CNGI-CERNET2: an IPv6 Deployment in China

Jianping Wu
Director, CNGI-CERNET2
jianping@cernet.edu.cn

Jessie Hui Wang
Tsinghua University, CERNET
hwang@cernet.edu.cn

Jaihai Yang
Tsinghua University, CERNET
yang@cernet.edu.cn

This article is an editorial note submitted to CCR. It has NOT been peer reviewed.
The authors take full responsibility for this article's technical content. Comments can be posted through CCR Online.

ABSTRACT

Research and promotion of next generation Internet have drawn attention of researchers in many countries. In USA, FIND initiative takes a clean-slate approach. In EU, EIFFEL think tank concludes that both clean slate and evolutionary approach are needed. While in China, researchers and the country are enthusiastic on the promotion and immediate deployment of IPv6 due to the imminent problem of IPv4 address exhaustion.

Since 2003, China launched a strategic programme called China Next Generation Internet (CNGI). China is expecting that Chinese industry is better positioned on future Internet technologies and services than it was for the first generation. Under the support of CNGI grant, China Education and Research Network (CERNET) started to build an IPv6-only network, *i.e.* CNGI-CERNET2. Currently it provides IPv6 access service for students and staff in many Chinese universities. In this article, we will introduce the CNGI programme, the architecture of CNGI-CERNET2, and some aspects of CNGI-CERNET2's deployment and operation, such as transition, security, charging and roaming service *etc.*

Categories and Subject Descriptors

C.2 [**Computer-Communication Networks**]

General Terms

Design, Management, Security

Keywords

Internet, IPv6, Deployment

1. CNGI: CHINA NEXT GENERATION INTERNET PROGRAMME

China has the largest Internet user base of any country and the number of high-speed Internet users has been much more than the number of its available IPv4 addresses. The lack of IPv4 addresses has greatly restricted Chinese ISPs from developing new services and new customers. Therefore, China is one of the most enthusiastic countries on the promotion and deployment of IPv6. China is expecting to avoid imminent problems of IPv4 address exhaustion with the implementation of IPv6.

In September 2003, China Next Generation Internet (CNGI) Programme was launched to empower the research community and the industry to conduct research and implementation of IPv6 in China. The programme is supervised and coordinated by eight ministries, including China Reform and Development Commission, Ministry of Industry and Information Technology, Ministry of Education, China National Science Foundation Commission, *etc.*

CNGI programme is a part of China five-year plans. Currently CNGI is in its fifth year of its second phase. The first phase is from 2003 to 2005. It is a part of $10th$ five-year plan. The first phase projects primarily focused on solving technical challenges during IPv6 deployment, and building experimental IPv6-enabled networks or demonstration networks. The second phase is a part of $11th$ five-year plan, lasting from 2006 to 2010. Projects in the second phase primarily focused on solving challenges in the operation and management of IPv6 networks, developing innovative IPv6 applications, building nationwide commercialized IPv6-enabled backbones and access networks to provide commercial IPv6 access services for network users.

Almost all major ISPs in China participated in this programme. China Telecom, China Unicom, China Netcom (now merged with Unicom), China Mobile and China Railcom (now merged with China Mobile) built their own IPv6 backbone networks based on IPv6/IPv4 dual stack technologies. As a research-oriented ISP, CERNET chose to build an IPv6-only backbone, *i.e.*, CNGI-CERNET2.

Under the support of CNGI grant, there have been 59 Giga-PoPs in Chinese IPv6 backbone networks, extending IPv6 network to over 22 major cities. More than 270 access networks are connected to this IPv6 backbone. Two IPv6 International Exchange Centers are established, *i.e.*, CNGI-6IX and CNGI-SHIX. CNGI-6IX is constructed by CERNET at Tsinghua University in Beijing, and CNGI-SHIX is constructed by China Telcom in Shanghai. These two exchange centers connect IPv6 backbone networks of different Chinese ISPs with each other, and also connect Chinese IPv6 networks with IPv6 ISPs in USA, European, and Asia Pacific Region. Figure 1 illustrates the structure of CNGI-6IX.

2. CERNET AND CNGI-CERNET2

The China Education and Research Network (CERNET) is the first nationwide education and research computer network in China. It accomplished or supported the implementation of a batch of important Internet application projects in China. CERNET is funded by the Chinese government and directly supervised by the Chinese Ministry of Education. Tsinghua and some other leading Chinese universities are responsible for its construction and operation.

