第32卷 第14期 计 算 机 工 程 2006年7月
Vol.32 № 14 Computer Engineering July 2006
·网络与通信· 文章编号：1000—3428(2006)14—0081—02 文献标识码：A 中图分类号：TP393

一种BGP路由配置错误动态检测方法

王洪君[1,2]，王大东[1]，梁海英[1]，高 远[1]
(1. 东北大学秦皇岛分校，秦皇岛 066004；2. 吉林师范大学计算机学院，四平 136000)

摘 要：针对BGP路由源配置错误和路由输出配置错误，提出了一种BGP路由配置错误动态检查方法。该方法通过对入境和出境路由的地址前缀进行所属关系检测来确定所声明前缀的合法性，发现路由源配置错误。依据自治系统之间的商业关系，通过分析出入境路由的AS路径属性来发现违反路由输出原则的路由输出配置错误。通过仿真实验证明了所给方法的正确性和可行性。
关键词：自治系统；BGP；路由策略；BGP配置错误

A Method to Dynamically Detect BGP Configuration Errors

WANG Hongjun[1,2], WANG Dadong [1], LIANG Haiying[1], GAO Yuan[1]
(1. Qinhuangdao Branch, Northeastern University, Qinhuangdao 066004; 2. School of Computer, Jilin Normal University, Siping 136000)

【Abstract】 A method to dynamically detect BGP configuration errors is proposed. The method focuses on two types of misconfigurations, origin misconfiguration and export misconfiguration. To find the origin misconfiguration, the method checks the prefixes of inbound or outbound routes to verify whether the prefixes announced belong to the original AS. According to the commercial relationship between ASes, the method finds the export misconfiguration by checking whether one AS in the AS-PATH violates the export guideline. Finally, the method is proved to be feasible through simulation.
【Key words】 Autonomous system; Border gateway protocol; Routing policy; BGP misconfiguration

BGP(Border Gateway Protocol)[1]目前已成为事实上的外部网关协议，被广泛应用于Internet，它根据所配置的路由策略选择和通告路由。然而所配置的路由策略有时会表现出意料外的路由行为，称为路由配置错误。BGP路由配置错误会导致目的网络不可达、路由循环、路由振荡，甚至是网络中断，增加丢包率，增加网络收敛时间，浪费路由器和链路资源，影响Internet整体性能，降低服务质量。

本文提出了一种BGP路由配置错误动态检查方法。该方法通过对入境和出境路由的地址前缀进行所属关系鉴别来确定所声明前缀的有效性，发现路由源异常。依据自治系统间关系和路由通告原则，通过分析出入境路由的AS路径属性来证明路由的有效性。

1 BGP路由通告原则

1.1 自治系统间关系

Internet被分割成自治系统(Autonomous System，AS)，所谓的自治系统，就是拥有同一选路策略、在同一技术管理部门下运行的网络，如大学、政府部门、企业和公司的网络，以及Internet服务提供者网络。在自治系统内部运行IGP(Interior Gateway Protocol)路由协议，自治系统间运行BGP协议。每个自治系统都独立地定义自己的路由策略，选择和通告到目的网络的路由。

AS根据彼此之间签订的商业服务合同，形成了不同的依赖关系。一般用无向图G=(V, E)表示Internet，其中，V表示自治系统，E表示自治系统间的链接。AS间的关系定义如下。

定义1 对∀u, v∈V，且{u，v}∈E，如果v从u购买接入Internet的服务，利用u的资源访问Internet上的其他网络，这时称v与u为客户－提供者关系(customer-provider)，记为：v←u，称u为提供者，v为客户。反之，如果u为v提供有偿连接服务，称之为提供者－客户关系(provider-customer)，记为：u→v。

定义2 对于∀u,v∈V，且{u，v}∈E，如果u和v之间相互为对方提供无偿的针对各自内部网络以及各自客户网络的访问服务，这时称u与v为对等者关系(peer-peer)，记为：u≈v。

