IEICE TRANS. COMMUN., VOL.E86–B, NO.2 FEBRUARY 2003

PAPER *Special Issue on Internet Technology III*

An Integrity Check for the Conflict Origin AS Prefixes in the Inter-domain Routing

Kengo NAGAHASHI[†a)], ***Nonmember***, **Hiroshi ESAKI**[†], ***and*** **Jun MURAI**[††], ***Regular Members***

SUMMARY In the Internet, the routing system consists of the Interior-domain and the Inter-domain. Within the Inter-domain routing, Autonomous System (AS) represents the administrative network domain, which is managed by a single institution with its operational policy. ASs exchange the ASs' reachability information to each other. Without the Inter-domain routing scheme, the nodes in the Internet can't communicate across the multiple ASs. The Inter-domain routing is an essential functional element in the global Internet operation. However, due to several reasons such as miss-configuration at the routers, the Inter-domain routing becomes unstable. This occurs that one AS (say AS1) propagates the prefix that has been already assigned to another AS (say AS2) and other peers receive its routing update and inject the misconfigured AS information to their peering routers. Since the routing information associated with AS1 is over written by AS2, AS1 loses the network connectivity. This problem is known as the Conflict Origin AS prefix or the Multiple Origin AS. We recognize that this is a serious problem which degrades the quality of Internet backbone infrastructure. We focus on this problem and propose the mechanism that can detect the Conflict Origin AS prefix automatically using the policy database. Based on the evaluation using the prototype system, we demonstrate that the proposed mechanism can work well with the existing Internet's Inter-domain routing system.

key words: *BGP, prefix, Autonomous System (AS), IRR*

1. Introduction

Routing in the Internet consists of Interior-domain and Inter-domain routing. The domain in this context means AS (Autonomous System), which is a collection of routers and links administered by a single institution such as ISPs (Internet Service Provider), enterprises, or universities. Interior-domain routing protocol exchanges the network prefixes information among the routers in a single AS, and the Inter-domain routing protocol exchanges the routing information across the ASs.

In this paper, we focus on the Inter-domain routing system. Most Interior-domain routing protocols use the link-state mechanism, where all routers in the routing domain maintain the complete topology database in the routing domain. Doe to too large a number of routers in the global Internet space*, Inter-domain routers do not maintain the topology databases.

In current Inter-domain routing, BGP [2], [3] is the standardized and commonly used routing protocol. BGP uses the Path Vector algorithm for exchanging and maintaining the routing information. Path Vector algorithm provides loop prevention mechanism as follows:

- AS_i originates the network prefix and creates directed graph called as_path, as_path=(i, AS_i) and propagates BGP update to peering AS_j. Here, i represents the identifier of the routing domain originated AS_i.
- AS_j receives its update from AS_i. AS_j prepends its own AS to the received as_path as as_path = (i, AS_i, AS_j), and sends it to other peers.
- if there is the duplicated AS in as_path, BGP regards it as a loop and discard its update.

Due to its loop prevention and scalable architecture, BGP is now the commonly used standard Inter-domain routing protocol. However, there still remains lots of problems in BGP. This problems will be addressed in this paper. In Sect. 2, we describe an issue regarding the Conflict Origin AS prefixes in detail. In Sect. 3, we introduce the related works around the Conflict Origin AS prefixes problem. In Sect. 4, we describe the proposed architecture for detecting the Conflict Origin AS prefixes. In Sect. 5, we implement and evaluate the proposed architecture. Finally, in Sect. 6, we summarize the discussion of this paper.

2. Problem Description

The following two are be serious problems, that the current Inter-domain routing system has.

1. Delayed convergence of routing information
2. Conflict origin AS prefix

In Inter-domain routing, when one AS sends the routing update to other peers, the peers transit the updates to other peers. With this hop-by-hop update propagation, the routing table update in the global Internet Inter-domain routers is finally updated and converged.

Manuscript received June 25, 2002.
Manuscript revised August 18, 2002.