CERNET is constructed with a four-layer hierarchy, *i.e.*,

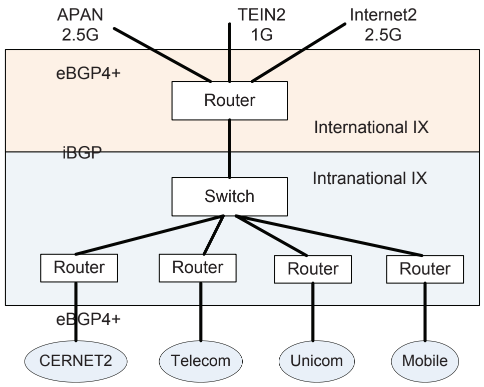

Figure 1: CNGI-6IX, Located in Tsinghua University, Beijing.

the nation-wide backbone, regional networks, provincial networks and campus networks. CERNET National Center is located in Tsinghua University, which is responsible for the operation and management of CERNET national backbone. 10 regional network centers are distributed across the country, and they are responsible for the operation, management, planning and construction of CERNET regional backbones. CERNET provincial nodes are distributed at 38 universities in 36 cities. Currently, more than 2000 campus networks with more than 20 million users in about 200 cities are accessing Internet service via CERNET.

CERNET is an important experiment platform for Chinese researchers to conduct study on next generation Internet. In 1998, CERNET joined 6Bone and became its backbone member. CERNET is also the first ISP in China that interconnects with Internet2.

In 2003, under the support of CNGI grant, CERNET started to construct its IPv6-only backbone CNGI-CERNET2. After seven years, CNGI-CERNET2 backbone has had 25 PoPs. These PoPs connect with each other via 2.5Gbps or 10Gbps links. The backbone provides IPv6 service for more than 200 access networks at 1Gbps, 2.5Gbps or 10Gbps. As an experiment platform, many important new technologies and large-scale applications are running on it. Figure 2 illustrates the architecture of CNGI-CERNET2.

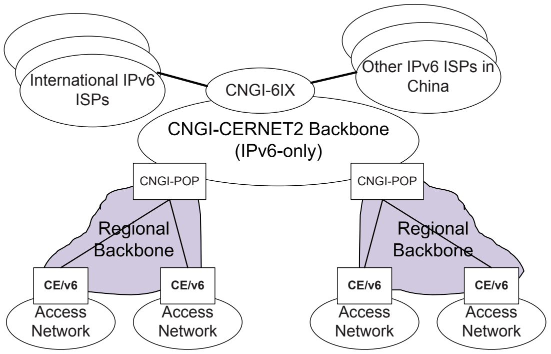

Figure 2: The Architecture of CNGI-CERNET2.

addressing: CNGI-CERNET2 obtained the IPv6 address block of 2001:0da8::/32. This block is further allocated to access networks according to the cities they are located at. 10 large cities each gets a /36 block, and 12 small cities each gets a /37 block. As stub nodes, each access network gets a /48 address block.

routing: CNGI-6IX receives an AS number 23911, and CNGI-CERNET2 backbone receives an individual AS number 23910. Each of 25 regional networks is also allocated an AS number respectively. CNGI-CERNET2 backbone network runs eBGP4+ to exchange routing information with CNGI-6IX. The core routers of CNGI-CERNET2 backbone communicate with each other using OSPFv3 (within AS 23910). At the same time, these core routers announce routing advertisements for their customer network using iBGP4+. All access networks are connected to their regional networks using static routing. OSPFv3 is exploited to exchange routing information within individual access network.

3. DEPLOYMENT AND MANAGEMENT OF CNGI-CERNET2

CNGI-CERNET2 backbone provides IPv6 access service for many university campus networks. Under the support of CNGI grant, each campus network has built its own IPv6-only subnet and connected the subnet to CNGI-CERNET2 backbone to provide IPv6 access service for its students and staff.

During the design, deployment and operation of CNGI-CERNET2, we primarily have the following three concerns:

- **transition**: How to make sure that IPv6 users in CNGI-CERNET2 can coexist and communicate with users in CERNET (which is an IPv4-only network) and IPv4 Internet. This is an important issue for all IPv6 networks.
- **security**: How to improve the network security, *e.g.*, preventing anonymous attacks, enabling the trace-back of attacks or criminals.
- **roaming**: In CNGI-CERNET2 architecture, each access network is an autonomous charging domain. How to control cross-domain access to enable user roaming, *i.e.* users of one campus network can access the Internet conveniently when they visit other campuses.

