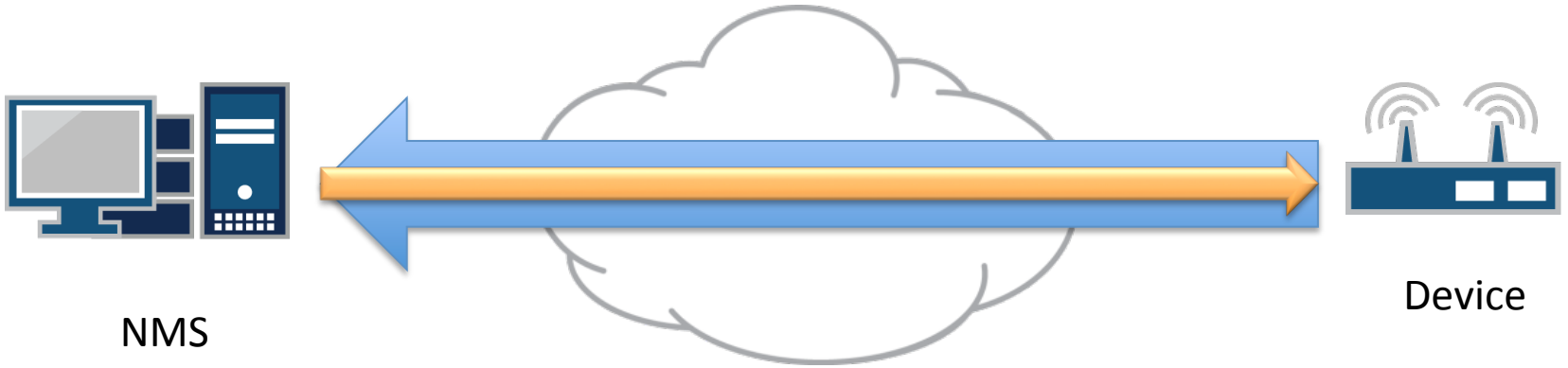
draft-ietf-netconf-reverse-ssh-03

NETCONF Call-Home using SSH

Recap

- NETCONF “call home” is a long time request
  - This draft enables it for SSH
  - RFC5539bis does it for TLS
- Discussed previously at IETF’s 88, 87 and even 81
- Solution
  - Only reverse TCP direction, SSH direction is const -00
  - Updates RFC 4253 -00
  - Requests an assigned port -00
  - Limited to NETCONF -01
  - Configuration unified with RFC 5539bis -02

Only reverses TCP direction, SSH direction is const



- Device initiates the TCP connection, and then runs SSH-server protocol
- NMS accepts TCP connection and then runs SSH-client protocol on top of it

Updates RFC 4253 (if approved)

NETCONF Working Group
Internet-Draft
Updates: 4253 (if approved)
Intended status: Standards Track
Expires: August 18, 2014

K. Watsen
Juniper Networks
February 14, 2014

2.2. Update to RFC 4253

This document updates the SSH Transport Layer Protocol [RFC4253] only by removing the restriction in Section 4 (Connection Setup) of [RFC4252] that the SSH Client must initiate the transport connection. Security implications related to this change are discussed in Security Considerations (Section 7).

IANA Considerations

Service Name:	reverse-ssh
Transport Protocol(s):	TCP
Assignee:	IESG iesg@ietf.org
Contact:	IETF Chair chair@ietf.org
Description:	Reverse SSH (call home)
Reference:	RFC XXXX
Port Number:	YYYY

Applicability Statement

- Added by Security area folks
- Essentially:

Reverse SSH MUST only be used for a NETCONF server to initiate a connection to a NETCONF client

Configuration unified with RFC 5539bis

The YANG moved to draft-kwatsen-netconf-server

- The draft now just directs readers to it

(This is the only real update since the -02 draft)

Current Status

- No Open Issues
- Reference implementation just released

Reference Implementation

https://github.com/Juniper/netconf-call-home

- Implements draft-kwatsen-netconf-server-01
  - Except for the TLS transport and the “periodic” connection type

- Fork it!

Questions / Concerns ?