[†]The authors are with the Graduate School of Information Science and Technology, The University of Tokyo, Tokyo, 113-8656 Japan.
[††]The author is with the Faculty of Environmental Information, Keio University, Fujisawa-shi, 252-8520 Japan.
a) E-mail: kenken@wide.ad.jp

*On 2000, there are at least 6474 ASes in use [1].

We call "delayed convergence of routing information" so that there is a delay to convergence of the routing information. R. Govidan [4] indicates that the recent increase of multihome sites, which have more than two upstream AS and propagate non-aggregated prefixes to "Default Free Zone" makes the convergence slower. According to G. Lavovits et al. [5], more than 25 percent of ASes in the global Internet are non-aggregated multihome sites.

As well as the delayed convergence, the Conflict Origin AS has been a serious issue for the Internet growth. The Conflict Origin AS problem can be defined as:

- AS_i originates network prefix P_1 and is propagated by other peers.
- With some reason, another AS_j ($AS_i \neq AS_j$) originates the same network prefix P_1 and sends the update to the peering routers.
- Peers withdraw $P_1(i, AS_i, \ldots)$ and select $P_1(i, AS_j, \ldots)$.
- AS_j doesn't have network connectivity associated with P_1 and AS_i loses network connectivity. It is the so-called "Black Hole Route."

This "Black Hole Route" has seirious impacts on the global Internet as follows:

- Not only one prefix but also AS itself, becomes unstable (i.e., route flapping), which also makes the convergence slower, described in the previous problem.
- As several researches are pointed out, Instability in one AS makes the global Internet pathological impacts.

The Conflict Origin AS problem has been widely observed and has increased in recent. According to X. Zhao et al. [6], the median of Conflict Origin AS prefixes per year at one Internet Exchange point is 683 in 1998, 810.5 in 1999 (18.7% increased), 951 (17.3% increased) in 2000 and 1294 in 2001 (36.1%). They pointed out several reasons why the Conflict Origin AS prefixes problem occurs:

Multihoming without BGP Suppose there is a link between two ASes, but the routing across this link does not use a BGP (i.e., relies on static routing or some IGP instead). From a BGP perspective, it appears as if one AS can directly reach prefixes belonging to the other AS.

Faulty and Malicious Configurations Conflict Origin AS can also occur when an AS incorrectly originates routes to some other organization's prefixes. This could occur due to configuration errors or even intentional malicious attacks.

We often observe this phenomenon, here and there, in the Internet. And if the the network administrators find the Conflict Origin AS prefix and lose network connectivity, the following procedures are usually taken:

- A query is made to the IRR (Internet Routing Registry) [7] and searches which AS announces the invalid prefix. Here, IRR provides the network resource information, such AS or routes.
- If there is a corresponding entry in IRR, IRR returns the records containing the origin-AS and technical contact associated with the conflict AS.
- The system administrator contacts the AS administrators who were indicated in the IRR database via telephone number or e-mail address.
- AS administrators try to fix the conflict origin-AS problem by re-configuring the router, rebooting, etc.

With these simple, manual procedures, it may take a long time to recover the connectivity and require a lot of human labar. So, the purpose and goal of this paper is automatically detecting the Conflict Origin AS prefixes in order to improve the recovery latency and reduce the consts from loss of connectivity.

3. Related Work

The Conflict Origin AS problem has been discussed at the IETF (Internet Engineer Task Force). RFC1930 [8] recommends that every network prefix should belong to only one AS. If every AS adheres to this operational recommendation, the Conflict Origin AS should not occur. Berkowitz [9] discussed the potential causes why the Conflict Multiple Origin AS occurs, but, the discussion is not complete and there is no implementation.

