Compliance Self Test Plan for Cisco IOS XE Layer 2 Switch

09 NOV 2023

SIGNATURES

Information Systems Security Manager:

_____	_____
Name	**Date**
ISSM	

Information Systems Security Officer:

_____	_____
Name	**Date**
ISSO	

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose

The purpose of the Cisco IOS XE Switch Test Plan is to provide all involved parties with a discrete set of measurement and expected outcomes in order to gauge successful security compliance self-testing for the Layer 2 Switch HARDWARE system at the installation location. Additionally, this document will outline the resources needed to successfully accomplish this test.

1.2 Scope

The scope of this test includes the test cases for the Cisco IOS XE Switch on the GENERIC baseline system. Including the technical security policies, requirements, and implementation details for applying security concepts to Cisco IOS XE switch devices such as the Catalyst 3650, 3850, and 9000 (9200, 9300, 9400) Series.

2. Environment (Target System)

The GENERIC system is comprised of the following sub-systems with associated operating systems and Original Equipment Manufacturer (OEM) as defined;

- INSERT SYSTEM (ABBREVIATION) [OPERATING SYSTEM, ORGANIZATION OWNER]

- LIST

The interface control systems that are testable in the target system include the account consoles to the GENERIC system, as defined by access through the sub-system.

2.1 Security Environment

The security environment will be at the [INSERT LEVEL OF SECURITY] level and will require the appropriate security and control measures suitable for the data being processed. All personnel will require access authorization to both the testing facility and the data produced on the system components. Any test materials, data, or reports identified as being classified will require the appropriate markings, protection, transmission, handling and storage procedures.

3. Responsibilities

3.1 Site ISSM

Organizational personnel will provide logistical and technical support to the OEM team during the installation and test period. Support should include any system administration or network administration that must be accomplished on the host environment in order to successfully integrate the test system into the [ORGANIZATIONAL] network.

3.2 Site ISSO

Implementation of appropriate security controls to maintain information system risk and associated mission risk at an acceptable level as determined by the Authorizing Authority (AO). The system controls, the particular controls with [ORGANIZATIONAL] defined parameters in applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems Instruction (CNSSI) 1253 are referenced by the following list:

- INSERT SYSTEM CONTROL (ABBREVIATION) [OPERATING SYSTEM, ORGANIZATION OWNER] [PARAMETER]

- LIST

3.3 [ORGANIZATION]

Develop the cybersecurity compliance self-test plan. The test procedures contained in this document are referenced to values for Cisco IOS XE Layer 2 Switch (L2S) security technical implementation guide (STIG) date of 25 October 2023 developed by the Defense Information Systems Agency (DISA). The configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

4. Test Execution Instructions

i) The test procedure sheet may be filled out manually or electronically.
   (1) Complete the entries for target system, date, and test representative at the beginning of the procedure.
   (2) All information assurance security controls in the table must be marked as:
      (a) Pass:
         (i) the device passed the security test
      (b) Fail:
         (i) the device failed the test; or
         (ii) device lacks the capability and is not compensated by another device/measure
      (c) Not Evaluated:
         (i) no test provided; or
         (ii) the device is not available for testing; or
         (iii) the device lacks the capability but is compensated by another device/measure
   (3) Provide comments for any control not marked as Pass.
   (4) Upon completion, the score sheet is digitized if necessary, and uploaded as an exhibit to the appropriate [ORGANIZATION] project reference.

4.1 Test Procedure

The following pages provide the detailed test procedure required to perform the target system compliance self-test plan.

Step	Step Description	Expected Results/Comments	P/F
Security Test Case TEST SCENARIO: The test executioner will log onto a [access interface] workstation and execute a series of commands and check the results against the respective expected results that are listed below. TEST SETUP: 1. The test executioner will log into a [access interface] workstation with valid LDAP user with privileged access (account should have a ".priv" at the end of it). 2. Once logged on, the test executioner will open a shell by clicking on Hosts and selecting Console, as referenced of switch console with elevated privileges. 3. Within the shell, the test execution will execute the following shell commands			
N/A	**Record Test Start Date/Time**	**Start Date:** _____ **Start Time:** _____	N/A
Test 1 NIST SP 800-53 :: IA-3 **CCI-000778; Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.** **CCI-001958; Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.**			

