

AD-WAN

应用驱动广域网

技术专刊

高效广域网运维及调优



Contents

目录

AD-WAN分支

1	概述
3	零配置开局
8	高可靠性
12	一键巡检
16	容量管理
20	多维可视
33	运维诊断工具
38	丰富的组网场景支持
44	精细化应用分类
49	智能调度技术RIR
52	安全
60	广域网优化

AD-WAN承载

概述	69
Segment Routing	71
SRv6概述	75
网络切片之资源隔离	79
一键巡检	90
容量管理	94
多维可视	97
丰富的流量调度策略	111
精细化应用分类	116
iFIT随流分析	123

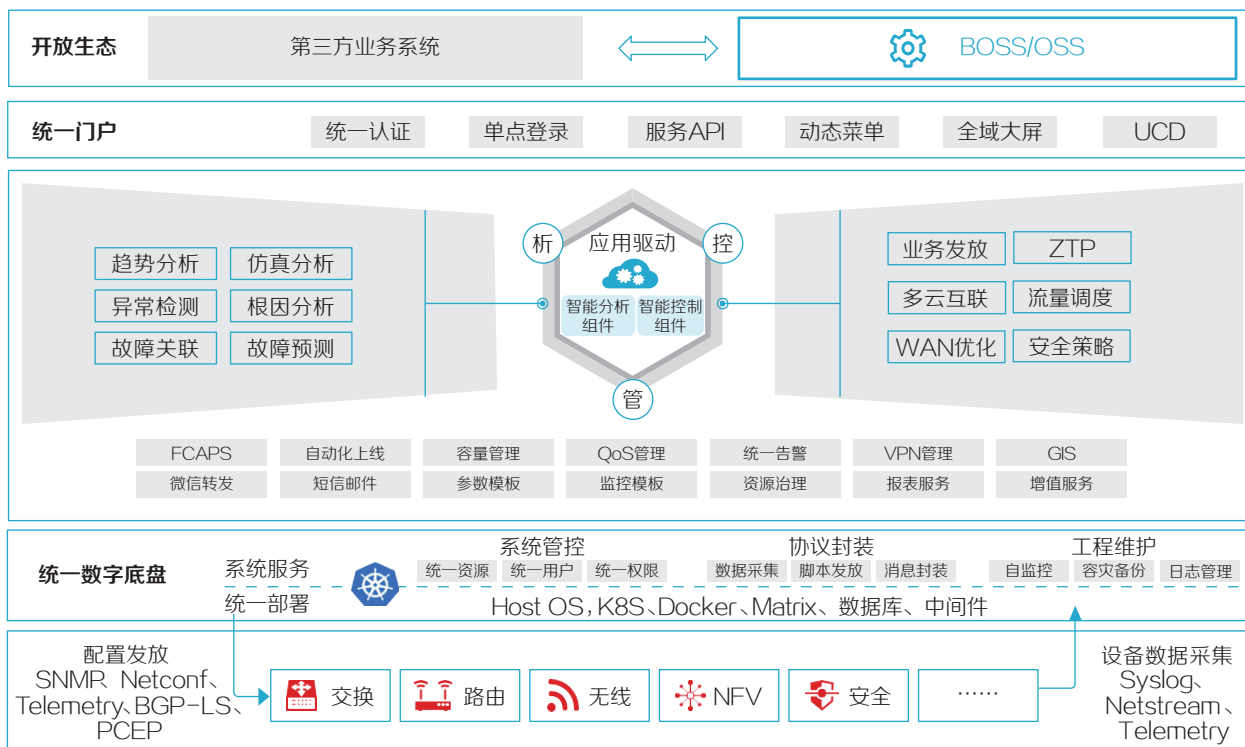
AD-WAN分支 解决方案概述

方案概述

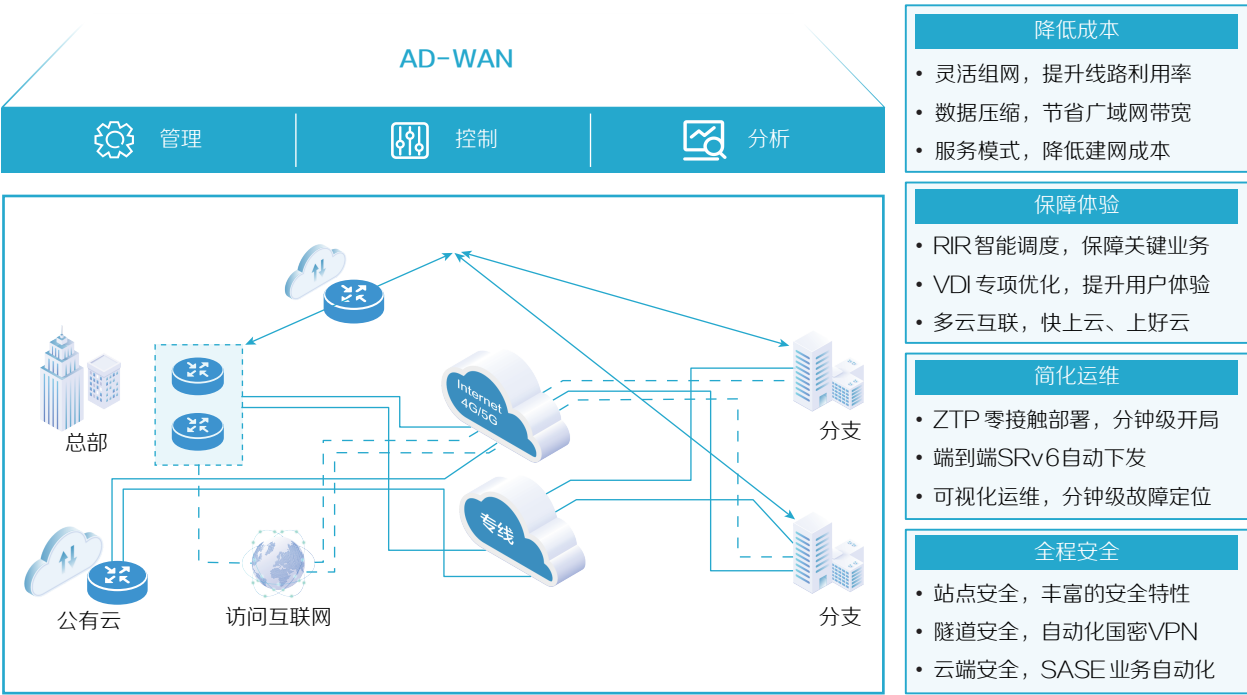
随着数字化转型的深入和新业务不断涌现，越来越多的应用上云，公有云、私有云、混合云的多云联接成为新常态。伴随着应用的云化和智能化，业务对广域网的需求也发生了变化，广域网流量激增，从而驱动广域网发生变革。此时软件定义广域网SD-WAN就成为数字化转型中网络重构的关键。

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按需互联，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with 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



方案核心产品

	AD-WAN 管控析智能融合			
	总部	汇聚	分支接入	虚拟化vCPE
路由器产品	SR6600X-系列 SR6600/SR6602 系列	MSR5600 系列	MSR2600 系列 MSR800 系列 MSR3600 系列 MSR 3610I-系列	vSR1000/2000
安全产品	M9000 系列	F5000 系列	F1000 系列	vFW1000/2000



AD-WAN分支解决方案之

零配置开局

■ 传统分支网络部署

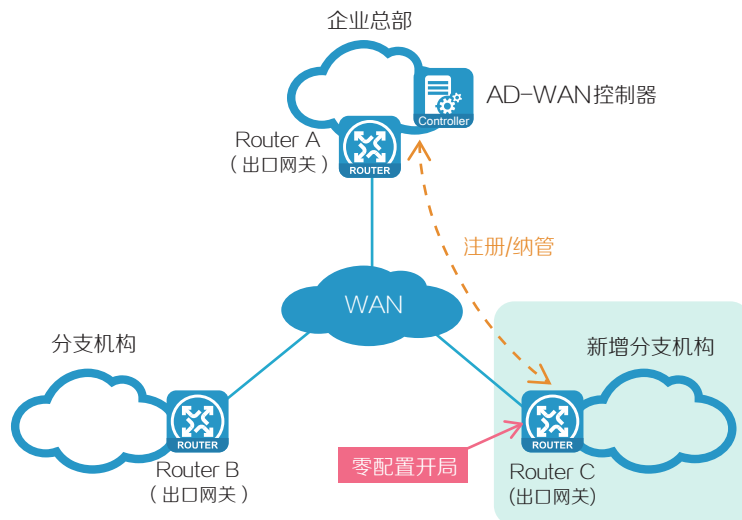
传统方式部署新的分支网络时，设备安装完成后，需要专业IT人员到安装现场，对设备**逐台**进行**手工配置**，才能将设备接入网络，完成开局。

当设备**数量较多**、**分布较广**时，这种部署方式不但**费时费力**，还大大增加了人力成本。



■ 功能简介

零配置开局是H3C推出的**自动化网络部署**方案。网络管理人员将基础连通性配置远程发送给设备，设备加电启动后自动完成配置加载，然后自动注册到AD-WAN控制组件，由**AD-WAN控制组件**完成**设备纳管**及**网络业务配置下发**。整个过程无需管理人员到现场进行开局配置，大大简化了开局过程，极大降低了开局成本。



整体流程

- 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：设备运送至分支机构，加电启动。
- ③ 初始配置：使用零配置开局完成设备初始配置。
- ④ 控制通道建立：设备向AD-WAN控制组件进行注册，校验通过后，双方建立控制通道。
- ⑤ 控制管理：AD-WAN控制组件远程管理设备。

部署方式

当前支持四种设备自动化部署方式，选择灵活、轻量化部署、即插式上线、省力省时又省钱。



开局技术	功能概述	使用场景
U盘开局	通过在设备上插入U盘的方式来完成设备开局的一种技术	• 开局人员需携带开局U盘至现场，将U盘插入设备 • 即插即用，对开局人员的专业技能零要求
邮件开局	通过开局邮件下发配置来完成设备开局的一种技术	• 开局人员需准备开局终端（智能手机、平板电脑、笔记本电脑和PC等）来接收开局邮件，并将开局终端连接到设备 • 对开局人员的专业技能要求较低
公有云开局	通过设备出厂携带的预配置来完成设备开局	• 要求在云简管理平台导入设备信息 • 要求设备能连接云简网络 • 即插即用，对开局人员的专业技能零要求
DHCP开局	通过DHCP服务器下发配置来完成设备开局	• 要求管理员具有DHCP服务器的配置权限，且DHCP服务器支持Option 253 • 即插即用，对开局人员的专业技能零要求

■ 开局流程

1、U盘开局



- ① 管理员在AD-WAN控制组件上导入新增分支出口网关的信息，为该设备完成开局配置，然后将开局配置导出成部署文件，保存至开局U盘的根目录。
- 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。
- 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，并自动与AD-WAN控制组件建立连接、注册并完成开局。

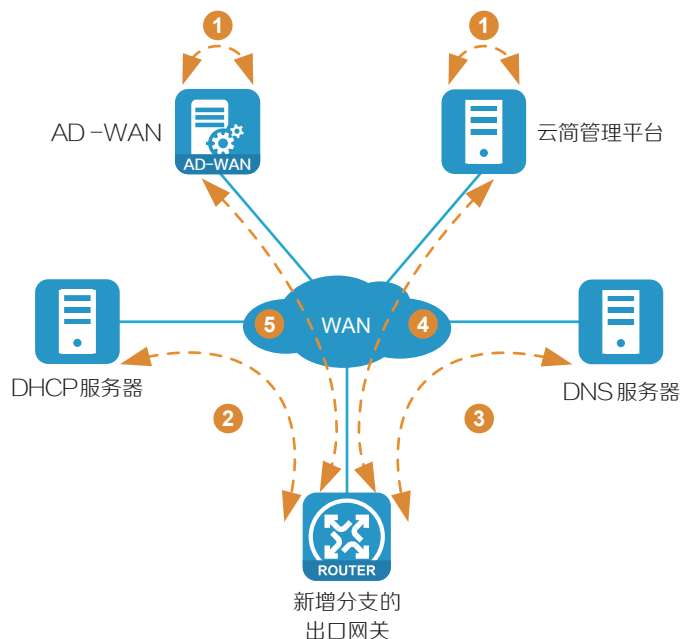
2、邮件开局

- ① 管理员在AD-WAN控制组件上导入新增分支出口网关的信息，为该设备完成开局配置。AD-WAN控制组件将开局配置封装成**URL格式（URL支持加密）**，通过**邮件**发送给开局人员。
- ② 开局人员接收到邮件后，通过网线直连设备LAN接口（或使用无线接入），再点击开局邮件中的URL链接，向设备发送URL中携带的开局配置。
- ③ 设备接收URL请求，自动跳转到开局配置**Web页面**。开局人员在该Web页面查看开局配置，**交互式确认**执行开局配置。
- ④ 设备根据开局配置进行初始配置，并自动与AD-WAN控制组件建立连接、注册并完成开局。



- 增加邮件开局时，支持填写加密密钥，用于加密邮件开局URL链接中配置信息的一串字符，密钥最长256个字符，不支持中文和空格。
- 收到URL链接后，若链接加密，则需根据提示先输入加密密钥。

3、公有云零接触开局



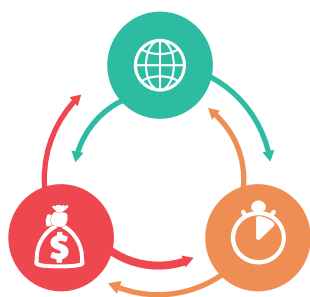
- ① 管理员在AD-WAN控制组件和H3C云简网络上分别导入新增分支出口网关的信息，并在H3C**云简网络**管理平台上为该设备配置AD-WAN控制组件的域名或IP地址/端口号等参数。
- ② 通过DHCP服务器为设备分配WAN接口地址、缺省网关和DNS服务器地址。
- ③ 通过DNS服务器解析云简网络管理平台的域名。（通常情况下，运营商网络提供的DHCP和DNS服务可满足云简开局需求，无需管理员额外部署）
- ④ 开局人员给设备上电，设备启动过程中先自动通过DHCP功能获取WAN接口地址、缺省网关和DNS服务器地址参数，再根据出厂配置**自动连接云简网络**管理平台，云简网络管理平台将开局**配置推送**至设备。（设备出厂配置中会携带云简网络管理平台的域名和端口号）
- ⑤ 设备根据开局配置进行初始配置，并自动与AD-WAN控制组件建立连接、注册并完成开局。

4、DHCP开局

- ① 管理员在AD-WAN控制组件上导入新增分支出口网关的信息。
- ② 管理员配置**DHCP服务器**，为设备分配WAN接口地址等上网参数以及AD-WAN控制组件的域名或IP地址/端口号等参数。
- ③ 开局人员给设备上电，设备启动过程中会主动向DHCP服务器发起请求，以获取接口IP地址。DHCP服务器在给设备分配IP地址同时，通过在DHCP报文中携带**Option选项253**将AD-WAN控制组件信息返回给设备。
- ④ 设备根据DHCP服务器推送的开局配置进行初始配置，并自动与AD-WAN控制组件建立连接、注册并完成开局。



方案亮点



省力 + 省时 + 省钱 = 零配置开局



降低技术要求

开局人员无需前往局点即可**远程**完成设备部署，界面向导式操作，简化流程，**降低网络部署人员技术要求**，非专业技术人员现场操作“0”门槛。



缩短开局时间

设备可批量完成部署，将传统网络按天部署**缩短为分钟级**，**大大缩短开局时间**，降低资源消耗。



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**。

AD-WAN分支解决方案之 高可靠性

简介

AD-WAN分支解决方案从不同维度为用户提供可靠性部署能力，并结合设备RRR自主流量调度特性提供了无控制模块干预下的业务智能调度保障，保证了AD-WAN控制组件故障时业务的连续性和高可靠性，提升广域网的健壮性。

01 / 控制模块高可靠

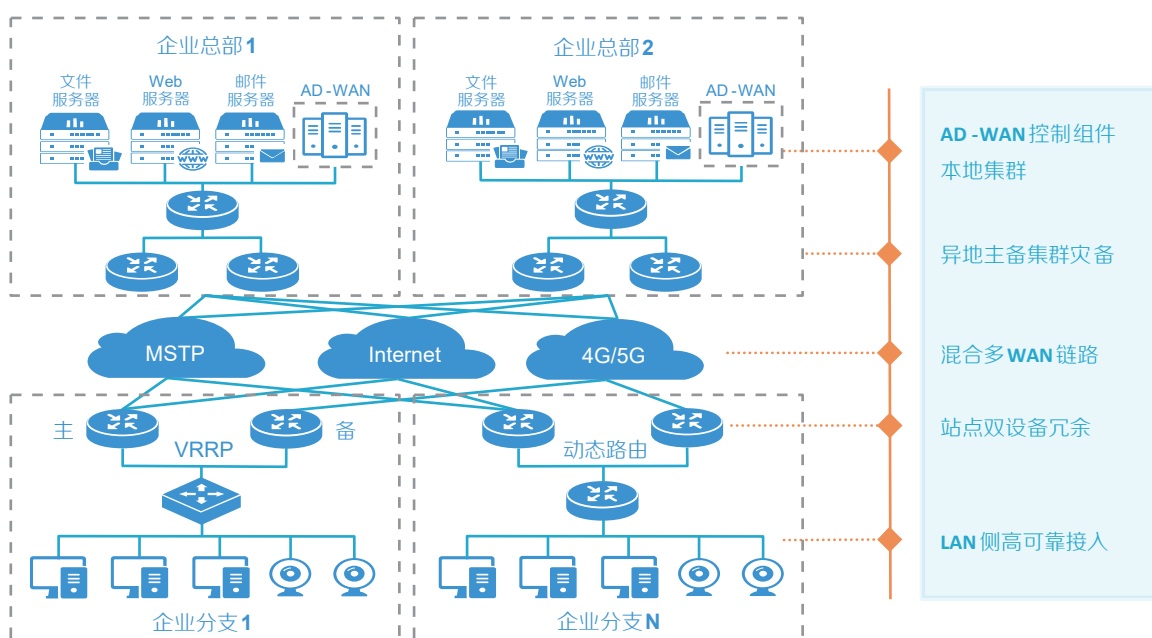
02 / 站点接入高可靠

03 / 传输链路高可靠

04 / 站点设备高可靠

分支方案整体网络设计

分支方案采用“多总部+单站点双设备+多链路”混合接入的网络高可靠性冗余设计。



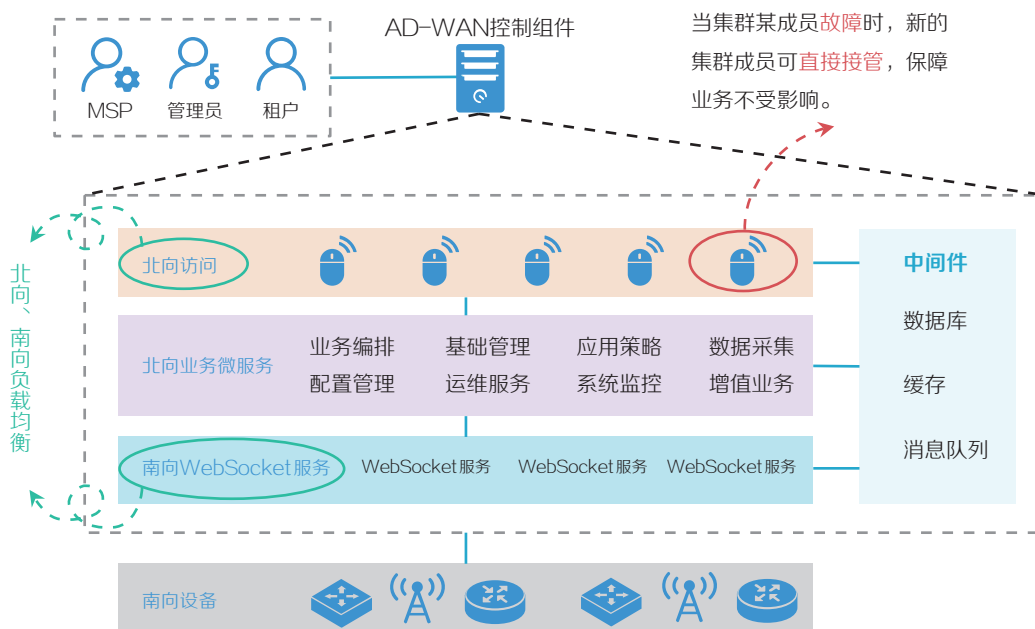
设备、链路、站点冗余备份，转发决策不依托于AD-WAN控制组件，设备自身即可实现多维度的智能选路，提升业务可靠性。

控制模块高可靠

AD-WAN分支解决方案中，控制模块的高可靠性通过2种部署模式来支持：

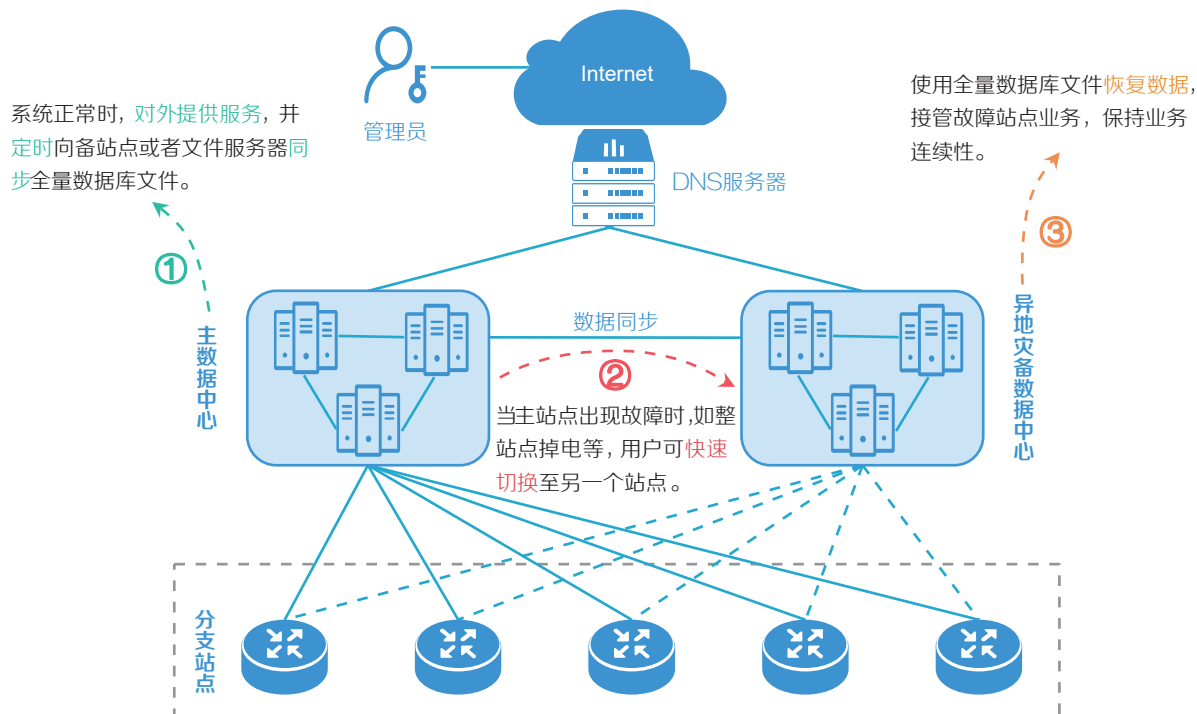
1、关键微服务在多集群成员上负载均衡部署

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。



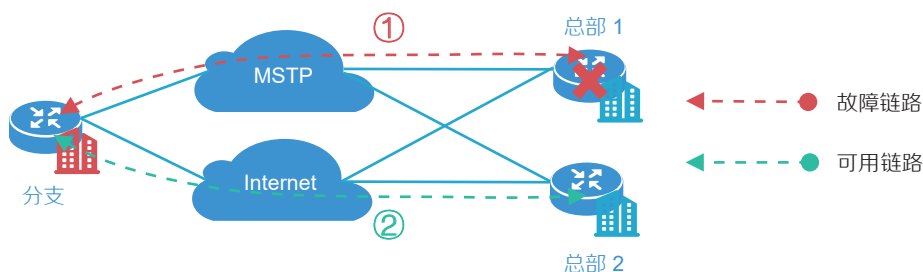
2、异地灾备部署

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。



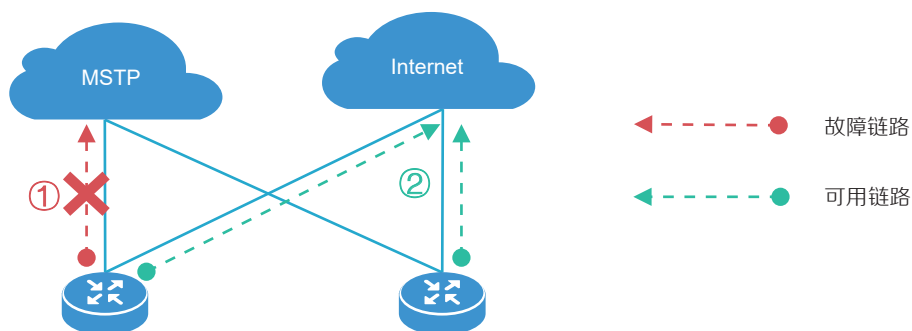
站点接入高可靠

AD-WAN分支解决方案通过支持分支站点同时连接多个总部站点的方式保证用户访问业务网络的可靠性。



传输链路高可靠

AD-WAN分支解决方案中，站点设备支持同时采用多链路上行与流量调度技术结合进行数据传输。



流量可以自动化切换到剩余设备和剩余可用链路，保证特定业务走特定转发链路或将业务流量均匀在多链路上进行负载分担，为用户提供业务保障和链路高可用性，提高数据传输可靠性。



支持多种链路类型

MPLS专线
MSTP专线
Internet
4G/5G



支持多链路配合使用

依据链路性能指标，
可配置链路优选传输模式
以及多链路分担模式



支持多种分担模式

- 逐流：适用于要求流量来回路径一致的应用
- 逐包：适用于下载类的大流量应用，充分利用链路带宽

站点设备高可靠

AD-WAN分支解决方案中，通过站点独立双设备模式实现站点设备高可靠。

站点独立双设备模式是两台设备独立部署，业务LAN侧通过**VRRP**或**动态路由**方式连接双网关设备。

双设备间彼此共享链路质量、带宽、带宽利用率、选路优先级等各种信息。最终，每台设备均综合组内双设备的链路信息来为应用优选最优链路。

VRRP

两台设备通过VRRP协议通信，
分为主和备两组

特点：作为网关，更适合在路由环境下层是二层设备时使用

动态路由

两台设备通过动态选路应对网关
设备故障

特点：作为网关，更适合在路由环境下层是三层设备时使用



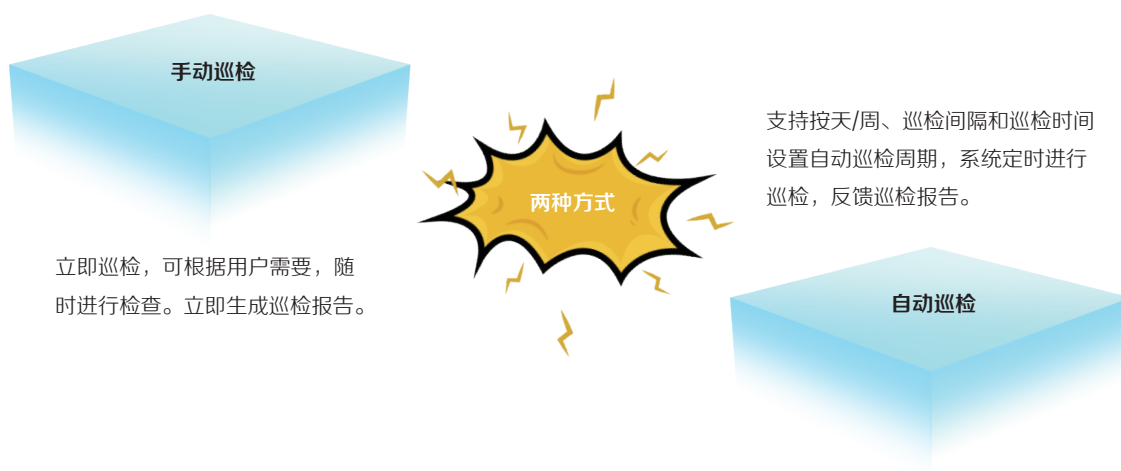
VRRP: Virtual Router Redundancy Protocol，虚拟路由器冗余协议

AD-WAN分支解决方案之 一键巡检

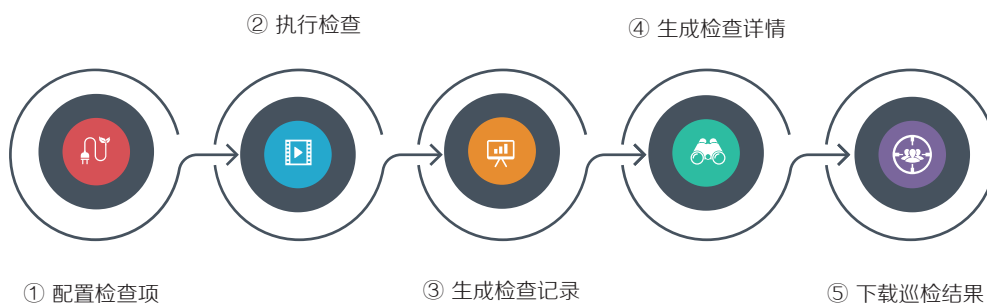
简介

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。

一键巡检功能通过将网络状态、管理状态和业务状态的巡检内容进行归纳、整理，以可视化的界面展示巡检内容和巡检结果，以此提高整体运维效率。



巡检流程



1、配置检查项

对系统进行一键巡检前请投先按需配置检查项，系统将按照检查项对系统、设备、业务、管理、接口进行检查。

配置检查项

☐ 全选

☐ WAN业务详情

☐ Underlay链路状态

☐ WAN侧Overlay BGP路由

☐ WAN侧Underlay OSPF路由

☐ WAN侧Underlay RIP路由

☐ LAN侧OSPF路由

☐ 路由策略

☐ 设备状态

☐ 设备板卡

☐ System IP口资源池

☐ VPN状态

☐ 应用实例状态

☐ STUN状态

☐ 网站缓存状态

☐ LAN业务详情

☐ Overlay链路状态

☐ WAN侧Underlay BGP路由

☐ WAN侧Underlay 静态路由

☐ LAN侧路由BGP路由

☐ LAN侧静态路由

☐ 路由策略前缀

☐ 设备接口

☐ 站点间互连链路状态

☐ 站点状态

☐ 设备与站点

☐ 接入区状态

☐ WAAS状态

状态检查项

资源检查项

设备检查项

业务检查项

检查项丰富多样

取消

确定

2、执行检查

根据配置的检查项及巡检方式执行检查。

立即执行检查，进度条显示检查进度。
立即生成检查记录；可快速查看检查详情；下载检查报告。

按需配置自动巡检策略，系统将按周期进行自动巡检。



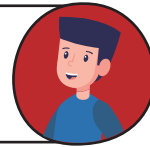
举个栗子



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“手动巡检”方式。



当用户需定时排查系统中的异常情况时，可选择“自动巡检”方式。配置自动巡检策略，时间间隔选择“1”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巡检记录。



自动巡检策略

自动巡检: ☒ 开启 ☐ 关闭

时间间隔单位: 天

时间间隔: 1

巡检时间: 10:00:00

配置 保存

自动巡检记录

检查日期	检查项	失败
2022-06-14 10:00:00	25	0

3、巡检结果

执行检查后，系统将生成巡检记录。在检查结果页面可查看指定巡检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 巡检记录

02 巡检详情

一键巡检

配置校验 配置审计 批量配置下发 数据导出 一键巡检 运维诊断

刷新 配置检查项 执行检查 自动巡检

检查日期	检查项	失败	异常	风险	正常	操作
2022-06-14 10:00:00	25	0	0	1	24	查看详情

一键巡检 > 检查结果

检查结果

系统状态: 正常

统计: 25 (失败: 0, 异常: 0, 风险: 1, 正常: 24)

序号	检查项	检查项介绍	执行结果	处理意见
1	WAN业务详情	检查当前系统中WAN业务网络详情状态	正常	
2	LAN业务详情	检查当前系统中LAN业务网络详情状态	正常	
3	Underlay链路状态	检查当前系统中的Underlay链路的状况	风险	请进入物理网络中的物理管理页面检查当前系...
4	Overlay链路状态	检查当前系统中的Overlay链路的状况	正常	
5	WAN侧Overlay BGP路由	检查当前系统中的WAN侧路由Overlay BGP路...	正常	
6	WAN侧Overlay 静态路由	检查当前系统中的WAN侧路由Overlay静态路由...	正常	
7	WAN侧Underlay BGP路由	检查当前系统中的WAN侧路由Underlay BGP...	正常	
8	WAN侧Underlay OSPF路由	检查当前系统中的WAN侧路由Underlay OSPF...	正常	

共有 25 条记录, 当前页 1 ~ 15, 页 1 / 2 页

执行结果

Internet To cpe-202-gigabitEthernet5/0, Internet To cpe-203-GigabitEthernet5/0, Internet To cpe-204-GigabitEthernet5/0, Internet To cpe-205-GigabitEthernet5/0, Internet To ri-201-GigabitEthernet5/0xUnderlay链路异常。

系统支持下载巡检报告，报告为Excel格式。

检查结果

执行检查项：25个，异常检查项：0个，存在风险：1个，执行失败：0个，检查结果正常：24个。

存在风险的检查项。报告中展示执行结果及风险处理意见。

序号	级别	检查项	检查项介绍	执行结果	处理意见
1	正常	WAN业务详情	检查当前系统中WAN业务网络详情状态	正常	
2	正常	LAN业务详情	检查当前系统中LAN业务网络详情状态	正常	
3	风险	Underlay链路状态	检查当前系统中Underlay链路的状态	正常	1-204-GigabitEthernet6/0、int 请进入物理网络中的链路管理页面检查当前系统中Underlay链路状态
4	正常	Overlay链路状态	检查当前系统中Overlay链路的状态	正常	
5	正常	WAN侧Overlay BGP路由	检查当前系统中的WAN侧路由由Overlay BGP路由状态	正常	
6	正常	WAN侧Overlay 静态路由	检查当前系统中的WAN侧路由由Overlay静态路由状态	正常	
7	正常	WAN侧Underlay BGP路由	检查当前系统中的WAN侧路由由Underlay BGP路由状态	正常	
8	正常	WAN侧Underlay OSPF路由	检查当前系统中的WAN侧路由由Underlay OSPF路由状态	正常	
9	正常	WAN侧Underlay 静态路由	检查当前系统中的WAN侧路由由Underlay 静态路由状态	正常	
10	正常	LAN侧路由BGP路由	检查当前系统中的LAN侧路由由BGP路由状态	正常	
11	正常	LAN侧路由OSPF路由	检查当前系统中的LAN侧路由由OSPF路由状态	正常	
12	正常	LAN侧静态路由	检查当前系统中的LAN侧路由-静态路由状态	正常	
13	正常	路由策略	检查当前系统中路由策略配置状态	正常	
14	正常	路由策略前缀	检查当前路由策略前缀模板中策略前缀状态	正常	
15	正常	设备状态	检查当前设备的设备状态	正常	
16	正常	设备接口	检查当前设备的接口状态	正常	
17	正常	设备板卡	检查当前设备的板卡状态	正常	
18	正常	站点间互连链路状态	检查站点间互连链路状态	正常	
19	正常	System IP口资源池	检查System IP口资源池的使用情况	正常	
20	正常	站点状态	检查所有站点状态	正常	
21	正常	VPN状态	检查VPN状态	正常	
22	正常	设备与站点	检查设备与站点的对应关系	正常	
23	正常	应用实例状态	检查应用实例状态	正常	
24	正常	接入区状态	检查接入区状态	正常	
25	正常	STUN状态	检查STUN状态	正常	

无风险检查项

方案亮点



一键启动

操作简单，用户可根据需要选择所需的巡检方式。

快速检查

无需“等待”，立即执行检查，生成检查记录。

清晰报告

检查结果清晰直观。

AD-WAN分支解决方案之 容量管理

简介

在传统网络中，网络管理人员（后续简称网管人员）的直接操作对象是设备。设备配置的变化、新业务的开通，都需要网管人员介入操作，因此网管人员对设备上的资源占用情况具有很强的掌控能力。在网络设备上配置操作时，若设备上资源不足，网管人员一般可通过设备反馈的信息，及时进行处理。在SDN场景中，网管人员的直接操作对象变成SDN控制组件。虽然简化了网管人员的工作，但从另一个角度看，也会导致网管人员对网络设备的掌控力变低：控制组件对网络设备下发的配置内容、时机，不能精准掌握，网管人员也无法再对设备的资源状态“了如指掌”。

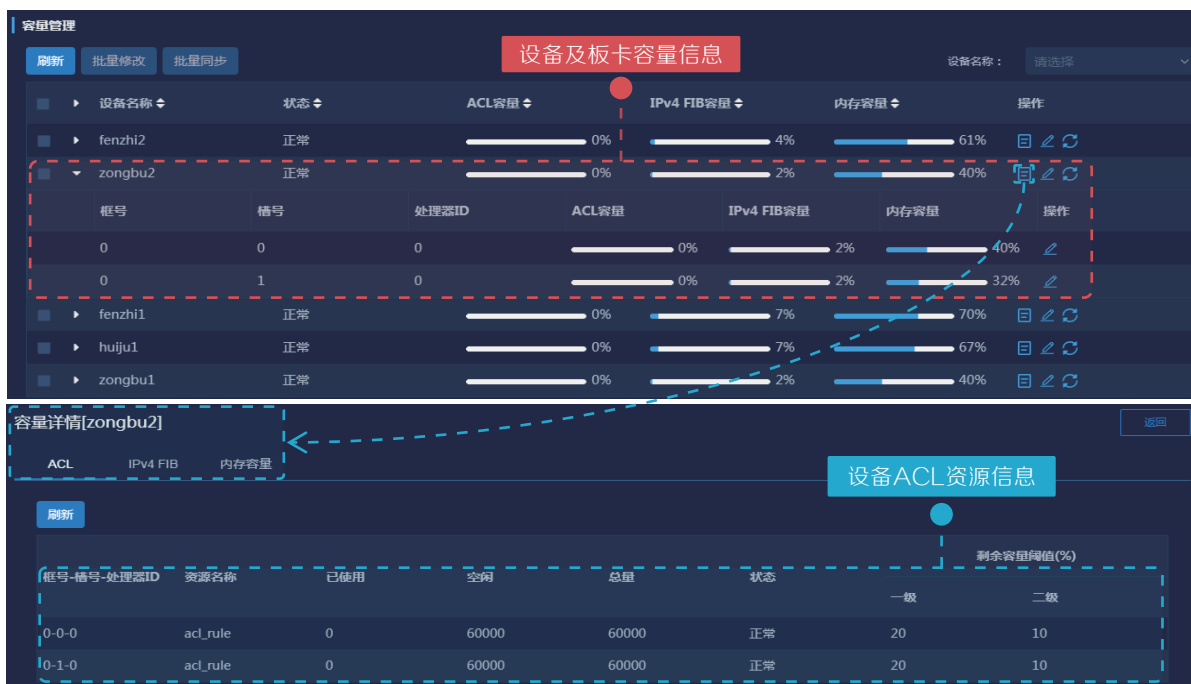
容量管理通过对设备的FIB资源、ACL资源以及内存进行监控，保障设备各项资源容量能够合理满足业务诉求，保障业务发放成功率。

主要功能



设备容量可视

以可视化的界面展示设备ACL资源和FIB资源的容量信息。



ACLIPv4 FIB内存容量

设备IPv4 FIB资源信息

刷新

框号-槽号-处理器ID	资源名称	已使用	空闲	总量	状态	剩余容量阈值(%)	
						一级	二级
0-0-0	ipv4fib	1269	78731	80000	正常	20	10
0-1-0	ipv4fib	1269	78731	80000	正常	20	10

ACLIPv4 FIB内存容量

设备内存容量信息

刷新

框号-槽号-处...	资源名称	已使用(KB)	空闲(KB)	总量(KB)	状态	警告	剩余容量阈值(MB)		
							一级	二级	三级
0-0-0	memory	818808	1232936	2051828	正常	288	192	128	96
0-1-0	memory	654756	1397072	2051828	正常	288	192	128	96



在容量管理列表可查看所有设备的资源容量信息。
在容量详情列表可查看设备ACL资源、IPv4 FIB 资源、内存容量的详细信息。



剩余容量阈值

为保障业务正确下发，可对设备剩余可用容量设置阈值，实现合理规划容量的效果。

开启 关闭

确定

容量管理

刷新 批量修改 批量同步

设备名称	状态
fenzhi2	正常
zongbu2	正常

框号	槽号
0	0
0	1

设备名称	框号	槽号	状态	ACL	IPv4 FIB	内存容量
fenzhi1	0	0	正常	0%	7%	70%
huiju1	0	1	正常	0%	7%	67%
zongbu1	0	0	正常	0%	2%	40%

修改全局容量阈值: zongbu2

ACL

一级阈值(%)

二级阈值(%)

IPv4 FIB

一级阈值(%)

二级阈值(%)

取消 确定

设备名称: 请选择

容量

操作

内存容量

操作

修改板卡容量阈值: zongbu2(0-0-0)

ACL

一级阈值(%)

二级阈值(%)

IPv4 FIB

一级阈值(%)

二级阈值(%)

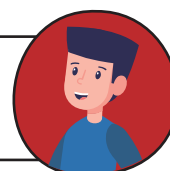
取消 确定



当剩余容量小于一级阈值时将产生次要警告；小于二级阈值时产生重要警告。

“

通过设置阈值，帮助用户合理安排不同资源的容量使用。可对整个设备的容量信息进行阈值设置，也可对单个板卡进行容量阈值设置。



超阈值下发

用户可通过“超阈值下发”选择当设备的资源超出阈值时是否下发配置。

超阈值下发配置

☒ 开启 ☐ 关闭

1. 当设备FIB 表剩余资源超出二级阈值或内存剩余资源超出一级阈值时，是否向超出阈值资源的设备下发配置。
2. 当ACL表剩余资源超出二级阈值时，是否向超出阈值资源的设备下发ACL资源相关的配置。

修改全局容量阈值

☒ ACL 警告告警

* 一级阈值 (%) :

* 二级阈值 (%) :

☒ IPv4 FIB 严重告警

* 一级阈值 (%) :

* 二级阈值 (%) :

容量状态正常：蓝色
 剩余容量<一级阈值：黄色警告告警
 剩余容量<二级阈值：红色严重告警



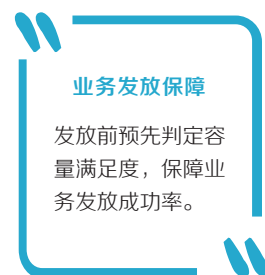
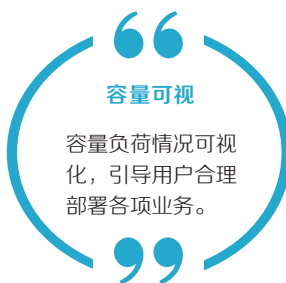
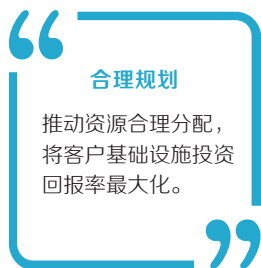
一级阈值数值>二级阈值数值