One of the essential problems of the Conflict Origin AS is how to prevent an AS from injecting inappropriate prefixes toward the Internet. In this point of view, a couple of possibilities have been are investigated. One is "BGP Route Flap Damping" [10]. BGP Route Flap Damping intends to prevent route flapping, which creates thousands of updates and withdraws in a minute, but this work is not related with the prevention of Conflict Origin AS problem. "S-BGP (Secure BGP)" [11] is another approach to prevent invalid prefix. This implements a strong security framework such as IPsec, Certificate Authority, in order to prevent inappropriate announcement from every AS boarder router.

Another approach is "prefix authentication using DNS" [12]. This approach defines the new DNS Resource Record which is named AS RR. Once this RR was referred by the BGP router, it was treated as the authenticated prefix. This approach has proposed in IETF but its draft has already expired and not became to the Internet standard.

In summary, there are couple of related works which focus on the prevention of the inappropriate network prefixes announcement and focus on just the IRR itself. There has been no research work that defines the interaction between IRR database and BGP router.

4. Proposed Architecture

In this section, we describe the system requirements and the proposed architecture for detecting the Conflict Origin AS prefix in detail.

4.1 Requirements

This subsection describes the system requirements, which can detect the Conflict Multiple Origin AS prefixes.

As we described in Sect. 2, the essential factors of the Conflict Origin AS are inappropriate network prefix(s) announcements by some AS, instead of the correct announcement by correct AS. The basic approach to detect the Conflict Multiple AS prefixes would be:

- store kinds of database about the prefix P_1 and associated origin AS AS_i, which should announce P_1 to the Internet. $(P_1 \Rightarrow AS_i)$
- check the origin AS (AS_j) in update message which should or should not announce the prefix (P_1), when every BGP boarder router receives the update message
- compare with AS_j and AS_i

As discussed in rfc2791 [13], the Inter-domain routing requires further operational scalability associated with the number of AS boarder routers, and severe security than the Interior-domain routing does.

Now, the following should be requirements for detecting the Conflict Multiple Origin AS:

1. integrity check whether every AS announces the correct and appropriate network prefix(es)
2. security which prevents faking of database entry
3. scalability regarding the number of boarder routers

We describe the detail of each requirement in the next section.

4.2 Architecture Overview

The overview of the proposed architecture to detect the Conflict Origin AS prefix is as follows:

1. When BGP router receives update from other peers, BGP router fetches out prefix (P_1) and its origin-as (AS_i).
2. BGP router examines to its own cache using the prefix (P_1) as a entry key.
3. If the cache holds prefix (P_1) and the associated origin-as (AS_c), return the origin-as (AS_c) value.
4. BGP router compares with AS_i and AS_c. if $AS_i \neq AS_c$, it regards it as the Conflict AS prefix and discards the received update request.
5. If there is no associated prefix entry in the cache, BGP router sends the query message to the IRR database (query key is prefix (P_1)).
6. The IRR database searches the origin-as (AS_r) using the prefix information in the query message, and returns it (AS_r) to the to the BGP router.
7. BGP router compares with the origin-as (AS_i) in update message and the (AS_r) in IRR database. If $AS_i = AS_r$, the BGP router regards P_1 is the correct origin-as prefix and stores it (P_1, AS_r) in its own cache. If $AS_i \neq AS_r$, the BGP router regards P_1 is the Conflict Origin AS prefix and discards it to ignore the update message.

BGP holds FSM (Finite State Machine) for each peer. FSM can define 3 phases: first phase is establishing the peer, second phase is operational and third phase is to disconnect the peer. We focus on establishing peer and operational phase. The reason why we focus on "establish and operational" is that BGP tend to update routing information dynamically after establishing a peer and so it is not enough to check only the establishing phase.

4.3 Integrity

As we described Sect. 4.1, in order to detect the Conflict Origin AS prefix, we need the database which stores the correct origin-as information, according to the network prefix. We propose that we use the IRR as the entity to store this information, since we can implement the database, we need some extension to the existing database in the IRR.

4.3.1 Database Using IRR Extension

IRR is the global Internet resource database that stores routing information such as AS number and prefix information. IRR consists of several objects (Route Object, Aut-num Object, Maintainer Object etc.), which have key attributes and associated attributes. The object itself, of course, has relation with other objects.