Step	Step Description	Expected Results/Comments	P/F
1	Verify if the switch configuration has 802.1x authentication implemented for all access switch ports connecting to LAN outlets (i.e., RJ-45 wall plates) or devices not located in the telecom room, wiring closets, or equipment rooms. MAC Authentication Bypass (MAB) must be configured on those switch ports connected to devices that do not support an 802.1x supplicant.	Step 1: Verify that 802.1x is configured on all host-facing interfaces as shown in the example below: interface GigabitEthernet1/0 switchport access vlan 12 switchport mode access authentication port-control auto dot1x pae authenticator ! interface GigabitEthernet1/1 switchport access vlan 13 switchport mode access authentication port-control auto dot1x pae authenticator ! interface GigabitEthernet1/2 switchport access vlan 13 switchport mode access authentication port-control auto dot1x pae authenticator Step 2: Verify that 802.1x authentication is configured on the switch as shown in the example below: aaa new-model ! ! aaa group server radius RADIUS_SERVERS server name RADIUS_1 server name RADIUS_2 ! aaa authentication dot1x default group RADIUS_SERVERS … … … dot1x system-auth-control Step 3: Verify that the radius	

Step	Step Description	Expected Results/Comments	P/F
		servers have been defined. SW1#show radius server-group RADIUS_SERVERS Note: Single-host is the default. Host-mode multi-domain (for VoIP phone + PC) or multi-auth (multiple PCs connected to a hub) can be configured as alternatives. Host-mode multi-host is not compliant with this requirement. If 802.1x authentication or MAB is not configured on all access switch ports connecting to LAN outlets or devices not located in the telecom room, wiring closets, or equipment rooms, this is a finding.	
Test 2 NIST SP 800-53 :: IA-7 **CCI-000803; Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.**			

Step	Step Description	Expected Results/Comments	P/F
2	VLAN Trunk Protocol (VTP) provides central management of VLAN domains, thus reducing administration in a switched network. When configuring a new VLAN on a VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. VTP pruning preserves bandwidth by preventing VLAN traffic (unknown MAC, broadcast, multicast) from being sent down trunk links when not needed, that is, there are no access switch ports in neighboring switches belonging to such VLANs. An attack can force a digest change for the VTP domain enabling a rogue device to become the VTP server, which could allow unauthorized access to previously blocked VLANs or allow the addition of unauthorized switches into the domain. Authenticating VTP messages with a cryptographic hash function can reduce the risk of the VTP domain's being compromised.	Review the switch configuration to verify if VTP is enabled using the show vtp status command as shown in the example below: Switch#show vtp status VTP Version capable : 1 to 3 VTP version running : 1 VTP Domain Name : VTP Pruning Mode : Disabled VTP Traps Generation : Disabled Device ID : 5e00.0000.8000 Feature VLAN: -------------- VTP Operating Mode : Off Maximum VLANs supported locally : 1005 Number of existing VLANs : 5 Configuration Revision : 0 MD5 digest : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD 0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC Switch# If mode is set to anything other than off, verify that a password has been configured using the show vtp password command. Note: VTP authenticates all messages using an MD5 hash that consists of the VTP version + The VTP Password + VTP Domain + VTP Configuration Revision. If VTP is enabled on the switch and is not authenticating VTP messages with a hash function using a configured password, this is a finding.	
Test 3 NIST SP 800-53 :: SC-5 (2) **CCI-001095; Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.**			

