NETCONF over TLS

Jürgen Schönwälder

IETF 86, Orlando, 2013-03-11
Motivation

- Alternate transport for platforms that do not support SSH, e.g., embedded systems
- Revision of RFC 5539 to adapt to the new chunked framing
- Defines a mechanism for generating NETCONF usernames from X.509 certificates or pre-shared keys

Status

- Current status in draft-ietf-netconf-rfc5539bis-02
- Last call running (so please read and send comments)
The identities etc. have been essentially copied from the SNMP configuration model. Are we really happy with this reuse by copying?

If so, do we keep the SNMP configuration model names or adapt them to the NETCONF context?

If not, where shall we define a reusable grouping for extracting a user name (security name) from an X.509 certificate?
Right now, the YANG module focuses on the username mapping only.

There are certainly more configuration objects for the TLS transport, e.g., which ports to listen on, which CERT to use etc.

Shall we add additional configuration objects? (The SNMP configuration model covers endpoints to listen on, it does not cover the CERT to be used by the TLS server.)
Open Issue #3: Call Home for TLS

Shall we add support for call home, i.e., a device, after initiating and establishing a TCP connection and executing the TLS handshake, would switch role and subsequently act as a NETCONF server.
Open Issue #3: Call Home for TLS

1. Device initiates TCP connection (based on a certain schedule)
2. Device initiates TLS exchange with pairwise X.509 authentication
3. Device hands connection over to a NETCONF server, config server hands over to a NETCONF client
4. NETCONF <hello> exchange ensures proper roles are picked