Route Object represents the network prefix information. For instance, it is the one that maintains the prefix, i.e., which AS should announce the prefix. The key attribute for this object is the network prefix of IPv4 or IPv6.

Aut-num Object represents the AS information, such as AS number, local-preference, MED, and inbound/outbound AS filter. The key attribute for this object is the AS number.

Maintainer Object represents the one that can access and create route, aut-num and other objects. Also, this object defines the authentication method, such as password, PGP, etc. The key attribute of this object is mntner which was assigned from registry such as MAINT-APNIC.

Figure 1 represents a sample of IRR Route Object. Most IRR databases are written by RPSL (Routing Polisy Specification Language) [14] which extends

```
route:          204.70.2/24
descr:          ROUTE-AA
origin:         AS65361
mnt-by:         MAINT-APNIC
changed:        sample@aa.net 20020607
source:         AA
```

Fig. 1 Example of Route Object in IRR database.

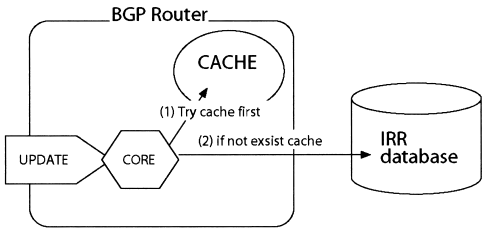

Fig. 2 Cache behavior.

RIPE-181 Language.

The main advantages of using IRR are:

- Most ISPs are using and registering there route, AS objects to the IRR for the Internet resource repository.
- User Interface between users and IRR is WHOIS and it is easy to access. And also protocol specification is simple to implement.
- Couple of IRRs are distributed in the global Internet space, and all of them are mirrored and sycronized each other once in a day.

However, there would be still remains couple of disadvantages to use the IRR. One of the most severe disadvantages would be the lack of IRR utilization. As L. Gao pointed out [15], all prefixes in the Internet may not registered into the IRR. This means that the system only using the IRR may not have enough database information for correct and reliable operation, since the queried origin-as by the BGP router is not registered in the IRR. Here, we analyze the current IRR utilization in Sect. 5.2.

To prevent this situation, we additionally introduce the BGP snapshots into the IRR. By introducing this supplemental approach, the IRR utilization can be good enough to use as the integrity check database.

4.4 Scalability

Scalability in this context is that our approach can apply in the contemporary BGP routing circumstance. So we examine the contemporary BGP routing circumstance,especially the number of update messages. By its result, the number of updates per hour is least 8,700 updates (send) and 2,100 updates (received) per hour, which is described in the Sect. 5.3.

4.5 Cache

As we described Sect. 4.4, to reduce the overloading of BGP router and the IRR searching, we introduce the cache mechanism in the BGP router. Figure 2 represents the flow of cache behavior.

The cache behaves as follows:

1. BGP router receives the update message and fetches out the prefix contained in the received update message.
2. BGP router examines the cache using the prefix information in the BGP router.The cache maintains pairs of prefix and corresponding origin-as derived from IRR replys against the queries issued by by the BGP router.
3. if the corresponding pair exists in the cache, the origin-as is returned from the cache. Here, the search is using the exact prefix match algorithm.
4. if corresponding pair does not exist, the BGP router queries to the IRR.
5. BGP router receives the replied orgin-as information from the IRR database.
6. BGP router compares the reply with the update message, and store the pair of prefix and origin-as, that is provide by the IRR.

4.6 Security

In Inter-domain routing, security means whether the BGP routers announce the “correct” updates to other peers.

We need the method to validate both Route Objects in the IRR and the BGP snapshots. The IRR has established the authentication method for the users, who register the routing information database. The IRR uses PGP to ensure that malicious person can not register invalid origin-as information. Regarding the BGP snapshot introduction to the proposed database, we use the snapshot based on all of the snapshots maintained by the major Internet Exchange points. We only use the prefixes that are duplicated in all IXes’ snapshot. Therefore, there is no chance, where some malicious user could register inappropriate network prefix information in the proposed database.

