浅析网络透明性问题

林容容[1] 丁伟 龚俭
（东南大学计算机科学与工程系 南京 210096）

摘要

在网络发展过程中，端到端体系结构中的透明性正受到各种因素的破坏。其中的种种因素可以归结为地址的非透明性和开放通信传输的封闭化。然而当视角上升到系统演化规律高度时，一定程度的非透明是网络社会化的必然结果。与之对应的是，透明性本身也需要相对的变通和发展。

本文对端到端网络体系中的透明性问题做出了综述性总结，并在此基础上深入阐述了透明性问题的根源，最后给出了解决透明性问题的思路和想法，为更深层次的研究提供一定的启发。

关键字：网络 透明性 端到端 信任

Internet 设计者 David D.Clark 等人在上世纪八十年代初期设计了端到端的网络体系模型。其思想主要是认为面向特定应用的功能的实现不应设计在网络的核心层，而应将其从核心层中分离出来。这种模型能降低网络核心层的复杂性，提高应用的可靠性。

当 1978 年 Cerf 基于 Pouzin 1974 年[1]的设想提出链式网概念（catenet concept）[2]时，就决定了未来的以此为基本思想实现的网络必然需具备透明性。而如今，网络透明性的日益减少已成为一个备受关注的问题。在 NAT 之前，关于地址透明性的解决办法就已在研究之中，其中的 SIPP（Simple Internet Protocol Plus）[3]发展为了最终的 IPv6。美国国防部已对区别于端到端的新的体系结构的研究立项。David D.Clark 等人对网络体系结构做出了新的思考[4]。中国的 973 项目也在研究该问题。但现在几乎所有的研究都尚未给出结论。

本文将对网络透明性的产生和解决中的相关问题展开讨论，全文组织如下：第一章分类总结破坏网络透明性的诸多因素；第二章挖掘和阐述透明性被破坏的根源；第三章深入讨论究竟怎样的透明性才是合适的；最后在第四章中给出结论。

1 破坏透明性的因素

网络的端到端模型要求尽可能地将应用级的功能从网络的核心部分中分离出来。端系统要实现通信的完整性维护，连接状态维护等通讯功能；而中间是透明传输。所谓透明，其实指的是具有单一的逻辑地址分配表和能将所有信息包从源端毫不改变地传送至目的地的一种机制[5]。尽管最初的网络设计是要求网络尽可能的透明，但随着网络的不断发展，最初的透明性已逐步地遭到破坏。

RFC2775 从技术角度列举了破坏网络透明性的诸多因素[5]。概括起来，一共九点：

首先，是 Intranet 模式的影响。Intranet 是一种使用 TCP/IP 技术的独立企业网络，

[1] 林容容，女，1981 年，硕士生，研究方向：网络测量，网络行为学。E-mail: rrlin@njnet.edu.cn
丁伟，女，1963 年，教授，博士生导师，研究方向：网络行为学，网络安全，网络测量。E-mail: wding@njnet.edu.cn

在一定的控制下与 Internet 相连。Intranet 是出于商业目的的，为了保护公司内部主机的敏感信息或是机密信息，许多公司的网管自己规定那些应用可以跨过 Internet/Intranet 之间界限。网络的透明性也就因此消失。

其次，动态地址分配。在网络中，大量的拨号上网用户的 IP 地址是在其拨号之时分配的，带宽大小由当地的 ISP 提供。也就是说，真正的 IP 地址是暂时——在线时，它依赖于端到端；而断线后，就不再存在了。对于局域网用户而言，其地址经常是系统启动时用动态主机配置协议（DHCP）找到的新的地址，因此，真正的 ZD 地址也是暂时，在每个会话之间不会被存储。

第三，防火墙。防火墙为了保证内部网的安全管理，需要拦截所有 Internet 和 Intranet 之间的报文，然后筛选出可以通行的报文。从本质上限制了 Internet 的透明性。

第四，私有地址。当出现 IPv4 的地址空间出现紧缺现象后，私有地址[6]随之而生。这些地址不能在公共的 Internet 中使用，如果没有特殊的转换，具有这些地址的主机不能在 Internet 中通信。

