ICS 07.060
CCS A45

HY

中 华 人 民 共 和 国 海 洋 行 业 标 准

HY/T XXXXX—XXXX

海洋信息通信网地面专网建设技术规范

Technical specification for the private ground network construction of marine information communication network

(点击此处添加与国际标准一致性程度的标识)

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国自然资源部　　发 布

目　　次

前　　言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 缩略语 2
5 拓扑规范 2
5.1 网络节点 2
5.2 骨干网拓扑 2
5.3 局域网拓扑 3
6 路由规范 3
6.1 路由体系 3
6.2 IGP 路由区域划分 3
6.3 BGP 路由区域划分 4
6.4 PE-MCE 路由 5
6.5 路由反射器部署 5
6.6 路由聚合 5
7 VPN 规范 6
7.1 VPN 编码 6
7.2 RD 值编码规范 6
7.3 RT 值编码规范 6
8 IP 地址规范 7
8.1 地址分类 7
8.2 编码规则 7
9 QoS 策略规范 10
9.1 QoS 模型 10
9.2 业务分类和标记设计 10
10 网络与安全管理技术要求 10
10.1 网络管理平台 10
10.2 安全管理平台 11
10.3 防火墙 11
10.4 路由协议 11
10.5 身份验证 11
11 外联其他网络要求 11
12 线路及设备要求 12
12.1 线路要求 12
12.2 设备功能要求 12
参　考　文　献 13

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国自然资源部提出。

本文件由全国海洋标准化技术委员会（SAC/TC 283）归口。

本文件起草单位：国家海洋信息中心、国家海洋局北海信息中心、国家海洋局东海信息中心、国家海洋局南海信息中心。

本文件主要起草人：李占斌、刘丰、王喜亭、吴文婷、周雪、吕憧憬、张彬、王颀、曹盛文、曲鹏、张峰、肖燕、魏海、诸茂华、王蕾、朱守荣、王金磊、金莹莹、陈升智、朱海滨、王园君、曹磊

海洋信息通信网地面专网建设技术规范

1 范围

本文件规定了海洋信息通信网地面专网的网络拓扑和路由、Virtual Private Network（VPN）、Internet Protocol（IP）地址、Quality of Service（QoS）等的设计要求，以及骨干网线路和主要网络设备的功能要求、网络与安全管理方面的技术要求等。

本文件适用于海洋通信网地面专网的骨干网建设和各级接入节点的用户局域网建设。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

海洋信息通信网 oceanic information communication network

传输海洋信息的业务专网，采用MPLS VPN技术构建,网络覆盖各级涉海管理部门、业务机构和有关科研院所，承载海域海岛、海洋观测预报、海洋经济、海洋权益、海洋生态等业务。

3.2

运营商核心路由器 provider router；P

转发从PE设备发过来的VPN数据的骨干网核心设备。

注：P设备仅与其他P设备和PE设备互联。在本文件中需要支持MPLS和LDP功能。

3.3

运营商边缘路由器 provider edge router；PE

骨干网和用户局域网直接相连的设备，在本标准中主要负责路由和VPN业务接入，完成报文在骨干网和局域网中的映射和转换。

注：海洋信息通信网采用分层PE设计，PE分为SPE设备和UPE设备。

3.4

超级运营商边缘路由器 super provider edge router；SPE

维护其通过UPE所连接的站点所在的VPN中的所有路由，包括本地和远程站点中的路由。

注：SPE设备上联P设备，下联UPE设备。

3.5

下层运营商边缘路由器 under layer provider edge router；UPE

维护其直接连接的VPN站点的路由，不维护VPN中其他远程站点的路由。

注：UPE设备上联SPE设备，下联MCE设备。

3.6

多实例用户边缘路由器 multi-vpn-instance customer edge router；MCE

用户局域网的出口设备，在本标准中需要支持并配置多VPN实例功能,为不同的VPN提供逻辑上独立的路由转发表。

注：MCE设备上联PE设备，下联局域网交换机或主机。

3.7

路由反射器 route reflector；RR

骨干网路由信息汇集和分发设备，用于汇集自治系统内部各邻居的路由信息并转发给另一个或一组邻居，防止出现网状路由连接。

4 缩略语

下列缩略语适用于本文件。

MPLS	Multiple protocol label switching 多协议标签交换
VPN	Virtual private network 虚拟专用网络
BGP	Border gateway protocol 边界网关协议
OSPF	Open shortest path first protocol 开放式最短路径优先协议
AS	Autonomous system 自治系统
LSA	Link state advertisement 链路状态通告
IP	Internet Protocol 网络之间互连的协议
MSTP	Multi-ServiceTransfer Platform 多业务传送平台
TCP	Transmission Control Protocol 传输控制协议
SSH	Secure Shell 安全外壳
SNMP	Simple Network Management Protocol 简单网络管理协议
RT	Route Target 路由目标
RD	Route Distinguisher 路由区分符
VRF	Virtual Routing Forwarding 虚拟路由转发表

