ICS

团　　体　　标　　准

XXXXXXXX

教育城域网网络技术要求

Educationalmetropolitanareanetworktechnicalrequirements

（征求意见稿）

20xx-xx-xx 发布　　20xx-xx-xx 实施

中国互联网协会　　发 布

目录

前　言

本文件提供了教育城域网技术指导，包括网络架构、出口安全、柔性网络、IPv6 业务部署、智能运维和园数融合。

本文件适用于参与组建教育城域网的各级组织。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由中国互联网协会提出并归口。

本文件起草单位：

本标准主要起草人：

教育城域网网络技术要求

1 范围

本文件提供了教育城域网技术指导，包括网络架构、出口安全、柔性网络、IPv6 业务部署、智能运维和园数融合。

本文件适用于参与组建教育城域网的各级组织。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

序号	标准编号	标准名称
1	IETFRFC2119	RFC中用于指示需求级别的关键词（KeywordsforuseinRFCstoIndicateRequirementLevels）
2	IETFRFC7348	VXLAN（VirtualeXtensibleLocalAreaNetwork)
3	IETFRFC7209	以太网 EVPN（RequirementsforEthernetVPN)
4	IETFRFC7432	BGP 基于 MPLS 的以太网 VPN（BGPMPLS-BasedEthernetVPN）

3 术语、定义和缩略语

3.1 术语和定义

本文件没有需要界定的术语和定义。

3.2 缩略语

下列缩略语适用于本文件

序号	词语	解释
1	SDN	SDN 软件定义网络（softwaredefinednetwork）

2	NAT	NAT网络地址转换（NetworkAddressTranslation）
3	FW	FW防火墙（Firewall）
4	SSL	SSL安全套接层(SecureSocketsLayer)，
5	IPSec	IPSec协议安全性(InternetProtocolSecurity,Internet)
6	VLAN	VLAN虚拟局域网(VirtualLocalAreaNetwork)，
7	VXLAN	VXLAN虚拟扩展局域网(VirtualeXtensibleLocalAreaNetwork)

4 教育城域网网络架构

教育城域网包括有线部分和无线部分，有线部分由接入，汇聚，核心三层设备组成，搭配城域网SDN控制器。无线部分由无线AC、无线AP组成。

整体网络架构如下：

（1）接入到汇聚使用VLAN进行联通，在汇聚层设备上，不同VLAN映射到不同Vxlan进行隔离，同时汇聚和核心设备之间运行Vxlan构建overlay网络，构建一个逻辑上的大二层网络，同时采用分布式L3网关并通过可靠的机制有效地抑制广播风暴。

（2）策略管理上采用了面向用户的分组模式，将属性或者访问权限相近的用户分到一个安全组中，同时也将服务器侧的资源划分到安全组进行统一管理。策略定义时，基于可视化的SDN控制台方式实现，简单直观。

（3）基于5W1H的灵活的用户认证接入机制，根据who（谁），whose（谁的设备），what（什么设备），when（什么时间），where（什么地点），how（什么方式）多个维度覆盖各种接入场景。用户可根据自己的需求，灵活定制场景，满足自己个性化的需求。

（4）支持用户终端在整个生命周期中mac和IP的强绑定，终端不管移动到哪里，可以做到终端始终绑定唯一固定的IP，满足城域网安全管理需求。

（5）整网的核心是城域网SDN控制器。所有对网络的自动化上线，接入管理，用户组/策略管理，业务配置管理全部在SDN控制器上通过直观的图形化界面完成。SDN控制器将管理员的操作在后台转化为网络设备的具体命令进行下发给设备执行。

在此架构下，为了实现分层设计分层部署，需要将Underlay和Overlay的部分分开进行设计。

4.1 Underlay 网络架构

城域网的Underlay网络系统是一张物理网，采取树形结构部署，分为核心层、汇聚层、接入层，以及无线管理区、网络管理区、出口互联区、安全检查区。其中核心层、汇聚层和网络管理区是最重要的部分，设计中需要重点关注。

各区/层有如下定义和作用：

- 核心层（Spine层）：是城域网数据交互的核心，连接城域网各个部分，负责路由反射、数据高速转发等，通常要部署性能高、稳定性好的交换机，多采用框式中高端交换机。部署于电教馆数据中心。
- 汇聚层（Leaf层）：是城域网用户的分布式网关，负责用户接入、东西向流量转发、南北向流量转发。通常在部署的时候要兼顾成本和性能，根据用户数选用满足成本要求的中低端盒式交换机。在一些对性能和稳定性要求高的应用场景，也可以选中端框式交换机。通常部署于各学校、教育机构的数据中心机房。
- 接入层（Access层）：负责城域网中有线用户接入和无线AP接入，通常选用中低端盒式交换机，端口数量多，不需要支持太多三层功能。接入层区分有线接入层和无线接入层，无线接入层选用的交换机需要支持POE供电，成本会较普通交换机高，所以有线接入层和无线接入层一般会分开部署，避免浪费POE端口。接入层交换机支持通过级联扩展接入端口数量，但是为了支持自动化，对接入层数有一定限制，一般不超过三层。通常部署于终端用户侧弱电间。
- 无线管理区：是城域网内部署无线控制器（后续简称无线AC）的区域。推荐使用独立AC部署，旁挂核心交换机，根据需要管理的无线AP数量和无线用户数量，可以选择一组或多组无线AC来进行管理。建议统一部署于电教馆数据中心机房。
- 网络管理区：用于部署网络管理服务器的区域，如网管系统，AAA认证服务器，SDN控制器等。网络管理区与核心区之间需要采用三层交换机连接，确保IP可达。
- 出口互联区：是城域网内部网络的边界，部署负载均衡设备，负责园区外部WAN网、专网、Internet与城域网内部网络的互通。
- 安全检查区：主要用于部署防火墙等安全检测设备，旁挂核心交换机，可以对南北向和东西向流量进行安全检测。

组网描述：

- 核心层交换机和汇聚层交换机采用堆叠，两两组成堆叠体，保证设备冗余和链路冗余，避免单点故障。核心交换机和汇聚交换机之间采用EVPN协议构建Overlay逻辑组网。
- 接入层交换机双线双归属到对应的汇聚交换机组中，同时接入交换机还可以进行多级级联（一般不超过三层），以满足不同场景下的特殊需求。
- 多速率PoE接入层交换机支持5G/2.5G/1G,可满足大功率高速WiFi6AP的接入。
- 无线网络，无线控制器旁挂在Spine上，无线控制器完成无线终端的认证，无线终端的网关落在Spine交换机上。
- 防火墙旁挂在Spine交换机上，采用聚合连接到两台Spine上，单臂模式，提供跨VRF和内部访问外部网络的安全控制。

- 服务器区提供设备自动化上线、业务部署、认证、管理、运维服务，与Spine三层互通。

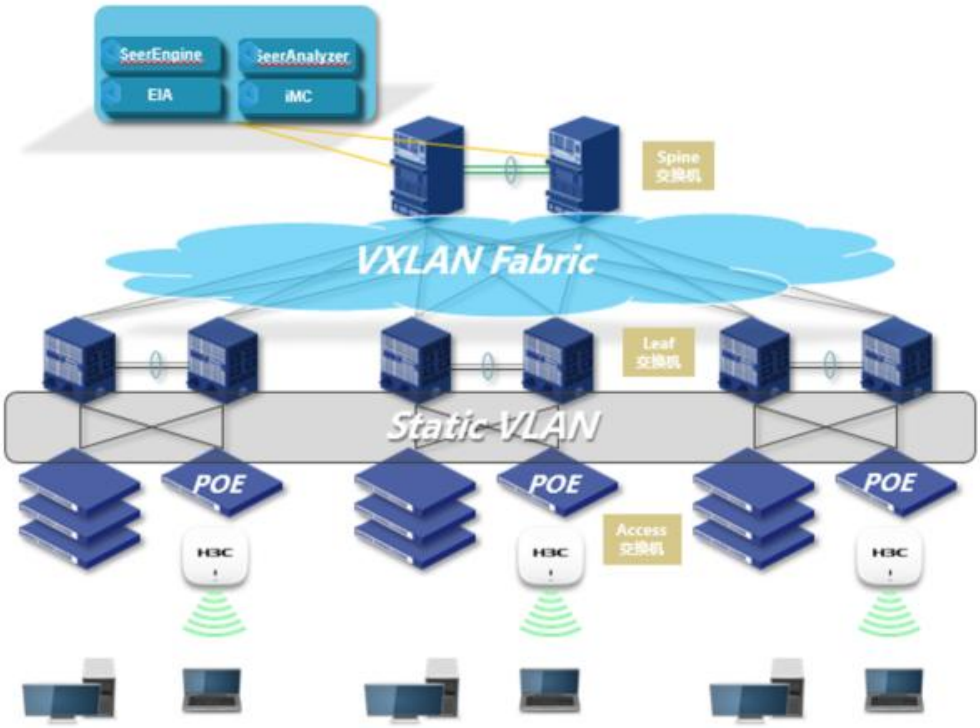
4.2 Overlay 网络架构

整体网络物理架构由核心层、汇聚层以及接入层设备构成，不同点是在核心层与汇聚层设备上启用Overlay技术，同时在内部服务器区部署SDN控制器，并由SDN控制器控制整个网络的运行。具体设计如下。

- 核心层和汇聚层设备之间构建overlay网络，构建一个无状态网络，同时采用分布式L3网关并通过可靠的机制有效地抑制广播风暴，接入层设备采用动态VLAN接入，汇聚层再完成VLAN到VxLAN的映射。
- 策略管理上采用了面向用户的分组模式，将属性相同的设备或者访问权限相近的用户分到一个策略组中，同时也将服务器侧的资源划分到相应的策略组进行统一管理。
- 采用认证系统，根据用户登录的用户名或设备的MAC地址与IP地址绑定，实现用户或设备不管到任何地方，其IP地址不变，从而使得其的安全策略也不便，方便管理运维。
- 方案的核心是SDN网控制器组件。整网的核心是城域网SDN控制器。所有对网络的自动化上线，接入管理，用户组/策略管理，业务配置管理全部在SDN控制器上通过直观的图形化界面完成。SDN控制器将管理员的操作在后台转化为网络设备的具体命令进行下发给设备执行。
- 服务器管理区，SDN控制器/DHCP服务器和网络设备之间三层互联；
- Spine设备与Leaf设备之间连接的链路为underlay链路，配置Spine和Leaf设备之间路由可达；
- Leaf下行口作为用户上线认证点
  - Leaf 与 Access 设备连接的链路为 Leaf 下行接口，Leaf 下行接口配置为认证接口，用于用户认证；
  - 当用户上线时，Leaf 设备通过“下行接口+VLANID”来识别不同的 Access 接口，并且根据不同的登录帐号进入到不同的安全组内；
  - 认证用户通过 DHCPRelay 在 option82 中携带不同的安全组信息，向 DHCPServer 申请分配 ip 地址；
  - DHCPServer 识别安全组信息，分配对应的 ip 地址；
- Access设备VLAN分配规则
  - Access 设备作为二层接入设备，用于连接终端设备。Access 与 Leaf 设备连接的链路为 Access 上行接口，配置为 porttrunkpermitVLANall；

- SDN 控制器会为 Access 设备的每个下行接口分配一个 VLANID，来标记每个终端的位置；从 VLAN101 开始，同一台 Leaf 下，不同下行接口连接的 Access 设备，VLAN 都是从 VLAN101 开始分配，可解决 VLAN 数量的限制问题。

4.3 标准 VXLAN 模型组网



适用于总部（电教馆）+多分支（下属学校）的接入场景，或者多个主园区接入场景。控制组件、分析组件、DHCP 服务器集中部署在一个主园区。AC 可集中部署在电教馆，所有的 AP 都注册到该 AC；也可在每个学校分布式部署，每个学校的 AP 注册到各自的 AC。

SDN 方案可以实现无状态网络、策略随行、网随人动、有线无线一体化、虚拟网络隔离、业务按需交付、设备自动部署、园区一键启动等全部方案亮点。

5 出口安全

5.1 数据安全

数据安全是在数据的整个生命周期中保护数据免受未经授权的访问、损坏或盗窃的做法。这个概念涵盖了信息安全的各个方面，从硬件和存储设备的物理安全到管理和访问控制，以及软件应用程序的逻辑安全。它还包括组织政策和程序。