Step	Step Description	Expected Results/Comments	P/F
3	Denial of service is a condition when a resource is not available for legitimate users. Packet flooding DDoS attacks are referred to as volumetric attacks and have the objective of overloading a network or circuit to deny or seriously degrade performance, which denies access to the services that normally traverse the network or circuit. Volumetric attacks have become relatively easy to launch by using readily available tools such as Low Orbit Ion Cannon or by using botnets. Measures to mitigate the effects of a successful volumetric attack must be taken to ensure that sufficient capacity is available for mission-critical traffic. Managing capacity may include, for example, establishing selected network usage priorities or quotas and enforcing them using rate limiting, Quality of Service (QoS), or other resource reservation control methods. These measures may also mitigate the effects of sudden decreases in network capacity that are the result of accidental or intentional physical damage to telecommunications facilities (such as cable cuts or weather-related outages).	Step 1: Verify that the class-maps are configured to match on DSCP values as shown in the configuration example below: class-map match-all C2_VOICE match ip dscp af47 class-map match-all VOICE match ip dscp ef class-map match-all VIDEO match ip dscp af41 class-map match-all PREFERRED_DATA match ip dscp af33 Step 2: Verify that the policy map reserves the bandwidth for each traffic type as shown in the following example: policy-map QOS_POLICY_SWITCHPORT class C2_VOICE priority level 1 10 class VOICE priority level 2 15 class VIDEO bandwidth percent 25 class PREFERRED_DATA bandwidth percent 25 class class-default bandwidth percent 25 verone interface GigabitEthernet1/1 switchport trunk allowed vlan 100,110,200 switchport mode trunk service-policy output QOS_POLICY_SWITCHPORT ! interface GigabitEthernet1/2 switchport access vlan 100 switchport mode access switchport voice vlan 200	

