

智慧园区固移多业务融合承载和统一认证方案

Fixed-Mobile Multi-Service Convergence Bearing and Unified Authentication Scheme for Intelligent Park

吕城锦, 钟志刚, 李颖, 佟恬 (中讯邮电咨询设计院有限公司, 北京 100048)

Lü Chengjin, Zhong Zhigang, Li Ying, Tong Tian (China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China)

摘要:

园区已成为中国经济发展的趋势之一,目前园区通信网络存在发展不均衡、网络结构复杂、扩展性差等问题。为了探讨建立可靠、高速的通信网络,在分析园区固移业务需求的基础上,研究了园区网络现状及存在问题。最后结合近几年网络新技术及相关应用案例,提出智慧园区网络承载解决方案、网络管理解决方案、网络接入解决方案。统一承载的网络构架可应用到大型国际体育赛事的通信组网构架中。

关键词:

智慧园区;区域路由;多业务融合承载;EVPN
doi:10.12045/j.issn.1007-3043.2020.12.004
文章编号:1007-3043(2020)12-0010-05
中图分类号:TN914
文献标识码:A
开放科学(资源服务)标识码(OSID):



Abstract:

The park has become one of the trends in China's economic development. At present, the communication network in the park has problems such as uneven development, complex network structure, and poor scalability. In order to explore the establishment of a reliable and high-speed communication network, the current situation and existing problems of the park network are studied based on the analysis of the fixed-mobile business needs of the park. Combined with new network technologies and related application cases in recent years, it puts forward network bearing solutions, network management solutions and network access solutions of intelligent park. The unified bearer network architecture can be applied to the communication networking architecture of large-scale international sports events.

Keywords:

Intelligent park; Segment routing; Multi-service convergence bearing; EVPN

引用格式:吕城锦,钟志刚,李颖,等.智慧园区固移多业务融合承载和统一认证方案[J].邮电设计技术,2020(12):10-14.

0 前言

发展创新性园区,走新型现代化发展道路,是提高国家竞争力的重要载体,目前我国已进入企业园区和产业集群互动发展阶段。随着科学技术的发展以及信息化水平的进一步提升,园区的网络业务也在逐步扩展,为了提高管理水平,提升企业经济效益和社会效益,必须建立高速、稳定、便捷、安全的通信网络。