5 拓扑规范

5.1 网络节点

地面专网采用“环型+树型”网络结构，四个核心节点构成环型网，二级节点对应海区和省级涉海管理部门、国家级涉海业务中心等同级别机构；三级节点对应市级涉海管理部门和海洋中心站等同级别机构；四级节点对应县级涉海管理部门和海洋站等同级别机构。不能参照上述分类的新增节点，宜按照就近原则接入，视为就近接入节点的下级节点。

5.2 骨干网拓扑

骨干网采用分层组网技术，便于网络分层规划、建设和维护，提高网络的稳定性、可扩展性和可管理性。MPLS骨干网由核心层、汇聚层和接入层三个层级构成，骨干网拓扑见图1。

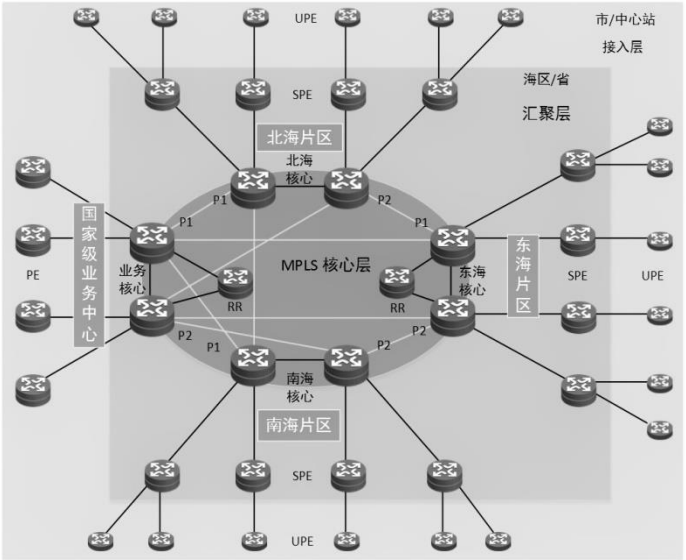


图1　骨干网拓扑

具体层级构成如下：

a) 核心层是由业务核心、北海区核心、东海区核心和南海区核心的 P 设备组成的环形网状网络。各核心节点均要求部署两台 P 设备，以负载均衡方式运行。业务核心节点与各海区核心节点采用双链路双 P 设备互联，各海区核心节点间要求至少采用单链路单 P 设备互联，确保链路可靠冗余。

b) 汇聚层由二级节点 SPE 设备组成，SPE 上联核心层 P 设备，下联三级节点 UPE 设备。汇聚层承担 MPLS 网络路由聚合功能，也承担用户网络接入 MPLS 网络功能。