Step	Step Description	Expected Results/Comments	P/F
		trust device cisco-phone service-policy output QOS_POLICY_SWITCHPORT ! interface GigabitEthernet1/2 switchport access vlan 110 switchport mode access switchport voice vlan 200 trust device cisco-phone service-policy output QOS_POLICY_SWITCHPORT If QoS has not been enabled, this is a finding.	
Test 4 NIST SP 800-53 Revision 4 :: SC-5 **CCI-002385; Protect against or limit the effects of organization-defined types of denial of service events.**			
4	Spanning Tree Protocol (STP) does not provide any means for the network administrator to securely enforce the topology of the switched network. Any switch can be the root bridge in a network. However, a more optimal forwarding topology places the root bridge at a specific predetermined location. With the standard STP, any bridge in the network with a lower bridge ID takes the role of the root bridge. The administrator cannot enforce the position of the root bridge but can set the root bridge priority to 0 in an effort to secure the root bridge position. The root guard feature provides a way to enforce the root bridge placement in the network. If the bridge receives superior STP Bridge Protocol Data Units (BPDUs) on a root guard-enabled port, root guard moves this port to a root-inconsistent STP state and no traffic can be forwarded across this port while it is in this state. To enforce the position of the root bridge it is imperative that root guard is enabled on all ports where the root bridge should never appear.	Review the switch topology as well as the configuration to verify that Root Guard is enabled on all switch ports connecting to access layer switches. interface GigabitEthernet0/0 spanning-tree guard root ! interface GigabitEthernet0/1 spanning-tree guard root … … … interface GigabitEthernet0/9 spanning-tree guard root If the switch has not enabled Root Guard on all switch ports connecting to access layer switches, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 5 NIST SP 800-53 Revision 4 :: SC-5 **CCI-002385; Protect against or limit the effects of organization-defined types of denial of service events.**			
5	If a rogue switch is introduced into the topology and transmits a Bridge Protocol Data Unit (BPDU) with a lower bridge priority than the existing root bridge, it will become the new root bridge and cause a topology change, rendering the network in a suboptimal state. The STP PortFast BPDU guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that has PortFast configured. The BPDU guard transitions the port into errdisable state and sends a log message.	Review the switch configuration to verify that BPDU Guard is enabled on all user-facing or untrusted access switch ports as shown in the configuration example below: interface GigabitEthernet0/0 spanning-tree bpduguard enable ! interface GigabitEthernet0/1 spanning-tree bpduguard enable … … … interface GigabitEthernet0/9 spanning-tree bpduguard enable If the switch has not enabled BPDU Guard, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 6 NIST SP 800-53 Revision 4 :: SC-5 **CCI-002385; Protect against or limit the effects of organization-defined types of denial of service events.**			
6	The Spanning Tree Protocol (STP) loop guard feature provides additional protection against STP loops. An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. In its operation, STP relies on continuous reception and transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs. When one of the ports in a physically redundant topology no longer receives BPDUs, the STP conceives that the topology is loop free. Eventually, the blocking port from the alternate or backup port becomes a designated port and moves to a forwarding state. This situation creates a loop. The loop guard feature makes additional checks. If BPDUs are not received on a non-designated port and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state.	Review the switch configuration to verify that STP Loop Guard is enabled as shown in the configuration example below: hostname SW2 … … … spanning-tree mode pvst spanning-tree loopguard default If STP Loop Guard is not enabled, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 7 NIST SP 800-53 Revision 4 :: SC-5 **CCI-002385; Protect against or limit the effects of organization-defined types of denial of service events.**			
7	The Cisco switch must have Unknown Unicast Flood Blocking (UUFB) enabled. Access layer switches use the Content Addressable Memory (CAM) table to direct traffic to specific ports based on the VLAN number and the destination MAC address of the frame. When a router has an Address Resolution Protocol (ARP) entry for a destination host and forwards it to the access layer switch and there is no entry corresponding to the frame's destination MAC address in the incoming VLAN, the frame will be sent to all forwarding ports within the respective VLAN, which causes flooding. Large amounts of flooded traffic can saturate low-bandwidth links, causing network performance issues or complete connectivity outage to the connected devices. Unknown unicast flooding has been a nagging problem in networks that have asymmetric routing and default timers. To mitigate the risk of a connectivity outage, the Unknown Unicast Flood Blocking (UUFB) feature must be implemented on all access layer switches. The UUFB feature will block unknown unicast traffic flooding and only permit egress traffic with MAC addresses that are known to exit on the port.	Review the switch configuration to verify that UUFB is enabled on all access switch ports as shown in the configuration example below: interface GigabitEthernet0/0 switchport block unicast ! interface GigabitEthernet0/1 switchport block unicast … … … interface GigabitEthernet0/9 switchport block unicast If any access switch ports do not have UUFB enabled, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 8 NIST SP 800-53 Revision 4 :: SC-5 **CCI-002385; Protect against or limit the effects of organization-defined types of denial of service events.**			
