指导性文件
GUIDANCE NOTES
GDXX

中　国　船　级　社

船舶网络交换机检验指南

（初稿）

2025

生效日期：2025 年 X 月 X 日

北京

目　　录

第 1 章 通则

第 1 节 一般规定

1.1.1 一般要求

1.1.1.1 本指南提出了船舶网络交换机的技术要求和产品检验要求，适用于申请中国船级社（China Classification Society, CCS）产品认可或检验的船舶网络交换机设备，包括实现网络数据交换的其它设备。

1.1.1.2 船舶网络交换机根据使用场景可分为核心交换机、接入交换机，以及在船舶计算机系统内部使用的 CBS 交换机。应用场景示例如下图 1.1.1.2 所示。

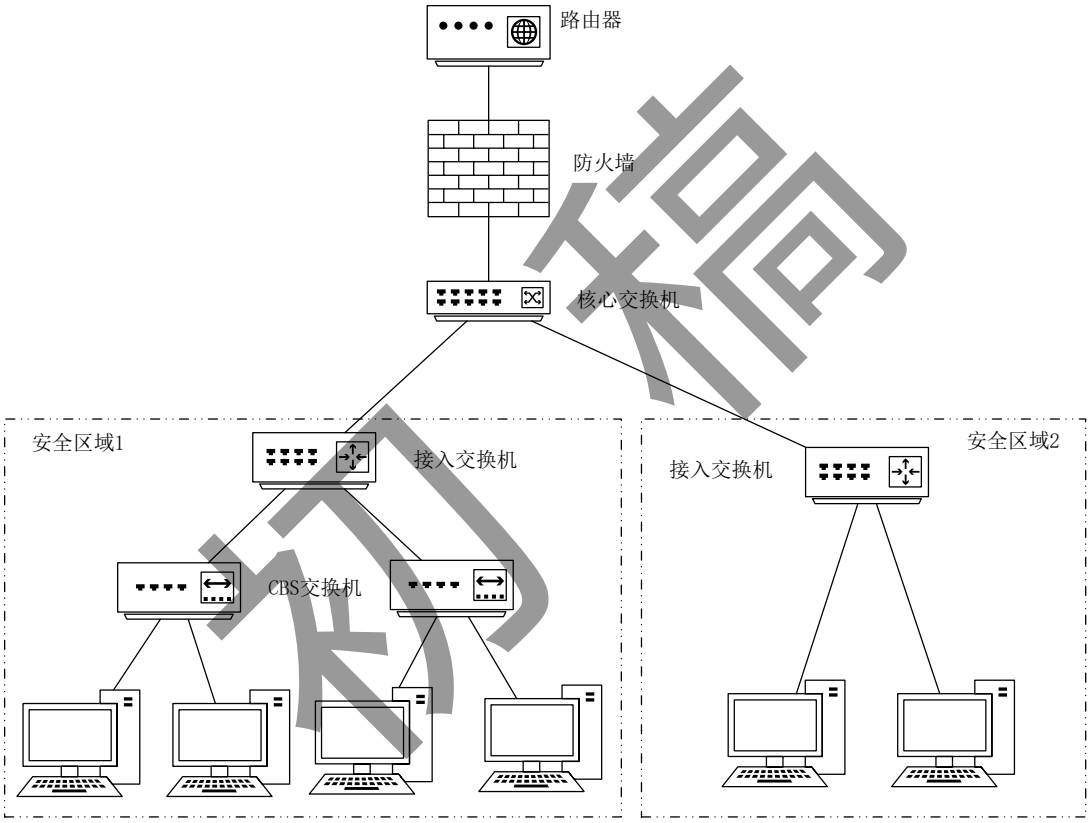

图 1.1.1.2 船舶网络交换机使用场景示例

1.1.1.3 船舶网络核心交换机系指船舶网络中实现船舶数据跨安全区域交换以及与船舶外互联网连通的数据交换设备。

1.1.1.4 船舶网络接入交换机系指船舶网络安全区域边界的网络数据交换设备。

1.1.1.5 船舶网络交换机分为 3 个级别：

船舶网络交换机分级表 **表 1.1.1.5**

序号	级别	防御能力
1	I	设备安全能力满足《船舶网络安全指南》 SL0 要求
2	II	设备安全能力满足《船舶网络安全指南》 SL1、SL2 要求
3	III	设备安全能力满足《船舶网络安全指南》 SL3、SL4 要求

