H3C
数字化解决方案领导者

AD-WAN技术专刊（二期）

应用驱动广域网

目录 Contents

AD-WAN承载

AD-WAN分支

AD-WAN承载网

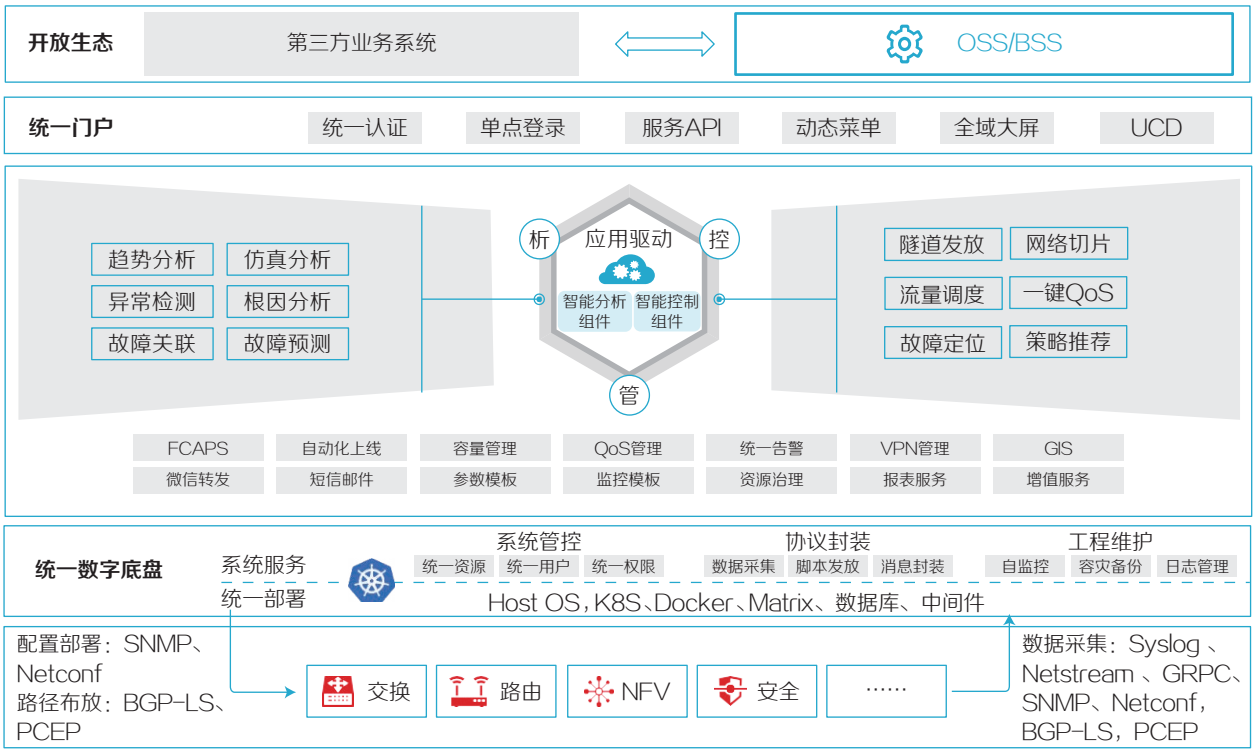
解决方案概述

方案概述

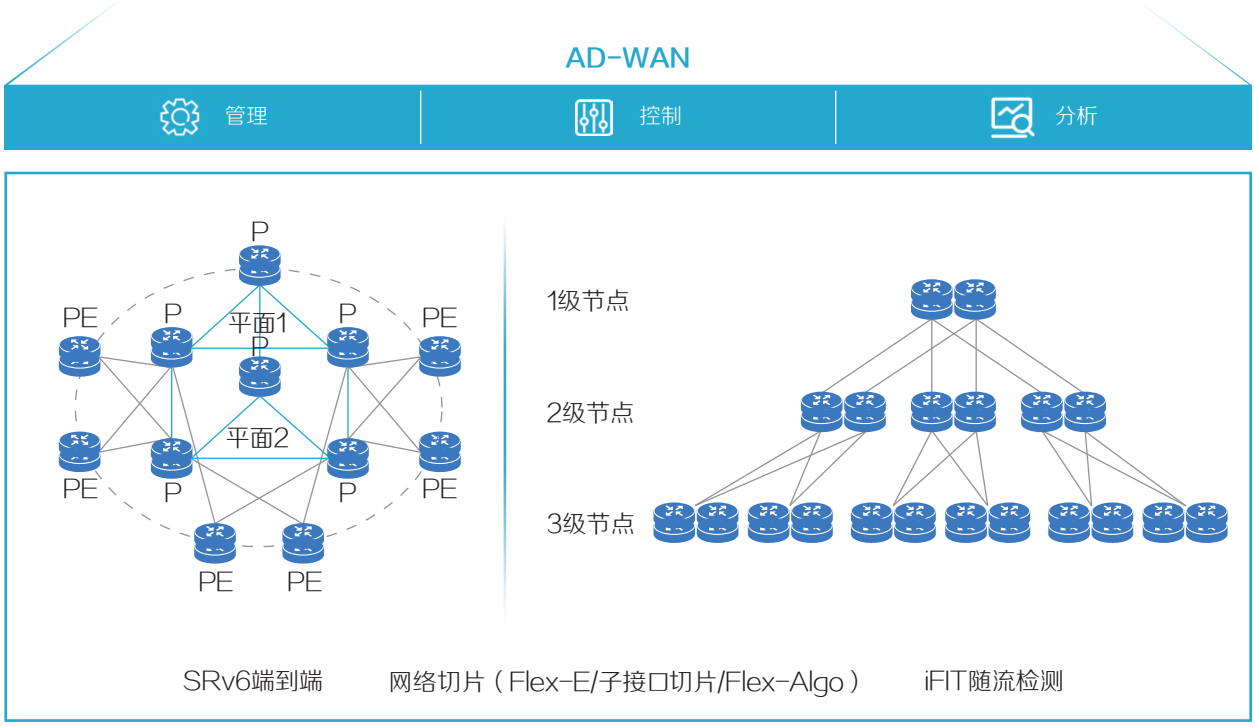
云时代随着网络规模越来越大，业务类型越来越多，新兴业务对承载的广域网络要求越来越高，网络需要在广联接、超宽、自动化、确定性、低时延和安全六个维度全面提升。

H3C以IPv6+为标准，面向金融、政府、电力能源、企业等行业，提出了应用驱动的AD-WAN (Application-Driven Wide Area Network)承载网解决方案，针对广域骨干、DCI互联和多级纵向等网络，通过SRv6、SR-TE、EVPN、网络切片、智能选路、随流检测和智能运维等功能，为用户提供更好的业务体验。

采用SDN相关技术，AD-WAN是一个融合、分层、开放、智能的网络技术架构，统一融合智能管理模块、智能控制模块、智能分析模块，实现“管”、“控”、“析” 三维一体。面向用户、统一Portal，真正做到“一次登录、一键发放、一体保障、一站运维”，结合大数据分析与AI学习能力，抓取网络实时快照、离线建模，实现网络的智能预测、智能仿真与智能排错，助力广大用户实现数字化网络智能升级。



方案价值



10倍
效率提升

业务自动化

- 业务自动化部署，分钟级上线
- 一键QoS下发，图形化体验
- 丰富调度策略，精细化管控

网络切片化

- K级切片，大规模覆盖
- 业务硬隔离，带宽独享可保障
- Slice ID灵活切片，免地址规划

K级
业界领先

40%
降低扩容成本

保障精细化

- 智能负载均衡，提升链路利用率
- 算网大脑，算力网络一体化
- DetNet场景，确定性网络体验

运维智能化

- 多维可视，提升使用体验
- 智能仿真，降低业务上线风险
- iFIT随流检测，分钟级故障定位

80%
节省运维成本

方案核心产品

AD-WAN

广域网管控析
智能融合系统

骨干

SR88-X系列

CR19000系列/CR16000系列

汇聚/总部

SR6600-X系列

MSR5600系列

SR6600/SR6602系列

接入/分支

MSR2600系列

MSR810系列

MSR3600系列

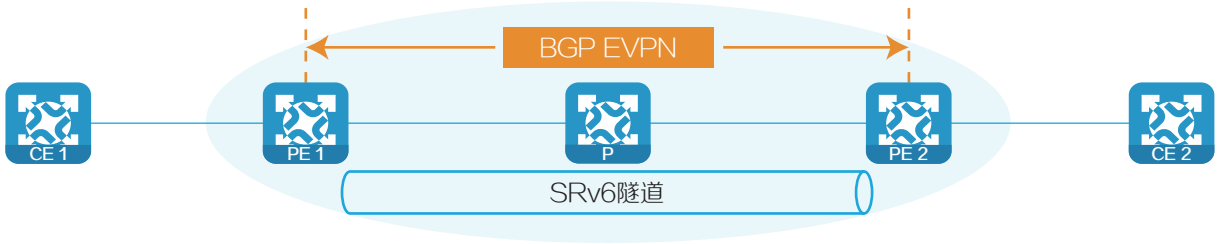
MSR830系列

EVPN over SRv6

EVPN over SRv6是指在IPv6骨干网上使用EVPN路由发布SID，建立SRv6隧道，并使用该隧道承载用户站点之间的二三层业务。

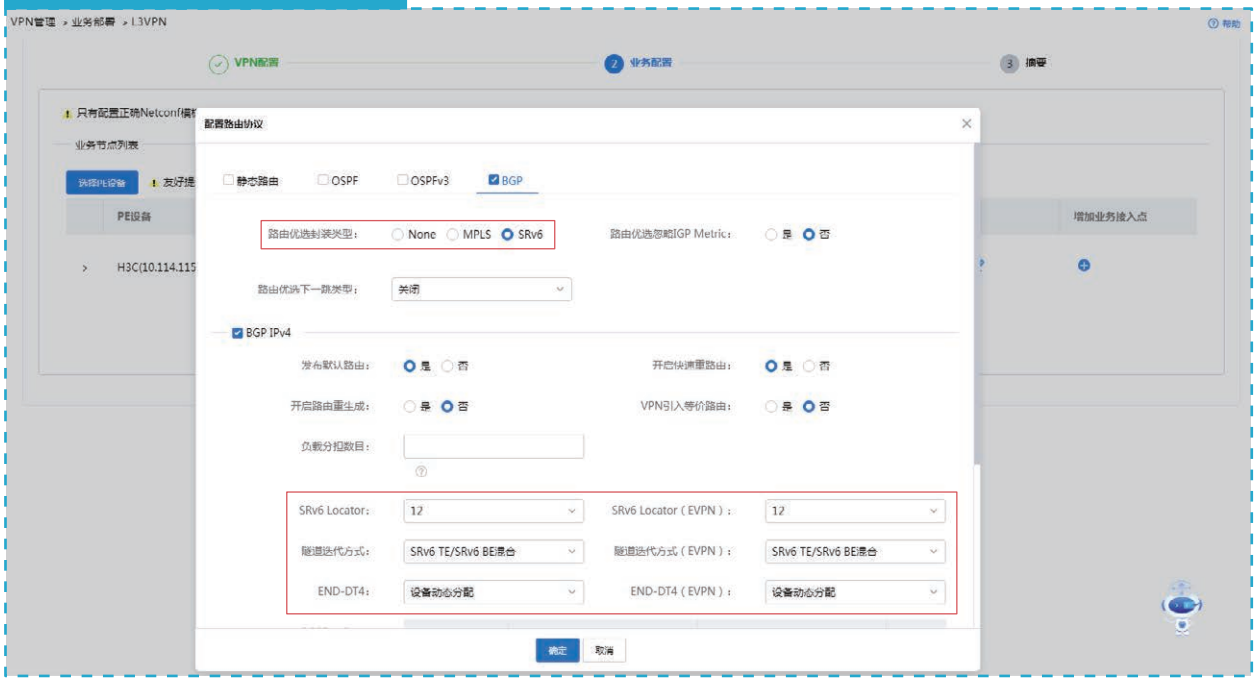
EVPN over SRv6根据IPv6骨干网使用的EVPN路由不同，分为

- EVPN L3VPN over SRv6
- EVPN VPWS over SRv6
- EVPN VPLS over SRv6

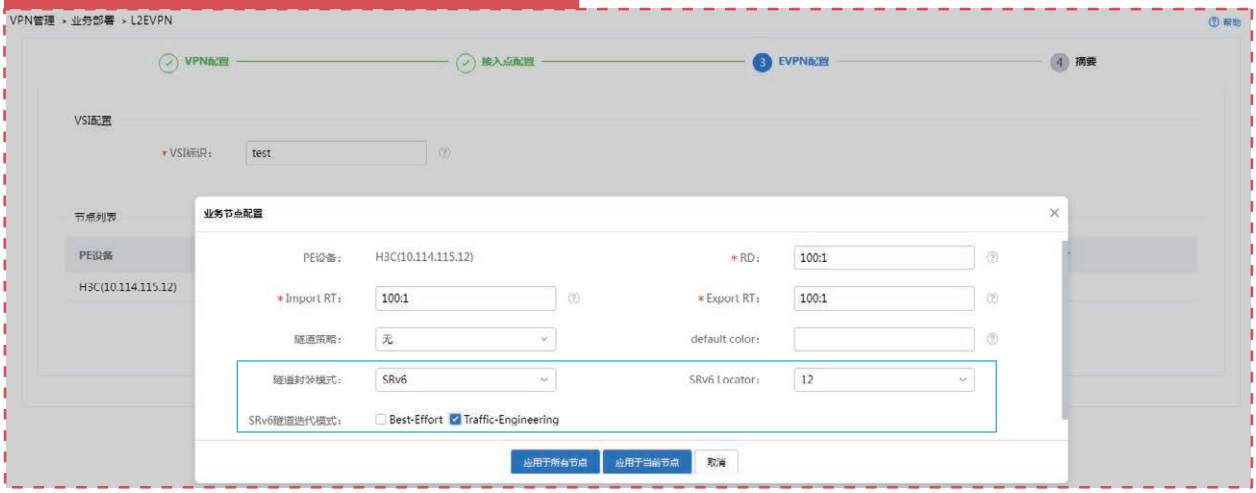


部署EVPN over SRv6

部署EVPN L3VPN over SRv6



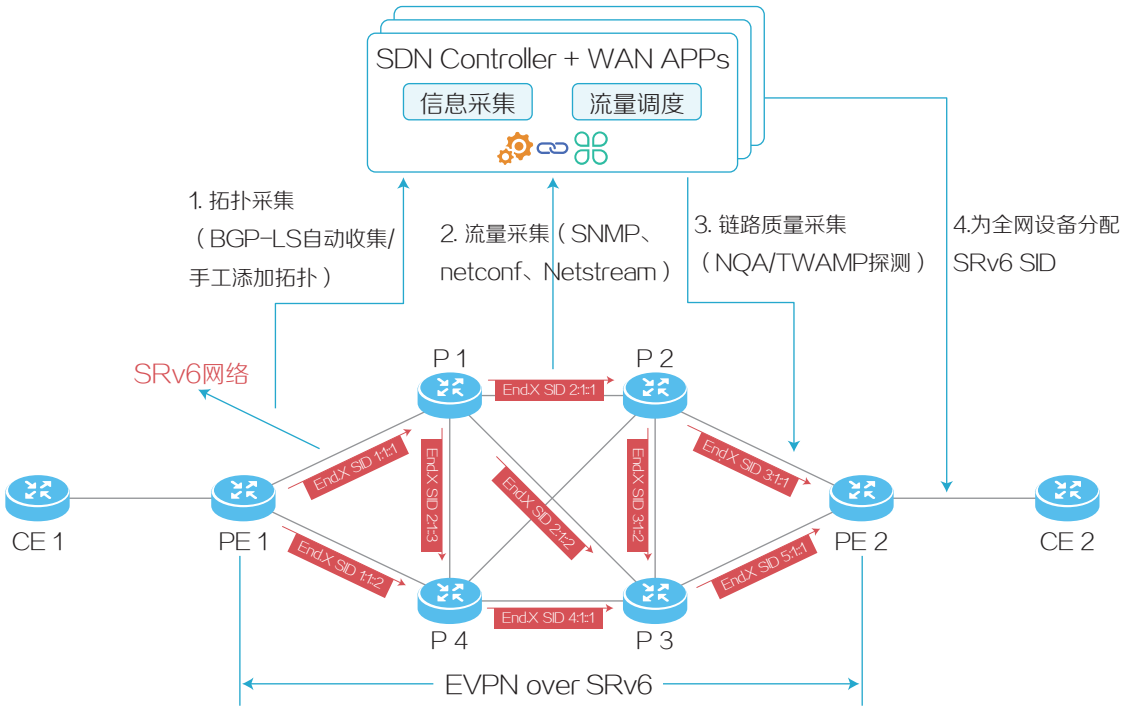
部署EVPN VPWS或EVPN VPLS over SRv6



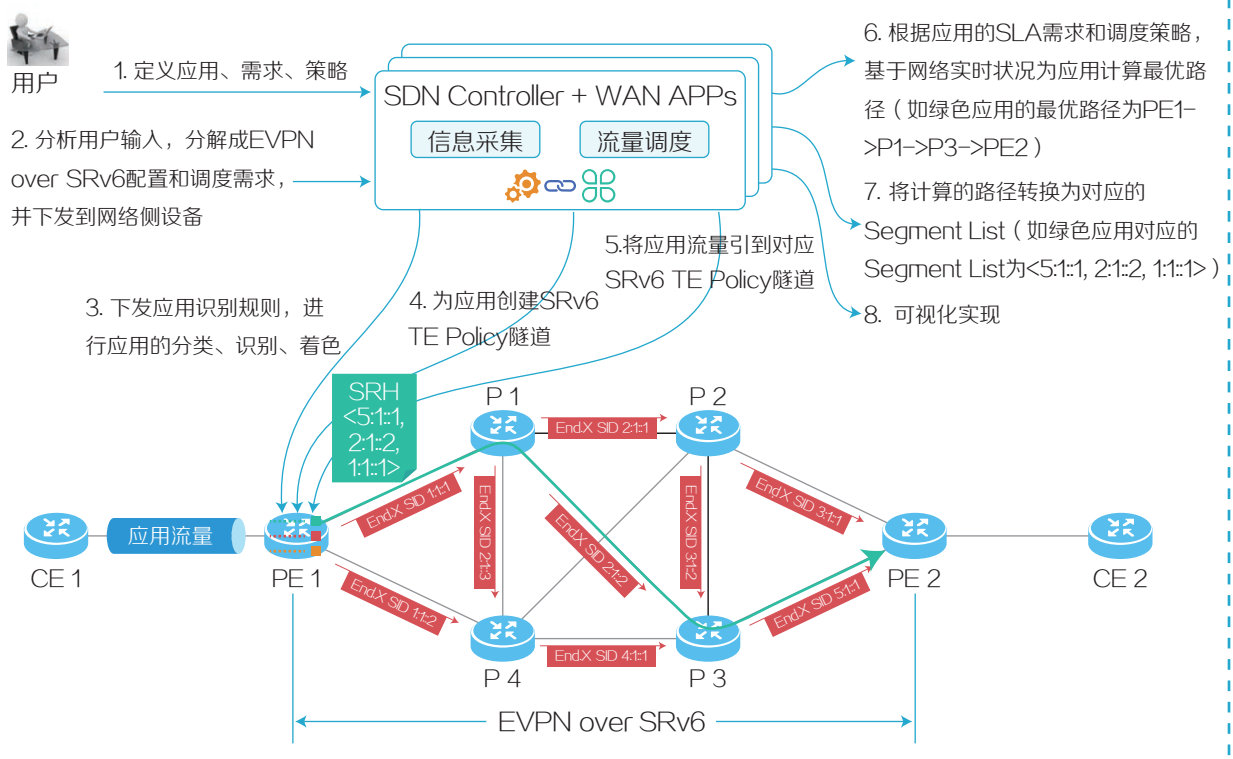
EVPN over SRv6控制组件侧工作机制

控制组件分配SRv6 SID

在SRv6网络中，控制组件通过 BGP-LS收集网络侧拓扑信息，采用 SNMP、NetStream、Netconf 功能采集网络侧的链路流量。控制组件通过NQA 或TWAMP 功能对网络侧链路质量进行分析，然后为全网设备分配SRv6 SID。



控制组件基于EVPN over SRv6实现应用调度



EVPN over SRv6设备侧工作机制概述

EVPN over SRv6 设备侧工作机制如下：

SRv6 SID

不同EVPN over SRv6组网中，使用的SRv6 SID不同，详见下表。

适用组网	SRv6 SID类型	携带SID的BGP EVPN路由	SID的功能
EVPN VPLS over SRv6	End.DX2 SID	AD per EVI路由 MAC/IP发布路由	标识一个AC，对应的转发动作是去掉IPv6报文头及其扩展头，然后将报文从指定的AC转发出去
	End.DT2U SID	AD per EVI路由 MAC/IP发布路由	标识一个VSI，对应的转发动作是去掉IPv6报文头及其扩展头，然后查找MAC地址表将报文转发到对应的出接口
	End.DT2M SID	IMET路由	标识一个VSI，对应的转发动作是去掉IPv6报文头及其扩展头，然后将报文在VSI内广播泛洪
EVPN VPWS over SRv6	End.DX2 SID	AD per EVI路由	标识一个AC，对应的转发动作是去掉IPv6报文头及其扩展头，然后将报文从指定的AC转发出去
EVPN L3VPN over SRv6	End.DT4 SID End.DT6 SID End.DT46 SID	EVPN的IP前缀路由	标识一个VPN实例，对应的转发动作是去掉IPv6报文头及其扩展头，然后将报文在指定的VPN实例内查找路由表转发出去
	End.DX4 SID End.DX6 SID	EVPN的IP前缀路由	标识一个下一跳信息，对应的转发动作是去掉IPv6报文头及其扩展头，然后将报文通过指定的下一跳地址和出接口转发出去

建立SRv6隧道

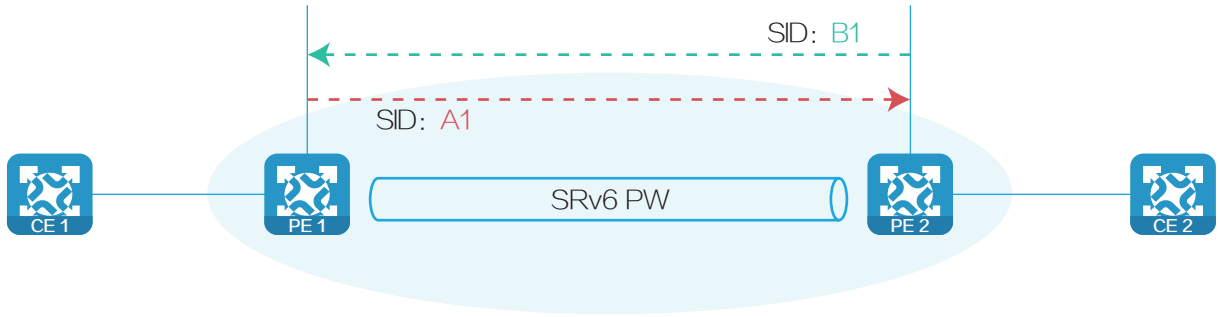
EVPN VPLS over SRv6

PE间通过BGP EVPN路由（IMET路由、AD per EVI路由和MAC/IP发布路由）交互SRv6 SID，以建立SRv6 PW。如下图所示，以PE 1与PE 2交互IMET路由为例，建立SRv6 PW的过程为：

① PE 1、PE 2之间相互发布IMET路由，在IMET路由中携带本端为VSI分配的End.DT2M SID。

② PE 1和PE 2收到IMET路由后，建立本端PE到远端PE的单跳SRv6隧道，该隧道的SID标识为路由中的End.DT2M SID。

③ PE 1建立本端（PE 1）到远端PE（PE 2）的单跳SRv6隧道，PE 2采用相同的方式建立PE 2到PE 1的单跳SRv6隧道，两条SRv6隧道组成一条SRv6 PW，用来承载用户二层数据。



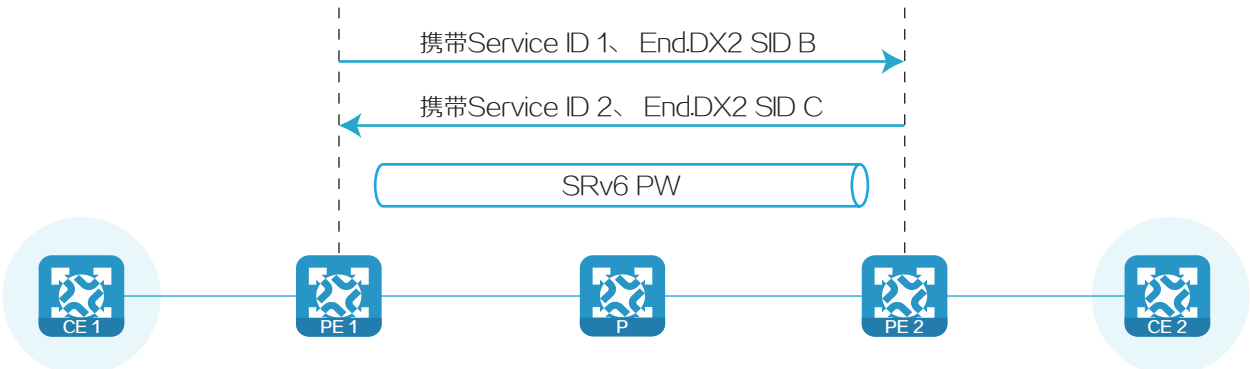
EVPN VPWS over SRv6

动态建立是指PE间通过BGP EVPN路由交互End.DX2 SID，以建立SRv6 PW。动态建立SRv6 PW的过程为：

① PE 1向PE 2发布EVPN的以太网自动发现路由时，在该路由中携带本端的Service ID、本端为交叉连接分配的End.DX2 SID。

② PE 2接收到EVPN路由后，如果路由中携带的Service ID与本地配置的远端Service ID相同，则建立PE 2到PE 1的单跳SRv6隧道，该隧道的SID标识为路由中的End.DX2 SID。

③ PE 1和PE 2均发布End.DX2 SID，并在两个方向上均建立单跳SRv6隧道后，两条SRv6隧道组成一条PW，用来承载用户二层数据。该PW称为SRv6 PW。



SRv6转发表	
In SID	Out SID
B	C

SRv6转发表	
In SID	Out SID
C	B

EVPN L3VPN over SRv6

如下图所示，控制组件下发的SRv6 TE Policy的SID List为<6:5::1, 4:3::10>，即所经过的SRv6节点为P和PE 2。

PE 1、P和PE 2通过IGP协议在公网发布Locator路由。

PE 2通过IGP（以IS-IS路由为例）协议将End.DT4 SID所在网段路由4:3::/64发布给P 2、P、P 1和PE 1。 P 2、P、P 1和PE 1收到PE 2发布的IGP路由后，将其学习到路由表中。同样， P 2、P、P 1、PE 1也发布自己的 Locator路由。

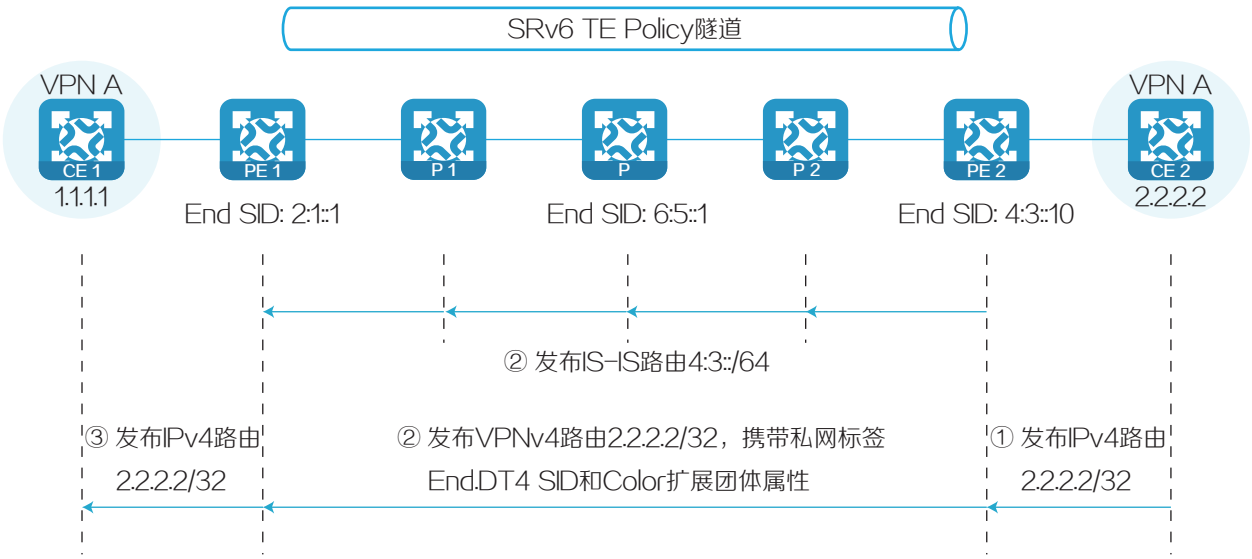
CE 2的私网路由发布到CE 1的过程如下：

① CE 2使用IGP或BGP，将本站点的私网路由2.2.2.2/32发布给PE 2。

② PE 2从CE 2学习到私网路由信息后，将私网路由存放到VPN实例A的路由表中。PE 2为私网路由增加RD和RT属性，并为私网路由分配End.DT4 SID 4:3::1，形成VPNv4路由。PE 2通过MP-BGP把携带 End.DT4 SID和Color扩展团体属性的VPNv4路由发布给PE 1。

③ PE 1收到VPNv4路由后，将该路由加入到VPN实例A的路由表中，同时将VPNv4路由按Color引流方式 引流到SRv6 TE Policy。PE 1将VPNv4路由转换成IPv4路由发布给CE 1。

④ CE 1收到私网路由后，将其学习到路由表中。



表项学习

EVPN VPLS over SRv6

在EVPN VPLS over SRv6组网中，PE根据学习到的MAC地址表项转发二层报文。PE上MAC地址学习分为两部分：

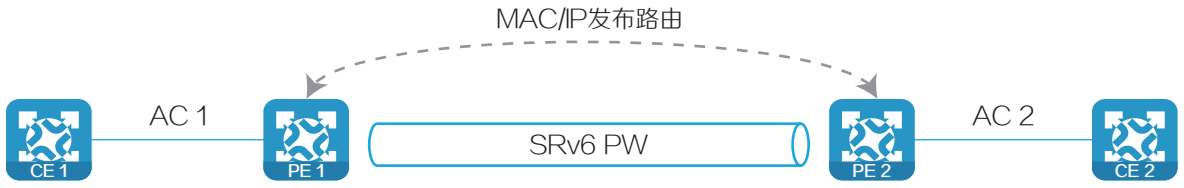
- 本地MAC地址学习：PE接收到本地CE发送的报文后，判断该报文所属的VSI，并将报文中的源MAC地址（本地CE的MAC地址）添加到该VSI的MAC地址表中，该MAC地址的出接口为接收到报文的AC。
- 远端MAC地址学习：PE通过MAC/IP发布路由将本地学习的MAC地址通告给远端PE。远端PE接收到该信息后，将MAC添加到对应的VSI的MAC地址表中，该MAC地址的出接口为两个PE之间的SRv6 PW。

VSI a的MAC地址表

MAC地址	VSI名称	出接口
CE 1	VSI a	AC 1
CE 2	VSI a	SRv6 PW

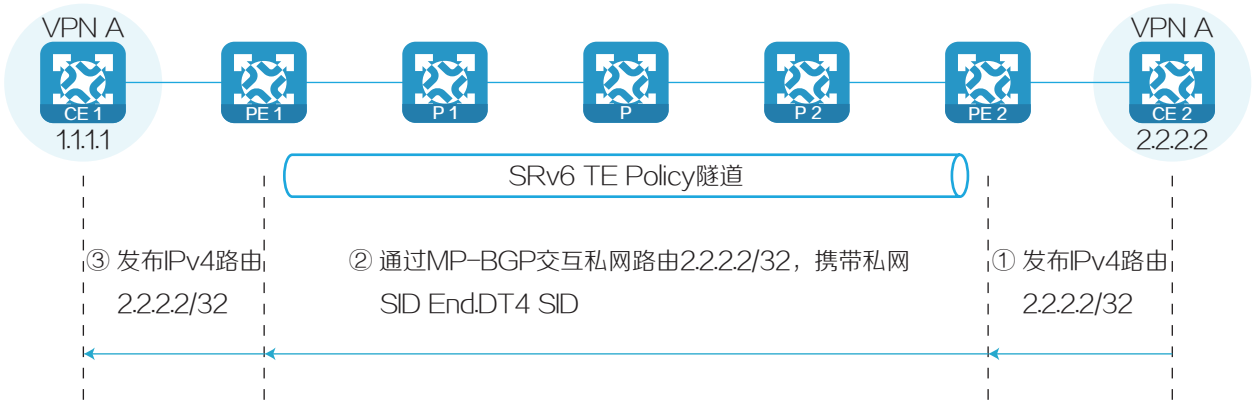
VSI a的MAC地址表

MAC地址	VSI名称	出接口
CE 2	VSI a	AC 2
CE 1	VSI a	SRv6 PW



EVPN L3VPN over SRv6

如下图所示，在EVPN L3VPN over SRv6组网中，PE之间通过通过MP-BGP交互私网路由。



报文转发

EVPN over SRv6支持SRv6 BE、SRv6 TE和SRv6 TE/SRv6 BE混合三种报文转发方式。不同转发方式之间存在如下差异。

转发方式	SRv6 TE方式	SRv6 BE方式
转发原理	根据报文属性查找匹配的SRv6 TE Policy，为报文添加携带特定的SID和SRv6 TE Policy SID列表的SRH头后，通过SRv6 TE Policy转发该报文	根据封装的SID查找IPv6路由表进行转发
转发路径	• 支持基于Color、隧道策略等多种引流方式，可以根据不同转发需求灵活选择引流方式 • 通过规划SRv6 TE Policy中的SID List实现转发路径可控，可以根据业务需求选择合适的转发路径	转发路径不可规划，通过IGP协议计算
可靠性	SRv6 TE Policy中存在多条候选路径，支持主备路径备份	网络故障时，转发路径的切换速度取决于路由收敛速度
负载分担	候选路径中存在多个SID List，可以根据SID List的权重进行负载分担	基于Locator路由的负载分担

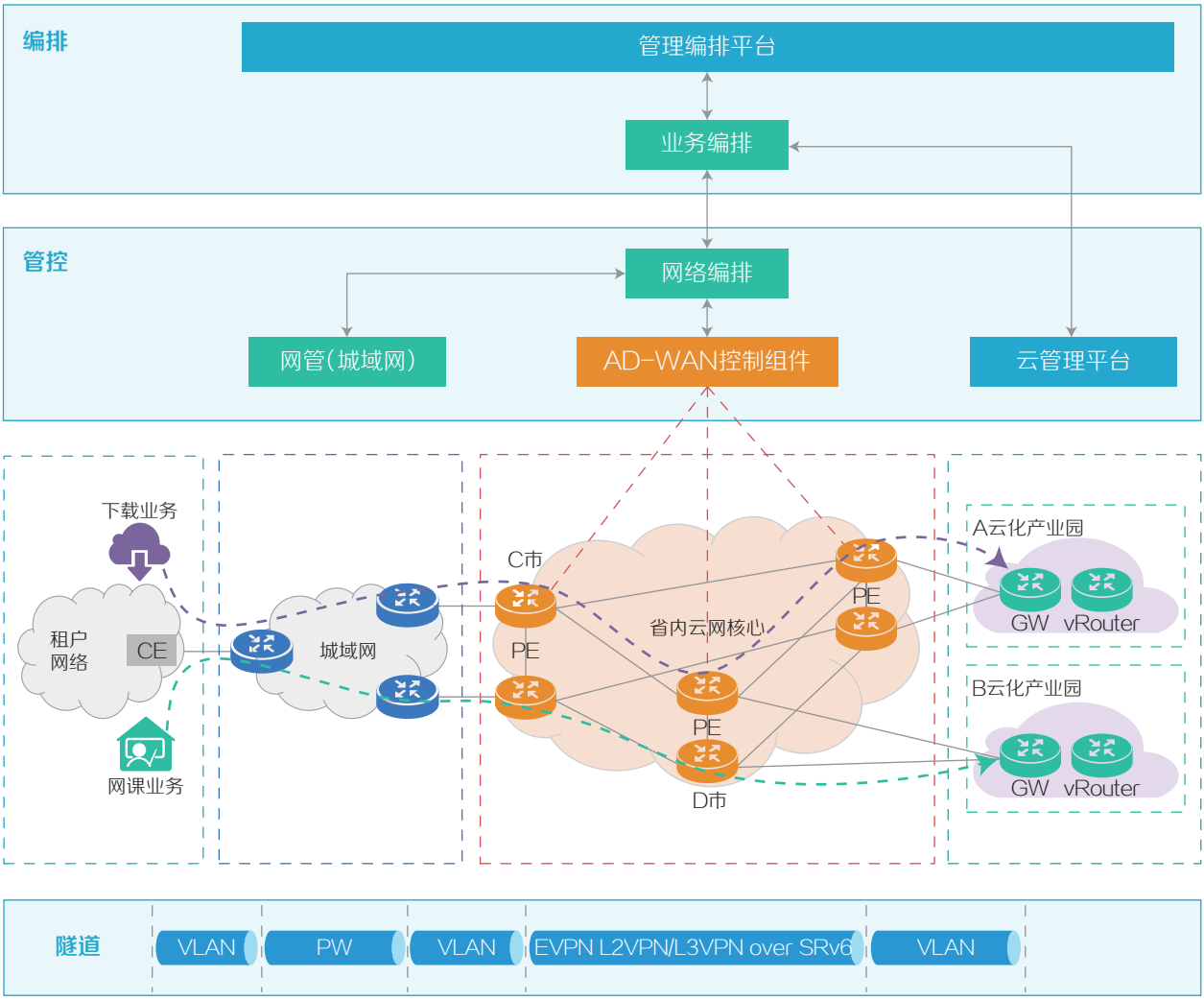
SRv6 TE/SRv6 BE混合方式：优先通过SRv6 TE方式选择转发路径；如果SRv6 TE方式未找到可用的SRv6 TE Policy，则通过SRv6 BE方式选择转发路径。

典型组网

如下图所示，在省内云网核心部署PE，分别连接城域网和云化产业园。其中：

- AD-WAN控制组件负责业务部署、自动化开通和智能调优。
- 管理编排平台负责管控端到端业务。

根据用户需求，控制组件向网络侧设备下发EVPN over SRv6配置，在省内云网核心建立EVPN L2VPN/L3VPN over SRv6隧道。通过SRv6的多种引流方式，满足用户的不同需求。



AD-WAN承载网 可靠性

功能简介

AD-WAN承载网方案的可靠性是其核心优势之一，通过设备、链路、网络、业务和集群等不同维度的可靠性设计，为企业的业务提供更加稳定和高效的网络支持。

01 / 控制模块高可靠

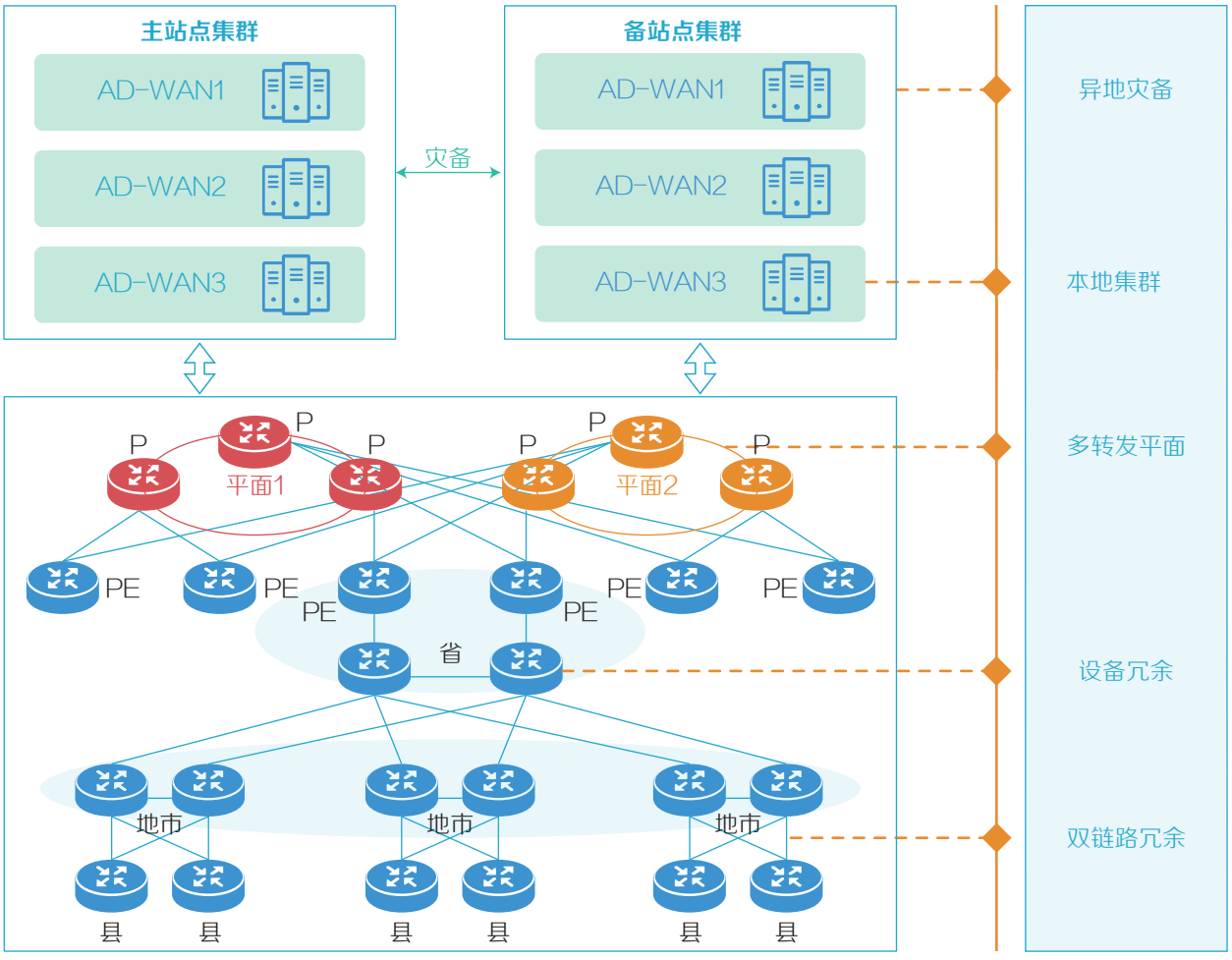
02 / 硬件/网络高可靠

03 / 业务高可靠

承载网方案整体网络设计

AD-WAN承载网解决方案采用“骨干网+纵向网”高可靠性冗余设计：

- 骨干网：采用FULL-Mesh网络，网络节点之间通过专线互连，通过不同转发平面承载不同区域之间的流量。
- 纵向网：采用树形多级纵向网络，节点为双设备双链路冗余，部分纵向网络与骨干网跨域对接。

