

Security considerations for Management Proxies 60802 Draft 3.0

October 2024

Jordon Woods, Self-affiliated



Background

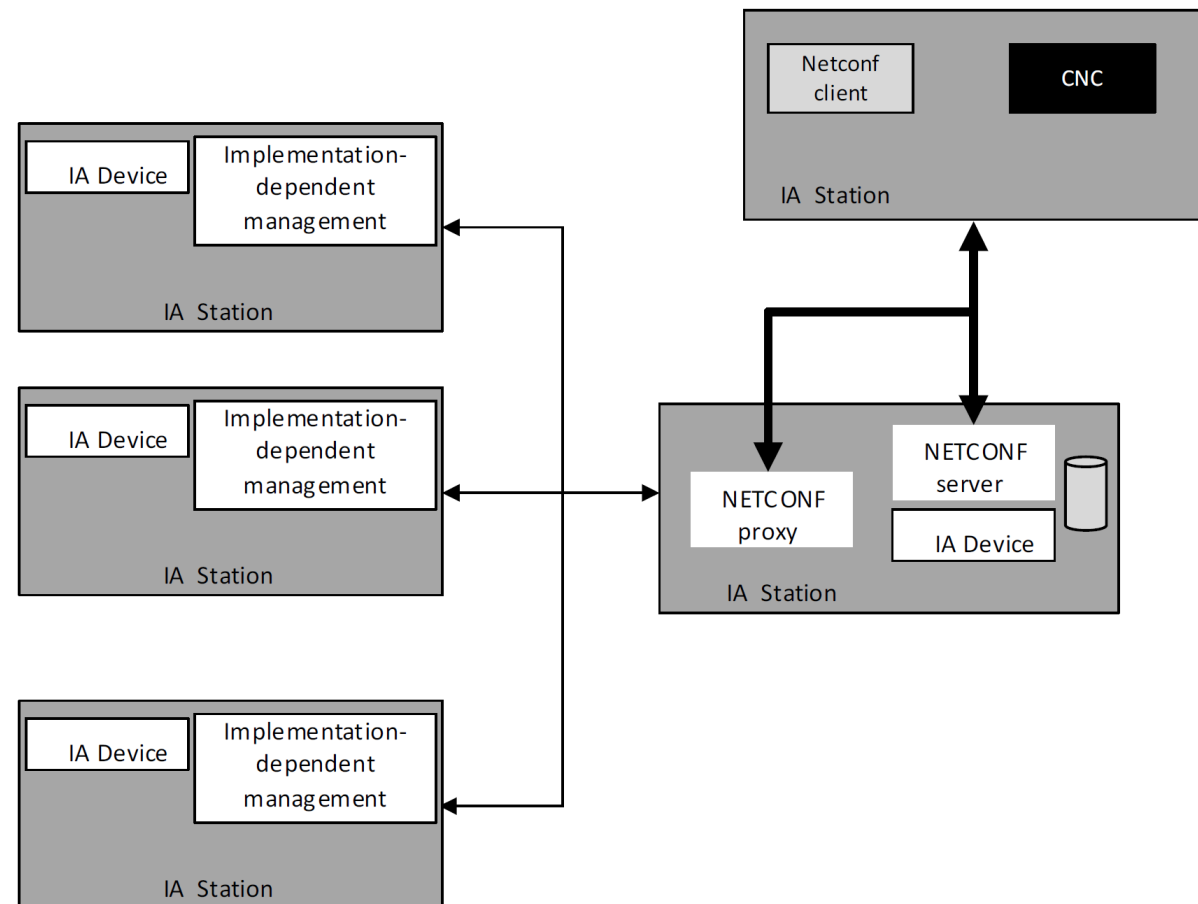
- IEC/IEEE 60802 D3.0 requires support of secure management using Netconf over TLS by all IA-stations
- This approach was the result of numerous discussions regarding constrained devices. Ultimately, despite concerns that constrained devices may lack the resources to support Netconf over TLS, the support of such devices was deferred to edition 2 of 60802
- Concerns that we are failing to address a significant portion of the market have resurfaced, leaving us with 3 proposed approaches:
 - Defer support of constrained devices to edition 2
 - Allow support of secure management to be optional for a certain class of bridge or end station component (e.g., ccB) effectively meaning these devices can only be used in engineered networks
 - Allow a proxy to act as the management entity for constrained devices

