Network Working Group
Internet-Draft
Expires: March 8, 2005

T. Goddard
ICEsoft Technologies Inc.

September 7, 2004

Using the Network Configuration Protocol (NETCONF) Over the Simple Object Access Protocol (SOAP)
draft-ietf-netconf-soap-03

Status of this Memo

Copyright Notice

Abstract

The Network Configuration Protocol (NETCONF) is applicable to a wide range of devices in a variety of environments. The emergence of Web Services gives one such environment, and is presently characterized by the use of the Simple Object Access Protocol (SOAP). NETCONF finds many benefits in this environment: from the re-use of existing standards, to ease of software development, to integration with deployed systems. Herein, we describe SOAP over HTTP and SOAP over

BEEP bindings that yield application protocols sufficient for NETCONF.

Table of Contents

1. Introduction

Given the use of XML [2] and the remote procedure call characteristics, it is natural to consider a binding of the NETCONF [1] operations to a SOAP [3] application protocol. This document proposes a binding of this form.

In general, SOAP is a natural application protocol for NETCONF, essentially because of the remote procedure call character of both. However, care must be taken with SOAP over HTTP as it is inherently synchronous and client-driven. SOAP over BEEP [15] is technically superior, but is not as widely adopted.

Four basic topics are presented: SOAP specifics of interest to NETCONF, specifics on implementing NETCONF as a SOAP-based web service, security considerations, and an appendix with functional WSDL. In some sense, the most important part of the document is the brief WSDL document presented in the Appendix. With the right tools, the WSDL combined with the base NETCONF XML Schemas provide machine readable descriptions sufficient for the development of software applications using NETCONF.

2. SOAP Background for NETCONF

Why introduce SOAP as yet another wrapper around what is already a remote procedure call message? There are, in fact, both technical and practical reasons. The technical reasons are perhaps less compelling, but let's examine them first.

The use of SOAP does offer a few technical advantages. SOAP is fundamentally an XML messaging scheme (which is capable of supporting remote procedure call) and it defines a simple message format composed of a "header" and a "body" contained within an "envelope". The "header" contains meta-information relating to the message, and can be used to indicate such things as store-and-forward behaviour or transactional characteristics. In addition, SOAP specifies an optional encoding for the "body" of the message. However, this encoding is not applicable to NETCONF as one of the goals is to have highly readable XML, and SOAP-encoding is optimized instead for ease of automated deserialization. These benefits of the SOAP message structure are simple, but worthwhile due to the fact that they are already standardized.

It is the practical reasons that truly make SOAP an interesting choice for device management. It is not difficult to invent a mechanism for exchanging XML messages over TCP, but what is difficult is getting that mechanism supported in a wide variety of tools and operating systems and having that mechanism understood by a great many developers. SOAP over HTTP (with WSDL) is seeing good success at this, and this means that a device management protocol making use of these technologies has advantages in being implemented and adopted. Admittedly, there are interoperability problems with SOAP and WSDL, but such problems have wide attention and can be expected to be resolved.

2.1 Use and Storage of WSDL and XSD

One of the advantages of using machine readable formats such as Web Services Description Language (WSDL) [4] and XML Schemas [5] is that they can be used automatically in the software development process. With appropriate tools, WSDL and XSD can be used to generate classes that act as remote interfaces or application specific data structures. Other uses, such as document generation and service location, are also common. A great innovation found with many XML-based definition languages is the use of hyperlinks for referring to documents containing supporting definitions. For instance, in WSDL, the import statement

```
<import namespace="urn:ietf:params:xml:ns:netconf:base:1.0"
        location="http://iana.org/ietf/netconf/base_1.0.xsd"/>
```

imports the definitions of XML types and elements from the base NETCONF schema. Ideally, the file containing that schema is hosted on a web server under the authority of the standards body that defined the schema. In this way, dependent standards can be built up over time and all are accessible to automated software tools that ensure adherence to the standards. Thus, it will gradually become as important for iana.org to host documents like

http://iana.org/ietf/netconf/base_1.0.xsd

as the IETF now hosts documents such as

http://www.ietf.org/rfc/rfc2616.txt

Note that WSDL declarations for SOAP over BEEP bindings are not yet standardized.

2.2 SOAP over HTTP

While it is true that SOAP focuses on messages and can be bound to different underlying protocols such as HTTP, SMTP, or BEEP, most existing SOAP implementations support only HTTP or HTTP/TLS.

There are a number of advantages to considering SOAP over protocols other than HTTP, as HTTP assigns the very distinct client and server roles by connection initiation. This causes difficulties in supporting asynchronous notification and can be relieved in many ways by replacing HTTP with BEEP.