c) 接入层由 UPE 设备组成，承担用户网络接入 MPLS 网络功能。部分暂无下级节点的国家业务中心等二级节点，其 PE 承担接入层设备功能。

5.3　局域网拓扑

除核心节点外，其他各级节点均部署有用户局域网。用户局域网采用标准站点结构建设，标准化站点拓扑结构见图2。

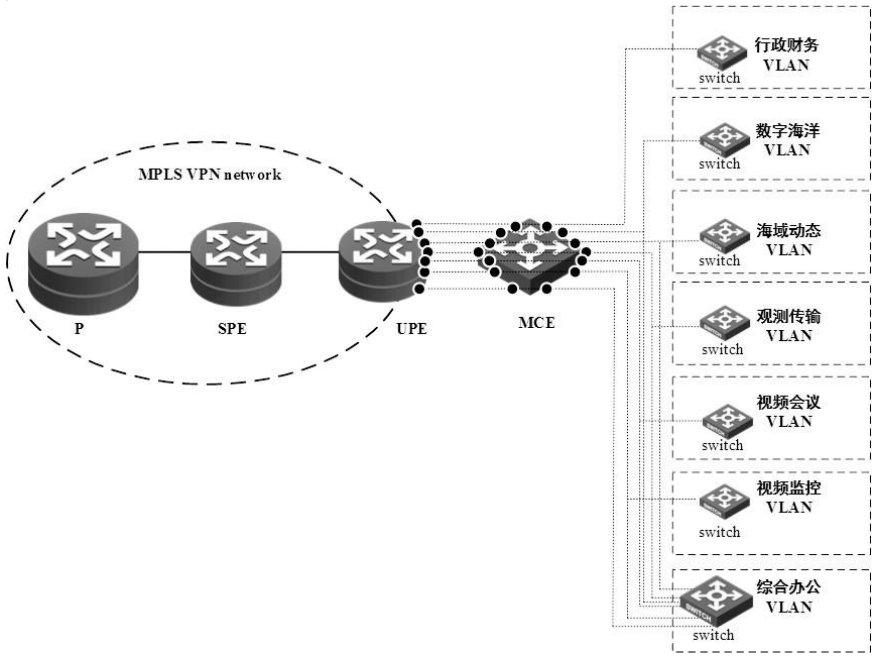


图2　标准化站点拓扑

MCE根据业务划分VLAN，为业务设备接入提供接口。MCE是各级节点局域网的网络出口设备，其中四级节点MCE上联三级节点UPE设备，三级节点MCE上联本级节点UPE设备，二级节点MCE上联本级节点SPE或PE设备。

6　路由规范

6.1　路由体系

骨干网采用MP-BGP+IGP的双层路由体系。IGP协议主要承载IPv4/IPv6基础设施路由信息，为MP-BGP的下一跳提供可达性信息；MP-BGP主要承载业务IPv4/IPv6以及MPLS VPN路由信息。骨干网与用户局域网间可采用静态或动态路由协议。

