Dotouch
触 点 互 动

IPv6 Ready 测试解决方案

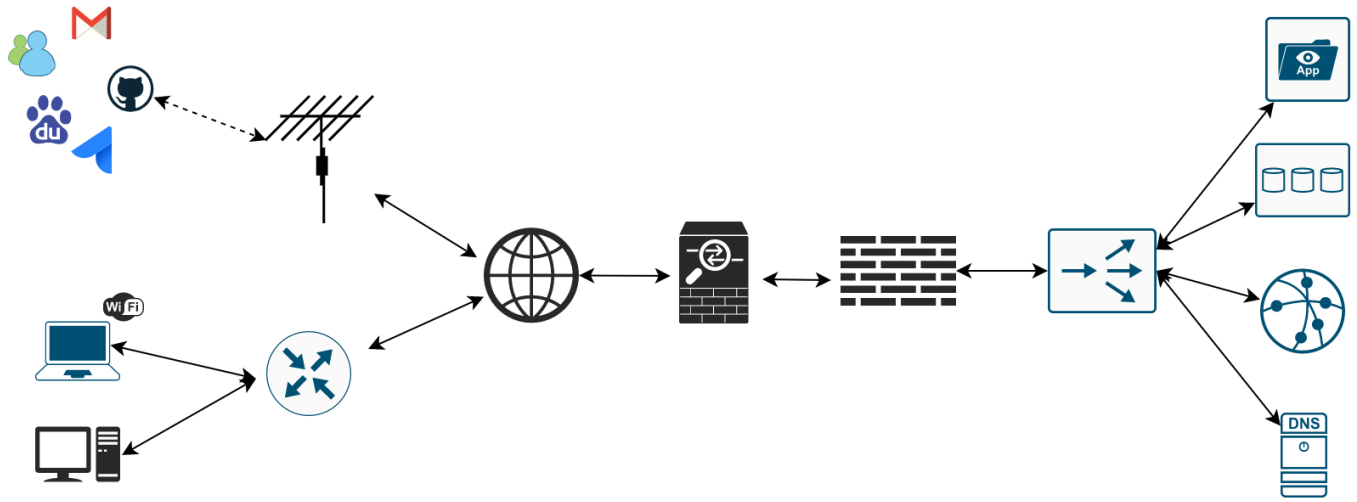
1 需求背景

IP 协议作为基础性的网络协议，承载了几乎全部企业网络与互联网的业务流量，成为支撑信息时代的基石。随着移动互联网应用的蓬勃发展，在 5G 技术的支持下，万物互联首次成为了可能。IP 地址作为万物在网络协议上的基础身份标识，我们传统上所使用的 IPv4 地址池面临枯竭，我们迫切需要引入支持超大规模地址池的 IPv6 协议以支持超大规模的网络互联，赋予万物独一无二的“身份标识”。

现实中，由于 IPv4 协议与 IPv6 协议在协议本身的差异性，IPv6 的协议长度、协议结构与 IPv4 有较大的差异性，而 IP 协议作为承载上层应用数据的基础协议，IPv6 与 IPv4 协议的这种差异性会直接影响上层应用的业务数据传输方式。同时，在 Internet 网络与企业网络中，我们还需要借助于多种类型的数据通信设备与安全类设备来完成数据的传输与处理，这些数据通信设备与安全类设备对流量的转发与处理与 IP 层协议有着直接的联系。因此，IPv4→IPv6 协议的升级不仅仅是一个简单的协议上的升级与改造，我们需要在升级改造过程中、升级改造后采取必要的测试验证手段，验证在 IPv4→IPv6 协议升级改造后的应用及基础网络设施设备能够正常使用与运行，真正发挥 IPv6 协议的价值。针对这一诉求，触点互动推出了完整的、端到端的 IPv4→IPv6 协议升级改造测试解决方案，助力 IPv6 协议的大规模商用。

