NETMOD WG
Internet-Draft
Intended status: Informational
Expires: January 20, 2015

Clyde Wildes
Cisco Systems
Agrahara Kiran Koushik
Brocade Communication Systems
July 20, 2014

SYSLOG YANG model
draft-wildes-netmod-syslog-model-02

Abstract

This document describes a data model for Syslog protocol which is used to convey event notification messages.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 20, 2015.

Table of Contents

1. Introduction

Operating systems, processes and applications generate messages indicating their own status or the occurance of events. These messages are useful for managing and/or debugging the network and its services. The BSD Syslog protocol is a widely adopted protocol that is used for transmission and processing of the messages.

Since each process, application and operating system was written somewhat independently, there is little uniformity to the content of Syslog messages. For this reason, no assumption is made upon the formatting or contents of the messages. The protocol is simply designed to transport these event messages. No acknowledgement of the receipt is made.

Essentially, a Syslog process receives messages (from the kernel, processes, applications or other Syslog processes) and processes those. The processing involves logging to a local file, displaying on console, user terminal, and/or relaying to syslog processes on other machines. The processing is determined by the "facility" that originated the message and the "severity" assigned to the message by the facility.

We are using definitions of Syslog protocol from [RFC3164] in this draft.

1.1. Definitions and Acronyms

IP: Internet Protocol

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

UDP: User Datagram Protocol

VRF: Virtual Routing and Forwarding

2. Problem Statement

This document defines a YANG [RFC6020] configuration data model that may be used to monitor and control one or more syslog processes running on a system. YANG models can be used with network management agents such as NETCONF [RFC6241] to install, manipulate, and delete the configuration of network devices.

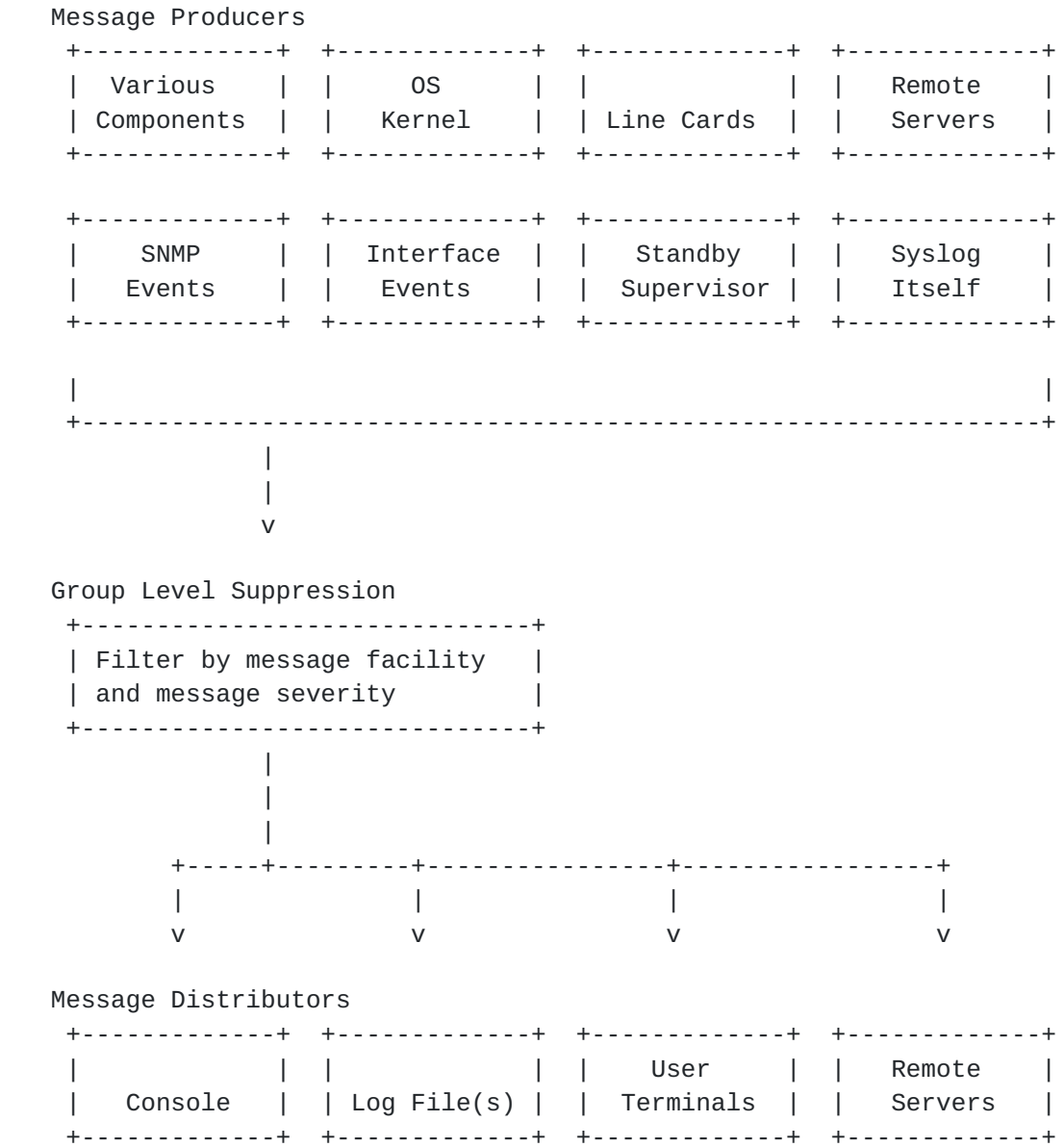
This module makes use of the YANG "feature" construct which allows implementations to support only those Syslog features that lie within their capabilities.

