YD

中华人民共和国工业和信息化部 发布

202×-××-××实施

202×-××-××发布

面向5G传输的PTN/SPN管控融合网络管理系统技术要求

Technical Specification of PTN/PTN Management and Control Convergence Network Management System for 5G Bearer Network

YD/T ××××—××××

中华人民共和国通信行业标准

ICS

M 11

目 次

[前 言 1](#_Toc53650043)

[范围 2](#_Toc53650044)

[规范性引用文件 2](#_Toc53650045)

[术语、定义和缩略语 2](#_Toc53650046)

[术语和定义 2](#_Toc53650047)

[缩略语 2](#_Toc53650048)

[1 智能化配置管理 2](#_Toc53650049)

[1.1 设备配置和管理 2](#_Toc53650050)

[1.1.1 网元配置和管理 2](#_Toc53650051)

[1.1.2 端口配置和管理 4](#_Toc53650052)

[1.2 L3VPN配置和管理 5](#_Toc53650053)

[1.2.1 L3VPN配置和管理（5G） 5](#_Toc53650054)

[1.3 同步配置和管理 6](#_Toc53650055)

[1.3.1 频率同步配置和管理 6](#_Toc53650056)

[1.3.2 时间同步相关配置 7](#_Toc53650057)

[1.4 业务智能调度 7](#_Toc53650058)

[1.4.1 5G业务智能调度 7](#_Toc53650059)

[1.4.2 L3VPN业务配置检查 8](#_Toc53650060)

[1.5 MTN配置和管理 8](#_Toc53650061)

[1.6 Segment Routing配置和管理 9](#_Toc53650062)

[1.6.1 协议配置 9](#_Toc53650063)

[1.6.2 SR节点和链路配置 10](#_Toc53650064)

[1.6.3 SR-TP隧道配置和管理 11](#_Toc53650065)

[1.6.4 重路由OAM配置管理 13](#_Toc53650066)

[1.6.5 PING/Traceroute检测 14](#_Toc53650067)

[1.7 5G快速基础配置 14](#_Toc53650068)

[1.7.1 资源池规划 14](#_Toc53650069)

[1.7.2 逻辑网络规划 14](#_Toc53650070)

[1.7.3 网元基础配置自动生成和发放能力 15](#_Toc53650071)

[1.8 网络切片管理 15](#_Toc53650072)

[1.9 高精度时钟管理 15](#_Toc53650073)

[1.9.1 时钟同步网络规划 16](#_Toc53650074)

[1.9.2 时间同步网络规划 16](#_Toc53650075)

[1.9.3 同步网络配置检测 16](#_Toc53650076)

[1.9.4 同步网络告警管理 16](#_Toc53650077)

[1.9.5 同步网络性能管理 16](#_Toc53650078)

[2 拓扑管理 17](#_Toc53650079)

[2.1 拓扑视图 17](#_Toc53650080)

[2.2 拓扑编辑 17](#_Toc53650081)

[2.3 拓扑浏览 18](#_Toc53650082)

[3 管控融合的故障管理 19](#_Toc53650083)

[3.1 告警属性 19](#_Toc53650084)

[3.1.1 告警名称 19](#_Toc53650085)

[3.1.2 告警类型 26](#_Toc53650086)

[3.1.3 告警级别 27](#_Toc53650087)

[3.1.4 告警状态 27](#_Toc53650088)

[3.1.5 告警信息 27](#_Toc53650089)

[3.2 告警处理 27](#_Toc53650090)

[3.2.1 告警级别重分配 27](#_Toc53650091)

[3.2.2 告警确认 27](#_Toc53650092)

[3.2.3 告警清除 28](#_Toc53650093)

[3.2.4 告警锁定 28](#_Toc53650094)

[3.2.5 告警过滤 28](#_Toc53650095)

[3.2.6 告警屏蔽 28](#_Toc53650096)

[3.2.7 告警反转 28](#_Toc53650097)

[3.2.8 告警备注 29](#_Toc53650098)

[3.3 告警监控和呈现 29](#_Toc53650099)

[3.3.1 显示内容和方式 29](#_Toc53650100)

[3.3.2 告警模板管理 29](#_Toc53650101)

[3.3.3 多窗口监控 29](#_Toc53650102)

[3.4 告警查询和统计 30](#_Toc53650103)

[3.5 告警压缩 30](#_Toc53650104)

[3.5.1 工程告警设置 30](#_Toc53650105)

[3.5.2 闪断告警分析 31](#_Toc53650106)

[3.6 告警关联分析 31](#_Toc53650107)

[3.6.1 相关性分析原则 31](#_Toc53650108)

[3.7 告警同步和存储 32](#_Toc53650109)

[3.7.1 告警同步 32](#_Toc53650110)

[3.7.2 告警保存与存储 32](#_Toc53650111)

[3.8 告警处理能力 33](#_Toc53650112)

[3.9 端到端告警管理 33](#_Toc53650113)

[3.10 断纤链路管理 33](#_Toc53650114)

[4 管控融合的性能管理 33](#_Toc53650115)

[4.1 性能监测管理 33](#_Toc53650116)

[4.1.1 性能监测参数设置 33](#_Toc53650117)

[4.1.2 性能监测参数查询/修改 34](#_Toc53650118)

[4.1.3 性能门限设置 34](#_Toc53650119)

[4.1.4 性能数据查询 34](#_Toc53650120)

[4.1.5 性能数据上报 34](#_Toc53650121)

[4.1.6 性能数据存储 34](#_Toc53650122)

[4.2 端到端性能管理 35](#_Toc53650123)

[4.3 性能监测参数要求 35](#_Toc53650124)

[4.4 性能监控能力 37](#_Toc53650125)

[5 管控融合的流量管理 37](#_Toc53650126)

[5.1 流量监测功能要求 37](#_Toc53650127)

[5.2 流量基础数据表要求 38](#_Toc53650128)

[5.2.1 业务流量基础数据表要求 38](#_Toc53650129)

[5.2.2 网络流量基础数据表要求 39](#_Toc53650130)

[5.2.3 查看端口毫秒级流量数据 41](#_Toc53650131)

[5.2.4 L3VPN业务接口流量报表数据 41](#_Toc53650132)

[5.3 流量分析报表和输出 42](#_Toc53650133)

[5.3.1 流量分析报表输出的基本要求 42](#_Toc53650134)

[5.3.2 业务流量报表 42](#_Toc53650135)

[5.3.3 PTN/SPN网络流量分析系统呈现功能要求 47](#_Toc53650136)

[5.4 流量地图呈现 50](#_Toc53650137)

[5.5 流量拓扑图呈现 50](#_Toc53650138)

[5.6 流量预警分析 51](#_Toc53650139)

[5.7 带宽动态调整 52](#_Toc53650140)

[5.8 流量监测的性能要求 54](#_Toc53650141)

[5.8.1 监测实例数量要求 54](#_Toc53650142)

[5.8.2 数据存储能力要求 54](#_Toc53650143)

[6 网络质量管理 54](#_Toc53650144)

[6.1 质量指标体系 54](#_Toc53650145)

[6.2 探针状态监控 56](#_Toc53650146)

[6.3 监测任务的管理 56](#_Toc53650147)

[6.3.1 监测任务创建 56](#_Toc53650148)

[6.3.2 监测任务修改 57](#_Toc53650149)

[6.3.3 监测任务删除 57](#_Toc53650150)

[6.4 监测数据的管理 57](#_Toc53650151)

[6.4.1 质量监测数据查看 57](#_Toc53650152)

[6.4.2 质量监测数据分析 58](#_Toc53650153)

[6.4.3 质量监测数据存储 58](#_Toc53650154)

[6.5 质量报表输出 58](#_Toc53650155)

[6.6 质量地图呈现 59](#_Toc53650156)

[6.7 质量告警分析 60](#_Toc53650157)

[6.8 质量监控分析的性能要求 60](#_Toc53650158)

[7 业务割接和网络优化调整 60](#_Toc53650159)

[7.1 网络业务割接管理 60](#_Toc53650160)

[7.1.1 割接任务管理 61](#_Toc53650161)

[7.1.2 割接组管理 61](#_Toc53650162)

[7.1.3 割接场景 61](#_Toc53650163)

[7.1.4 割接任务执行 62](#_Toc53650164)

[7.1.5 割接结果查看 62](#_Toc53650165)

[7.2 网络业务调整 63](#_Toc53650166)

[7.2.1 网络调整功能通用要求 63](#_Toc53650167)

[7.2.2 网络业务调整场景 63](#_Toc53650168)

[7.2.3 业务路由优化 68](#_Toc53650169)

[8 巡检管理 69](#_Toc53650170)

[8.1 巡检任务管理 69](#_Toc53650171)

[8.1.1 创建巡检任务 69](#_Toc53650172)

[8.1.2 查询巡检任务 70](#_Toc53650173)

[8.1.3 修改巡检任务 70](#_Toc53650174)

[8.1.4 删除巡检任务 70](#_Toc53650175)

[8.1.5 巡检任务的执行 70](#_Toc53650176)

[8.1.6 巡检结果管理 70](#_Toc53650177)

[8.2 巡检项目 71](#_Toc53650178)

[8.2.1 网元状态检查 71](#_Toc53650179)

[8.2.2 网元配置检查 74](#_Toc53650180)

[8.2.3 网络配置检查 75](#_Toc53650181)

[8.2.4 网络状态检查 78](#_Toc53650182)

[8.3 巡检结果调优 82](#_Toc53650183)

[9 智能运维 82](#_Toc53650184)

[9.1 流量预测 82](#_Toc53650185)

[9.2 SR-TP故障回溯 83](#_Toc53650186)

[9.3 带内性能诊断 83](#_Toc53650187)

[9.4 网络故障模拟仿真 84](#_Toc53650188)

[10 附录1--PTN/SPN网络流量指标体系与应用方案 84](#_Toc53650189)

[10.1 流量指标体系 84](#_Toc53650190)

[10.1.1 流量监测对象 85](#_Toc53650191)

[10.1.2 流量监测模式 86](#_Toc53650192)

[10.1.3 流量监测周期 86](#_Toc53650193)

[10.1.4 流量监测和分析流程 87](#_Toc53650194)

[10.1.5 流量监测和分析指标说明 87](#_Toc53650195)

[1 88](#_Toc53650196)

[10.1.6 流量监测和分析指标定义 90](#_Toc53650197)

[10.2 流量基础数据表要求说明 103](#_Toc53650198)

[10.3 PTN/SPN网络流量监测与应用方案 105](#_Toc53650199)

[10.3.1 流量监测点的设置方案 105](#_Toc53650200)

[10.3.2 业务流量的监测应用方案 111](#_Toc53650201)

[10.3.3 网络流量的监测应用方案 113](#_Toc53650202)

前 言

本标准按照GB/T XXXX给出的规则起草。

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这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位： 中国移动通信集团公司、中国移动通信集团设计院有限公司、华为技术有限公司

本标准主要起草人：吴超、成梦虹

面向5G传输的PTN/SPN管控融合网络管理系统技术要求

范围

本标准对xxxx原则性的要求。

本标准适用于指导在xxxx的应用方法设定。

本标准所述的面向5G传输的PTN/SPN管控融合网络管理系统具有网元管理功能和和子网管理功能，具有拓扑管理、配置管理、故障管理、性能管理、安全管理等功能模块。该系统不仅要具备基础管控能力，还应引入人工智能和大数据技术，更加高效地分析海量告警和性能数据，快速准确定位故障根因，预测、预警性能劣化和流量超限，提升现网运维效率。

规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改）适用于本标准。

|  |  |
| --- | --- |
| YD/T xxx | YYYY |
|  |  |
|  |  |
|  |  |

术语、定义和缩略语

术语和定义

下列术语和定义适用于本文件。

缩略语

下列缩略语适用于本标准。

# 智能化配置管理

## 设备配置和管理

### 网元配置和管理

#### 创建网元

网管在安装完成后并没有当前网络中的网元数据，网管应能提供在线和离线创建网元功能。创建网元时，用户应提供如下信息，信息不全时EMS应提供检测机制提示用户：

1. 网元类型；
2. 网元名称；
3. 网元与网管的连接方式（网关，非网关）；
4. 网元地址：包括网元IP地址（网关网元要求）；
5. 所属网关网元（非网关网元要求）；
6. 区域信息；注：区域信息是指标识网元所属的区域，可根据PTN网管分域管理的设置方式，以及流量分区监测方案的需要来划分区域。
7. 网元位置（所在的城市、局站、楼层、机架位置等）；
8. 网元经纬度，由用户人工输入
9. 设备分类（PTN、小型化接入PTN等）；
10. 网元所属的网络层级（如：接入层、汇聚层、核心层、骨干层、二干、一干），网络层级内容，建议采用勾选输入，使用客户采用人工输入方式。

其中“网络层级”默认为接入层。

1. 集客场景下，须填写网元对应的使用客户，由用户人工输入。
2. 网元开通时间，开通时间是指网元被网管管理的时间，即创建时间。
3. 支持一个预留的属性字段，满足后期个性化需求，长度为64个字符，支持中英文输入。
4. 其他可提供的网元配置信息。

网元创建后，网管根据创建网元时提供的地址信息到与其相连的网络中寻找符合上述地址的网元，建立网管与网元之间的通信联系，并以图标的方式出现在拓扑图中。

应具备非网关网元即插即用能力。即非网关网元上电并与网络完成物理连接后，不需要在机房现场软调，就可以在网管上创建该网元并进行配置管理。

#### 删除网元

用户应能删除在线网元和离线网元。删除网元时，网管应检查操作员是否具有该项权限。

#### 查询和修改网元

网管应支持使用多种组合设置条件查找网元，支持的查询条件包括：网元名称、网元ID、管理IP的网段、网元类型、网元开通时间(创建时间)等。

网管应能提供修改网元名称、管理IP地址的功能。

网管应能提供直观的机框正面板配置图，分别以图形方式显示机框中槽道和单元盘的布局（机框中所包含槽道、每个槽道所安装的单元盘）信息，用户可通过对图形界面的操作完成网元硬件配置参数的查询和修改功能。

用户可查询和修改的网元信息包括：

1. 插槽信息，包括：
2. 槽道中是否安装单元盘；
3. 槽道中的单元盘信息；
4. 为空闲插槽安装一个指定的单元盘。
5. 单元盘信息，包括：
6. 单元盘类型；
7. 单元盘型号；
8. 是否有保护及保护方式；
9. 网元信息，包括：
10. 区域信息（\*）；
11. 网络层次（\*）；
12. 使用客户（\*）；
13. 设备分类（\*）；
14. 预留字段（\*）

支持”网络层次”的批量设置和修改。

#### 批量版本升级

支持批量选择网元建立升级任务，升级任务可自动完成如下步骤：

1. 待升级网元升级前检查
2. 网元配置备份
3. 网元软件加载
4. 网元软件激活
5. 升级后自动检查
6. 升级失败自动回滚

### 端口配置和管理

#### TDM端口查询和配置

TDM端口包括以下信息，其中标\*属性可配置：

1. 端口名称，应包括该端口对应的客户业务种类（如2G、3G、4G、集客专线、有线宽带等）和集团客户名称（如中国银行XX支行、中石油XX分公司等）；
2. 端口使用状态：端口是否空闲；
3. 端口类型：光接口/电接口
4. 端口速率：E1/STM-N
5. 通道化属性：通道化、非通道化。
6. 容量为STM-N的设备端口的再生段跟踪字节和通道跟踪字节J0、J1、J2、C2信息(\*)等。
7. 备注(\*)

#### 以太网端口查询和配置

以太网端口包括以下属性信息，其中标\*属性可配置：

1. 端口名称，应包括该端口对应的客户业务种类（如2G、3G、4G、集客专线、有线宽带等）和集团客户名称（如中国银行XX支行、中石油XX分公司等）；
2. 端口使用状态：端口是否空闲；
3. 端口类型：光接口/电接口
4. 端口速率：100Mbps/1000Mbps/10GE/25GE/50GE/100GE/200GE/400GE
5. 工作模式：全双工/自协商(\*)
6. 物理端口MAC地址
7. 流控属性(\*)等。
8. 端口属性：网管支持自动判断端口是NNI或者UNI端口，并支持端口属性的手工修改。
9. 支持MTN模式使能
10. SD使能
11. 备注(\*)
12. 支持开启“性能监控实例”功能，默认为不开启，若用户选择开启，则可进行性能监控实例相关参数的设置。

查询端口的配置和其流量信息时，应在OMC的同一个入口相关联的一个或多个界面中呈现。

#### 端口环回设置和查询

网管系统应支持设置和查询特定的业务端口环回（Loop），以便于故障的维护、诊断，端口环回状态应包含内环回、外环回、不环回。

网管系统对已设置环回（Loop）的业务端口应在设备面板界面相应端口位置提供显示；并支持选择多个端口设置环回，并可定时（例如15分钟后）自动清除。

#### 网络侧接口链路聚合配置

网管系统应支持网络侧接口链路聚合配置功能。

#### L2和L3桥接配置管理

用户在对网元设备进行配置时，EMS应提供如下L2和L3桥接的配置管理功能。包括：

1. 支持创建L2VPN和L3 VPN桥接的虚端口；
2. 绑定L2 VPN业务和L3 VPN业务；
3. 提供L2 VPN业务和L3 VPN业务的关联关系查询功能；
4. 提供端到端的L2和L3业务路径视图功能。

## L3VPN配置和管理

### L3VPN配置和管理（5G）

OMC应支持L3VPN业务配置和管理，包括创建、修改和删除L3VPN业务。L3 VPN业务配置和管理功能包括：

1. 支持端到端创建多点到多点的静态MPLS L3VPN业务，并提供基于业务模板MPLS L3VPN创建功能。支持配置L3 VPN业务的如下参数：
2. 业务名称；
3. 入方向VRF标签；
4. 添加本端和远端PE设备、端口及其QoS、IP地址和子网掩码；
5. 客户侧设备（包括SGW/MME/CE路由器等）的名称、IP地址等；
6. 到与本端PE设备相连的客户侧设备的静态路由；
7. 端到端删除存在的MPLS L3VPN业务，删除后，OMC系统和设备应释放所占用的所有资源。
8. 支持查询/修改MPLS L3VPN业务的相关信息（\*为可修改）：
9. 业务名称(\*)；
10. 入方向VRF标签；
11. 本端和远端PE设备、端口及其QoS、IP地址和子网掩码(\*)；
12. 客户侧设备（包括SGW/MME/CE路由器等）的名称、IP地址等；
13. 到与本端PE设备相连的客户侧设备的静态路由(\*)；
14. 到与远端PE设备相连的网络侧设备的静态路由，包括：

—远端客户侧设备的IP地址和子网掩码；

—出方向VRF标签；

—到远端PE设备的SR-TP隧道；

1. 支持VPN FRR/IP FRR保护功能
2. 提供业务信息同步的功能。

业务信息的同步是把OMC系统显示的业务与网元实际的业务信息进行核对，当检测到信息不一致后，将设备上数据同步到OMC上。

1. 支持业务还原功能，当端到端的业务信息丢失时（设备还保留着单点的配置），应提供业务搜索和还原功能。
2. 提供L3 VPN的业务路径视图功能。
3. DHCP Relay配置管理。包括：
4. DHCP Relay的使能和去使能；
5. 配置DHCP服务器的IP地址；
6. 配置到DHCP服务器的跳数限制；
7. 支持DHCP Relay Option 82的使能和去使能。
8. L3 VPN新增加静态路由或者节点后，OMC应支持网络侧路由表的批量自动生成和配置，避免用户逐条配置路由。

OMC系统应支持私网IPv4/v6双栈接入能力，即L3VPN用户侧接口同时支持IPv4和IPv6地址族设置功能，包括不同接口支持分别设置IPv4或IPv6地址，同一个接口支持设置IPv4和IPv6地址。

OMC系统应支持私网IPv4/v6双栈路由转发能力，即同一L3VPN VRF同时支持基于IPv4和IPv6地址路由发布。

## 同步配置和管理

### 频率同步配置和管理

用户可对网元的同步定时参数进行配置和管理，包括：

1. 配置同步定时源的优先级，用户可选取的定时源包括：
   1. 外时钟（2MHz或2Mbit/s）；
   2. 线路输入信号中提取时钟（如STM-N、GE）；
   3. CES业务输入信号（E1、STM-N）中提取时钟；
   4. IEEE 1588V2报文恢复；
   5. 1pps输入；
   6. 设备内时钟自由振荡。
2. 配置外时钟输入/输出类型：2MHz或2Mbit/s；
3. 启动/停止同步质量等级协议；
4. 配置定时源恢复等待时间（WTR）；
5. CES定时恢复方式：差分、自适应、网络定时；
6. 查询时钟源状态（跟踪，自由振荡，保持等）。

### 时间同步相关配置

网管能提供如IEEE 1588v2 等精确时间同步协议相关配置功能。IEEE 1588v2 配置参数分为节点参数和端口参数。

节点参数包括（其中\*代表可配置）：

1. 配置设备的ptp时钟模型（\*）
2. 指定优先级（\*）
3. ptp延时机制选择, e2e 或p2p（\*）
4. 时钟所属ptp域号（\*）

端口参数包括：

1. 开启/禁用端口的ptp功能（\*）
2. 端口的ptp状态
3. ptp同步报文发送频率（\*）
4. ptp通告消息的发送频率（\*）
5. delay\_req消息发送时间间隔（\*）
6. 对端delay\_req消息发送时间间隔（\*）
7. ptp通告消息的接收超时（\*）

## 业务智能调度

OMC系统应基于对全网资源的实时感知，提供智能的业务管理能力，以自动化方式完成业务配置及故障时的业务恢复。

### 5G业务智能调度

OMC系统业务智能调度功能应支持：

1、在L3VPN到边缘的HoVPN场景下，设备上线时，OMC系统支持自动识别接入的私网路由扩散范围，也支持用户对自动识别的路由域进行调整；在接入的私网路由范围内（基站的x2直通），能够实现路由的自动化发布。

OMC系统根据VRF所在网元，带宽、用户侧接口、用户侧路由及L3VPN路由域，自动生成L3VPN网络侧路由，并下发到网元；

当遇到网元离线故障导致网络侧路由扩散失败时，支持网元上线后再次将网络侧路由下发到网元。

2、自动开通L3VPN业务，并可自动关联配置SR-TP隧道：

1. 支持用户指定网元、带宽、路由约束和策略、保护及恢复类型等信息；

支持保护类型包括：

无保护

1:1保护

支持恢复属性（带恢复/永久）

1. OMC系统根据上述的输入进行计算，支持用户预览SR-TP隧道的路径和关键参数（如跳数、带宽等）；
2. 下发到网络设备，实现业务路径的建立；
3. 支持业务使用的路由呈现。
4. 执行以上操作时，成功或失败应给出提示，且失败时应提供清晰的原因。

支持展现基站IP到基站IP、基站IP到核心侧用户侧IP的业务的路径。

用户删除用户侧接口、用户侧路由或VRF，OMC系统会根据用户删除的用户侧配置，自动回收对应的网络侧路由。

支持根据网元、目的IP地址等查看对应的网络侧路由的实际扩散情况，并支持用户手工调整失败的路由并重新发布。

### L3VPN业务配置检查

支持L3VPN业务配置完整性检查,即检查静态路由发布的范围是否符合预期、是否完整，检查内容如下：

1. UPE引入的基站网段是否都已发布给各个SPE；
2. SPE发布给UPE的默认路由是否完整，是否所有UPE都已经发布；
3. SPE发布给NPE的聚合路由是否完整，是否所有NPE和SPE都已经发布；
4. NPE引入的用户侧路由，是否完整发布给所有SPE。

以上检查内容支持用户单选或多选，并支持检查结果的查询和问题提示。

## MTN配置和管理

MTN Group链路接口（简称MTN接口）采用时分复用方式基于以太网PHY层提供硬管道隔离及监视技术。

1. OMC应支持MTN的基础配置，应满足如下功能要求：

a）支持使能端口的MTN模式；

b）MTN Group配置：

在MTN Group创建时，支持将N个PHY端口绑定为MTN Group（FG），OMC支持自动生成MTN Group number，并支持用户配置和修改MTN Group number；

在MTN Group创建时，可供选择的端口应为支持MTN模式的端口（即不支持MTN模式及未使能MTN模式的端口不显示），OMC应支持创建成功或失败的提示，若失败应给出失败原因，例如所选PHY端口不支持MTN模式；

应支持显示MTN Group中已使用和未使用的时隙；

c）MTN Client配置：

在MTN Client创建时，基于MTN Group（FG）支持创建多个MTN Client（FC），并支持自动生成MTNClientID，并支持用户配置和修改MTNClientID；

应支持配置MTNClient的带宽（时隙个数），并支持带宽调整（增加或减少时隙）；

d)MTN Client交叉配置：

支持将两个MTN Client（FC）绑定，形成FC交叉；

e)支持基于MTN Client创建虚拟以太网端口，用于承载LSP或SR隧道。

2. OMC应支持创建MTN Channel，应满足如下功能要求：

a) 应支持MTN Channel的端到端创建、删除、查看和状态监控；

b) 应支持指定MTN Channel的头节点和尾节点自动算路建立一条MTN Channel；

c) 应支持指定MTN Channel建立必需经过和必需不经过节点；

d) 应支持MTN Channel与承载时隙的绑定,一条MTNChannel邦定一个或多个时隙；

e) 应支持MTN Channel时隙或带宽配置调整；

f)应支持MTN Channel的相关OAM配置；

g)应支持MTN Channel的保护配置；

h）应支持MPLS-TP隧道和SR-TP隧道承载于MTN Channel功能；

i) 应支持MTN Channel的信息查看，包括图形化显示MTN Channel，占用的时隙和端口，承载的业务；状态监控（OAM告警、保护倒换的状态）；

j) 应支持MTN Channel的端到端删除。

## Segment Routing配置和管理

Segment Routing源路由技术（简称SR）可在隧道源节点通过一系列表征拓扑路径的Segment段信息(MPLS标签)来指示隧道转发路径。相比于传统隧道技术，Segment Routing隧道不需要在中间节点上维护隧道路径状态信息，提升隧道路径调整的灵活性。SR-TP隧道技术在Segment Routing源路由隧道基础上增强运维能力，扩展支持双向隧道、端到端业务级OAM检测等功能。SR-TP隧道技术提供面向连接业务和面向无连接业务的承载能力，即适用于点到点或点到多点和多点到多点业务。

此外，为满足5G边缘设备X2/eX2业务就近、低时延转发需求，5G网络应支持L3域扩大至边缘接入的L3VPN管理能力，以及L3域扩大至接入汇聚设备的L2VPN和L3VPN分段部署能力。

为适配以上的网络能力，OMC系统应支持如下功能：

### 协议配置

OMC实现Segment Routing的集中控制管理，需支持各种控制协议的配置，包括：SR使能及链路标签配置，ISIS(网络拓扑状态实时发现)、BGP-LS(拓扑状态实时反馈)、PCEP(隧道路径实时下发更新)。

1. SR使能及链路标签配置
2. OMC应支持网元级SR使能
3. OMC应支持配置链路标签，配置链路标签时需指定本地IP地址和远端IP地址，用来唯一标示一条链路。
4. ISIS（网络拓扑状态发现）

OMC应支持新建路由协议IS-IS进程，通过IS-IS协议发现网络拓扑以及实时拓扑状态。包括但不限于配置以下协议参数：

1. ISIS进程号
2. Level
3. SRGB起始值和结束值
4. ISIS接口
5. 网络实体
6. ISIS多拓扑
7. 引入路由
8. 节点标签
9. BGP-LS(拓扑状态反馈)

OMC应支持BGP-LS协议配置，通过BGP-LS协议可将IS-IS域内发现到的网络拓扑、拓扑状态实时反馈给OMC，确保OMC基于最新的网络拓扑及拓扑状态进行隧道路径调整。包括但不限于配置以下协议参数：

