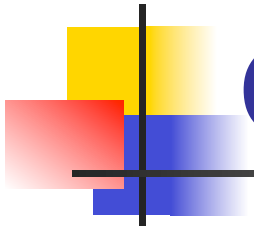
RFC 5539 Update Status

draft-badra-netconf-rfc5539bis-00

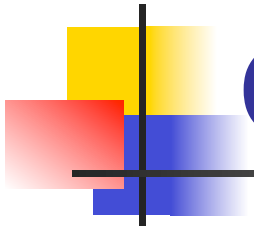
Mohamad Badra

ETF 82, Taipei, Taiwan



Goals of RFC5539bis

- Update RFC 4742 based on:
  - How to generate a NETCONF username and how does the document fulfill the requirements in 6241 for the format of the username?
  - How does the NETCONF transport handle the following two scenarios:
    - both peers advertise :base:1.1 capability
    - none or only one peer advertises :base:1.1 capability.
  - What are the security considerations for using the EOM frame for the <hello> message or using it if one of the peers does not support :base:1.1?
  - How to fix the EoM issues



Client/Server, Agent/Manager

- Suggestion for global terminology changes
  - Drop client/server, manager/agent terminology
  - Instead, refer to the TLS client, the TLS server, the NETCONF client and the NETCONF server throughout

NETCONF username generation: certificate case

- The document defines the ietf-netconf-tls-username YANG module
  - defines objects for remotely configuring the mapping of TLS certificates to NETCONF usernames.

NETCONF username generation: certificate case

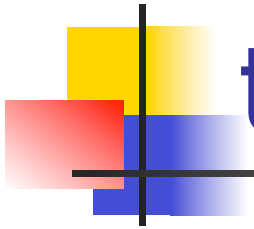
- For each enumerated value listed above, the NETCONF server derives the NETCONF from the presented client certificate

```
leaf map-type {
      type enumeration {
        enum specified                          { value 1;  }
        enum rfc822Name                         { value 2;  }
        enum dnsName                            { value 3;  }
        enum ipAddress                          { value 4;  }
        enum rfc822Name-dnsName-ipAddress       { value 5;  }
        enum rfc822Name-ipAddress-dnsName       { value 6;  }
        enum dnsName-ipAddress-rfc822Name       { value 7;  }
        enum dnsName-rfc822Name-ipAddress       { value 8;  }
        enum ipAddress-dnsName-rfc822Name       { value 9;  }
        enum ipAddress-rfc822Name-dnsName       { value 10; }
      }
```

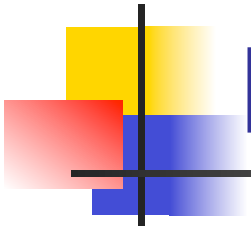
NETCONF username generation: PSK case

- Optional
- PSK-based authentication is described in RFC4279
  - During the TLS Handshake, the client indicates which key to use by including a "PSK identity" in the TLS ClientKeyExchange message
  - PSK identity is used as the NETCONF username.
  - RFC4279 provides more details on how the PSK identity MAY be encoded in UTF-8

The requirements in 6241 for the format of the username



- The username provided by the TLS implementation will be made available to the NETCONF message layer as the NETCONF user name without modification.
- If the username does not comply to the NETCONF requirements on usernames [RFC6241], i.e., the username is not representable in XML, the TLS session MUST be dropped.

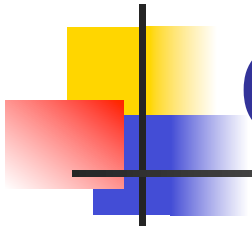


EoM issues

- The <hello> message MUST be followed by the character sequence]]>]]>
  - If the :base:1.1 capability is advertised by both peers, the chunked framing mechanism defined in Section 4.2 of RFC6242 is used for the remainder of the NETCONF session.
  - Otherwise, the old end-of-message-based mechanism (see Section 4.3 of RFC6242) is used.

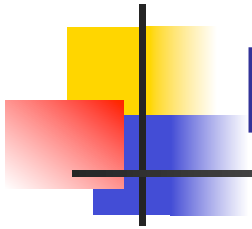
Capability advertisement – security consideration

- When the :base:1.1 capability is not advertised by both peers, an attacker might be able to deliberately insert the delimiter sequence]]>]]> in a NETCONF message to create a DoS attack.
  - If the :base:1.1 capability is not advertised by both peers, applications and NETCONF APIs MUST ensure that the delimiter sequence]]>]]> never appears in NETCONF messages;
  - otherwise, those messages can be dropped, garbled, or misinterpreted.



Contributors

- Juergen Schoenwaelder
- Alan Luchuk



Next Steps

- Make any agreed changes
- WG item?