Manage your **SDN Network** with **StableNet®**

infosim®

SDN - A Promising Approach for Next Generation Networks

Recently, Software Defined Networking (SDN) has become a very popular term in the area of communication networks. The key idea of SDN is to introduce a separation of the control plane and the data plane of a communication network. The control plane is removed from the normal network elements into typically centralized control components. The normal elements can be replaced by simpler and therefore cheaper off-the-shelf devices that are only taking care of the data plane, i.e. forwarding traffic according to rules introduced by the control unit.

SDN is expected to bring several benefits, such as reduced investment costs due to cheaper network elements, and a better programmability due to a centralized control unit and standardized vendor-independent interfaces. In particular, SDN is also one of the key enablers to realize network virtualization approaches which enable companies to provide application-aware networks and simplify cloud network setups.

There are various SDN use cases and application areas that mostly tend to benefit from the increased flexibility and dynamicity offered by SDN. The application areas reach from resource management in the access area with different access technologies, over datacenters where flexible and dynamic cloud and network orchestration are more and more integrated, to the business area where distributed services can be realized more flexibly over dedicated lines realized by SDN. Each SDN use case is, however, as individual as the particular company. A unified OSS solution supporting SDN, as offered with Infosim® StableNet®, should therefore be an integral part of any setup.

SDN Challenges – 6 things to think about before you go SDN

The benefits of SDN seem evident. It is a very promising approach to increase flexibility and reduce cost. The idea of a common standard further seems to ease the configuration and handling of an SDN network. However, our experience shows that with the decision to "go SDN" a lot of new challenges arise. Six major ones of these challenges – by far no complete list – are addressed in the following.

Bootstrapping, Configuration and Change Management

SDN aims at a centralization of the network control plane. Given that an SDN network is readily setup, a central controller can adequately manage the different devices and the traffic on the data plane. That is, however, exactly one of the challenges to solve. How to get the SDN network to be setup before any SDN protocols can actually be used? How to assign the different SDN devices to their controllers? How to configure backup controllers in case of outages, etc.? The common SDN protocols are not adequate for these tasks but focus on the traffic control of a ready setup network. Thus, to be ready to "go SDN" additional solutions are required.

Smooth migration from legacy to SDN

The previously mentioned phenomenon of a need for configuration and change management is furthermore exacerbated by the coexistence of SDN and non-SDN devices. From our experience in the Telco industry, it is not possible to start from scratch and move your network to an SDN solution. The challenge is rather to smoothly migrate an existing environment while continuously assuring the management of the entire system consisting of SDN and non-SDN elements. Thus, legacy support is an integral part of SDN support.

Configuration transparency and visualization

By separating control plane and data plane, SDN splits the configuration into two different levels. When sending commands to the SDN network, normally you never address any device directly but this "south bound" communication is totally taken care of by the controllers. All control steps are conducted using the "north bound" API(s). This approach on the one side simplifies the configuration process, on the other side leads to a loss of transparency. SDN itself does not offer any neutral/objective view on the network if the configuration sent via the north bound API actually was sent to the south bound API in the proper and desired way. However, such a visualization, e.g., as overlay networks or on a per flow base, is an important requirement to assure the correctness and transparency of any setup.
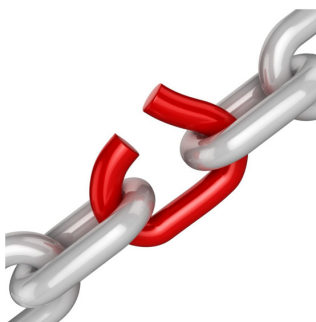
SLA monitoring and compliance

The requirements to SDN mentioned earlier even go one step further. Assuring the correctness and transparency of the setup as mentioned before only guarantees that path layouts, flow rules, etc. are setup in a way as desired during the configuration process. To assure the effectivity of resource management and traffic engineering actions and thus the satisfaction of the customers using the infrastructure, however, more than just the correctness of the setup is needed. SLAs have to be met to assure that the users really get what they expect and what they pay for. The term SDN often goes along with the notion of application-aware networks. However, SDN itself cannot provide any guarantee that this application-awareness really brings the expected benefits. Thus, a possibility for an objective monitoring of the network, its flows, services and their corresponding KPIs is necessary.

Handling of competing standards and proprietary solutions

One main expectation to SDN is that a common standard will remove the necessity to control any proprietary devices. However, recent developments show that first, the different standardization efforts cannot really agree on a single controller and thus a single north bound API. Furthermore, many popular hardware vendors even offer their proprietary flavor of SDN. To cope with these different solutions, an adequate mediation layer is needed.