容量管理

设备名称：

设备名称	状态	ACL容量	IPv4 FIB容量	内存容量	操作
fenzhi2	正常	0%	4%	61%	目 Z C
zongbu2	正常	0%	2%	40%	目 Z C
fenzhi1	警告	0%	7%	70%	目 Z C
huiju1	严重	0%	7%	67%	目 Z C
zongbu1	正常	0%	2%	40%	目 Z C

方案亮点



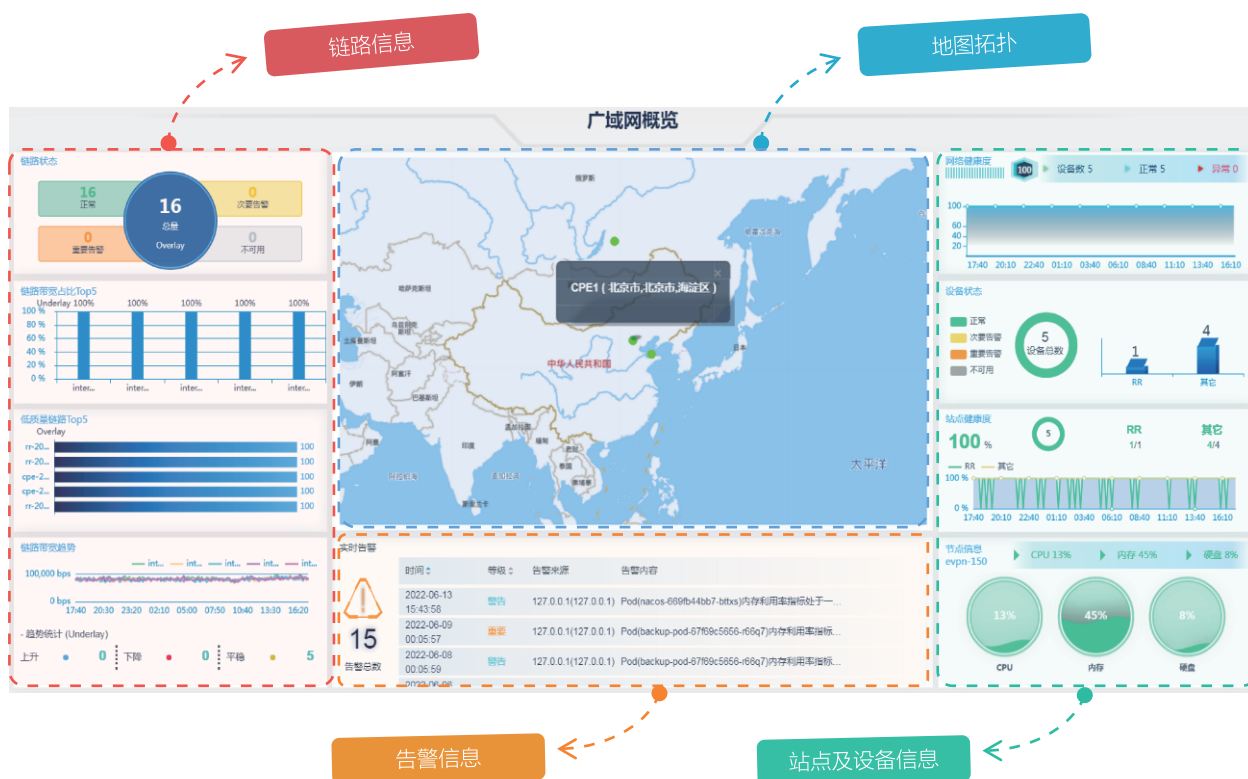
AD-WAN分支解决方案之 多维可视

简介

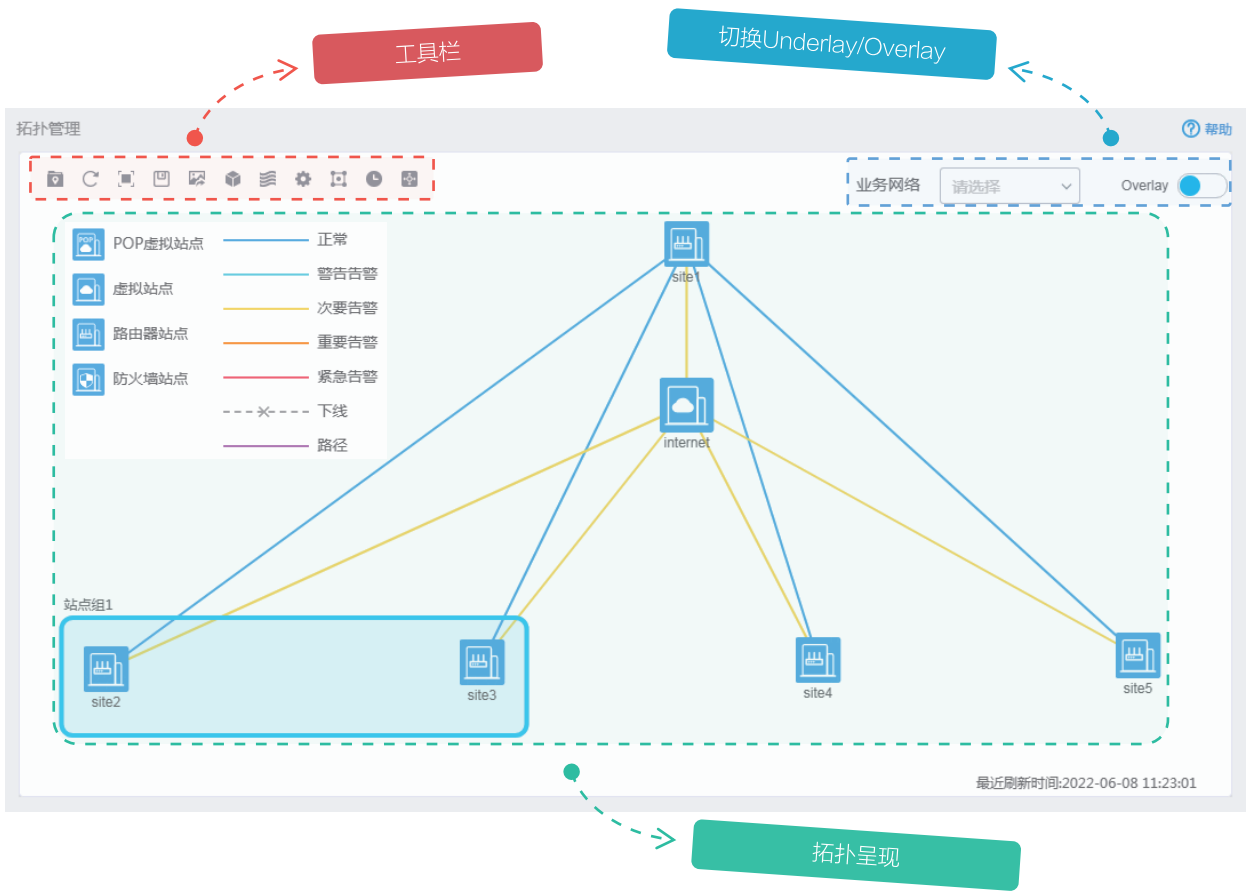
AD-WAN分支通过**相关信息采集技术、流采集技术以及网络质量采集技术**实现基于全局的多维度可视呈现能力，包括提供全局的网络拓扑呈现，设备状态、链路流量及状态呈现，链路质量呈现、应用的多维度呈现以及网络故障呈现。

主要功能

AD-WAN分支解决方案提供大屏可视功能，展示内容包括链路状态、链路带宽及质量、设备状态、站点和网络健康度、节点信息、实时告警、GIS地图等。用户可轻松掌握当前网络及资源的实时状态，支持按需定制大屏可视化呈现的形式。



其中，地图拓扑支持静态地图和GIS地图，实时展示设备地理位置和信息。
大屏可视还支持切换Underlay和Overlay链路，可在拓扑管理中查看详细信息。



1、设备可视

控制组件的设备可视提供设备、设备接口、板卡等信息的可视化管理。

设备基本信息

设备名称	节点状态	System IP	管理状态	序列号	设备类型	站点信息	Router ID	操作
rr-201	正常运行	1.1.1.1	已确认开局	005056bc31534a9022042409	H3C VSR1000	site1	201.201.201.201	编辑 删除 刷新 全屏 打印
厂商信息: H3C 软件版本号: 7.1.064 ESS 1360 节点下线原因: 维护状态: 升级中 5%								

软件版本信息

[上传版本](#) [刷新](#)

名称	版本名称	描述信息	版本类型	版本号	状态	操作
VSR	VSR1000-X64.ipe	--	IPE	7.1.064 ESS 1360	上传完成	编辑 删除 刷新 全屏 打印

设备接口信息							
选择设备							
rr-201							
接口列表							
刷新							
接口名称	状态	IP/掩码	接口MAC	接口速率(kbps)	接入网络名称	接口描述	操作
GigabitEthernet4/0	Up	32.32.32.1/24 --	00:50:56:bc:27:d2	10	mstp3	GigabitEthernet4/0 Interface	编辑 删除

设备板卡信息											
选择设备											
rr-201											
板卡列表											
刷新											
板卡索引	板卡描述	板卡所属的设备框号	板卡所在槽位号	板卡序列号	出厂日期	板卡角色	板卡物理状态	板卡运行状态	操作		
3	Main Processing Unit	0	0	005056bc31534a9022042409	0000-00-00	主控板	正常	单板稳定运行	--		
子卡名称	子卡索引	子卡描述	子卡所属设备框号	子卡所在槽位号	子卡所在子槽位号	子卡序列号	子卡型号	出厂日期	子卡物理状态	操作	
VNIC-VMXNET3	57	1-Port 10M/100...	0	0	1		VNIC-VMXNET3	0000-00-00	正常	--	
VNIC-VMXNET3	58	1-Port 10M/100...	0	0	2		VNIC-VMXNET3	0000-00-00	正常	--	

分析组件可以针对网络设备进行健康度评估分析。

健康度是一个综合的衡量指标，分析组件从系统平面、数据平面、控制平面三个维度对网络设备进行360度监控，对指标数据根据一定权重进行综合衡量，给出一个健康度评分来反映当前网络设备的运行状态。当健康度高时表示网络设备的运行状态良好，反之处于亚健康甚至异常状态。



2、链路可视

控制组件的链路可视提供链路状态、带宽等信息的可视化管理，支持切换Underlay和Overlay链路。

Underlay链路下不显示IP协议、物理接口和加密IPsec。

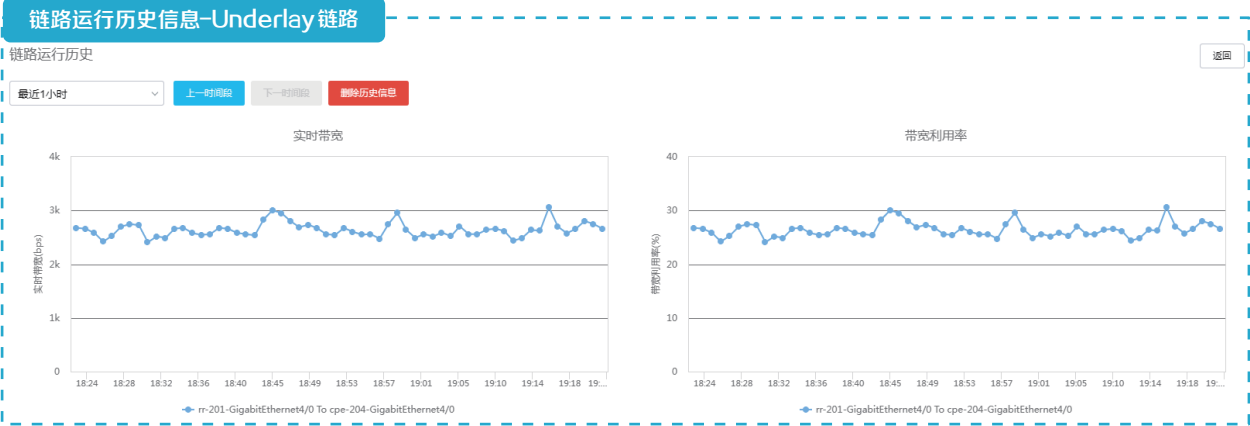
链路基本信息

链路名称	链路状态	IP协议	源设备	源接口	物理源接口
rr-201-GigabitEthernet4/0...	正常	IPv4	rr-201	Tunnel3	GigabitEthernet4/0
目的设备	目的接口	物理目的接口	可分配带宽(kbps)	加密IPsec	操作
cpe-204	Tunnel1	GigabitEthernet4/0	10	否	 

Underlay链路下可查看链路状态、实时带宽和带宽利用率，还可查看链路运行历史信息。

链路运行状态信息-Underlay 链路

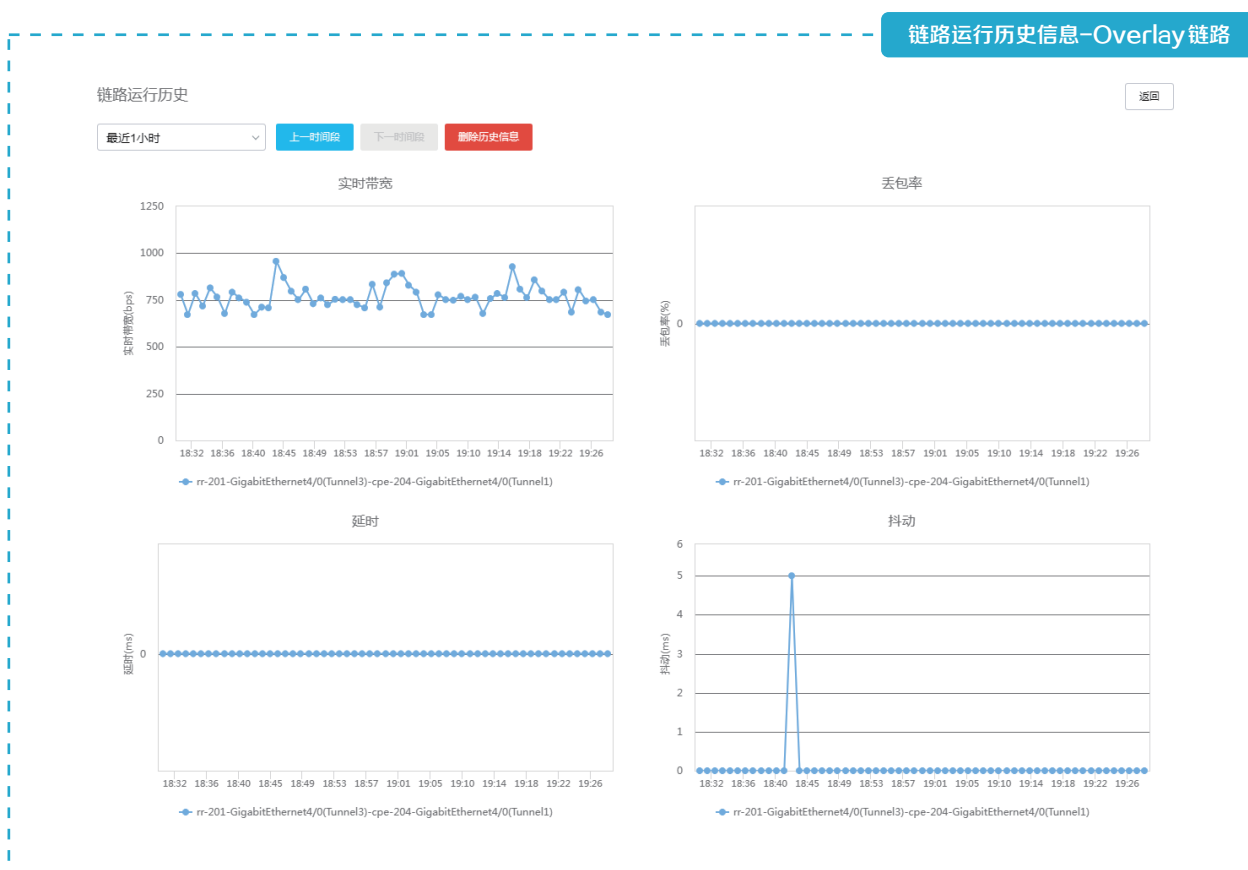
链路名称	链路状态	实时带宽(bps)	带宽利用率(%)	操作
rr-201-GigabitEthernet4/0 To cpe-20...	正常	2560	25.6%	
源设备: rr-201 源接口: GigabitEthernet4/0 物理源接口: -- 目的设备: cpe-204 目的接口: GigabitEthernet4/0 物理目的接口: --				



Overlay链路下可查看链路状态、IP协议、实时带宽、丢包率、延时、抖动及综合质量，还可查看链路应用组信息和链路运行历史信息。

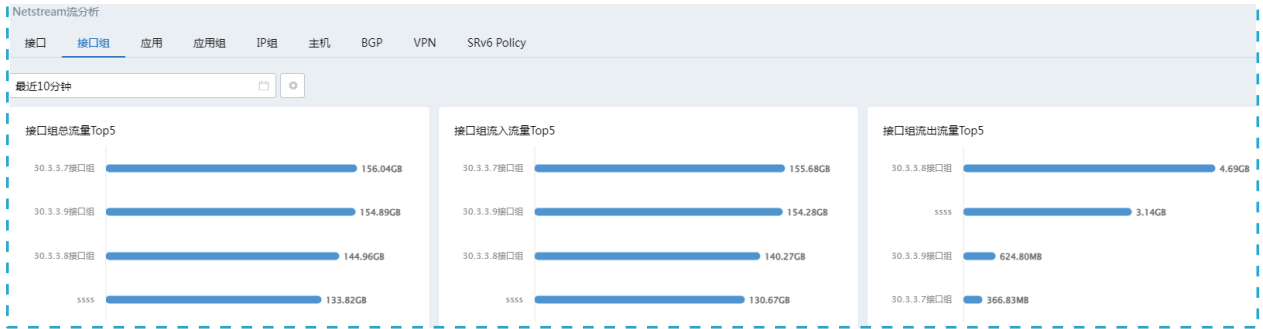
链路运行状态信息-Overlay链路								
链路名称	链路状态	IP协议	实时带宽(bps)	丢包率(%)	延时(ms)	抖动(ms)	综合质量	操作
rr-201-GigabitEthernet...	正常	IPv4	832	0	0	0	100	 
源设备: rr-201 源接口: Tunnel3 物理源接口: GigabitEthernet4/0 目的设备: cpe-204 目的接口: Tunnel1 物理目的接口: GigabitEthernet4/0								

综合质量 = 延时评估值(ms) * 延时权重分配 + 丢包率评估值(%) * 丢包率权重分配 + 抖动评估值(ms) * 抖动权重分配

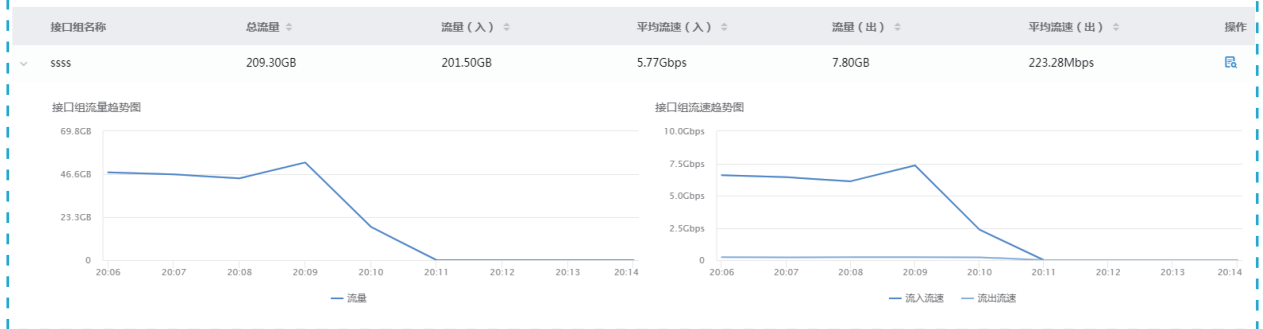


分析组件的Netstream流分析中的接口组流量分析可以统计全网所有接口组的流量排名，展示接口组流量趋势，并且可以查看每个接口组下的网络流量分布情况。

接口组全网流量排名展示

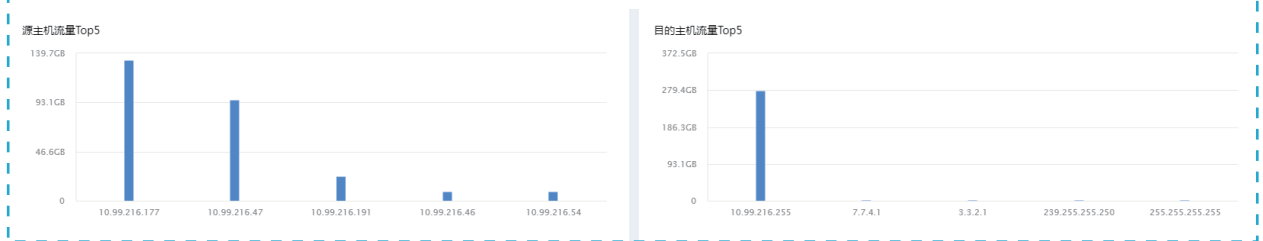


接口组流量统计列表以及各接口组的流量趋势展示



在指定接口组下可以按照主机、接口、应用、会话等类型查看该接口组下的流量统计。

接口组下的主机流量排名展示

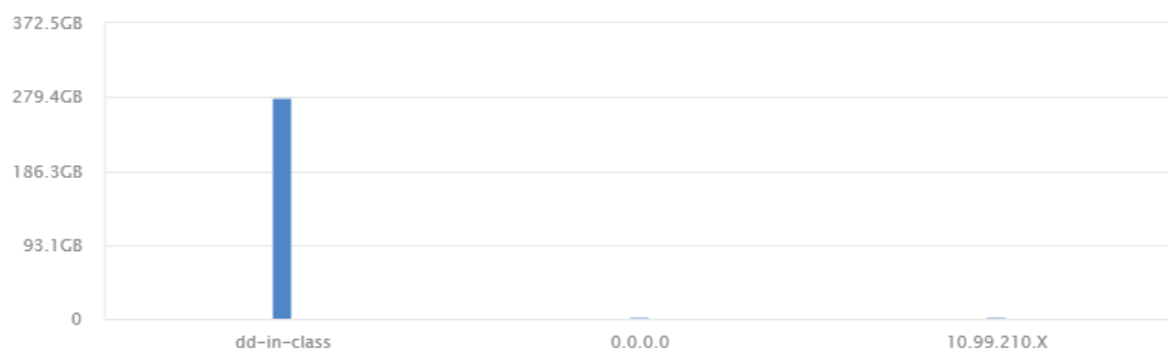


接口组下接口流量排名展示



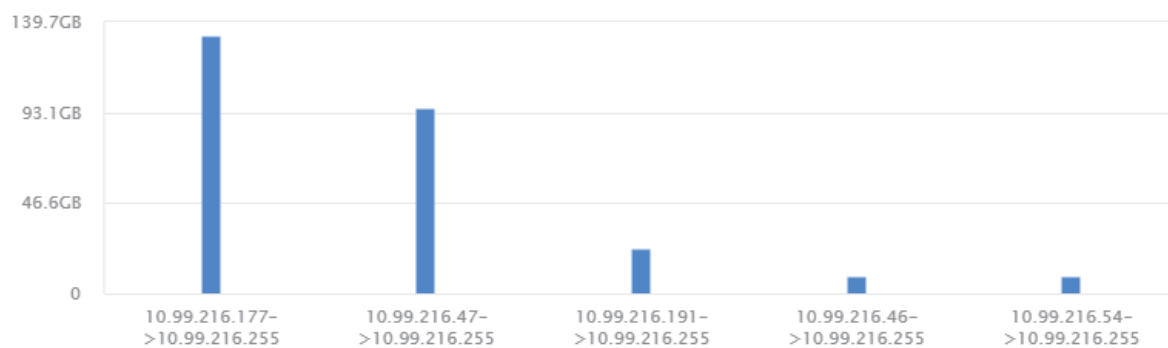
接口组下应用流量排名展示

应用流量Top5



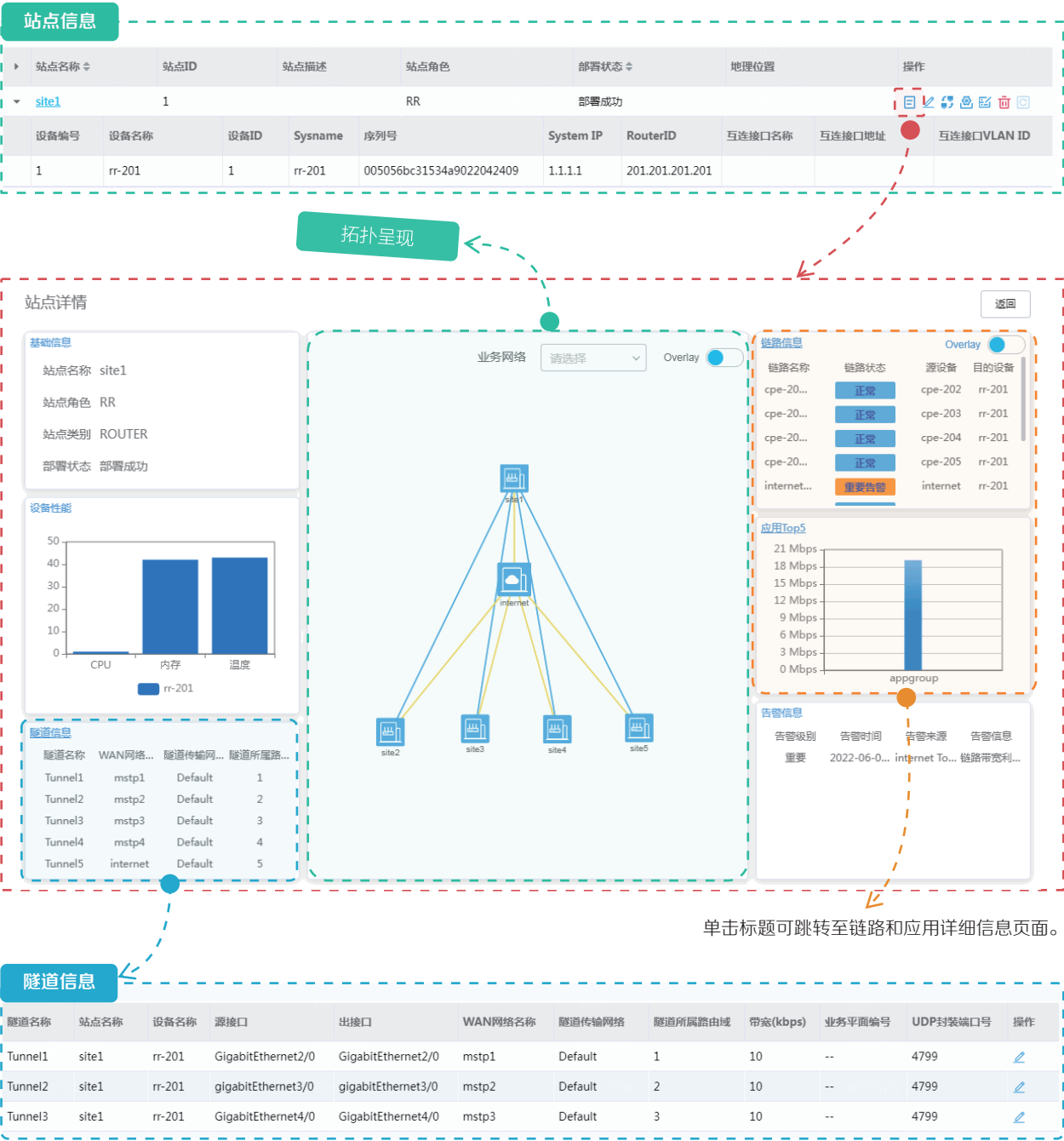
接口组下会话流量排名展示

会话流量Top5



3、站点可视

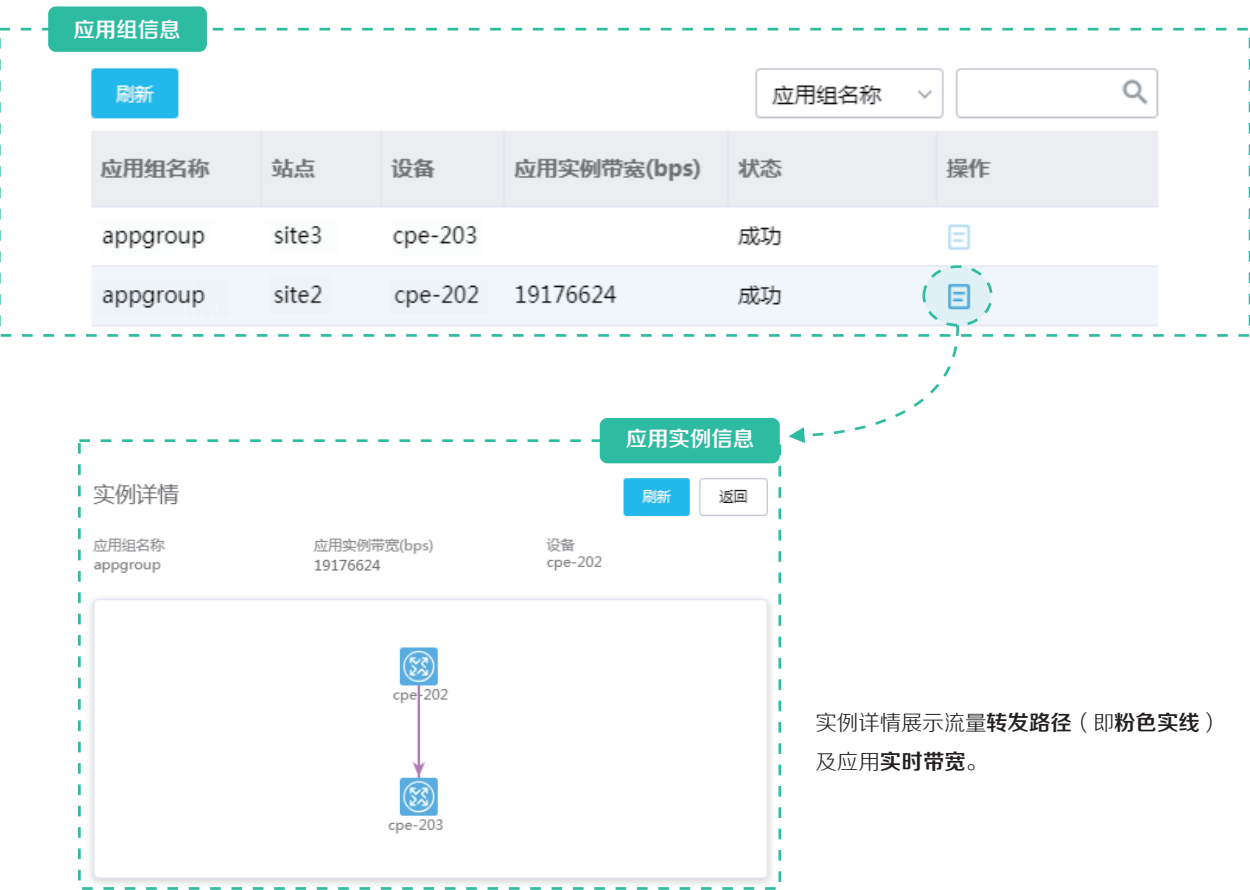
控制组件的站点可视提供站点组成等信息的可视化管理。



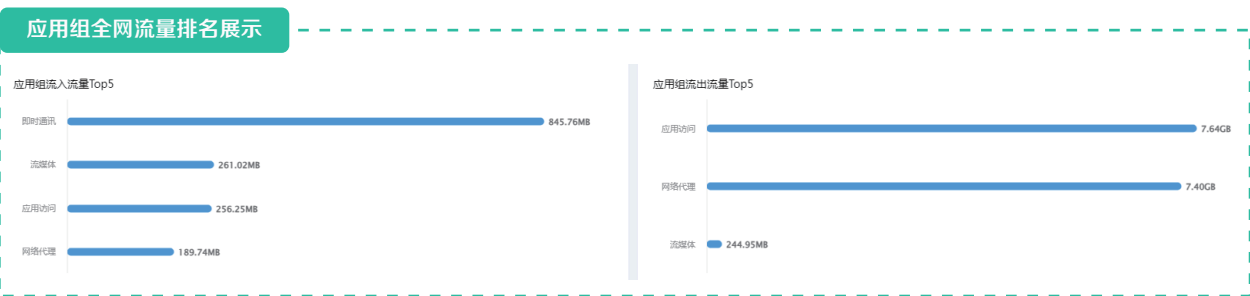
分析组件基于站点、站点间的维度，展示各个站点的链路以及应用统计分析结果，让客户更加有针对性地了解WAN网络情况，有助于快速的发现和定位相关的网络故障。

4、应用可视

控制组件的应用可视提供应用组及应用实例路径等信息的可视化管理。



通过在**分析组件**定义应用组信息，可在NetStream流处理匹配应用阶段，为五元组标识所属的应用组。应用组流量分析首先基于全网统计出流量最高的应用组排名，并给出每个应用组的流量统计列表、流量趋势图等信息。具体分析某个应用组详情时，则展示该应用组下应用的分布情况、应用的流量趋势、源主机访问排名等。



应用组流量统计列表以及各应用组的流量趋势展示

应用组列表

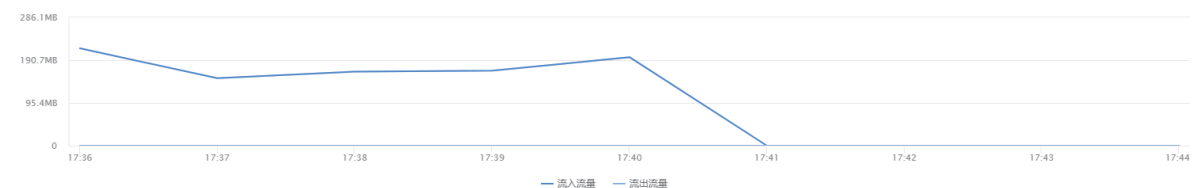
导出

自定义列选项

全部

应用组名称	流量（入）	平均流速（入）	流量（出）	平均流速（出）	操作
即时通讯	897.55MB	25.10Mbps	0.00B	0.00bps	⌵

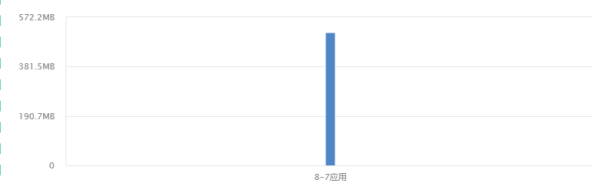
应用组流量趋势图



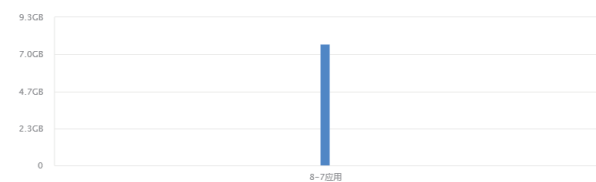
应用组下的应用流量排名展示

应用流量Top5

流入流量



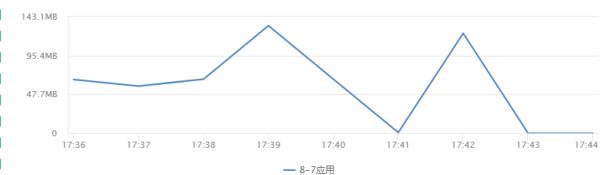
流出流量



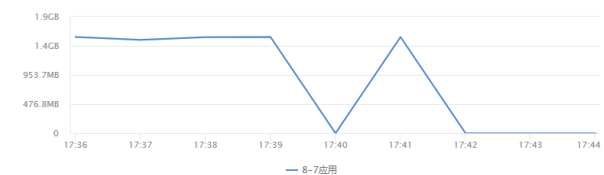
应用组下所有应用的应用流量趋势图

应用流量趋势图

流入流量



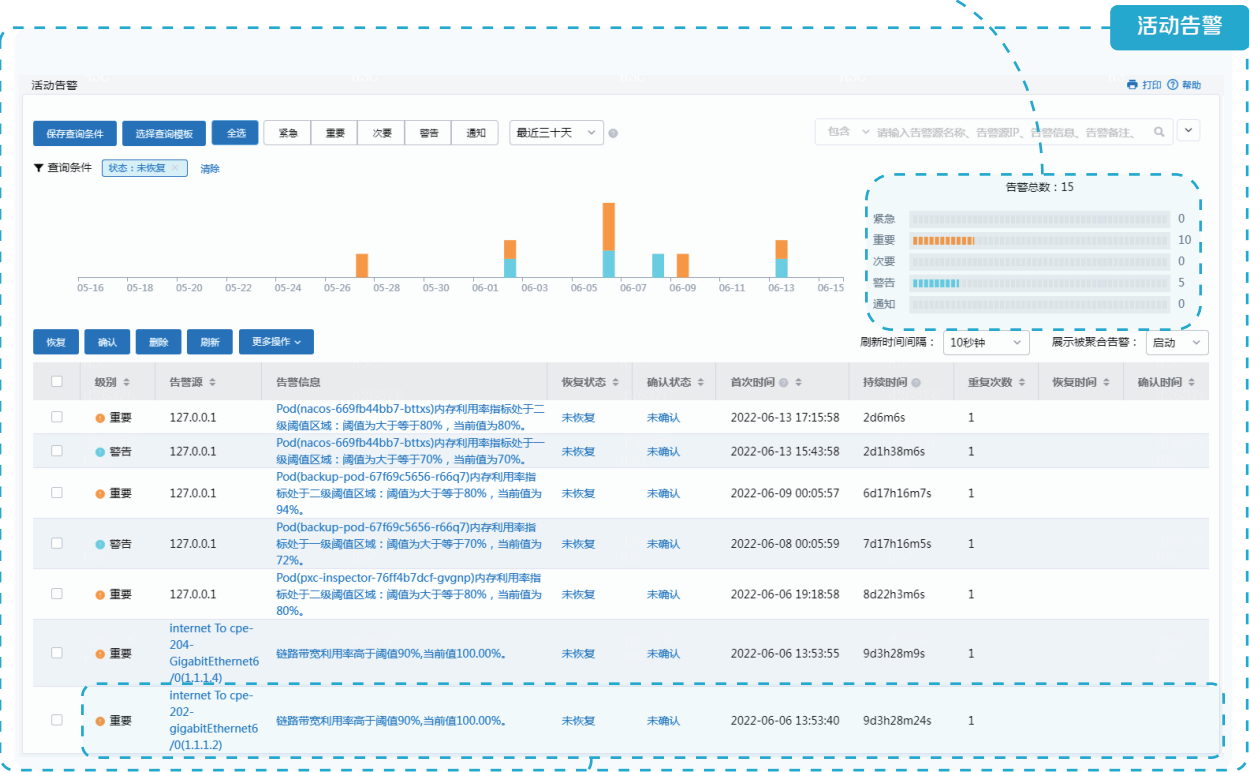
流出流量



5、故障可视

控制组件的故障可视提供实时告警和历史记录等信息的可视化管理。

告警级别从高到低依次为紧急 > 重要 > 次要 > 警告 > 通知



告警源可能是 设备 或者 链路

链路告警信息 返回

确认 恢复

☒	告警级别	告警时间	来源分类	告警来源	告警类型	告警信息	确认状态	恢复状态
☒	重要	2022-06-06 13:53:40	链路	Internet To cpe-202-giga...	链路带宽利用率	链路带宽利用率高于阈值90...	未确认	未恢复

支持4种告警转发方式：邮件、短信、企业微信、微信

告警转发

增加告警转发规则

帮助

基本信息

* 规则名称: 告警转发规则

告警设置

* 需要关注的告警级别: ☒ 紧急 ☒ 重要 ☒ 次要 ☒ 警告 ☐ 通知

* 需要过滤的资源: ☒ 所有资源 ☐ 选定的资源

* 需要关注的告警: ☒ 所有告警 ☐ 选定的告警

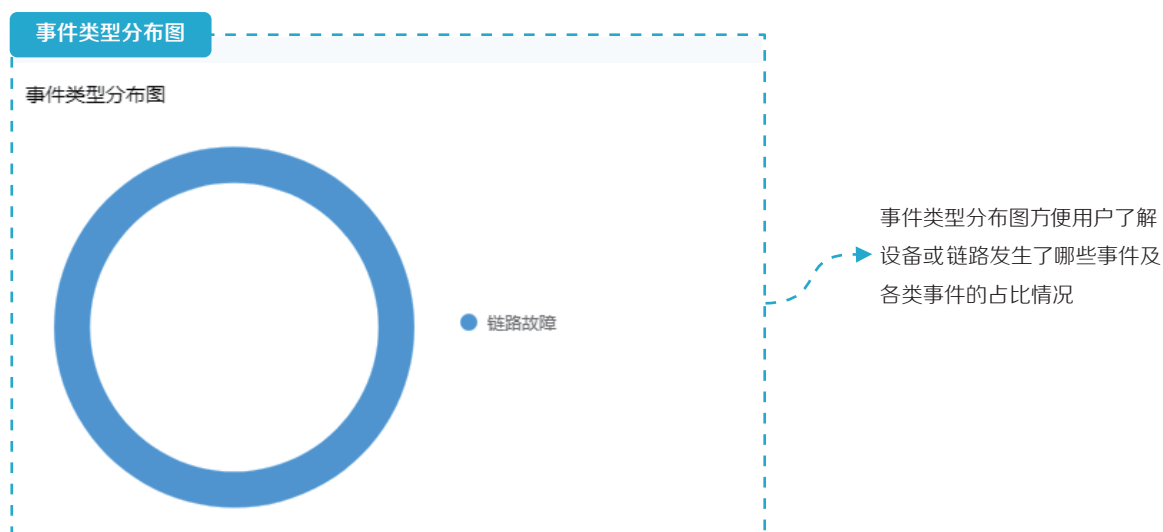
动作设置

邮件转发 短信转发 企业微信转发 微信转发 微信配置

时间段	动作类型	动作参数	操作
所有时间	手机号码	18810570992	
所有时间	邮件地址	test@h3c.com	
所有时间	微信转发	future_message	
所有时间	企业微信转发	Lucky企业转发	

确定 取消

分析组件对设备上报的选路信息进行分析，告知用户选路发生切换的原因，方便用户定位出设备哪些链路质量、带宽不满足业务流量需求，并做出相应调整。重点展示用户关注的选路前后隧道、站点、业务网络名称、出接口等信息



选路调度详情

设备ip	设备名称	应用组名称	流详情	选路前线路	选路后线路	调整时间	调整内容
10.99.216.115	设备115	115-116应用组	115.115.3.2:22972->116....	internet(site115->site116)	mpls(site115->site116)	2022-08-12 10:47:15	链路故障调整：因链路发生故障做出调整

