Z. Hou (Ed.)

doi:10.3233/ATDE231216

IPv4 to IPv6 Transition Strategy Based on Dual Stack Protocol

Yanan ZHANG[a], Yanfang FU[a], Qian WANG[a,1]
[a] *Beijing Fibrlink Communications Co., LTD., Beijing, 100071, China*

Abstract. To consider the different environments of the network and select the appropriate transition mechanism, this paper studies the Intranet IPv6 network integration and transition platform based on campus network. We focus on the service migration of IPv4/IPv6, and propose the design idea of network integrated service architecture. Then, from the engineering point of view, a scheme for dual protocol to find the logical layer independent and the physical layer shared is put forward, and a network service topology that supports IPv4/IPv6 user access is also proposed. In the actual deployment process, the dynamic routing, address resolution, network connectivity, are configured accordingly, and the specific scheme is tested. The experimental results show that the scheme can realize the safe and fast access of IPv4/IPv6 network resources for Intranet users, and achieve the interconnection between IPv4 and IPv6 networks.

Keywords. IPv6; Intranet; dual stack protocol; transition strategy; MSTP

1. Introduction

With the expansion of network scale and application scale, the limitations and shortcomings of the original IPv4 technology are exposed. First, the limitations of IPv4 address space can no longer meet the growing demand for address resources; Secondly, the performance of IPv4 is inadequate compared with the current huge network; At the same time, the inherent security problems of IPv4 exacerbate the urgency of the network's transition to the next generation of network protocols known as v6. To implement the known v6 network in the intranet, we must make full use of the existing network environment. To avoid excessive investment waste. In a short period of time, it is impossible to establish all network resources on known v6. Therefore, IPv6 network will coexist with IP v4 network for a long time. How to realize the smooth transition from IP v4 to IPv6 in the intranet is an important problem [1,2].

This paper mainly studies the problems of network interconnection, network service migration and network security in the IPv4/IPv6 transition phase, and puts forward the overall scheme of Intranet IPv6 network integration transition platform. First, the transition principle from IPv4 to V6 is discussed in depth according to the requirement analysis. Then, an improved IPv6 network transition strategy based on dual stack protocol is proposed, which divides each subsystem into modules, and links the decomposed modules according to the hierarchical structure through the module structure diagram. In the design process of each module, fully consider the relationship between network planning and address configuration, and expand the idea of IPv6 network construction and management. Finally, the overall test of the scheme is performed through the combination of actual test and simulation analysis, and the

[1] Corresponding Author: Qian Wang; Beijing Fibrlink Communications Co., LTD., Beijing, 100071, China; linxsg2022@163.com

results show that the transition strategy fully meets the communication requirements of intranet, laying a foundation for the physical environment for the comprehensive development of IPv6 in the future.

2. Intranet IPv6 Transition Technology

2.1 Principles of Network Design in The Transition Period

The design of network scheme in the transition period must face up to the above challenges, and the design process should follow the following principles [3]:

(1) Adopt the strategy of point to area and smooth upgrade. IPv6 address allocation follows the "clustering" principle, which reduces the length of routing table in the router, and improves the speed of forwarding packets in the router, which improves the overall throughput of the network. First, establish a small-scale IPv6 network to demonstrate the advantages of the new protocol, and then gradually expand its coverage.

(2) The seamless integration of IPv6 and IPv4 protocol stacks must be guaranteed. The use of dual stack enables the host or network device to support both IPv4 and IPv6 dual protocol stacks; Alternatively, IPv6 packets can be encapsulated in IPv4 packets through tunnel technology to achieve flexible network resource sharing.

(3) We should provide full play to the dominant role of enterprises in the development of IPv6, and stimulate market demand and the endogenous power of enterprise development and promote IPv6 integration and innovative application intensively.

