

BGP4 + 互操作性测试研究 *

李 华 张 涛 叶新铭

(内蒙古大学计算机学院 呼和浩特 010021)

摘 要 BGP4 是最主要的域间路由协议, BGP4+ 是对 BGP4 进行扩展之后支持 IPv6 的, 对于它的互操作性测试很重要。本文首先介绍了互操作性测试的目的, 分析了 BGP4 以及 BGP4+ 的功能、路由类型以及数据包种类。根据 BGP4 的说明生成了协议的输入输出有限状态机, 基于该模型生成了部分 BGP4+ 的互操作性测试套。然后对于协议的不同实现进行了互操作性测试设计与实践, 最后给出了结论以及下一步的研究工作。

关键词 BGP4, BGP4+, 互操作性, 测试

Interoperability Test Research on BGP4 +

LI Hua ZHANG Tao YE Xin-ming

(School of Computer Science, Neimongol University, Hohhot 010021, China)

Abstract BGP4 is a main inter domain routing protocol. BGP4+ is an extension of BGP4 for supporting IPv6. Therefore it is very important to test its interoperability. Firstly the purpose of interoperability testing is introduced and the function, the kinds of routing and the type of packet of BGP4 and BGP4+ are analyzed. According to the newest BGP4 specification, the Input and Output Finite State Machine is generated. Based on this formal model, part interoperability suits are produced. Whereafter many kinds of interoperability testing experiment are designed for the different implementations. Finally the conclusion and the work in the future are given.

Keywords BGP4, BGP4+, Interoperability, Testing

1 引言

互操作性测试的主要目的是测试两个或更多的协议实现实际的网络环境中是否能够正确地互连互通, 从而提供一定的功能, 侧重于测试实现间的交互行为。此外, 互操作性测试也被 IETF(互联网工程任务组)和 ETSI(欧洲测试标准协会)等国际标准化组织广泛应用到了协议设计过程中。随着 IPv6 的部署, 原本只能支持 IPv4 的 BGP4 协议承载路由信息的时候, 无法达到期望的目标。为了使 BGP4 协议能够支持 IPv6 协议, IETF 对 BGP4 进行了扩充, 修订完成了 RFC2858 (Multiprotocol Extensions for BGP4, 即 BGP4+) [1], 它是确保自治系统间成功通信的核心协议。BGP4+ 与 BGP4 的有限状态机相同、数据包种类相同, 因此在分析协议行为以及数据包时可以基于 BGP4 进行。

目前关于路由协议互操作性测试进行研究的主要有日本的 TAHI 项目研究 [2], 该项目开发了 IPv6 协议的一致性测试系统和互操作性测试系统; New Hampshire 大学的互操作实验室 IOL (Interoperability Lab) [3] 在协议测试方面也做了大量的工作, 在支持 IPv6 的路由协议方面包括 BGP4+、OSPFv3、RIPng 的互操作测试研究; 欧洲的 ETSI (European Telecommunications Standards Institute) [4] 对网络协议定义了通用的测试说明方法, 并对 RIPng 进行了互操作性测试, 发现了一些实现的互操作问题。但是所有这些项目都没有介绍它们的 BGP4+ 的测试例是如何生成的, 因此需要深入地研究并且进行测试实践。

本文结构如下: 第 2 部分介绍了 BGP4 [5] 以及 BGP4+ 的基本工作原理以及数据包结构; 第 3 部分给出了 BGP4 的输入输出有限状态机 (Input and Output Finite State Machines, IOFSM), 并基于该模型进行互操作性测试套生成; 第 4 部分针对三个 BGP4+ 实现进行了具体的互操作性测试实践, 列举了部分测试例的执行结果; 最后给出了结论以及下一步要进行的研究工作。

2 BGP4 介绍

BGP4 在 RFC1771 中提出了一套新的机制来支持无类域间路由 (CIDR, Classless InterDomain Roution) 技术, 这些机制包括广播 IP 地址前缀和取消网络中“类”的概念; BGP4 还引入路由聚合和路由过滤的机制, 减少了 BGP 发言者存储和交换的路由。BGP4 的最新版本 RFC 4271 [6] 完成于 2006 年 1 月, 它对引起 BGP 状态变化的事件进行了更详尽的描述。在 RFC1771 中, BGP 事件只有 13 个并且都是必须事件; 但是在 RFC 4271 中, BGP 事件共 28 个, 分为 Administrative 事件、计时器事件、TCP 连接事件和 BGP 消息事件四大类, 其中必需事件共 13 个, 可选事件 15 个, 使得 BGP4 协议的处理能力更加完善, BGP4+ 与 BGP4 的有限状态机相同, 因此我们基于 BGP4 最新的 RFC 进行了形式模型的提取。

