



双网络层方案——全新的下一代互联网解决方案

李 实

(中国电信股份有限公司上海研究院 上海 200122)

摘 要:传统的下一代互联网方案 IPv6 通过横向扩展地址长度来扩展地址空间,因其不兼容 IPv4 导致长期难以普及。提出一种全新的解决方案,通过纵向扩展协议栈以无限复用整个 IPv4 地址空间,在扩展地址空间的同时可以很好地兼容现有 IPv4 网络,因此升级涉及面极小、成本极低,并可迅速部署完成。

关键词:互联网;下一代互联网;IPv4;IPv6;双网络层

doi: 10.3969/j.issn.1000-0801.2014.08.020

Double-Network-Layer, a New Solution for IPng

Li Shi

(Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China)

Abstract: Traditional IPng solution——IPv6, extends the address space by extending the length of the address laterally. Thus it's incompatible with IPv4 and difficult to promote. A new solution: reuse the IP addresses by extending the protocol stack longitudinally was presented. In this way, it can not only get very big address space, but also have very good compatibility with current IPv4 network. So the upgrade has minimal impact, requires a minimum investment, and can be quickly deployed.

Key words: internet, IP-the next generation, IPv4, IPv6, double-network-layer

1 引言

基于 IPv4 的互联网是由美国军方的网络发展起来的,采用了 32 bit 的地址,总地址空间为 $2^{32} \approx 42$ 亿个。但后来 IPv4 网络迅速扩展到全球,再加上一些比较奢侈的设计浪费了较多的地址,地址资源早已经枯竭。互联网迫切需要一个新的方案来解决地址不足的问题。

2 现有解决方案特点及前景

2.1 IPv6

早在 20 世纪 90 年代初期,互联网工程任务组(IETF)就已经预见到这个问题并着手下一代互联网协议(IP-the next generation, IPng)的制定工作。IETF 在 RFC1550 里进

行了征求新的 IP(互联网协议)的呼吁,并公布了新的协议需实现的主要目标:

- 支持几乎无限大的地址空间;
- 减小路由表的大小;
- 简化协议,使路由器能更快地处理数据分组;
- 提供更好的安全性,实现 IP 级的安全;
- 支持多种服务类型,尤其是实时业务;
- 支持多目传送,即支持多播;
- 允许主机不更改地址实现异地漫游;
- 支持未来协议的演变;
- 允许新旧协议共存一段时间;
- 支持未来协议的演变以适应底层网络环境或上层应用环境的变化;

- 支持自动地址配置;
- 协议必须能扩展,它必须能通过扩展来满足将来互联网的服务需求;扩展必须是不需要网络软件升级就可实现的;
- 协议必须支持可移动主机和网络。

作为对 RFC1550 的响应,包括 SIPP 等在内的若干 IPng 提案被提交到 IETF。最终 IETF 决定以 SIPP 作为 IPng 的基础,同时把地址长度由 64 bit 增加到 128 bit。新的 IP 称为 IPv6。其版本是在 1994 年由 IETF 批准的 RFC1752,在 RFC1884 中介绍了 IPv6 的地址结构(现在 RFC1884 已经被 RFC2373 所替代)。

2.1.1 技术特点

IETF 在 RFC1550 中提出了若干要求,但不幸的是,其中偏偏没有对兼容性的要求。最终选定的 IPng 方案——IPv6,也确实与 IPv4 不兼容。IPv4 的地址空间约为 42 亿个,当这个网络因为地址不足而要升级的时候,可以想象网络中已经有了太多的 IPv4 终端和网络设备。兼容性的缺失导致全球网络升级变得极端复杂与昂贵。

2.1.2 推广面临的困难

虽然用 IPv6 来解决 IPv4 地址不足的问题俨然已是众望所归,但 IPv6 从 1994 年诞生至今已经过去了 20 年,使用范围仍然局限于少数的教育机构和实验场所,没有进行大规模的商用。究其原因,还是因为 IPv6 不兼容 IPv4 所致。

对网络而言,初期 IPv4 地址很多,用户很少,没有升级的必要;后期 IPv4 地址基本耗竭,但同时已经有太多的 IPv4 用户。网络需要升级以允许更多新用户加入,但需要首先解决数以亿计的既有用户的升级问题。实际上,由于 IPv6 与 IPv4 不互通,IPv6 网内可以访问的资源极其贫乏,SP 和用户并没有加入 IPv6 网络的愿望。

2.1.2.1 运营商的困境

(1) 由于西方国家在 IT 产业上的领先,西方国家的 IP 地址资源相对丰富,不急于升级到 IPv6;非西方国家因地址相对匮乏,更有升级的紧迫性。但是同样由于西方在 IT 产业上的领先优势,非西方国家又必须保持访问西方国家 IPv4 网络中的资源的能力。这就导致非西方国家的运营商即使在升级到 IPv6 之后也必须长期向公众提供 IPv4 接入服务(无论运营商自身网络运行在何种协议栈上)而不可能断然关闭 IPv4 服务。

(2) 由于 IPv4 地址紧张,长期以来运营商给每个宽带公众用户只分配 1 个 IP 地址,而用户又确实存在多终端

接入的需求,这导致用户自备 NAT 型家庭网关成为普遍现象,而这些家庭网关又普遍不支持 IPv6。如果运营商希望用户默认使用 IPv6 网络,将不得不为用户提供支持 IPv6 的家庭网关。否则,对用户而言,既然运营商仍然支持 IPv4 接入,那就继续使用原有家庭网关和 IPv4 吧!以中国为例:到目前为止中国已经有了约 2 亿户宽带用户,升级到 IPv6 需要为所有用户更换家庭网关。按保守价格每只 150 元计算,光家庭网关就要花费 300 亿元,代价极为巨大。同时,由于需要上门为用户更换设备,工程量也是巨大的。而这些被换下的用户家庭网关将很难再有新的用处,又形成了巨大的浪费。

(3) 升级到 IPv6 需要大规模地升级网络中的设备(多数是基于硬件的替换),而这个行为客观上只是替换了目前运行良好的 IPv4 设备。运营商投资巨大却无实际回报,从企业运营的角度来说不是个理性的行为。所以运营商更倾向于深入挖掘已有 IPv4 设备的潜力而没有升级到 IPv6 网络的积极性。

(4) 就过渡方案而言,兼容性太差会严重影响网络的正常使用,兼容性太好又会让用户感觉没有必要切换到 IPv6 网络,从而导致 IPv6 迟迟不能成为主流。目前主流运营商已经计划通过 NAT444、DS-Lite 和 LAFT 等技术来过渡。这些技术都包括了运营商给用户分配私网 IPv4 地址+NAT,在解决 IPv4 接入的同时又导致网络进一步向 NAT 结构的 IPv4 网络深度深化了。同时一些主流过渡方案也要求运营商对用户的家庭网关拥有最高控制权,这也导致必须由运营商来负责给用户家庭网关。

(5) 运营商需要为过渡准备若干软硬件设备,而这些设备仅仅是在过渡过程中临时使用的,在过渡完成后将没有任何价值,也形成巨大的浪费。

2.1.2.2 SP 的困境

IPv4 网络采用 32 bit 的地址标识主机,而 IPv6 网络采用 128 bit 的地址标识。对于很多在应用层标识主机的应用而言,如果要升级到 IPv6,必须修改应用层的主机标识。而要做到这一点,往往意味着软件甚至在应用层面也必须做出较大的调整。事实上这是所有在 IP 网络上提供较大范围业务的组织的困境,包括通常意义上的互联网 SP、拥有复杂内部业务网络的大型企业以及拥有诸多业务平台的运营商。对他们而言,这个升级实际上也只是替代了目前运营良好的业务系统,并没有功能的增强或者性能的提升,也是投入巨大但没有实际回报的行为。



另一方面,既然运营商仍然支持用户的 IPv4 接入,即使分配给用户的是私网地址并且需要经过 NAT 才能访问 SP 提供的业务,经过这么多年的发展,对大多数业务而言,这种模式也已经工作得足够好。也就是说,业务本身不要求 SP 升级。

如果 SP 不升级,那么将来还可能面临公网 IPv4 地址不足导致服务器无法开通的问题。考虑到目前有大量公网 IPv4 地址是动态分配给宽带用户的,随着分配私网地址的过渡方案的逐渐成熟,收回一些公网地址给服务器使用将是很容易做到的事。那么地址不足的问题对服务器而言也不复存在了。既然如此,为什么还要升级到 IPv6 呢?