选路信息

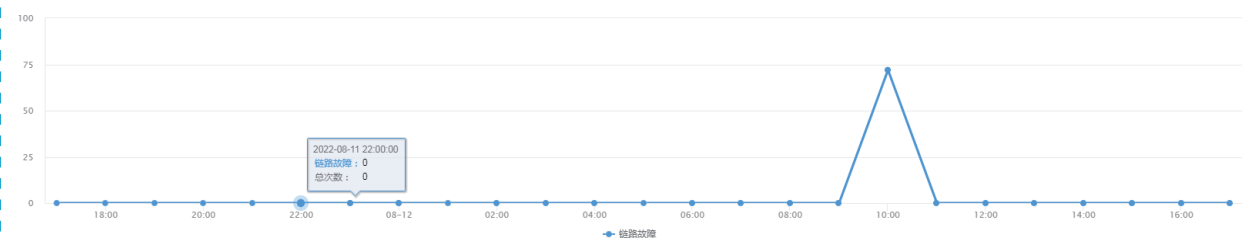
选路前线路详细信息

Tunnel描述: internet
源设备: 设备115
源端口(Tunnel): GigabitEthernet2/0/2(Tunnel1 Interface)
目的设备: 设备116
目的端口(Tunnel): GigabitEthernet2/0/2(Tunnel1 Interface)
peer: 0.0.0.0

选路后线路详细信息

Tunnel描述: mpls
源设备: 设备115
源端口(Tunnel): GigabitEthernet2/0/1(Tunnel2 Interface)
目的设备: 设备116
目的端口(Tunnel): GigabitEthernet2/0/1(Tunnel2 Interface)
peer: 0.0.0.0

事件类型调度次数趋势图



选路调度详情将重点放在业务流量选路前后的详细信息，包括用户关注的业务网络名称、站点、接口等信息。用户根据此详细信息对业务流量或者链路做出相应调整（比如调整SLA中的时延、抖动、丢包、调整链路优先级，让重要业务流量优先走高优先级流量等）。

方案亮点

多维度的数据展示

涵盖设备、链路、站点、应用组及故障等常用的数据指标



可视化的信息呈现

图形化的界面降低信息管理难度，提供各项信息的图表

AD-WAN分支解决方案之

运维诊断工具

简介

传统运维场景下，运维人员需要借助Telnet、Ping、Tracert等工具测试网络性能和定位故障，但这些工具无法和远端CPE设备直接互通。

AD-WAN分支解决方案提供一站式的运维诊断工具，包括Telnet、Ping和Tracert等。集中化、可视化的运维能力能够帮助运维人员快速进行故障排除和诊断，提升运维效率。

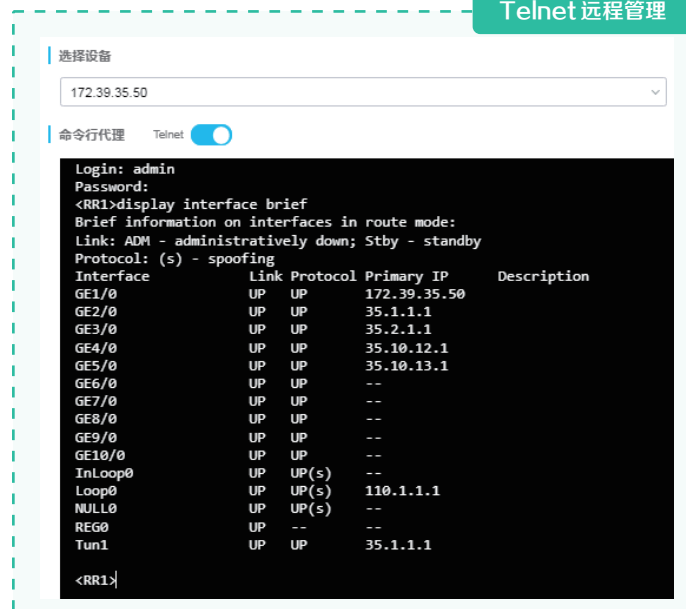
远程管理

远程管理用于远程登录设备进行交互，用户无需配置任何设备接入，在界面上键入命令后，会通过AD-WAN控制组件与设备的管理通道下发到设备上。远程管理支持Telnet和非Telnet两种模式。



非Telnet模式直接
通过WebSocket
主链接进行登录。

Telnet模式借用WebSocket管理网封装内部Telnet协议进行登录。



Telnet模式下支持配置登录验证:

- 登录认证为无用户名、密码认证时，对应设备上的VTY用户在线认证模式为“none”模式。
- 登录认证为用户名、密码认证时，对应设备上的VTY用户在线认证模式为“scheme”模式，可配置登录认证密码。

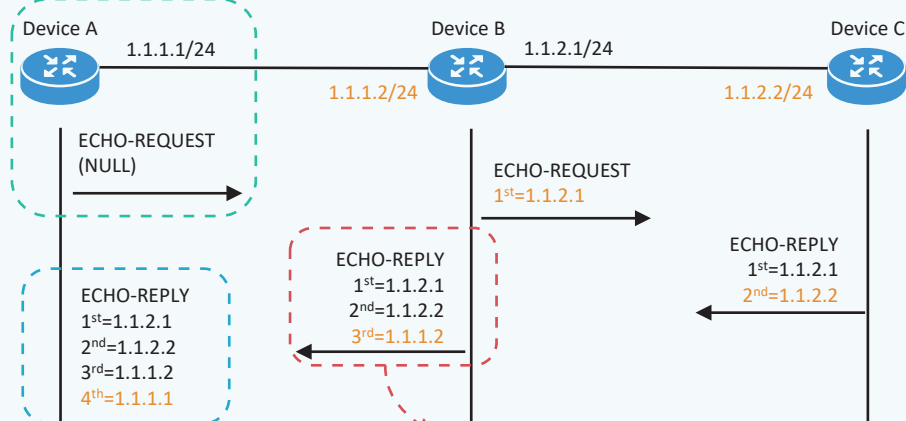
Ping

当网络出现故障时，通过Ping功能可以在设备上执行Ping操作，向目的地址持续发送若干个包，根据ICMP回显应答报文来诊断网络的连通性。

基本原理

Ping功能是基于ICMP(Internet Control Message Protocol，互联网控制消息协议)协议来实现的。

- ① 源端向目的端发送ICMP回显请求 (ECHO-REQUEST) 报文



- ② 根据是否收到目的端的ICMP回显应答 (ECHO-REPLY) 报文来判断目的端是否可达

- ③ 对于可达的目的端，再根据发送报文个数、接收到响应报文个数以及Ping过程报文的往返时间来判断链路的质量

Ping诊断流程

- ① 选择设备、IP类型
 - ② 填写目的地址
 - ③ 填写Ping参数 (包大小和包数量)
- 可选设备所属VPN

诊断

* 设备名称:

Hub1

VPN名称:

vpn

* IP类型:

IPv4

出接口名称:

请选择

源地址:

* 目的地址:

10.30.1.1

* 包大小(Bytes):

56

* 包数量:

5

取消

确定

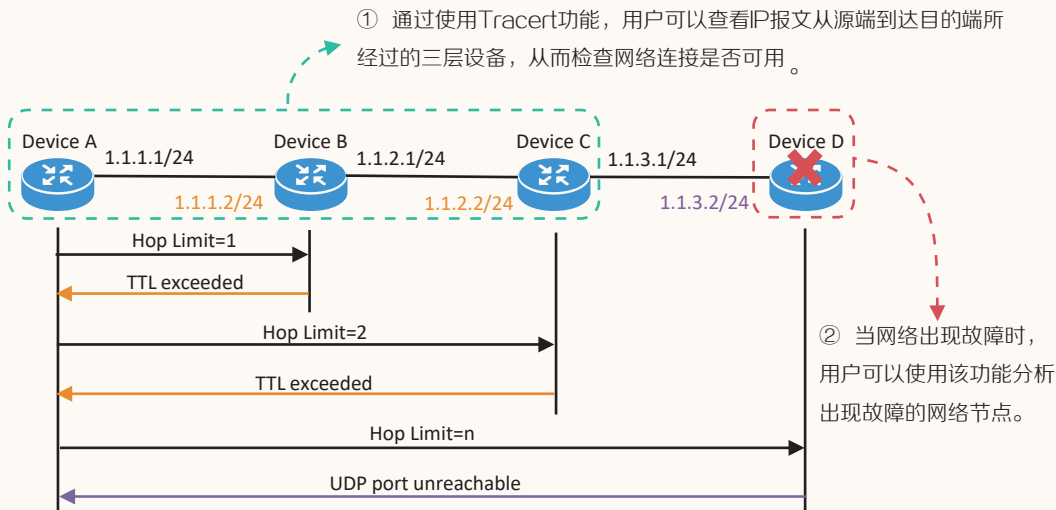
诊断结果



Tracert

当网络出现故障时，通过Tracert功能可以对设备进行Tracert操作，来诊断网络之间的故障节点。

基本原理



Tracert诊断流程

- ① 选择设备、IP类型
- ② 填写目的地址、端口
- ③ 填写Tracert参数（超时时间、初始TTL、最大TTL和包数量）
可选设备所属VPN

诊断

* 设备名称：

CPE1

VPN名称：

请选择

* IP类型：

IPv4

出接口名称：

请选择

源地址：

172.11.1.2

* 目的地址：

10.10.1.1

* 目的端口：

33434

* 超时时间(ms)：

5000

* 初始TTL：

1

* 最大TTL：

30

* 包数量：

3

取消

确定

诊断结果

刷新

诊断

清除

☐	站点名称	设备名称	出接口名称	VPN名称	源地址	目的地址	开始时间	状态	操作
☐	CPE1	CPE1	GigabitEthernet...		172.11.1.2	10.10.1.1	2022-06-13 17:4...	成功	

目的地址: 10.10.1.1

开始时间: 2022-06-13 17:46:41

站点名称：CPE1

设备名称：CPE1

该跳地址：172.11.1.2/24

平均时延(ms)：--

接口名称：GigabitEthernet2/...

方案亮点



简化运维操作

提供图形化操作界面，运维诊断工具轻松上手。Telnet方式无需配置即可接入设备。

直观数据展示

Ping、Tracert支持运维诊断数据的可视化，以图表形式呈现诊断结果。

一站式服务

常用运维诊断工具集中化，快速辅助故障排查与检测，提升运维效率。

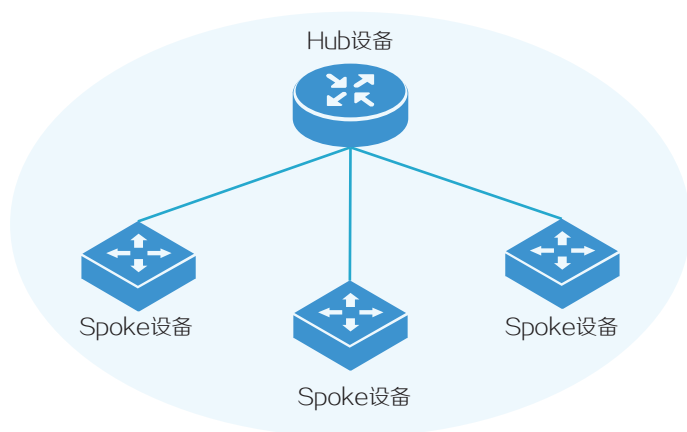
AD-WAN分支解决方案之

丰富的组网场景支持

简介

AD-WAN分支解决方案支持丰富多样的网络拓扑模型及组网场景。

拓扑模型

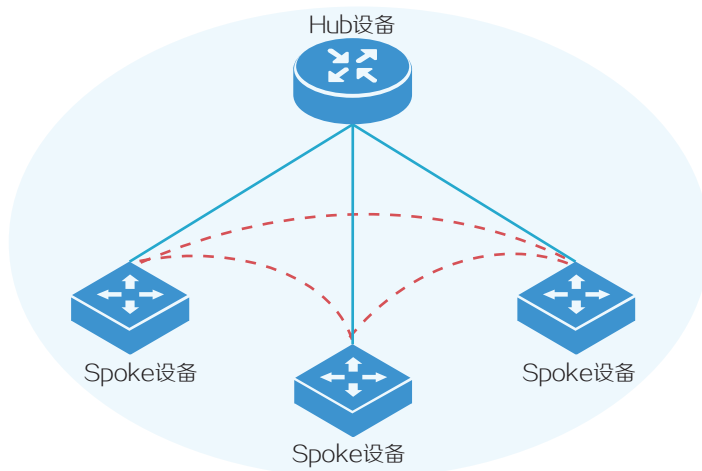


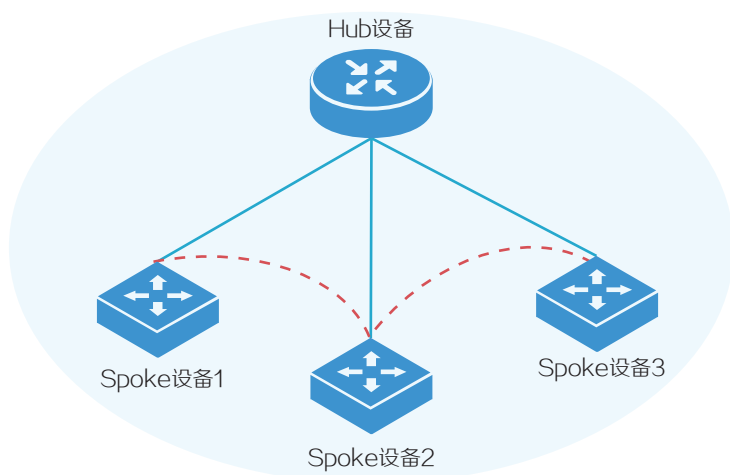
Hub-Spoke拓扑

- Hub-Spoke组网省略了汇聚层,核心层设备 (Hub设备) 直接和接入层设备 (Spoke设备) 相连
- Spoke之间不能建立隧道直接通信, 只能通过Hub转发数据
- 具有高扩展性

Full-Mesh拓扑

- Spoke和Spoke之间可以建立隧道直接通信
- 减轻核心层设备 (Hub设备) 负载



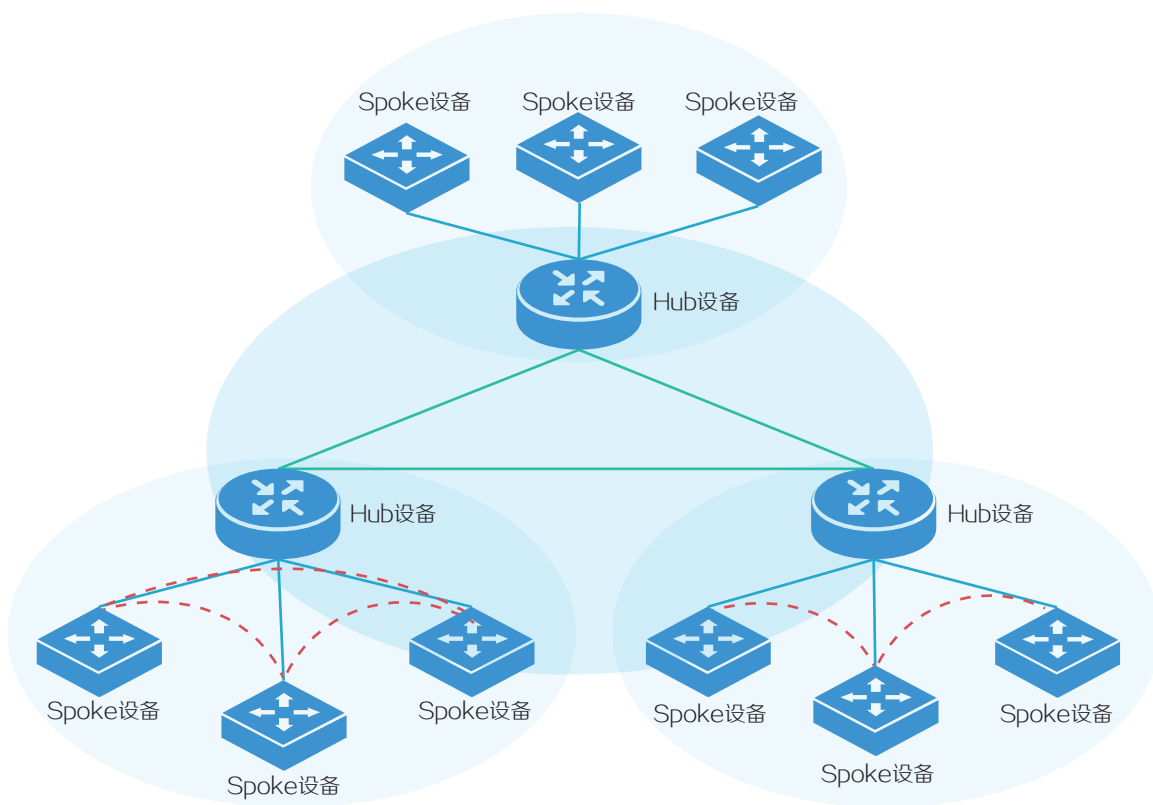


Partial-Mesh拓扑

- 部分分支不支持与各分支互联，可固定一个分支作为跳板和各分支互联
- 例如：分支3要访问分支1，分支1不能和分支3互联，则可以先访问分支2，再通过分支2访问分支1

分区域拓扑

与Hub-spoke或是Full-Mesh一样，区别在于：类似于区域和区域相连，再连接一个更大的区域，这个大的区域再和其他大的区域连接。适用于跨国网络。



组网场景



AD-WAN支持站点间任意灵活拓扑部署。

企业自建组网场景

- 多总部二级组网
- 多总部三级分层组网

运营商POP点组网场景

在运营商POP点部署AD-WAN
网关设备为多租户共用。

云管理组网场景

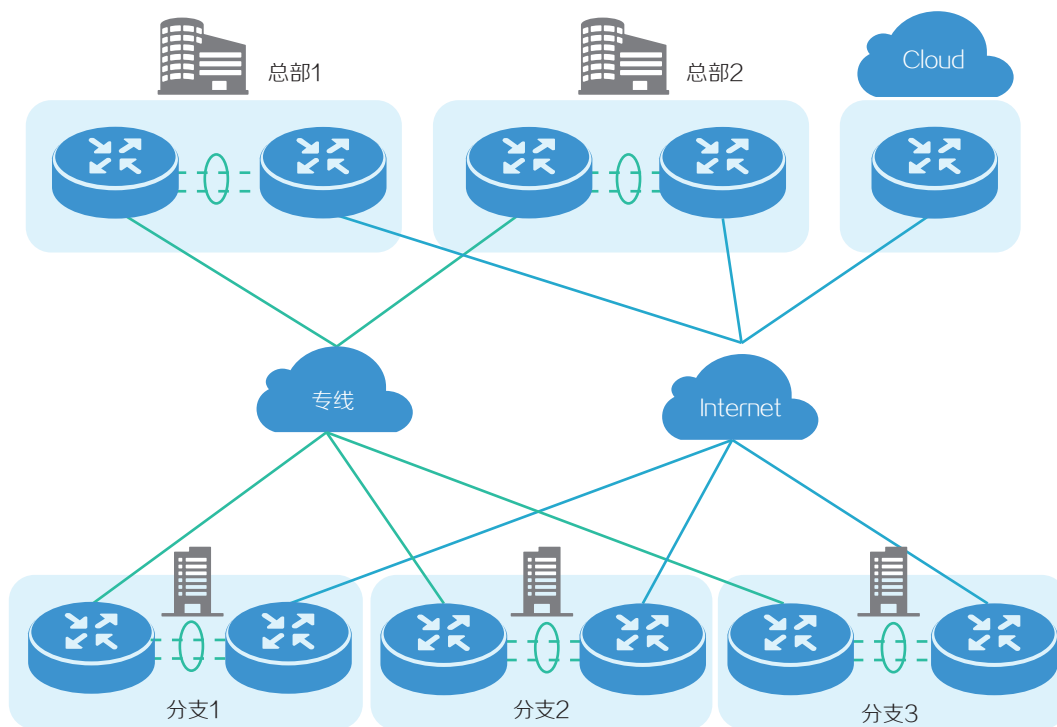
云端部署控制组件为企业
提供AD-WAN控制组件管理服务。



企业自建组网场景

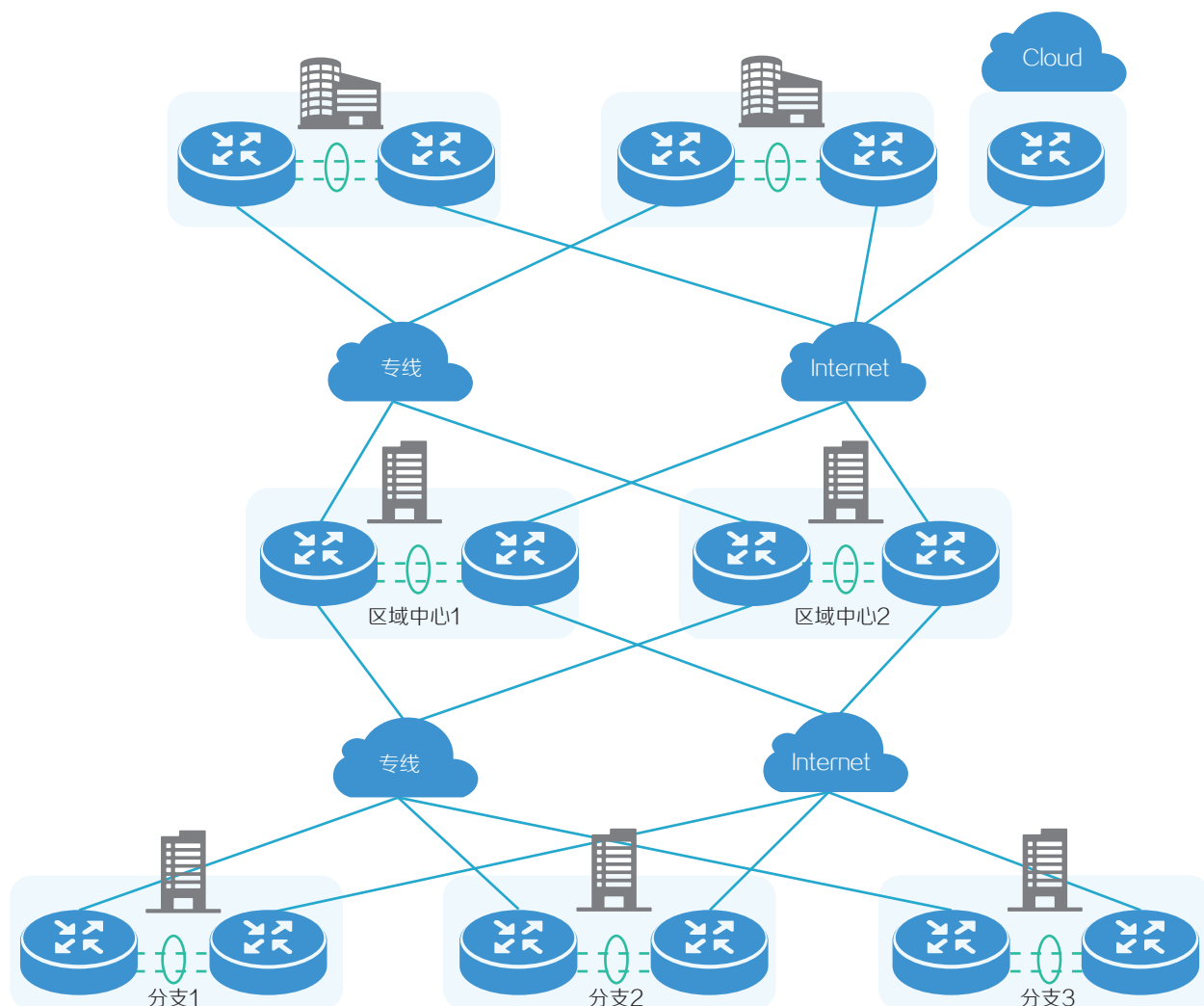
本地部署控制组件，由企业自己的运维团队进行维护管理。

多总部二级组网



企业分支、企业总部和数据中心之间直接连接的组网。分支访问的业务应用集中在企业总部或数据中心。

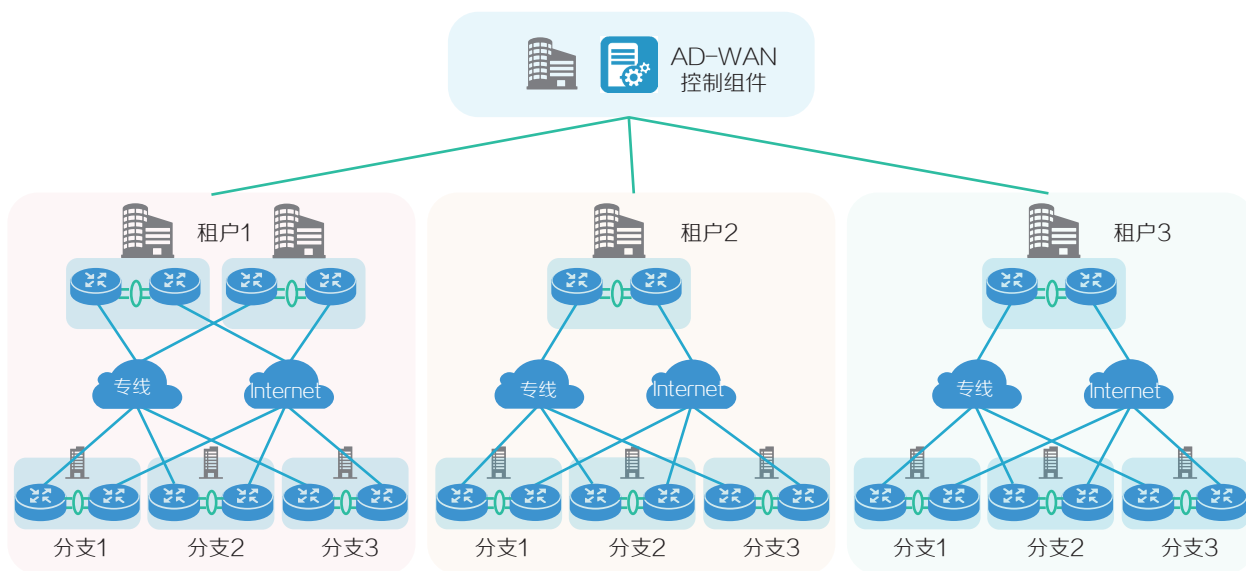
多总部三级分层组网



企业分支通过不同区域的汇聚中心连接企业总部，企业分支既有访问汇聚业务的需求也有访问企业总部业务的需求。

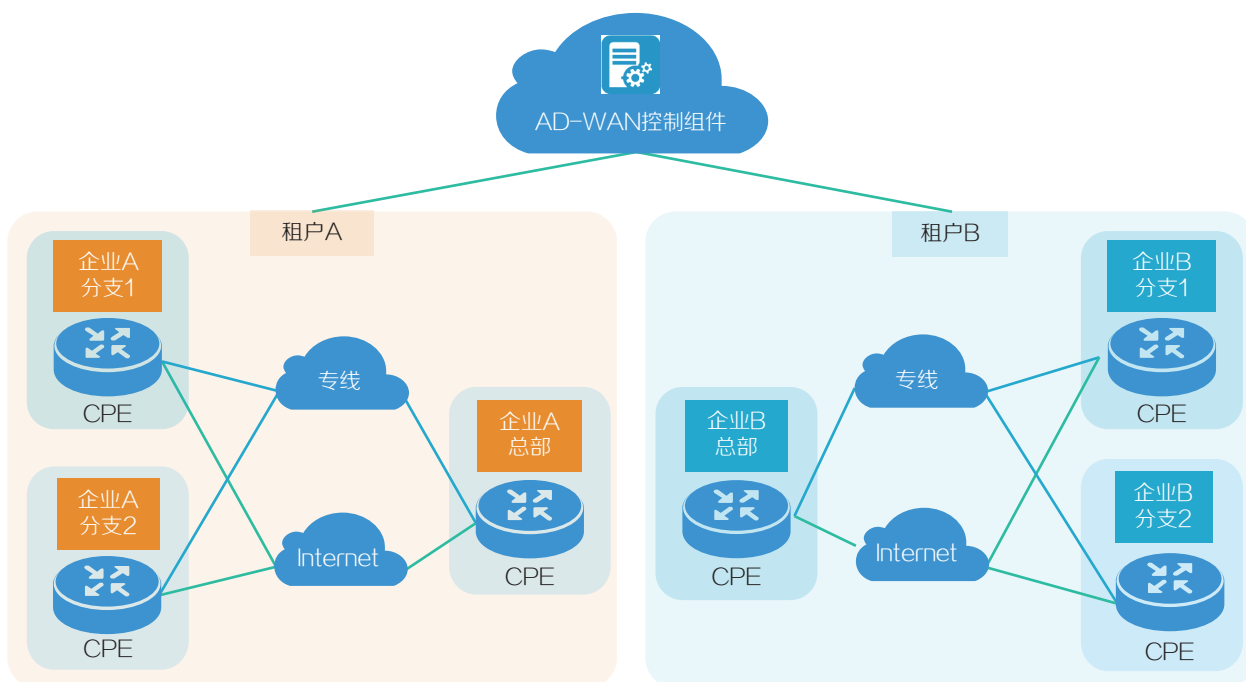
企业多网络实例组网场景

AD-WAN支持分支多租户需求，每个租户对应一个区域。控制组件在总部，区域“独立”使用控制组件。总部具有查看、管理分支区域的权限和能力。



云管理组网场景

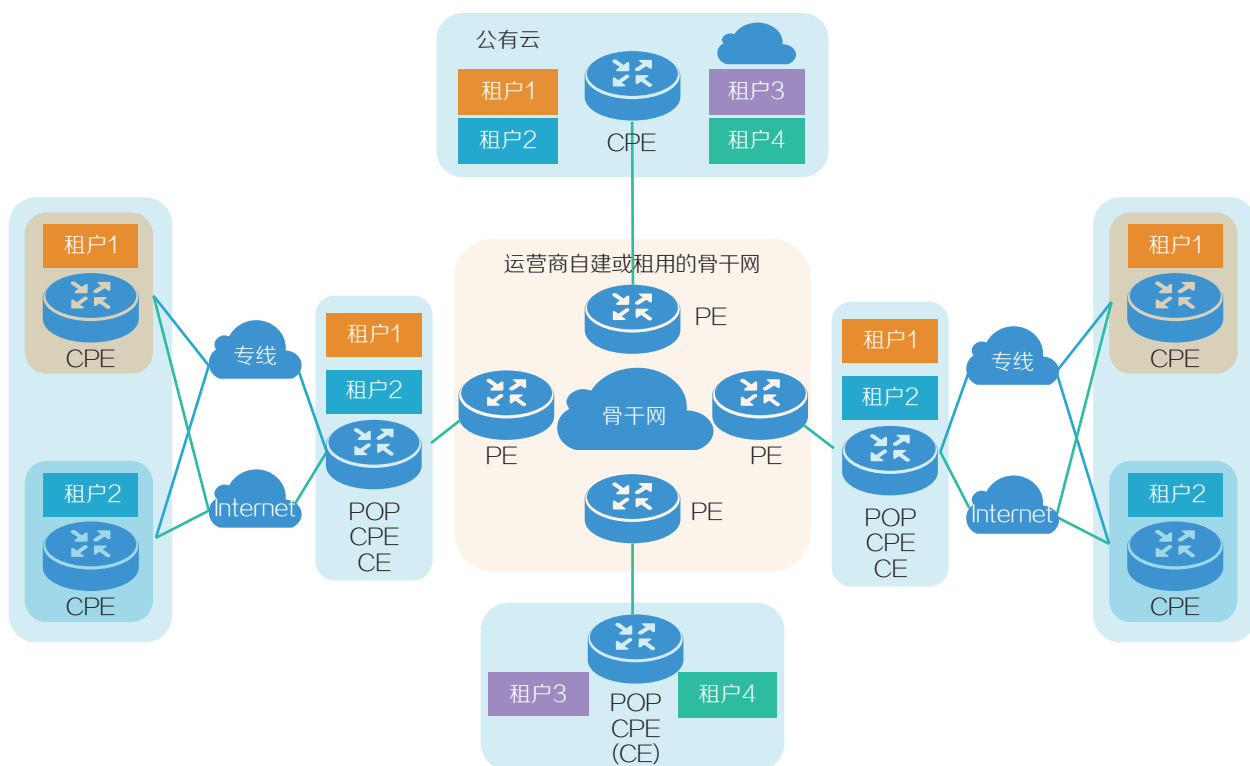
云端部署多租户共用的控制组件为多企业租户提供AD-WAN服务。企业作为租户租用AD-WAN服务。企业租户可管控本企业范围内所有站点的AD-WAN业务，但无法查看其他租户的业务。此场景下多租户设备不共用。





运营商POP点组网场景

在运营商POP点部署AD-WAN网关设备接入区域内企业站点。运营商POP点按地域分隔成不同区域，不同区域的POP点网关需要通过专门的区域互通POP网关才能互通（一般多用于跨国或跨地区POP组网）。



AD-WAN分支解决方案之 精细化应用分类

业务需求



流量识别

生产流量、办公流量、娱乐流量…



访问控制

完全访问、部分访问、禁止访问



流量统计/限速

实时统计、历史统计、限制下载速度…

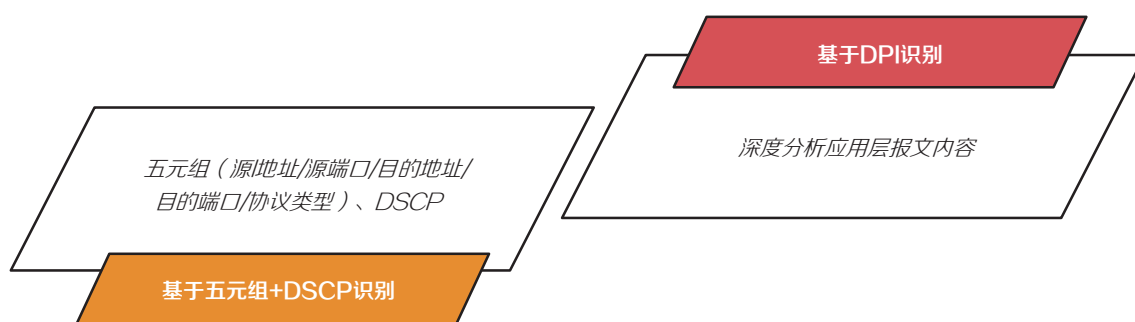


流量可视化

基于统计数据提供可视的分析图表

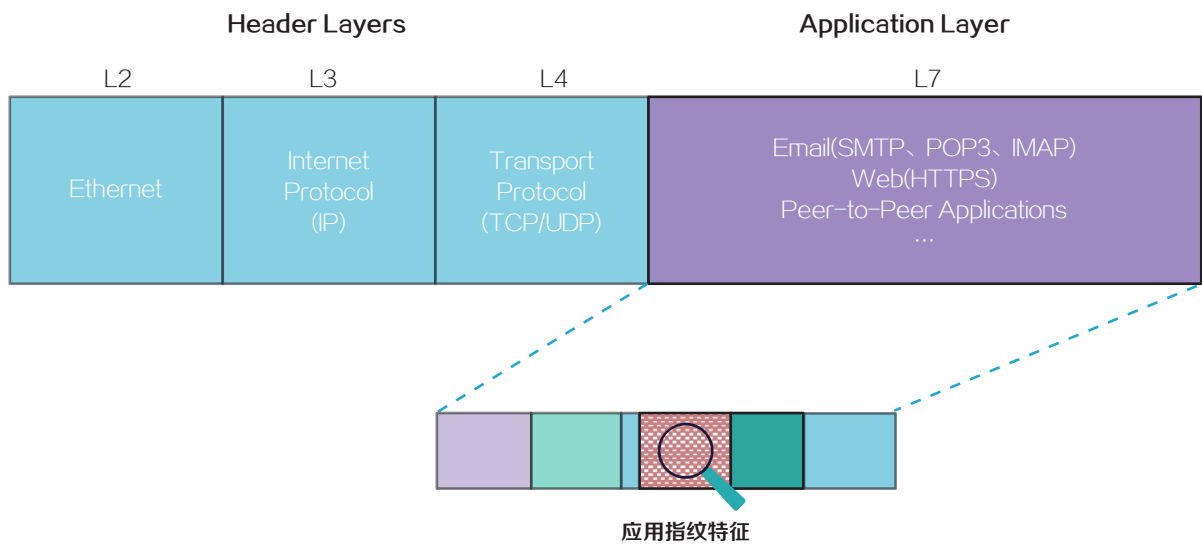
只有精准的识别应用流量，才能有针对性的提供差异化服务。

应用识别技术



传统网络的普通报文检测往往只分析IP分组四层以下的内容，一般包括源地址、源端口、目的地址、目的端口、协议类型以及DSCP。

一些基于应用的业务（例如QoS，带宽管理等）在进行报文处理时需要知道报文所属的应用层协议，这时普通的报文检测就无法满足需求，因此基于DPI（Deep Packet Inspection，深度报文检测）的应用识别技术应运而生。



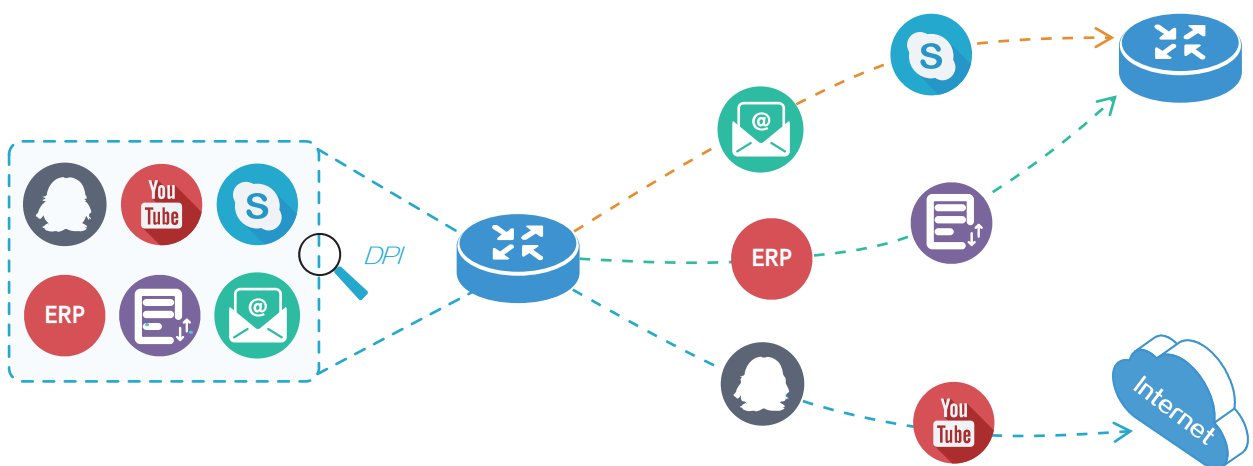
DPI简介

DPI是相对普通报文检测而言的一种新的检测技术，DPI对OSI协议中的第七层，即应用层的内容进行深度分析，从而根据应用层的净荷特征识别其应用类型或内容。

当IP数据包、TCP或者UDP数据流经过基于DPI技术的网络设备时，DPI引擎通过深入读取IP包载荷的内容来对七层协议中的应用层信息进行检测，从而识别出IP包的应用层协议。



DPI自动识别L4-L7层应用，精准调度流量



应用场景

AD-WAN控制组件使用DPI的APR（Application Recognition，应用层协议识别）作为应用识别的方式，并能够对接口上接收或者发送的某个应用层协议的报文进行数目和速率统计。

为了更好地识别报文所属的应用层协议，APR提供了两种应用识别方式：PBAR和NBAR。

1、PBAR

PBAR（Port Based Application Recognition，基于端口的应用识别），即根据定义的应用层协议端口与应用映射关系识别报文所属的应用层协议。



2、NBAR

NBAR（Network Based Application Recognition，基于内容特征的应用识别），即提取应用报文区别于其它应用报文的特征，通过将报文的内容与特征库中的特征项进行匹配来识别报文所属的应用层协议。



头域类型

- URI：匹配统一资源标识符（Uniform Resource Identifier），由协议、主机IP地址和主机资源的具体地址三部分组成
- Host：匹配请求资源的Internet主机和端口号

应用特征类型

应用特征分为预定义和自定义两种，预定义应用由系统缺省创建，自定义应用由用户通过手工配置创建。



配置流程

使用NBAR方式时,需要事先**配置规则和检查项**,在增加应用特征时绑定规则,通过头域和关键字来识别报文;使用PBAR方式时,仅需要在增加应用特征时**配置端口与应用映射关系**。

配置流程如下:

01 配置检查项

检查项中可以配置头域类型及关键字,用来匹配识别HTTP报文的URI和主机名,检查项可被规则引用。

02 配置规则

规则中可以配置头域类型及关键字,并可以引用多个检查项,同时满足匹配规则和所有检查项的报文为匹配规则的报文。

03 配置应用特征

包括预定义应用特征和自定义应用特征。对于NBAR方式,若报文符合应用特征中任意一条规则,则符合该应用特征。

04 配置应用特征组

应用特征组可引用多个自定义应用特征和预定义应用特征。若报文符合任何一个应用特征，则符合该应用特征组。

05 配置自定义应用

自定义应用时可引用应用特征组。若报文符合该应用特征组，则被识别为属于此应用，也即属于引用此应用的应用组。

方案亮点

1、快速识别

AD-WAN控制组件在对行业标准应用，如Email、Web、FTP等进行识别时，无需进行繁琐的应用预定义操作，可基于DP特征库进行自动化识别，提升应用识别效率。

2、精准识别

AD-WAN控制组件综合利用基于五元组识别和基于DPI识别两种应用识别技术，可精细化识别企业私有应用和行业标准应用，为做好精细化的流量调度打好基础。

AD-WAN分支解决方案之 智能调度技术RIR

>>> 简介

传统的链路优选一般基于链路开销或路由策略，无法根据实际的业务需求选择最适合的链路。

RIR (Resilient Intelligent Routing, 智能选路)可以根据不同业务流量的链路需求，如链路质量、链路带宽等，为其**选择最适合的链路**。如果业务流量当前选择的链路由于链路状态变化而不再符合要求，智能选路还可以**自动将流量切换到**另一条符合要求的链路上。

>>> 方案介绍

智能选路应用于总部-分支架构下的企业组网环境。在AD-WAN分支解决方案中，AD-WAN控制组件和支持RIR功能的设备结合使用，可以为用户提供分布式流量智能调度能力。