1 园区业务需求

园区网络服务包括企业内部组网、共享互联网、

互联网专线,共计3项业务需求。

a) 企业内部组网。为满足园区内各企业经营、管理需求,各企业需有各自独立虚拟专用网,用于信息化办公,包含有线和Wi-Fi 2种接入方式。

b) 共享互联网。为用户提供共享带宽的互联网接入服务,包含有线和Wi-Fi 2种接入方式。

c) 互联网专线。为有需求的企业提供互联网专线服务。

2 园区网络现状及存在问题

典型的园区三层网络架构如图1所示,分为核心层、汇聚层、接入层。

目前,园区网络建设技术整体比较落后,发展不均

收稿日期:2020-10-09

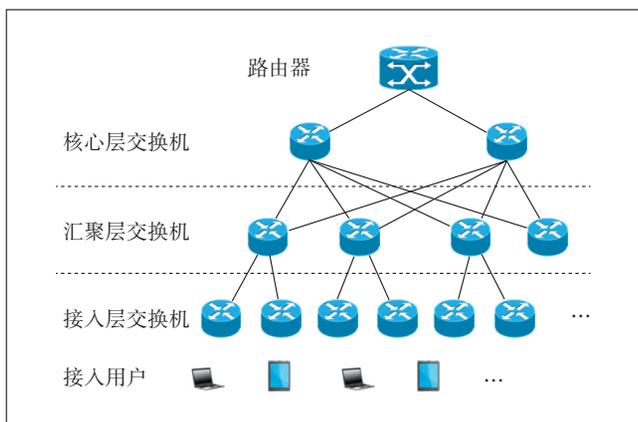


图1 园区典型网络架构

衡,标准不统一,缺乏长远规划,具体存在以下一些问题。

- a) 各业务单独组网,造成网络结构复杂,设备数量多,扩展性差,不易管理。
- b) 传统园区网络业务开通需1~3个月,业务开通周期长,设备配置复杂。
- c) 用户体验差,用户每次接入互联网均需认证,无法实现无感知认证。
- d) 故障定位难,排障时间长,运维难度大。
- e) 有线、Wi-Fi业务无法实现统一认证,需多套认证设备,造成资源浪费。
- f) 随着VR等新应用的发展,Wi-Fi带宽无法满足日益增长的带宽需求。
- g) 各业务均需设置独立的接入设备,不能实现接

入设备资源共享混合接入多种业务。

3 智慧园区网络承载解决方案

为了解决园区网络目前存在的问题,本文提出一种新型园区网络承载架构,采用“边缘(汇聚+接入)+核心”的结构,实现企业内部组网、共享互联网、互联网专线3种业务的统一承载,各业务逻辑隔离,网络总体架构如图2所示。

园区统一承载网各园区间采用三层协议组网,选用SR(Segment Routing)+EVPN(Ethernet VPN)技术。转发面采用SR技术以简化MPLS网络的控制平面,中间节点不需要维护路径信息,网络配置更简化,业务开通更迅速,实现路径故障快速恢复,网络容量扩展能力更强。EVPN在分离控制面与数据面的同时,可以简化配置,采用EVPN实现对不同业务的逻辑隔离,即互联网业务采用二层EVPN方式隔离共享和专线业务,企业内部组网采用三层VPN实现各园区内构建企业虚拟专网。

园区内作为小型局域网,采用二层组网方式,通过VLAN技术实现多业务的逻辑隔离。

网络采用SDN控制器,实现灵活简便的路径控制与调整,实现业务策略快速下发,实现网络资源直观可视,实现灵活的带宽调整与动态路由选择。及时发现和处理网络存在的风险,便于网络维护、降低业务故障概率。