2.1.2.3 宽带用户的困境

对宽带用户而言,升级不仅没好处,反而可能有诸多不便之处:需要追加投资、升级操作系统、更换家庭网关等。但因为网络转发 IPv6 报文效率偏低以及 IPv6 网络上资源不足等原因,用户得到的却是网络体验的下降。而如果什么也不做,现有的网络已经能够很好地满足需要。既然如此,为什么要升级到 IPv6 呢?

2.1.3 小结

概言之,对运营商、SP 和宽带用户而言,升级到 IPv6 带来的感受都是负面的。眼下就要付出很大的代价,面对很大的麻烦,好处却还在遥远的未来。所以各方都是口号大于行动也就很好理解了。

在 2011 年 6 月举办的“世界 IPv6 日”活动上,有不少专家认为:“尽管 IETF、ISOC 和其支持者正在不遗余力地推广 IPv6,但是 IPv6 并不是一件必然要发生的事情。”

2.2 NAT

网络中的地址至少有两个含义:主机在网络中的唯一标识;网络将报文转发至主机的寻路依据。NAT 协议通过为内网主机分配私网地址,并将私网的 IP:port 对映射为公网的 IP:port 对,一定程度上缓解了 IPv4 地址不足的问题。但 NAT 为主机分配私网地址,导致主机失去了网络中的唯一标识。NAT 破坏了网络的对称性,导致网络日益向 CS 结构演化。同时,家庭网关层面采用 NAT 技术也没有彻底解决 IPv4 地址不足的问题,运营商仍然缺乏足够的地址分配给用户。

前已述及,运营商计划通过给用户分配私网 IPv4 地址+NAT 将新用户接入 IPv4 网络。这样的方案同时包括在主流运营商优选的几个过渡方案如 NAT444、DS-Lite 和 LAFT 4over6 等方案中,虽然细节各有不同。虽然 NAT 的引入会破坏网络的对称性,但 NAT 技术在家庭网关上的

广泛应用已经充分证明了它的生命力。

虽然这些方案都是作为过渡方案出现的,但这些方案应用后的确会有效缓解 IPv4 网络中地址不足的问题。如果业界以 IPv6 为下一代互联网解决方案,考虑到所有各方升级到 IPv6 将要付出的成本和面对的麻烦,有理由相信这些过渡模式中的 NAT 成分会得到充分的发展。人们会信任并依赖这些方案中包含的 NAT 技术而忽略这些方案中的 IPv6 部分,地址不足不再是个问题,进而网络会长期停留在“过渡阶段”并失去向 IPv6 演化的动力。

3 IPng 应有的特点

如果不希望网络长久地停留在迈向 IPv6 的过渡状态中,不希望网络长久地停留在被 NAT 破坏了对称性的状态中,那么应该重新考虑:下一代互联网解决方案,是否有更好的选择?

IPng 应该具备哪些特点? 1993 年 IETF 提供的 RFC1550 列举了若干条件,唯独没有要求与已有的 IPv4 兼容。20 年后再来审视这份文稿,已经可以清晰地看到兼容性要求的缺失导致网络升级所面临的巨大困难。因为 IPv6 与 IPv4 不兼容,升级迟迟不能完成,甚至在 IPv4 地址已经耗竭的今天,仍然没有足够的乐观的理由。

有理由要求一个合格的 IPng 技术必须同时具备两个特点:地址空间充分大,以解决 IPv4 地址不足的问题;与 IPv4 网络兼容,以方便顺利升级。

一个偶然的机会,笔者想到了一个可以同时满足上述两个要求的方案。因为高度兼容 IPv4 网络,需要升级的网络设备极少,升级既经济又容易,与 IPv6 方案相比成本几乎可以忽略不计。在此将这个新方案介绍给大家。

4 新思路:双网络层方案

4.1 协议栈

新协议在原 IP 层之上增加一层,放入报文的源、目标主机的域名——姑且称之为域名层。以常见的 IP over Ethernet 为例,增加了域名层的新协议栈如图 1 所示。鉴于原协议被称为 TCP/IP,此处姑且将新协议称为 TCP/DN/IP (DN=domain name)。

新协议使用域名作为主机全球唯一的标识和寻址依据。

新协议在域名覆盖的范围内(可以包括部分或全部子域)使用整个 IPv4 地址空间进行编址,因此域名还可代表 IP 域。

层次	层名	关键信息
6	(HTTP/FTP/...)	
5	(TCP/UDP/ICMP/IGMP...)	源、目标端口等
4	domain name	源、目标主机域名
3	IP	源、目标IP地址
2	Ethernet	源、目标MAC地址
1	物理层	

图1 TCP/DN/IP 协议栈

IP 域的特点如下。

- 每个 IP 域独立编址,IP 地址在单个 IP 域内唯一。
- IP 域内的路由器按传统方式根据 IP 地址转发报文。也就是说,IP 域内的 IP 路由器不需要升级。(TCP/DN/IP 报文因为没有修改 IP 层报文格式,仍是标准的 IP 报文,在 IP 域内转发时可以在传统 IP 路由器上正常转发)。
- 不同的 IP 域在 IP 层不互通。报文跨 IP 域转发时,需要域名路由器(domain name router,DNR)根据报文头部的域名层信息进行转发。

不考虑少数被保留用于特殊目的的地址段,目前的 IPv4 地址正是在全球范围内统一编址的,正好符合定义,姑且称之为“全球域”。

第 4.2 节的“转发场景”可帮助理解上述概念、特点以及本方案的实现机制。

4.2 完整的转发场景

4.2.1 跨域访问

如图 2 所示,有 3 个 IP 域,分别是全球域(.)、中国国家域(cn.)和美国国家域(us.)。每个 IP 域独立编址。不同的 IP 域在 IP 层不互通,须通过域名路由器转发。

图 2 中各设备基本配置见表 1。

表 1 典型流程中各网络设备基本配置

设备	IP 域	域名地址	IP 地址
cn 域内主机	cn.	host.cn.	100.100.100.100
CN DNR	cn.	dnr.cn.	1.1.1.1
CN DNR	.	dnr.cn.	2.2.2.2
US DNS	.	dns.us.	3.3.3.4
US DNR	.	dnr.us.	3.3.3.3
US DNR	us.	dnr.us.	1.1.1.1
us 域内主机	us.	host.us.	100.100.100.100