01

AD-WAN控制组件定义策略

- 定义策略
- 定义应用
- 绑定策略

02

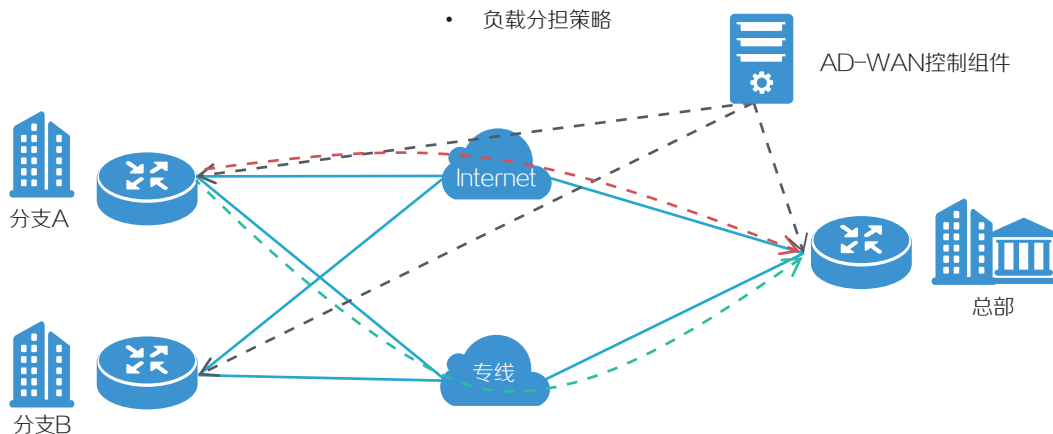
策略下发设备

- 链路优选策略
- 链路质量策略
- 链路带宽策略
- 时间调度策略
- 负载分担策略

03

设备自主决策

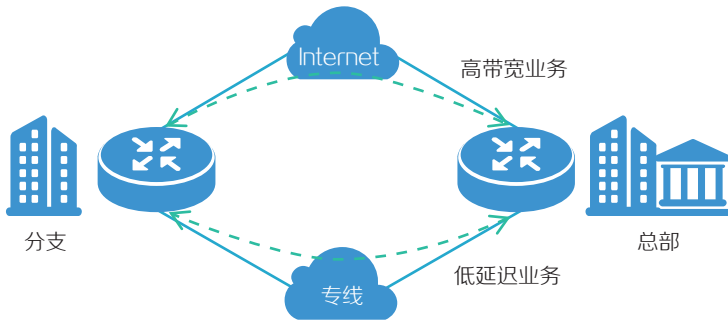
- 设备实时监控网络状态
- 根据网络状态及策略实时切换路径



AD-WAN控制组件仅下发策略，设备自主调度，反应速度更快、可靠性更高

>>> 使用场景

1、链路优选策略

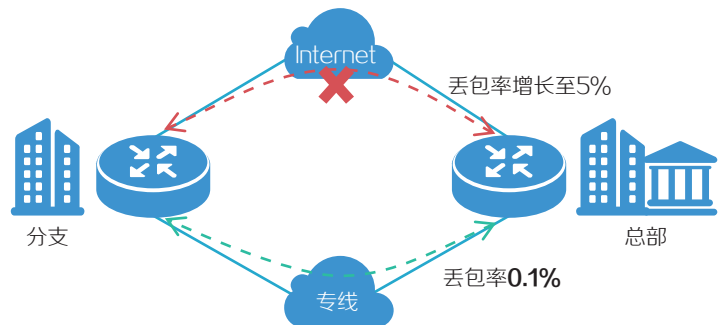


基于预定义的链路优先级选路：

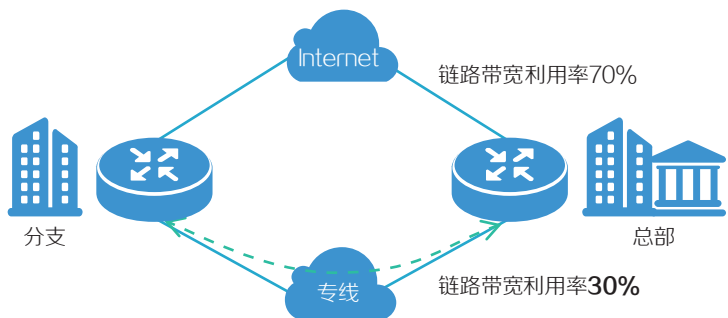
- 低延迟业务走专线
- 高带宽业务走Internet

2、链路质量策略

基于链路质量探测结果选路，
链路质量不符合业务要求时，
自动调整至新链路



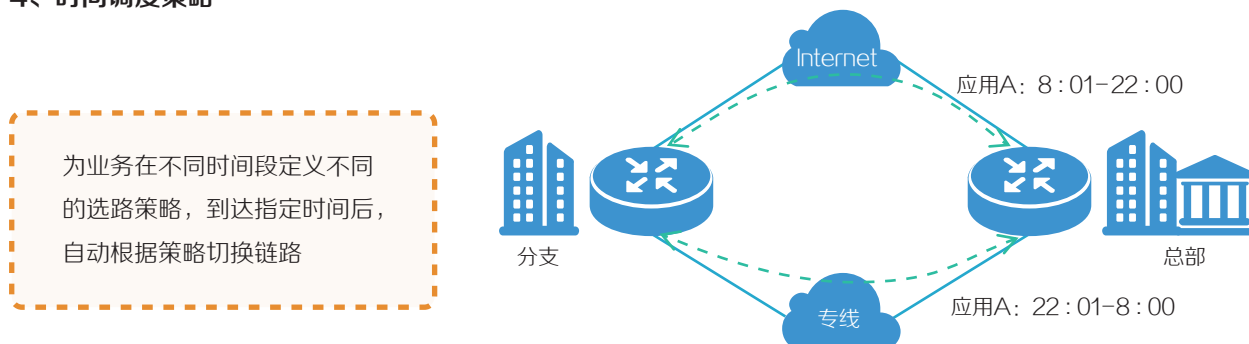
3、链路带宽策略



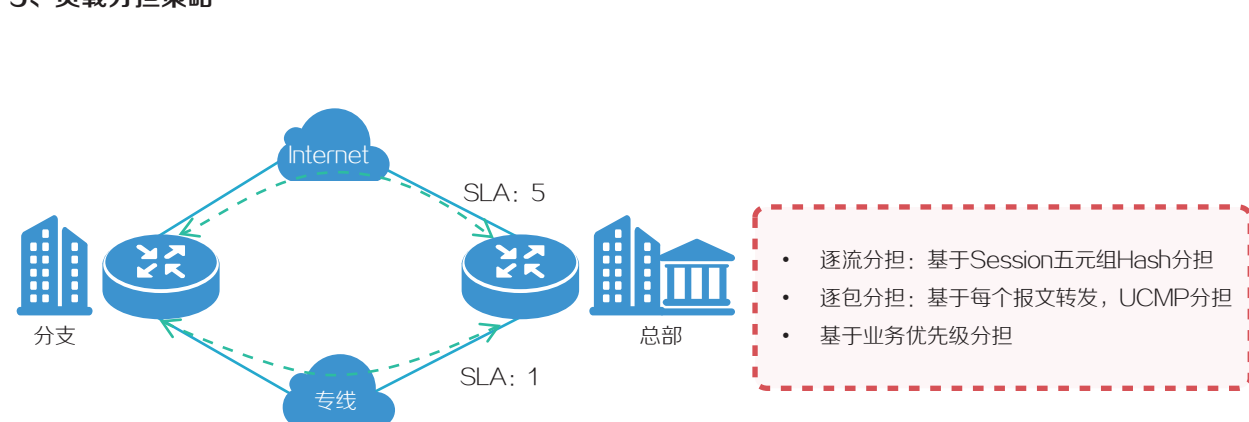
基于链路带宽状态和会话预计使用的
带宽选路：

剩余带宽、链路总带宽、带宽利用率

4、时间调度策略



5、负载分担策略



>>> 方案亮点

用户策略驱动选路

无需手工配置繁琐的策略路由，用户定义选路策略，AD-WAN控制组件集中完成选路策略统一部署

分布式实时选路

设备实时探测网络流量变化和网路质量、带宽利用率变化，根据网络现状，动态自主进行业务转发路径调整

智能选路

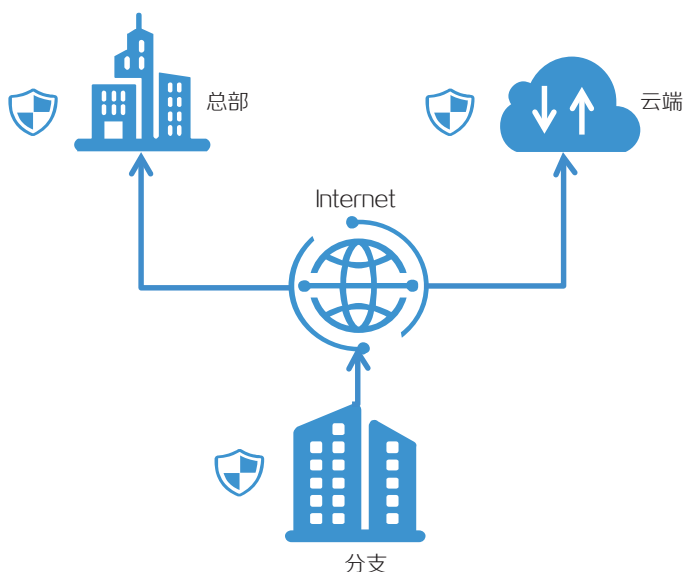
精细化选路

根据链路类型、链路带宽、链路质量、时间等丰富的选路 and 调度策略进行精细化选路

AD-WAN分支解决方案之安全

安全风险

由于大部分用户重视总部安全建设而忽略了分支机构的安全防护。现如今分支侧面临**传输安全**、**上网安全**、**边界安全**问题。



- **传输安全**：没有加密的数据传输存在被监听、拦截、窃取的风险。
- **上网安全**：内部员工上网安全管理，行为审计，出口管控，做到合法合规。
- **边界安全**：存在被攻击的风险，特别是未知威胁等新型攻击很容易绕过传统边界防御。

方案介绍

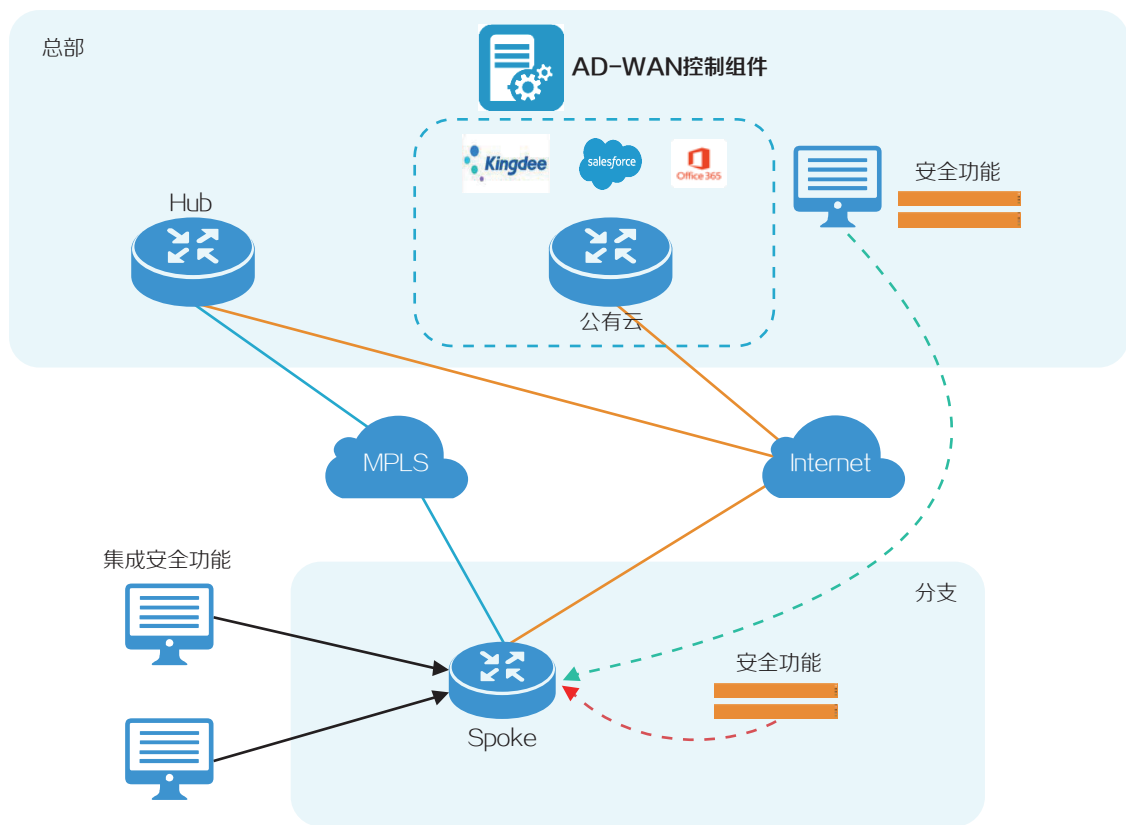
AD-WAN分支方案站点边界无需单独部署安全设备，简化部署；CPE设备自身集成安全功能，降低成本，加固分支安全。

目前全系列的SD-WAN设备，集成FW、IPS、URL过滤等安全功能，支持2~7层业务流量的全面监控和过滤。

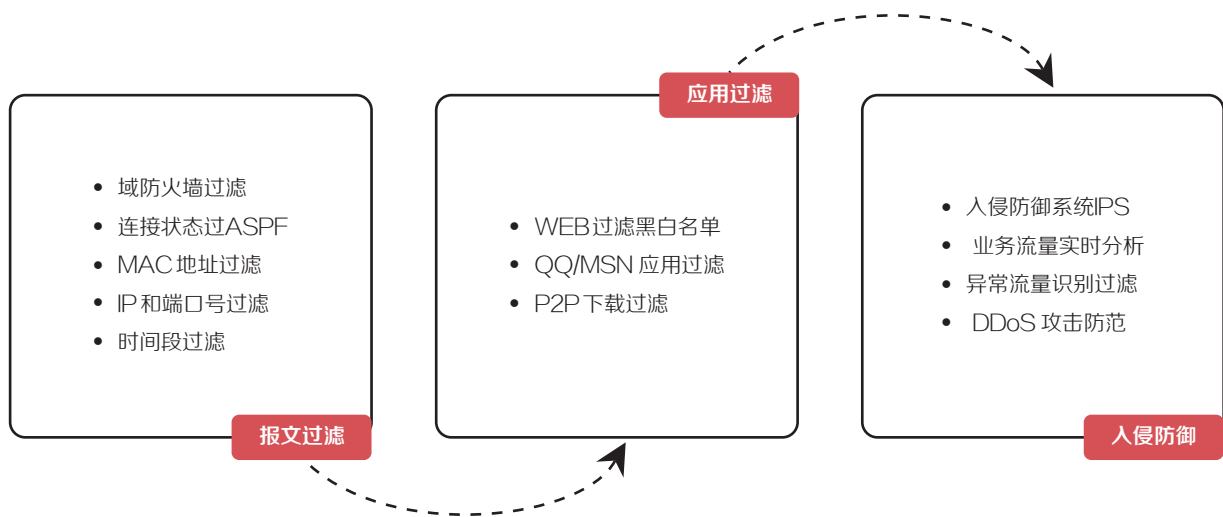
通过**安全控制组件**，安全业务也可以全流程自动下发，简化配置的复杂度，提升运维效率。

支持对接第三方安全云网关，利用第三方云安全网关对访问公有云、SaaS的业务流量进行安全防护。

全局自动化国密，一键部署。



2至7层业务流量全面监控和过滤



应用场景

1、传输安全

针对传输安全挑战，AD-WAN分支方案有对应的安全策略。通过不同的加密算法与认证算法的组合，搭配出不同的加密方案。

IPsec

AD-WAN分支方案支持配置和展示全局IPsec信息，支持IPsec抗重放检测。**使用场景：4G/5G/Internet/强加密需求时开启。**控制组件自动下发相应配置。

加密方案

AD-WAN分支方案支持多种加密方案。（简单分点介绍一下，重点介绍国密方案）

加密方案

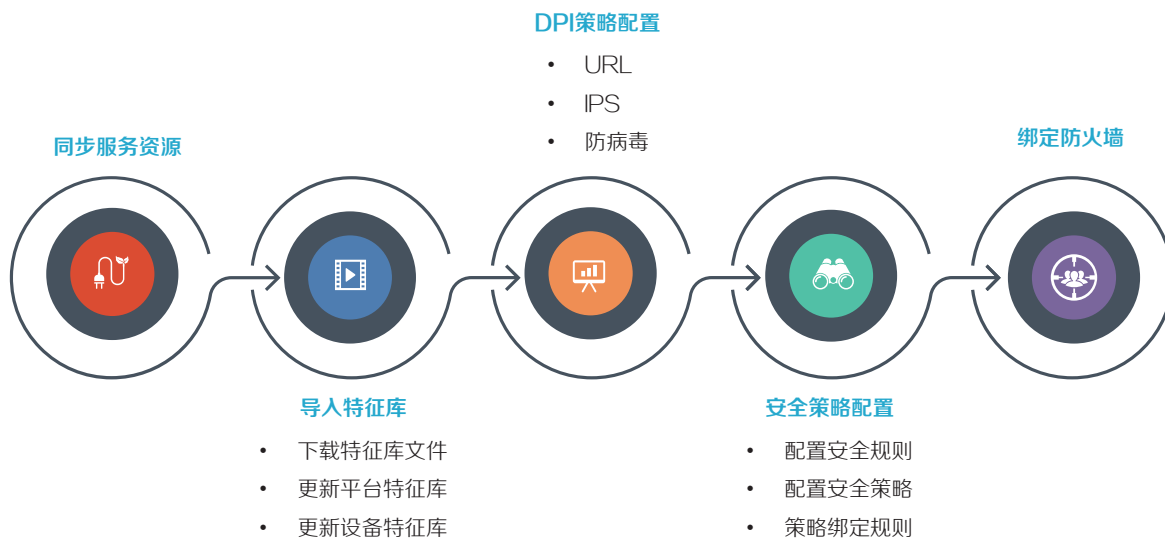
加密方案	请选择
报文封装方式	请选择
安全协议	推荐加密方案
加密算法	强加密方案
认证算法	国密加密方案
	国密硬件加密方案
	三重数据加密方案
	自定义加密方案

确定



2、上网安全

针对上网安全挑战，AD-WAN分支方案中边界设备支持防火墙、URL过滤、IPS以及防病毒安全策略。



基本包过滤防火墙

使能防火墙使能后，系统默认阻断从WAN侧网络主动访问内网的人方向业务，默认允许从内网主动访问WAN侧网络的出方向业务。

可通过创建“入方向允许列表”或“出方向禁止列表”来控制出入方向访问需求。

入方向允许列表/ 出方向禁止列表	协议	通过选择名字或选择“Protocol Number”并输入数字来指定规则匹配报文的协议类型。
	源IP	规则匹配报文的源IP地址。
	源端口	规则匹配报文的源端口。 仅在协议为“TCP”或者“UDP”时可以配置。
	目的IP	规则匹配报文的目的IP地址。
	目的端口	规则匹配报文的目的端口。 仅在协议为“TCP”或者“UDP”时可以配置。
	描述	描述规则的含义或注意事项，方便理解和维护。

IPS

IPS（Intrusion Prevention System，入侵防御系统）是一种可以对应用层攻击进行检测并防御的安全防御技术。IPS通过分析流经设备的网络流量来实时检测入侵行为，并通过一定的响应动作来阻断入侵行为，实现保护企业信息系统和网络免遭攻击的目的。

设备基于IPS策略对报文进行IPS处理。IPS策略中定义了匹配报文的IPS特征和处理报文的IPS动作。预定义IPS特征使用系统预定义的状态和动作。

URL过滤

URL过滤功能可以对用户访问的统一资源定位符URL（Uniform Resource Locator）进行控制，允许或禁止用户访问某些网页资源，达到规范上网行为的目的。当用户发起HTTP请求时，CPE设备作为企业网关通过URL过滤功能可以允许或禁止用户访问某些网站资源。设备支持预定义和自定义两种URL过滤规则。

防病毒

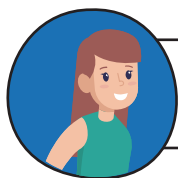
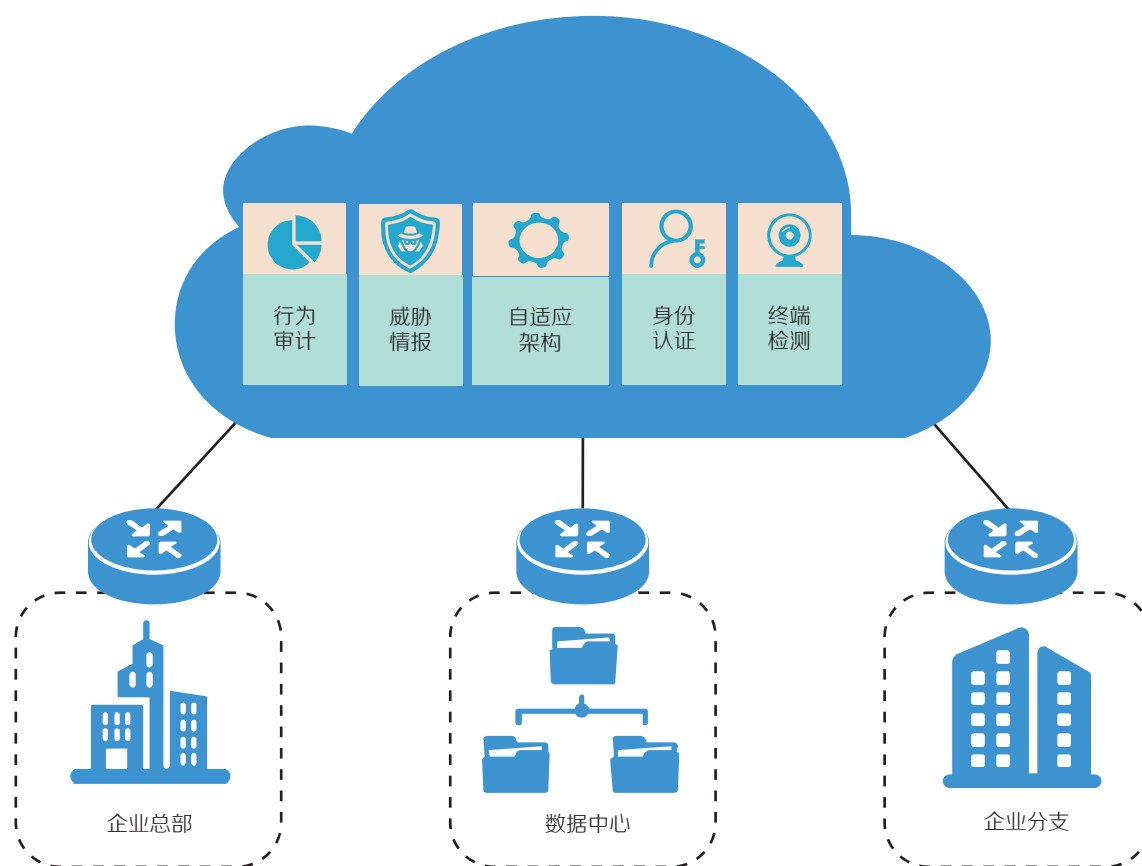
防病毒功能是一种通过对报文应用层信息进行检测来识别和处理病毒报文的安全机制。分预定义病毒特征库和自定义病毒特征系统。

3、边界安全

针对边界安全挑战，AD-WAN分支方案有对应的安全策略。

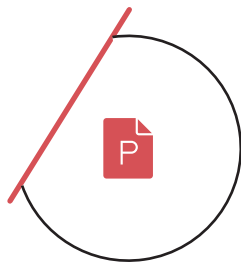
SASE

SASE（Secure Access Service Edge，安全接入服务边缘），是建立在SD-WAN网络解决方案之上，可在任何边缘（WAN边缘、云边缘、DC边缘、核心网络边缘、分支边缘和移动远程员工边缘）的任何地方保证安全连接和访问关键资源。对接第三方安全云网关，即AD-WAN方案通过GRE或IPsec隧道与安全云网关集成，为直接上网的站点/用户提供全面的安全性、可见性、控制和数据保护。

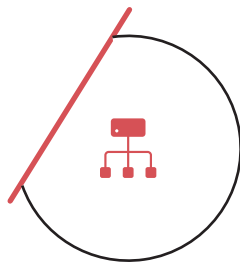


通过对接自己或者第三方安全云（Zscaler、Forcepoint等），以提供满足SASE场景的安全需求。通过建立点到点的隧道实现流量转发到指定云网关，实现对指定流量的安全审计与过滤。

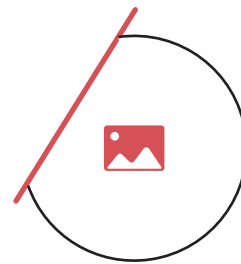
分支方案对接第三方安全云网关方案采用分离的方式实现，技术优点如下：



分离的方式实现使得SASE实现更加简单、灵活。



分离的方式仅需考虑方案CPE设备如何配置GRE即可，对端配置由客户自行解决，所有均为标准协议。

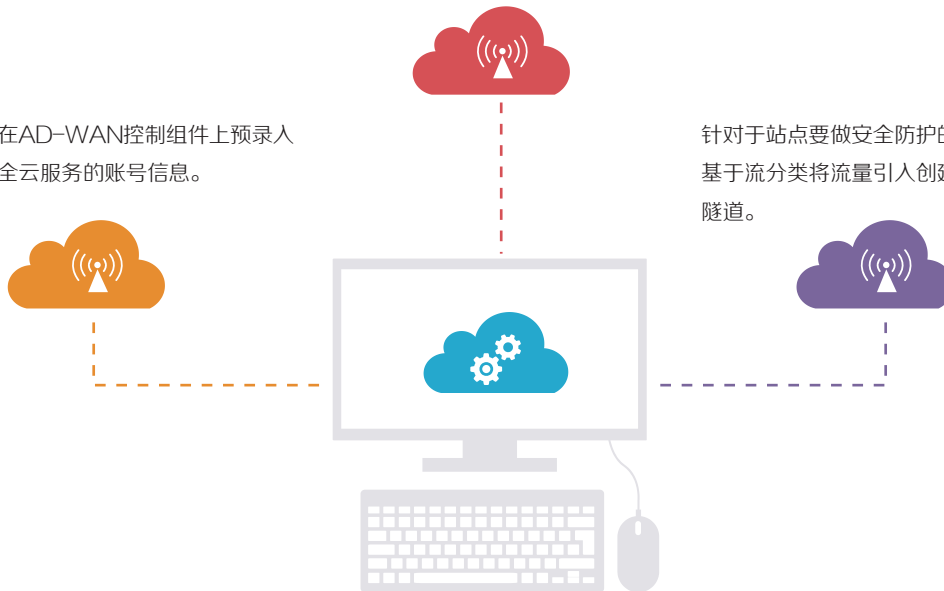


分离的方式对于后续配合更多的第三方云网关厂家也没有丝毫的限制。

登录 AD-WAN控制组件在站点设备上开启云安全策略时，自动在安全云网关和站点设备上配置GRE引流隧道。

管理员在AD-WAN控制组件上预录入登录安全云服务的账号信息。

针对于站点要做安全防护的上网流量，基于流分类将流量引入创建好的安全云隧道。



配置流程

增加云安全策略

* 策略名称 :

* ACL标识 :

* 设备名称 :
174

Keepalive周期(s)/重试... :
5 / 3

主隧道

备隧道

* GRE隧道IP :

GRE隧道IP :

* GRE隧道源IP/接口 :
请选择

GRE隧道源IP/接口 :
请选择

* GRE隧道目的IP :

GRE隧道目的IP :

* 远端GRE隧道IP :

远端GRE隧道IP :

GRE Key :

GRE Key :

GRE校验和 :
☐ 开启
☒ 关闭

GRE校验和 :
☐ 开启
☒ 关闭

确定

取消

方案亮点



AD-WAN分支解决方案之 广域网优化

传统广域网的挑战

随着企业数字化转型快速发展，传统广域网面对更多的挑战，在应用繁多、需求各异的业务场景下，存在如**音视频卡顿**、**应用运行缓慢**、**带宽快速消耗**等问题。为了改善用户体验，提高应用运行质量，**广域网优化**技术随之产生。

方案介绍

广域网优化功能包括：

- WAAS（广域网应用服务）技术：用于改善广域网络高延迟、低带宽的缺点。
- WebCache（网站缓存）技术：用于把用户访问过的静态资源及数据存储到代理服务器，可以达到降低访问延迟、提升访问速度的目的。

01

WAAS

通过TFO、DRE和LZ技术，加速文件传输，降低网络延迟，降低丢包率

02

FEC

根据实时丢包率调节平均抗丢包率，减少广域网链路传输的数据量，提高数据传输速度

03

多链路包复制

利用多链路优势，有效降低甚至解决因单条链路丢包导致的业务中断等问题

04

WebCache

通过代理服务实现Web资源和数据的缓存，减少链路传输的数据量，提升网站访问速度

主要功能

1、WAAS

WAAS是一种能够对广域网链路流量提供优化的技术，支持TFO优化、DRE和LZ技术。

TFO (Transport Flow Optimization，传输层流优化)

在不改变TCP流量的源、目的IP地址和端口号的情况下，在广域网链路两端对TCP连接进行透明代理。同时，对广域网链路两端的TCP流量进行优化，在确保可靠性传输的前提下，能尽可能增大网络吞吐量，又不会造成网络拥塞。



- ① 扩大接收缓冲区：灵活设置接收缓冲区大小，提升网络吞吐量。
- ② 慢启动优化：灵活设置拥塞窗口初始值，缩短TCP连接达到网络最大吞吐量的时间。
- ③ 选择性确认 (SACK)：允许接收端通知发送端所有正确接收的数据，减少不必要的重传。

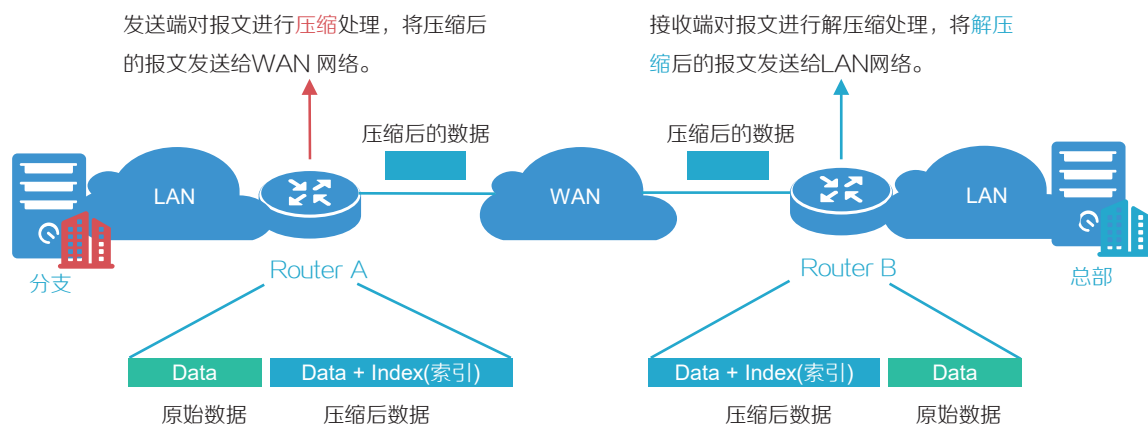
在TCP 握手建立连接的过程中，Router A 与Router B 协商出两者的TFO 优化能力交集，并使用双方都支持的 优化能力对数据流进行TFO优化处理。

DRE (Data Redundancy Elimination 数据冗余消除)

DRE是一种基于数据块和数据字段的数据压缩和还原技术。

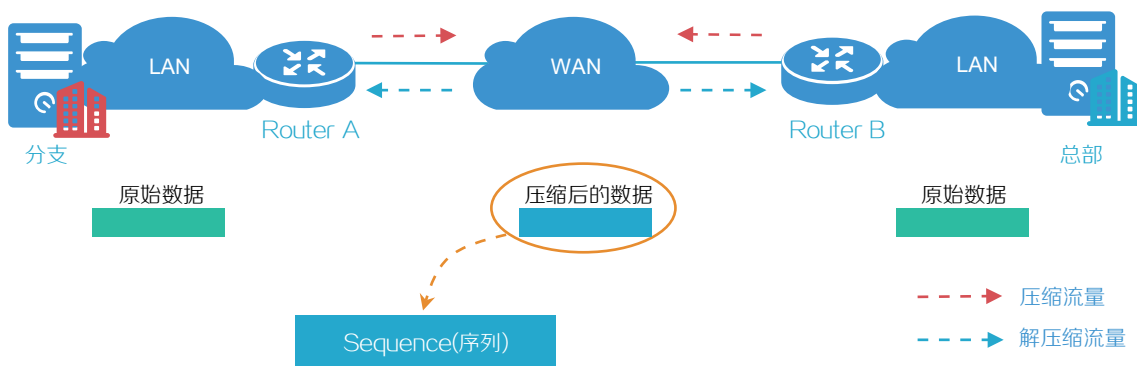
DRE压缩：将重复数据块替换为字典索引在广域网链路上传输。

DRE解压缩：接收端通过识别字典索引，将其还原成重复数据块。



LZ (Lempel-Ziv compression, LZ 压缩)

LZ是一种基于算法的数据压缩和还原技术，主要是通过自建字典方法来进行压缩替换，其压缩字典存在于压缩结果中。



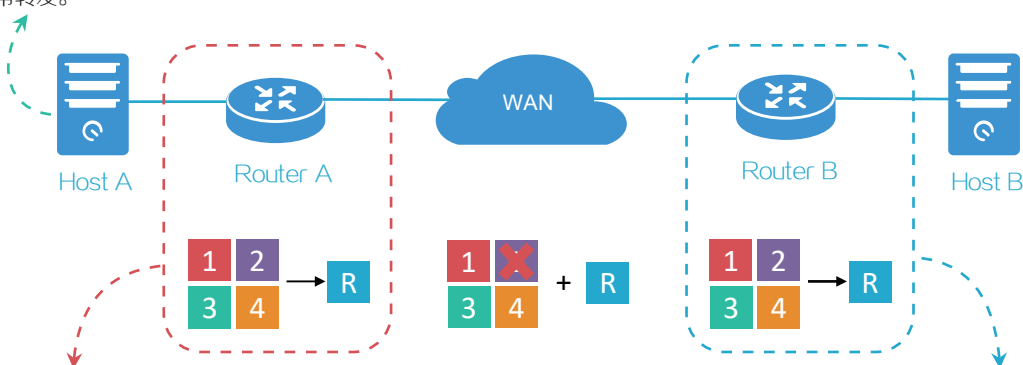
2、FEC

FEC是一种前向冗余纠错技术，可根据数据包和冗余包恢复出丢包数据，提高抗丢包能力，为实时传输的音视频数据（采用RTP实时传输协议）提供可靠保障。

FEC对报文的处理流程如下：

① 音、视频数据包识别

对RTP类匹配WAAS策略，如果匹配到策略，则创建FEC的快速转发表项并设置快速转发业务标记；如果没有匹配到策略，则正常转发。



② FEC编码

缓存数据包，达到编码块包数或缓存时间超时，数据包分组进行FEC编码生成若干冗余包R，分别发送原始数据包和冗余包。

③ FEC解码

缓存数据包，在解码超时时间内，原始数据报和冗余包之和大于等于分组数据包数时进行FEC解码。否则不解码直接发送原始数据报，丢弃冗余包R。

FEC根据平均抗丢包率的配置方式分为固定D-FEC和自适应网络质量的A-FEC。

- A-FEC 根据实时丢包率动态调节平均抗丢包率：发送端在冗余包中加入设备地址信息通告给接收端。接收端对实时数据进行丢包率采样，并周期性的反馈给发送端，从而使发送端调整冗余包个数的生成，减少广域网链路传输的数据量，提高数据传输速度。
- D-FEC 使用配置的固定平均抗丢包率，适用于链路丢包率比较稳定的场景。

3、多链路包复制

多链路包复制是一种冗余纠错技术，**利用多链路优势**，将同一份报文从多条链路发送出去。只要所有链路不同时丢弃报文，则接收端可通过将所有链路上接收到的同一份报文信息进行互相补充，整合成完整的报文流，从而能够有效降低甚至解决因单条链路丢包导致的业务中断等问题。

包复制对报文的处理流程如下：

① 报文识别

识别报文类型，不同报文需要满足不同的包复制条件。

③ 报文去冗余

维护**冗余链**，收到报文后在冗余链中查找报文信息，不存在时加入冗余链，存在时判断是重传报文还是冗余，丢弃冗余报文。

② 报文复制

复制报文，根据等价路由选路规则，选择原始报文出接口链路并发送，选择路由表中其他的等价链路发送复制报文。

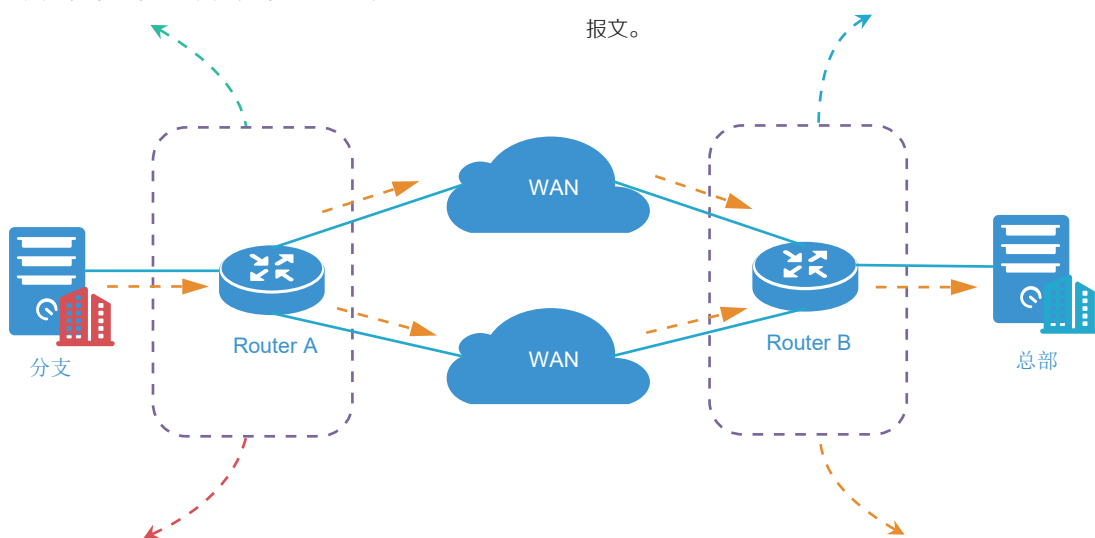
④ 报文保序

维护**保序缓存链**和**期望序号**，收到报文后判断是否为期望序号的报文。

- 若序号**小于等于**期望序号，则发送本报文并更新期望序号。同时，遍历保序缓存链，有相同情况则发送报文并更新序号，直到保序缓存链中缓存的期望序号报文全部发送完毕。
- 若序号**大于**期望序号，则加入保序缓存链。



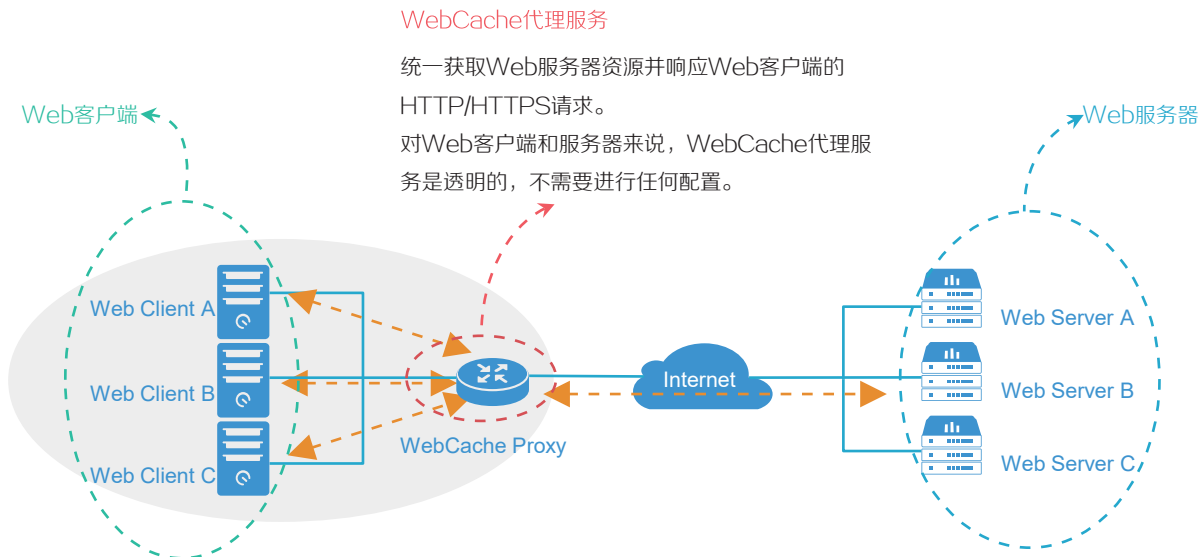
冗余链和保序缓存链均为报文缓存区域。



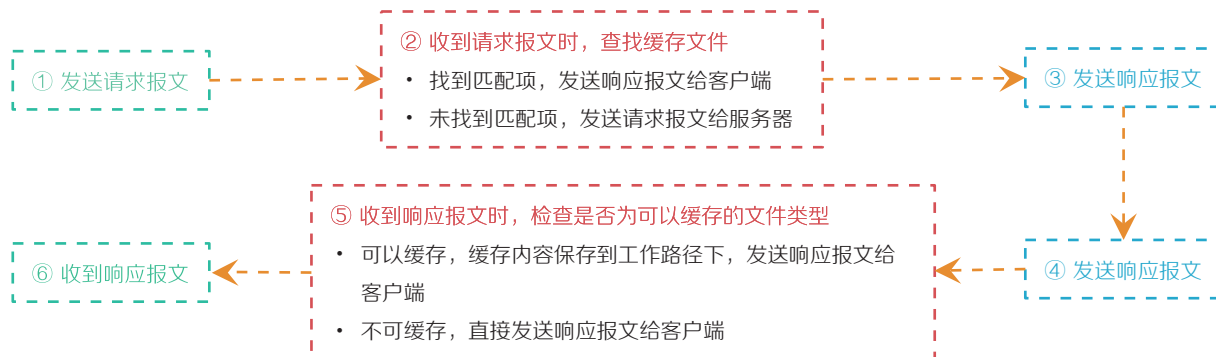
4、WebCache

WebCache是一种缓存技术，通过把用户访问过的静态的资源及数据存储在服务器，可以达到降低访问延迟、提升访问速度的目的。

WebCache 运行机制如下：



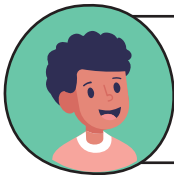
当有客户端请求访问时：



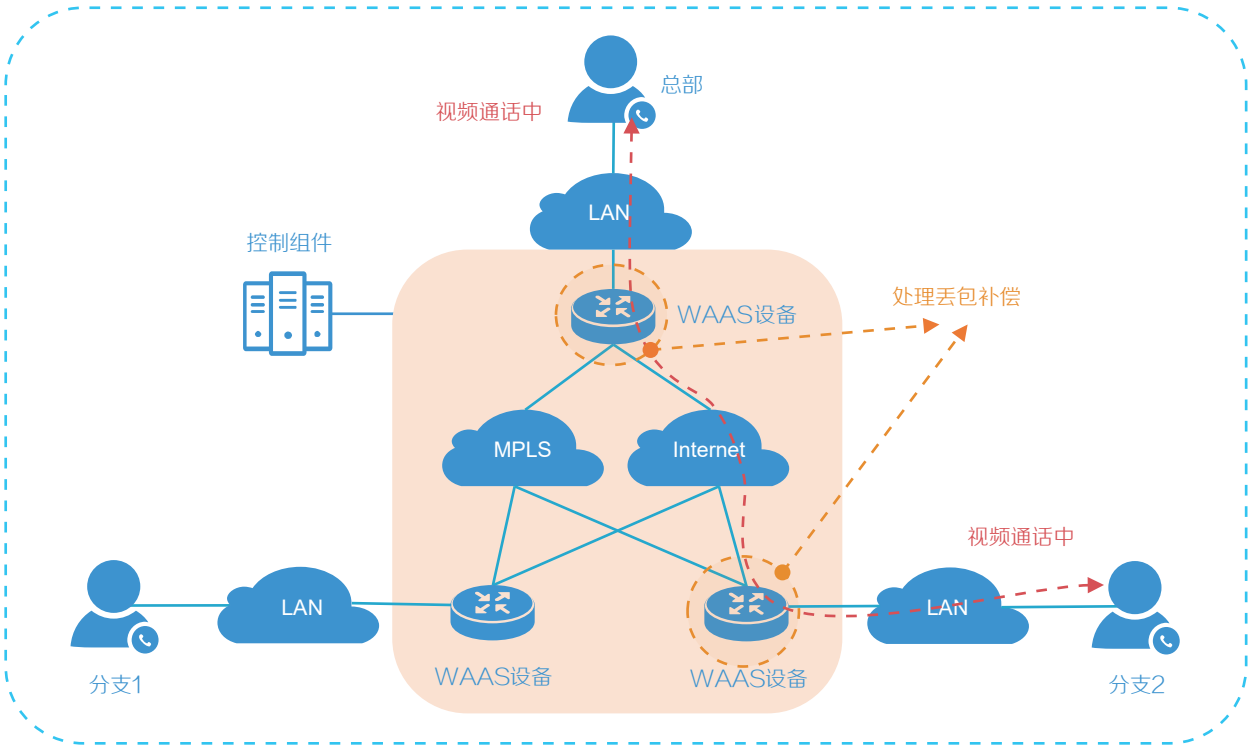
缓存文件：WebCache缓存内容以缓存文件形式存放在代理服务的工作路径中，缓存空间不足时，新文件将覆盖旧文件。

