6840102 NETWORK DEVICES
COMMENTS FROM INTERNAL/INDUSTRY REVIEW

David Choi
7143507470
david.choi@etherwan.com

Comments: (6-24-19)
684-1.2.5, #4, it says "Support of, at a minimum, Version 2 of the Internet Group Management Protocol (IGMP)". This can be applied to both layer 2 and layer 3. For layer 2, it would be related to IGMP snooping. For layer 3, it would be related to the full IGMP protocol for multicast routing. It would be good to clarify if #4 applies to the full IGMP protocol for layer 3 or if having just IGMP snooping for layer 2 is sufficient to satisfy this requirement.

Response: The changes don't show the full specification. The specification is for layer 2 switches. Layer 2 IGMP snooping is sufficient.

****

Tom Baker
763-957-6158
tom.baker@comtrol.com

Comments: (6-25-19)
Hello, our switch engineers went through the PDF posted for the network devices. Everything looked perfect except for the last part (which I highlighted in the attached document) which reads:
684-2.2.4 Configuration and Management: Provide a device server that supports local and remote configuration and management, which must include access to all user-programmable features, including but not limited to addressing, port configuration, device monitoring, diagnostic utilities, and security functions. Ensure that the device server supports configuration and management via serial login, SNMP, telnet login, and browser-based interface.

PortVision DX, the software we provide with the switch can set the IP address, subnet mask, and gateway addresses and allows uploading and downloading configuration files and uploading firmware files. Beyond that the user has to use the switch's built-in management interfaces. This has not been an issue in our DOT projects in Florida and throughout the US, but I wanted to be sure to reach out and let you know our complete feedback.

Response: This language is for device servers and not the network switches. Testing at the TERL will verify configuration via SNMP, a telnet interface and a browser based interface.

****

Ken Kao
513-250-8581
ken.kao@advantech.com

Comments: (6-25-19)

It appears the purpose of this change is all about “Cybersecurity” aspect, but all configuration or FW image file could be processed by SSL and SSH, they’re most popular the secured encryption tunnel/connection by exchanging the date from the switch and computer. More than that, the engineer may want to consider to add ACL (Access Control List), DHCP Snooping, ARP Spoofing Prevention, IP Source Guard and DoS (Denial of Service) because they’re the key advantage to build up L2/L3 security features.

Response: Thanks for the additional information. We will investigate these additional security requirements in a future release of the spec.

****

Katie King
386-943-5333
katie.king@dot.state.fl.us

Comments: (7-5-19)
1. The last sentence in Section 684-2.2.4 should be updated to be consistent with the other changes made to the specification. Remove “telnet login and browser-based interface” and replace with “Secure Shell (SSH), and secure web-based GUI”.

Response: This section is for device servers. We did not address security for device servers in this round of spec changes. We will investigate this for a future spec change.

2. (7-8-19) 684-1.2.5 Management Capability: Bullet 6 should reference support for SNMP v3.

Response: Thanks Katie. We will see if we can add this into the next version of the spec. We will discuss this with the communications group in the TSM&O section. For this round, we just aligned with the security guidance from the TSM&O section.

****