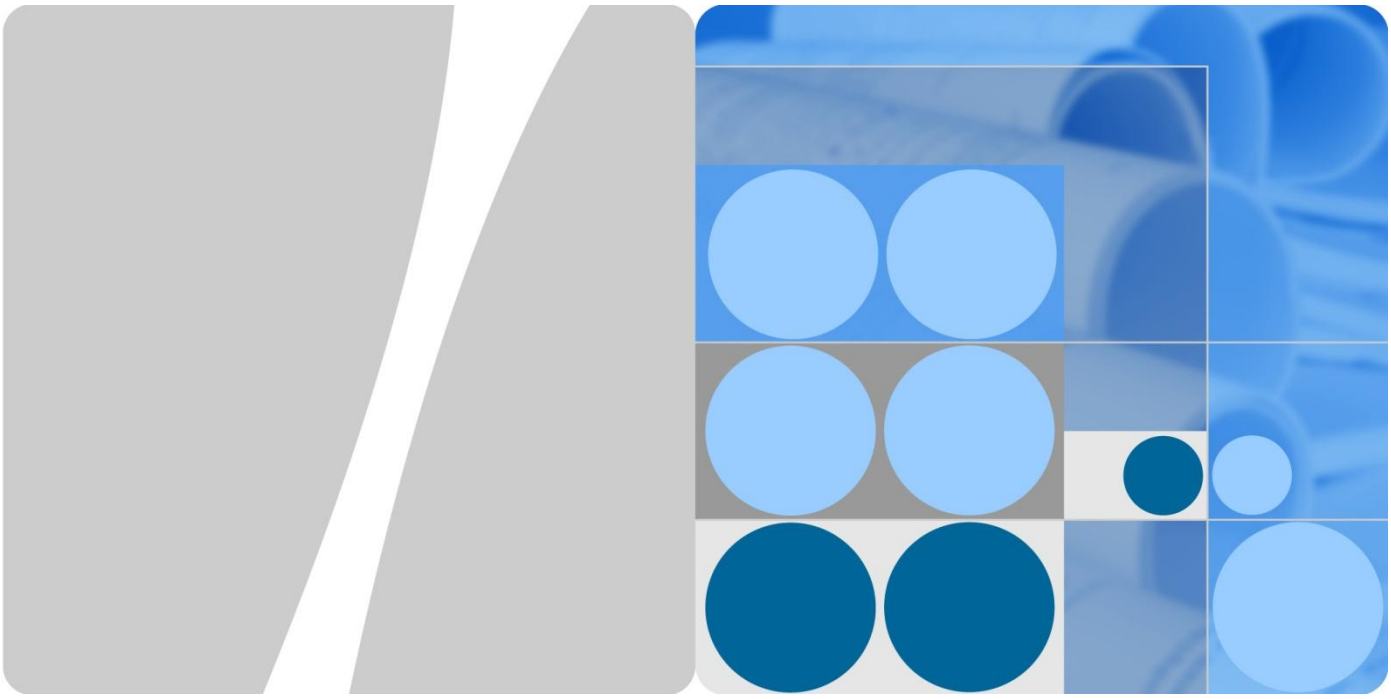
资料编码



One Net Campus 应急指挥基础网络解决方案 V100R001C03

技术建议书

文档版本 01

发布日期 2012-09-29

华为技术有限公司

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

目 录

1 应急指挥基础网络解决方案概述

1.1 应急指挥解决方案背景

应急指挥是指在紧急情况下，运用正确的指挥，充分发挥有限的应急力量，控制事态发展，减少损失、保护公众。顾名思义，应急指挥可以分为两个方面：一方面是应急，要求能够在任何时间、任何地点迅速部署指挥通信系统；另一方面是指挥，要求所构建的通信系统可以提供稳定、灵活的通信手段，在指挥中心与事件现场之间实时交互语音、数据、视频等信息，保证指挥人员远程就能全面的了解事件现场状况、掌握势态发展，从而作出准确的判断和指挥调度。

我国经济平稳较快增长，人民生活水平不断提高，社会政治和治安大局保持稳定。但是社会公共安全形势依然严峻、任重道远。

- 公共安全形势总体稳定、趋于好转，但依然严峻、任重道远

  年均死亡 1 万多人（近年年均 2500 人，伤病 100 万人）；

  每年有 3 亿人口受灾；

  年均损失 2000 亿元；

  年均倒塌房屋 300 多万间。

- 我国的事故灾难严重

事故总量大、伤亡大；重特大事故多；我国环境安全形势严峻；发达国家上百年工业化过程中分阶段出现的环境问题，在中国近 20 多年来集中凸现，呈现结构型、复合型、压缩型的特点。

- 公共卫生事件仍然威胁着人民群众的生命和健康

多种传染病尚未得到有效的遏制。全球新发现的 30 余种传染病已有半数在我国发现，有些还造成了严重后果（特别是非典疫情和高致病性禽流感疫情）。重大传染病和慢性病流行仍比较严重；职业病危害呈上升趋势；生产、销售假冒伪劣食品药品违法犯罪活动尚未得到有效遏制，食品药品安全事故多发。重大食物中毒事件每年 200 起以上，造成 200 多人死亡，数万群众健康受到伤害。

- 影响国家安全和社会稳定的因素依然存在

群死群伤的爆炸、投毒等恶性案件时有发生，杀人、绑架等暴力犯罪不断；社会安全形势严峻，违法犯罪活动日趋动态化、组织化、职业化、智能化、低龄化；由人民内部矛盾引发的群体性事件也明显增多；国内外极端势力制造的各种恐怖事件危及国家安全。

综上所述，自然灾害、事故灾难、公共卫生和社会安全等突发事件每年造成非正常死亡超过 20 万人，伤残超过 200 万人，经济损失超过 6000 亿人民币。公共安全形势严峻。

1.2 应急指挥业务网络需求

应急指挥业务系统如图 1-1 所示，主要包括预案管理、接警、决策、监控、移动指挥、视频会商、指挥调度、信息发布、善后处理及其它业务，业务繁多而且复杂。

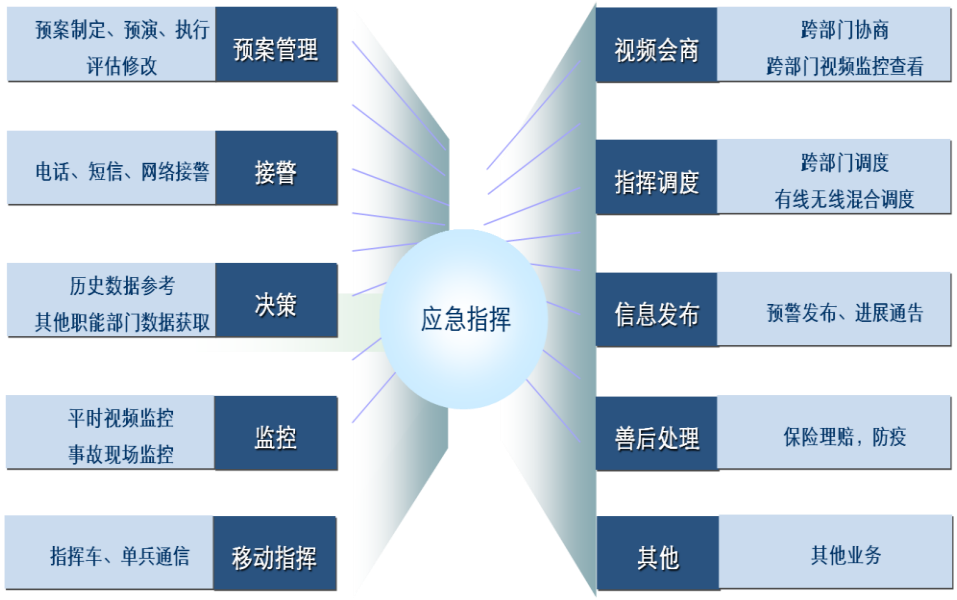


图 1-1 应急指挥业务总览

从业务类型考虑，主要涉及语音业务、视频业务及一般数据业务。每个类型业务都有自己的特点，数据业务特点是纵向隔离、横向共享、信息安全等，视频业务特点是稳定可靠、音视频同步、画质清晰等，语音业务主要特点是无时延、无抖动等，因此需要良好的网络质量保证，如图 1-2 所示，三种业务对于网络的可靠性、安全性（VPN 隔离）以及高效性（QoS 特性）等方面均提出了明确需求，在网络规划时需要重点考虑。

图 1-2 **应急指挥业务网络需求**

1.3 应急指挥业务流量模型

应急指挥体系按照应用范围分为国家级、省级、市级，各级之间存在跨城域的互访业务，具体如下：

- **各级行业部门垂直协作**

行业部门指挥中心监测到突发事件，行业部门指挥中心向上一级行业部门指挥中心汇报并接受指挥。

- **同级行业部门间协作**

行业部门监测到突发事件后向同级的相关部门请求协助。

- **政府指挥各行业部门**

行业部门监测到突发事件，行业部门上报同级的政府指挥中心，政府指挥中心上报给上一级政府，政府指挥中心协调指挥各行业部门。

从上述典型的业务流看，政府和各行业部门之间既有大量的数据互访需求，又有严格的数据安全隔离需求。数据互访和安全隔离是网络关注的重点问题之一。

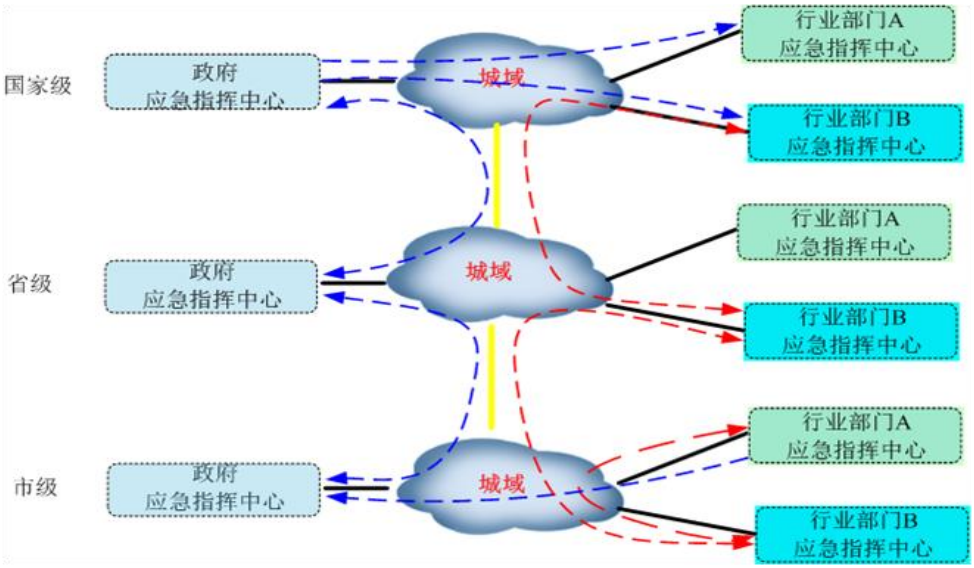


图 1-3 应急指挥体系流量模型

应急指挥中心是整个应急指挥系统的基础，是所有数据交互的枢纽。在跨部门、跨行业的复杂情况下，及时整合各类信息，对原始数据进行分析，辅助领导决策，保证整个体系的平稳运作。典型业务流如下：