1. BGP使能
2. BGP AS号
3. BGP对等体
4. 地址族实例，地址族类型支持Link\_state
5. BGP协议路由引入
6. OMC侧BGP对等体
7. PCEP(隧道路由计算结果下发更新)

OMC应支持配置PCEP协议，通过PCEP协议将集中算路结果实时下发网络。包括但不限于配置以下协议参数：

1. PCE连接，支持配置多个PCE连接（即客户端到主、备Server的PCE连接）

并可查看以下信息：

1. PCE连接
2. PCE会话信息（邻居状态、报文统计信息）

### SR节点和链路配置

支持配置SR节点标签及SR邻接标签：

1）支持配置SR节点的SRGB起止标签；

2）支持配置SR节点的Node SID，需支持配置偏移标签或绝对标签；

3）支持配置SR节点接口的Adjacency SID，且Adjacency SID需支持配置绝对标签。

### SR-TP隧道配置和管理

#### 创建SR-TP隧道

应支持端到端创建SR-TP隧道；

SR-TP隧道创建时，应支持源宿节点、带宽等条件的设置并支持根据输入自动计算端到端路径：

隧道名称；

指定SR-TP隧道源、宿节点（网元）；

配置SR-TP隧道带宽；

指定SR-TP隧道约束条件和算路策略:

1. 节点必经，节点禁止；
2. 路径必经，路径禁止；
3. 最短路径（即跳数最少）；
4. 时延最低
5. 带宽均衡（带宽是指已配置的CIR之和/总带宽）；
6. 双向隧道共路（默认）；
7. 主备隧道分离，源宿节点平行直连无中间节点主备隧道分离（备隧道绕行），支持用户设置；
8. SRLG共享风险链路组（支持用户设置SRLG）；

应遵循标准RFC5440定义的PCEP支持SRLG算路能力

支持提前规划网络风险链路组(SRLG),实现隧道的主路径与保护路径不会存在同一风险链路组中.可以解决主备保护路径不共接入汇聚机房,防止机房掉电业务中断,提升网络可靠性。

1. Affinity亲和属性（支持用户设置亲和属性）；

应该遵循标准RFC 3209 4.7.2章节定义的亲和属性算路约束方法

支持提前规划网络链路亲和属性, 用以实现多业务转发平面. 解决业务按照前期规划的亲和属性拓扑进行自动寻路. 例如将某些高价值链路标示亲和属性给专线使用.承载移动业务的隧道路径就不会运行到属于专线业务亲和属性标识的拓扑, 实现业务隔离。

1. 以上约束条件和算路策略的组合；

支持以下保护方式：无保护、无保护带恢复、1:1、1:1保护带恢复、永久1:1。

带保护情况下，支持保护参数配置，包括：保护类型、返回方式（返回、非返回）、等待恢复时间、倒换迟滞时间、APS协议等。

创建时，OMC应支持查询链路的可用带宽；若已超出链路带宽，则提示错误，隧道配置不予下发；若未超出链路带宽，则正常下发隧道配置。

支持用户选择不同策略（最短路径、带宽均衡）的同时计算并支持预览SR-TP隧道的路径和关键参数（如跳数、带宽等）。

创建成功后应能提供隧道工作路由和保护路由视图。

支持严格约束路径SR-TP隧道，即SR-TP隧道路径由邻接标签栈严格约束；

OMC系统应支持根据设备能力判断是否进行标签粘连，支持SR-TP隧道标签粘连（binding label）超长路径计算功能；

OMC系统应基于实时获取的网络拓扑及拓扑状态进行隧道路径计算和重路由。

在执行创建操作时，成功或失败，应给出提示，且失败时，应提供清晰的原因。

支持创建L3VPN业务时，承载于SR-BE和SR-TP隧道。

#### 查询/修改SR-TP隧道

支持查询和修改SR-TP隧道的属性（\*为可修改）：

a) 隧道标识

b) 源宿网元

c) 隧道名称（\*）

d) 工作/保护路由,包括约束条件

e) 带宽

f) 隧道OAM属性

g) 保护类型

h)开通时间、开通用户等，如对隧道修改需同步更新最后的开通时间与用户信息。

i)备注信息（\*）

#### 删除SR-TP隧道

支持删除SR-TP隧道。

#### SR-TP隧道重路由

支持SR-TP隧道的集中重路由保护机制。

由于网络调整、改造频繁，OMC系统应能支持SR-TP隧道重路由能力关闭（时段、范围、保护类型），避免在网络施工过程中业务路由频繁调整，造成网络改造的不可控。

根据计算出的新的业务路径进行路径重配置，使受影响的业务具备相应的保护类型。

SR-TP隧道重路由路径计算满足下述要求：

1）每条隧道均应根据创建时的输入条件进行重路由计算，即根据源宿网元、带宽、保护方式计算出满足需求的路由；

无法计算出满足带宽需求的路由时，则按照无带宽约束条件进行路由计算，并提示用户该隧道已降速；

2）多条隧道重路由时，先重路由隧道优先占用带宽资源；

3）未能计算出新的路径，则按照保护和恢复的类型进行排序，并支持查看重路由失败原因。

当网络故障恢复时，OMC系统应能支持重路由路径的恢复（参考9.13.1.4节）。

#### 恢复的性能要求

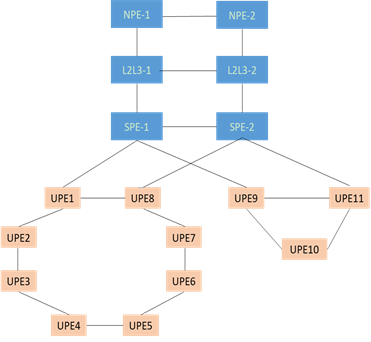


图1-1 组网图

性能要求：不少于2000条带恢复的业务，SPE-1到接入环每个UPE（1-8）网元的至少250条隧道，业务全部故障，从故障发生到重路由成功不大于8分钟。

#### SR-TP隧道重优化

在网络结构变化时，OMC系统可实现对SRTP隧道路由的优化。

#### SR-TP隧道自动发现

OMC支持SR-TP隧道自动发现。

### 重路由OAM配置管理

应支持以下SR-TP层OAM管理功能：

1、OAM初始配置，包括：

MEG配置、MEP配置、使能/禁止和帧发送周期等参数设置；

2、隧道层OAM功能：

1)连通性验证：

支持CC功能禁止/使能，支持设置时间间隔参数，支持查询连通性验证结果。当连通性验证失败时，可查询相关OAM连通性验证失效告警。

2）环回（LB）功能

支持启动LB功能，网管支持查询环回结果；

3）RDI告警功能

支持RDI禁止和使能功能，网管支持查询上报的RDI告警；

4）性能测量

包时延（DM）、包时延变化和丢包率（LM）性能测量；网管可设置DM报文的长度和优先级；网管支持查询性能测量结果。

### PING/Traceroute检测

网管系统应支持SR Ping和Traceroute，用于定位SR隧道的故障。

1、SR-TP和SR-BE都需要支持Ping/Trace。

2、支持将Trace出来的路径结果上报OMC系统并显示实际业务路径。

## 5G快速基础配置

### 资源池规划

支持基础配置资源池的规划，限制这些配置生成的范围。

1. LSR-ID（Router ID）资源池：

支持规划LSR-ID的地址段（起始地址和结束地址），对网元进行基础配置时，可使用资源池中分配未使用的LSR-ID，下发到该网元。

1. 链路IP资源池：

支持规划链路的IP地址段（起始地址和结束地址），对链路进行基础配置时，可使用资源池中分配未使用的链路IP，下发到该网元。

1. IGP进程号资源池：

支持规划IGP进程号的范围，在配置IGP域时，指定IGP进程号资源池后，可在资源池内分配未使用的IGP进程号。

支持查看已规划的LSR-ID（RouterID）资源池、链路IP资源池、IGP进程号资源池，显示地址段、进程号的范围和在用状态。

支持删除已规划的LSR-ID（RouterID）资源池、链路IP资源池、IGP进程号资源池。

### 逻辑网络规划

支持对逻辑网络进行规划，以作为基础配置下发的依据。

1. 规划地市：

对于省集中场景，能够在网络中规划多个地市。支持规划地市的名称、备注。支持规划地市对应的AS号。

1. 规划IGP进程：

支持规划IGP进程号或IGP进程号资源池。

支持查看已规划的逻辑网络，规划的地市名称、备注、对应的AS号；IGP进程号或IGP进程号资源池。

### 网元基础配置自动生成和发放能力

支持将网元及链路规划到IGP域中，并自动生成5G相关基础配置并下发到网元。

能够生成的基础配置包含：LSR-ID（Router ID），全局MPLS配置，网络侧端口IP地址，IGP进程相关配置（含IGP进程号），网络侧端口IGP配置，全局SR配置，SR节点标签，SR邻接标签，AS号，BGP-LS相关配置，PCEP相关配置。

网元在OMC上线通过此功能下发基础配置后，用户即可开始隧道和L3VPN业务的配置。

## 网络切片管理

OMC系统应支持如下功能：

1. 支持基于MTN技术对物理网络进行逻辑划分，新划分的虚拟网络vNet由虚拟网络节点vNode和虚拟网络链路vLink组成；该虚拟网络即网络切片(vNet=vNode+vLink)；
2. 支持不同速率（包括5G和小于5G）vNet的创建、修改、删除、查询、属性展示等功能，其直接承载路径可以是5G颗粒的MTN通道，也可是小颗粒（小于5G)的通道；
3. 支持vNet网络拓扑呈现；
4. 支持基于vNet创建SR隧道、L3VPN业务，基于虚拟网络进行SR路径计算，不同虚拟网络的业务实现隔离。
5. 在已有切片和新建切片上均支持批量添加已有MTN 链路（不少于1000）。资源范围（选择：1、全网，2、环系统中的一个或多个环，3、指定的MTN 链路）。
6. 在已有切片和新建切片上均支持批量新建MTN 链路（不少于1000）。资源范围（选择：1、全网，2、环系统中的一个或多个环，3、指定的MTN的物理链路）。
7. 支持基于网络切片可以查看该网络切片的所有SR-TP隧道

## 高精度时钟管理

网管提供智能化的同步网络配置管理、保护恢复、故障管理以及性能管理等功能，防止同步网络定时环、1588v2广播风暴、同步网络配置错误等问题，方便同步网络规划部署，增强同步网络运行安全可靠性，提升同步网络运维管理效率。

智能时钟包括时钟同步网络智能管理和时间同步网络智能管理。

### 时钟同步网络规划

根据设定的策略，对指定的网络进行时钟同步网络路径规划，应支持环网优先策略和最短跳数策略，规划结果应避免出现定时环。

**环网优先策略**基于拓扑中环型网络结构进行主备用时钟规划。

当单个环网具有一个时钟源注入时，从时钟源注入节点出发，将环网其中一个链路方向作为环上设备的主用源方向，将环网另外一个链路方向作为环上设备的备用源方向。对于环网时钟源注入节点，不在该环上配置主备用源，只提供时钟输出。

当单个环网具有两个及两个以上时钟源注入时，选择其中一个时钟源为主用，一个时钟源为备用。从该环网的主用时钟源注入节点开始，将环网其中一个链路方向作为环上设备的主用源方向。从该环网的备用时钟源注入节点开始，沿环网另外一个链路方向作为环上设备的备用源方向。对于环主用时钟源注入节点不在该环上配置主用源，只配置备用源。对于环备用时钟源注入节点不在该环上配置备用源，只配置主用源。

**最短跳数优先策略**支持以距离时钟源跳数最短的路径作为主用路径进行时钟规划，其他路径选为备用。

当网络具有多个时钟源时，多时钟源在规划时具有等同地位，不区分主用备用。

### 时间同步网络规划

网管根据域内物理拓扑和网元时间同步属性，自动规划和配置需要使能1588v2时间同步功能的端口。

对于每条物理链路，均需要选择端口使能1588v2时间同步功能。

### 同步网络配置检测

在网络已具备同步配置的情况下，网管支持根据域内物理拓扑和网元上报的同步配置，进行同步网络的检测，检测功能包括：

1）检测域内是否有缺失主用或备用同步源配置的节点。

2）检测域内是否有同步配置存在定时环风险的网络区域。

3）检测域内是否有时钟同步跳数（从域时钟源到节点）超过阈值的节点。该阈值应可设置，默认值建议为20。

4）检测域内是否有时间同步跳数（从域时间源到节点）超过阈值的节点。该阈值应可设置，默认值建议为30。

### 同步网络告警管理

网管支持根据域内设备上报的同步告警，进行故障分析。

### 同步网络性能管理

网管支持对同步网络进行时间同步不对称性能的检测评估，具体地，网管自动检测全网具有1588v2 Passive端口的节点设备，开启设备的Passive节点时间同步性能监测功能，并收集各个Passive节点时间差值以及越限告警，用于评估网络时间同步不对称性。

# 拓扑管理

拓扑管理用于构造并管理整个传送网络的拓扑结构。通过主拓扑完成网络的拓扑管理。支持在主拓扑上以图形的方式展示网元、子网和连接在网络中的拓扑关系，支持在主拓扑上对网元、子网、连接、路径的浏览、创建、搜索、配置和维护管理。

拓扑展现应友好、稳定。

## 拓扑视图

网络拓扑视图包括对象显示和实时告警显示，各视图之间可无障碍切换，支持拓扑搜索和手工创建两种方式建立网络拓扑视图，并对拓扑对象进行管理, 网络拓扑视图应能提供如下网络拓扑结构：

1. 网络资源图：显示所管辖的所有网元、子网，以相应的图标表示；
2. 设备面板图：显示机框，包括具体的槽位、单元盘、端口等，并标注相应的名称。
3. 物理视图：显示所管辖的所有网元、子网及其连接关系。节点可以是网元、子网，连线表示网元、子网之间的物理连接关系。应能提供子网的展开（收缩）功能，以显示构成该子网的各个网元。子网应可支持嵌套，要求至少支持6层嵌套。

拓扑上能够显示网元的实时状态，比如网元的通讯状态、是否是网关网元、网元数据跟网管是否一致，网元的配置状态等。

1. 隧道路由视图：显示指定隧道的工作和保护路径视图（源宿节点、经过的节点和物理链路），应能提供隧道及其承载的所有伪线的关联功能。
2. 伪线（PW）路由视图：显示指定伪线的路由视图，包括源宿节点、经过的节点和隧道，应能提供伪线与其所承载的所有客户业务的关联功能，并可以批量选择隧道关联到其承载的伪线。
3. 时钟和时间同步视图。视图上应能图形化直观显示时钟同步和时间同步的网络拓扑，实时体现网元主从时钟跟踪路径，网元各个端口的同步状态。
4. DCN视图：清晰显示全网的DCN子网组网拓扑，便于DCN子网规划、优化。网管支持导航到配置界面查看网元端口的DCN状态。
5. 客户业务视图：显示指定业务的源宿端点、路由视图。
6. 网元与子网的拓扑图标，可根据其功能类型选择不同图标，图标外观应有明显差异，以便于维护人员在网管上可以快速区分辨识。

## 拓扑编辑

1. 支持手工创建子网、网元。
2. 支持从拓扑图中删除网元、连接、子网对象。
3. 支持手工修改拓扑网元名称、网元IP、网元别名，网元位置信息等。
4. 支持手工修改拓扑对象，保存网元名称、别名、网元坐标信息等信息。
5. 支持搜索、创建、删除、修改物理连接功能。物理的光纤、链路属性中可以支持定义线路类型（支持直线、曲线、折线等至少任意一种）、线路宽度、线路颜色以及线路备注。光纤的属性中应包括设置时间和操作账号。
6. 支持创建子网，而且子网创建支持多级嵌套。
7. 支持虚拟网元创建，支持配置虚拟网元与本网络中网元之间的连接

对于传输网元对接很多业务侧重要设备，通过虚拟网元表示，通过修改修改虚拟网元名称、坐标和备注等属性来直观反映业务侧设备信息。

1. 支持修改拓扑对象图标。

网元、子网的拓扑图标可以支持修改，可根据其功能类型选择不同图标，图标外观应有明显差异，以便于维护人员在网管上可以快速区分辨。

1. 支持拓扑位置调整

当网元或子网的物理位置发生变化时，为方便后续的查看和管理，应该及时调整其在拓扑视图中的位置。

1. 支持同一个网元在多个子网中的呈现。
2. 支持拓扑布局功能

对于选择拓扑对象按所设置的布局方式进行排列。

1. 支持设置拓扑背景

支持根据设备的布局设置合适的背景图。通过背景图和设备位置的恰当设置，可以直观地了解设备所在的地理位置。

1. 支持拓扑过滤：

拓扑视图能够显示子网、连接、网元节点等类型的对象。当对象数量过多时，拓扑视图可能显得很拥挤，此时可以使用过滤显示条件进行过滤，从而在视图上保留关注的对象。

1. 支持拓扑数据保存功能，

通过导出拓扑数据到文件的功能，可以将物理视图上指定的数据以文件形式保存到客户端本地，方便维护查看以及备份。

1. 支持拓扑自动发现

设备具备相应功能时，当网管实现网关网元监控时，可实现其他设备的自动发现，网管上支持自动生成拓扑；

1. 支持拓扑搜索

拓扑主视图界面内，通过快捷方式或快捷按钮，提供基于人工输入界面，以供模糊查找搜索拓扑视图中某些特定对象（如：子网名称、网元名称、网元类型、设备型号、网元ID等）。

1. 支持设置物理连接和路径的命名规则；

## 拓扑浏览

1. 拓扑图应能放大和缩小，并且能上下、左右移动、锁定解锁功能，在拓扑图上用不同的图标来标识不同类型的节点（网元或子网）；
2. 网管系统应允许操作员通过点击网元图标，获得网元的详细配置信息，并可执行网元配置和其他管理功能；
3. 系统应保证页面显示内容的一致性，当多个用户同时操作系统的相同对象时，不同用户看到的显示内容相同；
4. 拓扑中网元对象提供告警状态、脱管状态、同步状态等几种常规状态。

-同步状态：实时反映网络设备配置的变更情况，网元配置信息的改变也应能通过某种方式（如图标闪烁或其他醒目的方式）在拓扑图中通知用户；

-脱管状态：当网管系统与网元之间的通信出现故障时应能在拓扑图上反映出来；

-告警状态：实时反映被管网元的告警事件，告警应以可视、可闻的形式提醒维护人员：

* 1. 系统对实时的业务告警事件做出及时反应，并可深入显示告警相关的设备，在拓扑图中以相应设备变色等形式提示；
  2. 告警信息未确认应保持对用户的提示；
  3. 系统应支持彩色高分辨率，并可根据用户需要进行设置。

告警级别与颜色的对应关系建议见下表：

表2-1 告警级别与颜色对应表

|  |  |
| --- | --- |
| **告警级别** | **颜色** |
| 紧急告警 | 红色 |
| 主要告警 | 橙色 |
| 次要告警 | 黄色 |
| 提示告警 | 蓝色 |
| 无告警（告警清除） | 绿色 |

1. 拓扑通过鼠标悬停操作获得与网元或网元间连接线相关的信息。
2. 当拓扑窗口中只能显示视图的部分内容时，可通过“鸟瞰图”浏览当前视图的全貌，并定位拓扑窗口显示的区域。
3. 拓扑图导航功能
   * 可逐层细化显示网元的信息，并提供返回前一视图与返回上层视图的功能；
   * 可分层显示节点间不同层次的路径；
   * 可以根据需要切换到不同的拓扑视图；
   * 可以拖动鼠标看到不在视野范围的视图；
4. 拓扑图定位功能
   * 可在当前或其他视图中，查找指定的网元；
   * 可以根据需要使用不同的方式选择网元，如单个网元选择和区域选择。
   * 在拓扑图上选中某个网元，能够过滤出所有与此网元有tunnel关联的网元的拓扑图。比如某网元故障或者某段光缆故障，可通过过滤此网元tunnel关联的所有网元的拓扑，准确判断出故障影响的网元数、影响范围等。

# 管控融合的故障管理

## 告警属性

### 告警名称

网管系统支持告警名称的重定义功能，用户可以根据运维要求将系统预定义的告警名称修改成用户期望的告警名称，重定义的告警名称支持中文。

告警列表:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **告警类型** | **告警原因** | | | | **告警名称-中文** |
| 1. | MPLS－TP告警 | PW层 | | 连续性丢失（LOC） | | PW连续性丢失 |
| 2. | 告警指示信号（AIS） | | PW告警指示信号 |
| 3. | 远端缺陷指示（RDI） | | PW远端缺陷指示 |
| 4. | 锁定LCK | | PW锁定 |
| 5. | 未期望的MEG | | PW未期望的MEG |
| 6. | 未期望的MEP (UNM) | | PW未期望的MEP |
| 7. | 未期望的CV包周期 | | PW未期望的CV包周期 |
| 8. | 客户侧信号失效（CSF） | | PW客户侧信号失效 |
| 9. | LSP层 | | 连续性丢失（LOC） | | LSP连续性丢失 |
| 10. | 告警指示信号（AIS） | | LSP告警指示信号 |
| 11. | 远端缺陷指示（RDI） | | LSP远端缺陷指示 |
| 12. | 锁定LCK | | LSP锁定 |
| 13. | 未期望的MEG | | LSP未期望的MEG |
| 14. | 未期望的MEP UNM | | LSP未期望的MEP |
| 15. | 未期望的CV包周期 UNP | | LSP未期望的CV包周期 |
| 16. | 前向缺陷指示（FDI）（可选如部署Y.1711则此告警替代AIS） | | LSP前向缺陷指示 |
| 17. | 后向缺陷指示（BDI）（可选如部署Y.1711则此告警替代RDI） | | LSP后向缺陷指示 |
| 18. | 段层 | | 连续性丢失(段层\_LOC) | | 段层连续性丢失 |
| 19. | 远端缺陷指示（RDI） | | 段层远端缺陷指示 |
| 20. | 锁定LCK | | 段层锁定 |
| 21. | 未期望的MEG（段层\_MMG） | | 段层未期望的MEG |
| 22. | 未期望的MEP ID（段层\_UNM） | | 段层未期望的MEP ID |
| 23. | 未期望时间间隔告警（段层\_UNP） | | 段层未期望时间间隔告警 |
| 24. | ETHOAM告警 | 以太网连续性丢失(ETH\_LOC) | | | | 以太网连续性丢失 |
| 25. | 以太网告警指示信号(ETH-AIS) | | | | 以太网告警指示信号 |
| 26. | 以太网远端缺陷指示（ETH-RDI） | | | | 以太网远端缺陷指示 |
| 27. | 未期望的MEP\_ID（ETH\_UNM） | | | | 以太网未期望的MEP\_ID |
| 28. | 未期望的MA层次 | | | | 以太网未期望的MA层次 |
| 29. | 未期望的MEG (误连接) | | | | 以太网未期望的MEG |
| 30. | 未期望的时间周期（ETH\_UNP） | | | | 以太网未期望的时间周期 |
| 31. | ETH锁定LCK | | | | ETH锁定 |
| 32. | 以太网环回信号超时（ETHLB\_LOS） | | | | 以太网环回信号超时 |
| 33. | 以太网业务告警 | 信号丢失（ETH-LOS） | | | | 以太端口信号丢失 |
| 34. | 丢包次数高于上限告警 | | | | 丢包次数高于上限 |
| 35. | 接收到的坏包字节数高于上限告警 | | | | 接收到的坏包字节数高于上限 |
| 36. | 发送的坏包字节数高于上限告警 | | | | 发送的坏包字节数高于上限 |
| 37. | 对齐错误数高于上限告警 | | | | 对齐错误数高于上限 |
| 38. | 校验错误数高于上限告警 | | | | 校验错误数高于上限 |
| 39. | TDM业务告警 | 客户侧2M | | | 信号丢失（LOS） | —   E1信号丢失 |
| 40. | 帧丢失（LOF）（针对成帧2M，可选） | —   E1帧丢失 |
| 41. | 告警指示信号（AIS） | —   E1告警指示信号 |
| 42. | 远端告警指示（RAI）（针对成帧2M，可选） | —   E1远端告警指示 |
| 43. | ES性能越限告警 | —   E1误码秒性能越限告警 |
| 44. | RMFAI远端多帧告警指示（针对成帧2M，可选） | —   RMFAI远端多帧告警指示 |
| 45. | CAS MFL多帧丢失（针对复帧结构的2M，可选） | —   CAS MFL多帧丢失 |
| 46. | CRC越限告警 | —   E1 CRC越限 |
| 47. | 客户侧155M | 物理接口 | | 信号丢失（LOS） | STM信号丢失 |
| 48. | 再生段 | | 帧丢失(LOF) | STM帧丢失 |
| 49. | 帧失步（OOF） | —   STM帧失步 |
| 50. | 再生段误码率越限(B1\_EXC) | —   STM再生段误码率越限 |
| 51. | 再生段信号劣化(B1\_SD) | —   STM再生段信号劣化 |
| 52. | 再生段跟踪标识失配（J0 RS\_TIM） | —   STM再生段跟踪标识失配 |
| 53. | 复用段层 | | 复用段远端缺陷指示(MS\_RDI) | STM复用段远端缺陷指示 |
| 54. | 复用段误码率越限(B2\_EXC) | STM复用段误码率越限 |
| 55. | 管理单元指针丢失（AU\_LOP） | STM管理单元指针丢失 |
| 56. | 复用段告警指示(MS\_AIS) | STM复用段告警指示 |
| 57. | 复用段信号劣化(B2\_SD) | STM复用段信号劣化 |
| 58. | 高阶通道 | | 高阶通道跟踪标识失配（J1 HP\_TIM） | STM高阶通道跟踪标识失配 |
| 59. | 高阶通道未装载(HP-UNEQ) | STM高阶通道未装载 |
| 60. | 高阶通道远端缺陷指示(HP-RDI) | STM高阶通道远端缺陷指示 |
| 61. | 高阶通道误码率越限(B3\_EXC) | STM高阶通道误码率越限 |
| 62. | 高阶通道净负荷失配(HP-PLM) | STM高阶通道净负荷失配 |
| 63. | 高阶通道信号劣化(B3\_SD) | STM高阶通道信号劣化 |
| 64. | 管理单元告警指示(AU\_AIS) | STM管理单元告警指示 |
| 65. | 低阶通道（适用于通道化STM-1） | | 支路单元指针丢失 | STM支路单元指针丢失 |
| 66. | 支路单元复帧丢失(TU-LOM) | STM支路单元复帧丢失 |
| 67. | 低阶通道跟踪标识失配(LP-TIM) | STM低阶通道跟踪标识失配 |
| 68. | 低阶通道未装载(LP-UNEQ) | STM低阶通道未装载 |
| 69. | 低阶通道远端缺陷指示(LP-RDI) | STM低阶通道远端缺陷指示 |
| 70. | 低阶通道误码率越限(LP-EXC) | STM低阶通道误码率越限 |
| 71. | 低阶通道误码率劣化（LP-SD） | STM低阶通道误码率劣化 |
| 72. | 低阶通道净负荷失配(LP-PLM) | STM低阶通道净负荷失配 |
| 73. | 低阶通道告警指示(TU-AIS) | STM低阶通道告警指示 |
| 74. | 硬件设备告警 | 单元盘脱位 | | | | 单元盘脱位 |
| 75. | 单元盘故障 | | | | 单元盘故障 |
| 76. | 单元盘失配 | | | | 单元盘失配 |
| 77. | 设备临终遗言（设备掉电提示、远端网元掉电） | | | | 远端设备掉电 |
| 78. | 环境告警 | 电源故障 | | | | 电源故障 |
| 79. | 环境温度过限 | | | | 环境温度越限 |
| 80. | 业务保护倒换告警 |  | | | | VRRP主备切换指示 |
| 81. |  | | | | PW冗余主备切换指示 |
| 82. |  | | | | VPN FRR主备切换指示 |
| 83. |  | | | | IP FRR 倒换状态指示 |
| 84. | L3VPN告警 | FRR保护降级（主或备中断） | | | | FRR保护降级(主或备中断) |
| 85. | FRR倒换/切换 | | | | FRR倒换 |
| 86. | FRR保护中断 | | | | FRR保护中断 |
| 87. | MTN告警 | MTN Group告警 | | | | MTN\_Group\_Mismatch |
| 88. | PHY\_Num\_Mismatch |
| 89. | PHY\_Map\_Mismatch |
| 90. | LOF |
| 91. | LOM |
| 92. | RPF |
| 93. | MTN\_calender\_mismatch |
| 94. | Slicing Ethernet OAM告警 | 连续性丢失告警 | | | | LOC |
| 95. | CC周期不匹配告警 | | | | Unexpected\_period |
| 96. | 远端告警指示 | | | | RDI |
| 97. | 客户信号的本地故障 | | | | CS\_LF |
| 98. | 连通性验证错误告警 | | | | CS\_RF |
| 99. | 时钟同步告警 | 频率输入参考源丢失 | | | | 频率输入参考源丢失 |
| 100. | 时钟失锁 | | | | 时钟失锁 |
| 101. | 同步处理硬件故障 | | | | 同步处理硬件故障 |
| 102. | 频率输出模块故障 | | | | 频率输出模块故障 |
| 103. | ESMC报文丢失 | | | | ESMC报文丢失 |
| 104. | 当前参考源FREQ越限 | | | | 当前参考源FREQ越限 |
| 105. | 频率输入参考源SSM等级劣化 | | | | 频率输入参考源SSM等级劣化 |
| 106. | 优先级列表中参考源FREQ越限 | | | | 优先级列表中参考源FREQ越限 |
| 107. | PTP检测频偏越限 | | | | PTP检测频偏越限 |
| 108. | 频率参考源倒换 | | | | 频率参考源倒换 |
| 109. | 设备频率同步状态切换 | | | | 设备频率同步状态切换 |
| 110. | 时间同步告警 | 1PPS+TOD输入丢失 | | | | 2PPS+TOD输入丢失 |
| 111. | 时间失锁 | | | | 时间失锁 |
| 112. | 同步处理硬件故障 | | | | 同步处理硬件故障 |
| 113. | 1PPS+TOD输入劣化 | | | | 2PPS+TOD输入劣化 |
| 114. | PTP输入劣化 | | | | PTP输入劣化 |
| 115. | PTP物理链路告警 | | | | PTP物理链路告警 |
| 116. | Announce报文丢失 | | | | Announce报文丢失 |
| 117. | Sync或Delay\_Resp报文丢失 | | | | Sync或Delay\_Resp报文丢失 |
| 118. | 时间偏差累加和越限 | | | | 时间偏差累加和越限 |
| 119. | 外部参考时间和PTP时间差值越限 | | | | 外部参考时间和PTP时间差值越限 |
| 120. | Passive节点时间差值越限 | | | | Passive节点时间差值越限 |
| 121. | Slave端口倒换 | | | | Slave端口倒换 |
| 122. | GM时钟切换 | | | | GM时钟切换 |
| 123. | 设备时间状态切换 | | | | 设备时间状态切换 |
| 124 | SR-TP告警 | 连续性丢失（LOC） | | | | LSP 连续性丢失 |
| 125 | 远端缺陷指示（RDI） | | | | LSP 远端缺陷指示 |
| 126 | 未期望的MEG | | | | LSP 未期望的MEG |
| 127 | 未期望的MEP (UNM) | | | | LSP 未期望的MEP |
| 128 | 未期望的 CV 包周期 UNP | | | | LSP 未期望的CV 包周期 |
| 129 | 端口告警 | 信号丢失（ETH-LOS） | | | | 以太网输入信号丢失 |
| 130 | ALM\_ALS | | | | 激光器自动关断告警 |
| 131 | ETH\_LINK\_DOWN | | | | 网口连接故障告警 |
| 132 | 光模块整体功能失效 | | | | 光模块整体功能失效 |
| 133 | 物理端口Down | | | | 物理端口Down |
| 134 | 近端故障告警 | | | | 近端故障告警 |
| 135 | 远端故障告警 | | | | 远端故障告警 |
| 136 | 链路断开告警 | | | | 链路断开告警 |