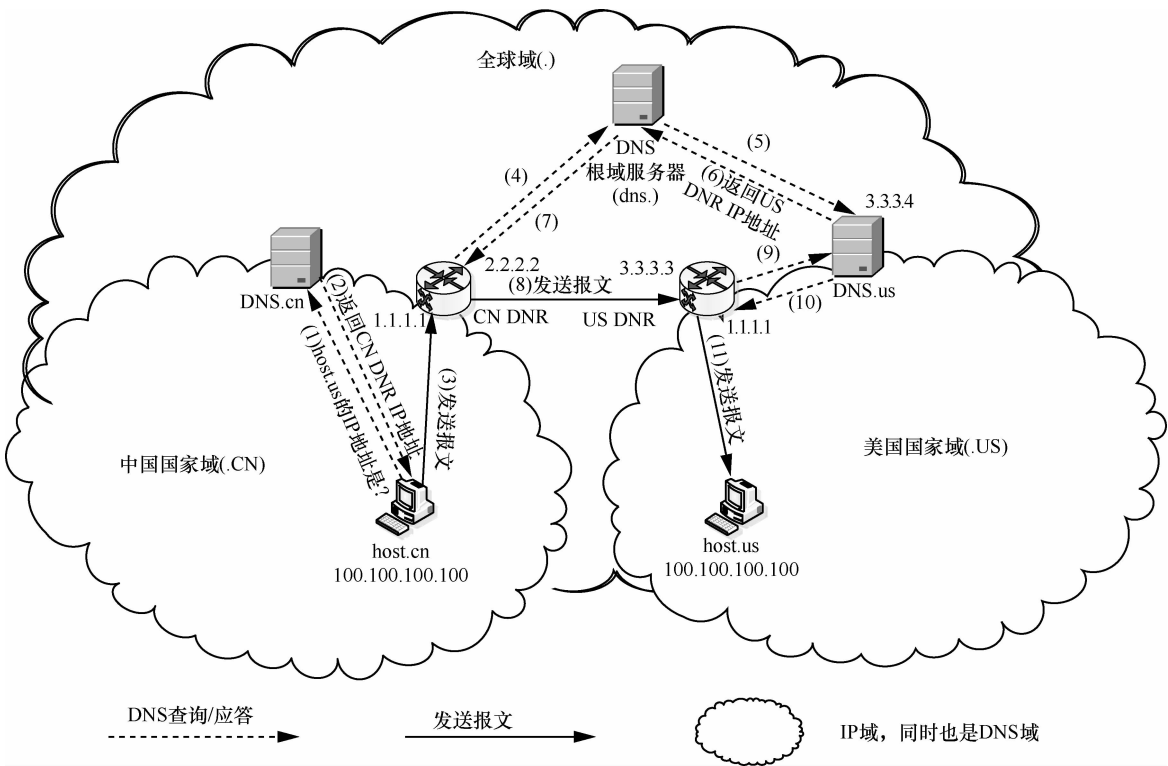


图2 典型的 TCP/DN/IP 报文跨域转发流程



可以看到,由于划分了不同的 IP 域,同一个域名在不同的域中可以映射为不同的 IP 地址,不同域中的主机也可以拥有同样的 IP 地址。

另外,需要在 DNS 中新增 DNA 资源类,已升级的主机在 DNS 中注册 DNA 资源,仍旧映射为 IP 地址,用以告知查询方目标主机已升级。未升级的主机只有 A 类型的资源。

host.cn 向 host.us 发出的报文全程转发流程如下。

(1)host.cn 向本域的 DNS 服务器查询 host.us 的 IP 地址(DNA 资源类型)。

(2)dns.cn 在 cn 域内的接口上维持表 2 所示的解析。

表 2 dns.cn 在 cn 域内的解析

域名	类型	IP 地址
host1.cn.	A/DNA	xxx.xxx.xxx.xxx
...	A/DNA	xxx.xxx.xxx.xxx
hostn.cn.	A/DNA	xxx.xxx.xxx.xxx
*,	DNA	1.1.1.1

此表将域内的域名(以 cn.结尾)解析为对应的域内 IP 地址,将所有其他域名(根据 DNS 命名规则,一个域名要么属根域,要么属根域的子域,必然可与“*”匹配)解析为通向全球域的 DNR 的 IP 地址。

在本例中,dns.cn 发现是域内主机在查询域外主机 host.us,返回相应的 CN DNR 在 cn 域内的接口 IP 地址:1.1.1.1。

(1)host.cn 收到 DNS 查询结果后,域名层填入 host.us 为目标地址,host.cn 为源地址,IP 层填入 DNS 返回的 CN DNR IP 作为目标地址,见表 3,然后将报文发出。

表 3 host.cn 发送报文前的报头内容

协议栈层次	源、目标主机地址
域名层	Dst: host.us Src: host.cn
IP 层	Dst: 1.1.1.1 Src: 100.100.100.100

(2) 此报文被 cn 域内的所有 IP 路由器作为标准 IP 报文转发,并最终抵达 dnr.cn。

(3) dnr.cn 收到报文后,发现目标地址是 host.us,在全球域内查询 host.us 对应的 IP。

(4) 全球域 DNS 维持的表格中包含表 4 所示记录。

表 4 全球域 DNS(dns.)解析

域名	类型	值
us.	NS	3.3.3.4

根据 DNS 的实现机制,全球域中的 DNS 3.3.3.4 负责解析 us.域内的域名。此时查询会被转向到 dnr.us。

dns.us 面向全球域的接口维持这样的解析表格,见表 5。

表 5 dns.us 在全球域内的解析

域名	类型	值
*,us.	DNA	3.3.3.3

也就是说,对所有从 us.域外查询 us.域内主机的请求,一律返回 3.3.3.3。

对于 dnr.cn 的查询 host.us 的请求,DNS 最终返回 3.3.3.3。

(5)dnr.cn 将 IP 层的目标地址替换为 DNS 返回值,IP 层的源地址替换为本机出口地址,见表 6。

表 6 dnr.cn 转发前的报头内容

协议栈层次	源、目标主机地址
域名层	Dst: host.us Src: host.cn
IP 层	Dst: 3.3.3.3 Src: 2.2.2.2

然后,dnr.cn 将报文从全球域端口发送出去。

(6) dnr.us 收到报文后,在 us.域内通过 DNS 查询到 host.us 的 IP 地址为 100.100.100.100,将 IP 层目标地址替换为 DNS 返回的 100.100.100.100,IP 源地址替换为 dnr.us 出口地址 1.1.1.1,见表 7。

表 7 dnr.us 转发前的报头内容

协议栈层次	源、目标主机地址
域名层	Dst: host.us Src: host.cn
IP 层	Dst: 100.100.100.100 Src: 1.1.1.1

然后将报文从 us.域内接口发出。报文在 us 域被若干 IP 路由器视为普通 IP 报文转发,直至抵达目标主机 host.us。

作一个类比:IP 报文穿越不同的以太网广播域时,IP 层的源和目标地址保持不变,而 MAC 层的源和目标地址在不停地变化。TCP/DN/IP 报文穿越不同的 IP 域时,域名层的源和目标地址保持不变,而 IP 层的源和目标地址在不停地变化。两者的思路是一致的。

最后,由于域名层含有源地址“host.cn”,反向报文可以循相同的机制返回。

4.2.2 域内访问

(1)hostA.cn (已升级主机) 发出基于 TCP/DN/IP 的 DNS query 到 DNS 服务器, 查询 hostB.cn 的 IP 地址 (DNA 资源类型)。

