GUIDANCE NOTES
GD029-2025

CHINA CLASSIFICATION SOCIETY

GUIDELINES FOR INSPECTION OF SHIP NETWORK SWITCHES

2025

Effective from December 1, 2025

Beijing

CONTENTS

CHAPTER 1 GENERAL

Section1 GENERAL PROVISIONS

1.1.1 General Requirements

1.1.1.1 This guideline stipulates the technical requirements and product inspection requirements for ship network switches. It is applicable to ship core switches, and other ship network switches may follow this guideline by reference.

1.1.1.2 Ship network switches are categorized by application scenarios into core switches and CBS switches used within Computer-Based Systems (CBS), etc. Typical application scenario examples are shown in Figure 1.1.1.2.

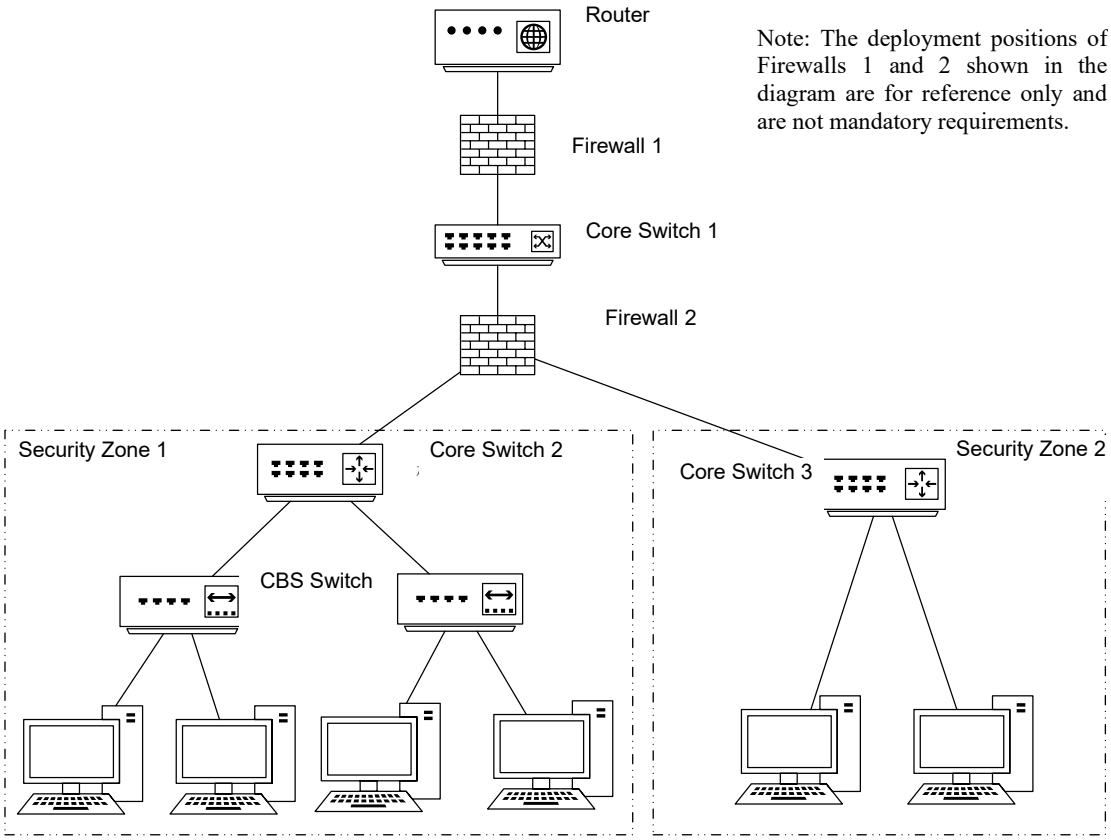

Figure 1.1.1.2 Examples of Ship Network Switch Application Scenarios

1.1.1.3 Switches used for 460 networks shall meet the relevant requirements of IEC 61162-460.

1.1.1.4 Ship network switches are classified into three levels based on technical capabilities and compliance requirements:

Level of Ship Network Switches **Table 1.1.1.4**

No.	Level	Technical requirements	Scope
1	Level 1	Meets SL0 requirements of the Guidelines for Ship Cyber Security and applicable requirements in Chapter 2 of this guideline.	SL0-class ships and CBS.
2	Level 2	Meets SL2 requirements of the Guidelines for Ship Cyber Security and applicable	SL1-SL2 class ships and CBS.

No.	Level	Technical requirements	Scope
		requirements in Chapter 2 of this guideline.	
3	Level 3	Meets SL4 requirements of the Guidelines for Ship Cyber Security and applicable requirements in Chapter 2 of this guideline.	SL3-SL4 class ships and CBS.

Note: Higher-level switches are compatible with application scenarios of lower-level switches.