2.2 Double Stack Mechanism

The most direct way to realize the interworking between IPv6 nodes and IPv4 nodes is to add IPv4 protocol stack to IPv6 nodes. The dual stack protocol structure is shown in figure 1. Nodes with dual protocol stacks are "IPv4/v4 nodes". These nodes can send and receive IPv4 packets as well as IPv6 packets. They can use IPv4 to interoperate with IPv4 nodes, or they can directly use IPv6 to interoperate with IPv6 nodes. For most nodes, especially if their Internet applications are upgraded to support both IPv4 and IPv6 protocols, the nodes can interoperate with any IPv4 node or IPv6 node. At the initial stage of IPv6 network construction, the dual protocol stack technology has solved the communication between IPv4 and IPv6 simply and intuitively, and has certain feasibility [4].

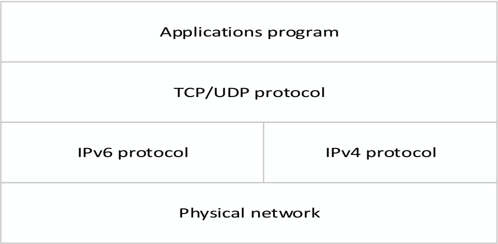


Figure 1. Basic principle and process of collaborative filtering

The advantage of dual protocol stack technology is good interoperability and easy to understand, but it needs to configure IPv4 addresses for each node at the same time, which cannot solve the problem of IPv4 address shortage. When the scale of IPv6 network develops to a certain stage, it is unrealistic to assign IPv4 and IPv6 global addresses to each node. For this reason, there is also a limited dual protocol stack model. In this case, the server and router are still dual protocol stacks, but non server hosts only need to support IPv6. It can save more IPv4 addresses, but to realize the communication between pure IPv6 and pure IPv4, it needs to combine other technologies, such as protocol conversion technology.

3. An Improved IPv6 Network Transition Strategy Based on Double Stack Protocol

3.1 Overall Design Scheme

When designing enterprise campus network, scalability is a main goal Hierarchical network design model is widely used in today's enterprise campus network design model,. A large and complex system is decomposed into several unidirectional dependency layers, that is, each layer provides a set of functions and these functions only depend on each layer within the layer. The most classic model used is the three-layer model - the core layer, the convergence layer and the access layer. Layer 3 switches based on IP addresses and protocols are commonly used in the core layer of the network, but also in the aggregation layer. Some Layer 3 switches also have Layer 4 switching functions, which can judge the target port according to the protocol port information of the data frame. As shown in figure 2, network equipment and corresponding links between equipment at the aggregation layer and core layer are redundant to meet the availability requirements of the network and reduce the possibility of single point failure on the network. The existing network hierarchy is used to divide the network into regions, so that the mobile nodes can be divided into intra domain mobile and inter domain mobile Enterprises must apply for legal public network IPv4 address exports and IPv6 global unicast address exports. In this design scheme, IPv4 and IPv6 dual exports are used to access the Intranet.

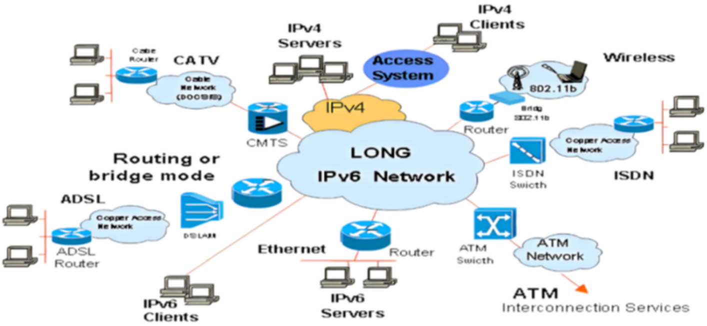


Figure 2. Scalable redundant network hierarchy of Intranet.

3.2 Network Address Planning

Priority shall be given to the original planning or use after optimization. When each service node provides services to users, the data download speed is different, and the actual bandwidth consumption of service nodes configured with the same number of IP addresses may be different [5]. In addition to meeting the requirements, each user's network segment address has a margin for standby expansion address and the address segments assigned by CERNET2 to a school are shown in table 1. Based on the above principles and the actual situation of network deployment, the total number of available addresses and the number of users connected to the node should be fully considered for allocation. In principle, in addition to meeting the requirements, the network segment addresses of each user shall retain certain reserved expansion addresses.

