ConfD NETCONF Call Home

Greg Olin
ConfD Solution Architect
2019-10-22

What is NETCONF Call Home?

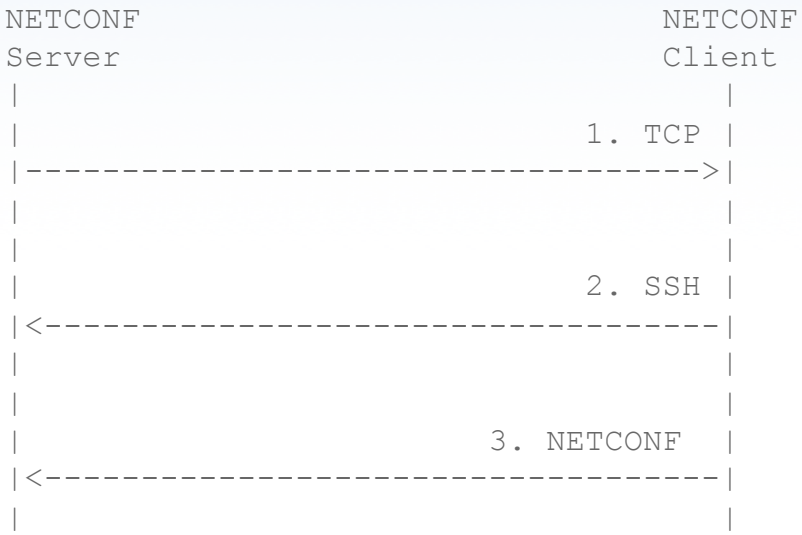
- Defined in RFC 8071
- Published in Feb. 2017
- Enables a NETCONF server to initiate a connection to a NETCONF client
- Client and server roles are preserved with the exception that there is a reversal at the TCP layer, namely who is the TCP client and the TCP server.
- Normally the network element is the TCP server
- But with Call Home, the network element takes on the role of TCP client
- With Call Home, the SSH roles and NETCONF roles stay the same

Why NETCONF Call Home?

- A network element may need to connect when first powered on to register with a management system
- A network element my receive a dynamic IP address but there is no dynamic mapping service, like dynamic DNS
- A network element may be behind a firewall that uses NAT, so it need to initiate the connection
- A network element may be behind a firewall that doesn’t allow the management system access to the internal network
- A network element may not have a fixed port that the management system can use
- The operator may prefer to secure just one port on the management system rather than a port on each network device.

Call Home from a protocol layering perspective

- More beautiful ASCII art



Call Home from a protocol layering perspective (cont'd)

- In this diagram, we see the NETCONF server initiating a TCP connection to the NETCONF client
- Using that TCP connection, the NETCONF client initiates a SSH session to the NETCONF server
  - The normal state of affairs
- Using the SSH session, the NETCONF client initiates a NETCONF session to the NETCONF server
  - Again, the normal state of affairs

What does the NETCONF client do

- Needs to listen on port 4334 for TCP connections
  - This is the IANA assigned port number
  - Could be configured to listen to another port
- When it initiates the SSH session, the client must the server's credentials (host key or certificate)
- Once the SSH connection is established, the client initiates the NETCONF client protocol.

What does the NETCONF server do

- Initiates a TCP connection to port 4334
  - The source port may be according to local policy or randomly assigned by the operating system.
  - Could be configured to listen to another port
- The server's sends its credentials (host key or certificate)
- Once the SSH connection is established, the server starts the NETCONF server protocol
- If you want the connection to be persistent, then the server should support some keep-alive mechanism. This could be a SSH_MSG_GLOBAL_REQUEST
- Configuration could be part of the NETCONF Client and Server Models (still in draft form ☹)

Changes in ConfD to support NETCONF Call Home

- New MAAPI call to initiate NETCONF Call Home
  - `maapi_netconf_ssh_call_home()`
  - Takes the NETCONF client either as IP address or host name, plus port
- We support both the internal SSH server and external SSH server
- For the internal SSH server, no additional configuration needed
- For the external SSH server, you need to specify a program which triggers the TCP connection
  - `/confdConfig/netconf/transport/sshCallHomeExecutable`
- `netconf_console` has been enhanced to support Call Home

Thank you for listening

www.tail-f.com