2 业务痛点

IPv4→IPv6 协议的切换并不是一蹴而就的，我们的长远目标是构建一个 100% 使用 IPv6 地址的网络，但受限于当前庞大的使用 IPv4 协议的应用以及众多基于 IPv4 协议来进行数据流量转发与处理的网络基础设施设备，要完成这一目标需要经历很长的一段时间，在较长的一段时间内，我们面临的是一个 IPv4 与 IPv6 协议混合使用的网络，我们需要边改造应用与网络基础设施设备，边升级 IPv6 协议。我们从整个网络视图出发，分析 IPv4→IPv6 协议升级过程中所面临的问题。



1) 在终端 App 侧，流量的发起方是终端上的各个应用程序，例如在移动端，主要是由各个 App 发起业务的访问；

2) 在 Internet 侧，主要由各类路由、交换类设备通过 IP 寻址完成流量的转发；

3) 在企业内网，业务流量经由路由交换类设备、安全检测设备、审计类设备进行流量的交换与检测；

4) 在应用侧，各个业务服务端接收业务请求并进行处理，返回响应数据；

在终端侧，接入网络完成对接入终端的 IP 地址分配，可分配 IPv4、IPv6 或 IPv4&IPv6 双栈 IP 地址，主要面临如下问题：

- 痛点 1：移动终端获得单栈 IPv6 地址，App 完成 IPv6 改造后，其是否可以通过 IPv6 完成业务的访问。是全部业务均可通过 IPv6 进行正常访问，还是仅部分业务可通过 IPv6 访问；
- 痛点 2：移动终端获得双栈 IPv4&IPv6 地址，App 完成 IPv6 改造后，哪部分流量通过 IPv4 承载，哪部分流量通过 IPv6 承载；
- 痛点 3：当 App 通过 DNS 解析获取服务端的 IP 地址时，此时在 IPv6 环境下通过 DNS 请求域名的 AAAA 记录获得服务域名的最终 IP 地址；

在 Internet 侧，由于网络规模庞大，无法在短时间内完成大网的 IPv6 协议的升级，因此为了支持 IPv6，往往通过 NAT 网关进行 NAT46 与 NAT64 的转换，此时面临如下问题：

- 痛点 1：NAT 网关对各类地址转换协议的支持程度，如 NAT46、NAT64 等；
- 痛点 2：NAT 网关进行地址转换时的性能是否满足要求；

在企业网络侧，网络层是由各类型的网络设备组成的，这其中包括路由、交换、安全类、审计类、流量分发类设备，在进行 IPv6 升级改造后，此时面临如下问题：

- 痛点 1：单个网络设备特别是工作在 L4~7 层的安全类设备在升级支持 IPv6 后，其流量处理性能(新建性能、并发性能、吞吐性能等)是否受到影响；
- 痛点 2：在升级支持 IPv6 后，单个网络设备的功能是否能够正常运行，如基于 IPv6 的各类 ACL 策略、应用识别与解析策略等；
- 痛点 3：在升级支持 IPv6 后，如何端到端的验证改造后的网络基础设施能够像改造前一样进行流量的转发与处理；

在应用服务侧，应用服务器如 DNS Server 在升级改造 IPv6 后，面临如下问题：

- 痛点 1：升级改造后的应用服务，能否正常对外提供服务；
- 痛点 2：升级改造后的应用服务，在单栈 IPv6、双栈 IPv4&IPv6 等不同场景下的业务请求处理性能表现；

针对上述不同测试场景下的痛点，为了支撑客户更好的完成 IPv6 的升级改造，触点互动推出了端到端的测试方案，帮助用户全面、深入的评估与分析 IPv6 升级改造过程中面临的问题，充分验证 IPv6 升级改造后的网络与业务可用性。