3. Design of the SYSLOG Model

The syslog model was designed by comparing various syslog features implemented by various vendors' in different implementations.

This draft addresses the common leafs between all vendors and creates a common model, which can be augmented with proprietary features, if necessary. The base model is designed to be very simple for maximum flexibility.

Syslog consists of message producers, a group level suppression filter, and message distributors. The following digram shows syslog messages flowing from a message producer, through the group level suppression filter, and if passed by the group filter to message distributors where further suppression filtering can take place.



The leaves in the base syslog model correspond to the group level suppression filter and each message distributor:

- console
- log file(s)
- user terminals
- remote server(s).

Optional features are used to specified fields that are not present in all vendor configurations.

3.1. SYSLOG Module

```
module: ietf-syslog
   +--rw syslog
      +--rw global-logging
      |  +--rw logging-severities [facility]
      |     +--rw facility    identityref
      |     +--rw severity?   syslogtypes:Severity
      +--rw console-logging
      |  +--rw (logging-level-scope)?
      |     +--:(all-facilities)
      |     |  +--rw logging-severity?     syslogtypes:Severity
      |     +--:(facility)
      |        +--rw logging-severities [facility]
      |           +--rw facility    identityref
      |           +--rw severity?   syslogtypes:Severity
      +--rw file-logging
      |  +--rw file-name             string
      |  +--rw file-size?            uint32
      |  +--rw (logging-scope)?
      |     +--:(all-facilities)
      |     |  +--rw logging-severity?     syslogtypes:Severity
      |     +--:(facility)
      |        +--rw logging-severities [facility]
      |           +--rw facility    identityref
      |           +--rw severity?   syslogtypes:Severity
      +--rw remote-logging
      |  +--rw remote-logging-destination [destination]
      |     +--rw destination           string
      |     +--rw logging-severities [facility]
      |     |  +--rw facility    identityref
      |     |  +--rw severity?   syslogtypes:Severity
      |     +--rw source-interface?     string
      |     +--rw vrf-name?             string
      +--rw terminal-logging
         +--rw (user-scope)?
            +--:(all-users)
            |  +--rw all-users
            |     +--rw (logging-scope)?
            |        +--:(all-facilities)
            |        |  +--rw logging-severity?     syslogtypes:Severity
            |        +--:(facility)
            |           +--rw logging-severities [facility]
            |              +--rw facility    identityref
            |              +--rw severity?   syslogtypes:Severity
            +--:(per-user)
               +--rw user-name [uname]
                  +--rw uname                 string
                  +--rw (logging-scope)?
```

```
                     +--:(all-facilities)
                     |  +--rw logging-severity?     syslogtypes:Severity
                     +--:(facility)
                        +--rw logging-severities [facility]
                           +--rw facility    identityref
                           +--rw severity?   syslogtypes:Severity
```