第五，网络地址解析（NATs）。使用私有地址的 Intranet 用户需要接入 Internet 的必然结果就是要进行网络地址解析。然而由于 NATs 改变了报文的 IP 地址[7]使得许多协议，比如 H.323（需要在应用层携带 IP 地址）通不过简单的 NATs。如果要考虑更多 Internet 应用的话，NATs 就必须外加应用层中的网关（ALGS）或代理服务器。

第六，应用层网关、信息转发、代理服务和缓存。在 Internet/Intranet 交界处，需要安装应用层网关，并提供信息转发，代理服务和缓存。它们可以在网络边界上准确地控制网络、传输、应用协议的进行，但同时也严重破坏了网络的透明性。

第七，孤立网和对等网。有些网在内部网络中通过代理网关和使用私有协议和地址表，如 WAP 论坛。类似的这种情况虽然是端到端地工作，但报文的传输不是端到端的。

第八，独立 DNS。Intranet 网在防火墙内外使用部分或完全不同的 DNS，使得地址无法实现单一性和持久性。

第九，负载平衡技术。IPv4 不支持任意播（anycast）[8]，于是出现了各种各样的实现负载平衡的技术。例如：路由器自动将报文发给相同地址的不同服务器等等。这些技术破坏了域名和地址的透明性。

网络是由工程技术构建起来的一个实体，但同时必须注意的是，它是直接面向应用的，是在具体的实践中一步步发展起来的。在网络的发展过程中，往往是使用需求的变化导致了新的网络技术的出现。一切网络服务和网络技术都是为了使网络的使用者能够更加方便有效的使用网络。因此，从网络的使用者的角度出发，透明性的减少是网络在实际使用过程中，由于使用者对网络的要求的变化引起的。网络的使用者很多，主要可视为三方面：

第一， 用户。在这里，用户的概念是区别于商业 ISP 及政府组织的端实体。可以说，用户是 Internet 最底层也是数量最大的使用者。随着接入 Internet 的用户的数目越来越多，用户与用户之间出现了越来越多的不信任。例如：网上的商业谈判，用户之间的通信可能完全没有信任；为了保护自己，用户需要在匿名的方式下在线投票或是进行电子交易；为防止其它端实体的攻击或是垃圾邮件，用户（内部网）需要一定的隔离措施。这些都是使得网络无法继续保持透明性的需求。

第二， 商业 ISP。出于商业的目的，ISP 希望将特殊的应用捆绑销售，不同的应用由不同的 ISP 提供。这些应用有可能需要穿越多个 ISP 网段，而各个 ISP 是相互独立的，因而无法实现端到端的透明传输。当用户选择各自的 ISP 时，好的 ISP 由于用户的增多就能得到更多的资金投入自身建设，从而造成 ISP 之间差异，于是又进一步影响了端到端模式的透明传输。

第三， 政府等机构组织。作为通信的端用户，认为自己有权利使用任何软件，传递任何信息给愿意接收的另一方。但作为政府，它需要了解网络中的各种通信，从而控制网络中的违法行为。于是，政府或是类似其它组织就需要作为第三方介入网络中的通信。这种第三方的介入势必破坏原网络的透明性。

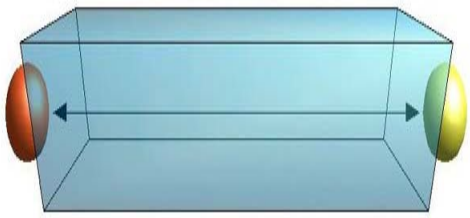

图 1 透明网络

网络透明性的减少已成为网络发展过程中不可避免的现象。就透明性本身而言，如果最初的设计是希望实现如图 1 所示的完全透明状态，那么，透明性的减少可以分为两种不同的表现形式——即单方非透明和双方非透明[9]。