(2)DNS 服务器发现是域内主机在查询域内主机的 IP 地址, 返回 hostB.cn 的 IP 地址。

(3)hostA.cn 将 hostB.cn 和 hostA.cn 分别作为报文的目标地址和源地址填入报文的域名层, DNS 返回的 IP 地址作为目标地址填入 IP 层, 即可正常访问 hostB.cn。

可以看到, 域内的访问流程与既有模式是完全一致的。值得一提的是, 本协议中在单个 IP 域内域名与 IP 地址保持一一对应关系, 既可以用域名标识主机, 也可以继续使用 IP 地址标识主机。这个特点为那些只需要在单 IP 域内运作的业务平台提供了很大的方便——它们根本就不需要升级。

4.3 NAT 家庭网关之后的终端接入方案

如前所述, 目前 NAT 型家庭网关得到了最为广泛的应用。

TCP/DN/IP 报文无法通过 NAT 路由器 (即使能通过, 因为 NAT 路由器无法进行反向映射, 返回的报文将无法到达正确的内网主机)。

可以考虑用如图 3 所示的方案来解决这个问题。如图 3 所示, 在 IP 层与 DN 层之间再插入一个标准的 UDP 层。这个新增的 UDP 层可以保证报文正常通过 NAT 网关。需要为 TCP/DN/IP 分配一个标准的 UDP 端口, 所有支持 TCP/DN/IP 的设备都在这个端口侦听, DNR 则仍然按前述规则根据域名转发。

层次	层名	关键信息
7	(HTTP/FTP/...)	
6	(TCP/UDP/ICMP/IGMP...)	源、目标端口等
5	domain name	源、目标主机域名
4	UDP	源、目标端口
3	IP	源、目标 IP 地址
2	Ethernet	源、目标 MAC 地址
1	物理层	

图 3 可通过 NAT 路由器的 TCP/DN/IP 协议栈

用户不必对 NAT 路由器做任何改动, 只要升级所有的终端使用这样的协议栈, 就可以同时实现多终端接入以及对全球网络的无障碍访问。

如果将来家庭网关设备商生产支持 TCP/DN/IP 的路

由器, 那么每个家庭内部将有一个独立的 IP 域, 而且仍然只需要运营商分配 1 个 IP 地址作为 WAN 口地址, 路由器根据域名进行转发, 那么家庭内部可以接入任意多个主机并且全部全球可达。

这个设计还有个附带的优点是: 升级对用户的影响是正向的。用户如果不升级家庭网关, 那么可以获得与当前一样的服务 (可以主动发起连接, 但不能接收传入的连接); 用户如果升级家庭网关, 那么家庭所有终端就外部可达了。因此用户会倾向于主动升级。

4.4 域名解析方案

4.4.1 DNS 响应规则

比较前述跨域访问与域内访问的全过程, 可以发现在两种场景下主机的行为并无不同。差异完全来自 DNS 的解析机制。事实上本方案嵌入的域名层成为了新的网络层, DNS 实际上构成了域名层的路由平面。

- 本方案中 DNS 响应规则如下。
- 对于同域的查询, 返回目标主机在本域内的 IP 地址。
 - 对于跨域的查询, 返回可以转发报文到目标域的 DNR 在本域内的接口 IP 地址。

在这个机制中, DNS 实际负责域名层的路由, 而 DNR 只负责转发。

4.4.2 固定域名解析

DNS 中增加一个 DNA 资源类型, 值为升级后的 TCP/DN/IP 主机的 IP 地址。DNS 以此方式告知查询发起方: 目标主机已支持 TCP/DN/IP。

主机完成升级后增加 DNA 类型的项目到 DNS 数据库中。

4.4.3 动态接入用户的域名自动配置方案

新协议要求每台主机都需要一个可解析的域名。这对原先已有域名的网站来说不是问题, 但动态接入的宽带用户则比较麻烦。目前的宽带用户多数是按需接入并动态分配 IP 地址的, 如果为它们提供可解析的域名, 则 DHCP 系统要进行调整, 涉及几乎所有的宽带用户 (数以亿计)。建议采用如下的自动配置主机域名方案, 只需对 DNS 稍作调整, 即可给动态接入的主机分配合法、可访问的域名而完全不必触及 DHCP。

自动配置主机域名方案如下。

(1) 在本域 DNS 中添加 localdomain 对应的别名, 值设置为本域域名。譬如 cn. 域内就将 localdomain 对应的别名设置为“cn.”。

(2) 升级到 TCP/DN/IP 的主机接入网络后, 按传统方



式通过 DHCP 向网络申请 IP 地址和 DNS 服务器。

(3)主机在配置 IP 并得到 DNS 地址后,向 DNS 服务器查询“localdomain”对应的 CName 字段,并将返回的别名设置为本机所在域的域名。

(4)将本机的 IP 地址的点分十进制字符串,用“[]”括起来作为主机名。

(5)通过以上方式生成本机的完整域名。譬如一台主机分配到的 IP 地址是 100.100.100.100,所在域是“cn.”,那么按这个规则生成的域名就是“[100.100.100.100].cn”。也可以考虑采用其他编码方式如十六进制等以充分缩短域名长度。

(6)可以考虑前述生成规则允许嵌套(例如当主机位于支持 TCP/DN/IP 的家庭网关之后时),这样会生成诸如“[192.168.1.10].[100.100.100.100].cn”形式的地址。这样的地址客观上具备源路由性质,但过长的域名同时也会降低报文的效率,需要谨慎考虑。

网络上的 TCP/DN/IP 主机在解析域名时,先比较目标主机所在域与本机所在域是否相同。若相同,视为处于同一个域。再看去掉域名后最右的部分是否符合自配置的主机域名的格式。如是,则直接从中还原出 IP 地址,不必再向 DNS 查询。其他情况仍旧向 DNS 查询目标主机 IP 地址。

(7)还可以再扩展一下:假设一个 NAT 网关公网地址为 100.100.100.100,一台位于该 NAT 网关之后的主机地址为 192.168.1.10,在 UDP 端口 2000 侦听 TCP/DN/UDP/IP 格式的报文,而 NAT 网关已经预先配置好将 UDP 端口 2010 映射到该主机的 2000 端口。该主机知道自己位于 NAT 网关之后并且知道端口对应关系,则可以将自己的地址配置为[100.100.100.100:2010].cn。域内其他主机看见这样格式的目标地址时,即可启用 TCP/DN/UDP/IP 协议栈并将目标端口设为 2010。通过这种方式,NAT 网关之后的多台主机能够接收外部发起的到 TCP/DN/UDP/IP 协议栈任意端口的传入连接。

这个机制同时还会带来另一个好处:主机除了在接入时查询一次本域域名外,同域其他主机访问时不需要查询 DNS,充分节省 DNS 资源。

4.5 过渡方案

4.5.1 未升级主机访问域内主机

(1) hostA.cn(未升级主机)向 DNS 服务器查询 hostB.cn 的 IP 地址(A 型资源)。

(2) DNS 服务器发现查询的是本域的目标主机,返回 hostB.cn 的 IP 地址(A 型资源)。

(3) hostA.cn 通过 TCP/IP 与 hostB.cn 通信。

此例中无论 hostB.cn 是否已升级,hostA.cn 均可使用 TCP/IP 与 hostB.cn 正常通信。

事实上,如果 hostA 没有访问域外主机的需求(可以相信较长一段时间之内 cn 域会是中国唯一的 IP 域,亦即用户没有访问境外主机的需求),那么用户主机甚至不需要升级。