4. SYSLOG YANG Models

4.1. SYSLOG-TYPES module

```
module ietf-syslog-types {
  namespace "urn:ietf:params:xml:ns:yang:ietf-syslog-types";
  prefix syslogtypes;

  organization "IETF NETMOD (NETCONF Data Modeling Language) Working
                Group";
  contact
    "WG Web:   <http://tools.ietf.org/wg/netmod/>
     WG List:  <mailto:netmod@ietf.org>

     WG Chair: Juergen Schoenwaelder
               <mailto:j.schoenwaelder@jacobs-university.de>

     WG Chair: Tom Nadeau
               <mailto:tnadeau@brocade.com>

     Editor:   Clyde Wildes
               <mailto:cwildes@cisco.com>

     Editor:   Agrahara Kiran Koushik
               <mailto:kkoushik@brocade.com>";
  description
    "This module contains a collection of YANG type definitions for
     SYSLOG.";

  revision 2014-06-03 {
    description
      "Version 1.0";
    reference
      "This model references RFC 5424 - The Syslog Protocol.";


  }

  typedef Severity {
    type enumeration {
      enum "emergency" {
        value 0;
        description
          "Emergency Level Msg";
      }
      enum "alert" {
        value 1;
        description
          "Alert Level Msg";
```

```
      }
```

```
      enum "critical" {
        value 2;
        description
          "Critical Level Msg";
      }
      enum "error" {
        value 3;
        description
          "Error Level Msg";
      }
      enum "warning" {
        value 4;
        description
          "Warning Level Msg";
      }
      enum "notice" {
        value 5;
        description
          "Notification Level Msg";
      }
      enum "info" {
        value 6;
        description
          "Informational Level Msg";
      }
      enum "debug" {
        value 7;
        description
          "Debugging Level Msg";
      }
    }
    description
      "The definitions for Syslog message severity.";
  }

  identity syslog-facility {
    description
      "The base identity to represent syslog facilities";
  }

  identity kern {
    base syslog-facility;
    description
      "The facility for kernel messages as defined in RFC 5424.";
  }
```

```
  identity user {
    base syslog-facility;
    description
      "The facility for user-level messages as defined in RFC 5424.";
   }

   identity mail {
     base syslog-facility;
    description
      "The facility for the mail system as defined in RFC 5424.";
   }

   identity daemon {
     base syslog-facility;
   }
    description
      "The facility for the system daemons as defined in RFC 5424.";
   }

   identity auth {
     base syslog-facility;
    description
      "The facility for security/authorization messages as defined
       in RFC 5424.";
   }

   identity syslog {
     base syslog-facility;
    description
      "The facility for messages generated internally by syslogd
       facility as defined in RFC 5424.";
   }

   identity lpr {
     base syslog-facility;
    description
      "The facility for the line printer subsystem as defined in
       RFC 5424.";
   }

  identity news {
    base syslog-facility;
    description
      "The facility for the network news subsystem as defined in
       RFC 5424.";
   }

   identity uucp {
     base syslog-facility;
```

```
     description
       "The facility for the UUCP subsystem as defined in RFC 5424.";
     }

     identity cron {
       base syslog-facility;
      description
       "The facility for the clock daemon as defined in RFC 5424.";
     }

     identity authpriv {
       base syslog-facility;
      description
       "The facility for privileged security/authorization messages
        as defined in RFC 5424.";
     }

     identity ftp {
       base syslog-facility;
      description
       "The facility for the FTP daemon as defined in RFC 5424.";
     }

     identity ntp {
       base syslog-facility;
      description
       "The facility for the NTP subsystem as defined in RFC 5424.";
    }

    identity audit {
      base syslog-facility;
      description
       "The facility for log audit messages as defined in RFC 5424.";
      }
```

```
  identity console {
    base syslog-facility;
    description
      "The facility for log alert messages as defined in RFC 5424.";
   }

   identity cron2 {
     base syslog-facility;
    description
      "The facility for the second clock daemon as defined in
       RFC 5424.";
   }

   identity local0 {
     base syslog-facility;
    description
      "The facility for local use 0 messages as defined in
       RFC 5424.";
   }

   identity local1 {
     base syslog-facility;
    description
      "The facility for local use 1 messages as defined in
       RFC 5424.";
   }

   identity local2 {
     base syslog-facility;
    description
      "The facility for local use 2 messages as defined in
       RFC 5424.";
  }

  identity local3 {
    base syslog-facility;
    description
      "The facility for local use 3 messages as defined in
       RFC 5424.";
   }

   identity local4 {
     base syslog-facility;
    description
      "The facility for local use 4 messages as defined in
       RFC 5424.";
   }

   identity local5 {
```

```
     base syslog-facility;
    description
      "The facility for local use 5 messages as defined in
       RFC 5424.";
   }

   identity local6 {
     base syslog-facility;
    description
      "The facility for local use 6 messages as defined in
       RFC 5424.";
   }

   identity local7 {
     base syslog-facility;
    description
      "The facility for local use 7 messages as defined in
       RFC 5424.";
  }
}
```