### 告警类型

网管系统应支持以下五种告警类型：

1. 设备告警：与设备硬件有关的告警；
2. 服务质量告警：反映传输性能的告警，如性能劣化、越门限等；
3. 通信告警：与传输状态有关的告警，如信号丢失、帧丢失、信号劣化、通信协议告警等；
4. 环境告警：通过外部接入的动力环境告警，如火警、门禁告警、温度/湿度告警等；
5. 处理失败告警：与软件处理有关的告警。

### 告警级别

网管系统应支持以下告警严重性级别：

1. 紧急告警（Critical）：使业务中断并需要立即采取故障检修的告警；
2. 重要告警（Major）：影响业务并需要立即采取故障检修的告警；
3. 次要告警（Minor）：不影响现有业务，但需采取检修以阻止恶化的告警；
4. 提示告警（Warning）：不影响现有业务，但有可能成为影响业务的告警，可视需要采取措施；

### 告警状态

网管系统应支持以下告警状态：

1. 未确认当前告警： 用户尚未确认且未被清除的告警；
2. 已确认当前告警： 用户已确认且未被清除的告警；
3. 未确认已清除告警： 即锁定告警， 用户尚未确认而已被清除的告警；
4. 已确认历史告警： 用户已确认且已被清除的告警。

### 告警信息

网管系统支持告警携带方便运维与故障定位的信息，相应的信息支持在告警界面呈现。告警信息应该包括如下内容：

1. 告警源：产生告警的网元或者OMC系统；
2. 定位信息：产生告警的对象，如单板、端口、激光器等；
3. 附加信息：告警详细描述。
4. 产生原因与修复建议。
5. 端口角色：若为端口告警则标识出该端口的端口属性UNI/NNI

对性能越限类告警，网管系统应显示当前的性能值、门限值以及处理建议。

对故障类告警，网管系统应显示受影响的业务类型、业务数量以及处理建议。

## 告警处理

### 告警级别重分配

用户可以为指定的告警原因重新分配严重级别。

### 告警确认

网管系统应提供告警确认功能。网管系统应支持操作用户对所有从网元接收到的，尚未确认的告警进行确认。未经确认的告警应保持对用户的提示，直到用户进行确认。

### 告警清除

网管系统应提供告警清除功能。网管系统提供的清除手段包括手工和自动清除两种方式。当网管系统收到网元自动上报的告警清除后，应将当前告警中相应的记录转移至历史告警中。对由网络通信故障造成的告警清除信息丢失，操作用户可手动清除指定告警。网管系统应在日志中记录用户的手动清除操作。

### 告警锁定

处于清除状态的未确认的告警，称为锁定告警。锁定告警保留在当前告警列表中，并应有相应图标显示。

### 告警过滤

告警过滤是指网管系统根据用户设定的过滤条件，有选择地显示当前或历史告警事件并可对生成的报告进行输出。告警显示过滤仅是告警信息的屏幕显示过滤，不应影响任何告警事件的上报及其存储。网管系统支持根据不同的过滤要求创建不同的过滤模板，用户可以根据模板打开不同告警监控界面（如工程告警）。告警显示过滤的条件可为以下信息，或以下信息的‘与’/‘或’的任意组合：

1. 告警源；
2. 告警级别；
3. 告警类型；
4. 告警时间；
5. 管理区域；
6. 确认状态（确认/未确认）。

### 告警屏蔽

告警屏蔽也称告警上报过滤。用户可设置告警上报条件，被管网元根据用户的设定，向网管系统上报符合条件的告警。用户可设定下面的告警上报条件及其‘与’/‘或’任意组合：

1. 告警源；
2. 类型级别；
3. 告警类型。

另外用户应能设置网元告警延迟时间，在指定延迟时间内，网元不再产生重复告警。

### 告警反转

网管应支持告警批量反转功能。应用告警反转功能时，网元上报的端口的告警状态与其实际告警状态是相反的。即NE中未加载业务的端口不上报告警，而当端口加载业务后则上报相关告警提示(LOS)；如果端口又回到未加载业务状态，则上报告警清除。告警反转功能不影响LOS告警对其它告警的抑制。

### 告警备注

网管系统可批量设置告警备注，备注中可手工设置告警可能产生的原因，一般处理原则及其它相关信息，并且支持按告警备注字段对告警进行过滤功能。

## 告警监控和呈现

### 显示内容和方式

网管系统应能实时收集网元发出的告警信息，并自动更新当前告警列表。对于新接收到的告警，网管系统至少应支持如下提示方式：

1. 颜色变化；
2. 图标闪烁；
3. 声音提示。

网管系统应允许用户根据下列条件设置新接收到告警的提示方式：

1. 告警源；
2. 告警类型；
3. 告警严重级别。

网管系统应在网络拓扑图中以不同形式如链路变色等，显示告警发生的位置及告警信息，并提示用户对告警进行确认。网管系统应针对不同严重级别的告警，以不同的颜色进行显示。对于已确认的告警，应以某种方式与未确认告警相区别。对于同一网络资源有多个告警发生时，图标颜色应与当前最高级别告警对应；当较高等级告警清除后，再顺序显示次等级告警的对应颜色。

网管系统支持呈现不同子网的告警数量，并实时自动更新相应的子网告警数量。

### 告警模板管理

网管系统支持告警模板管理能力，告警模板包括当前告警模板、历史告警模板、告警统计模板、事件日志模板等。网管系统支持设置具体模板为默认监控模板。

用户可以根据不同的维护域设置不同的告警模板，或者根据不同的角色运维要求设置不同的模板。

用户在网络工程阶段或者业务割接阶段，可以在网管系统上定义不同的告警模板。用户可以在工程阶段或者业务割接阶段前后通过告警模板查看的告警信息对比。

网管系统的告警模板包括如下的参数：

1. 模板名称；
2. 模板类型；
3. 创建者；
4. 备注。

### 多窗口监控

网管系统可以同时监控不同的告警界面，用户在不同的告警界面可以设置不同的告警过滤条件或者选择预先创建好的模板，能够更加精确的呈现需求告警，例如：根据需要创建监控界面和维护界面、工程界面、影响业务界面、自定义界面等，详细包括如下：

1. 监控界面：显示与故障相关的根源告警。
2. 维护界面：维护界面能够显示根源告警、衍生告警等全量告警。
3. 工程界面：只显示工程态的告警。
4. 自定义界面：由维护人员自定义的特殊需求显示界面，例如自定义界面呈现系统中所有的LOS告警，或区分接入层、汇聚层、核心层分层呈现相应层次的告警。

## 告警查询和统计

网管系统应提供对当前告警或者历史告警的查询和统计功能，并以表格或图形方式显示。查询或统计的条件为以下信息或以下信息的任意‘与’/‘或’组合：

1. 告警源；
2. 告警发生时间；
3. 告警严重等级；
4. 告警原因；
5. 告警状态；
6. 告警清除时间；
7. 告警确认时间
8. 确认用户；
9. 告警历时。

同时，网管系统应提供告警查询或统计信息的输出功能，网管系统允许用户设置告警输出条件，告警输出目的地和告警输出方式。

网管系统支持的告警输出条件包括以下信息或以下信息的‘与’/‘或’组合：

1. 告警类型；
2. 严重级别；
3. 告警源。

网管系统应至少支持如下告警查询/统计报告的输出方式：

输出为一个文件。

应支持在网管界面中查询至少12个月的历史告警。

## 告警压缩

### 工程告警设置

网管系统应具备工程告警状态管理，以便于在工程施工期间，有效抑制工程网元/单板/端口的相关告警信息，用户可根据子网批量选择网元，也可以选择特定的网元/单板/端口进行维护态设置。

网管系统可以设置在告警监控窗口中是否呈现工程告警以及设置是否上报OSS系统。

网管系统可以设置工程施工时间段，在此施工时间段处于工程态的资源对象产生的告警应自动标记为维护态；不在此时间段产生的告警为正常态。

工程任务包括如下的参数：

1. 名称;
2. 开始时间：
3. 结束时间：
4. 对象列表：
5. 备注：
6. 工程任务描述：
7. 联系人。

网管系统支持的工程任务数不少于200个，单个工程任务支持的网元/单板/端口资源数量不少于100个。

### 闪断告警分析

用户可自定义周期和在一个周期内产生同一条告警的次数，满足条件的告警即为闪断告警。闪断告警应进行提示，只增加次数，不再上报。

## 告警关联分析

### 相关性分析原则

网管系统应根据网络配置信息，以及接收的告警信息频度和种类，对告警信息进行综合关联分析，快速、自动完成故障根源的定位，正确区分出根源告警和衍生告警，并提供处理建议，以提升故障处理效率。

为保证告警上报的实时性，网管系统应支持告警全量上报OSS。

#### 设备类

设备会对单设备内产生的告警进行相关性分析，只向OMC上报根源告警并抑制掉衍生告警。网管系统应能以图形显示方式或文本显示方式将设备或通信故障定位在网元、单元盘或端口上，并给出可能的故障原因。

#### 路径和业务类

网管系统支持根据告警查询影响的业务，并以列表方式显示。

网管系统支持根据业务路径查看业务路径上的相关告警明细。

网管系统支持根据业务路径进行告警相关性分析，方便故障的定位。

网管系统支持基于端口、路径以及业务的告警相关性分析，支持但不限于如下规则；应提供关联规则配置能力，用户可自定义关联规则。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 相关性分析规则 | 根源告警 | 衍生告警 | 备注 |
| 1 | 以太端口->LSP MPLS-TP OAM | 信号丢失（ETH-LOS） | 连续性丢失（LOC） | 客户层服务层关系 |
| 2 | 以太端口->LSP MPLS-TP OAM | 校验错误数高于上限告警 | 连续性丢失（LOC） | 客户层服务层关系 |
| 3 | 以太端口->PW MPLS-TP OAM | 信号丢失（ETH-LOS） | 连续性丢失（LOC）、告警指示信号（AIS） | 客户层服务层关系 |
| 4 | 以太端口\STM\E1（客户侧）->PW MPLS-TP OAM | 信号丢失（LOS） | 客户信号失效告（CSF）警 | 业务从该端口接入。  若厂商不支持窄带业务AC接入故障的CSF传递，则不做要求。 |
| 5 | STM（客户侧）->PWE3-CES | 信号丢失（LOS） | 客户信号失效告警（CSF） | 业务从该端口接入。  厂商如果不支持PWE3-CES检测点，则不做要求。 |
| 6 | E1（客户侧）->PWE3-CES | 信号丢失（LOS） | 客户信号失效告警（CSF） | 同上 |
| 7 | 段层 MPLS-TP OAM->段层MPLS-TP OAM | 连续性丢失（LOC）、告警指示信号（AIS）、未期望的MEG | 远端缺陷指示（RDI） | 同一条业务 |
| 8 | LSP MPLS-TP OAM->LSP MPLS-TP OAM | 连续性丢失（LOC）、告警指示信号（AIS）、未期望的MEG | 远端缺陷指示（RDI） | 同一条业务 |
| 9 | PW MPLS-TP OAM->PW MPLS-TP OAM | 连续性丢失（LOC）、告警指示信号（AIS）、未期望的MEG | 远端缺陷指示（RDI） | 同一条业务 |

## 告警同步和存储

### 告警同步

告警同步是把网管系统显示的当前告警与网元实际的告警状态进行核准，应有人工和自动两种校正模式，可适用于以下情况：

1. 当网管系统与网元建立管理连接时；
2. 当网管系统与网元出现通信失败并且恢复后；
3. 当网管系统出现系统故障并且恢复后；
4. 当主用网管系统与备用网管系统发生倒换时；

当用户对网管系统显示的告警与网元实际的告警状态有疑问时（如网管系统显示的告警信息与网元显示告警信息不一致时）。

### 告警保存与存储

网管系统应支持告警记录的自动或手工保存，并可以导出保存到外部文件。

网管系统应支持告警日志的自动转储和手工转储，对于自动转储，可设立自动转储的条件，即：溢出转储的条件、周期转储的条件、转储位置。

## 告警处理能力

|  |  |  |
| --- | --- | --- |
| **No** | **指标名称** | **指标值要求** |
| 1 | 告警时延（指从网元发生告警到OMC显示告警）  [说明：告警产生后仍按照告警时延要求上报，即5s内，然后在告警相关性分析规则时间间隔即30s内进行告警相关性分析，刷新呈现] | ≤5秒 |
| 2 | 告警吞吐量 | ≥1000条/秒 |
| 3 | 活动告警 | ≥50万条 |
| 4 | 历史告警 | ≥12个月 |
| 5 | 告警相关性分析规则时间间隔 | ≤30秒 |
| 6 | 告警导出 | ≤30秒/1000条 |

## 端到端告警管理

网管系统应支持以下端到端路径和业务的告警管理功能：

1. 端到端隧道（MPLS-TP、SR-TP）和伪线告警：当设备发生告警时，网管系统应能将设备告警关联到受影响的隧道和伪线。
2. 端到端业务告警：当设备发生告警时，网管系统应能将设备告警关联到受影响的端到端以太网业务或TDM业务。
3. L3VPN业务告警：当设备发生告警时，网管系统应能将设备告警关联到受影响的LTE L3VPN、5G L3VPN业务。

告警定位功能：能够分析全网上报的告警信息，定位出可能的根源告警。

## 断纤链路管理

OMC系统针对光纤和网元故障应该具备以下监控功能：

1、支持对全网存在的故障连纤和相关网元进行集中监控，并可根据中断的产生时间进行筛选；

2、能够定位到拓扑上的故障对象，展示故障连纤影响的业务数据；

3、对于筛选出来的故障连纤和相关网元信息支持导出。

# 管控融合的性能管理

## 性能监测管理

### 性能监测参数设置

系统允许用户指定和查询网元性能监测的如下属性：

1. 性能监测对象（指定的网元、单元盘、端口、隧道、伪线等）；
2. 需要监测的参数名称；
3. 监测周期（15分钟、24小时、分钟/秒级）；
4. 监测状态（打开/关闭）；
5. 开始时间；
6. 结束时间；

并支持批量选取开启监测实例。

### 性能监测参数查询/修改

网管系统允许用户查询/修改性能监测的如下参数（标\*者为可修改参数）：

1. 性能监测对象（指定的网元、单元盘、端口、隧道、伪线等）；
2. 需要监测的参数名称(\*)；
3. 监测周期（15分钟、24小时、分钟/秒级）；
4. 监测状态（打开/关闭）(\*)；
5. 开始时间(\*)；
6. 结束时间(\*)；

支持对未开启性能监测对象或实例进行过滤。

### 性能门限设置

系统可对一个监测对象的某个性能参数设置上限和（或）下限。当该监测对象的指定性能参数超过设定的上限或下限时，网管系统应能产生越限告警（TCA）。

### 性能数据查询

网管系统应提供批量查询和统计性能数据的功能，并以表格和图形如折线图、直方图或饼图等方式显示查询统计结果。

网管系统应能根据性能监测结果，进行以太网业务、隧道、伪线、段、端口的实时流量统计和带宽利用率统计。

网管系统应能对查询统计结果进行输出。

### 性能数据上报

在每次监测周期到达后，网元根据要求向网管系统上报本周期内的性能数据，性能数据包括如下内容：

1. 监测对象；
2. 监测属性及其值；
3. 监测周期；
4. 本次监测间隔的结束时间。

### 性能数据存储

性能数据在网管系统存储设备上的保存期限最少为：

1. 测量周期为15分钟的测量数据：30天；
2. 测量周期为24小时的测量数据：60天。

网管系统应允许用户设置性能数据的存储期限和存储容量，对超过期限或容量的性能数据，应进行归档和删除。

## 端到端性能管理

网管系统应支持端到端路径和业务性能管理功能，包括：

1. 端到端路径性能管理：支持端到端隧道和伪线上各监测点的性能参数收集和管理，可设置性能监测点、性能监测参数、性能监测周期等性能监测参数。
2. 端到端业务性能管理：支持端到端以太网、TDM业务上各业务终端点的性能参数收集和管理，可设置性能监测点、性能监测参数、性能监测周期等性能监测参数。
3. 当前和历史性能查询：支持查询端到端路径和业务的当前性能和历史性能；

## 性能监测参数要求

网管系统应能对PTN/SPN网元中各层面的性能监测对象（端口、隧道、伪线、段等）的性能参数进行监测，网管系统应支持的性能监测参数参见下表。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序列号** | **性能类型** | **性能参数** | | | | **备注** |
|  | MPLS-TP性能 | PW层性能 | | 发送包总数 | |  |
|  | 发送字节总数 | |  |
|  | 接收包总数 | |  |
|  | 接收字节总数 | |  |
|  | 丢包率 | |  |
|  | 时延 | |  |
|  | 抖动 | |  |
|  | LSP层性能 | | 发送包总数 | |  |
|  | 发送字节总数 | |  |
|  | 接收包总数 | |  |
|  | 接收字节总数 | |  |
|  | 丢包率 | |  |
|  | 时延 | |  |
|  | 抖动 | |  |
|  | 段层 | | 发送包总数 | |  |
|  | 发送字节总数 | |  |
|  | 接收包总数 | |  |
|  | 接收字节总数 | |  |
|  | 丢包率 | |  |
|  | 时延 | |  |
|  | 抖动 | |  |
|  | 以太网业务性能 | 以太网物理接口发送光功率 | | | |  |
|  | 以太网物理接口接收光功率 | | | |  |
|  | 不同长度的包统计 | | | |  |
|  | 接收到的单播包数 | | | |  |
|  | 接收到的组播包数 | | | |  |
|  | 接收到的广播包数 | | | |  |
|  | 发送的单播包数 | | | |  |
|  | 发送的组播包数 | | | |  |
|  | 发送的广播包数 | | | |  |
|  | 接收的好包数 | | | |  |
|  | 接收到的好包字节总数 | | | |  |
|  | 发送的好包数 | | | |  |
|  | 发送的好包字节总数 | | | |  |
|  | 接收到的坏包字节数 | | | |  |
|  | 发送的坏包字节数 | | | |  |
|  | 检测到的监视器丢弃数据包事件的次数 | | | |  |
|  | 校验错误数 | | | |  |
|  | 丢包率 | | | |  |
|  | 时延 | | | |  |
|  | 抖动 | | | |  |
|  | TDM业务性能 | 客户侧2M | 误码秒 (ES) （适用于结构化E1） | | |  |
|  | 严重误码秒(SES)（适用于结构化E1） | | |  |
|  | 背景误码块（BBE）（适用于结构化E1） | | |  |
|  | 不可用秒(UAS)（适用于结构化E1） | | |  |
|  | 客户侧155M | 物理接口 | | 光发送功率 |  |
|  | 光接收功率 |  |
|  | 激光器偏置电流 |  |
|  | 激光器温度 |  |
|  | 再生段 | | 误码秒 (ES) |  |
|  | 严重误码秒(SES) |  |
|  | 背景块误码(BBE) |  |
|  | 不可用秒(UAS) |  |
|  | 复用段 | | 误码秒 (ES) |  |
|  | 严重误码秒(SES) |  |
|  | 背景块误码(BBE) |  |
|  | 不可用秒(UAS) |  |
|  | 高阶通道 | | 误码秒 (ES) |  |
|  | 严重误码秒(SES) |  |
|  | 背景块误码(BBE) |  |
|  | 不可用秒(UAS) |  |
|  | 低阶通道（适用于通道化的STM-1） | | 误码秒 (ES) |  |
|  | 严重误码秒(SES) |  |
|  | 背景块误码(BBE) |  |
|  | 不可用秒(UAS) |  |
|  | 单板性能 | 单板CPU利用率 | | | |  |
|  | 单板内存利用率 | | | |  |
|  | 单板温度 | | | |  |
|  | SR-TP性能 | 收发包速率 | | | |  |
|  | 收发字节数 | | | |  |
|  | 丢包数 | | | |  |
|  | 时延（最大、最小、平均值） | | | |  |
|  | 抖动（最大、最小、平均值） | | | |  |
|  | MTN Client性能 | BIP8误码数 | | | |  |
|  | BIP8误码率 | | | |  |
|  | 时延（最大、最小、平均值） | | | |  |
|  | 抖动（最大、最小、平均值） | | | |  |
|  | 端口 | 收发包数 | | | |  |
|  | 收发字节数 | | | |  |
|  | 丢包数 | | | |  |
|  | 时延（最大、最小、平均值） | | | |  |
|  | 抖动（最大、最小、平均值） | | | |  |

## 性能监控能力

支持全网监测对象的所有监测参数的性能数据按照15分钟上报和查询。

支持实时秒级监控（秒级监控，应支持不大于5s间隔的采样和分析），监控对象至少达到30个，可实现7\*24小时监控，同时性能数据至少保存30天，并支持图形化显示。

# 管控融合的流量管理

## 流量监测功能要求

OMC系统应支持以下流量监测、分析、输出和呈现功能：

**流量监测数据的获取**：定期采集获取PTN/SPN网络流量监测的基础数据；

**流量基础数据的统计分析**：对流量监测的基础数据进行分析处理，统计得出PTN/SPN网络所承载的各类业务端口的流量大小及变化趋势，以及PTN/SPN网络线路端口、LSP、PW等不同粒度管道的流量、带宽使用率和变化趋势；

**流量分析图表的呈现和输出功能**：支持对不同种类的业务端口流量、不同客户的业务流量，不同网络层面的线路端口流量（核心、汇聚和接入层）、不同传输系统的流量（环路、链路等）分别进行流量使用状态和分析指标图形化或报表的呈现和输出；

**流量预警分析管理功能**：支持预警分析，针对业务端口、线路端口、不同网络层面的指标支持设置资源使用的预警门限，支持列出超过预警门限的监测对象，并支持关联分析（下钻和上钻）。

## 流量基础数据表要求

### 业务流量基础数据表要求

支持基于UNI端口或端到端PW进行对业务层面的流量监测和管理分析，包括承载2G/3G基站回传以及集团客户业务的端到端L2PTN网络，以及承载TD-LTE基站回传的汇聚接入层L2PTN网络。

支持基于PW和UNI端口进行业务流量指标的统计分析，并输出相应的基础数据表。格式要求见下。

应支持为集客专线客户设立单独的业务流量基础数据统计分析界面。

表 5-1 PW业务流量基础数据表

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PW名称** | **采集起止时间** | **业务类型** | **区域信息** | **源网元名称** | **宿网元名称** | **配置的保证带宽(Mb/s)** | **忙时平均流速(M b/s)** | **保证带宽利用率(%)** | **峰值流速(M b/s)** | **峰值带宽利用率(%)** | **带宽利用率的忙时均值(%)** | **带宽繁忙度(%)** |
|  |  | 2G基站 |  |  |  |  |  |  |  |  |  |  |
|  |  | 3G基站 |  |  |  |  |  |  |  |  |  |  |
|  |  | LTE基站 |  |  |  |  |  |  |  |  |  |  |
|  |  | 集客专线 |  |  |  |  |  |  |  |  |  |  |

表 5-2 UNI端口流量基础数据表

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **端口名称** | **采集起止时间** | **业务类型** | **区域信息** | **网元名称** | **端口速率或端口限速(M b/s)** | **接收方向** | | **发送方向** | | **端口带宽利用率峰值(%)** | **带宽利用率忙时均值(%)** | **带宽繁忙度(%)** |
| **忙时平均流速(M b/s)** | **峰值流速(M b/s)** | **忙时流速(M b/s)** | **峰值流速(M b/s)** |
|  |  | 2G基站 |  |  |  |  |  |  |  |  |  |  |
|  |  | 3G基站 |  |  |  |  |  |  |  |  |  |  |
|  |  | LTE基站 |  |  |  |  |  |  |  |  |  |  |
|  |  | 集客专线 |  |  |  |  |  |  |  |  |  |  |

### 网络流量基础数据表要求

支持对线路端口、链路、传输环路和传输链路等监测对象的流量采集和统计分析，输出PTN/SPN网络层面的流量基础数据表，并支持基础数据的分类查询，如分别选择和查询核心层、汇聚层和接入层的线路端口流量数据。

基于线路端口、链路、传输环路、传输链路的基础数据表分别见下。基于线路端口或链路的网络流量监测同时适用于L2 PTN和L3 PTN网络。

表5-3 PTN/SPN网络的线路端口流量基础数据表

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 线路端口名称 | 采集起止时间 | 区域信息 | 网元名称 | 线路端口速率(M b/s) |  | 接收方向 | | 发送方向 | |  | 端口带宽利用率峰值(%) | 端口带宽利用率忙时均值(%) | 端口带宽繁忙度(%) |
| 端口配置的保证带宽(M b/s) | 忙时平均流速(M b/s) | 峰值流速(M b/s) | 忙时平均流速(M b/s) | 峰值流速(M b/s) | 端口配置的保证带宽利用率忙时均值 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

表5-4 PTN/SPN网络的链路流量基础数据表

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **链路名称** | **采集起止时间** | **区域信息** | **源网元名称** | **宿网元名称** | **链路速率(M b/s)** | **接收方向** | | **发送方向** | | **链路带宽利用率峰值(%)** | **链路带宽利用率忙时均值(%)** | **链路带宽繁忙度(%)** |
| **忙时平均流速(M b/s)** | **峰值流速(M b/s)** | **忙时平均流速(M b/s)** | **峰值流速(M b/s)** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