Table 1. IPv6 address planning table of certain school

Access department	IPv4 address	IPv6 address
Office buildings	172.16.1.0/24	2001:240:4e01:0::/64
Student activity center	172.16.2.0/24	2001:240:4e02:0::/64
Dining room	172.16.3.0/24	2001:240:4e03:0::/64
Library	172.16.4.0/24	2001:240:4e04:0::/64
Teaching building	172.16.5.0/24	2001:240:4e05:0::/64
Dormitory A	172.16.6.0/24	2001:240:4e06:0::/64
Dormitory B	172.16.7.0/24	2001:240:4e07:0::/64
Dormitory C	172.16.8.0/24	2001:240:4e08:0::/64
Network center	172.16.9.0/24	2001:240:4e09:0::/64
…	…	…

3.3 Security Policy

Aiming at the possible external attacks and security vulnerabilities in the transition process of the Intranet IPv6 network, the idea of Intranet IPv6 security architecture is proposed Incorporate IPv6 real source address verification scheme into the security system. IPv6 also defines a variety of extended headers, which makes IPv6 extremely flexible and can provide strong support for a variety of applications, while providing the possibility to support new applications in the future. These headers are placed between the IPv6 header and the upper layer header, which makes IPv6 extremely flexible and can provide strong support for multiple applications [6]. At the same time, it makes it possible to support new applications in the future. A complete IPv6 implementation includes the implementation of the following extended headers: route segment by segment option header, destination option header, routing header, segment header, identity authentication header, payload security encapsulation header, and final destination header.

The design idea of this paper is to define the packet priority header when IPv6 congestion occurs: header: 40Octets, 8fields, in order to provide special processing for specific data streams. It defines the total length of IP datagrams in addition to the basic header, and the extension that follows the IPv6 header in datagrams, including the extended header. The MD5 algorithm is used for encryption calculation to obtain 128 bit information digest. We also define a new source address verification option in the hop by hop option extension header, store the information summary as data, and send an IP packet with the source address verification option. At the remote address verification end, when receiving the data packet sent from the external network, we first extract the IP source address of the data packet, obtain the remote host ID information in the address, and look up the database to obtain the corresponding seed of the host's network. The improved IPv6 packets with source address verification information added are shown in figure 3.

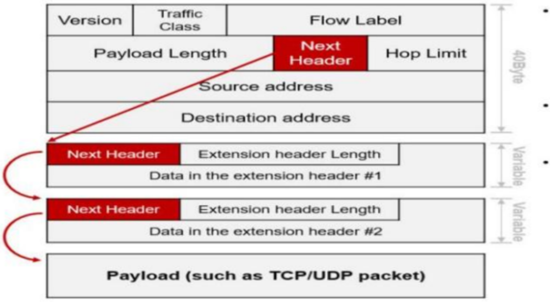


Figure 3. IPv6 packets with source address validation information addition

The extension header is behind the IPv6 header and is a sequence table of optional fields. The typical format of an extended header is an 8-bit optional type (the number of the next extended header included in the list), an 8-bit unsigned integer option data length (indicating the length of the header), and an option data payload (variable size length). Extension headers can be used in combination, and several of them appear in a single packet, but typically only some of them can be used in combination. This is easier because the destination address and hop by hop header appear earlier in the packet. The firewall needs to complete all the functions of a router and analyze the protocol information from the extension header to the upper layer. This increases the complexity of filtering policies and increases the burden of firewalls. The firewall is to determine whether packets should be allowed to pass or discarded. Since the terminal node receiving an IPv6 packet must completely analyze the entire header set and process it, the node has to do the hardest work.