1.1.2 持证要求

1.1.2.1 使用于船舶网络的核心交换机、接入交换机或含有交换功能的网络设备，应向CCS 提出申请，按照本指南要求在 CCS 或 CCS 认可/接受的试验机构进行测试验证，并按CCS《钢质海船入级规范》第 1 篇第 3 章要求完成型式认可。对于在船舶计算机系统内部使用的 CBS 交换机可自愿申请，参照本指南实施。

1.1.3 数据提供与保密

1.1.3.1 CCS 对申请方提交的数据和信息按 CCS《钢质海船入级规范》第 1 篇第 2 章第12 节的要求进行信息披露，知识产权及保密原则遵循 CCS《钢质海船入级规范》第 1 篇第2 章第 1 节 3.1.10 的要求。

1.1.4 变更管理

1.1.4.1 对于通过 CCS 认可/检验的船舶网络交换机，当其软件、设备部件等发生重要变更（包括但不限于软件版本重大升级，功能、性能的改变，操作流程的改变，设备部件的变更）时，申请方应通知 CCS，CCS 可要求重新评估，以确保其满足相关的技术要求。

1.1.5 规范性引用文件

1.1.5.1 相关文件中的条款通过本文件的引用将成为本文件的条款。凡是不注日期的引用文件，其最新版本适用于本文件。

引用文件列表　　表 1.1.5.1

序号	编号	文件名
1	R001-2025	《钢质海船入级规范》
2	GDXX-2025	《船舶网络安全指南》
3	GD008-2025	《船用软件安全及可靠性评估指南》
4	GD019-2024	《电气电子产品型式认可试验指南》
5	IACS UR E27 Rev.1	*Cyber resilience of on-board systems and equipment*
6	IEC 62443-1-1	*Industrial communication networks-network and system security-part 1-1: terminology, concepts and models*
7	IEC 62443-4-2	*Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components*
8	ISO/IEC 27033-4	*Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*
9	ISO/IEC 15408-2	*Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*
10	IEC 63154	*Maritime navigation and radiocommunication equipment and systems -Cybersecurity - General requirements, methods of testing and required test results*
11	IEC 61162-460	*Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security*
12	RFC 2544	*Benchmarking Methodology for Network Interconnect Devices*

1.1.6 术语及缩略语

1.1.6.1 本文件有关术语如下：

（1） 交换容量（Switching Capacity）：也称为背板带宽（Backplane Bandwidth）或交换带宽，是交换机内部接口处理器与数据总线之间所能吞吐的最大数据量，单位是 Gbps（吉比特每秒）或 bps（比特每秒）。它代表了交换机核心的数据交换能力。

（2） 包转发率（Packet Transfer Rate）：交换机单位时间内能够转发的最小长度数据

包的数量。

（3） 带外管理接口（Out-band Management Interface）：只能作为管理接口，不能作为业务数据接口的交换机接口。

（4） 带内管理接口（In-band Management Interface）：既可以作为数据接口用于业务数据收发，又可以作为管理接口的交换机接口。

（5） 吞吐量（Throughput）：交换机在不丢帧情况下所能达到的最大传输速率（单位：bit/s）。

（6） 时延（Latency）：对于存储转发设备，从输人数据包最后一个比特到达输入端口开始，至输出端口上输出该数据包的第一个比特为止的时间间隔。对于直通转发设备，从输入数据包第一个比特到达输入端口开始，至输出端口上输出该数据包的第一个比特为止的时间间隔。

（7） 时延抖动（Latency Jitter）：时延测量值与平均值的差值。

1.1.6.2 本文件缩略语如下：

（1） CBS：计算机系统（Computer Based System）

（2） VLAN：虚拟局域网（Virtual Local Area Network）

（3） ARP：地址解析协议（Address Resolution Protocol）

（4） PoE：以太网供电（Power over Ethernet）

（5） MAC：媒体访问控制（Media Access Control）

（6） ERPS：以太网环保护切换（Ethernet Ring Protection Switching）

（7） MRP：介质冗余协议（Media Redundancy Protocol）

（8） BPDU：网桥协议数据单元（Bridge Gateway Protocol）

（9） IGMP：互联网组管理协议（Internet Group Management Protocol）

（10） DoS：拒绝服务攻击（Denial of Service）

第 2 章 船舶网络交换机要求

第 1 节 一般规定

2.1.1 一般要求

2.1.1.1 本章主要描述船舶网络交换机的技术要求，包括接口要求、功能要求和设备安全要求和性能要求。

2.1.1.2 船舶网络交换机产生的日志等数据应满足船旗国相关法律法规要求以及 CCS《船舶网络安全指南》第 4.3.20 条和 CCS《船舶数据质量评估指南》附录 8 的相关要求。