表 5-5 PTN/SPN网络传输环路的流量基础数据表

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **传输环路名称** | **采集起止时间** | **区域信息** | **所属网络层面** | **出环节点网元名称** | **线路端口速率(M b/s)** | **接收方向** | | **发送方向** | | **环路带宽利用率峰值(%)** | **环路带宽利用率忙时均值(%)** | **环路带宽繁忙度(%)** |
| **环路忙时平均流速(M b/s)** | **环路峰值流速(M b/s)** | **环路忙时平均流速(M b/s)** | **环路峰值流速(M b/s)** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

表5-6 PTN/SPN网络传输链路的流量基础数据表

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **传输链路名称** | **采集起止时间** | **区域信息** | **所属网络层面** | **链路根节点网元名称** | **线路端口速率(M b/s)** | **接收方向** | | **发送方向** | | **链路带宽利用率峰值(%)** | **链路带宽利用率忙时均值(%)** | **链路带宽繁忙度(%)** |
| **链路忙时平均流速(M b/s)** | **链路峰值流速(M b/s)** | **链路忙时平均流速(M b/s)** | **链路峰值流速(M b/s)** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

### 查看端口毫秒级流量数据

支持UNI、NNI端口毫秒级流量数据查看，例如：发送方向和接收方向的周期内毫秒级利用率均值（%）、周期内毫秒级利用率峰值（%）、周期内越限毫秒数（ms）。

### L3VPN业务接口流量报表数据

支持基于L3VPN的业务接入接口进行对业务层面的流量监测和管理统计分析，并输出相应的基础数据表。格式要求见下。

表5-7 L3VPN业务接口流量报表数据

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **业务接口名称** | **采集起止时间** | **业务名称** | **区域信息** | **网元名称** | **出入端口PIR** | **出入端口CIR** | **接收方向** | | | **发送方向** | | | **平均流速(M b/s)** |
| **保证带宽利用率（%）** | **峰值带宽利用率（%）** | **平均流速(M b/s)** | **保证带宽利用率（%）** | **峰值带宽利用率（%）** | **平均流速(M b/s)** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## 流量分析报表和输出

### 流量分析报表输出的基本要求

应支持从业务流量和网络流量两个维度，分别输出PTN/SPN流量分析报表。

**一、报表呈现**

为了直观体现流量长期统计分析数据，应支持如下报表展现能力：

支持趋势曲线图表，并支持多个对象在同一图中进行趋势图对比；

支持TopN排序呈现，支持柱状数据分布图表；

支持报表下钻，灵活钻取各类有关联关系的网络资源报表；

支持基础数据报表和图形化之间转换；

支持资源对比，即多对象同周期对比和同对象多周期对比；

支持流量告警状态呈现，支持在图表上直接显示阈值线，并支持四个阈值状态呈现，按不同颜色着色，如：绿色（轻微告警）、橙色（普通告警）、黄色（重要告警）、红色（严重告警）；

支持多周期粒度汇总统计，即按刻、按小时、按天、按周和按月多种周期汇总呈现；

支持常规条件查询，即按周期类型、时间类型、关键字或者指标过滤查询，同时需支持按网络资源附加属性（如名称、区域属性、状态等）过滤；

支持在界面直接修改数据采集周期、采集时间进行报表导航查询。

**报表导出**

应支持报表导出功能，支持excel、csv、pdf格式输出；

应支持定制化推送邮件到指定的运维管理人员的邮箱。

### 业务流量报表

#### 各类业务的流量分析

支持以下功能：

按照PTN/SPN网络所承载的业务类型对PTN/SPN网络流量进行分类统计，分析各类型业务在PTN/SPN网络中的总流量和流量占比情况，反映各类型业务实际使用PTN/SPN网络带宽资源情况。应支持业务分类的流量统计表格、业务流量分类对比饼图或柱状图。

分析各类型业务在PTN/SPN网络中配置的保证带宽和保证带宽占比情况，反映为各类型业务分配的PTN/SPN网络带宽资源情况。

通过对流量历史数据的统计分析，呈现PTN/SPN网络所承载的各类型业务的流量随时间的变化趋势。

支持显示流量趋势图的具体名称、具体哪类业务流量、时间区间、峰值还是忙时平均流速等信息。

业务流量趋势图标点的粒度必须支持15分钟采集周期的流量，用折线图，图例的标识要直观，日趋势图应包括24小时的完整数据，周趋势图应包括7天的完整数据，月趋势图应包括每天的详细趋势图（不能每天仅显示一个点）。

各类业务的流量对比图示例：

图5-1各类业务的月流量及占比分析图

分析说明：上图说明2G基站业务在网络中的流量最大，实际使用了最多的带宽资源；3G基站业务其次；WLAN业务最小。2G基站业务的月流量为30375000Gbit，占比43%；3G基站业务的月流量为22781250Gbit，占比32%；WLAN业务月流量8100000Gbit，占比11%。

各类业务的保证带宽对比图示例：

图5-2务的保证带宽流量和占比分析图

**分析说明：**上图说明3G基站业务占用业务保证带宽最多；2G基站业务其次；WLAN业务最少。3G基站业务保证带宽总和为18000Mbit/s，占比为43%；2G基站业务保证带宽总和为12000Mbit/s，占比为29%；WLAN业务保证带宽总和为800Mbit/s，占比为2%。

各类业务的月流量变化趋势示例：

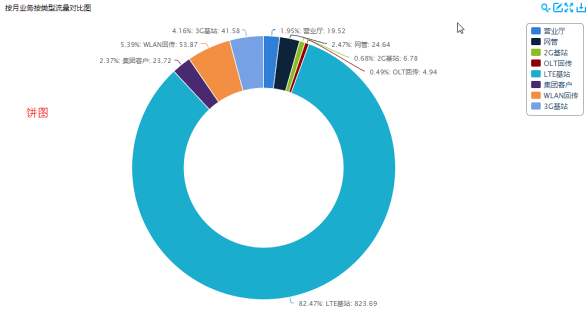
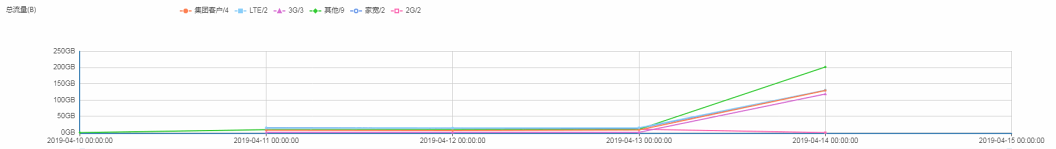


图5-3务的月流量变化趋势图

上左侧图说明各类型业务的流量总体变化趋势是随时间的变化情况。此外，支持总流量的月流量图形化展现变化趋势，支持在每个月的流量图中分颜色演示各类业务流量占比情况，如上右侧图。

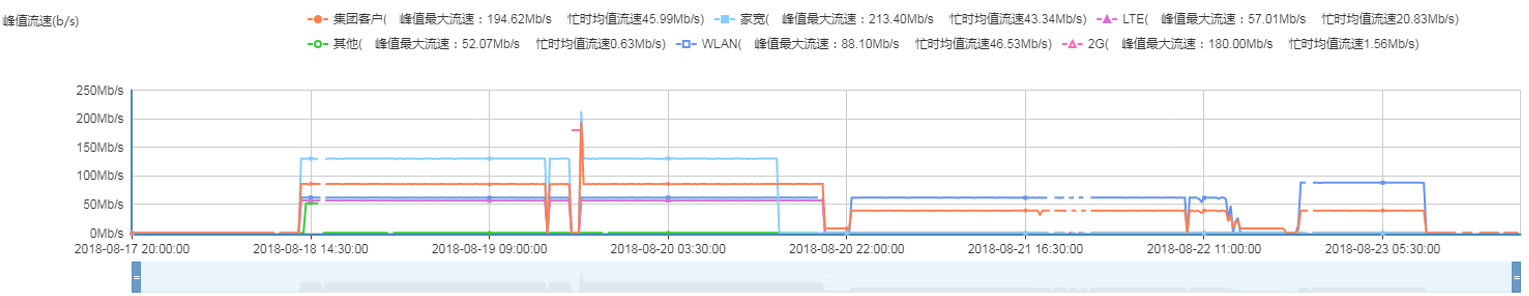


图5-4务流量的周趋势示意图

**分析说明：**PTN承载的各类业务日流量趋势图形具有相似性，一周七天。支持以15分钟采集周期的流量为基础数据，绘制各类业务流量的周趋势图，支持人工定制显示流量趋势的起始和结束时间，并支持图形化分别或统一呈现各类业务的周峰值最大流速和周忙时均值流速等必要的信息。

#### 业务流量的排名分析

对业务个体，按照流量大小进行排名，反映业务个体对PTN/SPN网络带宽资源的实际使用情况。

没有指明方向时，业务流量是指双向流量之和，即源到宿流量与宿到源流量之和。

对同类型的业务流量进行排名，如对3G基站进行流量排名，获得流量最大的ToP N个3G基站情况；对集团客户进行流量排名，获得流量最大的10个集团客户情况。

根据排名分析结果，便于对流量大的基站或集团客户进行重点监控和保障。

业务流量的排名分析示例：

(1) 3G业务的月流量ToPN排名表（N=10或N可定制）

表5-8业务的月流量TopN排名

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **3G业务-基站名称** | **流量排名** | **月流量（Gbit）** | **月峰值流速（Mbit/s)** | **月平均流速（Mbit/s)** | **业务保证带宽（Mbit/s)** | **保证带宽平均利用率** |
|  | 1 |  |  |  |  |  |
|  | 2 |  |  |  |  |  |
|  | 3 |  |  |  |  |  |
|  | 4 |  |  |  |  |  |
|  | 5 |  |  |  |  |  |
|  | 6 |  |  |  |  |  |
|  | 7 |  |  |  |  |  |
|  | 8 |  |  |  |  |  |
|  | 9 |  |  |  |  |  |
|  | 10 |  |  |  |  |  |

(2)集客业务的月流量ToPN排名表（N=10或N可定制）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **集客业务-客户名称** | **流量排名** | **月流量（Gbit)** | **月峰值流速（Mbit/s)** | **月平均流速（Mbit/s)** | **业务保证带宽（Mbit/s)** | **保证带宽平均利用率** |
| 南海富士通 | 1 | 525.1 | 19.5 | 17.8 | 20 | 89% |
| 农信社 | 2 | 170.6 | 7.2 | 5.8 | 10 | 58% |
| 顺安达航空 | 3 | 165.3 | 4.0 | 3.6 | 4 | 90% |
| 边防检查站 | 4 | 155.4 | 2.0 | 1.7 | 2 | 85% |
| 华南通商贸发展有限公司 | 5 | 143.8 | 1.9 | 1.6 | 2 | 80% |
| 大自然家居 | 6 | 130.7 | 1.8 | 1.5 | 2 | 75% |
| 红日不锈钢 | 7 | 120.9 | 1.7 | 1.4 | 2 | 70% |
| 大良公安局 | 8 | 116.8 | 1.6 | 1.4 | 2 | 70% |
| 宏宇陶瓷瓷海国际 | 9 | 108.5 | 1.6 | 1.3 | 2 | 65% |
| 虹宇塑料五金 | 10 | 102.3 | 1.5 | 1.2 | 2 | 60% |

#### 业务流量的区域分布和趋势分析

按照PTN/SPN网络的区域分布，分析各个区域的业务流量分布和流量发展趋势。

表5-9 PTN流量的区域分布报表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **排名** | **区域名称** | **PW业务数量** | **本月业务总流量（Gbit)** | | **上月业务总流量（Gbit)** | | **月流量变化率（%）** |
| **接收** | **发送** | **接收** | **发送** |
| **1** |  |  |  |  |  |  |  |
| **2** |  |  |  |  |  |  |  |
| **3** |  |  |  |  |  |  |  |

**分析说明：**

分别对各区域的业务总流量进行排名，并分析各个区域的本月总流量和上月总流量的最大变化率。

**业务总流量应为接收与发送流量之和。**

**月流量变化率（%），应为(本月业务总流量（Gbit)-上月业务总流量（Gbit)）/上月业务总流量（Gbit)\*100%。**

#### 重要业务的忙闲时流量分析

对重要业务的流量在一定监测时长范围内（如1天24小时、一周7天）的变化进行分析，获取业务繁忙时段（流量大的时段）和空闲时段（流量小的时段）。

#### 业务保证带宽利用率分析

“业务保证带宽利用率”反映了业务个体对所分配到的带宽资源的使用情况。对业务个体进行“业务保证带宽利用率”分析，可以指导对业务个体进行保证带宽调整。

业务个体一般有忙时和闲时，忙时和闲时的带宽利用率相差很大，分析“业务忙时保证带宽利用率”更具实际参考意义。

对于集团客户业务，提醒用户关注保证业务忙时带宽利用率大于70%的业务个体。

对于基站业务，提醒用户关注业务忙时保证带宽利用率大于70%和小于30%的业务个体。

### PTN/SPN网络流量分析系统呈现功能要求

#### 业务总流量分析

支持业务总流量分析以及同期对比分析，输出PTN/SPN网络承载的业务总流量的变化情况。

#### 端口带宽利用率分析

对“端口带宽利用率”进行统计，分析列出不同利用率分布区间的端口。

对于“端口带宽利用率”超过45%的端口需要重点关注，为了防止拥塞，应考虑调整流量。

分析全网端口带宽利用率，输出带宽利用率高于上限的端口清单。通过对端口带宽利用率历史数据的统计分析，获取各类型端口的带宽利用率随时间的变化情况。

#### 链路带宽利用率分析

链路是指两个网络侧端口之间的对接关系，包括源网元、源端口、宿网元和宿端口等信息。相对于端口，链路可以更加直观地反映出数据传送的源端和宿端。

链路是端口的组合，链路带宽利用率分析与端口带宽利用分析基本相同，请参照“端口带宽利用率分析”。



图5-5 链路的带宽利用率和繁忙度分析报表

#### 传输环路带宽利用率分析

以传输环路为对象进行区域流量分析和网络拓扑的图形化显示，具体反映传输环路的总体流量负载情况。支持传输环路的流量基础分析报表，并支持对流量监测分析的关键指标进行选取过滤显示。通过纵向对比分析，可以获知各传输环路带宽利用率的变化趋势。

分析示例：

(1) 传输环路带宽利用率分析报表：

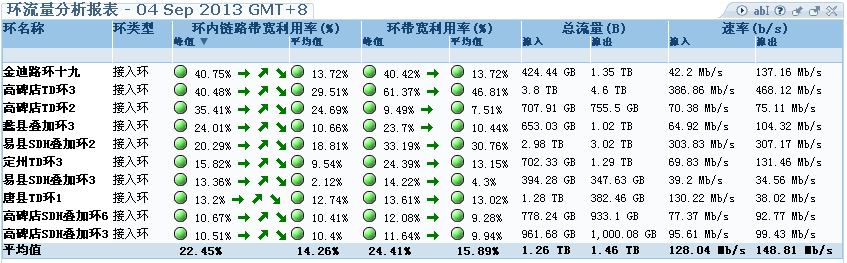


图5-6 PTN传输环路的流量分析报表

(2) 传输环路带宽利用率对比图

**分析说明：**PTN骨干环2的带宽利用率峰值为52%，存在拥塞的风险。

(3) 传输环带宽利用率变化趋势图

**分析说明**：5月带宽利用率增长最快和最慢的环分别为PTN骨干环4和PTN骨干环1。

（4）传输环路流量变化趋势分析

支持针对每个环网的流量分析变化趋势，支持环网流量变化率TopN排名（变化率的计算仅计入正增长），并支持导出。

#### 网络侧端口保证带宽占比分析

统计出经过网络端口的所有业务（PW或LSP）的保证带宽配置值的总和，然后计算出“网络侧端口保证带宽占比”。

#### 传输环路带宽利用率占比分析

根据环网的带宽利用率所在区间，统计环网数量，计算“环网的带宽利用率占比”。其中，带宽利用率的统计区间，支持设置。

#### 链路带宽利用率占比分析

根据链路的带宽利用率，计算“链路的带宽利用率占比”。

#### L2PTN业务总流量分析

支持L2PTN业务总流量以及各监测点流量分析以及同期对比分析，输出L2PTN业务总流量以及各监测点流量的变化情况。

#### L3PTN业务总流量分析

支持L3PTN业务总流量以及各监测点流量分析以及同期对比分析，输出L3PTN业务总流量以及各监测点流量的变化情况。

#### 隧道(LSP/SR-TP)带宽利用率分析

分析全网隧道(LSP/SR-TP)带宽利用率，输出带宽利用率高于上限（应支持设置）的隧道列表。

## 流量地图呈现

支持查看流量区域地图，可呈现不同区域的流量分布情况。

查看某区域的业务流量状况：在区域地图上单击区域名称，可显示当前区域相关的流量数据。支持按照业务类型分别呈现。

地图染色阈值设置：根据区域监控实例某个指标超过设置的阈值级别，支持以不同的颜色显示在界面地图上。

针对全网流量监控实例，监测和计算相应的流量指标；依据门限设定对监控实例进行标记，例如带宽利用率等严重越限的，标记为有严重问题的实例，稍有越限的，标记为重要问题的实例。

单个监测实例的流量问题等级可参照性能告警等级分为严重问题、重要问题、普通问题和轻微问题。

针对某一管理区域，遍历该区域下所有监测实例。针对每一区域，流量问题实例/所有实例 \*100%。

− 绿色表示区域流量指标情况为好级

− 黄色表示区域流量指标情况为中级

− 红色表示区域流量指标情况为差级

− 蓝色表示区域未监控

地图染色规则如下：

当某一区域的业务流量出现问题时，会根据问题的严重程度，以不同的颜色显示在地图上。建议：

■当该区域，有严重流量问题的比例(红色比例)>==10%，地图上该区域将显示红色。

■当该区域存在有严重流量问题时，有严重流量问题的比例(红色比例)<10%且有严重流量问题的比例(红色比例)+有重要流量问题的比例(黄色比例)>=10%，地图上该区域将显示黄色。

■当该区域，有严重问题的比例(红色比例)+有重要问题的比例(黄色比例)<10%，地图上该区域将显示绿色。

## 流量拓扑图呈现

流量拓扑应与网络拓扑保持实时同步，网元、链路、环网改变时，在流量拓扑上实时更新。

支持流量拓扑上查看环网、链路、网元、端口等相关的信息，同时支持带宽利用率和告警上浮。

支持PTN/SPN网络流量的拓扑分层视图，即分为核心层、汇聚层和接入层的网络流量视图分别显示并支持分层的上下钻取功能，例如当汇聚层某一网络节点的端口带宽利用率超门限时，支持点击该汇聚层节点钻取到其下挂的所有接入环，并对接入环带宽利用率超门限的进行着色显示

当端口或链路的带宽利用率超阈值门限时，应支持在网络流量拓扑视图上进行区域着色，并支持分区域的上下钻取功能。例如当某一区域某一环网带宽利用率超门限时，支持钻取显示该区域下所有环网系统找到具体带宽利用率超门限的环网，并支持该环网继续下钻所有网元节点，网元钻取具体的端口、单板等资源，直至具体流量报表；

在PTN/SPN网络流量拓扑视图中，支持显示端到端LSP隧道或PW业务的路径。在端口带宽利用率超门限时，支持从端口下钻显示分析该端口内的所有LSP和PW带宽。

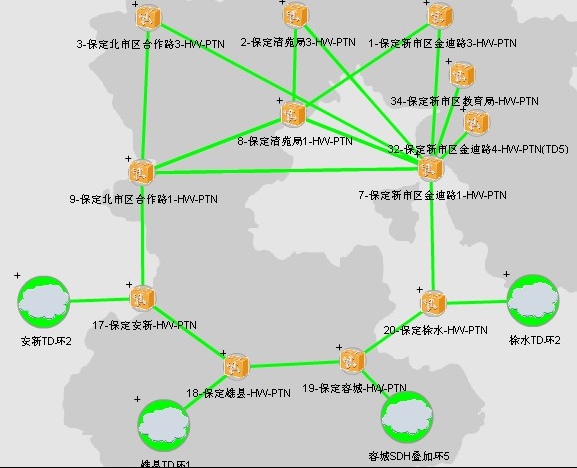


图5-7 PTN传输环路流量的拓扑分层视图-

## 流量预警分析

对PTN/SPN网络流量支持分级预警管理功能，应支持以下基本功能要求：

支持持续N天预警的设置；

支持设置紧急预警（红色）、重要预警（橙色）、次要预警（黄色）的预警门限值；

支持三级预警门限值的设置，门限值可设置，建议设置如下：

传输环路、传输链路的带宽利用率峰值的连续7天均值：达到80%及以上为紧急预警（红色）门限，达到70%为重要预警（橙色）门限，达到60%为次要预警（黄色）门限。

有网络保护的端口带宽利用率峰值的7天均值：达到40%及以上为紧急预警（红色）门限，达到30%为重要预警（橙色）门限，达到20%为次要预警（黄色）门限。

业务即PW的带宽利用率峰值的连续7天均值：达到80%及以上为紧急预警（红色）门限，达到70%为重要预警（橙色）门限，达到60%为次要预警（黄色）门限。

核心层L3PTN线路端口（链路）的带宽利用率峰值的连续7天均值：达到40%及以上为紧急预警（红色）门限，达到30%为重要预警（橙色）门限，达到20%为次要预警（黄色）门限。

支持在PTN/SPN网络拓扑上以颜色方式标识已产生预警的链路及其预警级别

PTN/SPN网络预警管理的增强功能要求：

支持在PTN/SPN网络拓扑上以颜色方式标识已产生容量预警的传输环路系统及其预警级别；

支持对已产生预警的某一区域网络拓扑进行分析钻取功能，并支持网络逻辑分层的钻取分析功能，例如通过点击产生预警的线路端口，可显示分析该端口内所有、PW的流量状态，支持该端口内LSP和PW的流量排序。

## 带宽动态调整

系统应支持将流量趋势分析结果指导QoS策略和带宽参数优化调整功能：

OMC系统应支持基于PW（业务）流量指标、各类业务的QoS带宽参数配置，并可结合业务部门的分析预测数据和流量经营策略来进行综合评估，提供分析结果和调整建议，并支持通过OMC系统自动下发（初期需提供人工干预，须运维人员确认）以进行优化调整。现阶段应至少支持依据业务的PIR或CIR利用率进行带宽调整，流程如下图所示，功能要求详述如下：

是否认可优化建议

是否继续调整

调整未完成业务的调整策略

基于调整策略计算为配置下发到网元

是否下发成功

设置业务的调整门限和调整策略

超过调整门限，系统提示用户调整并给出优化建议

是

是

是

否

否

否

结束

1、OMC系统应支持设置业务的PIR或CIR利用率门限，以作为触发条件，包括以下三种方式：

1）仅PIR门限

2）仅CIR门限

3）PIR门限或CIR门限、PIR门限和CIR门限

门限默认值为70%，且支持用户修改。

对应上述的触发方式，OMC系统呈现当前的监测情况，并给出调整建议。

1）仅PIR门限触发：

输出的信息至少具备以下字段：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 业务名称 | 业务类型 | 调整对象名称 | 配置的PIR(Mbps) | 当前PIR利用率(%) | PIR调整建议(%) | 调整后PIR(Mbps) | 调整后利用率(%) |

若OMC经过分析，发现无法进行带宽的优化，则给出失败的反馈，并提示失败原因，例如存在瓶颈端口等。

2）仅CIR门限触发：

输出的信息至少具备以下字段：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 业务名称 | 业务类型 | 调整对象名称 | 配置的CIR(Mbps) | 当前CIR利用率(%) | CIR调整建议(%) | 调整后CIR(Mbps) | 调整后利用率(%) |

若OMC经过分析，发现无法进行带宽的优化，则给出失败的反馈，并提示失败原因，例如存在瓶颈端口等。

3）PIR门限或CIR门限、PIR门限和CIR门限触发：

PIR门限或CIR门限出发时，输出的信息按照生效的门限，输出的信息具备的字段参照前述两项。

PIR门限和CIR门限触发，输出的信息至少具备以下字段

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 业务名称 | 业务类型 | | 调整对象名称 | | 配置的PIR(Mbps) | | 当前PIR利用率(%) | | PIR调整建议(%) | | 调整后PIR(Mbps) | 调整后利用率(%) |
| 配置的CIR(Mbps) | | 当前CIR利用率(%) | | CIR调整建议(%) | | 调整后CIR(Mbps) | | 调整后利用率(%) | |

2、PIR/CIR利用率越限达到一定的监测周期（监测周期可设置，≥1天）后，则输出优化建议，并提示用户，即忙时的PIR/CIR带宽利用率均值达到触发条件，则进行用户提示，其中忙时的选取可参考技术规范”日忙时的取值方法”，N的取值支持用户设置；

3、用户确认则进行PIR/CIR调整，调整的默认值为增加10%，且支持用户自定义设置，当PIR和CIR均需调整时，可支持按比例调整；

用户选择需要确认/否认的业务提示时应支持全选、多选、单选；

4、进行上述操作的业务可根据“业务类型”进行筛选，用户可指定一项或几项业务类型进行监测和自动调整；

业务类型的定义参见“7.2.2业务配置和管理”一节中业务的属性，如2G、3G、LTE、集客专线、家庭宽带、WLAN等。

## 流量监测的性能要求

### 监测实例数量要求

OMC系统支持的流量性能采集规格与流量采集周期、服务器的配置相关性较大。本标准以流量监测实例数来规范系统的性能规格，一个流量监测实例是指对一个流量监测对象（如端口、LSP、PW等）开启不超过10个流量基本参数的监测。

OMC系统支持的性能采集规格要求：

为实现全省范围的流量监测，应支持至少200万个流量监测实例数。

### 数据存储能力要求

原始性能数据：OMC系统采集到的未经系统处理的，保持设备厂家原始格式的数据。

应用性能数据：原始性能数据经过指标计算和各种纬度的汇总等处理后，输出或呈现的数据。

性能原始数据在系统中存储时间不小于3个月，处理后的应用数据，包括报表数据、分析数据在系统中保存不少于3年。支持流量数据的定期转储。

# 网络质量管理

## 质量指标体系

根据业务质量管理的模型，业务质量指标体系也是分层分域的。从业务传送的角度来说，业务传送质量KPI指标主要关注如下：

* 时延（Delay）：检测业务经过传送网络的时间；
* 抖动（Delay Variation）：检测业务经过传送网络的时间变化；
* 丢包率（Loss）：检测业务经过传送网络的丢包；
* 吞吐量(Throughput)：检测业务最大的使不丢包的发送速率。

表6-1 业务传送质量KPI指标

|  |  |  |
| --- | --- | --- |
| KPI指标 | 指标内容 | 相关标准 |
| 时延 | 业务经过传送网络的时间 | RFC2544/Y.1564/RFC5357（TWAMP）/Y.1731 |
| 抖动 | 业务经过传送网络的时间变化 | RFC2544/Y.1564/RFC5357(TWAMP) /Y.1731 |
| 丢包率 | 业务经过传送网络的丢包 | RFC2544/Y.1564/RFC5357(TWAMP) /Y.1731 |
| 吞吐量 | 业务最大的使不丢包的发送速率 | RFC2544/Y.1564 |

PTN/SPN网络中的质量检测协议:

TWAMP: 是一种双向主动性能统计协议，遵循RFC5357标准，标准质量检测协议，互通性较好。

ICMP Jitter：通过发送特定的ICMP协议报文检测业务性能，三层设备天然具备ICMP反射能力，但一般由设备软件处理，处理性能和精度有限。在设备具备TWAMP检测能力时，优先使用TWAMP检测协议。

RFC2544/Y.1564: 根据RFC2544/ITU-T Y.1564标准及业务场景开发的一种以太网业务测量功能，通常在网络业务割接之前使用，评估网络是否达到预先设计的性能指标，包括吞吐量、丢包、时延。