6.2　IGP 路由区域划分

海洋信息通信网采用OSPF动态路由协议作为IGP，IGP路由区域划分情况见图3。

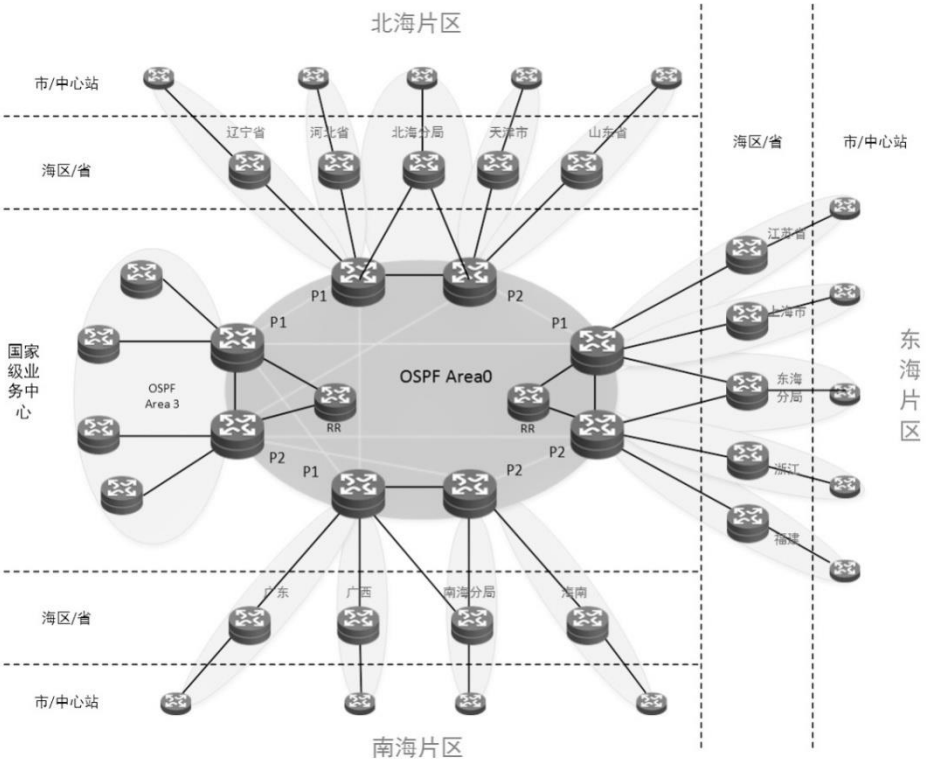


图3　IGP 路由区域

MPLS网络核心层与汇聚层设备单独划分为一个OSPF区域area0，为其他区域之间的路由更新提供路由交换服务，其他路由区域应跟此区域保持联通。

无下级节点的二级节点统一规划到一个OSPF区域area3。

具有三级节点的二级节点，按照二级节点/三级节点组对为单位，各自独立划分一个区域，area ID为三级节点的节点编码。

四级节点的OSPF区域根据所属的三级节点确定，即跟随所属的三级节点划入同一个区域。

6.3　BGP 路由区域划分

海洋信息通信网采用MP-BGP路由协议，承载业务IPv4/IPv6路由和MPLS VPN路由。MP-BGP路由区域划分情况见图4。

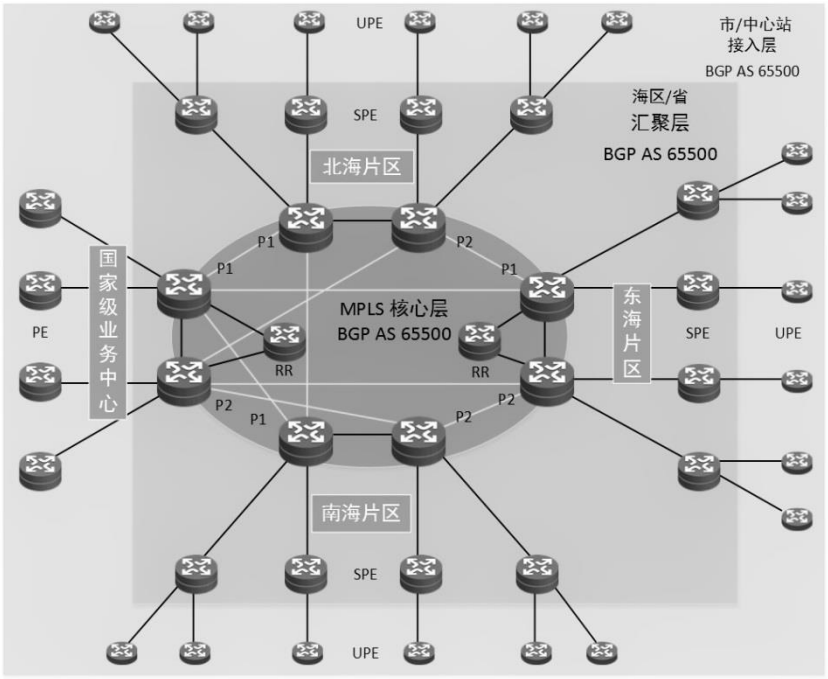


图4　MP-BGP 路由区域

骨干网中P、PE、SPE和UPE统一规划在一个ID号为“65500”的AS自治系统区域内。

6.4　PE-MCE 路由

MCE与PE之间应采用静态路由或OSPF协议进行路由承载。采用OSPF协议时，在PE及MCE侧需要添加与业务VPN数量对等的OSPF进程，各个OSPF实例的进程编号为业务编码，area编号统一为0。业务及OSPF进程编码见表1。

表1　业务及 OSPF 进程编码对照表

业务名称	业务编码	OSPF进程号	Area编号
非实时业务	110	110	0
数字海洋	115	115	0
行政财务	125	125	0
观测传输	141	141	0
视频会议	151	151	0
视频监控	161	161	0
综合办公	171	171	0

6.5　路由反射器部署

海洋信息通信网采用分级部署路由反射器（RR）解决MP-BGP的N平方连接问题。

一级路由反射器采用专用设备承担，部署在核心层网络，负责跟二级节点的汇聚路由器建立一个路由反射器集群。

二级路由器反射器由二级节点的汇聚路由器承担（兼用），负责跟辖区内的三级节点的接入路由器建立路由反射器集群。

同时，为防止路由反射器“单点失效”问题，核心层网络的两台路由反射器形成一个集群，配置相同的cluster-ID；二级路由器反射器作为一级集群的客户机（cluster-clients），采用各二级节点的节点编码作为cluster-ID。

6.6　路由聚合

海洋信息通信网中二级节点的汇聚路由器SPE承担了OSPF的ABR角色和BGP当中的二级路由反射器RR角色。按照前述路由区域划分方式和节点隶属关系，每个省/市级节点组对、海区/中心站节点组对都有单独的OSPF区域。汇聚路由器需按以下方式配置路由聚合功能：

ABR在向其他区域发布Type 3 LSA时，将区域的设备互联网段和管理地址网段汇总成聚合路由并由ABR发布。

汇聚路由器SPE结合静态路由对具体业务路由条目进行聚合，静态路由的目的地址为聚合后的地址段，下一跳为NULL0接口。

7 VPN 规范

7.1 VPN 编码

在海洋信息通信网中，不同VPN间的路由隔离通过VPN实例（VPN-instance）实现，VPN实例又称为虚拟路由转发（Virtual Routingand Forwarding，VRF）实例。全网设置7个VPN，VPN实例编码见表2。

表2 VPN 实例编码表

序号	业务系统名称	VPN编码	业务系统简称	VPN实例名称
1	非实时业务	110	NRTS	NRTS110
2	数字海洋业务	115	DOS	DOS115
3	行政财务业务	125	FAS	FAS125
4	观测传输	141	RTS	RTS141
5	视频会议业务	151	VCS	VS151
6	视频监控业务	161	VSS	VSS161
7	综合办公业务	171	ION	ION171