2.1.1.3 日志等数据出境应满足船旗国、入境国和出境国相关法律法规要求。

第 2 节 接口要求

2.2.1 电接口

2.2.1.1 船舶网络交换机的 10/100M 电接口应符合并兼容 IEEE802.3:2008 规定的 10BASE-T 和 100BASE-TX 规范。10/100/1000M 电接口应符合并兼容 IEEE802.3:2008 规定的 10BASE-T、100BASE-TX 和 1000BASE-T 规范。

2.2.2 光接口

2.2.2.1 船舶网络交换机的 100M 光接口应符合 IEEE802.3:2008 规范。1000M 光接口应符合 IEEE802.3:2008 规范，宜兼容 IEEE802.3:2008 规定的 100BASE-FX 规范。10G 光接口应符合 IEEE 802.3ae 规范。

2.2.3 PoE 供电

2.2.3.1 宜支持 PoE 供电，支持的 PoE 供电的接口应满足 IEEE802.3at，IEEE802.3af 或 IEEE802.3bt 等标准要求，应明确供电总功率。

第 3 节 功能要求

2.3.1 组网与部署

2.3.1.1 组网

船舶网络交换机应能采用国际标准协议进行组网，支持线型、星型或环形拓扑结构。

2.3.1.2 冗余

宜支持冗余的组网方式，如链路聚合（IEEE 802.3ad 标准）、设备堆叠、环网（ERPS、MRP 协议等）。

2.3.1.3 级联

船舶网络交换机应支持级联连接，宜支持通过光接口进行级联。

2.3.2 数据链路层功能要求

2.3.2.1 VLAN 划分

船舶网络交换机应支持符合 IEEE802.1Q 规定的虚拟局域网（VLAN）功能，支持在转发的帧结构中进行标识。

2.3.2.2 转发和过滤

应支持基于 MAC 地址表项的数据帧转发和过滤功能。

2.3.2.3 网络风暴抑制

（1） 应支持网络风暴抑制功能，通过限定每个端口入或/和出方向的已知或/和未知源的单播、组播和广播数据包的流量带宽，抑制非预期的数据流量。

（2） 对于启用 MAC 地址转发的交换机端口，应支持配置符合 IEEE802.1D 规定的生成树协议，避免网络风暴大量占用交换机资源。支持关闭生成树协议，或支持启用 Root Guard、BPDU Guard 等功能，防范针对生成树协议的攻击。