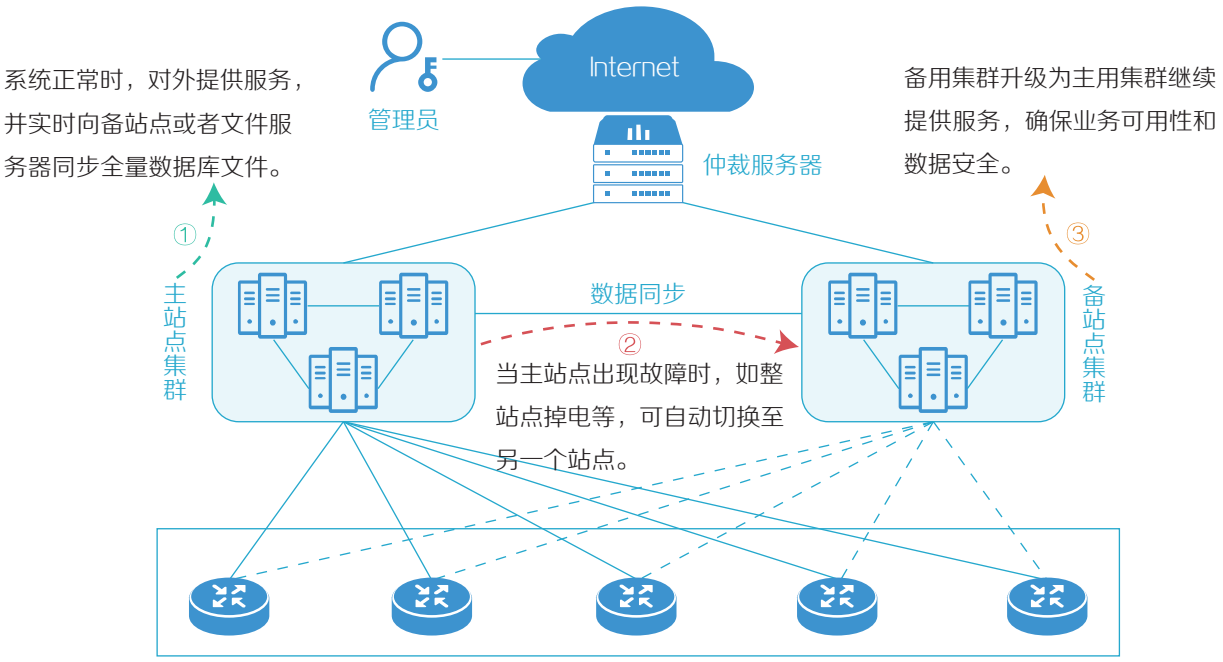


控制模块高可靠

AD-WAN承载网解决方案中，控制模块的高可靠性通过2种部署模式来支持：

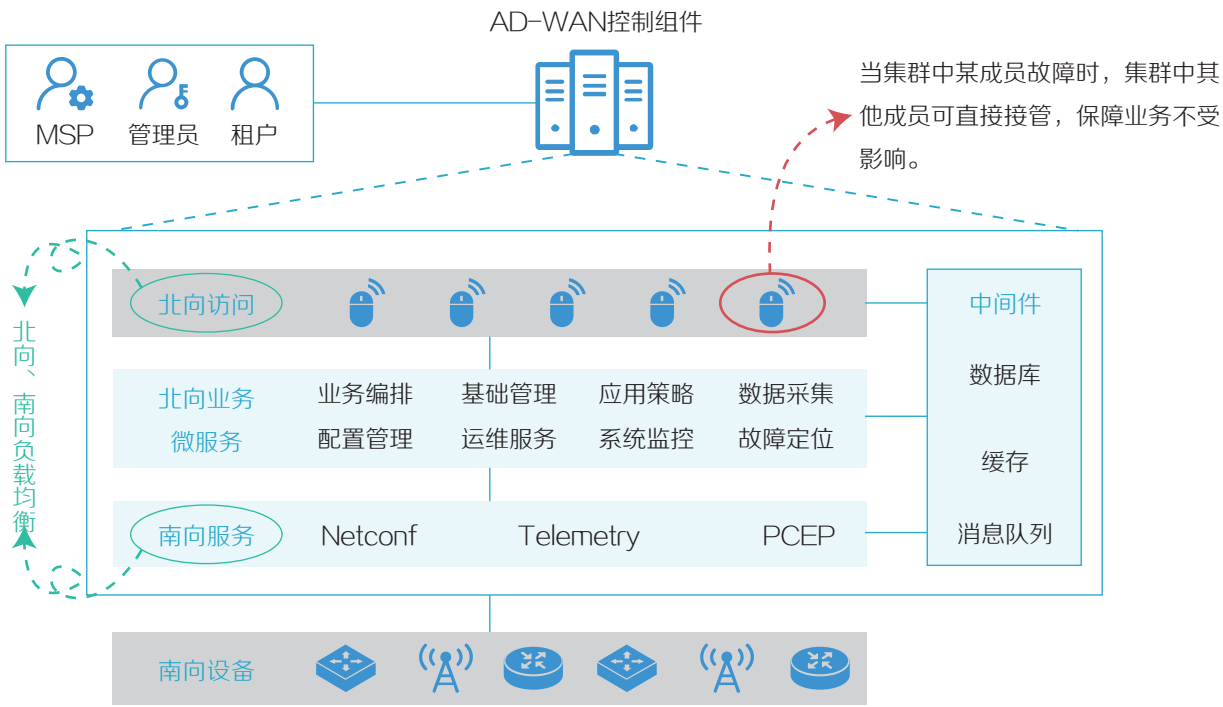
异地灾备

异地容灾系统是指处于异地的两个站点之间做主备容灾，每个站点都是一套完整的集群系统。



本地集群高可靠

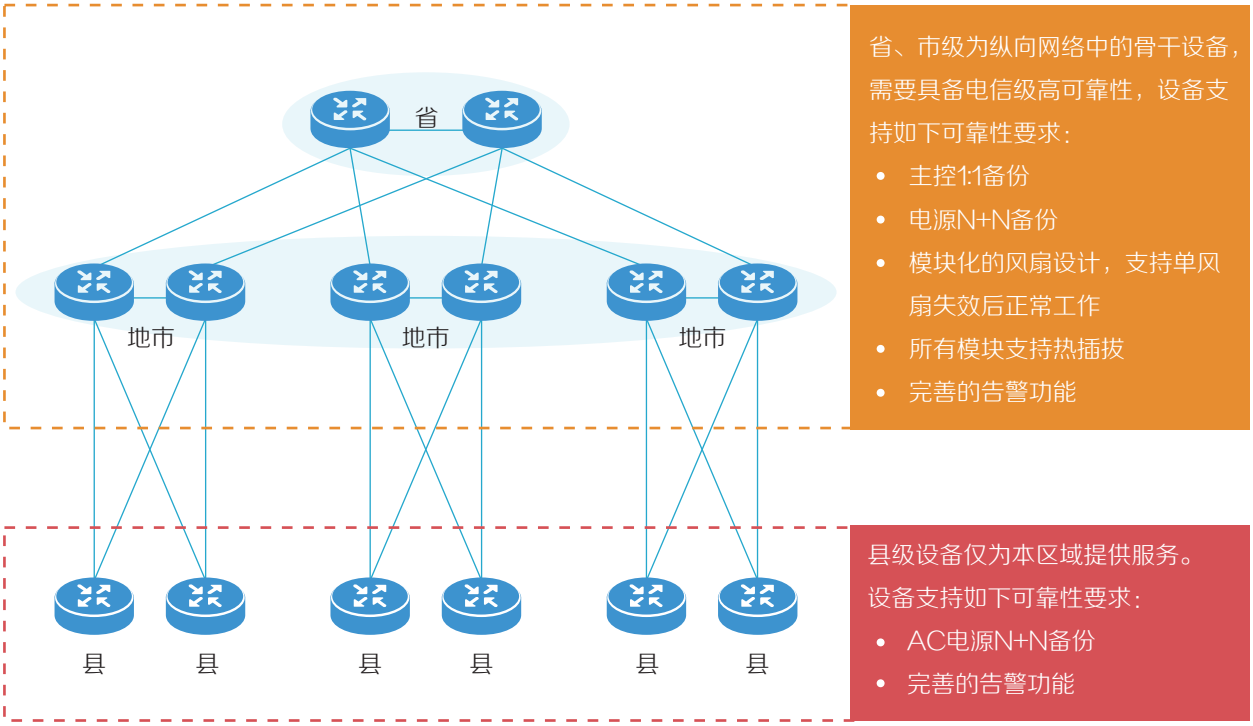
集群由3+N台服务器组成，互为备份。关键微服务在多个集群成员上冗余部署，业务共享数据。



硬件/网络高可靠

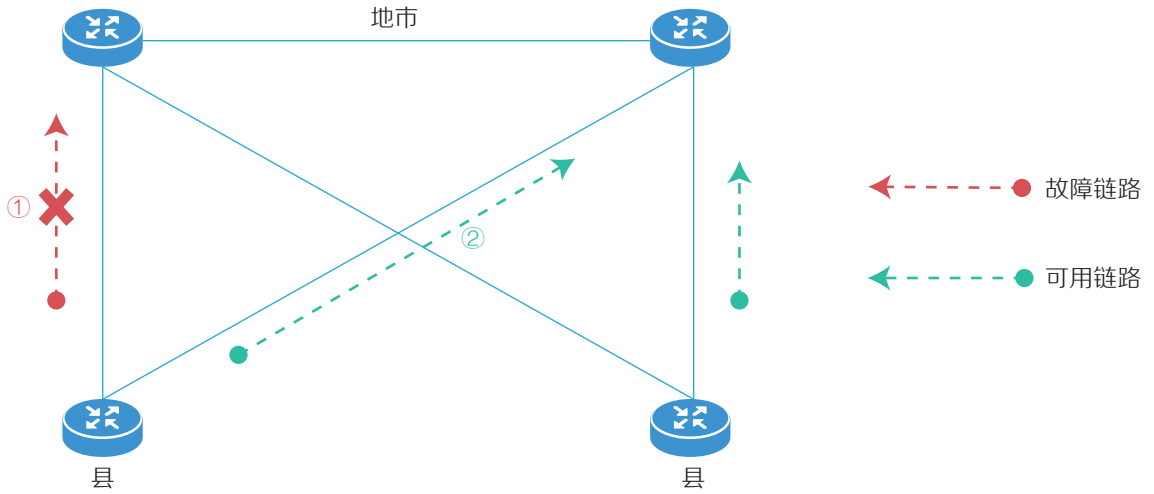
设备高可靠

设备级可靠性是保障网络服务可用的关键，AD-WAN解决方案常用的可靠性技术包括热插拔、冗余备份和不间断路由NSR等。这些技术一方面可以提供组件的冗余备份，另一方面可以保证设备出现故障时业务能够不间断转发。



链路高可靠

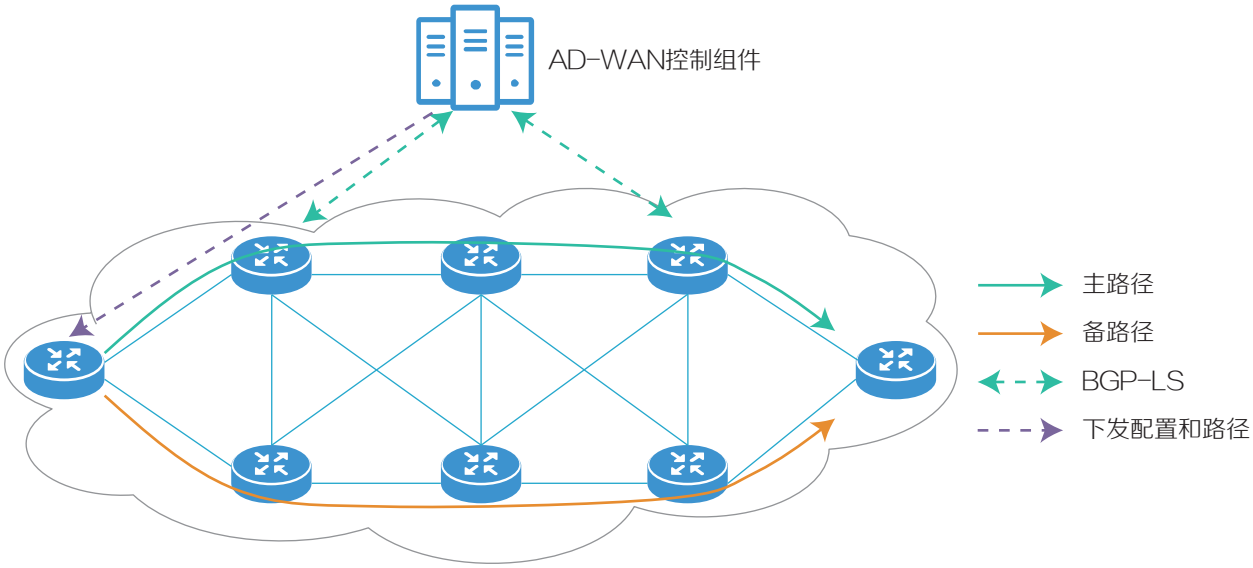
在AD-WAN解决方案中，各级节点间通过双链路互联，实现主备和负载分担，具备1+1保护能力。



业务高可靠

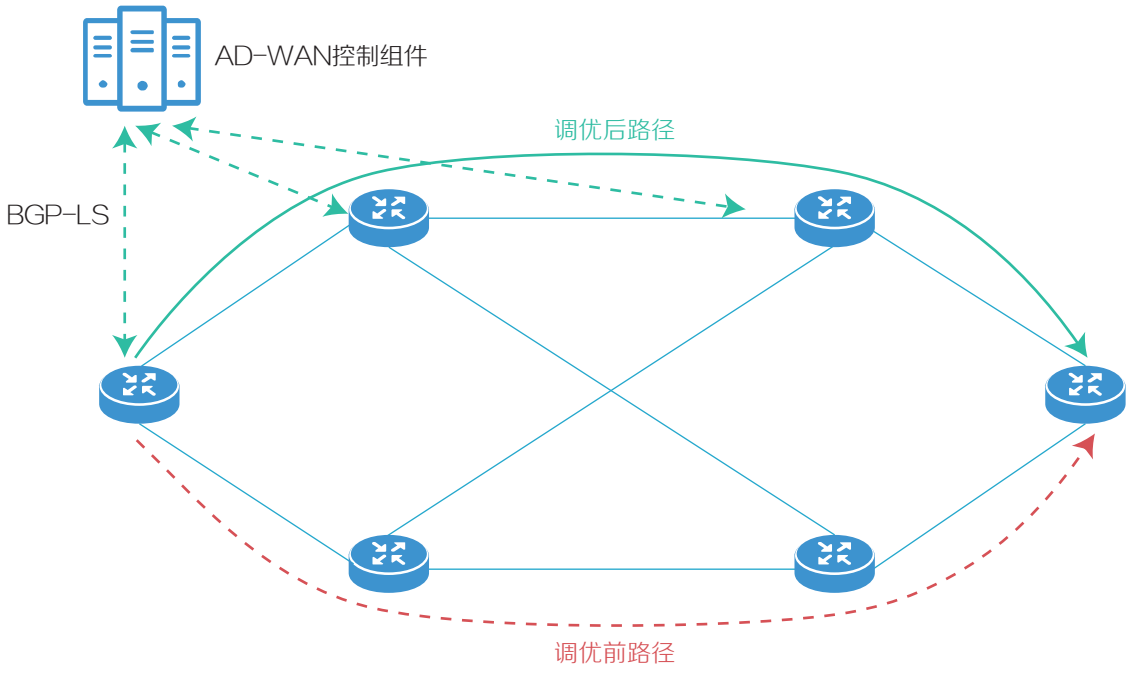
转发高可靠

针对重要业务部署主备路径的方式提供路径可靠性，并部署BFD实时检测主备路径的连通性，一旦发现主路径发生故障，会由设备立即自主切换到备份路径，无需控制组件干预，保证了主备切换的实时性。随后控制组件通过BGP-LS感知到网络侧拓扑变化后，会重新为应用计算最优的主备路径，并将优化后的主备路径下发到设备上，这样设备上会一直同时存在两条路径，保证应用转发路径可靠性。



SLA高可靠

AD-WAN实时检测网络状况，当部分链路质量劣变、带宽超阈值、隧道状态变化等因素触发调优，控制组件主动调整设备头节点业务转发路径。控制组件通过实时采集，实现高效调度，保证业务转发不丢包。



技术价值

集中管理

通过本地集群和异地容灾系统对所有设备进行远程管理和配置，提高网络管理的效率和准确性，提高网络的可靠性。

灵活SLA策略

灵活的SLA策略可以根据不同的应用需求，对网络资源进行智能分配和调整，提高网络的冗余性和可用性，从而保证网络的高可靠性。

弹性网络

支持灵活的网络拓扑结构，能够快速适应网络拓扑变化。在实际应用中，可以根据实际的网络状况进行动态调整，使网络具有更强的适应性和可靠性。

AD-WAN承载网

GIS地图

简介

过去系统的首页大屏只支持展示静态地图，且设备位置只能配置省、市和区/县。为了满足用户需要更加精确（经纬度）的设备位置的需求， AD-WAN方案全新推出GIS（地理信息系统，Geographic Information System）地图功能。

功能介绍

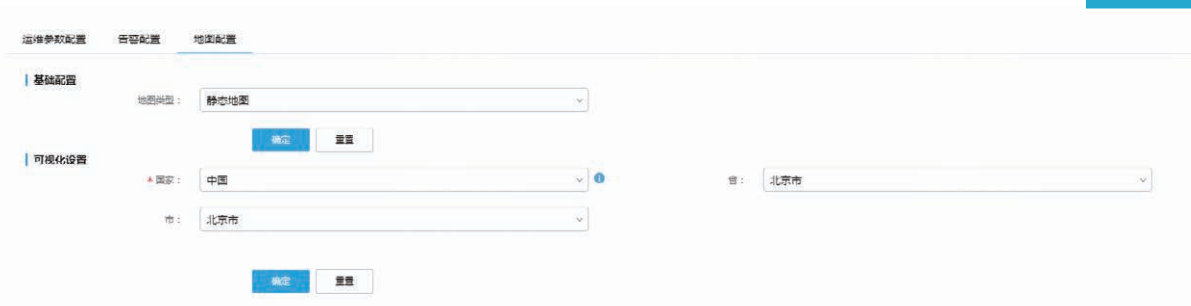
地图配置

用户可根据需要选择静态地图或百度地图：

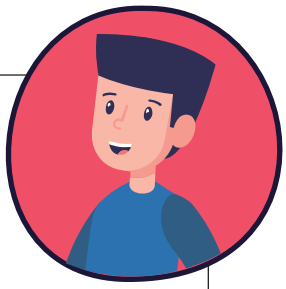
- 静态地图为AD-WAN控制组件首页大屏原有的地图。
- 百度地图依赖百度地图开放平台，需申请百度地图APIKey授权使用。

目前AD-WAN承载网方案中，GIS地图暂只支持百度地图。

静态地图



百度地图



两种地图类型均可设置地图初始展示区域：

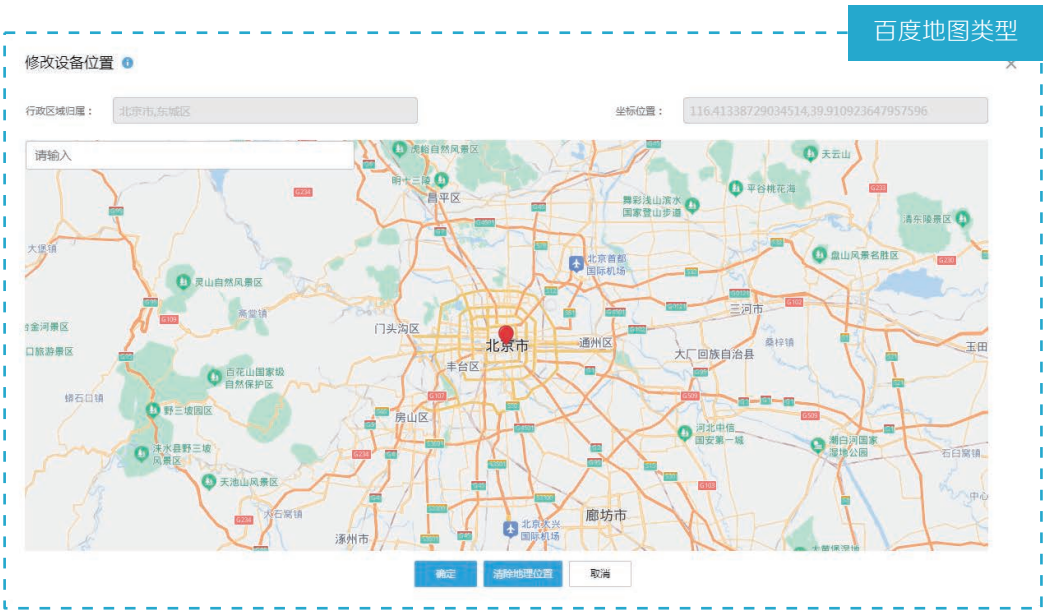
- 静态地图：使用所属行政区域记录设备的位置。
- 百度地图：使用经纬度定位记录设备的位置。通过缩放地图或标点，记录用户选择的设备初始位置和地图展示比例。

设备位置配置

静态地图类型：通过静态下拉选项配置设备地理位置。

静态地图类型

百度地图类型：可在地图上移动设备标点修改设备的位置信息；也可直接输入地点，根据提示配置设备地理位置。



百度地图可以兼容静态地图设置的位置，系统地图版本升级后，设备位置无需重新配置。

大屏GIS地图

设备位置标点展示：GIS地图标通过标点展示设备位置。

静态地图中，设备的位置是行政区域地址，地图中设备标点显示在对应的行政区域内。

百度地图中，设备的位置是经纬度地址，地图中设备标点显示在对应的经纬度坐标上。

设备状态及链路情况展示：设备状态通过GIS地图标点的不同颜色来直观展示；GIS地图标点的连线体现设备间链路情况，连线颜色体现链路状态，连线方向代表设备间链路的方向。

静态地图类型

通过GIS地图，用户可轻松掌握当前系统中的设备及链路的运行状态。

绿色—正常
灰色—下线
黄色—次要告警
红色—重要告警

百度地图类型

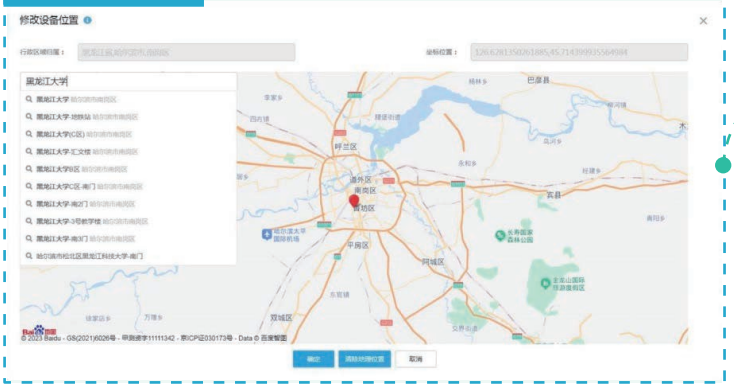
设备标点聚合：一个区域附近相邻的设备标点展示为一个带数字的聚合点，数字代表聚合设备的数量。缩小或放大地图，地图会根据聚合半径展示会聚的点。

静态地图类型

百度地图类型

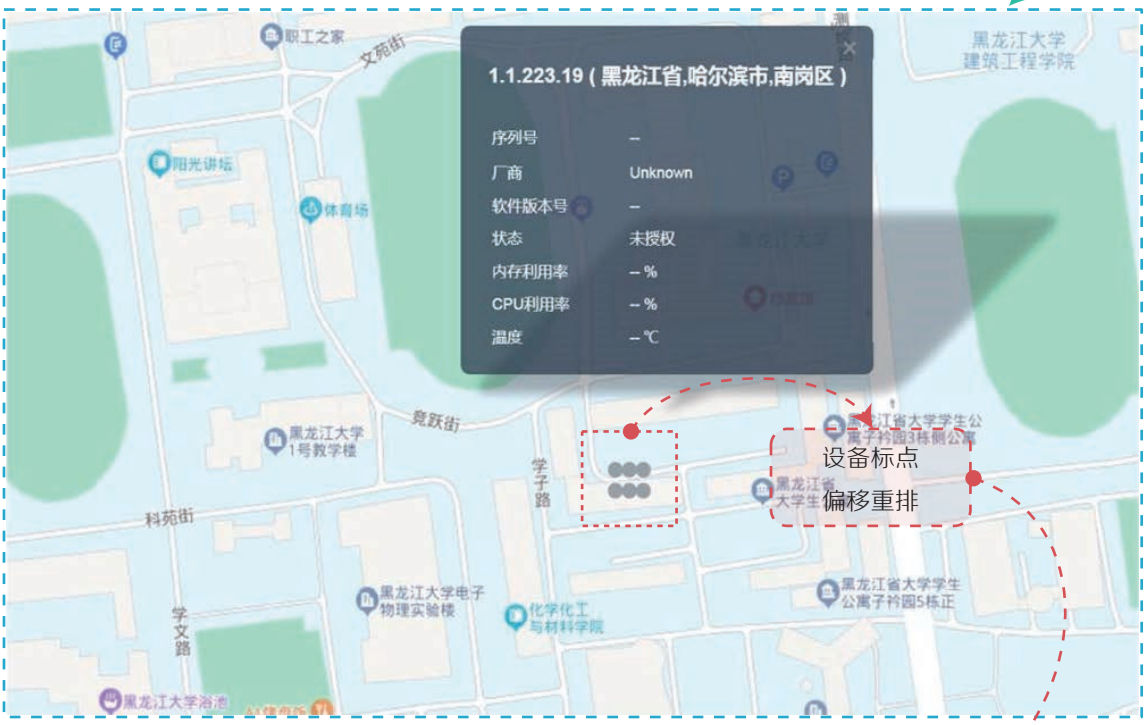
设备地理地址相邻点偏移重排：设备的经纬度在非常接近或者重复时，系统会自动将经纬度过近的标点偏移一定的经纬度重新排列展示，避免设备标点重叠的情况。

百度地图类型

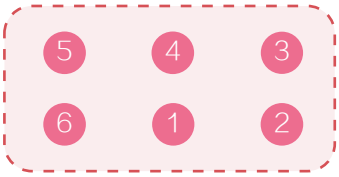


修改设备
地理位置

例如：将六台设备的地理位置改为同一地点。



静态地图类型



相同位置的设备，从第二个开始围绕第一个设备位置做上图所示偏移。

方案亮点

简单易用

用户界面配置简单，适用性广。

精确位置

经纬度展示设备位置，精准详细。

数据可视

用户可轻松掌握当前网络及资源的实时状态。

AD-WAN承载网

U盘开局

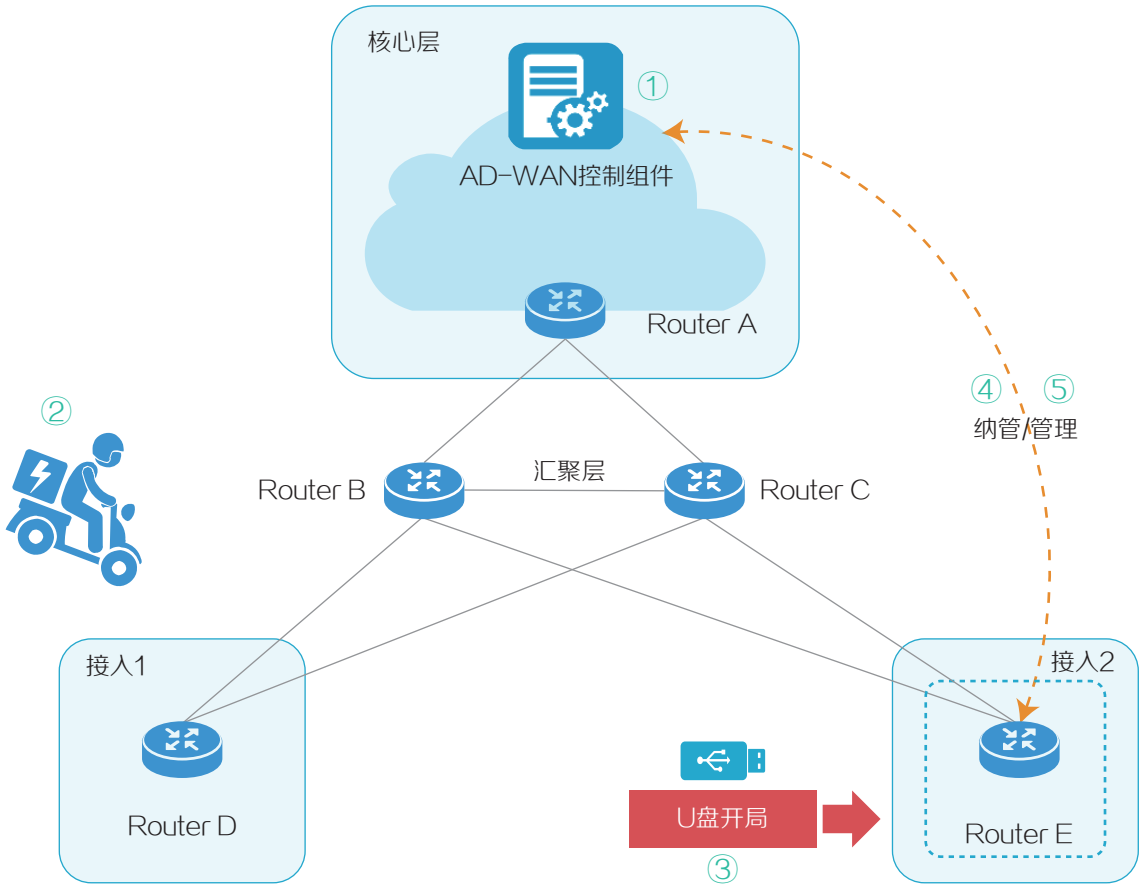
简介

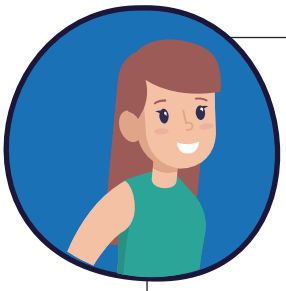
传统承载网方案开局时，设备完成安装后，由于方案整体涉及的设备配置较多，且部分配置暂不支持自动化，需手工配置，配置复杂且易出错，需具有一定技术能力的人员现场开局，这大大增加了项目费用。

方案介绍

U盘开局是H3C推出的极简开局方案功能。支持用户根据组网规划，自动生成U盘开局配置文件。用户根据设备名称取出开局配置文件，拷贝至U盘，然后将U盘插入对应空配置的设备，启动设备，完成U盘开局。

整个过程无需技术人员到现场进行开局配置，大大简化了开局过程，极大地降低了开局成本。

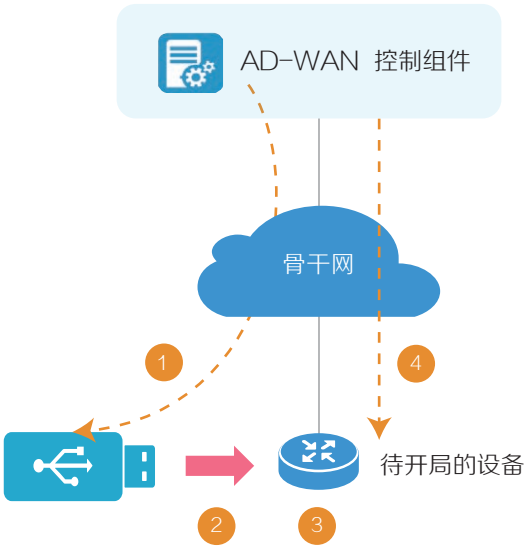




① 设备定义：管理员在AD-WAN控制组件上定义可管理设备列表。
② 设备运输：设备运送至现场，上电启动。
③ 初始配置：使用U盘开局方式完成设备初始配置。
④ 控制通道建立：管理员使用控制组件纳管设备，控制组件主动与设备建立NETCONF连接通道。
⑤ 控制管理： AD-WAN控制组件远程管理设备。

功能介绍

开局流程

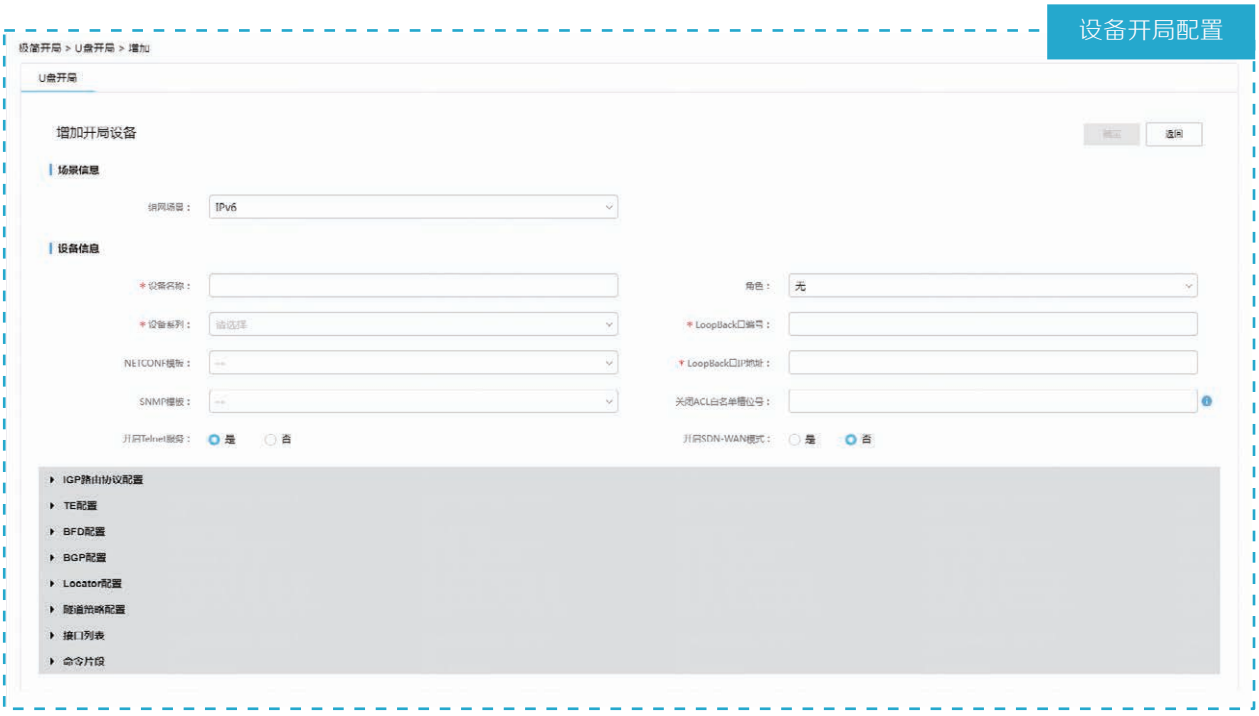


① 管理员在AD-WAN控制组件上生成开局配置文件，拷贝至U盘。
② 开局人员携带开局U盘至开局现场，将U盘插入设备，给设备上电。（U盘亦可通过邮寄到达开局现场。）
③ 设备启动时自动读取U盘中携带的开局配置进行初始配置。
④ 控制组件纳管设备并主动与设备建立NETCONF连接通道，进行远程管理。

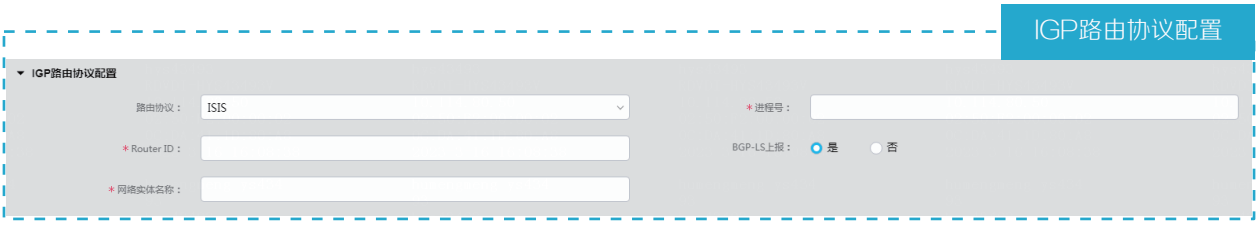
功能页面

查看U盘开局设备列表，页面支持批量导入设备配置、预览设备配置、批量下载设备配置。

手动配置设备开局配置文件：在增加开局设备配置页面，选择对应的组网场景，填写设备开局配置信息。

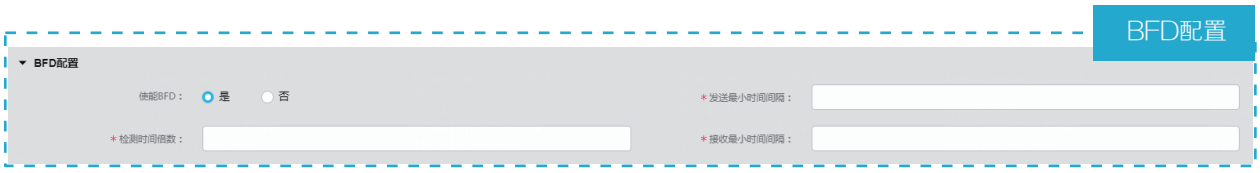


配置设备的IGP信息，包括路由协议、进程号、BGP-LS上报等。



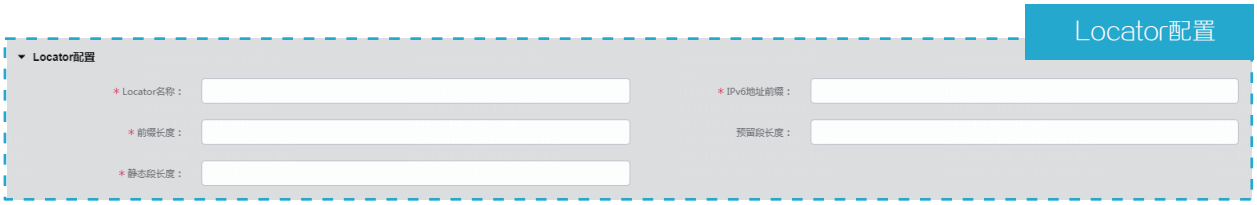
配置设备的TE信息。

配置设备的BFD信息，包括是否使能BFD及发送最小时间间隔、接收最小时间间隔、检测时间倍数。



配置设备的BGP信息，包括AS号、BGP Router ID、本地网段发布路由和邻居列表，邻居列表包括邻居IP、邻居AS号、连接口、邻居类型等。

配置设备的Locator信息，包括Locator名称、IPv6地址前缀、前缀长度、预留段长度、静态段长度。



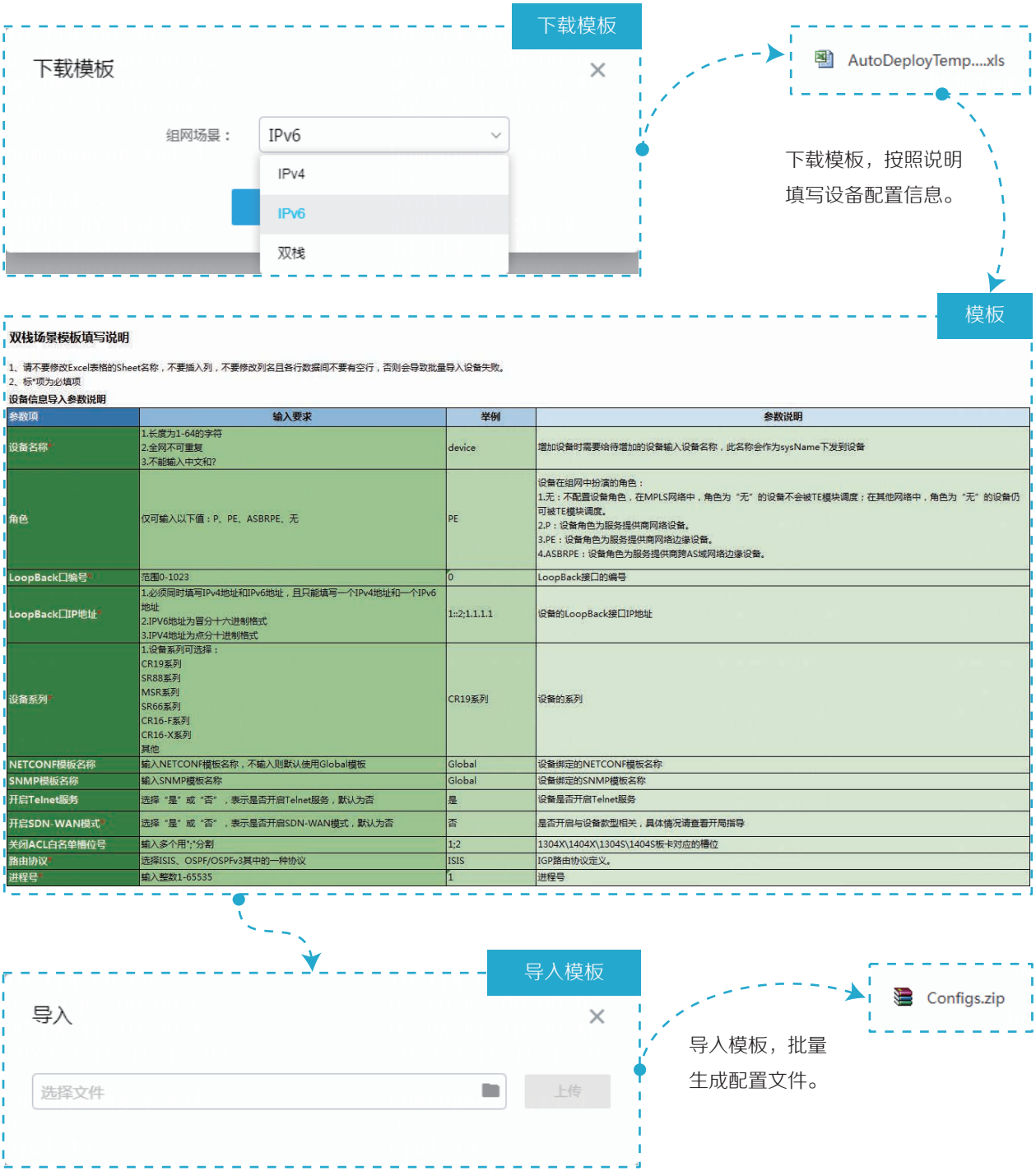
配置设备的隧道策略信息，包括隧道策略名称、负载分担的隧道策略类型、负载分担的隧道数目。

