The Current State of Routing and Dealing with Detected Anomalous Routes

Packets are consistently sent to the correct destinations over the Internet due to the proper transfer of routing information between networks. In this section we will give an overview of routing protocols and summarize the problems caused by the advertisement of incorrect routing information.

2.1 Routing Protocol Types and Applications

The Internet is composed of a great number of interconnected networks, and it is in a constant state of flux. New networks may be connected, and existing connections may be severed for some reason. The connected networks themselves also change. A single network may sprawl beyond the borders of a country or region, or disappear due to factors such as its operators withdrawing from operations. It is only possible for us to communicate with the intended recipients amidst such change because packets are properly routed to reach their destination.

Dealing manually with the many changes that the Internet undergoes is not feasible. For this reason, dynamic routing protocols that automatically find and regulate the optimal routes are indispensable. Dynamic routing also has the merit of enabling distributed IP addresses to be utilized easily according to demand. Routing protocols such as RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) are often used for comparatively small networks such as those within an organization. Meanwhile, for Internet routing between ISPs or large-scale networks, BGP (Border Gateway Protocol) is the standard routing protocol used.

When BGP was first designed, it was assumed that network architecture would use a protocol such as OSPF or IS-IS (Intermediate System to Intermediate System) as the IGP (Interior Gateway Protocol) for routing within an organization's network, and BGP as the EGP (Exterior Gateway Protocol) between networks, with routing information synchronized between the IGP and EGP during operation. However, IGPs such as OSPF or IS-IS were not designed to process the large volume of routing information handled by BGP, so it was necessary to deviate from this architecture. This meant that instead of the BGP passing on routing information to the IGP, architecture in which BGP and IGP operate asynchronously as separate entities became the standard.

Furthermore, large-scale networks have recently been switching to architecture in which only the network topology (architecture) and the minimum necessary routing information are handled by IGP, with all other routing information handled by BGP, in order to support an increase in routes within the network and accelerate IGP convergence speed. For this reason, it has become crucial to implement BGP properly in order to route traffic correctly both between networks and within a network.

2.2 Network Policies

Each network has individual routing policies. There are some policies that leave everything to the routing protocol, and some networks that take more care with route selection. Using BGP, the policies for each network can be configured when routing information is exchanged. However, only a few items can be configured. They are limited to route filtering and priority settings, and markers for post-processing. When routing with BGP there is a need to skillfully implement a network policy that combines these elements to design a system that achieves the intended state.

There are some policies that the majority of networks use as standard. These are the customer, peer, and upstream policies that are specific to the type of interconnecting party. Customers are relayed (transited) to other networks such as peer or upstream ISPs. When routing traffic, in addition to sending all routes on the network itself to customers, routes advertised from customers are also sent to other networks. Peer ISPs exchange traffic with one another and with customers, exchanging only routes for the network itself and customers. Upstream ISPs work in a manner opposite to customers, being networks that are relayed to other networks. In addition to advertising routes from the network itself and customers to upstream ISPs, all routes from upstream ISPs are also advertised (Figure 1).

2.3 The Current State of Route Numbers

The routing information advertised by BGP is transmitted out to the rest of the world via interconnected networks. Networks around the world also advertise their routing information similarly, so when using BGP, information from a variety of networks connected to the Internet is received.

At the time of writing the number of BGP routes on the Internet totaled approximately 320,000 for IPv4 and 2,300 for IPv6. Recently the route numbers for both IPv4 and IPv6 have been increasing almost linearly. We also have reason to believe that these numbers will continue to increase in the future. New network connections, additional networks for service expansion, and route advertisement for traffic control are some of the possible reasons for the increasing number of routes.

The increase in routing information will directly lead to higher memory consumption on routers, so this is a factor that should be noted when considering the timing for investing in more router hardware. One future concern is the possibility of IPv4 addresses running out. As a consensus was reached on a policy for IP address transfers at an APNIC meeting last year, routes are expected to be advertised in smaller units to improve the utilization efficiency of IPv4 addresses from around the time that they dry up. This is expected to lead to a further increase in the number of routes.