7.2 RD 值编码规范

路由区分符RD的编码规则为：65500:VPN编码。

示例：非实时业务的路由区分符 RD 值为：65500:110。

7.3 RT 值编码规范

7.3.1 RT 值分类

海洋信息通信网配置了两类路由目标RT值，一类为Public RT，一类为Private RT，分别用于全网跨VPN互通和特定节点间跨VPN互通。

每类VPN包括两种RT属性：

a) Export Target：由 PE 学习 IPv4 路由后，在将其转换为 VPN-IPv4 路由时为这些路由设置 Export Target 属性，并作为 BGP 协议的扩展团体属性随路由发布。

b) Import Target：PE 收到其它 PE 发布的 VPN-IPv4 路由时，检查其 Export Target 属性。当此属性与 PE 上某个 VPN 实例的 Import Target 匹配时，PE 就把该路由加入到该 VPN 实例的路由表，实现 VPN 之间互访。

7.3.2 Public RT 编码格式

Public RT值的编码规则为：65500:VPN编码。

示例：非实时业务的 Public RT 值为：65500:110。

海洋信息通信网各类业务VPN及对应的Public RT值编码见表3。

表3 VPN 及 Public RT 值编码表

序号	业务名称	业务编码	Import RT	Export RT
1	非实时业务	110	65500:110　65000:171	65500:110
2	数字海洋	115	65500:115　65000:171	65500:115

表3 VPN及Public RT值编码表（续）

序号	业务名称	业务编码	Import RT	Export RT
3	行政财务	125	65500:125 65000:171	65500:125
4	观测传输	141	65500:141 65000:171	65500:141
5	视频会议	151	65500:151 65000:171	65500:151
6	视频监控	161	65500:161 65000:171	65500:161
7	综合办公	171	ALL	65500:171

7.3.3 Private RT 编码格式

Private RT值编码规则定义为：X:Y。

其中“X”代表VPN编码，“Y”代表节点编码。“Y”用十进制6位数字表示，划分为前3位和后3位，当节点编码为一个字段时，“Y”用十进制3位数字表示，节点编码不足3位的，前面补0。当节点编码为双字段时，“Y”用十进制6位数字表示，前后字段各用十进制3位数字表示，其中任何一个字段的编码不足3位时，需在前面补0。

示例：某信息中心节点编码为 3，其非实时业务 VPN 的 Private RT 值为 110: 003。某卫星中心节点编码为 4.224，其数字海洋业务 VPN 的 Private RT 值为 115: 004224。当某信息中心非实时业务 VPN 中部署的系统需要访问卫星中心数字海洋业务 VPN 中部署的系统时，某卫星中心的数字海洋业务 VPN 的 RT（export）=65500:115 115: 004224，RT（import）=65500:115 110: 003。某信息中心的非实时业务 VPN 的 RT（export）=65500:110 110: 003，RT（import）=65500:110 115: 004224。

8 IP 地址规范

8.1 地址分类

8.1.1 设备管理地址

网络设备的环回地址，即Loopback地址。在海洋信息通信网中，该地址兼作OSPF、BGP的Router ID，MPLS的LSR ID。

8.1.2 网络互联地址

P设备、PE设备、MCE/CE设备间的互联地址。在海洋信息通信网中，每个业务VPN都要单独分配互联地址。

8.1.3 网管系统地址

网络管理系统IP地址，包括运行网管系统的服务器、终端的地址，以及网管系统管理对象的地址，如交换机、安全设备等所配置的专用网管地址。

8.1.4 业务地址

海洋信息通信网承载的各类业务系统的IP地址，包括服务器、终端配置的地址。

8.2 编码规则

8.2.1 设备管理地址编码

8.2.1.1 编码格式

设备管理IP地址采用A.B.C.D的编码格式，编码规则见表4。

表4 设备管理地址编码规则表

A	B	C	D	备注
8	8	节点编码	设备编码	核心层及二级节点设备
80	节点编码	0或节点编码	1-15用于PE设备 16-31用于MCE设备 32-64用于FW设备	其他设备
80	节点编码	0或节点编码	65以后用于备用资源	其他设备

8.2.1.2 核心层设备编码

A.B为核心层设备管理应用的编码，为固定值8.8。C为设备所在节点的节点编码。D为设备编码，按照先小后大的顺序进行地址分配。

示例：某节点编码为 3 的二级节点部署有 2 台 P 设备，名称序号分别为 P1 和 P2，按照分配原则，P1 和 P2 的设备管理 IP 地址分别是 8.8.3.1 和 8.8.3.2。

8.2.1.3 其他设备编码

A为设备管理应用的编码，为固定值80。如设备所在节点的节点编码为一个字段，则B为设备所在节点的节点编码，C为固定值0；如设备所在节点的节点编码为双字段，则B.C为设备所在节点的节点编码。D为设备编码，按照先小后大的顺序进行地址分配。