1.1.1.5 Ship network core switches shall meet the corresponding requirements according to Table 1.1.1.5.

Ship Network Switch Requirement Correspondence **Table 1.1.1.5**

No.	Requirements	Core Switch (Layer 3)	Core Switch (Layer 2)	CBS Switch
1	2.2.1 Electrical Interfaces	√	√	√
2	2.2.2 Optical Interfaces	○	○	○
3	2.2.3 Prohibition of Wireless Access	√	√	○
4	2.2.4 PoE Interface	○	○	○
5	2.3.1.1 Networking	√	√	√
6	2.3.1.2 Redundancy	√	√	○
7	2.3.1.3 Cascading	√	√	○
8	2.3.2.1 VLAN Segmentation	√	√	√
9	2.3.2.2 Forwarding and Filtering	√	√	√
10	2.3.2.3 Network Storm Suppression	√	√	√
11	2.3.2.4 Multicast	√	√	√
12	2.3.2.5 Port Mirroring	√	√	○
13	2.3.3.1 Network Layer Protocol Support	√	○	○
14	2.3.3.2 Routing and Forwarding	√	○	○
15	2.3.3.3 Access Control List (ACL)	√	○	○
16	2.3.3.4 Address Resolution Protocol (ARP)	√	○	○
17	2.3.3.5 Network Layer Multicast	√	○	○
18	2.3.4.1 Out-of-band Management Interface	√	○	○
19	2.3.4.2 In-band Management Interface	√	√	√
20	2.3.4.3 Clock Synchronization Interface	√	√	√
21	2.3.4.4 Log and Alarm Interface	√	√	√
22	2.3.5 Management Functions	√	√	√
23	2.4 Device Security Requirements	Meets corresponding level requirements in		

No.	Requirements	Core Switch (Layer 3)	Core Switch (Layer 2)	CBS Switch
		accordance with Section 2.4 of this guideline.		
24	2.5 Performance Requirements	√	√	√

Note:√ indicates applicable; ○ indicates optional.

1.1.2 Certification Requirements

1.1.2.1 ship network core switches shall obtain a Type Approval Certificate. For network switches used in other scenarios, applications may be submitted on a voluntary basis.

1.1.2.2 CBS switches may obtain a Type Approval Certificate in accordance with this guideline, or jointly meet the requirements of Chapter 2 of the Guidelines for Ship Cyber Security as a component of the CBS. When a CBS switch obtains a Type Approval Certificate in accordance with this guideline, it shall meet at least the corresponding requirements specified in Table 1.1.1.5.

1.1.3 Change management

1.1.3.1 For ship network switches approved/inspected by CCS, the applicant shall notify CCS of any major changes to software or equipment components (including but not limited to major software version upgrades, changes in functions or performance, modifications to operational processes, or changes in equipment components). CCS may require a re-evaluation to ensure compliance with relevant technical requirements.

1.1.4 Terms and Abbreviations

1.1.4.1 Terms and definitions in the Guidelines for Ship Cyber Security are applicable to this guideline. Additional terms and definitions for this document are as follows:

(1) Switch: A device that uses internal switching mechanisms to provide connectivity between networked devices, where switching technologies are typically implemented at Layer 2 or Layer 3 of the Open Systems Interconnection (OSI) reference model.

(2) Ship Network Core Switch: A switch in the ship network that realizes ship data exchange across security zones and/or connects the ship network with the Internet, including Layer 2 switches and Layer 3 switches.

Note 1: A Layer 2 switch works at Layer 1-2 of the OSI reference model. It determines the egress of the data packet based on the MAC address in the received data packet and the MAC address table maintained inside the switch, and forwards the data.

Note 2: Layer 3 Switch refers to an Ethernet switch with routing functions that operates at Layers 1-3 of the OSI Reference Model. It determines the output port and the next-hop switch address or host address based on the network layer address in the received data packets and the routing table maintained within the switch, and rewrites the packet headers.

(3) CBS Switch (Switch for CBS): Refers to a switch applied within the same security zone of a ship, or within a shipboard CBS.

(4) 460-Network: A network that meets the relevant requirements of IEC 61162-460.

(5) Packet Forwarding Rate: The number of minimum-length data packets that a switch can forward per unit of time.

(6) Access Control List (ACL): A table of entities with access control permissions, which are granted for accessing a specific resource.

(7) Out-of-band Management Interface: A switch interface that can only be used as a management interface and not as a business data interface.

(8) In-band Management Interface: A switch interface that can be used both as a data interface for business data transmission and as a management interface.

(9) Throughput: The maximum transmission rate a switch can achieve without frame loss (Unit: bit/s).

(10) Latency: For store-and-forward devices, the time interval from the moment the last bit of an input data packet arrives at the input port until the first bit of the packet is output on the output port. For cut-through devices, the time interval from the moment the first bit of an input data packet arrives at the input port until the first bit of the packet is output on the output port.

(11) Latency Jitter: The difference between the measured latency value and the average value.