2.3.2.4 组播

应支持组播功能，以避免网络拥塞：

（1） 应支持静态组播功能，至少能手动配置组播 MAC 地址表项，实现端口与组播 MAC 地址的静态绑定；

（2） 应支持基于符合 RFC 4541 的 IGMP snooping 的动态组播功能，并兼容 IGMPv2、IGMPv3 以降低 DoS 风险。

2.3.2.5 端口镜像

船舶网络核心交换机应支持端口镜像功能，应能对指定数据流量进行监控，并满足如下要求：

（1） 应支持多端口流量镜像到多个监控端口；

（2） 当镜像端口数据速率不大于端口转发速率时，不应出现帧丢失、帧乱序和帧复制现象。

2.3.3 网络层功能要求

2.3.3.1 路由转发

船舶网络交换机应支持路由转发功能，应能通过静态路由配置或通过动态路由协议（如 OSPF 等）建立路由表。路由控制协议具体安全要求如下：

（1） 应满足通信协议健壮性要求，以防范异常报文攻击；

（2） 应支持非明文路由认证（如 MD5 认证、SHA-HMAC 认证等）功能。

2.3.3.2 访问控制列表

船舶网络交换机应支持基于访问控制列表的报文过滤，并能依据以下规则进行数据流控制：

（1） 应支持基于源 IP 地址、目的 IP 地址的访问控制列表功能；

（2） 对于启用 MAC 地址转发的交换机端口，应支持基于源 MAC 地址、目的 MAC 地址的访问控制列表功能；

（3） 应支持基于源端口、目的端口的访问控制；

（4） 应支持基于 VLAN 的访问控制列表功能；

（5） 应支持基于协议类型的访问控制列表功能；

（6） 应支持用户自定义的安全策略，安全策略可以是基于 MAC 地址、IP 地址、端口、VLAN、协议类型的部分或全部组合。

2.3.3.3 地址解析协议（ARP）

应支持地址解析协议，应能通过静态 ARP 配置或通过 ARP 报文自动生成和维护 ARP 表项。

2.3.3.4 网络层组播

应具有网络层组播功能。应支持 IGMP 协议，并兼容 IGMPv2、IGMPv3，以降低 DoS 风险。

2.3.4 接口功能

2.3.4.1 带外管理接口

船舶网络交换机应配置至少一个带外管理接口。

2.3.4.2 带内管理接口

船舶网络交换机的数据端口宜能作为带内管理接口使用。

2.3.4.3 时钟同步接口

船舶网络交换机应具有时钟同步信息的输入接口，应至少支持使用 NTP 等协议实现时间同步。

2.3.4.4 日志和报警接口

（1） 船舶网络交换机应提供日志和报警信息输出接口。

（2） 应支持本地报警输出功能，报警内容应至少包括：电源失电、网络风暴、端口断线、端口连接、冗余网络故障恢复、用户认证次数超限、授权失败、异常流量。

（3） 核心交换机和接入交换机应支持基于 SNMP 或/和 SMTP(IETFRFC5321:2008)的远程报警功能，用于传送报警信息。

2.3.5 管理功能

2.3.5.1 船舶网络交换机至少应支持本地管理。

2.3.5.2 应支持与管理终端建立安全的通信信道，远程管理的通信数据应使用非明文传输。

2.3.5.3 船舶网络交换机应支持各项业务功能的启用和禁止，以及参数设置。

2.3.5.4 应支持设备配置的上传和下载。

2.3.5.5 应能恢复至出厂设置。

2.3.5.6 在非正常条件（如故障、异常掉电、强行关机等）关机再重新启动后，应满足如下要求：

（1） 配置应能恢复到关机前状态；

（2） 日志信息应正常保存；

（3） 用户应重新鉴别。

2.3.5.7 应具有容错、纠错和隔离错误的能力。当发生错误操作或输入不合理数据时, 应能进行信息提示并仍能有效运行。

2.3.5.8 应支持统计功能,统计信息至少应包括:设备资源利用率、带宽利用率、端口转发包数、丢弃包数。

第 4 节 设备安全能力要求

2.4.1 一般要求

2.4.1.1 船舶网络交换机应按照 1.1.1.5 节的分级满足《船舶网络安全指南》第 2 章相应的安全能力要求。

2.4.1.2 船舶网络交换机应能生成与安全相关的可审计记录，要求如下：

（1） 记录事件类型

①试图接入船舶网络交换机管理端口和管理身份鉴别请求；

②对船舶网络交换机系统所有配置操作，包括但不限于增/删账户，修改鉴别信息，修改关键配置，用户权限修改等；

③日志信息的备份等；

④重要安全事件；

⑤重启/关闭设备；

⑥其他应该记录的事件信息。

（2） 管理

①记录、日志、报告、设置和工具等审计信息应受到保护，防止未经授权的访问和篡改；

②应提供能查阅日志的工具，具备对审计事件以时间、日期、主体标识、客体标识等条件检索的能力；

③管理日志（显示管理活动）和事件日志（显示流量活动）应支持写入备用存储以备定期审查；

④日志应采用 SYSLOG 格式存储或兼容格式进行存储；

⑤应支持定义不同的系统事件类型，并设置日志级别；

