闽广〔2019〕206号

福建省广播电视局关于实施两项广播电视推荐性行业标准及一项行业暂行技术文件的通知

各设区市文旅局（广电局）、平潭综合实验区社会事业局，省广播影视集团、福建广电网络集团，省广播电视监测中心、省广播电视节目收听收看中心：

最近，国家广播电视总局组织审查并发布了《AVS2 4K超高清编码技术要求和测量方法》《AVS2 4K 超高清专业卫星综合接收解码器技术要求和测量方法》等两项中华人民共和国广播电视推荐性行业标准（内容已在总局门户网站

http://www.nrta.gov.cn 公开），及《全国有线电视网络云数据中心技术规范第 5 部分：数据中心互联》等一项广播电视行业暂行技术文件（内容详见附件）。现发给你们，请遵照执行。

附件：全国有线电视网络云数据中心技术规范第 5 部分：
数据中心互联

福建省广播电视局

2019 年 9 月 24 日

GD

中华人民共和国广播电视暂行技术文件

GD/J 077.5—2019

全国有线电视网络云数据中心技术规范 第5部分：数据中心互联

Technical specification of cloud data center for the national cable TV network—Part 5: Interconnection of data center

2019－09－06 发布　　2019－09－06 实施

国家广播电视总局科技司　　发布

目　次

前　言

GD/J 077《全国有线电视网络云数据中心技术规范》已经和计划发布以下部分：

——第1部分：总体；

——第2部分：配套设施；

——第3部分：基础设施；

——第4部分：PaaS平台；

——第5部分：数据中心互联；

……

本部分为GD/J 077的第5部分。

本部分按照GB/T 1.1—2009给出的规则起草。

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

本部分由国家广播电视总局科技司归口。

本部分起草单位：国家广播电视总局广播电视规划院、中国广播电视网络有限公司、新华三技术有限公司、浪潮集团有限公司。

本部分主要起草人：孙黎丽、聂明杰、白鹤、宫良、陈寒、杨旭、刘健、贾峰。

全国有线电视网络云数据中心技术规范
第5部分：数据中心互联

1 范围

GD/J 077的本部分规定了全国有线电视网络云数据中心互联的总体架构以及云管理平台互联、前端网络互联、业务网互联和存储网络互联的技术要求。

本部分适用于指导全国有线电视网络进行数据中心互联的规划与建设。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GD/J 037—2011 广播电视相关信息系统安全等级保护定级指南

3 缩略语

下列缩略语适用于本文件。

API 应用程序编程接口（Application Programming Interface）

CA 认证授权（Certificate Authority）

DC 数据中心（Data Center）

DCI 数据中心互联（DC Interconnetion）

DNS 域名系统（Domain Name System）

DWDM 密集波分复用（Dense Wavelength Division Multiplexing）

EVI 虚拟化以太网互联（Ethernet Virtualization Interconnect）

EVN 虚拟化以太网络（Ethernet Virtualization Network）

EVPN 虚拟以太网专用网络（Ethernet Virtual Private Network）

IPSec IP层协议安全结构（Security Architecture for IP network）

MPLS 多协议标签交换（Multi-Protocol Label Switching）

OTN 光传送网（Optical Transport Network）

OTV 叠加传输虚拟化（Overlay Transport Virtualization）

RHI 健康路由注入（Route Health Injection）

RTO 恢复时间目标（Recovery Time Objective）

RPO 恢复点目标（Recovery Point Objective）

SAN 存储区域网络（Storage Area Network）

SSL 安全套接层（Secure Sockets Layer）

VPN　虚拟专用网络（Virtual Private Network）
VxLAN　虚拟可扩展局域网（Virtual eXtensible LAN）

4　数据中心互联总体要求

4.1　概述

由于业务发展需要，同一有线电视网络运营商在不同地域分别进行数据中心的建设，为构建统一的云平台作为有线电视网络的支撑平台，不同数据中心之间可进行互联，支持不同数据中心之间的基础资源共享，对不同数据中心的云服务能力支持统一管理、统一调度。

4.2　业务交互要求

4.2.1　资源要求

数据中心互联建设，应考虑到不同业务在不同阶段对资源有不同需求，应支持对数据中心的各类资源实现统一管理与调配，确保满足业务的不同资源要求，保障生产业务的顺利运行。

通过虚拟化技术，对数据中心资源进行优化、统一管理，并为这类业务弹性分配资源，按照业务的实际需要弹性地分配、增加或减少计算和存储资源。并根据资源的实际使用情况进行计量，使峰时和闲时工作量的资源利用都保持在合理水平，实现低成本高效的IT运营模式，使资源得到合理、有效的利用，实现资源优化和成本节约。

