解析大规模网络地址转换NAT（LSN）架构思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E8_A7_A3_E6_9E_90_E5_A4_A7_E8_c101_644274.htm 传统的NAT已经使用了15年左右，我们主要通过它为大量专属设备提供少量公共IPv4地址的共享。就家庭用户和小型办公场所而言，其NAT界面外通常只有一个单独的公共IPv4地址。这一公共地址当然是由宽带服务供应商提供。 由于IPv4地址即将耗尽，宽带服务供应商现在正在想办法解决如何继续为其新客户提供IP地址的问题。问题的答案似乎很明显：如果NAT在服务供应商面对的客户端有效，那么它对于客户端所面对的服务商也应该同样有效。这也是大规模NAT(LSN)的基础。 LSN添加了新的转换层，因此，就如同IPv4地址用于CPE NAT内部一样，它们也可以被用来向CPE NAT外部指定地址。 服务供应商在其公共IPv4外指定的地址数达到了LSN设备联网接口的数量。在LSN与客户相连的一端，一个专属IPv4地址块外有一地址172.16.0.0/12它被指定到与CPE NAT相连的每一个界面。然后，每个客户可以使用另一个IPv4地址块通常是10.0.0.0/8来为其网络中的所有设备确立地址。 客户端网络中的设备有可能向带有10.1.1.1源地址的互联网终端发送数据包.而后，CPE NAT会通过附带的端口映射将源地址转换成类似172.16.1.1的地址。在LSN中，源地址会被转换成公共IPv4地址201.15.83.1，且其数据包会被发送到终端。与201.15.83.1响应的数据包会被发送到服务供应商的IPv4地址集，然后再发送到合适的LSN，而后NAT会将该终端地址转换成172.16.1.1，再把数据包转发给对应的CPE NAT，后者会将终端地址转

换成10.1.1.1。 要实现互联网到正确客户网络，再到准确设备的传输，取决于两个条件： 1. 对话由客户端网络发起，因此CPE NAT和LSN才能获取准确的地址和端口映射. 2. 外部路由图总是指向容易被识别的终端。因此，来自公共互联网的数据包可以被传送到服务供应商醒目的IPv4地址集.一旦数据包到达服务供应商的网络，便会有一个更为明确的路由将数据包发送到特定的LSN。LSN拥有从外之内的地址/端口映射，该映射指向一个特定的CPE NAT，而CPE NAT又拥有另一个从一个从外之内的地址/端口映射，可以将数据包发送到与之直接相连的终端，或是为数据包提供一条在客户网络边界里的特殊路由。 这一架构是一个NAT444架构：它将IPv4地址转换成另一个IPv4地址，再转换成第三个IPv4地址。这个方法之所以吸引人是因为可以在不更改现有CPE NAT的情况下，对其进行利用。而NAT不在乎其外部IPv4地址是公共的还是私有的，因此，对于CPE NAT而言，一切没什么不同。服务供应商部署该架构的时候，不需要对客户的设备提出特殊要求，也不需要更改其设备，任何传统NAT都可以使用。 尽管NAT444很简单，但也不是一劳永逸。任何架构，当然也包括LSN在内，可扩展性是我们经常顾虑的问题。对于宽带服务供应商而言，每个客户网络都代表着其CPE NAT背后的若干设备。而每个设备又能生成多个应用数据流。现在，我们还不知道一个单独的LSN究竟能处理多少客户网络，也不知道公共IPv4地址的性能如何。 NAT444有可能出现地址重叠问题，这种重叠发生在客户网络和服务供应商使用的私有地址之间。例如，如果服务供应商在LSN和CPE NAT之间，使用172.16.0.0/12地址块以外的地址，而客户也使用相同的地址

，那么两者之间的唯一性就被破坏，这可能导致数据包误传。要确保客户使用的地址范围与服务供应商所使用的不冲突。 如果用户想将数据包传送到同一NAT之后的其他客户。防火墙，路由ACL甚至是服务器中的过滤政策通常会阻止外部数据包进入拥有专属源地址的网络。为了回避这种过滤，数据包必须通过LSN，以便它们的源地址可以被转换成一个公共地址，然后再将数据包一起传送到终端。即便数据包不通过LSN到达终端，其NAT资源也会被消耗掉。 对于这两些问题，我们建议先留出剩下的公共IPv4空间作为ISP共享地址空间。因为地址块可能会被保留供NAT444架构使用，相同的地址可以和RFC1918地址一样，在不同LSN之后使用。但是由于它们不是RFC1918地址，它们不会与任何客户网络的专有地址相冲突。而且，正由于它们不是RFC1918地址，它们也不好被过滤政策阻止.同一LSN后客户间的数据流就不需要 穿越LSN。 还有一种方法可以解决这些问题。使用LSN和CPE NAT之间的公共IPv6地址。源于客户网络的IPv4数据包会被转换成IPv6数据包，以完成CPE NAT到LSN之间的交接，然后再被LSN转换回IPv4数据包。这一架构就是NAT464架构。 CPE NAT外部的IPv6地址和其内部的IPv4地址不会产生冲突。假设CPE NAT将传入的数据包转换成本地网络的IPv4地址，那么就不会出现过滤的问题，也就不会影响到同一LSN后两个客户端之间的沟通。 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