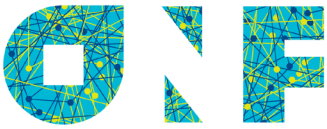

OPEN NETWORKING
FOUNDATION

Migration Tools and Metrics

Migration Working Group

ONF TR-507

ONF Document Type: Technical Paper
ONF Document Name: migration-tools-and-metrics

Disclaimer

Open Networking Foundation
2275 E. Bayshore Road, Suite 103, Palo Alto, CA 94303
www.opennetworking.org

Contents

1. Introduction

The first deliverable of the ONF Migration Working Group, *Use Cases and Migration Methods*,[1] describes migration approaches for several types of networks, includes three use cases documenting real-world SDN deployment examples, and provides recommendations for migration to OpenFlow™-based software-defined networks based on best practices derived from the lessons learned in those use cases.

Some of the best practices and recommendations refer to tools and procedures to perform during various stages of an SDN migration, including the planning phase, the migration process, and validation of the target network. Migration procedures include the assessment and preparation of the starting network, the migration procedure itself, and the assessment and verification of the target network and back-out procedures.

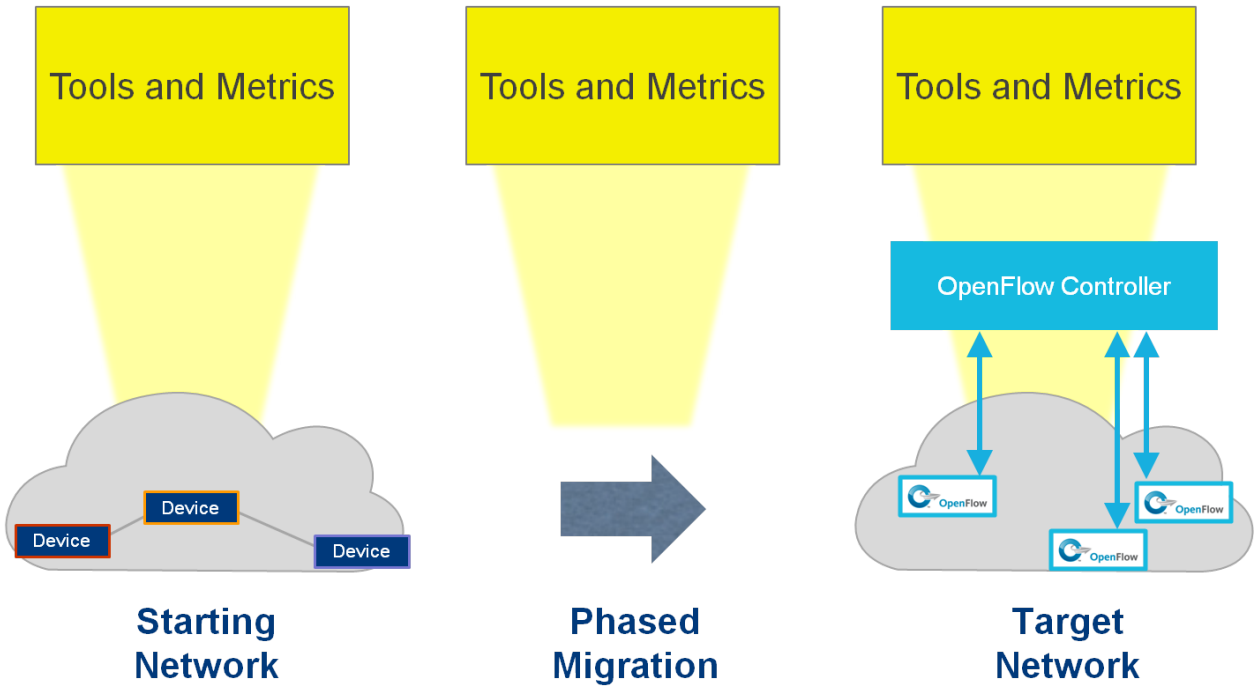

Figure 1 - Tools and metrics for different stages of SDN migration

As shown in Figure 1, various tools can be useful in different steps of an SDN migration process. In particular, tools may be used to monitor, configure, manage, test, and validate the network in any or all phases of the migration. Monitoring includes the collection of metrics in the starting and target networks. The purpose of collecting metrics is to assess the network and service performance and availability for the purposes of taking specific actions. In many cases, the starting network metrics can be used as benchmarks for the target network.

This document focuses on the tools and metrics that are useful in the three stages of an SDN migration process. It identifies features that are desirable during an SDN migration, performs an

analysis of open-source and commercial tools that are available today, and identifies gaps in the existing toolset.

The remainder of this document is organized as follows:

- Section 2 provides an overview of some key considerations for tools and metrics that can be effectively used in various phases of an SDN migration, including the preparation of the starting network; stages of the phased migration; and testing and verification of migration and validation of the OpenFlow-based software-defined target network.
- Section 3 provides a high-level description of available open-source and commercial tools, categorized as monitoring tools, configuration and management tools, or testing and verification tools.
- Section 4 outlines some key metrics and tool capabilities identified as desirable or needed during SDN migration but not commonly found in existing tools.
- Section 5 provides a brief conclusion with suggestions for future work.

2. Considerations for SDN Migration Tools and Metrics

This section describes key considerations for tools and metrics that can be used in various stages of an SDN migration, including the preparation of the starting network, the phased migration, as well as the testing and verification of the migration process and the target OpenFlow-based software-defined network. These considerations can range from “must have” to “nice to have,” and can relate to various operational needs, including general characteristics, functional characteristics, or performance-related characteristics.