2.3 HTTP Drawbacks

HTTP is not the ideal transport for messaging, but it is adequate for the most basic interpretation of "remote procedure call". HTTP is based on a communication pattern whereby the client (which initiates the TCP connection) makes a "request" to the server. The server returns a "response" and this process is continued (possibly over a persistent connection, as described below). This matches the basic idea of a remote procedure call where the caller invokes a procedure on a remote server and waits for the return value.

Potential criticisms of HTTP could include the following:

- server-initiated data flow is awkward to provide
- headers are verbose and text-based
- idle connections may be closed by intermediate proxies
- data encapsulation must adhere to MIME
- bulk transfer relies on stream-based ordering

In many ways these criticisms are directed at particular compromises

in the design of HTTP. As such, they are important to consider, but it is not clear that they result in fatal drawbacks for a device management protocol.

2.4 BCP56: On the Use of HTTP as a Substrate

Best Current Practice 56 [9] presents a number of important considerations on the use of HTTP in application protocols. In particular, it raises the following concerns:

- HTTP may be more complex than is necessary for the application
- The use of HTTP may mask the application from some firewalls
- A substantially new service should not re-use port 80 as assigned to HTTP
- HTTP caching may mask connection state

Fundamentally, these concerns lie directly with SOAP over HTTP, rather than the application of SOAP over HTTP to NETCONF. As BCP 56 indicates, it is debatable whether HTTP is an appropriate protocol for SOAP at all, and it is likely that BEEP would be a superior protocol for most SOAP applications. Unfortunately, SOAP over HTTP is in common use and must be supported if the practical benefits of SOAP are to be realized. Note that the verbose nature of SOAP actually makes it more readily processed by firewalls, albeit firewalls designed to process SOAP messages.

It is very important that HTTP caches are not inserted between NETCONF managers and agents as NETCONF session state is tied to the state of the underlying transport connection. Three defensive actions can be taken:

- Prohibit caching through the use of HTTP headers Cache-Control and Pragma: no-cache
- Ensure that HTTP proxies are not deployed within the management network
- Use HTTPS

It is also possible to respond to the concern on the re-use of port 80. A NETCONF SOAP service can be offered on any desired port, and it is recommended that a new standard port for SOAP over HTTP, or a new standard port for NETCONF over SOAP (over HTTP) be defined.

2.5 Important HTTP 1.1 Features

HTTP 1.1 [8] includes two important features that provide for relatively efficient transport of SOAP messages. These features are "persistent connections" and "chunked transfer-coding".

Persistent connections allow a single TCP connection to be used across multiple HTTP requests. This permits multiple SOAP request/

response message pairs to be exchanged without the overhead of creating a new TCP connection for each request. Given that a single stream is used for both requests and responses, it is clear that some form of framing is necessary. For messages whose length is known in advance, this is handled by the HTTP header "Content-length". For messages of dynamic length, "Chunking" is required.

HTTP "Chunking" or "chunked transfer-coding" allows the sender to send an indefinite amount of binary data. This is accomplished by informing the receiver of the size of each "chunk" (substring of the data) before the chunk is transmitted. The last chunk is indicated by a chunk of zero length. Chunking can be effectively used to transfer a large XML document where the document is generated on-line from a non-XML form in memory.

In terms of application to SOAP message exchanges, persistent connections are clearly important for performance reasons, and are particularly important when it is the persistence of authenticated connections that is at stake. When one considers that messages of dynamic length are the rule rather than the exception for SOAP messages, it is also clear that Chunking is very useful. In some cases it is possible to buffer a SOAP response and determine its length before sending, but the storage requirements for this are prohibitive for many devices. Together, these two features provide a good foundation for device management using SOAP over HTTP.

2.6 SOAP Over BEEP

Although not widely adopted by the Web Services community, BEEP is an excellent substrate for SOAP [16]. In particular, it provides for request/response message exchanges initiated by either BEEP peer and allows the number of response messages to be arbitrary (including zero). The BEEP profile for SOAP simply makes use of a single BEEP channel for exchanging SOAP messages and benefits from BEEP's inherent strengths for message exchange over a single transport connection.

2.7 SOAP Implementation Considerations

It is not the goal of this document to cover the SOAP [3] specification in detail. Instead, we provide a few comments that may be of interest to an implementor of NETCONF over SOAP.

2.7.1 SOAP Feature Exploitation

NETCONF over SOAP does not make extensive use of SOAP features. For instance, NETCONF operations are not broken into SOAP message parts, and the SOAP header is not used to convey <rpc> metadata. This is a

deliberate design decision as it allows the implementor to easily provide NETCONF over multiple substrates while handling the messages over those different substrates in a common way.