配置设备的接口信息，包括必填项接口名称、接口IP地址/掩码、接入网络名称等。

配置设备的命令信息。

用户在上述页面按需进行配置，选择需进行开局的设备，下载对应的开局配置文件，拷贝至U盘，插入对应待开局的空配置设备，完成开局。

U盘开局支持批量导入操作，可通过导入填写好的模板，批量导入设备配置信息，减少用户在控制组件页面的重复操作。



待开局设备即将使用的开局配置文件，若选择批量生成方式，建议在配置时将文件名赋予对应的设备信息，便于区分。

U盘开局功能支持以设备命令行的形式预览对应设备的开局配置信息。

通过开局预览，可直接阅读设备的开局配置，方便确认当前设备开局配置的正确性。

方案亮点

降低技术要求

管理员无需前往现场即可远程完成设备开局，界面图形化操作，简化流程，降低开局人员技术要求，非专业技术人员现场操作“0”门槛。

减少运营成本

免去人员差旅食宿等现场开局成本，节省人力、物力和财力，降低企业运营成本。

缩短开局时间

设备可批量进行配置，减少用户重复操作次数，大大缩短开局时间。

AD-WAN承载网

健康检查

简介

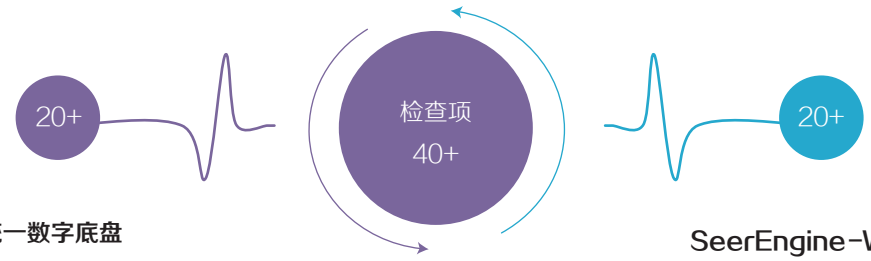
在传统网络运维的过程中，为了掌握和了解当前网络和管理系统的状态，需要运维人员手工去后台收集对应的系统数据和网络数据，并将收集到的数据交由专业人员进行分析比对处理。这种方式对于用户来说，非常不方便操作，且不能及时了解当前系统的运行状态及业务状态，无法预知和预防异常情况。

健康检查功能用于AD-WAN进行健康性检查的相关事项，检查控制组件运行依赖的集群等基础服务的运行情况，以及设备、虚拟网络等用户业务的运行情况，并生成相关的检查报告，以此提高整体运维效率。

立即检查，可根据用户需要，随时进行检查。立即生成检查报告。

支持按天/周/月和检查时间设置自动检查周期，系统定时进行检查，反馈检查报告。

检查项丰富多样



统一数字底盘

统一数字底盘运行环境、Pod运行情况、License 状态、容器平台等健康性检查

SeerEngine-WAN

控制组件运行状态、关键进程、关键端口、设备等健康性检查

统一数字底盘检查项

编号	检查结果	检查项名称
1.1.1	正常	检查各集群主机节点的运行负载是否过高
1.1.2	正常	检查安装路径空间
1.1.3	正常	检查设备的繁忙程度是否正常
1.1.4	正常	时钟健康检查
1.1.5	正常	检查各节点间系统时间差
1.1.6	正常	umask检查
1.1.7	正常	节点关键文件检查
1.1.8	正常	部署规格检查
1.1.9	正常	检查版本信息
1.1.10	正常	检查License信息
2.1.1	正常	默认路由检查
2.1.2	正常	防火墙状态检查
2.1.3	正常	SELinux配置检查
2.1.4	正常	检查网络质量
2.1.5	正常	SSH端口检查
2.1.6	正常	Matrix端口冲突检查
2.1.7	正常	Conntrack表项检查
2.1.8	正常	ETCD网络性能检查
3.1.1	正常	检查各pod资源情况
3.1.2	正常	检查kafka是否正常
3.1.3	正常	检查GFS空间使用率
4.1.1	正常	检查PXC节点运行情况以及公共表空间大小

SeerEngine-WAN检查项

基础服务型 检查失败 0 | 异常 0 | 存在风险 0 | 人工确认 0 | 正常 3

SeerEngine-WAN 检查失败 0 | 异常 0 | 存在风险 0 | 人工确认 0 | 正常 3

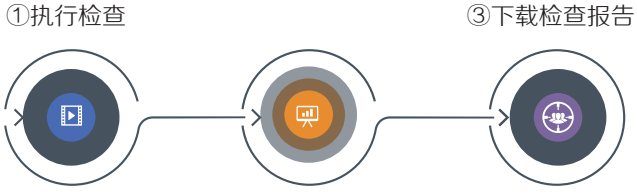
编号	检查结果	检查项名称
1	正常	集群信息
2	正常	MongoDB数据库连接
3	正常	License分配及使用

业务数据型 检查失败 0 | 异常 0 | 存在风险 0 | 人工确认 0 | 正常 18

SeerEngine-WAN 检查失败 0 | 异常 0 | 存在风险 0 | 人工确认 0 | 正常 18

编号	检查结果	检查项名称
4	正常	设备状态
5	正常	LAN接口状态
6	正常	设备板卡
7	正常	链路状态
8	正常	BGP邻居状态
9	正常	静态邻接标签状态
10	正常	动态邻接标签状态
11	正常	EPE标签状态
12	正常	节点标签状态
13	正常	应用组检查
14	正常	告警管理
15	正常	配置审计
16	正常	SRv6 locator状态
17	正常	链路SID状态
18	正常	节点SID状态
19	正常	Tunnel状态
20	正常	SRv6 Policy状态
21	正常	SR policy状态

检查流程

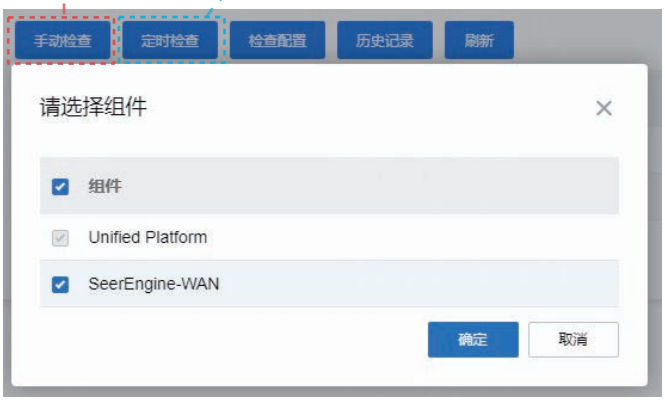


执行检查

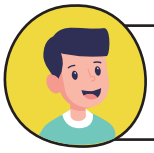
根据用户需求选择检查方式执行检查。

立即执行检查，立即生成检查历史记录；可快速查看检查详情；下载检查报告。

按需配置定时检查任务，系统将按周期进行自动检查。

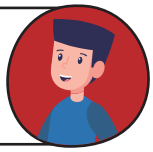


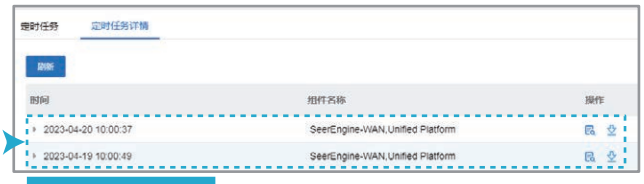
举个栗子



当用户需要立即排查系统中可能存在的异常情况时，可选择“手动检查”方式。

当用户需定时排查系统中的异常情况时，可选择“定时检查”方式。配置定时检查任务，频率选择“每天”，固定检查时间为“10”点，则用户每天可在固定时间段查询到新的检查记录。





定时检查记录

检查结果

执行检查后，系统将生成检查历史记录。在检查结果报告可查看指定组件检查记录的详细检查结果。针对存在风险的检查项，可查看执行结果详情，同时系统会给出相应处理意见。

01 历史记录

02 检查详情

03 下载检查报告

系统支持下载检查报告，报告为html格式。

方案亮点

全面覆盖

多维度检查，从系统型、服务型、业务型全方位覆盖反映整体健康情况。

检查丰富

支持状态、资源、设备、业务类等丰富多样的检查项。

快速检查

无需“等待”，立即执行检查，快速掌握整个系统的健康情况。用户可根据需要灵活选择手动检查或自动检查。

AD-WAN承载网

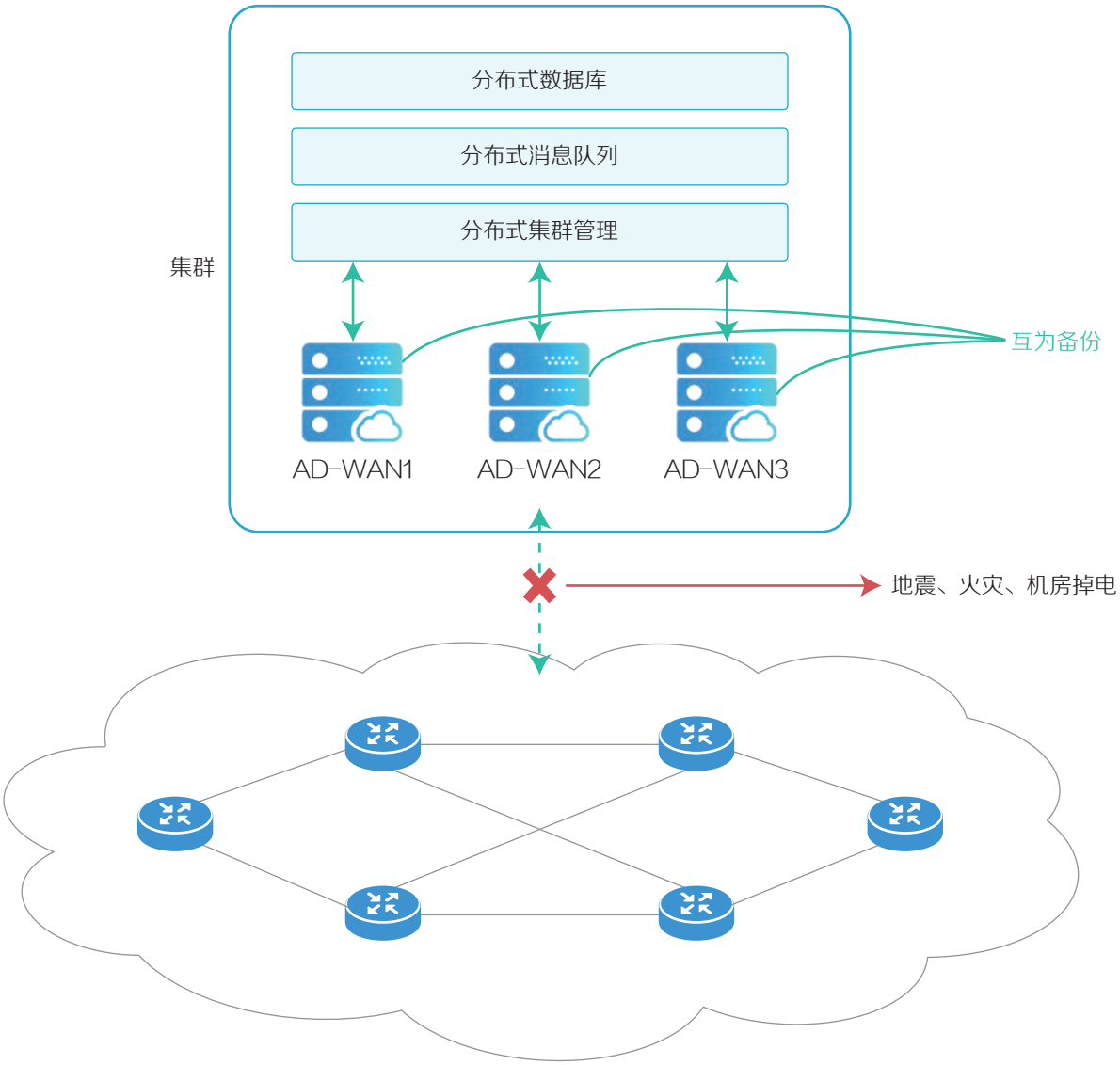
异地容灾

功能简介

技术背景

传统的集群可靠性方案，可以解决集群内部单节点异常时的故障问题。当发生地震、火灾、机房掉电等故障，导致整个集群不可用时，需要使用异地容灾方案来保障业务可用性。

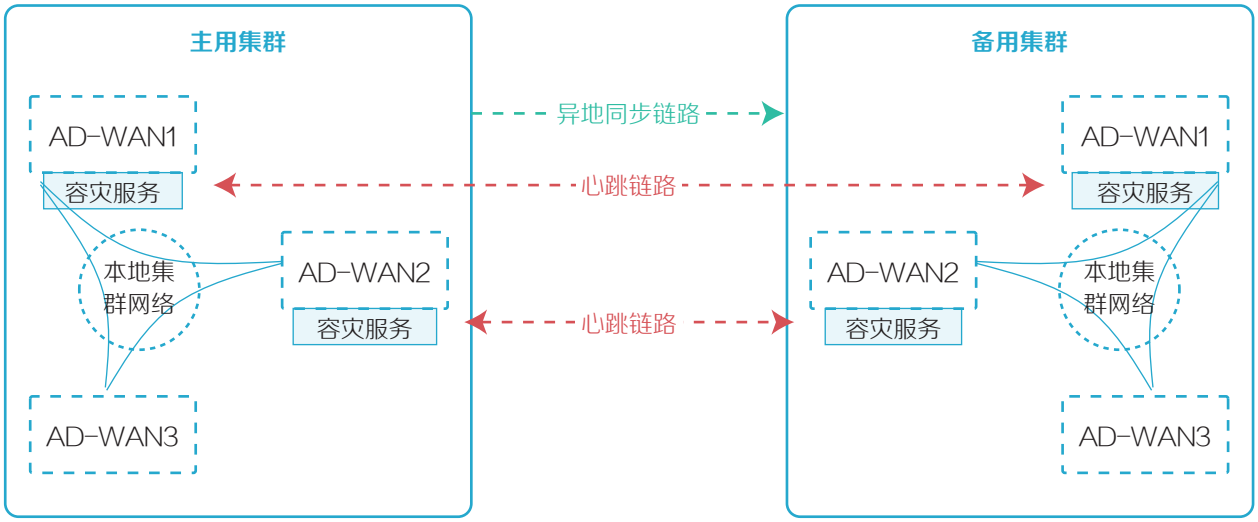
方案介绍



功能简介

异地灾备是一种更完备的容灾部署方式，用户需要在原有集群基础上，再额外增加一套相同的物理服务器，作为备份集群存在。用户通过在异地部署一套同样配置的集群，并和已有的集群配置容灾关系，实现在主集群遭到灾难性事件影响时，快速切换至备集群以确保业务可用性和数据安全。

异地容灾系统模型



基本原理

异地容灾方案，提供故障探测机制和仲裁服务。容灾系统会探测原有主用集群是否出现故障，包括节点故障、链路故障、以及服务故障。

通过心跳链路可以观察到原有主用集群是否发生故障。当原有主用集群出现故障时，通过手动或者自动切换方式，系统能够快速无缝地切换到备用集群上，备用集群升级为主用集群继续提供服务。

为了避免出现主集群里的单个容灾服务自身发生故障时，误判为整个主集群故障。同一个站点里有两个容灾服务互为备份关系，单个容灾服务故障时，另一个容灾服务可以快速接管容灾业务。

容灾系统备份模式

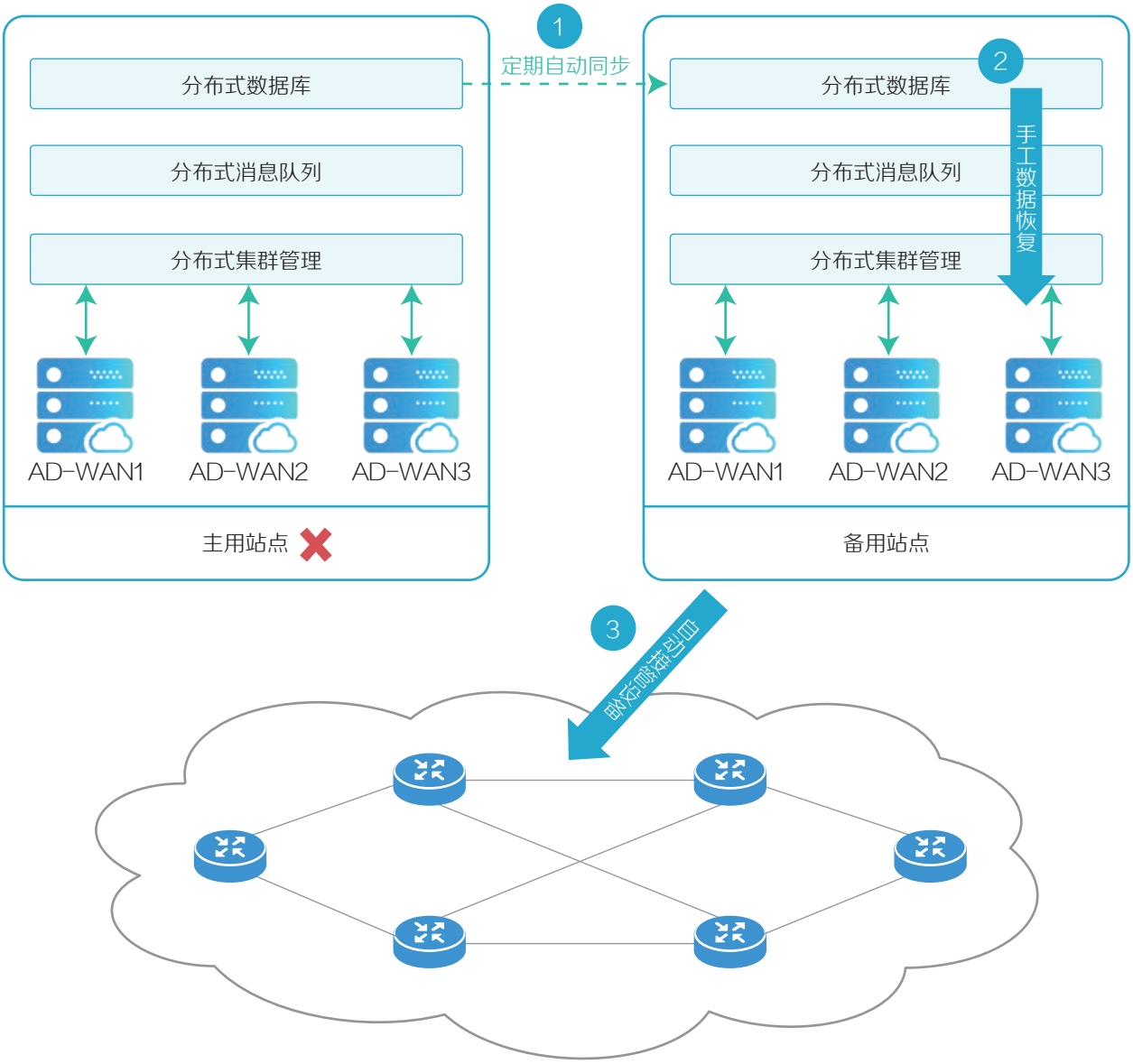
备份模式

容灾系统是由一主一备两个集群站点组成的，当主用站点出现各种故障无法工作时， 备用站点会升级为主用站点，接管所有设备，继续承担网络的管理工作，保障最大程度地缩减管理系统中断时间。容灾系统的备份模式有如下两种模式。

冷备

容灾系统不会自动监测主站点和备站点上的组件状态，由用户控制和指定组件在站点上的主用或备用状态，可以通过接管和降备功能，切换组件在站点上主用或备用状态。

AD-WAN支持冷备方式提供异地可靠性保障机制，在两地数据中心各部署一套控制组件集群，主站点处于活动状态管理广域网设备，主站点集群定期向备站点集群备份数据库。当主站点集群发生灾难性故障，管理员手工恢复数据库启动备站点集群服务，备站点集群启动后自动接管广域网设备。



热备

AD-WAN支持热备方式提供异地可靠性保障机制。在两地数据中心各部署一套控制组件集群，主站点处于活动状态管理广域网设备，主站点集群的数据是实时的，以增量方式向备站点集群进行同步。主备站点集群的切换支持两种切换模式：手工切换和带仲裁的自动切换。

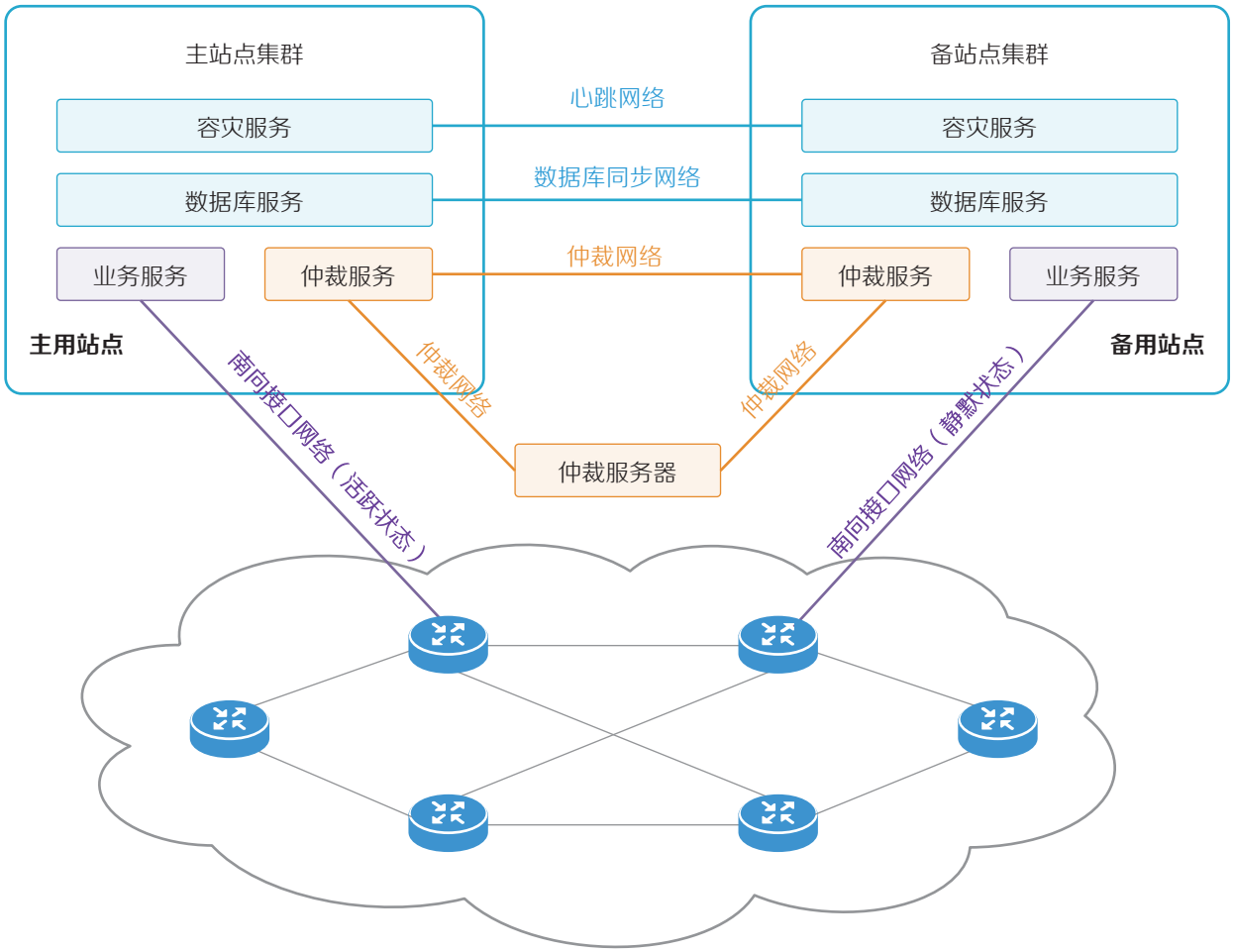
- 手工切换模式

  用户可登录主站点集群进行降备操作，完成主备集群服务的切换。当主站点集群发生故障无法登录管理页面时，可以登录备站点集群进行接管操作，同样可完成主备集群服务的切换。

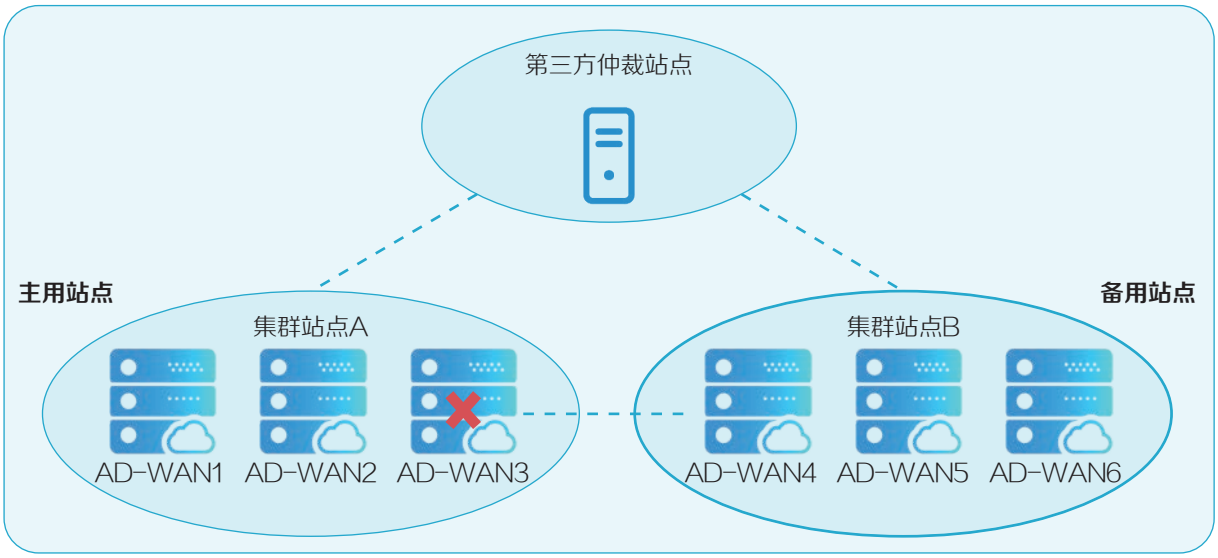
- 自动切换模式

  系统完成主备站点集群的自动切换需要部署仲裁服务器。推荐部署在第三方站点，仲裁可与主备站点集群三层路由可达，当无稳定的高可靠第三方站点选址时可以部署在备站点集群内部。当仲裁服务器探测当前主站点集群发生故障时，可以触发自动切换，整个过程不需要人工干预。该模式下，支持用户手动切换，在仲裁故障时也可进行主备站点集群切换。

如下图所示，异地容灾需要心跳网络、数据库同步网络和仲裁网络，三张网络可以复用一组IP地址。

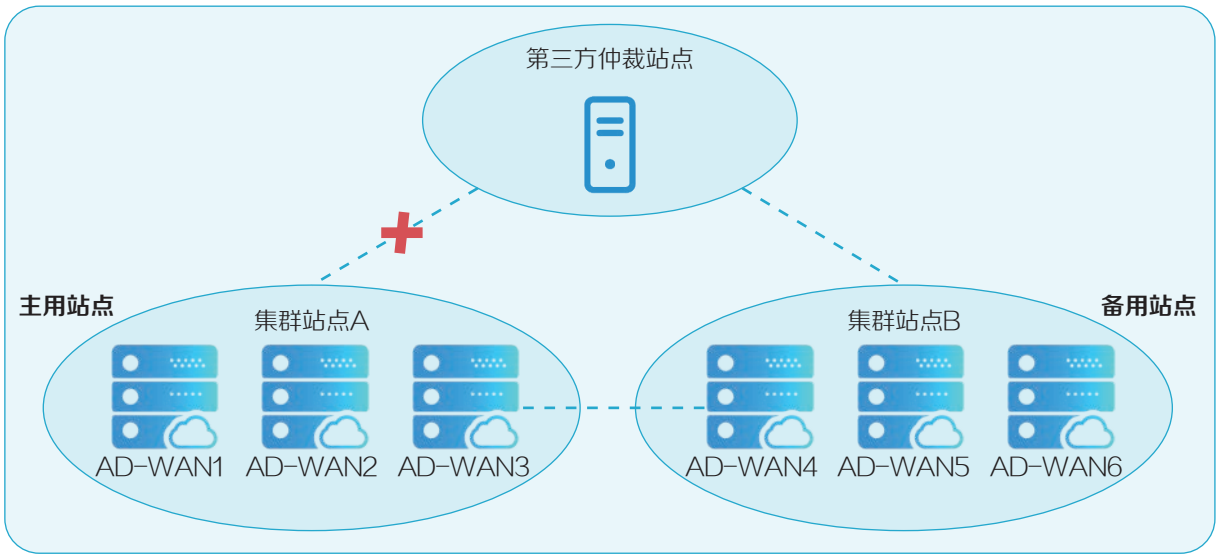


站点中的单节点故障



当容灾系统中的单个站点的单台服务器出现异常时，不会发生灾备倒换。因为在多数派的集群机制下，3台服务器组成的集群，出现一台服务器异常时，站点集群本身仍然是正常的，因此不需要进行主备站点之间的倒换。

主站点和仲裁站点的网络出现故障



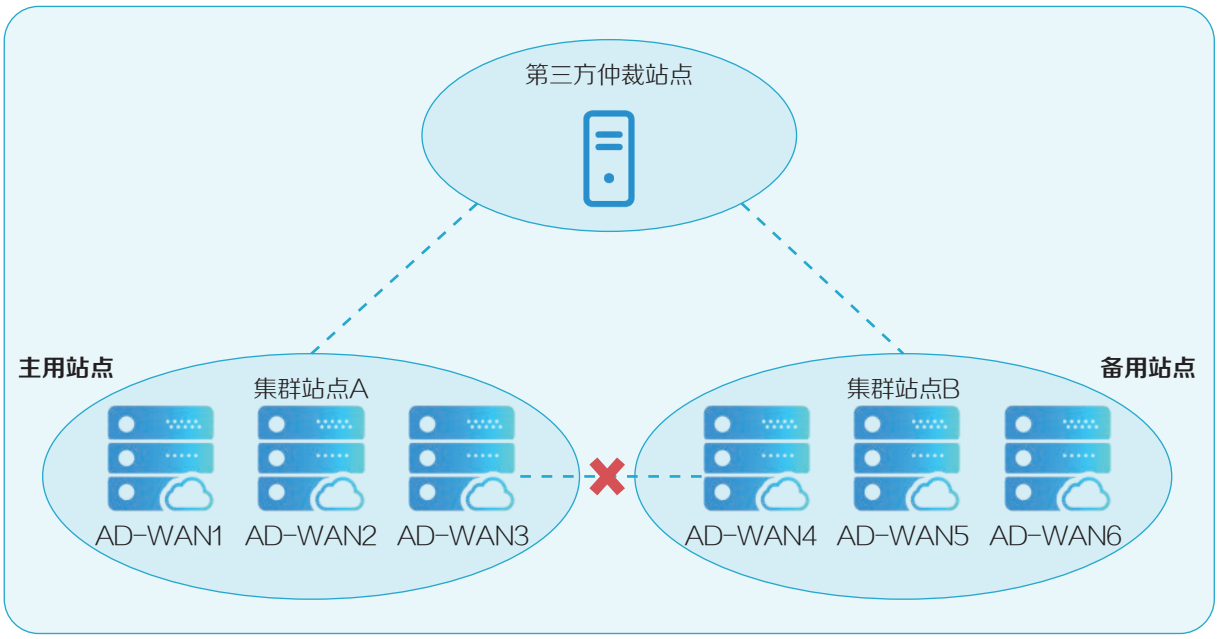
当主用站点和备用站点都能正常工作的前提下，如果主用站点和第三方仲裁站点出现网络断连的情况，不会发生主备倒换。由于主用站点仍然是能够正常工作的，仅仅是和仲裁站点失去联系，在这种情况下，仲裁节点会综合判断两点信息：

① 主用站点和仲裁站点失去联系；

② 主用站点和备用站点之间的保活心跳正常；

在这两点情况下，仲裁站点会认为主用站点仍然正常，仅仅是和自己失去了联系，不会发起倒换。

主站点和备站点的网络出现故障



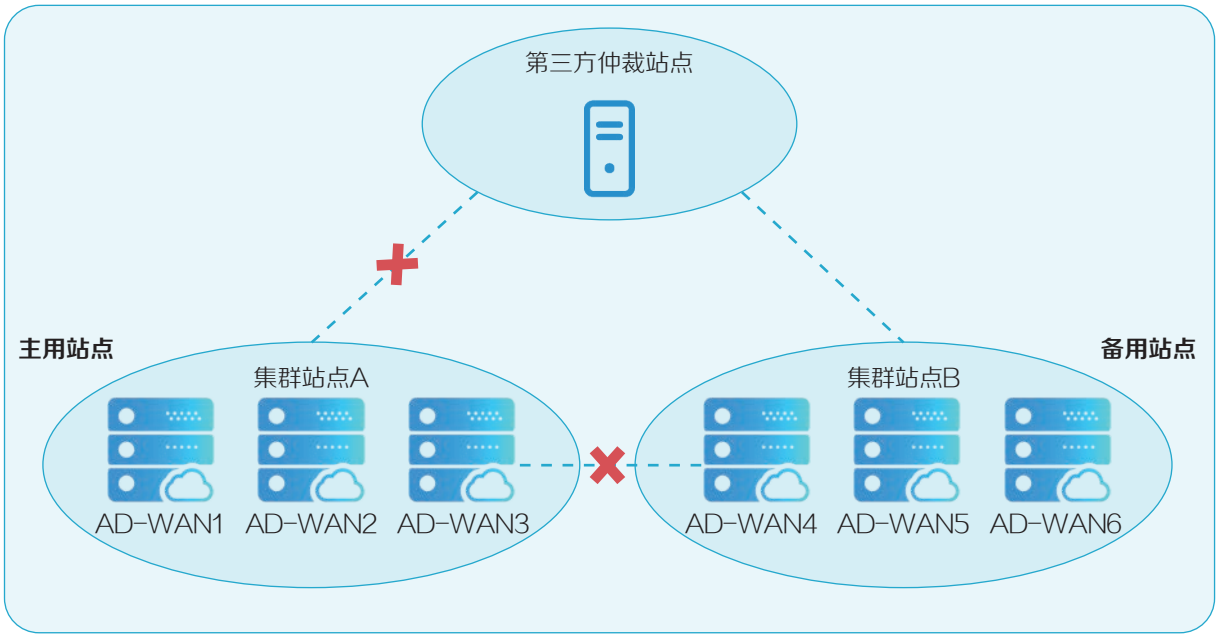
当主用站点和备用站点都能正常工作的前提下，如果主用站点和备用站点出现网络断连的情况，不会发生主备倒换。由于主用站点仍然是能够正常工作的，仅仅是和备用站点失去联系，在这种情况下，仲裁节点会综合判断两点信息：

① 主用站点和备站点失去联系；

② 主用站点和仲裁节点之间的保活心跳正常；

在这两点情况下，仲裁站点会认为主用站点仍然正常，仅仅是和备用站点失去了联系，不会发起倒换。

主站点的所有对外网络异常



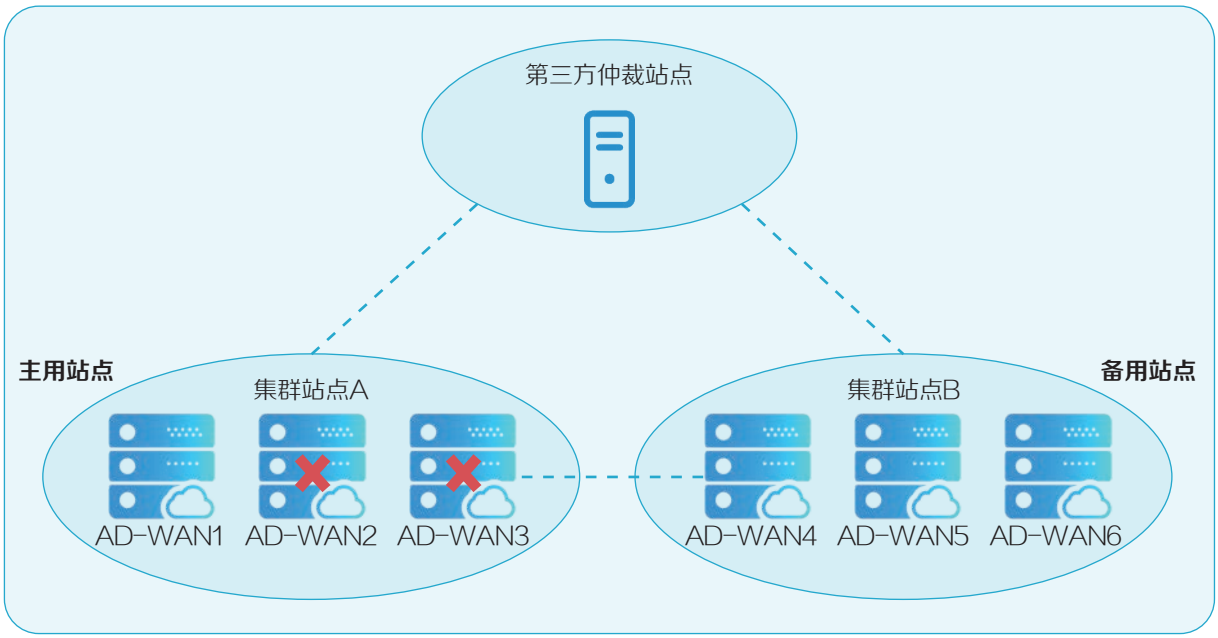
如果主用站点和第三方仲裁站点出现网络断连，同时也和备用站点出现网络断连的情况，这时仲裁站点会发起主备倒换。在这种情况下，仲裁站点同样综合判断两点信息：

① 主用站点和备站点失去联系；

② 主用站点和仲裁节点之间也失去联系，无从判断主用站点是否正常工作，但是认为主站点已经大概率出现异常，成为网络孤岛；

在这两点情况下，仲裁站点会认为主用站点出现异常，仲裁结果要求备用站点升级成为主用站点。

单站点多数派服务器异常



当容灾系统中的主站点集群出现多数节点异常，即主站点中超过一半的物理服务器出现异常，这时，主站点的集群异常，已经无法正常工作，无法响应用户请求。仲裁节点和备用站点会共同判断主站点出现异常，决策启动主备倒换。备用站点升级成为主用站点，开始工作，向设备下发配置，使设备全部重新连接到新的主站点控制器上。