老化时间：缓存文件的老化时间，接收到相同Web请求或重启时，会重新计算老化时间，超过老化时间仍没有用户请求的文件将被删除。

应用场景



远程办公时，语音、视频等数据流对于网络带宽和时延RTT都有较高的要求。
开启FEC优化功能可以保障关键的视频应用在20%丢包的情况下无卡顿、无花屏，能够为音视频会议的正常召开提供有力保障。



第一步

增加类

基本信息

类名称: 1

规则列表

增加

规则ID	匹配方向	匹配网段	端口号	协议类型	源地址	源端口	目的地址	目的端口	操作
200	Source & Destination	--	--	UDP	1.2.3.4/24	200	1.3.5.6/24	300	删除
100	Source	10.1.1.1/24	1000	UDP	--	--	--	--	删除

自定义WAAS类：配置类并增加规则，也可以使用系统预置的类

第二步

增加策略

基本信息

*策略名称：

类列表

选择

类名称	优化动作	平均抗丢包率(%)	编码块包数	编码超时时间(ms)	解码超时时间(ms)	操作
AFS	By Pass(Class)	--	--	--	--	编辑 删除
CIFS	By Pass(Class)	--	--	--	--	编辑 删除

自定义WAAS策略：配置策略的基本信息，选择类和对应的优化动作

第三步

选择站点

站点名称：

RR1

增加

刷新

批量删除

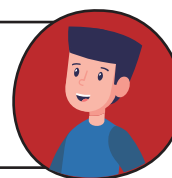
一键重试

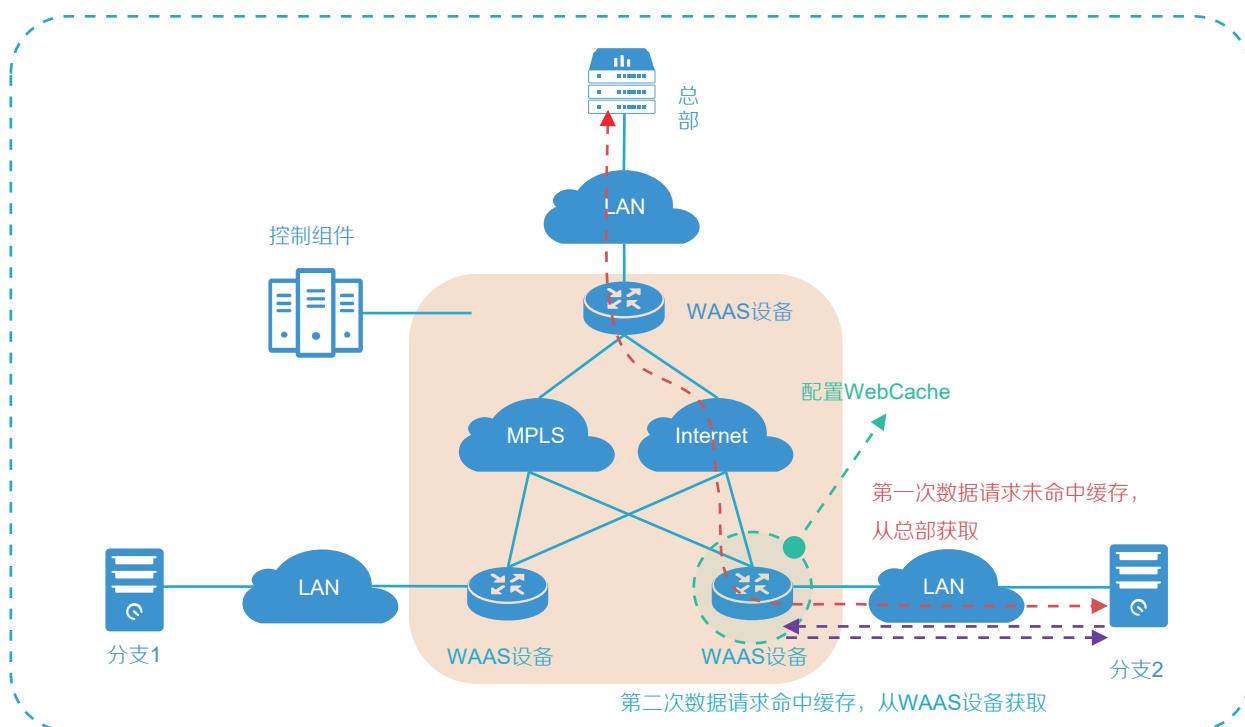
☐	策略名称	设备名称	接口名称	状态
☐	1	172.39.35.50	GigabitEthernet2/0	部署中

绑定WAAS设备：绑定应用策略的站点及设备

企业网内的用户访问相同的技术网站获取最新技术信息。

为了提高Web 网站访问速度、缓解Web 服务器压力，可以在局域网的网关设备上部署WebCache 代理服务功能，在代理服务器上缓存用户访问过的Web 页面。





① 选择设备，开启服务

支持HTTP和HTTPS网站缓存，能够提供安全访问。

增加网站缓存配置

* 站点名称: RR1

* 设备名称: 172.39.35.50

* 机架编号: 0

* 设备槽号: 0

HTTP网站缓存: ☒ 开启 ☐ 关闭

HTTPS网站缓存: ☒ 开启 ☐ 关闭

* 端口号 (HTTP): 8024

* 端口号 (HTTPS): 9528

* 缓存文件类型: doc, gif, jpg, pdf

* 工作目录: flash/webcache

* 缓存上限 (GB): 4

扩展文件类型:

端口映射

端口	协议	服务器端口	操作
63022	HTTP	63022	编辑 删除

② 配置缓存文件类型及工作目录

可选预置文件类型，也支持自定义扩展文件类型。

可指定缓存文件在代理上的存储位置及缓存上限。

③ 增加端口映射

可指定服务器与代理HTTP/HTTPS协议通信的端口映射

方案亮点



简化功能配置

提供图形化的操作界面，轻松实现功能配置。

降低组网成本

优化技术有效节省带宽，降低广域网开销。

优化用户体验

提供更好的音、视频效果和网络访问体验。

提高传输效率

压缩传输数据包，优化传输流。

AD-WAN承载网

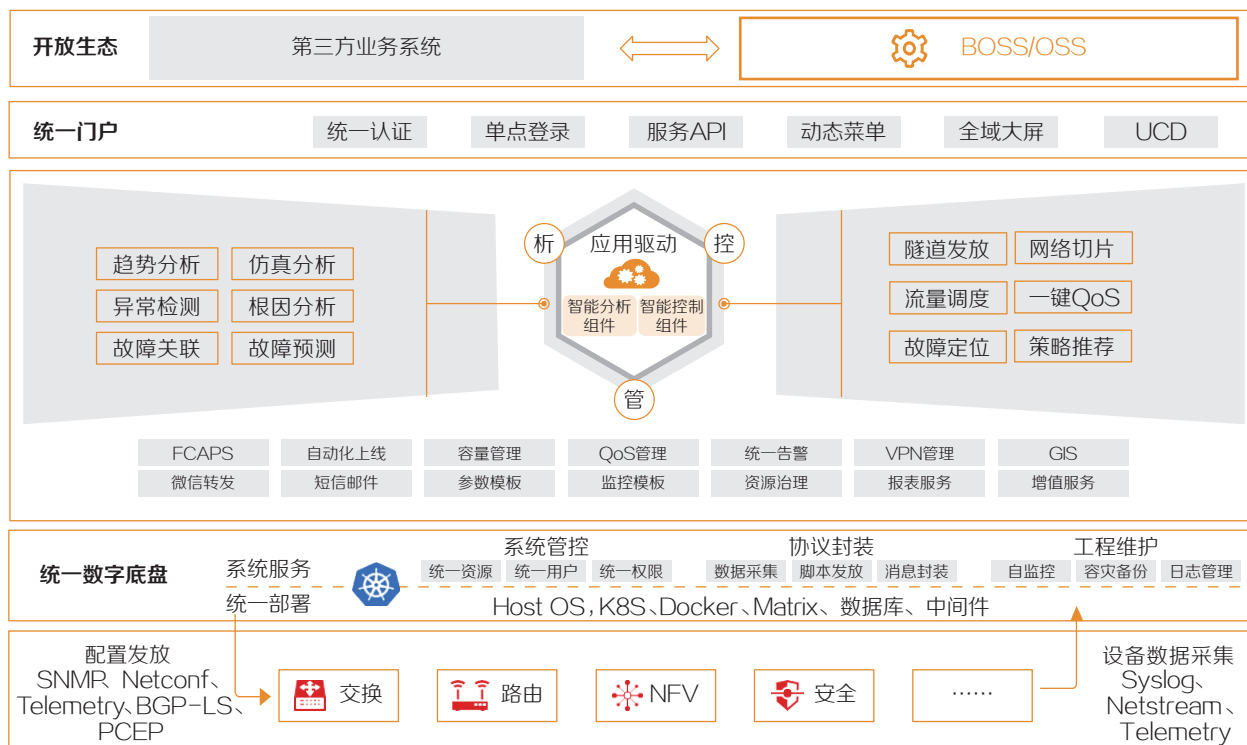
解决方案概述

方案概述

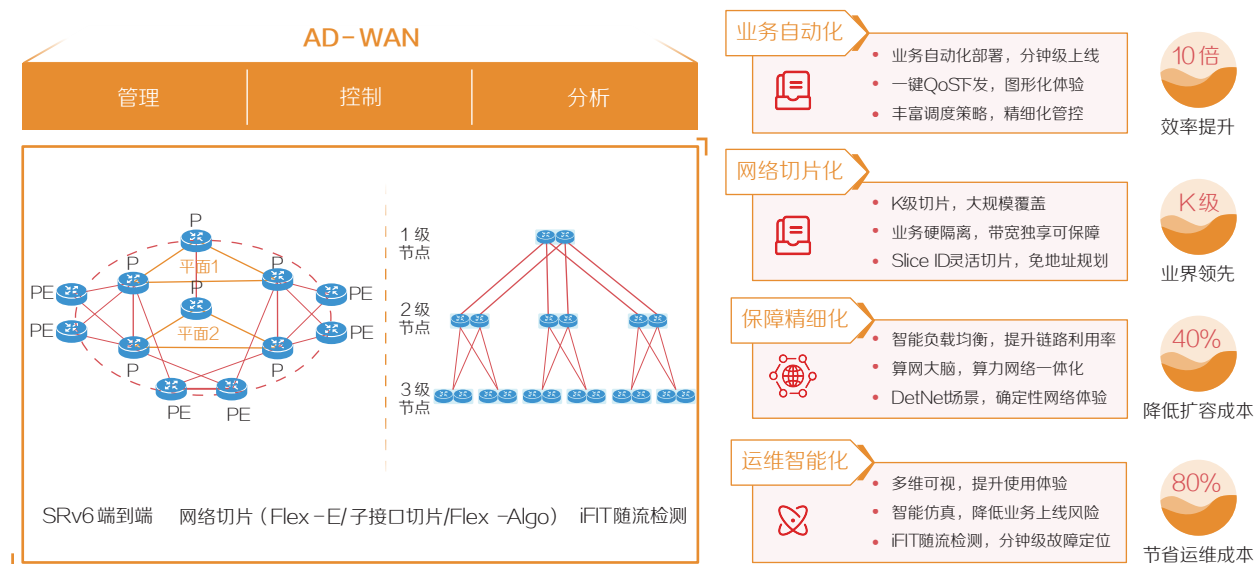
云时代随着网络规模越来越大，业务类型越来越多，新兴业务对承载的广域网络要求越来越高，网络需要在广联接、超宽、自动化、确定性、低时延和安全六个维度全面提升。

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智能选路、EVPN、SR-TE、网络切片、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 with 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



方案核心产品



AD-WAN承载解决方案之

Segment Routing

传统网络面临的问题

传统网络基于设备的**最短路径**转发，导致**网络资源**和**业务需求**难以有效匹配。

“
带宽利用率低
大多维持在**35%**左右
”

“
流量分布不均衡
不同链路之间流量
分布可能相差**60%**
以上
”

”
流量调整周期长
从抓取、分析数据，
到制定策略、下发、
生效，周期至少**3h**
“

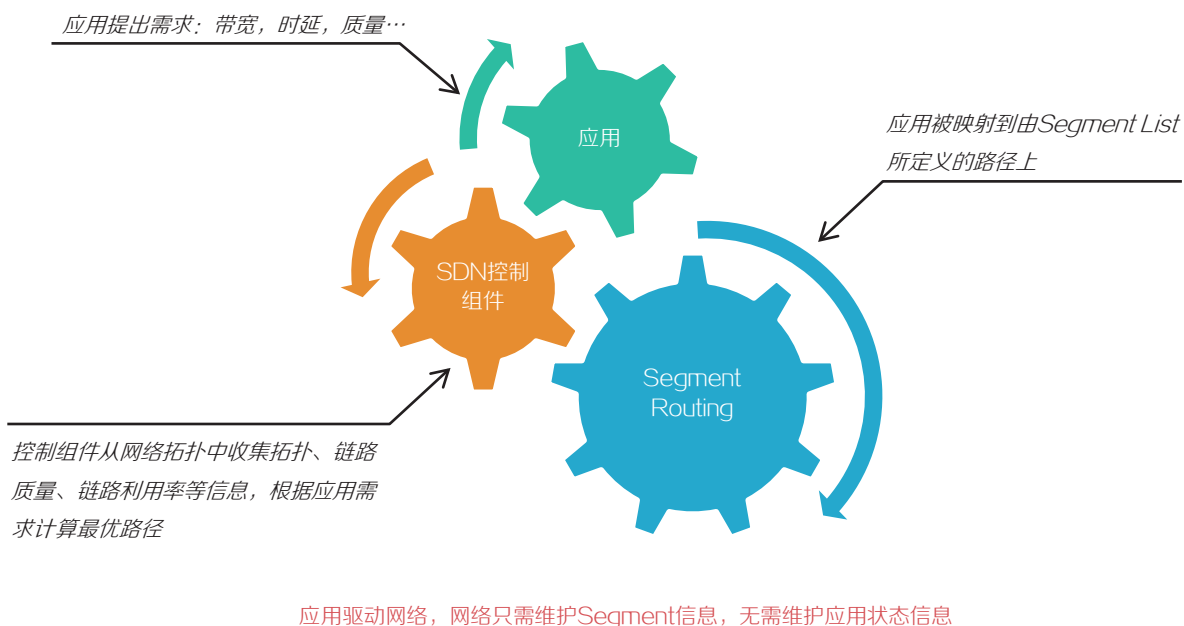
Segment Routing

AD-WAN承载解决方案以应用为中心，构建一个开放、智能、高效、易用的新一代广域网来承载日益丰富的应用流量，实现**应用按需驱动网络、网络动态适应应用**，将**Segment Routing(SR)**和**SDN**结合起来，充分发挥两者的技术优势，为DCI和骨干网提供一个集中、灵活的流量工程手段。

SR简介

Segment Routing (SR, 分段路由) 采用**源路径选择机制**，预先在源节点封装好路径所要经过节点分配的**SID** (Segment Identifier, 段标识)，当报文经过SR节点时，该节点根据报文的SID对报文进行转发。除源节点外，其它节点无需维护路径状态。

Segment Routing能够**使网络更加简化**，并具有良好的**可扩展能力**。



方案介绍

AD-WAN方案在DCI骨干网网络中，为用户提供了以下功能：



网络可视化

收集网络拓扑、链路状态、业务流量等信息，进行整合和分析，对网络和应用进行可视化呈现，并形成TE数据库，为流量调度提供输入。

资源统一管理

根据收集到的网络拓扑，统一为设备和链路分配Segment Routing标签，然后下发给设备。

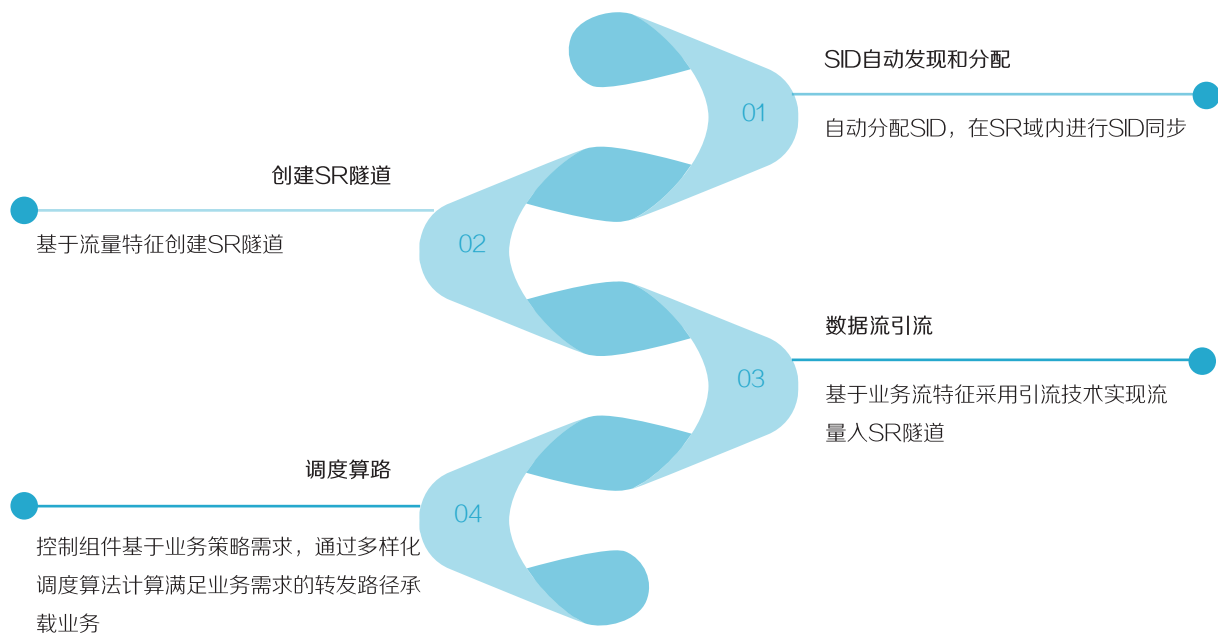
业务配置自动化

在控制组件上部署SR-TE隧道和引流策略后，将下发到网络设备，降低人工配置出错的风险，缩短上线周期。

流量智能调度

通过对全网的专线资源池化，集中调度，根据不同应用的带宽和SLA需求，动态为应用选择最优路径。将控制组件计算的路径信息转化为Segment Routing标签栈，并下发给设备，控制设备报文转发。

1、SR流量调度流程



2、SR调度策略

支持多种路径算法

- Mertic优先
- 时延优先
- 丢包率优先
- 抖动优先
- 可用度优先

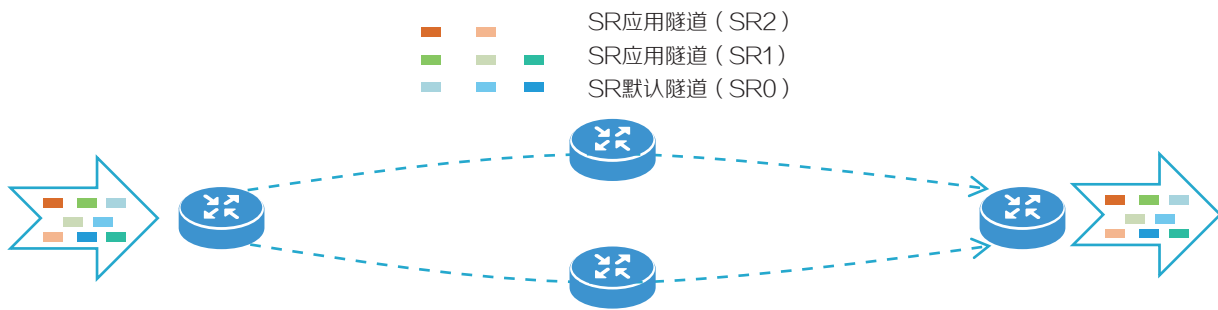
支持全方面策略调整

- 持续调优
- 全局优化
- 局部优化
- 链路策略调整
- 断路调整

支持多种调度因素

- 质量
- 带宽
- 亲和属性
- 优选链路
- 主备同路
- SRLG
- 隧道分离组

3、SR引流方式



- ① 根据应用特征及需求，将应用报文染色为不同的隧道转发类
- ② 将SR隧道设置为路由优选隧道
- ③ 报文转发是通过路由优选出一组路由等价的SR隧道，再通过CBTS/隧道策略/Color/DSCP引流/Flowspec引流引流方式选中具体的转发隧道。

方案亮点

可扩展性

无需维护协议状态，标签数量较少，具备良好的网络可扩展性

高可靠性

提供高可靠的TI-LFA能力，50ms保护倒换

可兼容性

支持传统网络和SDN网络，兼容现有设备，保障现有网络向SDN网络平滑演进

简化网络

使用控制组件或者IGP集中算路、分发标签，不再需要RSVP-TE、LDP等隧道协议

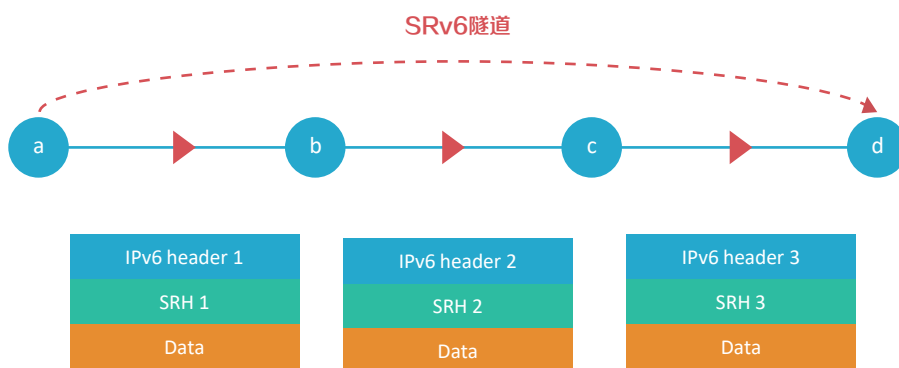


AD-WAN承载解决方案之

SRv6概述

SRv6简介

SRv6 (Segment Routing IPv6) 是指基于IPv6转发平面实现SR。SRv6通过在IPv6报文中插入一个SRH (Segment Routing Header)，在SRH中压入Segment List信息，指定该报文转发的IPv6显式路径，引导报文转发。



技术亮点



协议简单

SRv6在SR基础上进一步简化协议，完全去掉了MPLS数据平面，采用纯IPv6网络。

可靠性高

支持TI-LFA、尾节点保护、SBFD for SRv6，能为SRv6提供链路及节点的多重保护。

扩展性强

128 Bit超大地址空间，可支持网络编程。

无缝升级

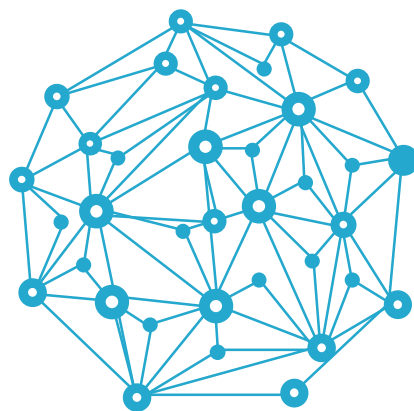
SRv6前向兼容IPv6，支持IPv6向SRv6存量演进，无需一次性全网升级，可通过增量升级的方式最大限度保护用户的已有资产，使网络平滑升级至SRv6。

负载分担

协议天然支持ECMP、UCMP，多路径部署更灵活，可实现负载分担。

灵活调度

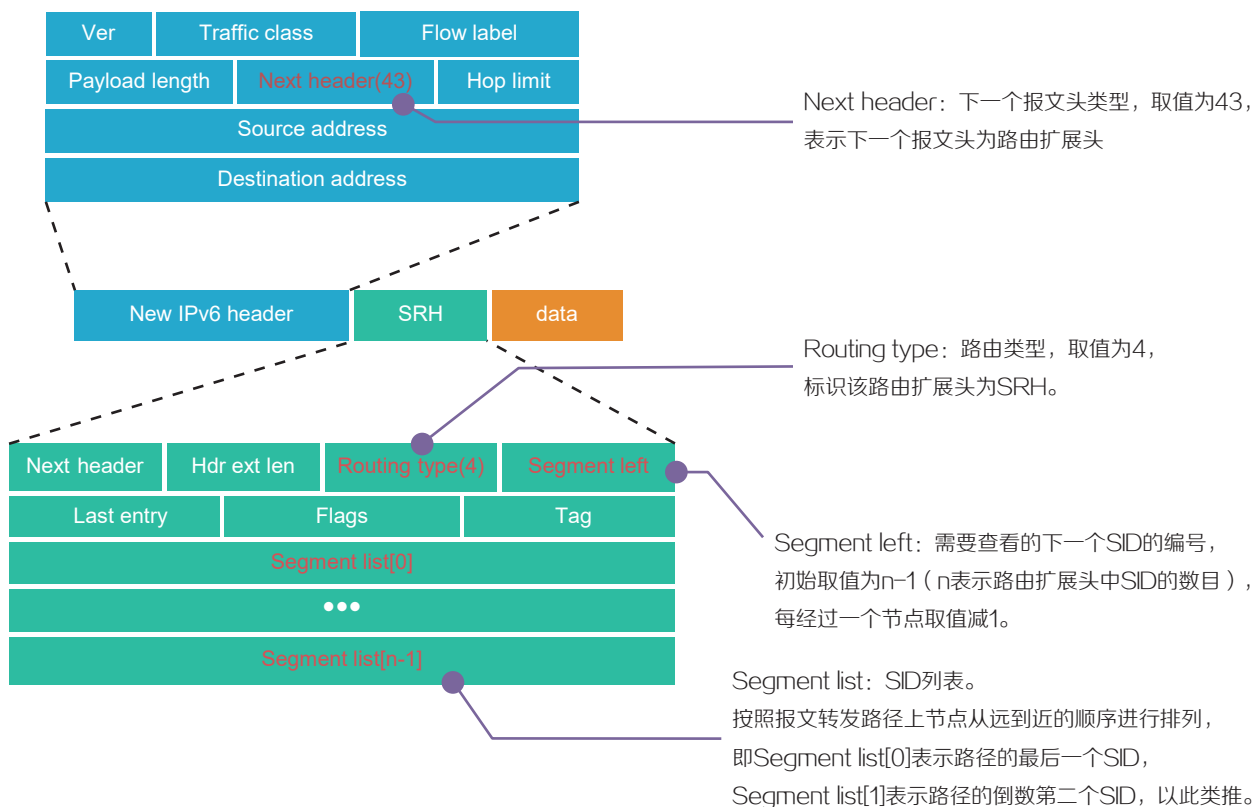
采用源路由技术，结合SDN可实现精细化的流分类和SLA差异化业务保障。



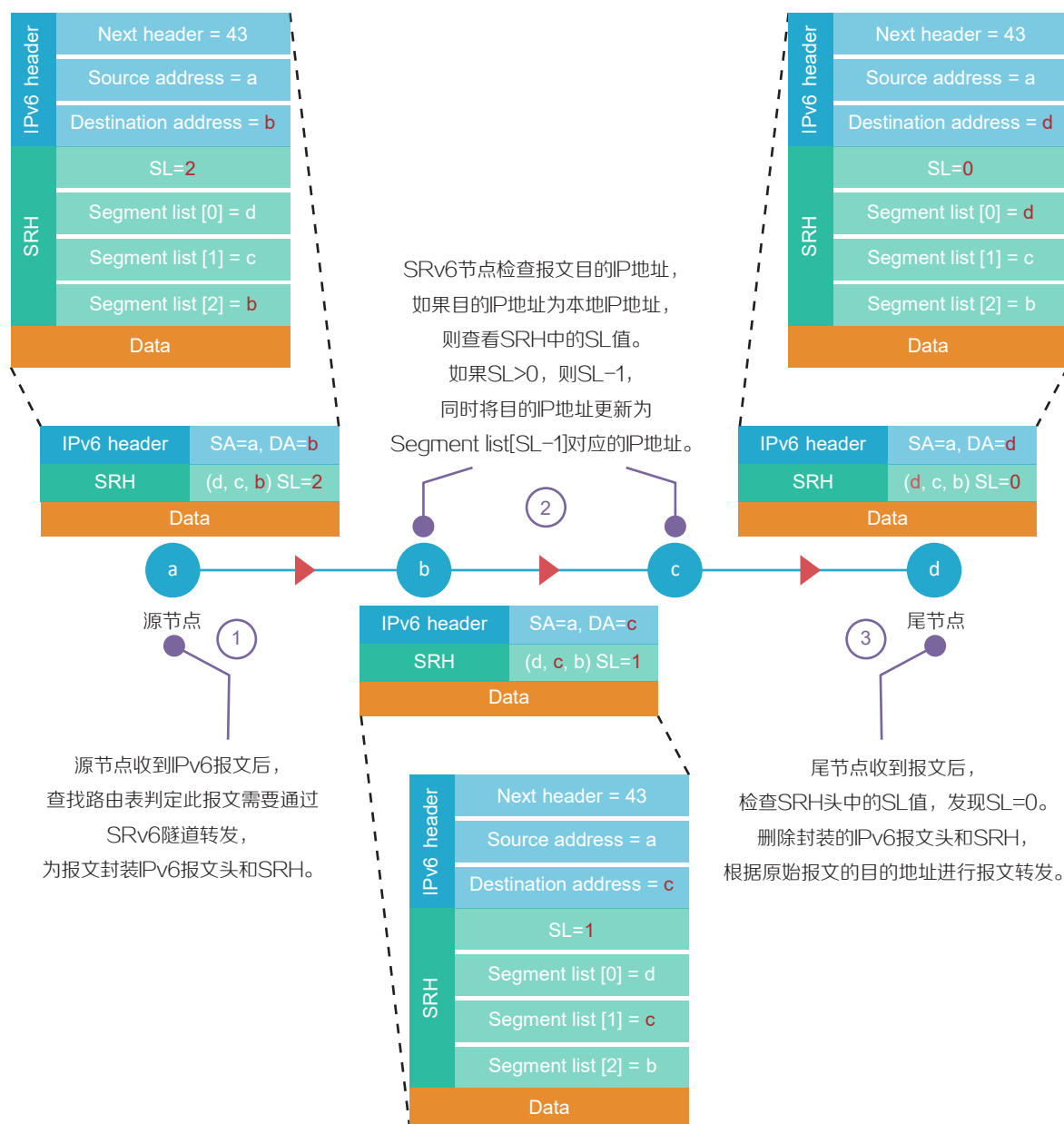
技术原理

1、报文封装

SRv6报文封装格式从外到内依次为IPv6头、SRH、三层原始数据，其中SRH是一种IPv6路由扩展头。



2、工作机制



隧道与引流技术

1、隧道技术

SRv6 BE (Best Effort)

and

SRv6 TE (Traffic Engineering)

- 按照最短路径原则进行路径计算。
- 提供VPN承载和可靠性服务。

- 按照候选路径的显式路径进行转发，根据丰富的SLA策略进行路径计算。
- 提供路径控制和调优、差异化SLA保障服务。

2、引流技术

引流技术是指通过匹配一定的报文特征或选路规则，引导特定报文流量转发。

SRv6 TE Policy支持的引流技术：

引流方式	引流规则
基于BSID引流	如果设备接收到的报文目的IPv6地址为某个SRv6 TE Policy的BSID，则通过该SRv6 TE Policy转发该报文
基于Color引流	基于Color和Endpoint将BGP路由迭代到SRv6 TE Policy。当设备收到匹配该BGP路由的报文时，会通过SRv6 TE Policy转发该报文
基于DSCP引流	根据报文的DSCP值查找与其关联的Color属性，再通过Color属性匹配到SRv6 TE Policy。这样，携带指定DSCP的报文可通过指定SRv6 TE Policy转发
基于隧道策略引流	在L2VPN和L3VPN组网环境中，通过部署隧道策略，将SRv6 TE Policy作为公网隧道来转发私网报文
基于CBTS引流	根据流分类匹配不同优先级，并映射到不同的隧道转发类值，以此来选择对应的SRv6 TE Policy隧道进行转发。没有对应的转发类值时，从没有配置转发类的隧道进行转发



SRv6 BE隧道为协议自动创建，不涉及引流或隧道选择技术。

技术对比

Segment Routing数据平面分为两种，MPLS和IPv6。

在MPLS数据平面中称为**SR-MPLS**，在IPv6数据平面中称为**SRv6**。

在AD-WAN方案中两种数据平面流程、功能基本一致，主要区分如下：

比较项	SR-MPLS	SRv6
数据面	IP + MPLS	IPv6
单标签长度	4字节	16字节
数据面可编程能力	SID长度限制 数据面不好扩展	128 Bit可编程空间 易于扩展的IPv6扩展头
路由聚合能力	无	有
和传统网络共存	无	有
端到端打通能力	SR-TE Seamless SR	简单 只需要端到端路由打通即可
网络可靠性	TE和VPN保护 依赖端到端BFD	任意点的本地50ms快速保护 不依赖端到端BFD
统一的Underlay/Overlay	否	是
转发性能	高	标签栈开销大，转发效率低
运维复杂度	传统运维经验可继承	IPv4→IPv6，路由协议变更（OSPFv3/IS-ISv6/BGP4+） 对运维人员要求提高
广域网线路要求	对接口MTU影响小 绝大部分场景下可不变更 MTU配置	接口MTU要求高 大概率要求变更广域网接口MTU配置

从主流技术同步演进的角度考虑，MPLS L3VPN over SR-TE向EVPN L2/L3 over SRv6演进，数据平面与控制平面分离，演进更加平滑。

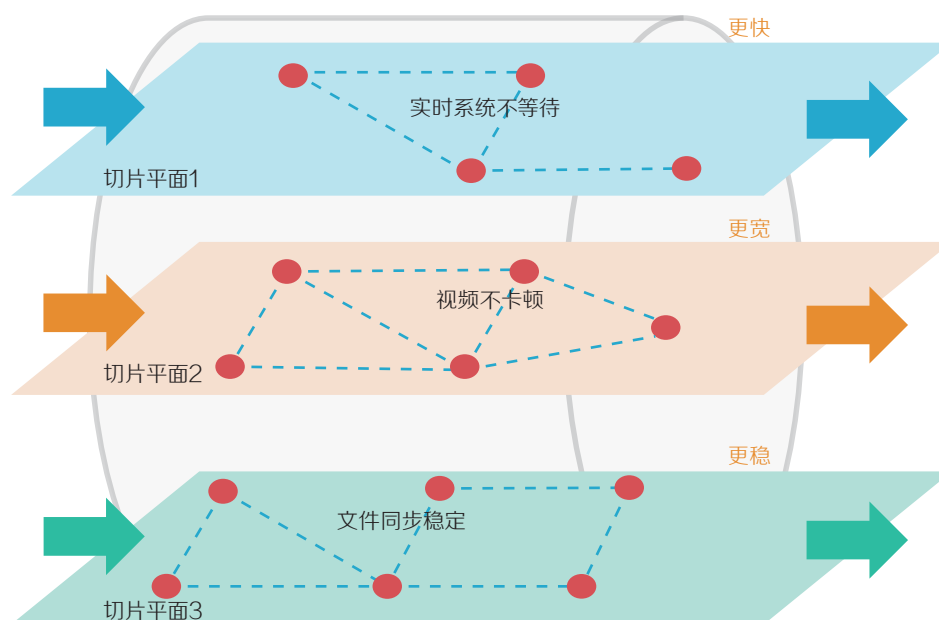
AD-WAN承载解决方案之

网络切片之资源隔离

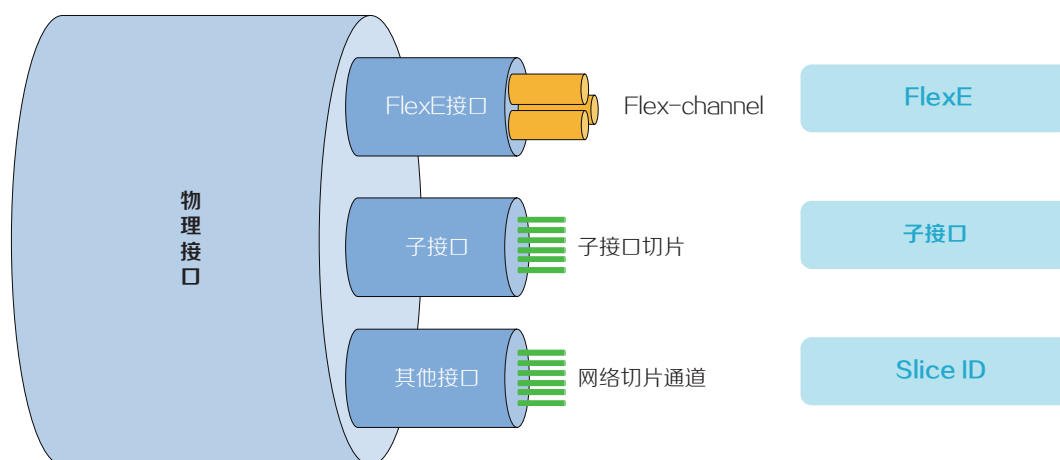


简介

网络切片是通过在一张物理网络上划分出多个虚拟的“专用”逻辑网络，来提供相互隔离、端到端和按需定制的服务。



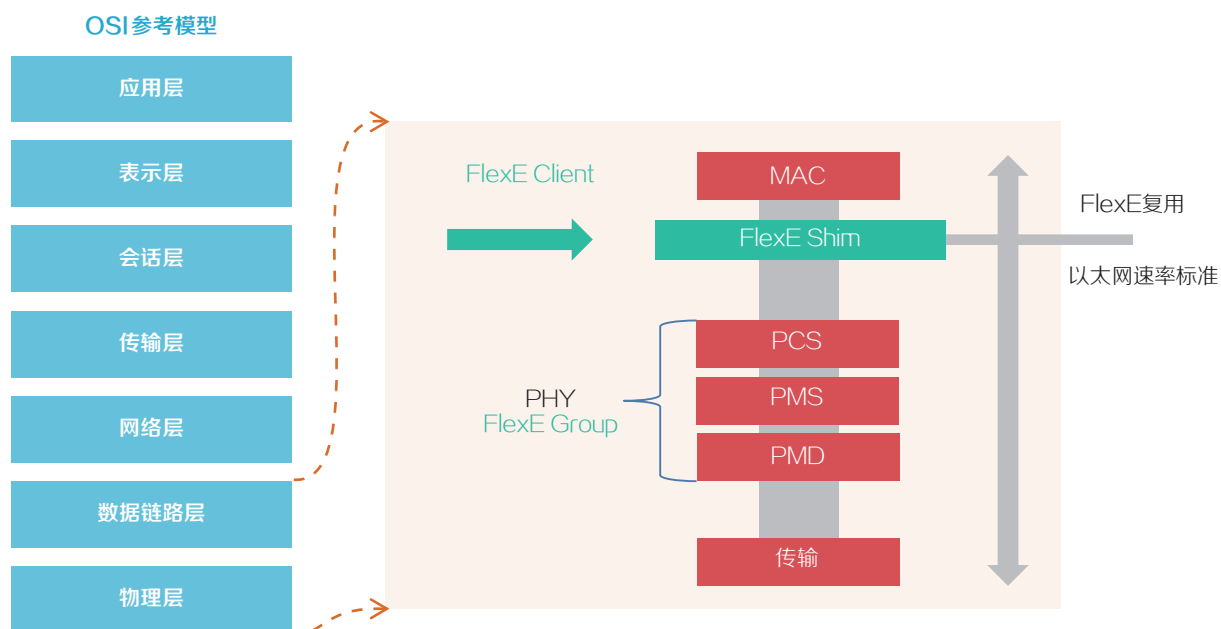
网络切片有哪些关键技术呢？



对比项	FlexE	子接口	Slice ID
时延保障效果	单跳时延最大增加10us	单跳时延最大增加100us	/
切片数量	百级	千级	千级
粒度	5Gbit/s	1Mbit/s	1kbps
适用场景	行业切片	行业切片、企业专网切片 (预部署)	企业点到点切片、企业专网切片 (随用随切)

FlexE技术

FlexE (Flex Ethernet, 灵活以太网) 技术是在Ethernet技术基础上, 为满足高速传送、灵活带宽设置等需求, 通过时隙交叉技术和端口捆绑技术实现的低成本、可动态配置的电信级接口技术。引入了全新的FlexE Shim层, 实现MAC (介质访问控制子层, 属于数据链路层) 和PHY (物理层) 的解耦。上层和下层的数据流速率, 不再强制绑定。