8	In an enterprise network, devices under administrative control are trusted sources. These devices include the switches, routers, and servers in the network. Host ports and unknown DHCP servers are considered untrusted sources. An unknown DHCP server on the network on an untrusted port is called a spurious DHCP server, any device (PC, Wireless Access Point) that is loaded with DHCP server enabled. The DHCP snooping feature determines whether traffic sources are trusted or untrusted. The potential exists for a spurious DHCP server to respond to DHCPDISCOVER messages before the real server has time to respond. DHCP snooping allows switches on the network to trust the port a DHCP server is connected to and not trust the other ports. The DHCP snooping feature validates DHCP messages received from untrusted sources and filters out invalid messages as well as rate-limits DHCP traffic from trusted and untrusted sources. DHCP snooping feature builds and maintains a binding database, which contains information about untrusted hosts with leased IP addresses, and it utilizes the database to validate subsequent requests from untrusted hosts. Other security features, such as IP Source Guard and Dynamic Address Resolution Protocol (ARP) Inspection (DAI), also use information stored in the DHCP snooping binding database. Hence, it is imperative that the DHCP snooping feature is enabled on all VLANs.	Review the switch configuration and verify that DHCP snooping is enabled on all user VLANs as shown in the example below: hostname SW2 … … … ip dhcp snooping vlan 2,4-8,11 ip dhcp snooping Note: Switchports assigned to a user VLAN would have drops in the area where the user community would reside; hence, the "untrusted" term is used. Server and printer VLANs would not be applicable. If the switch does not have DHCP snooping enabled for all user VLANs to validate DHCP messages from untrusted sources, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 9 NIST SP 800-53 Revision 4 :: SC-5 **CCI-002385; Protect against or limit the effects of organization-defined types of denial of service events.**			
9	IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports. Initially, all IP traffic on the protected port is blocked except for DHCP packets. After a client receives an IP address from the DHCP server, or after static IP source binding is configured by the administrator, all traffic with that IP source address is permitted from that client. Traffic from other hosts is denied. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address.	Review the switch configuration to verify that IP Source Guard is enabled on all user-facing or untrusted access switch ports as shown in the example below: interface GigabitEthernet0/0 ip verify source ! interface GigabitEthernet0/1 ip verify source … … … interface GigabitEthernet0/9 ip verify source Note: The IP Source Guard feature depends on the entries in the DHCP snooping database or static IP-MAC-VLAN configuration commands to verify IP-to-MAC address bindings. If the switch does not have IP Source Guard enabled on all untrusted access switch ports, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 10 NIST SP 800-53 Revision 4 :: SC-5 **CCI-002385; Protect against or limit the effects of organization-defined types of denial of service events.**			
10	The Cisco switch must have Dynamic Address Resolution Protocol (ARP) Inspection (DAI) enabled on all user VLANs. DAI intercepts Address Resolution Protocol (ARP) requests and verifies that each of these packets has a valid IP-to-MAC address binding before updating the local ARP cache and before forwarding the packet to the appropriate destination. Invalid ARP packets are dropped and logged. DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in the DHCP snooping binding database. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.	Review the switch configuration to verify that Dynamic Address Resolution Protocol (ARP) Inspection (DAI) feature is enabled on all user VLANs. hostname SW2 … … … ip arp inspection vlan 2,4-8,11 Note: DAI depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses. If DAI is not enabled on all user VLANs, this is a finding.	
Test 11 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
11	A traffic storm occurs when packets flood a LAN, creating excessive traffic and degrading network performance. Traffic storm control prevents network disruption by suppressing ingress traffic when the number of packets reaches a configured threshold levels. Traffic storm control monitors ingress traffic levels on a port and drops traffic when the number of packets reaches the configured threshold level during any one-second interval.	Review the switch configuration to verify that storm control is enabled on all host-facing interfaces as shown in the example below: interface GigabitEthernet0/3 switchport access vlan 12 storm-control unicast level bps 62000000 storm-control broadcast level bps 20000000 Note: Bandwidth percentage thresholds (via level parameter) can be used in lieu of PPS rate. If storm control is not enabled at a minimum for broadcast traffic, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 12 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
12	The Cisco switch must have IGMP or MLD Snooping configured on all VLANs. IGMP and MLD snooping provides a way to constrain multicast traffic at Layer 2. By monitoring the IGMP or MLD membership reports sent by hosts within a VLAN, the snooping application can set up Layer 2 multicast forwarding tables to deliver specific multicast traffic only to interfaces connected to hosts interested in receiving the traffic, thereby significantly reducing the volume of multicast traffic that would otherwise flood the VLAN.	Review the switch configuration to verify that IGMP or MLD snooping has been configured for IPv4 and IPv6 multicast traffic respectively. Below is an example of the steps to verify that IGMP snooping is enabled for each VLAN. Step 1: Verify that IGMP or MLD snooping is enabled globally. By default, IGMP snooping is enabled globally; hence, the following command should not be in the switch configuration: no ip igmp snooping Step 2: Verify that IGMP snooping is not disabled for any VLAN as shown in the example below: no ip igmp snooping vlan 11 Note: When globally enabled, it is also enabled by default on all VLANs, but can be disabled on a per-VLAN basis. If global snooping is disabled, VLAN snooping cannot be enabled. If the switch is not configured to implement IGMP or MLD snooping for each VLAN, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 13 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
