ERO Enterprise CMEP Practice Guide:

Assessment of Virtualized Networks

February 26, 2021

Background

In support of successful implementation of and compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards, the Electric Reliability Organization (ERO) Enterprise[1] adopted the Compliance Guidance Policy.[2] The Compliance Guidance Policy outlines the purpose, development, use, and maintenance of guidance for implementing Reliability Standards. According to the Compliance Guidance Policy, Compliance Guidance includes two types of guidance – Implementation Guidance and Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.

Purpose

This CMEP Practice Guide provides guidance to ERO Enterprise CMEP staff (CMEP staff) when assessing a Responsible Entity's applicable systems that incorporate Virtual Local Area Networks (VLAN). This Practice Guide outlines risks that CMEP staff should consider when verifying methods used to meet the security objectives. This risk information informs CMEP staff's understanding of a Responsible Entity's security posture and commensurate Compliance Oversight (i.e., Compliance Oversight Plan, audit approach, etc.). CMEP staff make compliance determinations in light of the specific facts and circumstances of the individual Responsible Entities and the language of the Requirements.

General Approach

CMEP staff should consider Cyber Assets providing functions for Cyber Assets within an Electronic Security Perimeter (ESP) and Cyber Assets outside an ESP to be shared infrastructure. CMEP staff should verify that the Responsible Entity identifies and protects any Cyber Asset providing shared infrastructure, regardless of type, to the highest "water mark" of CIP compliance. Each Cyber Asset providing shared infrastructure must comply with the applicable CIP Requirements for all BES Cyber Systems (BCS) to which it connects.

VLANs

A Virtual Local Area Network (VLAN) is defined in the IEEE 802.1Q communications standard[3]. A VLAN configuration allows a single network appliance (e.g., a switch) to operate in multiple Local Area Networks. Any switch port can belong to any one VLAN. Switch ports not explicitly configured to be on a specific VLAN are assigned to the default VLAN. Switches may additionally contain ports configured on an 802.1q interface, also known as a trunk port. Unicast, broadcast, and multicast packets are forwarded only to hosts within the VLAN where the packets originated.

[1] The ERO Enterprise consists of NERC and the Regional Entities

[2] The ERO Enterprise Compliance Guidance Policy

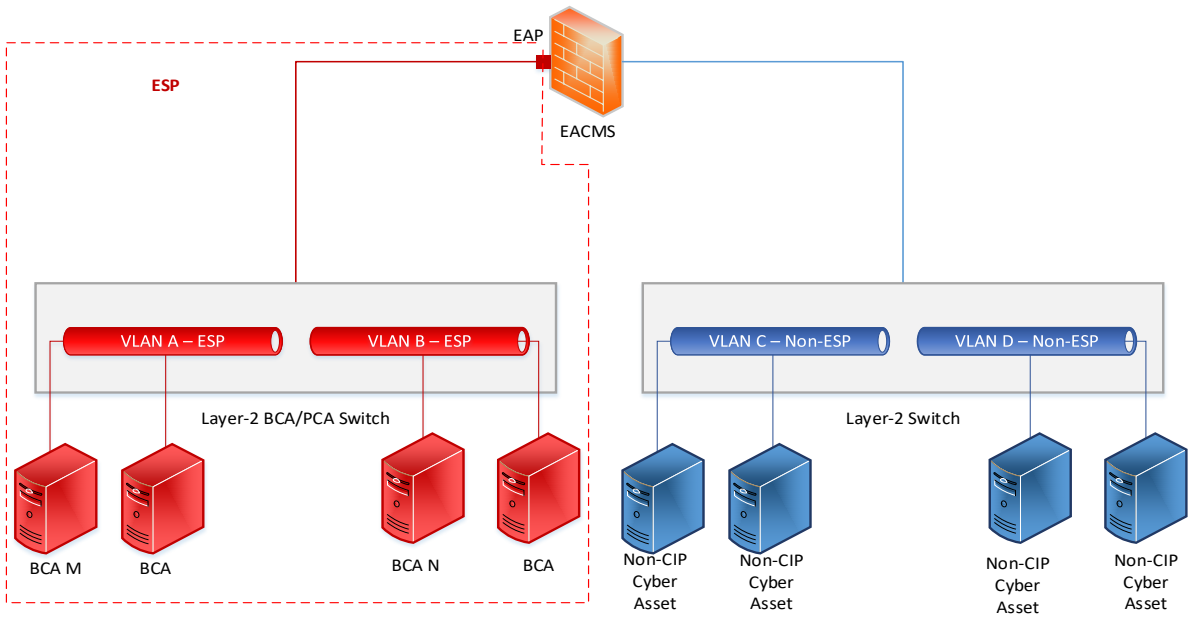
[3] IEEE 802.1Q-2018 - IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks.