单方非透明：如前所述，网络的透明性是指通信的双方地址单一通用，以明确标识网络端实体；通信的数据包毫不改变地在网络中传输，即提供开放的通信。但 NAT 网关和防火墙的出现，使得内部网只能在一定控制下向外通信，而外部的通信也将被隔离。外部的端实体只能看到防火墙，而看不到内部网里面的端实体，但里面的端实体可以看到外面。类似这样的情况可以称之为单方非透明。如图 2 所示，右边的端实体是非透明的，而左边的端实体透明。

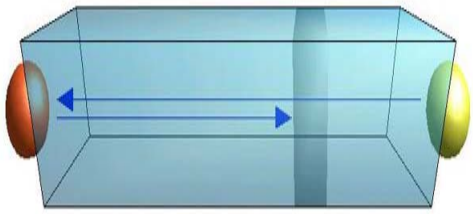

图 2 单方非透明

双方非透明：如果有两个 NAT 网关的存在就会出现图 3 所示的情况，即通信的两个端实体都是非透明的，相互不可见。类似这样的情况可称之为双方非透明。

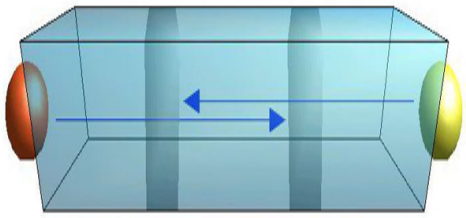

图 3 双方非透明

2 透明性减少的根源

虽然从技术、需求及自身形态这三个不同的角度分析，网络透明性的问题表现出不同的形式。但回归到最初的网络设计思想，即端到端网络模型时，透明性问题归根结底在于两方面的问题：单一通用地址和透明传输。

从地址方面来看，由于 Ipv4 的地址不够分配，导致 NAT、ALG 等机制的出现以使用一些内部的私有地址，从而破坏了网络地址的单一性和通用性。

使用私有地址节约了单一通用地址的地址空间。对企业网而言，私有地址使得网络设计中具备了更多的灵活性；使得操作和管理地址分配方案以及扩展路径时都变得更加容易和方便。但私有地址同时也带来了许多问题。例如，在访问 Internet 时，私有地址必须转换为通用地址，此时必须考虑地址转换的代价。再如，当若干私有网络需要合并时，由于合并前的私有网络的地址都是各自自己分配的，合并后就很可能不唯一，因而必须对不唯一的地址进行重新分配。

NAT 很好地解决了私有地址接入 Internet 网的问题，解决了地址紧缺问题，但其对透明性的破坏却带来了许多安全性问题。现有的网络层的安全模型是建立在端到端透明性的基础之上的，如 IPsec。隧道模式的 IPsec 无法用在网关和防火墙之间，传输模式的 IPsec 可以在

内部网中使用，但如果遇到 NAT 则不能使用。NAT 实质上只起到了访问控制的作用，而并不像 IPsec——具有从加密到身份认证等各项安全机制。IPsec 的无法使用会带来许多安全性问题。NAT 对报文解密再加密以改变 IP 地址，但此时的报文是明文的，很容易受到攻击。NAT 存有许多密钥，因而容易成为攻击对象。内部网的内部没有安全保护，则一旦网络边界被穿越，整个内部网都将被攻破。

私有地址和 NAT 还会影响其它许多应用协议，而从另一个角度来说，地址的紧缺问题仍旧存在，并会越来越恶劣。因为端实体的数量在不断的增加，而且越来越多的端实体从拨号上网方式转为了始终在线连接。动态主机配置协议（DHCP）和 PPP(端对端协议)的发展更使得地址透明性不复存在。

如今 IPv6 的发展似乎为地址空间问题提供了解决方法。IPv6 完全满足所有主机和路由器包括中间件、应用、管理系统的适配器的地址要求。其地址有足够大的空间满足所有应用需求。乐观地说来，IPv6 是可以恢复全局地址的透明性的，传输模式 IPsec 也就可被使用。但 IPv6 并不能排除防火墙和代理网关的使用。

从传输方面来看，最初的端到端设计是在假定所有的通信对象都是善意的，可信任的前提下实现的端到端透明传输。如今网络中的通信行为出现了许多新的需求。其中最重要的两个方面就是网络中的信任问题和第三方的介入问题。这些需求使得网络的传输无法再保持透明性。