3 解决方案

3.1 终端侧 App IPv6 升级改造测试方案

3.1.1方案介绍

触点互动推出的 IPv6 Ready 测试工具是一套面向移动终端 App 的 IPv6 测试方案，通过在测试移动终端上安装测试工具 APP，测试工具 APP 支持自动启动被测 APP，除支持测试人员手动点击被测 APP 各个功能模块触发业务流量外，测试工具 APP 还支持模拟自然人点击被测 APP 的部分功能模块会遍历被测 APP 的全部功能模块触发业务流量，测试工具通过监控与分析被测 App 在单栈 IPv6 环境、双栈 IPv4&IPv6 等不同业务场景下产生的业务流量，支撑应用开发方评估被测 App 的各个功能模块是否能够正常提供服务，通过分析原始数据报文，应用开发方可反向分析失败业务请求/响应所对应的 App 功能模块。

IPv6 Ready 测试工具工作方式如下图所示：



测试完成后，IPv6 Ready 支持输出的数据类型包含如下类型：

结果类型	结果	说明
统计类数据	DNS 会话总数/失败会话数	
	DNS over IPv4 会话总数/失败会话数	
	DNS over IPv6 会话总数/失败会话数	
	IPv4/IPv6 流量占比	按字节数统计
	IPv4/IPv6 报文比例	按包数统计
	IPv4/IPv6 上/下行流量	按字节数统计
	IPv4/IPv6 上/下行报文数	按包数统计
	TCP over IPv4 会话总数/失败会话数	
	TCP over IPv6 会话总数/失败会话数	
	UDP over IPv4 会话总数/失败会话数	
	UDP over IPv6 会话总数/失败会话数	
	HTTP/HTTPS over IPv4 连接总数/失败连接数	
	HTTP/HTTPS over IPv6 连接总数/失败连接数	
	HTTP/HTTPS over IPv4 包数/字节数	
	HTTP/HTTPS over IPv6 包数/字节数	
文件类数据	PCAP 文件	测试工具在测试期间捕获的被测 APP 所产生的业务报文

当用户为应用商店运营商时，由于需要满足工信部的合规性要求，需要对海量的 App 进行 IPv6 支持度的检测，触点互动 IPv6 Ready 测试工具支持通过自动化测试方案，并行开展多个 App 的测试，大大提高测试效率。

3.1.2部署特性

测试工具分为部署在移动终端的测试工具 APP 以及部署在 PC 端的管理平台，测试工具 APP 支持部署在各个品牌的 Android 移动终端之上，PC 端管理平台支持部署在 Windows 操作系统之上。

