

NETCONF Protocol Update

Eliot Lear

What is NETCONF?

- A protocol used to securely exchange configuration information with network elements
- Important component necessary for control of elements – without this your scripts WILL break (eventually).

For an overview, See NANOG 28.

NETCONF gets a haircut!

- Simplify the base protocol
 - No more channels in the base protocol
 - Reduce the number of required capabilities
 - Same capabilities whether you use SSH or BEEP (NETCONF *IS* NETCONF Lite)
- Notifications separated
 - SYSLOG exists; more than that deserves more effort
 - Could be added later as a capability, but...
- One connection, one use

Question 1: Directionality

Do you (want to) remotely manage customer devices that might be behind a firewall, NAT or on a DHCP-assigned address?

(Classic case of “managed offerings”)

Important in order to determine whether devices should connect to managers.

Question 2: Port 22 or elsewhere?

Should NETCONF/SSH be on another port?

How many device ACLs would you need to modify?

< 10

> 10

> 100

Things We're Thinking About

- What's the right Mandatory substrate?
 - SOAP/HTTP, SSH, or BEEP
- What authorization models should be supported?
- What sorts of existing toolkits (such as SOAP) can be used?
- Locking
 - Global initially, perhaps more fine grained later
 - Keep bad guys away from locks!
- Support for many different operating models
 - Is the protocol both general AND useful?

More Information

New drafts with these changes due out this month.

Web site <http://www.ops.ietf.org/netconf>

Mailing list: netconf@ops.ietf.org

Eliot in a bar: Somewhere here in Miami