>
<td>Scalability for new applications and services</td>
</tr>
</tbody>
</table>
### Common Network Challenges for Utilities (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay and jitter</td>
<td>▪ Bandwidth adjustments and performance to standards</td>
</tr>
<tr>
<td>High resiliency</td>
<td>▪ Avoiding network interruptions and attacks</td>
</tr>
<tr>
<td>Labor intensive management</td>
<td>▪ Manual configuration and maintenance at the device level</td>
</tr>
<tr>
<td>Flexible network topologies</td>
<td>▪ Proprietary hardware and firmware makes it difficult to configure and make changes</td>
</tr>
<tr>
<td>Smart Grid and new services</td>
<td>▪ Video surveillance, Internet access, power distribution automation, context-aware security, etc.</td>
</tr>
<tr>
<td></td>
<td>▪ More dynamic bandwidth; frequent M2M communication; Big Data storage, collection and analytics</td>
</tr>
</tbody>
</table>
Common Network Challenges for Utilities (continued)

| Security                                      | ▪ NERC CIP requirements  
|                                              | ▪ IT and power generation/transmission data  
|                                              | ▪ Analytics for collected data               |
| Restoration and Self Healing                 | ▪ Millisecond range restoration for operations |
| Financial resources for modernization       | ▪ Technology adoption cycle much slower due to heavy tax payer investment  
|                                              | ▪ Rip-and-replace is not common practice     |

Fujitsu Proprietary. All Rights Reserved, ©2014 Fujitsu Network Communications, Inc.
Utility Communications Network Requirements

Secure  Not easily penetrated by hackers or rogue insiders

Resilient  Provides sufficient redundancy so that a single failure does not affect the network: >99.999% availability

In Service Upgrades  Ability to upgrade software without losing visibility of the network

Scalable  Provides ability to scale the network for the foreseeable future

Teleprotection  Low latency with symmetrical delays, and low jitter for Teleprotection capabilities

Ease of Use  As easy and as deterministic as SONET
Major Drivers of Change

Identifying Motives for Modernizing

**Advanced Technology Deployments**
- AMI, HAN and customer engagement
- Teleprotection upgrade
- Distribution Automation (DA)
- Distributed generation integration
- Wireless & mobile applications (OMS, DMS)
- GIS

**Legacy/Out-of-Service Infrastructure**
- SONET/TDM networks
- Analog microwave
- 800MHz band rebranding
- Frame relay replacement

**Server/Storage Consolidations**
- Cost optimization
- Data center consolidations/relocations
- Applications centralized/outsourced
- Mergers/acquisitions

**Network & Services Management**
- Regulatory compliances
- Business process alignment
- Predictive maintenance
- Security

**Business Compelling Reasons to Act**
- Major application deployments
- Performance / availability
- Improving end-user experience through technology
- IT control / regulatory compliance
- Cost reductions
- Cyber security
- Mergers / acquisitions / new construction
- 700MHz & 4.9GHz branding
Existing Utility Networks Environment

Research Confirms Consensus Movement Toward Modernization

• Existing networking approaches vary widely …

- For your AMI network, which methods do you currently use for backhaul information?
  - Fiber: 41%
  - T1: 9%
  - Microwave: 16%
  - Star: 1%
  - Cellular: 13%
  - Radio: 7%
  - Other: 12%
  - Not applicable: 29%

- How do you plan to connect your smart meters to your datacomm network?
  - Unlicensed 900MHz RF Mesh: 15%
  - Unlicensed 2.4GHz RF Mesh: 8%
  - Unlicensed Point-to-Multipoint: 5%
  - Licensed Point-to-Multipoint: 17%
  - 2G/3G Public Cellular: 27%
  - 4G Public Cellular (LTE or WiMAX): 9%
  - PLC: 8%
  - Other: 21%
  - No plans: 24%

• But there is evidence of convergence for managing smart grid communications …

- Do you support standardizing on the use of the internet protocol (IP) for all Smart Grid (SG) communications?
  - No, 21%
  - Yes, for some, 16%
  - Yes, for all, 63%

Modernizing to Address the Future

Move Toward Open Standards

- 61850-substation automation
- Multi-protocol
- Scalable and future proof

- Low latency network
- QoS at the core layer
- Secure and fault-tolerant

Utility Networks of the Future Must Emphasize Simplicity, Programmability and Flexibility

- One multi-purpose communications network – avoids implementation of multiple single-purpose networks
- Communications network – grows as functional requirements change and technology evolves
- Invest in non-proprietary solutions to mitigate the risk of technology obsolescence
- Leverage industry standards to reduce OPEX
- Create capacity and infrastructure for secure and fault tolerant requirement

Source: DUKE Energy CTO Speech, 2010-2012
## SDN Addresses Most Network Challenges