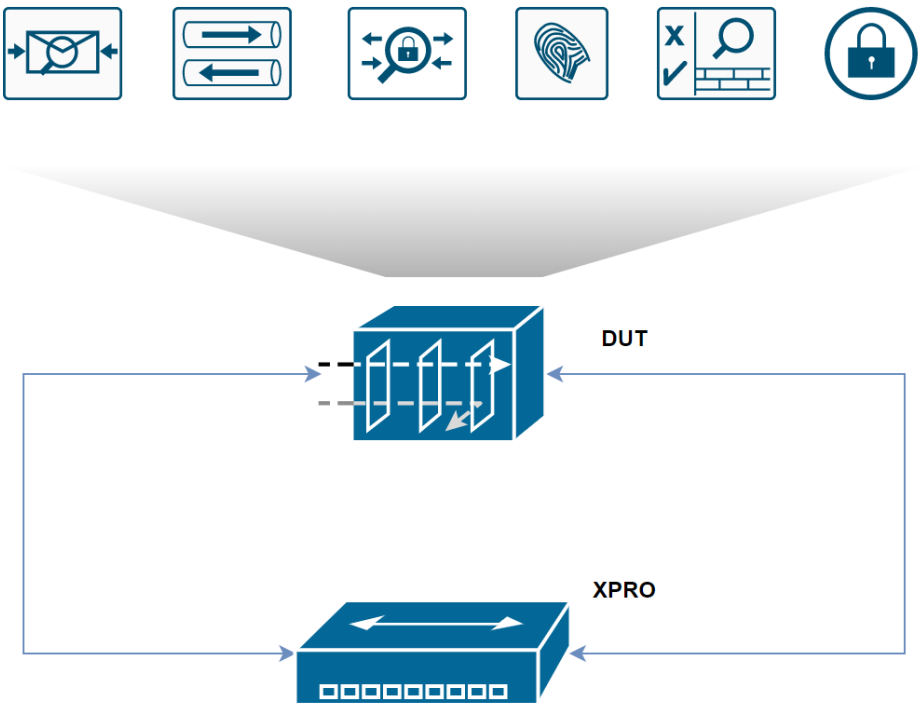
3.2 网络侧设备 IPv6 升级改造测试方案

3.2.1方案介绍

在网络中，网络侧设备包括各类数通类设备、安全防护类设备等，负责完成数据报文的转发、网络攻击行为的检测与阻断、特定流量的流控等。在网络侧设备进行 IPv6 升级改造后，我们需要验证升级改造后的网络设备的功能是否正常，性能指标是否降低，我们一般从如下几个方面来进行测试验证升级 IPv6 后的网络设备：

测试类型	测试内容	说明
功能类	NAT 功能，如 NAT46、NAT64 等	
	IPv6 下的 L4 ACL	
	IPv6 下的协议识别	
	IPv6 下的流量控制	
	IPv6 下的行为审计	
	IPv6 下的链路负载	
	IPv6 下的应用负载	
	IPv6 下的 DNS 代理	
	IPv6 下的 SSL 卸载(含国密与标密)	
	IPv6 下的 IPSec(含国密与标密)	
性能类	IPv6 下的 L4/L7 新建会话性能	
	IPv6 下的 L4/L7 并发会话性能	
	IPv6 下的 L4/L7 吞吐性能	
	IPv6 下的 HTTPS 新建会话性能(含国密与标密)	
	IPv6 下的 HTTPS 并发会话性能(含国密与标密)	
	IPv6 下的 HTTPS 吞吐性能(含国密与标密)	
	IPv6 下的 IPSec 隧道新建性能(含国密与标密)	含 Remote access 与 site-to-site 模式
	IPv6 下的 IPSec 隧道并发性能(含国密与标密)	含 Remote access 与 site-to-site 模式
	IPv6 下的 IPSec 吞吐性能(含国密与标密)	含 Remote access 与 site-to-site 模式
	IPv4&IPv6 混合业务模型叠加新建/并发/吞吐性能	
	RFC2544	
安全类	IPv6 下的 DDoS 网络攻击检测与防护	
	IPv6 下的应用层网络攻击检测与防护	
	IPv6 协议模糊测试	

触点互动研发的 XPRO NetworkSimulator 测试平台支持仿真基于双栈 IPv4&IPv6 的各类型网络与应用协议。XPRO NetworkSimulator 是一款以 L4~7 为主，同时兼顾 L2-3 层的全栈式仿真测试平台。在 L2-3 层支持仿如 IPv4、IPv6、PPPoE、DHCP、IGMP、MLD 等协议的仿真；在 L4-7 层，支持 TCP、UDP、HTTP、HTTPS、IPSec、DNS、RTSP、RTP、RTCP、SIP、L2TP、SMTP、POP3 等协议的仿真，同时，支持仿真主流的工控协议仿真，如 Handle、Modbus、OPC UA、LWM2M、MQTT 等，可对网络设备进行全面的功能与性能测试。



XPRO NetworkSimulator 基于通用的 X86/ARM 硬件平台，具备远超业内同类型产品的性能表现，单机支持超过 700 万/s 的 HTTP 新建会话性能、超 1.5 亿/s HTTP 并发会话性能，单机的 HTTP 吞吐性能高达 200Gbps。



3.2.2部署特性

XPRO NetworkSimulator 支持直接部署在 X86/ARM 硬件平台之上以获得最佳的性能表现，支持浪潮、曙光、华为、DELL、HP、H3C 等主流的 X86/ARM 双路或四路服务器。