⑥应至少保存一个检验周期的日志记录。

2.4.2 安全开发

2.4.2.1 船舶网络交换机开发者应至少在设备开发阶段对以下安全风险进行识别，并制定相应安全策略：

（1） 开发环境的安全风险；

（2） 第三方组件、固件或软件引入的安全风险；

（3） 开发人员导致的安全风险。

2.4.2.2 应建立设备安全开发操作规程，保障安全策略的落实。

2.4.2.3 应建立配置管理程序及相应配置项清单，配置管理系统应能与变更内容同步，并对变更进行授权和控制。

2.4.2.4 应采取措施防止设备被植入恶意程序。

2.4.2.5 应采取措施防范设备被设置未声明的接口或功能模块。

2.4.2.6 应采用漏洞扫描、代码审计、健壮性测试和渗透测试对设备进行安全性测试。

2.4.2.7 船舶网络交换机交付时应满足以下漏洞和恶意程序防范要求：

（1） 不应存在已公布的漏洞，或具备补救措施防范漏洞安全风险；

（2） 预装软件、补丁包/升级包不应存在恶意程序；

（3） 不应存在未声明的功能和访问接口（含远程调试接口）。

2.4.3 安全运维

2.4.3.1 船舶网络交换机提供者应制定安装、升级及维护等操作的指导性文件。如支持远程维护，应满足 CCS《船舶网络安全指南》第 4.3.16 条要求。

2.4.3.2 应建立针对设备安全事件的应急响应机制和流程，参照 CCS《船舶网络安全指南》第 4.3.21 条、第 4.3.22 条要求制定事件响应及恢复计划。

2.4.3.3 应支持对预装软件、配置文件的备份与恢复功能，使用恢复功能时支持对预装软件、配置文件的完整性检查。

2.4.3.4 应提供对退役设备中数据进行不可逆销毁的方法。

2.4.3.5 船舶网络交换机宜支持多种工作模式，保证船舶网络交换机在运行、维护过程中对其他系统的最小影响。

2.4.4 硬件和环境适应性

2.4.4.1 船舶网络交换机应能够适应船舶运行环境（高温、潮湿、振动等），能在中国船级社《钢质海船入级规范》第 7 篇第 2 章第 1 节的要求环境条件和工作条件下可靠地工作。

第 5 节 性能要求

2.5.1 一般要求

2.5.1.1 应标注船舶网络交换机的包转发率、交换容量。

2.5.1.2 应测量设备的吞吐量、丢包率、时延抖动等性能参数。

2.5.2 包转发率

2.5.2.1 船舶网络交换机的包转发率应满足如下要求：

整机包转发率 (Mpps) ≥ 端口数 × 相应端口速率的单端口包转发率

2.5.3 交换容量

2.5.3.1 船舶网络交换机交换容量应满足如下要求：

交换容量 ≥ 端口数量 × 端口速率 × 2

2.5.4 时延抖动

2.5.4.1 设备单机时延应小于等于 10 μs，单机时延抖动（测试数据帧长：64 字节）应小于等于 1 μs。

2.5.5 **组网性能**

2.5.5.1 组网性能应能符合下表的要求。

组网性能 **表 2.5.5.1**

项 目	指标	备注
网络时延	≤[10n+链路时延+测试数据包传输时间×(n—1)(μs)	—
网络时延抖动	≤n(μs)	—
丢包率	＜0.1%	流量不超过吞吐量
注：n 为网络中最长数据链路经过的交换机数量。		

第 3 章 检验要求

第 1 节 图纸资料

3.1.1 文件资料

3.1.1.1 申请船舶网络交换机认可/检验时，应根据表 3.1.1 向 CCS 提交所列资料。

资料清单表 **表 3.1.1.1**

序号	文件名称	说明	备注
1	技术规格书	阐明产品型号规格、功能和性能指标、使用限定、防护等级、电源条件、软件相关信息等	Ⓐ
2	技术原理图	--	Ⓐ
3	产品外形图	外形尺寸、防护等级、接口类型与数量、指示灯标识及其颜色等	Ⓐ
4	说明书（中英文）	产品硬件和软件版本、相关功能及性能描述，产品规格说明，如接口、环境条件等，以及产品操作、安装、维护和使用	Ⓘ
5	铭牌（中英文）	--	Ⓘ
6	安全能力说明	--	Ⓐ
7	安全配置指南	该文件应说明安全功能的建议配置及默认值，目标是确保安全功能的实施符合 UR E26 和系统集成商的所有规范（如用户帐户、授权、密码策略、 设备的安全状态、策略等）	Ⓘ
8	软件质量计划	阐明质量管理体系适用于将要交付的具体系统的设计、施工、交付和维护 阐明在系统和软件整个生命周期内对系统及其不同软件模块和同一软件模块的不同版本进行唯一标识的方法	Ⓘ
	变更管理程序	阐明系统软件模块、网络安全配置的初始安装和后续更新的控制程序	Ⓘ
9	安全开发生命周期文件	对安全开发生命周期的要求说明供应商的流程和控制措施。应说明软件更新与补丁情况	Ⓐ
11	维护和验证计划	维护内容、验证方式、记录等	Ⓘ
12	事件响应及恢复计划	制定响应、备份、恢复等计划方案	Ⓘ
13	配置核查报告		Ⓘ
14	型式试验大纲	测试对象、标准、方法、流程等	Ⓐ