*Foundation for Proactively Addressing Modernization*

<table>
<thead>
<tr>
<th>Utilities Challenge/Need</th>
<th>How SDN Can Address</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity of multiple networks</td>
<td>Provides global view and control</td>
<td>Simplicity</td>
</tr>
<tr>
<td>Multiple vendors and product lifecycles</td>
<td>Software-defined network configuration plus open standards</td>
<td>No vendor lock-in</td>
</tr>
<tr>
<td>Data center efficiency</td>
<td>Data center virtualization</td>
<td>Efficient resource use</td>
</tr>
<tr>
<td>Large security coverage: ability to control traffic per app</td>
<td>Logically centralized security control and more granular security arrangements</td>
<td>Reduced security breach</td>
</tr>
<tr>
<td>Need for flexible bandwidth – scalability for new and emerging apps</td>
<td>Bandwidth on-demand</td>
<td>Revenue opportunity</td>
</tr>
</tbody>
</table>

Fujitsu Proprietary. All Rights Reserved, ©2014 Fujitsu Network Communications, Inc.
### SDN Addresses Most Network Challenges

*Foundation for Proactively Addressing Modernization* (continued)

<table>
<thead>
<tr>
<th>Utilities Challenge/Need</th>
<th>How SDN Can Address</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay and jitter</td>
<td>Overall control at the SDN controller</td>
<td>Increased performance</td>
</tr>
<tr>
<td>High resiliency</td>
<td>Overall control at the SDN controller</td>
<td>Increased availability</td>
</tr>
<tr>
<td>Labor intensive management</td>
<td>Programmatic network control</td>
<td>Simplicity, reduced OPEX</td>
</tr>
<tr>
<td>Flexible network topologies</td>
<td>Topology abstraction at the SDN controller</td>
<td>Simplicity</td>
</tr>
</tbody>
</table>
### Guidelines and Security Standards

#### Cybersecurity and Internet Protocol Standards

<table>
<thead>
<tr>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>IETF</td>
</tr>
<tr>
<td>IEC</td>
</tr>
<tr>
<td>NERC</td>
</tr>
</tbody>
</table>

- **Radius (RFC 2865)**
- **LDAP (RFC 4511/4510)**
- **TLS (RFC 5246)**
- **DTLS (RFC 4347)**
- **IPsec (RFC 2401)**
- **SSH (RFC 4251/6239)**
- **Syslog (RFC 5424)**
- **IEC 62443-2-4: Building secure ICS systems**
- **CIP 001-009: Cybersecurity Utility Security Standards**

#### Reliability, Security and Technology Standards/Best Practices for Critical Infrastructure

<table>
<thead>
<tr>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST</td>
</tr>
</tbody>
</table>

- **ICSJWG: Conferences and papers**
- **DHS Cybersecurity Procurement Language for Control Systems**
- **NERC/DHS**
- **SGTF: Reliability Considerations from the Integration of Smart Grid**
- **NIST IR 7628 Smart Grid Security**
- **SP 800-82 Industrial Control Systems (ICS) Security**
- **FIPS PUB 140-2 Cryptography Modules**

#### Automation Standards

<table>
<thead>
<tr>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenSG</td>
</tr>
<tr>
<td>IEC</td>
</tr>
<tr>
<td>IEEE</td>
</tr>
</tbody>
</table>

- **Security profiles: WASA, Substation, Distributed Automation**
- **IEC 62351 Series: Cybersecurity for 61850 series protocols and IEC 60870-6 (ICCP)/60970-5 (European DNP3)**
- **IEEE 1686 IED Cybersecurity**
- **IEEE 1815 DNP3**
- **IEEE P1711 Serial Encryption**

#### Communication Standards

<table>
<thead>
<tr>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>IETF</td>
</tr>
<tr>
<td>ANSI</td>
</tr>
<tr>
<td>OpenSG</td>
</tr>
</tbody>
</table>

- **SNMPv3 (RFC 3411-RFC 3418)**
- **NETCONF (RFC 6241)**
- **YAN (RFC 6020)**
- **ANSI C12.22: Encryption of metrology data**
- **OPEN meter: Specification of open meter OSI layers and multi-metering networking interfaces**
- **IEEE 802.x series of wireless/wireline communication and security standards**
- **SEP 2.0: HAN networking**
- **Security profiles: AMI, 3rd party data access**
How SDN Addresses Network Security Challenges

- Logically Centralized Control
  - Eliminates confusion placing security appliances in large coverage areas
  - Logically central firewall present virtually and wherever needed

- Security as an Application
  - Multiple security layers as needed

- Cyber Security
  - Password control
  - Protection against hackers
  - Denial of Service (DoS)
  - Intrusion detection
## SDN Best Practices for Security Concerns