Y.1731：ITU-T Y.1731标准中定义的以太二层网络质量检测协议。

在设备具备TWAMP检测能力时，优先使用TWAMP检测协议，本标准的相关章节也以TWAMP协议为主进行介绍。

| 测试类型 | 主要指标 | 含义 | 遵循标准 |
| --- | --- | --- | --- |
| 主动TWAMP测试（双向测试） | 丢包率 | 丢失TWAMP数据包数与发送TWAMP数据包数的比率。 | RFC5357 |
| 抖动 | 到达同一目的端的相邻两个时延的变化。 |
| 时延 | 从发送到接收到环回的TWAMP报文的时间，即往返时延。 |
| ICMP jitter测试 | 丢包率 | 一段时间内，报文在链路上丢失的数量占传输报文总数量的比率。 | RFC768 |
| 时延 | 一个报文从发送到接收到环回所需要的时间，不包括探针处理报文时间。 |
| 抖动 | 到达同一目的端的相邻两个报文时延的变化。 |
| RFC2544/Y.1564（二选一） | 吞吐量 | 最大不丢包的发送速率。 | RFC2544/Y.1564（二选一） |
| 丢包率 | 从测试开始到测试结束，丢失数据包数与发送数据包数的比率。 |
| 时延 | 从测试开始到测试结束，测试报文从发送到接收到环回的的时间的平均值，即往返时延 |
| Y．1731 | 丢包率 | 一段时间内，报文在链路上丢失的数量占传输报文总数量的比率。 | Y．1731 |
| 时延 | 一个报文从发送到接收到环回所需要的时间 |
| 抖动 | 到达同一目的端的相邻两个报文时延的变化。 |

OMC应支持对内置探针的如下管理和监控功能。

## 探针状态监控

探针监控：

Ø 版本管理：支持探针版本升级以及软件版本管理；

Ø 状态监控：支持查看探针告警信息。

## 监测任务的管理

### 监测任务创建

采用TWAMP/RFC2544/Y.1564测量协议时，监测任务创建可以分为以下步骤：

1、创建监测TWAMP任务

支持设置以下任务属性（包括但不限于）：

* + 任务名称
  + 协议参数（可使用模板方式）
  + 告警模板（参见13.7节）
  + 测试类型（周期性、一次性测试）
  + 任务间隔（适用于周期性测试）
  + 发起端网元和终止端网元

2、创建RFC2544/Y.1564监测任务

支持设置以下任务属性（包括但不限于）：

* + 任务名称
  + 协议参数（可使用模板方式）
  + 测试类型（一次性测试）
  + 启动时间、 停止时间
  + 发起端网元、端口和终止端网元、端口

以上选择网元时，应支持对网元的过滤和筛选，过滤条件如下（包括但不限于）：

* + 区域信息
  + 设备型号
  + 网元名称（基于网元名称进行模糊匹配）

在质量监测任务创建时，支持对以上协议设置相应的告警模板。

### 监测任务修改

系统需要支持对监测任务基本属性的修改。

### 监测任务删除

支持监测任务删除，在系统界面一次选定一条或多条监测任务，对于正在执行的任务，提示用户等任务结束或者执行强制停止后，删除相应的监测任务和数据。执行中的任务不支持删除。

## 监测数据的管理

### 质量监测数据查看

系统需支持对所有质量监测任务的实时/历史测量结果进行列表查看。

TWAMP测量结果包括：

丢包

时延

时延抖动

RFC2544/Y.1564检测结果包括：

吞吐量检测结果

时延检测结果

丢包率检测结果

支持通过历史性能数据和实时性能数据来评估网络端到端的质量，历史性能数据支持设置不同的时间颗粒度，快速发现质量异常时间点。

提供TWAMP历史性能数据查看功能，支持通过系统查询日常监测结果的原始数据，可选择“性能指标”、“开始时间”、“结束时间”，系统可显示从“开始时间”到“结束时间”这段时间内的“性能指标”指标值，呈现方式包括：线图、表格方式，并提供历史数据导出功能。

提供实时性能数据查询功能，针对测试类型是“一次性测试”和“周期测试”的测试例都提供跳转到实时性能查看界面。系统周期自动刷新数据，更精确的展示时间值精细化的指标值。

### 质量监测数据分析

对于长期监测的任务生成的监测数据，系统会进行汇总计算，基于不同的时间颗粒度（15分钟，1小时，天，周，月）生成网络KPI统计数据，在此数据基础上可提供类型丰富的图表分析，例如：

区域排名统计分析

网络质量告警统计分析

专线质量统计分析

基础数据统计

### 质量监测数据存储

质量监测数据根据时间颗粒度有着不同的存储时长，系统可以对不同时间颗粒度数据的存储时长进行设置，建议分钟级数据默认存储7天；15分钟数据默认存储14天；1小时数据默认存储90；天粒度默认存储1年，周粒度默认存储1年，月粒度默认存储3年。

## 质量报表输出

支持对原始数据进行多维度汇总分析，输出完整的年/月/周/日统计报表及图表，报表支持时间粒度选择包括：15分钟；每小时；每天；每周；每月；每年。

| **时间粒度** | **汇聚规则** |
| --- | --- |
| 15分钟 | 表示数据汇聚采集时间以15分钟为单位。如配置测试任务时测试周期选择为5分钟，则15分钟有3个数值，“TWAMP质量报表”反映的是3个数值的平均，最大，最小质量指标值。 |
| 每小时 | 表示数据汇聚采集时间以1小时为单位。如配置测试任务时测试周期选择为15分钟，则1小时有4个数值，“TWAMP质量报表”反映的是4个数值的平均，最大，最小质量指标值。 |
| 每天 | 每天是采集小时的平均值数据进行展示，一天有24个小时，则每天有24个数值，“TWAMP质量报表”反映的是24个数值的平均质量，最大，最小指标值。 |
| 每周 | 每周是采集每天内小时的平均值数据进行展示，每天内有24个小时，则每周有168个数值，“TWAMP质量报表”反映的是168个数值的平均，最大，最小质量指标值。 |
| 每月 | 每月是采集每天的平均值数据进行展示，以每月为30天计，则每月有30个数值，“TWAMP质量报表”反映的是30个数值的平均，最大，最小质量指标值。 |
| 每年 | 每年是采集每天的平均值数据进行展示，以每年为365天计，则每年有365个数值，“TWAMP质量报表”反映的是365个数值的平均，最大，最小质量指标值。 |

支持数据排序：报表表头中提供向上或向下箭头，系统管理员可使用这些箭头对数据进行升序或降序排列。

支持过滤数据：报表支持对数据进行过滤显示。

支持自定义表头：可根据需求，删除或重新排序报表的表头。

查看并导出报表，可根据需要自定义时间粒度（15分钟、每小时等），报表数据列，并导出报表数据。

导出文件类型包括EXCEL、CSV、PDF。

## 质量地图呈现

支持查看TWAMP质量区域地图，可呈现不同区域的TWAMP质量分布情况。

支持配置地图指标：可选择TWAMP/ICMP对应性能指标。

地图染色告警设置：根据区域业务某个指标超过设置的阈值级别，支持以不同的颜色显示在界面地图上。

针对全网业务，使用TWAMP或ICMP监测相应的性能指标；依据门限设定对业务进行标记，例如时延、丢包或抖动指标严重越限的，标记为有严重质量问题的业务，稍有丢包和越限的，标记为重要质量问题的业务。

单个测量实例的质量问题等级可参照性能告警等级分为严重质量问题、重要质量问题、普通质量问题和轻微质量问题。

针对某一管理区域，遍历该区域下所有测量实例。针对每一区域，质量问题实例/所有实例 \*100%。

− 绿色表示区域业务指标情况为好级

− 黄色表示区域业务指标情况为中级

− 红色表示区域业务指标情况为差级

− 蓝色表示区域未监控

地图染色规则如下：

当某一区域的业务质量出现问题时，会根据问题的严重程度，以不同的颜色显示在地图上。建议：

■当该区域有严重流量问题的比例(红色比例)>=10%，地图上该区域将显示红色。

■当该区域存在有严重流量问题时，有严重流量问题的比例(红色比例)<10%且有严重流量问题的比例(红色比例)+有重要流量问题的比例(黄色比例)>=10%，地图上该区域将显示黄色。

■当该区域，有严重问题的比例(红色比例)+有重要问题的比例(黄色比例)<10%，地图上该区域将显示绿色

查看某区域的业务质量状况：在区域地图上单击区域名称，可显示当前区域相关的业务质量数据，并进一步钻取展开该区域所有测试例中的相应指标的详情，并支持对结果进行排序。

## 质量告警分析

支持针对时延、抖动、丢包率等指标设定阈值，在网络质量劣化超过阈值时产生告警，告警级别可设置，利于客户针对不同的告警采取不同的措施，建议设置为：

|  |  |  |
| --- | --- | --- |
| 告警级别 | 说明 | 处理办法 |
| 紧急告警 | 已经影响业务，需要立即采取纠正措施的告警，定义为紧急告警。 | 需紧急处理，否则系统有瘫痪或业务中断危险。 |
| 重要告警 | 已经影响业务，如果不及时处理会产生较为严重后果的告警，定义为重要告警。 | 需及时处理，否则会影响重要业务运行。 |
| 次要告警 | 目前对业务影响轻微，但需要采取纠正措施，以防止更为严重的故障的发生。这种情况下的告警定义为次要告警。 | 根据此类告警及时查找告警原因，消除故障隐患。 |
| 提示告警 | 检测到潜在的或即将发生的影响业务的故障，但是目前对业务还没有影响。这种情况下的告警定义为提示告警。 | 根据告警了解网络和设备的运行状态，视具体情况进行处理。 |

系统需支持告警模板功能。告警模板可对不同测量协议的KPI指标进行阈值指定，并设置相应的告警等级。

提供告警查看和过滤：告警发生后，告警标志会立即显示，提醒告警已经发生，并以不同的颜色标示告警级别。支持过滤条件查询，根据过滤列表中的级别、确认状态、清除状态、产生时间、更多选项进行随意组合，从而过滤出符合条件的告警。这样便于对大量告警进行快速查找及定位，节省时间，提高运维效率。

支持不同级别的告警区分不同的颜色在物理拓扑上体现，关联监测实例网元，告警名称等详细信息。

## 质量监控分析的性能要求

系统支持的质量测试实例总数不少于10万，，若因设备处理效率原因不能一次性监控和数据采集，应支持分批次处理，每批次可支持不少于100条。

# 业务割接和网络优化调整

## 网络业务割接管理

网管系统应支持网络业务割接管理(对网络业务进行批量的调整功能)，网络业务割接包括两个主要部分：创建和管理L2业务割接计划、执行业务割接操作。业务割接计划是用户对网络业务割接的一次规划，在用户确定一个割接任务后，首先需要创建一个“业务割接计划”，它是网络业务割接功能的基础。一个业务割接计划中可以包含一个或者多个业务割接组，割接组是割接业务的承载体，在割接组内添加割接前后的业务。

### 割接任务管理

网管系统应该支持业务割接计划的管理功能，包括：业务割接计划的创建、修改、查询、删除，操作结果应提示用户。

业务割接计划支持的参数应该包括：

1. 业务割接计划名称；
2. 业务割接模式（人工、自动）；
3. 业务割接策略（尽量割接（遇到错误继续进行）、回滚割接（遇到错误就回滚））；
4. 业务割接时间（自动割接时需要指定业务割接时间）；
5. 业务割接计划备注；

### 割接组管理

网管系统应该支持业务割接组的管理功能，包括：业务割接组的创建、修改、查询、删除，操作结果应提示用户；

业务割接组支持的参数应该包括：

1. 业务割接组名称；
2. 所属的业务割接计划名称；
3. 割接业务列表；
   * + - 割接前电路；
       - 割接后电路。

### 割接场景

#### 源变宿不变

业务源端发生变化，末端未变化的情况下，对所涉及到的业务实现全网自动批量割接。



图7-1 源变宿不变图

#### 宿变源不变

业务源端未变化，末端发生变化的情况下，对所涉及到的业务实现全网自动批量割接。



图7-2 宿变源不变图

#### 源宿不变，交换节点变

业务/末端均未变化、其中间交换节点发生变化的情况下，对所涉及到的业务实现全网自动批量割接。



图7-3交换节点变图

### 割接任务执行

网管系统应支持用户手工和定时方式执行业务割接计划。

* 1. 支持割接数据校验，并明确提示校验信息；
  2. 执行业务割接计划的参数应该包括：
     + - 业务割接计划名称；
       - 业务割接计划执行时间；

### 割接结果查看

业务割接计划执行的结果应该包括：

1. 业务割接计划执行时间（校验时间、实际割接时间）；
2. 业务割接计划执行状态；
3. 业务割接组执行结果：
   * + - 割接成功的电路信息列表；
       - 割接失败的电路信息列表；
4. 割接计划执行的日志记录明确（包括起止时间、割接组名称、操作结果）；

## 网络业务调整

网管系统应支持在线修改网络业务的路由信息，以实现链路容量扩容、链或环加点、减点、离线减点、多点离线减点等场景。

### 网络调整功能通用要求

自动列出所有受影响的业务及隧道；

自动修改相关网元上的配置；

1. 调整隧道标签交叉应支持自动分配、和原隧道标签交叉保持一致；
2. 支持异常数据检查；
3. 支持割接过程详细进度展示；
4. 支持异常错误详细信息展示；
5. 支持进度明细化展示，包括割接流程过程内容；
6. 割接过程中发生变更的数据需要保存，便于核查；
7. 当遇到异常时，支持用户人工干预并由用户决定干预策略，包括但不限于继续割接、回退操作等

### 网络业务调整场景

以下场景包括环或者链路上承载的隧道（MPLS-TP、SR-TP）的调整。

#### 扩容加点

网络业务不断增加，当发展到一定程度，原有设备不能满足要求，需要进行加点操作，并且需要将原有业务部分切换到新加节点上。根据实际使用场景分析，加点操作主要是针对环或者链路进行的，并且需要将该环或者链路上承载的隧道（MPLS-TP、SR-TP）同步修改。

**一、拆环加点**



图7-4 拆环加点图

二、拆链加点

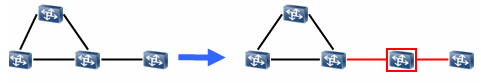


图7-5 拆链加点图

#### 接入环速率升/降级

****

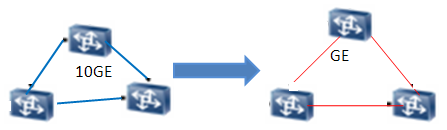
****

图7-6 环速率升级降级图

#### 减点

现网应用中，可能存在由于基站取消或基站搬迁等原因，需要修改穿通该设备的隧道不再经过该设备，并将通过该设备接入的相关业务取消，减点功能用来引导客户在网管中完成该过程。

一、拆环减点

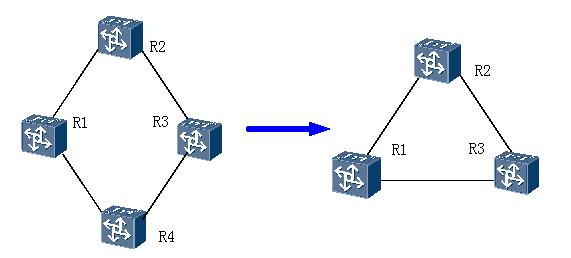


图7-7 拆环减点图

二、拆链减点

拆链减点分为3种场景，其中A节点是环与链的交点，B、C为链上网元。

场景1：拆链中间点

A是环与链相切点，彻底断开A-B和B-C之间的物理连接，进行减点。



图7-8 拆链中间点图

场景2：拆链末端点

A是环与链相切点，彻底断开B-C之间的物理连接，进行减点。



图7-9 拆链末端点图

场景3：拆链始端点

A是环与链相切点，彻底断开A-B之间的物理连接，把A 减掉，进行减点。A点摘除，B点作为环与链相切点

C

D

F

B

C

B

F

D

A

E

从链路摘出

E

图7-10 拆链始端点图

三、离线网元减点

离线网元减点包括以下两种场景：

* 链路减节点：如下图所示，在直连链路上减节点R3、R4（已离线），可以将原来经过R2-R3-R4-R5的MPLS-TP隧道和SR-TP隧道调整为经过R2-R5。

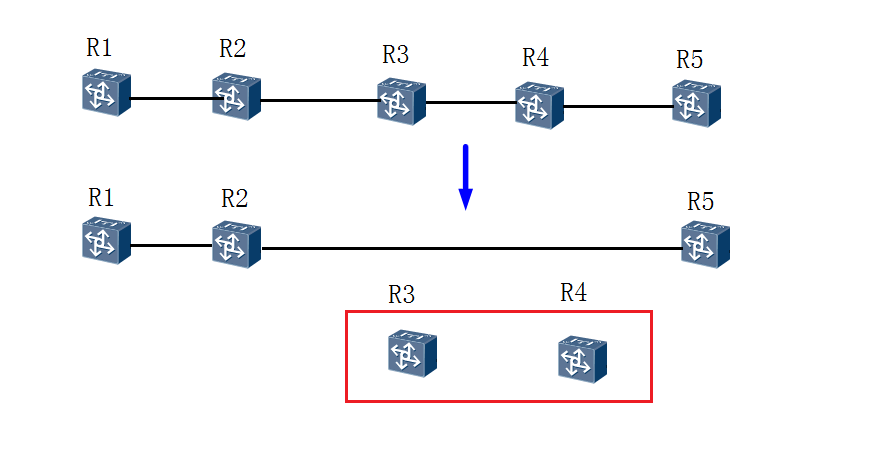


图7-11 离线网元链路减点图

* 环减节点：如下图所示，在环形链路上减节点R4、R5（已离线），可以将原来经过R1-R5-R4-R3的MPLS-TP隧道和SR-TP隧道调整为经过R1-R3。

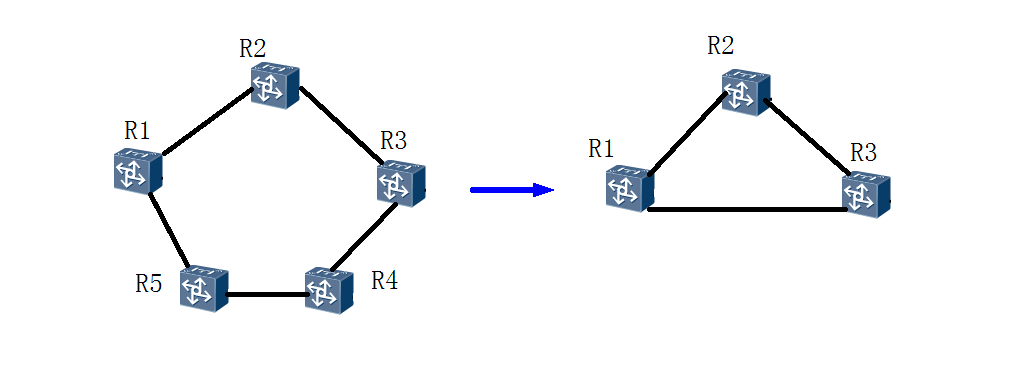


图7-12 离线网元环减点图

#### 链路调整

该功能解决了因单板故障或者单板容量升级等情况下将链路上业务全部或部分批量切换到另外一条链路上的需求。

升级/调整链路容量包括以下两种场景：

一、非负载分担场景

* 调整单端端口

如下图所示为非负载分担调整单端端口的场景，调整直连链路p1-p2到p1-p3，可以将原来经过R2(p1)-R3(p2)链路的隧道（MPLS-TP、SR-TP）调整为经过R2(p1)-R3(p3)链路。

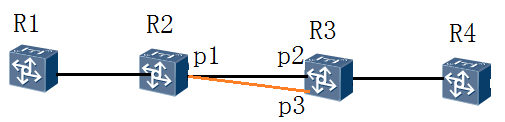


图7-13调整单端端口图

* 调整双端端口

下图所示为非负载分担调整双端端口的场景，调整直连链路p1-p2到p3-p4，可以将原来经过R2(p1)-R3(p2)链路的隧道（MPLS-TP、SR-TP）调整为经过R2(p3)-R3(p4)链路。

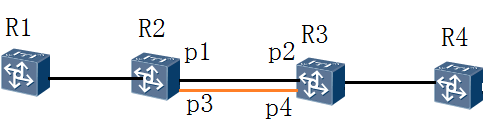


图7-14调整双端端口图

二、负载分担场景

如下图所示，负载分担场景主要通过添加一对端口链路p3-p4，可以将原来经过R2(p1)-R3(p2)链路的部分隧道（MPLS-TP、SR-TP）调整为经过R2(p3)-R3(p4)链路，待调整的业务需要用户手工进行选择。

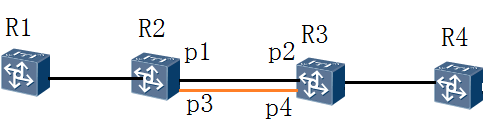


图7-15 负载分担图

#### 应急路由调整

当业务所在的工作和保护路径（MPLS-TP）均出现断纤故障，导致链路发生中断时，通过应急路由调整功能快速地计算、生成一条新的可用的临时逃生路由，让业务承载在逃生路由上，待断纤链路修复好之后再将业务回退到原有的路由上，从而避免了业务长时间的中断。

1、支持场景如下：

1）无隧道保护，隧道服务层链路中断

2）有隧道保护，两条隧道服务层链路都中断

2、应急路由调整前，支持数据备份，默认要求数据备份，以保障数据安全；

3、支持根据时间段或故障链路分析受影响的业务隧道；

4、支持选择需进行应急路由调整的故障隧道；

5、原中断链路恢复后，支持业务路径批量回迁；

6、支持应急路由调整的任务管理，应提供创建、查看、删除任务的功能，如果部分执行成功，支持再次对受影响的业务进行应急路由调整。

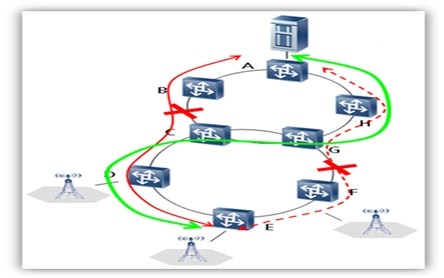


图7-16 应急路由调整图

#### 接入环上联节点变更

接入网上联节点退网情况下，支持将接入网业务割接到新的上联节点承载。

#### UNI端口业务迁移

落地点网元故障会造成较大范围的L2业务影响，OMC系统应支持指定的落地点网元一个和多个UNI端口，OMC系统自动分析受影响的业务，并批量迁移到另一指定的落地点网元UNI端口。

### 业务路由优化

OMC应支持隧道（MPLS-TP、SR-TP）同路由（工作和保护路径经过同一端口、同一板卡）的筛查，以列表形式呈现给用户，并支持用户指定其中一条、多条或全部进行计算和优化。

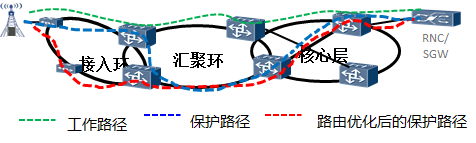


图7-17 业务路由优化图

# 巡检管理

巡检管理功能规范，主要确立了PTN/SPN网络关键的巡检项目及巡检指标，对自动巡检工具的输出内容进行了规范。

PTN自动巡检工具的主要功能包括网元检查、业务检查、保护检查、光功率检查、软件系统检查等等。该工具要求实现PTN/SPN网络日常巡检的批量化、自动化、模型化和定制化，输出标准化的网络巡检报表和巡检报告，给出处理建议，提升PTN/SPN网络巡检效率，保障网络质量。

PTN自动巡检工具的总体要求如下：

提供巡检任务管理。巡检任务可以自动或者手动执行；巡检任务可以定期执行；

巡检范围和巡检内容可以由用户自己定义；

巡检项目参数设置模板化，能够保存和修改；

巡检执行进度和执行结果随时可查；巡检结果以报表或者图形方式显示；

为了减少显示的数据量，所有巡检结果均只列出异常的设备或者业务，正常的结果不显示；

所有异常指标的标称值均提供自定义修改的功能。

## 巡检任务管理

完成巡检任务的定制、发布、修改编辑、删除等管理功能。

### 创建巡检任务

系统可支持用户创建新的巡检任务，用户创建巡检任务时需要指定如下巡检参数：

* 巡检对象范围，可以是全部网元，也可以指定的部分网元。
* 巡检项目，见17.2章节
* 巡检周期，支持不同粒度的周期，包括日、周、月、季度、半年、年。
* 巡检执行时间，在巡检周期内，指定巡检任务开始执行的时间或者时间范围。
* 系统可支持巡检任务模板功能：
  + 默认模板，用户在创建巡检任务时能直接调用和修改。
  + 自定义模板，支持用户自行创建巡检模板并存储，供后期巡检时直接调用。

### 查询巡检任务

用户可查询巡检任务的参数和巡检任务的执行状态以及执行进度。

巡检任务的执行状态包括：

* 未执行
* 执行中
* 已完成

巡检任务的执行进度通过进度条来显示。

### 修改巡检任务

用户可修改巡检任务的参数，可修改的参数包括：

* 巡检对象范围。
* 巡检项目。
* 巡检周期。
* 巡检执行时间。

注：执行中的任务不允许修改，必须先停止巡检任务才能修改。或者具备修改后的任务在下次执行时才生效的能力。

### 删除巡检任务

用户删除指定的巡检任务。

### 巡检任务的执行

1. 巡检任务调度

* 根据制定的巡检任务条件（手工执行、自动周期执行等）触发巡检任务执行。

对于手工执行的巡检任务，单次执行。

* 对于自动周期执行的任务根据任务执行周期定义定期调度执行。周期执行的任务可支持按日、周、月、季度、半年、年自动执行，也可定义单次执行任务；

1. 任务执行控制

负责调度任务的执行状态监视和控制。

* 监视任务执行过程：包括任务执行状态、任务执行原始结果记录实时查看等；
* 在任务监视界面可以启动、停止一个任务，或者暂停某个正在执行的任务；
* 提供手工触发巡检任务即时执行的功能。

### 巡检结果管理

根据预定好的巡检任务，对巡检任务的处理结果进行管理，包括巡检处理分析结果的输出，巡检原始结果和处理分析结果的存储、巡检结果的备份管理。

1. 巡检处理分析结果可以根据不同的任务，分为月、周和日以及自定义周期输出报告。分析结果以文件形式输出，输出格式支持EXCEL
2. 巡检结果的存储：

支持人工对巡检结果生成的文件保存，定时对分析结果进行备份。

## 巡检项目

### 网元状态检查

#### 网元告警检查

对用户需要关注的重要告警进行检查。提供定制化的模板，由用户自定义哪些告警属于需要关注的重要告警。

输出：存在问题的告警列表

|  |  |  |  |
| --- | --- | --- | --- |
| 网元名称 | 告警源 | 告警发生时间 | 告警名称 |
|  |  |  |  |

网元告警检查的默认项目：

* 网元设置环回检查

#### 网元性能检查

对用户需要关注的重要性能进行检查。提供定制化的模板，由用户自定义哪些性能属于需要关注的重要性能，每一种性能的标称值可以自定义。

输出：存在问题的性能列表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 性能标称值： | | | | | |
| 网元名称 | 性能源 | 性能名称 | 性能值 | 性能开始时间 | 性能结束时间 |
|  |  |  |  |  |  |

网元性能检查的默认项目：

* 端口误码异常检查
* 端口丢包异常检查
* 端口错误包异常检查

#### 单板状态检查

检查设备单板状态：在位/不在位，运行状态，输出报表。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网元名称 | 槽位 | 单板名称 | 在位状态 | 运行状态 |
|  |  |  |  |  |

#### 设备CPU使用率检查

检查设备CPU使用率，对于超过使用率门限的设备，以报表格式输出，输出内容包括：

* 网元名称
* CPU使用率

CPU使用率门限可以由用户自己修改。

|  |  |
| --- | --- |
| CPU使用率门限： | |
| 网元名称 | CPU使用率 |
|  |  |

#### 设备内存使用率检查

检查设备内存使用率，对于超过使用率门限的设备，以报表格式输出，输出内容包括：

* 网元名称
* 内存使用率

内存使用率门限可以由用户自己修改。

|  |  |
| --- | --- |
| 内存使用率门限： | |
| 网元名称 | 内存使用率 |
|  |  |

#### 设备风扇检查

检查网元的风扇是否存在风扇告警。

对于异常的网元，以报表形式输出，输出内容包括：

* 网元名称
* 告警源
* 告警发生时间
* 告警名称

|  |  |  |  |
| --- | --- | --- | --- |
| 网元名称 | 告警源 | 告警发生时间 | 告警名称 |
|  |  |  |  |