1.1.4.2 The terms and definitions in the Guidelines for Ship Cyber Security are applicable to this guideline. Additional abbreviations for this document are as follows:

(1) ARP: Address Resolution Protocol

(2) BPDU: Bridge Protocol Data Unit

(3) ERPS: Ethernet Ring Protection Switching

(4) IGMP: Internet Group Management Protocol

(5) MAC: Media Access Control

(6) MRP: Media Redundancy Protocol

(7) PoE: Power over Ethernet

(8) VLAN: Virtual Local Area Network

1.1.5 Normative References

The clauses in the relevant documents become provisions of this document through reference. For undated references, the latest edition of the referenced document applies to this document.

1.1.5.1 CCS Rules for Classification of Sea-going Steel Ships and its amendments

1.1.5.2 CCS Guidelines for Ship Cyber Security

1.1.5.3 IACS UR E26 Cyber resilience of ships

1.1.5.4 IACS UR E27 Cyber resilience of on-board systems and equipment

1.1.5.5 IEC 62443 series: Security for industrial automation and control systems

1.1.5.6 IEC 61162-460: Maritime navigation and radio communication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security

1.1.5.7 RFC 2544: Benchmarking Methodology for Network Interconnect Devices

CHAPTER 2 SHIP NETWORK SWITCH REQUIREMENTS

Section 1 GENERAL PROVISIONS

2.1.1 General Requirements

2.1.1.1 This chapter primarily describes the technical requirements for ship network switches, including physical interface requirements, functional requirements, device security requirements, and performance requirements.

2.1.1.2 Logs and other data generated by ship network switches shall meet the relevant requirements of Appendix 8 of the CCS Guidelines for Quality Assessment of Ship Data.

2.1.1.3 Ship network switches shall be capable of reliable operation under the environmental and working conditions required for computer systems specified in Chapter 2, Part 7 of the CCS Rules for Classification of Sea-going Steel Ships.

Section 2 PHYSICAL INTERFACES

2.2.1 Electrical Interfaces

2.2.1.1 Electrical interfaces shall comply with and be compatible with the 10BASE-T, 100BASE-TX, 1000BASE-T, or 10GBASE-T specifications defined in the IEEE 802.3 series standards.

2.2.2 Optical Interfaces

2.2.2.1 Optical interfaces shall comply with the 1000M or 10G optical interface requirements defined in the IEEE 802.3 series standards, and should preferably be compatible with the 100BASE-FX specification defined in IEEE 802.3.

2.2.3 Prohibition of Wireless Access

2.2.3.1 Wireless access shall be prohibited for ship network core switches.

2.2.4 PoE Power Supply

2.2.4.1 PoE power supply should be supported. Interfaces supporting PoE power supply shall meet the requirements of standards such as IEEE 802.3at, IEEE 802.3af, or IEEE 802.3bt, and the total power supply capacity shall be specified.

Section 3 FUNCTIONAL REQUIREMENTS

2.3.1 Networking and Deployment

2.3.1.1 Networking

The switch shall be capable of networking using international standard protocols and support linear, star, or ring topologies.

2.3.1.2 Redundancy

Redundant networking methods should be supported, such as link aggregation (complying with standards such as IEEE 802.1AX), device stacking, or ring networking (complying with standard protocols such as ERPS or MRP).

2.3.1.3 Cascading

Cascading connections shall be supported, and cascading via optical interfaces is preferred.

2.3.2 Data Link Layer Functional Requirements

2.3.2.1 VLAN Segmentation

Virtual Local Area Network (VLAN) functions complying with IEEE 802.1Q shall be supported, including support for VLAN identification within the forwarded data frame structure.

2.3.2.2 Forwarding and Filtering

Data frame forwarding and filtering functions based on MAC address table entries shall be supported.

2.3.2.3 Network Storm Suppression

(1) Network storm suppression shall be supported. Unexpected data traffic shall be suppressed by setting traffic thresholds for unicast, multicast, and broadcast packets from known and/or unknown sources in the ingress and/or egress directions of each port;

(2) For switch ports with MAC address forwarding enabled, the configuration of Spanning Tree Protocols (STP) complying with international standards shall be supported to prevent network storms from consuming excessive switch resources. The system shall support disabling the Spanning Tree Protocol or enabling functions such as Root Guard and BPDU Guard to protect against attacks targeting the protocol.

2.3.2.4 Multicast

Multicast functions shall be supported to avoid network congestion:

(1) Static multicast shall be supported, with the capability to manually configure multicast MAC address entries to achieve static binding between ports and multicast MAC addresses;

(2) Dynamic multicast based on IGMP snooping complying with RFC 4541 shall be supported, and compatibility with IGMPv2 and IGMPv3 shall be maintained to mitigate DoS risks.