BGP4+ 与 BGP4 拥有同样的有限状态机模型以及同样的数据包。

2.1 BGP4+ 的功能

BGP4+ 实现之间交互的主要目标是在自治系统间自动

* 内蒙古自然科学基金重点项目 (200711020803)、内蒙古自然科学基金项目 (200711020809)。李 华 教授, 硕士生导师, CCF 会员, 研究方向为分布式系统与网络计算; 张 涛 硕士, 主要研究方向为协议测试; 叶新铭 教授, 博士生导师, 主要从事计算机网络和分布式系统方面的研究。

交换网络可达信息,通过交换带有自治系统号(AS)序列的路由可达信息来构建自治区域的拓扑图,从而很好地避免了路由中的环路问题。每个 BGP4+ 路由器都维护一个路由信息库,该信息库包含三部分: Adj-RIBs-In, Loc-RIB, Adj-RIBs-Out。BGP4+ 通过与邻居路由器交换路由信息来工作。

2.2 BGP4 路由

在 BGP 中存在三种类型的路由: AS 间路由、AS 内部路由、贯穿(pass-through)AS 路由。其中:

(1)AS 间路由发生在不同 AS 的两个或多个 BGP 路由器之间,这些系统的对等路由器使用 BGP 来维护一致的网络拓扑,AS 间通信的 BGP 邻居必须处于相同的物理网络。因特网就是使用这种路由的实例,它由多个 AS(或称管理域)构成,BGP 用于在 AS 间提供最佳路径。

(2)AS 内部路由发生在同一 AS 内的两个或多个 BGP 路由器间,同一 AS 内的对等路由器用 BGP 来维护一致的网络拓扑。BGP 也用于决定 AS 内的哪个路由器作为外部 AS 的连接点。

(3)贯穿 AS 路由发生在通过不运行 BGP 的 AS 交换数据的两个或多个 BGP 对等路由器间。在贯穿 AS 环境中,BGP 通信既不源自 AS 内,目的地也不属于该 AS。BGP 必须与该 AS 内使用的路由协议交互,以便成功地通过 AS 传输 BGP 通信信息,如图 1 所示。

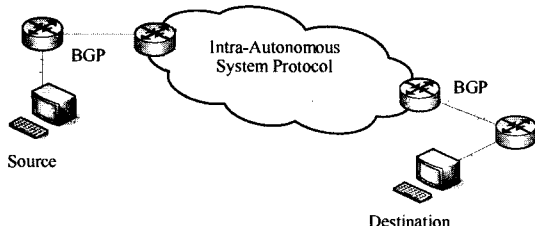


图 1 贯穿 AS 路由示例图

2.3 BGP4+ 的数据包

BGP4+ 包括 4 种数据包类型: Open, KeepAlive, Update, Notification。其中,

(1)Open 数据包:用来交换各自 BGP 的版本号、自治系统号、保持时间、BGP 标识等信息。

(2)Keepalive 数据包: BGP 对等路由器之间周期性地互发该数据包,以确保其连接有效。

(3)Update 数据包:携带更新路由信息,包括撤消路由信息、可达路由信息及其路径属性。该类报文由不可达路由、路径属性和网络可达性信息三部分构成。数据包分为三种情况:一次只能通告一个路由,但可以携带多个路径属性;一次可通告多个路由,但路径属性必须相同;一次可以列出多个被撤消路由。

(4)Notification 数据包:当 BGP 路由器检测到连接中断、协商出错、数据包差错时,关闭对等路由器的连接,并且通知对等路由器关闭连接的原因。

3 BGP4+ 的互操作测试设计

在互操作性测试的研究中,一般分为如下几步,构建包含测试环境的形式模型,侧重描述交互行为部分,然后基于形式模型进行测试生成研究,产生抽象测试套,写出测试例,根据测试例构建测试环境,进行测试,最后给出测试结果判定。

我们分析了 BGP4 以及 BGP4+ 中的状态转换。为了突出实现间交互,我们手工生成了 BGP4 的 IOFSM^[7],该模型的状态数较比以前版本并没有改变,只是变迁上的输入输出