网络是为人类活动服务的，于是在网络的应用过程中，不断的出现了社会化特征。

网络中的端实体间的通信出现了越来越多的不信任情况。例如网上的商业谈判中，通信的双方都会尽可能的保护和隐藏自己。在线投票、电子交易中，端实体需要在匿名的方式下进行通信。对于通信的双方，一方希望隐藏自己，而另一方则希望确认对方。另外，在现在网络世界中的恶意攻击愈演愈烈的情况下，由于端到端的设计是要求每个端实体自己对自身的安全负责的，这使得端实体必须需要保护和隐蔽自己。

不信任关系的增多使得端实体越来越重视自我保护，同时也导致了第三方的出现和发展。如公钥证书就是利用可信第三方解决信任问题的例子。除了具有信任关系的第三方，端实体的通信中同时也出现了具有不信任关系的第三方。例如政府[10]。在 Internet 发展之初，政府扮演了很重要的设计者及操作指导者的角色。Internet 的原型 NSFnet 就是政府支柱构建起来的。然而随着网络在现实社会的应用和发展，政府的角色发生了改变——更多的是关注网络中的商业行为和用户行为。从政府角度来看，它需要管理和控制其管辖范围内的方方面面的社会生活，网络中的行为当然也不例外。例如对网上商业行为的税收，或是对网上违法犯罪行为的监控和制裁等等。虽然类似这种第三方的介入与端到端透明传输是相违背的，但这种介入又是必须的。而更糟糕的是，作为通信的端实体，总是认为自己有权利不受到来自第三方的监控和管理。例如第三方需要检查传输的数据，端实体却通过加密等措施进行逃避。这就使得网络的透明性状况变得更加复杂和混乱。

网络发展之初，在其设计和实现的过程中，技术始终占据着主导地位。技术总是为应用服务的，总是因需求而产生。一旦有新的需求出现，便会有与之相关的技术的创新和实现来满足该需求。由于地址出现了紧缺问题，私有地址、NAT、Ipv6 等技术相继诞生；内部网需要隔离和保护自己内部敏感数据，于是防火墙、网关、过滤器等等技术不断涌现；要解决通信中的不信任关系，加密、解密、可信第三方机制……真正是“ 只有想不到的，没有做不到的 ”。

然而技术仅仅是表象的，并不能完全反映出网络发展的本质问题。尽管无论是最初还是现在，网络都是由纷繁复杂的技术构建起来的，但如今网络早已不再是一个单纯的技术实体。

然而与其说网络是一个经济实体，不如说是一个社会实体来得更加广泛和全面。网络的在经济方面的影响是不容忽视的，但其实除了“ make money ”之外，它早已渗透到了军事、教育、文化，甚至农业发展等社会生活的各个领域。网络中的行为似乎已越来越像现实世界的行为，或者说网络中的行为活动基本可视为现实社会中各种活动的一种映射。但同时，又不是一种简单的映射。毕竟网络有由其特性所造成的局限性，也有其优于现实社会活动的便利性。网络与社会之间呈现出的是一种交叉影响关系，并且这种交叉渗透关系将随着时间的推移变得愈加深刻。

尽管网络是由技术支撑的，但随着其在社会群体中的应用，网络的社会化发展及社会性的增加已成为其突出的特性之一。从网络的社会性角度去看透明性问题则不难发现，当网络已不再是一个单纯的技术实体后，要在网络上实现绝对的单纯的透明性是不可能的了。

举例说来，社会中的各种实体，小到每个个人，大到一个社团组织、企事业单位，甚至一个城市，国家，无论是怎样的组织形式，构建方式，它们都有自己的区域范围，并在此范围之内保护自身利益。个人尚且有隐私权，更不论大一点的组织单位了，各自都有针对其内部的保护机制。在网络中的情况也是一样的道理：端实体对自身保护的意识越来越强；若干端实体联合为内部网后，防火墙等技术的目的就恰似各种社会组织保护自己单位内部信息安全的做法。