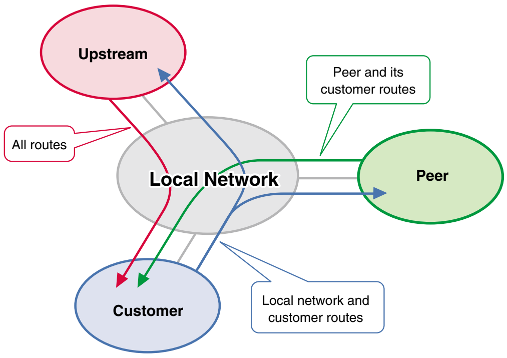
Upstream
Peer and its customer routes
All routes
Local Network
Peer
Customer
Local network and customer routes

Figure 1: Peers, Customers, and Upstream

2.4 Advertisement without Authority

Route hijacking is a common problem when using BGP. This problem is chiefly due to the unauthorized creation and advertisement of another entity's routing information, which causes communications directed to that network to be sent to another unrelated network, rendering communications impossible. When issues such as this are used as attack methods, there are a number of ways they can be exploited. In addition to the simple blocking of communications, they can also be used to pose as another person and create fraudulent websites, and to intercept communications. In fact, in 2008 a well-known video upload site was rendered inaccessible, and in April 2010 an incident occurred in which an AS in Asia advertised several tens of thousands of pieces of routing information around the world.

It is rare for the root cause of incidents such as these to be reported in detail, but from the circumstances we can surmise that they were caused by erroneous BGP configuration settings being made unintentionally. We can also speculate that most other incidents that have been reported up to now were due to erroneous configuration settings, and the term "route hijacking" may misrepresent the actual situation, so we believe that it is more appropriate to call these incidents "advertisement without authority."

Due to BGP not being aware of the routing information that is exchanged, this kind of advertisement without authority can occur. The question of which routing information to receive and which routing information to ignore is completely dependent on policies, or in other words the routing information controls for each network. Consequently, depending on the application, it may be possible to prevent this advertisement without authority, or reduce its impact.

For example, if routing information advertised from customers on each network is comprehensively filtered, no inconvenience will be caused to networks around the world through advertisement without authority. In the past it was pointed out that networks that do not filter incoming routes for customers were also responsible for having relayed routing information. At IIJ, we ask customers using BGP connections to contact us before advertising routing information, and then set comprehensive route filtering.

Meanwhile, if there is even one network without route filtering implemented in the upstream of a network that has carried out advertisement without authority, there is a chance that routing information will be spread worldwide. Problems like this still occur on and off, so we believe a large number of networks have still not implemented comprehensive incoming route filtering for customers. The likelihood of being able to reduce the impact of these incidents will increase if more networks implement suitable route filtering. We intend to continue calling for better operating procedures to be implemented through operator communities, etc.

2.5 Detecting Anomalous Routes

As we have demonstrated here, there is currently no way of completely preventing the advertisement without authority of another party's routing information over BGP. For this reason, when advertisement without authority occurs, it is crucial to be able to detect it swiftly. Various initiatives for the detection of anomalous routes are being implemented around the world.

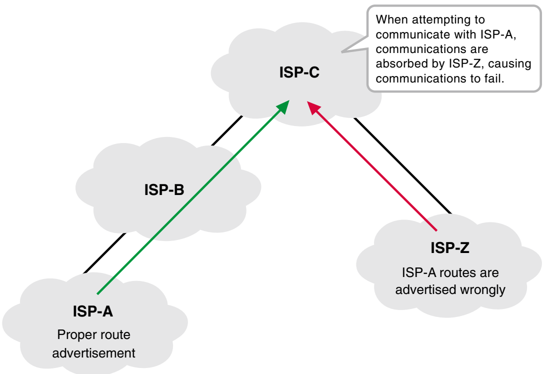
When attempting to communicate with ISP-A, communications are absorbed by ISP-Z, causing communications to fail.
ISP-C
ISP-B
ISP-Z
ISP-A routes are advertised wrongly
ISP-A
Proper route advertisement

Figure 2: Blocked Communications due to Route Advertisement Without Authority

Each detection system uses successive approximation to compare variations in the route that is considered correct and the actual route over BGP, and when there is a discrepancy it is treated as an anomalous route. Due to this structure, these detection systems face the following two issues.