数据安全主要分为三个方面：数据的传输加密、数据传输端点安全、数据传输通道安全和数据传输的访问控制。

5.1.1 数据传输加密

数据传输过程的数据加密，是确保数据传输安全最有效的技术之一。数据传输加密包括网络通道加密和信源加密，其中网络通道加密包括基于 SSL 和 IPSEC 协议的 VPN 技术，依托协议中的加密和认证技术，实现对网络数据包的机密性和完整性保护，满足移动办公接入、安全组网等需求。信源加密会在数据流动之前先应用加密技术进行加密，在接收端对加密的数据进行解密。每一次两点之间的数据传输过程，都会有加密及解密的过程，一个数据到达目的地之前，可能会经过很多的传输链路，也会经历很多加解密的过程。在线加密技术可以有效确保在网络传输过程的数据流是处于非明文状态，纵使被黑客拦截，也可以有效保障数据安全性，防止非授权用户的搭线窃听和入网，以及数据传输过程中被窃取和篡改。这是比较成熟的技术方案，但在实践应用过程，需要结合以下要点综合全面考虑环境部署。

数据机密性

数据传输过程的数据机密性，即传输的数据不能明文，这是数据传输安全最基本的要求。常见的数据加解密算法有以下几种：对称算法(国产算法 SM1、SM4，国际算法 DES、3DES、AES)，非对称算法（国产算法 SM2，国际算法 RSA）以及哈希算法(国产算法 SM3，国际算法 SHA512)。对称算法加解密优点是加密解密的速度快，适合于大量数据的加密；非对称算法的加解密效率低，一般也没有必须用于大量数据的加密，通常可以用于数据加密秘钥交换的加密。一般数据传输过程，采用 TLS、SSH 等加密协议，可以认为数据传输过程中数据保密性合规。

这些加密算法应用非常成熟，组织在应用加密技术时，不能以技术至上，需要从整个组织的角度，综合考量技术与经济效率的平衡，围绕“价值-风险”双元统一的风险管理思想，在保障数据传输安全基本要求的前提下，做出适合组织实际应用的决策。组织并不会使用单一的加密技术，往往会各类技术混合使用、互补优缺点使数据的传输更加安全。

数据完整性

数据传输过程的数据完整性，可以通过校验技术或密码技术来检测包括鉴别数据、业务数据、审计数据、配置数据、重要个人信息、网络数据等数据，确保数据正常传输、不掉包、传输过程未被篡改以及非授权访问。数据传输过程一般会通过协议来实现数据报文的完整性校验。如数据传输应用 TLS、SSH 协议，会通过 MAC 来校验，可以认为数据传输过程中数据完整性合规。

数据可用性

数据传输过程的数据可用性，主要为了保障对数据的持续访问以及当数据遭受意外攻击或破坏时，可以迅速恢复并能投入使用。具体包括为了避免网络设备以及通信线路出现故障时引起数据通信中断，针对关键链路采用冗余技术设计等手段增强数据访问的可靠性；为保障应用场景下的业务连续性，实现

冗余系统的平稳及时切换，快速恢复运行，尽可能减少数据传输的中断时间，例如通过磁盘阵列、数据备份、异地容灾等手段，以规避硬件故障、软件故障、环境风险、人为故障、自然灾害等风险，确保合法用户可以对信息和资源的顺利的使用。

近两年来，在政策驱动和需求牵引的共同作用下，隐私计算技术创新与落地应用快速推进。隐私计算是涉及密码学、统计学、人工智能、计算机硬件等多学科交叉融合的技术体系，具体是指由两个或多个参与方在不泄露原始数据的前提下，通过硬件可信执行环境、联邦学习、多方安全计算等技术手段，保障数据在使用、加工、传输、提供、公开等数据处理活动中的“可用不可见”，保护数据不透明、不泄露、无法被恶意攻击及被其他非授权方获取，同时满足数据开放共享和数据安全保护的双重要求，最终产生超出自身原始数据的更高价值。

5.1.2 数据传输端点安全

一般来说，应用加密技术能够有效确保数据存储安全。但是在实践中，对所有数据存储使用加密解密技术，会影响业务数据访问时效性，尤其是高频交互数据。因此，通过对数据传输端点搭建有效的安全防护体系，选取关键增强点进行加密，也是组织在实践中应用比较多的数据安全方案，主动防御数据不被篡改或泄露。

应用服务器到数据库

数据可分为结构化数据和非结构化数据，结构化数据存储于数据库，例如组织的人事资料、财务数据、销售采购数据等，一般会存储于数据库。数据库是一个应用系统、平台系统最核心的部分，随着数据的资产化，组织最重要的资产在于数据库。应用服务器数据流转到数据库，可以进行前置代理加密以及后置代理加密技术在数据出口第一时间进行数据加密。数据库加密网关，是数据库前置代理加密技术的一种，一般是独立的组件产品，部署在数据库服务器及应用服务器之间，解析数据库协议，在数据保存到数据库之前对敏感数据进行加密，并将密文存储于数据库中，从而起到保护数据安全的效果。

应用服务器到互联网

常见的应用服务器系统有 Web 服务器、FTP 服务器以及邮件服务器，这些服务器均需要发布到互联网让用户进行访问。Web 服务器通过 HTTP 协议规范了浏览器和 Web 服务器通信数据的格式，FTP 服务器通过 FTP 协议实现服务器与客户端之间的文件传输及共享，邮件服务器则通过 SMTP 及 POP 协议与客户端进行收发邮件。但 HTTP 协议、FTP 协议是以明文方式进行数据传输，没有提供任何方式的数据加密。如果攻击者截取终端与服务器之间的报文，将存在巨大的的安全隐患。因此，目前多数服务器会在应用层协议与 TCP/IP 协议间，增加 SSL 协议，保障数据传输安全合规。

应用服务器到终端

除了上述通过安全通信协议来确保应用服务器到互联网的数据传输安全之外，组织还会通过安全代理网关来进一步加强访问终端与应用服务器之间的传输安全。常见的安全代理网关，如 CASB 代理网关，

是利用云访问安全机制的委托式安全代理技术，不需要改造目标应用，通过适配目标应用，对客户端请求进行解析，并分析出包含的敏感数据，结合用户身份，通过安全策略对访问请求进行脱敏等控制来进行数据传输的安全管控。

5.1.3 数据传输通道安全

代理服务器到终端

基于 SSL 协议的传输加密技术主要应用于传输层的安全，采用密码算法和数字证书认证技术，确保登录用户的身份安全可信，以及数据传输的机密性、完整性，满足固定台式终端、移动办公用户、移动智能终端等不同场景、不同平台的可信接入需求。

代理服务器到互联网

https 在 http 的基础上加入了 SSL 协议，SSL 依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。可信安全 SSL 站点证书用于标识网站真实身份，它能够实现网站身份验证，确保用户访问网站的真实性，确保用户所浏览的信息是真实的网站信息，能有效防范假冒网站和钓鱼网站。

代理服务器到代理服务器

基于 IPSEC 协议的传输加密技术主要应用于网络层 IP 包传输的安全，包括传输模式和隧道模式，也就是网络层的安全传输。采用密码算法对用户报文进行加密，采用 ESP 协议对用户报文进行重新封装，确保用户信息传输安全，满足不同分支机构之间以及分支机构与总部之间的加密组网需求。

5.1.4 数据传输访问控制。

除了数据传输过程中对数据本身的安全考量，对数据进行访问控制管理，也能够有效控制数据传输安全。数据传输访问控制可以防止非授权人员访问、修改、篡改以及破坏系统资源，防止数据遭到恶意破坏。访问控制主要有以下实现方式。

身份认证

身份认证访问控制是指通过身份认证技术限制用户对数据或资源的访问。常见的身份认证方式，包括口令认证技术、双因素身份认证技术、数字证书的身份认证技术、基于生物特征的身份认证技术、Kerberos 身份认证机制、协同签名技术、标识认证技术等。常见的身份认证访问控制应用场景，包括：已经离职以及在职时采用生理特征进行访问控制的员工，应于离职后及时删除基于生物特征录入的信息；外部人员访问时应进行身份认证来进行访问控制；数据处理中心的物理安全也应进行身份认证来进行访问控制，如机房门口应配置电子门禁系统等技术手段进行访问控制。

权限限制

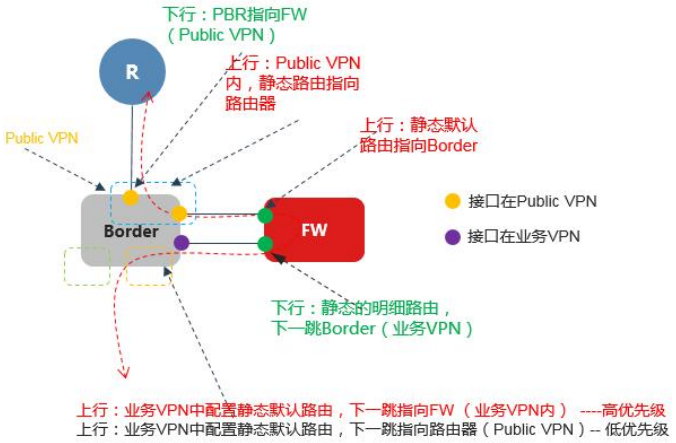
权限限制访问控制是指基于最小特权原则、最小泄露原则、多级安全策略来限制用户对数据或资源的访问。常见的权限限制访问控制方式，包括：访问控制表、访问控制矩阵、访问控制能力列表、访问控制安全标签列表等，例如，通过对比用户的安全级别和客体资源的安全级别（绝密、秘密、机密、限

制以及无级别）来判断用户是否有权限可以进行访问；对用户进行角色划分，并授予管理用户所需的最小权限，实现管理用户的权限分离；对系统资源的访问是通过访问控制列表加以控制的，即当用户试图访问资源或者数据时，系统会控制用户对有安全标记资源的访问。

端口开放访问控制

服务器传输数据过程，除了需要目标 IP 地址外，还需要开放一些服务端口。通过系统的端口，能够使运行不同操作系统的计算机应用进程互相通讯。端口分为公认的默认端口和动态端口。默认端口是用于明确某种服务的协议，例如默认情况 2 端口是分配给 FTP 服务，25 端口分配给 SMTP 服务，80 端口分配给 HTTP 服务；动态端口则是用于动态分配给一些系统进程或应用程序。应用服务器应根据提供服务的需求，有限开放对应端口，限制不必要的端口开放，从而有效限制数据传输泄密的风险。

5.2 FW 正常时的上下行路径规划

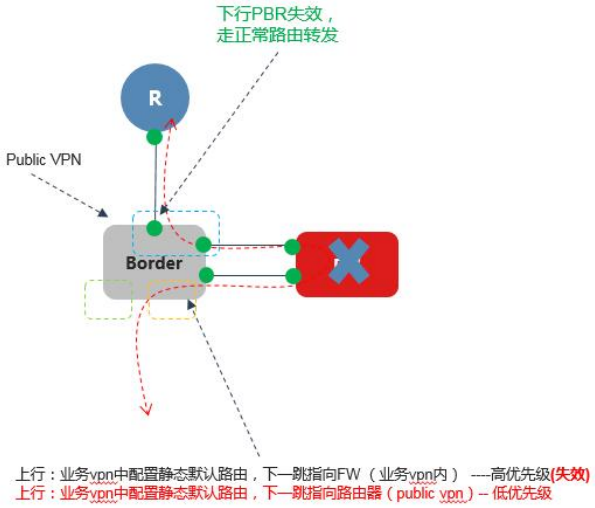


FW 正常时上下行路径规划

- 上行：业务流量到Border上，Border在业务VPN内查找静态默认路由，由于下一跳是FW的路由优先级高，故Border将报文转发到FW。FW上处理完后，根据静态默认路由，将报文转发到Border。Border在PublicVPN中，根据默认静态路由，将报文转发给路由器。
- 下行：外网回来的报文到Border后，Border通过匹配PBR，把匹配PBR的报文转发到FW。FW处理完后，根据配置的静态明细路由（安全组所在的网段）将报文转发到Border。Border在业务VPN内，查找路由，将报文转发到对应的Leaf设备。

注意：需要事先将 PublicVPN 跟业务 VPN 进行路由互引。

5.3 FW 故障时的上下行路径规划



FW 故障时上下行路径规划

- 上行流量：FW故障时，Border上的默认静态路由的下一条是路由器，故Border将业务VPN流量发给到路由器。
- 下行流量：由于FW故障时，Border配置的PBR失效，故Border走正常的路由转发，将报文转发到对应的Leaf设备。