#### 设备电源检查

检查网元的电源是否存在电压过低或者电压过高的异常。电压的门限值由用户自己定义。

对于异常的网元，以报表形式输出，输出内容包括：

* 网元名称
* 性能源
* 性能名称
* 性能值
* 异常原因：电源电压过低/电源电压过高

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 性能标称值：最小值~最大值 | | | | |
| 网元名称 | 性能源 | 性能名称 | 性能值 | 异常原因 |
|  |  |  |  |  |

#### 网元单板温度检查

检查网元单板温度是否超过设定的门限，超过门限的设备以报表形式输出。

输出：网元温度异常列表

|  |  |  |  |
| --- | --- | --- | --- |
| 温度标称值：45℃ | | | |
| 网元名称 | 设备类型 | 单板名称 | 温度性能值 |
|  |  |  |  |

#### 网元监控检查

检查网元监控状态，对于脱管的网元以报表的形式输出，输出内容包括：

* 网管名称
* 网元名称

|  |  |
| --- | --- |
| 网管名称 | 网元名称（脱管） |
|  |  |
|  |  |

#### 网元单板通讯检查

检查网元上单板的告警，对存在单板通讯异常类告警的网元，输出报表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网元名称 | 单板名称 | 槽位地址 | 告警名称 | 告警开始时间 |
|  |  |  |  |  |

#### 设备与网管时间检查

检查网管服务器时间与设备的网元时间是否一致，不一致的网元输出报表：

|  |  |  |  |
| --- | --- | --- | --- |
| 网元名称 | 网元时间 | 网管时间 | 偏差值（） |
|  |  |  |  |
|  |  |  |  |

其中：偏差值=网管时间-网元时间

#### 主控板存储卡容量检查

检查主控板的存储卡剩余容量是否越限，门限可设置，对存储卡容量不足的板卡，输出报表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 网元名称 | 槽位地址 | 单板名称 | 存储卡类型 | 存储卡总容量 | 存储卡剩余容量 |
|  |  |  |  |  |  |

#### 10GE、GE端口工作状态检查

检查10GE、GE端口的工作状态，主要包括以下内容：

* 偏置电流是否超过门限值
* 发送光功率是否超过门限值
* 是否存在告警

存在异常的端口输出报表，报表内容包括：

* 网元名称
* 槽位地址
* 单板名称
* 端口名称
* 端口速率
* 异常原因：偏置电流异常、发送光功率异常、告警名称

输出：网元端口异常状态列表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 网元名称 | 槽位地址 | 单板名称 | 端口名称 | 端口速率 | 异常原因 |
| Xxx | 1 | Bbb1 | T1 | 10GE | 发送光功率过低 |
| Zzz | 2 | Bbb2 | T2 | GE | LOS |
|  |  |  |  |  |  |

#### 在用端口告警状态检查

检查在用端口的告警屏蔽/反转状态，存在告警屏蔽或者反转的在用端口，输出报表。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 网元名称 | 槽位地址 | 单板名称 | 端口名称 | 端口速率 | 端口用途 | 告警名称 | 告警状态 |
| Xxx | 1 | Bbb1 | T1 | GE | UNI |  | 屏蔽 |
| Zzz | 2 | Bbb2 | T2 | GE | NNI |  | 反转 |
|  |  |  |  |  |  |  |  |

#### 单板复位检查

检查网元在某一段时间内是否存在单板复位，单板复位超过一定频率的，输出报表。

检查时间段可以由用户输入。

复位频次门限由用户输入。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 检查时间段：开始时间—结束时间  复位频次门限： | | | | |
| 网元名称 | 单板名称 | 槽位地址 | 复位次数 | 复位原因 |
|  |  |  |  |  |

### 网元配置检查

#### 设备与网管关键配置数据一致性检查

检查设备单板上的数据与网管上的数据是否一致，不一致的网元以报表形式输出：

|  |  |
| --- | --- |
| 网元名称 | 不一致内容 |
|  |  |

检查的数据包括但不限于以下内容：

* 隧道
* PW
* 以太网业务
* TDM业务
* L3VPN业务

#### 主备主控单板配置数据一致性检查

检查主用主控单板与备用主控单板之间的配置数据是否一致，不一致异常网元输出报表。输出：主备单板数据不一致列表

|  |  |  |
| --- | --- | --- |
| 网元名称 | 单板名称 | 槽位地址 |
|  |  |  |

#### 主备单板保护配置检查

网元的某些槽位能够配置一主一备两块单板，本项目检查这些槽位上的单板配置异常情况。 需要检查的单板类型包括：

* 主控板
* 交叉板

配置异常原因包括：

* 保护单板未配置
* 保护单板未配置数据

检查时发现存在上述异常的，输出报表：

|  |  |  |  |
| --- | --- | --- | --- |
| 网元名称 | 单板名称 | 槽位地址 | 异常原因 |
|  |  |  |  |
|  |  |  |  |

### 网络配置检查

#### 时钟检查

检查网元的时钟状态是否存在异常，异常的网元以报表的形式输出。异常情况定义如下：

* 把网元上的时钟设置，与网元当前的时钟来源进行比较，不一致的属于异常。
* 网元上的时钟设置虽然与网元当前的时钟来源相同，但是都是“自振”状态的，也属于异常。

输出：网元时钟异常列表

|  |  |  |  |
| --- | --- | --- | --- |
| 网元名称 | 时钟设置 | 当前时钟来源 | SSM协议 |
|  |  |  |  |

#### 软件版本检查

同一端设备内部，主控板的软件版本与其它单板的软件版本应该保持匹配。本项目检查同一端设备的各个单板软件版本之间的配套性是否存在问题。

单板软件版本之间的配套性信息由用户手工导入系统，巡检系统提供导入功能。

存在配套性问题的网元，输出下列报表：

|  |  |  |  |
| --- | --- | --- | --- |
| 网元名称 | 单板名称 | 槽位地址 | 异常原因 |
|  |  |  |  |

#### 主备隧道(MPLS-TP、SR-TP)同路由检查

检查主用隧道和备用隧道经过的节点，是否存在经过同一个网元或者同一块单板的情况。存在经过相同单板或者相同网元的隧道，MPLS-TP、SR-TP分别输出报表。报表内容如下：

* 保护组名称
* 主隧道名称、主隧道ID
* 备隧道名称、备隧道ID
* 同节点原因：同网元/同单板
* 节点名称：网元名称/单板名称

报表格式如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 保护组名称 | 主隧道名称 | 主隧道ID | 备隧道名称 | 备隧道ID | 同节点原因 | 节点名称 |
|  |  |  |  |  | 同网元 | 网元名称 |
|  |  |  |  |  | 同单板 | 单板名称 |

#### 隧道(MPLS-TP、SR-TP)保护配置检查

检查没有配置保护的MPLS-TP、SR-TP隧道，分别列出没有配置保护的隧道名称。

|  |  |  |  |
| --- | --- | --- | --- |
| 隧道ID | 隧道名称 | 源网元名称 | 宿网元名称 |
|  |  |  |  |

#### 隧道端口工作模式配置检查

检查隧道两端的以太网端口工作模式配置，要求两端端口的工作模式应该配置一致。以太网端口工作模式包括以下几种方式：

* 自动协商
* 10000M全双工
* 1000M全双工
* 100M半/全双工

两端端口工作模式不一致的隧道，输出报表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 隧道名称 | 源端口 | 源端工作模式 | 宿端口 | 宿端工作模式 |
|  |  |  |  |  |

#### 隧道告警检查

对用户需要关注的重要告警进行检查。提供定制化的模板，由用户自定义哪些告警属于需要关注的重要告警。

输出：存在问题的告警列表

|  |  |  |  |
| --- | --- | --- | --- |
| 隧道名称 | 告警源 | 告警发生时间 | 告警名称 |
|  |  |  |  |

#### LTE的L2 VPN保护配置检查

检查LTE的L2业务是否配置双归保护，对于存在配置问题（是否配置、配置参数问题）的业务，输出报表。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 业务ID | 业务名称 | 保护类型 | 是否配置 | 配置参数问题 |
|  |  |  |  |  |

#### L2/L3设备双网关配置检查

检查L2/L3设备三层虚接口/三层虚子接口的参数，比对是否实现双网关保护，输出参数报表。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 网元名称 | 接口名称 | 子接口名称 | IP | 掩码 | VLAN | MAC |
|  |  |  |  |  |  |  |

#### L2/L3设备双网关ARP热备检查

检查L2/L3设备是否开启了ARP热备，输出报表。

|  |  |  |
| --- | --- | --- |
| 网元名称 | 子接口名称 | ARP热备开启状态 |
|  |  |  |

#### L2/L3设备的ARP代理检查

检查L2/L3设备的三层虚接口/三层虚子接口是否开启了ARP代理，输出报表。

|  |  |  |
| --- | --- | --- |
| 网元名称 | 端口名称 | ARP代理状态 |
|  |  |  |

#### L2/L3设备的ARP表检查

检查L2/L3设备三层虚接口/三层虚子接口的主备ARP表，比对是否一致，输出报表。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网元名称 | 主/备状态 | 子接口名称 | IP | MAC |
|  |  |  |  |  |

#### L2/L3、L3设备路由完整性检查

检查L2/L3、L3设备主备路由表，输出报表。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 网元名称 | 网元ID | 目的IP | 掩码 | 下一跳IP/接口 | 优先级 |
|  |  |  |  |  |  |

#### L2/L3、L3设备路由一致性检查

检查L2/L3、L3设备主备路由是否完全相同，输出报表。

|  |  |  |
| --- | --- | --- |
| 主节点名称 | 备节点名称 | 路由表一致性 |
|  |  |  |

#### L3 VPN的UNI接口FRR保护配置检查

检查L3 VPN的UNI接口是否配置了FRR保护，输出报表。

|  |  |  |  |
| --- | --- | --- | --- |
| 网元名称 | 主路由 | 备路由 | 保护状态 |
|  |  |  |  |

#### QoS带宽配置检查

检查端口、隧道和业务的QoS配置是否合理，对于存在异常的对象，以报表形式输出。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 端口名称 | 带宽配置 | 隧道名称 | 带宽配置 | 业务名称 | 带宽配置 | 异常原因 |
|  |  |  |  |  |  |  |

#### L3节点BFD配置及状态检查

检查IP FRR的主路由是否配置了静态路由BFD，对于异常的网元，以报表形式输出(未配置BFD则对象字段显示为空)，报表字段可参考如下表格或其他正确表达结果的字段：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 节点名称 | VRF | 本端BFD ID | 对端BFD ID | 源BFD会话状态 | 宿BFD会话状态 |
|  |  |  |  |  |  |

#### DNI-PW保护场景下隧道同路由检查

检查承载DNI PW的工作和保护Tunnel是否存在同路由的情况，如同网元、同单板等，以报表形式输出。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| DNI PW ID | 主隧道名称 | 主隧道ID | 备隧道名称 | 备隧道ID | 同节点原因 | 节点名称 |
|  |  |  |  |  | 同网元 | 网元名称 |
|  |  |  |  |  | 同单板 | 单板名称 |

#### 隧道承载业务合规性检查

检查隧道是否有承载多条业务的情况，以报表形式输出。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 隧道ID | 隧道名称 | 源网元名称 | 宿网元名称 | 承载业务数 |
|  |  |  |  |  |

### 网络状态检查

#### DCN子网网元个数检查

检查每个网关网元下挂的网元数量是否超过门限值。门限值可以设置。超过门限值的网关网元输出报表：

|  |  |
| --- | --- |
| 门限值： | |
| 网关网元名称 | 下挂网元个数 |
|  |  |

#### 网关网元通达状态

检查网管服务器与网关网元的通信状态，通信异常的网关网元输出报表：

|  |
| --- |
| 网关网元名称 |
|  |

#### 主备网关网元的倒换状态

检查每一个网元当前使用的是主用网关网元还是备用网关网元，如果使用的是备用网关网元，输出报表：

|  |  |  |  |
| --- | --- | --- | --- |
| 网元名称 | 主网关网元名称 | 备网关网元名称 | 当前网关 |
|  |  |  |  |

#### IP地址与规划地址匹配检查

检查网元的IP地址是否在规划地址范围之内。规划地址范围可由用户输入。不在规划地址范围的网元，输出报表：

|  |  |
| --- | --- |
| 规划地址范围：xx.xx.xx.xx ~ xx.xx.xx.xx | |
| 网元名称 | IP地址 |
|  |  |

#### IP地址冲突检查

检查同一个域内网元或者端口的IP地址是否存在冲突。检查范围由用户指定。

对存在IP地址冲突的网元或者端口，输出报表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP地址 | 对象1 名称 | 对象2名称 | 对象3名称 | 对象N名称 |
|  |  |  |  |  |
|  |  |  |  |  |

对象：网元或者端口

#### CV帧发送时间检查

检查TMS层CV帧的发送时间是否为默认3.33ms，如果不为默认，要确保对通的两端的CV帧发送时间一致。

两端CV帧发送时间不一致的输出报表：

|  |  |  |  |
| --- | --- | --- | --- |
| 网元名称 | 发送时间 | 对端网元名称 | 对端发送时间 |
|  |  |  |  |

#### OAM帧状态检查

检查各设备TMS、TMP、TMC各层CV帧、环回帧、LM帧、DM帧状态，在正常情况下，确认其为“不使能”。

用户可以选择检查层次和需要检查的帧类型。

检查层次选项：

* TMS层
* TMP层
* TMC层

检查帧类型选项：

* CV帧
* 环回帧
* LM帧
* DM帧

检查发现其状态为“使能”的，输出报表：

|  |  |  |
| --- | --- | --- |
| 网元名称/隧道名/伪线名 | 层次名称 | 帧类型 |
|  |  |  |
|  |  |  |
|  |  |  |

#### 单板级保护倒换检查

检查主备单板之间是否发生了倒换，发生倒换的单板输出下列报表：

|  |  |  |  |
| --- | --- | --- | --- |
| 网元名称 | 槽位地址 | 单板名称 | 倒换时间 |
|  |  |  |  |

#### LAG端口保护倒换检查

检查LAG端口内部是否发生了倒换，发生倒换的端口输出下列报表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 链路聚合组编号 | 网元名称 | 槽位地址 | 单板名称 | 端口名称 | 倒换时间 |
|  |  |  |  |  |  |

注：LAG端口设置了负载均衡模式的除外。

#### 隧道保护倒换检查

检查具有保护配置的隧道，是否发生了倒换，发生了倒换的隧道输出下列报表：

|  |  |  |  |
| --- | --- | --- | --- |
| 保护组ID | 隧道名称 | 倒换网元名称 | 倒换时间 |
|  |  |  |  |

#### 双归端口保护倒换检查

检查配置了双归保护的端口，是否发生了倒换，发生倒换的端口输出下列报表：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 主网元名称 | 主槽位地址 | 主单板名称 | 主端口名称 | 备网元名称 | 备槽位地址 | 备单板名称 | 备端口名称 | 倒换时间 | 当前工作状态 |
|  |  |  |  |  |  |  |  |  | 主用/备用 |

#### LTE的L2 VPN保护状态检查

检查LTE的L2 VPN保护组是否发生了倒换，发生倒换的保护组输出下列报表。

|  |  |  |  |
| --- | --- | --- | --- |
| 网元名称 | 保护组名称 | 保护组状态 | 倒换时间 |
|  |  |  |  |

#### 链路端口参数检查

检查链路两端端口的配置参数（IP地址段，光模块传输距离、波长，工作模式）是否一致，对于配置参数不一致的链路，输出下列报表：

|  |  |  |  |
| --- | --- | --- | --- |
| 链路名称 | 本端端口 | 对端端口 | 不一致参数项 |
|  |  |  |  |

#### 光纤双方向损耗检查

检查光纤双方向（A端点的发光功率-Z端点的收光功率）-（Z端点的发光功率-A端点的收光功率）的绝对值是否大于门限值，门限值可设置。对于越限的链路，输出下列报表：

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A端网元端口名称 | Z端网元端口名称 | A端发光功率 | Z端收光功率 | A→Z光纤损耗值 | Z端发光功率 | A端收光功率 | Z→A光纤损耗值 | 双向损耗差值 | 是否越限 |
|  |  |  |  |  |  |  |  |  |  |

#### 工作光功率检查

采集光模块型号，并检查155M，GE，10GE等光口的光功率，光功率超过设定阈值范围的，输出报表。

光功率阈值可以由用户自定义，阈值按照严重程度分为两种，一种为预警阈值，报表中用橙色表示，一种为告警阈值，报表中用红色表示。并统计出光功率合格率。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 预警阈值：  告警阈值：  合格率： | | | | | | | | | |
| 网元名称 | 槽位地址 | 单板名称 | 端口名称 | 光模块型号 | 速率 | 收/发光功率 | 过载点 | 灵敏值 | 异常程度 |
|  |  |  |  |  |  |  |  |  |  |

异常程度：预警/告警

#### 光功率波动

检查一段时间内，端口的光功率相对于初始值的波动是否超过设定的阈值。

用户自定义内容：

* 检查时间段：开始时间、结束时间
* 光功率初始值：可以选择某一个15分钟历史性能作为初始值
* 光功率波动阈值

输出：光功率波动异常信息

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 波动阈值： | | | | | | | |
| 网元名称 | 槽位地址 | 单板名称 | 端口名称 | 速率 | 收/发光功率 | 初始值 | 波动值 |
|  |  |  |  |  |  |  |  |

#### 光功率趋势

检查一段时间内端口的光功率趋势，光功率的趋势采用折线图的方式显示。

光功率趋势图的时间间隔可以分为：每日、每周、每月、每季度、每半年、每年

光功率数据采样间隔分别为：

* 每2小时：日趋势图
* 每1天：周趋势图
* 每1周：月趋势图；
* 每1月：季度趋势图、半年趋势图
* 每3月：年趋势图

## 巡检结果调优

针对每项巡检结果，给出优化建议。用户根据这些优化建议，对网络实施整改并对调整结果进行确认，最终达到优化网络的目的。

# 智能运维

## 流量预测

OMC系统应支持基于历史流量数据，通过大数据分析算法进行流量预测，即能根据现网已有的历史流量数据，结合机器学习等人工智能算法，快速全面预测全网流量趋势，预警即将饱和的业务，精准定位网络资源（端口、链路、环网）瓶颈，以指导现网提前进行调整或扩容，并且可以帮助运营商提前进行大客户流量营销。

1·支持模型训练及管理

提供训练模型能力，支持模型保存；

提供模型管理能力，例如：模型的查看、删除或者外部模型导入等；

2、支持周期性流量趋势预测

支持利用历史流量数据，预测未来3个月~12个月的趋势；

流量趋势预测支持按照区域、对象（端口、链路和环网）指定；

应支持图形化呈现历史流量数据和周期性流量趋势预测结果；

支持流量预测功能的开启和关闭。

3、支持预测数据与真实数据准确率的对比

偏差率=**|**预测数据-真实数据**|**/真实数据

准确率= 偏差率小于20%的预测对象个数M/所有预测对象个数N，N为每个监测周期的（监测实例数\*每实例的预测的指标个数）\*监测周期数量，M<=N。

2、网络资源瓶颈直观可视

结合可监测的流量指标（不限于带宽利用率忙时均值和带宽利用率峰值）和设置的阈值，分析和呈现网络资源（端口、链路、环网）瓶颈，并可图形化展现瓶颈资源；

支持下钻查看网络资源瓶颈的流量趋势变化；

1. 支持周期性预测结果的查询。

## SR-TP故障回溯

OMC系统支持历史故障回溯，并通过分析路径（SR-TP）性能KPI（时延、丢包），快速定位故障。

1）历史故障回溯

OMC系统查看到路径（SR-TP）性能劣化告警，对产生告警的路径可进行历史故障回溯和诊断。

2）历史路径标注故障链路

支持根据时间轴回溯历史路径、故障和SR-TP性能（时延、丢包）。

3）性能劣化关联分析

支持故障链路、端口性能劣化的关联分析，支持查看逐跳路径详细信息，可下钻查看端口流量、光功率性能、队列丢包、端口误码等信息。

## 带内性能诊断

OMC系统基于真实业务流进行带内性能检测（In-Band OAM），提供实时、高精度的网络端到端性能可视化和逐跳故障定界能力，提升性能劣化类故障的定界、定位效率。

带内性能数据使用telemetry协议快速上报到OMC系统。

1．带内业务流自动识别

(1) OMC系统自动识别并标识业务流；

(2)根据基站IP地址、EPC IP地址，自动识别基站到EPC的端到端路径和业务质量。

2. 带内业务流手动创建

3. 带内业务质量指标

根据基站检测业务性能，输出性能指标包括平均时延、最大时延、丢包数、平均丢包率、最大丢包率等。

4．逐跳精确定界

检测到端到端性能异常，按需启动带内逐跳检测，逐跳数据叠加，精确定界故障位置。

5.历史路径回溯

支持业务路径历史回溯,。

## 网络故障模拟仿真

OMC具备网络故障的模拟仿真，通过模拟网络故障后流量分布，发现网络瓶颈点，提醒客户提前扩容。

1、设置故障点

用户按需设置多个网元、链路故障点，为后续分析做准备。故障设置分类：

-单网元故障

-多网元故障

-单条链路故障

-多条链路故障

-多网元、链路组合故障

网元、链路故障的设置，只用于故障仿真分析的输入，不影响现网网元。

支持网元、链路故障点撤销。

2、仿真分析

故障设置完成之后，进行SR-TP故障仿真分析。

故障仿真分析结束后，查看仿真统计信息，包括仿真时间、仿真链路及其承载的SR-TP隧道、链路带宽利用率、仿真对象数量等信息。

提示故障点对应影响的链路等网络瓶颈信息，及影响的SR-TP隧道。

# 附录1--PTN/SPN网络流量指标体系与应用方案

## 流量指标体系

PTN/SPN网络应从“业务”和“网络”两个维度开展流量的管理分析：

1. **业务维度：**针对业务层面进行流量统计分析，分析结果主要应用在以下方面：
2. 用于科学部署PTN/SPN网络各类业务的QOS应用策略和带宽参数，并配合定期开展的各类业务QoS性能评估测试工作，对应用策略和带宽参数进行优化调整；
3. 用于实施对重点业务性能质量（保证带宽等）的监控，并生成给用户的SLA报告，或解决用户对业务保证带宽不足问题的查障验证；
4. 用于定期分析掌握各类业务占用PTN/SPN网络流量的总体构成和发展趋势。通过对业务流量进行分类统计分析，可全面掌握2G基站、3G基站、LTE基站和集团客户专线等各类业务在PTN/SPN网络中各自占用的总流量情况；
5. 用于监测分析各类业务不同区域UNI端口流量现状和发展趋势，通过对各类业务端口流量进行长期监测和统计分析，可准确获知各类业务的保证带宽利用率和忙闲时流量特性，提供给相关业务部门，用于指导市场运营。
6. **网络维度：**针对网络层面进行流量统计分析，分析结果主要应用在以下方面：
7. 通过对“线路端口”、“LSP”、“PW”等对象的流量统计分析，便于实现PTN/SPN网络各层流量分布的关联分析，查找导致线路端口流量超出阈值的相关LSP和PW，指导进行网络业务路径的优化调整或带宽参数调整。
8. 通过“端口”、“链路”和“传输环路/系统”等对象的流量统计分析，便于全面掌握PTN/SPN网络流量的分布状态和增长趋势；
9. 实现对PTN/SPN网络资源的科学化预警管理，定期统计分析获得超过带宽使用阈值门限的端口、链路和传输环路/系统的列表，指导进行网络扩容、流量均衡和避免拥塞等；

### 流量监测对象

PTN/SPN网络流量监测的基本对象包括物理端口、伪线（PW）和隧道（LSP），具体示意见图11-1。其中，物理端口又分为用户侧端口（UN）和网络侧端口（NNI）；PW与业务流具有一一对应关系；LSP与PW可以是一一对应，也可以是多条PW复用到一条LSP。PTN/SPN网络流量监测的基本参数是某个监测对象在一定采集周期的发送和接收字节数，从收、发字节数可计算得出该采集周期内的收、发流量。

表10-1 PTN流量监测的基本对象及指标

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 流量监测的基本对象 | 分类 | 流量监测的子对象类型 | 基本监测指标 |
| 1 | 用户侧端口（UNI） | 物理对象 | TDM端口：E1、STM-1；  以太网端口：FE、GE、10GE等； | 收、发字节数 |
| 2 | 网络侧端口（NNI） | 物理对象 | 以太网端口类型：GE、10GE、40GE、100GE等；  城域传送网分层：接入层端口、汇聚层端口、核心层端口等。 | 收、发字节数 |
| 3 | 伪线（PW） | 逻辑对象 | 不同优先级的PW，对应不同优先级的业务流。  支持PW标识业务类型属性 | 收、发字节数 |
| 4 | 隧道（LSP） | 逻辑对象 | 对于PW和LSP 1:1对应的情况，要求同PW；  对于PW和LSP N:1复用的情况，LSP对应不同业务节点或客户的传送管道，如2G基站、3G基站、LTE基站、某个集客专线客户、某个PON系统的OLT上联端口等。 | 收、发字节数 |
| 5 | 传输环路 | 物理对象 | 通过分析带环节点的东西向的网络侧端口流量来实现。 | 收、发字节数 |
| 6 | 传输链路 | 物理对象 | 通过分析根节点的网络侧端口流量来实现。 | 收、发字节数 |

**链路：**是两个网络侧端口之间的连接对接关系，包括源网元和源端口、宿网元和宿端口等信息。相对于端口，以链路为对象进行PTN/SPN网络流量的统计分析可以更加直观地反映出数据传送的源端和宿端信息。链路流量可监测源端口的双向流量或宿端口的双向流量。

**业务优先级：**对于一些重要的TD-LTE基站、集团客户专线等业务，用户侧端口内包括不同优先级的业务流，可根据需要在PTN设备上开启针对不同优先级业务流的流量监测。由于VLAN业务流的VLAN优先级映射到PW的优先级，因此通过监视不同优先级的PW的流量可反应不同VLAN优先级业务流的流量情况。

**PTN传输环路：**是指以环形为拓扑的PTN传输系统，以PTN传输环路为对象进行网络流量监测和管理分析，可真实掌握每个环系统的已用容量和剩余容量。PTN传输环路流量是指出环节点的东西两个线路侧端口的流量之和。根据城域传送网的组网结构，PTN传输环路系统分为城域核心层传输环路、汇聚层传输环路和接入层传输环路三个子对象。

### 流量监测模式

PTN/SPN网络流量监测分为长期主动监测模式和短期按需监测两种模式。

**长期主动监测模式**是指PTN网管系统开启流量监测，配置相应的采集周期（一般为15分钟）和监测时长（如24小时、7天、1个月等，可具体配置起始和结束时间）后，持续以一定的采集周期（如15分钟）开展流量监测，在配置的监测时长内以一定的周期定期上报流量监测数据；该模式主要用于实施长期流量监测和管理分析。

**短期按需监测模式**是指PTN网管开启以秒为采集周期的短期流量监测，快速查询端口、PW或LSP的接收和发送流量状态；该模式主要用于发现丢包等流量异常问题后的实时查障和快速定位分析。

若不特殊指出，本标准所指的流量监测模式均是指长期主动监测模式。

### 流量监测周期

1. **采集周期：**是指进行流量监测基本数据采集的时间间隔；流量长期主动监测模式支持的采集周期应为15分钟；短期按需监测模式支持的采集周期可配置为1秒或5秒、1分钟或15分钟；
2. **监测时长：**是指流量监测的起始时间到结束时间之间的时间段，应支持监测时长的定制化配置，即配置具体开始时间点和结束时间点；对于长期主动监测模式，网管配置开启流量监测后，则一直长期监测，除非网管下发配置命令终止流量监测；对于短期按需监测模式，网管配置开始时间点和结束时间点或监测的次数。
3. **上报周期：**是指PTN设备向PTN网管系统自动上报流量监测数据的周期，上报周期一般等于采集周期，或者配置为采集周期的倍数；为了减少对DCN网的流量冲击，建议采用1小时或4小时上报一次。
4. **报表生成周期：**是指PTN网管系统自动生成流量分析报表的周期，支持配置为小时报、日报、周报和月报等，或支持用户自定义周期。

|  |  |  |  |
| --- | --- | --- | --- |
| 监测模式 | 采集周期 | 上报周期 | 监测规格 |
| 15分钟平均值 | 15分钟 | 15分钟 | 200万监测实例 |
| 15分钟秒级峰值 | 1秒/5秒 | 15分钟 | 200万监测实例 |
| 秒级精准监控 | 1秒 | 15分钟 | 网元支持的监控实例不少于100条，全网资源总实例数不少于1000个 |
| 分钟级平均值重点监控 | 5秒/10秒 | 1分钟 | 网元支持的监控实例不少于100条，全网同时监控网元不少于500个，实例数不少于5000条 |
| 秒级实时监控 | 5秒/10秒 | 5秒/10秒 | 同时监控和呈现的实例数不少于8个 |