1、FlexE 功能



捆绑

多路PHY一起工作，支持更高速率。



子速率

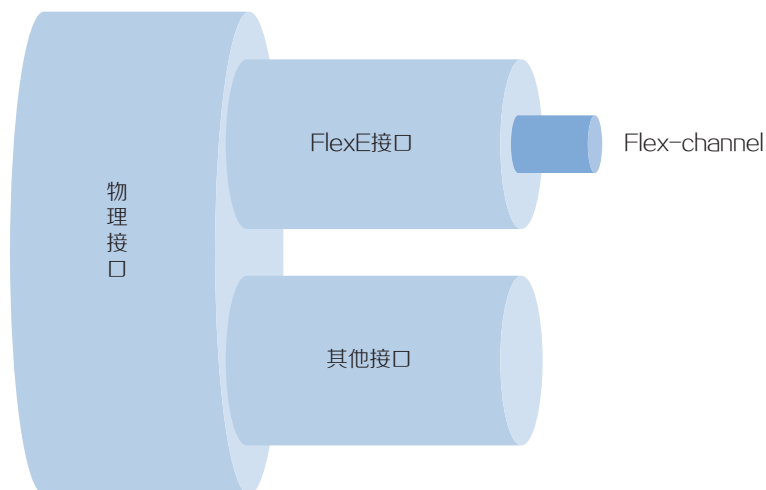
单一低速率MAC数据流共享一路或者多路PHY。



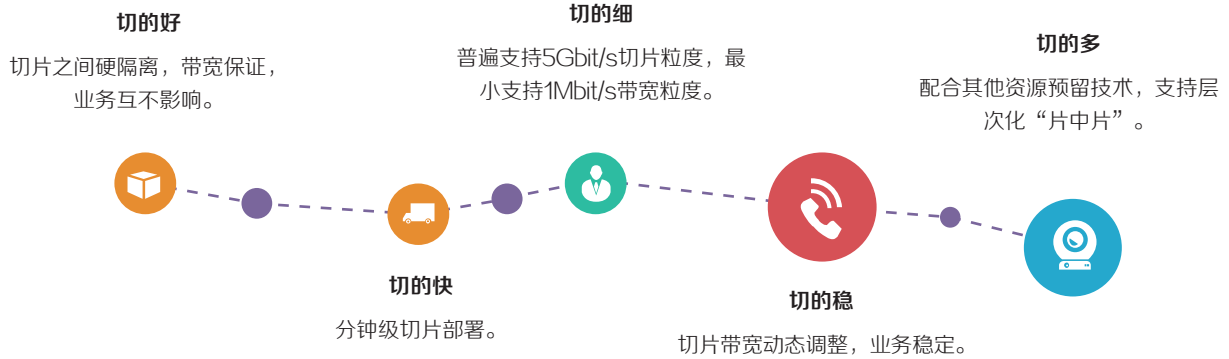
通道化

多路低速率MAC数据流共享一路或者多路PHY。

FlexE 提供了一种灵活、细粒度的切片方式——Flex-channel（灵活子通道），通过层次化的调度，实现资源灵活、精细化的管理。

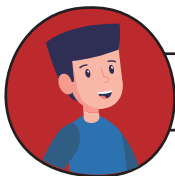
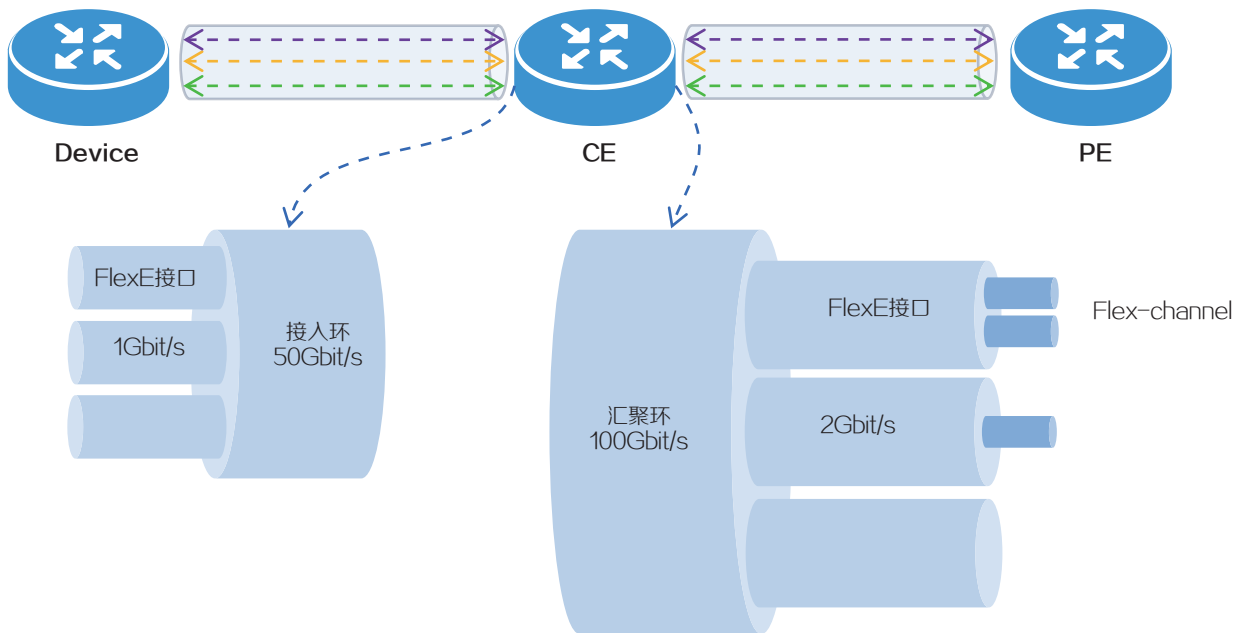


2、FlexE 技术特点

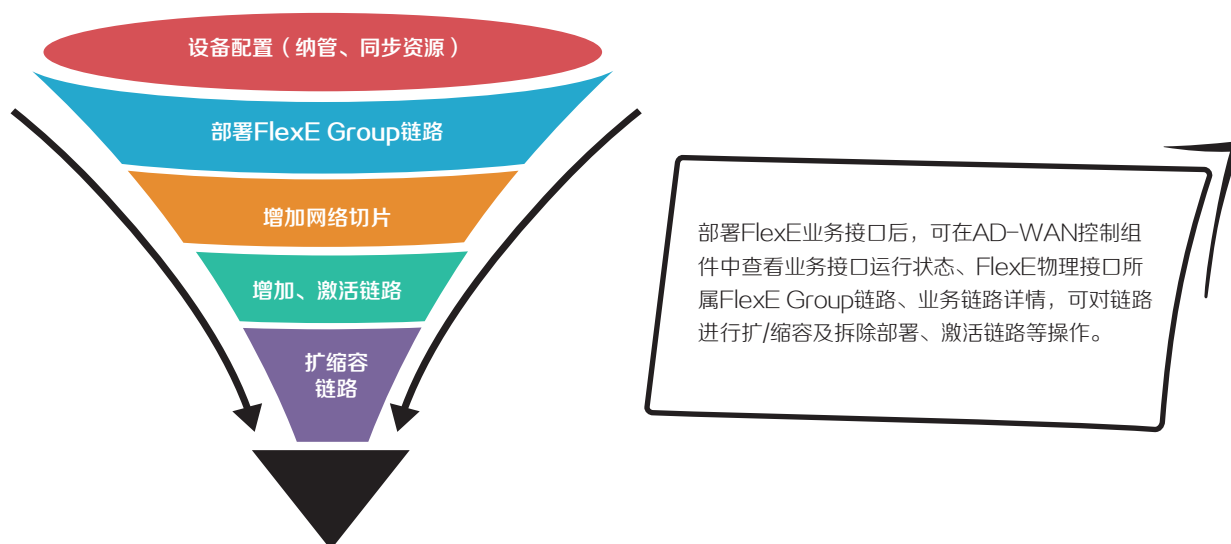


典型应用场景

为保障某个垂直行业对**资源隔离**和**超低时延**的需求。在接入环50Gbit/s带宽、汇聚环100Gbit/s带宽的网络中，采用FlexE接口预留5G带宽，实现业务硬隔离。

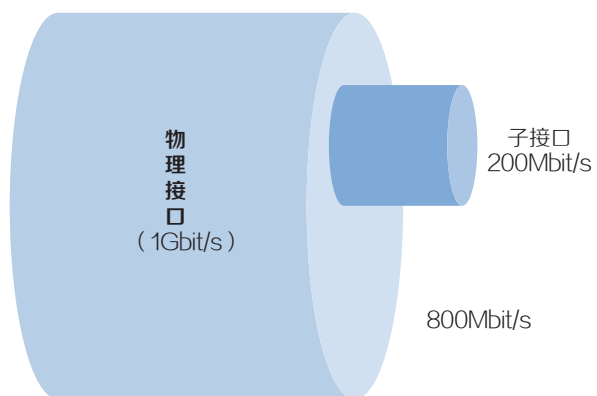


AD-WAN控制组件如何运用FlexE技术？



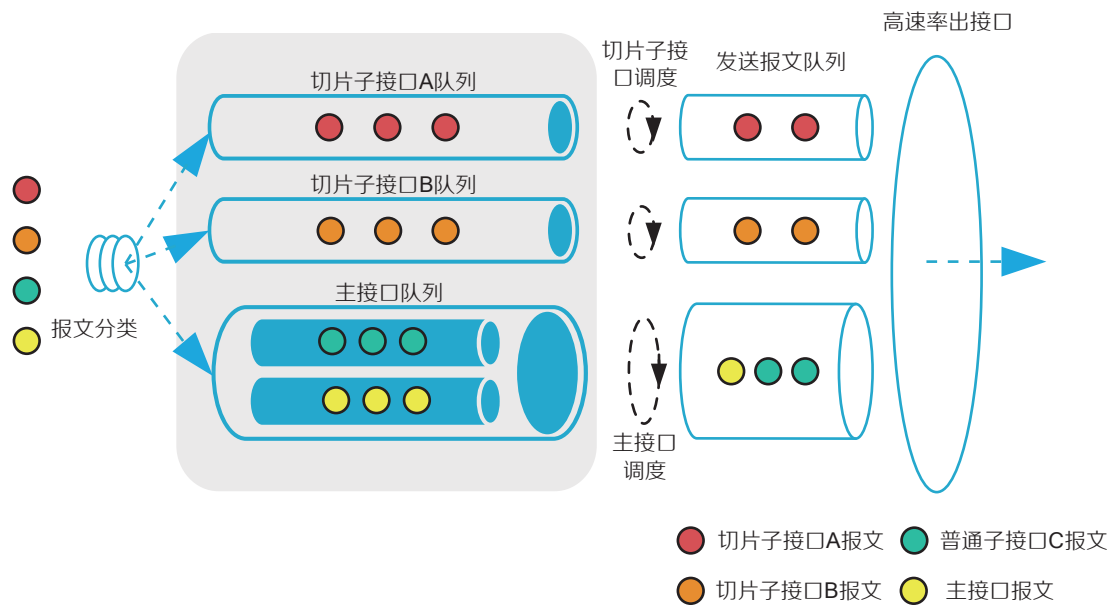
子接口切片技术

子接口切片是一种小粒度的网络切片技术。通过在高速率端口上创建子接口，并为某些子接口配置子接口切片带宽，实现子接口切片功能。子接口独占带宽，不能被抢占，能够为业务提供资源预留，保障业务带宽。



例如，当一个1Gbit/s端口配置了200Mbit/s子接口后，主接口带宽扣减为800Mbit/s。带宽扣减过程在子接口使能过程中自动实现。

1、工作机制



设备为切片子接口A和B各分配一个独立于主接口的流量管理队列，独立进行QoS调度。切片子接口独享带宽，主接口和其他子接口不能抢占切片子接口的带宽。每个切片子接口均可认为是一个独立接口。

普通子接口的报文和主接口报文统一进入主接口队列进行调度，共享接口的剩余带宽（主接口剩余带宽=主接口总带宽-所有切片子接口带宽的总和）。

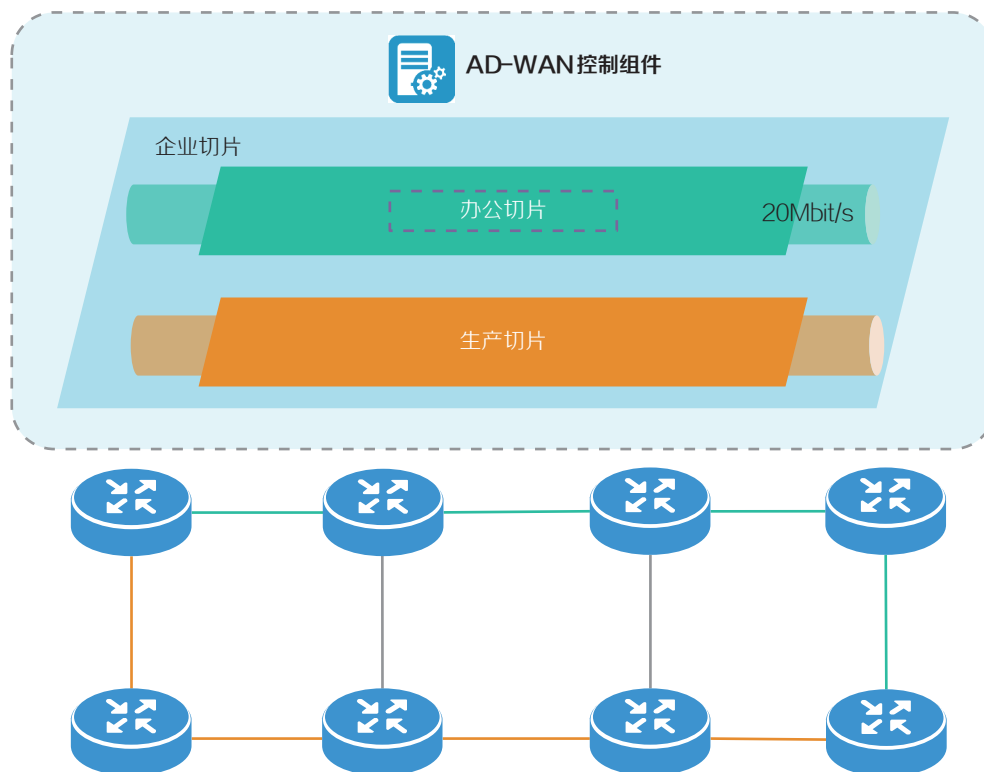


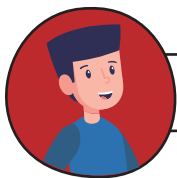
2、子接口切片技术特点



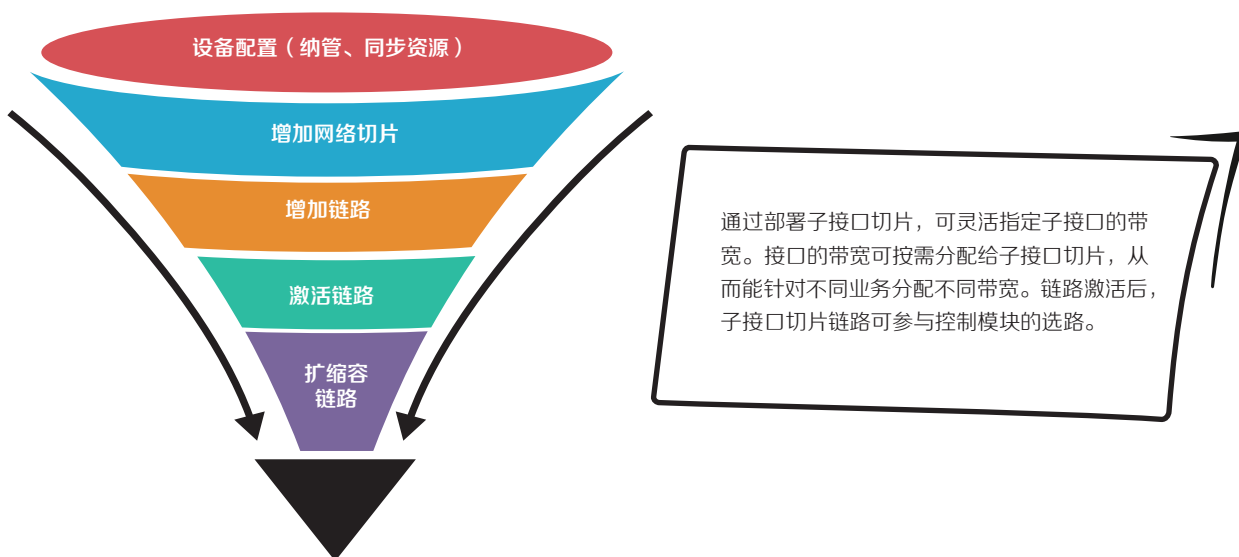
典型应用场景

当前企业切片中已有生产切片，需新规划办公切片。根据业务的时延和带宽等需求，在企业切片中为办公切片配置切片子接口，保证生产和办公之间的业务流量相互隔离。





AD-WAN控制组件如何运用子接口切片技术？

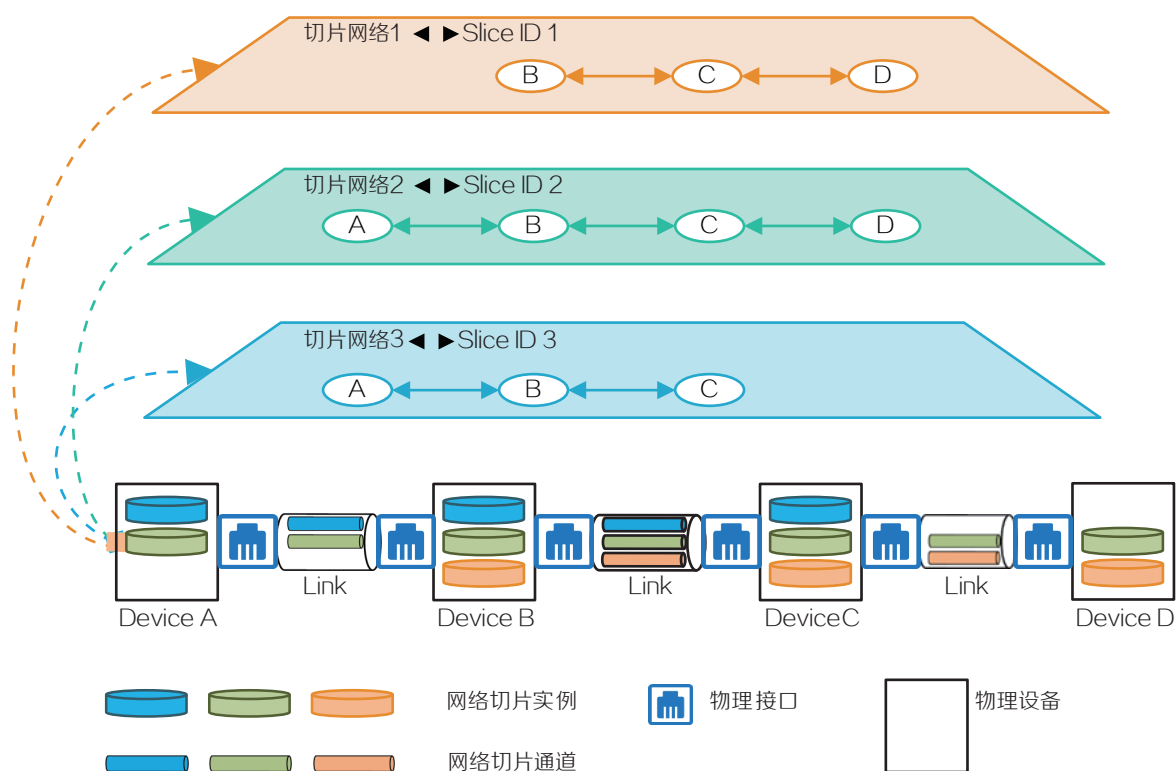


Slice ID技术

基于Slice ID的网络切片是一种应用在SRv6组网场景中的网络切片技术方案，它通过全局唯一的Slice ID标识虚拟的逻辑网络，以实现网络切片的功能。

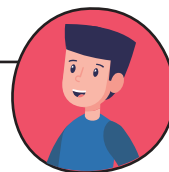
通过在SRv6源节点，为报文头增加IPv6逐跳扩展头（Hop-by-Hop Extension Header），且在IPv6逐跳扩展头中添加网络切片实例ID（Slice Instance ID）信息，中间设备根据网络切片实例ID查找资源出口。

1、实现方法



11

- ① 规划Slice ID: 根据业务需求, 为不同切片网络分配不同的Slice ID。
- ② 根据Slice ID将物理设备映射到虚拟切片网络: 在物理设备上创建网络切片实例, 网络切片实例的标识为Slice ID。这样, 就可以将该物理设备映射到Slice ID对应的虚拟切片网络。
- ③ 根据Slice ID将物理接口映射到虚拟切片网络: 在物理接口上开启切片功能并创建网络切片通道, 网络切片通道的标识是Slice ID。这样, 就可以将该物理接口映射到Slice ID对应的虚拟切片网络。同一物理接口下的不同网络切片通道具有独立的队列调度机制和带宽保障机制, 因此, 不同网络切片通道中的业务转发互不影响。
- ④ 具有相同Slice ID的网络切片实例和网络切片通道构成一个虚拟切片网络。



2、Slice ID技术特点

配置和实现简单

配置过程简单，通过物理网络的IP地址和切片网络的Slice ID就可以实现不同切片网络报文转发的隔离。所有切片网络仅需一套IP地址，避免IP地址浪费。

带宽可精细控制

物理接口下的网络切片通道的带宽值较小且可精细控制，相较于FlexE技术1Gbps的带宽粒度，产品支持的网络切片通道带宽最小值为1Mbps。

支持的接口类型丰富

三层以太网接口、三层聚合接口，三层聚合子接口，三层子接口和FlexE接口均支持网络切片通道。

支持的切片数量多

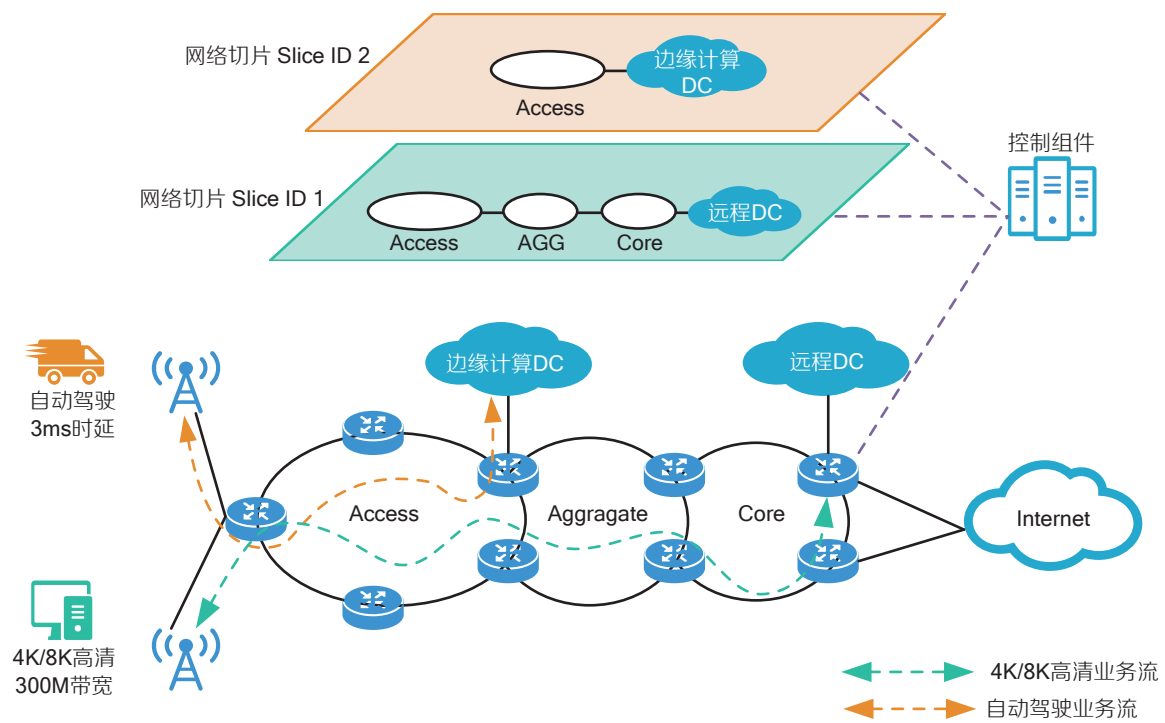
目前设备最大可支持6000个网络切片，充分满足现有业务需求。



典型应用场景

在运营商承载网络中，存在自动驾驶业务和4K/8K高清IPTV业务。采用基于Slice ID的网络切片技术将物理网络划分两个网络切片，分别承载这两类业务，为不同业务提供不同的QoS质量保证：

- 为切片网络Slice ID 1分配足够大的带宽，在该切片网络上承载4K/8K高清IPTV业务，以便为4K/8K高清IPTV业务提供带宽保障。
- 将边缘计算数据中心划分到切片网络Slice ID 2，直连接入环。切片网络Slice ID 2承载自动驾驶业务，通过边缘计算DC为自动驾驶业务提供超低时延保证。



AD-WAN承载解决方案之 一键巡检

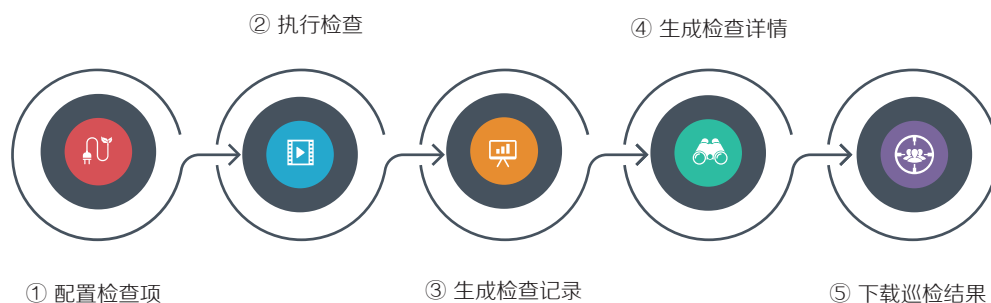
简介

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。

一键巡检功能通过将网络状态、管理状态和业务状态的巡检内容进行归纳、整理，以可视化的界面展示巡检内容和巡检结果，以此提高整体运维效率。

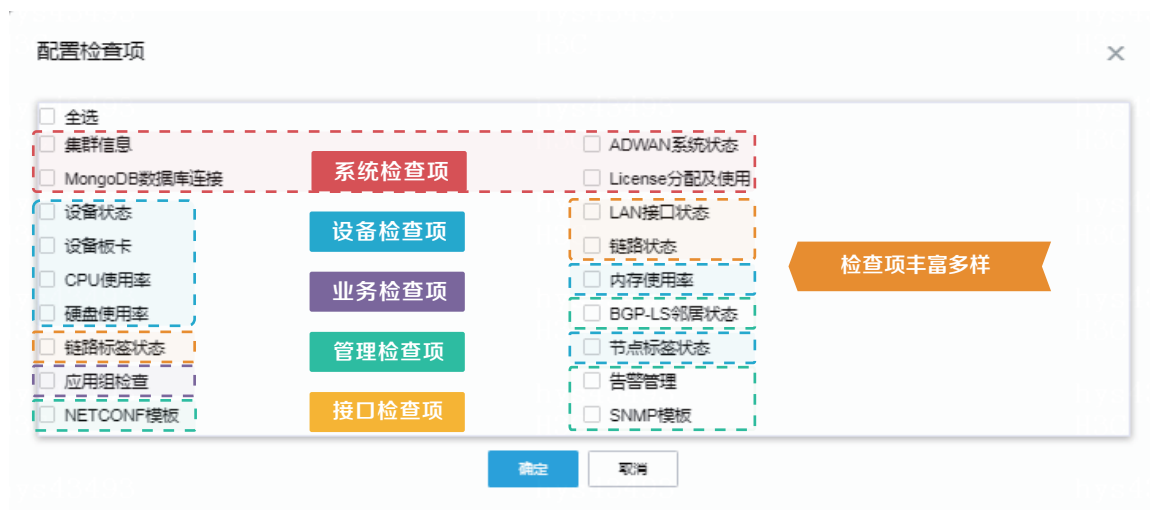


巡检流程



1、配置检查项

对系统进行一键巡检前请先按需配置检查项，系统将按照检查项对系统、设备、业务、管理、接口进行检查。



2、执行检查

根据配置的检查项及巡检方式执行检查。





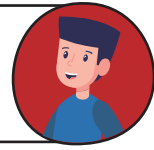
举个栗子



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“手动巡检”方式。



当用户需定时排查系统中的异常情况时，可选择“自动巡检”方式。配置自动巡检策略，时间间隔选择“1”天，固定检查时间为“7”点，则用户每天可在固定时间段查询到新的巡检记录。



自动巡检策略

是否开启自动巡检

是

否

自动巡检策略

* 时间间隔单位: 天

* 时间间隔: 1

* 巡检时间: 07:00:00

确定

重置

配置校验

配置审计

数据导出

一键巡检

容量管理

刷新

配置检查项

执行检查

自动巡检

检查日期

检查项

风险

2022-06-10 07:00:01

18

2

自动巡检记录

3、巡查结果

执行检查后，系统将生成巡检记录。在检查结果页面可查看指定巡检记录的详细检查结果。针对存在异常的检查项，系统会给出相应处理意见。

01 巡检记录

02 巡检详情



系统支持下载巡检报告，报告为Excel格式。

检查结果

执行检查项：18个，存在异常：0个，存在风险：2个，执行失败：0个，检查结果正常：16个。

存在风险的检查项。报告中展示执行结果及风险处理意见。

级别	检查项	检查项介绍	执行结果	处理意见
风险	设备状态	检查当前纳管的设备状态	1 设备状态异常	请进入物理网络中的设备管理页面检查当前系统中设备的状态
风险	告警管理	检查当前系统中的告警信息	存在未恢复的告警信息	请进入告警管理页面排查告警原因并解决
正常	集群信息	检查当前系统中集群信息	正常	
正常	ADWAN系统状态	检查当前ADWAN系统是否处于逃生状态	正常	
正常	MongoDB数据库连接	检查当前ADWAN上MongoDB连接状态	正常	
正常	License分配及使用	检查当前系统License使用情况	正常	
正常	LAN接口状态	检查当前纳管设备的LAN接口状态	正常	
正常	设备板卡	检查当前纳管设备的板卡状态	正常	
正常	链路状态	检查当前系统中链路的状态	正常	
正常	CPU使用率	检查当前系统各个节点的CPU使用率是否超过80%	正常	
正常	内存使用率	检查当前系统各个节点的内存使用率是否超过80%	正常	
正常	硬盘使用率	检查当前系统各个节点的硬盘使用率是否超过90%	正常	
正常	BGP-LS邻居状态	检查当前系统中BGP-LS邻居状态	正常	
正常	链路标签状态	检查当前系统中的链路标签状态	正常	
正常	节点标签状态	检查当前系统中的节点标签状态	正常	
正常	应用组检查	检查应用组状态	正常	
正常	NETCONF模板	检查NETCONF模板是否已配置	正常	
正常	SNMP模板	检查SNMP模板是否已配置	正常	

无异常检查项

方案亮点



一键启动

操作简单，用户可根据需要选择所需的巡检方式。

快速检查

无需“等待”，立即执行检查，生成检查记录。

清晰报告

检查结果清晰可视。

AD-WAN承载解决方案之

容量管理

简介

在传统网络中，网络管理人员（后续简称网管人员）的直接操作对象是设备。设备配置的变化、新业务的开通，都需要网管人员介入操作，因此网管人员对设备上的资源占用情况具有很强的掌控能力。在网络设备上

进行配置操作时，若设备上资源不足，网管人员一般可通过设备反馈的信息，及时进行处理。在SDN场景中，网管人员的直接操作对象变成SDN控制组件。虽然简化了网管人员的工作，但从另一个角度看，也会导致网管人员对网络设备的掌控力变低：控制组件对网络设备下发的配置内容、时机，不能精准掌握，网管人员也无法再对设备的资源状态“了如指掌”。

容量管理通过对设备的FIB资源、ACL资源进行监控，保障设备各项资源容量能够合理满足业务诉求，保障业务发放成功率。

主要功能



90%

以可视化的界面展示设备ACL资源和FIB资源的容量信息。

设备容量可视

设备及板卡容量信息





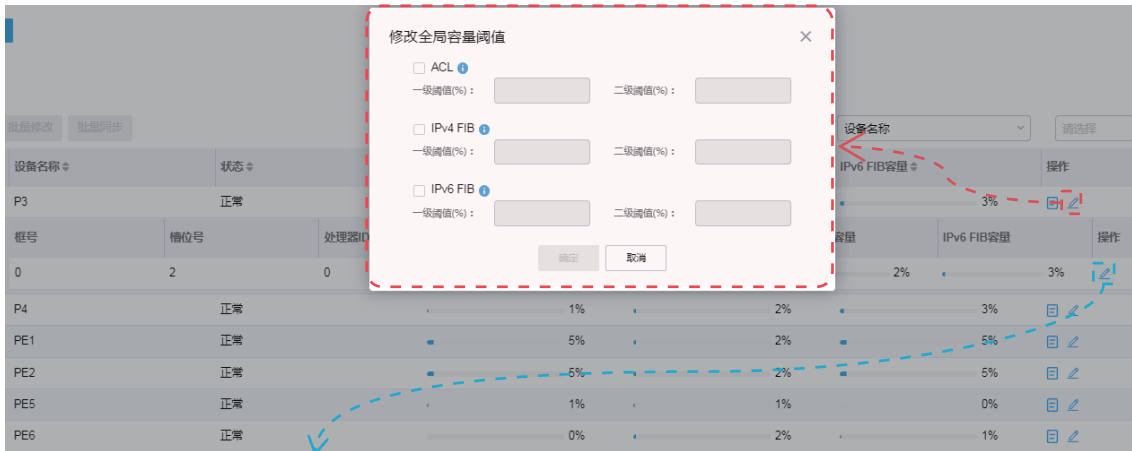
- ①在容量管理列表可查看所有设备的资源容量信息。
- ②在容量详情列表可查看设备资源表的详细信息。



60%

剩余容量阈值

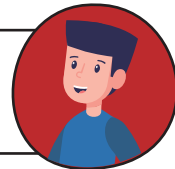
为保障业务正确下发，可对设备剩余可用容量设置阈值，实现合理规划容量的效果。



当剩余容量小于一级阈值时将产生**次要告警**；
小于二级阈值时产生**重要告警**。



通过设置阈值，帮助用户合理安排不同资源的容量使用。可对整个设备的容量信息进行阈值设置，也可对单个板卡进行容量阈值设置。



30%

超阈值下发

用户可通过“超阈值下发”选择当设备的资源超出阈值时是否下发配置。

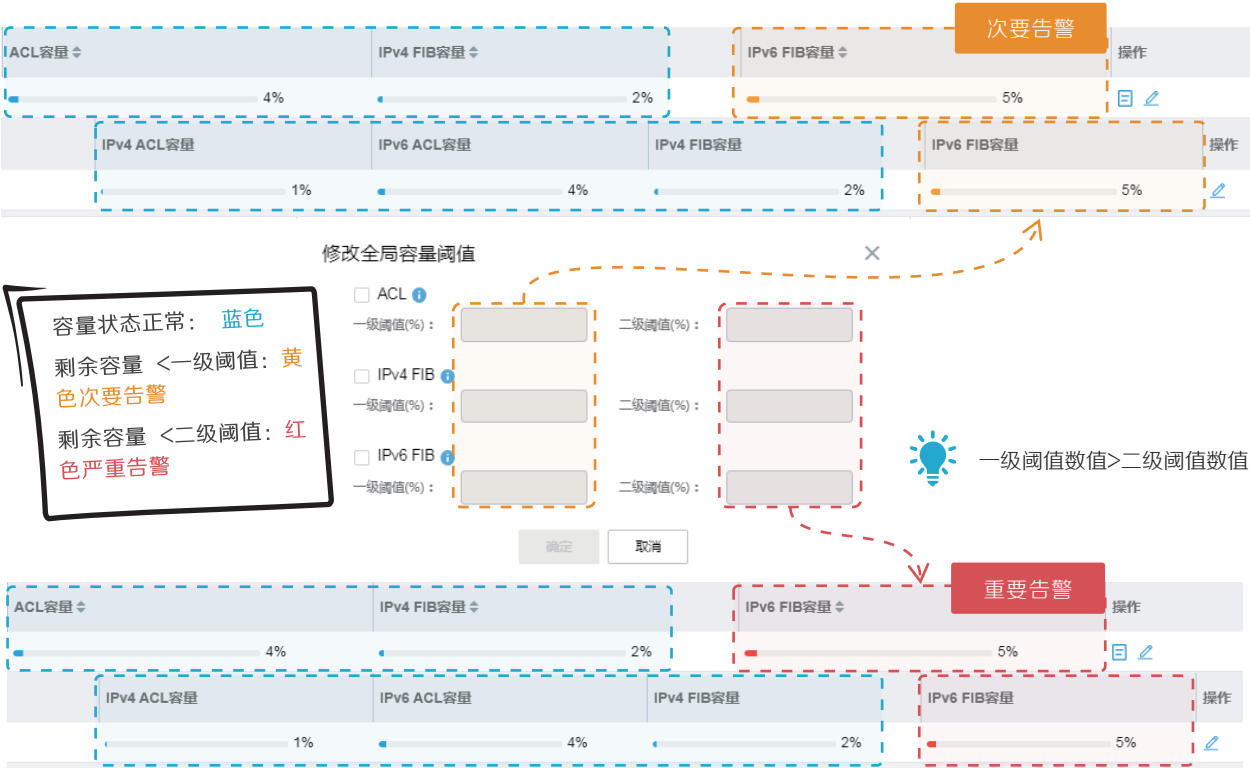
超阈值下发配置

是

否

确定

1. 当设备FIB 表剩余资源超出二级阈值或内存剩余资源超出一级阈值时，是否向超出阈值资源的设备下发配置。
2. 当ACL表剩余资源超出二级阈值时，是否向超出阈值资源的设备下发ACL资源相关的配置。



方案亮点

合理规划
推动资源合理分配，将客户基础设施投资回报率最大化。

容量可视
容量负荷情况可视化，引导用户合理部署各项业务。

业务发放保障
发放前预先判定容量满足度，保障业务发放成功率。

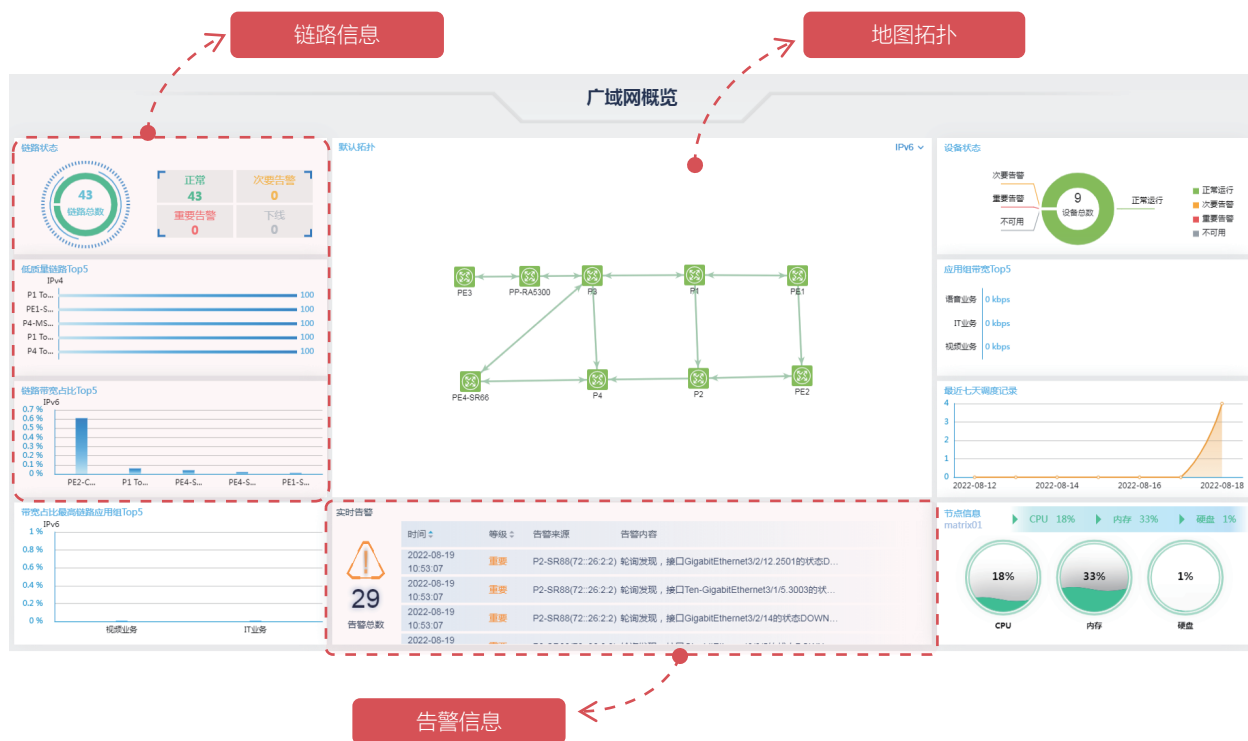
AD-WAN承载解决方案之 多维可视

简介

AD-WAN承载网通过SNMP/NETCONF/Telemetry/Netstream获取数据，支持从业务、网络运行状况等维度呈现图形化操作界面及数据展示，简化用户网络运维难度。

主要功能

AD-WAN承载解决方案提供大屏可视功能，展示内容包括链路状态、链路带宽及质量、设备状态、应用带宽及流量、节点信息、实时告警、地图拓扑等。用户可轻松掌握当前网络及资源的实时状态，支持按需定制大屏可视化呈现的形式。