Current Proposal

- Netconf server hosting & responsibility concept (allow splitting between Netconf hosting and the constrained device)
- Netconf server of an IA-station can be located in that IA-station or in another IA-station of the same TSN configuration domain
- Protocol(s) of communication between the Netconf server and the constrained devices is out of scope
- Constrained devices need to be able to communicate with their proxy, irrespectively of whether on-boarding already happened

Current Proposal

- Secure onboarding: the secure onboarding conformant to the 60802 is related to the Netconf server; the way the secure onboarding is done by the management entity of the constrained devices is out of scope
 - Protocol(s) of communication between the Netconf server and the constrained devices are secured by means equivalent to 6.3.
 - Note: In this context, the Netconf client (potentially collocated with the CNC) is not able to verify the security relationship between Netconf server and constrained device(s).



Concerns with the Current Proposal

- **Constrained devices need to be able to communicate with their proxy, irrespectively of whether on-boarding already happened**
 - Per D3.0 of 60802 the CNC acts as a “gatekeeper” for the network effectively deciding whether it is safe and secure to on-board a new device
 - Toward this end, 60802 established an “isolation VLAN” which allows a newly discovered device to communicate w/ the CNC only
 - The role of 60802 is to ensure that the CNCs and IA-stations have the appropriate tools to allow on-boarding of new devices according to the security policies of the user (e.g., port states, Netconf over TLS, secure management, isolation VLAN, etc.)
 - It is not the role of 60802 to establish security policy for the network (e.g., what to do when a new device is detected but can't be authenticated)
 - It is not the role of 60802 to specify a CNC
- The current proposal effectively removes the gatekeeper by allowing any new device to communicate on the isolation VLAN.

Concerns with the Current Proposal

- How does the CNC know that a given IA-station is acting as proxy for a given constrained device?
 - How does the CNC identify the capabilities of the new device?
 - How does the CNC receive the traffic requirements of the new device?
 - How does the CNC ensure that the traffic produced by the new device does not interfere with current network operation?
- No conformance criteria for proxied devices are established

Alternative proposal

- LLDP defines a management address that effectively enables one station to act as the management entity for a different station.
- The primary challenge to using this approach is the on-boarding of new devices.
- The issue is that a device connected to a boundary port in the Isolated state can only communicate w/ the CNC, not with its proxy.

Table 8-1—TLV type values

TLV type ^a	TLV name	Usage in LLDPDU	Reference
0	End Of LLDPDU	Optional	8.5.1
1	Chassis ID	Mandatory	8.5.2
2	Port ID	Mandatory	8.5.3
3	Time To Live	Mandatory	8.5.4
4	Port Description	Optional	8.5.5
5	System Name	Optional	8.5.6
6	System Description	Optional	8.5.7
7	System Capabilities	Optional	8.5.8
8	Management Address	Optional	8.5.9
9–126	Reserved for future standardization	—	—
127	Organizationally Specific TLVs	Optional	—

^aTLVs with type values 0–8 are members of the basic management set.