In this section, we would like to introduce our considerations and solutions to these three issues.

3.1 Coexistence and Communication of IPv6 Networks with IPv4 Internet

The coexistence and communication of IPv6 networks with IPv4 Internet is an important challenge for all IPv6-only networks. During the design of CNGI-CERNET2, we have two special considerations on this transition issue:

- unidirectionally initiated communication

  In order to encourage the deployment of IPv6, we have to make sure that IPv6 users can access IPv4 Internet, while we do not think it is necessary to support IPv4 users to visit resources in IPv6 Internet. In other words, IPv6 hosts can always initiate connection with any IPv4 hosts, while IPv4 hosts may not be able to initiate connection with any IPv6 hosts.

- exploit IPv6 backbone for IPv4 traffic

> Since there are only a few IPv6 services and applications in current Internet, many ISPs do not want to deploy new IPv6-only backbone networks because of high cost and low utilization rate. Instead, they choose to upgrade their IPv4 networks to dual stack to enable IPv6 access service. However, there are several challenges for dual stack transition: 1) address requirement: dual stack hosts or network devices still require IPv4 addresses, which are rare resources for Chinese ISPs; 2) security and quality of service: IPv6 services closely couple with IPv4 services, *i.e.*, the fault in IPv6 networks would affect the operation of IPv4 networks, and potentially attackers can exploit configuration errors in IPv6 network to attack important IPv4 service; 3) IPv6 promotion: dual stack hosts usually prefer IPv4 to IPv6, therefore dual stack transition cannot help IPv6 promotion, which is an important consideration of Chinese ISPs.
>
> As a result, CNGI-CERNET2 is designed to be a new IPv6-only network. To solve the problem of low utilization rate of IPv6 networks, we deploy IPv4 over IPv6 tunnel and then we can exploit IPv6 networks to transit IPv4 traffic flows. This cannot only increase the usage of IPv6 networks under the situation of insufficient IPv6 applications, but also ease the pressure of IPv4 traffic volume on CERNET IPv4 backbone. We do not need to invest a lot of money in IPv4 network to support the increasing IPv4 customers and services. Instead, we invest in IPv6 networks and avoid the transition cost in the future.

Figure 3 illustrates the network architecture for the coexistence and communication of IPv6 with IPv4. The 4over6 tunnel, which includes 4over6 initiator and 4over6 concentrator [4], is used to transit part of IPv4 traffic flows on IPv6 backbone. Since our IPv6 backbone can provide better quality of service than IPv4, the 4over6 tunnel service is attractive for campus network users. The campus IVI translator [1] is used for the communication between IPv6 users and IPv4 users on the same campus. The backbone IVI translator is used for IPv6 users to visit IPv4 resources in other campus networks or other ISP networks. Note that the deployment of 4over6 tunnel and IVI translator requires special arrangement of IP address allocation and routing configuration.

3.2 Security Architecture and Trust-worthy Network: SAVI

In current Internet architecture, data packets are forwarded hop by hop to their destination addresses without any check of their source addresses. Therefore, it is unreliable to use IP source addresses to determine the origins of data packets. Network attackers or criminals can spoof their IP source addresses to conceal their locations, even impersonate other network users. To make sure that the source addresses of all packets are reliable for network operators to diagnose and locate failures, charge users, and prevent or trace-back malicious attacks or misbehaving hosts, *etc*, we are trying to make the CNGI-CERNET2 a trust-worthy network based on Source Address Validation Improvement (SAVI) Framework [2].

With SAVI scheme, the SAVI device monitors the control packets sent by a host to get a legitimate IP address, binds the IP address to the host (specified by a particular link layer property of the host's network attachment, *i.e.*, binding anchor), and then filters out subsequent packets inconsistent with the binding entry. Obviously the implementation of SAVI would vary with the IP address assignment method and the binding anchor.