1、网络可视

网络可视提供设备、链路和网络拓扑的可视化管理。



拓扑可视

拓扑发现

拓扑管理



设备可视

设备状态

设备静态信息

设备动态信息及历史报表



链路可视

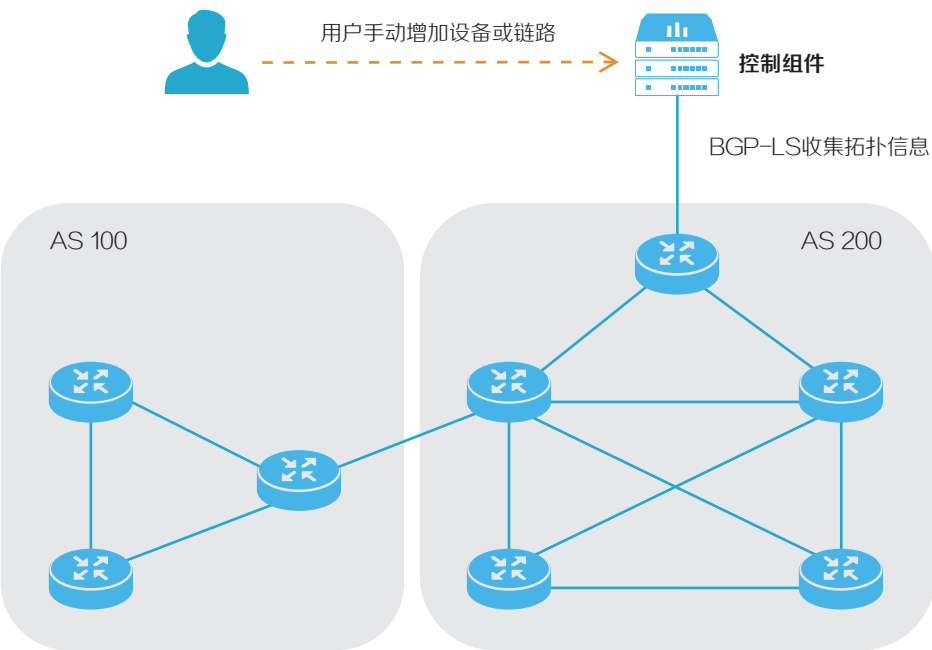
链路状态

链路静态信息

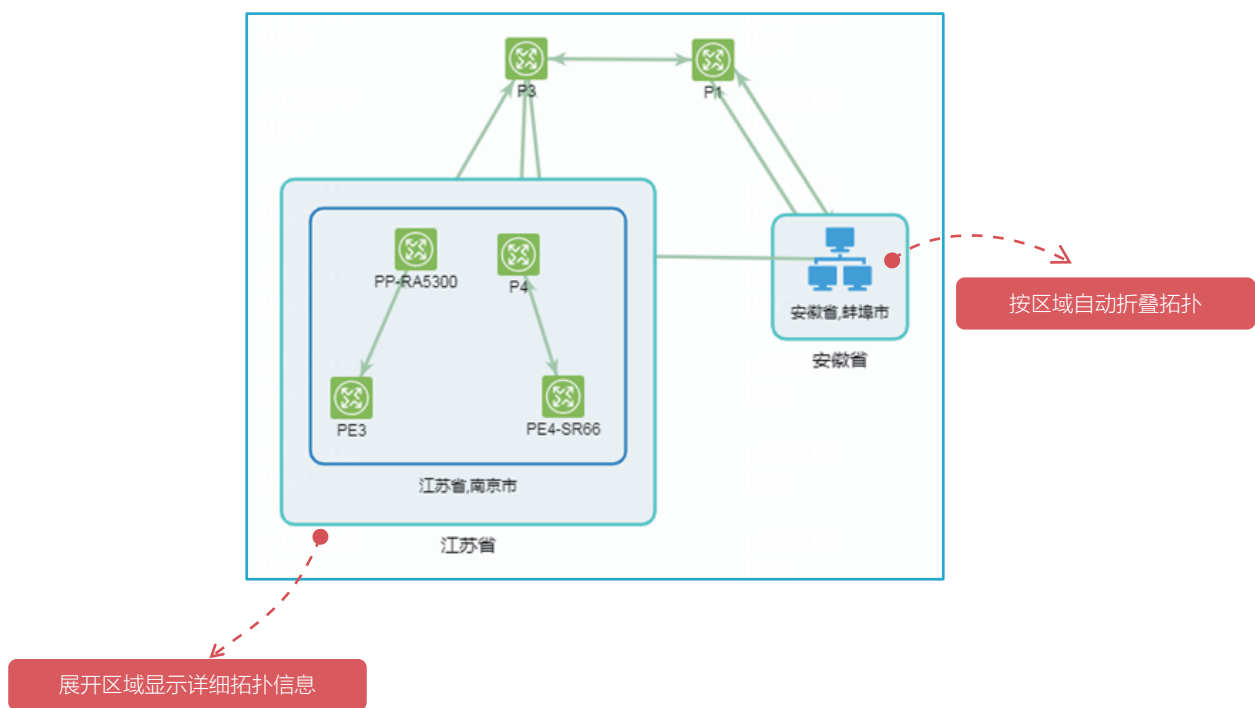
链路动态信息及报表

拓扑可视

控制组件通过BGP-LS自动收集全网设备信息及链路信息，基于网络地图构建全网拓扑，包括设备显示、设备间链路连接状态信息显示。也支持用户手动增加设备或链路。

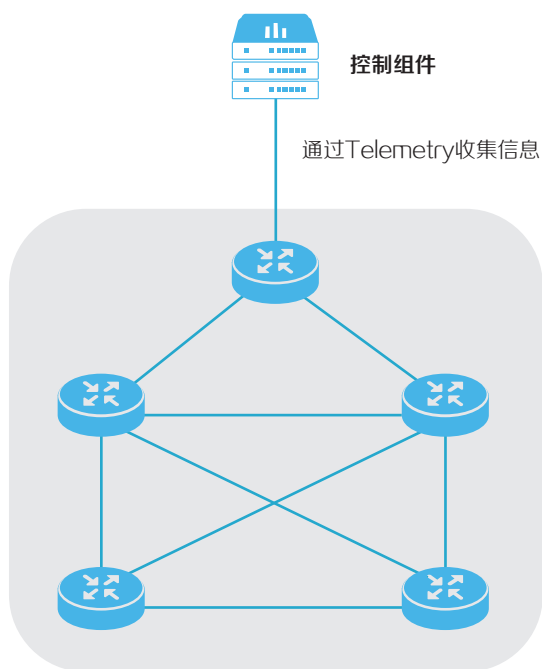


控制组件支持拓扑管理，提供了默认拓扑，也可以自定义拓扑。用户可以通过自定义拓扑手动在拓扑图上新建设备、配置设备信息，灵活控制网络拓扑。

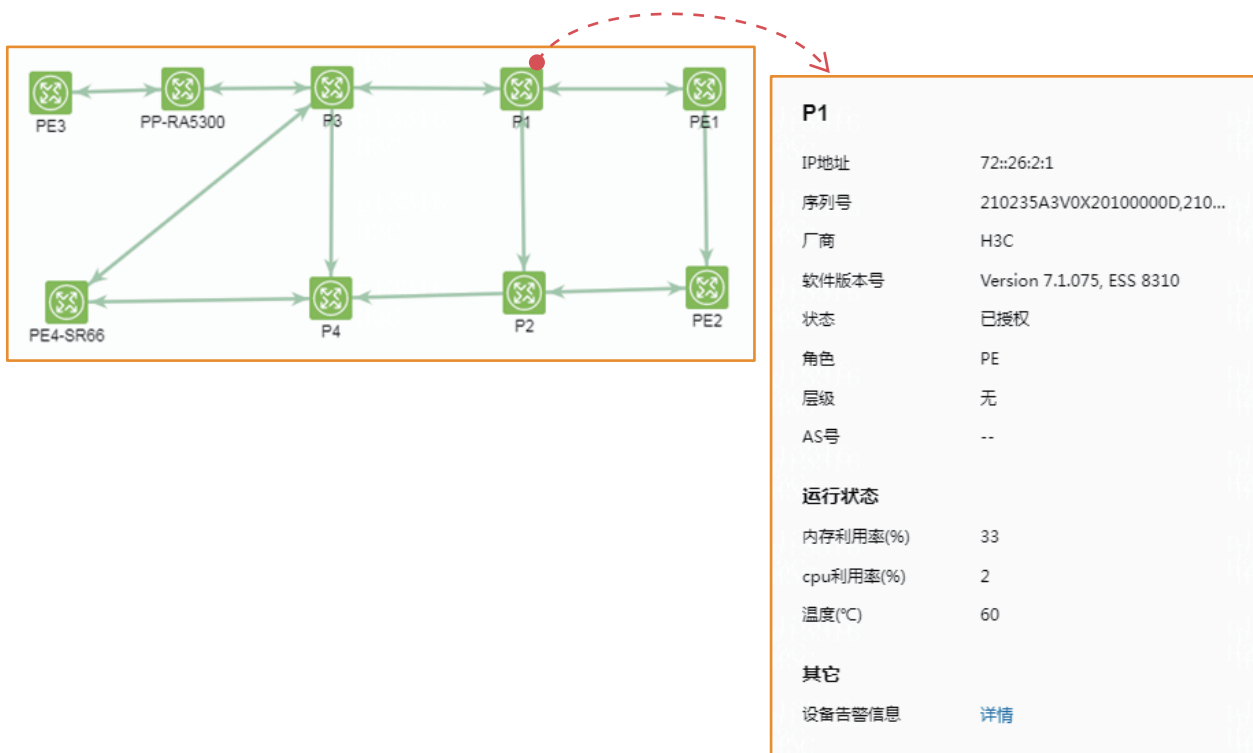


设备可视

控制组件通过Telemetry收集设备数据，提供设备详细信息、设备历史信息的可视化管理。



控制组件通过Telemetry采集到设备数据详情信息，在设备上悬停就可以查看设备实时信息。

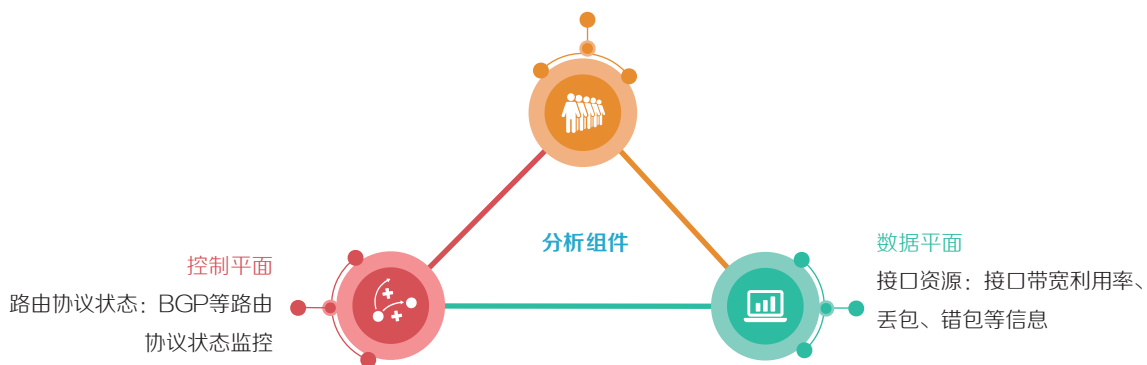


分析组件可以针对网络设备进行健康度评估分析。

健康度是一个综合的衡量指标，分析组件从系统平面、数据平面、控制平面三个维度对网络设备进行360度监控，对指标数据根据一定权重进行综合衡量，给出一个健康度评分来反映当前网络设备的运行状态。当健康度高时表示网络设备的运行状态良好，反之处于亚健康甚至异常状态。

系统平面

- 设备基础信息：版本、运行时间、位置等信息
- 设备状态信息：CPU、内存利用率、电源、风扇等状态数据
- 设备健康度：根据设备运行数据对设备健康度评分，实时健康度呈现及历史数据回溯



链路可视

控制组件的链路可视提供链路管理、链路连接信息、链路带宽信息、链路历史信息的可视化管理。

AD-WAN承载解决方案提供大屏可视功能，展示内容包括链路状态、链路带宽及质量、设备状态、应用带宽及流量、节点信息、实时告警、地图拓扑等。用户可轻松掌握当前网络及资源的实时状态，支持按需定制大屏可视化呈现的形式。



TopN链路展示

链路流量

链路历史流量TOPN

TOPN :

5

时间选择 :

最近1小时

查询

链路名称	源设备名称	目的设备名称	源接口	目的接口	链路历史总流量(MB)
P3-SR66 To P1 Link2 IPv6	P3	P1	Ten-GigabitEthernet2/2/0/1(72.13.1.2)	Ten-GigabitEthernet2/1/3(72.13.1.1)	36
P3-SR66 To P1 Link1 IPv4	P3	P1	Ten-GigabitEthernet2/2/0/1(72.13.1.2)	Ten-GigabitEthernet2/1/3(72.13.1.1)	36
PE4-SR66 To P3 Link1 IPv4	PE4-SR66	P3	GigabitEthernet2/0/0(72.33.1.2)	GigabitEthernet2/2/0/1(72.33.1.1)	32
PE4-SR66 To P3 Link2 IPv6	PE4-SR66	P3	GigabitEthernet2/0/0(72.33.1.2)	GigabitEthernet2/2/0/1(72.33.1.1)	32
PE2-CR19K To P2 Link2 IPv4	PE2	P2	Ten-GigabitEthernet1/4/4/2(72.52.1.1)	Ten-GigabitEthernet3/1/3(72.52.1.2)	29

共有 5 条记录, 当前第 1 - 5, 第 1 / 1 页

< 1 >

15 条/页

跳至

1 页

链路带宽TOPN

TOPN :

5

Q

链路实时带宽TOPN

链路名称	源设备名称	目的设备名称	源接口	目的接口	链路实时带宽(kbps)	链路带宽占比(%)
P3-SR66 To P1 Link1 IPv4	P3	P1	Ten-GigabitEthernet2/2/0/1(72.13.1.2)	Ten-GigabitEthernet2/1/3(72.13.1.1)	86	0
P3-SR66 To P1 Link2 IPv6	P3	P1	Ten-GigabitEthernet2/2/0/1(72.13.1.2)	Ten-GigabitEthernet2/1/3(72.13.1.1)	86	0
PE4-SR66 To P3 Link2 IPv6	PE4-SR66	P3	GigabitEthernet2/0/0(72.33.1.2)	GigabitEthernet2/2/0/1(72.33.1.1)	84	0.04
PE4-SR66 To P3 Link1 IPv4	PE4-SR66	P3	GigabitEthernet2/0/0(72.33.1.2)	GigabitEthernet2/2/0/1(72.33.1.1)	84	0.04

链路实时信息

物理网络 > 链路 > 链路总览 [PE1-SR8808H To P...] > 质量详情

设备

链路

链路总览

链路管理

链路限速

链路名称: PE1-SR8808H To PE2-CR19K Link1 IPv6

优先级名称	优先级	丢包率(%)	时延(us)	抖动(us)
Default	--	0	21	1

共有 1 条记录, 当前第 1 - 1, 第 1 / 1 页

链路历史信息

链路运行历史

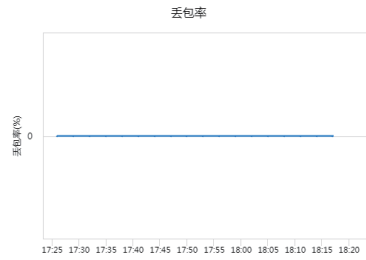
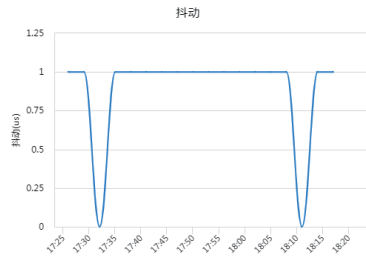
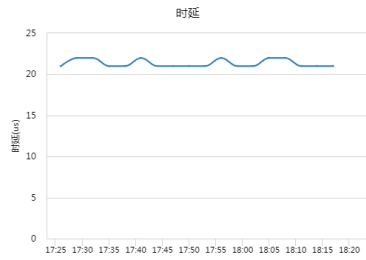
* 时间选择 :

最近1小时

上一时间段

下一时间段

删除历史信息



PE1-SR8808H To PE2-CR19K Link1 IPv6

PE1-SR8808H To PE2-CR19K Link1 IPv6

PE1-SR8808H To PE2-CR19K Link1 IPv6

分析组件的Netstream流分析中的接口组流量分析可以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。

接口组全网流量排名展示

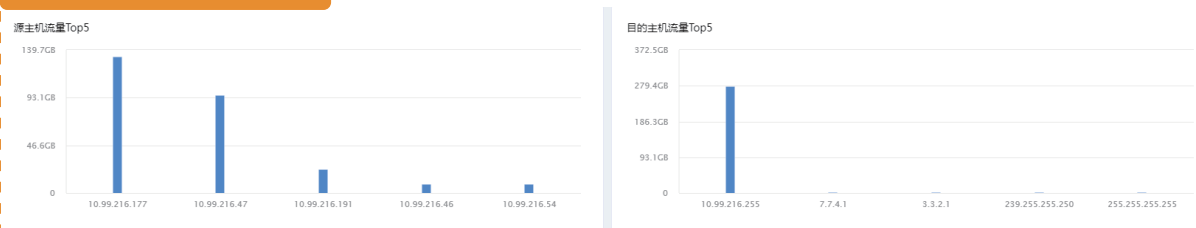


接口组流量统计列表以及各接口组的流量趋势展示

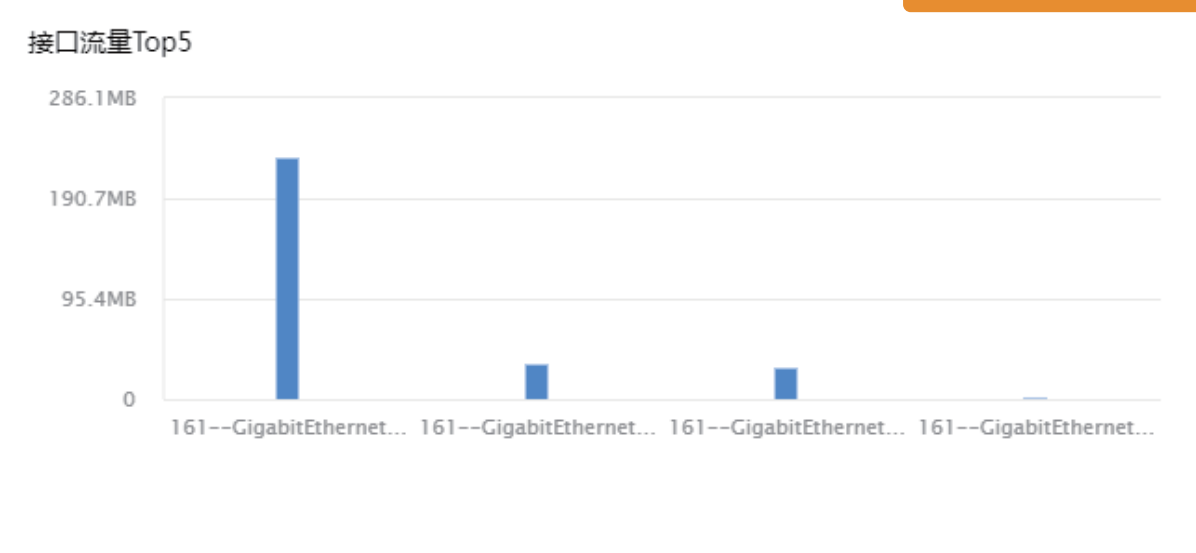


在指定接口组下可以按照主机、接口、应用、会话等类型查看该接口组下的流量统计。

接口组下的主机流量排名展示

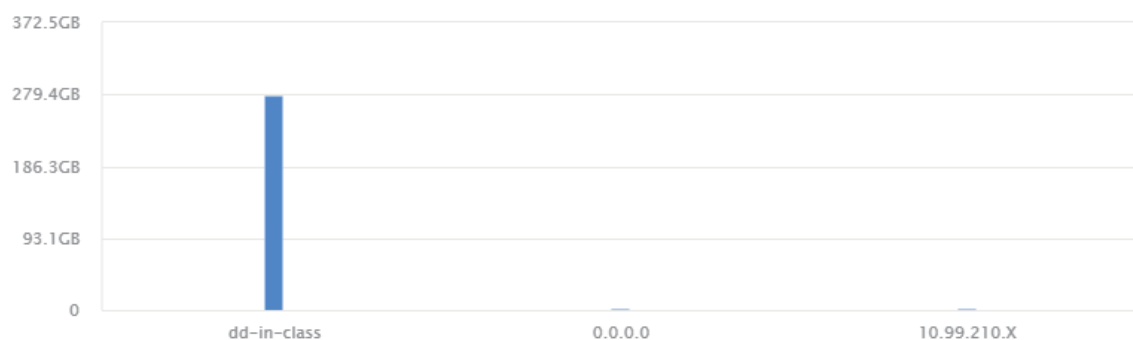


接口组下接口流量排名展示



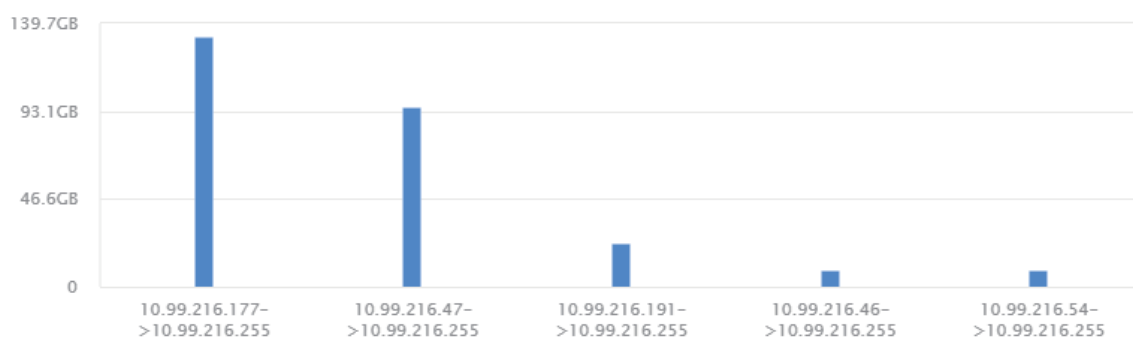
接口组下应用流量排名展示

应用流量Top5



接口组下会话流量排名展示

会话流量Top5



2、应用可视

应用可视提供应用流量、应用路径和应用质量的可视化管理。

应用流量



- TopN应用流量
- 应用流量历史报表
- 链路实时应用流量

应用路径



- 实时运行路径
- 调度主备路径

应用质量



- 应用质量：延时、抖动、丢包
- 应用健康度
- 应用质量历史报表

应用流量可视

控制组件定义业务类型（应用组）后，可以基于业务和业务实例查看业务流量详情，包括业务流量带宽、时延、抖动。

应用组流量Top5排行

应用组带宽Top5



应用组历史流量曲线

首页 > 应用组详情 [IT业务] > 历史信息

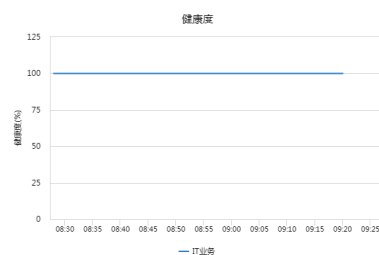
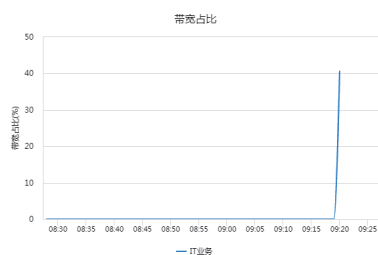
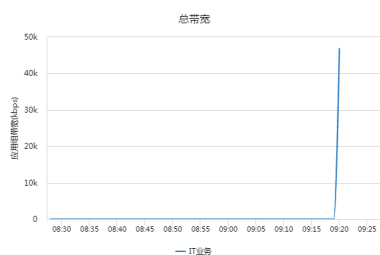
历史信息

* 应用组名称: IT业务

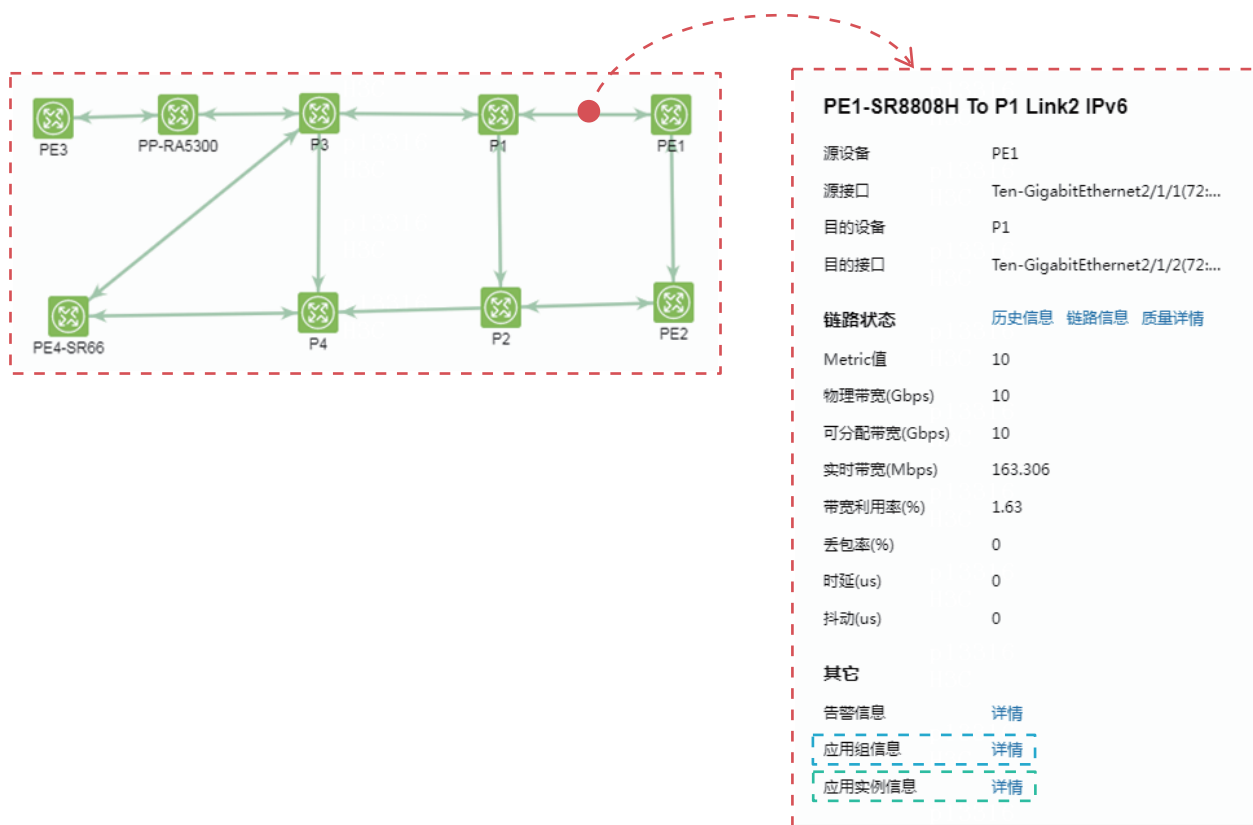
* 时间选择: 最近1小时

上一小时 下一小时 刷新历史曲线

返回



拓扑中，选择某链路，可以查看该链路上所有业务的实时流量信息。



链路上应用组的实时流量		
承载拓扑 > 链路 [PE1-SR8808H To P...] > 链路应用组带宽		
链路应用组带宽		
应用组名称	带宽(kbps)	带宽占用率(%)
IT业务	48945	0.49
视频业务	0	0
语音业务	0	0
共有 3 条记录, 当前第 1-3, 第 1 / 1 页		

链路上应用组实例的实时流量				
承载拓扑 > 链路 [PE1-SR8808H To P...] > 应用实例带宽				
应用实例带宽				
应用组名称	源设备	目的设备	带宽(kbps)	带宽占用率(%)
IT业务	PE1(72:26:1:1)	PE3(72:26:1:3)	48945	0.49
视频业务	PE1(72:26:1:1)	PE3(72:26:1:3)	0	0
视频业务	PE1(72:26:1:1)	PE4-SR66(72:26:1:4)	0	0
IT业务	PE1(72:26:1:1)	PE4-SR66(72:26:1:4)	0	0
语音业务	PE1(72:26:1:1)	PE3(72:26:1:3)	0	0
共有 5 条记录, 当前第 1-5, 第 1 / 1 页				

应用路径可视

控制组件可以基于业务显示拓扑路径，可以查看业务流量经过的设备名称、设备地址、设备出入端口号、业务流量大小。

拓扑中自动呈现应用实时运行路径、调度主备路径。控制组件基于用户策略（SLA、链路优选、时间策略、主备链路等）规划计算业务路径并进行业务流量转发。

选定应用组对应整网所有路径

源设备名称： 全选
目的设备...： 全选
路径类型： 全选
路径编号： 全选

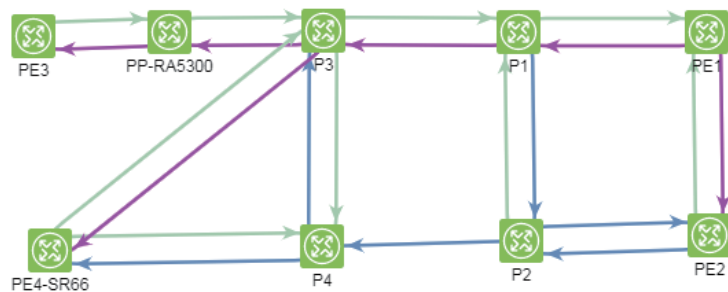
确定
取消

应用组

应用组名称	应用组状态	应用组类别
视频业务	正常状态	调度
语音业务	正常状态	调度
IT业务	正常状态	调度

共有 3 条记录，当前第 1 - 3，第 1 / 1 页

< 1 >
15 条/页



选定应用组指定起终点的路径

源设备名称：
目的设备...：
路径类型：
路径编号：

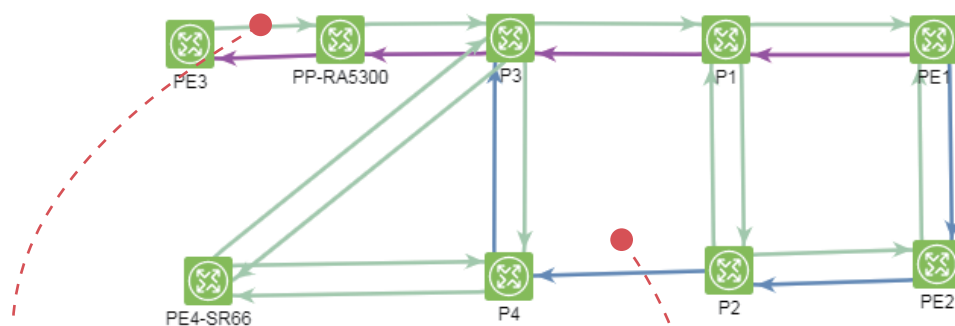
确定
取消

应用组

应用组名称	应用组状态	应用组类别
视频业务	正常状态	调度
语音业务	正常状态	调度
IT业务	正常状态	调度

共有 3 条记录，当前第 1 - 3，第 1 / 1 页

1
15 条/页



> PE1->PE2主路径

PE1->PE2备路径 <

拓扑图例

- 正常
- 候选路径1
- 候选路径2
- 默认路径
- 下线
- 警告告警
- 严重告警

应用流量可视

控制组件可以基于业务进行路径统计及流量统计、依据大数据计算并呈现应用健康度情况。当应用流量质量满足SLA要求时，应用链路显示为绿色，表示应用健康良好；当应用流量质量不满足SLA要求时，应用链路显示为黄色或红色（以不满足程度为准），表示应用健康有问题。

应用组实例符合SLA需求的比例。如所有应用组实例均符合，则健康度100%

应用组整体质量健康度					
应用组列表					
应用组名称	应用组带宽(kbps)	带宽占比(%)	健康度(%)	实例排行	历史
IT业务	48945	41.65	100	11	11
视频业务	0	0	100	11	11
语音业务	0	0	100	11	11

应用组实例SLA符合度										
应用组实例										
应用组名称	源设备	目的设备	调度隧道	默认隧道	SLA符合度	最小带宽(kbps)	正反向	候选路径	候选路径最大...	下发状态
IT业务	PE1(72:26:1:1)	PE2(72:26:1:2)	srv6-1-72:26:1:1-72:26:1:2	srv6-4002-72:26:1:1-72:26:1:2	●	--	1	1	1	下发成功
IT业务	PE1(72:26:1:1)	PE3(72:26:1:3)	srv6-1-72:26:1:1-72:26:1:3	srv6-4000-72:26:1:1-72:26:1:3	●	--	1	1	1	下发成功
IT业务	PE1(72:26:1:1)	PE4-SR66(72:26:1:4)	srv6-1-72:26:1:1-72:26:1:4	srv6-4001-72:26:1:1-72:26:1:4	●	--	1	1	1	下发成功

应用组实例质量满足应用组SLA要求则符合，显示为绿色。

3、故障可视

故障可视提供故障识别和实时告警的可视化管理。

设备故障

- ✓ 设备无法连接
- ✓ 设备接口DOWN
- ✓ 设备CPU、内存、温度过高

链路故障

- ✓ 链路质量低于阈值
- ✓ 链路中断

应用质量故障

- ✓ 应用质量不满足需求

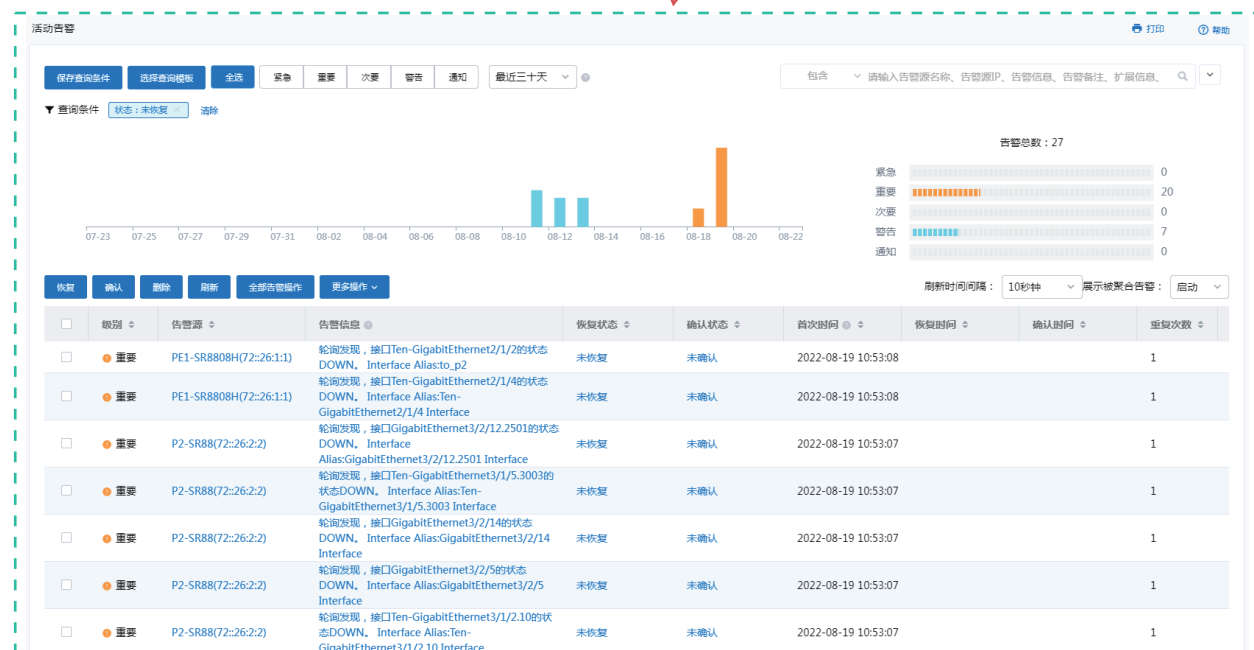
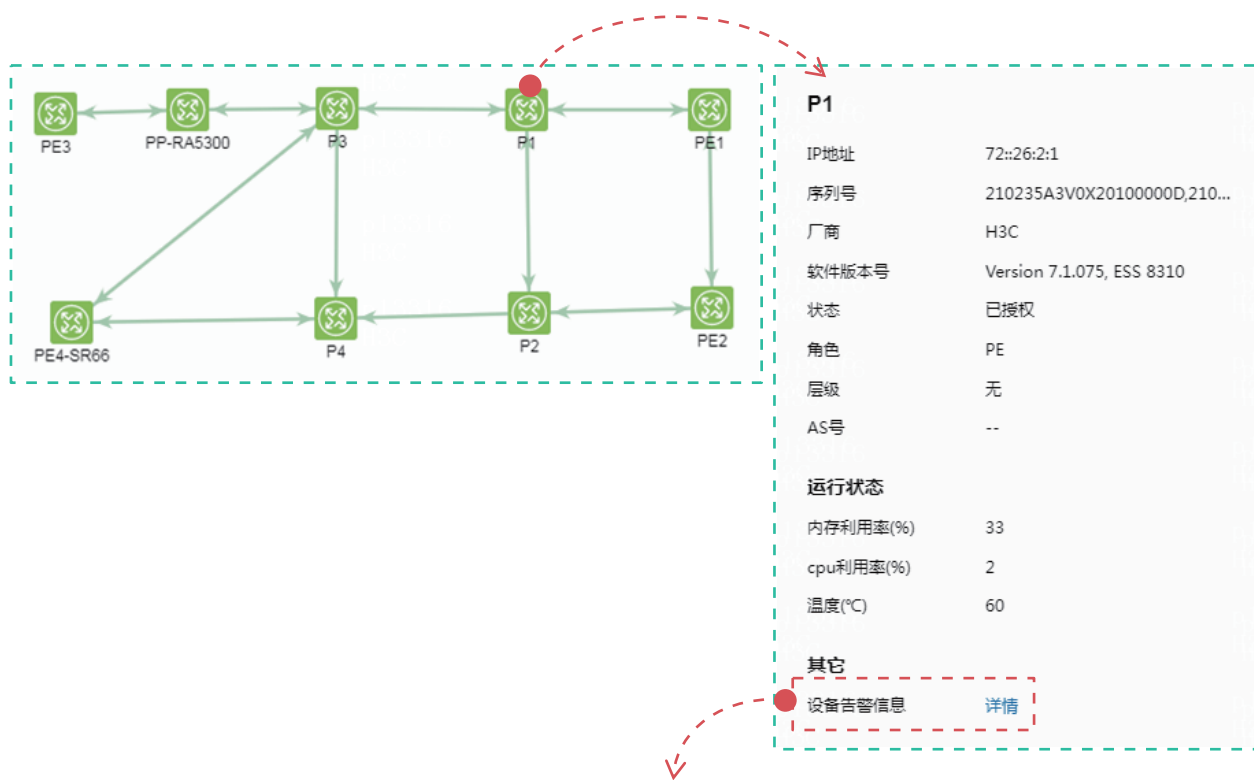


页面告警

- ✓ 拓扑图呈现告警信息
- ✓ 推送告警消息

告警推送

- ✓ Email方式推送告警
- ✓ 短信推送告警
- ✓ 微信/企业微信告警



方案亮点

多维度的数据展示

涵盖设备、链路、站点、应用组及故障等常用的数据指标



可视化的信息呈现

图形化的界面降低信息管理难度，提供各项信息的图表

AD-WAN承载解决方案之 丰富的流量调度策略

传统网络面临的问题

随着网络的快速发展，各行各业对WAN网络的需求飞速增长，传统WAN网络中，业务开通周期长、业务质量无保障等问题亟待解决。

以企业用网场景为例，企业往往要求新业务能够快速上线，策略可灵活部署，重点业务能得到保障。



方案介绍

AD-WAN承载网解决方案提供丰富的流量调度策略，支持基于带宽、时延、抖动、丢包率、时间段、优选链路、排除链路、可选链路等多种策略进行路径计算，对业务进行灵活的链路切换，从而满足用户业务的需求。

1、SLA策略

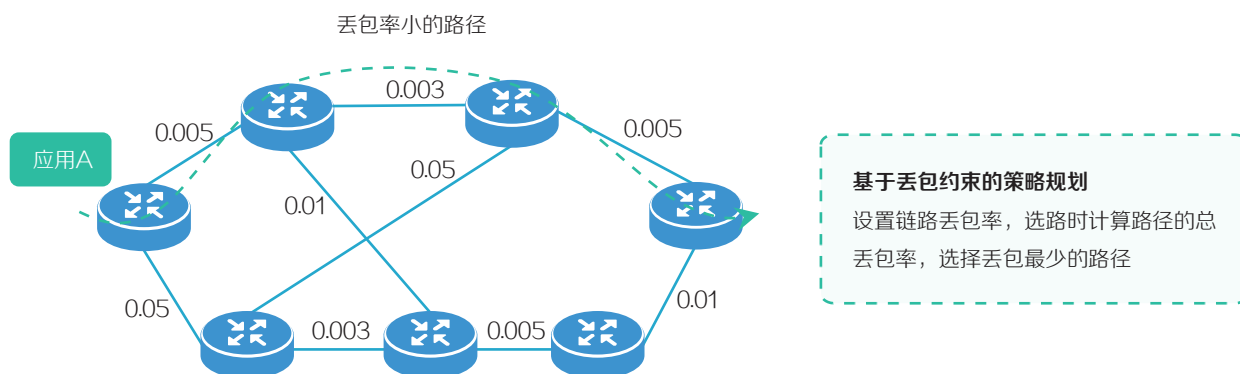
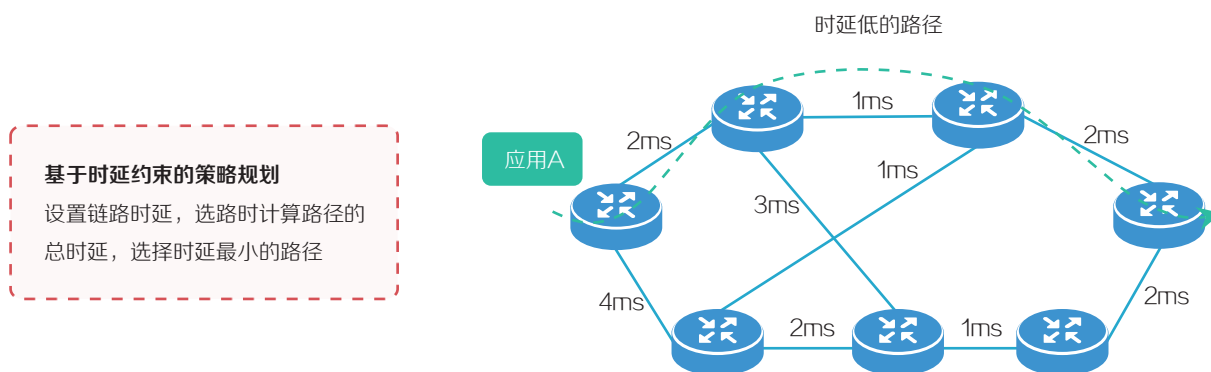
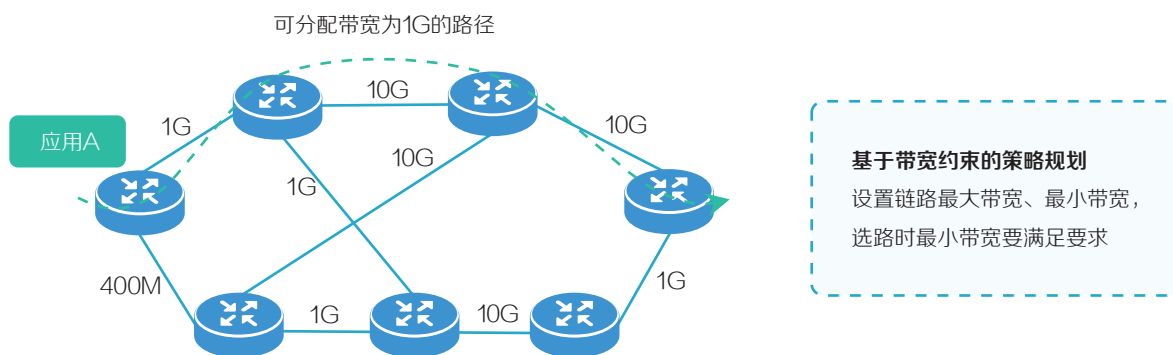
SLA策略用于指定业务流量调度时要满足的链路质量要求。