4.5.2 已升级主机访问域内主机

(1)hostA.cn(已升级主机)发出基于 TCP/DN/IP 的 DNS query 到 DNS 服务器,查询 hostB.cn 的 IP 地址。为了促进全网早日完成升级,操作系统默认优先查询 DNA 类型。

(2)DNS 服务器发现查询的是本域目标主机,应返回 hostB.cn 的 IP 地址:

- 如果数据库中有对应于 hostB.cn 的 DNA 资源类型,说明 hostB.cn 已升级,返回标明为 DNA 类型的 IP 地址;
- 如果数据库中只有对应于 hostB.cn 的 A 资源类型,说明 hostB.cn 未升级,返回标明为 A 类型的 IP 地址。

(3)hostA.cn 收到 DNS 查询结果:

- 如果收到的是 DNA 类型的返回结果,说明目标主机已升级,采用 TCP/DN/IP 与之通信;
- 如果收到的是 A 类型的返回结果,说明目标主机未升级,采用 TCP/IP 与之通信。

4.5.3 未升级主机访问域外主机

未升级主机是无法访问域外主机的。本方案可以自然地用户导向指导升级的网页。

(1)host.cn(未升级主机)发出基于 TCP/IP 的 DNS query 到 DNS 服务器,查询 host.us 的 IP 地址(A 型资源)。

(2)DNS 服务器发现这是一个域外的主机域名,且源主机未升级(因其查询 A 型资源),返回引导升级的 Web 服务器的 IP 地址。

(3)host.cn 如果是想打开目标主机上的 Web 网页,此时会自然打开引导升级的 Web 页面。

4.5.4 已升级主机访问域外未升级主机

4.5.4.1 NAT 方案

如图 4 所示,本场景中,中国国家域内的主机 host.cn 和 DNS.cn 均已升级,而全球域中的目标主机 server.com 未升级。

步骤(1)~步骤(3)同第 4.2.1 节,步骤(4)如下。

CN DNR 收到报文后,发现目标地址是 host.us,在全球域内查询 host.us 对应的 IP 地址。由于 server.com 未升级,

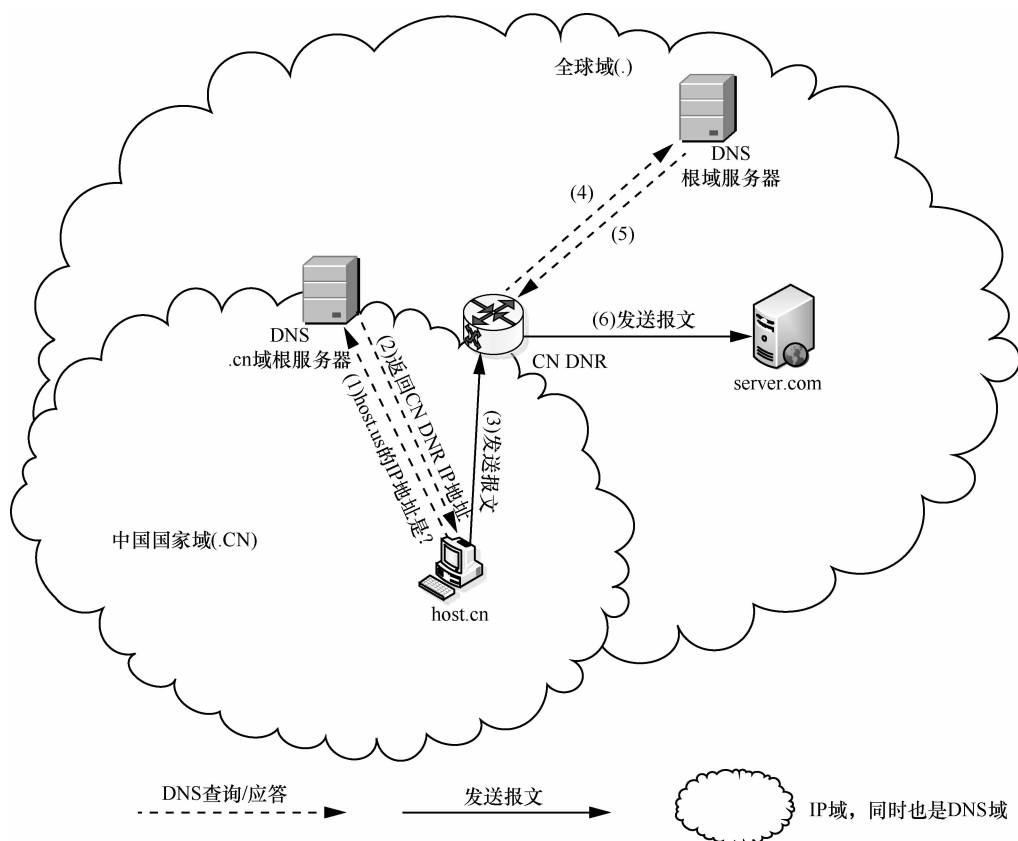


图4 TCP/DN/IP 主机访问 TCP/IP 主机-NAT 型过渡方案

CN DNR 只能得到一条 A 记录的返回。

- 如果继续转发报文到 server.com, 连接将会因为 server.com 无法解析 TCP/DN/IP 协议栈而失败。为避免这种情况, CN DNR 转入 NAT 模式, 将 cn 域内的 (DN $\leftrightarrow$ DN) 报文映射为全球域内的 (IP $\leftrightarrow$ IP) 报文。
- 目前已经从 IANA 申请到的所有 IP 地址均可视为全球域中的地址, 可作为此 NAT 中的源地址。由于地址数量充足, 此处的 NAT 甚至不需要进行端口转换。此举可以节省相当多的路由器资源。

本方案属过渡方案, 是 DNR 的可选功能。

4.5.4.2 VPN 方案

通常 NAT 方案已经满足要求。有一些特殊的应用如果未及时升级, 可能会因为 ALG 问题不能成功连接。此时用户可选择 VPN 方案。

(1) 用户通过 TCP/DN/IP 连接到全球域内的 VPN 服务器, 获得一个全球域内有效的 IP 地址。此时即可通过 TCP/IP 访问全球域内任意主机。

(2) VPN 建立期间, 主机同时拥有两个 IP 域的 IP 地

址, 可能会导致一定的混乱。可以考虑利用协议栈区分两者。即, 只用 TCP/DN/IP 访问物理接口所在的 IP 域, 只用 TCP/IP 访问 VPN 接口所在的 IP 域。需要为两个协议栈启用独立的路由表。

(3) 运营商鼓励用户和服务提供商尽快升级操作系统。VPN 方案可交由社会上独立的商业机构运营, 运营商不一定需要自己建立这样的服务器。互联网上现有的 VPN 提供商的服务器稍加改造即可提供此项服务。

4.5.4.3 部署策略

客观上, 过渡技术始终面临一个悖论: 如果新技术的兼容性不好, 那么会面临强烈的反对; 如果兼容性太好, 那么用户根本没有过渡的愿望。所以运营商必须在过渡技术的选择上寻找一个平衡点。

事实上, 运营商可以完全不部署本节描述的两个过渡方案, 只需要在主流网站和多数终端升级之后从全球域中分离出国家域。这样, 未升级的主机将无法完成跨域的访问, 未升级的服务器也无法响应跨域的请求, 如此也可以对用户和服务商形成升级压力, 促进全网加速升级。