4.2.2　业务要求

在业务层面上，数据中心互联应满足：

——快速业务交付能力，可实现业务应用系统的精简部署、快速上线；

——业务应用平滑扩充的能力，各种业务的应用可根据业务量变化和用户的工作负荷变化而扩展或缩小应用规模；

——提供高可用性和高稳定性的能力，保障业务的连续性。应提供最大的可持续运行时间和最小的非计划宕机时间保障。

4.2.3　管理要求

为管理用户提供统一自服务管理门户，管理用户可通过自服务门户完成包括但不限于以下业务操作：

——提供虚拟机模板的高效创建和管理，可方便地将业务应用打包成应用模板，实现用户业务应用系统的精简部署、快速上线。平台支持模板分级管理，不同的用户群可共享或授权使用模板。

——可查询提供的服务种类、服务描述与规格等及服务的订购、续订、退订等操作，用户可通过自服务门户对申请的资源（包括存储、计算、交换链路等资源）进行管理。

——管理员可通过自服务门户对虚拟机进行快照和快照恢复操作，还可删除虚拟机快照，可对虚拟硬盘进行快照和快照恢复操作，还可删除虚拟硬盘快照。

——管理员可通过自服务门户看到虚拟机创建成功后的提示信息和查看订单申请的审批状态。

4.3　业务容灾要求

4.3.1　概述

云平台内的重要业务应具备连续服务能力，即使在单站点数据中心发生灾难的情况下，仍能由异地站点提供持续的服务，将业务中断时间降到最低，即减小RTO，这要求业务系统能在多个数据中心实现双活或主备部署，并在主站点或部分站点灾难失效的情况下，自动将用户访问请求重新调度到健康站点进行受理。

云平台内业务系统中的重要数据资源应考虑跨站点的备份保护，在主用数据系统故障或站点灾难发生时，最大限度将数据损失降到最低，即减小RPO。这要求在不同站点的系统间进行异地的数据复制，可以是不同层面的数据复制，如基于中间件或应用软件的数据复制、基于数据库本身的数据复制、存储系统的数据复制等。

4.3.2 主备方式

主备方式下业务系统应同时在至少两个数据中心站点部署，有一个站点作为主用站点，其他站点作为备用站点，其业务容灾架构见图1。在正常情况下，只有主用站点的业务系统对外提供服务，其他备用站点的业务系统不提供对外服务。当主用站点业务系统发生灾难时，备用站点的业务系统才对外提供服务。备用站点平时负责对主用站点的业务数据进行备份。

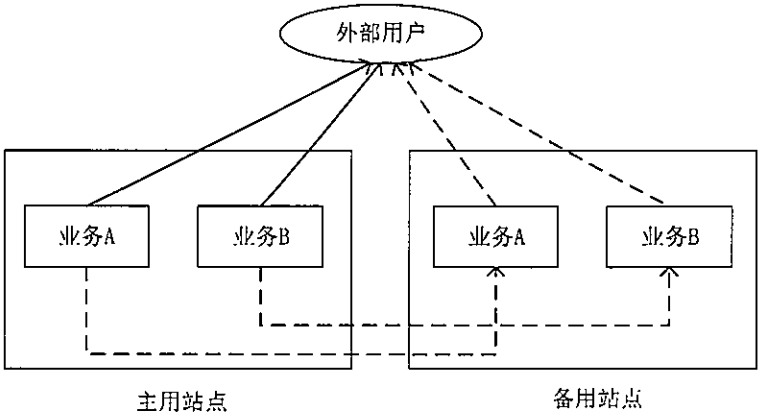

图1 主备方式业务容灾架构

4.3.3 双活（Dual Active）方式

双活方式下业务系统应同时在至少两个数据中心站点部署，从全局角度看，所有站点均同时对外提供服务，并且数据中心间相互进行数据备份。当单个站点的业务系统灾难发生时，其他站点能顺利切换业务，保证业务的连续性。站点的具体双活方式还可划分为分业务双活、全业务双活，这取决于业务的具体对外发布方式。一般数据中心业务的对外发布方式可分为基于IP地址方式发布（一般为C/S架构）、基于域名方式发布（一般为B/S架构）两种。

