Benefits of Implementing NETCONF

David Eror, Network Consulting Engineer, NIL

June 17, 2015

Network Configuration Protocol (NETCONF) is a standardized network management protocol that provides a simple mechanism of configuration data retrieval and new configuration data upload and manipulation. NETCONF uses Extensible Markup Language (XML)-based data encoding for the configuration data and protocol messages, with several possible capabilities of a secure transport.
**Intro**

NETCONF protocol is used in network devices such as routers and switches by some of the major equipment vendors. A particular strength of NETCONF is that it supports the robust configuration change transactions over a number of devices. It was introduced as a proposed alternative to the usual operators’ choices – a proprietary Command Line Interface (CLI) and Simple Network Management Protocol (SNMP). However, CLI often requires scripts with an unpredictable output, and SNMP does not provide an option to configure devices.

As an attempt to have a single vendor-independent XML-based configuration scheme, NETCONF was first standardized by Internet Engineering Task Force (IETF) in RFC 4741 in December 2006, with several other extensions published later.

**NETCONF Architecture for Network Management**

NETCONF uses an XML-based Remote Procedure Call (RPC) mechanism, an inter-process communication that enables a computer program to initiate a procedure to be executed in another address space. XML provides an enhanced, flexible, and hierarchical representation of data that suits the needs of networking devices. NETCONF carries configuration data and operations such as requests and replies over RPCs encoded in XML through a connection-oriented transport, and using Yet Another Next Generation (YANG) as a data modeling language in an XML tree format.

The NETCONF protocol can be partitioned into four layers:

1. The Secure **Transport Protocol** layer provides a secure and reliable transport of messages between a client and a server.
2. The **Messages** layer provides a mechanism for encoding remote procedure calls (RPCs) and notifications.
3. The **Operations** layer defines a set of base protocol operations to retrieve and edit the configuration data.
4. The **Content** layer consists of configuration data and notification data.

Secure transport of NETCONF is implemented over two options:

- NETCONF over SSHv2 – uses RSA crypto keys
- NETCONF over Blocks Extensible Exchange Protocol (BEEP) – uses Simple Authentication and Security Layer (SASL), and requires a crypto image to use a Transport Layer Security (TLS)

**NETCONF for different Cisco devices**

NETCONF is compatible with Cisco IOS, IOS XE, IOS XR and NX-OS platforms.

SW versions that include the NETCONF simple mechanism:

- IOS 12.2(33)SB
- IOS XE 2.1

XML-based enhanced NETCONF is supported from SW versions:

- IOS 15.3(1)S
- IOS XE 3.8S
- IOS XR 5.3.0
- NX-OS Release 5.1(3)N2(1)
**An example of XML messages**

XML-based NETCONF messages to and from the Cisco routers are shown below. It is possible to use different available NETCONF GUI clients.

After connecting using NETCONF over SSH, the router answers with the capabilities:

```
linux:~$ ssh -s cisco@192.168.6.10 netconf
Password:
<?xml version="1.0" encoding="UTF-8"?><hello><capabilities>
<capability>urn:ietf:params:netconf:base:1.0</capability>
<capability>urn:ietf:params:netconf:capability:writeable-running:1.0</capability>
<capability>urn:cisco:params:netconf:capability:notification:1.0</capability>
</capabilities>
</hello>
```

In order to send a `hello` to the Cisco router, it is possible to use the following XML message:
A `get-config` request for the configuration retrieval would look like the below example:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
     xmlns:cpi="http://www.cisco.com/cpi_10/schema">
    <get-config>
        <source>
            <running/>
        </source>
    </get-config>
</rpc>
```

Router would respond with the configuration with this message:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="101">
    <data><cli-config-data-block>
        version 12.4
        service timestamps debug datetime msec
        service timestamps log datetime msec
        no service password-encryption
        hostname cisco
    </cli-config-data-block></data>
</rpc-reply>
```
NETCONF basic configuration

NETCONF needs to be enabled on the routers. There are slight platform-dependent differences:

- **IOS XR** (default port is 830)

  ```
  ssh server netconf port 380
  netconf-yang agent ssh
  ```

- **IOS and IOS XE**

  ```
  netconf ssh
  netconf lock-time 60
  netconf max-sessions 16
  netconf max-message 37283
  ```

Prior to configuring NETCONF over SSHv2, rsa crypto keys also need to be generated.