13	The Cisco switch must implement Rapid STP where VLANs span multiple switches with redundant links. Spanning Tree Protocol (STP) is implemented on bridges and switches to prevent layer 2 loops when a broadcast domain spans multiple bridges and switches and when redundant links are provisioned to provide high availability in case of link failures. Convergence time can be significantly reduced using Rapid STP (802.1w) instead of STP (802.1d), resulting in improved availability. Rapid STP should be deployed by implementing either Rapid Per-VLAN-Spanning-Tree (Rapid-PVST) or Multiple Spanning-Tree Protocol (MSTP), the latter scales much better when there are many VLANs.	In cases where VLANs do not span multiple switches, it is a best practice to not implement STP. Avoiding the use of STP will provide the most deterministic and highly available network topology. If STP is required, then review the switch configuration to verify that Rapid STP has been implemented. hostname SW2 … … … spanning-tree mode rapid-pvst Note: Multiple STP (MSTP) can be configured as an alternate mode. MSTP which uses RSTP for rapid convergence and enables multiple VLANs to be grouped into and mapped to the same spanning-tree instance; thereby reducing the number of spanning-tree instances needed to support a large number of VLANs. If either RSTP or MSTP has not been implemented where STP is required, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 14 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
14	The Cisco switch must enable Unidirectional Link Detection (UDLD) to protect against one-way connections. In topologies where fiber optic interconnections are used, physical misconnections can occur that allow a link to appear to be up when there is a mismatched set of transmit/receive pairs. When such a physical misconfiguration occurs, protocols such as STP can cause network instability. UDLD is a layer 2 protocol that can detect these physical misconfigurations by verifying that traffic is flowing bidirectional between neighbors. Ports with UDLD enabled periodically transmit packets to neighbor devices. If the packets are not echoed back within a specific time frame, the link is flagged as unidirectional and the interface is shut down.	If any of the switch ports have fiber optic interconnections with neighbors, review the switch configuration to verify that UDLD is enabled globally or on a per-interface basis as shown in the examples below: hostname SW2 … … … udld enable or interface GigabitEthernet0/1 udld port Note: An alternative implementation when UDLD is not supported by connected device is to deploy a single member Link Aggregation Group (LAG) via IEEE 802.3ad Link Aggregation Control Protocol (LACP). If the switch has fiber optic interconnections with neighbors and UDLD is not enabled, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 15 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
15	The Cisco switch must have all trunk links enabled statically. When trunk negotiation is enabled via Dynamic Trunk Protocol (DTP), considerable time can be spent negotiating trunk settings (802.1q or ISL) when a node or interface is restored. While this negotiation is happening, traffic is dropped because the link is up from a layer 2 perspective. Packet loss can be eliminated by setting the interface statically to trunk mode, thereby avoiding dynamic trunk protocol negotiation and significantly reducing any outage when restoring a failed link or switch.	By default, Dynamic Trunking Protocol (DTP) is enabled on all Cisco switches. Review the switch configuration to verify that trunk links will not form trunk via negotiation as shown in the example below: SW2#show interfaces switchport Name: Gi0/0 Switchport: Enabled Administrative Mode: dynamic auto Operational Mode: static access Administrative Trunking Encapsulation: negotiate Operational Trunking Encapsulation: native Negotiation of Trunking: On If trunk negotiation is enabled on any interface, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 16 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
16	The Cisco switch must have all disabled switch ports assigned to an unused VLAN. It is possible that a disabled port that is assigned to a user or management VLAN becomes enabled by accident or by an attacker and as a result gains access to that VLAN as a member.	Step 1: Review the switch configurations and examine all access switch ports. Each access switch port not in use should have membership to an inactive VLAN. interface GigabitEthernet0/0 switchport access vlan 999 shutdown ! interface GigabitEthernet0/1 switchport access vlan 999 shutdown … … … interface GigabitEthernet0/9 switchport access vlan 999 shutdown Step 2: Verify that traffic from the inactive VLAN is not allowed on any trunk links as shown in the example below: interface GigabitEthernet1/1 switchport trunk allowed vlan 1-998,1000-4094 switchport trunk encapsulation dot1q switchport mode trunk Note: Switch ports configured for 802.1x are exempt from this requirement. If there are any access switch ports not in use and not in an inactive VLAN, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 17 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
17	The Cisco switch must not have the default VLAN assigned to any host-facing switch ports. In a VLAN-based network, switches use the default VLAN (i.e., VLAN 1) for in-band management and to communicate with other networking devices using Spanning-Tree Protocol (STP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)—all untagged traffic. As a consequence, the default VLAN may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.	Review the switch configurations and verify that no access switch ports have been assigned membership to the default VLAN (i.e., VLAN 1). VLAN assignments can be verified via the show vlan command. SW1#show vlan VLAN Name Status Ports ---- ---------- --------- ---------- 1 default active 10 User VLAN active Gi0/3, Gi1/0, Gi1/1, Gi1/2 Gi1/3, Gi2/1 20 Management VLAN active Gi0/2 999 VLAN0999 active Gi2/0 If there are access switch ports assigned to the default VLAN, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 18 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
