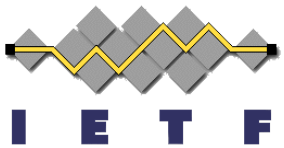
82nd IETF meeting

NETCONF over WebSocket

(http://tools.ietf.org/html/draft-iijima-netconf-websocket-ps-01)

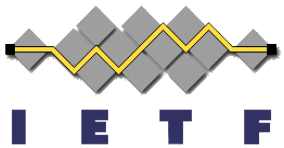
Tomoyuki Iijima,
(Hitachi)
Hiroyasu Kimura, Yoshifumi Atarashi, and Hidemitsu Higuchi
(Alaxala Networks)



Objective of the I-D

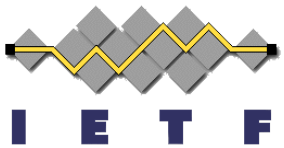
- To propose a way of sending NETCONF over WebSocket protocol.

- But, not to intend to make this proposal as mandatory.♪



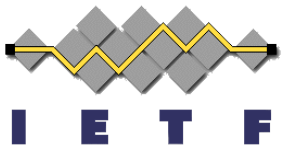
Background

- The number of browser-based management system is increasing with the advancement of web technologies and cloud computing.
  - E.g. AWS (Amazon Web Service), DMTF CIMI (Cloud Infrastructure Management Interface)
- Although NETCONF has high compatibility with HTML/HTTP in that it uses XML as its messaging, NETCONF is rarely used for browser-based management system. Some of the reasons might be…
  - There's no easy way to develop browser-based management system.
  - HTTP lacks bi-directional capability.
- But now, WebSocket, an extension of HTTP, is under development.
  - WebSocket provides JavaScript API to be used for web browser.
  - WebSocket provides bi-directional capability.
- NETCONF should be used for browser-based management systems by supporting WebSocket.



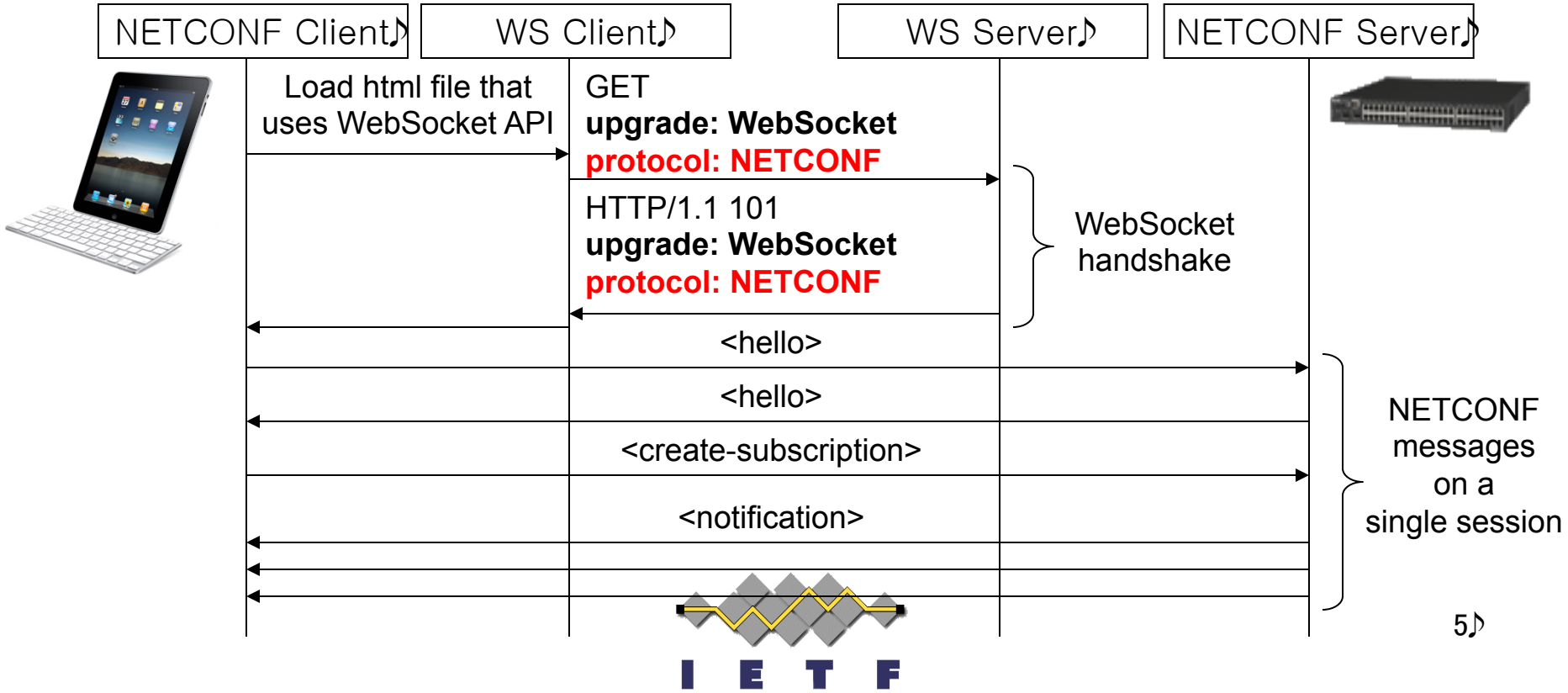
Changes since 80th IETF meeting

- As per comments received at the 80th IETF meeting, we've made following changes.
  - Expanded the description into configuration.
  - Changed the NETCONF diagram from the one from RFC5277 to the one from RFC6241.
  - Expanded the description about security.