注： Ⓐ批准 Ⓘ备查

第 2 节 型式试验

3.2.1 一般要求

3.2.1.1 申请船舶网络交换机型式认可时，应根据《电气电子产品型式认可试验指南》进行基本试验、电磁兼容性试验，并有如下要求：

（1） 按 CCS 批准的网络安全型式试验大纲，在 CCS 网络安全实验室或经 CCS 认可的实验室进行型式试验；

（2） 应按照本章**错误!未找到引用源。**和**错误!未找到引用源。**的要求完成所有适用

要求的型式试验；

（3） 应进行漏洞扫描、代码审计、健壮性测试和渗透测试对设备进行安全性测试并提供报告。

3.2.1.2 船舶网络交换机应按照表 3.2.1.2 满足对应要求。

船舶网络交换机要求对应表[1] **表 3.2.1.2**

序号	要求	核心交换机	接入交换机	CBS 交换机
1	电接口	√	√	√
2	光接口	○	○	○
3	PoE 接口	○	○	○
4	组网	√	√	○
5	冗余	√	√	○
6	级联	√	√	○
7	VLAN 划分	√	√	○
8	转发和过滤	√	√	√
9	网络风暴抑制	√	√	√
10	组播	√	√	○
11	端口镜像	√	○	○
12	路由转发	√	○	○
13	访问控制列表	√	○	○
14	地址解析协议	√	○	○
15	网络层组播	√	○	○
16	带外管理接口	√	○	○
17	带内管理接口	√	√	√
18	时钟同步接口	√	√	○
19	日志和告警接口	√	√	○
20	管理功能	√	√	√
21	设备安全能力	按照本指南 2.4 节满足对应等级的要求		
22	性能要求	√	√	√

3.2.2 **测试准备**

3.2.2.1 制造商应根据第 2 章要求编制船舶网络交换机型式试验大纲，测试内容涵盖船舶网络交换机的硬件、功能、性能以及安全能力测试， 描述测试文档中标识的测试项与船舶网络交换机技术要求的对应性。

3.2.2.2 测试前，被测设备必须按照提供给用户的配置指南完成配置，配置并开放所有的支持协议，且测试过程中不应修改配置。

3.2.2.3 测试仪表一般连接到设备的业务接口，用于模拟发送数据包。安全测试工具一般连接到设备的业务接口或管理接口，用于进行漏洞扫描、端口扫描等安全测试。管理终端一般连接到设备的管理接口，用于对被测设备进行配置管理。