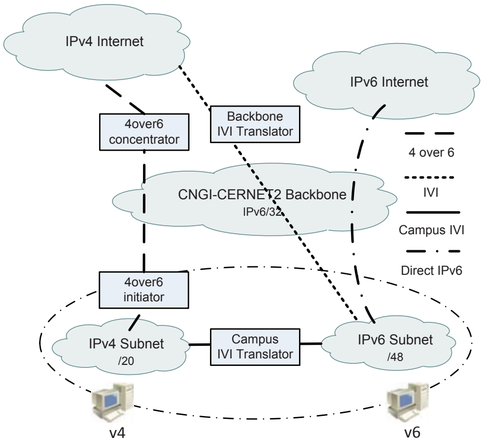

Figure 3: The Coexistence and Communication of IPv6 Users with IPv4 Users

SAVI can be deployed at any locations to achieve different granularity of validation, and it is designed to be purely network-based, *i.e.*, needs no cooperation of hosts. In CNGI-CERNET2, we choose to deploy SAVI on all access switches between hosts in IPv6 subnets and their corresponding default routers, which is the closest location to hosts. It is regarded as the most effective deployment and can provide the finest-grained source address validation – packets have to undergo IP source address validation even if they are exchanged locally on the link.

Our current SAVI implementation accommodates two legitimate IP addresses assignment methods, *i.e.*, Stateless Address Autoconfiguration and DHCP. The binding anchor is determined as the host's MAC address together with the port of the Ethernet switch to which the IPv6 host attaches.

Currently we are still working to improve the source address validation solution for the scenario where some access switches cannot be upgraded to enable SAVI function easily. The basic idea of the solution is as follows. We first analyze the network topology to determine necessary check points. The devices on these check points are called as key devices. Then we collect information of address prefix configurations of these devices. Based on these information, we can derive and configure filter rules on these devices automatically for network operators. We refer this solution as Intra-AS SAV [3].

Apparently, how to determine check points is the most important part in this framework. The selection of check points must satisfy following requirements: 1) a packet with a source address of SAVI-enabled subnets is trustworthy, which means computers in SAVI-disabled subnets cannot spoof SAVI-enabled subnet addresses; 2) a packet with a source address of SAVI-enabled subnets can be reliably traced back to its corresponding *host*, which is the responsibility of SAVI-enabled access switches; 3) a packet with a source address of SAVI-disabled subnets can be reliably traced back

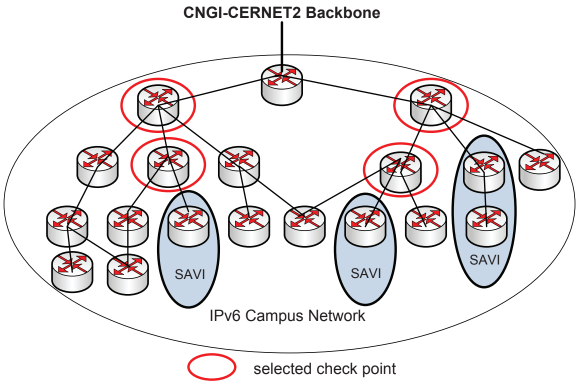

Figure 4: An Example of SAVA Deployment

to its corresponding *subnet*. Figure 4 shows an example of SAVA deployment.

3.3 Charging and Cross-domain Roaming Access

How to improve user mobility is an important concern of next generation Internet. In the current stage, CNGI-CERNET2 does not plan to propose and deploy any revolutionary architecture to improve mobility. Instead, we are trying to provide as much as possible mobility based on currently available technologies and architecture.

In CNGI-CERNET2, each campus network needs to pay CERNET2 backbone for its traffic flows. At the same time, each campus network can determine its own charging policies and collect money from its network users. Therefore, most campus networks assign passports to their legitimate users, and deploy accounting gateways at the exit points of their networks to CNGI-CERNET2 backbone. The gateways only allow packets from legitimate users to traverse and they also log the traffic volume of each user for charging.

We develop and deploy SAVI module and access control module on all IPv6 access switches. Figure 5 shows the procedure of an IPv6 user getting Internet access service. The user first contacts with DHCP server and gets a legitimate IPv6 address. The SAVI module in the access switch monitors this connection, binds the IP address with the related switch port and the host's MAC. This is to ensure that all packets from this switch are with authentic source addresses. Then the access control module asks the user to provide its passport ID and password, which is further sent to the authentication server for authentication. If the information is correct, the switch would allow the host to access this campus network. At the same time, the authenticated user information is sent to the accounting gateway. The gateway binds the user ID with its IP address, allows the users' packets to traverse, and sends its aggregated traffic information to the accounting server for charging.