4.7 Contorol Messages

It is assume that the BGP router and the IRR palce to the separated equipment. The BGP router accesses IRR over the Internet. Therefore, we needs to define the control messages between the BGP router and the IRR. All of the messages described below uses TCP (port number is 2107):

- QUERY message
- REPLY message
- KEEPALIVE message

4.7.1 QUERY Message

BGP router issues QUERY message, when BGP router queries to the IRR after receiving update message from other peers.

QUERY message consists of 1 octet of Message-Type field (fixed value 1) and 20 octets of prefix field. The prefix field contains only one prefix.

4.7.2 REPLY Message

IRR database issues REPLY message. When the IRR receives the QUERY message from the BGP router, it examines own database using the prefix information in the QUARY message. IRR replies its result as the REPLY message to the BGP router.

REPLY message consists of 1 octet of Message-Type filed (fixed value 2) and 4 octects of origin-as field which contains only one AS Number.

4.7.3 KEEPALIVE Message

The BGP router issues KEEPALIVE message to maintain the TCP connection with the IRR every 30 seconds. When the BGP router sends KEEPALIVE message to the IRR, the IRR also sends back the KEEPALIVE message.

If the BGP router receives the KEEPALIVE message from the IRR, a keep alive flag in the BGP router is turned on. For both the IRR and the BGP router, all of the messages (i.e., QUERY, REPLY and KEEPALIVE messages) can be issued only when the keepalive flag has turnd on.

KEEPALIVE message consists of 1 octet of Message-Type field (fixed value 3 (from BGP router) and 4 (from IRR database)).

5. Implementation and Evaluation

Based on the proposed architecture described above, we implemented the prototype system. Table 1 shows the implementation plathome.

The modification of the BGP router is the BGP update processing and the message definition. As shown in Fig. 3, we define bgp_registry structure in the BGP update processing.

Also we modified the IRR, in general, if one user queries the IRR, the IRR returns all of the records indicated by the request message. In the proposed system, it takes processing overhead to parse only the origin-as field in whole Route-Object. Therefore, we modify the IRR so that the IRR only replies the origin-as records to the BGP router, against the QUARY message.

Table 1 Implementation plathome.

OS	FreeBSD 4.3
BGP daemon	zebra-0.92a [16]
IRR	YARD-0.1a

5.1 Evaluation

As we described Sect. 4.3, we evaluated the IRR utilization (i.e., how many percentage of routing prefixes is registered in the IRR) in the contemporary BGP environment. Also, based on our implementation, we evaluated the effectiveness of the proposed architecture.

5.2 Integrity Check by the IRR Database

To evaluate the exact IRR utilization, we examined how many percentage of prefixes in the Internet is registered in the IRR based on the following procedures:

1. We fetched out the Route object from all IRRs[†]. Total number of Route object in IRRs is 76,083 (ommited a duplicated prefixes).
2. We also took snapshot of the BGP routing table from the BGP router which connectsI the Internet Exchange Point. The total number of BGP routing table is 113,973.
3. We applied the exact match method for each prefix length (i.e., /24, /25, etc.) between the IRR prefixes and the BGP routing table prefixes.

The measurement result indicates that the percentage of the IRR utilization in the BGP routing table (= average of the number of the Route objects / number of th e BGP routing table for each prefix length) is 66%. It means that 34% network prefixes are not registered in the IRR. Especially, regarding the prefix length /24 which is the highest distribution of all prefix length, the number of BGP routing table is 58,775 entries but the number of Route Objects in the IRR is only 26,248 records and the IRR utilization is 44.6%.

To improve the IRR utilization, we introduced the use of BGP routing table snapshots. We examine to

```
struct bgp_registry_config
{
  int sock ;
  int enabled ;
  struct stream *ibuf;
  struct stream_fifo *obuf;
  struct stream *host;
  struct stream *as;
  struct stream *rr_as;
  struct hash *cache;
  struct addrinfo *res;
  u_int32_t is_keepalive;
};
```

Fig. 3 bgp_registry_config structure.