4.2. SYSLOG module

```
module ietf-syslog {
  namespace "urn:ietf:params:xml:ns:yang:ietf-syslog";
  prefix syslog;

  import ietf-syslog-types {
    prefix syslogtypes;
  }

  organization "IETF NETMOD (NETCONF Data Modeling Language)
                Working Group";
  contact
    "WG Web:   <http://tools.ietf.org/wg/netmod/>
     WG List:  <mailto:netmod@ietf.org>

     WG Chair: Juergen Schoenwaelder
               <mailto:j.schoenwaelder@jacobs-university.de>

     WG Chair: Tom Nadeau
               <mailto:tnadeau@brocade.com>

     Editor:   Clyde Wildes
               <mailto:cwildes@cisco.com>

     Editor:   Agrahara Kiran Koushik
               <mailto:kkoushik@brocade.com>";
  description
    "This module contains a collection of YANG definitions
     for Syslog configuration.";

  revision 2014-06-10 {
    description
      "Initial revision.";
  reference
    "This model references RFC 5424 - The Syslog Protocol.";

  }

  feature global-logging {
    description
      "This feature represents the ability to adjust
       log message severity per logging facility on the
       global level.";
  }

  feature console-facility-logging-config {
    description
      "This feature represents the ability to adjust
       log message severity per logging facility for console
```

```
       logging.";
  }

  feature file-logging {
    description
      "This feature represents the ability to log
       messages into a file.";
  }
```

```
  feature file-facility-logging-config {
    description
      "This feature represents the ability to adjust
       log message severity per logging facility for file logging.";
  }

  feature terminal-facility-logging-config {
    description
      "This feature represents the ability to adjust
       log message severity per logging facility for terminal
       logging.";
  }

  feature terminal-facility-user-logging-config {
    description
      "This feature represents the ability to adjust
       log message settings for individual terminal users.";
  }

  feature use-vrf {
    description
      "This feature allows logging of messages to a particular VRF.";
  }
  grouping facility-logging {
    description
      "This grouping defines a list of facility-severity pairs.
       Messages from a facility in the list that have the
       corresponding specified severity level or higher will be
       logged.";
    list logging-severities {
      key "facility";
      description
        "This list describes a collection of Syslog facilities.";
      leaf facility {
        type identityref {
          base syslogtypes:syslog-facility;
        }
        description
          "The leaf uniqueuely identifies a Syslog facility.";
      }
      leaf severity {
        type syslogtypes:Severity;
        description
          "This leaf specifies the severity of Syslog messages
           for this facility.";
      }
    }
  }
```

```
  container syslog {
    config true;
    description
      "This container describes the configuration parameters for
       Syslog.";
    container global-logging {
      if-feature global-logging;
      description
        "This container describes the configuration parameters for
         global logging.";

      uses facility-logging;
    }
    container console-logging {
      description
        "This container describes the configuration parameters for
         console logging.";
      choice logging-level-scope {
        description
          "This choice describes the option to specify all
           facilities or a specific facility.";
        case all-facilities {
          description
            "This case specifies all facilities.";
          leaf logging-severity {
            type syslogtypes:Severity;
            description
              "This leaf specifies the severity of Syslog messages
               for all facilities.";
          }
        }
        case facility {
          if-feature console-facility-logging-config;
          description
            "This case specifies a specific facility.";
          uses facility-logging;
        }
      }
    }
```

```
    container file-logging {
      if-feature file-logging;
      description
        "This container describes the configuration parameters for
         file logging configuration.";
      leaf file-name {
        type string;
        mandatory true;
        description
          "This leaf specifies the name of the log file.";
      }

      leaf file-size {
        type uint32;
        description
          "This leaf specifies the log file size.";
      }
      choice logging-scope {
