60802 NETCONF Capabilities

Author:

Martin Mittelberger (Siemens AG)

Dec 2022

1 Rationale

During comment resolution of D1.4 the following comment was discussed, and a contribution was expected for the next draft to break down the NETCONF capabilities into atomic requirements and options:

Cl **5**	*SC* **5.5.5.2**	*P* **41**	*L* **1249**	# 304

Weber, Karl — Beckhoff Automation

Comment Type **TR** *Comment Status* **A**

There are 8 capabilities defined in RFC 6241 in clause 8. But these capabilities do not match with the capabilities defined in 60802 for RFC 6241

SuggestedRemedy

Do not use verbal constructs for requirements but select the approprate clause numbers. DO NOT refer to other parts of 60802 but use this clause for state the mandatory elements of other standards clauses.

Response *Response Status* **C**

ACCEPT IN PRINCIPLE. Break the 8 capablities defined in RFC 6241 into atomic requirements and options. A contribution is expected for the next draft.

2 NETCONF Capabilities

RFC 6241 specifies following capabilities:

2.1 Writable-Running Capability (8.2)

This capability indicates that the device supports direct writes to the <running> configuration datastore.

This functionality is not required for 60802 devices.

2.2 Candidate Configuration Capability (8.3)

This capability indicates that the device supports a candidate configuration datastore, which is used to hold configuration data that can be manipulated without impacting the device's current configuration.

A <commit> operation causes the device's running configuration to be set to the value of the candidate configuration.

This functionality is mandatory for 60802 devices.

2.3 Confirmed Commit Capability (8.4)

This capability indicates that the server will support the <cancel-commit> operation and the <confirmed>, <confirm-timeout>, <persist>, and <persist-id> parameters for the <commit> operation.

A confirmed <commit> operation MUST be reverted if a confirming commit is not issued within the timeout period (by default 600 seconds = 10 minutes).

This functionality is not required for 60802 devices.

2.4 Rollback-on-Error Capability (8.5)

This capability indicates that the server will support the "rollback-on-error" value in the <error-option> parameter to the <edit-config> operation.

This functionality is mandatory for 60802 devices.

2.5 Validate Capability (8.6)

Validation consists of checking a complete configuration for syntactical and semantic errors before applying the configuration to the device.

This functionality is mandatory for 60802 devices.

2.6 Distinct Startup Capability (8.7)

The device supports separate running and startup configuration datastores. The startup configuration is loaded by the device when it boots.

This functionality is not required for 60802 devices.

2.7 URL Capability (8.8)

The device has the ability to accept the <url> element in <source> and <target> parameters

This functionality is not required for 60802 devices.

2.8 XPath Capability (8.9)

This capability indicates that the device supports the use of XPath expressions in the <filter> element.

This functionality is not required for 60802 devices.

3 Requirements Statements in 60802

Currently there are following statements in 60802:

3.1 IA-station requirements for management

This contains line 1249(f) where Karl's comment refers to.

1248 **5.5.5.2 Network Configuration Protocol (NETCONF)**

1249 IA-stations for which a claim of conformance to this document is made shall support the Network
1250 Configuration Protocol (NETCONF) with the following capabilities:

1251 a) NETCONF Server functionality according to IETF RFC 6241.

1252 b) NETCONF capabilities according to 6.7.2.

3.2 Management

2230 **6.7.2 NETCONF**

2231 The Network Configuration Protocol (NETCONF) as specified in IETF RFC 6241 is used as
2232 remote management protocol in industrial automation networks together with the following
2233 capabilities:

2234 a) NETCONF over TLS with Mutual X.509 Authentication as described in IETF RFC 7589,
2235 which includes support of DHCP (IETF RFC 2131), IPv4 (IETF RFC 791) and TCP (IETF
2236 RFC 793).

2237 NOTE The SSH transport protocol which is mandatory in IETF RFC 6241, 2.3, is out of scope for IEC/IEEE 60802
2238 conformant IA-stations.

2239 b) Candidate configuration capability as described in IETF RFC 6241, 8.3.

2240 c) Validate capability as described in IETF RFC 6241, 8.6.

2241 d) NETCONF Event Notifications as described in IETF RFC 5277.

2242 e) Dynamic Subscription to YANG Events and Datastores over NETCONF as described in IETF
2243 RFC 8640.

2244 f) NETCONF Extensions to Support the Network Management Datastore Architecture (NMDA)
2245 as described in IETF RFC 8526.

2246 g) NETCONF Configuration Access Control Model (NACM) as described in IETF RFC 8341.

4 Proposed Resolution

Karl's comment requires the mandatory NETCONF capabilities to be specified in the conformance clause instead of referring to other locations in 60802. Thus, the mandatory NETCONF capabilities should be moved from clause 6.7.2 to clause 5.

Additionally, the Rollback-on-error capability (which was not mentioned in D1.4) should be included as a mandatory capability there as well.

Other NETCONF capabilities shouldn't be mentioned in 60802 as before, because it's up to the device to implement them or not.

Subclauses 6.7.2 a and d–g should be moved to clause 5 as well.