基于IP地址方式发布的业务在部署时，一般采用分业务双活方式，其业务容灾架构见图2，即不同站点分别作为不同业务的主用站点对外发布该业务的最优路由，牵引外部用户的访问流量来提供服务，但具体到某个业务上，同一时刻只有一个站点作为其主用站点，其他站点均为备用站点，只有待主用站点的该业务系统失效后备用站点才将本地该业务系统的对应路由作为最优路由对外发布，重新牵引外部用户的访问流量提供服务。

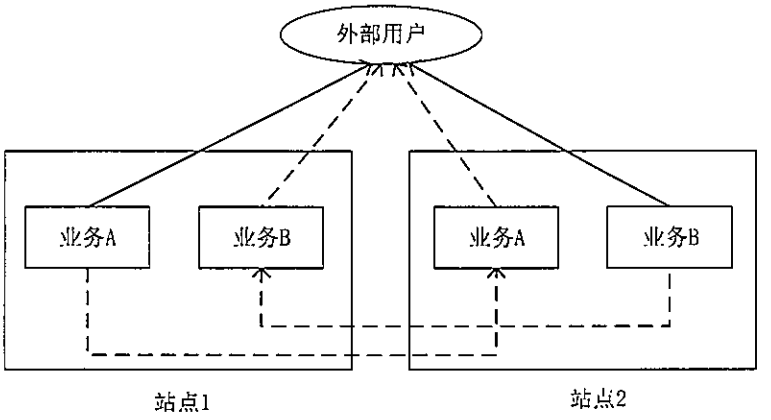

图2　分业务双活方式业务容灾架构

基于域名方式发布的业务在部署时，一般采用全业务双活方式，其业务容灾架构见图3，即对任一业务而言，所有站点可同时对外提供该业务的服务。位于不同地理位置的外部用户发起对该业务域名的DNS解析请求时，部署在广域网的DNS全局负载均衡系统会进行智能调度。DNS全局负载均衡系统在处理外部用户的业务DNS解析时，会综合考虑用户IP的就近性、各站点部署的该业务系统的健康状态、负载情况等因素选择最优的站点业务IP作为结果反馈给用户终端，实现多个数据中心站点同时为不同位置的用户提供全局负载分担的业务服务。

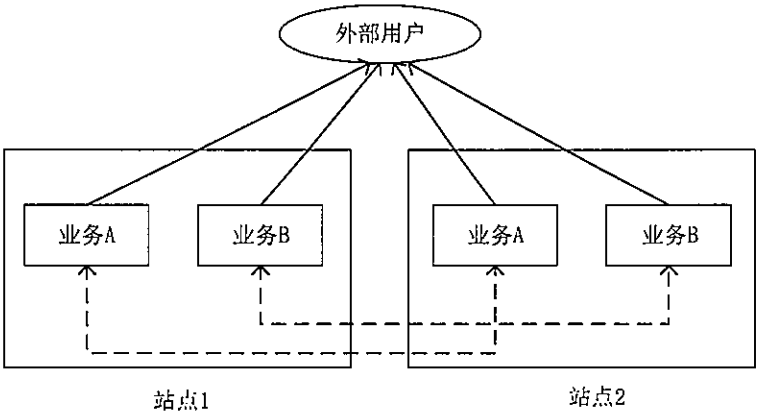

图3　全业务双活方式业务容灾架构

5　总体架构

数据中心互联总体框架见图4。

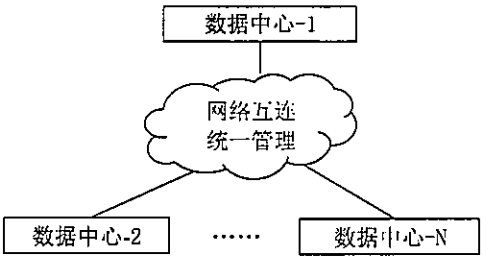

图4　数据中心互联总体框架

一个云平台由多个数据中心站点构成，多个数据中心之间网络实现互联，实现服务门户的统一、资源状态监控界面的统一、安全边界的统一，实现在统一的云平台上对不同数据中心的云基础资源的统一申请、统一审批、统一监控和统一计费。