有变化,基于该模型我们进行了测试套生成研究,图 2 是 BGP4 的 IOFSM 片段,变迁上的信息为事件/输出,如果没有输出,则相应位置为空。

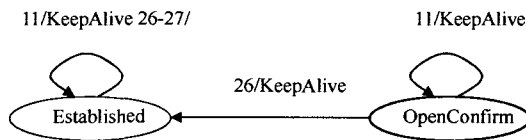


图 2 BGP4 的 IOFSM 片段

表 1 图 2 的事件及其输入

事件	输入
11	KeepaliveTimer 超时
26	输入 keepalive
27	输入有效的 update

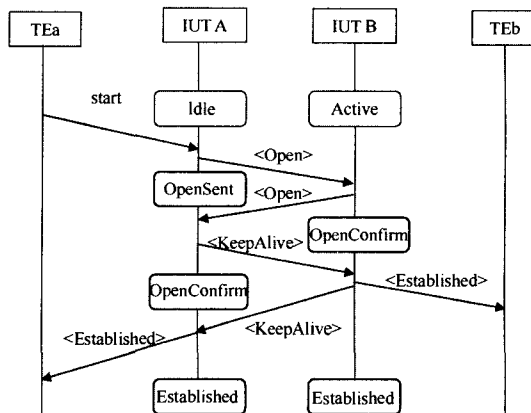


图 3 BGP4+消息交互实例中的输出数据包序列

在对 BGP4+ 协议进行互操作性测试的研究中,我们假设:(1)慢环境。即系统工作在慢环境中,所谓慢环境是指只有当被测系统对前一个外部输入响应完毕之后,外界环境才可以向被测系统发送下一个外部输入;(2)协议说明规范和协议实现中都不存在活锁(livelock)。即针对某一外部输入,变迁双方的交互不会无限执行下去。在此我们还假设被测系统中的每个协议实现都已经经过了单独的协议一致性测试。

我们采用文献[8]所提到的互操作性测试套自动生成的算法生成了部分 BGP4+ 的互操作性测试套。下面以图 3 中的 BGP4+ 消息交互实例来说明互操作性测试套的生成算法的功能,其中 TEa 和 TEb 是测试器,而 IUT A (Implementation Under Test) 和 IUT B 是两个不同的 BGP4+ 协议实现。

用同样的算法,我们可以自动生成下面 10 个 BGP4+ 协议的互操作测试套:

- (1) (Idle, Active) — start-a / { (nil, Open), (close, nil) } → (Idle, Idle);
- (2) (Active, Idle) — start-b / { (Open, nil), (nil, close) } → (Idle, Idle);
- (3) (Idle, Active) — start-a / { (nil, Open), (nil, Open), (nil, KeepAlive), (nil, NotiFMsg), (close, nil) } → (Idle, Idle);
- (4) (Active, Idle) — start-b / { (Open, nil), (Open, nil), (KeepAlive, nil), (NotiFMsg, nil), (nil, close) } → (Idle, Idle);
- (5) (Idle, Active) — start-a / { (nil, Open), (nil, Open), (nil, KeepAlive), (Estab, KeepAlive), (nil, UpdateMsg), (nil, KeepAlive), (Estab, nil), (Estab, nil) } → (Idle, Idle);
- (6) (Active, Idle) — start-b / { (Open, nil), (Open, nil), (KeepAlive, nil), (KeepAlive, Estab), (UpdateMsg, nil),

- (KeepAlive, nil), (nil, Estab), (nil, Estab) → (Idle, Idle);
- (7) (Idle, Active)—start-a/{(nil, Open), (nil, Open), (nil, KeepAlive), (Estab, KeepAlive), (nil, UpdateMsg), (close, NotiFMMsg), (close, nil)} → (Idle, Idle);
- (8) (Active, Idle)—start-b/{(Open, nil), (Open, nil), (KeepAlive, nil), (KeepAlive, Estab), (UpdateMsg, nil), (NotiFMMsg, close), (nil, close)} → (Idle, Idle);
- (9) (Estab, Estab)—NoTIFICATION/(closed, nil) ((Idle, Idle);
- (10) (Estab, Estab)—Update/(nil, nil) → (Estab, Estab)。