主备站点之间的配置数据是实时同步的，因此设备切换控制器之后，所有业务配置会继续保持。

技术价值

高可靠性

容灾服务支持双节点部署，提高容灾核心功能可靠性，降低误报故障的概率。

灵活切换

容灾系统支持手动切换和自动切换，通过这两种方式能够快速无缝地切换到备用集群上，备用集群升级为主用集群继续提供服务。

网络丰富

容灾系统可以在IPv4、IPv6和双栈网络中为集群提供可靠性保证。

AD-WAN承载网

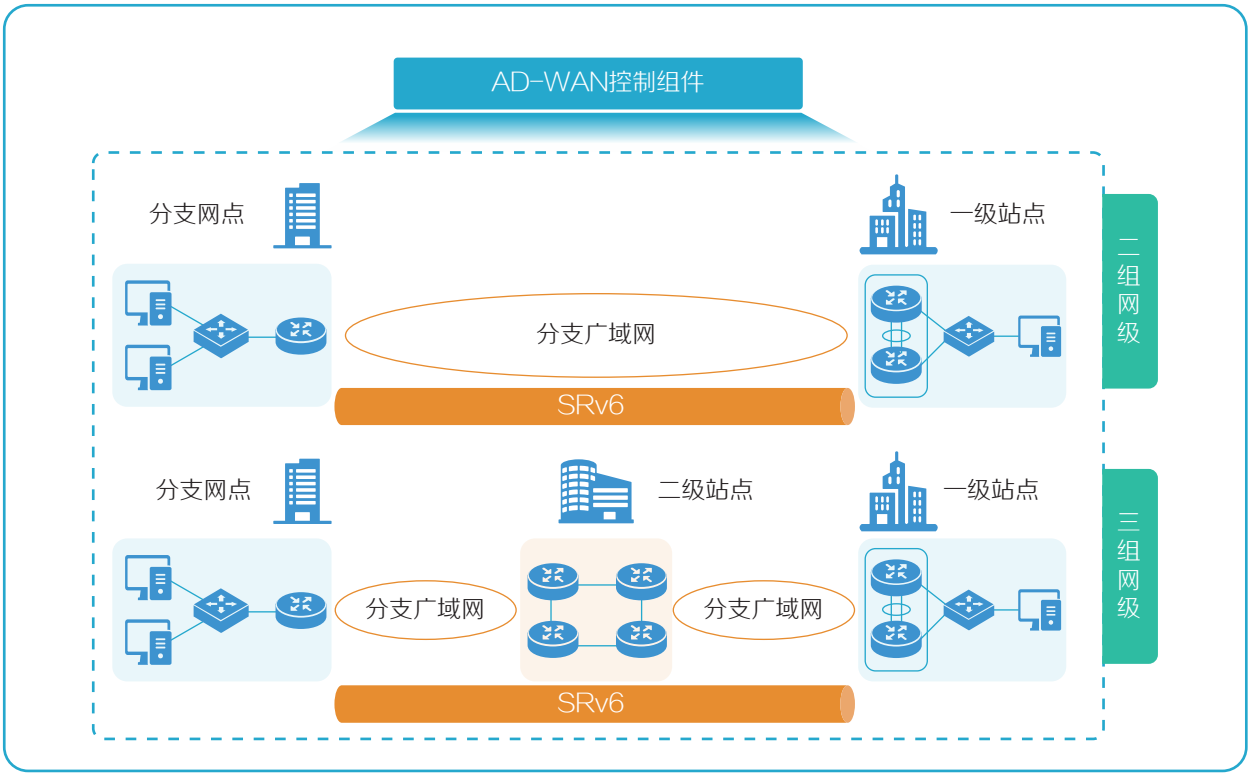
SRv6 SDWAN

方案简介

用户的SRv6骨干网已经建设完成后，当前需要开展分支SRv6网络建设。

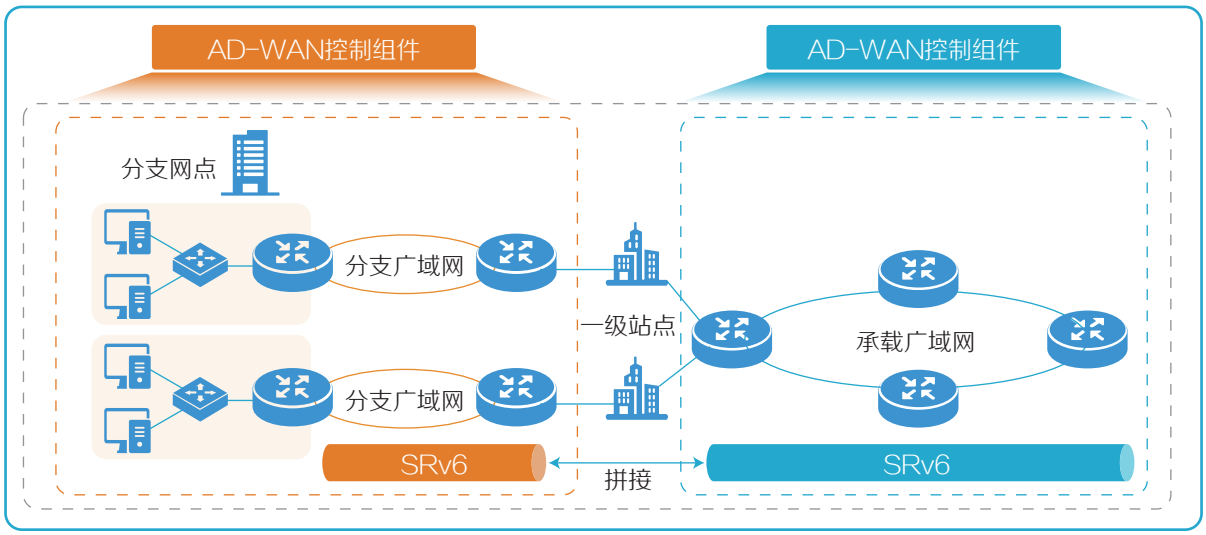
方案场景如下：

- 中小型企业分支单独建设SRv6
- 网点、各机构、总部间通过SRv6隧道一跳打通。



- 大型企业分支部署SRv6和骨干SRv6网络拼接

  以省级为单位，省内各网点、机构间通过SRv6隧道一跳打通，省内分支接入网由分支控制组件管控，骨干SRv6网络由承载控制组件管控。



方案设计

分支独立部署SRv6

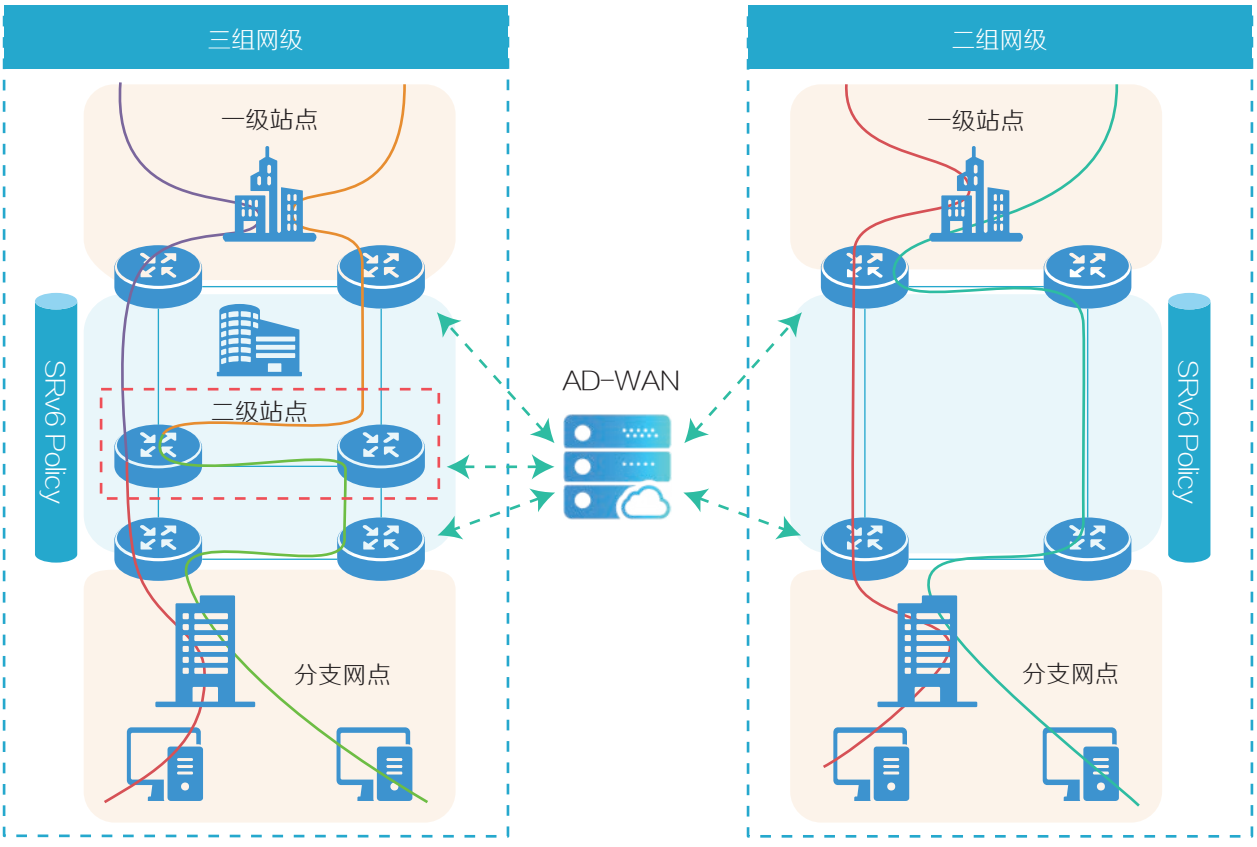
在中小型企业已建立的分支网络中部署SRv6 Policy，建立端到端转发隧道。

- **二级组网**

  控制组件下发两条SRv6 Policy做为设备头端两条SDWAN隧道；设备头端基于iFIT结果自主选择SDWAN隧道进行报文转发。

- **三级组网**

  控制组件分别在分支网点和二级站点下发两条SRv6 Policy做为设备头端两条SDWAN隧道；设备头端基于iFIT结果自主选择SDWAN隧道进行报文转发。



分支SRv6拼接承载SRv6

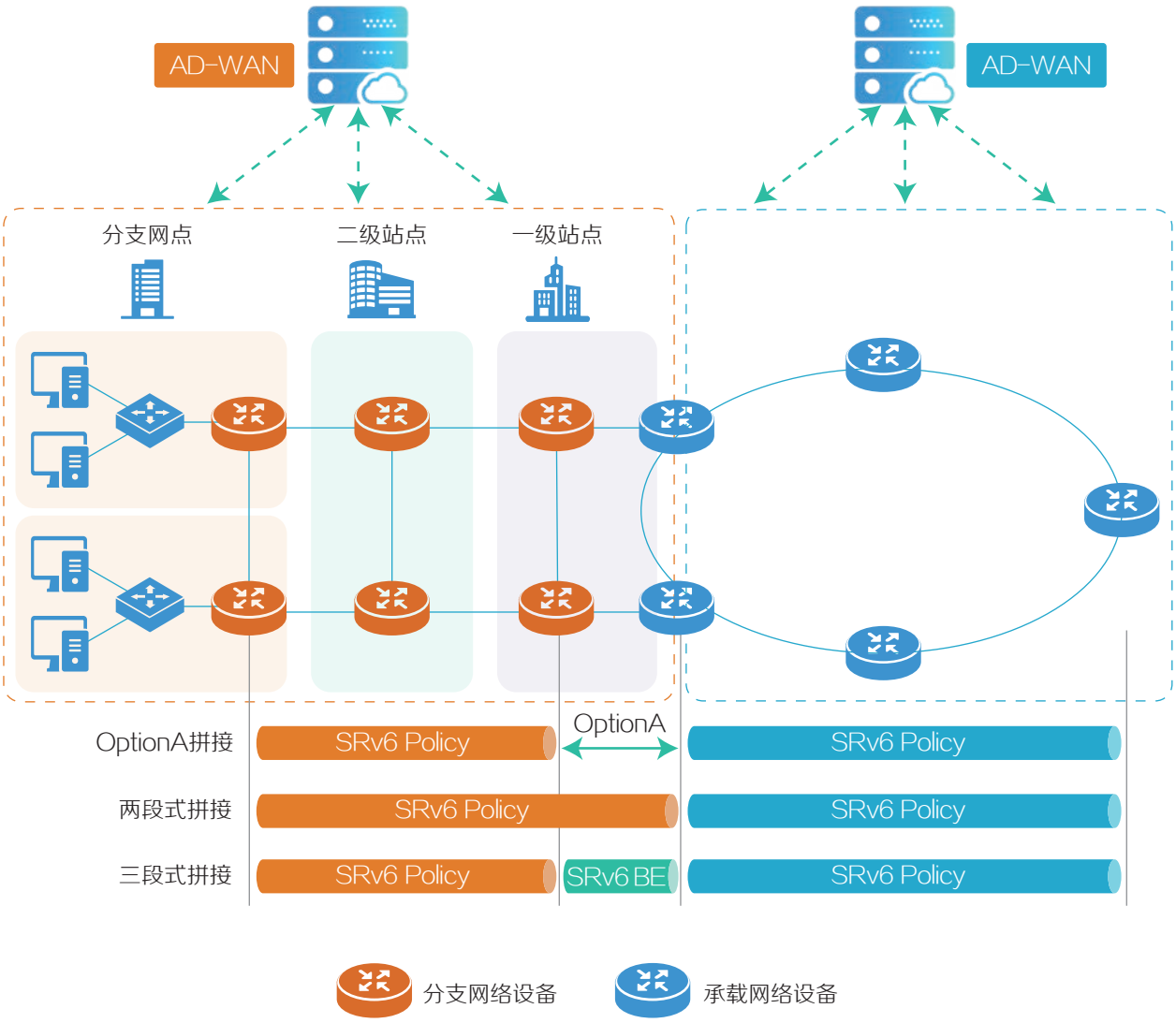
分支和承载网络区域分别部署控制组件，进行网络独立纳管。分支网络和承载网络的头节点根据iFIT检查结果智能选择SRv6 Policy隧道转发报文。

在分支网络一级站点部署下联及上联设备：

- 下联设备作为分支网络终结设备，终结SRv6业务隧道。
- 上联设备作为承载网络边缘设备，用于分支网络接入。

分支网络接入承载网络时，有以下拼接方式：

- OptionA拼接：上下联路由器间业务采用“背靠背”方式部署，通过EBGP引入业务路由，互为CE，实现跨域互通。
- 两段式拼接：上下联设备间通过路由重生成功能，实现跨域转发。
- 三段式拼接：下联设备到上联设备间、上联设备到承载网络间分别进行一次路由重生成，在上下联设备间建立SRv6 BE隧道，实现跨域转发。



技术实现

智能选路流程

隧道质量检测

在AD-WAN控制组件上部署iFIT功能，对SRv6 TE Policy隧道的性能指标进行实时测量。

隧道质量检测主要分为以下步骤：

① **数据发送**

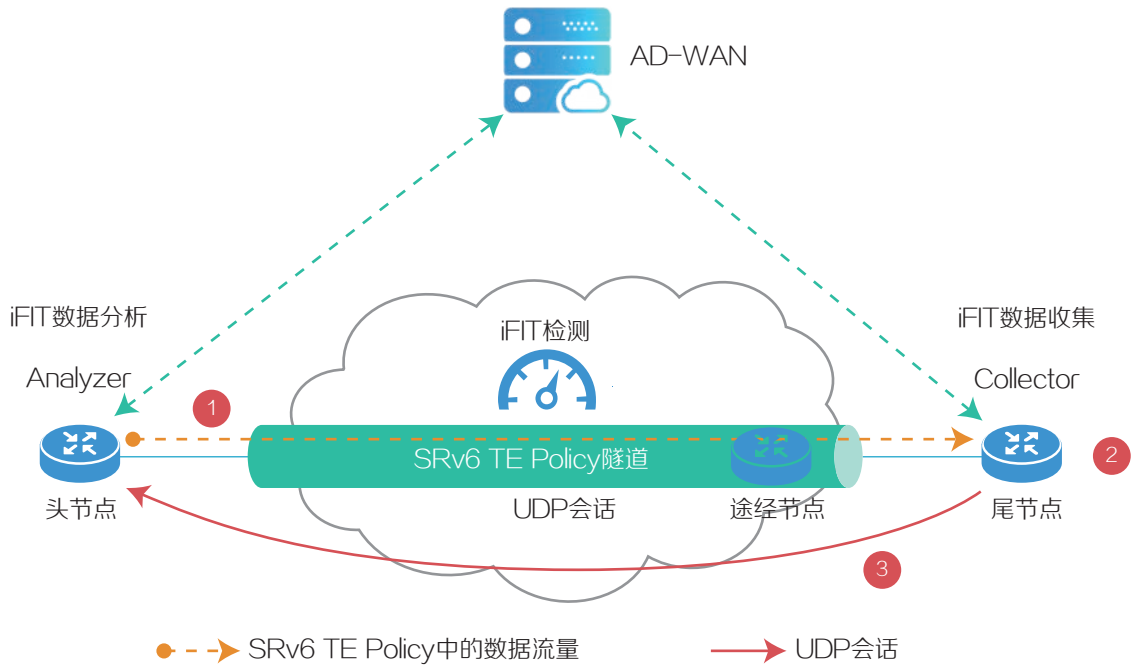
SRv6 TE Policy头节点将iFIT信息发送给尾节点，并且记录发送报文数量和时间戳等信息。

② **数据接收**

SRv6 TE Policy尾节点解析iFIT信息，并根据该信息记录接收到的报文数和接收到报文时间戳。

③ **分析计算**

尾节点作为数据接收端，将记录的接收到报文数和接收到报文时间戳通过UDP会话告知SRv6 TE Policy头节点。由SRv6 TE Policy头节点计算分析隧道的质量。



使能iFIT检测隧道质量

最优隧道计算

AD-WAN控制组件定义iFIT质量标准，对隧道进行监控和优选：

① **定义质量标准**

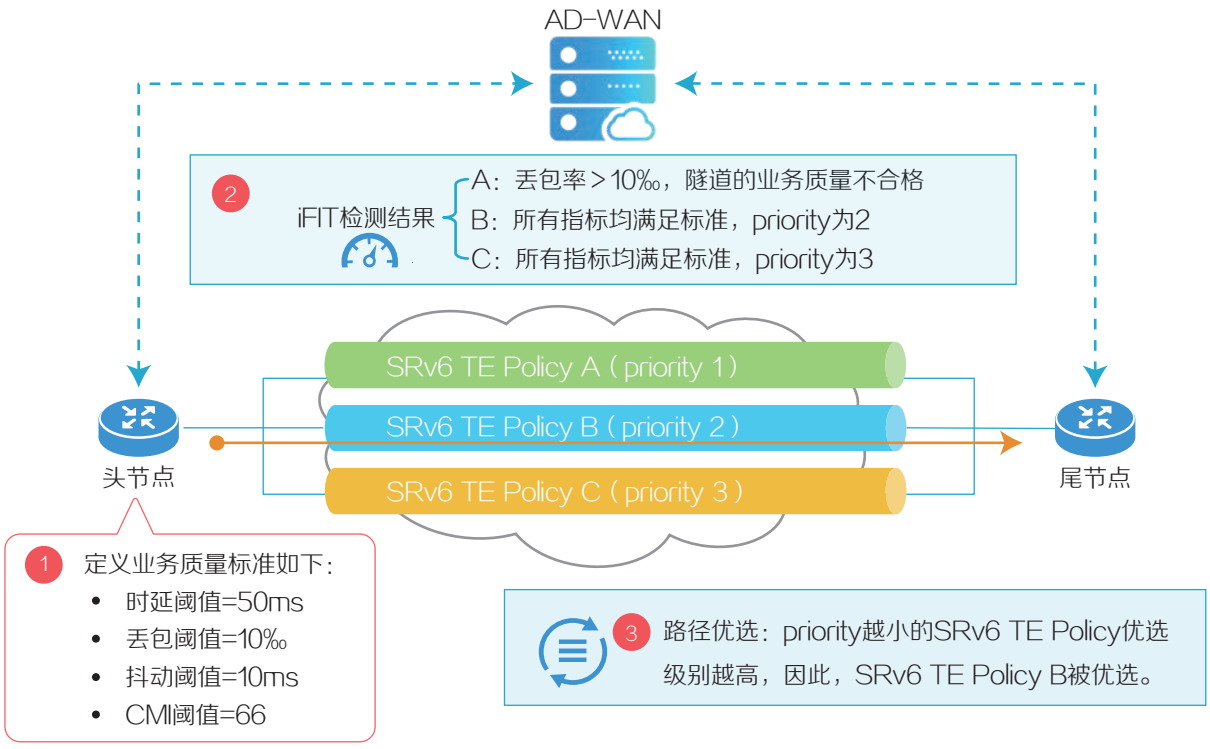
根据业务的需求，用户自定义一个业务质量标准。

② **排除劣质隧道**

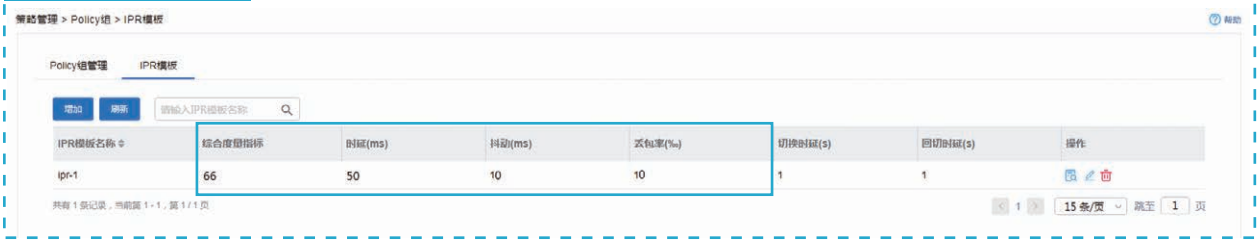
控制组件通过iFIT周期性检查所有SRv6 TE Policy隧道是否符合用户自定义的业务质量标准。网络侧设备根据iFIT检测结果排除不符合标准的隧道。

③ **隧道优选**

网络侧头端设备根据控制组件的iFIT检测结果进行智能选路，从排除劣质隧道后的剩余SRv6 TE Policy隧道中，选取优先级最高的SRv6 TE Policy作为当前最优隧道。



定义业务质量标准



iFIT检测结果

流量引入隧道

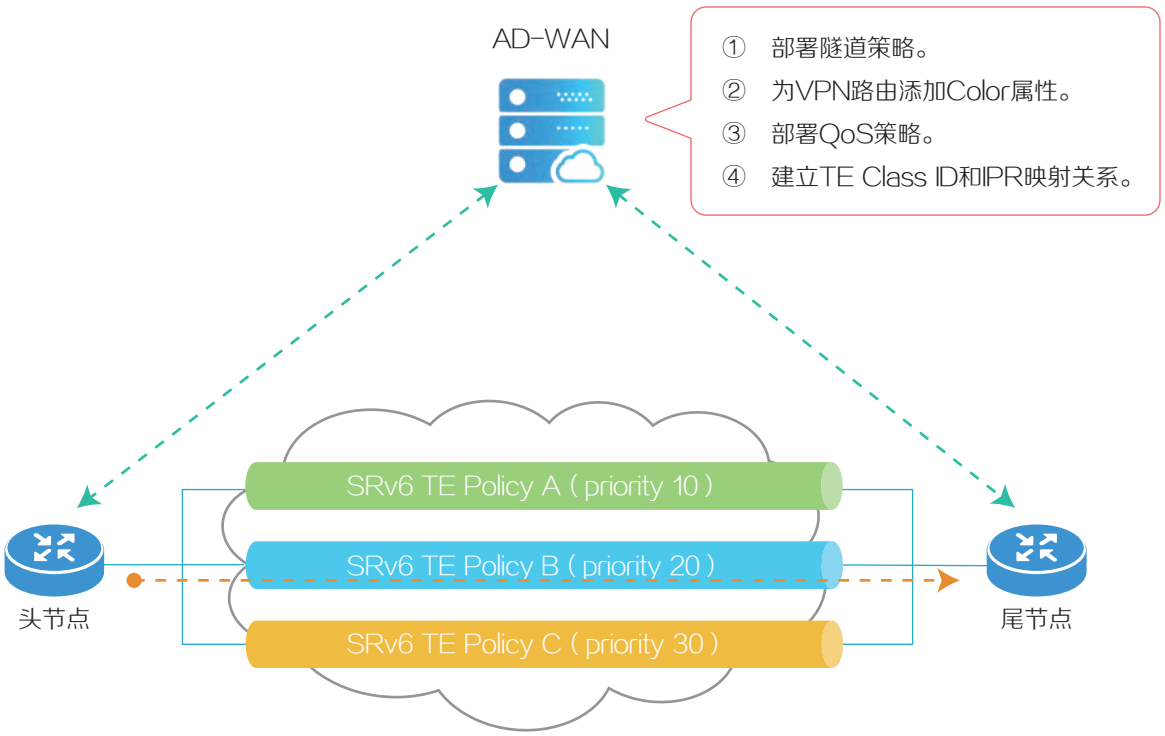
通过Color引流到至SRv6 TE Policy组后，基于TE Class ID和IPR（Intelligent Policy Route，智能策略路由）的映射关系，使业务流量通过智能选路计算出的最优SRv6 TE Policy转发。具体过程为：

① 部署隧道策略，采用SRv6 TE Policy组隧道转发业务流量。

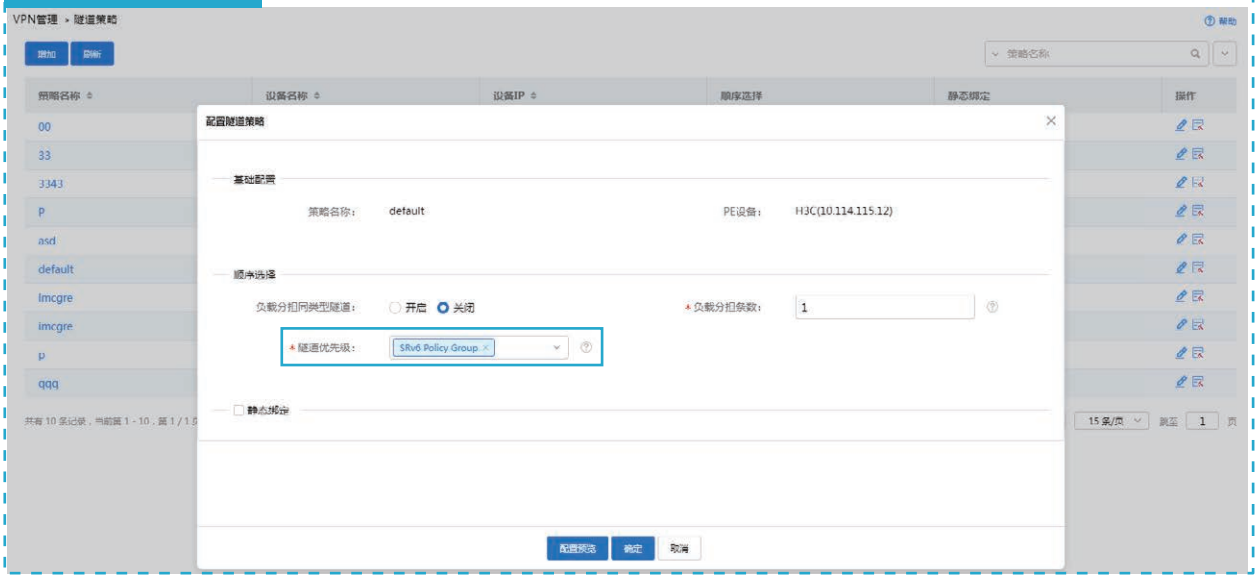
② 通过BGP路由的Color属性匹配到SRv6 TE Policy组。

③ 通过QoS策略标记关键业务流量的TE Class ID值

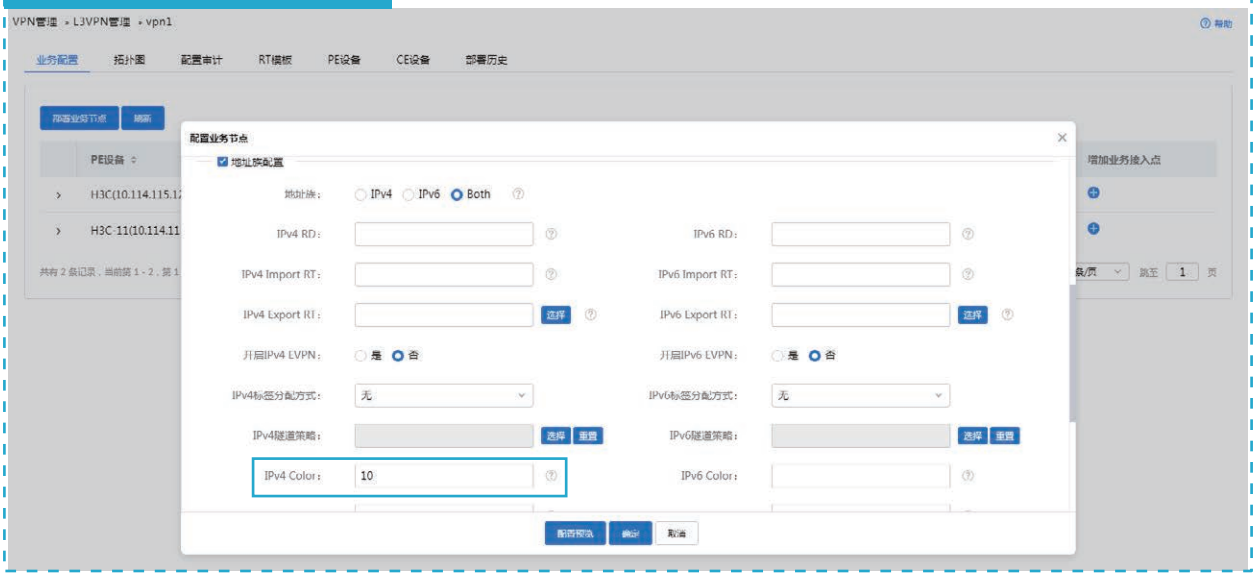
④ 建立TE Class ID和IPR映射关系。


AD-WAN
① 部署隧道策略。
② 为VPN路由添加Color属性。
③ 部署QoS策略。
④ 建立TE Class ID和IPR映射关系。
SRv6 TE Policy A (priority 10)
SRv6 TE Policy B (priority 20)
SRv6 TE Policy C (priority 30)
头节点
尾节点

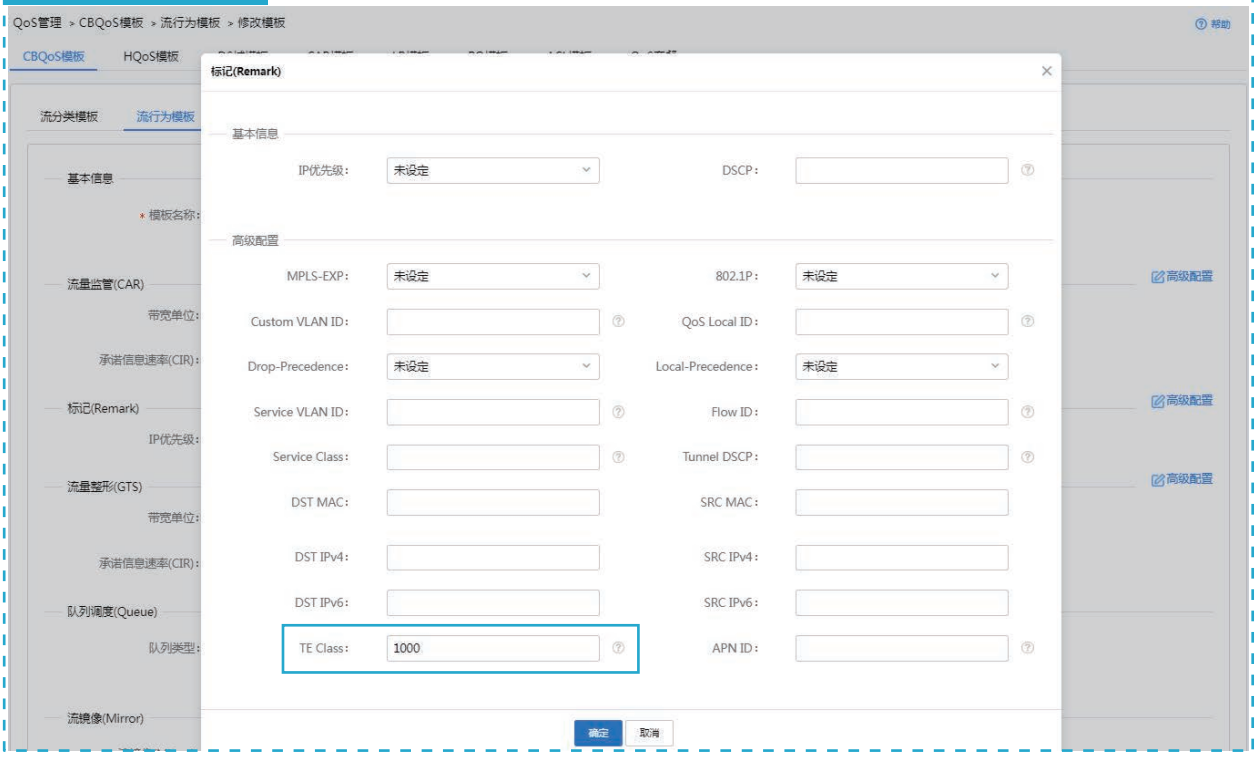
① 部署隧道策略


VPN管理 ▸ 隧道策略
增加
刷新
策略名称
设备名称
设备IP
顺序选择
静态绑定
操作
00
33
3343
p
asd
default
lmcgre
imcgre
p
qqq
配置隧道策略
基础配置
策略名称：
default
PE设备：
H3C(10.114.115.12)
顺序选择
负载分担同类型隧道：
开启
关闭
负载分担条数：
1
隧道优先级：
SRv6 Policy Group
静态绑定
配置预览
确定
取消

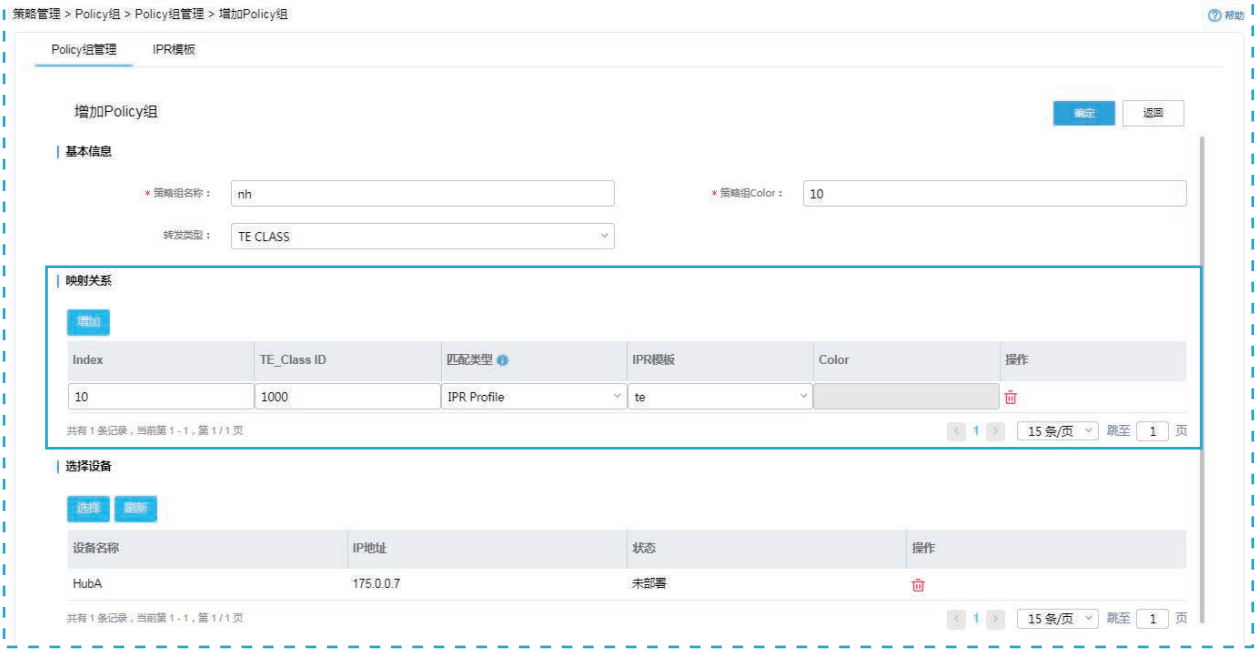
② 为VPN路由添加Color属性



③ 部署QoS策略



④ 建立TE Class ID和IPR映射关系



技术价值

敏捷开通，便捷运维

AD-WAN控制组件协同管理所有网元，在网络侧使用SRv6技术打通分支网络和承载网络，并由SRv6隧道统一承载业务数据。AD-WAN控制组件将转发路径下发给头节点，快速实现端到端业务的开通。

网络质量可控

在AD-WAN控制组件上部署iFIT，实时监控网络侧端到端的业务质量，实现网络质量的可视化。AD-WAN控制组件检测到转发路径的网络质量低于阈值标准时，网络侧设备可以根据iFIT检测结果智能切换转发流量的SRv6隧道，从而保障业务质量。

AD-WAN承载网
NetStream流分析

简介

NetStream是一种基于网络流信息的统计技术，定义了用于设备输出网络流量统计数据的方法，设备对通过的数据进行统计、分析，并上报给网络流量分析组件，经合并处理后存入数据库，并进行下一步的分析处理。为网络管理人员提供详细的数据流统计信息，帮助其了解企业内部网络的运行状况，及时发现并解决网络中的性能瓶颈问题、网络异常现象，也可为用户进行网络优化、网络设备投资、网络带宽优化等提供参考。

方案介绍

H3C AD-WAN解决方案中，分析组件采用NetStream技术在设备的各端口上采集业务流量，以提供更加精细化的业务流量分析能力。

目前分析组件主要提供以下分析能力：

接口流量分析

基于设备接口进行网络流量分析，能够统计全网所有设备接口的流量排名。

VPN流量分析

基于VPN进行流量的分析与统计，展示VPN的全网流量Top排名。

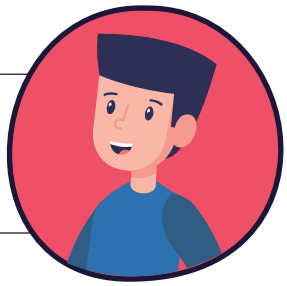
应用流量分析

应用流量分析关注全网应用，计算应用的流量、流速指标，以及每个应用的详细情况。

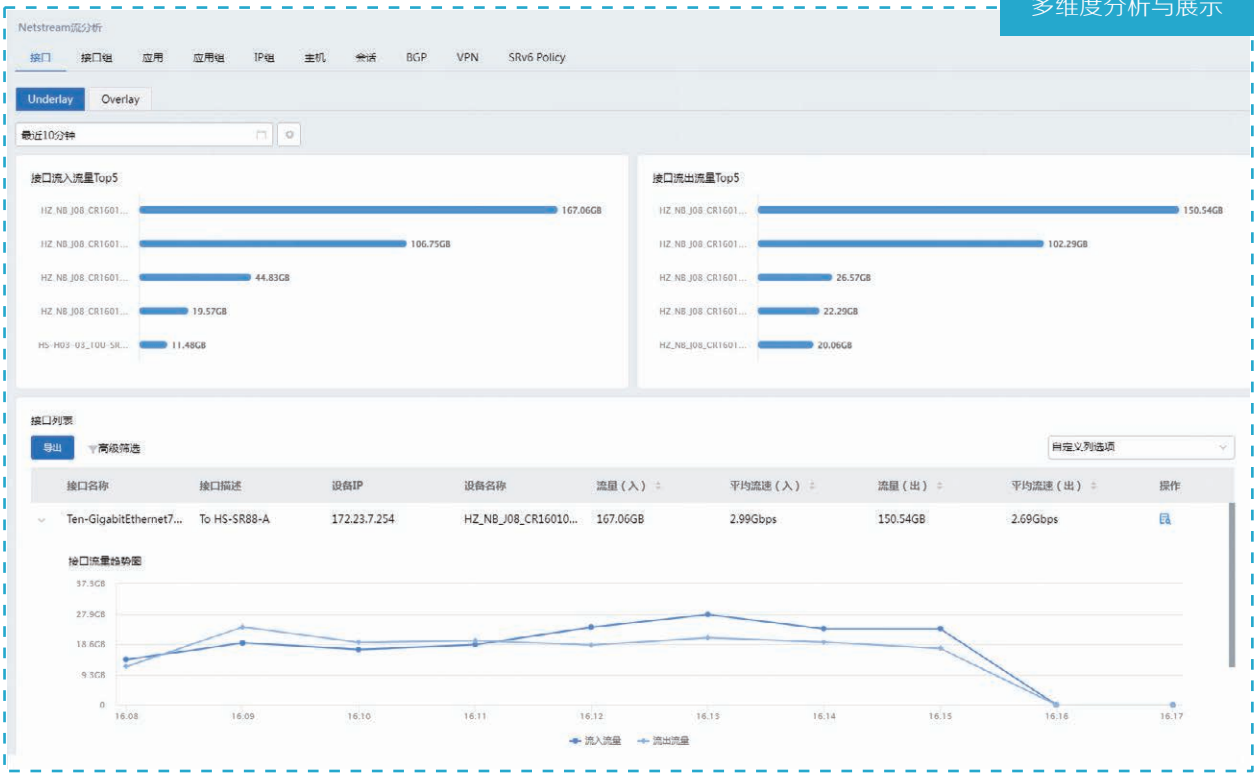
应用组流量分析

通过在分析组件或者控制组件定义应用组信息，可在NetStream流处理中根据流量的五元组信息匹配应用，同时匹配应用所属的应用组，对流量进行统计分析。

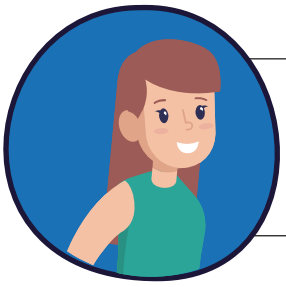
除上述维度以外，分析组件还支持基于接口组、IP组、主机、会话、BGP、SRv6 Policy维度对业务流量进行分析与展示。



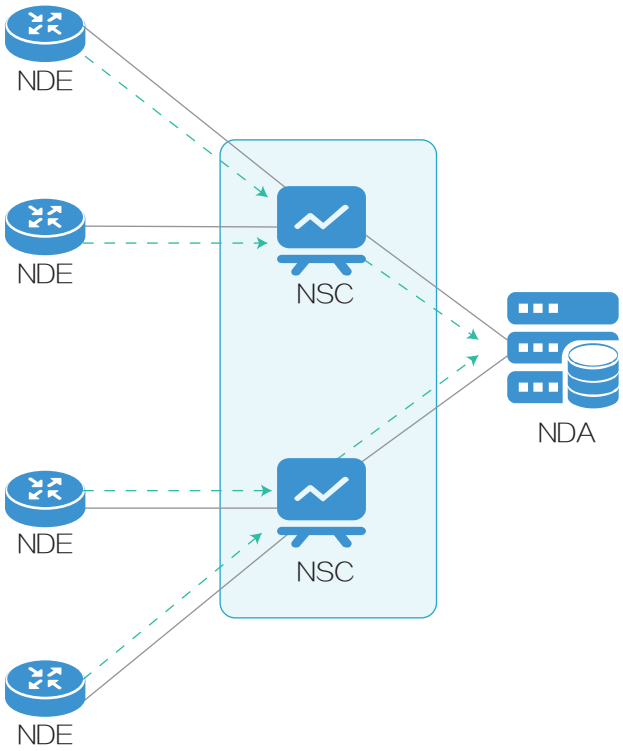
多维度分析与展示



技术介绍



一个典型的NetStream系统由NDE（NetStream Data Exporter，网络流数据输出者）、NSC（NetStream Collector，网络流数据收集者）和NDA（NetStream Data Analyzer，网络流数据分析者）三部分组成。



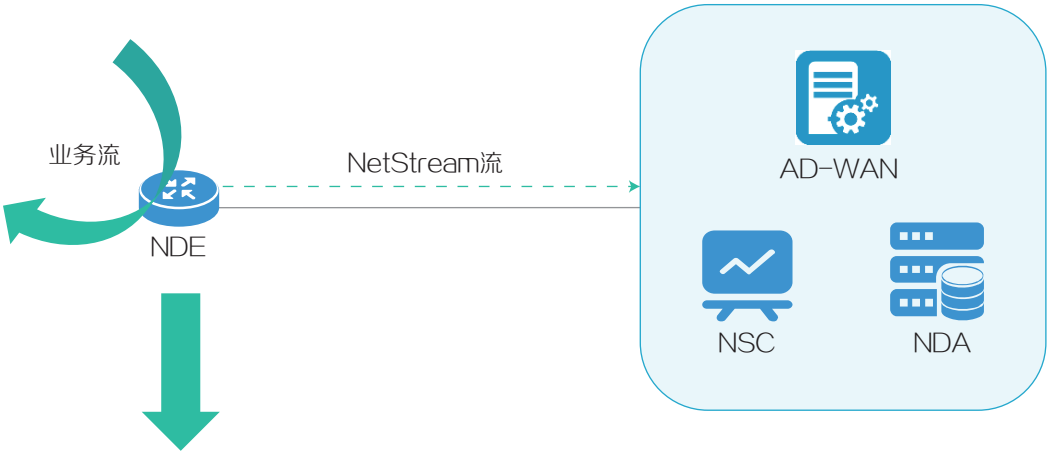
NetStream系统中的设备角色

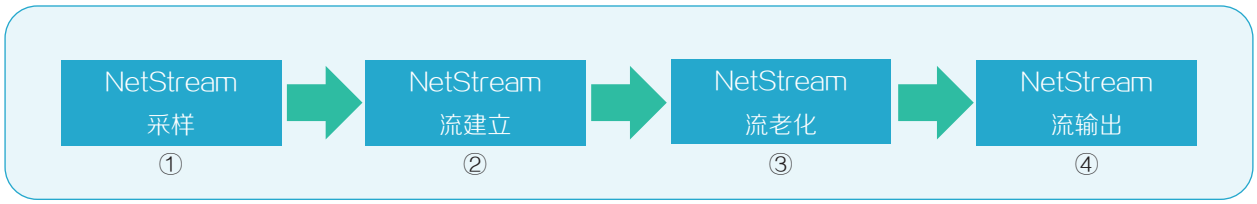
- NDE：把采集到的关于流的详细统计信息定期发送给NSC。
- NSC：将统计信息收集到数据库后发送给NDA。
- NDA：对数据进行分析，用于计费、网络规划等应用。