2.7.2 SOAP Headers

Implementors of NETCONF over SOAP should be aware of the following characteristic of SOAP headers: a SOAP header may have the attribute "mustUnderstand" and, if so, the recipient must either process the header block or not process the SOAP message at all, and instead generate a fault. A "mustUnderstand" header must not be silently discarded.

In general, however, SOAP headers are intended for application-specific uses. The NETCONF SOAP binding does not make use of SOAP headers.

2.7.3 SOAP Faults

A SOAP Fault is returned in the event of a NETCONF <rpc-error>. It is constructed essentially as a wrapper for the <rpc-error>, but allow SOAP processors to propagate the <rpc-error> to application code using a language-appropriate exception mechanism.

A SOAP Fault is constructed from an <rpc-error> as follows: the SOAP Fault faultcode is "Client" in the SOAP envelope namespace, the SOAP Fault faultstring is the contents of the NETCONF <rpc-error> "tag", and the SOAP Fault detail is the original <rpc-error> structure.

For instance, given the following <rpc-error>,

```
    <rpc-error message-id="102"
          xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <tag>EXAMPLE_MTU_RANGE</tag>
      <error-code>128</error-code>
      <severity>error</severity>
      <statement>mtu 21050;</statement>
      <message>MTU 21050 on Ethernet/1 is
               outside range 256..9192</message>
    </rpc-error>
```

the associated SOAP Fault message is

```
<soapenv:Envelope
      xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <soapenv:Fault>
      <faultcode>soapenv:Client</faultcode>
      <faultstring>EXAMPLE_MTU_RANGE</faultstring>
      <detail>
        <rpc-error message-id="102"
              xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
          <tag>EXAMPLE_MTU_RANGE</tag>
          <error-code>128</error-code>
          <severity>error</severity>
          <statement>mtu 21050;</statement>
          <message>MTU 21050 on Ethernet/1 is
                   outside range 256..9192</message>
        </rpc-error>
      </detail>
    </soapenv:Fault>
  </soapenv:Body>
</soapenv:Envelope>
```

3. A SOAP Service for NETCONF

3.1 Fundamental Use Case

The fundamental use case for NETCONF over SOAP is that of a management console ("manager" role) managing one or more devices running NETCONF agents ("agent" role). The manager initiates an HTTP or BEEP connection to an agent and drives the NETCONF session via a sequence of SOAP messages. When the manager closes the connection, the NETCONF session is also closed.

3.2 NETCONF Session Establishment

A NETCONF over SOAP session is established by the initial message exchange on the underlying substrate. For HTTP, a NETCONF session is established once a SOAP message is POSTed to the NETCONF web application URI. For BEEP, a NETCONF session is established once the BEEP profile for SOAP handshake establishes the SOAP channel.

3.3 NETCONF Capabilities Exchange

Capabilities exchange, if defined through a NETCONF RPC operation, can easily be accommodated in the SOAP binding.

3.4 NETCONF Session Usage

NETCONF sessions are persistent for both performance and semantic reasons. NETCONF session state contains the following:

1. Authentication Information
2. Capability Information
3. Locks
4. Pending Operations
5. Operation Sequence Numbers

Authentication must be maintained throughout a session due to the fact that it is expensive to establish. Capability Information is maintained so that appropriate operations can be applied during a session. Locks are released upon termination of a session as this makes the protocol more robust. Pending operations come and go from existence during the normal course of RPC operations. Operation sequence numbers provide the small but necessary state information to refer to operations during the session.

In the case of SOAP over HTTP, a NETCONF session is supported by an HTTP connection with an authenticated user. For SOAP over BEEP, a NETCONF session is supported by a BEEP channel operating according to the BEEP profile for SOAP [16].

3.5 NETCONF Session Teardown

To allow automated cleanup, NETCONF over SOAP session teardown takes place when the underlying connection (in the case of HTTP) or channel (in the case of BEEP) is closed. Note that the root cause of such teardown may be the closure of the TCP connection under either HTTP or BEEP as the case may be. NETCONF managers and agents must be capable of programatically closing the transport connections associated with NETCONF sessions; thus, the HTTP or BEEP substrate implementation must expose this appropriately.