2.1. METRICS

There are hundreds of already defined non-SDN-specific metrics that may be collected in traditional networks. TMForum (www.tmforum.org) describes several metrics and has work in progress that will document additional metrics. For example, many business metrics[2] are relevant to measure during SDN migration. Other metrics related to the customer experience and service-level agreements are also relevant, and TMForum has work in progress in those areas. This document does not cover all relevant metrics in this area, but instead focuses on a few important ones that are of particular interest during an SDN migration.

In OpenFlow-based SDN networks, there are also new measurements that are specific to these networks. These measurements relate to the OpenFlow protocol messages, the OpenFlow controller(s), or the OpenFlow switches.

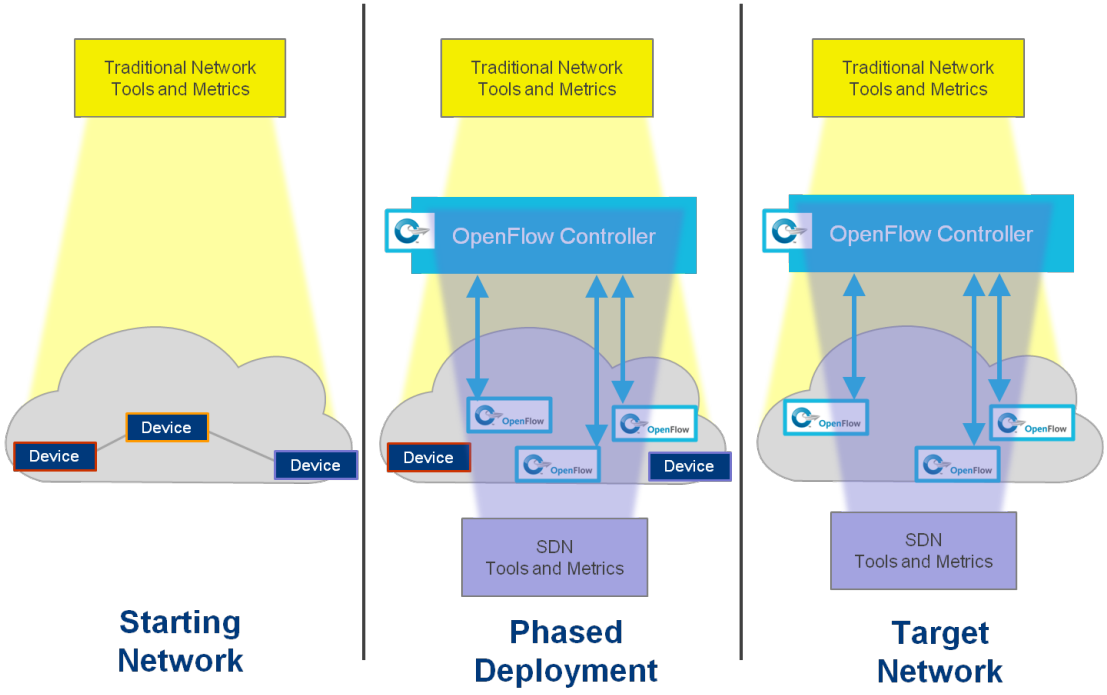

Figure 1 - Metrics collection during the three migration phases

Figure 1 illustrates how tools are used to collect metrics during the three migration phases. Traditional tools are used throughout the phases to collect non-SDN-specific metrics. In the phased deployment and target networks, new SDN metrics are collected by SDN-enabled tools while the non-SDN-specific metrics continue to be collected with the traditional network tools or by the SDN-enabled tools if the functionality is combined in the same tool set.