3.2.2.4 船舶网络交换机的功能、安全能力及性能验证环境如图 3.2.2.4（1）~（4）所示。

[1] √表示适用，○表示可选。

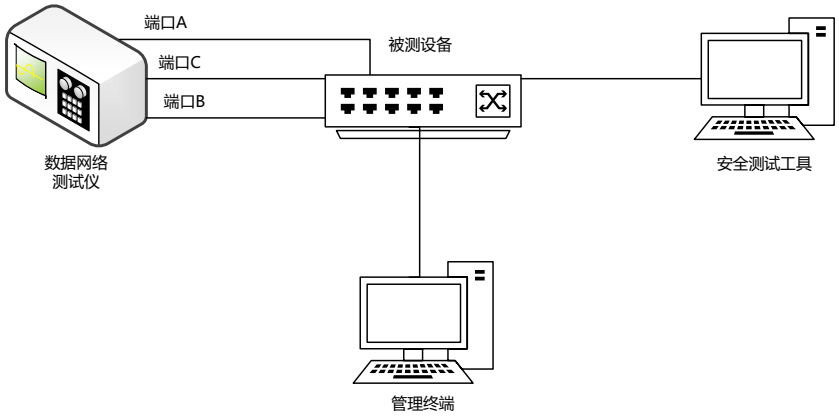

图 3.2.2.4（1） 测试环境 1

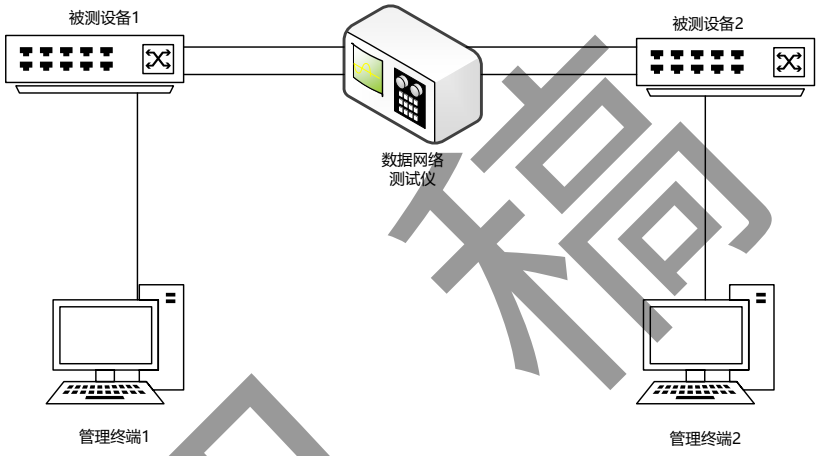

图 3.2.2.4（2）测试环境 2

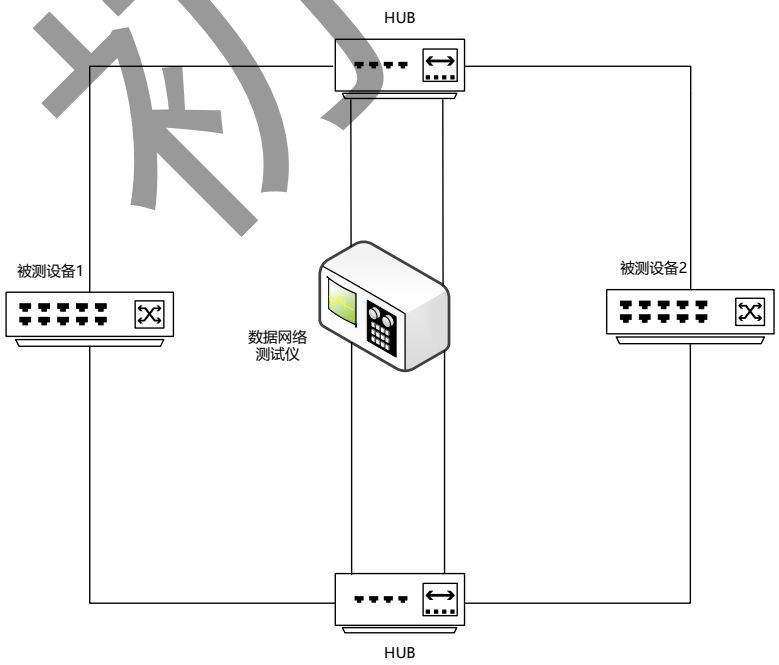

图 3.2.2.4（3）测试环境 3

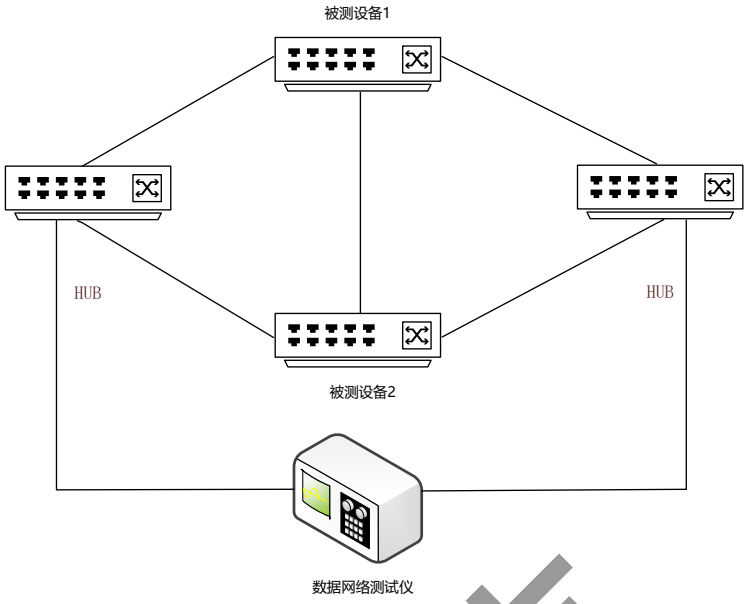

图 3.2.2.4（4）测试环境 4

3.2.3 功能验证

3.2.3.1 应按照表 3.2.1.2 进行对应的功能验证。验证环境及技术要求参考表 3.2.3.1 所示。

验证环境及技术要求　　表 3.2.3.1

序号	验证项目	验证环境	技术要求
1	组网	图 3.2.2.4（4）	2.3.1.1
2	冗余	图 3.2.2.4（1）、（4）	2.3.1.2
3	级联	图 3.2.2.4（4）	2.3.1.3
4	VLAN 划分	图 3.2.2.4（1）	2.3.2.1
5	转发和过滤	图 3.2.2.4（1）	2.3.2.2
6	网络风暴抑制	图 3.2.2.4（2）、（3）	2.3.2.3
7	组播(数据链路层)	图 3.2.2.4（1）	2.3.2.4
8	端口镜像	图 3.2.2.4（1）	2.3.2.5
9	路由转发	图 3.2.2.4（1）	2.3.3.1
10	访问控制列表	图 3.2.2.4（1）	2.3.3.2
11	地址解析	图 3.2.2.4（1）	2.3.3.3
12	组播(网络层)	图 3.2.2.4（1）	2.3.3.4
13	带外管理	图 3.2.2.4（1）	2.3.4.1
14	带内管理	图 3.2.2.4（1）	2.3.4.2
15	时钟同步接口	图 3.2.2.4（3）	2.3.4.3
16	日志和告警接口	图 3.2.2.4（1）	2.3.4.4
17	管理功能	图 3.2.2.4（1）	2.3.5

3.2.4 安全能力验证