### 流量监测和分析流程

PTN/SPN网络流量监测和管理分析的基本流程如下：

1. **流量数据采集：**PTN网管选择流量监测对象，设置合适的采集周期、监测时长和上报周期，开启流量监测功能，支持以设定的采集周期获取和显示最基本的流量数据（在采集周期内，被监测对象发送和接收的数据流量）。
2. **流量数据分类：**是指PTN网管系统对被监测对象及其流量数据进行统计分类，可按照所承载业务类型（2G基站、3G基站、LTE基站、集团客户专线业务等）、传输系统层次（接入层、汇聚层和骨干层）和地理区域信息等进行分类。
3. **流量指标计算：**是指PTN网管系统计算被监测对象的各项流量监测和分析指标，得到“流量”、“流速”和“带宽利用率”等指标。
4. **输出“基础数据表”：**是指PTN网管系统完成被监测对象的所有流量指标计算后，根据用户要求输出“PTN/SPN网络流量监测基础数据表”，具体内容和格式要求见规范的PTN/SPN网络流量分析的基础数据表。
5. **流量深度统计分析：**在“基础数据表”的基础上，PTN网管系统针对业务流量和网络流量开展更深入全面的统计分析，输出呈现各项分析结果和报表。



图10-1 PTN/SPN网络流量监测和管理分析的基本流程

### 流量监测和分析指标说明

#### 方向性

流量在PTN/SPN网络的管道（端口、LSP、PW）中有收、发两个相反的传输方向，如端口发送方向和端口接收方向，这种特性称为“方向性”。在计算和分析PTN/SPN网络流量指标时需要指明方向，如“端口发送带宽利用率”，“端口接收带宽利用率”，“链路源到宿流量”和“链路宿到源流量”等。

关于“端口”的流量指标分为“发送”和“接收”两个方向。

关于“链路”的流量指标分为“源到宿”和“宿到源”两个方向。

关于“业务”的流量指标分为“源到宿”和“宿到源”两个方向。

关于“传输环路”和“传输链路”的流量指标分为“发送”和“接收”两个方向。

#### 忙闲时

“流速”和“带宽利用率”等指标与采集时间段有明显关系，对于同一个流量监测对象，忙时的流速和带宽利用率可能远远大于闲时的流速和带宽利用率，计算忙时流速的均值或忙时带宽利用率的均值，比不区分忙时和闲时计算得到的相关指标结果更有实际参考意义。例如，参考忙时平均流速指标值来设置QoS带宽参数中的保证带宽（CIR），比不区分忙闲时计算得到的均值流速作为CIR参考值，更符合业务流量模型，也能更好保证高优先级业务的时延性能；忙时峰值流速指标的最大值可用于设置QoS带宽参数中的峰值带宽（PIR）。

对于一个监测对象，流量采集周期为15分钟，若监测时长为1天，则共有4\*24=96个采集点，可计算得到96对收、发流速值，绘制成流速曲线，可能存在单峰、多峰，对称、非对称等不同分布趋势特性，因此采用取多个峰值点的方式来确定忙时时段具有较多不确定性，可能造成每次确定的忙时具体时段不同，不具备流量指标的长期可比性。

为了便于统一分析对比不同地市的PTN/SPN网络忙时利用率，本标准给出了忙时的定义和计算方法，并建议各省公司在PTN流量监测分析试点过程中，针对系数的取值范围和默认值进行深入分析，并且在流量分析结果中需要说明忙时的时长和具体的忙时起止时间。

**日忙时的取值方法：**采用取 15 分钟指标的基础数据 TopN 平均值方法，将不小于 TopN 平均值的采样点对应的时段作为忙时时段。 N 越小，忙时均值指标越接近峰值指标； N=40~50，则忙时均值接近日均值；建议N 取值可以等于 20或 30，即Top20平均值、Top30平均值。

#### 流量监测和分析指标汇总

针对端口（链路）、PW、LSP、传输环路和传输链路五大类监测对象，规范了表11-2中的16项流量管理分析指标的定义、计算方法和基础数据获取方式，其中PW业务流量、峰值流速、忙时平均流速、带宽利用率忙时均值、带宽利用率峰值、端口配置的保证带宽利用率、业务（PW）配置的保证带宽利用率、各类业务流量占比等8个指标为关键指标。

表10-2 PTN流量管理分析指标汇总

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 基本指标名称 | 获取方式 | 指标适用性 | | | | |
| 端口  (物理) | PW  (逻辑) | LSP  (逻辑) | 传输环路(物理) | 传输链路(物理） |
| 1 | 流量（关键指标：PW业务流量） | 通过监测直接获取 | √ | √ | √ | √ | √ |
| 2 | 流速 | 通过监测数据计算获取 | √ | √ | √ | √ | √ |
| 3 | **峰值流速（关键指标）** | 通过监测数据计算获取 | √ | √ | √ | √ | √ |
| 4 | **忙时平均流速（关键指标）** | 通过监测数据计算获取 | √ | √ | √ | √ | √ |
| 5 | 带宽利用率 | 通过监测数据和配置数据计算获取 | √ | √ | √ | √ | √ |
| 6 | 带宽利用率均值 | 通过监测数据和配置数据计算获取 | √ | √ | √ | √ | √ |
| 7 | **带宽利用率忙时均值（关键指标）** | 通过监测数据和配置数据计算获取 | √ | √ | √ | √ | √ |
| 8 | **带宽利用率峰值(关键指标)** | 通过监测数据和配置数据计算获取 | √ | √ | √ | √ | √ |
| 9 | 带宽繁忙度 | 通过监测数据和配置数据计算获取 | √ | √ | √ | √ | √ |
| 10 | 端口的保证带宽占比 | 通过监测数据和配置数据计算获取 | √ | — | — | √ | √ |
| 11 | **端口配置的保证带宽利用率(关键指标)** | 通过监测数据和配置数据计算获取 | √ | — | — | √ | √ |
| 12 | **业务（PW）配置的保证带宽利用率(关键指标)** | 通过监测数据和配置数据计算获取 | √（UNI端口） | √ | — | — | — |
| 13 | 业务总流量 | 通过监测数据计算获取 | √（UNI端口） | √ | — | — | — |
| 14 | **各类业务流量占比(关键指标)** | 通过监测数据计算获取 | √（UNI端口） | √ | — | — | — |
| 15 | L2PTN/SPN网络总流量 | 通过监测数据计算获取 | √ | √ | — | — | — |
| 16 | L3PTN/SPN网络总流量 | 通过监测数据计算获取 | √ | — | √ | — | — |

### 流量监测和分析指标定义

#### 端口、LSP/SR-TP或PW的流量

**定义：**一个时间段内，经过流量监测对象（如端口、PW、LSP等）传输的数据总量，具有方向性。在没有指明方向时，“流量”等于两个方向传输的数据量之和。

**基本单位：**兆比特（Mbit）。

**计算公式：**采集周期为15分钟时

端口：

收流量 =（总接收字节数+20\*帧数）\*8bit/1000000

发流量 =（总发送字节数+20\*帧数）\*8bit/1000000

LSP、PW：

收流量 =总接收字节数\*8bit/1000000

发流量 =总发送字节数\*8bit/1000000

总流量=收流量+发流量

**说明：**“流量”是一个累计值，一般情况下，其数值随采集时间延长而增加。在分析“流量”时，需要指明统计的时间段或长度，如“时流量”、“日流量”、“周流量”或“月流量”等。

#### 端口、LSP/SR-TP或PW的流速

**定义：**在单位时间内，经过流量监测对象所传输的数据量，具有方向性。

**基本单位：**兆比特/秒（Mbit/s）。

**计算公式：以15分钟采集周期为例，**

**收流速=**15分钟的收流量/（15\*60）

**发流速=**15分钟的发流量/（15\*60）

**流速=** MAX（收流速，发流速）

**说明：**“流速”是一个瞬时值，一般情况下，其数值随时间变化而上下波动。

#### 端口、LSP/SR-TP或PW的峰值流速

**定义：**在N个采集周期内，流量监测对象的最大流速，具有方向性。

**基本单位：**兆比特/秒（Mbit/s）。

**计算公式：**以15分钟采集周期为例，对于N个采集周期，

**收峰值流速=** MAX（收流速1, 收流速2,…,收流速N-1, 收流速N）

**发峰值流速=** MAX（发流速1, 发流速2,…, 发流速N-1, 发流速N）

**流速=** MAX（收峰值流速，发峰值流速）

**说明：**峰值流速可用于设置端口、LSP或PW的峰值带宽（PIR），可以取监测时长为1天、1周7天或1个月的峰值流速作为峰值带宽设置值，也可按照峰值流速的一定比例适当放大后作为峰值带宽设置值。

#### 端口、LSP/SR-TP或PW的忙时平均流速

**定义：**将某一监测时长（如1天或1周7天）内所采集的流速点绘制成流速分布曲线，将忙时时段内（忙时时段的取值方法见3.2.2节）的所有采集点的流速平均值作为忙时平均流速，具有方向性。

**基本单位：**兆比特/秒（Mbit/s）。

**计算公式：以15分钟采集周期为例，假设忙时内有M个采集点。**

**忙时平均收流速=**（忙时收流速1+忙时收流速2+…+忙时收流速M-1+忙时收流速M）/M

**忙时平均发流速=**（忙时发流速1+忙时发流速2+…+忙时发流速M-1+忙时发流速M）/M

**忙时平均流速=** MAX（忙时平均收流速，忙时平均发流速）

**说明：**忙时平均流速用于设置端口、LSP或PW的保证带宽（CIR）。

由于忙闲时段的定义与业务流量的具体时间分布特性密切相关，因此针对不同业务类型的UNI端口，其忙闲时段的定义将有所不同。例如，对于基站业务，通常忙时为6：00~22:59，而对于某些集团客户专线业务，忙时为8:00~17:59。为了方便忙时平均流速计算，对于线路端口、LSP、PW的忙时时段定义应统一，忙时的具体取值方法见3.2.2节，得到忙时时段对应的M个采集点。

#### 端口、LSP/SR-TP或PW的带宽利用率

**定义：**流量监测对象的流速与端口的物理带宽（Mbit/s）或LSP、PW设定的峰值带宽（PIR，Mbit/s）的比值，具有方向性。

**基本单位：**%

**计算公式：**

发方向带宽利用率 = 发流速/（端口物理带宽或LSP、PW的峰值带宽配置值）

收方向带宽利用率 = 收流速/（端口物理带宽或LSP、PW的峰值带宽配置值）

带宽利用率= MAX（收流速，发流速）/（端口物理带宽或LSP、PW的峰值带宽配置值）

**说明：**“带宽利用率”是一个瞬时值，一般情况下，其数值随时间变化而上下波动。

#### 端口、LSP/SR-TP或PW的带宽利用率均值

**定义：**N个采集周期的带宽利用率的平均值，具有方向性。

**基本单位：**%

**计算公式：15分钟为一个采集周期，对于N个采集周期，**

发方向带宽利用率均值=（发方向带宽利用率1+发方向带宽利用率2+…+发方向带宽利用率N-1+发方向带宽利用率N）/ N

收方向带宽利用率均值=（收方向带宽利用率1+收方向带宽利用率2+收方向带宽利用率3+…+收方向带宽利用率N）/ N

带宽利用率均值=MAX（发方向带宽利用率均值，收方向带宽利用率均值）

**说明：**以15分钟为采集周期为例，持续采集N个采集周期，可以得到N个带宽利用率，对N个带宽利用率取平均值，即为N\*15分钟的带宽利用率均值。对于日均值，则N=4\*24=96个；对于7天均值，则N=7\*96=672。

#### 端口、LSP/SR-TP或PW的带宽利用率忙时均值

**定义：**该监测对象在某一监测时长（如：日或周）内忙时时段内所有N个采集周期的带宽利用率平均值，具有方向性。

**基本单位：**%

**计算公式：假设忙时时段共有N个采集周期，**

发方向带宽利用率忙时均值=（发方向带宽利用率1+发方向带宽利用率2+…+发方向带宽利用率N-1+发方向带宽利用率N）/ N

收方向带宽利用率忙时均值=（收方向带宽利用率1+收方向带宽利用率2+收方向带宽利用率3+…+收方向带宽利用率n）/ n

带宽利用率均值=MAX（发方向带宽利用率均值，收方向带宽利用率均值）

**说明：与忙时时段的取值方法相关**。

#### 端口、LSP/SR-TP或PW的带宽利用率峰值

**定义：**N个采集周期的带宽利用率的最大值，具有方向性。

**基本单位：**%

**计算公式：**

收方向带宽利用率峰值= MAX（收方向带宽利用率1，收方向带宽利用率2，…，收方向带宽利用率N-1，收方向带宽利用率N）

发方向带宽利用率峰值= MAX（发方向带宽利用率1，发方向带宽利用率2，…，发方向带宽利用率N-1，发方向带宽利用率N）

带宽利用率峰值= MAX（收方向带宽利用率峰值，发方向带宽利用率峰值）

**说明：**以15分钟为采集周期为例，持续采集60分钟，可以得到4个带宽利用率， 4个带宽利用率的最大值，即为（60分钟）带宽利用率峰值。

#### 端口、LSP/SR-TP或PW的带宽繁忙度

**定义：**在N个采集周期内，被监测对象的带宽利用率峰值超过阈值门限的次数占总采集次数的百分比，具有方向性。

**基本单位：**%

**计算公式：**

带宽繁忙度=（N个采集周期内带宽利用率峰值超过阈值门限的次数/总采集次数N）\*100%

**说明：**流量采集周期设置为15分钟，持续采集60分钟，则N=4，假设4个带宽利用率峰值分别为33%、50%、55%、43%，设定阈值门限为45%，则（60分钟）繁忙度为2/4=50%，指标范围0~1。

#### 线路端口配置的保证带宽占比

**定义：**配置在网络侧线路端口（NNI）上的所有LSP保证带宽总和（包括保护LSP关联的所有业务的保证带宽）与线路端口可用物理带宽的比值。

**基本单位：**%

**计算公式：**

线路端口的保证带宽占比=（该端口已配置的所有LSP保证带宽之和）/（线路端口物理带宽-带内网管DCN带宽）

**说明：**

1. 对于PW和LSP一一对应的场景，通过LSP保证带宽之和来计算和校验物理端口的保证带宽；对于PW和LSP 是N：1的对应关系，需要PTN网管支持自动计算N个PW保证带宽之和来设置LSP的保证带宽，并支持计算多个LSP保证带宽之和与物理端口带宽进行校验。
2. “保证带宽占比”越大，说明网络资源利用率越高，但是出现拥塞的概率也越大；“保证带宽占比”越小，说明网络资源利用率越低，出现拥塞的概率也越小。计算线路端口已配置的保证带宽之和，应考虑发生保护倒换的情况，需要将经过该端口的保护LSP所承载的业务保证带宽计算在内，例如：某端口承载了2条LSP，一条是工作LSP 1，另一条是保护LSP2，工作LSP1承载了以太网业务A，其保证带宽配置为10Mbit/s；保护LSP2对应另一个端口配置的工作LSP2，承载了以太网业务B，其保证带宽配置为5Mbit/s，则该端口已配置保证带宽为10Mbit/s + 5Mbit/s = 15Mbit/s。
3. 由于LSP保证带宽配置考虑了LSP的OAM带宽，因此端口的实际可用带宽应为端口物理带宽减去该端口内配置的带内DCN带宽。对于已升级并启用G.8113.1（即GACh+Y.1731）OAM的PTN设备，LSP的CC报文长度通常为101字节，周期为3.33ms对应每秒300个报文，所有LSP的OAM带宽=已配置的LSP总数N\*（101\*8\*300）/1000000=N\*0.2424（单位：Mbit/s）
4. PTN线路端口配置的带内网管DCN通道，一般带宽配置为2M或10M，需根据实际配置值进行计算。

#### 线路端口配置的保证带宽利用率

**定义：**某线路端口的忙时平均流速与该端口所配置的所有LSP保证带宽之和的比值，具有方向性。保证带宽利用率可分为不同时段（总监测周期、忙时、闲时）的均值利用率。

**基本单位：**%

**计算公式：**

端口的保证带宽利用率日均值=总监测周期的端口日平均流速/（端口内已配置的所有LSP的保证带宽之和+带内网管DCN配置保证带宽）

端口发方向的忙时保证带宽利用率日均值=总监测周期的端口日发送平均流速/（端口内所有LSP保证带宽配置值之和+带内网管DCN配置保证带宽）

端口收方向保证带宽利用率日均值=总监测周期的端口日接收平均流速/（端口内所有LSP保证带宽配置值之和+带内网管DCN配置保证带宽）

端口保证带宽利用率忙时均值=端口的忙时平均流速/（端口内所有LSP保证带宽配置值之和+带内网管DCN配置保证带宽）

**说明：**“端口保证带宽利用率”反映端口对其所分配的网络资源的实际使用情况。

#### 业务（PW）配置的保证带宽利用率

**定义：**单个业务（PW）的平均流速与该业务（PW）个体所配置的保证带宽的比值，具有方向性。保证带宽利用率可分为不同时段（总监测周期和忙时）的均值利用率。

**基本单位：**%

**计算公式：**

业务保证带宽利用率日均值=总监测周期的PW日平均流速/PW的保证带宽配置值

发方向保证带宽利用率日均值=总监测周期的PW发送日平均流速/PW的保证带宽配置值

收方向保证带宽利用率日均值=总监测周期的PW接收日平均流速/PW的保证带宽配置值

业务保证带宽利用率的忙时均值=PW的忙时平均流速/PW的保证带宽配置值

**说明：**“业务保证带宽利用率”反映业务个体对其所分配的网络资源的实际使用情况。

#### 传输环路的流量

传输环是“端口”或“链路”的组合，其流量指标定义有别于“端口”、“链路”和“业务”等流量监测对象，从系统的角度进行定义，不需要区分方向。

**定义：**该传输环路与上层网络互连的出环节点的线路端口的流量，有方向性。

环路流量监测需区分单归节点和双归节点两种网络模型，具体见图11-3。对于图11-3（1）的单归节点组网模型，汇聚环路的流量监测点是带该汇聚环的核心节点在该汇聚环路上的东西向线路端口；对于图11-3（2）的双归节点组网模型，汇聚环路的流量监测点是双归的核心节点A和核心节点B在该汇聚环路的东西向线路端口。



图10-2传输环路的流量监测点

**基本单位：**兆比特（Mbit）。

**计算公式：**采集周期为15分钟时

**环路收流量** =（线路端口1的接收字节数+20\*帧数+线路端口2的接收字节数+20\*帧数）\*8bit/1000000

**环路发流量** =（线路端口1的发送字节数+20\*帧数+线路端口2的发送字节数+20\*帧数）\*8bit/1000000

**环路总流量**=环路收流量+环路发流量

**说明：**以一个由3个网元组成的10GE汇聚环为例，整个汇聚环共有6个组环端口，每个端口均有“发流量”和“收流量”两个指标数值，传输环路流量是指该汇聚环连接核心环的出环节点的组环端口的流量。

若出环节点的数量多于两个，则参照上述公式进行累加。

#### 传输环路的流速

**定义：**在单位时间内，经过传输环路出环节点的线路端口所传输的数据量，具有方向性。

**基本单位：**兆比特/秒（Mbit/s）。

**计算公式：以15分钟采集周期为例，**

**环路收流速=**15分钟的环路收流量/（15\*60）

**环路发流速=**15分钟的环路发流量/（15\*60）

**环路流速=** MAX（环路收流速，环路发流速）

**说明：**“流速”是一个瞬时值，一般情况下，其数值随时间变化而上下波动。

#### 传输环路的峰值流速

**定义：**在N个采集周期内，传输环路出环节点的线路端口的最大流速，具有方向性。

**基本单位：**兆比特/秒（Mbit/s）。

**计算公式：以15分钟采集周期为例，对于N个采集周期，**

**环路收峰值流速=** MAX（环路收流速1, 环路收流速2,…, 环路收流速N-1, 环路收流速N）

**环路发峰值流速=** MAX（环路发流速1, 环路发流速2,…, 环路发流速N-1, 环路发流速N）

**环路峰值流速=** MAX（环路收峰值流速，环路发峰值流速）

#### 传输环路的忙时平均流速

**定义：**将某一监测时长（如1天或1周7天）内所采集的传输环路流速点绘制成流速分布曲线，将忙时时段内的所有采集点的传输环路的流速平均值作为忙时平均流速，具有方向性。

**基本单位：**兆比特/秒（Mbit/s）。

**计算公式：以15分钟采集周期为例，假设忙时内有M个采集点。**

**环路忙时平均收流速=**（环路忙时收流速1+环路忙时收流速2+…+环路忙时收流速M-1+环路忙时收流速M）/M

**环路忙时平均发流速=**（环路忙时发流速1+环路忙时发流速2+…+环路忙时发流速M-1+环路忙时发流速M）/M

**环路忙时平均流速=** MAX（环路忙时收流速，环路忙时发流速）

#### 传输环路的带宽利用率

**定义：**该传输环路与上层网络互连的出环节点的线路端口的带宽利用率，有方向性。

**基本单位：**%

**计算公式：**采集周期为15分钟时，

**环路收方向带宽利用率** =环路收流速/环路最大物理带宽

**环路发方向带宽利用率** =环路发流速/环路最大物理带宽

**环路带宽利用率** =MAX（环路收流速，环路发流速）/环路最大环路物理带宽

**说明：**以一个由3个网元组成的10GE汇聚环为例，整个汇聚环共有6个组环端口，每个端口均有“发带宽利用率”和“收带宽利用率”两个指标数值，传输环路带宽利用率是指该汇聚环连接核心环的出环节点的组环端口的带宽利用率。带宽利用率是考虑全部配置网络保护时的组网场景。

#### 传输环路的带宽利用率均值

**定义：**出环节点的传输环路端口（线路侧端口）N个采集周期的带宽利用率平均值，有方向性。

**基本单位**：%

**计算公式：对于N个采集周期，**

**环路收方向带宽利用率均值** =（环路收方向带宽利用率1+环路收方向带宽利用率2+…+环路收方向带宽利用率N-1+环路收方向带宽利用率N）/N

**环路发方向带宽利用率均值** =（环路发方向带宽利用率1+环路发方向带宽利用率2+…+环路发方向带宽利用率N-1+环路发方向带宽利用率N）/ N

**环路带宽利用率均值** =MAX（环路收方向带宽利用率均值，环路发方向带宽利用率均值）

#### 传输环路的带宽利用率忙时均值

**定义：**传输环路在某一监测时长（如：日或周）的忙时时段内所有N个采集周期的带宽利用率平均值，有方向性。

**基本单位**：%

**计算公式：对于忙时时段的N个采集周期，**

**环路收方向带宽利用率均值** =（环路收方向带宽利用率1+环路收方向带宽利用率2+…+环路收方向带宽利用率N-1+环路收方向带宽利用率N）/N

**环路发方向带宽利用率均值** =（环路发方向带宽利用率1+环路发方向带宽利用率2+…+环路发方向带宽利用率N-1+环路发方向带宽利用率N）/ N

**环路带宽利用率均值** =MAX（环路收方向带宽利用率均值，环路发方向带宽利用率均值）

#### 传输环路的带宽利用率峰值

定义：出环节点的传输环路端口（线路侧端口）N个采集周期的带宽利用率的最大值，有方向性。

基本单位：%

**计算公式：对于N个采集周期，**

**环路收方向带宽利用率峰值** = MAX（环路收方向带宽利用率1，环路收方向带宽利用率2，…，环路收方向带宽利用率N-1，环路收方向带宽利用率N）

**环路发方向带宽利用率峰值** = MAX（环路发方向带宽利用率1，环路发方向带宽利用率2，…，环路发方向带宽利用率N-1，环路发方向带宽利用率N）

**环路带宽利用率峰值** = MAX（环路收方向带宽利用率峰值，环路发方向带宽利用率峰值）

#### 传输环路的带宽繁忙度

**定义：**在N个采集周期内，传输环路的带宽利用率峰值超过阈值门限的次数占总采集次数的百分比，具有方向性。

**基本单位：**%

**计算公式：**

带宽繁忙度=（N个采集周期内带宽利用率峰值超过阈值门限的次数/总采集次数N）\*100%

**说明：**流量采集周期设置为15分钟，持续采集60分钟，则N=4，假设4个带宽利用率峰值分别为33%、50%、55%、43%，设定阈值门限为45%，则（60分钟）繁忙度为2/4=50%，指标范围0~1。

#### 传输链路系统的流量

**定义：**某一传输链路系统的根节点带该链路的线路端口的流量，有方向性，参见图11-4。

**基本单位：**兆比特（Mbit）。

**计算公式：**采集周期为15分钟时

**链路收流量** =（端口总接收字节数+20\*帧数）\*8bit/1000000

**链路发流量** =（端口总发送字节数+20\*帧数）\*8bit/1000000

**链路总流量**=链路收流量+链路发流量



图10-3传输链路的流量监测点

#### 传输链路系统的流速

**定义：**在单位时间内，经过传输链路的根节点线路端口的数据量，具有方向性。

**基本单位：**兆比特/秒（Mbit/s）。

**计算公式：以15分钟采集周期为例，**

**链路收流速=**15分钟的收流量/（15\*60）

**链路发流速=**15分钟的发流量/（15\*60）

**链路流速=** MAX（链路收流速，链路发流速）

**说明：**“流速”是一个瞬时值，一般情况下，其数值随时间变化而上下波动。

#### 传输链路系统的峰值流速

**定义：**在N个采集周期内，传输链路根节点的线路端口的最大流速，具有方向性。

**基本单位：**兆比特/秒（Mbit/s）。

**计算公式：以15分钟采集周期为例，对于N个采集周期，**

**链路收峰值流速=** MAX（链路收流速1, 链路收流速2,…, 链路收流速N-1, 链路收流速N）

**链路发峰值流速=** MAX（链路发流速1, 链路发流速2,…, 链路发流速N-1, 链路发流速N）

**链路峰值流速=** MAX（链路收峰值流速，链路发峰值流速）

#### 传输链路系统的忙时平均流速

**定义：**将某一监测时长（如1天或1周7天）内所采集的传输链路根节点的流速点绘制成流速分布曲线，将忙时时段内的所有采集点的传输链路的流速平均值作为忙时平均流速，具有方向性。

**基本单位：**兆比特/秒（Mbit/s）。

**计算公式：以15分钟采集周期为例，假设忙时内有M个采集点。**

**链路的忙时平均收流速=**（链路忙时收流速1+链路忙时收流速2+…+链路忙时收流速M-1+链路忙时收流速M）/M

**链路的忙时平均发流速=**（链路忙时发流速1+链路忙时发流速2+…+链路忙时发流速M-1+链路忙时发流速M）/M

**链路的忙时平均流速=** MAX（链路忙时收流速，链路忙时发流速）

#### 传输链路系统的带宽利用率

**定义：**该传输链路的根节点的线路端口带宽利用率，有方向性。

**基本单位：**%

**计算公式：**采集周期为15分钟时，

**链路收方向带宽利用率** =链路收流速/物理带宽

**链路发方向带宽利用率** =链路发流速/物理带宽

**链路带宽利用率** =MAX（链路收流速，链路发流速）/链路物理带宽

#### 传输链路系统的带宽利用率均值

**定义：**该传输链路根节点的线路端口的N个采集周期带宽利用率的平均值，有方向性。

**基本单位**：%

**计算公式：对于N个采集周期，**

**链路收方向带宽利用率均值** =（链路收方向带宽利用率1+链路收方向带宽利用率2+…+链路收方向带宽利用率N-1+链路收方向带宽利用率N）/N

**链路发方向带宽利用率均值** =（链路发方向带宽利用率1+链路发方向带宽利用率2+…+链路发方向带宽利用率N-1+链路发方向带宽利用率N）/ N

**链路带宽利用率均值** =MAX（链路收方向带宽利用率均值，链路发方向带宽利用率均值）

#### 传输链路系统的带宽利用率忙时均值

**定义：**该传输链路根节点的线路端口在某一监测时长（如：日或周）忙时时段的所有N个采集周期带宽利用率的平均值，有方向性。

**基本单位**：%

**计算公式：对于忙时时段的N个采集周期，**

**链路收方向带宽利用率均值**=（链路收方向带宽利用率1+链路收方向带宽利用率2+…+链路收方向带宽利用率N-1+链路收方向带宽利用率N）/N

**链路发方向带宽利用率均值** =（链路发方向带宽利用率1+链路发方向带宽利用率2+…+链路发方向带宽利用率N-1+链路发方向带宽利用率N）/ N

**链路带宽利用率均值** =MAX（链路收方向带宽利用率均值，链路发方向带宽利用率均值）

#### 传输链路系统的带宽利用率峰值

定义：该传输链路根节点的线路端口的N个采集周期带宽利用率的最大值，有方向性。

基本单位：%

**计算公式：对于N个采集周期，**

**链路收方向带宽利用率峰值** = MAX（链路收方向带宽利用率1，链路收方向带宽利用率2，…，链路收方向带宽利用率N-1，链路收方向带宽利用率N）

**链路发方向带宽利用率峰值** = MAX（链路发方向带宽利用率1，链路发方向带宽利用率2，…，链路发方向带宽利用率N-1，链路发方向带宽利用率N）

**链路带宽利用率峰值** = MAX（链路收方向带宽利用率峰值，链路发方向带宽利用率峰值）

#### 传输链路系统的带宽繁忙度

**定义：**在N个采集周期内，传输链路的带宽利用率峰值超过阈值门限的次数占总采集次数的百分比，具有方向性。

**基本单位：**%

**计算公式：**

带宽繁忙度=（N个采集周期内带宽利用率峰值超过阈值门限的次数/总采集次数N）\*100%

**说明：**流量采集周期设置为15分钟，持续采集60分钟，则N=4，假设4个带宽利用率峰值分别为33%、50%、55%、43%，设定阈值门限为45%，则（60分钟）繁忙度为2/4=50%，指标范围0~1。

#### 业务总流量

**定义：**在一个时间段内，PTN/SPN网络接入的所有PW的发送和接收流量之和。（注：不加MPLS-TP标签封装的纯业务流量）；也可以根据业务分类，分别统计各类业务UI端口的发送流量之和。

**基本单位：**兆比特（Mbit）

**计算公式：假设全网各类业务对应有N条PW，某类业务有M条PW。**

**业务总流量** = SUM (PW1的发流量，PW2的发流量，…，PWN-1的发流量，PWN的发流量，PW1的收流量，PW2的收流量，…，PWN-1的收流量，PWN的收流量)

**某类业务的总流量** = SUM (某类业务PW1的发流量，某类业务PW2的发流量，…，某类业务PWM-1的发流量，某类业务PWM的发流量，某类业务PW1的收流量，某类业务PW2的收流量，…，某类业务PWM-1的收流量，某类业务PWM的收流量)