示例：某节点编码为131的二级节点部署有2台PE设备和2台MCE设备，名称序号分别为PE1和PE2、MCE1和MCE2，按照分配原则，PE1和PE2的设备管理IP地址分别是80.131.0.1和80.131.0.2，MCE1和MCE2的设备管理IP地址分别是80.131.0.16和80.131.0.17。

8.2.2 网络互联地址编码

8.2.2.1 编码格式

网络互联IP地址采用A.B.C.D的编码格式，编码规则表见表5。

表5 网络互联地址编码规则表

序号	A	B	C	D	备注
1	8	10、11	3	接口编码	P设备互联
2	8	12、13	SPE节点编码	接口编码	P-SPE设备互联
4	8	SPE节点编码	UPE节点编码	接口编码	SPE-UPE设备互联
3	111	节点编码	0或节点编码	接口编码	非实时业务VPN互联
4	115				数字海洋VPN互联
5	125				行政财务VPN互联
6	141				观测传输VPN互联
7	151				视频会议VPN互联
8	161				视频监控VPN互联

8.2.2.2 P 设备互联编码

A.B为核心设备互联应用的编码，为固定值8.10，8.11。C为核心层互联专用代码，为固定值3。D为设备互联接口编码。其中：

a) 业务核心的 P1 设备跟对端 P 设备互联的网段采用 8.10.3.0/26，P2 设备跟对端 P 设备互联的网段采用 8.11.3.0/26。一个物理接口分配 4 个地址，子网掩码采用“/30”。

b) 各海区核心按照从北到南的地理方位顺序分配互联网段，北海核心分配子网 8.10.3.64/26，东海核心分配子网 8.10.3.128/26，南海核心分配子网 8.10.3.192/26。一个物理接口分配 4 个地址，子网掩码采用“/30”。一条物理链路划分为多个子接口链路时，每个子接口分配 4 个地址，子网掩码采用“/30”。

c) 接口编码按照先节点内部再节点之间，先业务核心再海区核心的顺序进行分配。同层级的网络设备，依据 Loopback 地址末位值确定分配顺序，末位值小的设备分配小号，末位值大的分配大号。

示例：业务核心 P1 互联 P2 时，P1 分配 8.10.3.1，P2 分配 8.10.3.2。业务核心 P1 互联北海核心 P1 时，业务核心 P1 分配 8.10.3.5，北海核心 P1 分配 8.10.3.6。业务核心 P2 与北海核心 P2 互联时，业务核心 P2 分配 8.11.3.1，北海核心 P2 分配 8.11.3.2。北海核心 P1 与南海核心 P1 互联时，北海核心 P1 分配 8.10.3.69，南海核心 P1 分配 8.10.3.70。

8.2.2.3 P-SPE 设备互联编码

A.B为核心设备互联应用的编码，为固定值8.12，8.13。C为SPE设备节点编码，D为设备互联接口编码。其中：

a) SPE 与 P1 互联时采用 8.12，与 P2 互联时采用 8.13。接口编码按照先 P 设备再 SPE 设备的顺序分配；

b) 一个物理接口分配 4 个地址，子网掩码采用“/30”。一条物理链路划分为多个子接口链路时，每个子接口分配 4 个地址，子网掩码采用“/30”。

示例：以东海核心 P2，浙江省 PE 为例。浙江省 PE 上联 P2 的地址为 8.13.128.2，P2 下联浙江省 PE 的地址为 8.13.128.1。

8.2.2.4 SPE-UPE 设备互联编码

A为互联应用的编码，为固定值8。B为SPE设备节点编码，C为UPE设备节点编码。D为设备互联接口编码。其中：

a) 接口编码按照先上层设备再下层设备的顺序分配，即 SPE 设备采用小号，UPE 设备采用大号。

b) 一个物理接口分配 4 个地址，子网掩码采用“/30”；一条物理链路划分为多个子接口链路时，每个子接口分配 4 个地址，子网掩码采用“/30”。

示例：以浙江省 SPE，台州市 UPE 为例。浙江省 UPE 下联台州 UPE 的地址为 8.128.131.1，台州 UPE 上联浙江省 SPE 的地址为 8.128.131.2。