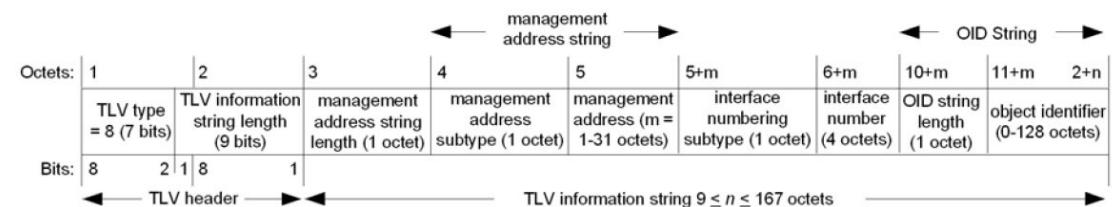
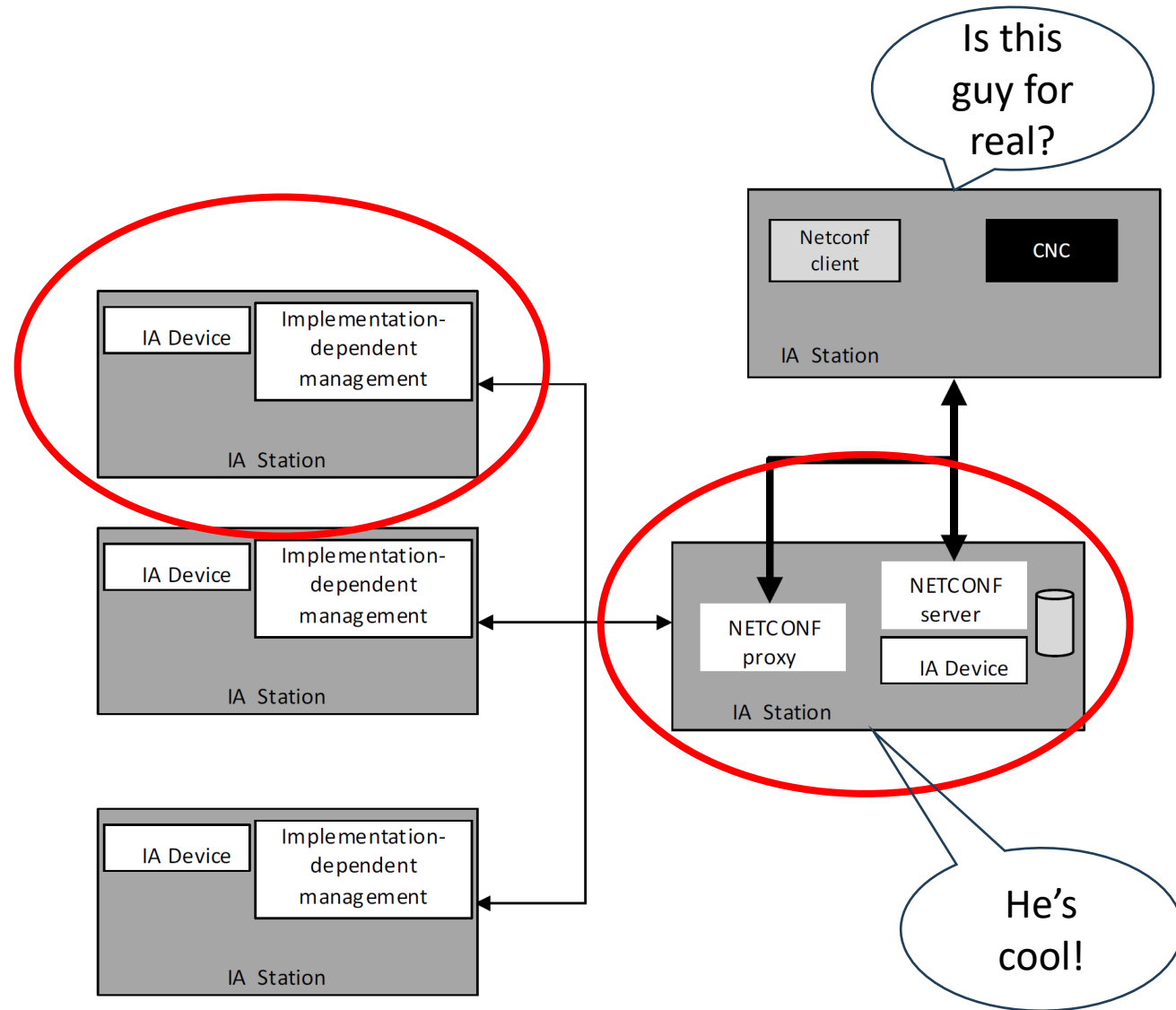


Figure 8-11—Management Address TLV format

Alternative proposal

- The CNC detects via LLDP that the proxied device is using a different management address.
- If and only if, that management proxy exists in the network, the CNC issues an RPC to the proxy
- The proxy performs the following steps:
 - Joins the isolation VLAN.
 - Authenticates the new device via a user-specific means. Ensuring the security of this user-specific mechanism is the responsibility of the user.
 - Returns the result of the Authentication to the CNC.
 - Leaves the isolation VID.
- Based upon the results of the authentication, the CNC sets the boundary port state appropriately.