新建Wi-Fi网络的园区采用802.11 ax/ac设备,通

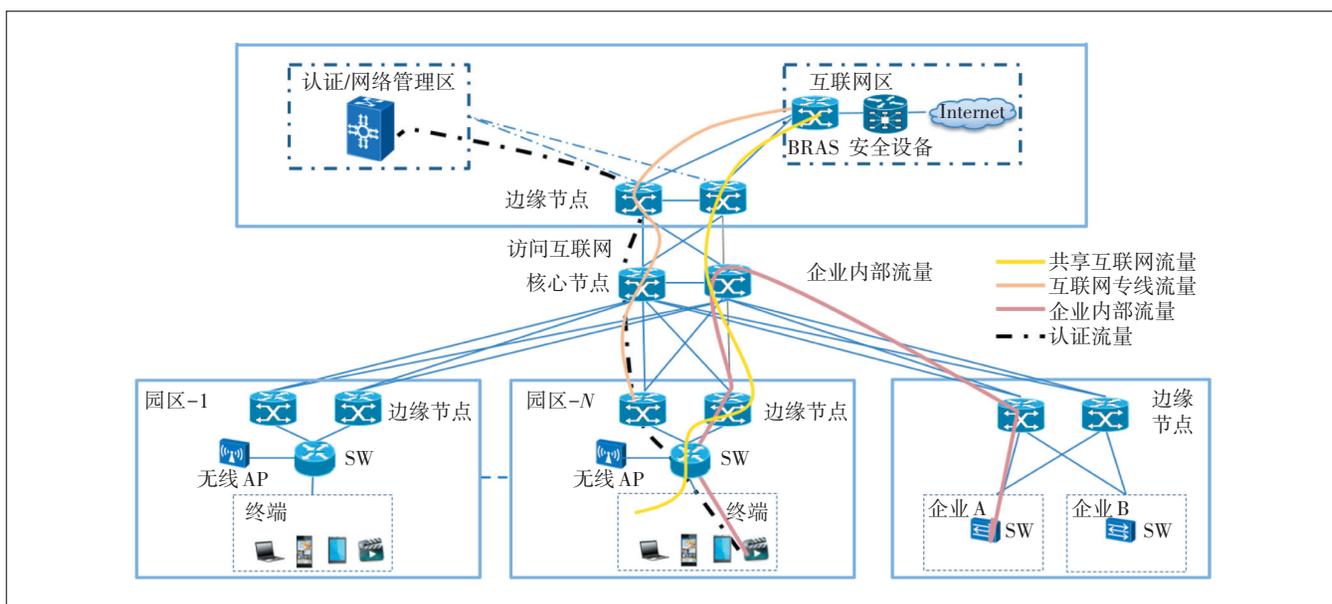


图2 网络总体架构

过AC集中部署的方式实现Wi-Fi服务。

4 智慧园区网络管理解决方案

4.1 LAN及WAN网络的统一管控

通过SDN网管控制器实现LAN、WAN网络的统一控制、统一管理、统一运维,实现网络的可视化、自动化、智能化,解决分支园区业务开通慢、部署难等问题。

目前,传统网络由若干个物理设备,比如路由器、交换机和防火墙等组成,这些设备本质上还是一个一个单独的“盒子”,而且这些“盒子”之间通常存在着复杂的网络关系,一旦其中一个节点出现问题,可能会影响整个网络。而SDN是一种网络架构,其从根本上改变了整个网络的设计、管理和运营方式,让网络变得更加灵活、可靠。

SDN通过将数据层面和控制层面分离,让传统的物理网络设备不再具备决定转发的能力,而是统一交给上层能理解整个网络拓扑的统一控制器。借助控制器,网络工程师可通过软件的方式,实现新业务的转发策略。

SDN网管控制器可实现对网络核心和汇聚设备进行管控;可实现网络资源可视、业务自动化部署、业务快速开通、网络性能优化、电信级可靠性保障等功能。具体包含以下功能。

a) 配置发放自动化。通过对网络设备和业务进行抽象,实现多种类型配置的自动发放,提供多种业务配置模板和批量配置模板,应支持自动配置校验。可实现接入交换机及AP的即插即换。

b) 带宽按需分配功能。按需调整带宽、业务预约发放。

c) 集中算路及流量调优要求。对于具有重路由恢复能力的业务,当业务的工作路径或者保护路径发生故障时,网元控制平面会自动向控制器请求路径计算,控制器根据全网拓扑计算一条最优路径返回给网元,网元则按照最优路径建立恢复路径。