如果 FW 为两台，需要 FW 运行 VRRP。

- 上行路径中，Border上的静态默认路由的下一跳是VRRP组的虚IP地址。这样，当其中一台FW故障，由于下一跳是VRRP的虚IP地址，Border不感知，仍会把报文转发到FW，由正常工作的FW做后续处理。
- 下行路径中，Border上的PBR配置的下一跳是VRRP组的虚IP地址。这样，当其中一台FW故障，Border不感知，仍会把报文发给FW，由正常工作的FW做后续处理。

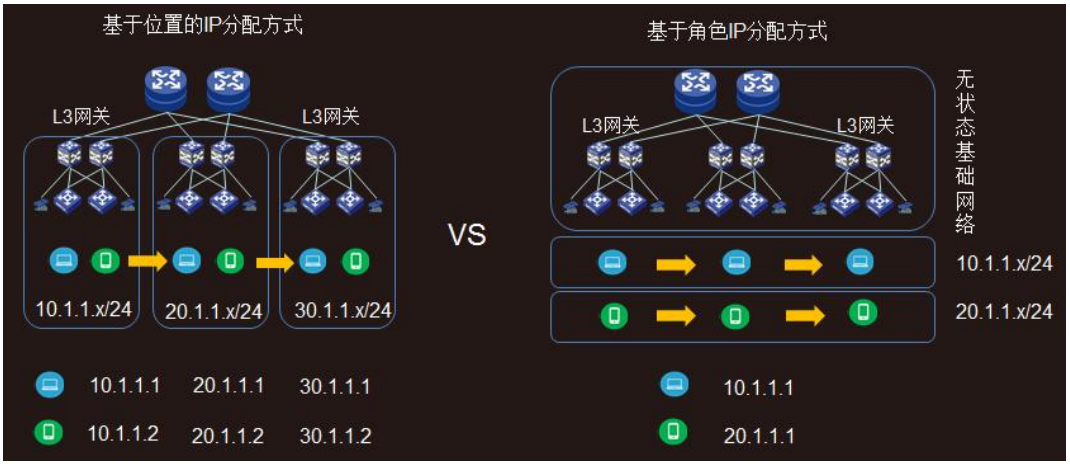
6 柔性网络

柔性一方面指网络架构本身非常灵活，业务部署（应用/终端）可以做到与位置无关；另一方面指彻底改变传统网络通道就绪，终端和人根据位置匹配通道的模式，将人和应用作为中心，所有网络的资源跟随人和应用移动。柔性具体涵义包括如下几个亮点：

6.1 无状态网络

SDN 方案中“位址分离”位指位置，“址”指 IP 地址，“位址分离”就是 IP 地址与位置解耦，让 IP 地址可以在任意位置接入，无需改变网络的配置。

位址分离



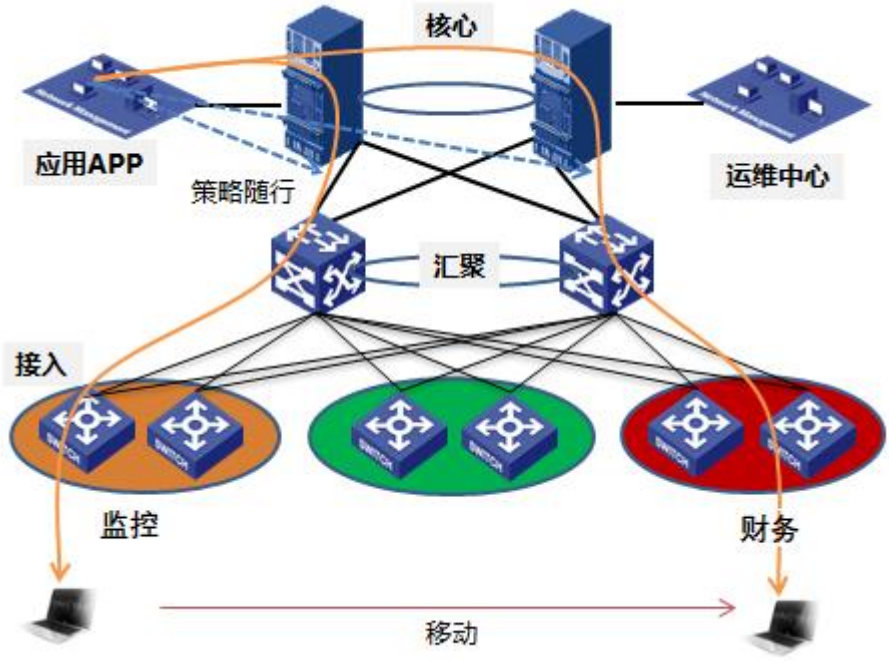
6.2 用户策略随行

策略随行：指用户移动到哪里，用户的体验不变；一般上要实现策略随行，都需要对用户进行分组，传统的分组方式与地理位置紧耦合，同一个用户组位于一个办公区，一个楼层或者一个大楼之内，很难跨越地理的局限。这样用户一旦移动起来，策略实施就非常复杂，想达到策略跟随或者体验一致也非常困难。

SDN 方案策略随行的核心就是“名址绑定”，名址绑定就是用户和 IP 地址一一对应；传统网络用户名和 IP 地址是难以做到绑定的，一方面 DHCP 的方式并不能保证单用户每次获取相同的 IP，静态地址分配的方式又不能保障用户在移动过程中保持相同 IP 能够在不同的位置进行正常的网络连接；SDN 方案中无状态网络本身提供了 IP 任意位置访问的能力，再配合名址绑定实现用户位置发生了变化，IP 地址段也没有变，甚至 IP 地址没有变，针对 IP 的策略也没有变，而这种针对 IP 的策略其实就是针对用户的策略，最终实现了用户的策略随行。

除了用户和 IP 绑定，在某些场合可能不需要做非常强的捆绑，SDN 可以提供业务和 IP 网段的绑定，或者用户组和 IP 网段的绑定，比如：视频监控终端尽管分布在全网任意位置，但可以将其 IP 全部分配在某一个网段之内；又比如财务的人员可能也分布在网络不同的位置，我们也可以将其分配在同一个网段内；最终实现通过 IP 段标识用户组或业务组。

策略随行

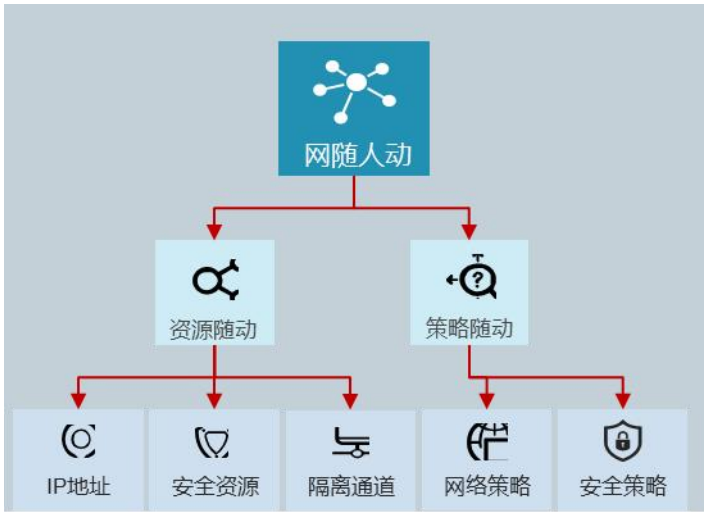


6.3 网随人动

传统园区网络首先是通道就绪，终端根据最初的规划，接入到相关接入交换机的端口，从而实现VLAN等权限和终端的匹配，一方面不能够解决用户和终端任意位置接入权限分配的问题，另外终端接入位置也受限制。

SDN将人和应用作为核心，所有网络的资源跟随人和应用移动，用户在哪里接入、资源就下发到哪里，真正体现柔性网络的网随人动的特点。

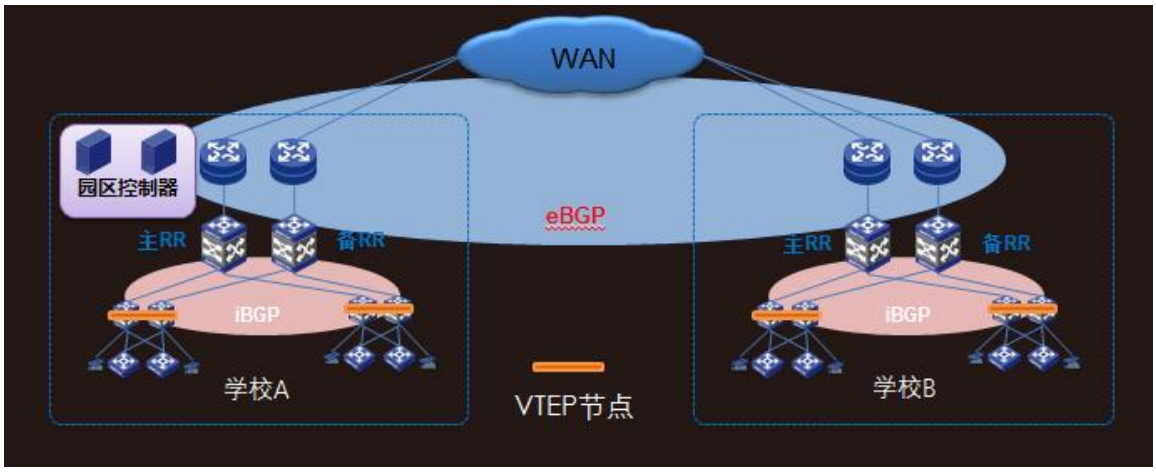
网随人动



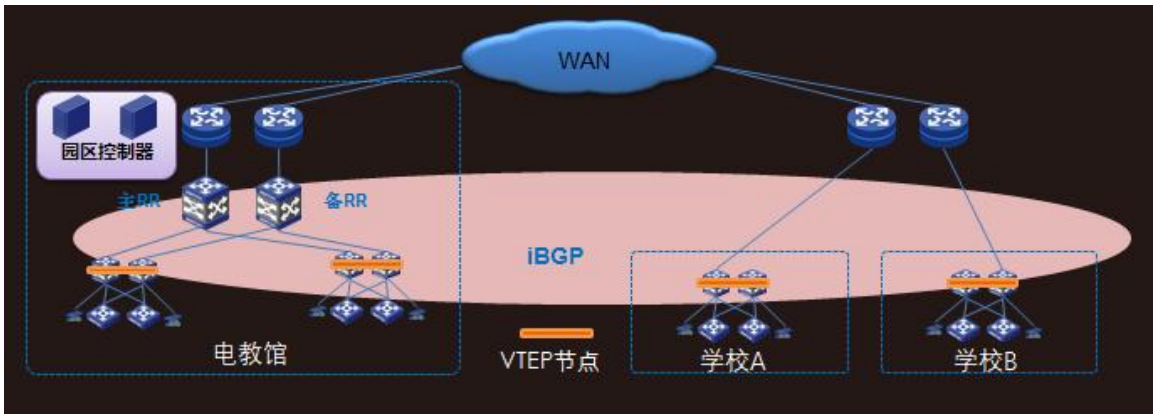
6.4 无差别网络

园区分支无差别：SDN 无状态网络、用户策略随行、网随人动不仅仅可以在单园区实现，还可以跨园区、在园区分子之间实现，满足业务、用户在更大范围内移动化办公，符合电教馆的多分支架构。

