Network Working Group
Internet-Draft
Expires: May 16, 2005

E. Lear
K. Crozier
Cisco Systems

November 15, 2004

Using the NETCONF Protocol over Blocks Extensible Exchange Protocol (BEEP)
draft-ietf-netconf-beep-03

Status of this Memo

Copyright Notice

Abstract

This document specifies an application protocol mapping for the NETCONF protocol over the Blocks Extensible Exchange Protocol (BEEP).

Table of Contents

1. Introduction

The NETCONF protocol [1] defines a simple mechanism through which a network device can be managed. NETCONF is designed to be usable over a variety of application protocols. This document specifies an application protocol mapping for NETCONF over the Blocks Extensible Exchange Protocol (BEEP) [2] .

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [4].

1.1 Why BEEP?

Use of BEEP is natural as an application protocol for transport of XML. As a peer to peer protocol, BEEP provides an easy way to implement NETCONF, no matter which side of the connection was the initiator. This "bidirectionality" allows for either side to play the role of the manager with no protocol changes. Either side can open a channel. Either side could initiate an RPC. This is particularly important to support operational models that involve small devices connecting to a manager, and those devices that must reverse the management connection in the face of firewalls and NATs.

The SASL profile used by BEEP allows for a simple and direct mapping to the existing security model for CLI, while TLS provides a strong well tested encryption mechanism with either server or server and client-side authentication.

2. BEEP Transport Mapping

All NETCONF over BEEP implementations MUST implement the profile and functional mapping between NETCONF and BEEP as described below.

2.1 NETCONF Session Establishment

Managers may be either BEEP listeners or initiators. Similarly, agents may be either listeners or initiators. Thus the initial exchange takes place without regard to whether a manager or the agent is the initiator. After the transport connection is established, as greetings are exchanged, they should each announce their support for TLS [6] and optionally SASL [5] (see below), as well as for the SYSLOG profile [7]. Once greetings are exchanged, if TLS is to be used and available by both parties, the listener STARTs a channel with the TLS profile.

Once TLS has been started, a new greeting is sent by both initiator and listener, as required by the BEEP RFC.

At this point, if SASL is desired, the initiator starts BEEP channel 1 to perform a SASL exchange to authenticate itself. When SASL is completed, the channel MUST be closed.

Once authentication has occurred, there is no need to distinguish between initiator and listener. We now distinguish between manager and agent.

2.2 Capabilities Exchange

The manager now establishes an NETCONF a new channel. As initiators assign odd channels and listeners assign even channels, this next channel is BEEP channel 1 or 2, depending on whether the manager is the initiator or the listener.

Certain NETCONF capabilities may require additional BEEP channels. When such capabilities are defined, a BEEP mapping must be defined as well.

At this point, the NETCONF session is established, and capabilities have been exchanged.

2.3 NETCONF Session Usage

Nearly all NETCONF operations are executed through the <RPC> tag. To issue an RPC, the manager transmits on the operational channel a BEEP MSG containing the RPC and its arguments. In accordance with the BEEP standard, RPC requests may be split across multiple BEEP frames.

Once received and processed, the agent responds with BEEP RPYs on the same channel with the response to the RPC. In accordance with the BEEP standard, responses may be split across multiple BEEP frames.

2.4 NETCONF Session Teardown

Upon receipt of <close-session> from the manager, once the agent has completed all RPCs, it will close BEEP channel 0. When an agent needs to initiate a close it will do so by closing BEEP channel 0. Although not required to do so, the agent should allow for a reasonable period for a manager to release an existing lock prior to initiating a close. Once the agent has closed channel 0, all locks are released, and each side follows tear down procedures as specified in [3]. Having received a BEEP close or having sent <close-session>, a manager MUST NOT send further requests. If there are additional activities due to expanded capabilities, these MUST cease in an orderly manner, and should be properly described in the capability mapping.

2.5 BEEP Profile for NETCONF

There are two commands in the BEEP profile. <rpc> and <rpc-reply>.