5 升级路线

5.1 运营商网络升级

5.1.1 DNS 服务器

IP 域内的全部 DNS 服务器需要升级以按前述本协议的响应规则动作。理论上在域边界上至少设置一台本域的 DNS 服务器以响应外部主机查询本域主机地址的请求。

同时所有 DNS 服务器在数据库中新增 DNA 数据类型,升级到 TCP/DN/IP 的主机在 DNS 数据库中配置此数据。查询方借此可获得被查询方是否已完成升级的信息。

5.1.2 边界路由器

将域边界(相当于国际出口)上的路由器升级为 DNR。这个升级可能是基于硬件的,但网络一直在扩张,换下来的路由器可以用在 IP 域内其他节点,不会形成浪费。

国际出口链路通常有多根,域边界 DNR 也可能不止一台。DNS 可以顺次返回不同的 DNR 域内接口地址给查询者以引导流量至不同的出口链路,以实现流量均衡。

5.2 用户主机升级

5.2.1 家庭网关

家庭网关可以有如下调整办法。

(1) 家庭网关工作在二层桥接模式(关闭 NAT 功能)。运营商给用户多个终端分配同网段的 IP 地址。此方案可以让用户使用 TCP/IP 访问域内主机、使用 TCP/DN/IP 访问全球主机,但要求运营商分配较多的地址资源。

(2) 家庭网关工作在三层路由模式(关闭 NAT 功能)。运营商给用户分配 WAN 口地址以及 LAN 网段的地址段。此方案可以让用户使用 TCP/IP 访问域内主机、使用 TCP/DN/IP 访问全球主机,但对运营商要求较高,运营商不仅要有足够的资源分配给用户,同时还要考虑分配的技术,如用户的 LAN 网段的地址段如何分配(手工还是自动分配),用户的内网路由如何与运营商的网络路由协同。

(3) 家庭 NAT 网关保持不变

- 用户终端继续使用 TCP/IP,按传统方式访问域内其他主机。
- 用户终端使用 TCP/DN/IP 中的 TCP/DN/UDP/IP 协议栈,访问全球已升级主机。

(4) 长远来看,家庭网关会向支持 TCP/DN/IP 发展。此时运营商只需要分配 1 个 IP 地址给用户,用户的 LAN 网

段自成 IP 域,自行分配地址即可。此时只需要做一个事情:将用户的 TCP/DN/IP 路由器注册到 Internet 的域名系统以实现正常解析。

比较而言,方案(1)、方案(2)对地址资源要求比较高,而且技术较复杂,运营商需要调整为数众多的接入层设备。同时,因为需要分配较多的地址给用户,将来可能不得不设立省级 IP 域,会带来较大的复杂度(譬如,如果运营商只在国家级设一个 IP 域,那么运营商的业务平台系统都在同一个 IP 域中,现有平台不需要任何调整,可以继续运行在 TCP/IP 上。而如果设立省级 IP 域,则运营商的业务平台系统需要升级以支持 TCP/DN/IP),不是笔者推荐的方案。方案(3)则比较合适,无论运营商还是用户都不需要调整。如果有合适的协议让新增的 TCP/DN/IP 路由器可以自动注册到域内 DNS,方案(3)可以自然发展到方案(4)。

5.2.2 开发平台

在操作系统升级之后,业界主流的开发平台需要及时升级,提供新的 API 以支持新的协议栈。以此为基础,应用软件可以及时升级以使用新的协议栈。

5.2.3 操作系统

用户如果不升级操作系统,不影响对域内主机的访问。

操作系统升级后处于 TCP/IP 和 TCP/DN/IP 的双栈模式。操作系统升级以支持 TCP/DN/IP 后:

- 按第 4.4.2 节的方案配置本机;
- 为了支持 VPN 过渡方案,主机还应当支持在 VPN 接口启用时,根据协议选择网络端口的路由方式(如第 4.5.4.2 节所描述)。

5.2.4 应用软件

5.2.4.1 客户端(发起方)

将目标主机的域名传递给操作系统提供的新 API,理论上就足够了。

有些应用层携带的 IP 地址信息,如 FTP、H.323 等,这些协议/应用需要升级,用域名代替 IP 地址才可以在跨域的 TCP/DN/IP 网络上正常运作。

5.2.4.2 服务端(接收方)

软件打开一个 TCP 端口进行侦听时,操作系统自动在 TCP/IP 和 TCP/DN/IP 两个栈上同时打开。如果软件涉及具体的 IP 地址,那么需要用域名代替 IP 地址;如果软件不涉及具体的 IP 地址,那么服务端软件就随着操作系统的升级而自动升级了。

5.3 平滑升级方案

第一阶段,业界形成共识,确定 TCP/DN/IP 方案为下一代互联网方案。然后通信设备厂商研发支持 TCP/DN/IP 转发的 DNR,DNS 软件供应商研发支持 TCP/DN/IP 解析规则的 DNS 升级版本,操作系统厂商准备支持 TCP/DN/IP 协议栈的 OS 升级版本,开发软件供应商提供支持 TCP/DN/IP 的 API 等。

第二阶段,政府发出公告,向社会公示下一代互联网升级方案,并明示不升级的主机可能面临的访问限制。运营商部署 DNS(暂时按传统规则解析)和 DNR(暂时无流量)、用户升级操作系统,服务提供商根据开发软件供应商提供的新接口升级自己的应用软件。这个方案需要至少一台全球 DNS 根服务器升级。各方可以自行升级,不必以其他任意一方已升级为前提。

第三阶段,运营商从 DNS 查询的资源类型比例统计出网络中已升级终端比例。当新协议支持率达到一定比例时,可以确定升级 0 时。0 时到来时,让 DNS 按 TCP/DN/IP 要求进行解析,正式从全球域中分离出国家域,将流量引导至 DNR 进行跨域转发。国家域一旦分离,可能出现第 4.5.3 节描述的“未升级主机访问域外主机”以及第 4.5.4 节描述的“已升级主机访问域外未升级主机”两种需要特殊处理的情况,按各自的预案处理即可。由于操作系统已经准备好了升级版本,境外的未升级主机可以认为不打算接受 TCP/DN/IP 主机的访问,可以考虑为这样的访问提供 NAT,也可以直接忽略这样的主机。

在升级阶段可能遭遇 DNR 和 DNR NAT 性能瓶颈。国际出口可能有巨大的流量,需要较多的路由器(包括 NAT)资源。同时,本方案采用长度可变的域名作为唯一寻址依据。比起定长的 IPv4/IPv6 地址,路由器在处理变长的地址时效率会略低。对策为:多设置 DNR 数量。在遇到跨域查询时,DNS 返回不同的 DNR 的 IP 地址作为网关,可以有效地均衡负载。

6 方案优势

(1)此方案与既有 IPv4 网络兼容度极高。IP 域内所有三层设备不需要升级。包括运营商设备中的绝大多数,单此一项就可为运营商节省大量投资。

(2)本方案不要求家庭网关升级。推荐的方案是保持 NAT 网关不动,任其自行向 TCP/DN/IP 路由器演进。目前中国有 1.9 亿户宽带用户、全球有 6.7 亿户宽带用户,

除欧美(约 2 亿户用户)地址比较富裕之外,其他地方(包含中国共 4.7 亿)绝大多数宽带接入用户不可避免地用到 NAT 型家庭网关。对比 IPv6 方案必须升级家庭网关的要求,本方案既可以在经济上、工程上和时间上做到极其可观的节省,同时也完全避免了家庭网关对升级形成的阻碍。