Localization of failures without any "distributed intelligence"

In a traditional network with decentralized control plane, the localization of failed components can be done as a part of the normal distributed protocols. Since devices are in continuous contact anyway, failure information is spread in the network and the actual location of an outage can thus be identified. In an SDN environment, what has been a matter of course suddenly cannot be relied on anymore. By design, devices normally only talk to the controller and only send requests if new instructions are needed. Devices never talk to any other devices and might not even have such capabilities. Therefore, on the one hand a device will in general not recognize if any adjacent link is down, and on the other hand in particular, will not spread such information in the network. Therefore, new possibilities have to be found to recognize and locate failures.

StableNet® SDN Portfolio

StableNet® is a fully integrated 4 in 1 solution in a single product and data structure, which includes Configuration, Performance, and Fault Management, as well as Network and Service Discovery. By integrating SDN, StableNet® can now leverage the following functionalities:
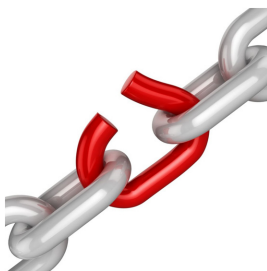
Handle 10,000's of devices, including SDN and legacy

StableNet® is equipped with a powerful and highly automated discovery engine. Besides its own enhanced network CMDB, it offers inventory integration with third-party CMDBs. Furthermore, StableNet® supports many different standardized and vendor-specific interfaces and protocols. Altogether, this leads to an ultra-scalable unified inventory for legacy and SDN devices.

Check your SLAs! Do you get what you want?

The StableNet® Performance Module offers a holistic service monitoring on both server and network level. It thereby combines traditional monitoring approaches such as NetFlow with new SDN monitoring approaches. A powerful script engine allows for the configuration of sophisticated End-to-End monitoring scripts. The availability of cheap Plug & Play StableNet® Embedded Agents furthermore simplifies the distributed measurement of a service. Altogether, this gives the possibility to measure all necessary KPIs of a service and to assure its SLA compliance.

Mitigate failures in SDN and legacy environments

The StableNet® Fault and Impact Modules with the SDN extension combines a device-based automated root cause analysis with a service-based impact analysis to provide visibility.
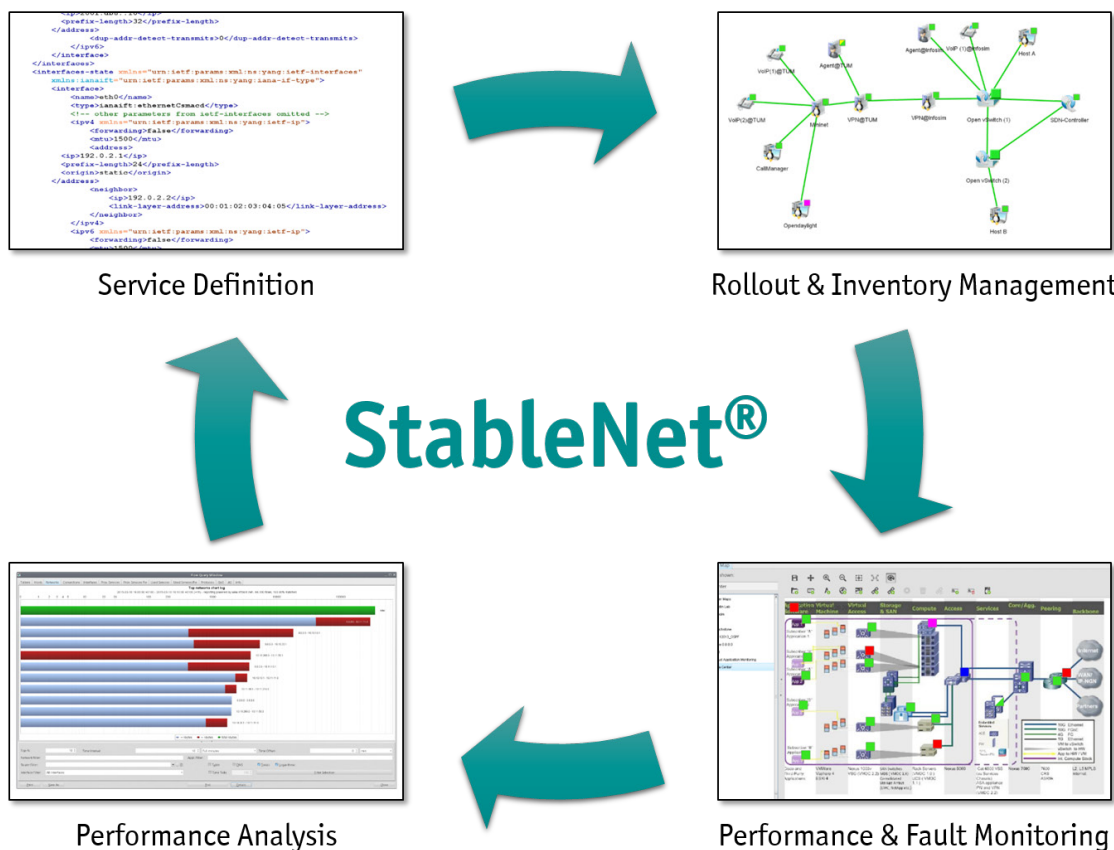
Looking for automate service provisioning, incl. SDN?

