思科推出IPTV业务承载网解决方案 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/205/2021_2022__E6_80_9D_E7_A7_91_E6_8E_A8_E5_c101_205600.htm 1. IPTV业务概述 互联网和通信业务发展的更大潜力在于突破终端瓶颈，而电视机是最直接、最有潜力转化的家庭终端。IPTV即是这样一种利用电视作为宽带网络终端的极具发展潜力的业务。IPTV应用能有效地将电视、网络和PC三个领域结合在一起，充分提高了宽带的利用效率，有利宽带产业的理性繁荣。 IPTV将为宽带运营商和内容提供商注入新的活力。宽带运营商除了能给用户提供通讯和资讯方面的服务之外，通过IPTV能为用户提供丰富的、个性化的电视节目，对于吸引用户提高用户ARPU值来说都具有很大的意义，因此有专家认为中国已基本具备了大力发展IPTV的技术条件和市场条件。 在各厂家提供的IPTV解决方案中，人们更多地把目光集中在IPTV业务系统及家庭终端方面，承载网络的作用则被忽略了。并且，从目前来看，运营商仍然采用IP数据网络的建设及运营思路来开展IPTV业务，旧瓶装新酒，是否合适？我们是否需要重新审视IPTV承载网络的建设和运营思路呢？ 2. 思科IPTV承载网解决方案 思科从多年前就预言网络及业务融合将是一种趋势，目前的IPTV业务恰恰可看作是融合网络中的一种关键应用。利用目前的宽带城域网开展IPTV业务，思科提出基于业务的监测与控制、网络品质量化及主动的运维机制、端到端的安全保障等“ 3＋1 ”的运营理念，帮助电信运营商更好的经营自己的网络。 2.1基于业务的监测与控制 随着IPTV等新型业务的开展，运营商必须提高对网络中传送业务的了解和控

制。由于目前的网络管理工具及流量分析工具无法区分视频、VoIP、Web浏览、音乐下载、以及P2P流量等服务，因而不能保障单个业务的服务质量，也不能对其进行有效的控制。思科服务控制平台SCP(Service Control Platform)，能够帮助运营商掌握网络中各种业务（如，P2P、视频流量等）对带宽的占用情况，从而依据一定的业务模型，对网络中的各种业务流量实施灵活的带宽分配策略，以保证IPTV业务得以健康有序的发展。 在Cisco 服务控制平台的帮助下，宽带运营商能够用全新的方法定义和提供宽带服务。运营商可以根据规定的策略，为每个用户以及每种应用提供特定的宽带服务，真正实现宽带服务个性化。 2.2 网络品质的量化及主动运维模式 利用CISCO IP SLA技术为运营商提供全面的服务质量参数检测与分析 当前宽带IP城域网的建设与维护中，对网络整体性能和服务能力的测量评估与长期统计往往成为网络运维与网络管理中被忽略的重要的一环。很多情况下，简单的排错和判断工具并不能提供足够和准确的参考数据，还需要准确和量化的数据以及一段时间内的历史基线统计才可以为运维提供强有力的帮助。 在开展IPTV业务的同时，我们需要考虑如何让传统的运维模式能够适应新型业务的需求，例如：如何定位网络的瓶颈点？如何能够实时、主动验证网络运营状况和精确测量网络端到端性能？如何能验证网络自身的服务水平和服务能力？这些问题都需要十分具体的关于网络性能的统计数字和历史记录，通过比较得出科学准确的结论。 即使网络中实施QOS以后，也并不意味着一劳永逸，因为IP网的流量和结构都会随着用户的变化而变化。要保证网络的质量，还需要对网络进行实时的监控，然后根据实际情况即使进

行调整。否则，即使成功地实施了QOS也会因为网络实际情况的变化而造成部分用户业务质量下降。目前，思科在IOS中提供的SLA Agent功能可以帮助运营商通过网管软件实时地监测网络中任意两点间的时延、丢包率和抖动。 利用CISCO Netflow技术建立一套适合IPTV业务的流量模型分析机制 NetFlow现在是业界最主要的网络流量统计技术。Cisco路由和交换平台中的NetFlow服务可以提供网络流量统计功能。为了更好地运营IPTV业务，运营商可以利用CISCO Netflow技术对IPTV业务流量进行精确的统计和分析，建立一套完整的适合IPTV业务的流量模型分析机制。 通过上述网络服务质量及业务流量的实施监测和长期统计，运营商可以预先定位到网络中潜在的故障点，及时排除故障，从而减少用户投诉，提高用户满意度。 2.3 IPTV业务的安全保护 从安全性的角度来看，IPTV业务承载网不同于传统宽带网。它不但需要像传统宽带网一样防止网络病毒和网络攻击，同时对用户向网络发送的内容是否合法也一定要严格地控制，并对IDC中节目源进行保护。在保证IP网安全性方面，思科已经可以通过自防御网络战略，帮助运营商将网络从被动的防御，转为主动的防御。特别是在对DDOS攻击防护方面，CISCO 提供的解决方案能够有效的保护IPTV的业务服务器，业务管理平台不受DDOS攻击。 利用CISCO Guard 提供IPTV视频源的保护 Cisco Guard解决方案提供完整保护来防御各种DDoS攻击，甚至那些还未出现的DDOS攻击。以积极缓解性能为特色，快速检测攻击，从合法业务中分离出恶意数据包，Cisco Guard解决方案提出以秒计而不是以小时计的快速DDoS响应。该方案容易布署在关键路由器和交换机附近，并且不影响现存的

网络部件的性能和可靠性。 Cisco Guard解决方案套件包括两个独立的组件Cisco Detector和Cisco Guard，两部分协同工作，能为任何环境提供DDoS保护。 Cisco 监测器（CISCO Detector）：作为早期报警系统，Cisco检测器提供对最复杂DDoS攻击的深入分析，搜寻与“ 正常 ”行为的偏差或DDoS攻击的基本行为。攻击被识别后，检测器发警报给Cisco保护器，提供详细的报告和具体警报来快速响应该威胁。例如，即使在没有超出全面界限的情况下，检测器也能观测到从单个源头来的UDP包速率超出了范围。 Cisco保护器(CISCO Guard)：Cisco保护器是Cisco DDoS解决方案套件的基石它是一个高性能DDoS攻击缓解设备，保护IPTV业务中心来的数据资源。 当保护器被通知有一个目标处于被攻击状态（无论是来自Cisco检测器还是其它诸如入侵检测或防火墙的安全监测设备）时，指向目标的业务将被转移到与该目标设备相连的保护器。然后，业务将通过五个阶段的分析和过滤，以除去所有恶意业务使得好的数据包能不间断的继续传送。 保护器位于一个单独网络接口处的路由器或交换机附近，在不影响其他系统的数据业务流情况下实现按需保护。由于它的位置，保护器可同时保护多个可能的目标，包括路由器、Web服务器、DNS服务器、LAN和WAN带宽。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com