- **接警中心**

接警中心统一接听和处理公众的报警和求助，接警中心为公众提供紧急特服号码，如：110、119、120 等。公众通过电话，短信，网站多种方式向接警系统求助。

- **视频监控**

提供可视化监控平台，实时呈现现场视频图像，方便行业部门及时了解现场情况，并采取进一步的措施。

- **协商决策**

上/下级指挥中心统一接入，了解分析事故现场状况，并通过公网接入进行视频协商，制定紧急处理预案，分配应急资源，启动应急行动。

- **指挥调度**

对下级指挥中心，行业指挥中心，事故现场进行统一指挥调度。

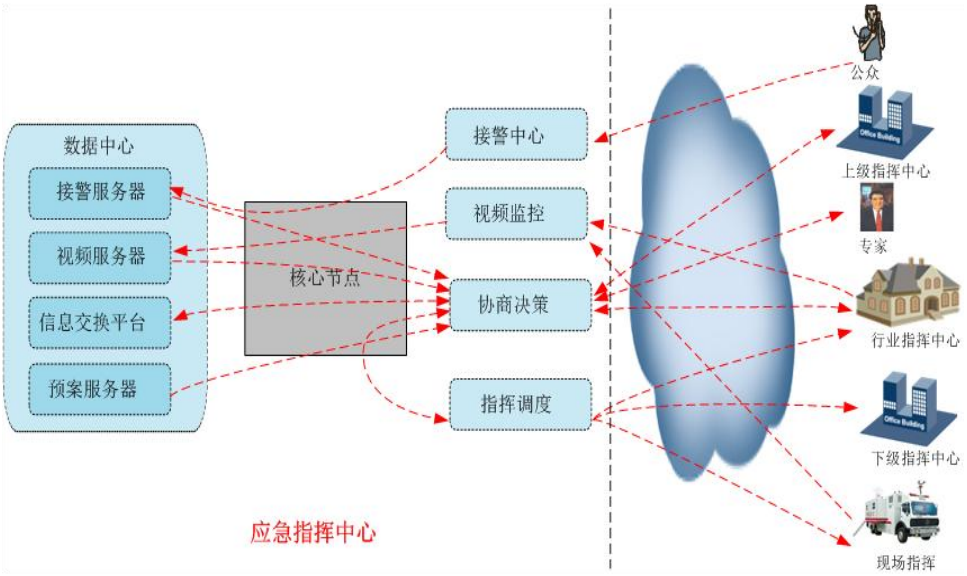


图 1-4 **应急指挥中心流量模型**

1.4 华为应急指挥基础网络解决方案

图 1-5 **解决方案整体框架**

华为应急指挥基础网络解决方案依托 IP 网络，建设智能、高效、可靠的应急指挥平台。系统以信息（数据）处理为核心，从基础架构建设、支撑业务设计、个性化应用定制等方面规划应急平台的建设，通过全方位的应急业务体系和流程，为国家的稳定和发展，人民的幸福和安康提供保障，创建和谐社会。

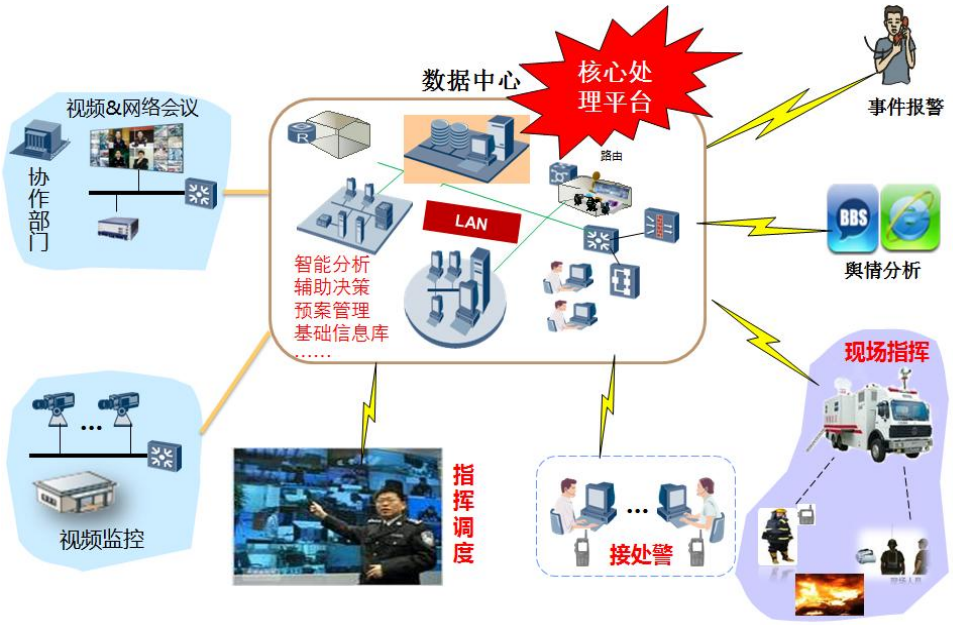


图 1-6 解决方案全景视图

华为应急指基础网络挥解决方案以信息（数据）为核心，包括视频监控系统、统一通信系统、指挥调度系统、现场指挥系统以及以数据中心为基础的核心处理平台。预测预警和快速处置是应急系统的关键能力，华为应急指挥平台通过视频监控、传感器、信息捕捉器等信息收集平台，将海量信息通过无线集群、IP 传输网络等将信息传递给核心处理平台，核心处理平台采用智能分析、模式识别等技术，对现场情况进行快速分析，识别风险，为现场处置提供辅助决策。

华为应急指挥基础网络解决方案亮点如下：

- **接入灵活**

多种网络接入方式，以太接入、Wlan 接入、3G 接入、微波接入、卫星接入等，可以根据需要选择，接入更具灵活性。

- **高安全性**

多种 VPN 技术，实现关键业务的安全隔离；全新一代万兆防火墙、IPS(或 IDS)数据安全，有效阻止外网攻击。

- **高可靠性**

多种备份方式，设备组件的备份、链路冗余、集群堆叠技术、多线路接入备份等，实现网络的高可靠性；丰富的路由协议，实现故障快速检测和及时恢复，充分保证应急指挥业务的不中断。

2 网络规划建议

2.1 组网规划

网络规划是应急指挥解决方案重要组成部分，按照应急指挥网络的地域规模分为广域网、城域网、局域网，根据不同地域规模将分别进行网络组网规划。

2.1.1 网络拓扑规划

应急指挥广域网组网方案如**错误！未找到引用源。**所示，广域网按照政府规模大小划分成多级骨干网，由骨干路由器组成，一级网络包括中央骨干网、中央城域网和中央级政务部门接入网。二级部门包括省级骨干网、省级城域网和省级政务部门接入网。三级网络包括地市级骨干网、地市级城域网和市级政务部门接入网。

大部分国家政府机构通常利用电子政务网络承载应急业务，部分国家电子政务网络区分内网（涉密）、外网（非涉密），如中国、美国，相应的应急网络也区分为内、外网。

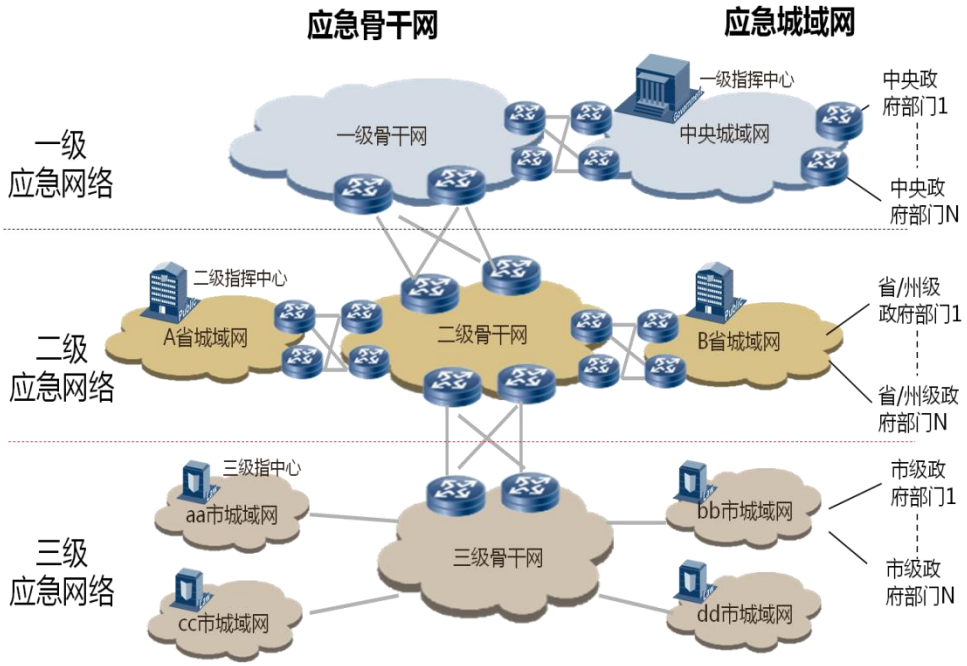


图 2-1 **应急指挥广域网组网方案**

应急指挥城域网组网方案如**错误！未找到引用源。**所示，城域网包括城域骨干网和接入网，其接入点分布范围比较广，通过多种方式接入骨干网，移动平台通过 3G 接入，各部门通过有线接入，偏远地区通过微波接入，卫星通信也应用到诸多场合。各行政部门数据流量汇聚到骨干网。

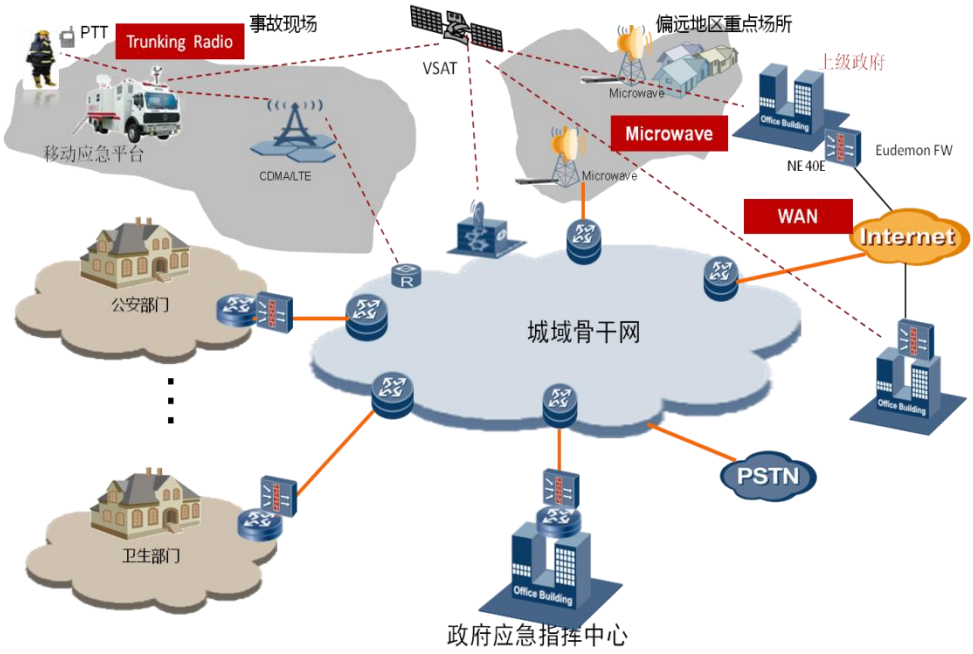


图 2-2 **应急指挥城域网组网方案**

应急指挥局域网组网方案如**错误！未找到引用源。**所示，局域网分为接入层、汇聚层和核心层，内部部署交换机星型组网，局域网出口部署路由器，同时部署防火墙保护内部数据安全。出口通过 WAN 网或者 Internet 与外部网络相连。外部接入方式丰富，包括 3G 接入、微波接入、有线接入等。

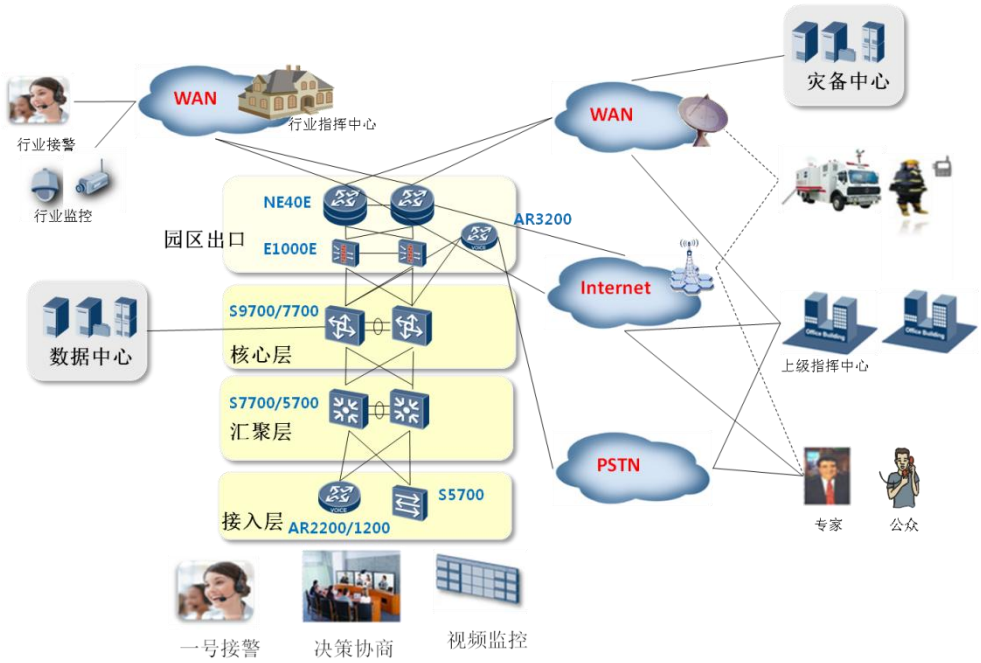


图 2-3 **应急指挥局域网组网方案**

应急指挥行业部门组网方案如**错误！未找到引用源。**所示（以警察网举例），对于建设专用网络的行业部门，应急业务由部门专网承载；大部分行业部门专用网络租用运营商线路作为传输，军用/警用网络通常自建。