AD-WAN分析组件支持NetStream功能，实时统计业务流量信息并进行分析与展示。

设备作为NDE的NetStream处理过程主要分为以下几个步骤：

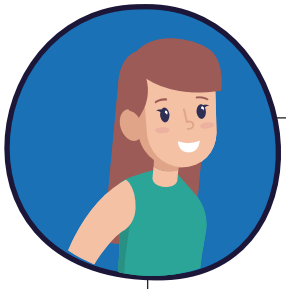
NetStream流老化是设备向AD-WAN分析组件输出流统计信息的前提。





① 设备按照配置的采样方式对业务流量进行NetStream采样。
② 设备根据关键值对采样报文进行NetStream流建立。
③ 设备按照老化方式进行NetStream流老化。
④ 设备按照输出方式进行NetStream流输出。

功能介绍

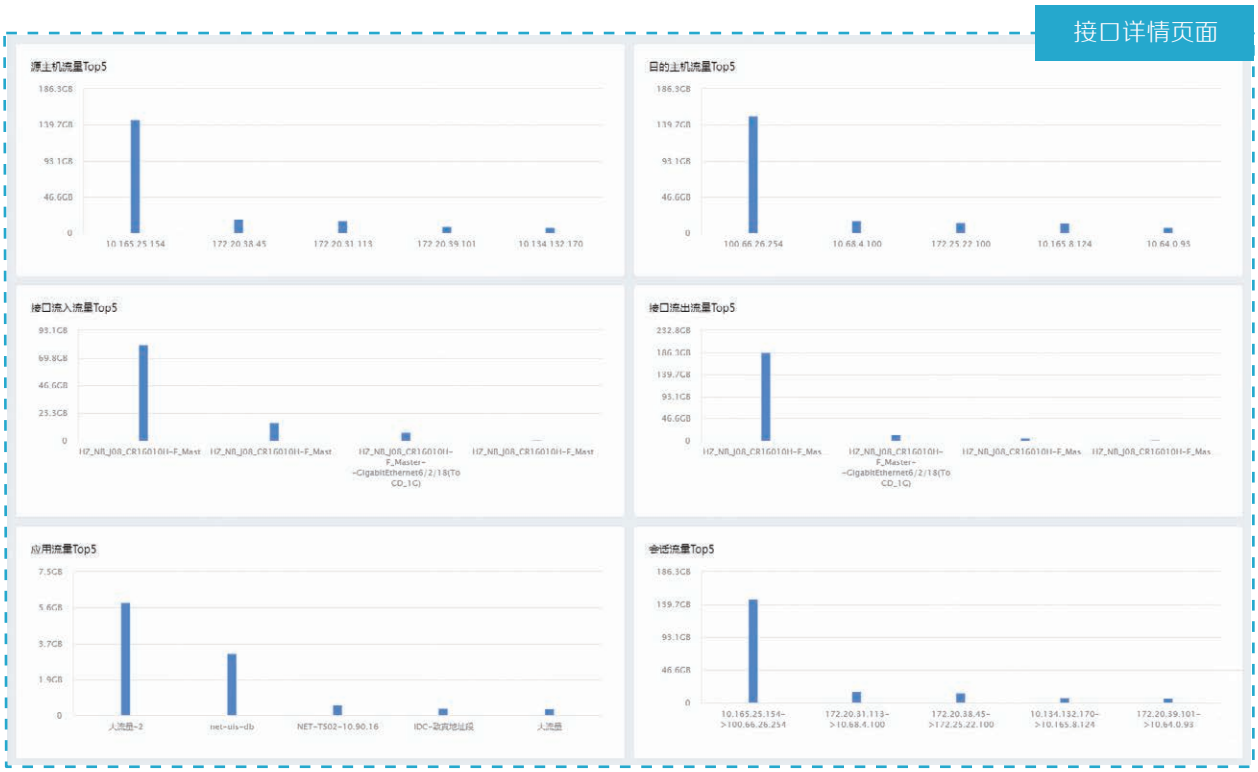


Netstream流分析利用Flink分布式计算引擎，将设备上报的NetStream网络流量进行实时解析和处理，通过从AD-WAN获取应用定义信息，识别出每个五元组所属的应用，基于不同维度对网络流量进行可视化度量，分别展示不同维度下的流量Top排名、流量趋势和流量详情列表等。

展示维度

NetStream流分析所有维度均支持查看流量基本信息和流量详细信息，本文主要展示流量基本信息。

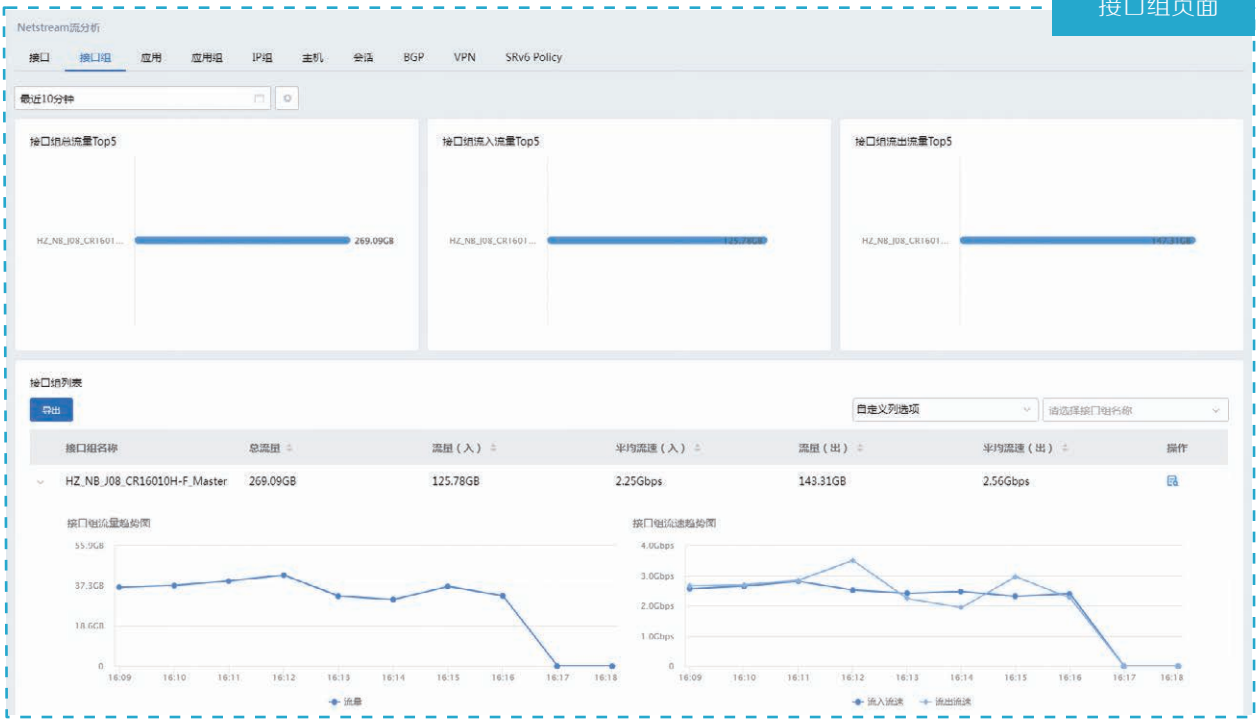
接口流量分析：基于设备接口进行网络流量分析，能够统计全网所有设备接口的流量排名。展示接口流量趋势，并且可以查看每个设备接口的网络流量详情，分析该接口上流量的应用流量排名、会话流量排名、源（目的）主机流量排名、接口流入（流出）流量排名等。



AD-WAN方案支持用户在全局配置中，将一组想关注的设备接口自定义为接口组，并在NetStream流分析功能中对这一组接口统一进行流量分析与展示。

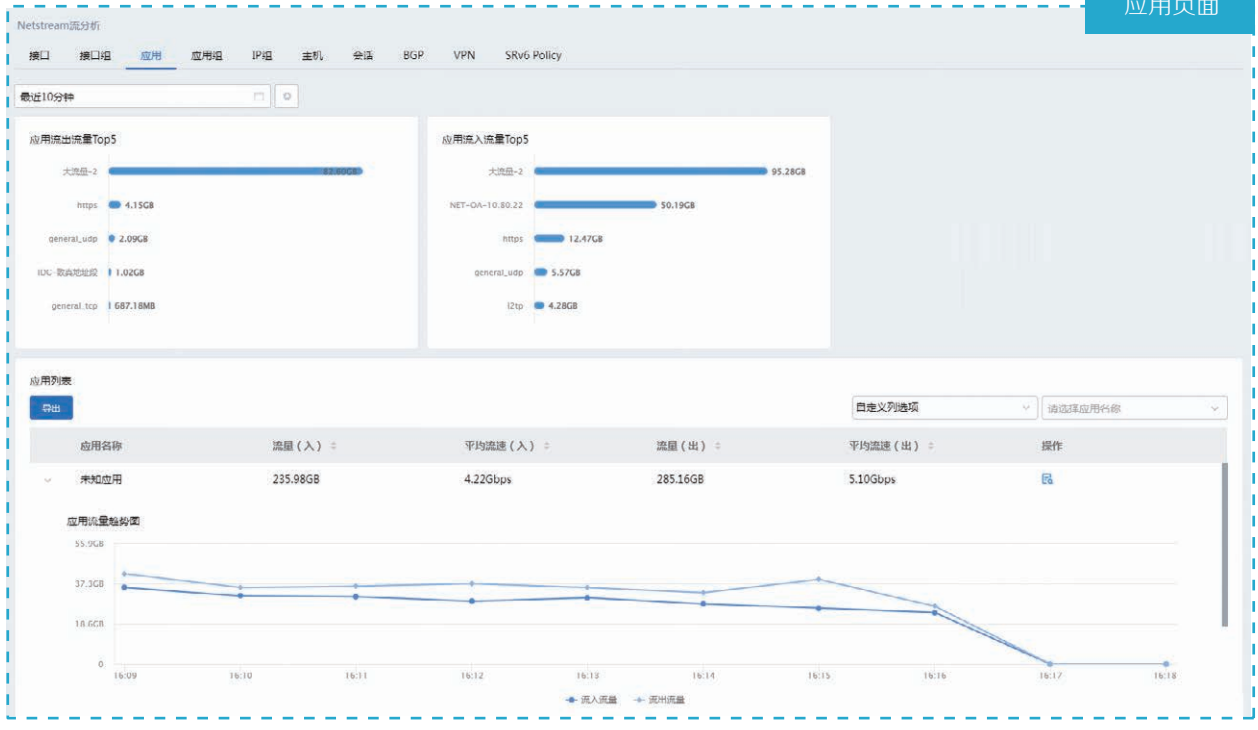
接口组流量分析：基于配置的接口组规则进行网络流量分析，能够统计全网所有接口组的流量排名，展示接口组流量趋势，并且可以查看每个接口组下的网络流量分布情况。

接口组页面



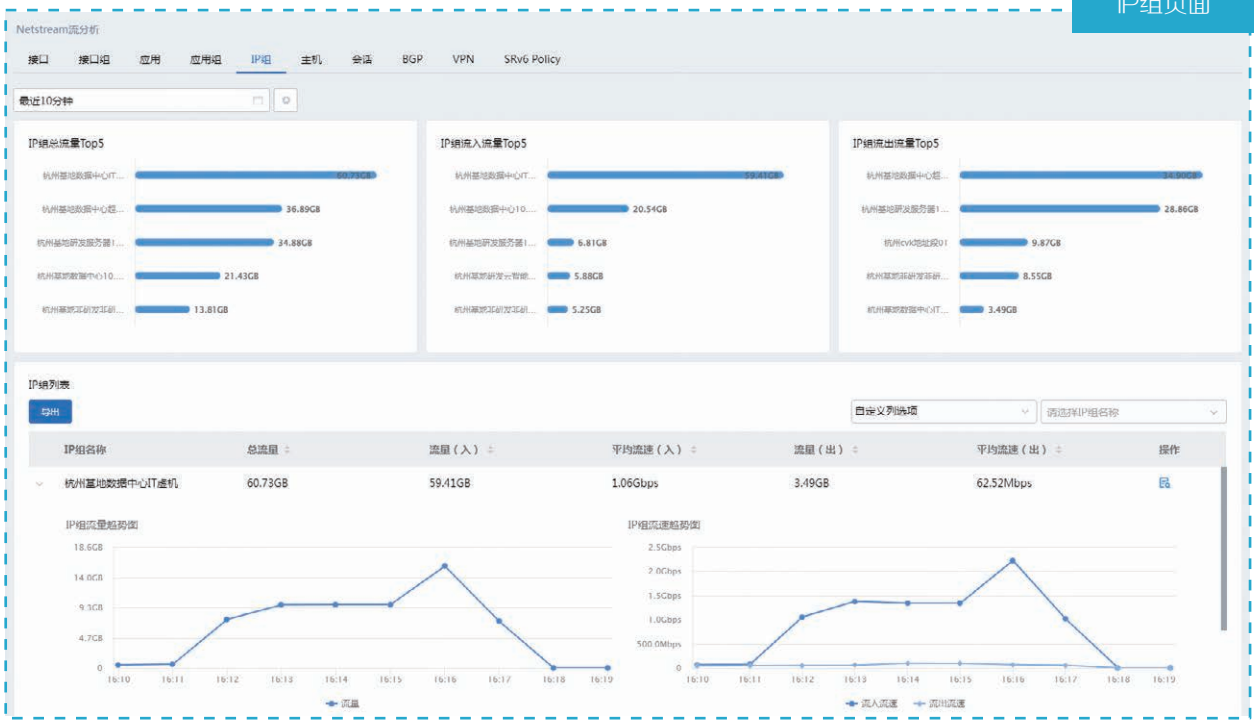
应用流量分析：基于应用进行网络流量分析，可对全网应用进行流量分析，计算应用的流量、流速指标，以及每个应用的详细情况，包括应用的五元组列表（五元组的流量路径）、应用在设备组网中的分布情况以及访问该应用的源主机排名等。

应用页面



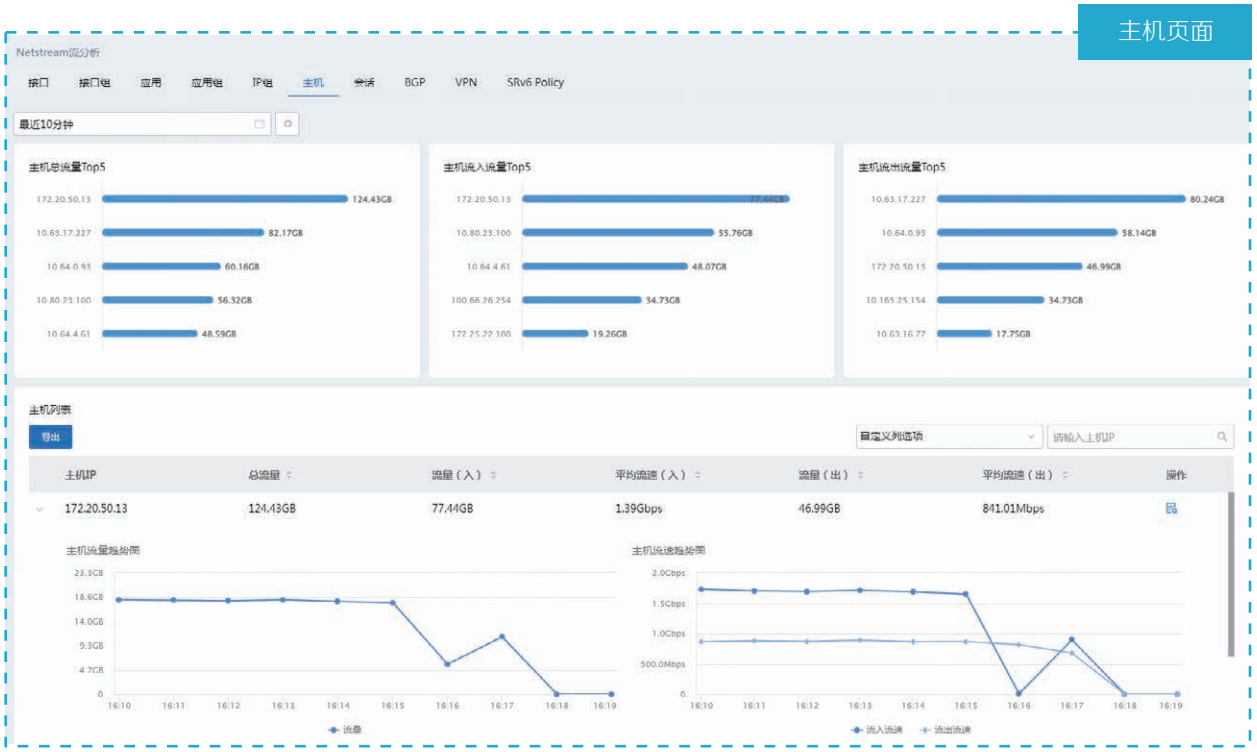
IP组流量分析：基于配置的IP组规则进行网络流量分析，能够统计全网所有IP组的流量排名，展示IP组流量趋势，并且可以查看每个IP组下的网络流量分布情况。

IP组页面



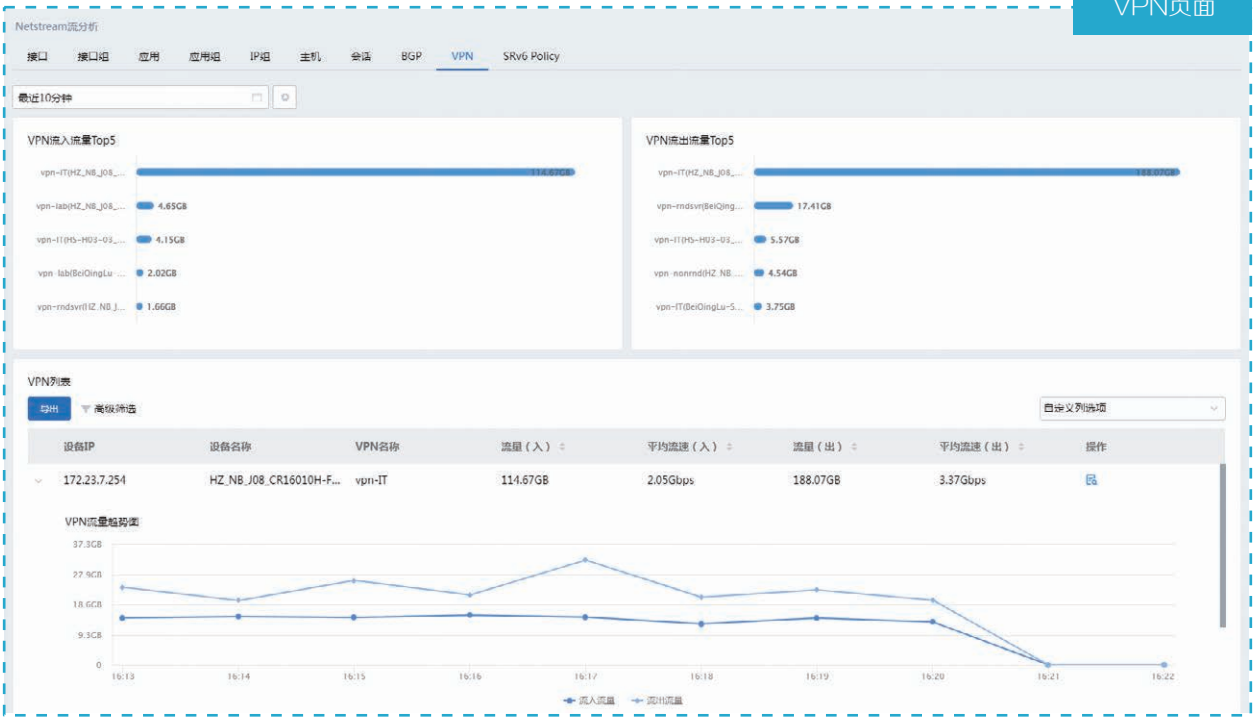
主机流量分析：基于主机维度进行流量的分析与统计，展示以主机IP聚合后的全网流量TOP排名、主机流量趋势，以及每个主机下的接口、应用、会话等维度的流量分布情况。

主机页面



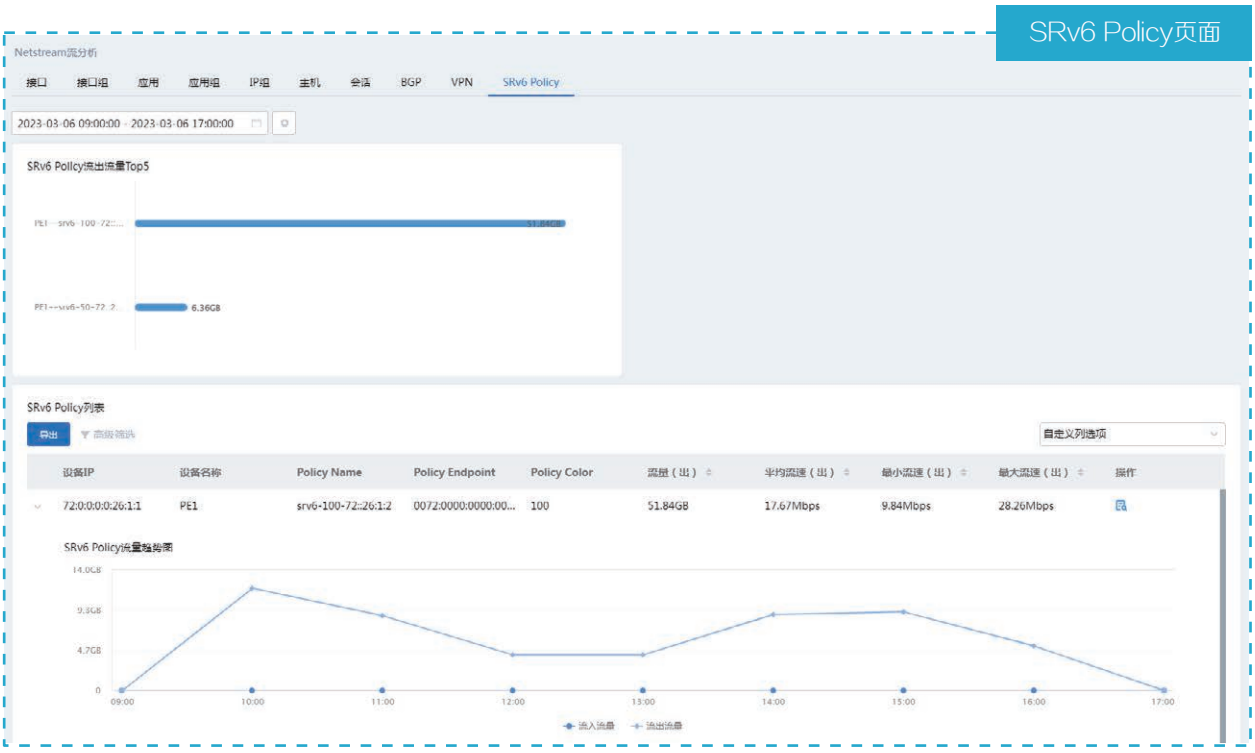
VPN流量分析：基于VPN进行流量的分析与统计，展示VPN的全网流量Top排名，以及每个VPN承载的应用流量排名、应用的流量趋势图和源主机访问排名等。

VPN页面



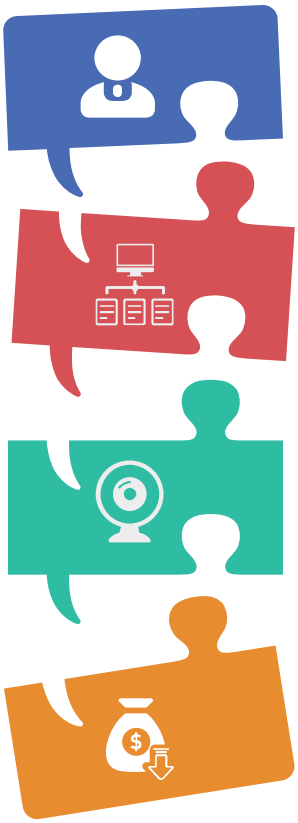
SRv6 Policy流量分析：基于SRv6 Policy进行网络流量分析，能够统计全网SRv6 Policy流量。展示全网SRv6 Policy的流量Top排名、流量统计列表和流量趋势，以及每个SRv6 Policy的网络流量分布情况。

SRv6 Policy页面



典型应用场景

AD-WAN方案中NetStream功能的应用场景主要有以下几种：



用户监控和分析

通过NetStream技术，可以使网络管理者轻松获取用户使用网络、应用资源的详细情况，有助于高效地规划以及分配网络资源，保障网络的安全运行。

网络规划

NetStream可以为网络管理工具提供关键信息，如各个AS域之间的网络流量情况，有助于优化网络设计和规划，实现以最小的网络运营成本达到最佳的网络性能和可靠性。

网络监控

在出口部署NetStream，对连接Internet网络的接口进行实时流量监控，分析各种业务占用出口带宽的情况。网络管理者可以根据这些信息判断网络的运行情况，尽早发现不合理的网络结构或网络中的性能瓶颈，方便网络管理者合理规划和分配网络资源。

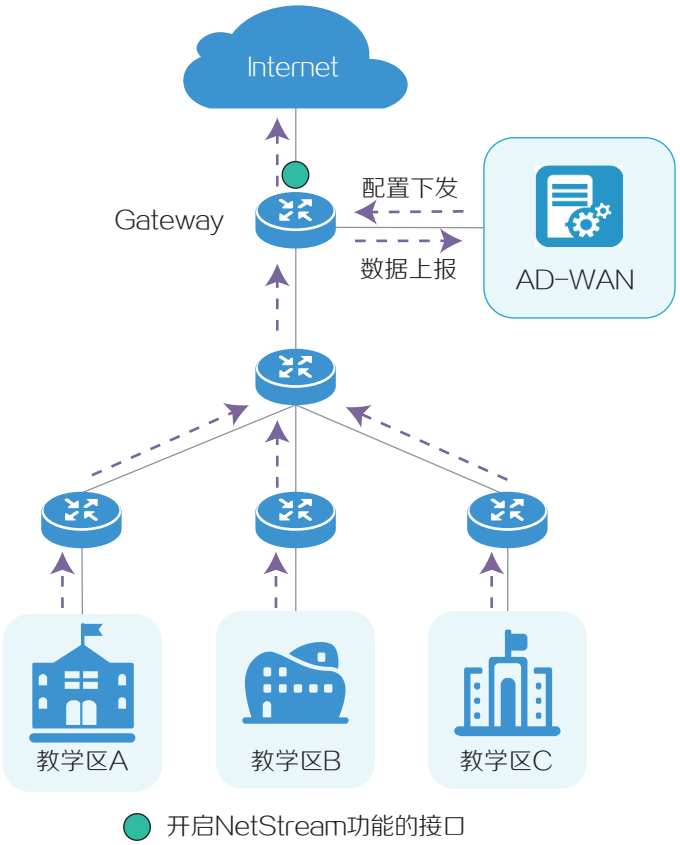
计费

NetStream为基于资源（如线路、带宽、时段等）占用情况的计费提供了精细的数据。Internet服务提供商可以利用这些信息来实行灵活的计费策略，如基于时间、带宽、应用、服务质量等。企业客户可以使用这些信息计算部门费用或分配成本，以便有效利用资源。

NetStream应用于网络规划场景

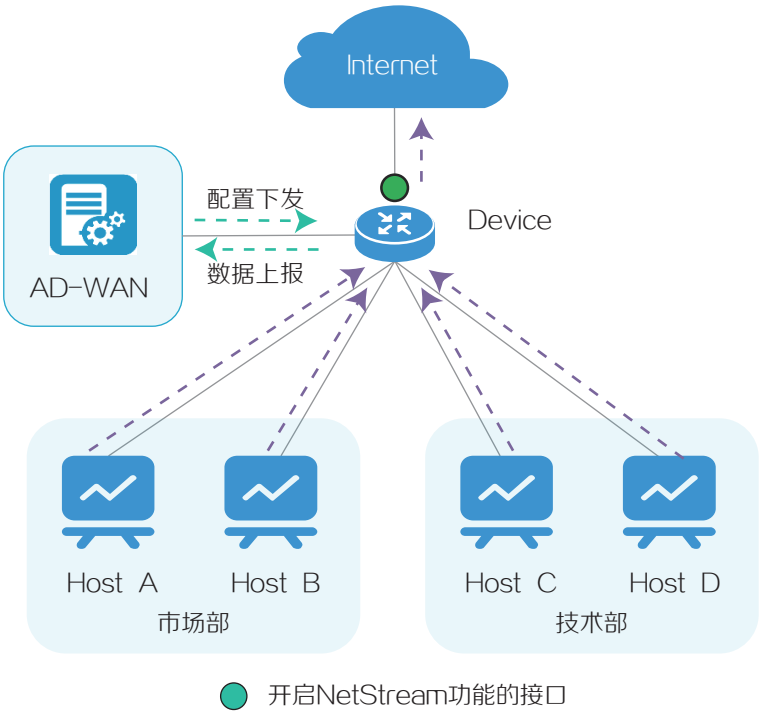
某校园被划分为三个教学区，最初网络管理员为每个教学区分配了相同的带宽。但是随着VoIP、P2P、IPTV等新业务的应用，之前的网络划分已经无法满足学生和老师们的需求，同时也不利于管理。

管理员可以在Gateway连接Internet网络侧的接口上部署NetStream功能，统计接口出、入方向的流量信息，并上送给AD-WAN进行后续的分析，以便通过获取到的带宽使用率的详细信息进行合理地网络的规划和分配，同时对网络流量进行监管。



NetStream应用于流量计费场景

某公司的市场部和技术部通过Device接入到Internet网络，公司希望能够掌握两个部门的上网情况，以便进行分部门计费。



设备连接Internet网络的接口上，通过NetStream统计功能，可以统计接口出、入方向的流量信息，并上报给AD-WAN进行后续的分析，以便监控两个部门的上网情况，为分部门计费提供依据。

方案亮点

多维度数据展示

涵盖接口、应用、应用组、IP组、主机、VPN等常用数据指标的分析与展示。

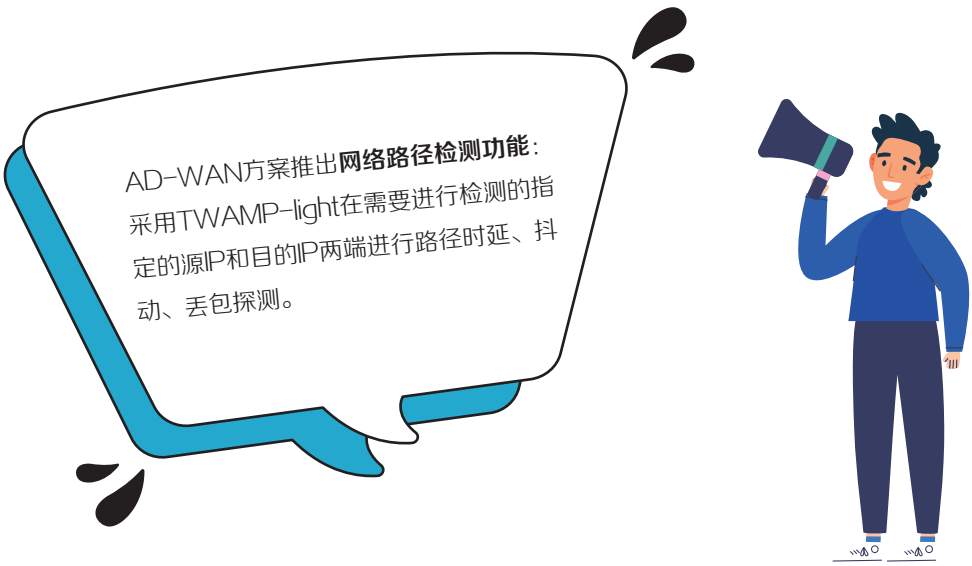
可视化信息呈现

图形化界面降低流量信息管理难度，提供各项流量数据图表。

AD-WAN承载网 网络路径检测

简介

随着网络技术的飞速发展，网络中承载的业务越来越多，语音、视频等业务对网络丢包和时延要求越来越高。网络管理者需要一种测量工具来及时了解网络中的丢包和时延情况，以便可以根据测试结果及时对网络进行调整、优化，满足业务需求。



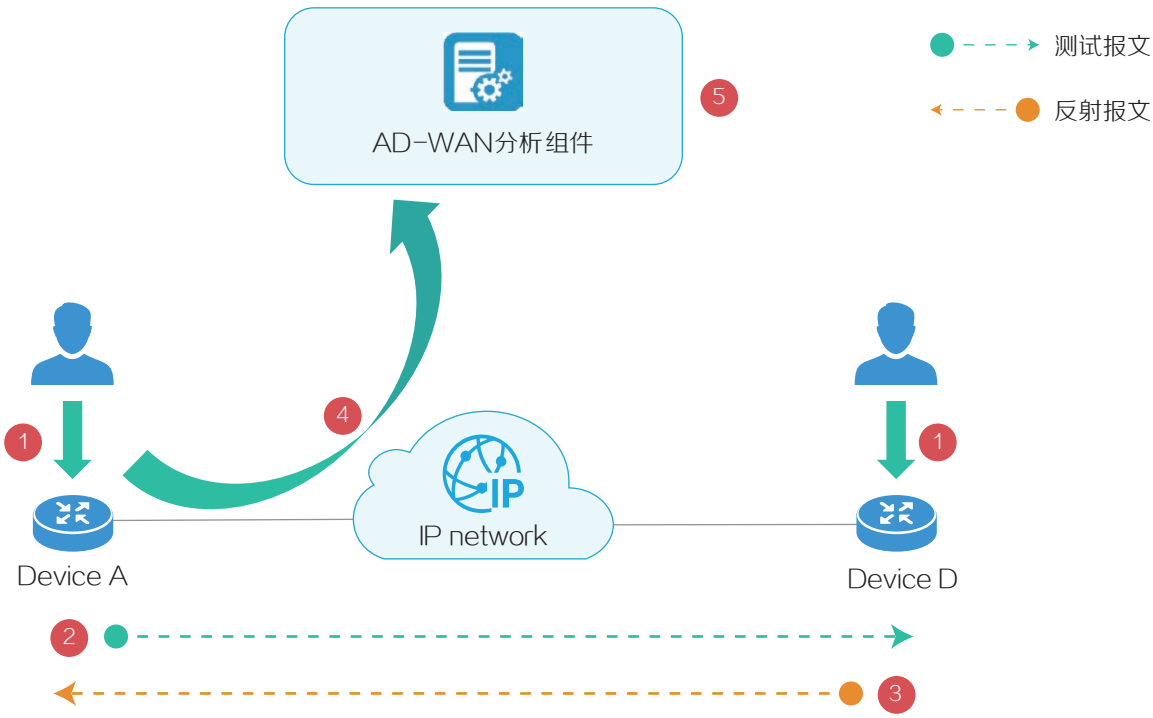
方案介绍

AD-WAN方案中，分析组件通过网络路径检测功能采集和分析网络中所有设备TWAMP-light模块的测试会话数据和测试结果数据，对数据根据不同的时间粒度进行计算，实现对网络中各个转发路径的质量测量和分析。AD-WAN方案当前支持TWAMP双向、单向时延，TWAMP for trunk双向、单向时延的质量采集与分析。

网络路径检测功能配置流程

AD-WAN方案支持对网络路径质量阈值进行配置，超阈值推送异常分析。

组网示意图



1 TWAMP配置下发：用户可通过控制组件向设备下发TWAMP配置，亦可通过手动配置。

2 3 设备间发送测试报文与反射报文，探测网络路径质量。

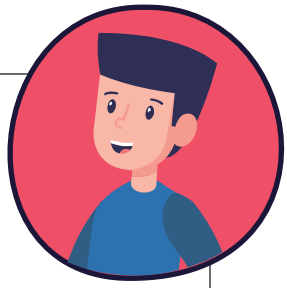
4 设备根据探测到的数据，分析网络路径质量并上报至分析组件。

5 AD-WAN分析组件对收集的网络路径质量数据进行分析与展示。

技术介绍

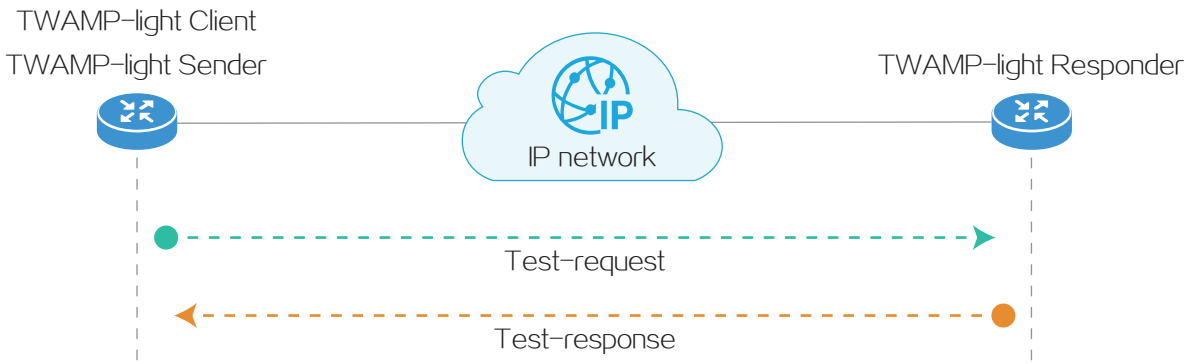
TWAMP(Two-Way Active Measurement Protocol，双向主动测量协议)用来测量网络中任意两台设备之间报文的双向时延、抖动、丢包率等性能参数，为网络质量分析提供依据。

TWAMP-light是TWAMP协议定义的轻量级架构，简化了建立性能测量会话的控制协议，提高了测试性能。



如下图所示，在TWAMP-light网络模型中包含以下角色：

1. TWAMP-light在测试源端设备定义了两个角色：
   ① TWAMP-light Client：负责配置TWAMP-light测试会话。
   ② TWAMP-light Sender：负责启动、停止TWAMP-light测试会话。
2. TWAMP-light在测试目的端设备定义了TWAMP-light Responder，负责将会话测试报文反射回去。



TWAMP-light测量机制。

概念百科

1. Sender使用预先配置好的IP地址、UDP端口号等参数，构造测试报文(Test-request)，每隔一段时间进行一次测试，每次测试发送一个Test-request给Responder。
2. Responder收到探测报文后，构造反射报文(Test-response)，填充时间戳和TTL等信息，将报文反射回Sender。
3. Sender根据收到Test-response报文个数、接收时间计算Test-request报文的丢失率、往返时延和时延抖动，从而判断源端到目的端、目的端到源端网络路径质量的优劣。

功能介绍

路径检测概览页面主要展示路径质量Top5和路径质量详情列表，系统默认展示最近30分钟内的网络路径质量数据。

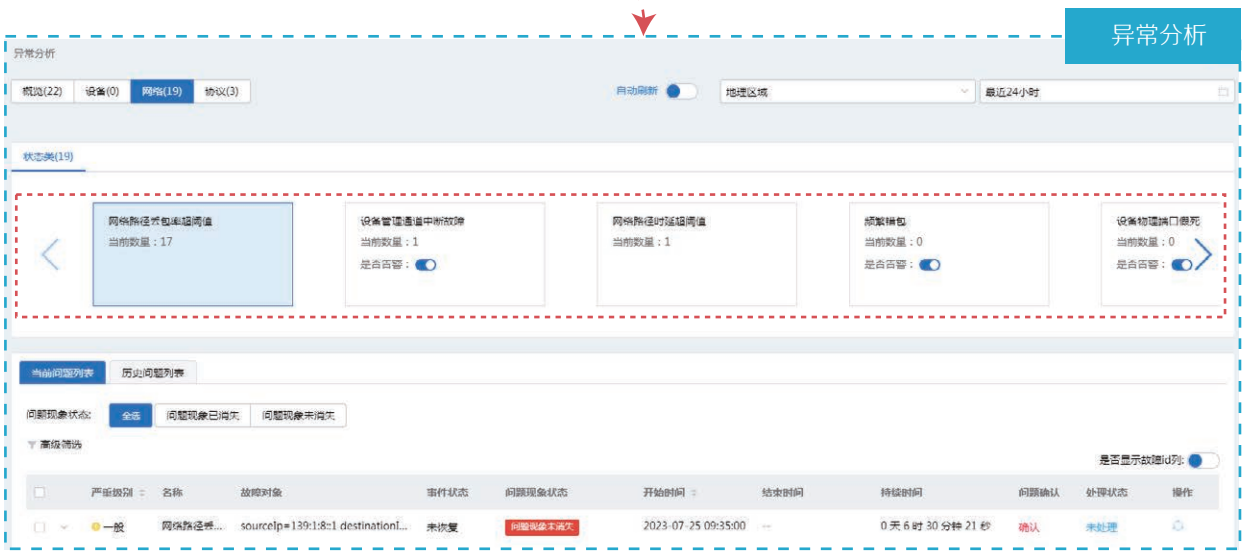
用户可按需选择区域、时间范围展示网络路径质量数据。

路径质量Top5的展示：包括路径时延Top5、抖动Top5、丢包率Top5和错包率Top5，展示结果可用于快速定位质量指标较差的网络路径。

路径质量列表：展示测试会话基本信息和路径质量参数。测试会话基本信息展示测试会话的配置或运行参数，用于区分不同的路径与测试会话。路径质量参数展示用户所选时间段内测试会话的路径质量指标的平均值，例如平均时延、平均抖动等。