4. Case Analysis

4.1 Network Configure

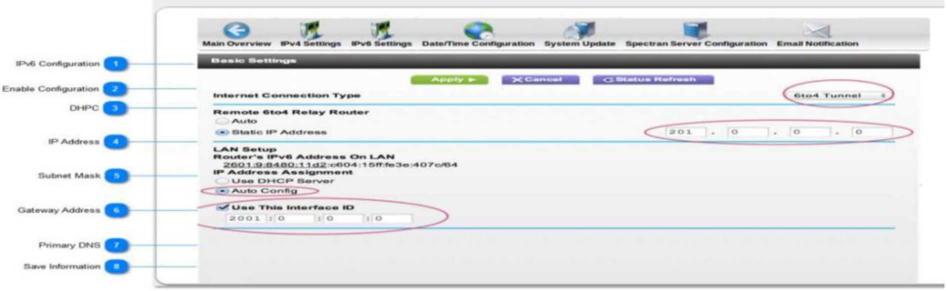
Enable IPV6 on the interface, configure the IPV6 address of the interface, and the IPV6 configuration instructions of the exchange routing device.

```
//Enable global IPv6 on the device
ipv6 enable
……
// Dual stack configuration on the virtual interface of the switch
……
interface FastEthernet1/0 ip address 12.1.1.1 255.255.255.0 ipv6 address
2000:12::1/64
dhcp select relay
dhcp relay server-select 4
ipv6 dhcp relay server-address
2001:250:2C01:30::57
```

```
…
//router configure
ipv6 route-static :: 0 FEC0:10::10:1 preference 1
ipv6 route-static 2001:250:2C01:: 52
FEC0:10::30:2
…
ipv6 route-static FEC0:10::10:4 126 FEC0:10::20:2
……
```

4.2 Management Platform Design

The AFTR address, domain name. draft IETF Softwire Dslite Radius ext-02 issued through the Radius extended attribute has become a working group document The initiator PC obtains IPv4/IPv6 IP and transparently transmits all applications Layer 3 routing is mainly performed on the service control layer equipment and MAN exit equipment. For CR and service control layer equipment BRAS/SR, it is recommended to enable dual stack, so as to enable the corresponding IPv6 based routing process as required When the user conducts IPv6 communication, the data message can be transmitted to the user through SSL VPN tunnel to complete IPv6 communication. During the test, the current system network parameter configuration is captured as shown in figure 4.



Basic Settings

Internet Connection Type: 6to4 Tunnel

Remote 6to4 Relay Router
○ Auto
● Static IP Address 201 . 0 . 0 . 0

LAN Setup
Router's IPv6 Address On LAN
2601:9:8480:11d2:c604:15ff:fe3e:407c/64
IP Address Assignment
○ Use DHCP Server
● Auto Config

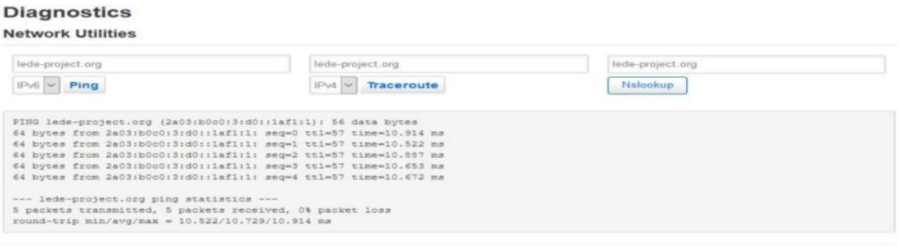
☑ Use This Interface ID
2001 : 0 : 0 : 0

Figure 4. Configuration of main network parameters of the system

Remote access equipment can be easily integrated with the existing campus network system to achieve unified identity authentication and user management, and can support the establishment of adjacency between dual stack routers and IPv4 routers.

4.3 Function Tests

The configuration complexity, connectivity and quality of service of these transition technologies are tested. By compared and analyzed, it is verified whether IPv4/IPv6 and necessary network parameters are obtained through ipconfig command line, as shown in figure 5. The connection test of the ipv6 in the vm is normal. We can ping the IPv6 address of the VM locally. The connection test of the mobile phone IPv6 is normal. In order to test the connectivity of the external network, the network outside the intranet has been tested. It can be pinged, and the SSH protocol has no pressure.

