# 相互同意的路由安全规范（MANRS）

## 引言

一般来说，就奖励措施而言，安全是一个困难的领域。全球互联网基础设施的安全（无论是域名系统（DNS）或路由），都带来其他挑战：安全措施的效用取决于许多其他各方的协调行动。

在整个互联网历史中，参与者之间的协作以及对互联网平稳运行的共同责任一直是支撑互联网巨大增长和成功以及安全性和弹性的两大支柱。技术解决方案在这里至关重要，但仅靠技术还不够。为促进这一领域的明显改善，有必要对集体责任文化进行更大的改变。

本文旨在抓住这种协作精神，为网络运营商解决全球互联网路由系统的安全性和弹性提供指导。另一个重要目标是记录行业领导者对解决这些问题的承诺，当更多支持者加入时，这种影响应放大。

## 目标

1. 展示日益增长的支持者群体的承诺，提高认识并鼓励采取行动
2. 倡导集体责任文化，应对互联网全球路由系统的弹性和安全性
3. 展示业界本着集体责任精神解决互联网全球路由系统的弹性和安全性问题的能力
4. 为互联网服务提供商（ISP）提供一个框架，以更好地理解和帮助解决与互联网全球路由系统的弹性和安全性相关的问题

## 范围

存在许多不同的建议来提高域间路由系统的安全性和弹性。一些建议甚至看起来有些矛盾，通常关键的决定可能是要考虑给定网络的规模和资源，外部连接数量，客户和终端用户，规模和规模，从而确定对于给定网络最重要或最合适的网络。员工的专业知识等等。

下面的“预期和高级操作”强调了一组建议，这些建议对于全球路由系统的整体安全性和弹性以及网络运营商本身绝对有价值。它们解决了三类主要问题：

- 与错误的路由信息有关的问题；
- 欺骗性源IP地址流量相关的问题；和
- 与网络运营商之间的协调与协作有关的问题。

预期行动定义了一个最低限度的“一揽子计划”–一套支持MANRS文件的运营商绝对应该实施的建议。这一方案并非详尽无遗，人们期望许多网络运营商已经在实施或计划实施更强大的措施和控制。本文档后面的“高级操作”进一步扩展了最低套餐。

我们意识到以下事实，即任何特定的行动都不能全面解决上述问题。但是，每一步都是很小的一步，如果乘以大量支持者，则可以成为全球互联网路由系统弹性的重大提高。因此，选择行动的依据是对小的，增量个人成本与潜在的共同利益之间的平衡进行评估。

# 定义

为了阐明“预期和高级行动”的具体内容，有必要明确定义一些术语，与它们在互联网行业的普遍使用相关。

- 基础设施–运营商的内部网络，必须在互联网上可以访问。
- 最终用户–运营商的路由和管理域内的网络。
- 对等网络–与各自基础设施和客户网络交换流量的外部网络。
- 转接网络–一种将与基础设施和客户网络相关的流量发送到的外部网络，但通常从该外部网络接收来自互联网的流量。
- 客户网络–运营商为其提供转接服务的外部网络。
- 单宿主K网络之间的单个，简单链接，或将最终用户连接到基础设施。这表示流量可以在网络内部或网络之间流动的单一路径。
- 多宿主K网络（甚至多个网络）之间的多条路径，或最终用户与基础设施之间的连接；这样可以在基础设施和互联网上创建流量可以通过的多个路径。

# 原则

1. 组织（互联网服务提供商/网络运营商）认识到全球路由系统的相互依存性及其在为安全，有弹性的互联网做出贡献方面的作用。
2. 该组织根据《行动》将与路由安全和弹性相关的最新最佳实践整合到其网络管理流程中。
3. 该组织致力于通过与对等方和其他互联网服务提供商（按照行动）进行协作和协调，预防，检测和缓解路由事件。
4. 组织鼓励客户和同行采用这些原则和行动。

# 预期行动

**1. 防止传播错误的路由信息。**

- 网络运营商定义了清晰的路由策略，并实施了一个系统，以前缀和ASKpath粒度确保自己的公告和客户到相邻网络的公告的正确性。
- 网络运营商能够与相邻网络通信哪些公告正确。
- 网络运营商在检查客户公告的正确性时会进行尽职调查，特别是确保客户合法持有公告的ASN和地址空间。

**2. 使用欺骗性源IP地址阻止流量。**

- 网络运营商实施为最少单个Khomed 存根客戶网络，自己的终端用戶和基础设施启用源地址验证的系统*。网络运营商实施欺骗欺骗过滤以防止数据包进入和离开网络的不正确来源IP地址。

**3. 促进网络运营商之间的全球运营通信和协调。**

- 网络运营商维护全球可访问的最新联系信息。

# 高级操作

- 4.促进在全球范围内验证路由信息。
- 网络运营商已公开记录了路由策略， ASN和前缀，旨在向外部广告。

# 详细阐述和参考

**措施1.防止传播错误的路由信息。**

- 网络运营商定义了清晰的路由策略，并实施了一个系统，以前缀和AS-path粒度确保自己的公告和客户到相邻网络的公告的正确性。
- 网络运营商能够与相邻网络通信哪些公告正确。
- 网络运营商在检查客户公告的正确性时会进行尽职调查，特别是确保客户合法持有公告的ASN和地址空间。