This authentication and charging architecture greatly restricts users' mobility, *i.e.*, users from one campus cannot access Internet when they visit other campuses due to the lack of cross-domain authentication and charging. Here, we cannot simply distribute CERNET ID to replace campus ID to solve the issue – we have to respect the decision of the home campus network on whether a user is allowed to roam to a destination campus, because campus-campus settlement or campus-backbone settlement is preferred to the scheme that the destination campus network collects money directly from the roaming users.

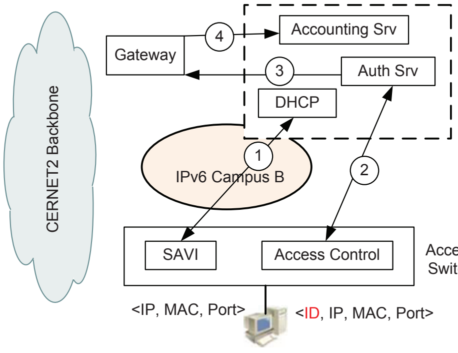

Figure 5: IPv6 Access Service: Authentication and Charging

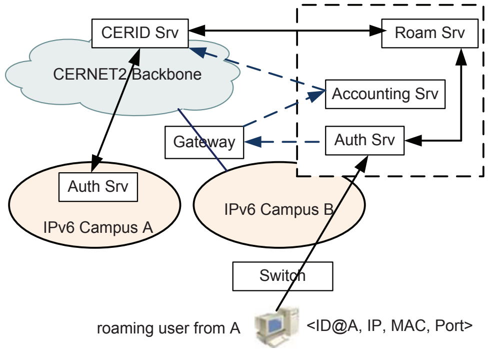

Figure 6: IPv6 Cross-Domain Roaming Service

Figure 6 illustrates the procedure of cross-domain roaming service. When a user roams from its home campus A to a destination campus B, same as B's local users, it first sends an authentication request to B's authentication server. The authentication server realizes it is a roaming user, and then sends a roaming authentication request to B's roaming server. The roaming server would ask CERNET-ID server to forward authentication request to A's authentication system. To reduce the latency of this authentication procedure, the CERNET-ID server can cache, even pull, authentication information from A's authentication system.

After B's authentication server confirms that the roaming user is authenticated successfully, B starts to treat the roaming user in the same way as local users, *i.e.*, notifying the gateway, collecting traffic information for accounting *etc.* B's accounting sever reports roaming transaction fees periodically to the CERNET-ID server and gets reimbursement from CNGI-CERNET2 backbone. We can see that CERNET-ID server is responsible to control roaming access, authenticate and log the behavior of roaming users, and help accomplish settlement between the home campus and destination campus.

4. CONCLUSION

CERNET is enthusiastic on deploying IPv6 to solve the imminent problem of IPv4 address exhaustion for Chinese

ISPs. In this article, we introduced the CNGI programme, presented the architecture of CNGI-CERNET2 and described some concerns during its deployment and management, *i.e.*, transition, security improvement, charging and roaming service. We are still working on all kinds of challenges in the widely deployment of commercial IPv6 networks. We sincerely invite all researchers who are interested in this area to collaborate with us.

5. REFERENCES

[1] Xing Li, Congxiao Bao, Maoke Chen, Hong Zhang, and Jianping Wu. The cernet ivi translation design and deployment for the ipv4/ipv6 coexistence and transition. http://tools.ietf.org/html/draft-xli-behave-ivi-07.

[2] Jianping Wu, Jun Bi, Marcelo Bagnulo, Fred Baker, and Christian Vogt. Source address validation improvement framework. http://tools.ietf.org/html/draft-ietf-savi-framework-01.

[3] Jianping Wu, Jun Bi, Xing Li, , Gang Ren, Ke Xu, and Mark I. Williams. A source address validation architecture (sava) testbed and deployment experience. http://www.rfc-editor.org/rfc/rfc5210.txt.

[4] Jianping Wu, Yong Cui, Xing Li, Mingwei Xu, and Chris Metz. 4over6 transit solution using ip encapsulation and mp-bgp extensions. http://www.rfc-editor.org/rfc/rfc5747.txt.