8.2.2.5 VPN 业务互联编码

A为VPN业务的应用编码，为固定值。如设备所在节点的节点编码为一个字段，则B为节点编码，C为固定值0；如设备所在节点的节点编码为双字段，则B.C为节点编码。D为设备互联接口编码。其中：

a) MCE 设备与 PE 设备互联时，采用 PE 设备所在节点编码；与同级 MCE 设备互联时，采用 MCE 设备所在节点的节点编码。

b) 接口编码取值，按照先上层设备再下层设备的顺序分配，也就是上层设备采用小号，下层设备采用大号。同层级设备互联时，依据 Loopback 地址末位值确定分配顺序，末位值小的设备分配小号，末位值大的分配大号。

c) 一个物理接口分配 4 个地址，子网掩码采用“/30”。一条物理链路划分为多个子接口链路时，每个子接口分配 4 个地址，子网掩码采用“/30”。

示例：以业务核心节点 PE1，MCE1 为例。非实时业务 VPNMCE1 上联 PE1 的子接口地址为 111.3.0.2， PE1 下联 MCE1 的子接口地址为 111.3.0.1。以辽宁省丹东市东港区 MCE 上联丹东市 PE 为例，非实时业务 VPN 业务东港区 MCE 上联丹东市 PE 的子接口地址为 111.66.0.2，丹东市 PE 下联东港区 MCE 的子接口地址为 111.66.0.1。

8.2.3 网管系统地址编码

网管系统地址采用A.B.C.D的编码格式。A为网络管理应用的编码，为固定值81；如设备所在节点的节点编码为一个字段，则B为设备所在节点的节点编码，C为固定值0；如设备所在节点的节点编码为双字段，则B.C为设备所在节点的节点编码。D为设备编码。按照先小后大的顺序进行地址分配。具体编码规则表见表6。

示例：某节点编码为 64 的二级节点部署有 2 台 MCE 设备，名称序号分别为 MCE1 和 MCE2，按照分配原则，MCE1 和 MCE2 的网络管理 IP 地址分别是 81.64.0.1 和 81.64.0.2。该节点有 2 台网管服务器，2 台网管终端，名称序号分别为 S1 和 S2，C1、C 2，其 IP 地址分别为 81.64.0.128，81.64.0.129，81.64.0.160，81.64.0.161。

表6 网管系统地址编码规则表

A	B	C	D	备注
81	节点编码	0或节点编码	1-31用于MCE设备；32-95用其他交换机设备；96-127用于安全设备；128-159用于服务器；160-191用于终端设备	网关设在MCE上，适当减小广播域

8.2.4 业务地址编码

业务地址采用A.B.C.D的编码格式。A为VPN业务的应用编码，为固定值；如设备所在节点的节点编码为一个字段，则B为设备所在节点的节点编码，C为网段编码；如设备所在节点的节点编码为双字段，则B.C为设备所在节点的节点编码；D为业务设备地址编码。具体编码规则见表7。

表7　业务地址编码规则表

节点类型	A	B	C	D
国家业务中心、派出机构、省/直辖市/自治区海洋管理部门	10 15 25 41 51 61 71	节点编码	0-15服务器地址段 16-31客户端地址段	1-239 240以后预留，254为网关。如有41业务，0-10用于实时数据传输。
其他部属单位、市级海洋管理部门、中心站、海洋站			前两个C用于服务器 其他网段用于客户端	1-239 240以后预留，254为网关。如有41业务，0-10用于实时数据传输。
县级海洋管理部门			节点编码C段（一个C类地址）	1-31服务器地址 32-239客户端地址 240以后预留，254为网关。如有41业务，0-10用于实时数据传输业务。

9　QoS 策略规范

9.1　QoS 模型

海洋信息通信网地面专网承载多业务数据，包括实时数据、非实时数据、视频流数据等，每种业务所需的带宽资源不一。为确保强实时性业务在流量高峰期优先转发，海洋信息通信网采用差分服务（Diff-Serv）模型提供QoS传输保障。

海洋信息通信网差分服务模型采用基于IP地址的业务分类方法和DSCP（差分服务代码点，differentiated services code point）标记机制，对报文按业务分类进行优先级标记。转发设备根据报文的DSCP字段执行相应的转发行为，包括EF（加速转发，expedited forwarding），AF（确保转发,assured forwarding）、BE（尽力转发,best-effort）。

9.2　业务分类和标记设计

海洋信息通信网各业务优先级及相应的DSCP参数设计见表8。

表8　业务优先级标记对照表

数据业务	优先级	DSCP标记	EXP标记	类别
视频会议	5	101000	101	EF
观测传输	4	100000	100	AF4
视频监控	3	011000	011	AF3
预留	2	010000	010	AF2
预留	1	001000	001	AF1
预留	0	000000	000	BE

10　网络与安全管理技术要求

10.1　网络管理平台

10.1.1　平台组成

网络管理平台由国家级网络管理平台和海区级网络管理平台组成。国家级网络管理平台将全网各级分支机构纳入平台进行管理，对设备、线路及流量等状态进行监控。海区级网络管理平台将海区网络（包括海区局及其下属中心站、海洋站节点等和省、自治区、直辖市及其下属市、县级节点等）各级分支机构纳入平台进行管理，对设备、线路及流量等状态进行监控。