由此可以得出推断，透明网络只是网络设计中的一种理想状态，在网络建立之初，网络呈现最简单的原始形态时，是可以满足透明性要求的；但随着网络社会化的发展，其社会性的增强，绝对的单纯的透明性是不可能实现，也正因为此，最初的透明性被一系列的因素所破坏。

3 关于合适的透明性的探讨

在本文的第 1 节中就给出了透明性的定义，从这个定义出发，可以看到网络的透明性从根本上说由两方面特征组成：地址的透明和通信传输的透明。下文将从这两个方面讨论网络中究竟怎样的透明性才是合适的。

在端到端网络模型中，端实体的唯一标识是由地址实现的。由于内部网的出现，IPv4 的地址紧缺问题，引发了一系列的解决地址空间问题的技术。如果 IPv6 能够顺利的取代 IPv4，则网络的地址透明性是有可能可以恢复的。但在防火墙，网关等技术发展的如此完备的今天，IPv6 是无法避免这些问题的。对通信传输而言，通信的内容应尽可能透明，但又不得不考虑部分公开通信内容的需要。需要通信的端实体双方如果存在非信任关系，通信不可能也不可以完全透明。因而，此时的透明必须是在一定的控制之下，具有一定约束要求的透明。

给传输的报文加上 Label 的做法[10][11]对透明性问题具有一定的启发。Label 可以很好的标识传输的内容以及用户的类型。通过对内容的分类标识，在需要过滤或者审查的时候就能保护报文的内容不被完全公开和改变。其实 Internet 中提供了一种简单的类似 Label 的形式，那就是端口号。不同的应用使用不同的端口号标识，因而现在许多地方使用地址加端口号的方式标识报文。但这种由端口号划分报文类型的方式十分粗略。Label 可以在保护报文内容的前提下提供报文的类别信息，但它的实现还必须依赖于一定的法律管理。例如内容的分类是否符合标准，Label 的使用是否合乎法律等等。

在通信中一个至关重要的问题就是信任。在此问题上，可以借鉴 PGP 的思想，建立信任的模型，给出信任评估的定量刻划，从而控制和解决信任问题。首先，信任是什么呢？对

信任的定义有很多，但似乎尚没有可以被广泛接受的标准。[12]中给出了几个心理学和社会学学者对信任的定义。分析这些定义，至少可以总结出三方面要点：

1) 信任是主观的，由于不同实体对同一事物的看法会有所不同；
2) 信任是一系列行为之后所产生的，没有交互是无法建立信任的；
3) 信任与否的决定由实体做出，可以定义不同的信任程度。

信任可以表达为近似数学的形式，也就是说，可以在某种程度上可以定量地表示出来。有研究把信任度表示为一个实数区间，如[0,1]，0 代表完全不信任，1 代表完全信任，从而利用概率的理论来建立信任模型。这样的做法虽然过于简单，但为信任的度量提供了思路。结合模糊数学思想，可以引入不确定性[13]来表示信任度。

在信任关系上，可分为直接信任与间接信任。通过端实体在网络中的各种行为特征，建立信任模型，在交互中给出相互的信任度。当一个端实体需要与其它端实体通信时，只要参考该端实体的信任度，就可做出是否与其交互的决定。如果通信的发起方与另一端实体有过交互，则可参考通过直接交互得到的直接信任度；如果未曾交互过，则可参考其它实体做出的信任度以得到间接信任度。在端实体不断交互过程中，可以动态地更新信任度，以及时反映网络中各个实体的当前状况。

在信任模型建立好了的基础上，就可以根据端实体间的信任程度来控制报文的交互的透明性。

内部网结构的出现对网络的透明性产生了严重的影响，但它是网络社会化的必然趋势和要求。在此透明性的要求也必须修正。从对自然的系统或是社会系统来看，虽然系统看起来很复杂，但如果将系统的任意局部加以放大，内部子系统之间常常是相关的，这称之为有序态的自相似形，即结构和原来的系统是相同的。内部网其实也是这样的。因而透明性的要求也需要有相应的调整。如果将内部网内部的端实体之间的网络定义为绝对的透明性，那么内部网与其外部端实体就是相对的透明，前提是网络能够容忍一定程度的非透明性。