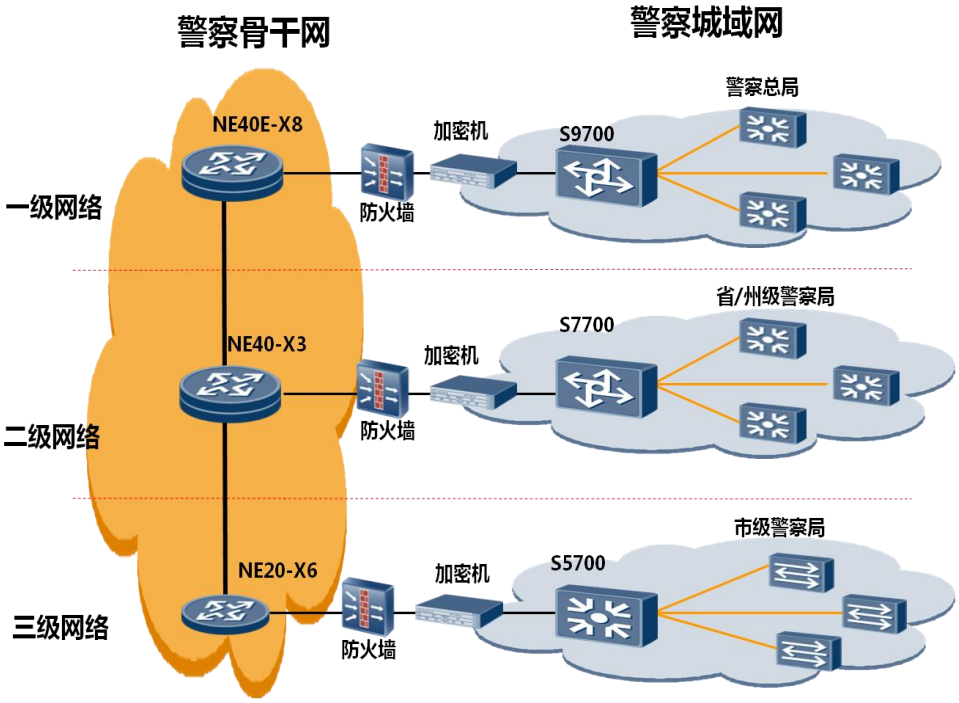


图 2-4 **应急指挥行业部门组网方案**

2.1.2 接入规划

不同部门的自身网络需求不同，采用的接入方式也不同。需要根据具体情况进行选择，接入线路既可以采用租用运营商线路，也可以采取自建方式。

其中，租用运营商线路包括：

专线：SDH/MSTP、ADSL/HDSL、 3G VPDN

互联网线路：ADSL、xPON、3G、WiFi

自建线路适用于对安全性和网络质量要求比较高的用户，主要用于新建网络。

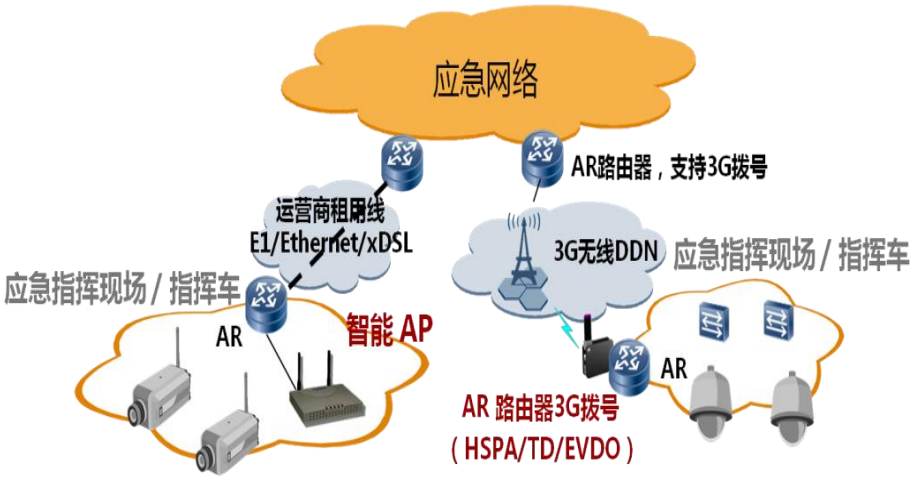


图 2-5 **应急指挥接入规划**

2.1.3 典型业务系统组网规划

- **视频会商**

极高的网络可靠性与会议安全性，支持 H.235 信令与媒体流加密技术，与 MCU、管理平台融合，提供端到端的全网全业务信令，保障会议安全可靠；

视讯和监控完美融合，视频会议和监控系统的全数字融合，提供更多信息辅助决策；

多级可视化调度指挥，多个指挥中心之间的“面对面”讨论和指挥，实现异地协同作战。

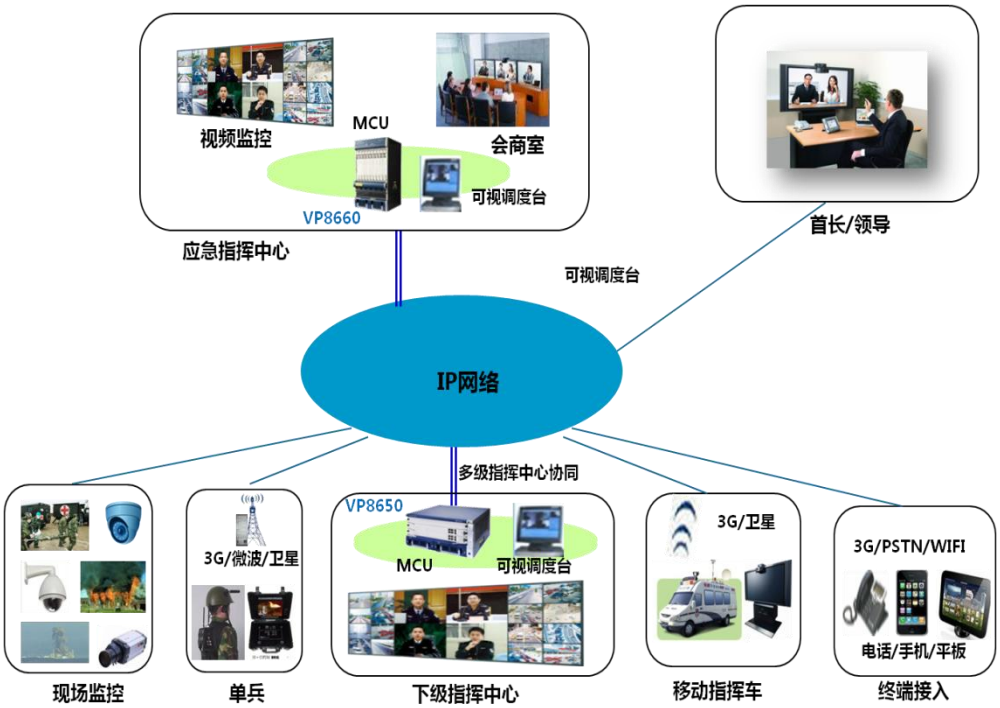


图 2-6 **视频会商组网规划**

- **视频监控**

城域骨干部署高性能路由器，承载整个城域视频业务；

高性能交换机组成汇聚层，之间通过 VPLS/VLL 等二层 VPN 技术建立互通；

接入层采用 LAN 接入为主，距离远的摄像头采用 xPON 方式，对于无法部署光纤的监控区域部署无线接入；

为了网络可靠性，可以组成自愈环网保护。

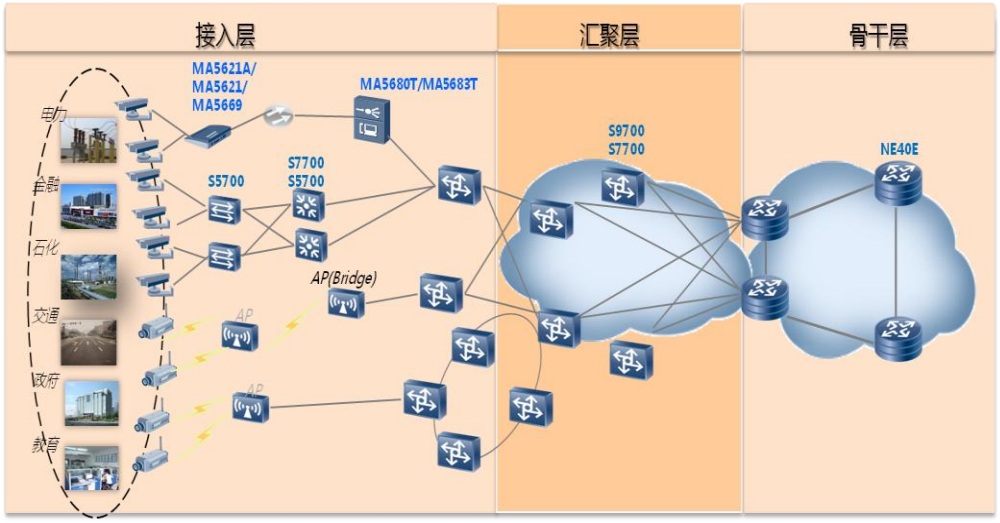


图 2-7 **视频监控组网规划**

2.2 VLAN 规划

VLAN 主要用于应急指挥网络接入部门局域网内部，将局域网内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个 LAN 内隔离广播域的技术。VLAN 技术既隔离了广播域，减少了广播风暴，又增强了信息的安全性。每个接入部门划分为一个 VLAN，互通的部门之间划分为一个 VLAN。网络结构简单，易于部署。

2.3 IP、DHCP、DNS 规划

2.3.1 IP、DHCP、DNS 概述

在应急指挥网络中，除于对网络资源的统一利用、避免重复建设，对于新建网络，可以统一进行 IP、DHCP、DNS 的规划；如果接入部门已经建有网络的话，可以在尽量沿用原有的 IP、DHCP、DNS 的规划基础之上，重新进行统一规划、整合有关网络资源。整合已有网络时，由于各接入部门局域网使用大量的私网地址，因此可能会存在 IP 地址冲突，需要重点考虑私网地址冲突的问题。

2.3.2 IP 地址规划

IP 地址规划的原则

- 唯一性

  一个 IP 网络中不能有两个主机采用相同的 IP 地址。即使使用了支持地址重叠的 MPLS/VPN 技术，也尽量不要规划为相同的地址。建议为每类接入单位分配一个独立的 C 网私有地址网段。

- 连续性

  连续地址在层次结构网络中易于进行路由聚合，大大缩减路由表，提高路由算法的效率。

- 扩展性

  地址分配在每一层次上都要留有余量，在网络规模扩展时能保证地址叠合所需的连续性。

- 实意性

  “望址生意”，好的 IP 地址规划使每个地址具有实际含义，看到一个地址就可以大致判断出该地址所属的设备。

IP 地址基本分类

- Loopback 地址

  为了方便管理，会为每一台路由器创建一个 Loopback 接口，并在该接口上单独指定一个 IP 地址作为管理地址。

  Loopback 地址务必使用 32 位掩码的地址。最后一位是奇数的表示路由器，是偶数的表示交换机，越是核心的设备，Loopback 地址越小。

- 互联地址

  互联地址是指两台网络设备相互连接的接口所需要的地址，互联地址务必使用 30 位掩码的地址。核心设备使用较小的一个地址，互联地址通常要聚合后发布，在规划时要充分考虑使用连续的可聚合地址。

- 业务地址

  业务地址是连接在以太网上的各种服务器、主机所使用的地址以及网关的地址。业务地址规划时所有的网关地址统一使用相同的末位数字，如：.254 都表示网关。

- 内部私有 IP 地址

  建议使用私网 IP 地址，在边缘网络通过 NAT 转换成公网地址后接入公网。

IP 地址规划

由于公网地址有限，推荐应急指挥网络内部采用 B 类私有地址（172.16.0.0～172.31.255.255），每个接入部门分配一个 C 类私有地址；应急指挥网络出口处统一进行 NAT 转换，将需要对外提供访问服务的内部私网地址转换成公网 IP 地址，以便对外提供服务。地址转换方法可以根据情况灵活选择静态转换、动态转换等方式。