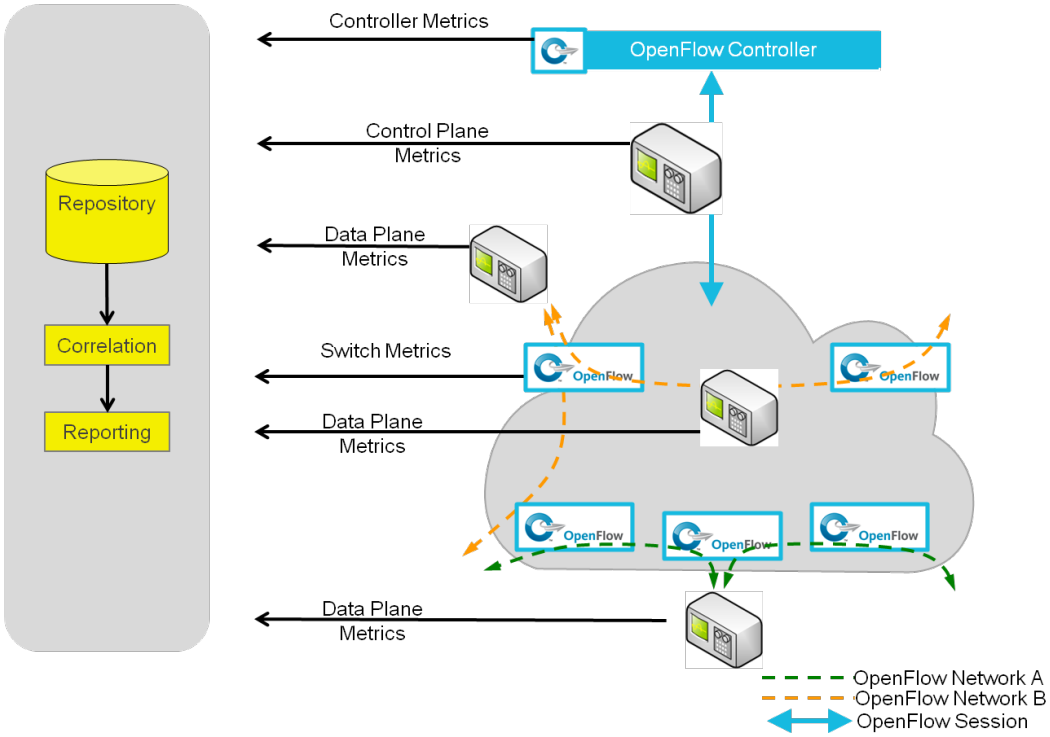

Figure 3 - Metrics collection

Figure 3 shows how metrics are collected from the data plane, control plane, switch, and controller. All metrics are collected over a period of time. Tools may therefore analyze the metrics over time to report trends as well as minimum and maximum values. Tools may also correlate various metrics to generate more complex reports. This document does not go into the detailed correlation and reporting that may be performed with the various collected metrics.

2.1.1. OpenFlow SDN metrics

This section describes the metrics that may be collected and analyzed in the three migration stages. The metrics may be collected on the starting network during the pre-migration phase, on the various phased networks during the migration itself, and on the target network during the post-migration phase.

There are metrics associated with the new messages introduced by the OpenFlow protocol during the migration. Those messages can be collected and analyzed. The response times may also be collected and analyzed both at the controller and the switch. On the switch, the activation times may also be collected and analyzed.

There are also metrics associated with the OpenFlow controller and OpenFlow switches. Those metrics include controller availability, reliability, capacity, accuracy, and security.

2.1.1.1. Quantitative metrics for the OpenFlow protocol

Several quantitative metrics can be collected related to the OpenFlow messages themselves.

The number of OpenFlow messages may be collected and categorized as follows:

- By message type
- By OpenFlow switch
- By OpenFlow controller*
- By direction
  - OpenFlow switch → OpenFlow controller
  - OpenFlow controller → OpenFlow switch
- By status
  - Received
  - Dropped, lost, or received unacceptably late

2.1.1.2. Timeliness metrics related to the OpenFlow protocol

There are several timeliness aspects metrics that can be measured in an OpenFlow network. Some of these metrics are related to the response times associated with OpenFlow messages, i.e., the amount of time between a request and the receipt of the response. Other metrics are related to the activation times associated with the OpenFlow requests, i.e., the amount of time between an OpenFlow request and a corresponding change in the datapath.

- **OpenFlow protocol response times.** The response times and variation in response times may be collected and categorized as follows:
  - By message type
  - By OpenFlow switch
  - By OpenFlow controller*
  - By direction
    - OpenFlow switch → OpenFlow controller
    - OpenFlow controller → OpenFlow switch
- **OpenFlow protocol activation times.** The activation times and variation in activation times may be collected and categorized as follows:
  - By message type
  - By OpenFlow switch
- **OpenFlow switch entry duration.** The duration of OpenFlow entries may be collected based on OpenFlow counters maintained on the switch and categorized as follows:
  - Per flow entry
  - Per OpenFlow port
  - Per OpenFlow queue
  - Per OpenFlow meter

2.1.1.3. OpenFlow controller metrics

The following metrics can be collected and reported for each OpenFlow controller:

- **Availability metrics.** The percentage of time the controller is up and available.
- **Reliability metrics.** The mean time between controller failures or restart, the mean time to repair†, and the mean time to restart the controller.

---

* For deployments that include multiple OpenFlow controllers
† The mean time to repair includes a human resources factor associated with the repair.

- **Capacity metrics.** The percentage of compute resources used by the controller.
- **Accuracy metrics.** The percentage of packets forwarded accurately as specified in the controller's tables.
- **Security metrics.** The number of TLS handshake failures.

2.1.1.4. OpenFlow switch metrics

The following metrics can be collected and reported for each OpenFlow switch:

- **Availability metrics.** The percentage of the time the OpenFlow switch is up and available to communicate with the OpenFlow controller, and the percentage of the time the OpenFlow switch is up and available to perform data-plane–related functions.
- **Reliability metrics.** The mean time between OpenFlow switch failures or restart, and the mean time to repair or restart the OpenFlow switch.
- **Capacity metrics.** The percentage of OpenFlow switch resources used (e.g. flow tables).
- **Accuracy metrics.** The percentage of packets forwarded accurately, as specified in the switch's flow tables.
- **Security metrics.** The number of TLS handshake failures.

2.1.2. Traditional metrics of high relevance in SDN

There are several metrics that are defined and collected in traditional non-SDN networks. It is expected that those metrics will continue to be collected during and after an SDN migration. In the post-migration phase, OpenFlow counters may be used to assist in the metrics collection related to the packets processed by each OpenFlow switch. OpenFlow counters are maintained on each OpenFlow switch and include packet counters per port (received and transmitted), per queue (transmitted) as well as several other optional counters.

A few of the most relevant metrics to monitor during an SDN migration are described here with notes on the possible SDN migration impact on those metrics.