除支持服务器裸机部署外，XPRO NetworkSimulator 还支持虚拟化部署，支持如下类型的虚拟化平台部署，以满足在私有云与公有云环境下的测试需求：

1) VMware ESXi；
2) KVM；
3) Openstack；

4) 阿里云；

5) 天翼云；

6) 华为云；

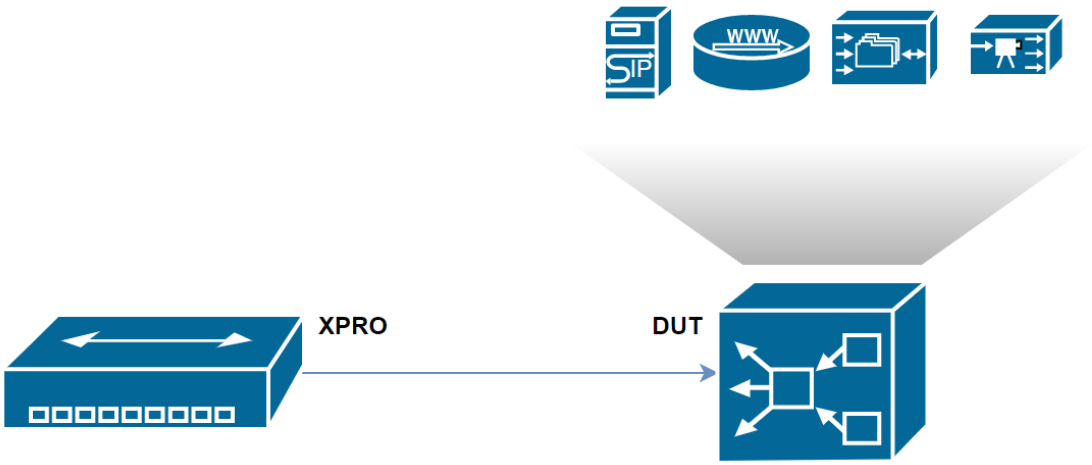
7) AWS；

针对网络接口，XPRO NetworkSimulator 支持从 1GbE 到 100GbE 各个规格的物理端口，在云化部署时，XPRO NetworkSimulator 支持 e1000 等主流使用的虚拟接口。

3.3 应用侧 IPv6 升级改造测试方案

3.3.1方案介绍

服务侧应用 IPv6 升级改造完成后，我们需要借助必要的技术手段对改造后的服务进行充分的测试与验证，以确保升级改造后的应用能正常对外提供服务，XPRO NetworkSimulator 支持单臂测试模式，支持仅模拟应用客户端对服务端进行测试。例如 XPRO NetworkSimulator 可模拟仿真海量 SMTP、DNS 客户端对升级改造后的 SMTP、DNS 服务端发起业务请求，验证改造后的 SMTP、DNS 服务端的性能表现。



XPRO NetworkSimulator 支持仿真如下类型协议的客户端：

1) HTTP/HTTPS 协议客户端；

2) SMTP/POP3 协议 客户端；

3) SIP 协议 客户端；

4) RTSP 协议客户端；

5) FTP 协议客户端；

6) DNS 协议客户端；

7) L2TP 协议客户端；

8) IPSec 协议客户端；

9) SSL VPN 协议客户端；

10) Handle 协议客户端；

11) Modbus 协议客户端；

12) MQTT 协议客户端；

13) LWM2M 协议客户端；

14) OPC UA 协议客户端；

通过 XPRO NetworkSimulator 对上述协议客户端的仿真，可对被测服务在升级改造支持 IPv6 后开展如下类型

测试：

1) 协议一致性测试；
2) 服务端每秒所能处理的接入请求性能；
3) 服务端每秒能处理的并发请求性能；
4) 服务端每秒能处理的业务流量吞吐性能；

3.3.2部署特性

XPRO NetworkSimulator 支持直接部署在 X86/ARM 硬件平台之上以获得最佳的性能表现，支持浪潮、曙光、华为、DELL、HP、H3C 等主流的 X86/ARM 双路或四路服务器。

除支持服务器裸机部署外，XPRO NetworkSimulator 还支持虚拟化部署，支持如下类型的虚拟化平台部署，以满足在私有云与公有云环境下的测试需求：

1) VMware ESXi；
2) KVM；
3) Openstack；
4) 阿里云；
5) 天翼云；
6) AWS；
7) 华为云；