2.3.3 DHCP 规划

为了减少运维工作量和难度，应急指挥网络中建议使用 DHCP，为接入部门自动分配 IP 地址。每个 DHCP 网段应保留部分静态 IP 供服务器等设备使用。

DHCP 部署基本架构

- 在应急指挥网络中统一的数据中心或服务器区部署独立的 DHCP Server。
- 在接入部门出口路由器或内部网关部署 DHCP Relay，指向 DHCP Server 统一分配地址。
- DHCP 一般通过 VLAN 分配地址，如有特殊要求，在接入交换机部属 Option82，由接入交换机提供的 Option82 信息分配地址。

DHCP 部署基本原则

- 固定 IP 地址段和动态分配 IP 地址段保持连续。
- 按照接入部门及其业务区域进行 DHCP 地址的划分，便于统一管理及问题定位。
- DHCP 需要跨网段获得 IP 地址时，启动 DHCP Relay 功能。
- 启动 DHCP 安全功能，禁止非法 DHCP Server 的架设和非法用户的接入。

2.3.4 DNS 规划

DNS 服务器的角色划分

- Master 服务器：主服务器

  作为 DNS 的管理服务器，可以增加、删除、修改域名，修改的信息可以同步到 Slave 服务器，一般部署 1 台。

- Slave 服务器：从服务器

  从 Master 服务器获取域名信息，采用多台服务器形成集群的方式，统一对外提供 DNS 服务，一般采用基于硬件的负载均衡器提供服务器集群的功能。一般部署 2 台从服务器。

- Cache 服务器：缓存服务器

  用于缓存内部用户的DNS请求结果，加快后续的访问。一般部署在Slave服务器上。

DNS 服务器的 IP 地址

- Master 服务器：采用应急指挥网络内网地址。
- Slave 服务器：分配私网地址，并可在负载均衡器上分配一个虚拟的内网地址。

Internet 域名地址有两种方案：

- 一种是在防火墙上做 NAT 映射，把 Slave 服务器的虚拟地址映射为一个公网 IP 地址，用于外部 Internet 用户的访问。
- 另一种是在链路负载均衡设备上通过智能 DNS 为外部 Internet 用户提供服务。

DNS 部署规划

由于接入部门众多，为便于使用和管理，可以在骨干网上统一部署 DNS 服务器。根据网络应用情况，既可以发布公共的 DNS 服务，也可以提供内网专用的 DNS 服务。

Master 服务器，建议放置在 DMZ 区域，并在同区内部建立 Slave DNS 服务器。如只对内提供服务的 DNS 服务器，可以作为二级的 DNS 服务器，放入其他非 DMZ 区域。

2.4 路由规划

2.4.1 路由概述

应急指挥网络拥有众多接入部门，部分部门已经建有自己的局域网，因此，应急指挥网络的路由规划主要考虑网络互联情况，主要包括两个方面：一方面是应急指挥网络上下级的路由规划，另一方面是应急指挥网络与其下辖的各接入部门之间的路由规划。

2.4.2 IGP 设计

应急指挥网络可以划分自治域 AS，在其内部采用 IGP 协议，实现 AS 域接入部门的内部互通互联。

IGP 协议选择

由于应急指挥网络内部可能存在不规则区域，且路由节点不是特别多，建议使用 OSPF 路由协议。骨干网和每个接入部门作为一个单独的 OSPF 区域。

OSPF 规划

- 规划合理的 RouteID

  RouteID 建议采用 Loopback 接口 IP 地址。

- OSPF 核心区域规划

  骨干网路由器作为 OSPF 的 Area0，作为 ASBR 和 ABR。每个接入部门与骨干路由器组网部署为不同的 OSPF Area ID1，2，…，N。

- OSPF 边缘区域规划

  每个接入部门的出口路由器或交换机与骨干路由器组网部署为不同的 OSPF Area ID1,2,…,N。Area1,2，…,N 使用 OSPF NSSA 区域。与原先的普通的完全 OSPF 区域相比，通过规划减少 LSA 在区域间的传播，减少路由条数；和纯 stub 区域相比部署路由协议更加灵活。另外可以通过区域汇总，限制区域间传播的 LSA 条目。

  边缘区域使用 NSSA 区域的优势在于：能精简骨干区域路由器的路由表；减少骨干区域内 OSPF 交互的信息量；提高路由表项的稳定性。一个区域的路由计算和网络调整不会影响其它区域，因故障引起的路由震荡被隔离在区域内部。

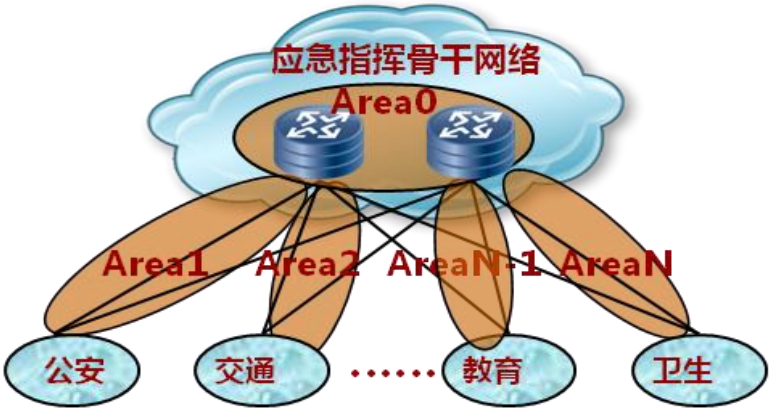


图 2-8 **应急指挥网络 OSPF 规划**

2.4.3 BGP 设计

使用 BGP 的场景

- 多 AS 互联场景

  应急指挥网络上下级连接时，可能属于不同的 AS，因此，需要使用 BGP 实现不同 AS 的互联互通。

- 使用路由策略场景

  由于业务需要，需要大量的使用路由策略，使用 OSPF 等协议不擅长，使用 BGP 可以方便的控制路由策略，来分配业务流向。

- 采用 MPLS VPN 场景

  部署 MPLS VPN 技术时，用于复杂的隔离策略等。

使用 BGP 的基本规划

- Routerid 的规划

  BGP 的 routerid 与 OSPF 的 routerid 共用一个，与 Loopback 接口地址相同。

- AS number 的规划

  由于应急指挥网络属于私有网络，所以 BGP 使用私有的 AS number。

- IBGP 和 EBGP 的选择

  由于要实现不同私有 AS 的互联，因此采用 EBGP。

BGP 对设备的要求

BGP 协议本身并不消耗很多资源，只有当运行 BGP 的设备需要学习到很多条路由，需要建立很多邻居关系时才会要求设备自身的性能很高。只要规划得当，任何设备（包括接入层设备）都可以运行 BGP 协议。

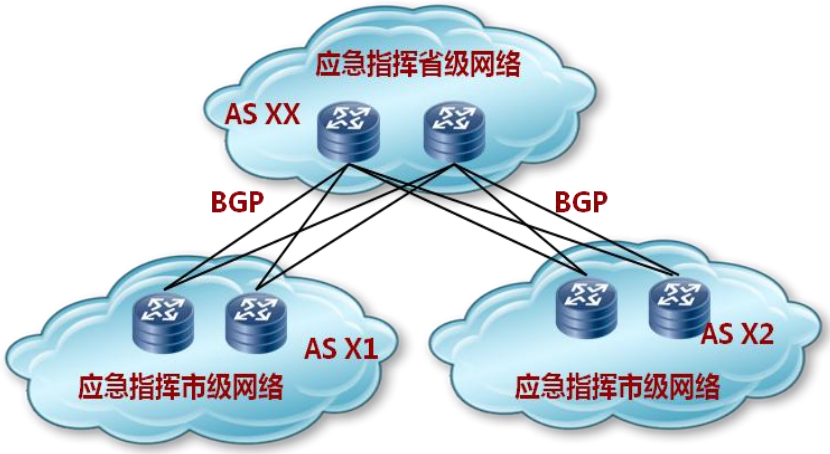


图 2-9 **应急指挥网络 BGP 规划**

2.5 MPLS 规划

在应急指挥网络中，使用 MPLS L3VPN 技术来实现网络的逻辑划分和隔离，因此必须在部署 VPN 的区域部署 MPLS。

MPLS 域规划

MPLS 域的范围由划分 VPN 的 PE 节点位置决定：

- 如果 PE 位置是在汇聚层，则 MPLS 域包含核心层设备和汇聚层设备。
- 如果 PE 位置是在核心层，则 MPLS 域只包含核心层设备。

MPLS 域中的每一台设备均需启用 MPLS 功能，LSR ID 建议设置为该设备的 Loopback0 接口的 IP 地址。

LSR ID 规划

使能 MPLS 的设备，需要配置 LSR ID。通常可以使用设备的某个 Loopback 地址作为 LSR ID（例如 Loopback0）。

LSP 规划

LSP 是每一个沿着从源端到终端的路径上的结点的标签序列。LSP 可以通过手动逐跳建立，也可以通过标签分发协议建立，如 LDP、RSVP 或者建于路由协议之上的一些协议，如 BGP 及 OSPF。

静态 LSP 的配置工作量巨大，扩展性不好，而且很容易引入人为操作错误，所以现在网络应用除非特殊情况，基本不会采用静态 LSP。

基于 RSVP 的 MPLS TE 隧道（CR-LSP）可以预留资源、保证带宽，同时可以提供高可靠性的保护措施。但是 RSVP-TE 对网络和设备的要求很高，一般运用在典型运营级的骨干网络之中。

LDP 会话规划

如果采用 LDP 协议来创建 LSP，则需要进行对 LDP 会话进行规划。

由于应急指挥网络需要通过 MPLS 网络进行通信，因此既需要建立本地 LDP 会话，也需要建立远端 LDP 会话，即需要同时支持基本发现机制和扩展发现机制。

2.6 VPN 规划

在应急指挥网络中，为了实现业务的隔离和安全，采用 VPN 技术进行安全隔离，将不同的业务进行纵向和横向隔离，保证在信息共享的基础上实现业务安全隔离。纵向虚拟化方案中，最基本的部署是通过 VPN 技术，将不同部门的终端、服务器、网络资源等划分到不同的 VPN 中，实现业务的安全隔离。企业网络中划分了 VPN 之后，还需要考虑 VPN 用户的对外访问、外部分支/用户等接入 VPN 网络等方面的问题。

2.6.1 VPN 概述

在应急指挥网络中，根据业务类型和范围将 VPN 分为两大类：纵向隔离 VPN、横向互通 VPN。

2.6.2 纵向隔离 VPN 规划

纵向隔离 VPN 主要是实现不同类型业务系统之间相互隔离，互相不能访问，即每种类型的业务只能访问自身垂直业务系统，不能访问其他业务系统。纵向隔离 VPN 规划如图 2-所示，其中三级城域网卫生系统可以与上级部门进行业务互通，但不能与其他业务系统（如教育）互通，这就是通过将卫生系统作为一个独立的 VPN 进行设置，卫生系统内部可以相互通信，但外部不能访问。其他业务也设置同样类型的纵向隔离 VPN，保证上下级业务系统的业务安全。

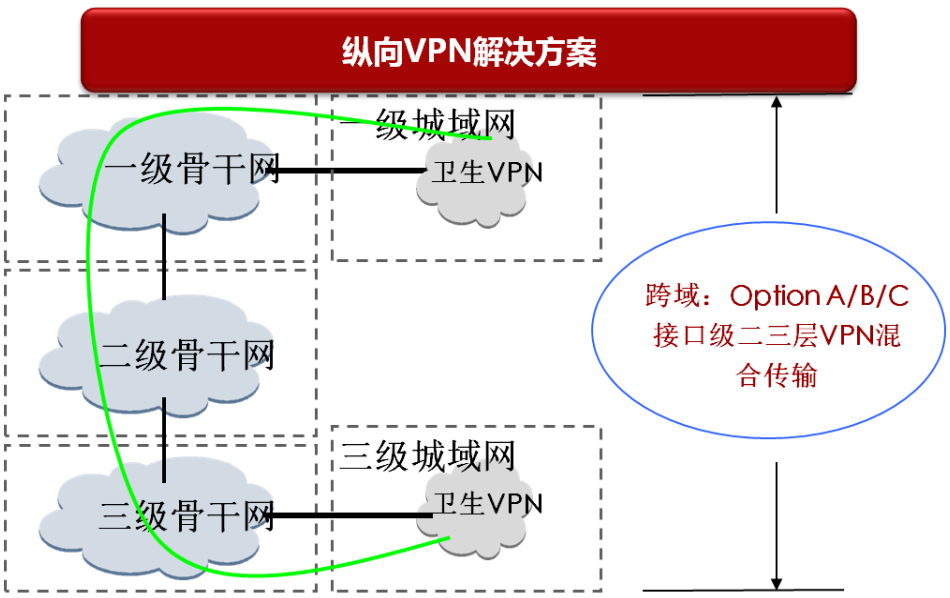


图 2-10 **应急指挥网络纵向隔离 VPN**

2.6.3 横向互通 VPN 规划

在应急指挥网络中，不同业务系统需要共享信息，如卫生和交通系统之间数据共享，需要提供不同业务系统之间的信息互通通道。对此，可以设置横向互通 VPN，允许指定的业务系统之间进行信息互通。