跨园区组网



园区分支无差别组网



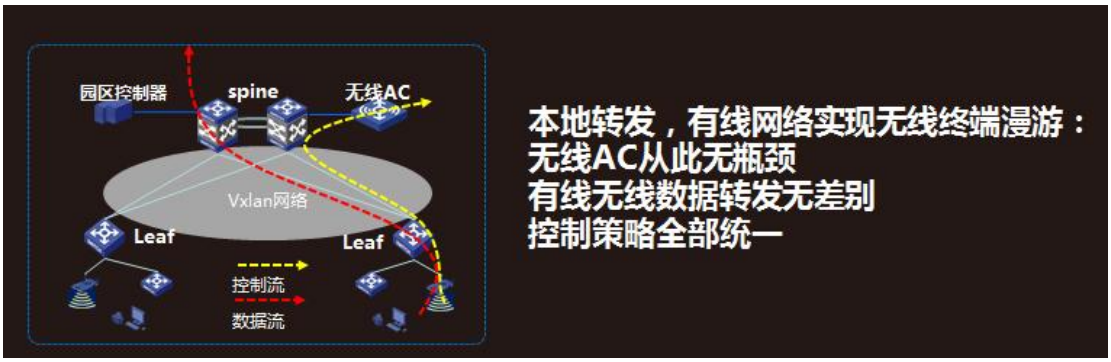
6.5 有线无线深度统一

SDN 的有线无线深度融合网络采用如下方式极大解放了 AC 和 AP，面向未来的高速无线时代。

- 统一管理：通过统一的 SDN 控制器实现有线无线统一管理。一套管理系统，统一的有线无线拓扑展示，有线无线用户统一认证，统一的基于 5W1H 划分用户组。

- 统一转发：AC 仅负责控制和管理下辖的大量 AP，AP 的数据流量转发不再上 AC，而是本地转发。这样带来两个好处：1）由于 AC 不再负责数据转发，性能瓶颈完全消除，完全顺应将来高速无线的趋势，而且 AC 成本可以大幅降低。甚至将来 AC 完全可以做成软件集成到 SDN 控制器中作为一个功能管控模块。2)从 AP 转发出来的报文不再封装 CAPWAP，而是 802.3 格式的 Ethernet 报文，L3 网关也都设置在交换机上。这样消除了 CAPWAP 的加减封装的处理消耗，效率更高。AP 发送出来的无线流量和从交换机/PC 发送出来的有线流量一模一样，有线/无线流量完全混跑在一起，其他设备无法区分也不需要区分。
- 统一策略：由于无线的数据转发完全从 AC 卸载到交换机上，之前我们策略随行矩阵定义的业务策略完全适用于有线和无线流量，也不需要单独给无线再定义组间访问策略。此外，在 AP 本地转发模式下，依赖有线的无状态网络，解决跨三层漫游的问题，无线终端依旧可以跨整个园区漫游，而且不需要在 AC 侧做复杂的处理。

有线无线融合

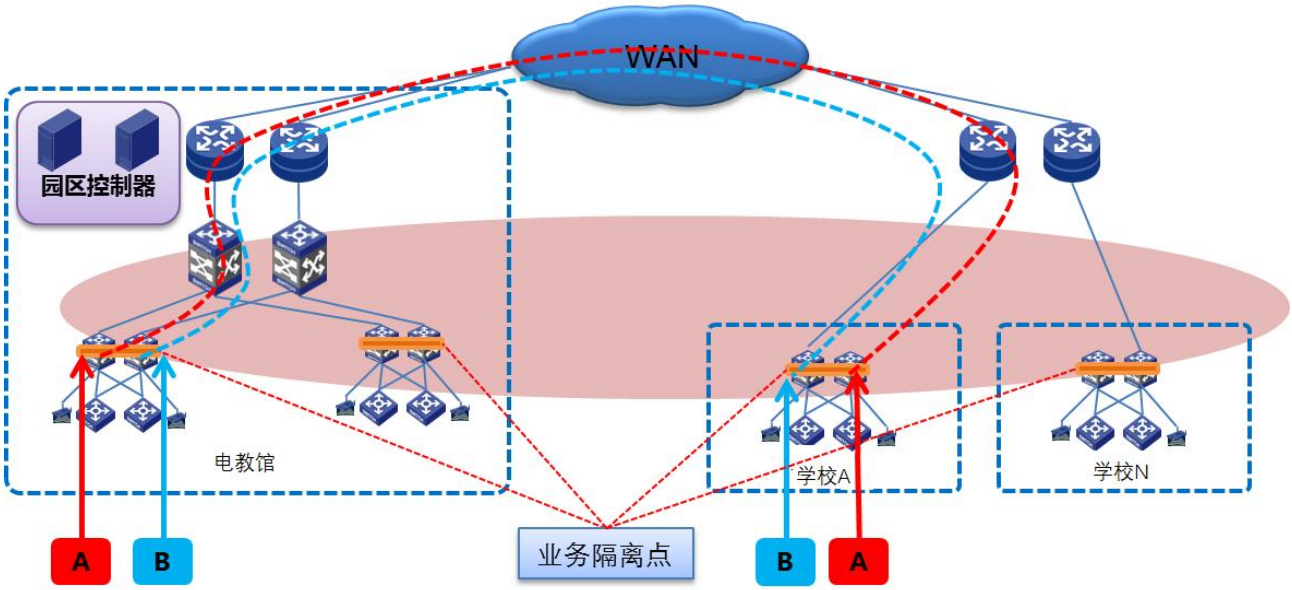


6.6 网络虚拟通道隔离

整网采用 overlay 的技术，天然具备跨广域网的通道隔离能力，相比 MPLS 的隔离方式，VXLAN 的隔离只需要在端点（VTEP）做隔离，不需要全网隔离，端点之间只需要 IP 互通既可。一方面让整个运维节点大幅减少，另一方面端点之间支持多运营商连接，负载均衡可以直接通过 ECMP 来实现，让整个组网清晰、运维更简单。

在隔离方式上，SDN 提供两种隔离方式，一是类似 MPLS 的 VRF 隔离，每个用户组在 VTEP 节点分配不同的 VRF，VRF 之间在路由层面实现隔离，每个用户在 VRF 内通过 VLAN 映射成不同的 VXLAN，最终实现在通道内通过 VXLAN 数据传输，实现隔离。二是 ACL 的隔离方式，因为每个用户组在 IP 分配的时候已经分配在不同的网段，因此不同用户组在接入之后获取的是不同网段的 IP，ACL 隔离相对比较简单，一条 ACL 就可以实现不同用户组之间的网络隔离。

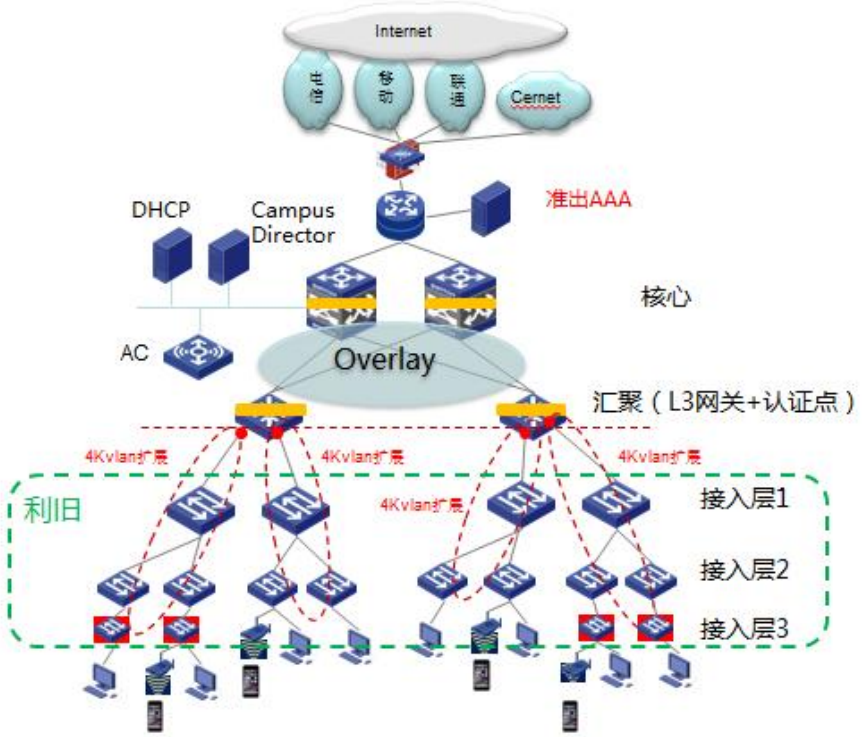
网络虚拟通道隔离



6.7 良好的兼容性

SDN 方案采用了 VXLAN 扁平化组网进行二层隔离，结合分布式网关技术在将原本集中在核心的压力分散到各汇聚层设备上保障了整网的健壮性，提升了网络的性能规格的同时，在控制组件统一管控下实现了策略自动跟随、设备自动化上线等功能，这不仅降低了运维成本，同时实现了自动化，进一步的节省了运维的人力，可以称得上是升级版的扁平化方案，是新建园区的不二之选。另一方面，仅需要汇聚、核心设备支持 VXLAN，在老园区改造中，可以最大程度的保护用户的原有投资（V5、V7、第三方的接入设备），降低用户的改造成本，真正的做到物尽其用。

良好的兼容性



6.8 弹性扩展，扩容无忧

SDN 方案使用标准的 EVPN 协议（RFC7348+draft-sd-l2vnp-evpn-overlay，RFC7209，RFC7432）作为 VXLAN 的控制平面构建了分布式网关的组网模型，解决了 VXLAN 依赖于数据平面的 flood-and-learn 学习远端地址信息所带来的 BUM 报文广播问题；避免了采用集中式网关组网模型下，全网的规模受限于核心层网关单台设备的标箱规格的局限；使得园区内的流量可以按照最优的路径进行转发，避免了绕行及对核心设备的冲击；同时借助 EVPN 协议完成园区网络的初始化配置，避免了过多的人为手工配置，是自动化部署的技术基础。正因如上的诸多好处，使得 EVPN 成为园区网的控制平面首选。采用了 EVPN 的园区网络的规模可以进一步扩展，满足各行业网络规模的不断发展。

此外园区网控制组件支持分布式部署模式，当园区规模发生变化的时候，通过增加相关组件 license，将园区控制组件的各组件依据所需的性能要求进行升级或扩容，采用分布式部署模型，满足对跟大规模园区的管控需求。

6.9 IPv4/IPv6 双栈部署

SDN 方案目前推荐部署 IPv4/IPv6 双栈方式承载 IPv6 业务：

1、IPv4/IPv6 双栈部署方式同 IPv4 部署方式；

2、网络管理、underlay 网络仍然采用 IPv4；

3、Overlay 网络同时承载 IPv4/IPv6 流量；

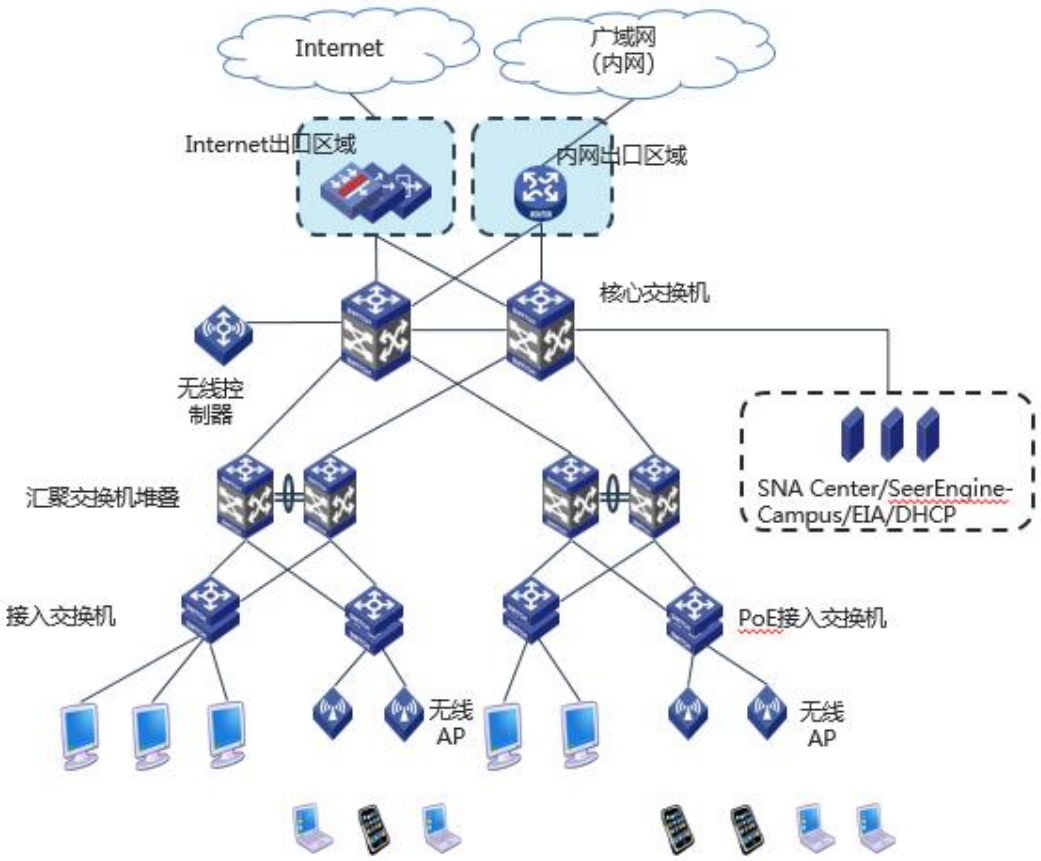
4、用户 IPv4MACPortal 认证成功后，直接转发该用户的 IPv6 流量；