        description
          "This choice describes the option to specify all
           facilities or a specific facility.";
        case all-facilities {
          description
            "This case specifies all facilities.";
          leaf logging-severity {
            type syslogtypes:Severity;
            description
              "This leaf specifies the severity of Syslog messages
               for all facilities.";
          }
        }
        case facility {
          if-feature file-facility-logging-config;
          description
            "This case specifies a specific facility.";
          uses facility-logging;
        }
      }
    }
    container remote-logging {
      description
        "This container describes the configuration parameters for
         the remote logging configuration.";
      list remote-logging-destination {
        key "destination";
        description
          "This list describes a collection of remote logging
           destinations.";
        leaf destination {
```

```
          type string;
          description
            "The leaf uniquely specifies the address of the remote host. One
             of the following must be specified: an ipv4 address, an ipv6
             address, or a host name.";
        }
```

```
        uses facility-logging;
        leaf source-interface {
          type string;
          description
            "This leaf sets the source interface for the remote
             Syslog server. Either the interface name or the
             interface IP address can be specified.";
        }
        leaf vrf-name {
          if-feature use-vrf;
          type string;
          description
            "This leaf specifies the name of the virtual routing
             facility (VRF).";
        }
      }
    }
    container terminal-logging {
      description
        "This container describes the configuration parameters for
         the terminal logging configuration.";
      choice user-scope {
        description
          "This choice describes the option to specify all users
           or a specific user. The all users case implies that
           messages will be sent to all terminals";
        case all-users {
          description
            "This case specifies all users.";
          container all-users {
            description
              "This continer describes the configuration parameters
               for all users.";
            choice logging-scope {
              description
                "This choice describes the option to specify all
                 facilities or a specific facility.";
              case all-facilities {
                description
                  "This case specifies all facilities.";
                leaf logging-severity {
                  type syslogtypes:Severity;
                  description
                    "This leaf specifies the severity of Syslog
                     messages for all facilities.";
                }
              }
```

```
              case facility {
                if-feature terminal-facility-logging-config;
                description
                  "This case specifies a specific facility.";
                uses facility-logging;
              }
            }
          }
        }
        case per-user {
          if-feature terminal-facility-user-logging-config;
          description
            "This case specifies a specific user.";
          list user-name {
            key "uname";
            description
              "This list describes a collection of user names.";
            leaf uname {
              type string;
              description
                "This leaf uniquely describes a user name.";
            }
            choice logging-scope {
              description
                "This choice describes the option to specify all
                 facilities or a specific facility.";
              case all-facilities {
                description
                  "This case specifies all facilities.";
                leaf logging-severity {
                  type syslogtypes:Severity;
                  description
                    "This leaf specifies the severity of Syslog
                     messages for all facilities.";
                }
              }
              case facility {
                if-feature terminal-facility-logging-config;
                description
                  "This case specifies a specific facility.";
                uses facility-logging;
              }
            }
          }
        }
      }
    }
  }
}
```