定义3 对于∀u,v∈V，且{u，v}∈E，如果v只在与其他提供者之间的连接出现故障时，才通过u访问Internet上的其它网络，这时称u与v为备份连接服务关系(backup)，记为：v u。

1.2 BGP路由通告原则

自治系统根据商业关系制定路由策略，一个AS只有愿意为某个AS承载到目的网络的流量时，才向该AS通告路由。Huston[2]给出了配置路由输出策略时需要遵守的原则：

(1)输出给一个提供者：当一个客户向提供者通告路由信息时，作为客户的自治系统可以输出自己的路由和它客户的路由，但不能输出从其它提供者或对等者获得的路由。

(2)输出给一个客户：当提供者向客户通告路由信息时，作为提供者的自治系统可以输出自己的路由和它客户的路由，也可以输出从其它提供者或对等者获得的路由。

(3)输出给一个对等者：当与对等者交换路由信息时，可以输出自己的路由和客户的路由，但不能输出从其它提供者或对等者获得的路由。

2 BGP路由配置错误检测方法

2.1 BGP路由配置错误

BGP路由包含目的网络前缀、到达目网络所经过的AS路

基金项目：国家自然科学基金资助项目(60073059，60273078)
作者简介：王洪君(1965－)，男，博士生，主研方向：Internet路由稳定性和Internet路由体系结构；王大东、梁海英，博士生；高 远，教授、博导
收稿日期：2005-07-26 **E-mail：**whj@mail.neuq.edu.cn

径、下一跳路由器等信息。BGP路由行为完全依赖于路由策略配置，而BGP路由配置的灵活性，使得BGP路由表现出意料外的路由行为。例如：通告目的网络不存在的无效路由、路由循环和路由振荡。一个好的路由应具有如下特点[3]：(1)有效性：存在到达目的网络的路由，沿着路由提供的路径，所传输的数据能够到达目的地；(2)可见性：存在到达目的网络的路径，就一定存在到目的网络的路由；(3)安全性：路由协议存在唯一的、稳定的路由赋值，使网络收敛；(4)确定性：路由的选择是时间无关的，不依赖于路由到达的先后顺序，同时最佳路由的选择不受其他路由的存在与否的影响；(5)信息流控制：路由按照路由策略要求进入、离开和穿越一个AS。

所有导致违反上述路由特点的 BGP 配置都是错误的。例如：路由输入策略没有对收到的路由进行可达性检测，就会影响路由的有效性，而安装不可达的路由。

本文只讨论两种类型的BGP配置错误[4]及其检测方法。

(1)路由更新源配置错误

BGP路由包含地址前缀Pre和到达该地址所经过的AS序列[AS_m AS_{m-1} … AS_0]，表示为(pre，[AS_m AS_{m-1} … AS_0]),其中，AS_m为通告该路由的AS，AS_0为生产该路由的自治系统，称为路由更新的源。路由源错误可能导致网络不可达，违反路由有效性。路由源错误主要包括：1)没有对具体路由进行汇聚；2)通告了别人的或没有被分配的地址空间；3)向外通告了本应存在于AS内的地址，例如：私有地址。

(2)路由输出配置错误

路由器在发送路由更新信息之前，根据路由输出策略对路由进行过滤和属性修改。路由输出策略配置错误是指 AS 路径中的某个 AS 违反了路由输出策略。例如：把来自提供者的路由通告给了另外一个提供者 AS，或通告给了一个具有对等关系的 AS。把来自具有对等关系 AS 的路由通告给了另外一个具有对等关系的 AS 或通告给了提供者 AS。

2.2 路由配置错误检测算法

定义 4 customers(u) = { v | ∀v, 有 v ← u}为 u 的所有客户构成的集合；providers(u)={v | ∀v, 有 v → u }为 u 的所有提供者构成的集合；peers(u)={v | ∀v, 有 v ≈ u }为 u 的所有对等者的集合。