7 IPv6 业务部署

7.1 典型组网

当前 SDN 可以支持 underlay 为 IPv4 场景；Overlay 可以为 IPv6 单栈，也可以是 IPv4、v6 双栈。IPv6 对硬件资源消耗几倍于 IPv4，在非微分段模式下启用 IPv6 的组间策略会让网络难以为继，所以建议在微分段模式下使用 IPv6 的组间策略能力。

SDN 部署 IPv6 典型组网



7.2 IPV6 部署设计

7.2.1 IPv6 网络设计

IPv6网络的部署一般考虑以下两种方式：

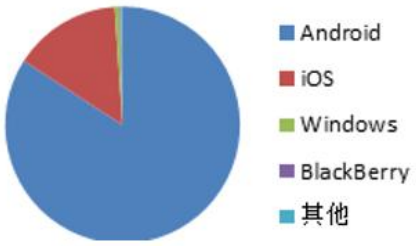
- 与IPv4共存一段时间作为过渡，双栈部署

- 去除IPv4，仅保留IPv6，为IPv6单栈网络

IPv6地址的分配也存在多种方式，可以通过DHCPv6服务器自动分配，也可以通过网关无状态方式。多数终端两种方式都可以支持，但无线终端略有不同。

无线终端主流的操作系统是IOS系统和Android系统，这两种系统的终端获取IPv6地址方式见下图：

	IOS系统	Android系统
DHCPv6	支持	不支持
网关无状态	支持	支持
默认双栈	是	是
双栈下未获取IPv4地址时可获取IPv6地址	可获取	不可获取
协议栈选择	支持	支持



为兼容两种操作系统无线终端，无线IPv6部署限制：

- 需为无线终端同时提供IPv4、IPv6地址
- 无线终端通过网关无状态分配方式获取IPv6地址

7.2.2 IPv6 路由学习

内网路由同步：园区网终端经过认证后，会在LEAF设备上上线，生成IPv6的EVPN路由信息。

Leaf设备上终端的128位主机路由（ND）可以通过EVPN协议同步到Spine设备上，并加入到IPv6路由表中

7.2.3 DHCPv6Server 部署

终端 IPv6 支持度：

	Windows 系统	MAC 系统	Andriod 系统	IOS 系统
DHCPv6	Y	Y	N	Y
网关无状态	Y	Y	Y	Y
默认双栈	Y	Y	Y	Y
NDRDNSS	Y	Y	Y	Y

备注：

- Android系统需先获取IPv4地址，然后才能通过网关无状态方式获取IPv6地址
- NDRDNSS指通过ND的RA报文通告IPv6DNSServer对应IPv6地址
- 终端IPv6支持度来源于全球IPv6测试中心《2019IPv6支持度报告》

在交换芯片中，IPv6主机路由表项占用资源是IPv4主机路由表项占用资源的2倍或4倍（取决于交换芯片），为了减少IPv6临时地址数量，建议网络IPv6地址分配方式：

- 有线业务，推荐PC采用DHCPv6申请地址
- 无线业务，推荐采用网关无状态地址分配方式：Android手机不支持DHCPv6

8 5G和教育城域网的融合

8.1 5G推出关键技术

2019年6月，世界移动大会在上海召开。大会举行了“5G赋能教育·智慧点亮未来”分论坛，发布了《5G+智慧校园白皮书》，标志着5G技术在教育领域应用的开启。《5G+智慧校园白皮书》对5G的关键技术进行了阐释，主要包括：①虚拟局域网（VirtualLocalAreaNetwork，VLAN），是指通过使用通用性硬件和虚拟化技术，取代通信网络中私有、专用、封闭的网元，搭建“统一通用硬件平台+业务逻辑软件”的开放架构，加快网络部署和调整的速度，降低业务部署的复杂度。5G的VLAN技术可实现终端与企业网同处于一个局域网内，支持企业用户对终端的灵活管理。②网络切片，是指将物理网络划分为多个虚拟网络，每一个虚拟网络可以满足不同的服务需求；同时，为不同垂直行业、不同客户、不同业务提供相互隔离。③可定制网络，是指结合行业需求，规划面向场景的5G网络切片样板，赋能垂直行业，提供可定制网络，满足不同用户需求。④移动边缘计算（MobileEdgeComputing，MEC），是指在靠近数据源或用户的地方提供计算、存储等基础功能，并为边缘应用提供IT环境服务和云服务。相较于集中部署的云计算服务，MEC解决了时延过长、汇聚流量过大等问题，可为实时性和带宽密集型业务提供更好的支持。此外，MEC在网络边缘运行，逻辑上并不依赖于网络的其它部分，故能为敏感型业务提供通信安全保障。⑤毫米波传输，是指波长在1～10毫米之间的电磁波通讯传输。5G数据传输使用24.25～52.6GHz频段，利用毫米波传输大带宽的特性，使数据速率高达10Gbps甚至更多。

8.2 区域教育城域网的“云化”

随着各校对教育网络应用和资源需求的不断增长，区域教育城域网对网络质量也提出了更高的要求，势必造成存储和服务器等硬件设备的快速发展，区域教育城域网“云化”势在必行。“云化”将原有对互联网带宽和网络硬件的需求逐渐转化为对教育应用和资源的需求，强调视频类远程教育、视频会议、网络电视台的低延时、高带宽和广接入。不同学校之间除了用高带宽光纤互联以保证有线网络的高速接

入，还可通过5G无线网络的快速部署，突破传统有线网络和中心机房对地点、用户人数的限制，从而随时随地享受更快捷、更稳定的智慧教育体验。

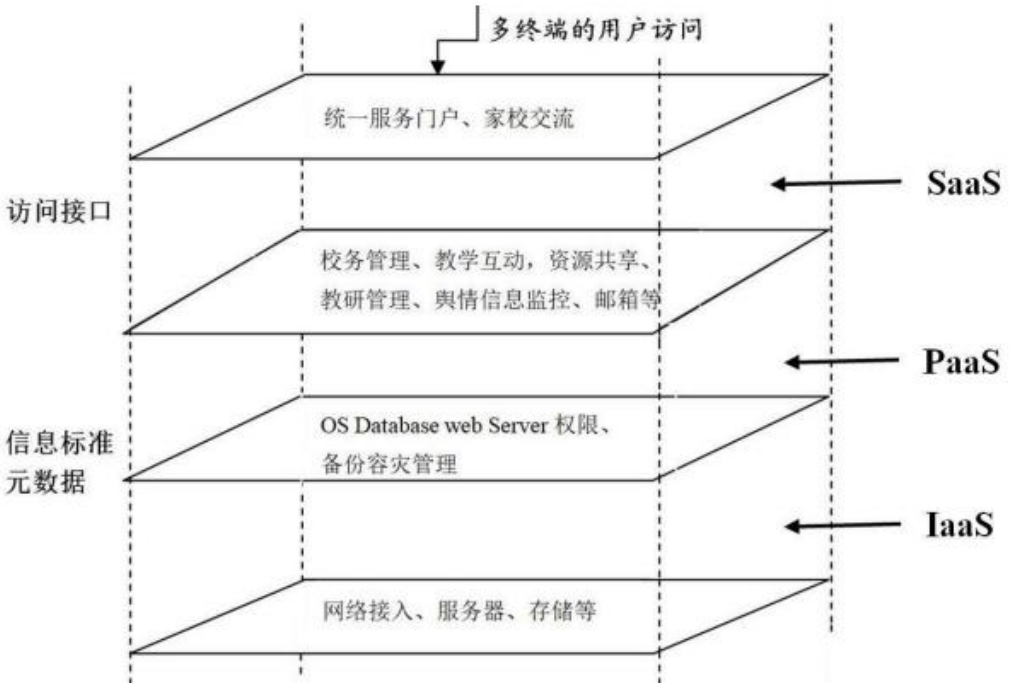
8.3 5G融入区域教育城域网的建设方向

5G网络环境因其大带宽、低延时、较强的边缘计算和管控能力等优势，将成为未来智慧教育环境的基础，并将成为区域教育城域网建设的重要发展方向。结合传统的2G/3G/4G、宽带、Wifi等网络，未来的区域教育城域网将从目前“以语音和数据为核心”转为“以内容和流量为核心”。基于此，5G融入区域教育城域网的建设方向为：①核心网从扁平的集中化架构调整为“中心+边缘”的分布式架构，传统机房被重构为云数据中心，新建或改造边缘基础设施，以满足新设备形态所需的空间、电源、散热、网络配套等需求。②传统网元与虚拟化网元长期共存，多制式混合组网，传统网元容量逐步向虚拟化网络迁移；部署面向服务的虚拟化网络功能，按需生成网络切片，以满足不同用户在不同场景的业务需求。综上所述，5G融入区域教育城域网是以网络功能虚拟化（NetworkFunctionVirtualization，NFV）、软件定义网络（SoftwareDefinedNetworking，SDN）技术为基础，实现资源可全局调度、业务可快速部署、能力可全面开放、容量可弹性伸缩、架构可灵活调整的新一代网络。

8.4 5G融入区域教育城域网的相关设计

5G融入区域教育城域网的特色功能①弹性计算：提供弹性云主机、专用物理机和分布式计算云，以满足用户虚拟机、物理服务器承载业务与分布式计算的各类需求；支持云主机规格变更和弹性伸缩，可实现计算资源的垂直和水平变化。②弹性存储：包括集中存储和分布式存储两类产品，可满足用户不同数据种类、不同数据读取要求、不同数据存储时限的数据存储场景。③网络与分发：包括虚拟私有云（VirtualPrivateCloud,VPC）、弹性负载均衡、云专线接入和内容分发网络（ContentDeliveryNetwork，CDN），服务于安全保障、能力提升和质量保证。④弹性负载均衡：自动将访问流量分发到多台弹性云主机，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。

5G融入区域教育城域网的云服务模式5G融入区域教育城域网具有虚拟化和云化的特点，可以满足区域内行政管理、师生教育教学的需求，其云服务模式如图所示。



5G融入区域教育城域网的云服务模式

（1）基础设施即服务（InfrastructureasaService，IaaS）层

IaaS层提供支持云服务所需的软、硬件资源，包括计算、存储、网络、安全等基础资源，具有弹性可扩展能力，能利用云平台提供数据分布式存储、数据高速并行处理、资源池管理与动态调度、虚拟机建立与多租户管理、数据安全加密、大用户量并发访问、负载均衡与失败转移、容灾和容错等功能。