<table>
<thead>
<tr>
<th>Category</th>
<th>Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security as after thought</td>
<td>• Security as application</td>
</tr>
<tr>
<td>Security appliances everywhere</td>
<td>• Logically centralized security intelligence (acting as a whole)</td>
</tr>
<tr>
<td>Coordinated attacks</td>
<td>• Security analytics as a security application</td>
</tr>
<tr>
<td></td>
<td>• Historical visibility for computing correlation</td>
</tr>
<tr>
<td>Increased vulnerability with more ports</td>
<td>• End-to-end network visibility</td>
</tr>
<tr>
<td>Real time attacks</td>
<td>• Fine-grained controls to counter attack</td>
</tr>
</tbody>
</table>
### SDN Best Practices for Security Concerns (continued)

<table>
<thead>
<tr>
<th>Static security configuration via CLI</th>
<th>Low-touch configuration of security appliances</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical ports define security perimeter</td>
<td>Security perimeter is defined by concepts introduced by applications</td>
</tr>
<tr>
<td>Cloud/DCs security complications</td>
<td>Security policies are applied based on application layer features</td>
</tr>
<tr>
<td>Virtualization</td>
<td>Functional policies rather than physical attributes</td>
</tr>
</tbody>
</table>
SDN Security Concerns

- Centralized Controller as a single point of attack
- Controller unavailability creating control vacuum
- Southbound (OpenFlow) seen as vulnerability
What are some Recommended SDN Migration Approaches?
SDN Migration Approaches

1. Direct Upgrade

Upgrading existing equipment with OpenFlow Agents
SDN Migration Approaches

2. Phased (Parallel) Upgrade
SDN Migration Steps
ONF Migration Working Group

1. Identify core requirements of target network
2. Prepare the starting network for migration
3. Phased migration of service
4. Validate the result

- 2  Device
  Device
  Device
  Starting Network
  Phased Migration
  Target Network

- 4  OpenFlow Controller
  OpenFlow
  OpenFlow
  OpenFlow

33 Fujitsu Proprietary. All Rights Reserved, ©2014 Fujitsu Network Communications, Inc.
SDN Migration Steps

Target Network

1. Identify core requirements of target network

- **Programmability** must support APIs for extending functionality, leveraging feature combination available in underlying devices.

- **Serviceability** software dynamically updated, with minimal service interruption. Software upgrade and rollback are automated.

- **Heterogeneity** can support multiple devices from different vendors.

- **Maintainability** enables software tool chain, including simulators.

- **Simplify network and lower cost of operation**

- **Improve utilization**

- Not all traditional starting network requirements need to be met, initially, by target software-defined network.
SDN Migration Steps
Starting Network

2. Prepare starting network for migration

- If necessary, move starting network (in a relatively arbitrary state) to clean intermediate standard state, so rest of migration proceeds safely

- System prep phase can be highly complex

- Recommend guidelines, systems, and tools to prepare traditional starting network for migration
SDN Migration Steps
Phased Migration

3 Phased migration of service

- Migration to target network can be source of risks
- Outages during a migration, impairment of diagnostic and monitoring tools, or simply the scale and performance of the new technology, are all conditions that may be encountered during the intermediate steps
- Owing to device and network heterogeneity, entails device specific drivers and methods. Workflow orchestration infrastructure and associated tool chain may be generic
- Define guidelines, systems, and tools to facilitate and validate steps required for target network migration
Once the migration has completed, the target network must be validated against a documented set of requirements or expectations.

Recommend guidelines, systems, and tools for result validation, including metrics for evaluating compliance of requirement and encountered disruptions.
Some SDN Tools for Self-Education

- **OpenDaylight**
  - Open SDN Controller
  - [http://.opendaylight.org](http://.opendaylight.org)

- **FloodLight**
  - Open SDN Controller
  - [http://projectfloodlight.org](http://projectfloodlight.org)

- **Mininet**
  - SDN n/w simulator
  - Mininet.org

- **Open Networking Lab**
  - FlowVisor, Open Network OS (ONOS)
  - [http://onlab.us](http://onlab.us)
In Summary

Software-Defined Networking (SDN) open source technology virtualizes and manages complex utility networks.

SDN simplifies configuration and control of network elements, plus their connection to each other and the cloud.

SDN addresses most utility network challenges today, and provides a solid technology foundation moving forward.
Conclusions and a Call to Action

- **Offers real value** Utilities, oil and gas companies can benefit from adoption of SDN

- **The time has come** Virtualization is now evolving into networks via SDN

- **Start planning** Research how to best utilize the benefits of SDN for day-to-day needs in your communications networks

- **Get involved in SDN working groups** Share your vision on how modernized and smarter networks should be configured
References

• NFV White paper
  – http://www.layer123.com/downloadnow&doc=NFV_White_Paper

• “Migration Use Cases and Methods”, Migration Working Group, Open Networking Foundation (ONF)

• MEF CE4Cloud/SDN Marketing Committee Work

• Open Networking Lab (ON.LAB) from Stanford University and UC Berkeley
  – http://onlab.us
References (continued)

• SDN Central (News, Education, Tools, Projects, etc.)
  – http://sdncentral.com

• SDN for Utilities and Energy Sector
QUESTIONS AND COMMENTS