3.6 A NETCONF Over SOAP example

Since the proposed WSDL (in Appendix A.1) uses document/literal encoding, the use of a SOAP header and body has little impact on the representation of a NETCONF operation. This example shows HTTP/1.0 for simplicity. Examples for HTTP/1.1 and BEEP would be similar.

```
POST /netconf HTTP/1.0
Content-Type: text/xml; charset=utf-8
Accept: application/soap+xml, text/*
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 470

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <rpc id="101"
         xmlns="http://iana.org/ietf/netconf/base_1.0.xsd">
      <get-config>
        <source>
          <running/>
        </source>
        <config xmlns="http://example.com/schema/1.2/config">
          <users/>
        </config>
        <format>xml</format>
      </get-config>
    </rpc>
  </soapenv:Body>
</soapenv:Envelope>
```

The HTTP/1.0 response is also straightforward:

```
HTTP/1.0 200 OK
Content-Type: text/xml; charset=utf-8

<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <rpc-reply id="101"
               xmlns="http://iana.org/ietf/netconf/base_1.0.xsd">
      <config xmlns="http://example.com/schema/1.2/config">
        <users>
          <user>
            <name>root</name>
            <type>superuser</type>
          </user>
          <user>
            <name>fred</name>
            <type>admin</type>
          </user>
          <user>
            <name>barney</name>
            <type>admin</type>
          </user>
        </users>
      </config>
    </rpc-reply>
  </soapenv:Body>
</soapenv:Envelope>
```

4. Security Considerations

NETCONF is used to access and modify configuration information, so the ability to access this protocol should be limited to users and systems that are authorized to view or modify the agent's configuration data.

Because configuration information is sent in both directions, it is not sufficient for just the client or user to be authenticated with the server. The identity of the server should also be authenticated with the client.

Configuration data may include sensitive information, such as user names or security keys. So, NETCONF should only be used over communications channels that provide strong encryption for data privacy.

If the NETCONF server provides remote access through insecure protocols, such as HTTP, care should be taken to prevent execution of the NETCONF program when strong user authentication or data privacy is not available.

4.1 Integrity, Privacy, and Authentication

The NETCONF SOAP binding relies on an underlying secure transport for integrity and privacy. Such transports are expected to include TLS [12] and IPSec. There are a number of options for authentication (some of which are deployment-specific):

- within the transport (such as with TLS client certificates)
- within HTTP (such as Digest Access Authentication [10])
- within SOAP (such as a digital signature in the header [18])

HTTP, BEEP, and SOAP level authentication can be integrated with RADIUS [13] to support remote authentication databases.

4.2 Vulnerabilities

The above protocols may have various vulnerabilities, and these may be inherited by NETCONF over SOAP.

NETCONF itself may have vulnerabilities due to the fact that an authorization model is not currently specified.

It is important that device capabilities and authorization remain constant for the duration of any outstanding NETCONF session. In the case of NETCONF, it is important to consider that device management may be taking place over multiple substrates (in addition to SOAP)

and it is important that the different substrates have a common authentication model.

4.3 Environmental Specifics

Some deployments of NETCONF over SOAP may choose to use transports without encryption. This presents vulnerabilities but may be selected for deployments involving closed networks or debugging scenarios.

A device managed by NETCONF may interact (over protocols other than NETCONF) with devices managed by other protocols, all of differing security. Each point of entry brings with it a potential vulnerability.

5. References

5.1 Normative References

[1] Enns, R., "NETCONF Configuration Protocol", draft-ietf-netconf-prot-03 (work in progress), June 2004, <http://www.ietf.org/internet-drafts/draft-ietf-netconf-prot-03.txt>.

[2] 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, <http://www.w3.org/TR/2000/REC-xml-20001006>.

[3] Box, D., Ehnebuske, D., Kakivaya, G., Layman, A., Mendelsohn, N., Nielsen, H., Thatte, S. and D. Winer, "Simple Object Access Protocol (SOAP) 1.1", W3C Note NOTE-SOAP-20000508, May 2000, <http://www.w3.org/TR/2000/NOTE-SOAP-20000508>.

[4] Christensen, E., Curbera, F., Meredith, G. and S. Weerawarana, "Web Services Description Language (WSDL) 1.1", W3C Note NOTE-wsdl-20010315, March 2001, <http://www.w3.org/TR/2001/NOTE-wsdl-20010315>.

[5] Thompson, H., Beech, D., Maloney, M. and N. Mendelsohn, "XML Schema Part 1: Structures", W3C Recommendation REC-xmlschema-1-20010502, May 2001, <http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/>.

[6] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996, <http://www.ietf.org/rfc/rfc2045.txt>.

[7] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996, <http://www.ietf.org/rfc/rfc2046.txt>.

[8] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999, <http://www.ietf.org/rfc/rfc2616.txt>.

[9] Moore, K., "On the use of HTTP as a Substrate", RFC 3205, February 2002, <http://www.ietf.org/rfc/rfc3205.txt>.