2.3.2.5 Port Mirroring

Port mirroring shall be supported to enable monitoring of specified data traffic, meeting the following requirements:

(1) Mirroring of traffic from multiple ports to a monitoring port shall be supported, and the number of monitoring port configurations shall meet actual application requirements;

(2) When the data rate of the mirrored port does not exceed the port forwarding rate, no frame loss, frame disorder, or frame duplication shall occur.

2.3.3 Network Layer Functional Requirements

2.3.3.1 Network Layer Protocol Support

Ship network switches with routing functions shall:

(1) Support the IPv4 protocol, including subnetting and IP broadcasting functions;

(2) Support the ARP protocol;

(3) Support the ICMPv4 protocol;

(4) Support the ICMP Router Discovery Protocol (IRDP);

(5) Support the DHCP protocol.

2.3.3.2 Routing and Forwarding

Routing and forwarding functions shall be supported. The routing table shall be established through static route configuration or dynamic routing protocols (e.g., OSPF, RIP, etc.). Specific security requirements for routing control protocols are as follows:

(1) Communication protocol robustness requirements shall be met to protect against abnormal packet attacks;

(2) Non-cleartext route authentication (e.g., SHA-HMAC authentication) shall be supported.

2.3.3.3 Access Control List (ACL)

Packet filtering based on Access Control Lists (ACLs) shall be supported, with data flow control based on the following rules:

(1) ACL functions based on source and destination IP addresses shall be supported;

(2) For switch ports with MAC address forwarding enabled, ACL functions based on source and

destination MAC addresses shall be supported;

(3) Access control based on source and destination ports shall be supported;

(4) ACL functions based on VLANs shall be supported;

(5) ACL functions based on protocol types shall be supported;

(6) User-defined security policies shall be supported, which may consist of partial or full combinations based on MAC address, IP address, port, VLAN, protocol type, etc.

2.3.3.4 Network Layer Multicast

Network layer multicast functions shall be provided. The IGMP protocol shall be supported, with compatibility for IGMPv2 and IGMPv3 to mitigate DoS risks.

2.3.4 Interface Functions

2.3.4.1 Out-of-band Management Interface

At least one out-of-band management interface shall be configured.

2.3.4.2 In-band Management Interface

Device management via data ports shall be supported.

2.3.4.3 Clock Synchronization Interface

It is advisable to have an input interface for clock synchronization information. At least time synchronization using protocols such as NTP shall be supported.

2.3.4.4 Log and Alarm Interface

(1) Output interfaces for logs and alarm information shall be provided;

(2) The output of switch logs via the syslog protocol shall be supported as a minimum;

(3) Local alarm output functions shall be supported. Alarm content shall at least include common faults such as: power loss, network storm, port disconnection, port connection, redundant network fault recovery, user authentication limit exceeded, authorization failure, abnormal traffic, and ring network failure;

(4) Remote alarm functions based on SNMP and/or SMTP shall be supported for the transmission of alarm information.

2.3.5 Management Functions

2.3.5.1 Local management shall be supported.

2.3.5.2 The establishment of secure communication channels with management terminals shall be supported. Communication data for remote management shall be transmitted in non-plaintext.

2.3.5.3 The enabling and disabling of various business functions, as well as parameter settings, shall be supported. Configuration management shall be available for the following functions: multicast, spanning tree, VLAN, port mirroring, link aggregation, network storm suppression, system clock, redundant network, routing, user permissions, and ACLs.

2.3.5.4 Uploading and downloading of device configurations shall be supported.

2.3.5.5 Restoration to factory settings shall be possible.

2.3.5.6 After restarting from a shutdown under abnormal conditions (e.g., fault, abnormal power loss, forced shutdown), the following requirements shall be met:

(1) Configurations shall be restorable to the normal state prior to shutdown;

(2) Log information shall be preserved normally;

(3) Users shall undergo re-authentication.

2.3.5.7 Capabilities for fault tolerance, error correction, and error isolation shall be provided. In the event of incorrect operations or the input of unreasonable data, information prompts shall be

provided, and the system shall remain capable of effective operation.

2.3.5.8 Statistical functions shall be supported. Statistical information shall at least include: device resource utilization, bandwidth utilization, number of packets forwarded per port, and number of dropped packets.

Section 4 DEVICE SECURITY REQUIREMENTS

2.4.1 General Requirements

2.4.1.1 Corresponding security capability requirements in Chapter 2 of the Guidelines for Ship Cyber Security shall be met according to the classification in Section 1.1.1.4.

2.4.1.2 The capability to generate security-related auditable records shall be provided, with requirements as follows:

(1) Event types to be recorded:

① Attempts to access management ports of the ship network switch and management authentication requests;

② All configuration operations on the ship network switch system, including but not limited to adding/deleting accounts, modifying authentication information, changing critical configurations, and modifying user permissions;

③ Backups of log information;

④ Significant security events;

⑤ Restarting or shutting down the device;

⑥ Other events defined by security policies that require recording.