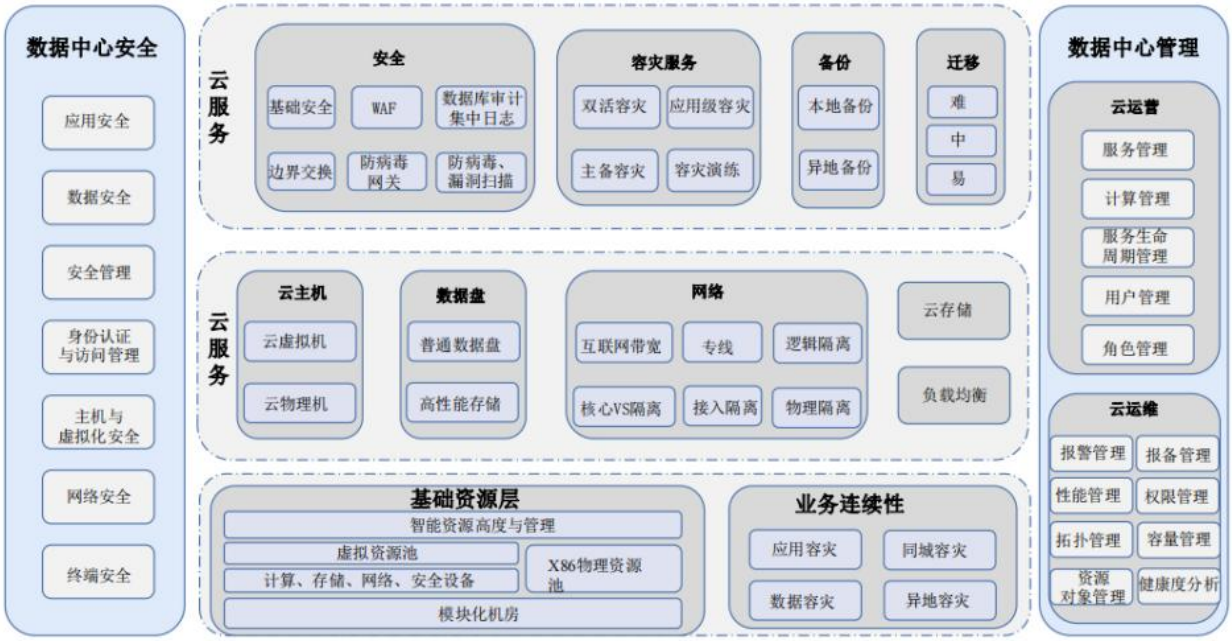
（2）平台即服务（PlatformasaService，PaaS）层基于IaaS层的相关功能，PaaS层提供应用服务云平台，为上层应用提供在线服务接口和相关服务，主要包括：①用户身份和授权服务，负责对整个平台的各类用户进行身份验证与权限分配；②移动访问接口服务，负责提供各个应用系统数据的移动访问接口，对各数据进行加工并实现在移动设备上访问；③开放访问接口，提供平台向第三方开放的基础数据，如用户信息、登录论证、消息访问接口等；④分布式计算与部署服务，为各系统横向扩展提供计算能力增长的支撑，实现系统的统一部署与容灾容错管理。

（3）软件即服务（SoftwareasaService，SaaS）层SaaS层提供区域教育行政管理应用、资源共建共享、教师研修、网络教学管理、家校互动、终身学习、舆情信息监控、邮箱等服务，同时提供云终端设备访问的所有信息服务。

8.5 5G融入区域教育的云服务平台

考虑到未来教育云服务的建设任务重、安全压力大、技术要求高，本研究基于5G融入区域教育城域网的云服务模式，对区域教育的云服务平台进行了设计：各主要模块采用购买服务的方式进行建设、管理和运维，其具体功能的设置可以根据区域教育城域网的实际情况进行增删，特别是基础资源层、云运营、云运维和安全部分的相关功能可以灵活调整。区域教育云服务平台的功能拓扑图如图所示，主要包

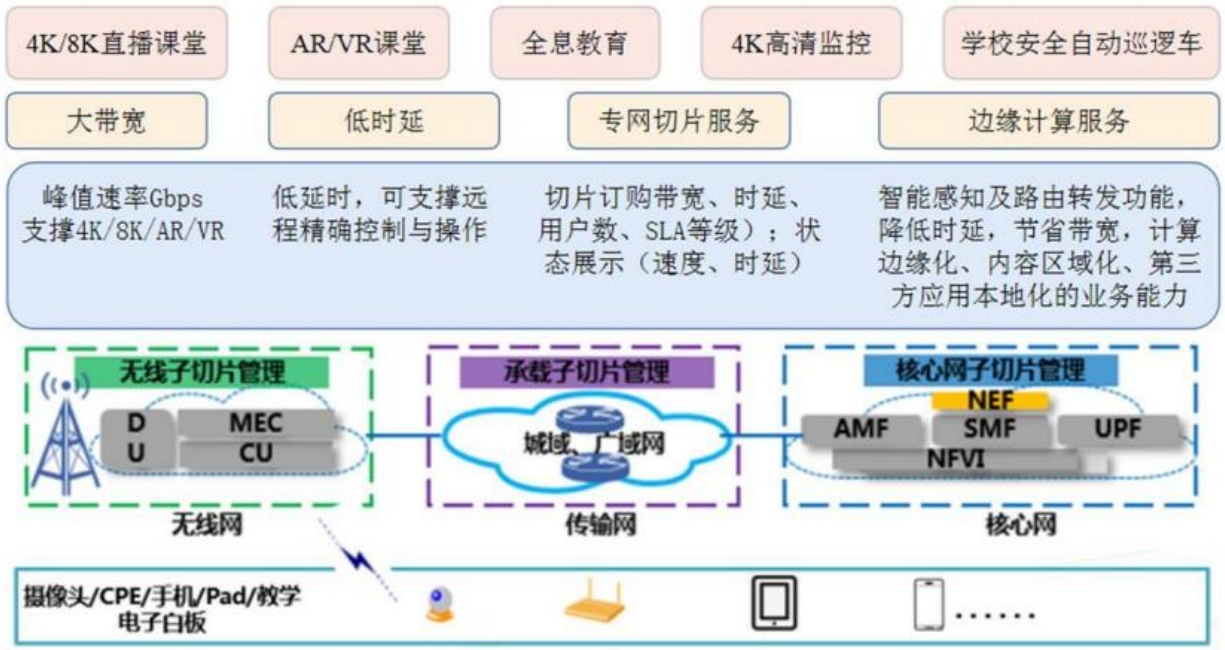
括数据中心安全、云服务、基础资源层、业务连续性和数据中心管理等功能模块，是硬件系统的云运营和云运维框架。



区域教育云服务平台的功能拓扑图

8.6 5G 区域教育城域专网的构建

随着5G时代的来临，沉浸式教育走进真实的课堂，并且更多的教育资源将被传送到贫困地区和偏远地区。相较于4G移动网络，5G通过网络切片技术和边缘计算技术可以更好地满足行业用户的应用需求。而在教育领域中应用网络切片技术和边缘计算技术，可以实现区域教育城域专网的搭建。基于此，本研究设计了基于网络切片技术和边缘计算技术的5G区域教育城域专网架构，如图所示。



基于网络切片技术和边缘计算技术的5G区域教育城域专网架构

在5G区域教育城域专网中，网络切片技术构建了多个专用的、虚拟的、隔离的、按需定制的逻辑网络，来满足业务对网络的不同要求（如时延、带宽、连接数等），并通过全连接使5G、4G、窄带物联网

（NarrowBandInternetofThings，NB-IoT）、专线网络的数据共享，避免造成不同网络之间的数据孤岛；同时，对教师、学生、家长等用户的隐私数据进行本地化传输与存储，以保障用户的数据安全。5G切片基于独立组网（StandAlone，SA）实现，具有以下特征：①基于不同的业务提供不同专网，在调度不同业务时，先保障高优先级业务；②提供业务安全，保障学校的隐私数据安全；③基于业务对专网带宽、时延等网络要求，按需调整学校间（如附属学校、分校）专网，共享4K/8K效果的AR、VR等业务。

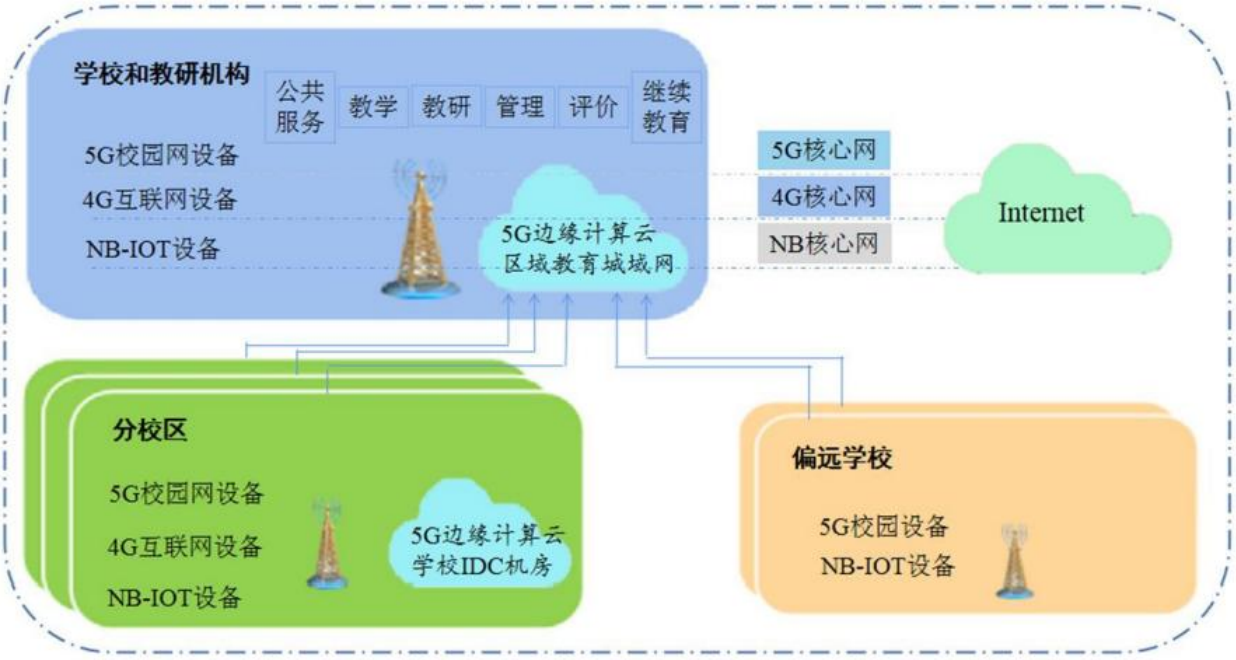
此外，在5G区域教育城域专网的传输网架构中引入边缘计算技术，并在靠近接入侧的边缘机房部署网关、服务器等设备，可以增强计算能力，破解带宽和时延抖动等性能瓶颈，满足不同应用带来的多样化网络需求，从而降低时延、减少回传压力、提升用户体验。

总的来说，5G区域教育城域专网的建设，可实现人脸识别、云桌面、云管理平台、教学平台、资源平台、服务平台、家校沟通平台、社会实践服务平台等智慧应用在云端的部署，并利用5G网络的高带宽、低时延等优势，为用户提供更强大的功能和更优质的体验。

8.7 5G 融入区域教育城域网的价值

8.7.1 重构智慧校园建设

目前，尽管以云计算为核心的集中式数据处理模式能够满足云端的计算和存储能力，但面对高质体验需求的新业务时仍然存在诸多不足，主要表现为：①所有的业务流均通过云计算中心进行处理，时延和拥塞的问题将严重影响业务体验，无法满足用户对超低时延的要求；②随着接入终端数的迅速增加，海量数据回传会给运营商接入网和核心网带来巨大压力，进而降低网络的运行效率。5G技术融入区域教育城域网，要求重构区域教育城域网建设的技术标准和应用标准，随之而来的是区域内的智慧校园建设也需要重构。基于此，本研究设计了重构后基于5G的智慧校园建设拓扑图，如图所示。



重构后基于5G的智慧校园建设拓扑图

重构后基于5G的智慧校园建设的主要内容有：①针对云AR/VR教学、全息课堂、云端智能管理等新业务对网络提出的超低时延、超大带宽、实时计算等需求，利用5G技术提供海量的终端管理、高可靠低时延组网、分级质量保证、数据实时计算和缓存加速、应用容器服务等基础功能，并通过多级边缘计算系统，为智慧校园提供实时、可靠、智能和泛在的端到端服务。②针对多种教育场景提供多级边缘计算的解决方案，将边缘计算节点部署于基站侧、基站汇聚侧或核心网边缘侧，为智慧校园提供多种智能化的网络接入和高带宽、低时延的网络承载，并基于开放可靠的连接、计算与存储资源，支持多生态业务在接入边缘侧的灵活承载。

8.7.2 推动课堂教学变革

5G融入区域教育城域网,推动着课堂教学发生了较大变革:①工具与技术变革主要表现为电化教育、PPT课件、网络空间人人通等；②教学模式变革主要表现为慕课、专递课堂、名师课堂、名校网络课堂等，并且师生关系也不再固定，在网络课堂上每个人的角色可以不断变化；③教学目标变革主要表现为学习可以随时、随地进行，教学内容也不再限于专业知识，使终身学习和“21世纪核心素养”[4]的培养皆成为可能。