- **Packet loss rate.** The packet loss rate consists in the sum of packets that are not received or received unacceptably late, divided by the total number of packets transmitted. This metric may differ significantly between the starting network and the target network if the packets received by the datapath on the OpenFlow switch are sent to the controller in the target network at a faster rate than the controller can handle.
- **Latency and latency variation.** Latency is also known as delay. Latency consists in the average measurement of one-way latency of packets between two endpoints. This is also known as jitter or delay variation. Latency variation is the variance in one-way latency of packets between two endpoints. These metrics may differ significantly between the starting network and the target network because of different processing delays caused by OpenFlow. Some packets received by the datapath on the OpenFlow switch may be sent to the controller in the target network.
- **Outage downtime.** This is the amount of time where the users experienced an outage, i.e., lack of network connectivity. This metric is relevant because the migration process itself may provoke outages at various stages.

- **Service activation time.** This is the amount of time it takes from when the order for a new service is placed until the service is activated and available to the user. This metric is relevant because SDN is expected to bring the activation time down.

2.1.3. Pre-migration metrics collection

Pre-migration metrics collection falls into two categories. The first category consists of metrics that characterize the pre-migration network. This can be done by collecting traditional network metrics for availability, reliability, performance, service-level agreements, and business aspects. Those metrics will be used for benchmarking. The second category consists in evaluation of the OpenFlow controller and OpenFlow switches in a non-production network to characterize the OpenFlow network behavior to better prepare for the migration itself.

2.1.4. Phased migration metrics collection

During the actual migration, the collection of traditional network metrics continues. The data can be analyzed to determine any user impact and allow for rollback decisions to be made.

In addition, OpenFlow SDN-related metrics may now be collected and analyzed to identify any bottlenecks that may be responsible for a decrease in network performance. The packet loss rate, latency, latency variation, and any outage duration are collected and used to monitor network performance. This information can be used in all phases of the migration to determine any user impact and allow for rollback decisions to be made.

2.1.5. Post-migration metrics collection

The collection of traditional network metrics and OpenFlow SDN-related metrics continues in the post-migration phase. The metrics may now be compared to pre-migration metrics. OpenFlow SDN-related metrics may be monitored over time to detect problems as the network changes or as new versions of OpenFlow switch or controller software are introduced. OpenFlow counters may help with metrics collection in this phase.

2.2. GENERAL CONSIDERATIONS

There are several general and functional characteristics of tools which, if considered properly, can determine the success of migration from a traditional network to an OpenFlow-enabled network. General considerations such as security, scalability, and redundancy of tools, and functional considerations describing data and information flow, input/output formats, and authentication of users, can greatly increase the chances of a smooth migration, as well as help in quick diagnosis and troubleshooting of issues experienced during migration.

2.2.1. Orchestration and control

The management and orchestration system plays a critical role in the SDN environment. It is important that both the controller and orchestrator have complete inventory and visibility of network resources available to them. Fragmented resources will pose challenges in allocating and keeping track of the physical and logical resources needed for the services being provided over the network. While adequate redundancy and availability of the management and orchestration system must be ensured, an orchestrator and controller with a comprehensive view of the resources and some hierarchy for scaling purposes is desirable.

2.2.2. Interoperability

Interoperability and multi-vendor support are fundamental requirements in any network environment of larger scale. Particularly for migration, tools and metrics need to support heterogeneous network environments composed of elements from different vendors in the starting network setup, as well as components and devices newly added or replacing traditional network devices during the transition to the target network. In addition, it is important that the tools used during migration are usable in broader scope and support different deployment models, including traditional network devices, OpenFlow devices, and hybrid devices (those with concurrent traditional and OpenFlow capabilities). Using a plethora of tools is neither necessary nor helpful for smooth migration process. Whenever possible, a smaller number of tools that support heterogeneous networks should be used.

2.2.3. Redundancy and high availability

While changes to network resources are inevitable during a migration process, the required level of availability and robustness for running services must be maintained in a live network. Accordingly, migration tools that facilitate high network availability and redundancy are vital. Tools in this category would, for instance, enable simulating or emulating migration scenarios or migration processes before the implementation in the live network, or assist in instrumentation and monitoring during the migration phase.

2.2.4. Scalability

While tools for migration, in general, need to cover different types of networks, scalability is one of the key requirements. This includes supporting large numbers of network elements (both SDN-enabled as well as traditional network devices) and several network controllers. For instance, tools that are used to diagnose the network and/or service migration process need to provide sufficient scale and performance to continuously monitor all conditions in the network, across potential intermediate steps of the migration, and in the target network. In order to meet the goal of simplifying the operation of the network including the migration procedure, tasks and tool functions need to be automated as much as possible.

2.2.5. Technological independence

Technological independence is the ability to run the tool without any third party needed. That means the tool will able to execute without any external license or specific platform.

2.2.6. Network abstraction

Network abstraction is the process of taking away the different subnetworks in order to reduce complexity and increase efficiency

2.2.7. Mixed/hybrid deployments

Though greenfield deployments are likely to occur, it is expected that more often than not, OpenFlow deployments will be in a mixed or hybrid environment. Therefore, any tools used during migration need to support heterogeneous network environments containing elements

from different vendors in the starting network setup, as well as components and devices newly added or replaced during the transition to the target network.

2.2.8. Rollback strategy

Having a rollback and checkpoint strategy is one of the fundamental requirements in medium to large-scale networks to track any changes that are made via the migration tools GUI or CLI, or in-house applications that use APIs, as described in 2.2.10. In some cases, migration tools may be used to modify configurations or flows associated with many devices and need a way to back out from the last x number of modifications made to those devices. There may be users who wished they had not done something to harm the network and want to revert to known working configuration.

