

IPv6突如其来企业准备好应对了吗？思科认证 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/590/2021_2022_IPv6_E7_AA_81_E5_A6_82_c101_590384.htm 尽管企业都表示他们在经济上没有部署IPv6网络的优势，出现在今年的FutureNet的小组成员称他们可能在不久后将不得不选择IPv6。 IPv6是下一代的互联网层协议，它是由互联网工程任务小组(IETF)制订的，目的是为解决当前IPv4互联网层协议下IP地址日趋枯竭的问题。如果按照现在的发展态势，互联网IPv4地址将会耗尽，而这显然会导致一系列重大问题。 当我们发现已经没有地址可供使用的时候，不出几个月就会产生问题网络主干将无法添加用户除非能找到更多的地址空间。 然而，到目前为止IPv6的拥护者已经遭遇到的麻烦是经济危机以来，个别企业现在并没有打算将时间和金钱投资到IPv6网络的部署中来。经济危机分散了他们的投资兴趣和投资重心。或许，人们在真正需要IPv6以前不会意识到这种客观需求的存在。 IPv6的安全意义 Scott Hogg是思科认可的IPv6安全手册撰写人之一，他认为，IPv6会为公司网络，即便是那些尚未部署新的互联网层协议的公司，带来重大安全问题。因为诸如Vista和Linux这样的操作系统已经支持IPv6，因此任何使用这些操作系统的网络都可以处理IPv6流量。另外，IPv6地址通过IPv4网络彼此相连是利用在IPv4数据包中装载封装的IPv6数据然后将其传送到以前的网络上实现的。技术方面的原因导致一般情况下防火墙无法为这些IPv4数据包解封，因此也就不能够检查数据包中的数据，这样就无形中为黑客提供了可乘之机。好在一些供应商正携手合作，开始关注这一问题。 创建一个能够同时支

持IPv4和Ipv6的双堆栈转换网络会导致网络漏洞的出现，因为这样的网络会成为黑客攻击的目标。任何创建双堆栈网络的企业应该确保其网络在使用所有IPv6功能前都是安全的。这意味着要首先确保网络周边的安全，强化网络设备以及从网络核心开始部署IPv6然后再向边缘网络辐射。IPv6只能解决部分问题 即便每个企业和ISP都曾打算在网络上成功部署IPv6，但是一些基本的互联网路由可扩展性问题还有待解决。IETF在今年早些时候成立了一个工作组旨在处理多重地址所引发的扩展性问题，同时该机构承认IPv6可能带来一些问题。IETF的举措就是想通过多个承运商来分裂用户网络以达到稳定用户互联网连接的目的。多重地址之所以会引发一系列问题是因为它会增加路由表的大小以至于造成路由硬件的拥堵。英国电信公司的高级网络架构师Tom Nadeau估计我们将会用15年的时间来修复路由问题或者我们届时会需要IPv12。NTT美国的IP工程副总裁Doug Junkins称，虽然路由可扩展性的问题确实存在，但是现在就开始部署IPv6网络也是很重要的，这样可以解决更为迫切需要解决的地址问题。IPv6的通过解决了所有问题中的一部分，但是在这之后还需要有后续发展。他希望在部署IPv6网络后，修复未来路由架构将变得更加容易。更多优质资料尽在百考试题论坛 百考试题在线题库 思科认证更多详细资料 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