StableNet® offers an ultra-scalable, automated change management. An integration with the SDN Northbound Interface adds the possibility to configure SDN devices. The different options offered by the module help to keep track of changes done to the configuration or to check for policy violations and vulnerabilities.

Infosim® StableNet® Service Workflow

One key driver to successfully implement SDN networks is the availability of a service catalogue for providing a holistic view on any service in a network, including all involved entities, e.g. network components, servers and user devices.
Offering a holistic, aggregated view on these services enables

the creation of a service matrix that hugely facilitates different NMS tasks, e.g. configuration or SLA monitoring.
In the following, a StableNet® example workflow is illustrated, consisting of the definition of a service, the rollout, the monitoring, and the analysis.

Service Definition

Rollout & Inventory Management

StableNet®

Performance Analysis

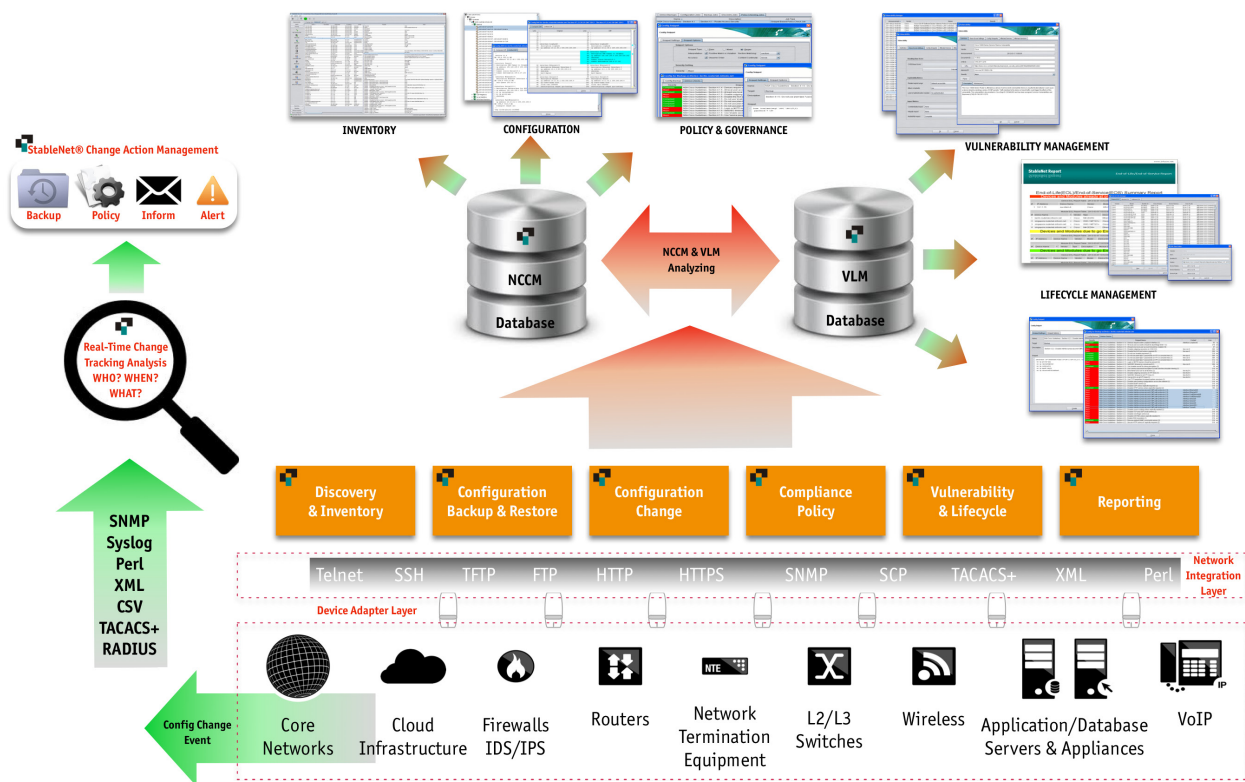

Performance & Fault Monitoring

NFV - Going beyond SDN

Network Functions Virtualization (NFV) is another term that has garnered a great deal of attention in the Telco market over the last couple of years. NFV is related to SDN, but differs in detail. This concept aims at removing network functions from inside the network and putting them to typically central places, such as datacenters. Similar as for SDN, the main objectives are