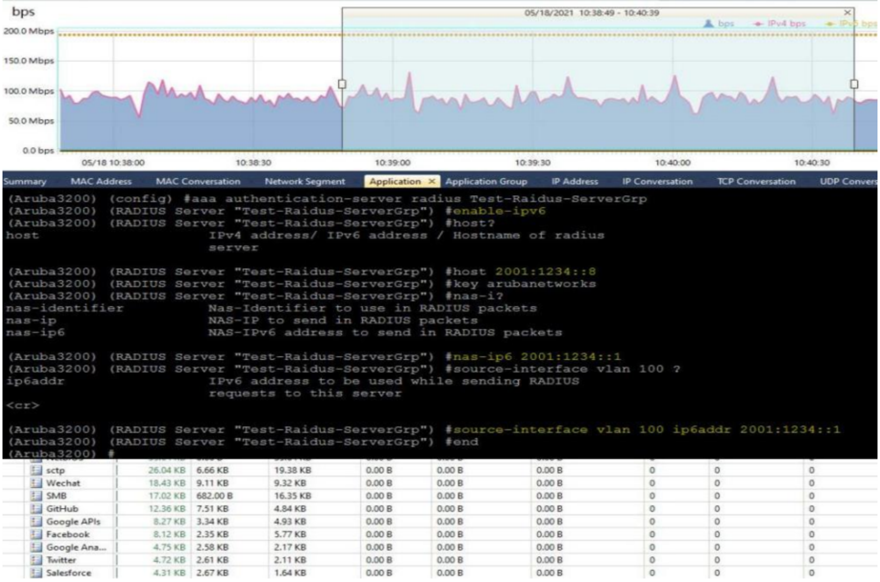


```
PING lede-project.org (2a03:b0c0:3:d0::1af1:1): 56 data bytes
64 bytes from 2a03:b0c0:3:d0::1af1:1: seq=0 ttl=57 time=10.914 ms
64 bytes from 2a03:b0c0:3:d0::1af1:1: seq=1 ttl=57 time=10.522 ms
64 bytes from 2a03:b0c0:3:d0::1af1:1: seq=2 ttl=57 time=10.887 ms
64 bytes from 2a03:b0c0:3:d0::1af1:1: seq=3 ttl=57 time=10.653 ms
64 bytes from 2a03:b0c0:3:d0::1af1:1: seq=4 ttl=57 time=10.672 ms

--- lede-project.org ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 10.522/10.729/10.914 ms
```

Figure 5. Host address connectivity test results

To verify whether the operation of the convergence layer and access layer switches running MSTP can achieve the purpose of load balancing and backup as specified in the command configuration, an industrial application verification environment for MSTP based single stack IPv6 IoT access is established, and the backbone section relies on the backbone SDH network for transmission. It can be seen from figure 6 that MSTP can block redundant links in the Layer 2 network, which prune the network into a tree, and eliminate loops. SwitchA, SwitchB, SwitchC, and SwitchD all run MSTP, only losing 1-2 packets. Under normal conditions, MSTP can makes full use of the link of the switch to realize the load sharing of data flow forwarding. When MSTP detects a port failure, it can quickly enable the backup line, so that the user's business can continue to operate normally without being affected.



```
(Aruba3200) (config) #aaa authentication-server radius Test-Raidus-ServerGrp
(Aruba3200) (RADIUS Server "Test-Raidus-ServerGrp") #enable-ipv6
(Aruba3200) (RADIUS Server "Test-Raidus-ServerGrp") #host?
host                       IPv4 address/ IPv6 address / Hostname of radius
                           server

(Aruba3200) (RADIUS Server "Test-Raidus-ServerGrp") #host 2001:1234::8
(Aruba3200) (RADIUS Server "Test-Raidus-ServerGrp") #key arubanetworks
(Aruba3200) (RADIUS Server "Test-Raidus-ServerGrp") #nas-i?
nas-identifier             Nas-Identifier to use in RADIUS packets
nas-ip                     NAS-IP to send in RADIUS packets
nas-ip6                    NAS-IPv6 address to send in RADIUS packets

(Aruba3200) (RADIUS Server "Test-Raidus-ServerGrp") #nas-ip6 2001:1234::1
(Aruba3200) (RADIUS Server "Test-Raidus-ServerGrp") #source-interface vlan 100 ?
ip6addr                    IPv6 address to be used while sending RADIUS
                           requests to this server
<cr>

(Aruba3200) (RADIUS Server "Test-Raidus-ServerGrp") #source-interface vlan 100 ip6addr 2001:1234::1
(Aruba3200) (RADIUS Server "Test-Raidus-ServerGrp") #end
(Aruba3200) #
```