讨论：最重要的是通过使用显式前缀级别过滤器或等效机制来保护入站路由公告，特别是从客户网络获取入站路由公告。其次，可能会使用AS路径过滤器来要求客户网络明确哪些客户自治系统（ASes）位于该客户下游。或者，AS路径过滤器阻止客户与提供商有无结算关系的A-es的公告，可以防止某些类型的路由“泄漏”。仅通过AS路径过滤器过滤客户BGP公告不足以在系统级别上预防灾难性路由问题。

参考文献：

“推荐的互联网服务提供商安全服务和程序”，网络基础设施部分，
http://www.rfcKeditor.org/bcp/bcp46.txt

“ BGP操作和安全”，安全http://tools.ietf.org/html/draftKietfKopsecKbgpK

边界网关协议安全性，NIST：特殊出版物SP 800K54，
http://csrc.nist.gov/publications/nistpubs/800K54/SP800K54.pdf

“大型互联网服务提供商（ISP）IP网络基础设施的运营安全要求”，
http://tools.ietf.org/html/rfc3871

“在实践中使用RPSL”，http://tools.ietf.org/html/rfc2650

“将RIPE数据库用作互联网路由注册中心”，
https://labs.ripe.net/Members/denis/usingKtheKripeKdatabaseKasKanKinternetKroutingKregistry

BGP安全最佳实践，FCC CSRIC III WG4最终报告，http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_ March_%202013.pdf

**措施2.使用欺骗性源IP地址阻止流量。**

- 网络运营商实施的系统至少应支持单宿主存根客戶网络，其最终用戶和基础设施的源地址验证。网络运营商实施了反欺骗过滤，以防止源IP地址不正确的数据包进入和离开网络。
- 讨论：解决此问题的常用方法包括软件功能，如电缆调制解调器网络上的SAV（源地址验证）或路由器网络上的严格uRPF（单播反向路径转发）验证。在路由和拓扑相对不太动态的情况下，这些方法可以减轻管理开销。另一种方法可能是使用入站前缀过滤器信息创建一个数据包过滤器，这将仅允许数据包具有源IP地址的网络可以合法地通告其可达性。

参考文献：

“网络入口过滤：击败采用IP源地址欺骗的拒绝服务攻击”，
http://tools.ietf.org/html/bcp38

“多宿主网络的入口过滤”，http://tools.ietf.org/html/bcp84

“保护边缘”，http://www.icann.org/committees/security/sac004. txt

“ RIPE防欺骗工作队如何” http://www.ripe.net/ripe/docs/ripe-431

BGP安全最佳实践，FCC CSRIC III WG4最终报告，
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

**行动3：促进网络运营商之间的全球运营通信和协调。**

- 网络运营商维护全球可访问的最新联系信息。

讨论：维护此类信息的常见场所是PeeringDB，RIR的whois数据库和大型IRR（如RADB和RIPE）。网络运营商应至少在这些数据库之一中注册和维护24/7联系信息。此联系信息应包括运营商针对AS NOC的当前联系信息，所有网络块和域名。鼓励运营商在IRR中记录其网络路由策略。也欢迎提供其他信息，例如，在其PeeringDB记录的相应字段中的窥镜URL。

参考文献：

“在实践中使用RPSL”，http://tools.ietf.org/html/rfc2650

对等数据库，https://w.peeringdb.com

RADB，http://www.radb.net/

**行动4.促进在全球范围内验证路由信息。**

- 网络运营商已公开记录了路由策略，ASN和前缀，旨在向外部广告。

讨论：为促进全球其他网络对路由信息的验证，有必要向外部各方发布有关路由策略，ASN和前缀的信息。

公开发布策略的方法之一是在由RADB镜像的互联网路由注册中心（如RIPE，ARIN，RADB等）之一中使用RPSL记录策略。在这种情况下，运营商必须注册并维护至少一个（或多个）“设定值” IRR对象，其中包含打算发布给外部各方的ASN列表，自动工具可以使用这些前缀生成前缀过滤器。运营商还必须在IRR中维护其信息以确保是最新的。

另一种更安全的手段是通过RPKI系统促进全球范围内的验证。运营商可以从为这些前缀分配了前缀的RIR获得自己的前缀的RPKI证书，并发布和维护与其宣布的前缀相对应的ROA。

运营商必须鼓励客户网络运营商也这样做。这将允许其他网络在全球范围内验证公告。

参考文献：

“在实践中使用RPSL”，http://tools.ietf.org/html/rfc2650

“将RIPE数据库用作互联网路由注册中心”，
https://labs.ripe.net/Members/denis/usingKtheKripeKdatabaseKasKanKinternetKroutingKregistry

“基于资源公钥基础设施（RPKI）的原始验证操作”，
http://www.rfcKeditor.org/bcp/bcp185.txt