10.1.2　基本功能与部署配置

网络管理平台基本功能与部署配置应包括以下部分：

a) 拓扑管理：具备创建网络拓扑功能；应创建包括网络设备、安全设备在内的网络拓扑，国家级网络管理平台应创建全网拓扑，海区级网络管理平台应创建海区网络拓扑；
b) 流量管理：具备获取物理接口流量功能，能够按照 VPN 流量、特定协议流量、特定用户流量等不同维度进行流量划分和提取；
c) 故障管理：能够自动检测设备和线路故障并告警，提供故障分析与排查工具；
d) 统计管理：具备测度网络带宽资源利用情况功能；
e) 配置管理：能够对网络设备的配置进行获取和管理，对主流厂商设备具有兼容性。

10.2 安全管理平台

10.2.1 平台组成

海洋信息通信网将各分支机构防火墙接入安全管理平台，实现多层级网络安全信息的采集和分析应用。安全管理平台由国家级安全管理平台和海区级安全管理平台组成，国家级安全管理平台与海区级安全平台采用级联方式部署。国家级安全管理平台将全网各级分支机构的安全信息纳入平台进行管理，海区级安全管理平台将海区网络（包括海区局及其下属中心站、海洋站节点等和省、自治区、直辖市及其下属市、县级节点等）各级分支机构的安全信息纳入平台进行管理。

10.2.2 基本功能与部署配置

安全管理平台基本功能与部署配置包括以下部分：

a) 信息集成：具备集成防火墙等安全设备的安全日志的功能；应集成各级分支机构的防火墙产生的安全日志信息。
b) 级联运行：国家级和海区级安全管理平台应级联部署；海区级安全管理平台应向国家级安全管理平台自动报送所采集的各级分支机构的安全信息，国家级安全管理平台可向海区级安全管理平台下发安全信息，级联信息的交互应符合国家级安全管理平台的通信接口和数据格式要求。
c) 拓扑管理：具备创建分支机构可视化拓扑功能；国家级安全管理平台应创建全网拓扑，海区级安全管理平台应创建海区网络拓扑；拓扑节点应集成所对应的分支机构的安全信息，拓扑连线应集成分支机构间的访问行为安全信息。
d) 策略管理：能够对防火墙安全策略进行在线集中统一管理。
e) 溯源举证：能够追溯攻击行为源 IP 地址，对攻击行为及安全漏洞进行举证。
f) 态势感知：具备流量分析、关联分析、威胁可视化等功能；能够以分支机构为单元进行安全评价，能够对全网安全态势进行整体评价。

10.3 防火墙

防火墙应配置以下安全功能：

a) 访问控制策略:各节点出口防火墙应配置全网统一的综合办公网单向访问控制策略；
b) 攻击防护策略:各节点出口防火墙应开启常用的攻击防护策略；
c) 安全信息报送:防火墙应配置至本级安全管理平台的日志同步连接，并开启了日志同步功能。

10.4 路由协议

路由协议应配置以下安全功能：

a) OSPF 协议配置接口验证功能，避免路由信息外泄或者对 OSPF 路由器进行恶意攻击；
b) BGP 对等体间建立 TCP 连接时应进行 MD5 验证，避免与非法的 BGP 路由器建立 TCP 连接。传递 BGP 报文时，应对封装 BGP 报文的 TCP 报文段进行 MD5 运算，保证 BGP 报文不会被篡改。

10.5 身份验证

网络设备登录应采用SSH协议进行身份合法性验证。

11 外联其他网络要求

外联其他相同安全等级的专网时，应通过互联防火墙（可利用本节点的海洋信息通信网防火墙，或者新增专用的网络互联防火墙）设备建立本节点MCE与其他专网有关设备的物理连接。部署静态路由及双向NAT地址转换策略，按访问范围最小化原则部署访问控制策略，实现受控条件下的特定地址范围之间的互访。

12 线路及设备要求

12.1 线路要求

海洋信息通信网骨干网各级节点间要求采用MSTP线路，其MTU值应不小于1600。线路两端接口采用全双工工作模式。

12.2 设备功能要求

P设备支持MPLS。

PE设备支持MPLS VPN和虚拟化。

MCE设备支持多实例VPN和虚拟化。

参 考 文 献

[1]GB/T25068-2010 信息技术 安全技术 IT 网络安全第 1 部分:网络安全管理
[2]YDT 1477-2006 基于边界网关协议_多协议标记交换的虚拟专用网(BGP_MPLS VPN)组网要求
[3]YDT 1476-2006 基于边界网关协议_多协议标记交换的虚拟专用网(BGP_MPLS VPN)技术要求