Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 6, 2004.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

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

1. Introduction ...................................................... 3
1.1 Why BEEP? ....................................................... 3
2. BEEP Transport Mapping ........................................... 4
2.1 NETCONF Session Initiation ..................................... 4
2.2 NETCONF RPC Execution ......................................... 4
2.3 NETCONF <rpc-abort> and <rpc-progress> ...................... 5
2.4 NETCONF Session Teardown ...................................... 5
2.5 BEEP Profiles for NETCONF Channels ......................... 5
2.5.1 Management Channel Profile ................................. 5
2.5.2 Operations Channel Profile ................................. 7
2.5.3 Notification Channel Profile ............................... 9
3. Security Considerations .......................................... 10
4. IANA Considerations ............................................. 11
5. Acknowledgments ................................................. 12
    Normative References ........................................... 13
    Informative References ......................................... 14
    Authors’ Addresses ............................................. 14
    Intellectual Property and Copyright Statements .............. 15
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 [3].

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.
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 Initiation

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 [5] and optionally SASL [4] (see below), as well as for the SYSLOG profile [6]. 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.

The manager now establishes an NETCONF management channel for the purpose of exchanging capabilities, monitoring progress, and aborting remote procedure calls. As initiators assign odd channels and listeners assign even channels, the management channel is BEEP channel 1 or 2, depending on whether the manager is the initiator or the listener.

The manager next establishes the NETCONF operational channel for the purpose of issuing RPC requests. This channel is BEEP channel 3 or 4.

Finally, if either manager or agent wishes to send or receive notifications, it may issue a start on the next available channel if the other side has sent the send or receive NETCONF capability.

At this point, the NETCONF session is established.

2.2 NETCONF RPC Execution

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.

2.3 NETCONF <rpc-abort> and <rpc-progress>

<rpc-abort> and <rpc-progress> requests are issued by the manager on the NETCONF management channel, and the agent responds with BEEP RPYs on that same channel.

2.4 NETCONF Session Teardown

Either side may initiate the termination of an NETCONF session. In This is done by issuing a BEEP close on the operational channel after the current RPC has completed. The same is done with any notification channels by the end that transmits notifications. Finally, BEEP channel 0 is closed.

2.5 BEEP Profiles for NETCONF Channels

There are two profiles, the management channel profile and the operations channel profile. These are not to be confused with the BEEP control channel.

The operations channel will have two commands, <rpc> and <rpc-reply>. The management channel will have one additional operation with <rpc-progress>.

2.5.1 Management Channel Profile

<!-- DTD for netconf management over BEEP

Refer to this DTD as:

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

<!-- Contents

Overview

Includes
Profile Summaries
Entity Definitions

Operations
rpc
drpc-reply
drpc-progress

-->  

<!-- Overview NETCONF Management channel -->

<!-- Includes -->

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

<!-- Profile summaries

BEEP profile NETCONF-MANAGEMENT

<table>
<thead>
<tr>
<th>role</th>
<th>MSG</th>
<th>RPY</th>
<th>ERR</th>
</tr>
</thead>
<tbody>
<tr>
<td>I or L</td>
<td>rpc</td>
<td>ok</td>
<td>error</td>
</tr>
<tr>
<td>I or L</td>
<td>rpc-reply</td>
<td>ok</td>
<td>error</td>
</tr>
<tr>
<td>I or L</td>
<td>rpc-progress</td>
<td>ok</td>
<td>error</td>
</tr>
</tbody>
</table>

-->  

<!-- Entity Definitions

<table>
<thead>
<tr>
<th>entity</th>
<th>syntax/reference</th>
<th>example</th>
</tr>
</thead>
<tbody>
<tr>
<td>a PRC</td>
<td>RPC-DATA</td>
<td>Alpha</td>
</tr>
<tr>
<td>a RPC reply number</td>
<td>RPC-REPLY</td>
<td>1*3DIGIT</td>
</tr>
<tr>
<td>a RPC progress number</td>
<td>RPC-PROGRESS</td>
<td>1*3DIGIT</td>
</tr>
</tbody>
</table>

-->  

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

<!--
Progress of RPC operation.
-->
<!ELEMENT rpc-progress   (#PCDATA)>  
<!ATTLIST rpc-progress
  rpc-progress %RPC-PROGRESS;                #REQUIRED>

<!-- End of DTD -->

2.5.2 Operations Channel 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

Lear & Crozier Expires April 6, 2004 [Page 7]
rpc
rpc-reply
-->

<!-- Overview NETCONF operation channel -->

<!-- Includes -->

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

<!-- Profile summaries -->

BEEP profile NETCONF-MANAGEMENT

<table>
<thead>
<tr>
<th>role</th>
<th>MSG</th>
<th>RPY</th>
<th>ERR</th>
</tr>
</thead>
<tbody>
<tr>
<td>I or L</td>
<td>rpc</td>
<td>ok</td>
<td>error</td>
</tr>
<tr>
<td>I or L</td>
<td>rpc-reply</td>
<td>ok</td>
<td>error</td>
</tr>
</tbody>
</table>

<!--

Entity Definitions

entity syntax/reference example
====== ================ ========
a PRC 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

Lear & Crozier Expires April 6, 2004 [Page 8]
2.5.3 Notification Channel Profile

The NETCONF notification channel profile is defined in RFC 3195 [6].
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 [9], 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. Thus, 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.
Normative References


Informative References


Authors’ Addresses

Eliot Lear
Cisco Systems
170 W. Tasman Dr.
San Jose, CA  95134-1706
US
EMail: lear@cisco.com

Ken Crozier
Cisco Systems
170 W. Tasman Dr.
San Jose, CA  95134-1706
US
EMail: kcrozier@cisco.com
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION.
HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgment

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