Note: This is an example of one security policy. Others may include not permitting proxied devices, informing the user that a proxied device has been connected to the network, etc.,

60802 Requirements for CNC and CUC

- This approach implies requirements for the CNC
- The current draft of 60802 includes requirements for the CNC (5.11) and the CUC (5.13)
- The structure of these requirement in the current draft seems problematic
 - The structure implies we are establishing conformance criteria for the CNC and the CUC
 - The intent is to impose additional management requirements on IA-stations that claim to support CNC and CUC functionality (i.e., these are IA-station management requirements conditional on the present of a CNC or CUC function within the IA-station).
- These requirements should be moved under 5.5 IA-station requirement and any additional requirements for support of proxies should be contained within that subclause.

Example of Proposed RPC

6.4.10.4.2 Action is-this-guy-for-real

6.4.10.4.2.1 General

This Action requests an IA-station acting as a proxy authenticate the designated device.

6.4.10.4.2.2 Input

MAC address of the device to be authenticated

6.4.10.4.2.3 Output

Result - Status information indicating if the designated device has been successfully authenticated

Example of Proposed Changes to the draft

5.5.4.2 Secure management requirements

IA-stations which contain a ccA Bridge or a ccA end station component and for which a claim of conformance to this document is made shall support the following list of requirements.

- a) NETCONF server functionality according to IETF RFC 6241 including:
 - 1) Candidate configuration capability as described in IETF RFC 6241, 8.3,
 - 2) Rollback-on-Error capability as described in IETF RFC 6241, 8.5, and
 - 3) Validate capability as described in IETF RFC 6241, 8.6.
- b) NETCONF-over-TLS server according to 6.3.2.1 and 6.3.4.

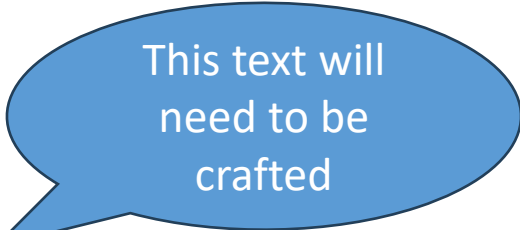
.
. .
.

Example of Proposed Changes to the draft

5.5.4.2 Secure management options

IA-stations containing only ccB Bridges or ccB end station components and for which a claim of conformance to this document is made may support the following list of requirements.

- a) NETCONF server functionality according to IETF RFC 6241 including:
 - 1) Candidate configuration capability as described in IETF RFC 6241, 8.3,
 - 2) Rollback-on-Error capability as described in IETF RFC 6241, 8.5, and
 - 3) Validate capability as described in IETF RFC 6241, 8.6.
- b) NETCONF-over-TLS server according to 6.3.2.1 and 6.3.4.
- .
- .
- .
- x) Management proxy functionality per 6.3.x.x.



This text will need to be crafted

Open Questions

- Is the proposed approach for limiting proxies to ccB-only IA-stations acceptable or is it desirable to have ccA devices with proxy capability?
 - If yes, does the presence of secure management become optional for ccA devices as well?
- What is the role of 60802 in providing conformance criteria for proxied devices?
 - Is it our responsibility to ensure that the proxied device and the proxy interact in a conformant manner?
 - In the opinion of this contributor the answer is no.
 - We cannot establish conformance criteria for a user-defined interface. That responsibility lies with user.
- What is the role of 60802 in providing conformance criteria for the proxy?
 - The only measurable requirement is support of the RPC.

Open Questions

- How do the CNC and the proxy distinguish between communications intended for the proxy and those intended for the proxied device?
- Is there other useful information which should be included in the RPC exchange?
- Do we need a managed object indicating that a given IA-station supports proxy capability?
- Does the current (or future) l2vlan interface naming scheme work for proxied devices?
- Does the current method for discovering the structure of an IA-station work for proxied devices?
- Does this approach raise additional security concerns (i.e., attack surfaces)?

Summary

- This contributor would still prefer that addressing constrained devices be deferred to edition 2 to ensure that any such approach receives proper technical scrutiny prior to publication
- That said, concerns that we are failing to address a significant portion of the market are, in the opinion of this contributor, legitimate.
- With that in mind, this contributor kindly requests the following:
 - Review of the approach by subject matter experts (SME) to ensure that the approach is viable
 - Review by security SMEs to ensure that any attack surfaces opened by this approach are understood and acceptable

Thank you