**Conclusion**

NETCONF might be considered as a potential tool for configuring network devices differently. Using NETCONF can also be seen as an attempt to use a single XML-based configuration scheme for upload and download, regardless of (your choice of) vendor. Several vendors have already begun
supporting NETCONF. This might look similar to what OpenFlow (or Cisco proprietary alternative OpFlex) is used for, only the actual commands sent to change the configuration of the device would be XML-based. NETCONF opens also a window to the extended use of perl or python scripting.

We could conclude that while clear advantages of NETCONF are seen, it will probably take some time for the vendors to implement it wider, and for the operators to utilize it to its full capacity, replacing of the old CLI commands. SNMP, which has been used from the beginnings of IP networking, will surely remain a viable choice, together with NETCONF.
NIL – More Than Just a Training Company

NIL Learning delivers the leading-edge Cisco and CWNP training to IT professionals and companies around the globe. Through field-proven experts — each both active engineer and instructor — NIL Learning enhances the standard learning curriculum with real-life experience and helps clients to maximize their training investment.

NIL Learning is part of NIL, a leading global IT solutions provider. Since 1992, NIL has been at the forefront of advanced contributors to strategic partner Cisco’s technologies, learning curriculum and value-added solutions deployed to clients around the globe. Today, NIL has earned the highest certifications offered by Cisco, VMware, EMC, HP, IBM, Microsoft, F5, MobileIron, RSA, VCE and others. Their portfolio of solutions consists of managed services, professional services and learning services.

NIL is headquartered in Slovenia, with regional offices in Croatia, Serbia, Saudi Arabia, the U.S., South Africa, Morocco, Nigeria, Kenya and Botswana.

Why Learn at NIL LEARNING?

- All NIL LEARNING instructors are field-proven experts - each both active engineer, content developer and instructor.
- 75% of NIL LEARNING engineers hold CCSI certifications, and 20 have already achieved the respected CCIE rank.
- NIL LEARNING enhances the standard learning curriculum with real-life experience and helps clients to maximize their training investment.
- NIL has been a Cisco training partner since 1993; today NIL holds Cisco Learning Partner Specialized status and Cisco Business Learning Partner status.
- NIL was awarded the Cisco Most Business Relevant Learning Partner in MEA in 2010 and the Most Innovative Learning Partner in MEA.
- NIL received the Innovation Award for its Technology Led Training and its extensive contribution to Cisco learning solutions at the Cisco EMEAR Learning Partner Summit in 2012.
• NIL received the **Innovation Award** for its Technology Led Training and Advanced Engineer Program at the Cisco Global Learning Partner Summit in 2013.

• NIL won the **Cisco Global Learning Partner of the Year** award at the Cisco Partner Summit in 2014.

• NIL Learning runs a centralized training schedule across the whole EMEAR region.
More Info

Slovenia
T: +386 1 4746 500
E: sales-support@nil.com

Saudi Arabia
T: +966 1 465 4641
E: info.nilme@nil.com

Botswana
T: +267 318 1684
E: training@it-iq.bw

Serbia
T: +381 11 2420 388
E: info-nilserbia@nil.co.rs

Croatia
T: +385 (0)51 583 255
E: info-nilcroatia@nil.com

South Africa
T: +27 (0)11 575 4637
E: mea_sales@nil.com

Kenya
T: +254 773 145 680
E: mea_sales@nil.com

Turkey
T: +386 1 4746 500
E: sales-support@nil.com

Morocco
T: +212(0) 660 808 394
E: info-nilmorocco@nil.com

USA
T: +1 612 886 3900
E: info-nilusa@nil.com

Nigeria
T: +234 1 903 53 47
E: mea_sales@nil.com

learning.nil.com