NETCONF over TLS

Jürgen Schönwälder

j.schoenwaelder@jacobs-university.de

draft-ietf-netconf-rfc5539bis-04
Major changes since IETF 86

• Switching roles after TCP connection has been established and before TLS starts
• Added applicability statement proposed by Stephen Hanna
• Added configuration objects (ideas borrowed from the reverse SSH draft)
Issue #1: port numbers

- I-D allocates new port number on which a NETCONF client supporting call-home listens for incoming connections
- Joe expressed concerns whether this is a new service or not (or whether the port number can be saved)
- No concrete alternative proposal so far
Issue #2: call-home config objects

```plaintext
+-rw call-home {tls-call-home}?
  +-rw client* [address port]
    +-rw address inet:host
    +-rw port inet:port-number
  +-rw (connection-type)?
    |   +-:(persistent)
    |     +-rw persistent-connection? empty
    |   +-:(periodic)
    |     +-rw periodic
    |       +-rw interval? uint16
    |       +-rw linger? uint16
  +-rw reconnect-strategy
    +-rw retry-interval? uint16
    +-rw max-attempts? uint16
```
Issue #2: call-home config objects

• Enable 'button' to quickly disable call-home?
• Connect to all clients or iterate through the list until the first connection succeeds?
• Reconnect strategy sufficient or too simple?
• Same reconnect strategy for all clients?
• Do we need to configure the cert/key to use?
• Ideally, this should be a grouping used by both SSH call-home and TLS call-home...