d) 网络性能监控及分析功能。

e) 资源可视化。通过图形化的方式实时呈现链路、隧道等资源利用率。显示业务多层信息,端到端显示业务路径。

f) 网络生存性分析和资源预警。

4.2 多业务统一无感知认证

一套认证系统实现多业务统一认证(包含有线/Wi-Fi),企业内部组网业务终端实现完全无感知认

证,共享互联网业务终端第一次登录需输入“账号+密码”,终端再次登录即可实现自动登录,实现无感知认证。各业务认证流程如下。

4.2.1 企业内部组网

企业内部组网认证流程分为登录、录入、接入、认证、IP地址分配5部分,如图3所示。

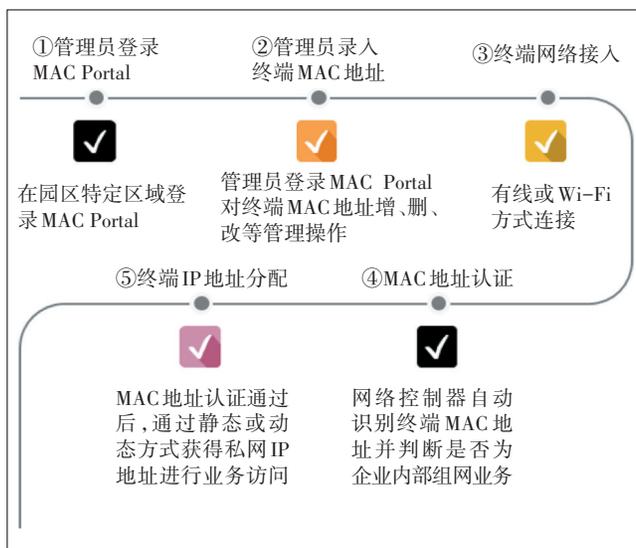


图3 企业内部组网认证流程

a) 管理员登录MAC地址注册门户(MAC Portal)。为使用企业内部组网服务的企业提供MAC地址注册门户(MAC Portal)管理员账号及密码,实现对各自终端MAC地址进行增、删、改等管理操作。各家企业管理员在园区特定区域通过管理员账号及密码登录MAC Portal,无需控制器MAC地址识别,终端自动获得或静态配置IP地址,通过管理员账号及密码登录MAC Portal。

b) 管理员录入终端MAC地址等字符段。管理员登录MAC Portal后,即可手工通过逐条或批量导入方式,完成对使用企业内部组网服务的终端MAC地址等字符段信息的增加、修改、删除等管理操作,字符段包含的字符类型及格式如表1所示。

表1 字符段信息

序号	字段名称	数据格式	最大长度	使用描述
1	序列号	字母数字	15	设备序列号
2	MAC地址	十六进制字母数字	18	AA:BB:CC:11:22:33
3	设备	字母数字	20	设备的文字说明
4	用户	字母数字	20	用户名
5	企业	字母数字	15	企业名称

c) 终端网络接入。企业管理员在MAC Portal中

录入终端 MAC 地址后,终端可立即通过有线/无线方式接入网络。

(a) 有线接入:在园区特定位置,提供共享的 RJ45 插口(10/100/1 000M 自适应)。用户终端通过网线连接 RJ45 插口。

(b) Wi-Fi 接入:终端设备搜索并连接 SSID,输入 Wi-Fi 密码。

d) 网络认证。用户终端通过有线或无线方式接入网络后,网络控制器自动识别终端 MAC 地址,判断该终端是否为企业内部组网服务。如 MAC 地址认证通过,即为该终端分配 VLANID,引入专用 VRF;如 MAC 地址认证未通过,不提供企业内部组网服务,终端自动进入共享互联网认证通道。

e) IP 地址分配。各企业自行搭建内部组网及相关服务器,根据各企业的业务需求提供一定范围的专用私网 IP 地址段(B类/16位),私网地址定义以 RFC1918 为准。在各园区(C类/24位)进行详细划分、管理和业务部署,每个/24地址段通过网关地址实现企业虚拟专用网内的 DHCP 中继功能。

各企业用户终端通过静态或者 DHCP 动态方式获得私网 IP 地址,在终端设置 FTP 服务器的 IP 地址后即可使用企业组网服务。

4.2.2 共享互联网

有线接入:端口为 10M/100M/1 000M 自适应。终端首次接入,打开电脑的网页浏览器,弹出用户认证的 Portal 页面,输入统一发放的“账号+密码”,认证通过后即可访问共享互联网业务,终端再次在共享互联网业务覆盖范围内接入时,无需再次输入“账号+密码”进行认证。

Wi-Fi 接入:终端首次接入,搜索并连接 SSID,输入 Wi-Fi 密码。在自动弹出或打开网页浏览器后弹出的用户认证 Portal 页面,输入“账号+密码”进行认证,认证通过后即可访问共享互联网业务,终端再次在共享互联网业务覆盖范围内接入时,无需再次输入“账号+密码”进行认证。

哑终端接入:有哑终端访问共享互联网需求的用户需提前将哑终端接入申请的相关信息(相机 MAC、共享互联网账号等)通过邮件等方式反馈给园区管理部门,之后后台技术部门将哑终端相关信息集中录入至认证系统,实现与共享互联网用户账号绑定,录入完成后,哑终端设备进入园区指定覆盖区域即可自动实现免 Portal 访问共享互联网。