3.2.4.1 应按照表 1.1.1.5 进行对应等级的安全能力验证。验证环境及相关要求参考表 3.2.4.1 所示。

安全能力验证环境及技术要求　　表 3.2.4.1

序号	验证项目	验证环境	技术要求
1	标识与鉴别	图 3.2.2.4（1）	《船舶网络安全指南》2.3.1.1
2	使用控制	图 3.2.2.4（1）	《船舶网络安全指南》2.3.1.2

			本指南 2.4.1.2
3	系统完整性	图 3.2.2.4（1）	《船舶网络安全指南》2.3.1.3
4	数据保密性	图 3.2.2.4（1）	《船舶网络安全指南》2.3.1.4
5	受限数据流	图 3.2.2.4（1）	《船舶网络安全指南》2.3.1.5
6	事件的及时响应	图 3.2.2.4（1）	《船舶网络安全指南》2.3.1.6
7	资源可用性	图 3.2.2.4（1）	《船舶网络安全指南》2.3.1.7
9	安全开发	-	本指南 2.4.2
10	安全运维	图 3.2.2.4（1）	本指南 2.4.3

3.2.5 **性能测试**

3.2.5.1 标注的包转发率和交换容量应分别满足 2.5.2 和 2.5.3 的要求。

3.2.5.2 性能测试一般采用测试环境 1，参考 RFC2544 使用流量发生器对被测设备进行不同帧长度数据包发包，测试船舶网络交换机的吞吐量、时延与抖动、丢包，验证是否满足 2.5 的要求。

（1） 吞吐量

①测试应至少包括 64、128、256、512、1518 字节的帧长度数据包，也可采用帧大小混合测试，结合现场环境和业务需求设置混合帧比例。

②报告输出形式：结果应使用表格或图表的形式表示，标识出不同帧长不同负载下的测试值。

（2） 时延抖动

①测试应至少包括 64、128、256、512、1518 字节的帧长度数据包，也可采用帧大小混合测试，结合现场环境和业务需求设置混合帧比例。

②报告输出形式：结果应使用表格的形式表示，标识出不同帧长不同负载下的最小时延、平均时延和最大时延。

（3） 丢包率

①测试应至少包括 64、128、256、512、1518 字节的帧长度数据包，也可采用帧大小混合测试，结合现场环境和业务需求设置混合帧比例。

②报告输出形式：结果应使用表格的形式表示，标识出不同帧长不同负载下的丢包率。