如图 2-所示，每级接入网由各接入单位和数据共享区组成，数据共享区位于独立 VPN，该 VPN 能够与所有接入单位 VPN 互通，各接入单位 VPN 之间隔离。 通过 MPLS RT 属性控制各接入单位和数据共享区的访问权限。

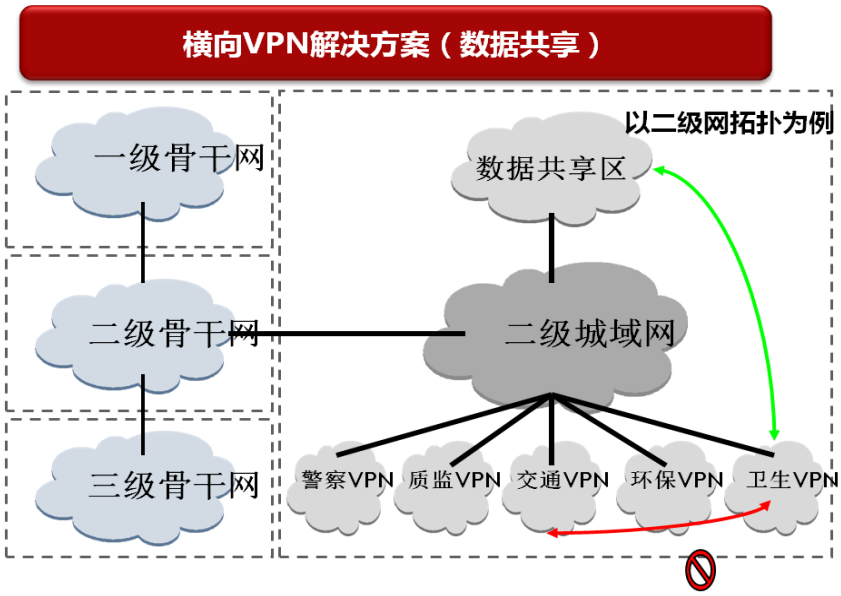


图 2-11 **应急指挥网络横向互通 VPN**

2.7 可靠性规划

2.7.1 可靠性概述

应急指挥网络接入部门众多，网络情况复杂，用户覆盖面非常广，业务体验效果要求比较高，因此，要求网络必须具有非常高的可靠性，对此，华为提供全方位的高可靠性解决方案，以丰富的可靠性技术提供端到端的质量保证。

可靠性是反映网络设备本身的稳定性以及网络保持业务不中断的能力，主要包括设备级可靠性、网络级可靠性和业务级可靠性三个层次。其中，业务级可靠性更多的是从业务管理的层面来要求的，要求业务不中断，有关内容与网络关联不大，此处不详述。

2.7.2 设备级可靠性规划

在应急指挥网络中，设备的可靠性是最关键的，减少设备故障才能保障电子政务的服务质量。网络设备级可靠性的技术很多，常用的有热插拔技术、冗余备份技术、不间断转发技术等，通过这些技术一方面可以提供组件的冗余备份，另一方面可以保证在设备出现故障时，即使控制层面出现故障，业务仍然能够不间断转发。

华为网络设备本身具有电信级 99.999%的可靠性，网络设备支持：

- 主控 1:1 备份
- 交换网 1+1/1:1 两种方式
- DC 电源 1+1 备份；AC 电源 1+1/2+2 备份
- 模块化的风扇设计，高端配置支持单风扇失效
- 无源背板，高可靠性
- 独立的设备监控单元，和主控解耦
- 所有模块支持热插拔
- 完善的告警功能
- 设备管理 1:1 备份

设备本身通过部件的冗余设计来保证高可靠性。对于路由器故障，一般通过网络协议感知故障点后进行动态调整，实现流量的快速切换，提高可靠性。交换机通过集群 CSS（Cluster Switch System）和堆叠 iStack 技术，能够把多台物理设备连接在一起，对外表现为一台逻辑设备，从功能和管理方面，都可以作为一台设备来看待。单节点物理设备的故障，逻辑设备能够快速感知，并快速将流量切换到 UP 状态的链路上，减少丢包时间，具有更高的可靠性。

2.7.3 网络级可靠性规划

在应急指挥网络中，网络的可靠性由双设备、链路冗余来保证。对于双设备、链路冗余的网络，采用三层路由的方式，通过等价路径再辅助部署 BFD（Bidirectional Forwarding Detection）快速检测故障，就能够保证链路故障、设备故障的快速切换，同时也能够充分利用冗余链路。网络根据需要部署以下可靠性技术：IP FRR、NSF/GR、BFD、MPLS OAM。

IP FRR

IP FRR（IP Fast Reroute）即 IP 快速重路由。IP FRR 是一种转发快速切换技术，当物理层或链路层检测到故障时无需等待路由收敛，立即开始采取措施，使用一条备份的链路将报文转发出去，从而将链路故障对承载业务的影响降低到最小限度。

NSF(GR)

NSF（None Stop Forwarding）是设备本身可靠性的一种，属于 GR（Graceful Restart）的一种形态。NSF 是指在路由器控制层面故障的过程中，数据转发不间断地正常执行。

通常情况下，路由器故障后，其路由协议层面的邻居会检测到它们之间的邻居关系 Down 掉，然后过段时间再次 UP，这个过程被称之为邻居关系震荡。这种邻居关系的震荡将最终导致路由震荡的出现，使得重启路由器在一段时间内出现路由黑洞或者导致邻居将数据业务从重启路由器处旁路，从而导致网络的可靠性大大降低。NSF 技术的目标就是为了解决上述路由震荡的问题，在设备主控倒换时，转发层面不等待控制平面重新计算路由，先保持现有转发路径不变。

BFD

BFD 是一种三层检测机制，对相邻转发引擎之间通道故障提供轻负荷、持续时间短的检测。这些故障包括接口、数据链路，甚至是转发引擎本身。BFD 提供一个单一的机制，它能够用来对任何媒介、任何协议层进行实时地检测，并且检测时间与开销范围比较宽。

BFD 故障检测机制与以往的其他“Hello”检测机制相比，具有许多独到的优势。目前的网络路由协议一般采用慢 Hello 机制，在没有硬件帮助下，检测时间会很长（例如：OSPF 需要 2 秒的检测时间，ISIS 需要 1 秒的检测时间）。这对某些应用来说时间太长了，当故障发生时，故障感应时间越长代表着数据丢失量越大。BFD 协议的出现，为上述问题提出了一种解决方案，BFD For 路由，就是将 BFD 和路由协议关联起来，通过 BFD 对链路故障的快速感应进而通知路由协议，从而加快路由协议对于网络拓扑变化的响应，提供端到端的 200ms 延时保证。

MPLS OAM

MPLS OAM 是一个针对 MPLS 的 LSP 连通性的快速检测机制，通过 LSP 中各节点之间的 OAM 报文的快速交互，实现对于 LSP 连通性的检测。

MPLS OAM 不依赖于任何上层或下层的机制，主要实现以下功能：

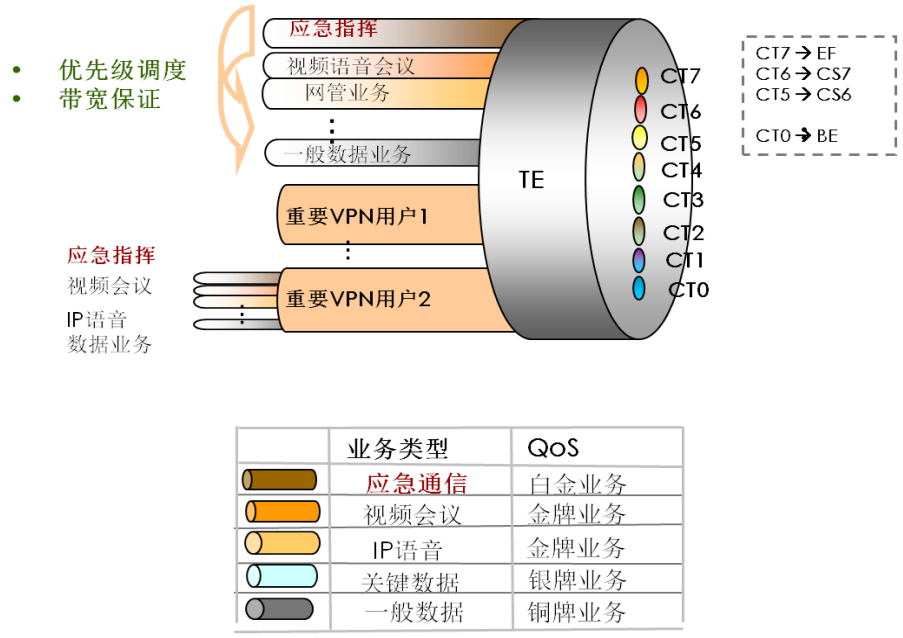
- 有效检测、识别和定位 MPLS 用户层面故障。
- 衡量网络的利用率以及度量网络的性能。
- 在链路出现缺陷或故障时迅速进行保护倒换，以便能根据与客户签订的 SLA（Service Level Agreements）提供业务。

2.8 QoS 规划

在应急指挥网络中，由于业务类型多而杂，不同类型业务对网络质量要求不同。某些关键业务既需要保证流量带宽要求，也需要保证传输时延要求。在多业务共存的应急指挥网络中需要采用 QoS 技术对关键业务的网络质量进行差异化保障。

针对带宽、时延、抖动、丢包率等要求，QoS 可以通过优先级映射、流量监管、流量整形、队列调度、拥塞避免等技术提升网络服务质量，满足用户在有限的资源限制情况下，获得多业务部署的最佳体验。

在应急指挥网络中， QoS 策略主要部署在业务汇集的骨干网。应急指挥网络主要基于 TE 的 MPLS-HQoS 完成不同类型业务的保障，如图 2-12 所示。重要用户（公安部门）建立高优先级的 VPN，VPN 内根据业务不同标记不同优先级，进行优先级调度，保证高优先级业务带宽（例如：应急通信、视频会议、IP 语音），VPN 内一般数据业务进行剩余带宽的公平调度调度。



	业务类型	QoS
	应急通信	白金业务
	视频会议	金牌业务
	IP语音	金牌业务
	关键数据	银牌业务
	一般数据	铜牌业务

图 2-12 **基于 TE 的 MPLS-HQoS 规划**

3 网络维护建议

3.1 网络管理

3.1.1 VPN 管理

场景分析

在应急指挥网络中部署 MPLS VPN 可以有效进行业务安全隔离，但是随着网络越大，对于每个 VPN 的业务管理就变得越发困难。

场景建议

通过 eSight 对 MPLS VPN 进行管理。eSight 具有以下优势：

- 一键式故障诊断：提供多种工具对各种链路的连通性进行诊断，助力定位网络故障。
- 与 SLA 智能联动，监控业务质量：快速评估 MPLS VPN 业务质量，提升用户运维管理能力。
- 与报表管理的智能联动，满足运维需求。
- 与性能监控的智能联动：通过统计各种性能指标，实现对 MPLS VPN 网络的性能管理。

3.1.2 设备管理

场景分析

在应急指挥网络中，除了一些网络 IP 设备外，还存在许多 IT 设备，例如：打印机、服务器、传真机等，因此对于所有设备的一体化管理成为一项运维重要需求。

场景建议

通过 eSight 对 IP 和 IT 进行一体化的管理，减少管理复杂度。eSight 具有以下优势：

- eSight 预集成业界主流设备，默认已包含 Cisco20 个系列 140 余款设备、H3C14 个系列 130 余款设备、其他厂商 100 余款设备、以及数十款打印机、服务器。企业运维人员不做任何配置，即可管理全网设备，大大提升管理效率。
- eSight 拥有厂商新款设备自动配套能力，通过 eSight 厂商类型自动识别能力，对于友商新发布的设备也可实现拓扑、告警、性能等管理能力。

- 针对业界主流设备深入分析，不仅支持标准的流量采集，还同时支持设备面板、设备 CPU 利用率等私有属性的管理。

3.2 故障处理

应急指挥网络系统是由网络设备、连接设备间链路和一些相关其它设备组成。因此出现网络系统故障的原因也基本上从链路、网络设备状态、其它相关状态等方面来查找。这些组件的任何一个出现故障，都会导致应急指挥业务无法正常工作。我们重点介绍一下网络设备故障的处理。