网络的透明性意味着对开放通信的要求，然而 Internet 从最初的开发系统形式发展至今，端实体似乎正走向越来越封闭的状态。 众所周知，只有开放的系统，才能不断和外边交换物质、能量和信息，才能使其更具生命力。而封闭只会使系统状态走向无序和灭亡。在技术的自由，应用的开放前提下，我们有理由相信，网络的透明性将在有序的控制和管理之下得到一定程度的恢复，及更深层次的进化和发展。

4 结论

从技术、需求及表现形式各种角度来看，端到端的网络透明性正不断地遭到威胁甚至是破坏。这固然是网络在现实世界中不断演化的必然趋势，但透明性的减少却给网络发展本身带来了诸多的问题。恢复网络原始形态的透明性是不可能，也不需要的。网络发展至今，透明性本身也需要更新和进化。在一定控制和管理下的部分的相对的透明性是可实现的，只要其中某些原有的透明性的牺牲对网络而言是能够容忍的。

参考文献

[1] Cerf, V., “The Catenet Model for Internetworking,” Information Processing Techniques Office, Defense Advanced Research Projects Agency, IEN 48, July 1978.
[2] Pouzin, L., “A Proposal for Interconnecting Packet Switching Networks,” Proceedings of EUROCOMP, Brunel University, May 1974, pp. 1023-36.
[3] R.Hinden, “Simple Internet Protocol Plus White Paper,” Internet RFC 1710, October 1994.
[4] David D.Clark, Marjory S. Blumenthal, “Rethinking the design of the Internet: The end to end arguments vs. the brave world,” Version for TPRC submission, August 10, 2000.
[5] B. Carpentert, “Internet Transparency,” Internet RFC 2775, February 2000
[6] Rekhter, Y., Moskowitz, B., Karrenberg, D. and G. de Groot, “Address Allocation for Private Internets”, RFC 1597, March 1994.
[7] Hain, T., “Architectural Implications of NAT”, Work in Progress.
[8] Partridge, C., Mendez, T. and W.Milliken, “Host Anycasting Service”, RFC 1546, November 1993.
[9] Todd E. Sundsted, “How trends in network design have jeopardized the Internet's transparency,” Facts and Figures, Etcee LLC, August 2002.
[10] http://rene.efa.org.au/liberty/label.html
[11] http://www.w3.org/Metadata
[12] Pradip Lamsal, Understanding Trust and Security, http://www.cs.Helsinki.FI/u/lamsal/papers/UnderstandingTrustAndSecurity.pdf, November 2002.
[13] Audun Jøsang, “An Algebra for Assessing Trust in Certification Chains,” In J. Kochmar, editor, Proceedings of the Network and Distributed Systems Security Symposium(NDSS’99). The Internet Society, 1999.

Elementary Analysis of Network Transparency

Lin rongrong Ding wei Gong jian
（Department of Computer Science & Engineering, Southeast University, Nanjing 210096）

Abstract
With the development of network, various recent inventions have led to the loss of end-to-end transparency in the Internet, which compose of the loss of address transparency and the alteration of packets flowing from source to destination. However, from the angle of the theory of system evolution, the loss of the network transparency is due to the socialization of the network. That request the evolution of the transparency itself.

This dissertation has studied the problem of end-to-end transparency in the Internet. On the basis of the summarization, it then goes deep into the primary reason of the problem. And it has provided the brainchild of the solutions, to illumine the further research to some extent.

Key words: Network, Transparency, End-to-end, Trust

作者简历：
林容容，女，1981 年，硕士生，研究方向：网络测量，网络行为学；
丁伟，女，1963 年，教授，博士生导师，研究方向：网络行为学，网络安全，网络测量；
龚俭，男，1958 年，教授，博士生导师，研究方向：网络行为学，网络安全，网络体系结构。
传真：83614842　　电话：83794000　　邮编：210096