(2) Management of auditable records:

① Audit information such as records, logs, reports, settings, and tools shall be protected against unauthorized access and tampering;

② Tools for reviewing logs shall be provided, which can retrieve audit events based on conditions such as time, date, subject identity, and object identity;

③ Management logs (showing management activities) and event logs (showing traffic activities) shall support writing to backup storage for periodic review;

④ Defining different types of system events and setting log levels shall be supported;

⑤ Synchronizing logs, alarms, and other information to a log server via the SYSLOG protocol shall be supported;

⑥ Log storage shall support preservation in non-volatile storage media, with alarms issued when thresholds are reached.

2.4.2 Secure Development

2.4.2.1 The requirements in Section 2.4 of the Guidelines for Ship Cyber Security shall be met, along with the following supplementary requirements:

2.4.2.2 Developers shall identify at least the following security risks during the device development phase and formulate corresponding security policies:

(1) Security risks in the development environment;

(2) Security risks introduced by third-party components, firmware, or software;

(3) Security risks caused by development personnel.

2.4.2.3 Operating procedures for secure device development shall be established to ensure the implementation of security policies.

2.4.2.4 A configuration management procedure and a corresponding list of configuration items shall be established. The configuration management system shall be capable of synchronizing with change content and providing authorization and control for changes.

2.4.2.5 Measures shall be taken to prevent the implantation of malicious programs into the device.

2.4.2.6 Measures shall be taken to prevent the setting of undeclared interfaces or functional modules on the device.

2.4.2.7 Vulnerability scanning, code auditing, and robustness testing shall be employed for security testing of the device.

2.4.2.8 Ship network switches shall meet the following requirements for vulnerability and malware prevention upon delivery:

(1) No published medium-to-high risk security vulnerabilities shall exist, or remedial measures shall be available to prevent security risks associated with such vulnerabilities;

(2) Pre-installed software, patch packages, and upgrade packages shall not contain malware;

(3) No undeclared functions or access interfaces (including remote debugging interfaces) shall exist.

2.4.3 Secure Operation and Maintenance (O&M)

2.4.3.1 Manufacturers of ship network switches shall develop guidance documents for operations such as installation, upgrades, and maintenance. If remote maintenance is supported, it shall meet the requirements of Article 4.3.16 of the CCS Guidelines for Ship Cyber Security.

2.4.3.2 Emergency response mechanisms and processes for device security incidents shall be established. Incident response and recovery plans shall be formulated with reference to the requirements of Articles 4.3.21 and 4.3.22 of the CCS Guidelines for Ship Cyber Security.

2.4.3.3 Backup and recovery functions for pre-installed software and configuration files shall be supported. Integrity checks for pre-installed software and configuration files shall be supported when using the recovery function.

2.4.3.4 Methods for irreversible destruction of data in decommissioned equipment shall be provided.

Section 5 PERFORMANCE REQUIREMENTS

2.5.1 General Requirements

2.5.1.1 The performance indicators of the data interfaces of ship network switches shall, at a minimum, comply with the relevant provisions of IEEE 802.3.

2.5.1.2 Under the specified test environment and basic configuration, performance parameters such as throughput, packet loss rate, and latency jitter shall meet the following requirements:

(1) Throughput

Device throughput shall be no less than the nominal value.

(2) Packet Loss Rate

The packet loss rate shall be 0 when the traffic does not exceed the throughput.

(3) Latency and Jitter

The per-device latency shall not exceed 10μs, and the per-device latency jitter (test data frame length: 64 bytes) shall not exceed 1μs.

CHAPTER 3 INSPECTION REQUIREMENTS

Section 1 DRAWINGS AND DOCUMENTATION

3.1.1 Documents

3.1.1.1 When applying for approval/inspection of ship network switches, documents shall be submitted to CCS in accordance with Table 3.1.1.1.

List of Documents **Table 3.1.1.1**

No.	Document Name	Details	Remarks
1	Technical Specifications	Clarify product models and specifications, functional and performance indicators, usage restrictions, protection ratings, power conditions, software-related information, etc.	Ⓐ
2	Technical Schematics	--	Ⓐ
3	Product Outline Drawings	External dimensions, protection ratings, interface types and quantities, indicator markings and colors, etc.	Ⓐ
4	Manuals (Chinese and English)	Product hardware and software versions, descriptions of relevant functions and performance, product specifications (such as interfaces and environmental conditions), as well as product operation, installation, maintenance, and use.	Ⓘ
5	Nameplates (Chinese and English)	--	Ⓘ
6	Security Capability Statement	Refer to the requirements of 3.1.3.2 of the Guidelines for Ship Cyber Security.	Ⓐ
7	Security Configuration Guide	This document shall specify recommended configurations and default values for security functions. The objective is to ensure that the implementation of security functions complies with UR E26 and all specifications of the system integrator (e.g., user accounts, authorization, password policies, device security status, policies, etc.).	Ⓘ
8	Software Quality Plan	Clarify that the quality management system is applicable to the design, construction, delivery, and maintenance of the specific system to be delivered; clarify the method for unique identification of the system, its various software modules, and different versions of the same software module throughout the system and software lifecycle.	Ⓘ
9	Change Management Procedure	Clarify the control procedures for the initial installation and subsequent updates of system software modules and cyber security configurations.	Ⓘ
10	Security Development Lifecycle Documentation	Refer to Section 4, Chapter 2 of the Guidelines for Ship Cyber Security.	Ⓐ
11	Maintenance and Verification Plan	Maintenance content, verification methods, records, etc.	Ⓘ