Migration tools should be able to verify and restore a backup via CLI and/or GUI. There could be a malicious or runaway application that is programming flows in the network and therefore needs to be disabled. After disabling the application, users need to be able to revert to the last known healthy state. Migration tools should be able to take a snapshot of the current configuration/state and provide the option to revert back to a saved snapshot. Developers may implement an option to roll back the configuration to a previous state in their respective applications.

2.2.9. Authentication

Authentication is the process of determining which users are allowed to use the software. Authentication is done through the use of login/password. It precedes authorization (see “Role-based access control”).

2.2.10. Open framework

An application programming interface (API) specifies how external tools should interact with the software. It allows the software to be perfectly integrated in an existing environment. A software development kit (SDK) is a set of software development tools that developers use to write applications for a specific platform. The SDK allows developers to create and debug additional features. Migration tools should provide an open API to interact with the controller or other applications and tools deployed in the network.

2.2.11. Firmware and image management

Firmware and image management change the firmware running on a device to another image, such as a release or patch. Migration tools should be able to provide firmware and image management capabilities to the controller as well as to the OpenFlow devices in the network.

2.2.12. Role-based access control (RBAC)

RBAC regulates access to a system based on users’ roles and authorization. RBAC enables an authorized user to perform a specific task, such as viewing, creating, or modifying a device. It permits users to carry out a wide range of authorized tasks by dynamically regulating their actions according to flexible functions, relationships, and constraints. Migration tools should

have the capability to provide role-based access to the controller as well as to the OpenFlow devices in the network.

2.2.13. Multi-tenancy

Multi-tenancy means that multiple customers can use the same instance of the software. Each customer's data is isolated and remains invisible to other customers. While not a "must-have" feature in migration tools, multi-tenancy can be economically beneficial because software development and maintenance costs are shared.

2.2.14. Network emulation and simulation

Network emulation allows a user to simulate an existing or planned network environment in order to predict the impact of change or future performance. As in any network deployment, the ability to simulate networks to test capabilities of different network elements and the behavior of the network itself with synthetic traffic is always helpful. Such simulation helps in understanding different aspects of the network and avoids any last-minute problems during deployment. Therefore, any simulation capabilities involving the controller and the OpenFlow switches before deployment can be extremely helpful for smooth migration.

2.2.15. GUI

A graphical user interface (GUI) is an interface that allows users to interact with computer features through graphical screen. A GUI is more user friendly than command line interface.

The optional unified multi-layer tool for a GUI tool provides visibility of all the network layers integrated in an easy to browse format that allows the network operator to use fewer tools.

2.2.16. Diagnostics and troubleshooting

The tool should offer a feature to determine the cause of certain symptoms. By identifying the source of a problem, it can be solved to make the process operational again. Troubleshooting will help the user quickly find the origin of the problem by eliminating other potential causes.

2.2.17. OpenFlow considerations

In addition to the general considerations, some OpenFlow-specific considerations are included:

- **Support for OF-Config.** The OpenFlow Management and Configuration Protocol (OF-Config) protocol is used to manage devices in an OpenFlow environment. OF-Config allows users to access and modify configuration data on an OpenFlow device using an OpenFlow controller. Tools may support the OF-Config protocol.
- **Protocol version interoperability.** Tools may support multiple versions of the OpenFlow protocol. Implementation and usage should be totally transparent for the user.

3. SDN Migration Tools and Metrics

This section provides a list of tools and metrics that can be used either to migrate network services from a traditional network to a software-defined network based on OpenFlow, or simply to integrate OpenFlow-based software-defined network components into traditional networks. These various tools and metrics are classified in the following categories:

- Monitoring tools
- Configuration and management tools
- Testing and verification tools

For each category, a table summarizes the tools and the key features considered for this category based on a list of requirements.

The subsequent section attempts to list tools that can be used independently regardless of the bundle they may be included in, along with other products from the same vendor for all tool categories.

Organization / Project & Tools	Commercial	Open Source	Monitoring	Configuration and Management	Testing and Validation	Available Since
Cacti http://www.cacti.net						
Cacti		X	X			2004
Codenomicon http://www.codenomicon.com						
OF Controller TS[3]	X				X	
OF Switch TS[4]	X				X	
Deutsche Telekom						
OFrewind[5]	X				X	
Hewlett-Packard http://hp.com						
OpenView / HP BTO Software	X		X			2007
Ixia http://www.ixiacom.com						
IxANVL[6]	X				X	2011
IxNetwork6	X				X	2011

Organization / Project & Tools	Commercial	Open Source	Monitoring	Configuration and Management	Testing and Validation	Available Since
Luxoft http://www.luxoft.com						
Twister		X		X		2010
Nice						
NICE[7]		X			X	
Paxterra Solutions http://www.paxterrasolutions.com						
TestON		X			X	
Project Floodlight http://www.projectfloodlight.org						
OFTest[8]		X			X	2011
Stanford University http://www.stanford.edu						
ATPG[9]		X			X	
Cbench		X	X		X	2009
Hassel and NetPlumber[10]		X			X	
Mininet[11]		X			X	2011
OFPeck[12]		X	X		X	2010
OFtrace[13]		X			X	2008
OpenSeer[14]		X	X			2009
UBIqube Solutions http://www.ubiqubesolutions.com						
MSActivator[15]	X		X	X		2009
Wireshark http://www.wireshark.org/						
Wireshark	X				X	2014