2.5.1 BEEP Profile

```
      <!-- DTD for netconf operations over BEEP

        Refer to this DTD as:

          <!ENTITY % NETCONF PUBLIC "netconf/Operation/1.0" "">
          %NETCONF;
        -->

      <!--   Contents

          Overview

          Includes
          Profile Summaries
          Entity Definitions

          Operations
           rpc
           rpc-reply
        -->

      <!--  Overview   NETCONF operation channel  -->
```

```
      <!-- Includes -->

             <!ENTITY % BEEP PUBLIC "-//Blocks//DTD BEEP//EN"
                       "">
             %BEEP;

      <!--  Profile summaries


          BEEP profile NETCONF

          role        MSG                       RPY        ERR
          ====        ===                       ===        ===
          I or L      rpc                               ok         error
          I or L      rpc-reply                 ok         error

      -->

      <!--
        Entity Definitions

              entity        syntax/reference     example
              ======        ================     =======

        a RPC
           RPC-DATA       Alpha
        a RPC reply number
              RPC-REPLY      1*3DIGIT
      -->

      <!ENTITY % RPC-REPLY    "CDATA">
      <!ENTITY % RPC-DATA     "CDATA">

       -->

      <!--
        RPC command
        -->

      <!ELEMENT RPC        (#PCDATA)>
      <!ATTLIST RPC
                RPC-DATA        %RPC_DATA;                #REQUIRED>

   <!--
        Result of RPC.
        -->

      <!ELEMENT RPC-REPLY    (#PCDATA)>
```

```
      <!ATTLIST RPC-REPLY
                RPC-REPLY       %RPC-REPLY;               #REQUIRED
                RPC-DATA    %RPC-DATA             #REQUIRED>

      <!-- End of DTD -->
```

3. Security Considerations

Configuration information is by its very nature sensitive. Its transmission in the clear and without integrity checking leaves devices open to classic so-called "person in the middle" attacks. Configuration information often times contains passwords, user names, service descriptions, and topological information, all of which are sensitive. A NETCONF application protocol, therefore, must minimally support options for both confidentiality and authentication.

BEEP makes use of both transport layer security and SASL. We require that TLS be used in BEEP as described by the BEEP standard. Client-side certificates are strongly desirable, but an SASL authentication is the bare minimum. SASL allows for the use of protocols such as RADIUS [10], so that authentication can occur off the box.

SASL authentication will occur on the first channel creation, and prior to issuance of any protocol operations. No further authentication may occur during the same session. This avoids a situation where rights are different between different channels. If an implementation wishes to support multiple accesses by different individuals with different rights, then multiple sessions are required.

Different environments may well allow different rights prior to and then after authentication. An authorization model is not specified in this document. When an operation is not properly authorized then a simple "permission denied" is sufficient. Note that authorization information may be exchanged in the form of configuration information, which is all the more reason to ensure the security of the connection.

4. IANA Considerations

The IANA will assign a TCP port for NETCONF.

5. Acknowledgments

This work is the product of the NETCONF IETF working group, and many people have contributed to the NETCONF discussion. Most notably, Rob Ens, Phil Schafer, Andy Bierman, Wes Hardiger, Ted Goddard, and Margaret Wasserman all contributed in some fashion to this work, which was originally to be found in the NETCONF base protocol specification. Thanks also to Weijing Chen, Keith Allen, Juergen Schoenwaelder, and Eamon O'Tuathail for their very constructive participation.

6. References

6.1 Normative References

[1] Enns, R., "NETCONF Configuration Protocol", draft-ietf-netconf-prot-03 (work in progress), June 2004.

[2] Rose, M., "The Blocks Extensible Exchange Protocol Core", RFC 3080, March 2001.

[3] Rose, M., "Mapping the BEEP Core onto TCP", RFC 3081, March 2001.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC 2222, October 1997.

[6] Dierks, T., Allen, C., Treese, W., Karlton, P., Freier, A. and P. Kocher, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[7] New, D. and M. Rose, "Reliable Delivery for syslog", RFC 3195, November 2001.

6.2 Informative References

[8] Bray, T., Paoli, J., Sperberg-McQueen, C. and E. Maler, "Extensible Markup Language (XML) 1.0 (Second Edition)", W3C REC REC-xml-20001006, October 2000.

[9] Hollenbeck, S., Rose, M. and L. Masinter, "Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols", BCP 70, RFC 3470, January 2003.

[10] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

Authors' Addresses

Eliot Lear
Cisco Systems
Glatt-com
Glattzentr
um, Zurich 8301
CH

EMail: lear@cisco.com

Ken Crozier
Cisco Systems
170 W. Tasman Dr.
San Jose, CA 95134-1706
US

EMail: kcrozier@cisco.com

Appendix A. Change Log

03, 04: minor gnits relating to <close-session>

02: added comments about locking

01: Removed management channel, rpc-status, rpc-abort, and associated profile changes.

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.