No.	Document Name	Details	Remarks
12	Incident Response and Recovery Plan	Formulate plans for response, backup, recovery, etc.	Ⓘ
13	Configuration Check Report	Refer to the requirements of 3.1.3.2 of the Guidelines for Ship Cyber Security.	Ⓘ
14	Test Procedure	Covers environmental tests and network tests, including test objects, standards, methods, processes, etc.	Ⓐ

Note: Ⓐ For approval; Ⓘ For reference.

Section 2 TEST AND VERIFICATION

3.2.1 General Requirements

3.2.1.1 When applying for type approval of ship network switches, relevant tests shall be conducted based on computer systems in the CCS Guidelines for Type Approval Test of Electric and Electronic Products, with the following requirements:

(1) Type tests shall be conducted in a CCS cyber security laboratory or a CCS-recognized laboratory according to the cyber security type test outline approved by CCS;

(2) Type tests for all applicable requirements shall be completed in accordance with Section 3.2 of this guideline;

(3) Vulnerability scanning shall be performed during on-site tests. The manufacturer shall complete code auditing and robustness testing and provide reports for on-site review.

3.2.2 Test Preparation

3.2.2.1 Manufacturers shall formulate a type test outline for ship network switches in accordance with the requirements of Chapter 2. The test content shall cover hardware, functions, performance, and security testing of the switches, describing the correspondence between test items identified in the test documentation and the technical requirements of the ship network switch.

3.2.2.2 Before testing, the equipment under test (EUT) must complete configuration according to the configuration guide provided to users. All supported protocols shall be configured and enabled, and no modification to the configurations shall be made during the test process.

3.2.2.3 Test instruments[①] are generally connected to the service interfaces of the device to simulate the transmission of data packets. Security testing tools are generally connected to the service or management interfaces of the device to perform security tests such as vulnerability scanning and port scanning. Management terminals are generally connected to the management interface of the device for configuration management of the EUT.

3.2.2.4 The verification environments for the functions, security, and performance of ship network switches are shown in Figures 3.2.2.4(1) to (4).

[①]Note: Test instruments shall be calibrated in accordance with relevant national or international standards and be traceable.