4.3 基于大数据及 AI 的智能运维

将大数据、AI 引入网络运维中,实时感知网络/用户数据,实现基于大数据、AI 的数据分析,依据数据分析结果,完成自动化/半自动化处理,实现网络运维智能化、主动化、自动化。

a) 网络隐患预测。对精确的网络状态、KPI 等数据实时自动获取分析,通过异常配置识别、资源超限预测等 AI 技术挖掘网络隐患,实时预测网络隐患,在业务受损前消除隐患。

b) 实现故障分钟级自动定位。基于海量运维大数据实现故障传播图自学习,结合在线的嵌入式 AI 异常识别能力+关联聚类算法实现故障根因分钟级定位,历史故障可回溯。

c) 用户体验可视化。以用户体验为中心,提取用户体验关键指标,实时感知并依托大数据分析指标,逐步提升用户体验,提高用户满意度。

5 智慧园区网络接入解决方案

5.1 Gbit/s 级无线接入

随着 VR/AR、4K 视频、超高清视频会议等高带宽、低时延应用的出现,无线接入对吞吐性能的要求越来越高。Gbit/s 级无线接入能力依托新一代 WiFi-6 产品,适用于高密度无线接入和高容量无线业务,满足用户带宽、时延需求,使用户获得最佳体验。

WiFi-6 是下一代 802.11ax 标准的简称,引入多种新技术,使得传输速度更快、并发连接数更多、吞吐量更大,具有以下一些优势。

a) 采用 OFDMA 技术:相同信道同时传输多个数据,提高信道利用率。

b) 采用 MU-MIMO 技术:支持 2.4 与 5G 的多用户并发,提升传输效率,增加覆盖范围,降低使用成本。

c) 采用空间复用技术:减少 AP 之间的同频干扰,达到信道资源的共享。

5.2 多业务任意端口灵活接入

共享互联网和企业内部组网业务在园区内通过有线(任意 RJ45 面板/有线接入交换机端口)和无线 Wi-Fi(同一 SSID)接入,实现多业务任意端口灵活接入。

有线接入用于电脑、打印机、相机等终端接入,可依据需求提供 RJ45 面板或者 RJ45 交换机接口,对于有供电需求的位置,可在提供 RJ45 交换机接口的同时,提供 IEEE 802.3bt 标准 POE 供电,每个端口提供最高 60 W 功率供电。

6 大型体育赛事组网解决方案

大型体育赛事的业务需求包括共享互联网、媒体专用网、互联网专线。

共享互联网:对于大型体育赛事,无论是赛事的组织者,还是国内外的媒体记者,现场观赛者,在比赛的准备和进行过程中,都需要信息的传递和共享,快速沟通。因此,需为媒体、工作人员、观众,提供共享带宽的互联网接入服务。在以往大型体育赛事中,认证方式比较复杂,难以实现无感知认证。

媒体专用网:是指为各家媒体分别组建一个虚拟专用网,提供赛时照片即拍即传和文件回传至各自媒体独立工作间的服务,同时电脑、手机、相机等终端认证方式要简单,尤其针对相机这类无法弹出Portal页面的哑终端。在以往大型体育赛事中,媒体专用网和共享互联网都是物理隔离的,通过独立组建一张物理网络,再划分不同VLAN给不同新闻社使用。网络结构复杂,设备数量多,组网成本很高。同时,用户每次接入专网均需认证,无法实现一次认证,永久在线,用户体验差。

互联网专线:是指通过有线网络为有专线需求的用户,在特定位置提供固定带宽的互联网接入服务,带宽速率需可选可调节。而以往大型体育赛事中,专线业务开通周期长,设备配置复杂,无法实现带宽随选,或者带宽调整很不灵活。