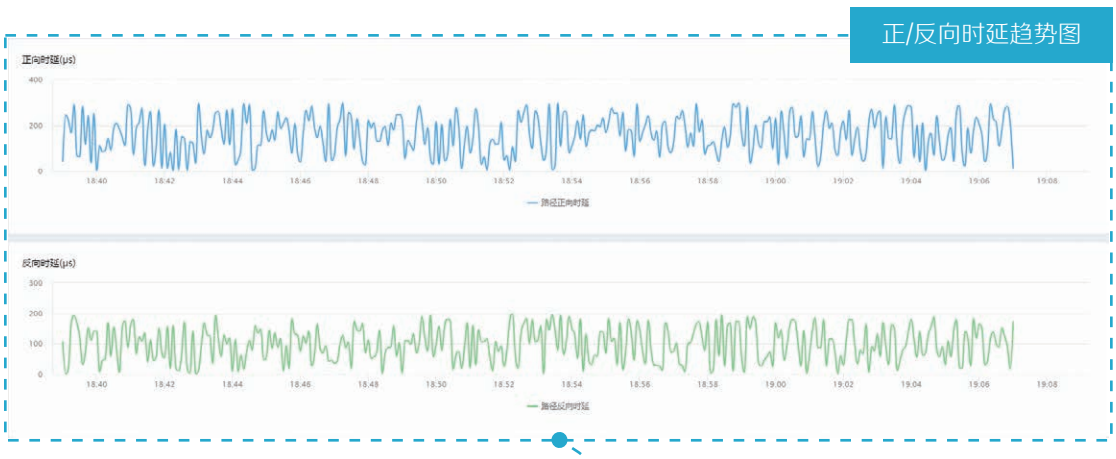
可以配置全局质量阈值，或为指定TWAMP会话单独配置质量阈值。

当网络路径质量指标超阈值时，会将网络路径及质量详情推送至异常分析。

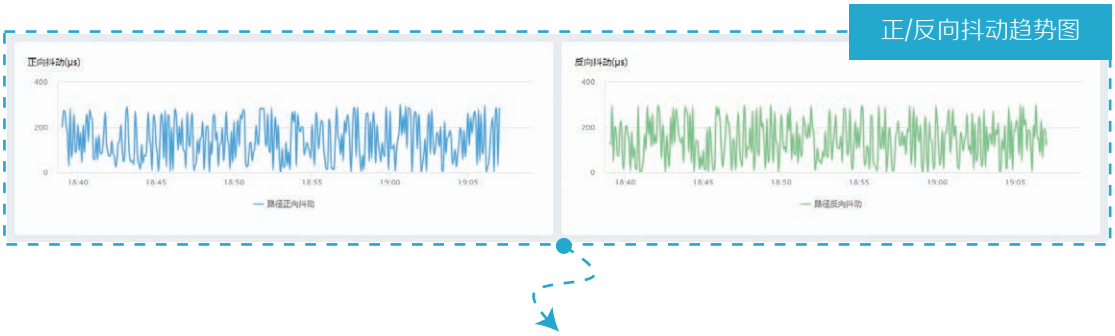


路径质量详情：展示测试会话基本信息和路径质量指标趋势曲线。默认情况下不展示路径的单向时延趋势图，可根据需要使能会话的单向时延探测功能（OWAMP），并增加相应仪表进行展示。路径质量详情支持展示绑定的聚合口，同时可以选择聚合口下的成员口进行细粒度的展示。

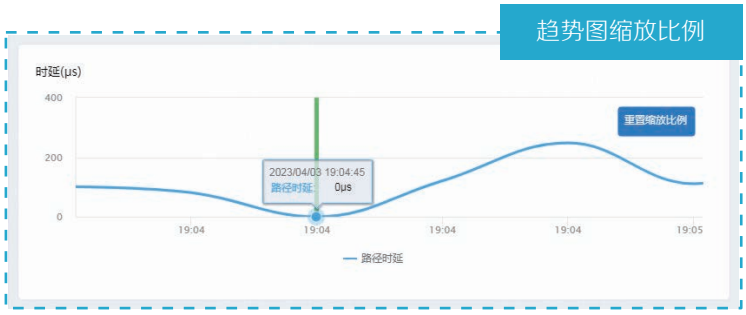
时延/抖动/丢包率/错包率趋势图：展示所选时间段内当前TWAMP测试会话的双向抖动/时延、丢包率以及错包率的变化趋势。



正/反向时延趋势图：展示所选时间段内当前TWAMP测试会话的正向时延与反向时延变化趋势；正向时延表示源设备到目的设备方向的时延大小；反向时延表示目的设备到源设备方向的时延大小。

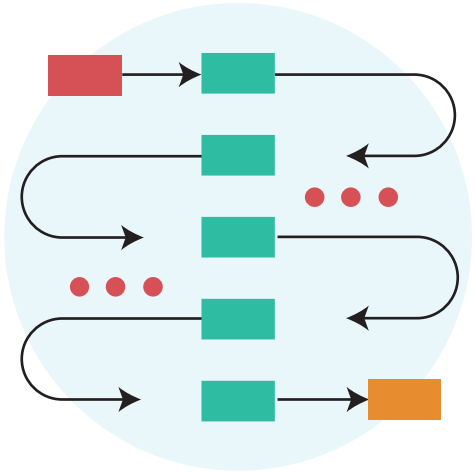


正/反向抖动趋势图：展示所选时间段内当前TWAMP测试会话的正向抖动与反向抖动变化趋势；正向抖动表示源设备到目的设备方向的抖动值；反向抖动表示目的设备到源设备方向的抖动值。



若用户选择查询的时段小于一小时，页面将会展示测试会话原始详细统计数据。页面趋势图支持重置缩放比例功能，可局部放大趋势图，展示精确时间点的网络路径质量指标。

方案亮点



多维度指标分析

涵盖时延、抖动、丢包率、错包率等常用网络路径质量指标的分析与展示。

可视化信息呈现

图形化界面展示网络路径质量指标趋势，帮助用户更好地监测网络路径。

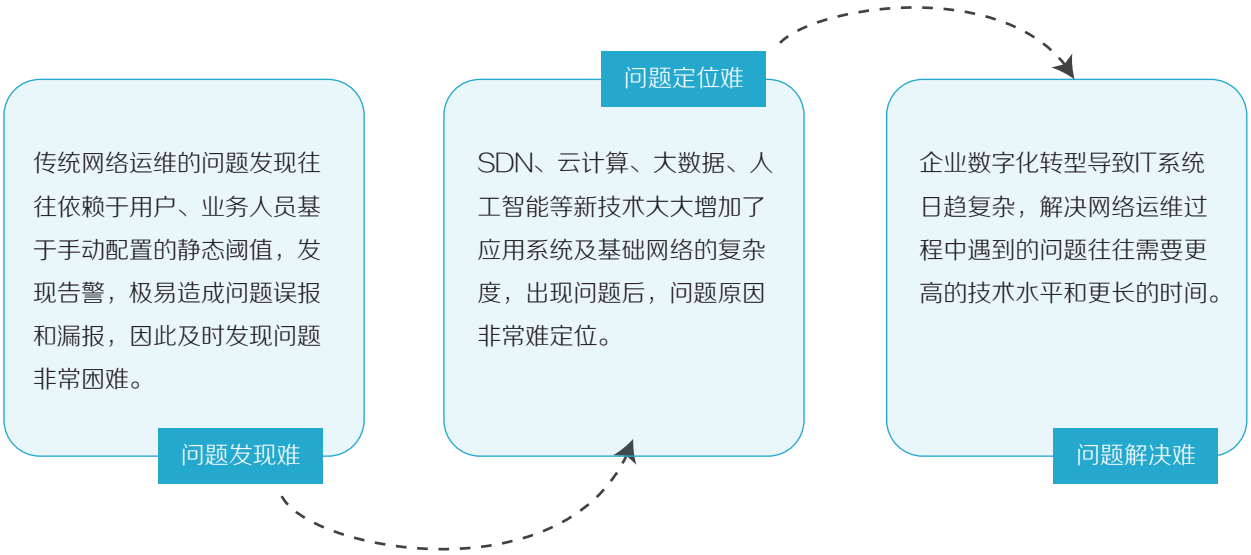
联动异常分析

网络路径质量指标超阈值时，可联动异常分析，查看系统中当前或历史网络路径问题详情。

AD-WAN承载网 异常分析

简介

随着企业数字化转型进程的推进，网络的规模、复杂度也在快速增加以满足上层应用的各种需求，传统的运维手段在问题发现、定位和解决的过程中逐渐变得力不从心。



为解决上述问题，AD-WAN方案推出异常分析功能：故障智能发现，智能定位与闭环。

方案介绍

AD-WAN方案中，异常分析功能展示在所选时间内，整个组网中发生故障的统计，包括基于设备、网络、协议等分类后的故障信息。

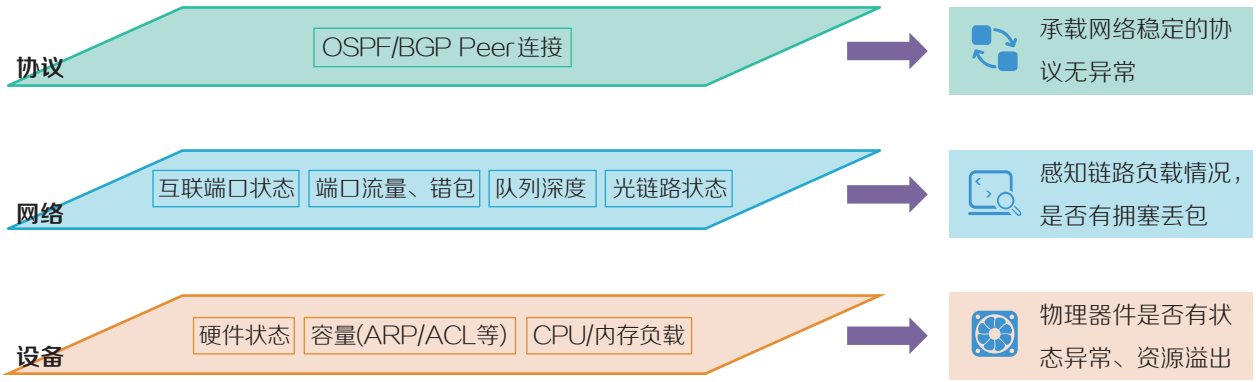
协议类故障

综合协议规范分析路由状态，判定故障点。可检测路由参数配置不一致、认证方式不同、区域号不一致等9种常见问题。

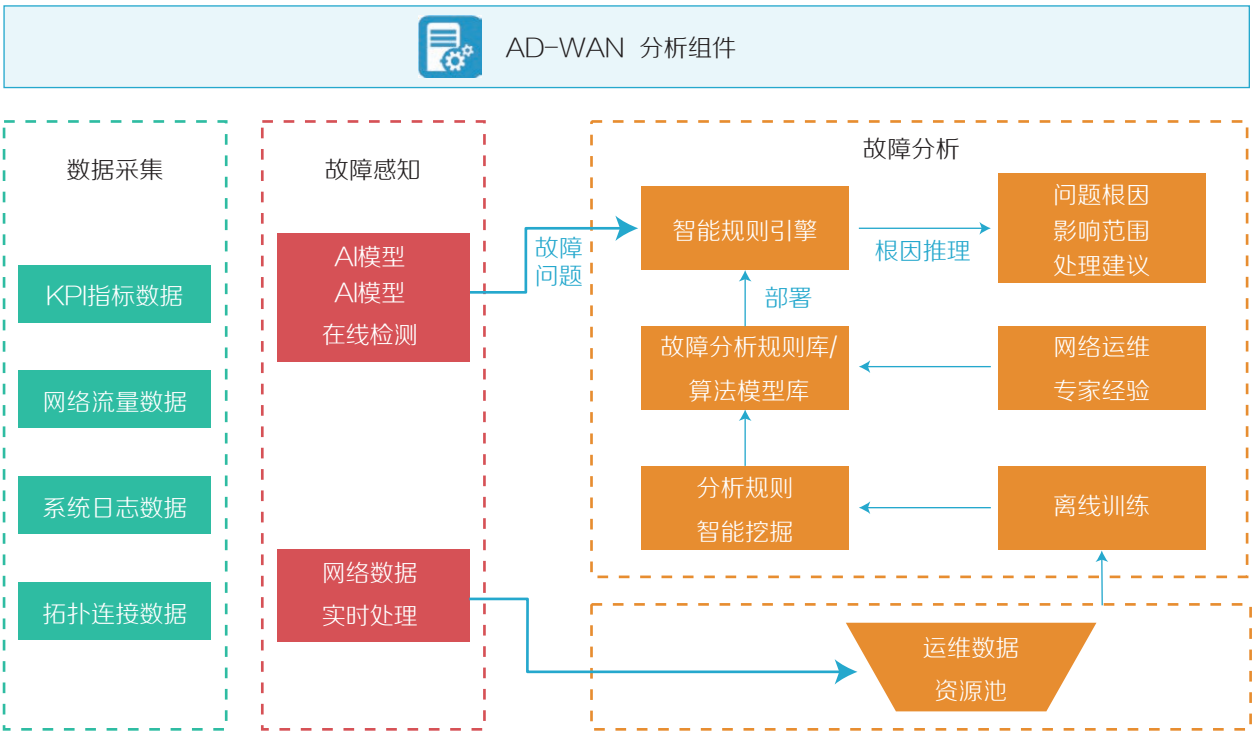
异常分析功能配置流程

设备基础配置	数据采集配置	解析任务配置
• gRPC配置	• gRPC采集	• 异常分析
• SNMP配置	• SNMP采集	• 异常分析Java
• SYSLOG配置	• SYSLOG采集	• 异常分析gRPC
• NETCONF配置	• NETCONF采集	

AD-WAN方案异常分析支持三层评估模型，自动发现故障。



AD-WAN方案异常分析功能，支持协议 、网络、设备三大类常见故障分钟级发现，定位根因并给出处理建议。



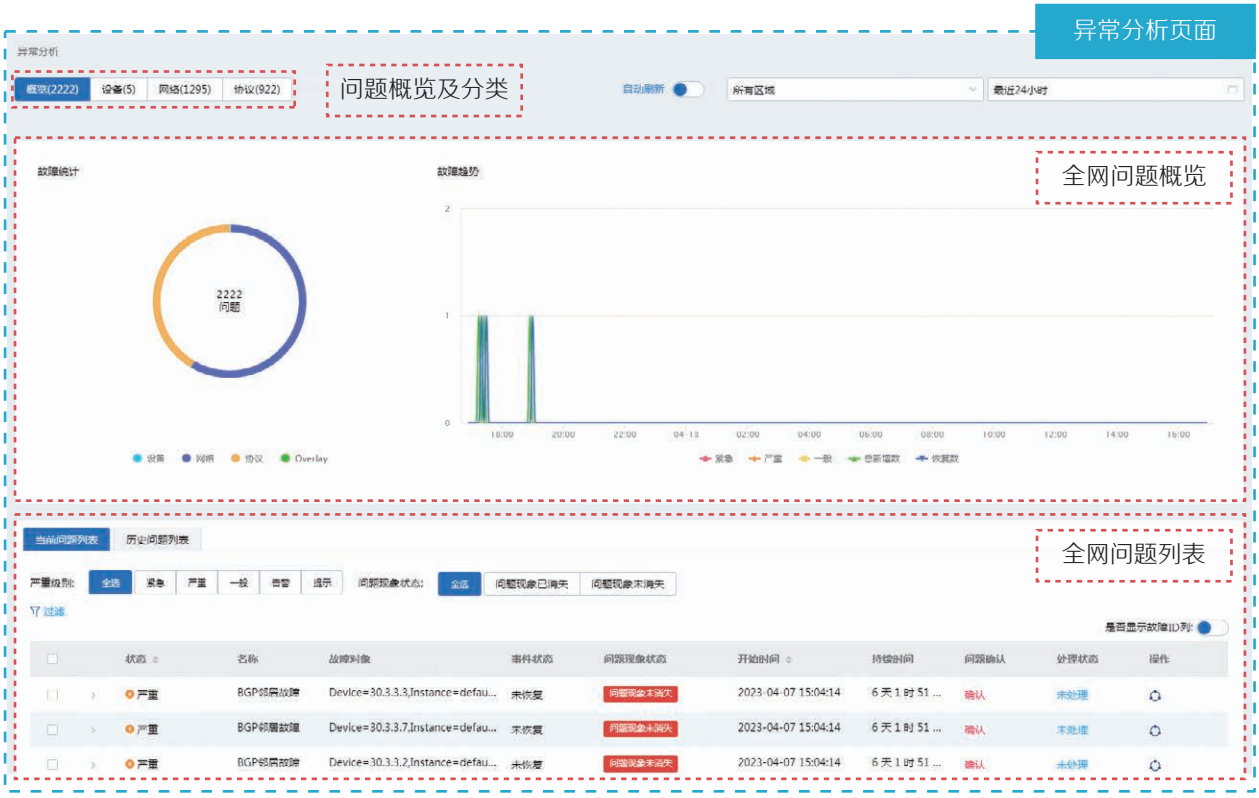
数据采集：采集网络和流量的数据指标，采集粒度支持秒级和分钟级。
故障感知：基于AI模型检测KPI指标异常，实现分钟级感知网络故障。
故障分析：基于AI算法和规格模型分析推理产生故障的原因，实现分钟级的故障定位。

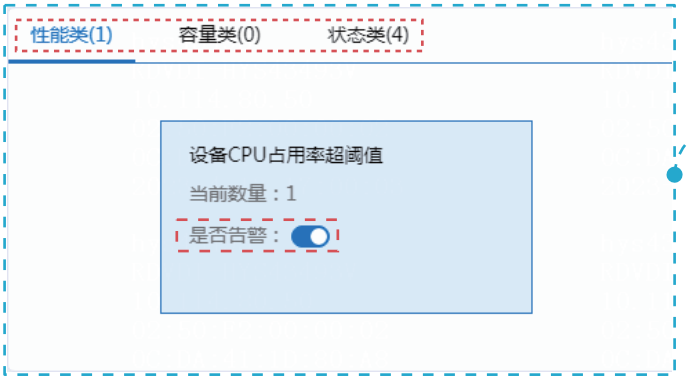
概念百科

AI模型检测KPI指标：使用NETCONF等协议周期性采集数据，根据数据使用AI预测，推演出某一项指标数据的上、下限，当系统中数据超过预测的上下限即产生告警，推送至异常分析。
故障分析规则库/算法模型库/智能规则引擎：根据固定的业务逻辑对系统中的数据进行规则判断，是故障诊断的基础。

功能介绍

异常分析分类展现系统发现的问题，方便用户查询。提供概览、设备、网络、协议几大问题列表详情。分别展示问题趋势图；当前/历史问题列表；问题详情，根因分析，处理建议；问题开始/持续时间及状态。





设备页签

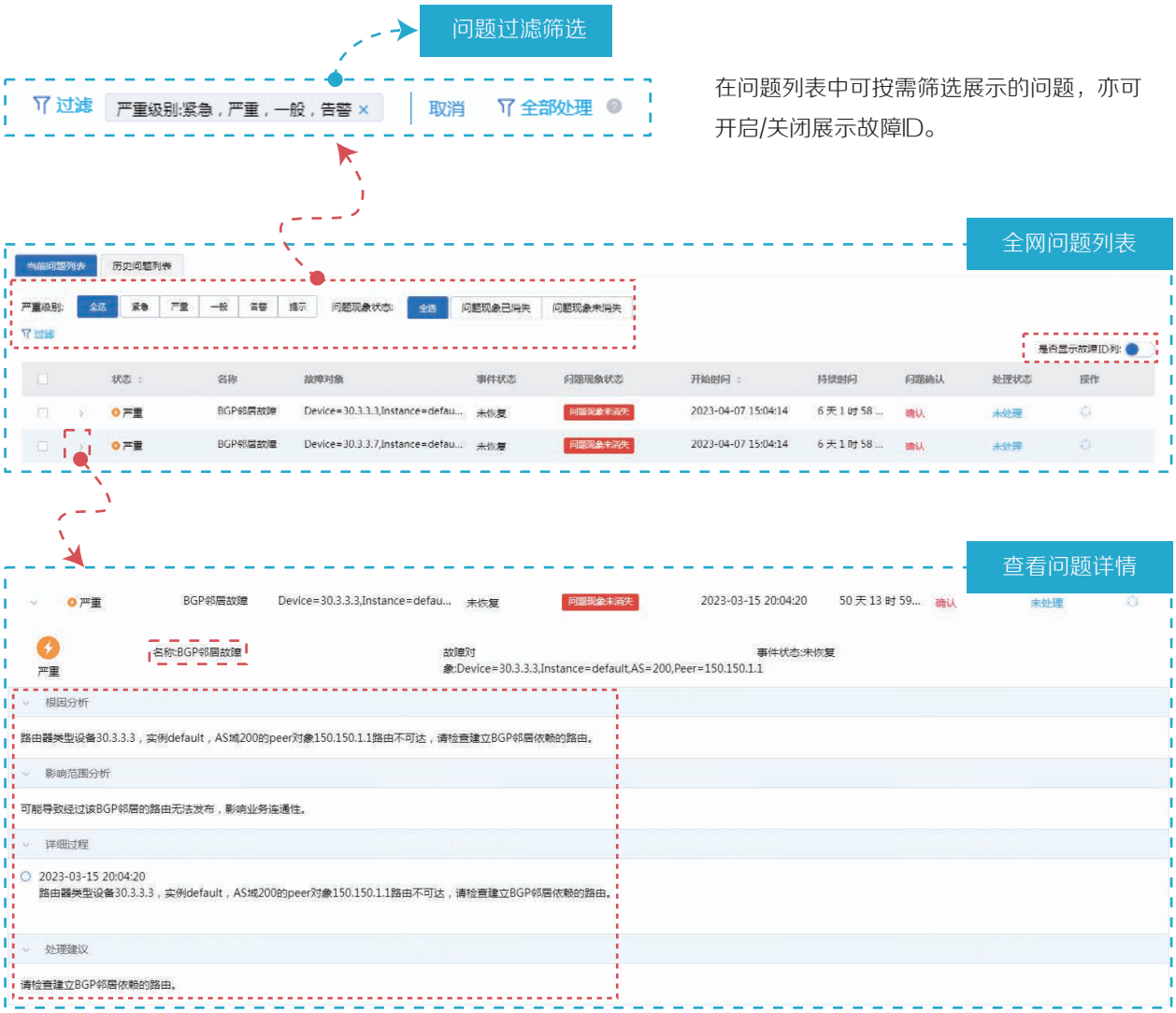
根据设备性能类、容量类、状态类展示全网设备故障信息。

根据网络状态类、策略类展示全网网络问题信息。

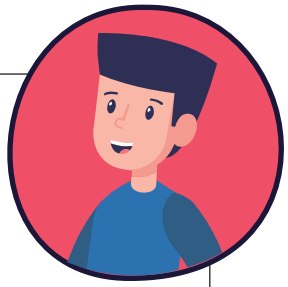
根据协议状态类展示全网协议问题信息。

针对不同的问题现象，用户可自定义选择是否告警。

问题列表展示当前系统中用户未手动处理、已手动处理的问题。未手动处理的问题将会纳入故障统计，已手动处理的问题不会纳入故障统计。



在问题列表中可按需筛选展示的问题，亦可开启/关闭展示故障ID。



典型故障Case举例：BGP邻居中断故障诊断

问题发现：

- 定时对纳管的设备进行轮询检查；
- 发现设备的BGP连接状态不是Edtablisded；

定位过程：

- 查询设备配置信息、设备接口信息、设备BGP状态信息，可以定位并通知用户设备出现了BGP故障问题及故障原因；

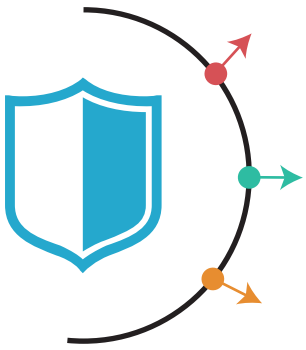
闭环动作：

- 用户可根据处理建议对故障进行处理，形成闭环。

用户可对故障问题进行处理及确认，确认后的问题将不再允许进行操作，将会在已处理问题列表进行展示。

用户可选择问题针对性的进行处理和确认，也可通过过滤筛选批量处理、确认问题。 全部处理

方案亮点



问题快速发现

分析组件通过对采集数据基于AI模型进行检测，以及网络数据的实时处理，快速感知网络故障。

问题快速定位

分析组件通过AI算法快速分析推理出故障原因及定位。

问题处理，形成闭环

分析组件给出根因分析、影响范围分析以及处理建议，方便用户快速解决问题形成闭环。

AD-WAN分支

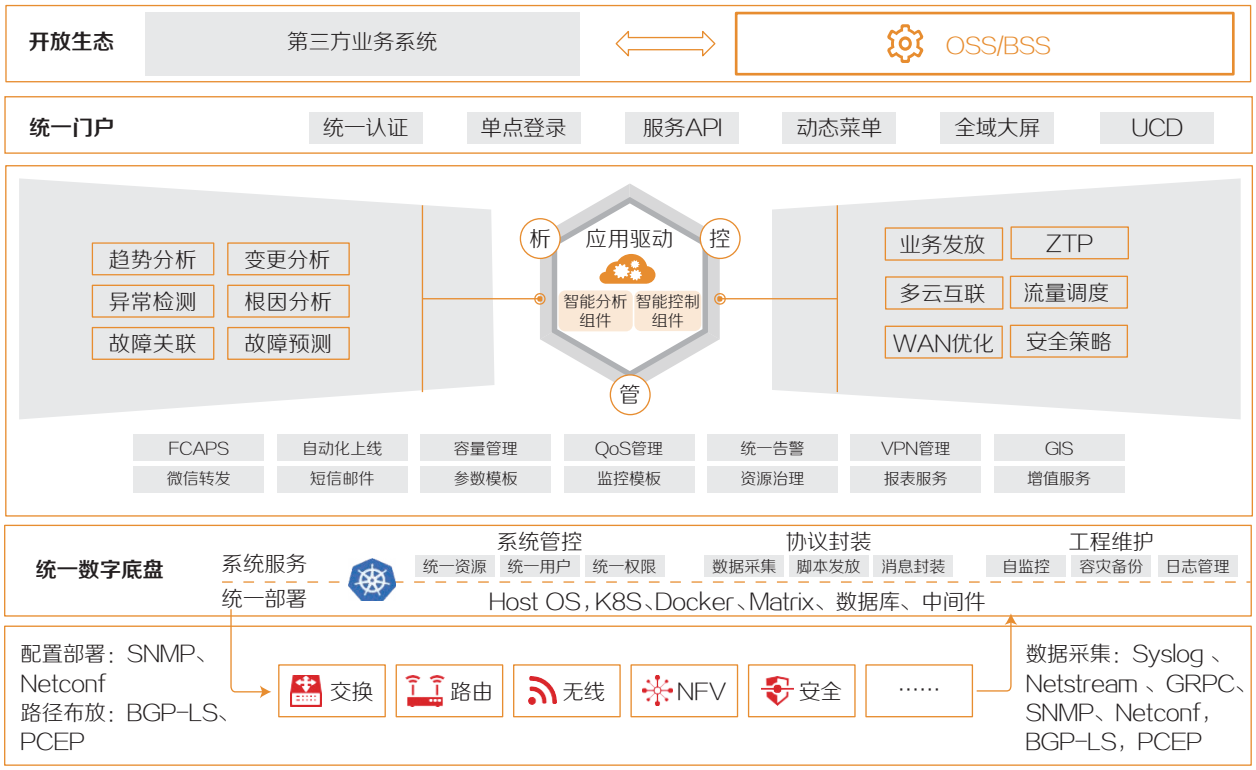
解决方案概述

方案概述

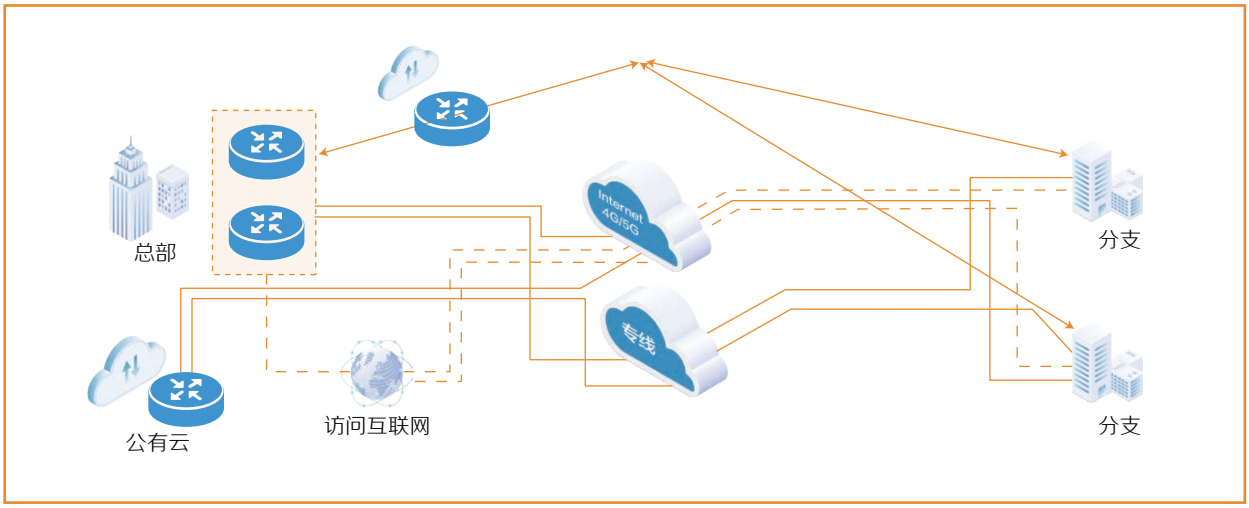
随着数字化转型的的深入和新业务不断涌现，越来越多的应用上云，公有云、私有云、混合云的多云联接成为新常态。伴随着应用的云化和智能化，业务对广域网的需求也发生了变化，广域网流量激增，从而驱动广域网发生变革。此时软件定义广域网SD-WAN就成为数字化转型中网络重构的关键。

H3C基于应用驱动的AD-WAN (Application-Driven Wide Area Network)分支解决方案，面向企业、能源、金融、交通等行业，提供分支与分支、分支与数据中心、分支与云之间的全场景随需互联，并通过ZTP零配置上线、智能选路、WAN优化、智能运维和全程安全等功能，为用户提供更好的业务体验。

采用SDN相关技术，AD-WAN是一个融合、分层、开放、智能的网络技术架构，统一融合智能管理模块、智能控制模块、智能分析模块，实现“管”、“控”、“析” 三维一体。面向用户、统一Portal，真正做到“一次登录、一键发放、一体保障、一站运维”，结合大数据分析与AI学习能力，抓取网络实时快照、离线建模，实现网络的智能预测与智能排错，助力广大用户实现数字化网络智能升级。



方案价值



降成本

- 灵活组网，提升线路利用率
- 数据压缩，节省广域网带宽
- 服务模式，降低建网成本

70%
节约成本

优体验

- RIR智能调度，保障关键业务
- 广域网优化和加速，提升用户体验
- 多云互联，快上云、上好云

50%
应用性能提升

简运维

- ZTP零接触部署，分钟级开局
- 端到端SRv6自动下发
- 可视化运维，分钟级故障定位

3倍
运维效率提升

高安全

- 站点安全，丰富的安全特性
- 隧道安全，自动化国密VPN
- 云端安全，SASE业务自动化

3层
安全防护

方案核心产品

AD-WAN

管控析智能融合

	路由器产品	安全产品
总部	 SR6600-X系列  SR6600/SR6602系列	 M9000系列
汇聚	 MSR5600系列	 F5000系列
分支接入	 MSR2600系列  MSR800系列  MSR1000系列  MSR3600系列  MSR 3610-I系列	 F1000系列
虚拟化vCPE	 vSR1000/2000	 vFW1000/2000

AD-WAN分支

双栈支持（IPv6平滑演进）

随着IPv4地址逐渐耗尽，IPv6网络的部署是未来趋势，但是网络演进无法做到一步到位，必然会存在IPv4和IPv6业务共存的场景。

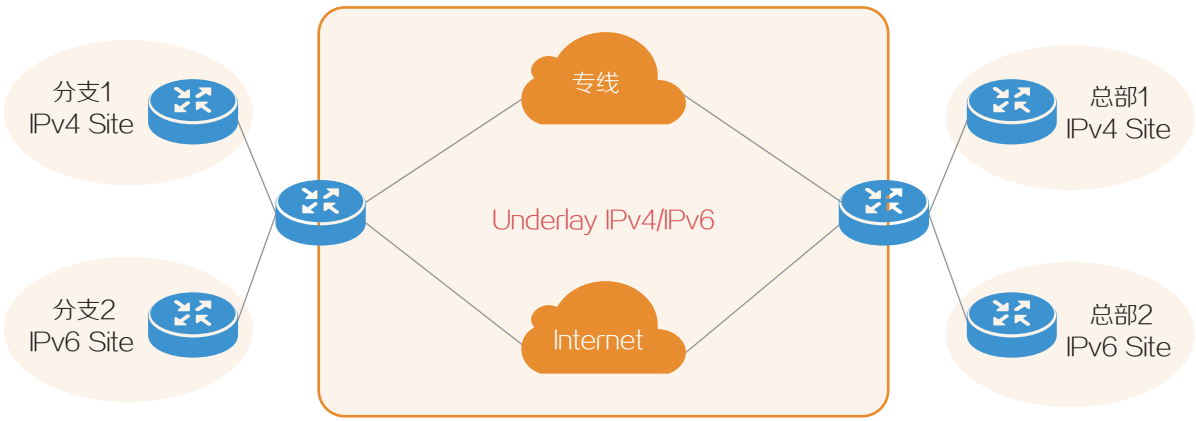
双栈协议的引入，改变了以往网络只能部署单一协议类型的问题。通过在网络设备上同时部署IPv4和IPv6协议，使得网络设备既支持IPv4接入，又支持IPv6接入，大大提高当前IPv4网络向IPv6网络过渡的可行性。

双栈协议简介

广域网中通常采用双协议栈作为过渡技术。

双协议栈是一种最简单直接的过渡机制。同时支持IPv4协议和IPv6协议的网络节点称为双协议栈节点。当双协议栈节点流量入接口配置IPv4地址和IPv6地址后，就可以在相应接口上转发IPv4和IPv6报文。双协议栈技术适合IPv4网络节点之间或者IPv6网络节点之间通信，是所有过渡技术的基础。

如下图所示，Underlay网络部署IPv4/IPv6双栈，使得IPv4和IPv6分支站点可以同时通过Underlay网络访问对应的总部站点。

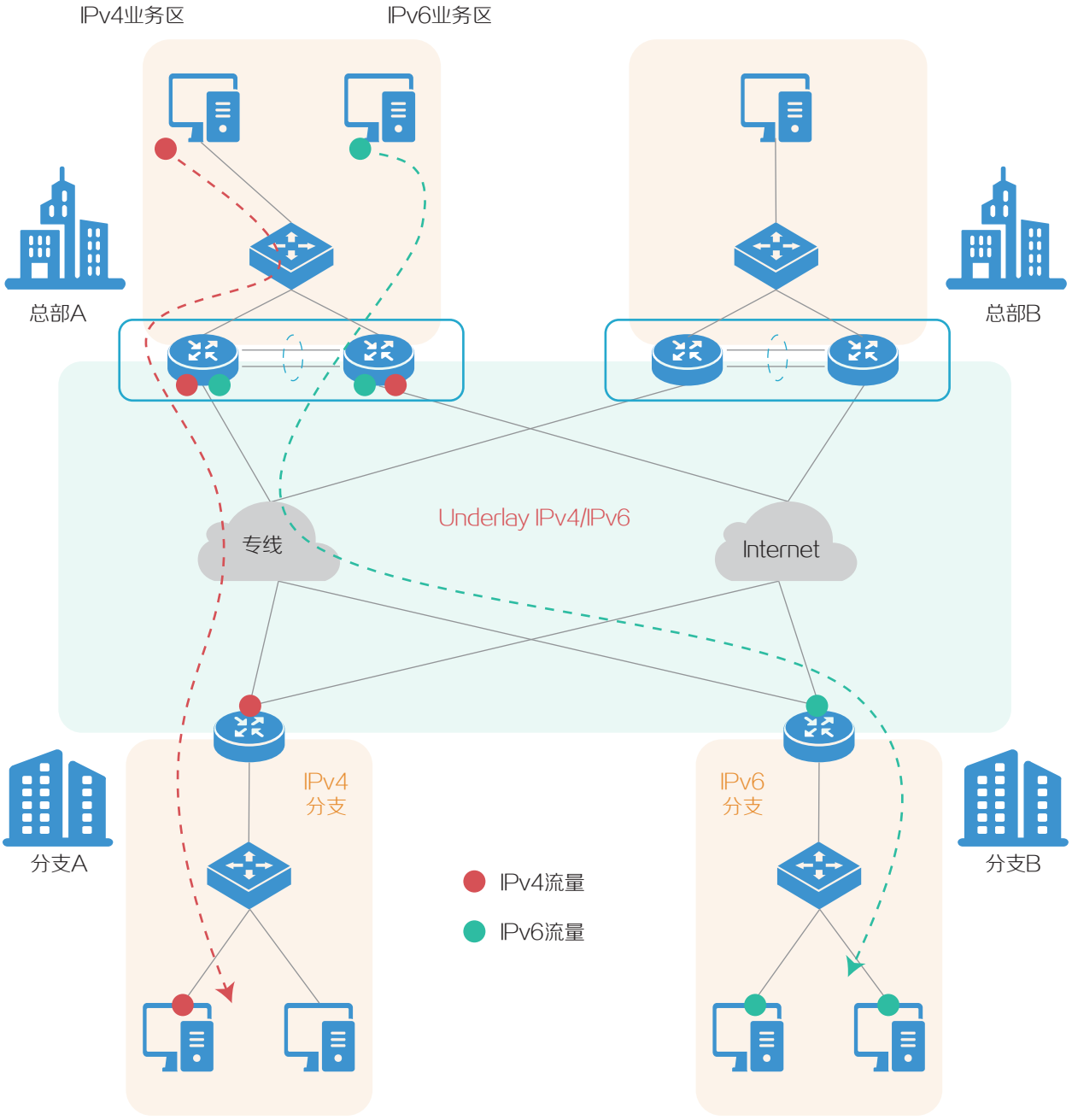


双栈部署方案

Underlay双栈 + Overlay双栈

如下图所示，WAN侧IPv4和IPv6双栈承载用户业务流量：

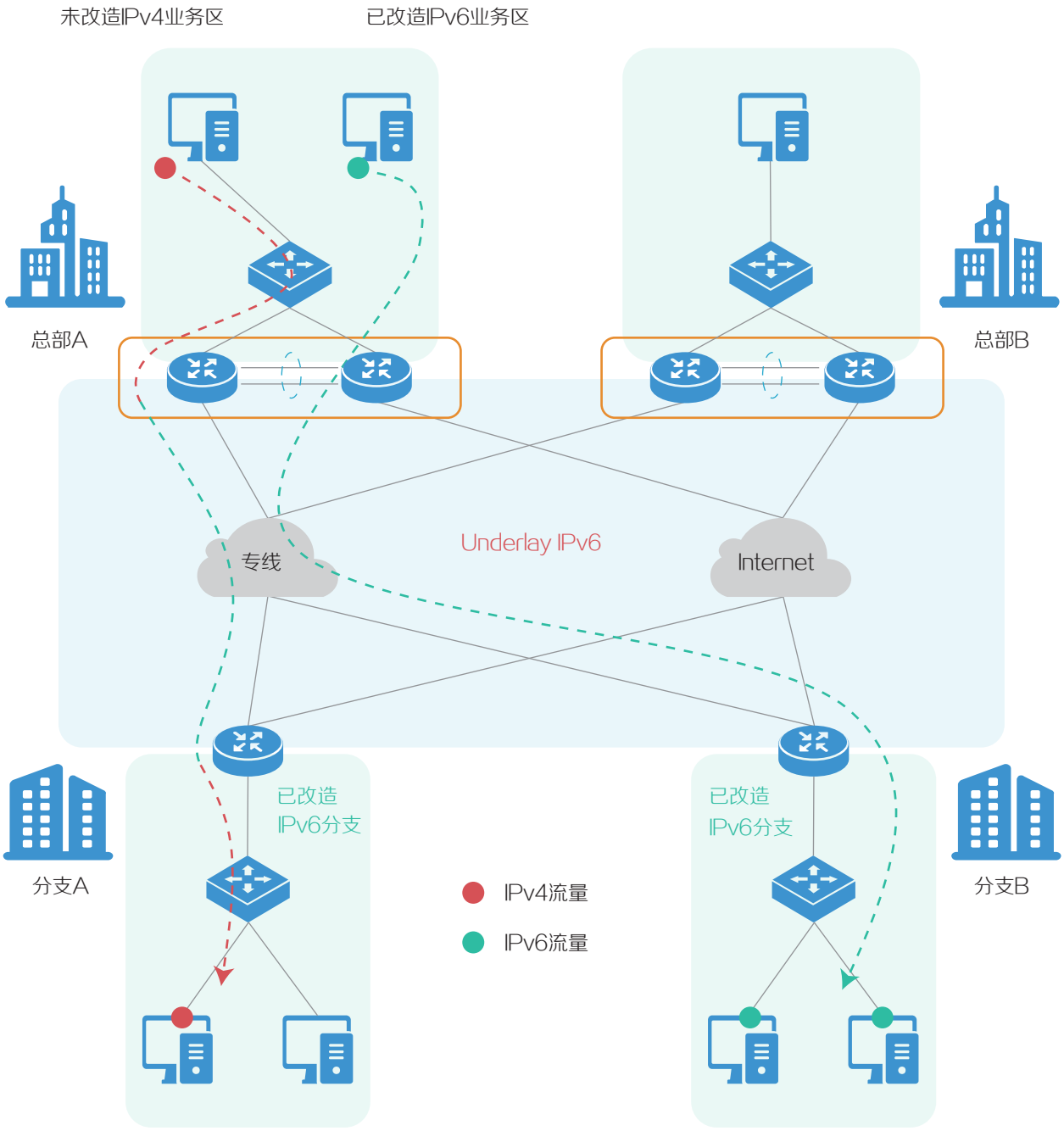
- Overlay网络为用户网络，可控性强，但也需要考虑整网各分支站点、各种存量业务分批次分阶段向IPv6过渡（甚至需考虑部分业务长期不支持IPv6）。
- Underlay网络跨越接入网、骨干网，涉及到边缘设备、中间传输设备、骨干网设备均需支持双栈部署。



Underlay IPv6 + Overlay双栈

如下图所示，AD-WAN网络的IPv6未来演进方向：

- 考虑部分存量应用无法改造支持IPv6，Overlay业务需长期支持双栈。
- Underlay网络全面完成IPv6改造（涉及到网络、终端）。



AD-WAN分支

站点上网

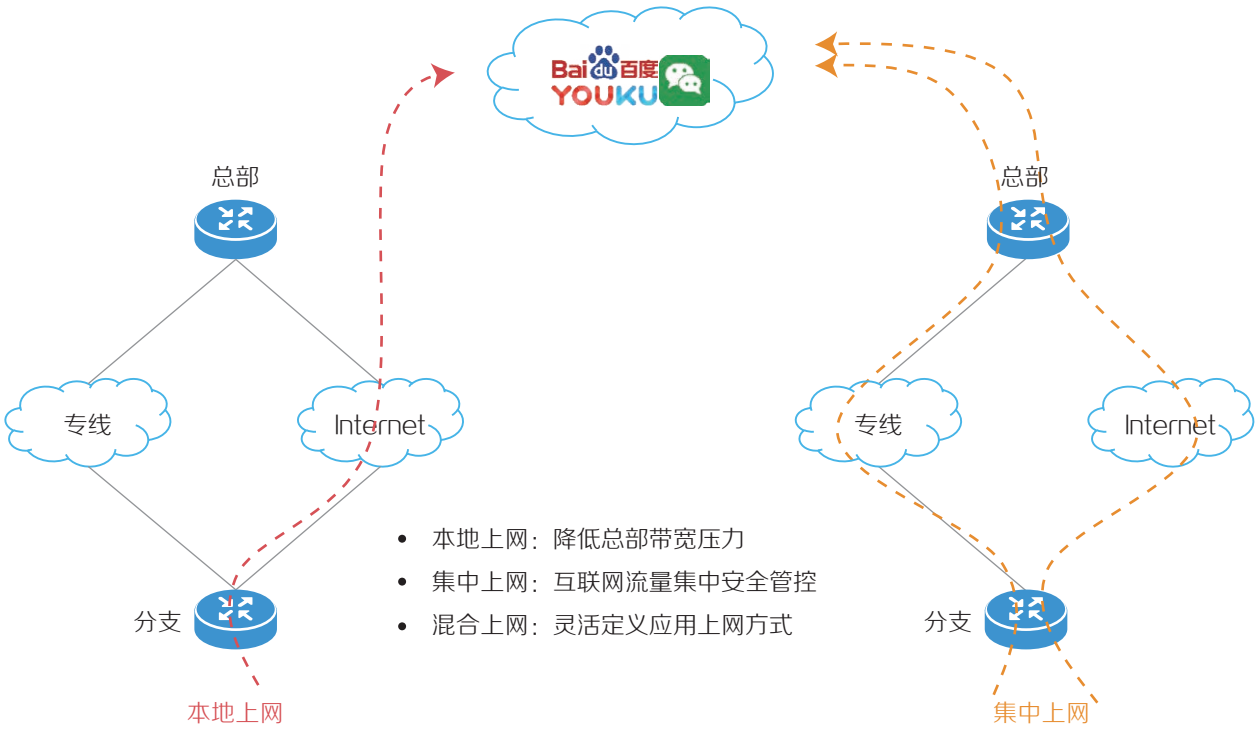
概述

AD-WAN解决方案将企业访问Internet的流量进行场景抽象和业务自动化编排，从而提供丰富多样的上网方式。通过将Internet做为一种业务进行自动编排，使得用户无需在复杂的场景中进行缺省路由的计算和规划，大大简化上网业务的配置。