表 2 BGP4+ 互操作测试例举例 I

测试项目: 验证 BGP4+ 协议的不同实现能否正确协商 Hold Time
测试目的: 验证 BGP4+ 协议的不同实现能否正确协商 Hold Time
测试配置:
预期结果:
1)和2)中路由器 Cisco 1721 和 Bird 的 Hold Time 的实际值为 3 秒。
判定原则: 测试结果与预期结果相符, 否则不符合要求。
测试判定: 路由器 Cisco 1721 和 Bird 正确协商 Hold Time。

4 BGP4+ 互操作性测试举例

4.1 BGP4+ 互操作性测试过程设计

协议互操作性测试的主要目的是要验证两个或两个以上的实现在实际的环境中能否正确地互连互通互操作。因而, 在进行互操作性测试过程中, 要尽量减少实现之外的其它设备以及人为对被测实现的干预。但是, 在有些互操作性测试的实验中, 需要向被测系统中的某一实现(如 IUT A)发送一些符合特殊要求的数据包, 以便观察实现能否正确处理该数据包。比如在对 BGP4+ 协议的实现进行互操作性测试时, 验证 BGP4+ 路由器能否正确处理次序颠倒的通路属性的实验中, 由于我们无法让路由器按照我们的需要在特定的时候发出路径属性错误的 Update 数据包, 所以只能借助辅助工具来向其中一个实现发送路径属性颠倒的 Update 包, 然后观察 IUT A 是否正确处理这一数据包并根据需要向 IUT B 转发该包; 还有在 BGP4+ 互操作性测试的一些实验中, 所参与的实现之一需要接收特定组成的数据包, 因此需要互操作性测试工具的干预。特别是在涉及路由转发以及选项处理的测试套中, 都需要互操作性测试工具向特定的路由器发送特定的数据包。因此, 我们自主开发了 BGP4+ 的互操作性测试工具^[7], 在需要时辅助测试工作的进行。

我们根据生成的抽象互操作性测试套, 用自然语言描述为包含测试目的、测试配置和测试步骤的实际的测试例, 然后进行了测试。表 2 给出了一个 BGP4+ 实现 Cisco1721 和 Bird 的互操作性测试例的部分描述。首先要配置完 BGP4+ 协议的实现, 然后启动实验中的各个实现。通过从监测仪捕获到的数据包观察比较得知, 路由器 Cisco 1721 和 Bird 的 Hold Time 值均为 3 秒, 符合 RFC 协议说明, 所以这个 BGP4+ 协议互操作性测试例的测试结果为 PASS, 即路由器 Cisco 1721 和 Bird 在 Hold Time 协商上可以正确互操作。

在这个测试例的配置图中, 没有使用互操作性测试工具, 因为这个测试例本身不涉及数据包的转发, 不需要外界的干预。但是, 在 BGP4+ 互操作性测试的一些实验中, 所参与的实现之一需要接收特定构造的数据包, 因此需要互操作性测试工具的干预。特别是在涉及路由转发以及选项处理的测试套中, 都需要互操作性测试工具向特定的路由器发送特定的数据包, 如表 3 所述测试例。

表 3 BGP4+ 互操作测试例举例 II

测试项目: 验证 BGP4+SPEAKER 加入 AS 联盟时 NEXT_HOP, MED 和 LOCAF_PREF 属性功能正常。
测试目的: 验证 BGP4+SPEAKER 加入 AS 联盟时 NEXT_HOP, MED 和 LOCAF_PREF 属性功能正常。
测试配置:
预期测试结果
捕获的数据包显示: Zebra 转发 Update 消息到 Cisco1721, MED 属性不变, NEXT_HOP 不变, Zebra 应为新路由计算 LOCAL_PREF。至 Cisco1721 的 Update 消息应该包含新 LOCAL_PREF 属性。
测试结果: 与预期结果相同。

4.2 BGP4+ 互操作性测试报告

在对 BGP4+ 协议的实现进行互操作性测试的过程中, 我们把所有的测试套分为两部分: 一部分是 BGP4+ 实现的基本过程的互操作测试, 另一部分是 BGP4+ 实现对协议中可选项处理的互操作性测试^[7]。在测试的过程中, 我们也发现了一些 BGP4+ 实现不能互操作的地方, 如在验证 BGP 实现为加入 AS 联盟而传播 Update 消息时, Zebra 和 Cisco1721 就不能进行互操作。以 BGP4+ 实现 Zebra 和 Cisco1721 为例, 我们对协议中可选项处理的情况给出测试报告, 如表 4 所示。我们共计做了 37 个互操作测试例的执行。例如对 IUT A 与 IUT B 分别为 Zebra 和 CISCO 1721 而言, 有 5 个测试例与预期的目标不同; 对 IUT A 与 IUT B 分别为 CISCO 1721 和 Bird 而言, 有 2 个测试例与预期的目标不同。