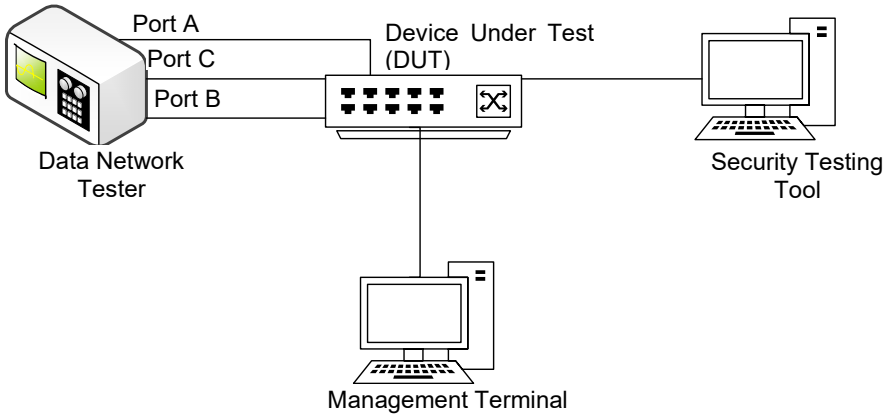

Figure 3.2.2.4(1) Test Environment 1

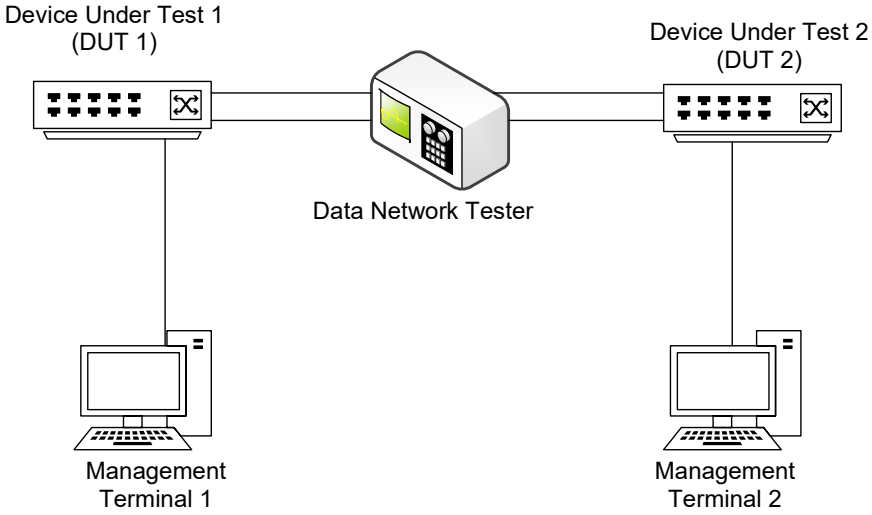

Figure 3.2.2.4(2) Test Environment 2

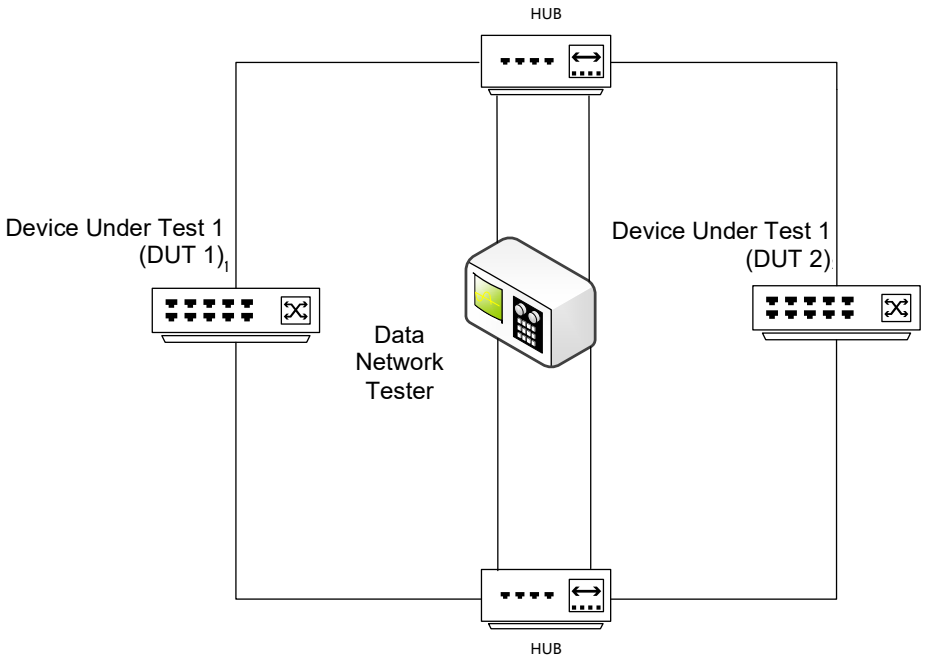

Figure 3.2.2.4(3) Test Environment 3

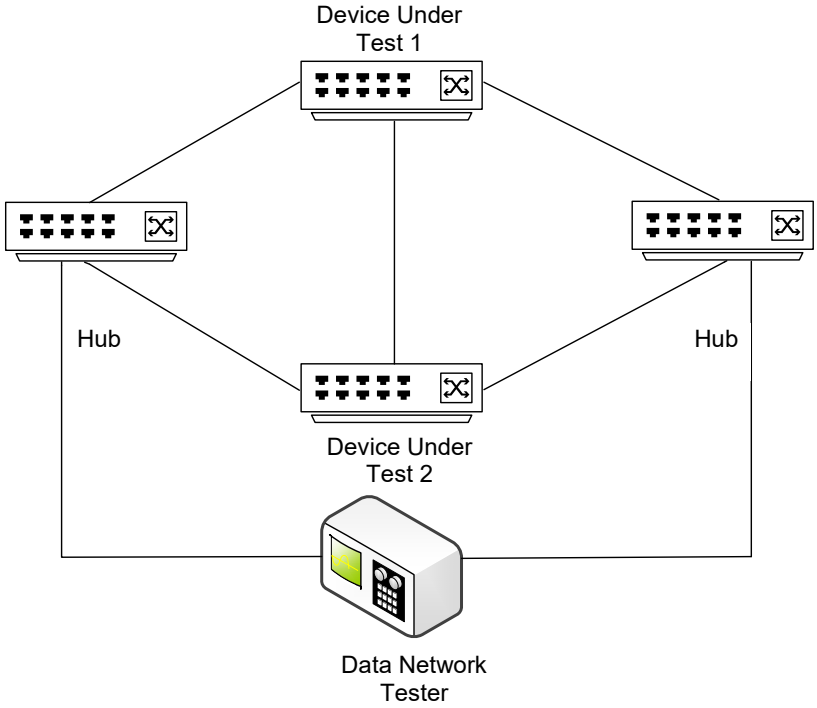

Figure 3.2.2.4(4) Test Environment 4

3.2.3 Interface Testing

3.2.3.1 With reference to the product manual, verify that the interface types and quantities conform to the specified requirements.