#### 各类业务流量的占比

**定义：**在一个时间段内，PTN/SPN网络接入的各类业务流量占业务总流量的比例。

**基本单位：**百分比

**计算公式：假设全网共有N个PW，某类业务共有M个PW，**

**各类业务流量的占比** = 某类业务的总流量/业务总流量\*100%= SUM (某类业务PW1的发流量，某类业务PW2的发流量，…，某类业务PWM-1的发流量，某类业务PWM的发流量，某类业务PW1的收流量，某类业务PW2的收流量，…，某类业务PWM-1的收流量，某类业务PWM的收流量) /SUM (PW1的发流量，PW2的发流量，…，PWN-1的发流量，PWN的发流量，PW1的收流量，PW2的收流量，…，PWN-1的收流量，PWN的收流量)\*100%

#### L2PTN业务总流量

**定义：**所有业务落地的核心L2PTN节点的A类监测点UNI端口发送与接收流量之和，体现L2PTN/SPN网络实际承载的流量负荷。

**计算公式：针对所有业务落地的核心L2PTN节点，假设有N个监测点A端口**

**L2PTN/SPN网络业务发送总流量**=SUM (业务落地的核心PTN节点1的A端口的总发送流量，业务落地的核心PTN节点2的A端口的总发送流量，…，业务落地的核心PTN节点N-1的A端口的总发送流量，业务落地的核心PTN节点N的A端口的总发送流量)

L2PTN/SPN网络业务接收总流量-接收=SUM (业务落地的核心PTN节点1的A端口的总接收流量，业务落地的核心PTN节点2的A端口的总接收流量，…，业务落地的核心PTN节点N-1的端口A的总接收流量，业务落地的核心PTN节点N的A端口的总接收流量)

L2PTN/SPN网络业务总流量=L2PTN/SPN网络业务发送总流量+ L2PTN/SPN网络业务接收总流量

#### L3PTN业务总流量

**定义：**L3PTN/SPN网络内涉及业务落地的所有L3PTN节点的A类监测点 UNI端口发送与接收流量之和，体现L3PTN/SPN网络实际承载的流量负荷。

**计算公式：针对所有业务落地的核心L3PTN节点，假设有N个监测点A端口**

**L3PTN/SPN网络业务发送总流量**= SUM (业务落地的核心PTN节点1的A端口的总发送流量，业务落地的核心PTN节点2的A端口的总发送流量，…，业务落地的核心PTN节点N-1的A端口的总发送流量，业务落地的核心PTN节点N的A端口的总发送流量)

L3PTN/SPN网络业务接收总流量= SUM (业务落地的核心PTN节点1的A端口的总接收流量，业务落地的核心PTN节点2的A端口的总接收流量，…，业务落地的核心PTN节点N-1的A端口的总接收流量，业务落地的核心PTN节点N的A端口的总接收流量)

L3PTN/SPN网络业务总流量=L3PTN/SPN网络业务发送总流量+L3PTN/SPN网络业务接收总流量

## 流量基础数据表要求说明

“基础数据表”主要由监测对象、基础流量指标和流量分类信息组成。

“端口发送流量”和“端口接收流量”两项基础指标只能通过设备直接获取，其他大部分基础指标都可以通过“端口发送流量”和“端口接收流量”两项基础指标计算得到。

流量分类信息，用于对流量数据进行分类，如“端口类型”、“区域信息”和“业务类型信息”等。

表10-5 PTN流量“基础数据表”字段说明

|  |  |  |
| --- | --- | --- |
| **字段** | **获取方式** | **说明** |
| **PW名称** | OMC基础数据 | 开启流量监测的PW名称，通过PW名称来获取该PW的路径信息（包括源网元名称和宿网元名称）以及该PW承载的业务类型信息。  **PW名称的标识配置规则：** PW名称标识应便于识别三个属性信息，包括该PW的源网元名称（接入侧）、宿网元名称、该PW承载的业务信息。 |
| **业务类型信息** | OMC基础数据 | PW或UNI端口关联的业务分类信息；对于业务接入的UNI端口，业务信息才有意义。对于线路端口，不需要业务信息。  **业务信息的分类标识建议配置规则：**  （1）2G基站  （2）3G基站，站型子标签分类见表8  （3）LTE基站，站型子标签分类见表9  （4）集团客户（具体标识客户名称）  （5）WLAN回传  （6）OLT回传  （7）营业厅  应在业务类型信息中标注中各种基站的站型（如S111、S222、S333等）和基站名称，区分站型有利于分析不同站型的CIR好PIR，以及今后CIR和PIR的批量调整。  针对集客专线业务，还应标识集团客户的名称。 |
| **端口名称** | OMC基础数据 | 开启流量监测的端口名称，通过端口名称获取该端口所在网元名称（物理站点名称）和网元类型（是核心层、汇聚层或接入层的网元）。 |
| **端口类型** | OMC基础数据 | 分为网络侧线路端口（NNI）和用户侧接入端口（UNI）两大类 |
| **网元名称** | OMC基础数据 | 网元名称用于标识该网元所处的区域信息和物理机房、站点信息。 |
| **网元分类** | OMC基础数据 | 网元分类用于标识该网元所处的网络层次（如分为省干、城域核心层、汇聚层和接入层，对于跨两层的网元向上层归属）和传输系统信息（传输环路或传输链路的系统名称）。建议可根据业务自动识别。 |
| **采集时间** | OMC基础数据 | 采集周期的开始或结束时刻  支持用户配置采集时间，支持按需定制报表周期，小时报表、日报表、周报表和月报表。 |
| **发送流量（Mbit/s）** | 同步或网关网元直接获取 | 采集周期内，监测对象（PW或端口）发送的数据总量**（Mbit**）/采集周期的秒数（s） |
| **接收流量(Mbit/s)** | 同步或网关网元直接获取 | 采集周期内，监测对象（PW或端口）接收的数据总量**（Mbit**）/采集周期的秒数（s） |
| **发送流速（Mbit/s)** | 同步、网关网元直接获取或计算获取 | 等于“采集周期内端口发送的数据总量(Mbit)”/“采集周期（s）”。 |
| **接收流速（Mbit/s)** | 同步、网关网元直接获取或计算获取 | 等于“采集周期内端口接收的数据总量(Mbit)”/“采集周期（s）”。 |
| **发送带宽利用率(%)** | 计算获取 | 对于端口：等于“每秒发送流速（Mbit/s)”/“端口速率（Mbit/s)”  对于PW：等于“每秒发送流速（Mbit/s)”/“PW配置的保证带宽速率（Mbit/s)” |
| **接收带宽利用率(%)** | 计算获取 | 对于端口：等于“每秒接收流速（Mbit/s)”/“端口速率（Mbit/s)”  对于PW：等于“每秒接收流速（Mbit/s)”/“PW配置的保证带宽速率（Mbit/s)” |
| **端口速率（Mbit/s)** | 同步 | 物理端口的标称速率，例如GE端口对应1000Mbit/s,10GE端口对应10000Mbit/s。 |
| **PW/LSP配置的保证带宽（Mbit/s)** | 同步 | PW/LSP配置的保证带宽速率（CIR） |
| **PW/LSP配置的峰值带宽（Mbit/s)** | 同步 | PW/LSP配置的峰值带宽速率（PIR） |
| **区域信息** | OMC基础数据 | 标识网元所属的区域（如汇聚区或综合业务接入区名称），可根据PTN网管分域管理的设置方式，以及流量分区监测方案的需要来划分区域 |

## PTN/SPN网络流量监测与应用方案

PTN流量监测设置方案与流量监测应用方案选择需要结合不同的PTN组网应用方案，可参考附录1-PTN/SPN网络流量监测与应用方案。

### 流量监测点的设置方案

#### 汇聚接入层L2PTN+核心层L3PTN/SPN网络

PTN流量监测点的选择需要结合不同的PTN组网应用方案。对于TD-LTE移动回传网络，汇聚接入层采用二层PTN（L2 PTN）设备，核心层采用三层PTN（L3PTN）设备，组网拓扑如图1所示。根据流量监测需求，可在图3中选择A、B、C、D、E、F等作为流量监测点，分别开启对端口或者LSP、PW的流量监测。



图10-4 汇聚接入层L2PTN+核心层L3PTN/SPN网络的流量监测点选择

下表给出了汇聚接入层L2PTN+核心层L3PTN/SPN网络的流量监测点选择方案说明，包括监测点位置描述、监测对象和流量监测分析功能。

表10-6 汇聚接入层L2PTN+核心层L3PTN/SPN网络的流量监测点选择方案说明

|  |  |  |  |
| --- | --- | --- | --- |
| **流量监测点** | **监测点具体位置描述** | **监测对象** | **流量监测分析功能** |
| **A类** | 核心层L3PTN业务落地节点上联LTE核心网设备（S-GW、MME）的L3 IP端口 | UNI端口 | 监测TD-LTE的 S1-U（S-GW）和S1-C（MME）业务落地的总流量，用于分析业务流量 |
| **B类** | 核心层L3PTN设备和其它核心层L3PTN设备互联的线路端口 | 1）线路端口 | 1）监测L3PTN设备的线路端口流量，用于分析网络流量，计算线路带宽利用率和L3PTN核心层网络总流量等，并进行预警管理 |
| 2）LSP | 2）监测核心层某一个L2/L3桥接L3PTN设备到业务落地的L3 PTN设备的工作LSP总流量，用于分析网络流量（预警和查障）和业务流量（分析某一片区接入TD-LTE基站业务总流量） |
| **C类** | 汇聚PTN节点上联核心层L2/L3桥接PTN设备的L2线路端口 | 1）线路端口 | 1）监测某一汇聚片区上联到核心层L3PTN节点的流量，用于分析网络流量，计算某一汇聚片区的总流量和带宽利用率，并进行预警管理； |
| 2）LSP或PW | 2）监测某一接入节点接入PTN/SPN网络的流量，用于分析网络流量，如预警分析和查障 |
| **D类** | 某一个或一对核心或汇聚节点带汇聚环的两个线路端口 | 1）线路端口 | 1）监测某一汇聚环路的最大流量，用于分析网络流量，计算传输环路带宽利用率，并进行汇聚环的预警分析管理 |
| 2）LSP或PW | 2）监测某一接入节点接入PTN/SPN网络的流量，用于分析网络流量，如预警分析和查障 |
| **E类** | 某一个或一对汇聚节点带接入环的两个线路端口 | 1）线路端口 | 1）监测某一接入环路的最大流量，用于分析网络流量，计算传输环路带宽利用率，并进行接入环的预警分析管理 |
| 2）LSP或PW | 2）监测某一接入节点接入PTN/SPN网络的流量，用于分析网络流量，如预警分析和查障 |
| **F类** | 带接入链路的根节点的线路端口 | 1）线路端口 | 1）监测某一接入链路的最大流量，用于分析网络流量，计算传输链路带宽利用率，并进行接入链路的预警分析管理 |
| 2）LSP或PW | 2）监测某一接入节点接入PTN/SPN网络的流量，用于分析网络流量，如预警分析和查障 |
| **G类** | TD-LTE基站上联接入PTN设备的以太网端口 | UNI端口 | 监测每个LTE基站接入总流量，用于分析业务流量 |

#### 端到端L2PTN/SPN网络

承载2G/3G移动回传的PTN/SPN网络是端到端的L2PTN/SPN网络，其流量监测点选择建议见图2：



图10-5端到端L2PTN的流量监测点选择

表2给出了端到端L2PTN/SPN网络的流量监测点选择方案说明，包括监测点位置描述、监测对象和流量监测分析功能。

表10-7 端到端L2PTN/SPN网络的流量监测点选择方案说明

|  |  |  |  |
| --- | --- | --- | --- |
| **流量监测点** | **监测点具体位置描述** | **监测对象** | **流量监测分析功能** |
| **A类** | 核心层L2PTN业务落地设备上联2G BSC、3G RNC或其他业务网设备的端口 | UNI端口 | 监测2G、3G或某类业务落地的总流量，用于业务流量分析 |
| **B类** | 核心层L2PTN设备互连的线路端口 | 1）线路端口 | 1）监测核心层PTN/SPN网络流量，用于分析某一核心环或传输系统的总流量和带宽利用率，并进行预警管理； |
| 2）LSP或PW | 2）监测某一接入节点接入PTN/SPN网络的流量，用于网络流量的预警分析和查障 |
| **D类** | 某一个或一对核心或汇聚节点带汇聚环的两个线路端口 | 1）线路端口 | 1）监测某一汇聚环路的最大流量，用于分析网络流量，计算传输环路带宽利用率，并进行汇聚环的预警管理 |
| 2）LSP或PW | 2）监测某一接入节点接入PTN/SPN网络的流量，用于网络流量的预警分析和查障 |
| **E类** | 某一个或一对汇聚节点带接入环的两个线路端口 | 1）线路端口 | 1）监测某一接入环路的最大流量，用于分析网络流量，计算传输环路带宽利用率，并进行接入环的预警管理 |
| 2）LSP或PW | 2）监测某一接入节点接入PTN/SPN网络的流量，用于网络流量的预警分析和查障 |
| **F类** | 带接入链路的根节点的线路端口 | 1）线路端口 | 1）监测某一接入链路的最大流量，用于分析网络流量，计算传输链路带宽利用率，并进行接入链路的预警分析管理 |
| 2）LSP或PW | 2）监测某一接入节点接入PTN/SPN网络的流量，用于分析网络流量，如预警分析和查障 |
| **G类** | 2G、3G基站或集团客户设备上联接入PTN设备的以太网端口 | UNI端口 | 监测2G、3G基站或集团客户设备接入的总流量，用于业务流量分析 |

#### 端到端L3到边缘PTN/SPN网络

PTN流量监测点的选择需要结合不同的PTN组网应用方案。对于5G移动回传网络，采用L3到边缘（SR-TP）三层PTN设备，组网拓扑如图1所示。根据流量监测需求，可在图3中选择A、B、C、D、E、F等作为流量监测点，分别开启对端口或者SR-TP的流量监测。

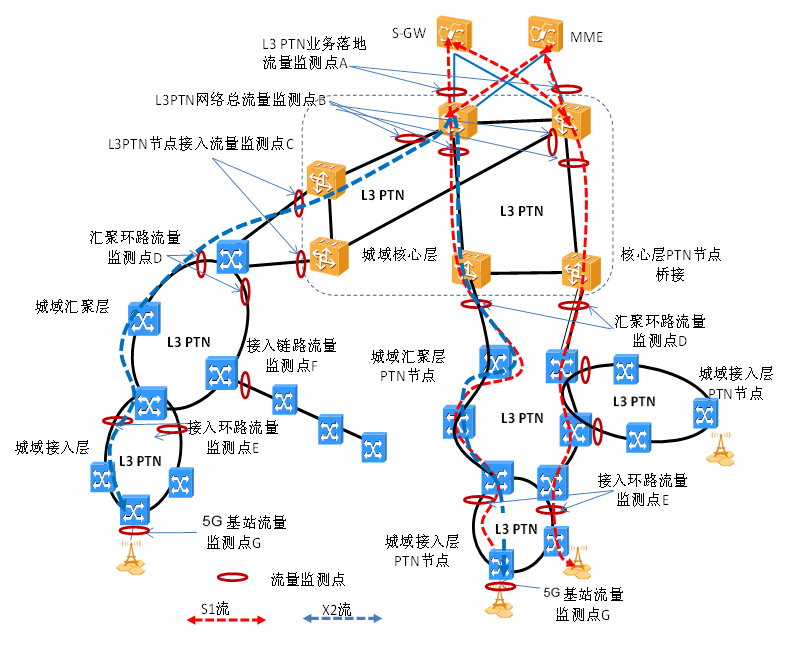


图10-6 L3到边缘5G移动回传网络的流量监测点选择

下表给出了L3到边缘5G移动回传网络的流量监测点选择方案说明，包括监测点位置描述、监测对象和流量监测分析功能。

表10-8 L3到边缘5G移动回传网络的流量监测点选择方案说明

|  |  |  |  |
| --- | --- | --- | --- |
| **流量监测点** | **监测点具体位置描述** | **监测对象** | **流量监测分析功能** |
| **A类** | 核心层L3PTN业务落地节点上联5G核心网设备（S-GW、MME）的L3 IP端口 | UNI端口 | 监测5G的 S1-U（S-GW）和S1-C（MME）业务落地的总流量，用于分析业务流量 |
| **B类** | 核心层L3PTN设备和其它核心层L3PTN设备互联的线路端口 | 1）线路端口 | 1）监测L3PTN设备的线路端口流量，用于分析网络流量，计算线路带宽利用率和L3PTN核心层网络总流量等，并进行预警管理 |
| 2）SR-TP | 2）监测核心层某一个桥接L3PTN设备到业务落地的L3 PTN设备的工作SR-TP总流量，用于分析网络流量（预警和查障）和业务流量（分析某一片区接入5G基站业务总流量） |
| **C类** | 汇聚PTN节点上联核心层桥接PTN设备的线路端口 | 1）线路端口 | 1）监测某一汇聚片区上联到核心层L3PTN节点的流量，用于分析网络流量，计算某一汇聚片区的总流量和带宽利用率，并进行预警管理； |
| 2）SR-TP | 2）监测某一接入节点接入PTN/SPN网络的流量，用于分析网络流量，如预警分析和查障 |
| **D类** | 某一个或一对核心或汇聚节点带汇聚环的两个线路端口 | 1）线路端口 | 1）监测某一汇聚环路的最大流量，用于分析网络流量，计算传输环路带宽利用率，并进行汇聚环的预警分析管理 |
| 2）SR-TP | 2）监测某一接入节点接入PTN/SPN网络的流量，用于分析网络流量，如预警分析和查障 |
| **E类** | 某一个或一对汇聚节点带接入环的两个线路端口 | 1）线路端口 | 1）监测某一接入环路的最大流量，用于分析网络流量，计算传输环路带宽利用率，并进行接入环的预警分析管理 |
| 2）SR-TP | 2）监测某一接入节点接入PTN/SPN网络的流量，用于分析网络流量，如预警分析和查障 |
| **F类** | 带接入链路的根节点的线路端口 | 1）线路端口 | 1）监测某一接入链路的最大流量，用于分析网络流量，计算传输链路带宽利用率，并进行接入链路的预警分析管理 |
| 2）SR-TP | 2）监测某一接入节点接入PTN/SPN网络的流量，用于分析网络流量，如预警分析和查障 |
| **G类** | 5G基站上联接入PTN设备的以太网端口 | UNI端口 | 监测每个5G基站接入总流量，用于分析业务流量 |

### 业务流量的监测应用方案

PTN/SPN网络承载了2G/3G/LTE基站回传、集团客户专线/专网业务、WLAN回传、PON OLT回传等各类业务，各省、地市公司应结合业务流量监测和管理分析的实际需求，开展各类业务流量的监测分析，表3给出了PTN/SPN网络开展各类业务流量监测的典型应用方案，供各省、地市公司参照执行。

表10-9 PTN/SPN网络监测各类业务流量的典型应用方案

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 监测业务类型 | 监测方案要求 | 流量监测对象 | | |
| 接入PTN设备的UNI端口（监测点G） | 核心PTN设备的业务落地UNI端口（监测点A） | UNI端口内不同优先级的业务流（监测点G） |
| 2G/3G基站（N\*E1） | 全部监测，或针对重要基站监测  采集周期：15分钟  监测时长：自定义（日、周、月、年等） | E1端口 | 通道化STM-1端口 | 不适用 |
| 3G IP化基站回传 | 全部监测，或针对重要基站监测  采集周期：15分钟  监测时长：自定义（日、周、月、年等） | FE端口 | GE端口 | G点监测所有PW流量 |
| LTE基站回传 | 全部监测  采集周期：15分钟  监测时长：自定义（日、周、月、年等） | GE端口 | 10GE端口 | G点监测所有PW流量 |
| 集团客户专线 | 全部监测  采集周期：15分钟  监测时长：自定义（日、周、月、年等） | FE/GE | FE/GE/10GE | G点监测所有PW流量 |
| 全部监测  采集周期：15分钟  监测时长：自定义（日、周、月、年等） | E1/STM-1 | E1/STM-1 | 不适用 |
| W-LAN回传 | 根据需求开启监测  采集周期：15分钟  监测时长：自定义（日、周、月、年等） | FE/GE | GE/10GE | 不监测 |
| OLT回传 | 根据需求开启监测  采集周期：15分钟  监测时长：自定义（日、周、月、年等） | GE/10GE | GE/10GE | 不监测 |
| 2.5G等 |

业务流量监测以PW为主，UNI端口流量可根据PW流量数据计算汇总，UNI端口监测按需打开，开启UNI端口和PW流量监测的原则：

对于基站类业务，一个UNI端口对应一个PW或一个LSP，建议仅开启PW层的流量监测；对于多个基站电路共享一个UNI端口以及重要基站的UNI端口，建议同时监测UNI端口和PW流量；

对于集团客户专线业务和多条业务在一个UNI端口的情况，同时开启UNI端口和PW层流量，监测UNI端口的峰值流量主要用于分析该端口是否需扩容；

对于PTN与业务网互通的UNI端口，以及不同PTN子网之间通过UNI端口互通的情况，需要监测UNI端口流量，用于指导预警扩容。

### 网络流量的监测应用方案

按照1.5.1节的流量监测点选择建议，对网络规模较大的地市，建议针对PTN不同网络层面的重要线路端口（如PTN核心层所有线路端口、计算传输环路和传输链路系统流量的线路端口等）、接入层所有PW、L3PTN核心层的所有LSP和部分UNI端口开启流量监测，根据流量管理需求对重要的LSP或PW实施流量监测；对网络规模较小的地市，可以针对所有PTN/SPN网络设备的所有线路端口、接入层所有PW和核心层L3PTN的所有LSP开启流量监测，根据流量管理需求对LSP或PW按需开启流量监测。

#### 汇聚接入层L2PTN+核心层L3PTN/SPN网络

对于汇聚接入层L2PTN+核心层L3PTN/SPN网络，典型的流量监测应用方案见下表：

表10-10汇聚接入层L2PTN+核心层L3PTN/SPN网络的流量监测典型应用方案

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 监测对象 | 核心层业务落地L3 PTN设备的线路端口  （图 4中监测点B） | 核心层L2/L3桥接L3PTN设备的线路端口（图 4中监测点C） | 核心节点带汇聚环的线路端口（图 4中监测点D） | 汇聚节点带接入环的线路端口（图 4中监测点E） | 带接入链的汇聚节点线路端口（图 4中监测点F） |
| 线路端口 | 全部选取，长期监测  采集周期：每15分钟 | 全部选取，长期监测  采集周期：每15分钟 | 全部选取，长期监测  采集周期：每15分钟 | 全部选取，长期监测  采集周期：15分钟 | 全部选取，长期监测  采集周期：15分钟 |
| 支持网管配置数据的统计上报：LSP数量、PW数量和承载业务类型 | 支持网管配置数据的统计上报：LSP数量、PW数量和承载业务类型 | 支持网管配置数据的统计上报：LSP数量、PW数量和承载业务类型 | 支持网管配置数据的统计上报：LSP数量、PW数量和承载业务类型 | 支持网管配置数据的统计上报：LSP数量、PW数量和承载业务类型 |
| LSP | 全部选取，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 |
| PW | 不适用 | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 |
| 注 | 为了进行L3PTN/SPN网络流量的预警管理和分析查障，所有LSP的流量必须监测。 | 1）对于L2PTN中PW和LSP为1:1复用情况，建议重点针对产生预警或接近预警门限的线路端口监测LSP；  2）对于L2PTN中PW和LSP为N:1复用情况，建议重点针对产生预警或接近预警门限的的线路端口监测LSP和PW。 | | | |

#### 端到端L2PTN/SPN网络

对于端到端L2PTN/SPN网络，典型的流量监测应用方案见下表：

表10-11端到端L2PTN/SPN网络的流量监测典型应用方案

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 流量监测对象 | 核心层业务落地PTN节点的两个线路端口  （图 5中的监测点B） | 核心节点带汇聚环的两个线路端口  （图 5中的监测点D） | 汇聚节点带接入环的两个线路端口  （图 5中的监测点E） | 带接入链的汇聚节点线路端口（图 4中监测点F） |
| 线路端口 | 全部选取，长期监测  采集周期：每15分钟 | 全部选取，长期监测  采集周期：每15分钟 | 全部选取，长期监测  采集周期：15分钟 | 全部选取，长期监测  采集周期：15分钟 |
| 支持网管配置数据统计上报：LSP数量、PW数量和承载业务类型 | 支持网管配置数据统计上报：LSP数量、PW数量 | 支持网管配置数据的统计上报：LSP数量、PW数量和承载业务类型 | 支持网管配置数据的统计上报：LSP数量、PW数量和承载业务类型 |
| LSP | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 |
| PW | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 | 按需选取注，长期监测  采集周期：15分钟 |
| 注 | 1）对于L2PTN中PW和LSP为1:1复用情况，建议重点针对产生预警或接近预警门限的线路端口监测LSP；  2）对于L2PTN中PW和LSP为N:1复用情况，建议重点针对产生预警或接近预警门限的的线路端口监测LSP和PW。 | | | |