表 4 部分测试例列表

测试套序号	测试套描述	测试结果
1	验证 BG PSPEAKER 加入 AS 联盟时传播 Update 消息功能正常	FAIL
2	验证 BG PSPEAKER 加入 AS 联盟时始发 Update 消息功能正常	PASS
3	验证 BG PSPEAKER 加入 AS 联盟时 NEXT_HOP, MED 和 LOCAF_PREF 等可选属性的处理	PASS
4	验证 BG PSPEAKER 配置为路由反射器时功能正常	PASS
5	验证 BG PSPEAKER 实现 COMMUNITIES 属性选项时功能正常	FAIL

结束语 BGP4 是 TCP/IP 协议簇中重要的域间路由协议之一, BGP4+ 是对 BGP4 进行扩展支持 IPv6 的, 对 BGP4+ 协议实现的互操作性测试进行研究很重要。本文分析了

(下转第 41 页)

- tem; theory and practice [M]. Fourth Edition, Springer-Verlag, 1997
- [4] Priyantha N, Chakraborty A, Balakrishnan H. The CRICKET location-support system [C]//Proc. of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM'00). Boston, MA, August 2000; 32-43
 - [5] Niculescu D, Nath B. Ad hoc positioning (APS) using AOA. // Proc. of Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'03). San Francisco, CA, April 2003; 1734-1743
 - [6] Bahl P, Padmanabhan V N. RADAR: An in-building RF-based user location and tracking system [C]//Proc. of Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'00). Tel Aviv, Israel, March 2000; 775-784
 - [7] Bulusun N, Heidemann J, Estr I D. GPS-less low cost outdoor localization for very small devices [J]. IEEE Personal Communications, 2000, 7 (5): 28-34
 - [8] He T, Huang C, Blum B M, et al. Range-free localization schemes in large scale sensor networks [C]//Proc. of the 9th Annual International Conference on Mobile Computing and Networking (MOBICOM'03). San Diego, CA, August 2003; 81-95
 - [9] Niculescu D, Nath B. DV-based positioning in ad hoc networks [J]. Journal of Telecommunication Systems, 2003, 22 (1/4): 267-280
 - [10] Nagpal R, Shrobe H, Bachrach J. Organizing a global coordinate system from local information on an ad hoc sensor network [C]//Proc. of the 2nd International Workshop on Information Processing in Sensor Networks (IPSN'03). Palo Alto, California, April 2003; 151-152
 - [11] Sastry N, Shankar U, Wagner D. Secure verification of location claims [C]//Proc. of the 2003 ACM Workshop on Wireless Security (WISE'03). San Diego, California, September 2003; 1-10
 - [12] Meadows C, Syverson P, Chang L W. Towards more efficient distance bounding protocols [C]//Proc. the Second International Conference on Security and Privacy in Communication Networks (SecureComm'06). Baltimore, MD, August 2006; 1-5
 - [13] Hancke G P, Kuhn M G. An RFID distance bounding protocol [C]//Proc. of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05). Athens, Greece, September 2005; 67-73
 - [14] Capkun S, Hubaux J P. Secure positioning of wireless devices with application to sensor networks [C]//Proc. of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'05). Miami, Florida, March 2005; 1917-1928
 - [15] Zhang Y, Liu W, Fang Y, et al. Secure localization and authentication in ultra-wideband sensor networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(4): 829-835
 - [16] Capkun S, Cagalj M, Srivastava M. Secure Localization with Hidden and Mobile Base Stations [C]//Proc. of the 25th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'06). Barcelona, Spain, April 2006; 23-29
 - [17] Anjum F, Pandey S, Agrawal P. Secure localization in SN using transmission range variation [C]//Proc. of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS'05). Washington, DC, November 2005
 - [18] Lazos L, Poovendran R. SeRLoc: Secure range-independent localization for wireless sensor networks [C]//Proc. of the 2004 ACM Workshop on Wireless Security (WISE'04). Brisbane, Australia, November 2004; 21-30
 - [19] Lazos L, Poovendran R, Capkun S. ROPE: Robust position estimation in wireless sensor networks [C]//Proc. of the International Symposium on Information Processing in Sensor Networks (IPSN'05). Los Angeles, CA, April 2005; 324-331
 - [20] Lazos L, Poovendran R. HiRLoc: High-resolution robust localization for wireless sensor networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 233-246
 - [21] Ekici E, Vural S, McNair J, et al. Secure probabilistic location verification in randomly deployed wireless sensor networks [J]. Ad Hoc Networks, 2007
 - [22] Du W L, Fang L, Ning P. LAD: Localization anomaly detection for wireless sensor networks [J]. The Journal of Parallel and Distributed Computing, 2006, 66(7): 874-886
 - [23] Liu D G, Ning P, Du W L. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks [C]//Proc. of the 25th International Conference on Distributed Computing Systems (ICDCS'05). Columbus, Ohio, June 2005; 609-691
 - [24] Li Z, Trappe W, Zhang Y, et al. Robust statistical methods for securing wireless localization in sensor networks [C]//Proc. of the International Symposium on Information Processing in Sensor Networks (IPSN'05). Washington, 2005; 91-98
 - [25] Liu D G, Ning P, Du W L. Attack-resistant location estimation in sensor networks [C]//Proc. of the International Conference on Information Processing in Sensor Networks (IPSN'05). Los Angeles, CA, April 2005. 99-106
 - [26] Wang C, Liu A, Ning P. Cluster-based minimum mean square estimation for secure and resilient localization in wireless sensor networks [C]//Proc. of the International Conference on Wireless Algorithms, Systems and Applications (WASA'07). Chicago, IL, August 2007
 - [27] Brands S, Chaum D. Distance-bounding protocols [C]//Proc. of Workshop on the theory and application of cryptographic techniques on Advances in cryptology. New York, 1994; 344-359
 - [28] Ganu S, Krishnakumar A S, Krishnan P. Infrastructure-based location estimation in wlan networks [C]//Proc. of IEEE Wireless Communications and Networking Conference (WCNC'04). Los Alamitos, 2004; 465-470
 - [29] Przytek B, Song D, Perrig A. SIA: Secure information aggregation in sensor networks [C]//Proc. of the 1st International Conference on Embedded Networked Sensor Systems (SenSys'03). Los Angeles, CA, November 2003; 255-265
 - [30] Wagner D. Resilient aggregation in sensor networks [C]//Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04). Washington DC, October 2004; 78-87
 - [31] Raya M, Hubaux J P. The security of vehicular ad hoc networks [C]//Proc. of the 3rd ACM Workshop on Security of ad hoc and Sensor Networks (SASN'05). Alexandria, Virginia, November 2005; 11-21