6　云管理平台互联

6.1　概述

在一个由多个数据中心站点构成的云平台内，每个站点都会部署本地的云管理平台，为了构成一个统一的云平台管理系统，需要对各个站点的云管理平台进行互联设计。

云管理平台的互联设计可考虑采用异平台的分级式互联和同平台的分布式互联。

6.2　互联方式

互联方式主要包括：

a)　异平台的分级式互联：见图5，在该方式下，不同的数据中心站点采用不同架构或解决方案的云管理平台作为下级管理平台，对本地云资源、业务和用户进行管理，下级管理平台具有完整的管理权限，可独立开展业务运营。在此基础之上，再部署一个顶层云管理平台，实现对下级管理平台的统一调度、监控和管理，并可作为服务门户入口。

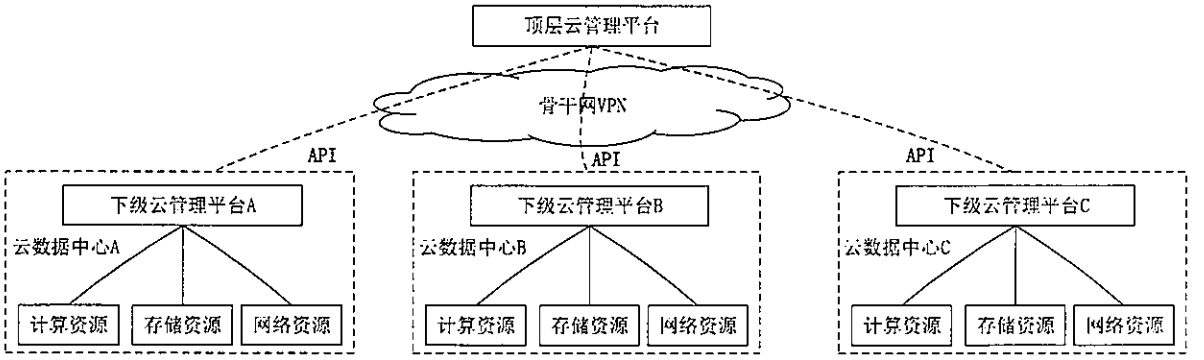

图5　异平台的分级式互联架构

b)　同平台的分布式互联：见图6，在该方式下，不同的数据中心站点部署了相同架构或解决方案的云管理代理系统（Agent），对本地云资源、业务和用户进行代理管理；在此基础之上，部署统一的云管理平台，与各代理系统进行交互，完成对多个站点云资源、业务和用户的统一管理，并作为统一的服务和管理门户入口。所有的鉴权均在上层云管理平台完成。

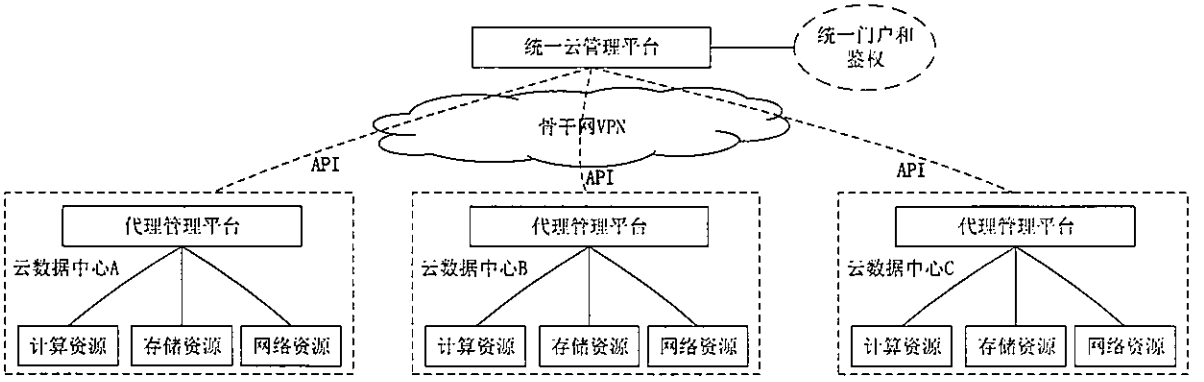

图6　同平台的分布式互联架构

6.3　关键技术

异平台的分级式互联方式下，顶层云管理平台架构见图7，它可实现对下级的多种异构云管理平台的纳管，其内部通过适配层对下层的云管理平台软件进行对接。顶层云管理平台应定义开放的南向API接口集，不同的下级异构云管理平台通过实现该南向API，以插件的方式对接顶层云管理平台。顶层云管理平台上的具体业务操作通过调用适配层的具体插件实现对具体的下级云管理平台的资源、业务和用户的调度操作。