网络设备发生故障可以分为几种：

- 设备宕机：设备上的电源或者其他指示灯都不亮，没有任何工作时的声响。
- 设备 CPU 使用率高：监控软件或者登陆设备时，发现设备的 CPU 利用率很高，同时相关应用响应较慢。
- 有错误消息：查看日志服务器或者登陆设备时，发现设备有错误消息。
- 有报警信息：设备状态指示灯报警，显示为红色等。

设备宕机

如果发现一旦发现设备宕机，首先检查电源连接线和机房电源。如果电源连接线和电源均正常，立即拨打设备提供商和服务提供商的服务号码，请求支持。如果发现设备硬件存在问题，可要求设备提供商和服务提供商在最短时间内做备件更换服务。

设备 CPU 利用率高

立即报告服务提供商，要求提供技术支持。待技术支持工程师远程处理或到场后，协助工程师找出设备 CPU 利用率高的原因。一般情况下，可以判断为设备受到病毒的攻击。

有错误消息

将错误消息发送给服务提供商，并跟踪进度。经过服务提供商分析后，给出错误消息的原因，如果设备有隐形的故障，可以预先做好相应的准备工作或者更换设备。

报警信息

报告服务提供商和设备提供商，要求对设备进行报警故障排除或者更换硬件。

3.3 网络扩容

场景分析

随着业务不断增加，现有应急指挥网络容量已经不能满足长期发展的需求，对网络的扩容迫在眉睫，在不影响现有业务的情况下实现平滑扩容，是网络扩容的基本要求。

场景建议

网络扩容包含如下三种场景。针对不同的扩容场景需要使用不同的扩容策略，实现业务的平滑过渡。

- 服务器扩容

服务器扩容包含在原区域扩容服务器和在新区域新建服务器两种情况，针对这两种情况，所采取的扩容策略不尽相同。

- 原区域扩容服务器

  随着业务的不断增加，当前服务器资源已经不能满足业务发展需要，需要进行服务器的扩容，实现平滑扩容需要使用该区域初期规划好的 VLAN，保持 VLAN 的连续性，并且 IP 地址使用该区域初期规划好的地址段，这样做可以保证上游路由和防火墙策略不需要进行修正，便于维护的同时也减轻了扩容工作量。

- 新区域新建服务器

  新建区域需要为该区域重新规划 VLAN 资源和 IP 地址资源，重新进行路由和防火墙策略规划，这样做可以确保新区域的建设不会影响到现有业务，实现现有业务的平滑扩容，划分新的区域也便于今后运维管理。

- 网络设备扩容

推荐采用堆叠和集群技术，首先消除破环协议，其次简化网络规模，并且利于网络设备扩容。使用堆叠和集群技术后，网络结构由环形简化为树形。首先利于网络运维管理，其次网络设备扩容时，只需要在原有的堆叠环境下新增设备，对网络结构不产生影响，也不需要添加额外物理链路。

- 链路带宽扩容

随着业务的扩展，链路带宽也会成为瓶颈，除了使用更换高性能、高带宽单板外（比如 GE 换成 10GE 单板，10GE 换成 40GE 单板），还可以通过链路捆绑技术进行链路带宽扩容，在不影响现网业务的情况下实现链路带宽的平滑扩容。

3.4 灾难应急

场景分析

当出现意外灾害（例如地震、火灾等）时，应急指挥网络地面上的接入线路遭到破坏时，存在故障恢复时间长的问题。如何及时进行应急处理，及时恢复应急指挥业务，将应急指挥业务损失降低到最小，这些需要在网络规划时进行充分考虑。

场景建议

- 采用双链路接入，有线和无线线路组合。对于条件比较好、距离比较近的接入单位，可以采用两条有线线路直接连接，对于偏远地方和容易发生有线线路中断的地方（比如地质灾害引起有线线路中断），可以采用无线和有线的组合。
- 采用微波技术如图 3-1 所示，作为现有有线接入线路的有效备份，丰富的保护机制，适于传输网补网和应急抢险。当发生自然灾害，地面有线接入线路遭到破坏时，作为一种灾难应急手段。

- 采用卫星通信作为备份链路，如图 3-2 所示，主链路中断时，能够自动切换至卫星链路，快速建立本级指挥中心至上、下级指挥中心之间的网络连接。结构灵活，组网迅速方便。

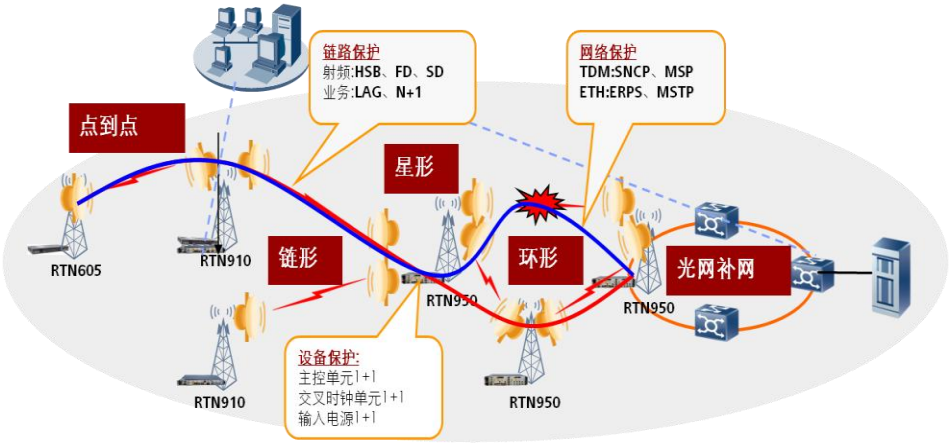


图 3-1 **应急指挥微波通信链路备份**

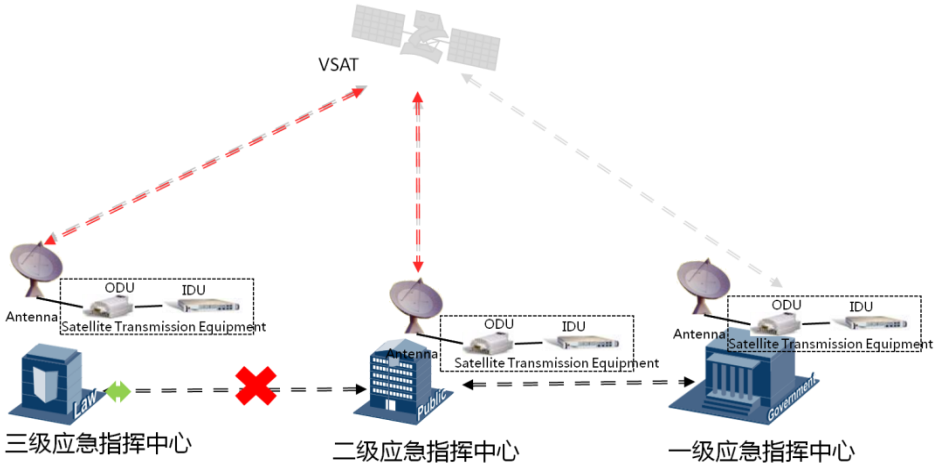


图 3-2 **应急指挥卫星通信链路备份**

4 产品介绍

4.1 AR 系列路由器

4.1.1 概述

HuaWei ®AR12/22/32 系列路由器是华为公司为满足新一代企业分支、中小企业的 WAN 接入和运营商转售市场多业务承载需求而推出的新一代接入路由器产品。

AR12/22/32 系列路由器基于新一代高性能硬件和华为公司统一的 VRP 软件平台，支持丰富的广域网接口，提供高密度以太、语音等用户接入，支持 IPSec VPN 和防火墙等安全功能，可充分满足企业分支互联、中小企业广域接入和运营商转售等多种场合的需求。

4.1.2 产品型号

HuaWei ®AR12/22/32 分为 AR12、AR22 和 AR32 三个系列产品。

表4-1 AR 系列产品

产品型号	设备外观	备注
AR1220		整机容量：8Gbps 转发性能：350Kpps/200Mbps(64byte)
AR1220V		整机容量：8Gbps 转发性能：350Kpps/200Mbps(64byte)
AR1220W/1220VW		整机容量：8Gbps 转发性能：350Kpps/200Mbps(64byte)
AR2220		整机容量：32Gbps 转发性能：1Mpps/500Mbps(64byte)
AR2240		整机容量：80Gbps 转发性能：2Mpps/1333Mbps(64byte)

产品型号	设备外观	备注
AR3260		整机容量：160Gbps 转发性能：3.5Mpps（SRU80 高性能主控板）/2000Mbps(64byte)

4.1.3 产品特点

AR 系列产品的特点如下：

高性能

华为 AR 产品采用最新的 ASIC 芯片和多核 CPU。LAN 模块内接口之间线速转发，LAN 模块之间具有高带宽 Fabric。CPU 采用 500MHz 两核到 750MHz12 核的 MIPS 处理器，25M 到 1G 的 WAN 转发性能，CPU 内置高性能加解密模块，具有 25M 到 300M 的加解密性能。

多业务集成

华为 AR 产品除了提供对数据业务的支持外，还可以同时作为 IP PBX、IPSec VPN 网关和防火墙使用，AR12 还有支持 WLAN AP 的型号，真正做到数据、语音、视频、安全、无线等多业务的统一集成。

强大的 QoS

华为 AR 产品支持 3 级 HQoS，其中 3260 通过 TM 硬件提供更强的转发性能。

高密度接入

华为 AR 提供高密度的语音和数据接入，通过不同类型的插卡组合，可以充分满足各种场景下语音和数据的混合接入。

丰富的广域网接口

华为 AR 提供丰富的广域网接口，包括 E1/T1、ISDN BRI、FR、3G 等各种主流接口，并支持作为 MPLS VPN 的 CE 和 PE 设备。

4.2 NE40E 核心路由器

4.2.1 概述

NetEngine40E 系列核心路由器（以下简称 NE40E）是华为公司推出的高端网络产品，广泛适用于 IP 国干网、IP 省干以及其他各种大型 IP 网络的核心、汇聚层。

NE40E 基于分布式的硬件转发和无阻塞交换技术，采用华为自主研发的 Solar 系列芯片，具有良好的线速转发性能，优异的扩展能力，完善的 QoS 机制和强大的业务处理能力。NE40E 基于最新的可扩展 400G 平台，实现 40G/Slot 到 400G/Slot 的平滑扩展，且兼容现网所有线卡，最大限度保护客户的投资。

NE40E 具有强大的汇聚接入能力。凭借丰富的特性支持，可以灵活部署 L2VPN、L3VPN、组播、组播 VPN、MPLS TE、QoS 等，实现业务运营级的可靠性承载。同时 NE40E 全面支持 IPv6，可以实现 IPv4 到 IPv6 的平滑过渡。

NE40E 可以灵活应用在 IP/MPLS 网络的核心、汇聚，可以简化网络结构，提供丰富的业务类型和可靠的服务质量，是 IP/MPLS 网络向宽带化、安全化、业务化、智能化发展的重要源动力。

4.2.2 产品型号

NetEngine40E 核心路由器的产品型号如下。

表4-2 NetEngine40E 核心路由器系列产品型号

产品型号	描述
NE40E-X16	支持 16 块 LPU 交换网容量 12.58T（双向） 背板容量 30Tbit/s 转发能力 3200Mpps
NE40E-X8	支持 8 块 LPU 交换网容量 7.08T（双向） 背板容量 15Tbit/s 转发能力 1600Mpps
NE40E-X3	支持 3 块 LPU 交换网容量 1.08T（双向） 背板容量 1.35T 转发能力 300Mpps