(上接第 31 页)

BGP4 以及 BGP4+ 协议及其功能,介绍了相关的各种数据包功能,基于协议的说明生成了它的 IOFSM,基于已有算法自动生成了 10 个互操作性测试套。我们对现有的三个 BGP4+ 协议实现进行了互操作性测试,发现了一些不可互操作的地方,本项工作有利于检查产品的互联互通互操作能力。本文的实践结果可以为协议标准的设计提供合理的建议,减少说明中影响互操作性测试因素的存在。如果将互操作性测试方法用在协议开发的早期,可以增强产品的互操作能力。下一步的研究工作针对多激励原则展开互操作性测试,即从外界环境中可以同时向两个实现输入外部消息。这种原则要比单激励原则更加复杂,同时也需要研究新的形式化建模方法和测试套自动生成的算法,从而适用新的工作环境。

参考文献

- [1] Bates T, Rekhter Y, Chandra R. Multiprotocol Extensions for BGP-4 (BGP4+). RFC 2858, June 2000
- [2] <http://www.tah.org>
- [3] <http://www.unh.edu>
- [4] <http://www.etsi.org>
- [5] Rekhter Y, Li T. A Border Gateway Protocol 4 (BGP-4). RFC 1771, March 1995
- [6] Rekhter Y, Li T, Hares S. A Border Gateway Protocol 4 (BGP-4). RFC 4271, January 2006
- [7] 张涛. 边界网关协议 BGP4+ 的互操作性测试研究. 内蒙古大学, 2007
- [8] Seol S, Kim M, Kang S, et al. Fully automated interoperability test suite derivation for communication protocols. Computer Networks, 2003, 43(6): 735-759