to increase the flexibility of the control and to reduce costs by moving from expensive special purpose hardware to common off-the-shelf devices. Having your NFV use case in mind and looking for an adequate OSS solution? Please contact us to discuss about more details!

Our Strengths
Innovation & Quality

StableNet® Change Action Management

Backup   Policy   Inform   Alert

Real-Time Change Tracking Analysis WHO? WHEN? WHAT?

SNMP
Syslog
Perl
XML
CSV
TACACS+
RADIUS

Config Change Event

INVENTORY   CONFIGURATION   POLICY & GOVERNANCE

VULNERABILITY MANAGEMENT

LIFECYCLE MANAGEMENT

NCCM
Database

NCCM & VLM Analyzing

VLM
Database

| Discovery & Inventory | Configuration Backup & Restore | Configuration Change | Compliance Policy | Vulnerability & Lifecycle | Reporting |

Telnet   SSH   TFTP   FTP   HTTP   HTTPS   SNMP   SCP   TACACS+   XML   Perl

Network Integration Layer

Device Adapter Layer

Core Networks   Cloud Infrastructure   Firewalls IDS/IPS   Routers   Network Termination Equipment   NTE   L2/L3 Switches   Wireless   Application/Database Servers & Appliances   VoIP

StableNet® is Vendor-Agnostic - supports more than 60+ Manufacturer Types and over 800+ Model Types.

About Infosim®

Infosim® is a leading manufacturer of automated Service Fulfillment and Service Assurance solutions for Telcos, ISPs, Managed Service Providers and Corporations. Since 2003, Infosim® has been developing and providing StableNet® to Telco and Enterprise customers. Infosim® is privately held with offices in Germany (Wuerzburg - Headquarter), USA (Austin) and Singapore.

Infosim® develops and markets StableNet®, the leading unified software solution for Fault, Performance and Configuration Management. StableNet® is available in two versions:
- Telco (for Telecom Operators and ISPs) and
- Enterprise (for Corporations)

StableNet® is a single platform unified solution designed to address today´s many operational and technical challenges of managing distributed and mission-critical IT infrastructures.

Many leading organizations and Network Service Providers have selected StableNet® due to its rich set of features and reduction in OPEX & CAPEX. Many of our customers are well-known global brands spanning all market sectors.

At Infosim®, we place paramount focus on customer satisfaction. We uphold an indomitable spirit for innovation and high quality products.

Why Infosim®?
- Quality software design you can trust and rely on
- Proven solution with a large number of installed sites
- Unified solution which covers Configuration, Fault/RCA and Performance Management in a single product
- Reduction in OPEX & CAPEX via product consolidation, step-by-step migration and retirement of existing legacy element management solutions
- Automated Service Delivery directly from your Integrated Service Catalogue
- Configuration & Policy Governance that maximizes Service Availability and reduces MTTR
- Rapid ROI by reduction in OPEX & CAPEX and customer service credits realized via greater Service Availability
- SOA-based technology, meaning it is highly integrable and flexible

Differentiation

StableNet® is a 3rd generation highly automated Network Management System. The key differentiation of StableNet® to other legacy type Operational Support Systems (OSS) is that StableNet® is a unified OSS system with three integrated functionalities that focus on Fault, Performance and Configuration Management, with automated Root-Cause-Analysis (RCA). StableNet® can be deployed on a Multi-Tenant, Multi-Customer, or Dedicated platform and can be operated in a highly flexible and dynamic environment like a Cloud or dynamic flex-compute environment.

We look forward to hearing from you!

Infosim GmbH & Co. KG · Friedrich-Bergius-Ring 15 · 97076 Würzburg, Germany · Phone +49 931 20592 200 · www.infosim.net
Infosim, Inc. · 3721 Executive Center Drive · Bldg 11, Suite 215 · Austin, TX 78731 · Phone +1 512 522 0955
Infosim Asia Pacific Pte Ltd. · 8 Ubi Road 2 · #08-04 Zervex · 408538 Singapore · Phone +65 6562 8286