图4-1 NE40E-X16 外观图

图4-2 NE40E-X8 外观图

图4-3 NE40E-X3 外观图

4.2.3 产品特点

400G 路由平台

NE40E 是目前业界最强的 400G 平台路由器，满足未来至少十年的发展需求。

最紧凑，端口密度最大，最高密度 1320*GE/机柜，达到业界 2 倍。

最绿色的 400G 平台，每 GE 端口功耗不到 9W，低于业界 10%。

兼容设计，从 40G 升级到 400G 平台，单板、软件完全兼容。

全业务承载

NE40E 的全业务承载能力业界领先，可为电信级业务运营保驾护航。

支持 BRAS、DPI 等功能模块，保证多业务接入能力。

业界最完整的 HQoS 解决方案，支持 HQoS、DS-TE、MPLS HQoS，保证多场景的 QoS 部署。

高可靠性

NE40E 提供完善的端到端可靠性解决方案，可保证业务不中断。

设备级可靠：关键部件冗余备份，配合 ISSU/NSR/GR 等技术，最大限度避免业务中断运行。

网络级可靠：华为独有的 BFD For anything、E 系列增强保护技术，保证业务端到端 200ms 保护倒换。

4.3 NE20E 多业务路由器

4.3.1 概述

NE20E 路由器是华为公司面向金融、电力、政府、教育、企业、运营商等客户自主研发的高智能业务路由器，旨在满足客户汇聚接入网络的电信级可靠性、高可用性要求。

NE20E 基于分布式的硬件转发和无阻塞交换技术，叠加业务时保持保持高转发性能、具备优异的扩展能力，完善的 QoS 机制和强大的业务处理能力。NE20E 凭借丰富的业务特性，可以灵活部署 MPLS VPN、IPSec、GRE、组播、组播 VPN、MPLS TE、QoS 等，为客户快速部署新业务提供弹性平台；同时，NE20E 全面支持 IPv6，可以实现 IPv4 到 IPv6 的平滑过渡。NE20E 路由器作为高性能的汇聚设备，提供了全方位的网络解决方案，致力于在超带宽、业务系统融合化、用户需求个性化及运作全球化的趋势下，成为客户强有力的网络支撑平台。

4.3.2 产品型号

表4-3 NetEngine20E 核心路由器系列产品型号

产品型号	描述
NE20E-X6	支持 2 块 LPU 交换网容量 345 Gbps/950Gbps 转发能力 225 Mpps

图4-4 NE20E-X6 外观图

4.3.3 产品特点

丰富业务支持能力

NE20E-X6 可以提供丰富的特性支持和强大的业务处理能力，可以满足 IP/MPLS 承载网，企业的业务需要。

NE20E-X6 具有强大的路由能力，提供 RIP、OSPF、IS-IS、BGP4 和多播路由等丰富的路由协议，支持明/密文认证，具备快速收敛功能，保证在复杂路由环境下安全稳定。

NE20E-X6 具有强大的 VPN 能力，根据组网需求可以同时部署 L2VPN、L3VPN、MVPN，支持和 TE （Traffic Engineering）同时部署，支持丰富的接入类型（ATM、TDM、POS、Ethernet、E1/cE1 等），支持灵活 QinQ，支持 DHCP/IPoE，可以适应传统的接入需求和新兴的业务需求，满足多业务融合丰富的承载需求。

NE20E-X6 提供全面的 NAT 增强功能，包括 NoPAT、PAT、内部服务器 NAT、NAT ALG、业务报文目的地址替换、NAT E-Log。同时还提供 IPSec 助力客户构筑安全及可控的网络。

丰富路由处理能力

NE20E-X6 全面支持 RIP、OSPF、BGP、IS-IS 等单播路由协议和 IGMP、PIM、MBGP、MSDP 等多播路由协议，支持路由策略以及策略路由。面支持 IPv4 和 IPv6 双协议栈，实现硬件 IPv6 转发，提供丰富的 IPv6 协议。支持多种 IPv4 向 IPv6 的过渡技术：手工配置隧道、自动配置隧道、6to4 隧道等；支持 IPv6 静态路由，支持 BGP4/BGP4+、RIPng、OSPFv3、ISISv6 等动态路由协议；支持 ICMPv6 MIB、UDP6 MIB、TCP6 MIB、IPv6 MIB 等。

NE20E-X6 支持丰富的 IPv6 特性包括 IPv6 用户接入/认证、NAT、双栈/DS-Lite, 隧道及翻译。NE20E-X6 提供了完善的 IPv4-IPv6 解决方案，满足客户网络在以上各种演进场景下向 IPv6 过渡的需求。

全面汇聚能力

NE20E-X6 端口类型丰富，支持各种速率的 POS、ATM 接口卡、高密 GE 卡，在满足传统广域汇聚需求的同时，也可支持以太 MSTP 的汇聚。全面满足客户业务需求。

完善 OAM 技术

支持丰富全面的 OAM 技术，包括 MPLS 及以太网 OAM 技术。使用 MPLS OAM 机制，可以有效地检测、确认并定位出 MPLS 层内部的缺陷；报告缺陷并做出相应的处理；在出现故障的时候，能够提供保护倒换的触发机制。

NE20E-X6 支持的以太网 OAM 功能包括故障管理和性能管理两大部分。故障管理是通过定时或手动触发的方式发送检测报文来探测网络的连通性，可对以太网进行故障定位。故障管理可用于触发保护倒换，从而实现小于 50ms 的保护倒换。性能管理主要指对网络传输中的丢包率、时延、抖动等参数的衡量，也包括对网络中各类流量（如接收发送字节数、错误报文数等）进行统计。

4.4 S9700 系列核心交换机

4.4.1 概述

HuaWei ®S9700 系列运营级核心交换机是由华为公司自主开发的新一代高性能核心路由交换机产品，为满足多种业务在城域以太网上高质量的传输，。S9700 主要应用于城域网中的业务接入、汇聚和传输层，作为城域网的接入和汇聚节点，提供线速的 FE、GE 和 10GE 接口，同时可提供 155M、622M 和 2.5G 的 WAN 接口。也可以应用于行业网、数据中心，提供高密度的端口和丰富的增值业务能力。

4.4.2 产品型号

表4-4 S9700 系列核心交换机

产品型号	设备外观图	说明
S9703		交换容量2.88Tbit/s 背板容量7.2Tbit/s 转发能力1440Mpps
S9706		交换容量3.84/5.76Tbit/s 背板容量14.4Tbit/s 转发能力2880/4320Mpps
S9712		交换容量3.84/5.12/7.68Tbit/s 背板容量19.2Tbit/s 转发能力2880/3840/5760Mpps

4.4.3 产品特点

S9700 系列产品有如下特点：

灵活的扩展能力

- 供电能力：目前系统电源 AC 模块的最大供电能力为 2200W，DC 模块的最大供电能力是 2200W，支持 M+N AC/DC 电源备份。

强大的转发能力

- S9700 产品实现组播线速转发，硬件完成两级复制：交换网板复制到接口板和转发引擎复制到接口。

丰富的业务性能

- 提供丰富的二层业务特性，主要特性包括：VLAN、GARP/GVRP、灵活 QinQ、RRPP、SEP、Smartlink、STP/RSTP/MSTP、DHCP snooping、IGMP snooping、MLD snooping、Ethernet OAM；
- 提供丰富的 IP 业务特性，包括 IPv4 和 IPv6 单播路由协议、组播路由协议、VRRP、DHCP Relay/ DHCP Server/Option82 等；
- 全面支持 MPLS 业务，主要包括：MPLS 转发、LDP、MPLS-TE、MPLS-OAM；
- 提供完善 VPN 业务，主要特性包括：VPLS、VLL、BGP/MPLS IP VPN;
- 支持防火墙/NAT；
- 支持负载均衡；
- 支持 IPSec VPN。

周密的安全设计

- S9700 产品确保了数据平面和控制平面之间的自然分离，提供业界领先的安全性能。

电信级的可靠性

- S9700 产品的整机结构还提供了功能强大的监控系统。通过独立的监控单元实现对整个系统的管理维护。实现对单板、风扇和电源配电模块的管理、监控和维护。
- S9700 产品完全满足 EMC（Electro Magnetic Compatibility）要求。系统采用模块级屏蔽，实现了单板间的 EMC 隔离。

良好的可维护性

- 支持以太网 OAM；支持 MPLS OAM 能力；支持端到端的 OAM；支持基于物理端口、VLAN、LSP、ACL 的流量统计；支持 eSight 管理；支持远程设备维护功能；支持热补丁功能；支持版本回退功能。

4.5 S7700 系列汇聚交换机

4.5.1 概述

HuaWei ®S7700 系列运营级园区汇聚交换机是由华为公司自主开发的新一代高性能核心路由交换机产品，提供大容量、高密度、模块化的二到四层线速转发性能，具有强大组播功能，完善的 QoS 保障、有效的安全管理机制和电信级的高可靠设计，满足高端用户对多业务、高可靠、大容量、模块化的需求，降低运营商的建网成本和维护成本，可广泛应用于构建各种类型型园区网核心层和汇聚层交换机。

4.5.2 产品型号

表4-5 S7700 系列交换机

产品型号	说明
S7703	支持 3 块 LPU 交换容量 720Gbit/s 背板容量 1.2Tbit/s 转发能力 576Mpps
S7706	支持 6 块 LPU 交换容量 1T/2Tbit/s 背板容量 2.4Tbit/s 转发能力 1152Mpps
S7712	支持 12 块 LPU 交换容量 1T/2Tbit/s 背板容量 4.8Tbit/s 转发能力 1344Mpps

图4-5 S7703 外观图

图4-6 S7706 外观图

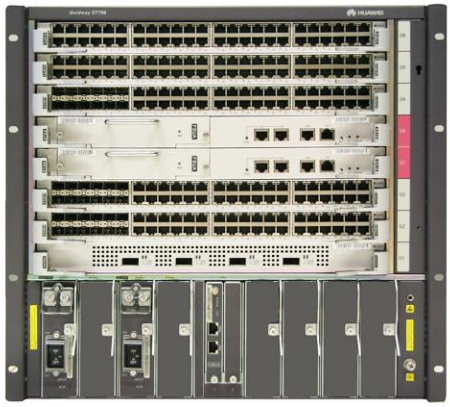
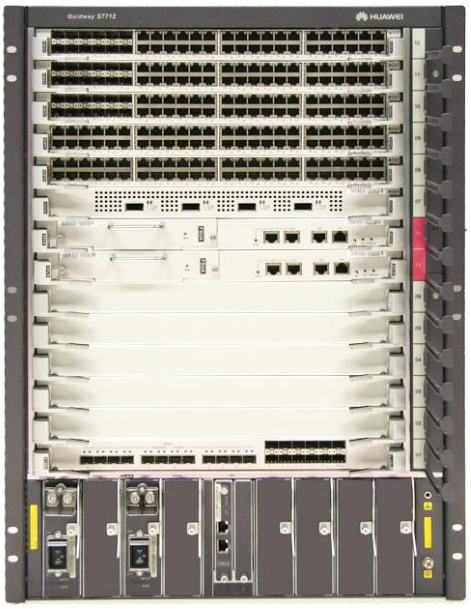


图4-7 S7712 外观图



4.5.3 产品特点

S7700 系列产品有如下特点：

先进体系结构，高性能，配置灵活

- S7700 系列交换机采用先进的全分布式体系结构设计，采用业界最新的硬件转发引擎技术，所有端口支持的业务能够线速转发，业务包括 IPv4/MPLS/二层转发等。支持 ACL 线速转发。
- S7700 系列交换机实现组播线速转发，硬件完成两级复制：交换网板复制到接口板和转发引擎复制到接口。
- S7700 支持 1.536Tbps 交换容量，支持多种高密度板卡，满足核心、汇聚层设备大容量、高端口密度的要求，可以满足用户日益增长的带宽需求，能够极大的保护和节约用户投资。

完善的安全机制

- S7700 系列交换机支持 OSPF、RIP v2 及 BGP v4 报文的明文及 MD5 密文认证，支持安全的 SSH 登录、命令行分级保护、基于用户安全策略的 SNMP V3、DHCP Snooping、IP Source Guard、DAI、层次化 CPU 通道保护，并提供以下几种用户认证方式：本地认证、RADIUS 和 HWTACACS 认证。
- 支持防网络风暴攻击、防 DOS/DDOS 攻击、防扫描窥探攻击、防畸形报文攻击、防网络协议报文攻击等安全技术。

全面的可靠性

- S7700 系列交换机最大支持 128 个汇聚组，每个汇聚组内支持最多 8 个成员端口，支持跨单板端口间的汇聚。
- 支持 DLDP，可以监控光纤或铜质双绞线的链路状态。如果发现单向链路存在，DLDP 会根据用户配置，自动关闭或通知用户手工关闭相关端口，以防止网络问题的发生。

- 支持 RRPP 及多实例，相比其他以太环网技术，RRPP 具有以下优势：拓扑收敛速度快，低于 50ms。收敛时间与环网上节点数无关，可应用于网络直径较大的网络。
- 支持标准 STP/RSTP/MSTP 二层环网保护协议。
- 支持 SmartLink 及多实例。
- 支持 BFD for 单播路由/VRRP/FRR/PIM。

4.6 S5700 系列汇聚交换机

4.6.1 概述

HuaWei ®S5700 系列以太网交换机（简称 S5700）是华为公司推出的集接入、汇聚和传送功能于一身的以太网交换机，满足企业网对多业务可靠接入和高质量传输的要求。