3.1. MONITORING TOOLS

Monitoring tools and solutions play a critical role during all three stages of a migration process. Monitoring the starting network is necessary to set the baseline readouts of the metrics under consideration for integration and migration. During the transition phase from the starting network to the target network, these tools become useful to observe the changes in those metrics, helping to raise red flags so that operators can initiate corrections. Moving into the starting network, monitoring tools help secure the stability of the new network, making sure that readouts are in an acceptable range for the operator. Among other capabilities, a properly designed monitoring system allows operators to:

- Detect and avoid network incidents.
- Determine which actions may solve a network incident.
- Execute recovery and contingency plans

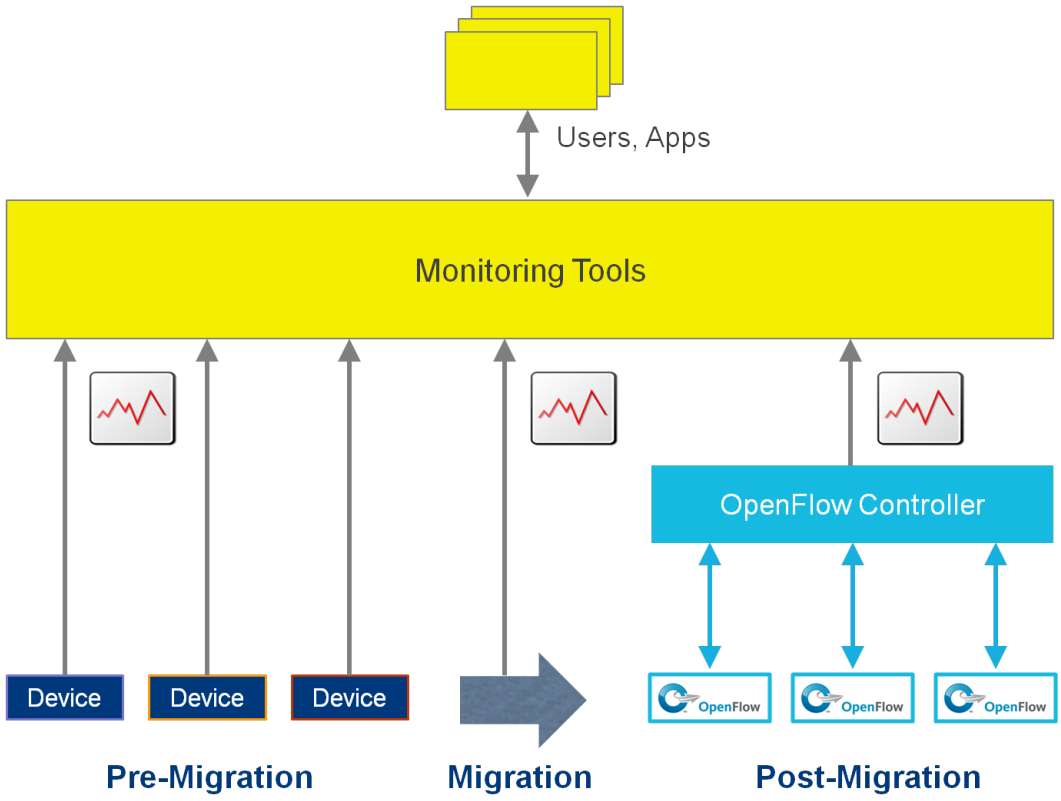

Figure 2 – Monitoring process during a migration

Considerations and Metrics	Tools					
	Cacti	**Cbench**	**MSActivator**	**OFPeck**	**OpenSeer**	**OpenView**
Multi-tenancy (2.2.13)	X	X	X	X	X	X
Packet loss rate (2.1.2)	X	—	X	X	X	X
Latency/latency variation (2.1.2)	X	—	X	X	X	X
Outage downtime (2.1.2)	—	—	—	X	—	X
OpenFlow protocol response times (2.1.1.2)	—	X	—	X	X	—
OpenFlow protocol activation times (2.1.1.2)	—	—	—	X	X	—
OpenFlow controller Availability Metrics (2.1.1.3)	—	—	—	—	—	—
OpenFlow controller reliability metrics (2.1.1.3)	—	—	—	—	—	—
OpenFlow controller capacity metrics (2.1.1.3)	—	—	—	—	—	—
OpenFlow controller accuracy metrics (2.1.1.3)	—	—	—	—	—	—
OpenFlow controller security metrics (2.1.1.3)	—	—	—	—	—	—
OpenFlow switch availability metrics (2.1.1.4)	—	—	—	—	—	—
OpenFlow switch reliability metrics (2.1.1.4)	—	—	—	—	—	—
OpenFlow switch capacity metrics(2.1.1.4)	—	—	—	—	—	—
OpenFlow switch accuracy metrics (2.1.1.4)	—	—	—	—	—	—
OpenFlow switch security metrics (2.1.1.4)	—	—	—	—	—	—

3.2. CONFIGURATION AND MANAGEMENT TOOLS

Configuration and management tools make integration and migration easier by enabling operators to manage both traditional network devices and SDN devices.

With centralized control, configuration, and management tools, operators can manage traditional network devices, hybrid devices, and SDN controllers. These tools also allow a company to migrate easily from a traditional network to SDN architecture. In case of failure, these tools offer the possibility to roll back to an older configuration. These are safety tools to minimize migration risks and service disruption on live networks.