(3)DNS 需要升级,但数量极为有限,与家庭网关和路由器的数量不在同一数量级上,且升级基本属于软件升级。另外 IPv6 方案一样要求 DNS 升级(只是可能很多 DNS 已经完成了这个工作而已)。但是本方案要求 DNS 做一点路由平面的控制工作,这是特别的地方。

(4)边界(初期相当于国际出口)上的路由器需要升级为 DNR,但数量也极其有限。同时由于网络仍处于扩张当中,换下的路由器可用于网络其他节点,不会造成任何浪费。截至 2013 年底中国出口总带宽 3.4 Tbit/s。如果 DNR 可以在 10 Gbit/s 链路上线速转发(包括 NAT),那么需 340 条链路。如果用高密度服务器或者插卡式路由器,也就 20~30 台,占用的机房面积也很小。如果可以在更高速率的接口上实现,数量还可以大大缩减(视业界实现水平而定)。

(5)此方案中地址空间是真正无限的。IPv6 的地址虽然号称无限,但其分配规则仍然是“先到先得,按需分配”,要求使用者向国际组织申请地址。而在本方案中,任何组织或个人只要获得一个 DNS 域名,就可以在其下任意派生无限子域,每个子域都可以作为一个独立的 IP 域并拥有整个 IP 地址空间。相比 IPv6 方案,本方案对后发国家更加公平。

(6)如果规划得当,即便是中国这样的人口大国,运营商设立一个国家级的 IP 域就可以了。运营商已有的业务平台的内部管理可以继续使用现有的模式而不必升级。

目前 DNS 已经是个部署完善的系统。根据早期的一些反馈,有专家认为触动 DNS 不妥。但综合比较下来,特别是比较不同方案需要升级的设备数量与资金投入,通过升级 DNS 和边界路由器来升级到下一代互联网的方案,比起 IPv6 方案还是拥有巨大的优势。

IPv6 是现在被广泛认同的下一代互联网协议,而 NAT 是实际应用最广泛的解决方案。表 8 比较了一下 TCP/DN/IP 与 IPv6、NAT 技术的各方面特点。

概括而言,如果以 IPv6 为目标,则会出现以下情况。



表 8 TCP/DN/IP 与 IPv6、NAT 技术的各方面特点

	IPv6	NAT	TCP/DN/IP
全球标识 寻址根据	全球唯一 IPv6 地址	无全球唯一身份	全球唯一域名标识; IP 域内也可根据 IP 地址标识
地址空间	$2^{128} \approx 3.4 \times 10^{38}$	$2^{32} \times 65\,536 / 200 = 1.4 \times 10^{12} \text{①}$	$>> 10^{95} \text{②}$
地址分配	由国际组织统一分配,需申请	用户在国际组织预留的地址段内自主分配	可以在自己的 IP 域内自主分配整个地址空间的地址,并可自由设置数量无限的子域
转发机制	根据 IPv6 地址和路由表转发	需进行私网 IP:port 到公网 IP:port 的映射并保留映射关系,必要时还要作为 ALG 直接改变应用层中的 IP 地址,功能复杂	在 IP 域内按传统方式转发; 跨 IP 域时根据域名转发
现网兼容性	改造所有 3 层及 3 层以上设备,投资大,时间长; 升级全网 DNS 服务器; 需要运营商统一更换用户家庭网关,成本极高; 因为地址格式不同,升级过渡阶段需要复杂的地址转换以实现两网互通	NAT444 要求运营商在网内部署大量电信级 NAT 设备以解决地址不足的问题; 作为 IPv6 过渡技术的一些方案中的 NAT 需要运营商统一更换用户家庭网关	运营商只需要升级边界路由器(相当于国际出口)和域内 DNS 服务器; IPv4 网络永远使用不必关闭; 同 IP 域内主机不升级也不影响使用; 未升级的主机无法完成跨 IP 域的访问,但需要时主机可以很容易地升级
迁移动力	运营商投资巨大却无实际回报.SP 迁移正常运营的系统也无实际回报,并且必须长时间维护两个平台的系统。由于 IPv6 网内资源极少,用户更愿意留在 IPv4 网内; 对所有各方,升级的感受都是负面的; 同时,发达国家 IPv4 地址充足不急干升级,导致其他国家必须长期开通 IPv4 网络	运营商不得不部署大量电信级 NAT 网关以解决地址不足问题,满足业务发展要求; SP 不得不为 NAT 之后的用户设计特别的方案,导致了业务的复杂化和投资的增加; 宽带用户在多终端接入与损失对称性之间权衡,不得已选择前者; 对各方而言升级都利弊参半,属于不得已而为之	用户、业务提供商升级到双栈系统之后原有资源可以无障碍访问,升级是水到渠成之事; 运营商只需要升级极少量设备,即可解决地址不足的问题; SP 不升级仍可为域内提供服务,升级则可给全球提供服务; 用户不升级仍可访问域内主机,升级则可访问全球; 对所有各方,升级的感受都是正面的
用户接入	对称	不对称; NAT444 的引入甚至导致了 NAT 嵌套,进一步破坏了网络的对称性,网络将向主从结构演化; 需要特殊的配置或者公网主机的协调,私网内的主机才能接收外部主机发起的连接	对称
域名查询	DNS 需返回 IPv6 地址	没有变化	DNS 实际承担起跨 IP 域间路由的任务,需要对 DNS 进行一定的改造
升级平滑度	不平滑。需要地址翻译,可能形成孤岛。新旧网络很难互通		平滑。新旧网络几乎融为一体

①NAT 本质上是通过将 16 bit 的端口号分配给多个私网主机的方式实现对公网地址的复用。如果给每个宽带用户 200 个端口,那么每个公网地址可以供 327 个用户共享,相当于 IPv4 的地址空间扩大了 327 倍,一定时期内应能满足需要。如果考虑到将来可能出现如物联网等需要大量地址的应用,长远来看 NAT 方案提供的地址空间还是不足的。

②英文国际域名可以使用的字符有 26 个字母和 10 个阿拉伯数字以及横杠“-”,每个层次最长不超过 26 个字母,完整域名最长不能超过 63 个字符。精确地算出所有可能似乎是个很复杂的排列组合题,简单算一下形如[26].[26].[9]的域名的所有组合已经达到 $37^6 = 4.57 \times 10^{95}$ (其中完全由数字形成的组合共 10^6 种,比例太低可以略去)。因为“.”的位置和数量还有复杂的变化,实际的组合还远超出这个数值。

- 运营商不得不向用户提供双栈接入,需要升级所有三层及三层以上设备,包括路由器、DNS 以及所有宽带用户的家庭网关(数以亿计),过渡方案还要求在网内新增部署地址翻译设备等,耗时耗力,投资巨大。
- 因为运营商会(不得不)在较长一段时间内继续提供 IPv4 接入,并且运营商为数以亿计的宽带用户替换支持 IPv6 的家庭网关需要很长时间,SP 会倾向于留在 IPv4 平台,不会急于向 IPv6 迁移。等到运

营商经过漫长的时间终于将所有的家庭网关都换完时,SP会觉得经过长期考验的私网IP地址+NAT的访问模式已经很成熟,没有升级的必要。

- 因为IPv6网内资源较少,已升级到双栈的宽带用户也会更多地使用IPv4访问,IPv6流量寥寥无几。

也就是说,运营商花费了漫长的时间、付出了巨大代价将网络升级到双栈之后,用户会继续使用NAT技术访问IPv4平台上的SP而对IPv6平台置之不理,网络最终会演变成一个充分NAT化的网络,甚至可能包括嵌套的NAT模式。