18	The Cisco switch must have the default VLAN pruned from all trunk ports that do not require it. The default VLAN (i.e., VLAN 1) is a special VLAN used for control plane traffic such as Spanning-Tree Protocol (STP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP). VLAN 1 is enabled on all trunks and ports by default. With larger campus networks, care needs to be taken about the diameter of the STP domain for the default VLAN. Instability in one part of the network could affect the default VLAN, thereby influencing control-plane stability and therefore STP stability for all other VLANs.	Review the switch configuration and verify that the default VLAN is pruned from trunk links that do not require it. SW1#show interfaces trunk Port Mode Encapsulation Status Native vlan Gi0/1 on 802.1q trunking 1 Gi0/2 on 802.1q trunking 1 Port Vlans allowed on trunk Gi0/1 1-998,1000-4094 Gi0/2 1-4094 If the default VLAN is not pruned from trunk links that should not be transporting frames for the VLAN, this is a finding.	
Test 19 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
19	The Cisco switch must not use the default VLAN for management traffic. Switches use the default VLAN (i.e., VLAN 1) for in-band management and to communicate with directly connected switches using Spanning-Tree Protocol (STP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)—all untagged traffic. As a consequence, the default VLAN may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.	Review the switch configuration and verify that the default VLAN is not used to access the switch for management. interface Vlan22 description Management VLAN ip address 10.1.22.3 255.255.255.0 If the default VLAN is being used for management access to the switch, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 20 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
20	The Cisco switch must have all user-facing or untrusted ports configured as access switch ports. Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victim's MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attacker's VLAN ID (probably the well-known and omnipresent default VLAN) is stripped off by the switch, and the inner tag that will have the victim's VLAN ID is used by the switch as the next hop and sent out the trunk port.	Review the switch configurations and examine all user-facing or untrusted switchports. The example below depicts both access and trunk ports. interface GigabitEthernet0/1 switchport trunk encapsulation dot1q switchport mode trunk negotiation auto ! interface GigabitEthernet0/2 switchport access vlan 11 negotiation auto ! interface GigabitEthernet0/3 switchport access vlan 12 negotiation auto If any of the user-facing switch ports are configured as a trunk, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 21 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
21	The Cisco switch must have the native VLAN assigned to an ID other than the default VLAN for all 802.1q trunk links. VLAN hopping can be initiated by an attacker who has access to a switch port belonging to the same VLAN as the native VLAN of the trunk link connecting to another switch that the victim is connected to. If the attacker knows the victim's MAC address, it can forge a frame with two 802.1q tags and a layer 2 header with the destination address of the victim. Since the frame will ingress the switch from a port belonging to its native VLAN, the trunk port connecting to the victim's switch will simply remove the outer tag because native VLAN traffic is to be untagged. The switch will forward the frame on to the trunk link unaware of the inner tag with a VLAN ID of which the victim's switch port is a member.	Review the switch configurations and examine all trunk links. Verify the native VLAN has been configured to a VLAN ID other than the ID of the default VLAN (i.e. VLAN 1) as shown in the example below: interface GigabitEthernet0/1 switchport trunk encapsulation dot1q switchport trunk native vlan 44 switchport mode trunk negotiation auto Note: An alternative to configuring a dedicated native VLAN is to ensure that all native VLAN traffic is tagged. This will mitigate the risk of VLAN hopping since there will always be an outer tag for native traffic as it traverses an 802.1q trunk link. If the native VLAN has the same VLAN ID as the default VLAN, this is a finding.	

Step	Step Description	Expected Results/Comments	P/F
Test 22 NIST SP 800-53 :: CM-6 b **CCI-000366; Implement the security configuration settings.**			
22	The Cisco switch must not have any switchports assigned to the native VLAN. Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victim's MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attacker's VLAN ID (probably the well-known and omnipresent default VLAN) is stripped off by the switch, and the inner tag that will have the victim's VLAN ID is used by the switch as the next hop and sent out the trunk port. Configure all access switch ports to a VLAN other than the native VLAN.	Review the switch configurations and examine all access switch ports. Verify that they do not belong to the native VLAN as shown in the example below: interface GigabitEthernet0/1 switchport trunk encapsulation dot1q switchport trunk native vlan 44 switchport mode trunk negotiation auto ! interface GigabitEthernet0/2 switchport access vlan 11 negotiation auto ! interface GigabitEthernet0/3 switchport access vlan 12 negotiation auto ! If any access switch ports have been assigned to the same VLAN ID as the native VLAN, this is a finding.	
Notes:			

4.2 Reporting

A final After Action Report (AAR) will be provided to all [ORGANIZATION] stakeholders within 30 days of completion of demonstration execution.