包括 SLA级别，最大、最小带宽，是否限速，报文优先级着色等信息。

AD-WAN控制组件提供8种内置SLA级别，优先级从0-7，定义了初始的延时、抖动和丢包率。



SLA: Service Level Agreement，服务等级协定

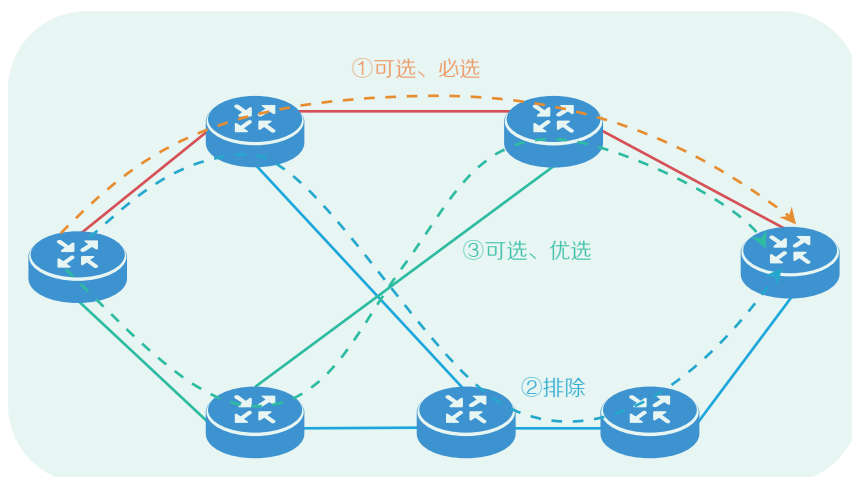


2、路径优选策略

路径优选策略用于规划应用组优先经过的链路，通过对链路进行**着色**后，根据应用的优选策略完成选路。支持链路优选和节点优选。

链路着色，即给设备间的链路打上颜色标记。选路时根据链路组的**颜色**要求选择合适的路径。

- 可选链路组 R G
- 可选链路组 B
- 必选链路组 R
- 优选链路组 G



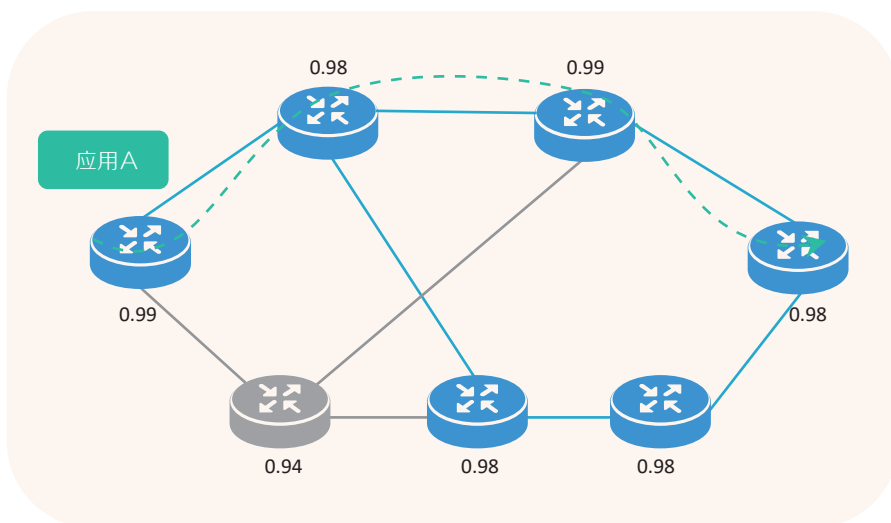
3、基于可用度的调度策略

基于全网流量分析计算可用度指标，并根据可用度大小进行选路。

指定周期内，可用度 = (总运行时长 - 链路不可用的时长) / 总运行时长

链路丢包率、时延、抖动超过预设阈值，则认为**链路不可用**。链路阈值可手动设置，丢包率默认阈值为100%，时延、抖动默认值建议设置为10秒。

- 可用度为1表示链路完全可用，值越小可用度越差。
- 可用度为0表示链路完全不可用。



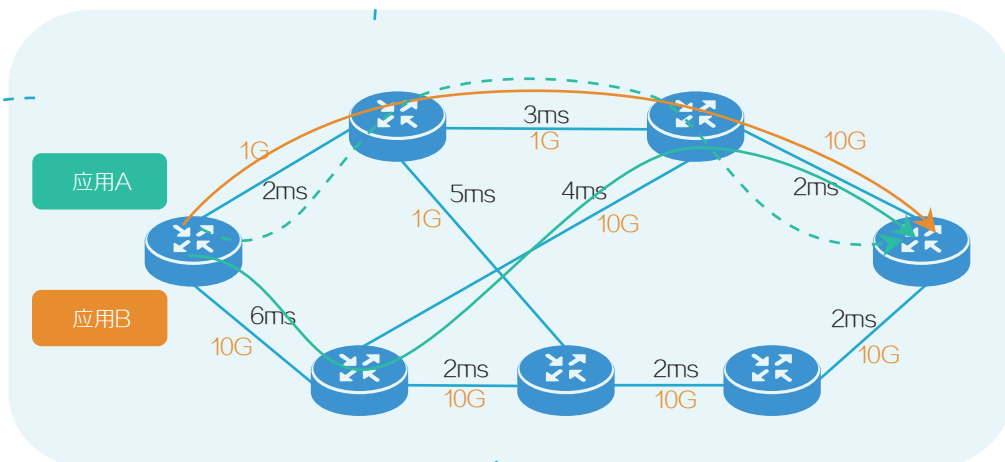
4、优先级抢占策略

在资源有限的情况下，可应用**优先级抢占策略**：高优先级应用会抢占低优先级应用的转发路径，优先级低的应用将重新选路。

应用A需求：最小带宽500M，延时<10ms，优先级低
应用B需求：最小带宽600M，延时<10ms，优先级高

② 增加高优先级应用B，此时，由于绿色虚线为当前网络中延时最低的路径资源，为优先保障应用B，按优先级顺序抢占绿色虚线路径（即橙色实线路径）。

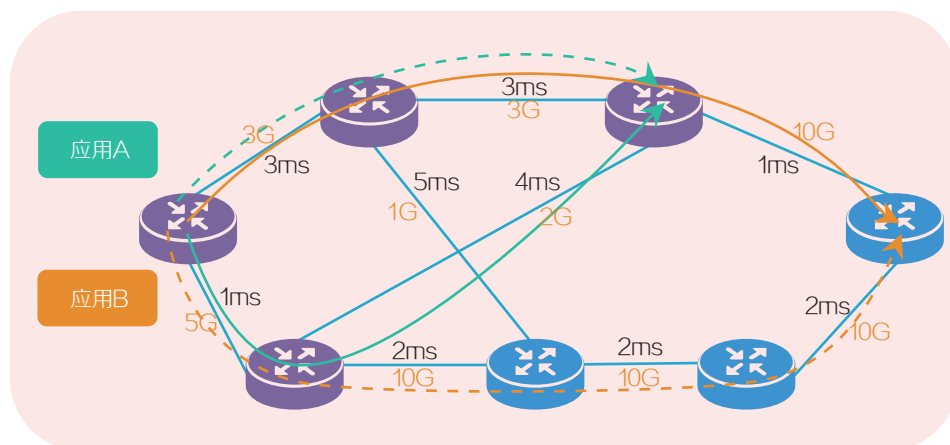
① 初始网络中仅承载应用A，应用A选择满足条件的绿色虚线路径转发。



③ 低优先级的应用A重新选路（即绿色实线路径）。

5、全局/局部优化策略

用户可根据需要应用全局/局部优化策略，网络中的转发流量将自动调整到最优路径。



应用A需求：最小带宽4G，延时<20ms
应用B需求：最小带宽2G，延时<10ms

当前网络中，应用A选择满足条件的绿色虚线路径转发，应用B选择满足条件的橙色虚线路径转发。

1

2

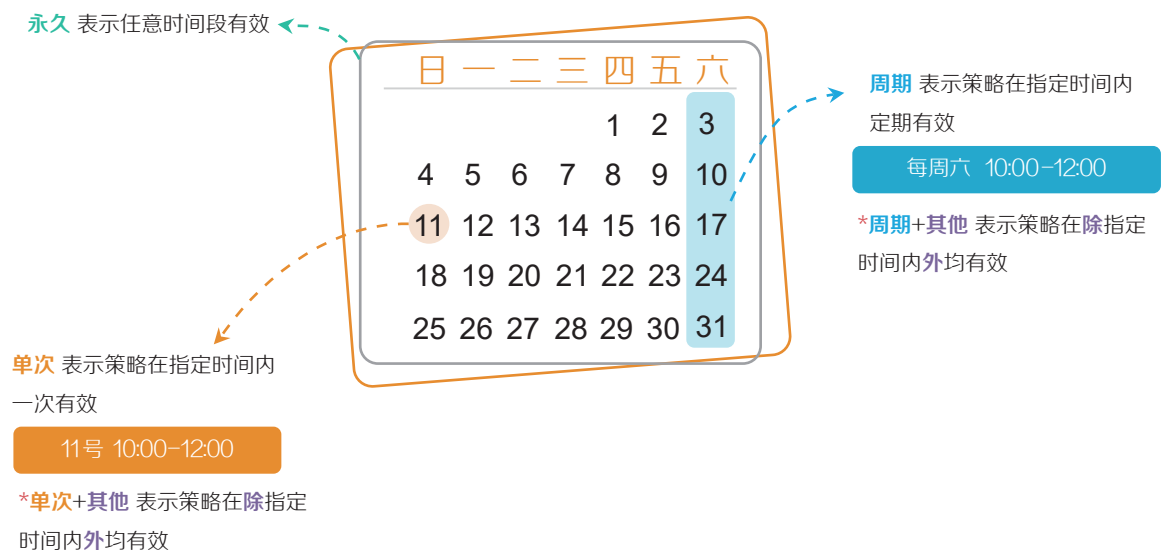
3

- 若应用全局优化策略，将优化应用A和应用B的路径。
- 若应用局部优化策略（即紫色区域），将仅优化应用A的路径。

先进行局部优化后进行全局优化，应用A将调整到绿色实线路径转发，应用B将调整到橙色实线路径转发。

6、时间策略

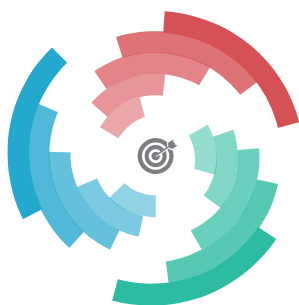
时间策略用于指定业务流量调度的时间段，包括**永久**、**单次**、**周期**，单次和周期可搭配**其他**使用。不同时间段内可使用不同的SLA策略。



调度策略应用流程



小结



调度灵活

路径优选策略可提供多条路径，满足业务差异化承载。

满足多样需求

方案提供丰富的调度策略，多样的组合满足不同需求。

基于用户体验的选路

优先基于用户配置的调度策略进行选路。



AD-WAN承载解决方案之

精细化应用分类

业务需求



流量识别

生产流量、办公流量、
娱乐流量…



访问控制

完全访问、部分访问、
禁止访问



流量统计/限速

实时统计、历史统计、
限制下载速度…

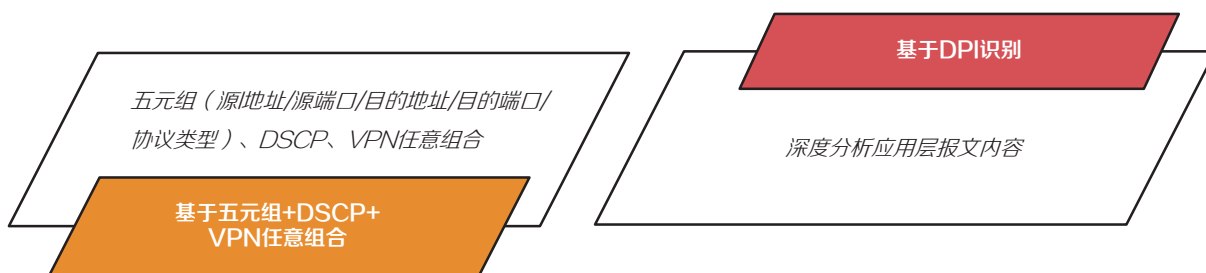


流量可视化

基于统计数据提供可视的
分析图表

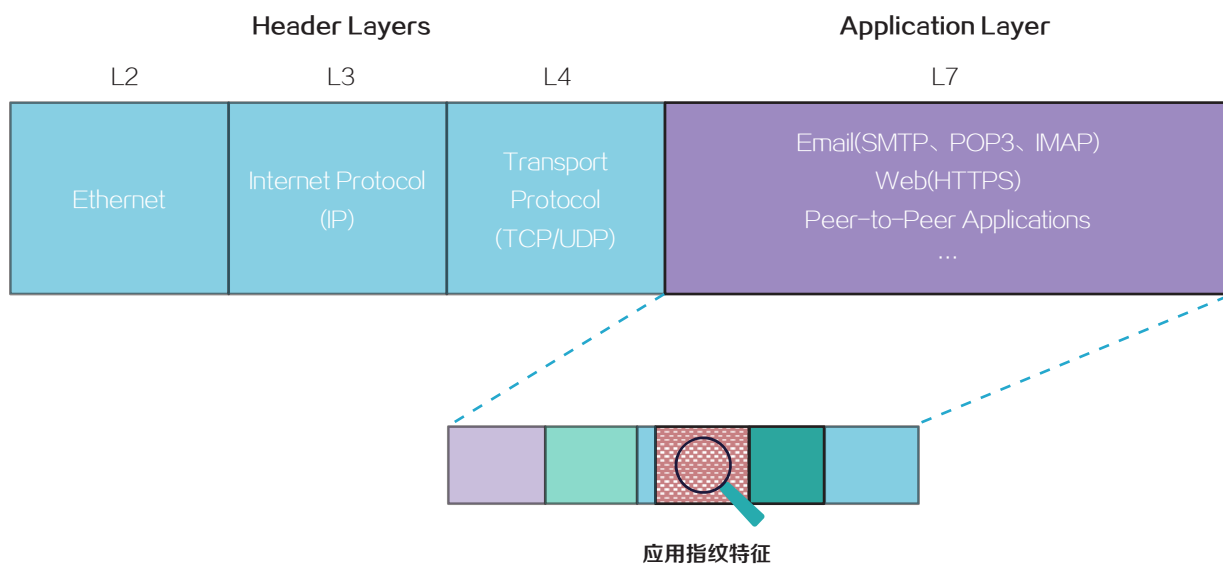
只有精准地识别应用流量，才能有针对性的提供差异化服务。

应用识别技术



传统网络的普通报文检测往往只分析IP分组四层以下的内容，一般包括源地址、源端口、目的地址、目的端口、协议类型、DSCP以及VPN组合。

一些基于应用的业务（例如QoS，带宽管理等）在进行报文处理时需要知道报文所属的应用层协议，这时普通的报文检测就无法满足需求，因此基于DPI（Deep Packet Inspection深度报文检测）的应用识别技术应运而生。



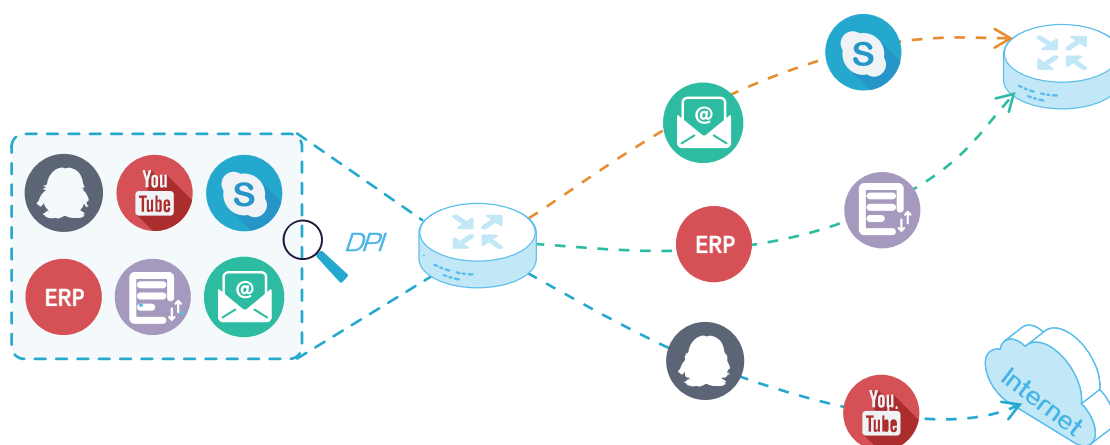
DPI简介

DPI是相对普通报文检测而言的一种新的检测技术，DPI对OSI协议中的第七层，即应用层的内容进行深度分析，从而根据应用层的净荷特征识别其应用类型或内容。

当IP数据包、TCP或者UDP数据流经过基于DPI技术的网络设备时，DPI引擎通过深入读取IP包载荷的内容来对七层协议中的应用层信息进行检测，从而识别出IP包的应用层协议。



DPI自动识别L4-L7层应用，精准调度流量

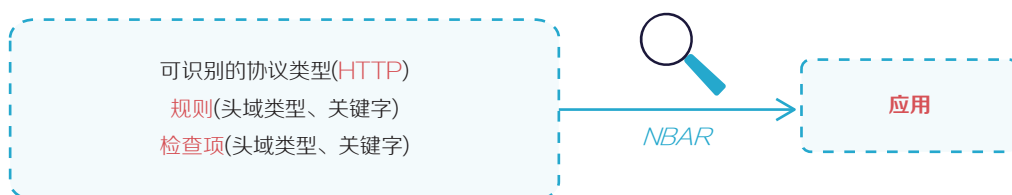


应用场景

AD-WAN使用DPI的APR（**Application Recognition，应用层协议识别**）作为应用识别的方式，并能够对接口上接收或者发送的某个应用层协议的报文进行数目和速率统计。
为了更好地识别报文所属的应用层协议，APR提供了NBAR应用识别方式。

NBAR

NBAR（Network Based Application Recognition，**基于内容特征的应用识别**），即提取应用报文区别于其它应用报文的特征，通过将报文的内容与特征库中的特征项进行匹配来识别报文所属的应用层协议。



头域类型

- URI：匹配统一资源标识符（Uniform Resource Identifier），由协议、主机IP地址和主机资源的具体地址三部分组成
- Host：匹配请求资源的Internet主机和端口号

应用特征类型

应用特征分为预定义和自定义两种，预定义应用由系统缺省创建，自定义应用由用户通过手工配置创建。



配置流程

使用NBAR方式时，需要事先配置规则和检查项，在增加应用特征时绑定规则，通过头域和关键字来识别报文。
配置流程如下：

01
配置检查项

检查项中可以配置头域类型及关键字，用来匹配识别HTTP报文的URI和主机名，检查项可被规则引用。

增加检查项

* 检查项名称：

* 头域类型：Host

* 匹配方式：关键字

* 匹配值：

描述：描述

确定

取消

02
配置规则

规则中可以配置头域类型及关键字，并可以引用多个检查项，同时满足匹配规则和所有检查项的报文为匹配规则的报文。

增加规则

规则基本信息

* 规则名称：

* 头域类型：Host

* 匹配方式：关键字

* 匹配值：

描述：描述

检查项列表

选择

检查项名称	头域类型	匹配方式	匹配值	描述	操作
暂无数据					

共有0条记录

引用检查项

选择检查项

检查项名称

检查项名称	头域类型	匹配方式	匹配值	描述
暂无数据				

共有0条记录

确定

取消

03 配置应用特征

包括预定义应用特征和自定义应用特征。对于NBAR方式，若报文符合应用特征中任意一条规则，则符合该应用特征。

自定义/预定义 应用特征

自定义应用特征

增加

删除

应用特征名称	识别方式	协议类型	定义类型	规则名称	描述	操作
暂无数据						

共有0条记录

115 条/页 跳至 1 页

预定义应用特征

应用特征名称	定义类型	描述
AnFangForum	预定义	AnFangForum
DRACU-RIOT	预定义	DRACU-RIOT
syslog	预定义	syslog

应用特征名称

Q

增加自定义应用特征

自定义特征基本信息

应用特征名称

描述

识别方式

NBAR

协议类型

HTTP

规则列表

选择

规则名称	头域类型	匹配方式	描述	操作
暂无数据				

共有0条记录

115 条/页 跳至 1 页

引用规则

选择规则

规则名称

Q

规则名称	头域类型	匹配方式	描述
暂无数据			

共有0条记录

115 条/页 跳至 1 页

确定

取消

应用特征组可引用多个自定义应用特征和预定义应用特征。若报文符合任何一个应用特征，则符合该应用特征组。

自定义/预定义 应用特征组

自定义应用特征组

增加

编辑

应用特征组名称	应用特征名称	描述	操作
暂无数据			

共有0条记录

1

15 条/页

跳至 1 页

预定义应用特征组

应用特征组名称	应用特征名称	描述
DBM	应用特征名称	DBM
E-Mail	应用特征名称	E-Mail applications list
Financial_Management	应用特征名称	Financial_Management applications list

增加自定义应用特征组

特征组定义

应用特征组名称:

描述:

应用特征列表

选择

应用特征名称	定义类型	描述	操作
暂无数据			

共有0条记录

1

15 条/页

跳至 1 页

引用应用特征组

选择应用特征

应用特征名称

Q

☐	应用特征名称	定义类型	描述
☐	AnFangForum	预定义	AnFangForum
☐	DRACU-RIOT	预定义	DRACU-RIOT
☐	syslog	预定义	syslog

自定义应用时可引用应用特征组。若报文符合该应用特征组，则被识别为属于此应用，也即属于引用此应用的应用组。

增加应用

增加应用

应用基本信息

应用名称:

应用描述:

匹配规则列表:

IP类型:

确定
取消

应用组匹配规则列表

增加

匹配模式	协议类型	端口类型	源子网及掩码	目的子网及掩码	源端口	目的端口	EXP	VNI	DSCP	VRRP名称	操作
暂无数据											

共有0条记录

1
15 条/页
跳至
1
页

方案亮点

1、快速识别

AD-WAN在对行业标准应用，如Email、Web、FTP等进行识别时，无需进行繁琐的应用预定义操作，可基于DPI特征库进行自动化识别，提升应用识别效率。

2、精准识别

AD-WAN综合利用基于五元组识别和基于DPI识别两种应用识别技术，可精细化识别企业私有应用和行业标准应用，为做好精细化的流量调度打好基础。

AD-WAN承载网解决方案之 iFIT随流分析

简介

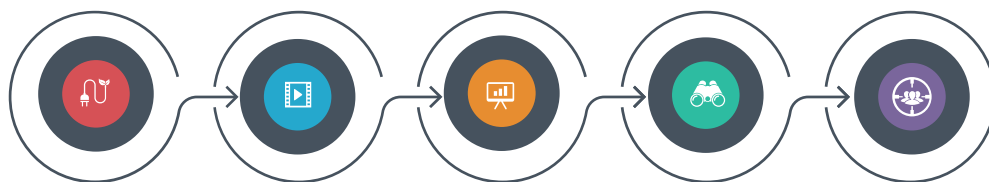
随着网络的普及和通信技术的发展，各种网络业务层出不穷，新业务对网络性能提出了更高的要求。当网络业务质量下降时，用户希望能够快速定位并排除网络故障。

iFIT（In-situ Flow Information Telemetry，带内流信息测量）是一种通过直接测量业务报文得到网络真实丢包率、时延等性能参数的检测方式，具有部署方便、统计精度高等优点。

方案介绍

AD-WAN方案中，iFIT主要应用于MPLS、SR和IPv6 SR网络。使用该功能前需先完成设备开局，控制组件下发SRv6 Policy、VPN等配置，分析组件采集组网设备数据。

用户可通过分析组件简单直观的查看业务流的质量信息。



设备侧配置

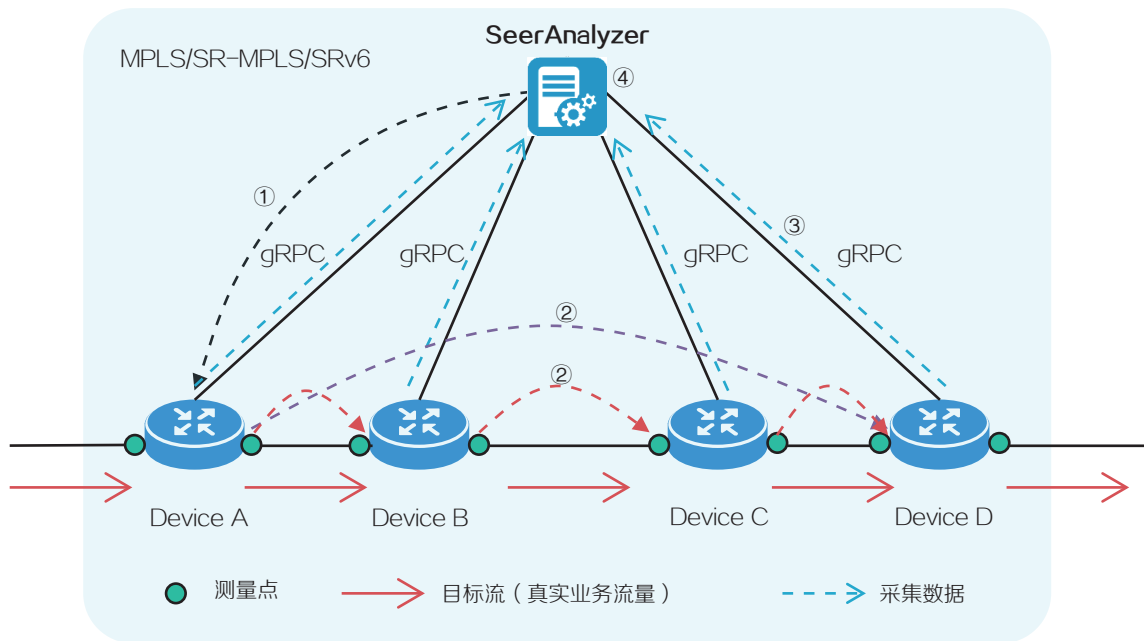
- 组网配置
- 时间同步配置
- gRPC配置
- iFIT配置

分析组件配置

开启gRPC采集

分析组件 采集任务配置

开启iFIT流分析

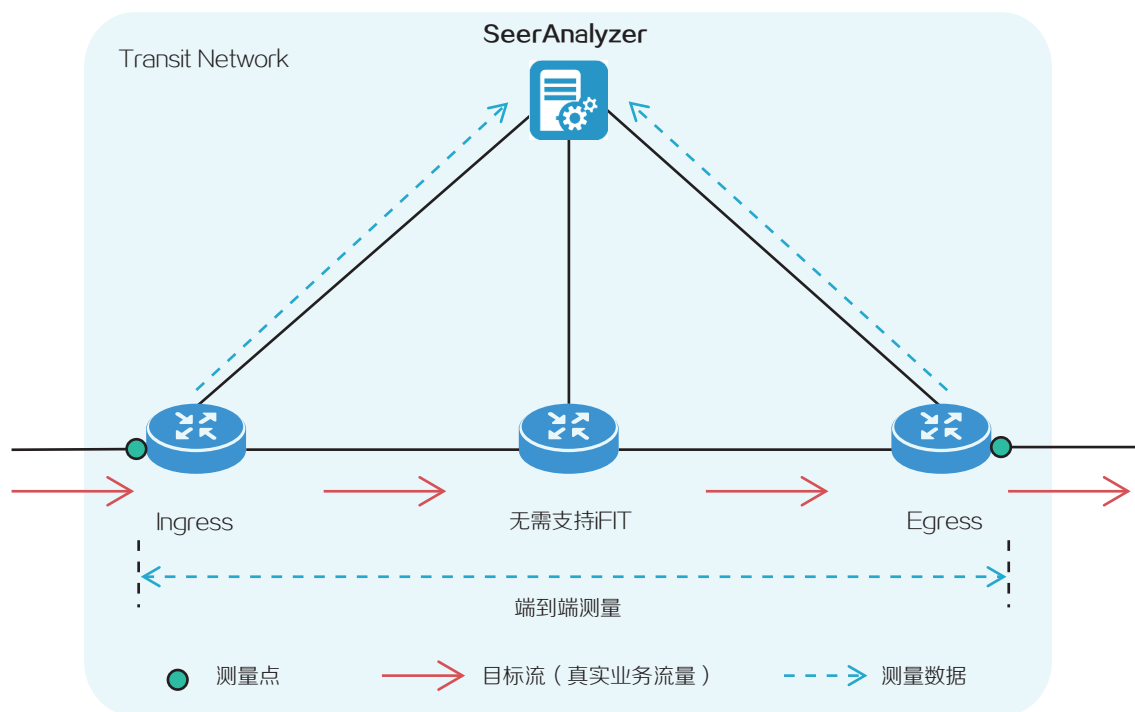


- ① iFIT部署：包括时间同步、gRPC采集、使能iFIT测试。
- ② 网元自动识别业务流。对丢包、时延、实时流量进行性能测量，获得实时业务路径上逐个网元节点、逐段链路的SLA测量结果。
- ③ 网元通过Telemetry协议，将逐个网元、端口、逐段链路的丢包、时延的统计结果周期性地主动上报SeerAnalyzer。
- ④ SeerAnalyzer计算业务流的丢包、时延指标。支持设置实时流量的丢包、时延阈值，并在阈值越限时为流量染色。

测量模式

1、端到端测量方案

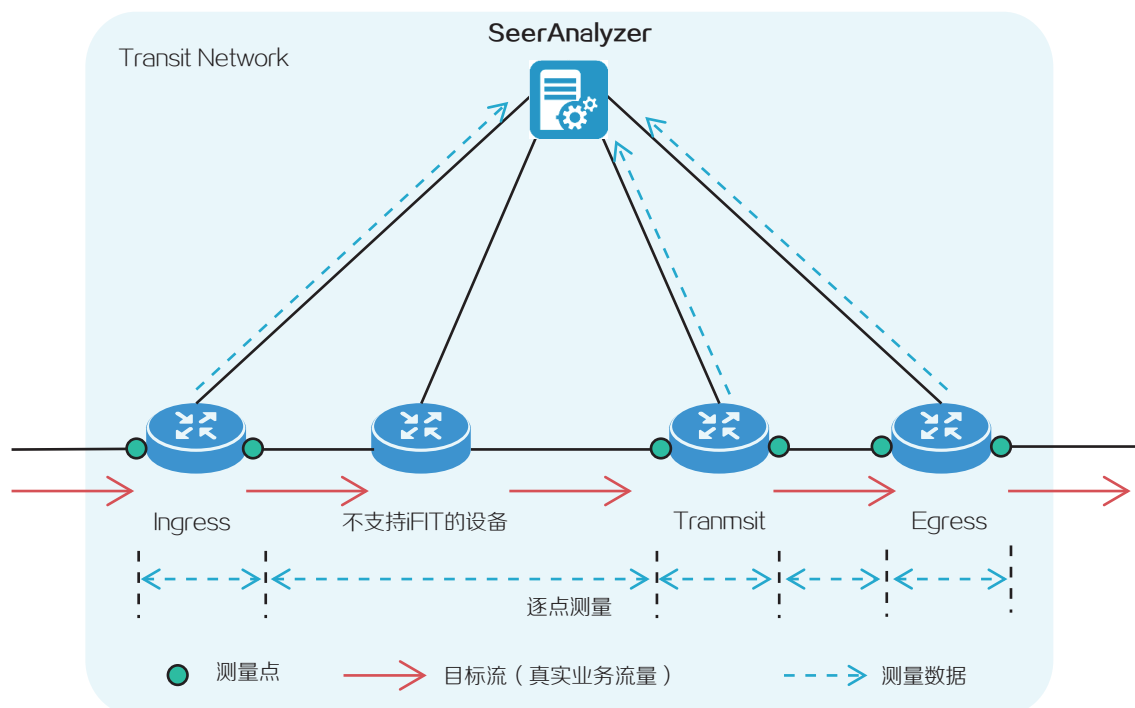
端到端检测方案部署在流量入接口（Ingress）和出接口（Egress）两节点上，可实时检测传输网络（Transit Network）中端到端真实业务报文的丢包和时延指标，便于用户在网络性能劣化时及时进行业务调整。



SeerAnalyzer计算业务流Ingress端、Egress端的丢包、时延指标。支持设置阈值，阈值超限染色。

2、逐点测量方案

当根据端到端检测结果发现被检测业务有丢包或时延不满足业务要求时，可以将端到端之间的网络划分为多个更小的测量区段，测量每两个节点之间的丢包、时延值，进一步定位影响网络性能的网元位置。



SeerAnalyzer根据质差流逐跳路径计算每个网元端口的丢包、时延指标。支持设置阈值，阈值越限染色。



应用场景

SR MPLS、SRv6组网场景均可采用iFIT进行网络性能分析。

设备侧采用Telemetry技术将iFIT检测的全网性能数据统一送给分析组件进行计算，获得用户流的实时SLA性能指标。

分析组件随流检测特性基于实时SLA数据提供日常**主动运维**和**故障快速定界**两大典型应用场景。

iFIT实例配置

针对关注的业务可在分析组件配置业务对应的实例。

配置测量周期，选择测量模式

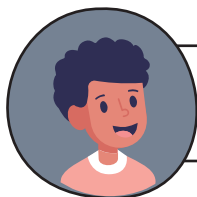
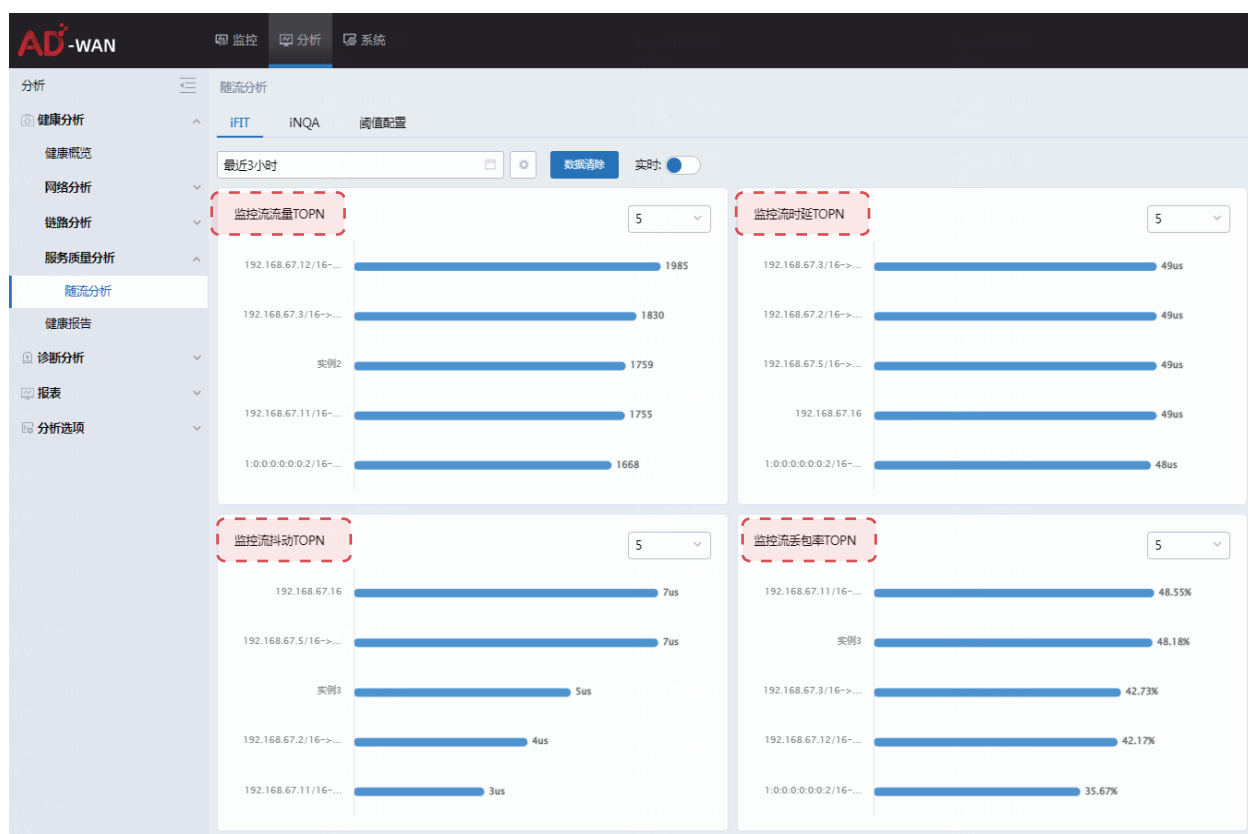
配置测量阈值

配置监控流信息

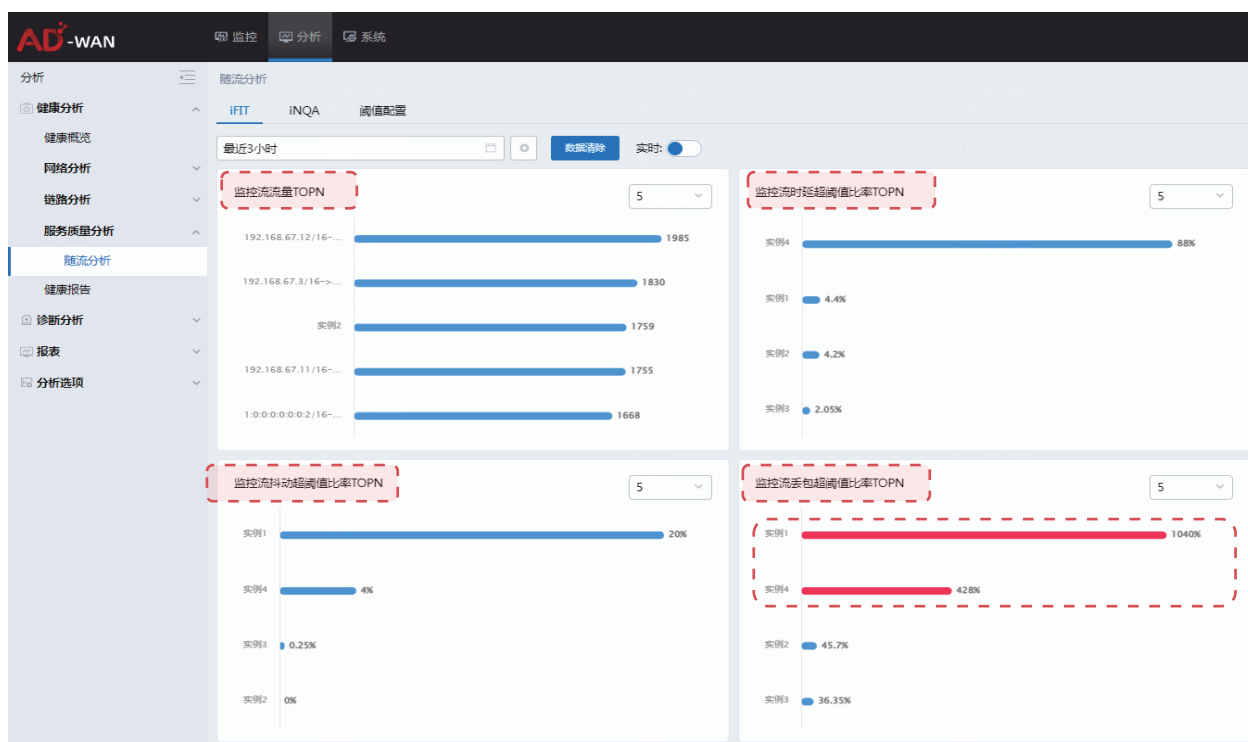
配置监控设备信息

主动运维

管理员针对关键业务可开启iFIT检测。分析组件通过业务流SLA的TOP排名方式，多维度展现监控区域内的业务流转发质量信息，实时、全方位的监控网络运行状态，保障网络运行质量。

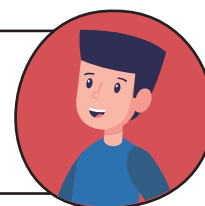


分析组件（Analyzer）基于实际业务流，实时展示现网流量的性能数据变化(流量、时延、丢包、抖动)。

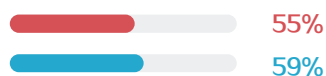


11

当设备或链路中实际业务流的SLA数据超阈值时，分析组件会将其标红，方便用户直观的监测到网络性能质量变化。



故障快速定界



当业务流所经过的设备或链路的SLA数据超过设定的阈值时，业务流的拓扑转发路径上的相应设备和链路会自动染色标红，依次标识故障位置，达到故障快速定界的目的。

配置实例（端到端逐点）

监控参数

* 实例名称: 3

* 测量周期: 10s

全局下一跳IP: 请输入全局下一跳IP

* 实例描述: 实例3

* 测量模式: 逐点

* 老化系数: 30

阈值配置

配置测量阈值

* 端到端时延阈值(us): 2000

* 端到端抖动阈值(us): 2000

* 端到端丢包阈值: 2000

* 逐点时延阈值(us): 2000

* 逐点抖动阈值(us): 2000

* 逐点丢包阈值: 2000

超阈值详情

基本信息

开始时间: 2022-06-02 13:59:50

结束时间: 2022-06-03 12:59:50

最大时延: 9.57ms

平均时延: 3.45ms

平均抖动: 6.81ms

累计丢包数: 2644441

实例描述: 实例3

超阈值统计

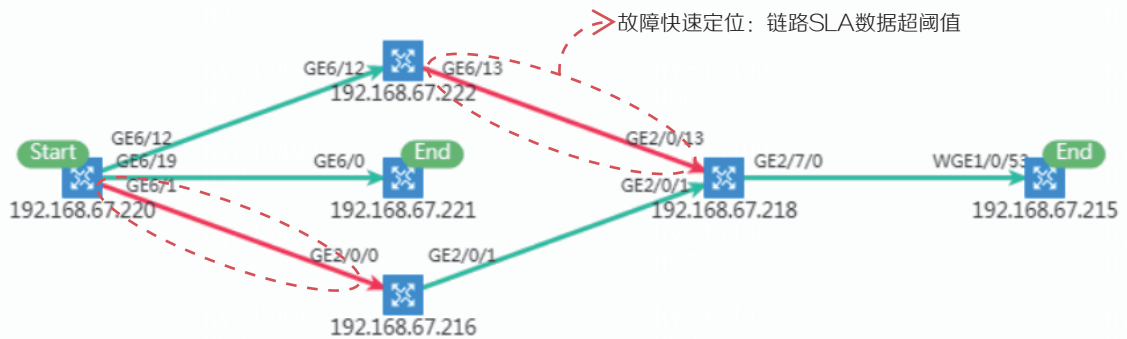


● 时延超阈值次数: 22

● 抖动超阈值次数: 44

● 丢包超阈值次数: 0

链路故障



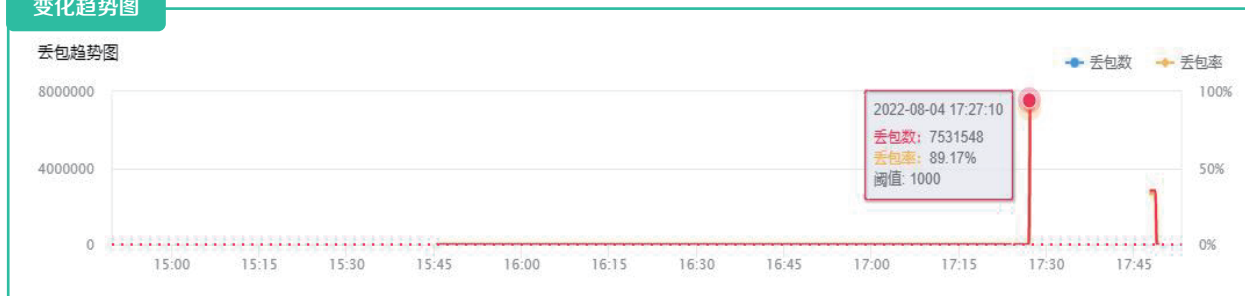
节点故障

故障快速定位: 设备SLA数据超阈值



支持展示流量、时延、抖动、丢包趋势图。

变化趋势图



还原业务转发路径，辅助用户进行故障快速定界。展示业务流实际拓扑转发的逐段链路、逐个设备的SLA实时数据；还原业务流所经的拓扑路径，对时延、丢包越限的链路、网元、端口进行染色预警；基于染色（红色）的网元、链路或端口，查看SLA指标的变化趋势。

方案亮点

网络多维可视

通过概览、拓扑方式，多维度展现数据面相关业务质量、流量信息，帮助用户快速了解当前网络运行状态。

业务路径实时可视

提供IP、VPN业务级的端到端和逐点测量，通过拓扑识别业务经过的隧道、网元等信息，快速还原实时业务路径。

智能故障定界定位

基于业务流级的端到端检测，快速定界网络故障。基于业务流级的逐点检测，快速定位故障点。

—— 编委 ——

王永伟 宋焕启 杜鑫 胡发明 李鑫 刘冠池 曲进 李月光
黄杰殊 冯敬伟 王伟峰 李志安 牛淑强 彭飞 胡梦梦

—— 顾问 ——

陈友琨 黄小东 蒋文栋 赵晓丹 刘恒胜 张刚
张延杰 陈国华 朱萍

—— 美术编辑 ——

郑晓兰 龙厅 张欣岩

广域网管理与运维产品 × 资料开发部联合出品

Copyright © 2022 新华三技术有限公司 版权所有，保留一切权利。