[†]Currently 44 IRRs are existed in the Internet.

Table 2 Measure environment.

Duration	2001/11/20 16:00 - 2001/11/22/ 16:00
Network I/F	FastEthernet (100base-TX)
Number of peers	13

Table 3 Number of BGP updates.

Total Num. of send updates	44,677
Unique prefix in updates	606
Percentage of unique prefix	1.4%
Total Num. of received updates	23,671
Unique prefix in updates	302
Percentage of unique prefix	1.2%

collect a couple of BGP routing tables from various Internet Exchange points, AADS, MAE-EAST, MAE-WEST, PACBELL, PAIX (all from [17]) and OREGON [18]. The total number of the unique origin-as prefix about all IX points is 122,028. As a result, the total utilization of the proposed IRR (IRR + BGP routing table snapshots) becomes 94.5%. Regarding /24 prefix length, the utilization is 90.5% (53,225(IRR+snapshot)/58,775(BGP routing table)).

5.3 Evaluation of Scalability

Scalability in this context is whether the proposed system can work with the scale of existing the BGP in the contemporary Internet routing environment. We have examined the scalability of the proposed system, associated with the number and frequency of update messages.

Table 2 describes the environment of the measurement. We measured the number of updatesthe inbound and outbound for each peer. Table 3 shows the total number of the BGP updates. The percentage of the unique prefix means that the number of unique prefixes in the total number of updates. As of send-updates, the percentage of unique prefix is only 1.4% and another is 98.6%. This means that only specific one or few prefixes are continue to update and withdraw. This phenomenon is called "Route Flapping" which single prefix repeats hundreds of updates and withdraws in a minute. When we use a simple integrity check without the cache discussed in Sect. 4.5, the BGP router queries to the IRR in every time whenever the BGP router receives the update message. In this case, it is hard to operate the IRR, due to overloading by the reception of updates within a short period of time. In order to solve this issue, we have proposed the cache mechanism.

Figure 4 shows the frequency of update message reception per hour. The maximum number of updates per hour was 8,700 updates per hour (for send) and 2,100 updates per hour (received), respectively. These large number of the BGP updates derives mainly from the change of routing policy or from the outage of border routers. This results indicate that, when we operate the proposed architecture without the cache at the

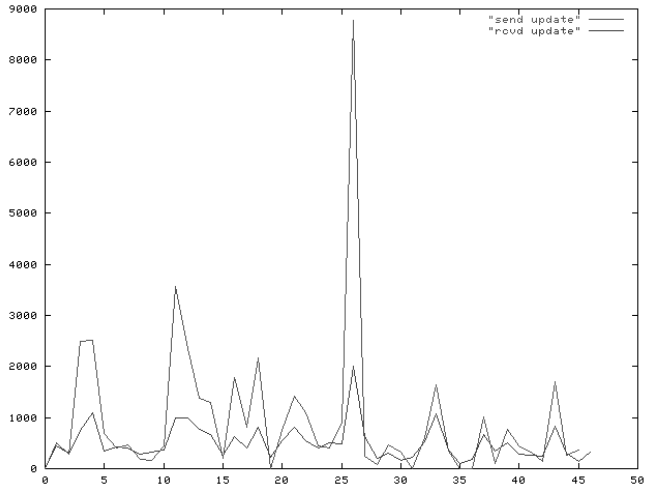

Fig. 4 Number of send/received updates per hour.

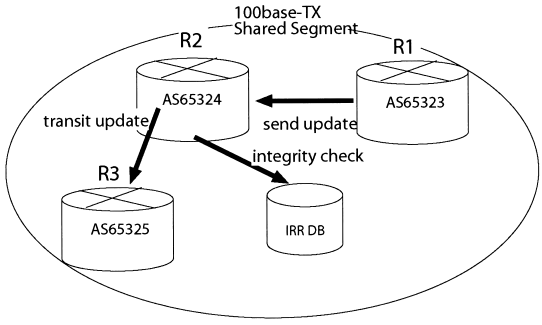

Fig. 5 Evaluation network.