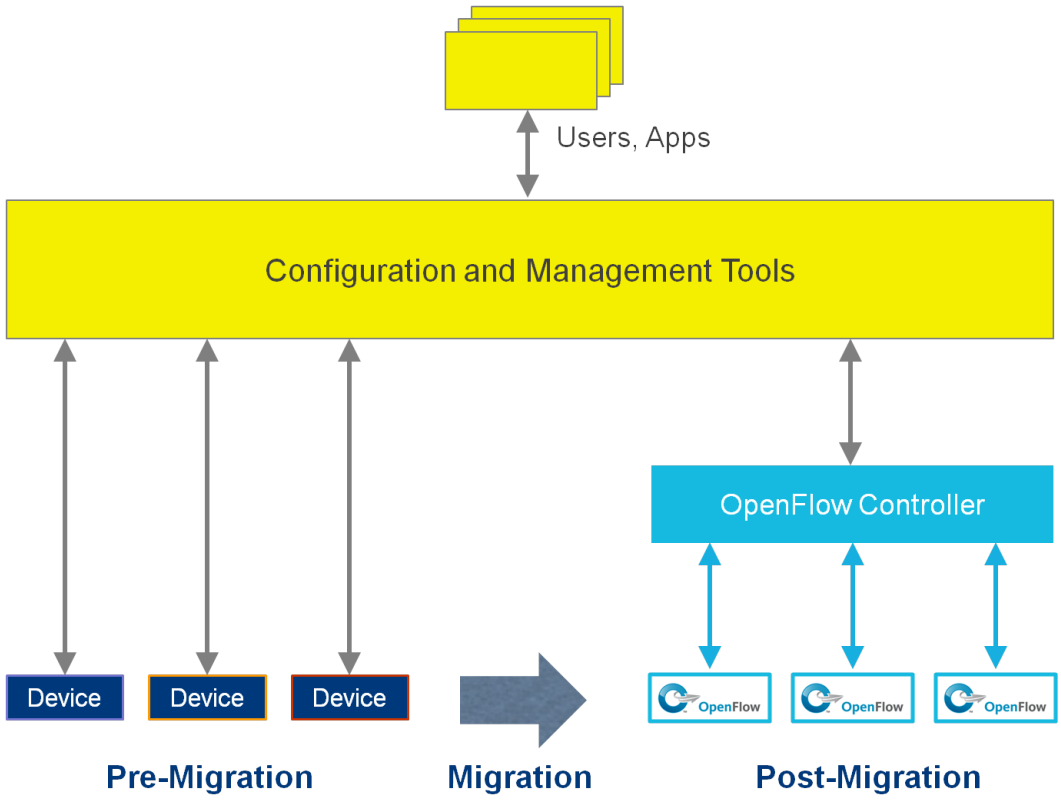

Figure 3 – Migration process using external tools

Considerations	Tools	
	MSActivator	**Twister**
Orchestration and control (2.2.1)	X	—
Interoperability (2.2.2)	X	—
Redundancy and high availability (2.2.3)	X	—
Scalability (2.2.4)	X	—
Technological independence (2.2.5)	X	—
Network abstraction (2.2.6)	—	X
Mixed/hybrid deployments (2.2.7)	X	—
Rollback strategy (2.2.8)	X	X
Authentication (2.2.9)	X	—
Open framework (2.2.10)	X	—
Firmware/image management (2.2.11)	X	—
Role-based access control (2.2.12)	X	—
Multi-tenancy (2.2.13)	X	X
Diagnostics and troubleshooting (2.2.16)	X	X
Support for OF-Config (2.2.17)	—	—
Protocol version interoperability (2.2.17)	—	—

3.3. TESTING AND VERIFICATION TOOLS

Testing and verification tools are expected to be in use on the target network to test and verify the SDN and traditional network functionalities of that target network. These tools can also be used during the phases of the migration to gauge the health of the migration and integration processes. The results from these tests will trigger corrections when necessary. The following table lists the testing and verification tools currently available for SDN migration and features they possess.

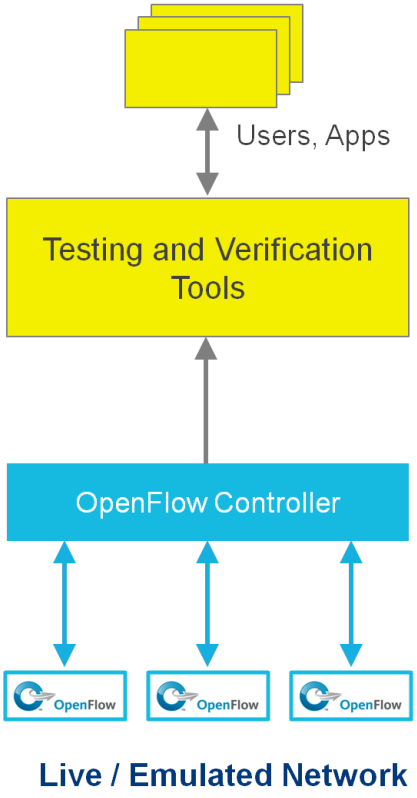

Figure 6 - Migration verification

Considerations	Tools														
	ATPG	Cbench	IxANVL	IxNetwork	Mininet	NetPlumber	NICE	OF Controller TS	OFPeck	OFrewind	OF Switch TS	OFTest	OFtrace	TestON	Wireshark
Scalability (2.2.4)	—	—	X	—	X	X	X	—	—	X	—	X	—	—	—
Multi-tenancy (2.2.13)	X	X	X	X	X	X	—	X	X	X	X	X	—	X	—
Network emulation (2.2.14)	—	—	X	X	X	—	—	—	—	—	—	—	—	—	—
GUI (2.2.15)	—	X	X	X	X	—	—	X	X	—	X	X	—	X	X
Optional unified multi-layer view GUI (2.2.15)	—	X	X	X	X	N/A	N/A	X	X	N/A	—	X	N/A	X	—

4. Gap Analysis

Section 2 outlined some key considerations for the tools and metrics that can be used in various stages of an SDN migration.