- How to determine that a route is correct
- Where to obtain the BGP routing information for comparison

Regarding the first issue of how to determine that a route is correct, a number of methods have been tested. For example, some systems determine routes that have been advertised stably for long periods to be correct, and treat variations from this advertisement source as anomalous. There are also systems that involve registering the correct routes manually, with discrepancies from this data treated as anomalous.

The second issue of where to obtain routing information for comparison is a difficult one. Each network has their own routing policies, so naturally the routing information that they retain also differs. There are also routers that use BGP within a network. These also potentially retain different routing information. To detect localized impact it would be necessary to obtain routing information from a larger number of networks and routers.

2.6 Initiatives within Japan

Initiatives within Japan for detecting anomalous routes include a route monitoring system - Keiro-Bugyo (Route Magistrate) governed by Telecom-ISAC Japan. Route Magistrate utilizes the route objects registered to JPIRR (IRR (Internet Routing Registry) operated by JPNIC), as standards to determine correct routing, using successive approximation to compare this data with BGP routing information submitted to the system by ISPs in Japan and detect anomalous routes. Routing information that is advertised from a source other than the one registered to the route object is treated as anomalous, so this system is useful for detecting anomalous routes due to configuration errors. Additionally, because routing information is obtained from ISPs in Japan, it is possible to predict the impact within Japan to a certain extent. IIJ has participated in the operation of this system since it was introduced, and we have been committed to activities that further improve detection rates. IIJ also takes advantage of this system as a user to monitor our own routes. In the past we have received warnings from Route Magistrate when routing information advertised by IIJ was advertised from other networks.

2.7 Dealing with Detected Anomalous Routes

When a warning is received, we first confirm the current status using an external looking glass site. In most incidents to date the routing information in question has been restored within a few minutes, so there is a chance of the situation already being resolved when the alert from the detection system is received.

However, when problematic route advertisement is still occurring, we attempt to contact the advertisement source for the route in question. When doing this, it is important to update IR (Internet Registry) and IRR registered information on a regular basis in order to communicate the legitimacy of our route advertisement.

When the source of the advertisement problem cannot be contacted, it can be helpful to contact the network thought to be their upstream ISP for assistance. When the matter still cannot be resolved, it is necessary to do whatever possible to work toward a solution by asking peripheral networks or the operator’s community for contact details or assistance.

While implementing measures such as these in the near-to-mid term, we will explore more streamlined methods for identifying correct routes in the long term. One such method is RPKI (Resource Public Key Infrastructure), which uses digital signatures to carry out authentication. Using RPKI, when an IP address is allocated by the IR, a digital signature called a resource certificate is issued, clarifying who has the right to use that IP address. Under this system routing information is authenticated by routers, automatically determining that the routing information is being advertised by a legitimate advertisement source. This system is already in the process of being implemented by a number of router vendors, and firmware that enables routing information to be authenticated using digital signatures is actually undergoing verification tests. However, there are still problems that need to be resolved with the issuing of certificates and the use of digital signatures, and it appears that it will be some time before RPKI can be introduced. Meanwhile, IIJ will continue to participate in activities for achieving more reliable routing.

Author:
Yoshinobu Matsuzaki
Mr. Matsuzaki is a Senior Engineer in the Technology Promotion Section of the Network Service Division in the IIJ Network Service Department. Mr. Matsuzaki is always finding things that pique his interest while striving at his work. He is an IIJ-SECT member, co-chair of The Asia Pacific OperatorS Forum, chair of APNIC IPv6 SIG, and an expert advisor for JPCERT/CC.