顶层云管理平台和下级云管理平台之间的互联网络通道可采用基于骨干网或互联网上的MPLS VPN、IPSec VPN、SSL VPN、VxLAN VPN等安全VPN通道。

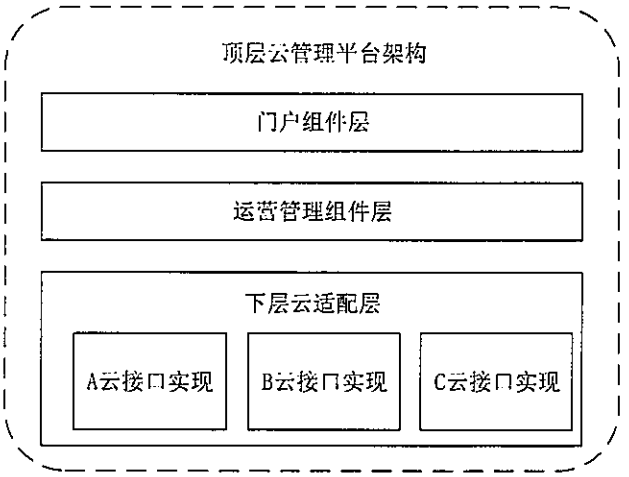

图7　顶层云管理平台架构

同平台的分布式互联方式下，统一云管理平台与下级代理管理系统之间通过内部API方式进行交互。代理管理系统不具有任何自主管理权限，只接收来自统一云管理平台的调用，对本地云资源池进行管理，并监控本地云资源的状态和向上反馈。包括流程、租户、计费、鉴权等其他管理功能均向上反馈至上层的统一云管理平台，实现对多站点异地部署下的集中化云管理。

7 前端网络互联

7.1 概述

前端网络指数据中心站点与用户之间、以及不同数据中心站点之间进行互访的物理或逻辑网络。前端网络互联应支持：

——前端网络的VPN互联：为了满足不同DC之间的业务系统互联，应通过安全的逻辑通道实现流量互访，宜采用VPN技术；

——前端网络的IP骨干网互联：业务系统分布式部署在多个数据中心，形成负载分担或灾备冗余，数据中心的前端网络通过IP网络互联，外部用户通过前端网络访问各数据中心，当某个数据中心站点的业务系统发生灾难时，前端IP网络将通过全局负载均衡系统实现收敛，外部用户访问业务资源的请求被重新调度到健康的站点。

7.2 互联方式

互联方式主要包括：

a) 前端网络的VPN互联：由于多个数据中心站点之间存在主次关系，且数量一般不多，前端网络的互联多存在于上级站点和下级站点之间，因此上级站点到下级站点可采用多点网状、点到多点、点到点互联方式。下级站点之间的前端网络互联需求较少，可采用点到点方式。

b) 前端网络的IP骨干网互联：通过IP骨干网进行互联，并支持全局负载均衡，实现对外网用户的访问请求在多个站点内的相同业务系统间进行最优调度。

7.3 关键技术

前端网络的VPN互联可采用以下方式：

——骨干网MPLS VPN互联：不同站点接入的骨干路由器之间建立L3或L2 MPLS VPN，实现支持多点网状、点到多点、点到点方式下的前端网络互联；

——IPSec VPN互联：不同站点出口防火墙之间建立IPSec VPN通道，实现点到点方式的前端网络互联；

——VxLAN VPN互联：不同站点的出口交换机之间建立VxLAN隧道，实现多点网状、点到多点、点到点方式的前端网络互联。

前端网络的IP骨干网互联主要采用多数据中心间的负载均衡技术，对于基于域名方式发布的业务，应支持以分布式部署的全局负载均衡系统的智能DNS方式来实现外网用户访问请求在多个数据中心站点的双活负载均衡；对于基于IP地址方式发布的业务，应支持以分布式部署的服务器负载均衡系统的路由健康注入（RHI），在主站点故障的情况下将外网用户访问请求导入到备用站点，实现正常访问。

8 业务网互联

8.1 概述

业务网指数据中心站点内部署的承载具体应用与用户间交互流量、具体应用各子系统间交互流量的物理网络。由于单个数据中心的空间、电力等资源有限，业务系统部署规模的快速增长会造成本地数据中心出现瓶颈，这就要求本地数据中心站点能实现跨机房的扩展，为业务提供类似本地化的部署能力。通过虚拟化以太网络将新增的机房网络接入到原有的数据中心业务网络，可部署更多的业务系统，并拥有统一的网络出口、安全策略和运维管理。