Section 3 provided a description of some open-source and commercial tools suitable for SDN migration, categorized as monitoring tools, configuration and management tools, and testing and verification tools. It also provided an overview of the level of support that these tools currently offer for the considerations (metrics and tool capabilities) outlined in Section 2. Such a cross-matching between what is desired and what is currently available forms the basis of our ongoing gap analysis work.

This section is a placeholder for our gap analysis work and provides simple examples of metrics and tool capabilities identified as desirable for an SDN migration, but not commonly supported in existing tools. Our work aims to serve as input to industry discussions around the need to enhance current SDN migration processes through leveraging some of the best practices from the IT world (e.g., software tool chains and workflow automation). Per the Migration Working Group's current charter, we intend to build a prototype and a demo of an SDN migration tool chain, demonstrating some of the metrics and tool capabilities described in this document.

While quite a few gaps have been identified in Section 3 (see tables), a number of other considerations, tool capabilities, and metrics have not yet been covered in detail in this document. These remain for further study. Examples of such items include:

- Ability for monitoring tools to support new metrics through simple addition of new SNMP object identifiers (OIDs).
- Several controller-related metrics, particularly desirable for large-scale OpenFlow-based SDN deployments:
  - Metrics for measuring sensitivity to the geographic distance for stateful/stateless switchover (e.g. in clustered and/or geographically distributed deployments).
  - Metrics for software and hardware error measurements.
  - Metrics related to orchestration, including hierarchical and distributed controllers.
- Metrics related to OF-Config for managing devices.
- Ability to check and verify protocol version interoperability.

We expect to expand and refine the list of gaps in subsequent versions of this document.

5. Conclusion

One of the main objectives of this document was to examine tools and metrics that can be useful in the three stages of an SDN migration process, namely:

- Preparation of the starting network
- The phased SDN migration
- Post-migration testing and verification of the target OpenFlow-based SDN network.

Various considerations for such tools and metrics were discussed with a focus on their fit and suitability in the three stages. Some of these considerations, for example, relate to security, scalability, and redundancy of the tools, as well as OpenFlow-specific metrics. Collectively, these tools and metrics could lay the groundwork for a successful and smooth SDN migration. They could help network operators detect and avoid network incidents, determine specific responses for rapid recovery, and apply timely contingency plans if issues are experienced at any stage during an SDN migration process.

In this document, an effort has been made to identify both open-source and commercial tools for monitoring, configuration and management, and testing and troubleshooting. In addition, an attempt has been made to map these tools according to their applicability in the three SDN migration phases. The intention here is not necessarily to recommend specific tools, but rather to provide an overview of the spectrum of available tools and their SDN-specific capabilities, which are important for a seamless SDN migration. The broader objective of this work is to help accelerate a broader adoption of open SDN in the industry.

Future work, as currently planned, includes identifying an SDN migration use case, developing a prototype working code for SDN migration validating some of the metrics, and demonstrating a prototype migration tool chain.

As networks continue to evolve and as new technologies and challenges emerge, some of the considerations and SDN migration tools and metrics identified in this document might need to be revisited in the future. As such, this will be a living document, and new findings and requirements will be captured in possible future releases.

Contributors

Salman Asadullah

Hakki C. Cankaya

Justin Dustzadeh (Editor)

Bhumip Khasnabish

Guillaume Reffet

Evelyne Roch (Editor)

Mukhtiar Shaikh (Editor)

Pascal Smacchia

References

[1] *Use Cases and Migration Methods*, ONF Migration Working Group https://www.opennetworking.org/images/stories/downloads/sdn-resources/use-cases/Migration-WG-Use-Cases.pdf

[2] Business Metrics Solution Suite 2.0 http://www.tmforum.org/DownloadRelease13/14772/home.html

[3] OF Controller TS, http://www.codenomicon.com/products/openflow-switch.shtml

[4] OF Switch TS, http://www.codenomicon.com/products/openflow-controller.shtml

[5] OFrewind, http://archive.openflow.org/wk/index.php/OFRewind

[6] IxNetwork, http://www.ixiacom.com/solutions/sdn-openflow-test/products/index.php

[7] NICE, https://code.google.com/p/nice-of/

[8] OFTest, http://www.projectfloodlight.org/oftest/

[9] ATPG, https://bitbucket.org/peymank/hassel-public/

[10] Hassel and NetPlumber, https://bitbucket.org/peymank/hassel-public/

[11] Mininet, http://onlab.us/mininet.html

[12] OFPeck, http://archive.openflow.org/wk/index.php/Ofpeck

[13] OFtrace, http://archive.openflow.org/wk/index.php/Liboftrace

[14] OpenSeer, http://archive.openflow.org/wk/index.php/OpenSeer

[15] MSActivator http://www.youtube.com/watch?v=Nq3-ERkir5M&feature=youtu.be

http://www.ubiqubesolutions.com/solutions-overview/sdn/