VLAN technologies accomplish isolation by inserting tag information to the Ethernet frame header. These tags identify the assigned VLAN for that frame. Each VLAN works as a separate logical network. Packets addressed for endpoints external to the originating VLAN (or subnet) must forward through a device that supports routing.

Routing between multiple VLANs may occur on a Cyber Asset separate from the VLAN switch. CMEP staff should view routable protocol as defined in layer-3 of the OSI Model[4]. Additional information can be found in the National Institute of Standards and Technology (NIST) Special Publication 800-125: Guide to Security for Full Virtualization Technologies.[5]

Potential VLAN Implementations

Any Cyber Asset interface routing between VLANs within an ESP and outside an ESP should be identified as an Electronic Access Point (EAP) and assessed by CMEP staff accordingly against all applicable CIP Requirements. CMEP staff should be cognizant that the layer-3 VLAN routing EAP may exist on a Cyber Asset independent from the Cyber Asset performing the layer-2 VLAN switching. In addition, the Cyber Asset containing the EAP should be identified as an EACMS. CMEP staff should verify that all External Routable Connectivity (ERC) passes through an identified EAP and the EAP has inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.



[4] https://www.sans.org/reading-room/whitepapers/standards/osi-model-overview-543 The OSI Model: An Overview, 2001, Rachelle Miller, SANS Reading Room, retrieved 1/22/2021

[5] http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

In the example illustrated above, a possible use of VLAN technology is depicted. Two Layer-2 switches implementing VLANs are used to physically segment ESP traffic from non-ESP traffic. In addition, the switches are separated using a firewall and all ERC passes through the EAP on the firewall.

Traffic between VLAN A and VLAN B travels through the connection to the EAP and into the firewall. Within the firewall, the traffic is filtered and routed to the appropriate network. For example, BCA M on VLAN A sends traffic to a BCA N on VLAN B. The traffic flows through the EAP to the firewall. The firewall determines the destination network and applies the appropriate filters to the traffic. If permitted, the traffic flows back through the EAP to VLAN B and arrives at BCA N.

CMEP staff should verify all Cyber Assets used to implement VLAN technology comply with all applicable CIP Requirements.

Special Cases

CMEP staff may observe ESP and non-ESP network traffic in a single Cyber Asset. CMEP staff should review each case and make a compliance determination based on the language of the applicable Reliability Standards and professional judgment.

Low Impact BES Cyber Systems Considerations

CMEP staff should assess the use of VLANs in a network containing low impact BES Cyber Systems in a similar way to that of a network containing high or medium impact BES Cyber Systems. For each asset containing low impact BES Cyber Systems, the Responsible Entity is required to permit only necessary inbound and outbound electronic access to low impact BES Cyber Systems in accordance with Attachment 1 Section 3 of CIP-003. While identification and protection of an ESP is not required for low impact BES Cyber Systems, the concepts used to control access are similar to those for high or medium impact BES Cyber Systems. CIP-003 Reference Models 9 and 10 may be of guidance in evaluating logical separation of networks.

Conclusion

In assessing a Responsible Entity's VLAN configuration, CMEP staff should identify and ensure all VLANs configured within an ESP are externally accessible only through an identified EAP. In addition, CMEP staff should assess the configuration of the network supporting VLANs and the Cyber Assets used to implement VLANs against the applicable CIP Requirements.