sctp	26.04 KB	6.66 KB	19.38 KB	0.00 B	0.00 B	0.00 B	0	0	0
Wechat	18.43 KB	9.11 KB	9.32 KB	0.00 B	0.00 B	0.00 B	0	0	0
SMB	17.02 KB	682.00 B	16.35 KB	0.00 B	0.00 B	0.00 B	0	0	0
GitHub	12.36 KB	7.51 KB	4.84 KB	0.00 B	0.00 B	0.00 B	0	0	0
Google APIs	8.27 KB	3.34 KB	4.93 KB	0.00 B	0.00 B	0.00 B	0	0	0
Facebook	8.12 KB	2.35 KB	5.77 KB	0.00 B	0.00 B	0.00 B	0	0	0
Google Ana...	4.75 KB	2.58 KB	2.17 KB	0.00 B	0.00 B	0.00 B	0	0	0
Twitter	4.72 KB	2.61 KB	2.11 KB	0.00 B	0.00 B	0.00 B	0	0	0
Salesforce	4.31 KB	2.67 KB	1.64 KB	0.00 B	0.00 B	0.00 B	0	0	0

Figure 6. MSTP communication under IPv6 environment

5. Conclusion

With the rapid development of the Internet, more and more Internet resources and services are added to the IPv6 network. The enterprise network should also follow the trend, adopt security measures to prevent external intrusion, serve the enterprise's internal IPv6 network and have the function of connecting to the Internet. This paper discusses and analyzes the construction scheme of campus network in the transition period from IPv4 protocol to IPv6 protocol, adopts the transition scheme of IPv4/IPv6 dual protocol stack to implement the simulation enterprise, and simultaneously receives, sends and processes IPv4 and IPv6 data packets. Each access section adopts MSTP equipment for convergence access and builds a dual link basic transmission network. The test results show that the scheme has high scalability, high reliability and high availability, and can provide an overall scheme integrating authentication, network and security, helping the intranet to quickly realize the overall construction and operation of IPv6.

Acknowledgments

This work was supported by Beijing Fibrlink Communications Co., LTD. "Test and verification of production network IPv6 interoperability and convergence technology for typical industries", under grant no. 546826210001.

References

[1] Li Xingliang, Yang Xing. Overview of intranet IPV6 transition strategy. Gansu Science and Technology, 2008, 24(20): 33-34

[2] Arafat M Y, Ahmed F, Sobhan M A. On the Migration of a Large Scale Network from IPv4 to IPv6 Environment. International Journal of Computer Networks & Communications, 2014, 6(2):111-126

[3] Levin S L, Schmidt S. IPv4 to IPv6: Challenges, solutions, and lessons. Telecommunications Policy, 2014, 38(11):1059-1068

[4] Zhang Le, Xia Xin, Chen Meng. Overview of IPv4 to IPv6 Transition Strategy. Research Science and Technology Plaza,008, 12:94-95

[5] Miyakawa S. IPv4 to IPv6 Transformation Schemes. IEICE Transactions on Communications, 2010, 93 (5):1078-1084

[6] Hemalatha M, Rukmanidevi S. RETRACTED ARTICLE: Real time prefix matching based IP lookup and update mechanism for efficient routing in networks. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(3):3669-3678