此外,大型赛事网络的室内外场馆数量多,距离远,故障定位难,排障时间长,备品备件数量多,各场馆都需要运维专家团队,整体运维难度比较大。

以上3项业务需求与园区业务需求类似,因此本文提出的园区组网解决方案可以应用到大型体育赛事组网方案中。

智慧园区网络承载解决方案、网络管理解决方案、网络接入解决方案均可应用到大型体育赛事组网解决方案中,可以实现多业务融合承载、业务无感知认证、网络智能运维、多业务任意端口灵活接入等。

7 结束语

智慧园区统一承载网采用SR+EVPN技术,为智能业务提供条件,网络配置更简化,业务开通更迅速,可以实现多业务融合承载、业务统一无感知认证、基于大数据及AI的智能运维等。

可以预见,智慧园区统一承载网将为园区提供质

量更好、可靠性更高、便捷性更强的通信网络,推动智慧园区网络高质量、高水平发展。

参考文献:

- [1] 张丽华,齐可翠,张艳玲. Segment Routing 技术浅析[J]. 数字化用户, 2019, 25(23): 15.
- [2] 刘强,石磊. Segment Routing 技术及其应用分析[J]. 电信技术, 2017(12): 56-58.
- [3] JOHN DRAKE, WIM HENDERICKX. BGP MPLS-Based Ethernet[EB/OL]. [2020-03-10]. https://xueshu.baidu.com/usercenter/paper/show?paperid=bdd6821e9a373907e36ae531f4a3295a&site=xueshu_se.
- [4] CLARENCE FILSFILS, SIVA SIVABALAN. Segment Routing Policy Architecture[EB/OL]. [2020-03-10]. https://blog.csdn.net/hesy_h/article/details/98205847.
- [5] 陈树靖. 路由Vlan在大型园区网络中的应用探讨[J]. 软件导刊, 2008(1): 122-123.
- [6] 韩明. 浅谈企业园区网络设计[J]. 信息通信, 2018, 183(3): 168-170.
- [7] 高榕. 中小型企业园区网络设计与实现[J]. 软件导刊, 2010, 9(8): 123-125.
- [8] 古艳艳,孟庆伟. 中小型园区网的设计与实现[J]. 现代电子技术, 2010, 33(22): 152-155, 158.
- [9] 徐伟华. MPLS VPN在园区网中的设计与实现[J]. 科技创新与应用, 2019(7): 91-92.
- [10] 沈宁国,于斌,黄明祥,等. 园区网络架构与技术[M]. 北京:人民邮电出版社, 2019: 172-175.
- [11] CLARENCE FILSFILS, KRIS MICHELSEN, KETAN TALAU-LIKAR. SEGMENT ROUTING 详解[M]. 苏远超,蒋治春,译. 北京:人民邮电出版社, 2019: 84-93.
- [12] 王玮. 高校WLAN无感知认证系统的设计与实现[J]. 软件工程, 2019, 22(9): 23-27.
- [13] 杨建军. 电信运营商网络运维智能化的应用思路与实践[J]. 数字通信世界, 2020(1): 143.
- [14] 江波. 5G技术和wifi6技术在高校智慧校园建设中的应用探讨[J]. 数字技术与应用, 2020, 38(4): 28-30.
- [15] 周亮. 数据中心设备及机房的智能化运维管理策略研究[J]. 数码世界, 2020(4): 44.
- [16] 李俊林. 浅谈数据中心设备及机房的智能化运维管理[J]. 数字通信世界, 2020(2): 284.
- [17] 赵旭. 数据中心设备及机房的智能化运维管理[J]. 信息周刊, 2018(2): 52-53.

作者简介:

吕城锦,毕业于上海交通大学,工程师,硕士,主要从事IP网规划和设计工作;钟志刚,毕业于武汉大学,中讯邮电咨询设计院有限公司总工程师,教授级高级工程师,先后从事微波、卫星和移动通信领域咨询、规划、设计、研究等工作;李颖,毕业于北京联合大学,高级工程师,本科,主要从事IP网规划和设计工作;佟恬,毕业于北京邮电大学,工程师,硕士,主要从事IP网规划和设计工作。