NETCONF message(1)

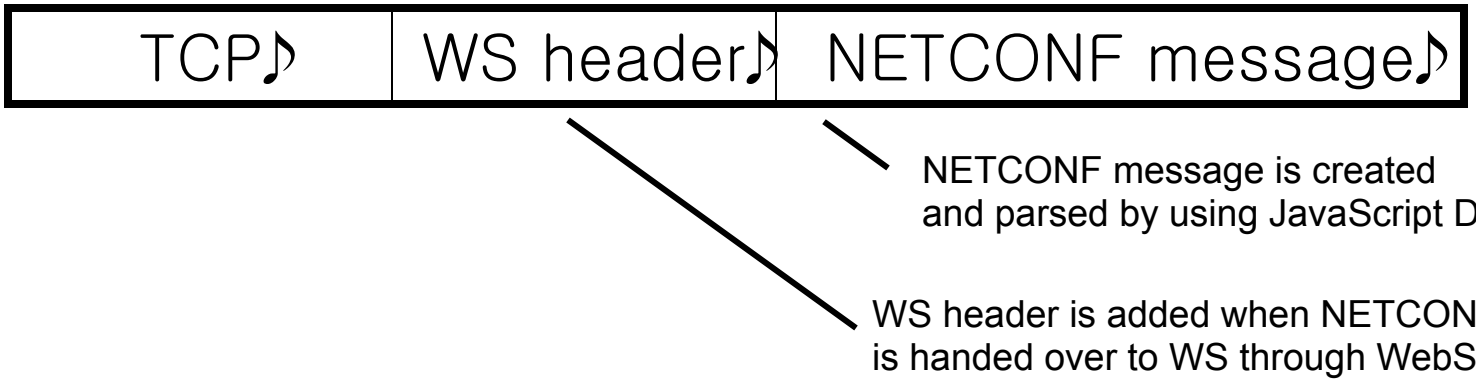
- NETCONF messages are exchanged after WS handshake is complete.
- NETCONF notifications from NETCONF server are sent after NETCONF session is established by <hello> exchange and session ID allocation.



NETCONF message(2)

- NETCONF messages should be sent according to the specification of Data Framing specified by WebSocket protocol.

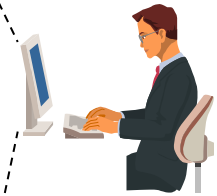
- According to the recent specification (-17, and in RFC queue), NETCONF message should be encapsulated as follows.



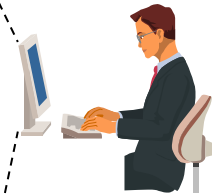
Security

- According to WebSocket I-D, NETCONF's requirements for transport protocol are fulfilled by following security mechanisms.
  - Authentication
    - Fulfilled by mechanisms available to generic HTTP server during WS handshake, which include Cookies, HTTP Authentication, and TLS authentication (see WebSocket I-D, sec. 10.5).
  - Integrity and Confidentiality
    - Fulfilled by TLS (see WebSocket I-D, sec. 10.6).
- Thus, the use of TLS is necessary for NETCONF over WebSocket, as in the case of NETCONF/SOAP/HTTPS.
  - TLS is provided as a set of WebSocket. Easy to use.
- In addition, WebSocket itself has its own security mechanisms.
  - Client is checked by |Origin| header at server during WS handshake.
  - Server is checked by |Sec-WebSocket-Accept| header at client.
  - Payload is masked by masking-key.

Example of NETCONF/WebSocket



Operator A



Operator B

NETCONF configuration message

NETCONF notification message

1. Browser-based NMS is realized, which doesn't require installment

NETCONF client A
(HTTP + WS browser)

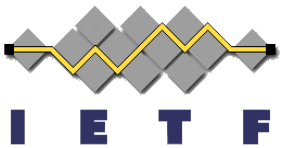
NETCONF client B

2. Real time notification is realized, which is useful for failure notification.

Configuration

Event Notification

NETCONF server
(HTTP + WS server)



Conclusions

- We proposed a way of sending NETCONF over WebSocket protocol.
- We think that for NETCONF to support WebSocket is meaningful for NETCONF's deployment.
- Does WG have interests?
- If YES, should this I-D move forward as an Experimental I-D?