8.7.3 促进学习方式变革

5G融入区域教育城域网，也促进学习方式发生了重要变革，即由传统的面对面单向讲授模式，发展为多终端、多地点、双向、线上线下相结合的混合式模式。而利用AR、VR等多技术辅助下的多教学场景，学习将更加真实立体、互动将更加多元，黑板不再是唯一的展示工具，学生可通过Pad等终端接入区域教育城域网开展在线学习、讨论互动与展示评价。总的来说，充分利用5G技术背景下教育资源获取的便利性、即时性、共享性等优势，变革课堂教学和学习方式，打通学校与学校、学校与社会教育机构、学校与家庭之间的壁垒，并以学生为中心开展5G融入区域教育城域网的建设与应用，对于推动教育的优质均衡发展有重要作用。在教学方式和学习方式发生变革的背景下，利用5G、大数据、人工智能等现代技术，一套新的教育生态系统、一种面向未来的教育模式就完全可以成为现实。

9 智能运维

9.1 网络运维

SDN 分析组件通过对设备运行状态、用户接入及在线状态、业务流量的实时数据采集和状态感知，并通过大数据分析技术和 AI 算法，将网络的运行可视化，主动感知网络的潜在风险并自动预警。

SDN 分析组件围绕如下几点构建：

- 多维可视：

- 网络 360 度可视：包括网络拓扑、设备运行状态（CPU、内存占用率等）、链路状态等信息的可视
- 用户 360 度可视：包括用户接入网络过程的健康度数据、行为状态数据，以及用户网络使用量数据及趋势数据等的可视
- 应用 360 度可视：包括 TopN 应用流量、应用流的转发路径、应用流的实时大小、应用质量（延时、抖动、丢包等）、应用健康度等信息的可视

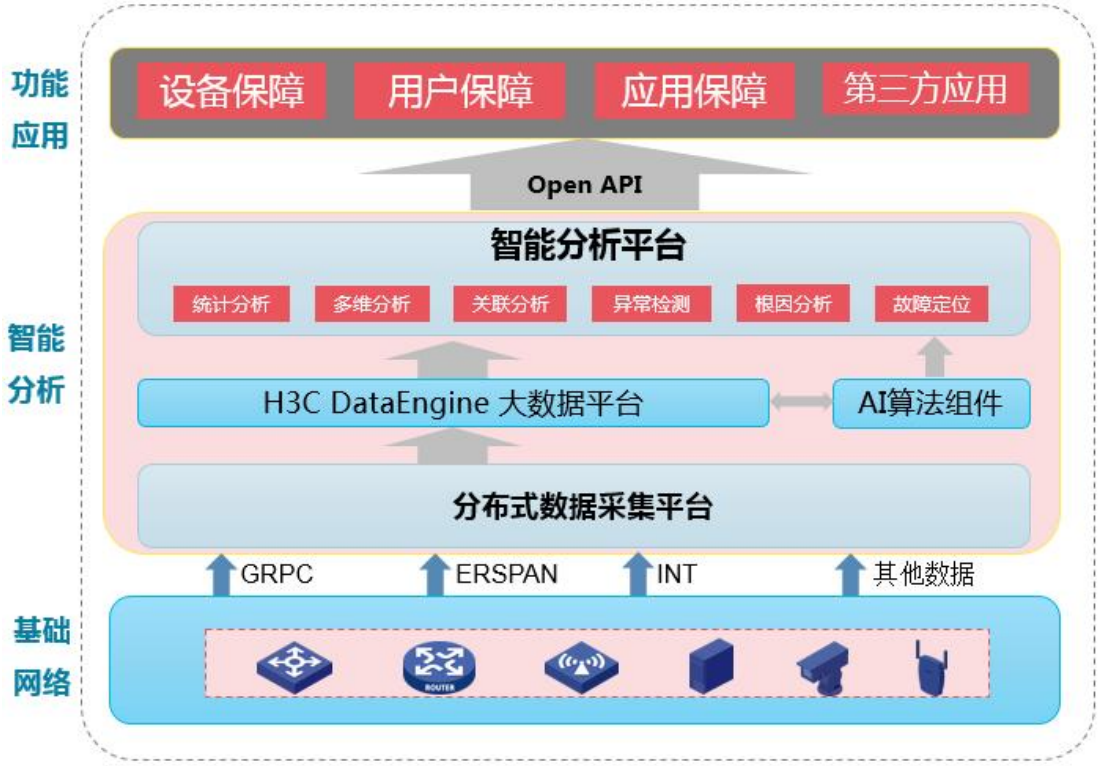
- 动态基线、智能预测：
  - SDN 分析组件自动对采集上来的海量数据进行大数据分析，并结合 AI 算法，计算设备运行状态基线、用户在线状态基线、应用流基线及预测值；
  - 将实测值与基线数据进行比较，判断实测值是否异常；
  - 对数据进行多维度相关性分析，明确异常直接因素。

9.2 技术实现

9.2.1 整体架构

为了解决融合园区、数据中心、WAN 网络场景的业务部署，网络保障功能，引入了 SDN 控制组件和分析组件。下面是 SDN 整体架构：

SDN 分析组件基于 DataEngine 大数据平台构建，通过 gRPC、ERSPAN、INT 等 Telemetry 技术接收来自网络设备的数据上报，运用智能算法对网络数据进行分析、呈现。SDN 分析组件系统架构见下图：



SDN 分析系统整体架构分为四部分：数据采集、数据存储、数据分析、数据呈现：

- 数据采集：
  - SDN 分析采集器负责收集网络的场景数据和运行数据。场景数据可来自于控制组件和北向 API 接口，包括物理网络中各个设备的类型、角色、连接关系，以及逻辑网络中的各个逻辑元素，如虚拟网络、子网等内容。运行数据来自于物理网络中的各个网络设备，网络设备通过 Telemetry 方式上报的数据：包括采用 ERSPAN/INT 技术采集的网络设备的流量数据、基于 gRPC 协议上报的性能 Metrics 数据、基于 SNMP/NETCONF 协议上报的设备的运行状态数据等。
  - 采集器收集的所有数据都具有时间属性，代表了某一时刻网络的运行状态。对于 ERSPAN 采集的流量数据报文，采集器将收到的报文打上时间戳，INT 数据报文内部已经携带时间戳。之后将采集报文打包发送给分析组件进行分析。
  - SDN 分析采集器通过分布式部署架构，实现数据采集层的按需扩容，来满足海量数据的采集需求。
- 数据存储：
  - 采集的数据根据业务需要，分类分级进行存储。存储要包括原始数据库、基础数据库、业务主题库、应用库。不同数据的保存周期需要可管理。并且，因应用场景的差异，SDN 分析组件支持大小数据模式。

- SDN 分析组件采用 DataEngine 大数据平台完成海量数据的分布式存储。

- 数据分析：-
  - SDN 分析组件能够对网络进行完整的透视，理解整个网络物理拓扑和业务运行状态。对采集的数据从业务需求角度进行计算，包括实时计算和离线计算。
  - SDN 分析组件采用 Spark、Flink 等分布式计算引擎完成数据在线、离线分析任务，来满足分析任务的计算能力需求。

- 数据呈现：
  - 设备 360 度健康度及网络健康度概览
  - 用户终端 360 度健康度及用户健康度概览
  - 应用 360 度健康度及应用健康度概览
  - 网络、用户、应用问题聚类及分布

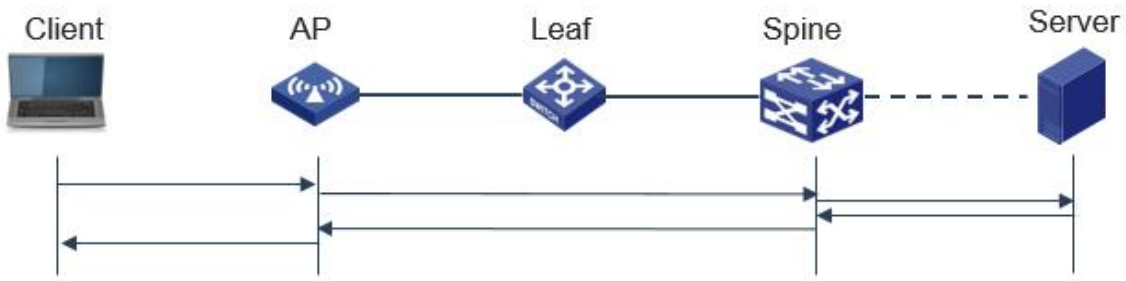
9.2.2 ERSPAN 流分析技术

ERSPAN（EncapsulatedRemoteSwitchPortAnalyzer）封装远程端口镜像，其功能是将镜像报文封装为协议号是 0x88BE 的 GRE 报文，通过三层网络路由转发到远端监控设备。

9.2.3 DHCP 交互报文

用户终端上线过程中，DHCPServer 向终端分配 IP 是重要一环，分析 DHCPServer 回应报文将有助于终端 IP 地址申请失败问题定位。通过 ERSPAN 将 Spine 与 DHCPServer 之间交互 DHCP 报文送到 SeerAnalyzer 分析组件，以避免 SeerAnalyzer 与各厂商 DHCPServer 对接。

DHCP 交互报文



9.2.4 Telemetry 技术

Telemetry 是一项监控设备性能和故障的远程高速数据采集技术。Telemetry 技术采用 gRPC 协议，通过推模式（PushMode）主动把设备数据信息上送给采集器，从而实现比传统 SNMP 查询方式更实时、更高效的数据采集性能。

- gRPC 协议

  gRPC（GoogleRemoteProcedureCall，Google 远程过程调用）是 Google 发布的基于 HTTP2.0 传输层协议承载的高性能开源软件框架，提供了支持多种编程语言的、对网络设备进行配置和管理的方法。通信双方可以基于该软件框架进行二次开发，从而使得双方可以聚焦于业务，无需关注 gRPC 软件框架实现的底层通信。

  gRPC 协议栈分层如下表所示：

分层	说明
内容层	业务模块的数据 通信双方需要了解彼此的数据模型，才能正确交互信息
ProtocolBuffers编码层	gRPC通过ProtocolBuffers编码格式承载数据
gRPC层	远程过程调用，定义了远程过程调用的协议交互格式
HTTP2.0层	gRPC承载在HTTP2.0协议上
TCP层	TCP连接提供面向连接的、可靠的、顺序的数据链路

  根据设备和网管的数据传输方式的不同，gRPC 网络架构分为 Dial-in 和 Dial-out：

  - Dial-in 模式的设备作为 gRPC 服务器，采集器作为 gRPC 客户端。由采集器主动向设备发起 gRPC 连接并订阅需要采集的数据信息,Dial-in 模式适用于小规模网络和采集器需要向设备下发配置的场景。
  - Dial-out 模式的设备作为 gRPC 客户端，采集器作为 gRPC 服务器。设备主动和采集器建立 gRPC 连接，将设备上配置的订阅数据推送给采集器，Dial-out 模式适用于网络设备较多的情况下向采集器提供设备数据信息。

- gRPC 网络工作机制：

  - 服务器通过监听指定服务端口来等待客户端的连接请求。
  - 用户通过执行客户端程序登录到服务器。

- 客户端调用.proto 文件提供的 gRPC 方法发送请求消息。
- 服务器回复应答消息。

9.2.5 故障分析与感知

SDN 分析组件根据客户现网的实际应用场景，对采集上来的 ERSPAN 流数据、INT 流数据、Telemetry 性能 Metrics 等数据，从网络分析、应用分析、用户分析三个维度，进行大数据分析。同时，结合异常检测动态基线等 AI 算法进行智能分析，主动感知网络是否存在潜在风险并预警。

- 网络分析

  网络分析主要是对网络拓扑、网络设备、以及设备资源进行动态实时监控，通过智能分析，来判断是否发生突变，从而进行预警。如网络链路流量监控、光模块监控、设备 CPU、内存占用率监控、芯片转发层面表项资源监控等。

- 应用分析

  应用分析，主要侧重与识别应用的交互行为是否出现异常、应用的服务质量是否出现异常等，如 TCP 异常检测、应用的转发路径可视及延时分析等。

- 用户分析

  用户分析侧重于用户上线体验，无线用户在线体验；

- 上线体验主要是无线关联、AAA、DHCP 过程是否成功；
- 在线体验主要是无线用户在线 RSSI、上下行速率、上下行流量、重传率等；

9.3 典型应用场景

9.3.1 无线覆盖盲区分析

见下图，终端用户从 AP-1 漫游到 AP-3。

获取 AP 侧用户的无线接入状态数据：单播流量、时延、错误率、丢包率、重传率、接收速率、发送速率、最大协商速率、信道利用率、RSSI 平均值、漫游上线次数等数据。

