ORIGINATION FORM
Proposed Revisions to the Specifications
(Please provide all information - incomplete forms will be returned)

Date: **Office:**

Originator: **Specification Section:**

Telephone: **Article/Subarticle:**

email:

Will the proposed revision require changes to:

Publication	Yes	No	Office Staff Contacted
Standard Plans Index			
Traffic Engineering Manual			
FDOT Design Manual			
Construction Project Administration Manual			
Basis of Estimate/Pay Items			
Structures Design Guidelines			
Approved Product List			
Materials Manual			

Will this revision necessitate any of the following:

Design Bulletin   **Construction Bulletin**   **Estimates Bulletin**   **Materials Bulletin**

Are all references to external publications current?   Yes   No

If not, what references need to be updated? (Please include changes in the redline document.)

Why does the existing language need to be changed?

Summary of the changes:

Are these changes applicable to all Department jobs?   Yes   No
If not, what are the restrictions?

Florida Department of Transportation

RON DESANTIS
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

KEVIN J. THIBAULT
SECRETARY

M E M O R A N D U M

DATE: June 20, 2019

TO: Specification Review Distribution List

FROM: Stefanie D. Maxwell, Manager, Program Management Office

SUBJECT: Proposed Specification: **6840102 Network Devices.**

  In accordance with Specification Development Procedures, we are sending you a copy of a proposed specification change.

  This change was proposed by Derek Vollmer of the State Traffic Engineering Research Lab (TERL) to modify the language.

  Please share this proposal with others within your responsibility. Review comments are due within four weeks and should be sent to Mail Station 75 or online at http://www2.dot.state.fl.us/ProgramManagement/Development/IndustryReview.aspx . Comments received after July 18, 2019, may not be considered. Your input is encouraged.

SM/dt
Attachment

NETWORK DEVICES.
(REV 5-30-19)

SUBARTICLE 684-1.2.2 is deleted and the following substituted:

684-1.2.2 Networking Standards: Ensure that the MFES complies with all applicable IEEE networking standards for Ethernet communications, including but not limited to:
1. IEEE 802.1~~DQ~~ ~~S~~standard for ~~Media Access Control (MAC)~~Local and Metropolitan Area Networks – Bridges and Bridged Networks used with port-based virtual local area networks (VLANs) ~~the~~and Rapid Spanning Tree Protocol (RSTP).
2. ~~IEEE 802.1Q standard for port-based virtual local area networks (VLANs).~~
~~3.~~ IEEE 802.1P standard for Quality of Service (QoS).
~~4~~3. IEEE 802.3 standard for local area network (LAN) and metropolitan area network (MAN) access and physical layer specifications.
~~5~~4. IEEE 802.3u supplement standard regarding 100 Base TX/100 Base FX.
~~6~~5. IEEE 802.3x standard regarding flow control with full duplex operation.

SUBARTICLE 684-1.2.5 is deleted and the following substituted:

684-1.2.5 Management Capability: Ensure that the MFES supports all Layer 2 management features and certain Layer 3 features related to multicast data transmission and routing. These features shall include, but not be limited to:
1. An MFES that is a port-based VLAN and supports VLAN tagging that meets or exceeds specifications as published in the IEEE 802.1Q standard, and has a minimum 4-kilobit VLAN address table.
2. A forwarding/filtering rate that is a minimum of 14,880 packets per second for 10 megabits per second and 148,800 packets per second for 100 megabits per second.
3. A minimum 4 kilobit MAC address table.
4. Support of, at a minimum, Version 2 of the Internet Group Management Protocol (IGMP).
5. Support of remote and local setup and management via ~~telnet~~secure shell (SSH) and secure Web-based GUI.
6. Support of the Simple Network Management Protocol (SNMP). Verify that the MFES can be accessed using the resident EIA-232 management port~~,~~ or a telecommunication network~~, or the Trivial File Transfer Protocol (TFTP)~~.
7. ~~Port security through controlling access by the users. Ensure that the MFES has the capability to generate an alarm and shut down ports when an unauthorized user accesses the network.~~Support of Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+).
8. Support of remote monitoring (RMON) of the Ethernet agent and the ability to be upgraded to switch monitoring (SMON), if necessary.

9. Support of Secure Copy (SCP) or Secure File Transfer Protocol (TSFTP) and either Network Time Protocol (NTP) or the Simple Network Time Protocol (SNTP). Ensure that the MFES supports port mirroring for troubleshooting purposes when combined with a network analyzer.

SUBARTICLE 684-2.2.4 is deleted and the following substituted:

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.