定义 5 prefix(u)为自治系统 u 所拥有的前缀，即 u 所要生产的前缀；客户前缀集 customer_prefix(u)={pre|∀pre，∃v∈customers(u), pre∈prefix(v)}, 对等体前缀集 peer_prefix(u) ={ pre|∀pre, ∃v∈peers(u), pre∈prefix(v)}。

定义 6 设 u∈V，adj_AS_Object 是 u 内用于描述相邻 AS 的数据结构，adj_AS_Object=<AS_n, relationship, prefix_in, prefix_out>，其中，AS_n 为邻居 AS 的自治系统号，relationship∈{←, →, ≈}，prefix_in 是 AS_n 声明的输入前缀，prefix_out 输出给 AS_n 的前缀。

定义 7 rib-in-errors(u)为节点 u 的输入策略机对收到的路由进行检测所发现的错误路由。rib-out-errors(u)为节点 u 的输出策略机对即通告的路由进行配置错误检测所发现的错误路由。

(1)入境路由检测算法

设节点 v 和节点 u 为两个相邻节点，即{v, u}∈E，u 接收 v 输出路由 r。入境路由检测算法如下：

```
u receive r from v；
if (| r.as_path | = 1 and r.NLRI ∉ prefix_in(v))
   or (first(r.as_path) ≠ v) {
      reject route r;
      put route r in rib-in-errors(u);
}
if rib-in-errors(u) ≠ ∅
   output the routes in rib-in-errors(u);
```

其中，| r.as_path |为路由所经过的 AS 数，first(r.as_path)为提供路由的 AS。

(2)出境路由检测算法

设节点 v 和节点 u 为两个相邻节点，即{v, u}∈E，u 向 v 输出路由 r，出境路由检测算法如下：

```
if |r.as_path| = 0 and r.NLRI ∉ prefix_out(v) {
   reject route r;
   put route r in rib-out-errors(u);
}
if u←v and (first(r.AS_Path)∈providers(u)) or
   first(r.AS_Path)∈peers(u)
      put route r in rib-out-errors(u);
   if u≈v and (first(r.AS_Path)∈providers(u)) or
first(r.AS_Path)∈peers(u)
   put the route r in rib-out-errors(u);
if rib-in-errors(u) ≠ ∅
   output routes in rib-in-errors(u);
```

3 仿真实验

为了限制路由器获得或通告的选路信息，可以基于来自或去到一个特定对等体的路由更新进行过滤。以图 1 为例进行仿真实验，其中，AS1 是 AS3 和 AS4 的提供者，AS2 是 AS3 的另外一个提供者，AS4 是 AS3 的客户。

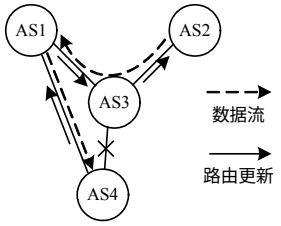

图 1 仿真网络拓扑结构

设置 AS1 的网络前缀为 202.206.16.0/24，AS4 的网络前缀为 172.16.16.0/24，AS2 的网络前缀为 198.168.16.0/24。首先，配置基于前缀对路由进行过滤，允许 AS3 把地址前缀 172.16.16.0/24 通告给 AS2，但不允许通告 202.206.16.0/24 给 AS2。AS3 对 AS2 的路由输出策略配置如表 1，在 AS3 到 AS4 的链路存在时，这个配置是正确的。

表 1 AS3 到 AS2 路由策略错误配置

策略机	路由策略
输入策略机	True ⇒ permit
输出策略机	ip address = 172.16.16.0/24 ⇒ permit ip address = 202.206.16.0/24 ⇒ deny

如果 AS3 到 AS4 的链路中断，这时表 1 给出的配置就会出问题，节点 3 报告一个输出错误，指出到 AS2 的路由输出有错。节点 3 的输出结果为：

```
export errors:
   record 1：
   AS number = 2
   prefix = 172.16.16.0/24
   as_path = [1 4]
   prefix ∈ prefix_in(4)
```

（下转第 103 页）