Safe Harbor

At-A-Glance

What Is Safe Harbor?

Safe Harbor is a Cisco® program that focuses on satisfying customer quality requirements in critical vertical markets. This program linksand expands on product testing conducted within development engineering, regression testing, and systems test groups within Cisco Systems®. Safe Harbor certification marks the successful completion of extensive integrity testing that validates targeted releases.

Testing Goals

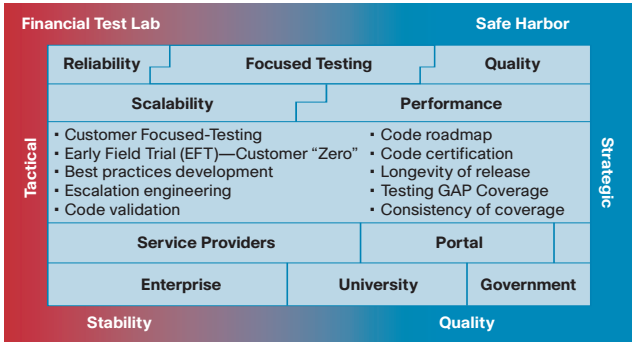
The goal of Safe Harbor is simple: improve the quality of the release through direct customer partnerships and testing. Safe Harbor provides testing coverage for critical feature areas as required by customer use. It complements internal product-testing efforts with customer-specific testing to certify functionality. Most importantly, Safe Harbor delivers on the quality commitment provided to Cisco customers. Safe Harbor involves testing select code releases and feature sets primarily on the Cisco Catalyst® 6500 Series platform. Coverage is currently in place for the Cisco Content Services Switch (CSS) appliance and for services modules (Catalyst 6500 Series Firewall Services Module, Cisco Content Switching Module [CSM], Catalyst 6500 Series Intrusion Detection System [IDSM] Services Module, Catalyst 6500 Series Wireless LAN Services Module [WLSM], and Catalyst 6500 Series SSL Services Module [SSLSM]). Testing is targeted primarily at the enterprise financial vertical market. Commercial, service provider, governmental, educational, and other customers benefit from the Safe Harbor process, because they can take advantage of the testing coverage applied to the common feature areas.

Testing Conditions

This combination of features, hardware, and image set is tested in a laboratory environment that simulates an enterprise financial-services network environment. Cisco updates its testing with best-practices guidelines as well as topologies and configurations provided by customers deploying the Cisco Catalyst 6500 Series in their environment. Test results are unique to technologies covered and actual scenarios in which they were tested.

Table 1. Testing Scope—Primary Coverage Areas

Layer 2: Channeling, Unidirectional Link Detection Protocol (UDLD), VLAN Trunking, **802.1x,** Spanning Tree Protocol	**Layer 3 Routing:** Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Hot Standby Router Protocol (HSRP), Multicast, Open Shortest Path First (OSPF), Recovery, Routing Information Protocol (RIP), Cisco Express Forwarding, NAT	**Traffic Management:** Load balancing, Maps, "Stickiness"
Network Management: Authentication, Authorization, and Accounting **(AAA),** SNMP, TACACS, Syslog	QoS	**Health and Redundancy:** Adaptive Session Redundancy (ASR), Box-to-Box, Keepalive Intervals, Resets
Web Cache Communication Protocol (WCCP)	Jumbo Frame	NetFlow Data Export (NDE)
Dynamic Host Configuration Protocol (DHCP)	Switched Port Analyzer **(SPAN)**	User Datagram Protocol (UDP)
Memory Leaks	Software Upgrades	Security: **NAC,** SSH, ACLs
Parser (command line-interface)	**High Availability,** NSF/SSO	Network Time Protocol (NTP)



Testing Results

Safe Harbor test documentation stipulates that the tests either pass, pass with exception, or fail. Testing schedules are based on code quality, not a date target.

- **Pass:** The underlying assumption for certifying and publishing a Safe Harbor release is that testing passed, because all individual tests passed. Failure of any test has to be properly resolved, closed, or determined by the Safe Harbor engineering team to be a non-impacting defect, and noted as such in the test results.
- **Fail:** If a given test fails, and the impact on Cisco's financial customer base is decided to be broad enough, the entire release fails. Failed releases will not be certified or documented. If a test fails, and the impact to the financial customer base is identified to be minor, the release may still be certified, with DDTSs noted so that customers can review the testing to see if they are impacted.
- **Pass with Exception:** Exceptions to any given test are noted for disclosure purposes and clarification. Customers are advised to carefully review selected tests, by test suite and feature, particular to their environment.

Testing Methods

Safe Harbor certification is based on a range of tests including: Functionality tests to verify feature functionality, Regression tests to validate existing features and verify that functionality is maintained, and Negative tests to stress the features and their interoperability.

During testing, the network is placed under load that is consistent with traffic in a live network. Network testing includes a combination of automated and manual tests. Simple Network Management Protocol (SNMP) is used to poll the network during the tests and all tests are analyzed. Safe Harbor testing does not address issues that might exist in the customer change-control and operations processes.

205377.BL_ETMG_CC_11.05