S5700 定位于企业网多业务的接入汇聚层，具有大容量、高密度、高性价比的分组转发能力。借助 S5700 可构建高可靠的环网拓扑，具有多业务接入能力、良好的扩展性、QoS、强大的组播复制能力和运营级的安全性。

4.6.2 产品型号

表4-6 S5700 系列交换机

产品型号	设备外观图	备注
S5700-28C-EI		三层交换机 ● 下行 24 个 GE 电 ● 上行支持三种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 ● 增强三层功能
S5700-28C-EI-24S		三层交换机 ● 下行 24 个 GE 光 ● 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 ● 增强三层功能

产品型号	设备外观图	备注
S5700-52C-EI		三层交换机 ● 下行 48 个 GE 电 ● 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 ● 增强三层功能
S5700-24TP-SI	DC  AC 	三层交换机 ● 24 个 GE 电 ● 基本三层功能
S5700-24TP-PWR-SI		三层交换机 ● 24 个 GE 电 ● 基本三层功能 ● 支持 PoE
S5700-48TP-SI		三层交换机 ● 48 个 GE 电 ● 基本三层功能
S5700-48TP-PWR-SI		三层交换机 ● 48 个 GE 电 ● 基本三层功能 ● 支持 PoE
S5700-28C-PWR-EI		三层交换机 ● 下行 24 个 GE 电 ● 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 ● 增强三层功能 ● 支持 PoE

产品型号	设备外观图	备注
S5700-52C-PWR-EI		三层交换机 ● 下行 48 个 GE 电 ● 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 ● 增强三层功能 ● 支持 PoE
S5700-28C-SI		三层交换机 ● 下行 24 个 GE 电 ● 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 ● 基本三层功能
S5700-52C-SI		三层交换机 ● 下行 48 个 GE 电 ● 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 ● 基本三层功能

4.6.3 产品特点

S5700 系列交换机的特点是：

电信级的可维护性

- S5700 遵循电信级标准设计，风扇、电源可现场更换，方便维护；机箱重量轻，可以安装在 600mm 深机柜中，且安装方便。
- S5700 提供软件热补丁技术，实现设备软件在线平滑升级。
- S5700 支持快速保护倒换机制 RRPP（Rapid Ring Protection Protocol），可以快速实现链路级和业务级保护倒换，满足运营级的可靠性要求。

强大的多业务接入能力

- S5700 通常部署在企业网的汇聚层，可直接接入来自下游 AMG（Access Media Gateway）和 LSW（LAN Switch）等设备的业务，并汇聚到上游设备。可接入的业务包括：VoIP、IPTV/VOD（Video On Demand）视频业务以及宽带上网业务。

- S5700 采用成熟、经济的 IP 内核技术，借助高性能 ASIC（Application Specific Integrated Circuit）芯片，提供大容量的数据交换能力，满足传统电信业务对低时延抖动、高可靠性的需求。S5700 采用以太网组网技术，支持组播业务，提供良好的 QoS 机制和多种保护倒换技术，实现了良好的带宽保证和多业务支持能力。

灵活的组网能力

- S5700 提供 10/100/1000BASE-T 以太网电接口、100/1000BASE-X 以太网光接口及万兆以太网光接口，支持 Access、Trunk 和 Hybrid 等多种接口类型。
- 对于千兆光纤连接，S5700 提供可插拔的 SFP（Small Form-Factor Pluggable）类型光模块。对于万兆光纤连接，S-switch 提供可插拔的 XFP（10Gigabit SmallForm Factor Pluggable）和 SFP+（SmallForm-Factor Pluggable Plus）类型光模块。光纤长度可以根据用户对传输距离的需求灵活选配。
- S5700 可以组成树状、星型和环状以太网。对于环状以太网，S5700 提供 STP（Spanning Tree Protocol）和 RRPP，消除环路并提供快速保护倒换。

网络级 QoS 保障

S5700 具备完善的 QoS 机制。S5700 能够智能感知业务，能够对 OSI 模型 2～4 层信息进行流分类，根据流分类结果提供访问过滤、流量监管、队列调度策略，从而确保不同业务对差别服务的要求。

多层面的扩展能力

- S5700 以华为公司拥有自主知识产权的 VRP（Versatile Routing Platform）平台为基础，结合设备和网络管理技术，提供高速的交换能力和丰富的业务特性。
- S5700 支持灵活业务插卡和多功能插槽，满足未来业务的扩展需求。

周密的安全措施

S5700 保障设备和数据传输的安全，有效的防止恶意用户对网络的攻击。

- 支持基于 MAC 地址的过滤。
- 提供丰富的 ACL 策略。
- 提供“VLAN＋MAC”的查表机制。
- 支持流量抑制。

S5700 提供安全的用户登录操作保护。

- 对登录用户提供口令保护，口令可加密功能。
- 通过配置用户级别和命令级别实现对命令的分级保护。
- 通过命令锁定当前配置终端，防止设备被非法使用。
- 对影响系统性能的重要命令，提供确认和提示。

S5700 提供 ALS（Automatic Laser Shutdown）功能，在光纤连接断开时停止发送激光，有效避免激光对用户的伤害。

便捷的操作维护

S5700 不仅自身提供基于接口的流量统计功能，支持 IP 网络中 Ping、Tracert 等故障检测和定位技术。而且还能配合华为公司 eSight 企业网络管理系统，提供丰富的性能监视、告警和快速的故障定位能力。

S5700 还支持基于 GUI 的 Web 网管界面，为用户提供友好的配置和管理界面。通过 Web 网管，用户可以很方便的通过 GUI 界面管理设备，降低对初级维护人员的要求。

此外，S5700 还支持 HGMP（Huawei Group Management Protocol）集群管理，通过自动收集设备拓扑的方法以及集中的维护管理通道，使一台设备可以管理多台二层交换机。

绿色节能设计

S5700 采用多种节能措施，包括：

- 采用静音风扇，风扇转速自动调整，降低系统的噪音，节省风扇功耗。
- 当检测不到业务端口对端连接设备，即端口空闲，则芯片进入省电模式，以减小功耗。
- 采用先进工艺、高集成度、低功耗芯片，并配合智能设备管理系统充分利用芯片的低功耗特性，在提升系统性能的同时还降低了整机功耗。

先进的防雷技术

S5700 采用华为专利内置防雷技术，可以应对各种恶劣环境，如架空走线。从而降低设备在雷击天气中的损坏概率，大大提高设备可靠性，将安全系数提高 30 倍。

人性化的 PoE 供电方式

S5700 支持 PoE（Power over Ethernet）功能，即可以通过双绞线向远端下挂的 IP 电话、无线 AP(Access Point)、便携设备充电器、刷卡机、摄像头、数据采集等终端设备提供集中式的电源供电，降低用户的初期投资成本。

S5700 支持 802.3af 标准和 802.3at 标准，解决不同厂家设备远端供电问题。其中，802.3at 标准支持最大 30W 的供电能力，可以为新一代的 IP 可视电话、双频 WiFiAP，视频监控摄像机，多功能 STB11，RFID 读卡器等大功率设备提供电力，降低网络复杂度。

S5700 提供基于时间段的供电控制能力，有效管理网络设备和电力消耗，降低运营成本。

4.7 WLAN 系列

4.7.1 概述

WLAN 系列产品主要包括 AC6605 盒式 AC 和 S9700/7700 ACU 插卡式 AC，以及 AP6010SN/DN，AP6310SN，AP6510DN，AP6610DN 等多款 AP。

4.7.2 产品型号

产品型号	设备外观图	备注
AP6010SN		室内型单频 AP
AP6010DN		室内型双频 AP

产品型号	设备外观图	备注
AP6310SN		经济型室分单频 AP
AP6510DN		标准型室外双频 AP
AP6610DN		全规格室外双频 AP
AC6605		盒式 AC
S9700/S7700 ACU 插卡		插卡式 AC

4.7.3 产品特点

AP 产品特点

- 2x2 多入多出(MIMO)，2 条空间流
- 支持最大比合并(MRC)
- 支持 802.11n 和 802.11b/g 波束赋形
- 支持 20- 和 40-MHz 信道，PHY 数据速率高达 300Mbps
- 数据包聚合：A-MPDU(Tx/Rx)；A-MSDU(Rx only)
- 802.11 动态频率选择(DFS)

插卡式 AC 产品特点

- AP 管理与用户接入
  - 大容量：每块 SPU 插卡支持管理 1024 个 AP，最大可支持管理 11K 个 AP
  - 支持按模板批量配置 AP
  - 灵活多样的用户认证模式：MAC、Portal 和 802.1x、Portal 免认证
  - 支持全局调优、局部调优和射频捕盲
- 安全及权限控制
  - 丰富灵活的用户权限控制，支持用户分组、隔离、ACL 等
  - 支持多种安全协议标准：WEP、WPA/WPA2(PSK/1X)、WAPI
  - 支持密钥管理，支持 AP 黑名单
  - 防 STA IP 地址仿冒、ARP 攻击（DAI）、DHCP 服务器仿冒
- 无线网络

- 支持 CAPWAP 隧道协议、线速转发
- 支持 WMM、优先级映射、CAR、流级别定义，支持负载分担和 AC 备份
- 灵活的组网模式（本地转发/集中转发/集中认证、本地转发，二三层组网）、WDS 网络部署

4.8 eSight 网管

4.8.1 概述

eSight 是华为面向企业市场推出的新一代网络运维解决方案，是华为企业业务 IP 产品线面向企业市场推出的新一代 IP+IT 统一网络运维系统，遵循 ITIL 规范，实现对企业资源、业务以及用户的统一管理，为企业和合作伙伴提供融合、开放的运维平台，实现以企业设备-业务-应用-用户为核心的企业立体化运维。

4.8.2 产品特点

基础设备管理

基础设备管理功能包括如下几点。

- 管理设备范围：eSight 除了全面支持华为路由器、交换机、AR、安全设备的配套外；还预集成了对 H3C、CISCO 部分第三方设备的管理。同时提供有线、无线设备的统一管理。同时支持对服务器，打印机等企业 IT 资源的管理。
- 第三方定制能力：eSight 提供了方便快捷的第三方设备管理定制能力，包括设备厂商、设备类型、面板、性能、拓扑、告警管理的定制。用户可以基于 eSight 提供自定义能力增强对其他厂家设备的管理能力。
- 可定制的 Portal：eSight 提供可定制的 Portal，满足不同角色差异化的维护需求。
- 设备发现：eSight 实现 SNMP 网络设备的添加，支持手动输入 IP 地址、IP 地址网段，以及通过文件方式导入设备列表的方式完成设备添加。
- 拓扑管理：eSight 实现网络设备的图形化、层次化展示，同时显示子图、网元、链路，以及网元状态的显示。
- 告警管理：eSight 即时的接收设备上报的告警，并进行界面展示。包含当前告警管理、历史告警管理、告警转储、告警通知等功能。
- 性能管理：eSight 实现监控实例的管理，并支持采集数据的阈值管理、支持指标模板管理、历史性能数据管理。
- 报表管理：eSight 提供丰富的预定义报表，同时提供强大易用的报表设计功能，用户可根据行业特点和自身运维要求进行客户报表定制。
- 智能配置工具：eSight 智能配置终端预置了常用的业务配置模板，用户可以方便的选择模板，快速进行批量设备业务部署和维护。
- 企业 CPE 即插即用：eSight 提供基于 TR069 的 CPE 即插即用开局方案，降低服务成本。

分级网络管理

eSight 契合企业总部-分支结构，支持企业分级、分层次构建网管管理区域，建立层次化的管理体系。用户能够查看下级网管的告警、拓扑、性能和报表等功能。

网络业务运维

- WLAN 业务管理：eSight 提供对华为 AC 设备管理，通过对 AC 的配置管理实现对 WLAN 业务的配置功能。
- IPSec VPN 业务管理：eSight 支持 IPSec VPN 业务监控管理，提供浏览业务拓扑功能。
- MPLS L3VPN 业务管理：eSight 提供 MPLS L3VPN 业务监控管理，支持业务拓扑、业务还原、业务告警、性能管理。支持跨域 Option B、HoVPN、MCE 组网的自动发现、拓扑展示及业务监控。
- 网流分析：eSight 支持业界主流的网流技术，如 Netstream、Netflow、sFlow、IPFIX、Cflowd、J-flow 等。

开放开发平台

- 北向功能：eSight 提供 SNMP 告警北向接口，实现与上层 OSS 系统对接。
- 二次开发：通过采用类似 Eclipse 的扩展点机制提供灵活的扩展性及二次开发能力，基于扩展点机制，可实现增量功能的开发以及增量网元版本的适配。