功能简介

针对于不同企业上网管控需求不同，AD-WAN解决方案提供了不同的站点上网策略部署能力：

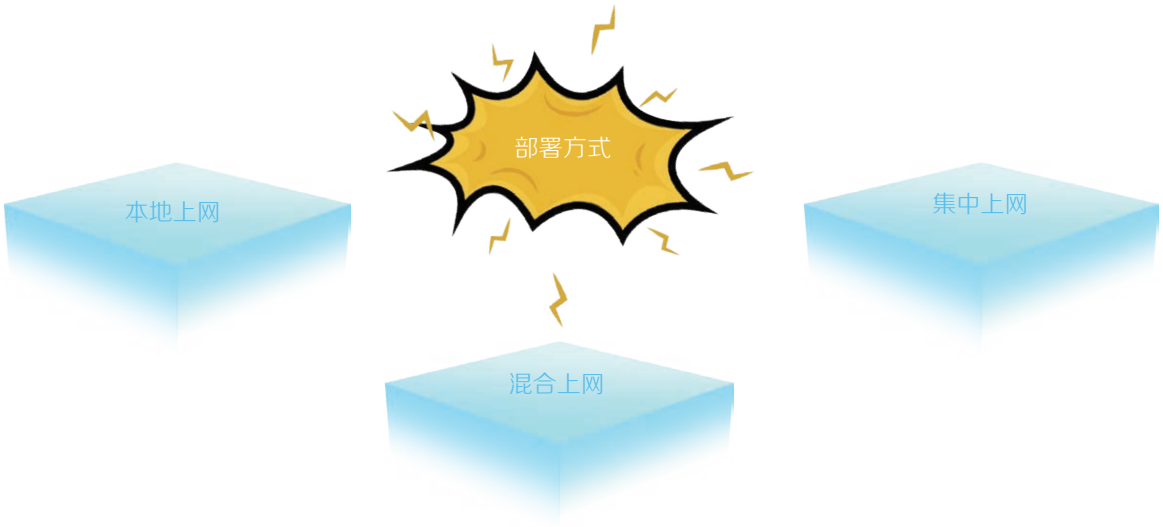
- 本地上网：上网流量从本地站点的Internet链路接口直接出局上网。
- 集中上网：企业内所有站点都需要通过企业的集中上网网关出局上网。
- 混合上网：默认上网流量通过集中上网站点出局，部分指定的业务流量通过本地Internet链路直接上网。



部署方式

传统场景下访问Internet的流量，本质上是缺省路由的计算和规划。在AD-WAN场景下，由于Underlay、Overlay、多业务VPN等概念的引入，人工去计算规划缺省路由显得尤为复杂和困难。AD-WAN解决方案将Internet流量做为一种业务进行自动化编排，使得访问Internet可以作为一种业务按需开启。

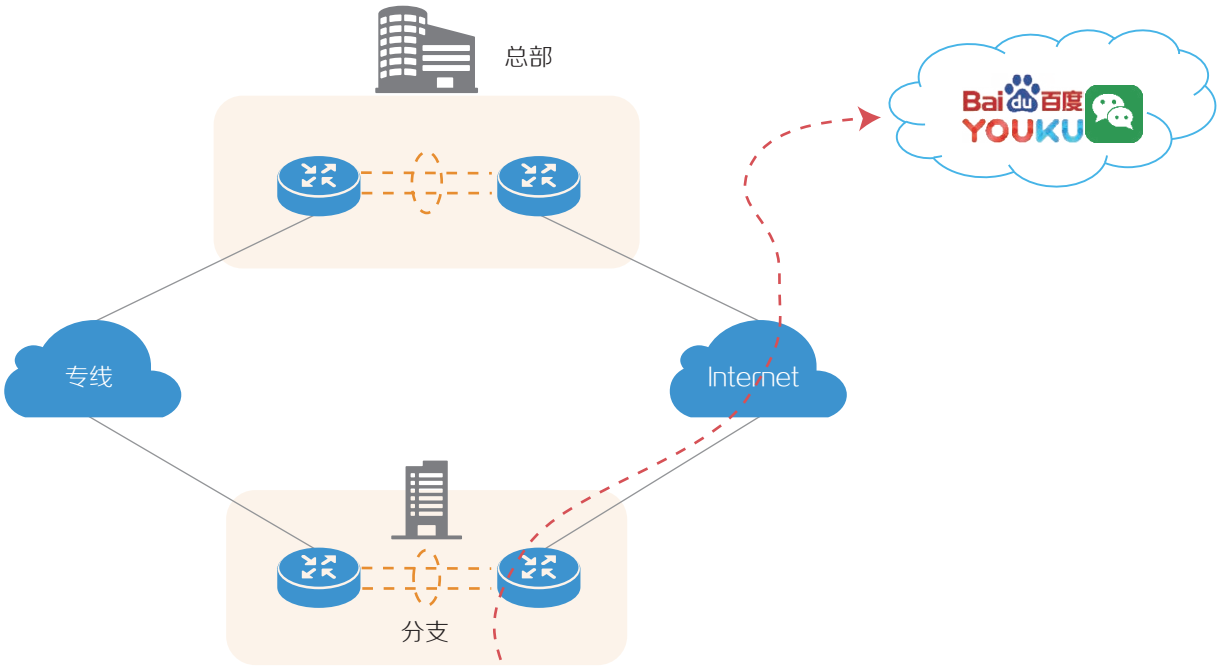
用户可以基于不同的部门/VPN来定义上网业务。即某个站点的某个业务VPN可以单独选择是否选择进行Internet访问以及通过以下方式中的哪一种方式进行Internet方式访问。



1、本地上网

本地上网需要选择上网出接口，如果同时选择多个访问Internet出接口，根据选择接口的优先级实现访问Internet链路的备份，支持配置相同的链路优先级访问Internet实现多条链路负载分担。

本地上网一般适用于规模较小的企业，每个站点都具有独立的Internet链路，并且所有站点上网流量不需要集中管控。可以基于不同的部门不同的站点配置本地上网策略。




VPN管理
LAN网络部署
VPN管理
区域拓扑
增加
刷新
VPN名称
VPN描述
VPN实例名称
站点信息
状态
操作
VPN1
VPN1
VPN1
站点信息
部署成功
444
444
444
站点信息
部署失败
lrj1
22
站点信息
部署失败
VPN2
VPN2
VPN2
站点信息
部署成功
共有 4 条记录，当前第 1 - 4，第 1 / 1 页
15 条/页
跳至
1
页


VPN管理 [VPN1] > 站点上网 > 本地上网
站点上网
返回
集中上网
本地上网
增加
刷新
站点名称
站点名称
配置状态
操作
暂无数据
共有0条记录
15 条/页
跳至
1
页


VPN管理 [VPN1] > 站点上网 > 本地上网 > 增加本地上网
增加本地上网
确定
返回
* 站点名称：
请选择
接口配置
增加
刷新
设备名称
接入上网接口
上网接口VPN
路由优先级
下一跳类型
下一跳IP
通断探测
探测IP
出方向动态地址转换
操作
暂无数据
共有0条记录
15 条/页
跳至
1
页

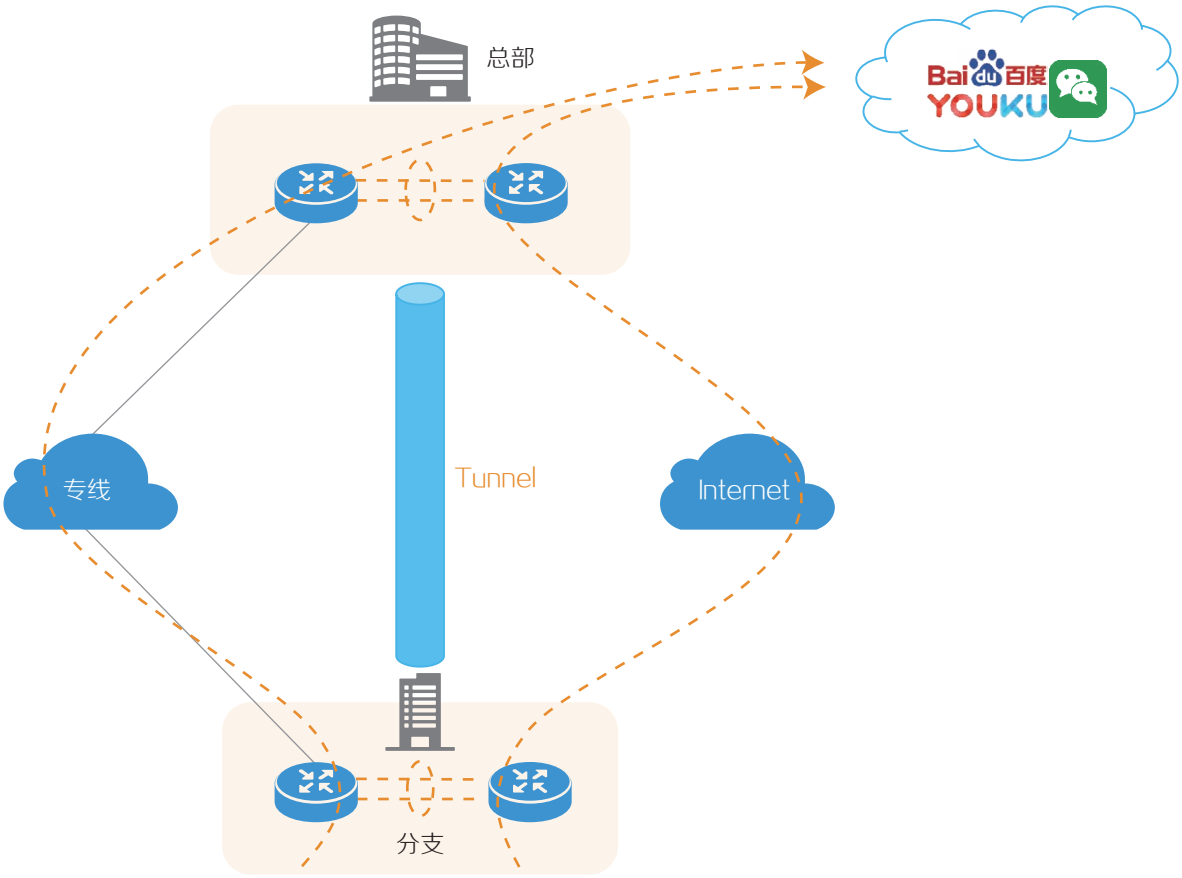

增加接口配置
* 设备名称：
请选择
* 接入上网接口：
请选择
上网接口VPN：
PublicInstance
* 路由优先级：
3
下一跳类型：
静态IP地址
* 下一跳IP：
通断探测：
开启
关闭
出方向动态地址转换：
开启
关闭
确定
取消

2、集中上网

集中上网是将需要本地上网的业务VPN与远端集中上网网关之间打通Overlay隧道，并且通过该Overlay隧道学习到指向集中上网网关的缺省路由。

集中上网一般适用于中大型企业，站点没有访问Internet的链路，或者是企业访问Internet的流量需要进行集中安全管控。

为了确保集中上网网关的可靠性，可同时选择两个站点作为集中上网网关，两个集中上网网关之间是主备方式。

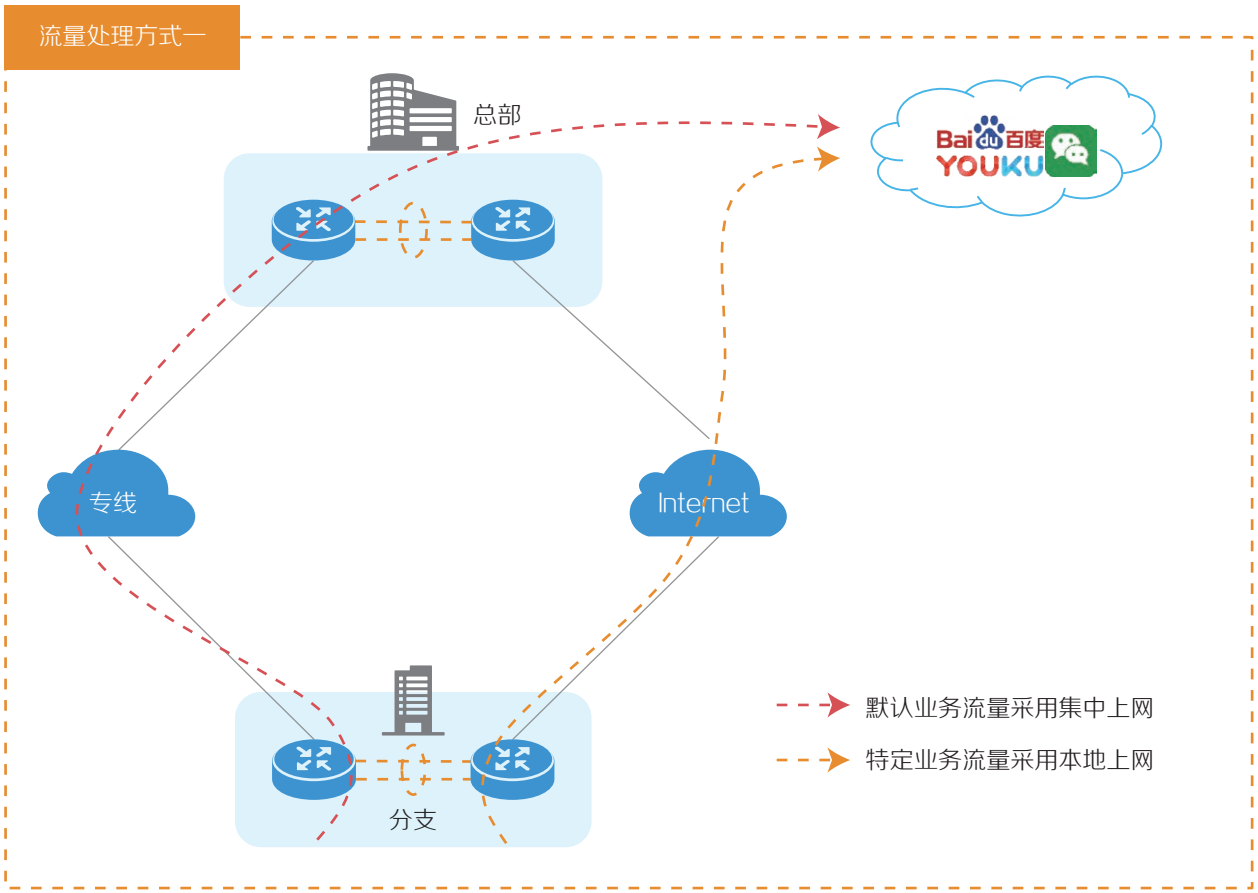


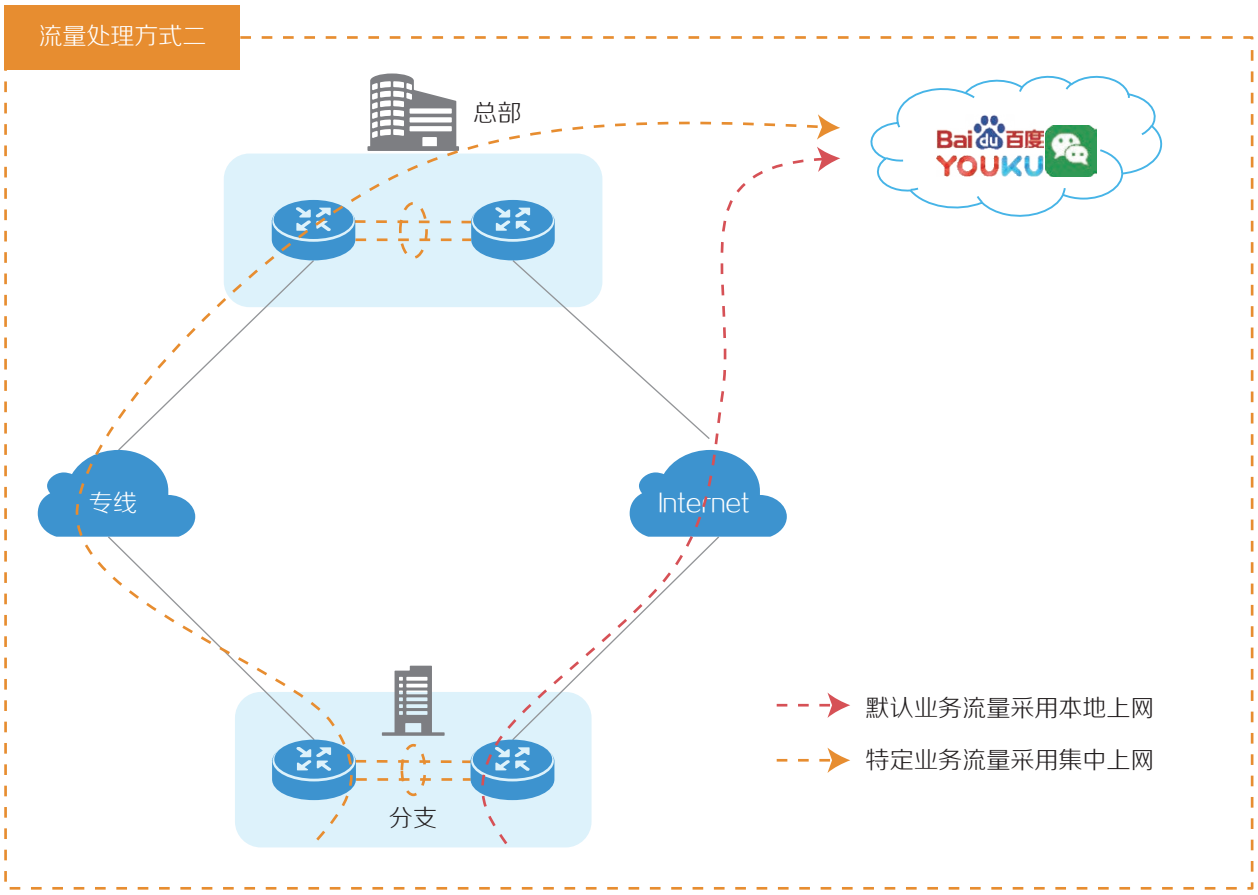
3、混合上网

混合上网是将本地上网和集中上网两种工作方式进行了有机的组合，一般适用对上网的流量需要集中安全管控，但是对于明确的指定业务的上网流量又可以指定从本地上网，以减少应用访问延迟，从而获取最佳的应用体验。

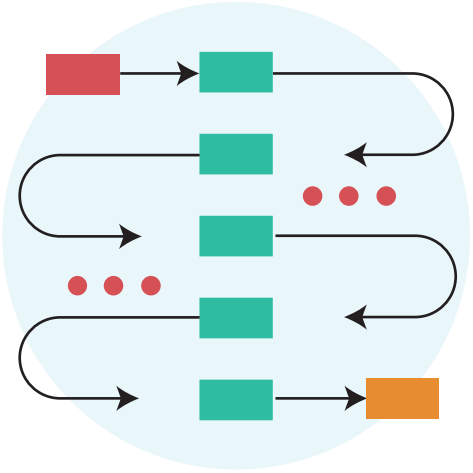
混合上网支持以下两种流量处理方式：

- 默认流量集中上网+特定流量本地上网
- 默认流量本地上网+特定流量集中上网


流量处理方式一
总部
专线
Internet
分支
默认业务流量采用集中上网
特定业务流量采用本地上网


流量处理方式二
总部
专线
Internet
分支
默认业务流量采用本地上网
特定业务流量采用集中上网

方案亮点



丰富多样的上网方式

AD-WAN解决方案将企业访问Internet的流量进行场景抽象和业务自动化编排，从而提供丰富多样的上网方式。

便捷的业务配置式

AD-WAN解决方案将Internet做为一种业务进行自动编排，使得用户无需在复杂的场景中进行缺省路由的计算和规划，大大简化上网业务的配置。

AD-WAN分支 4G/5G监控

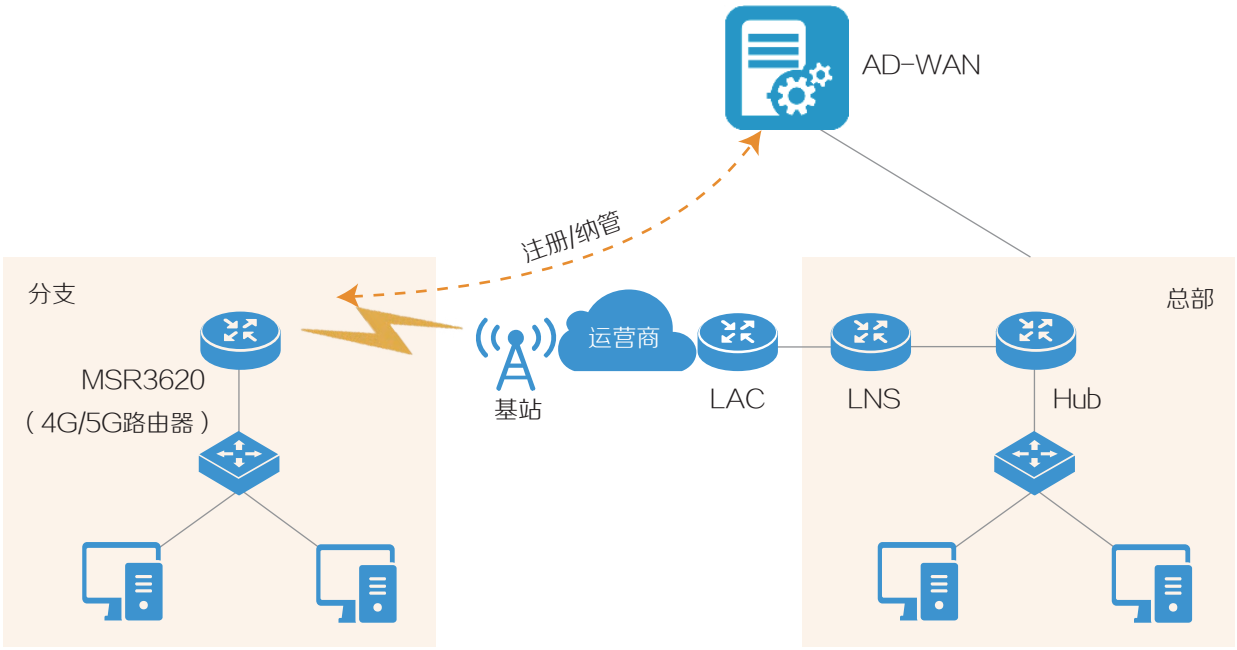
简介

近年5G技术发展迅速，用户业务使用4G/5G线路的场景越来越多。5G专线的质量逐步提高，通过接入4G/5G VPDN专线的方式在保障网络质量的同时可降低链路成本。

方案中的实现

AD-WAN实现对4G/5G VPDN（Virtual Private Dial-up Network，虚拟专用拨号网络）专线场景的支持，能够区分Internet网络和4G/5G专线网络。同时支持对4G/5G路由器或安装移动通信4G/5G Modem模块设备的状态和链路质量进行可视化管理及监控，辅助运维人员快速定位故障，运维层面更清晰，提升运维效率。

设备纳管 | 定位&电子围栏 | 监控可视化 | 告警



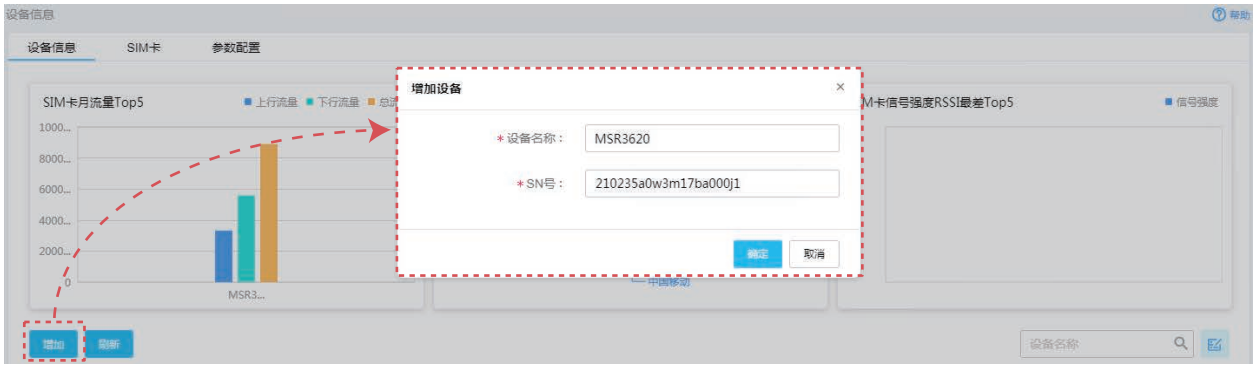
设备纳管

根据管理通道注册连接WebSocket通道，使支持4G/5G设备通过WebSocket上线。

1、在设备上配置

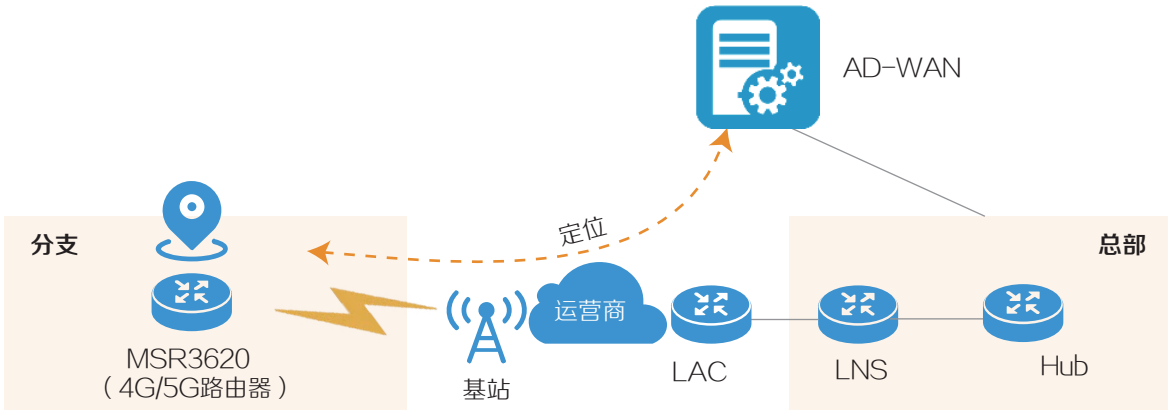
cloud-management server domain x.x.x.x（统一数字底盘北向地址）

2、在监控设备页面增加设备：



设备定位

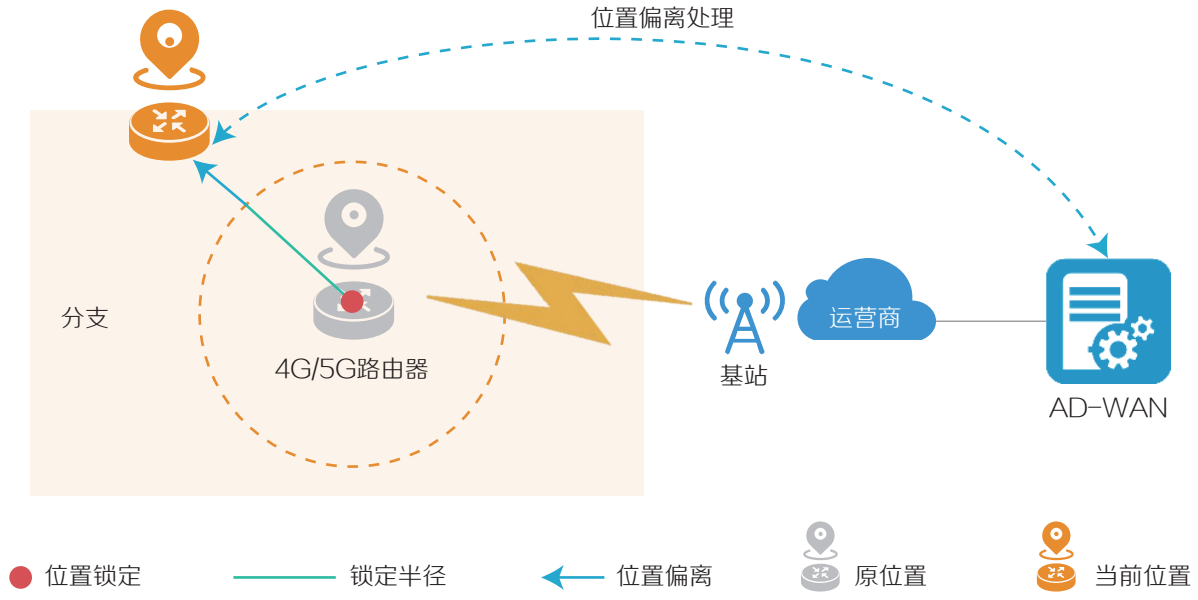
4G/5G路由器设备上线时，在AD-WAN上可根据基站信息查询设备经纬度和地理位置。



设备经纬度和地理位置

电子围栏

电子围栏是根据设置设备位置锁定和租户全局锁定策略，如果设备发生偏离位置，查询当前全局锁定策略，发送设备位置偏离通知。



设备位置锁定

根据用户需求选择锁定设备方式：使用当前位置或自定义经纬度。

租户全局锁定

1、锁定半径

以设备锁定位置为中心点向外延伸的长度为锁定半径（单位：m）。锁定位置及锁定半径能确定一个区域，超出该区域的位置会相对于锁定位置产生一个偏离。

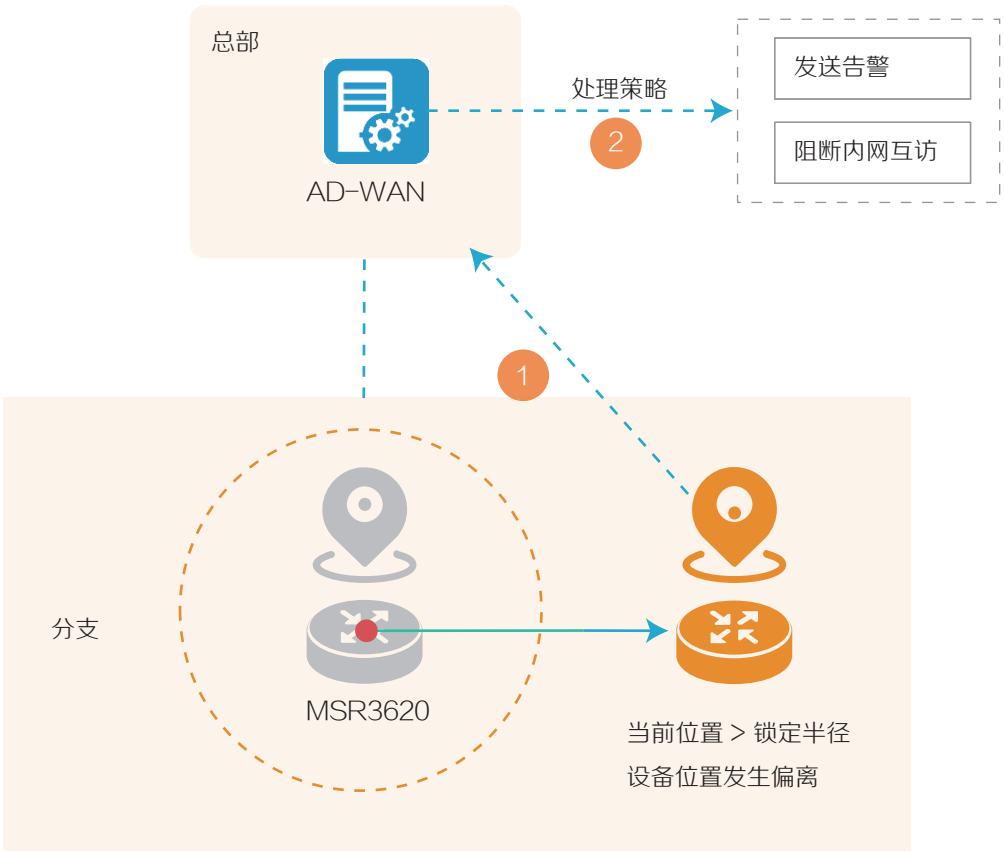
2、超出锁定位置策略

设备位置发生偏离时，用户自定义位置偏离处理策略，可同时配置两种处理方式：

- 发送告警：产生设备位置偏移告警
- 阻断内网互访：在接入区的RR设备上下发 peer x.x.x.x ignore配置，断开设备与RR的overlay连接。

阻断内网互访需在分支控制组件上线，站点角色为CPE，且已接入接入区。

设备位置偏移



1、当4G/5G设备发生偏离，在设备信息页面显示偏离经纬度。

设备发生偏离，显示偏离经纬度

2、根据超出锁定位置策略处理：发送告警和阻断内网互访

发送告警

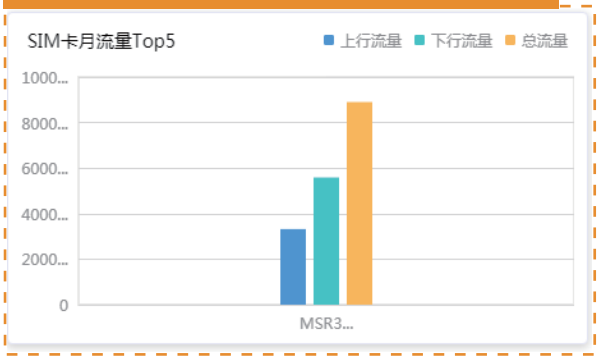
阻断内网互访

4G/5G设备监控

在AD-WAN上支持统计设备名称、IMSI、运营商、SIM卡状态、信号强度（RSSI）、状态、在线时长（管理通道）、离线时长、下行流速、上行流速、本月总流量、电子围栏使能状态（是否锁定位置）、是否已偏离。

设备信息

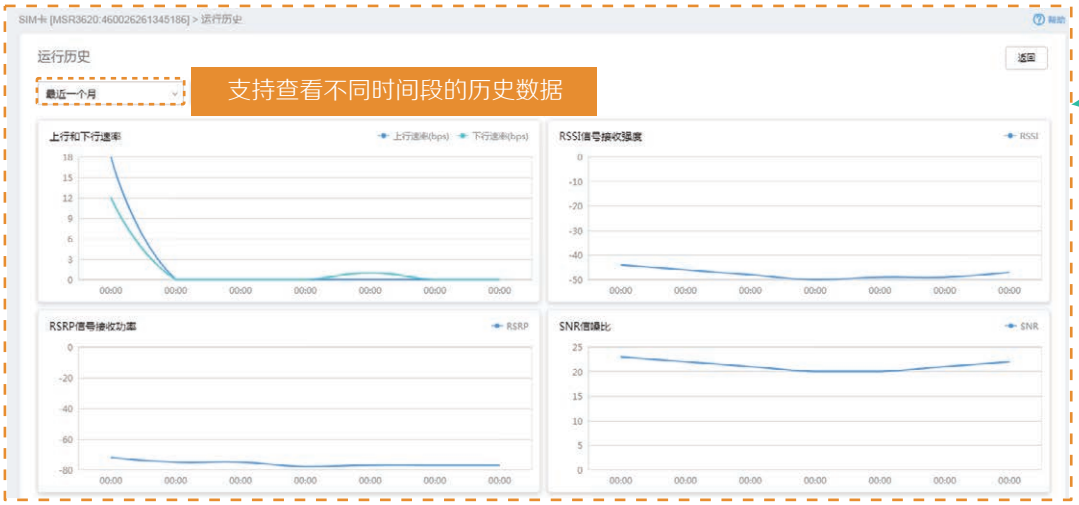
以月为统计单位各流量排名Top 5的设备统计图



设备接入运营商分统计图布

SIM卡信息

查看SIM卡相关信息，包括设备名称、IMSI、手机号、运营商、SIM卡状态、上下行速率、上下行流量、月累计流量、套餐总流量、信号接收强度、信号接收功率、信噪比运营商分布等。



方案亮点

灵活线路选择

具体化网络类型，能够区分Internet网络和4G/5G专线网络。

灵活配置

支持总部设备和LNS设备合一、分离两种不同的方案，用户可以根据不同的组网场景进行灵活配置。

灵活组网

通过Radius标准认证协议对分支站点的拨号进行认证，屏蔽了不同运行商的差异，使得组网更加灵活。

AD-WAN分支
安全架构

面临的挑战

公网

数据易被窃取，不安全

纯Internet网络质量差

VPN

自建VPN搭建维护复杂

开源潜在漏洞风险

专线

专线价格高

施工周期长

无法弹性伸缩

传统广域网面临的挑战

高成本
- 分支网络节点多
- 传统专线昂贵

扩张慢
- 专线申请开通周期长
- 网络配置复杂
- 需要专业技术人员实施

网络不可靠
- 互联网质量不稳
- 故障及时处理难
- 关键业务质量无保障

运维能力弱
- 节点分散，集中管控难
- 故障定位恢复慢
- 人工配置错误率高

安全能力缺失
- 传统设备仅支持ACL
- 缺乏深层安全能力
- 设备部署和策略配置复杂
- 全面安全建设费用高

方案介绍

广域网：网络即服务

软件定义网络

为满足更加灵活的广域网建设要求，降低运维和部署成本，组网快速开局、零成本上线、QoS质量控制、智能选路、高可靠性、网络可视化等，成为新型广域网方案的基本能力。

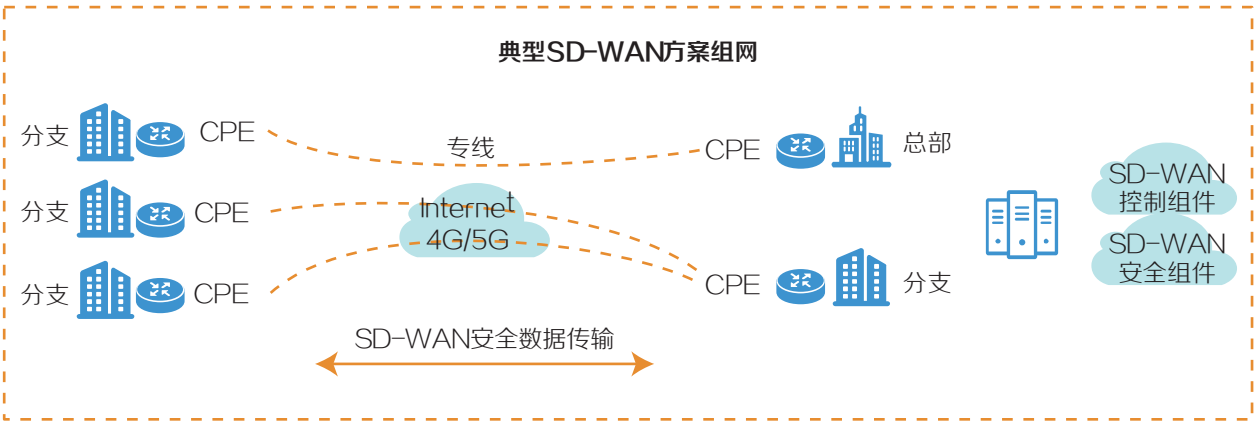
安全：安全即服务

软件定义安全

在网络安全法和等级保护2.0的要求下，广域网安全建设迈向新阶段。为满足边缘节点安全能力需求，全网需具备统一的设备部署、统一管理、策略配置、威胁防护与可视化呈现等能力。

网安融合：网络服务化，安全服务化，业务自动化，管理统一化

网安融合最佳实践



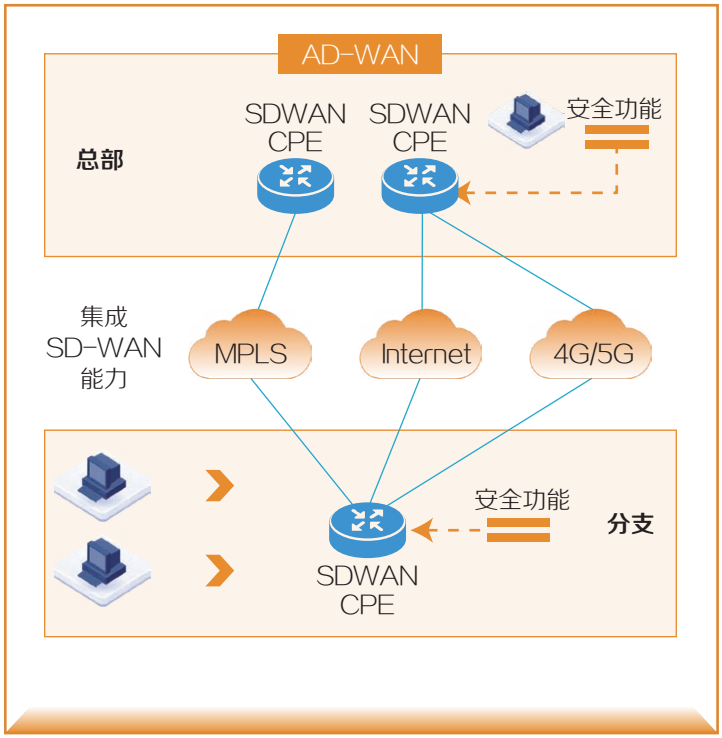
应对WAN挑战的关键能力

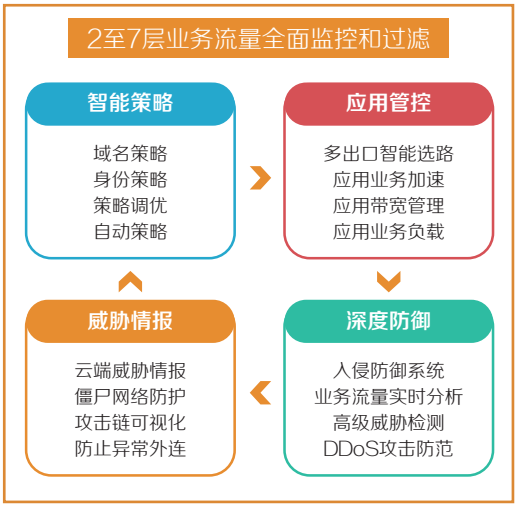
- 支持混合链路接入（MPLS/Internet/5G等）
- 全自动服务开通，灵活组网
- 支持动态链路调整，保障关键应用可靠运行
- 企业广域网管理简单高效