BGP router, the IRR has to be able to take care of, at least, ten thousands of QUARY messages per hour.

Below, we evaluate the scalability of the proposed architecture using the prototype system. Figure 5 shows the evaluation network of our implementation. On this network, we evaluate our implementation as following procedures.

1. R1 periodicaly sends the burst number of BGP update messages, which contains 10 prefixes to R2.
2. R2 receives (received time is t_1) the update messages from R1 and validates the origin-as via the following two methods.
   a. without cache, the direct query to the IRR database, whenever R1 receives the update message.
   b. with cache, R2 examines its cache, at first. If the cache is missed, R1 issues the query message to the IRR.
3. After the validation, R2 sends the update message to R3.
4. R3 receives (received time is t_2) the update message from R2.

With this evaluation model, we measured the time

Table 4 Evaluation result.

updates/min.	D_t	C_t
6	34.3	35.4
60	31.9	36.2
120	38.7	34.4
180	41.2	33.9
300	48.9	32.3
600	62.4	36.1

of the BGP update processing, $t_2 - t_1$, by parameterizing the update frequency. The result of the evaluation is shown Table 4. Here, D_t represents $t_2 - t_1$ without cache, and C_t represents $t_2 - t_1$ with cache.

When the update message frequency becomes larger than 120 updates per minutes, the performance without cache is getting degraded because of direct and every querying to the IRR.

For 6 or 60 updates per minitues, there is a little performance difference between with cache and without cache.

Here, 600 messages per minutes corresponds to 36,000 per hour. This means that the above evaluation would cover the practical Internet environment. This because, as discussed above, the IRR has to be able to take care of, at least, ten thousands of QUARY messages per hour.

In summary, the proposed system with cache will work well without overloading due to too frequent update message reception, though the proposed architecture without the cache will not work well due to the overloading of too frequent update message receptions.

5.3.1 Scalability Consideration

BGP is running over the global Internet infrastructure so it needs to consider about scalability which can sustain the global Internet infrastructure. To sustain the global Internet infrastructure means that our approach is still an efficient if all BGP routers in the Inter-domain implement our approach. Here is one of t he most serious issues that we need to consider:

1. what happen if all BGP routers query the IRR.
2. what happen if the BGP routers reboot by somehow reasons and receive the full routes from other peers.
3. what happen if transit BGP routers are down and thousands of the BGP update and withdraw messages are issued.

Regarding with issue 1, when one BGP router injects the Conflict Origin AS prefix and sends the BGP update to other peers, another BGP router that receives its update can detect the Conflict Origin AS prefix and discards its prefix silently, so there doesn't propagate the Conflict Origin AS prefix all over the BGP routers. Regarding with issue 2, the BGP router that recovers from reboot will query the same frequency of full routes and it requires somehow mechanisms that can handle piggy back query. Regarding with issue 3, if the transit BGP router goes down, other peering BGP routers still hold the cache and no need to the query to the IRR.

6. Conclusion

In this paper, we discussed the Conflict Origin AS prefix problem in the Inter-domain routing. Based on the discussion for system requirements to come up with this particular issue, we proposed the new architecture to detect the Conflict Origin AS prefix. The proposed system should satisfy the scalability, serucity and integrity. We evaluated the proposed architecture using the prototype system. We can show that the proposed architecture will work well even with the large route update frequency, that is observed in the actual Internet.

The future work around this research would be 2 ways. One is to apply this approach to the global Internet infrastructure such as Internet Exchange point and measure its perfomance. The other is to introduce this approach to the Interior-domain routing scheme, such as OSPF.