如果以TCP/DN/IP为目标:

- 运营商只需要升级国际出口路由器和DNS(两者数量都极少)并适时从全球域中分离出国家域(让DNS改变解析策略即可),不必触及所有其他路由器,不必再新增其他设备;投资极低,工程量极小,可以迅速地部署完成;
- 对于SP和宽带用户而言,升级以支持TCP/DN/IP可以获得全球访问的能力,不升级也不影响域内(相当于国内)的访问。

也就是说,运营商只要付出极低的代价将网络升级到支持跨域的TCP/DN/IP转发(域内不触及),运营商的所有工作就完成了。剩下的只是SP决定是否以及何时让自己的业务平台支持新协议。同时,因为分离出了自己的IP域,运营商在自己的IP域内有了足够多的地址,运营商不再需要部署NAT。而用户仍可以继续使用他们的NAT家庭网关且不会有任何不便。

从历史的经验来看,升级终端是比升级网络要容易许多的。20世纪90年代初IETF开始考虑下一代互联网方案的时候,很多提议均假设网络会先于终端完成升级。但历史已经证明互联网实际的发展恰恰与这个假设完全相反。经过20年的高速发展之后,IP地址已经基本耗竭,几乎所有主流操作系统都已经支持IPv6,但网络却迟迟没有完成升级。细究其原因,恐怕还是因为终端升级主要是以软件形式进行的,而且网络协议只是操作系统的一小部分,因此操作系统在升级的时候顺便就可以完成网络协议的升级。而对运营商网络而言,首先部署零星的IPv6设备没有意义,其次升级通常是基于硬件的而且每个IPv6的许可都需要单独支付费用,因此运营商没有部署IPv6路由器的愿望。而本方案最大的特点恰恰在于运营商需要升级的部分

被最小化,主要的升级工作由终端通过操作系统软件升级来完成。

另外,随着用户终端和家庭网关的不断升级,网络将自动从被NAT技术扭曲的状态下解放出来,恢复为对称结构,在不需要任何特殊配置的情况下,所有的终端都将在**范围内可达。

7 TCP/DN/IP 发展远景

7.1 待明确和解决的问题

(1) 协议栈选择

先后提出了两个协议栈,TCP/DN/IP和TCP/DN/UDP/IP。前者报文头开销较小,后者可以保证报文顺利通过NAT路由器。是同时支持两个协议栈,还是仅仅支持后者?

(2) TCP/DN/IP 报文头

本文只是描述了报文头部必需的关键字段,其他还需要哪些字段以及各字段具体该如何定义,需要业界共同明确。

(3) 用SDN实现的可能性

在本方案中,域名层构成新的网络层,DNS成为DNR分离的路由平面。用DNS进行流量引导,DNR执行转发和地址翻译功能,正好与SDN的控制平面与转发平面分离的理念相吻合。本协议可能成为SDN技术的研究方向。

(4) 最优路由策略

由于DNS体系是严格的树型结构,如果IP子域有多个出口连接到父域(如中国有多个国际出口),或者同一个父域下的多个子域彼此相邻时,网络的实际拓扑与DNS的架构有一定的偏离。需要研究这些情况下的最佳路由策略。

同时,因为TCP/DN/IP中有IP和DN两个网络层,还可能会有两个平面路由协同优化的问题,需要进一步研究加以解决。

7.2 定位

(1) 作为IPng的最终解决方案

TCP/DN/IP采用变长的域名作为地址。变长的域名优点是真实的世界相一致,缺点是转发效率略低。

TCP/DN/IP本身具有极大的地址空间,事实上可以作为下一代互联网的最终解决方案。

(2) 作为向IPv6的过渡方案

如果业界偏爱定长的IP地址,坚持以IPv6作为最终的互联网解决方案,事实上TCP/DN/IP也可以作为从IPv4



到 IPv6 的过渡方案。

主机同时支持 3 个协议栈:TCP/IPv4、TCP/DN/IPv4 和 IPv6。先从 TCP/IPv4 平滑过渡到 TCP/DN/IPv4,再从 TCP/DN/IPv4 平滑过渡到 TCP/IPv6。从 IPv4 平滑过渡到 TCP/DN/IPv4 的方案已在前文详述,从 TCP/DN/IP 过渡到 IPv6 时,DNS 和 DNR 对于 TCP/DN/IPv4 报文按不同 IP 域处理,对 IPv6 报文按同 IP 域处理,即可完全平滑地实现过渡。

8 结束语

概而言之,双网络层方案有这样一些特点:地址空间无限、与 IPv4 网络高度兼容、升级过程非常平滑、投资极小,很好地满足了对下一代互联网技术方案的要求。

特别有趣的是,这个方案对升级的激励是正向的,所有各方都会有升级的主动性;对运营商而言,升级只需要极少的投资,就可以获得无限的地址空间;对 SP 而言,如果只是服务于 IP 域内用户那么就根本不需要升级,如果升级就可以服务于全球用户;对宽带用户而言,如果满足于目前的主动访问域内服务器的模式也不用升级,如果升级就可以双向访问全球网络,而且升级还很可能是完全自动的。

但一个新的协议从提出到成熟,毕竟需要较长的时间来充分发展。本文只是提出了一个简单的框架。笔者希望这个方案能得到大家的认同。更多的工作,还要期待业界共同推进和完成。

参考文献

- 1 RFC1550. IP: Next Generation (IPng) White Paper Solicitation, 1993
- 2 RFC1752. The Recommendation for the IP Next Generation Protocol, 1995
- 3 RFC2373. IP Version 6 Addressing Architecture, 1998
- 4 RFC1034. Domain Names-Concepts and Facilities, 1987
- 5 RFC1035. Domain Names-Implementation and Specification, 1987
- 6 RFC1123. Requirements for Internet Hosts—Application and Support, 1989
- 7 IETF. NAT444(draft-shirasaki-nat444-06), 2012
- 8 IETF. LAFT6: Lightweight Address Family Transition for IPv6 (draft-sun-v6ops-laft6-01), 2011
- 9 IPv6 发展为何如此纠结. 人民邮电报, 2013-10-10
- 10 姜明. IPv6 协议产生的背景过程和现状. http://tech.ccidnet.com/art/218/20030605/48972_1.html
- 11 Marsan D C. What happens if IPv6 fails. Network world, 2011

[作者简介]

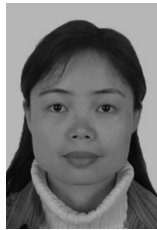


李实,男,中国电信股份有限公司上海研究院工程师、研究员,主要研究方向为基础网络。

(收稿日期:2014-07-02)

(上接第 135 页)

[作者简介]



陶彩霞,女,中国电信股份有限公司广东研究院高级工程师,主要研究方向为大数据、移动互联网、云计算。



陈康,男,中国电信股份有限公司广东研究院高级工程师,主要研究方向为大数据、云计算、电信支撑系统、移动互联网。



袁海,男,中国电信股份有限公司江苏分公司高级工程师,主要研究方向为互联网应用与平台开发运营。



马安华,男,中国电信股份有限公司江苏分公司工程师,主要研究方向为用户行为分析、数据挖掘。

(收稿日期:2014-03-12)