安全防护成为关键功能

- 主动安全体系融入网络，保障端到端全程安全
- 连接云端安全能力中心，提升安全防御能力
- 融合态势感知平台，全网安全态势可见
- 海量分支接入安全，端侧安全ALL IN ONE

业务融合自动编排





端到端的全网自动化安全防护

从分支到总部，再到云端，全流程自动化的安全防护能力，保障链路安全、数据安全、业务安全，提高安全运维效率，降低安全运维成本。

设备集成FW、IPS、AV、URL过滤等安全功能，实现端到端全程安全保障

核心价值

降本增效，稳定可靠

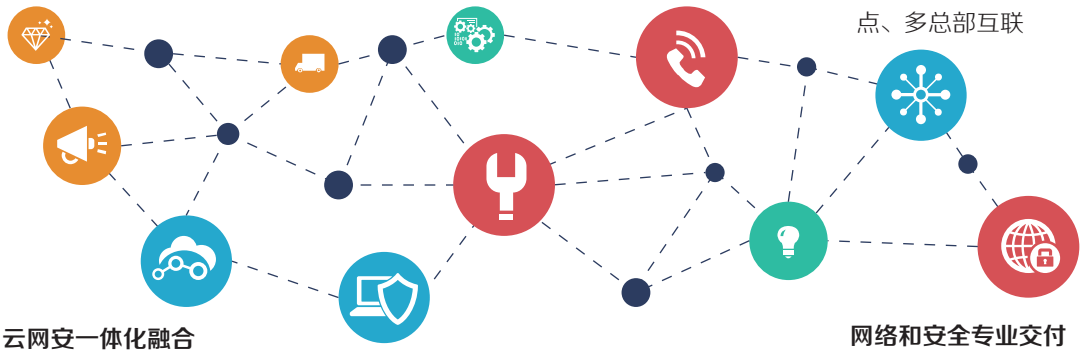
带宽弹性更具性价比，上云成本低

灵活部署，极简运维

ZTP安装，永不掉线的远程管理

全场景多端接入

海量分支节点、边缘节点、多总部互联



云网安一体化融合

原生安全接入云，安全资源随需部

安全能力全面提升

集成丰富安全功能，保障业务数据安全

网络和安全专业交付

具备全国交付能力的网络和安全专业服务商

AD-WAN分支 NetStream流分析

简介

NetStream是一种基于网络流信息的统计技术，定义了用于设备输出网络流量统计数据的方法，设备对通过的数据进行统计、分析，并上报给网络流量分析组件，经合并处理后存入数据库，并进行下一步的分析处理。为网络管理人员提供详细的数据流统计信息，帮助其了解企业内部网络的运行状况，及时发现并解决网络中的性能瓶颈问题、网络异常现象，也可为用户进行网络优化、网络设备投资、网络带宽优化等提供参考。

方案介绍

H3C AD-WAN解决方案中，分析组件采用NetStream技术在设备的各端口上采集业务流量，以提供更加精细化的业务流量分析能力。

目前分析组件主要提供以下分析能力：

接口流量分析

基于设备接口进行网络流量分析，能够统计全网所有设备接口的流量排名。

VPN流量分析

基于VPN进行流量的分析与统计，展示VPN的全网流量Top排名等。

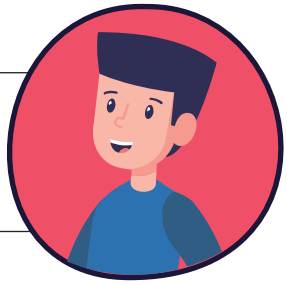
应用流量分析

应用流量分析关注全网应用，计算应用的流量、流速指标，以及每个应用的详细情况。

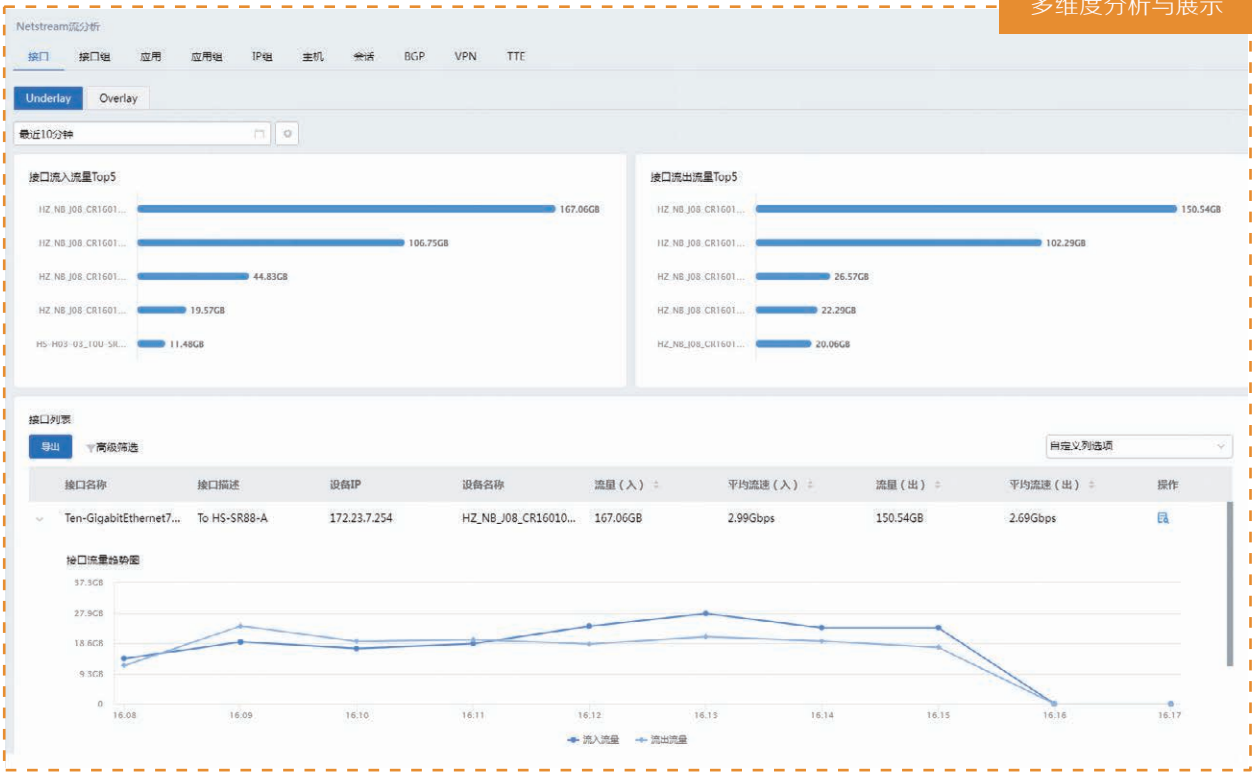
应用组流量分析

通过在分析组件或者控制组件定义应用组信息，可在NetStream流处理中根据流量的五元组信息匹配应用，同时匹配应用所属的应用组，对流量进行统计分析。

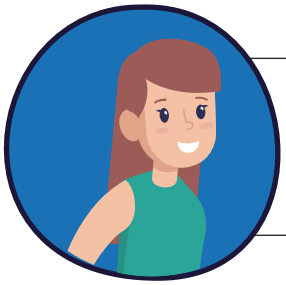
除上述维度以外，分析组件还支持基于接口组、IP组、主机、会话、BGP、TTE维度对业务流量进行分析与展示。



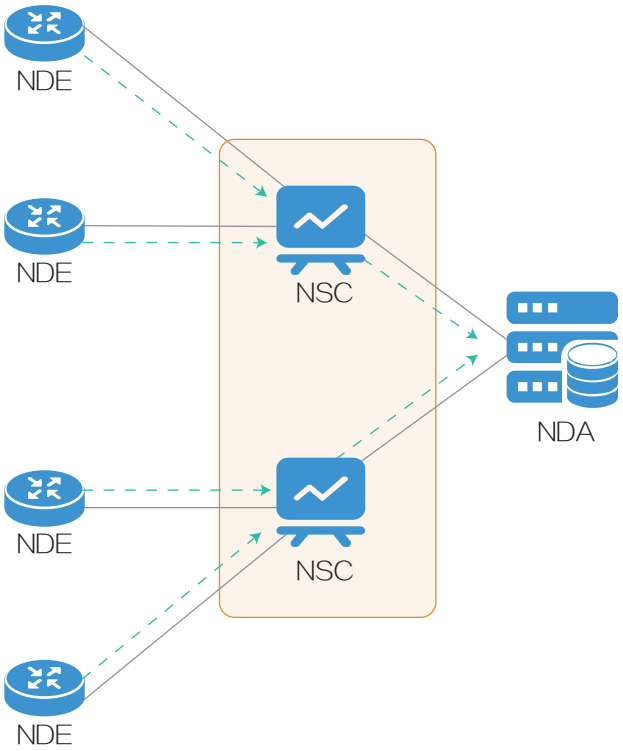
多维度分析与展示



技术介绍



一个典型的NetStream系统由NDE（NetStream Data Exporter，网络流数据输出者）、NSC（NetStream Collector，网络流数据收集者）和NDA（NetStream Data Analyzer，网络流数据分析者）三部分组成。

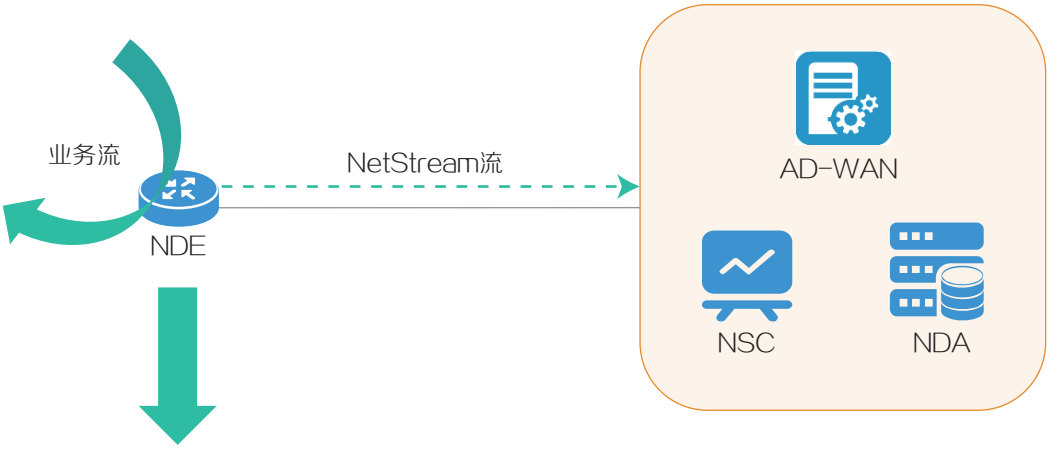


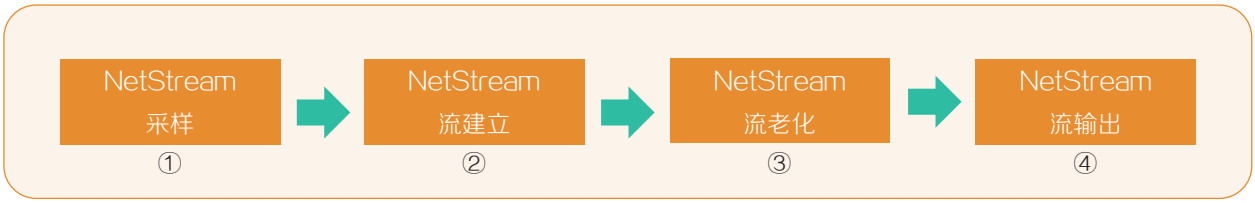
NetStream系统中的设备角色

- NDE：把采集到的关于流的详细统计信息定期发送给NSC。
- NSC：将统计信息收集到数据库后发送给NDA。
- NDA：对数据进行分析，用于计费、网络规划等应用。

AD-WAN分析组件支持NetStream功能，实时统计业务流量信息并进行分析与展示。
设备作为NDE的NetStream处理过程主要分为以下几个步骤：

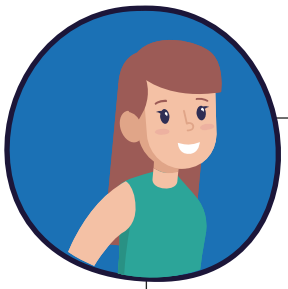
NetStream流老化是设备向AD-WAN分析组件输出流统计信息的前提。





① 设备按照配置的采样方式对业务流量进行NetStream采样
② 设备根据关键值对采样报文进行NetStream流建立
③ 设备按照老化方式进行NetStream流老化
④ 设备按照输出方式进行NetStream流输出

功能介绍

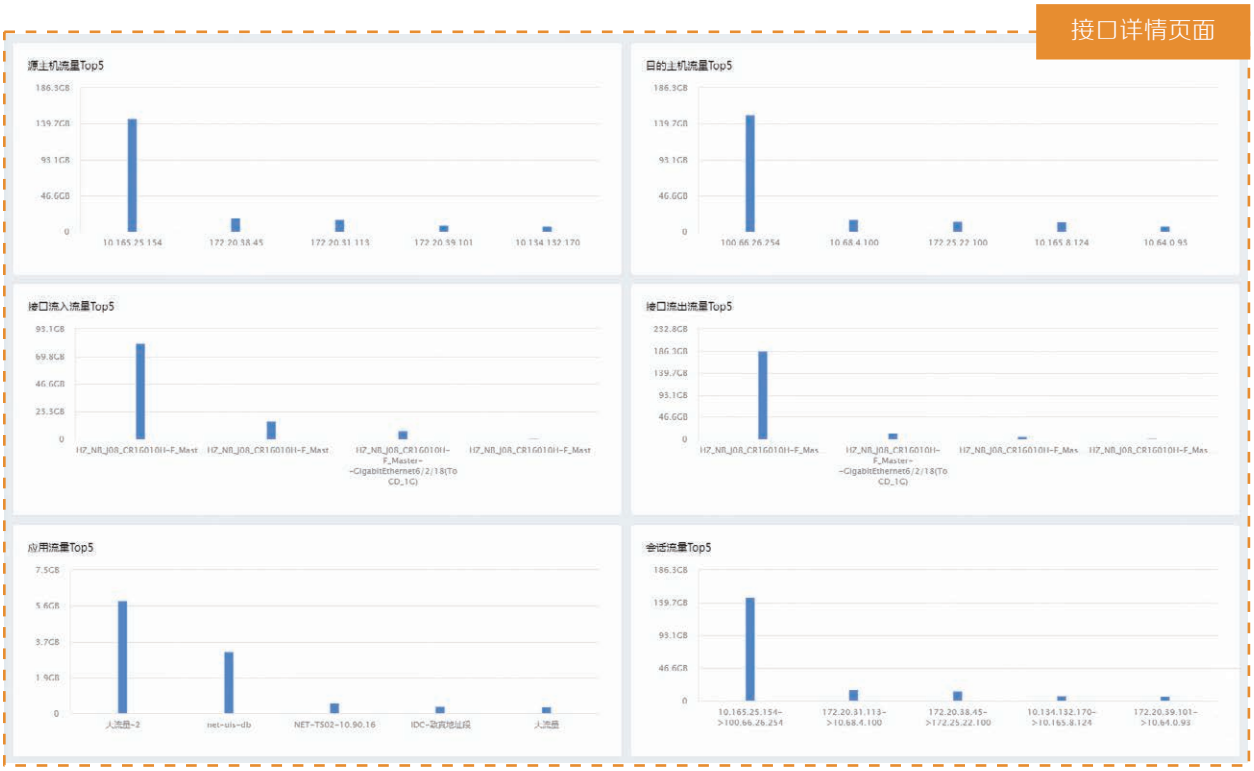


Netstream流分析利用Flink分布式计算引擎，将设备上报的NetStream网络流量进行实时解析和处理，通过从AD-WAN获取应用定义信息，识别出每个五元组所属的应用，基于不同维度对网络流量进行可视化度量，分别展示不同维度下的流量Top排名、流量趋势和流量详情列表等。

展示维度

NetStream流分析所有维度均支持查看流量基本信息和流量详细信息，本文主要展示流量基本信息。

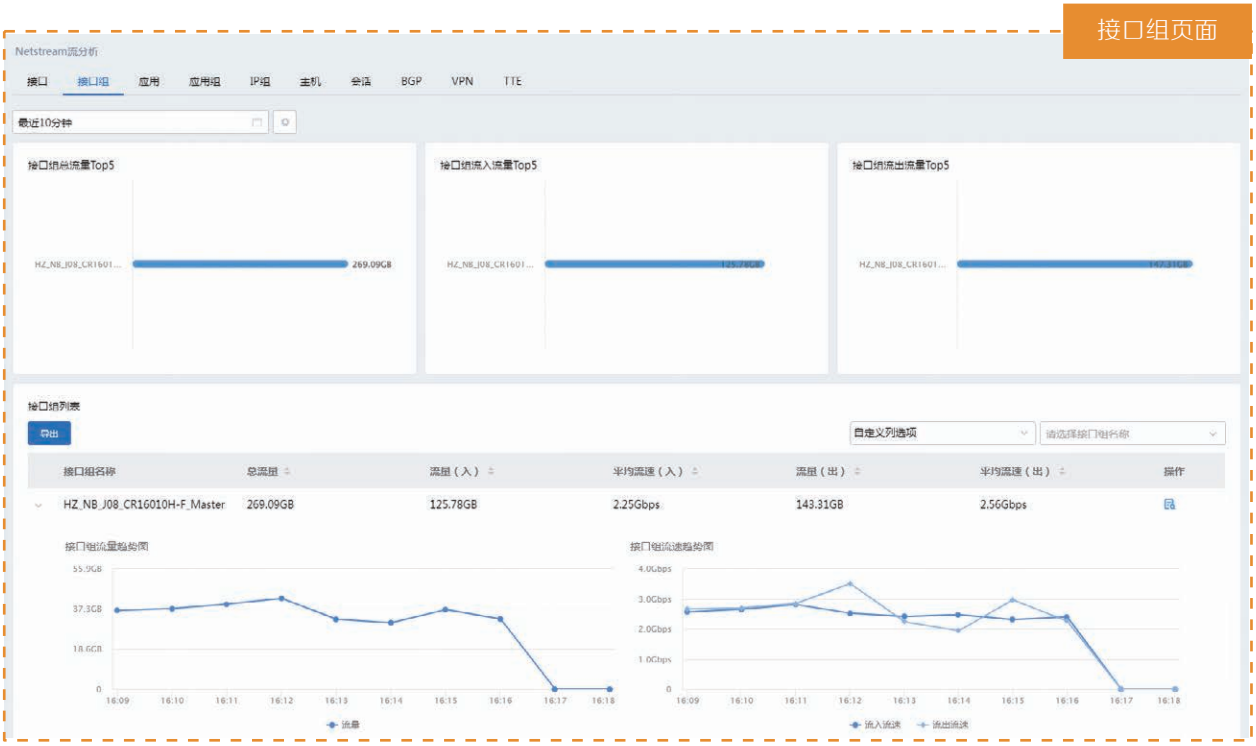
接口流量分析：基于设备接口进行网络流量分析，能够统计全网所有设备接口的流量排名。展示接口流量趋势，并且可以查看每个设备接口的网络流量详情，分析该接口上流量的应用流量排名、会话流量排名、源（目的）主机流量排名、接口流入（流出）流量排名等。



AD-WAN方案支持用户在全局配置中，将一组想关注的设备接口自定义为接口组，并在NetStream流分析功能中对这一组接口统一进行流量分析与展示。

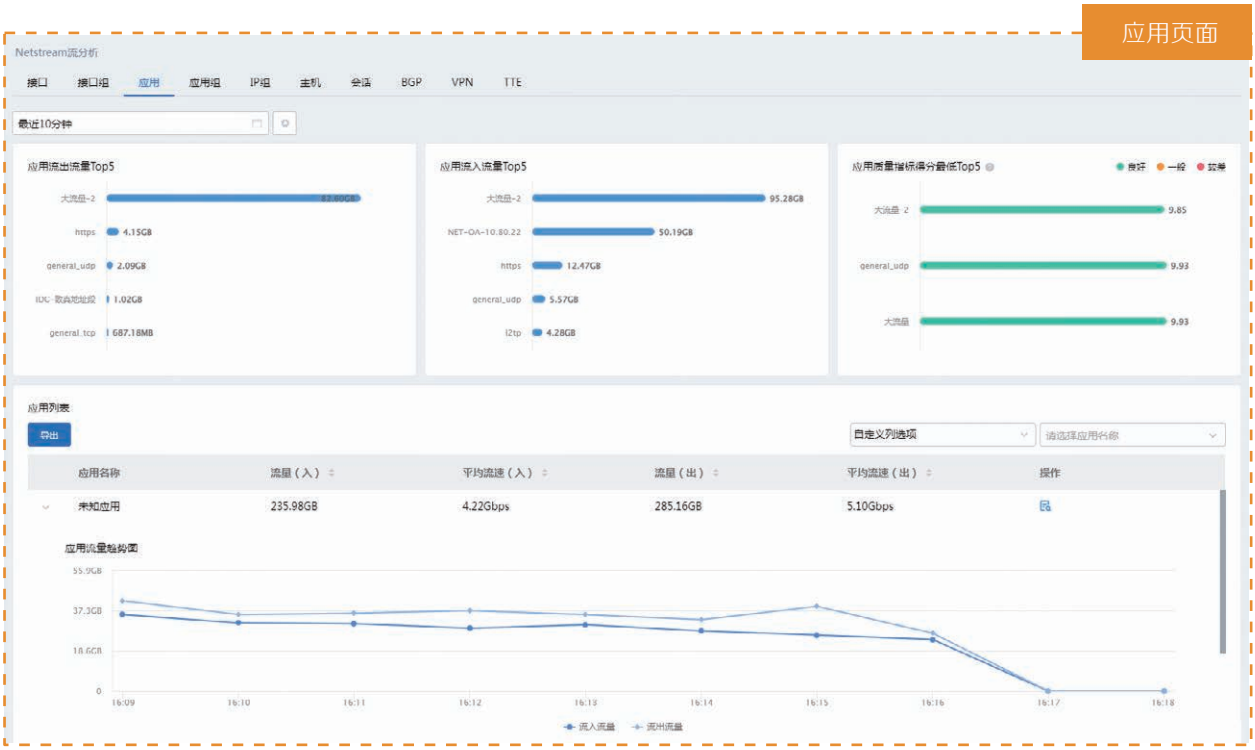
接口组流量分析：基于配置的接口组规则进行网络流量分析，能够统计全网所有接口组的流量排名，展示接口组流量趋势，并且可以查看每个接口组下的网络流量分布情况。

接口组页面



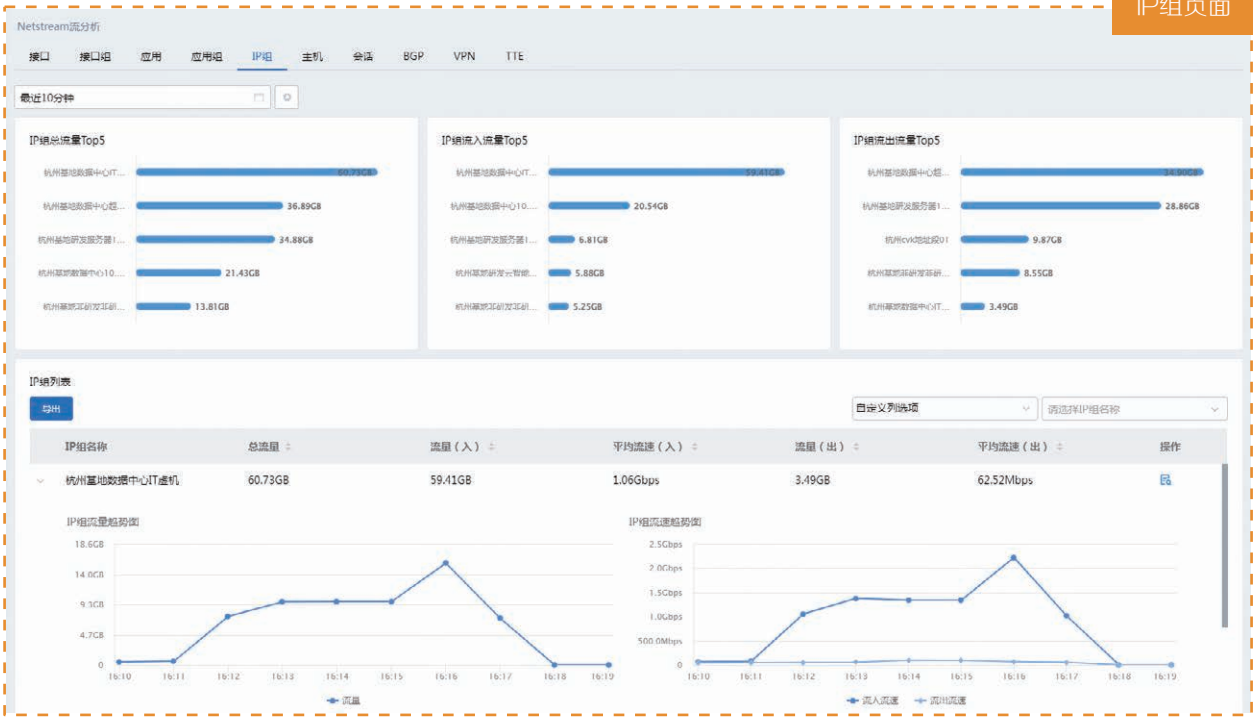
应用流量分析：基于应用进行网络流量分析，可对全网应用进行流量分析，计算应用的流量、流速指标，以及每个应用的详细情况，包括应用的五元组列表（五元组的流量路径）、应用的通信质量、应用在设备组网中的分布情况以及访问该应用的源主机排名等。

应用页面



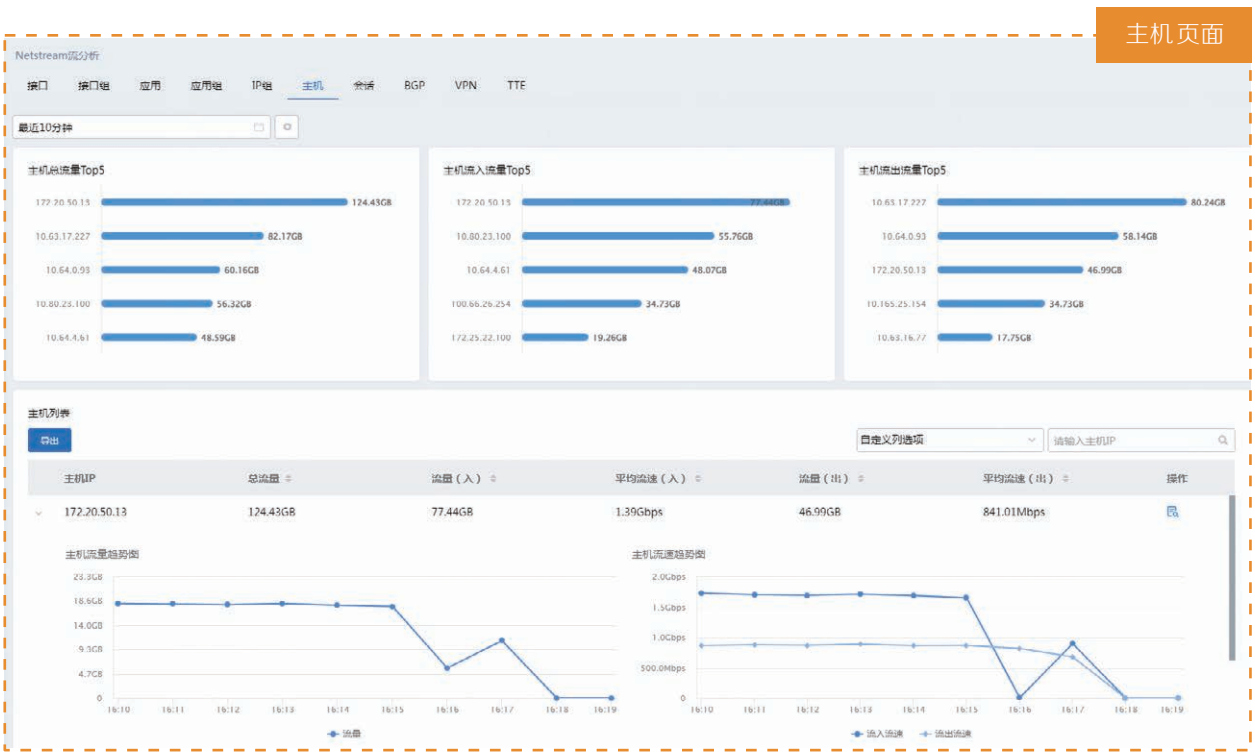
IP组流量分析：基于配置的IP组规则进行网络流量分析，能够统计全网所有IP组的流量排名，展示IP组流量趋势，并且可以查看每个IP组下的网络流量分布情况。

IP组页面



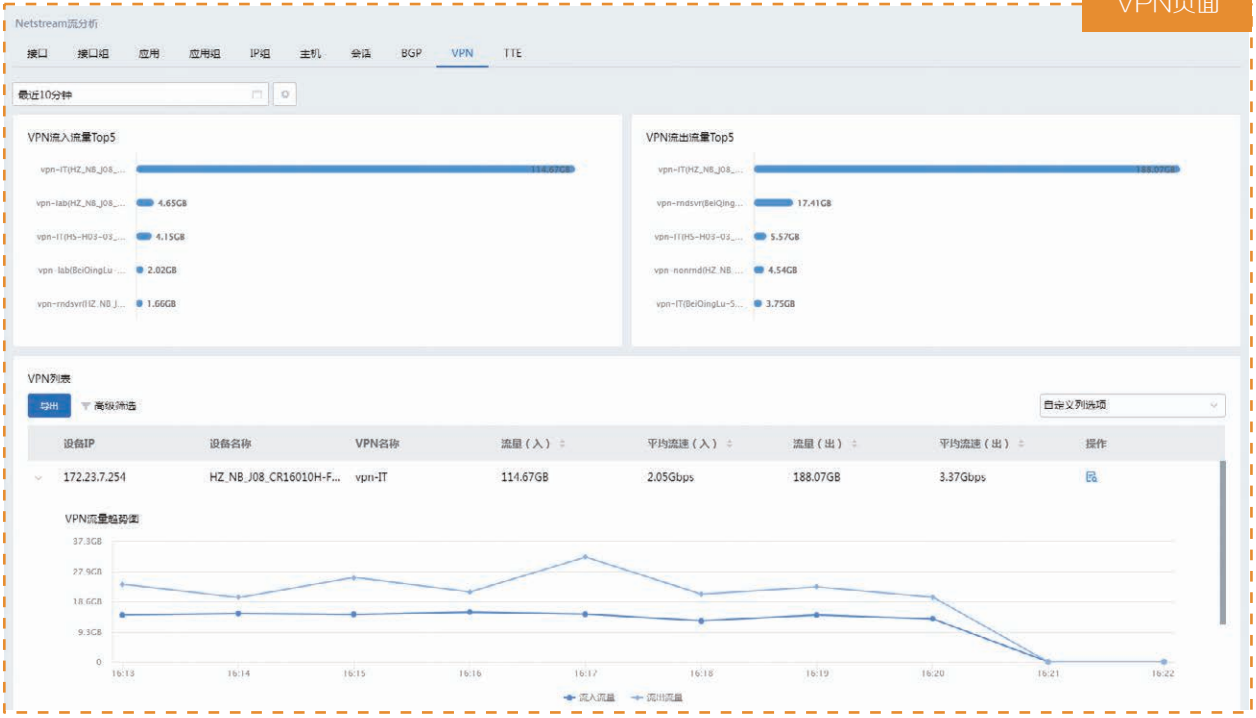
主机流量分析：基于主机维度进行流量的分析与统计，展示以主机IP聚合后的全网流量TOP排名、主机流量趋势，以及每个主机下的接口、应用、会话等维度的流量分布情况。

主机页面



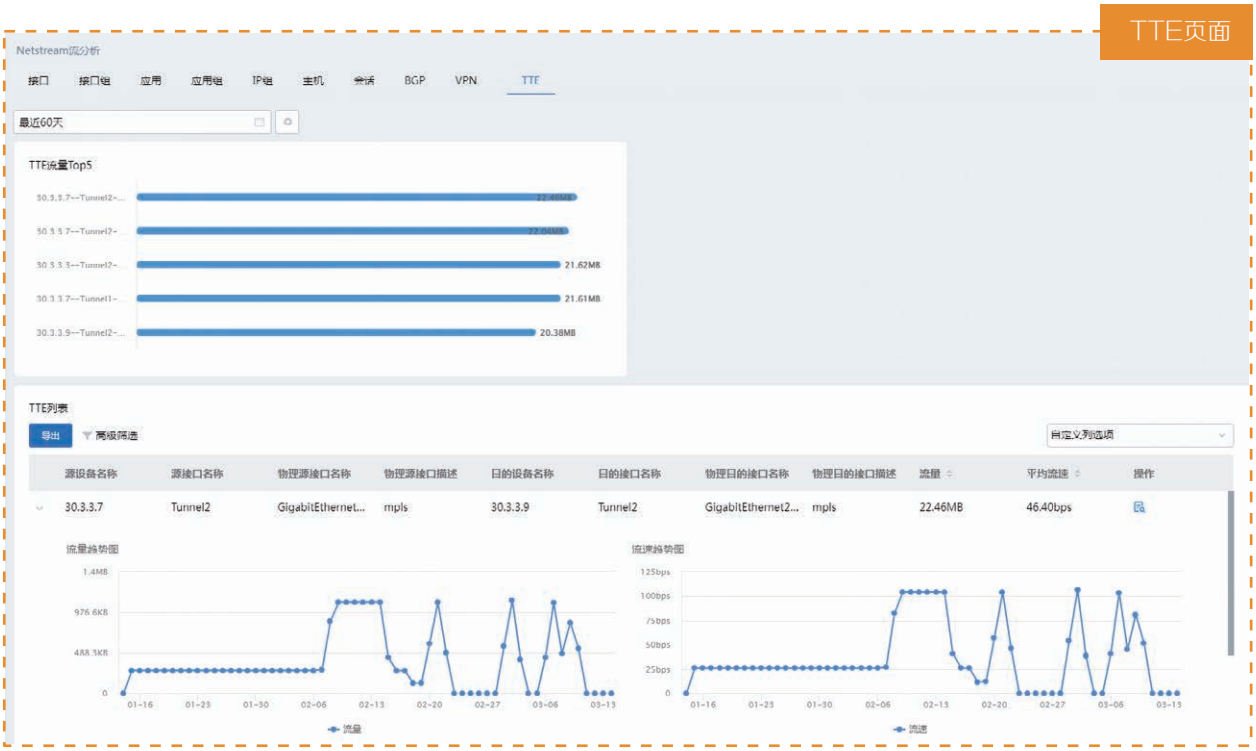
VPN流量分析：基于VPN进行流量的分析与统计，展示VPN的全网流量Top排名，以及每个VPN承载的应用流量排名、应用的流量趋势图和源主机访问排名等。

VPN页面



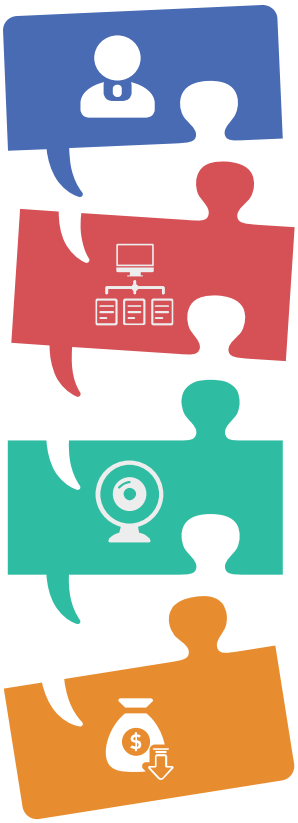
TTE流量分析：基于TTE（传输隧道端点）进行网络流量分析，能够统计全网TTE连接的流量。展示全网TTE连接的流量Top排名、流量统计列表和流量趋势，以及每个TTE连接的网络流量分布情况。

TTE页面



典型应用场景

AD-WAN方案中NetStream功能的应用场景主要有以下几种：



用户监控和分析

通过NetStream技术，可以使网络管理者轻松获取用户使用网络、应用资源的详细情况，有助于高效地规划以及分配网络资源，保障网络的安全运行。

网络规划

NetStream可以为网络管理工具提供关键信息，如各个AS域之间的网络流量情况，有助于优化网络设计和规划，实现以最小的网络运营成本达到最佳的网络性能和可靠性。

网络监控

在出口部署NetStream，对连接Internet网络的接口进行实时流量监控，分析各种业务占用出口带宽的情况。网络管理者可以根据这些信息判断网络的运行情况，尽早发现不合理的网络结构或网络中的性能瓶颈，方便网络管理者合理规划和分配网络资源。

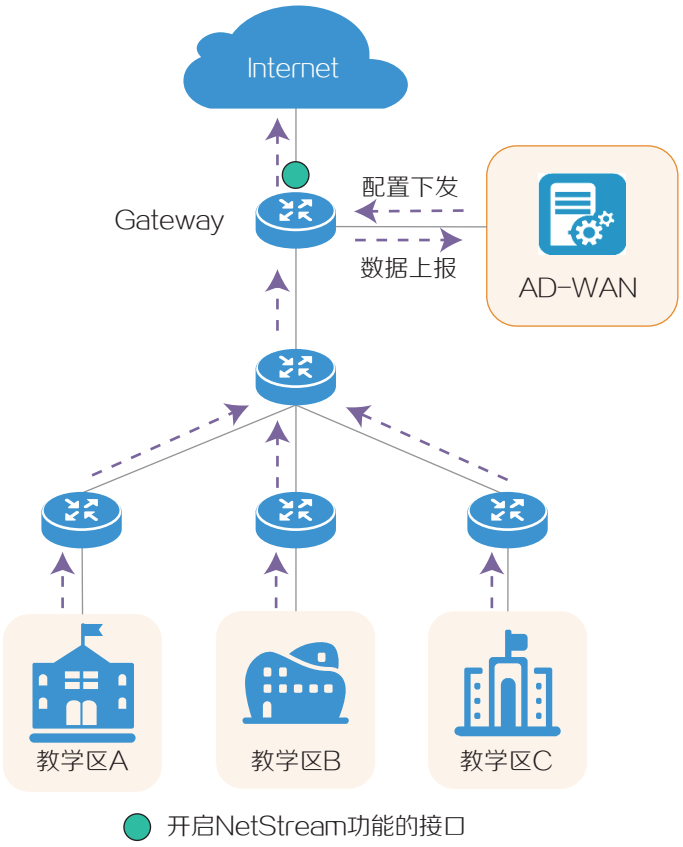
计费

NetStream为基于资源（如线路、带宽、时段等）占用情况的计费提供了精细的数据。Internet服务提供商可以利用这些信息来实行灵活的计费策略，如基于时间、带宽、应用、服务质量等。企业客户可以使用这些信息计算部门费用或分配成本，以便有效利用资源。

NetStream应用于网络规划场景

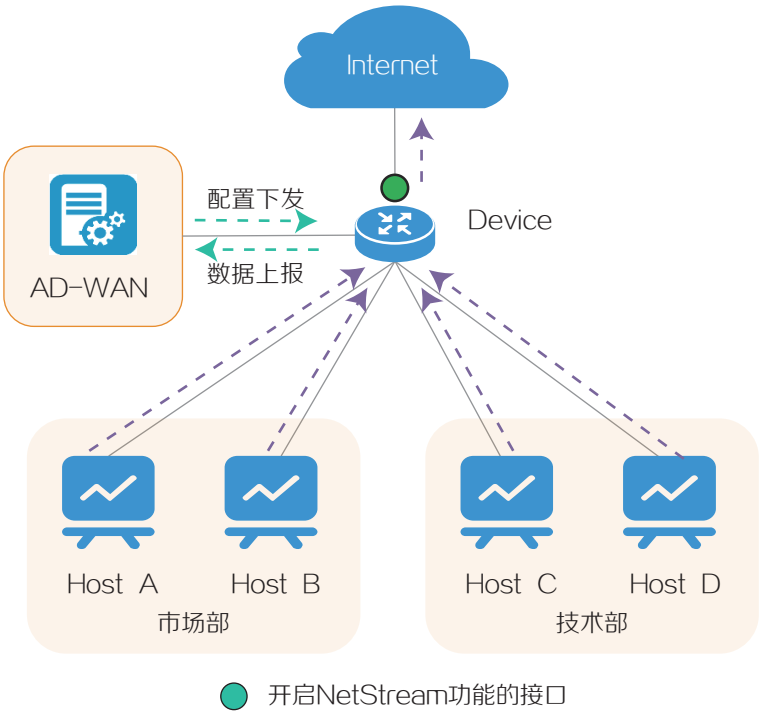
某校园被划分为三个教学区，最初网络管理员为每个教学区分配了相同的带宽。但是随着VoIP、P2P、IPTV等新业务的应用，之前的网络划分已经无法满足学生和老师们的需求，同时也不利于管理。

管理员可以在Gateway连接Internet网络侧的接口上部署NetStream功能，统计接口出、入方向的流量信息，并上送给AD-WAN进行后续的分析，以便通过获取到的带宽使用率的详细信息进行合理地网络的规划和分配，同时对网络流量进行监管。



NetStream应用于流量计费场景

某公司的市场部和技术部通过Device接入到Internet网络，公司希望能够掌握两个部门的上网情况，以便进行分部门计费。



设备连接Internet网络的接口上，通过NetStream统计功能，可以统计接口出、入方向的流量信息，并上报给AD-WAN进行后续的分析，以便监控两个部门的上网情况，为分部门计费提供依据。

方案亮点

多维度数据展示

涵盖接口、应用、应用组、IP组、主机、VPN等常用数据指标的分析与展示。

可视化信息呈现

图形化界面降低流量信息管理难度，提供各项流量数据图表。

编委

牛淑强 彭飞 胡梦梦 刘冠池 曲进 张延杰 宋焕启

王永伟 王伟峰 蒋文栋

顾问

陈友琨、赵晓丹、陈国华、朱萍

美术编辑

郑晓兰 龙厅

广域网管理与运维产品 × 资料开发部联合出品