References

[1] L. Gao, "On inferring autonomous system relationshops in the Internet," IEEE/ACM Trans. Netw., no.6, pp.733–745, Dec. 2001.
[2] Y. Rekhter and T. Li, "A border gateway protocol 4 (BGP-4)," RFC 1771, Match 1995.
[3] D. Katz, Y. Rekhter, T. Bates, and R. Chandra, "Multiprotocol extensions for BGP-4," RFC 2283, Feb. 1998.
[4] R. Govindan and A. Reddy, "An analysis of inter domain topology and route stablity," Proc. IEEE INFOCOM, April 1997.
[5] G. Labovits, G. Robert, and F. Jahanian, "Internet routing instability," IEEE/ACM Trans. Netw., no.5, pp.515–528, Oct. 1998.
[6] X. Zhao, D. Pei, L. Wang, D.M. Allison, M.S. Felix, and W.L. Zhang, "An analysis of BGP multiple origin AS (MOAS) conflicts," ACM SIGCOMM Internet Measurement Workshop, Aug. 2001.
[7] Internet Routing Registry Web. http://www.irr.net/
[8] J. Hawkinson, "Guidelines for creation, selection, and registration of an autonomous system (AS)," RFC 1930, March 1996.
[9] E. Davies, H. Berkowitz, and L. Andersson, "An experimental methodology for analysis of growth in the global routing table," Internet-Draft, Working in Progress, 2001.
[10] C. Villamizar, R. Chandra, and R. Govindan, "BGP route flap damping," RFC 2439, Nov. 1998.
[11] S. Kent, C. Lynn, J. Mikkelson, and K. Seo, Secure Border Gateway Protocol (S-BGP)—Real World Performance and Deployment Issues, Aug. 1998.
[12] http://www.academ.com/nanog/feb1998/origin.html
[13] J. Yu, "Scalable routing design principles," RFC 2791, July 2000.
[14] C. Alaettinoglu, T. Bates, E. Gerich, D. Karrenberg, and D. Meyer, "Routing policy specification language (RPSL)," RFC 2280, Jan. 1998.

[15] L.J. Gao, "Stable internet routing without global coordination," ACM SIGCOMM 2000, Aug. 2000.
[16] Zebra Project, http://www.zebra.org/
[17] Merit Internet Performance Measurement and Analysis Project, http://www.merit.edu/~ipma/routing_table/
[18] Oregon Exchange BGP Route Viewer, Host:route-views.oregon-ix.net.

Kengo Nagahashi was born in Shizuoka, Japan, on July 28, 1977. He received his B.A. and M.A. degrees, from Keio University, Kanagawa, Japan in 2000, 2002 respectively. He is currently Ph.D. student at the Graduate School of Information Science and Technology, The University of Tokyo, Japan. His current interests include a policy based network.

Hiroshi Esaki received the B.E. and M.E. degrees from Kyushu University, Fukuoka, Japan, in 1985 and 1987, respectively. And, he received Ph.D. from University of Tokyo, Japan, in 1998. In 1987, he joined Research and Development Center, Toshiba Corporation, where he engaged in the research of ATM systems. From 1998, he works for University of Tokyo as an associate professor, and works for WIDE project as a board member. He has been at Bellcore in New Jersey (USA) as a residential researcher from 1990 to 1991, and has engaged in the research on high speed computer communications. From 1994 to 1996, he has been at CTR (Center for Telecommunications Research) of Columbia University in New York (USA) as a visiting scholar. He is currently interested in a high speed Internet architecture, including MPLS technology, a mobile computing, and IPv6.

Jun Murai is a professor, Faculty of Environmental Information, Keio University. He graduated Keio University in 1979, Department of Mathematics, Faculty of Science and Technology, received M.S.for Computer Science from Keio University in 1981, received Ph.D. in Computer Science, Keio University, 1987. He is a director of Keio Research Institute at SFC, The President of Japan Network Information Center (JPNIC), The Internet Corporation for Assigned Names and Numbers (ICANN) Board of Director, Adjunct Professor at Institute of Advanced Studies, United Nations University.