[10] Franks, J., Hallam-Baker, P., Hostetler, J., Leach, P., Luotonen, A., Sink, E. and L. Stewart, "An Extension to HTTP: Digest Access Authentication", RFC 2069, January 1997,

<http://www.ietf.org/rfc/rfc2069.txt>.

[11] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997, <http://www.ietf.org/rfc/rfc2119.txt>.

[12] Dierks, T., Allen, C., Treese, W., Karlton, P., Freier, A. and P. Kocher, "The TLS Protocol Version 1.0", RFC 2246, January 1999, <http://www.ietf.org/rfc/rfc2246.txt>.

[13] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000, <http://www.ietf.org/rfc/rfc2865.txt>.

[14] Rose, M. and D. New, "Reliable Delivery for syslog", RFC 3195, November 2001, <http://www.ietf.org/rfc/rfc3195.txt>.

[15] Rose, M., "The Blocks Extensible Exchange Protocol Core", RFC 3080, March 2001, <http://www.ietf.org/rfc/rfc3080.txt>.

[16] O'Tuathail, E. and M. Rose, "Using the Simple Object Access Protocol (SOAP) in Blocks Extensible Exchange Protocol (BEEP)", RFC 3288, June 2002, <http://www.ietf.org/rfc/rfc3288.txt>.

5.2 Informative References

[17] Barton, J., Nielsen, H. and S. Thatte, "SOAP Messages with Attachments", W3C Note NOTE-SOAP-attachments-20001211, Dec 2000, <http://www.w3.org/TR/2000/NOTE-SOAP-attachments-20001211>.

[18] Brown, A., Fox, B., Hada, S., LaMacchia, B. and H. Maruyama, "SOAP Security Extensions: Digital Signature", W3C Note NOTE-SOAP-dsig-20010206, Feb 2001, <http://www.w3.org/TR/2001/NOTE-SOAP-dsig-20010206/>.

Author's Address

Ted Goddard
ICEsoft Technologies Inc.
Suite 300, 1717 10th St. NW
Calgary, AB T2M 4S2
Canada

Phone: (403) 663-3322
EMail: ted.goddard@icesoft.com
URI: http://www.icesoft.com

Appendix A. WSDL Definitions

A.1 NETCONF SOAP Binding

The following WSDL document assumes a hypothetical location for the NETCONF schema.

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  xmlns:SOAP="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:tns="urn:ietf:params:xml:ns:netconf:soap:1.0"
  xmlns:xb="urn:ietf:params:xml:ns:netconf:base:1.0"
  targetNamespace="urn:ietf:params:xml:ns:netconf:soap:1.0"
  name="soap_1.0.wsdl">

  <import namespace="urn:ietf:params:xml:ns:netconf:base:1.0"
          location="http://iana.org/ietf/netconf/base_1.0.xsd"/>

  <message name="rpcRequest">
    <part name="in" element="xb:rpc"/>
  </message>
  <message name="rpcResponse">
    <part name="out" element="xb:rpc-reply"/>
  </message>

  <portType name="rpcPortType">
    <operation name="rpc">
      <input message="tns:rpcRequest"/>
      <output message="tns:rpcResponse"/>
    </operation>
  </portType>

  <binding name="rpcBinding" type="tns:rpcPortType">
    <SOAP:binding style="document"
         transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="rpc">
      <SOAP:operation/>
      <input>
        <SOAP:body use="literal"
             namespace="urn:ietf:params:xml:ns:netconf:base:1.0"/>
      </input>
      <output>
        <SOAP:body use="literal"
             namespace="urn:ietf:params:xml:ns:netconf:base:1.0"/>
      </output>
    </operation>
  </binding>
```

```
</definitions>
```

A.2 Sample Service Definition

The following WSDL document assumes a hypothetical location for the NETCONF over SOAP WSDL definitions. A typical deployment of a device manageable via NETCONF over SOAP would provide a service definition similar to the following to identify the address of the device.

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions
  xmlns="http://schemas.xmlsoap.org/wsdl/"
  xmlns:SOAP="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:xs="urn:ietf:params:xml:ns:netconf:soap:1.0"
  targetNamespace="urn:myNetconfService"
  name="myNetconfService.wsdl">

  <import namespace="urn:ietf:params:xml:ns:netconf:soap:1.0"
          location="http://iana.org/ietf/netconf/soap_1.0.wsdl"/>

  <service name="netconf">
    <port name="rpcPort" binding="xs:rpcBinding">
      <SOAP:address location="http://localhost:8080/netconf"/>
    </port>
  </service>

</definitions>
```

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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