当前某些网络业务规模快速扩张，在单个数据中心部署业务系统已经难以满足需要，应能实现业务系统集群的跨数据中心站点的部署。为了实现业务的跨站点高可靠性和冗余部署，可在多个数据中心站点部署对应的业务资源，实现站点间的资源动态调配和管理，包括虚拟机在数据中心之间自由迁移。上述业务系统的跨站点扩展同样要求异地站点之间可实现二层网络互联。

在原站点业务系统故障情况下，为保持用户业务访问路径不变，全局负载均衡系统应在数据中心站点间建立虚拟化以太网络，通过该网络将用户请求转发到可用站点内的业务系统进行响应。

8.2 互联方式

数据中心业务网互联一般考虑点到点、多点网状互联两种，互联通道或网络应是二层网络，可采用OTN或DWDM作为二层通道，也可基于传统IP网络来构建二层网络。该二层网络应满足以下要求：

——站点相互独立：数据中心二层互联后，某个站点的故障不会传递到其他站点，如广播风暴；站点内的拓扑互不影响和依赖；

——传输无关性：对站点之间传输数据时使用的技术与站点位置、提供商的网络无特殊要求，要求使用最通用的技术，例如只要求核心网络支持 IP 即可；

——高可靠性：使用多归宿来提供冗余接入，并具有在站点间避免流量环路的机制；

——链路使用效率：站点之间的流量包括组播和广播应充分优化以尽量节省带宽，在具有冗余链路时实现负载分担；

——灵活性：数据中心互联不依赖于站点的拓扑结构，不对站点拓扑结构有特定要求；

——运营维护简单：站点互联使用的技术应简单，可快速新增和减少站点。边缘设备上的配置应尽量简单，并且对站点现有的网络变动最小化，部署过程对流量转发不产生影响。

8.3 关键技术

基于数据中心业务网间特定的虚拟化以太网互联需求，应采用基于VxLAN等二层Overlay网络技术、EVPN控制协议开发的DCI虚拟化以太网络技术，可选技术方案如EVI、EVN、OTV等。

9 存储网络互联

9.1 概述

存储网络是数据中心内部署的承载具体应用系统与存储资源间交互流量的物理网络。对于双活或主备数据中心，为了实现不同DC间存储系统的数据同步和灾备，应借助存储互联网络打通两端存储系统，实现不同站点存储系统间的数据复制。

9.2 互联方式

跨站点的存储SAN互联宜只考虑点到点方式实现站点间的数据同步或异步复制。

9.3 关键技术

跨站点的存储SAN互联宜采用DWDM传输线路或者裸光纤互联，利用基于磁盘阵列的同步/异步复制功能实现主数据中心和备份中心的操作系统、文件系统、数据库的实时拷贝维护。

10 带外管理网络互联

10.1 概述

带外管理网络是数据中心站点内部署的承载运维管理IT系统和运维工作终端与站点各类设备和应用系统间管理维护类交互流量的物理网络。对于同一运营商建设的多站点数据中心，应实现各站点数据中心带外管理网络的安全互联，以方便对多站点数据中心内的计算、存储、网络、安全设备资源进行统一的远程运维管理。

10.2 互联方式

带外管理网络的互联应采用运维管理IT系统所在网络与所有数据中心站点带外管理网络区域的点到多点互联。运维管理IT系统宜部署在中心站点，运维管理IT系统通过内网，以安全受控方式接入到中心站点的带外管理网络区域，通过公网，以SSL VPN或IPSec VPN方式接入到其他下级站点的带外管理网络区域，并实现安全访问控制。

10.3 关键技术

带外管理网络的互联宜重点考虑安全要求，应满足GD/J 037—2011、GB/T 31167—2014、GB/T 31168—2014和GB/T 22239—2019的要求，达到等级保护三级，要求在每个站点的带外管理网络出口部署VPN网关、深度检测防火墙、运维审计系统，以及内部部署CA认证系统。VPN网关和CA系统对通过VPN接入的运维客户端进行双因素认证，深度检测防火墙对内外交互的运维流量进行4层～7层安全检测，运维审计系统和CA系统对运维人员的身份进行认证，对权限进行授权，对行为进行记录审计。

福建省广播电视局办公室　　2019年9月24日印发