4.3. A SYSLOG Example

```
   Requirement:
   Enable global logging of two facilities:
     kern - severity critical(1)
     auth - severity error(3)

   Enable console logging of syslogs of severity
   critical(1)

   Here is the example syslog configuration xml:

   <rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <edit-config>
       <target>
         <running/>
       </target>
       <config>
         <syslog xmlns="urn:cisco:params:xml:ns:yang:syslog">
           <global-logging>
             <facility>syslogtypes:kern</facility>
             <severity>syslogtypes:critical</severity>
             <facility>syslogtypes:auth</facility>
             <severity>syslogtypes:error</severity>
           </global-logging>
           <console-logging>
             <logging-severity>syslogtypes:critical</logging-severity>
           </console-logging>
         </syslog>
       </config>
     </edit-config>
   </rpc>

   <?xml version="1.0" encoding="UTF-8"?>
   <rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <ok/>
   </rpc-reply>
```

5. Implementation Status

[Note to RFC Editor: Please remove this section before publication.]

This section records the status of known implementations of the Syslog YANG model at the time of posting of this Internet-Draft.

Cisco Systems, Inc. has implemented the proposed IETF Syslog model for the Nexus 7000 NXOS OS as a prototype, together with an augmentation model for operating system specific Syslog configuration features.

Five leaves were implemented in the base IETF model and three leaves were implemented in the NXOS specific augmentation model as follows:

Leaf XPATH	Sample NXOS CLI Command(s)
syslog:global-logging	logging level cron 2
syslog:console-logging	logging console 1
syslog:file-logging	logging logfile mylog.log 2 4096
syslog:terminal-logging	logging monitor 2
syslog:remote-logging	*logging server server.cisco.com 2 facility user use-vrf management *logging source-interface loopback 0
cisco-syslog:logging-timestamp-config	logging timestamp milli-seconds
cisco-syslog:origin-id-cfg	logging origin-id string abcdef
cisco-syslog:module-logging	logging module 1

*The "logging server" and "logging source-interface" commands were combined into one base model leaf.

The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs.

6. Security Considerations

The YANG module defined in this memo is designed to be accessed via the NETCONF protocol [RFC6241] [RFC6241]. The lowest NETCONF layer is the secure transport layer and the mandatory-to-implement secure transport is SSH [RFC6242] [RFC6242]. The NETCONF access control model [RFC6536] [RFC6536] provides the means to restrict access for particular NETCONF users to a pre-configured subset of all available NETCONF protocol operations and content.

There are a number of data nodes defined in the YANG module which are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., <edit-config>) to these data nodes without proper protection can have a negative effect on network operations.

TBD: List specific Subtrees and data nodes and their sensitivity/ vulnerability.

7. IANA Considerations

This document registers a URI in the IETF XML registry [RFC3688] [RFC3688]. Following the format in RFC 3688, the following registration is requested to be made:

URI: urn:ietf:params:xml:ns:yang:syslog

Registrant Contact: The IESG.

XML: N/A, the requested URI is an XML namespace.

This document registers a YANG module in the YANG Module Names registry [RFC6020].

name: syslog namespace: urn:ietf:params:xml:ns:yang:syslog prefix: syslog reference: RFC XXXX

8. Acknowledgements

9. Change log [RFC Editor: Please remove]

10. References

[RFC3164] Lonvick, C., "The BSD syslog Protocol", BCP 81, RFC 3164, August 2001.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

[RFC6020] Bjorklund, M., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, June 2011.

[RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, March 2012.

Authors' Addresses

Clyde Wildes
Cisco Systems Inc.

Email: cwildes@cisco.com

Kiran Agrahara Sreenivasa
Brocade Communications Systems

Email: kkoushik@brocade.com