3.2.3.2 Test the communication connection status and functional integrity of corresponding interfaces with reference to given data interface protocol standards/descriptions and interface functional specifications.

3.2.3.3 Review documentation and switch configurations to verify that wireless access is prohibited.

3.2.3.4 If PoE power supply is supported, verify compliance with the standard requirements described in 2.2.4 and verify that the power supply meets the nominal value.

3.2.4 Functional Verification

3.2.4.1 Corresponding functional verification shall be conducted in accordance with Table 1.1.1.4. For verification environments and technical requirements, refer to Table 3.2.4.1.

Verification Environments and Technical Requirements **Table 3.2.4.1**

No.	Verification Item	Verification Environment	Technical requirements
1	Networking	Figure 3.2.2.4(4)	2.3.1.1
2	Redundancy	Figures 3.2.2.4(1) and (4)	2.3.1.2
3	Cascading	Figure 3.2.2.4(4)	2.3.1.3
4	VLAN Segmentation	Figure 3.2.2.4(1)	2.3.2.1
5	Forwarding and Filtering	Figure 3.2.2.4(1)	2.3.2.2
6	Network Storm Suppression	Figures 3.2.2.4(2) and (3)	2.3.2.3
7	Multicast (Data Link Layer)	Figure 3.2.2.4(1)	2.3.2.4
8	Port Mirroring	Figure 3.2.2.4(1)	2.3.2.5
9	Network Layer Protocol Support	Figure 3.2.2.4(1)	2.3.3.1

No.	Verification Item	Verification Environment	Technical requirements
10	Routing and Forwarding	Figure 3.2.2.4(1)	2.3.3.2
11	Access Control List (ACL)	Figure 3.2.2.4(1)	2.3.3.3
12	Address Resolution	Figure 3.2.2.4(1)	2.3.3.4
13	Multicast (Network Layer)	Figure 3.2.2.4(1)	2.3.3.5
14	Out-of-band Management	Figure 3.2.2.4(1)	2.3.4.1
15	In-band Management	Figure 3.2.2.4(1)	2.3.4.2
16	Clock Synchronization Interface	Figure 3.2.2.4(3)	2.3.4.3
17	Log and Alarm Interface	Figure 3.2.2.4(1)	2.3.4.4
18	Management Functions	Figure 3.2.2.4(1)	2.3.5

3.2.5 Security Verification

3.2.5.1 Security verification shall be conducted in accordance with Table 1.1.1.4. For verification environments and relevant requirements, refer to Table 3.2.5.1.

Security Verification Environments and Technical Requirements Table 3.2.5.1

No.	Verification Item	Verification Environment	Technical requirements
1	Identification and Authentication	Figure 3.2.2.4(1)	Guidelines for Ship Cyber Security, 2.3.1.1
2	Use control	Figure 3.2.2.4(1)	Guidelines for Ship Cyber Security, 2.3.1.2 Section 2.4.1.2 of this guideline
3	System Integrity	Figure 3.2.2.4(1)	Guidelines for Ship Cyber Security, 2.3.1.3
4	Data confidentiality	Figure 3.2.2.4(1)	Guidelines for Ship Cyber Security, 2.3.1.4
5	Restricted data flow	Figure 3.2.2.4(1)	Guidelines for Ship Cyber Security, 2.3.1.5
6	Timely Response to Events	Figure 3.2.2.4(1)	Guidelines for Ship Cyber Security, 2.3.1.6
7	Resource availability	Figure 3.2.2.4(1)	Guidelines for Ship Cyber Security, 2.3.1.7
8	Additional Security Requirements for Network Devices	Figure 3.2.2.4(1)	Guidelines for Ship Cyber Security, 2.3.2.1
9	Secure Development	-	Section 2.4.2 of this guideline
10	Secure Operation and Maintenance (O&M)	Figure 3.2.2.4(1)	Section 2.4.3 of this guideline

3.2.6 Performance Testing

3.2.6.1 Performance testing is generally based on Test Environment 1. With reference to RFC 2544, a traffic generator is used to send data packets of different frame lengths to the EUT. The throughput, latency and jitter, and packet loss rate of the ship network switch are tested to verify compliance with the requirements of Section 2.5 of this guideline.

(1) Throughput

① The test shall include data packets with frame lengths of at least 64, 128, 256, 512, and 1518 bytes;

② Report output form: Results shall be represented in the form of tables or charts, identifying tested values under different frame lengths and loads.

(2) Latency and Jitter

① The test shall include data packets with frame lengths of at least 64, 128, 256, 512, and 1518 bytes;

② Report output form: Results shall be represented in the form of tables, identifying the minimum, average, and maximum latency under different frame lengths and loads.

(3) Packet Loss Rate

① The test shall include data packets with frame lengths of at least 64, 128, 256, 512, and 1518 bytes;

② Report output form: Results shall be represented in the form of tables, identifying the packet loss rate under different frame lengths and loads.