对采集的无线接入状态数据采用逻辑回归算法，生成终端综合健康度指标数据：

漫游过程中终端健康度变化：（AP-1，优）→（AP-1，差）→（AP-3，差）→（AP-3，优）

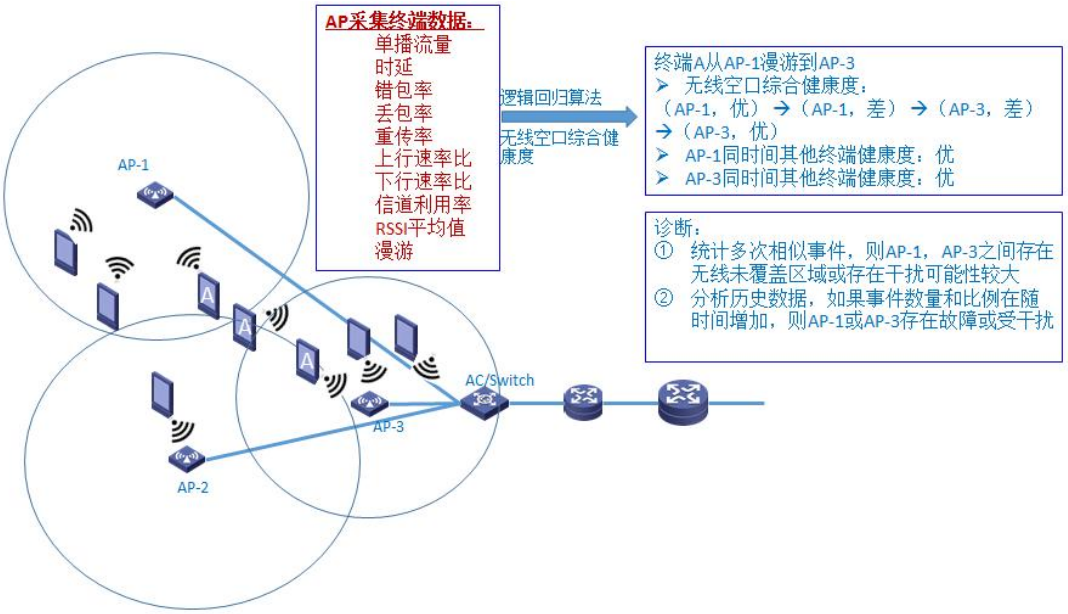
AP-1 同时间其他终端健康度：优

AP-3 同时间其他终端健康度：优

统计多次相似事件，则 AP-1，AP-3 之间存在无线未覆盖区域或存在干扰可能性较大。

分析历史数据，如果事件数量和比例在随时间增加，则 AP-1 或 AP-3 存在故障或受干扰。

无线覆盖盲区分析



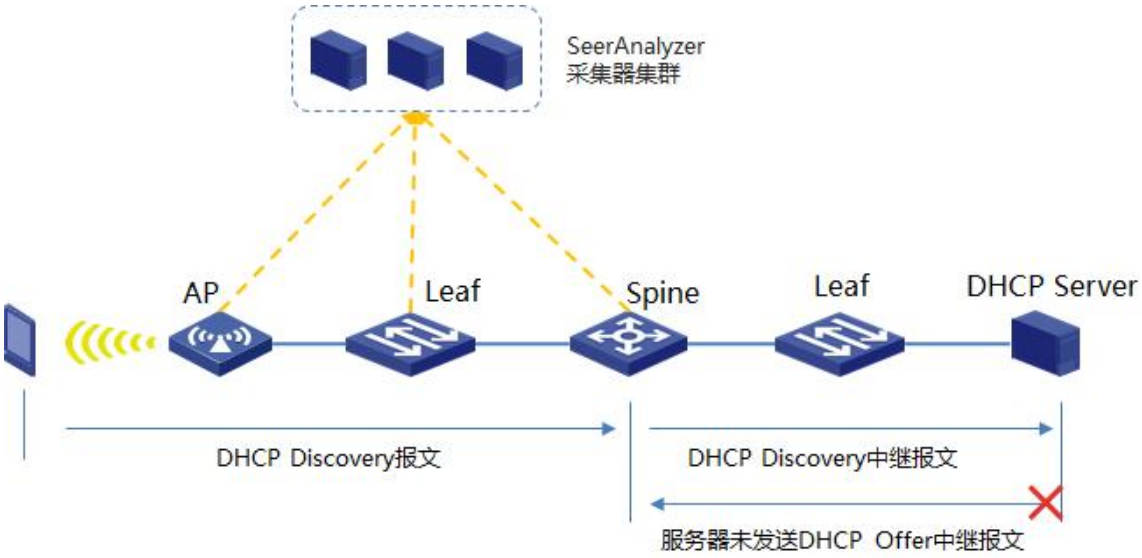
9.3.2 DHCP 异常分析

如下是 AP 侧用户发现 DHCP 认证失败问题分析：

通过在 AP、Leaf、Spine 设备上捕获 DHCP 报文，上送 SDN 分析采集器，SDN 分析组件对采集 DHCP 报文进行分析，确认失败原因是服务器未发送 DHCPOffer 中继报文：

- 分析组件收到 AP 上送的 DHCPDiscovery 报文摘要的。
- 分析组件收到 Leaf 上送 DHCPDiscovery 报文摘要。
- 分析组件收到 Spine 通过 ERSPAN 流镜像捕获的 DHCPRelay 报文。
- 分析组件未收到 Spine 通过 ERSPAN 流镜像捕获的 DHCPoffer 中继报文。

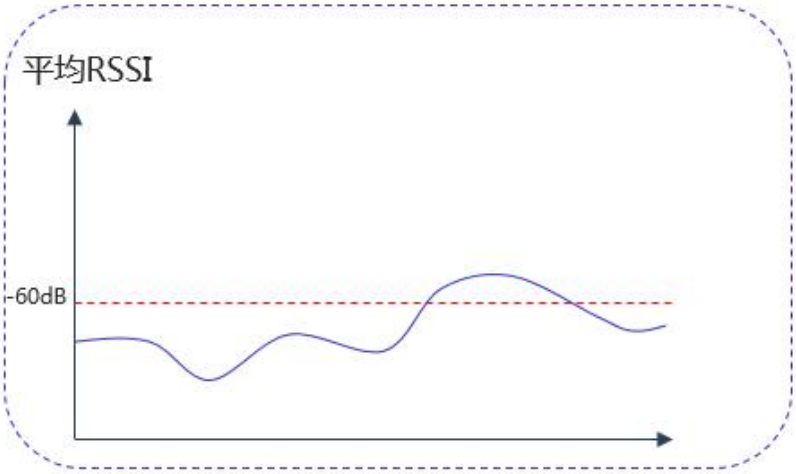
图 1 DHCP 异常分析



9.3.3 无线信号差

学生甲反馈教室 101 无线体验差，访问校园网慢，经过查看无线 AP 的在线用户数、在线用户 RSSI、信道利用率等参数，确认是由于信号差导致无线访问体验差，需要工勘进一步确认无线信号差原因。

图 2 信号差算法



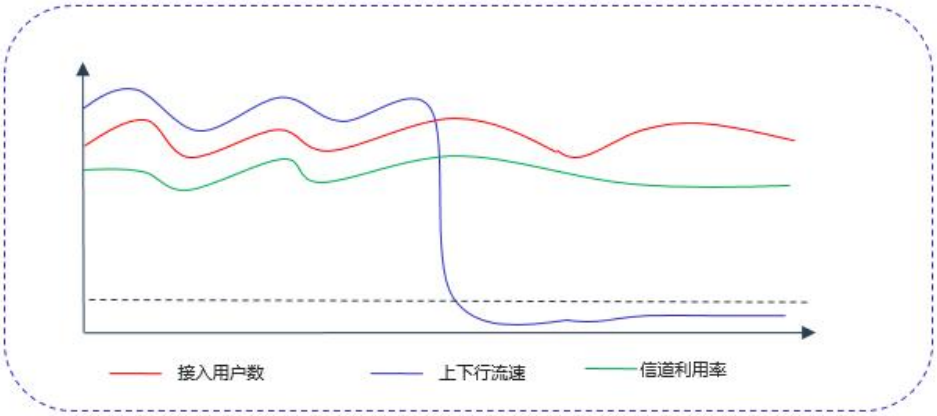
信号差算法：

- 5分钟内，AP下挂终端平均RSSI<=-60dB的终端占比>50%

9.3.4 无线 AP 业务异常

老师反馈办公室无法接入无线，经过查看，AP 健康度正常，但是通过分析 AP 历史在线用户数、上下行流速、信道利用率历史基线，判断 AP 业务异常，需要进一步确认 AP 业务异常原因。

图 3 无线 AP 业务异常分析



9.3.5 接入失败问题识别

管理员在接入用户失败 Top10 终端列表中，发现自己的 PC 有 700 多次上线失败，为何没有认证还有接入失败，经过排查，发现 PC 无线网卡在尝试自动接入无线网络，将无线网卡禁用即可。

图 4 接入失败问题分析

接入失败算法：

- 终端反复尝试接入失败超过10次

接入慢算法：

- 终端收到接入成功耗时超过2秒

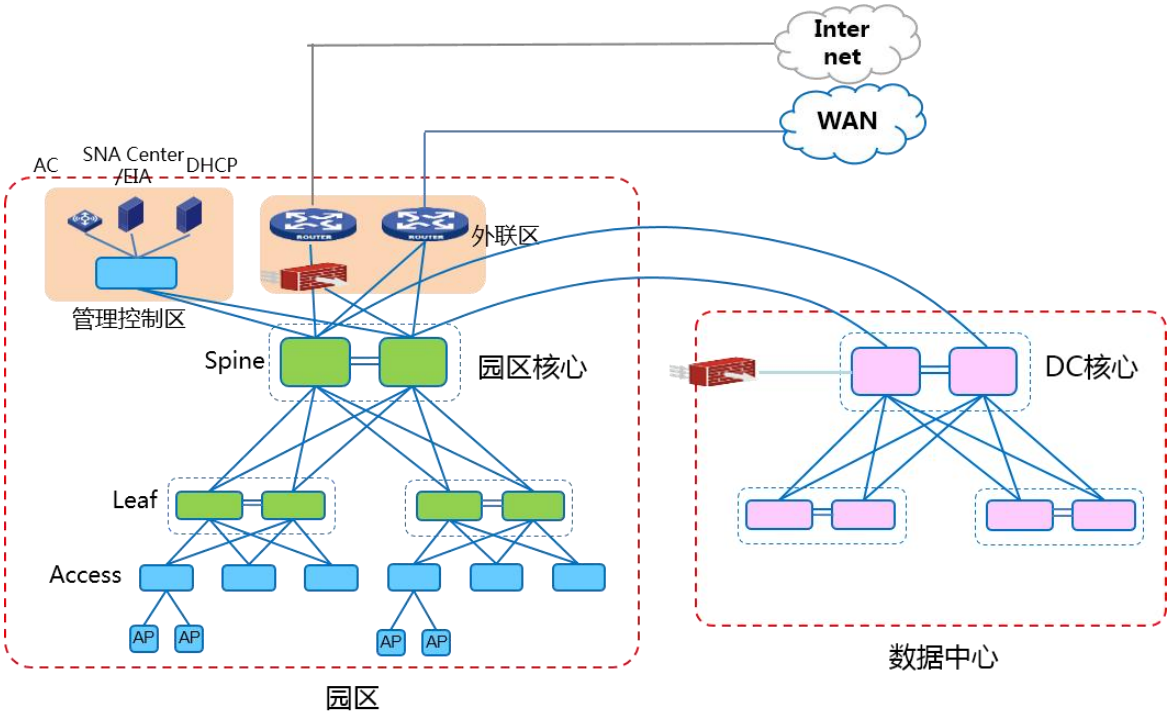
9.3.6 终端迁移

9.3.7 终端准入

10 园数融合

10.1 典型组网

园数融合场景的典型组网如下，园区核心交换机和 DC 核心交换机之间可以通过光纤直连，也可以通过 IP 网络进行连接（Underlay 路由可达），当通过 IP 网络进行连接时，需要中间的 IP 网络的 MTU 能支持 1600 字节以上。



10.2 控制组件

园数融合场景下，服务器中可以同时安装园区控制组件、数据中心控制组件，实现园区和 DC 统一部署，统一界面展示，统一运维。