IOP Conf. Series: Materials Science and Engineering **322** (2018) 072005 doi:10.1088/1757-899X/322/7/072005

AS Migration and Optimization of the Power Integrated Data Network

Junjie Zhou [1,2], Yue Ke [1*]

[1]School of Computer, Hubei University of Technology, Wuhan, China
[2]Department of Computer,Wenhua College, Wuhan, China

*Corresponding author e-mail: zjj0718@126.com

Abstract. In the transformation process of data integration network, the impact on the business has always been the most important reference factor to measure the quality of network transformation. With the importance of the data network carrying business, we must put forward specific design proposals during the transformation, and conduct a large number of demonstration and practice to ensure that the transformation program meets the requirements of the enterprise data network. This paper mainly demonstrates the scheme of over-migrating point-to-point access equipment in the reconstruction project of power data comprehensive network to migrate the BGP autonomous domain to the specified domain defined in the industrial standard, and to smooth the intranet OSPF protocol Migration into ISIS agreement. Through the optimization design, eventually making electric power data network performance was improved on traffic forwarding, traffic forwarding path optimized, extensibility, get larger, lower risk of potential loop, the network stability was improved, and operational cost savings, etc.

1. Introduction

The migration of AS network integrated power company is the network topology transfer from one domain to another state grid provided in another domain of the project, the project is mainly to the network protocol when migration and migration of BGP AS to ensure the normal operation of the data network. Its characteristic is that the network topology scale is huge in this network, and the service is complex. With the development of computer networks, more and more networks are moving from small networks to large enterprise networks or even wide area networks.

At this stage most of the domestic IGP networks stay at the OSPF level, and most enterprises have not tried to smoothly migrate the OSPF protocol to the ISIS protocol. Therefore, this phenomenon will last for a long time. The comprehensive transformation of the power system data network, from the previous research assessment, the implementation of the project and the results of the transformation point of view, after AS migration and optimization of the upgraded network access to the national grid smoothly, in line with user expectations. So it can give reference for the future power grid IGP smooth migration from OSPF to ISIS[1], as well as to modify BGP AS number.

2. The Key of Technologies

BGP: External Gateway Protocol[2]. Different AS can connect and exchange routes. However, the ability to calculate routes is relatively poor, which is mainly used to deliver routes and manage routes.

MPLS VPN：A routing protocol based on label switching, early to solve the problem of poor performance of routing switching, and later gradually become a VPN technology to achieve business isolation in large-scale networks, mainly based on routing information to form a label switching table.

OSPF: OSPF is a typical routing protocol based on link state[3]. It belongs to the Interior Gateway Protocol (IGP) and is used in the same routing domain and runs inside the autonomous system.

ISIS: A relatively simple and powerful routing protocol[4]. This protocol has no complicated network type nor rich area division, only has the backbone area and the non-backbone area. Therefore, with its simple and performance advantages of low consumption make it one of the most excellent agreement with in the network protocol.

Because ISIS is a hierarchical link state routing protocol based on the DEC net Phase V routing algorithm[5], the modular design of TLV valve thresholds provides strong scalability for ISIS protocol extensions.

In theory, ISIS has optimized Dijkstra's algorithm[6], so ISIS has a more flexible application scenario than OSPF in a large-scale network. ISIS belongs to the second layer of the agreement, and OSPF belongs to the third floor, so the use of ISIS in the network protocol to reduce the transmission and decapsulation of a data package, so the processing of data relative to OSPF will be less, the efficiency of forwarding Will be higher. In addition ISIS increased support for IPv6 better, in line with the tide of network development.

3. Migration and optimization of AS

Due to the limited size of early networks, the division of AS has not been refined to accommodate a diverse network. As a result, the AS in some large networks need to be re-planned. However, the range of networks involved in the AS is too large. Most enterprises are reluctant to re-plan the AS, considering the importance of the services carried on the network. This article analyzes a successful case of modifying an AS.

3.1. The problems of power network

Taking the entire power network in Beijing as an example, the underlying routing protocol of the power integrated data network is OSPF. By dividing the OSPF area into the service division of the entire network, the routing protocol alone can not achieve the isolation of different services. Therefore, MPLS is introduced to distribute labels, and BGP delivers private network routes to form MPLS VPN[7]. As a routing protocol that bears VPN in the network, BGP delivers all VPN route entries directly to other PE(MPLS network edge routers). The OSPF protocol uses a multi-area design approach. The interconnection ports between the core devices belong to area 0, and the ports of the downstream aggregation devices belong to other non-backbone areas. The core devices also serve as OSPF ABR border routers.

As the power network uses OSPF as the internal gateway protocol, the core backbone network operates in area 0. According to the different business and location, the entire network is divided into different OSPF areas. The core backbone equipment serves as the gateway in this area. All the equipment enable MPLS VPN and BGP technology. MPLS VPN is responsible for the generation and forwarding of labels. BGP is responsible for the delivery of service routes. Logical switching is used to implement the logic division of different services so that the traffic between different services will not interfere with each other and the three-dimensional design of service traffic is realized. In a large-scale network, the complexity of the network structure, service traffic, area and OSPF protocol itself leads to complicated network structure and too many layers. The core network equipment has too many roles (gateway, ABR, route forwarding)Network bottleneck. Due to the DV algorithm used in the inter-OSPF area[8], with the further increase of the network complexity, the increased risk of the loop and the future expansion of the network all pose a huge operational risk to the integrated data network of the power.

3.2. The migration method of AS

The main idea of the migration is to adopt an over-mobility solution of the access equipment of the tangent plane. The access equipment is firstly divided into new domains and then used as a bridge to

IOP Conf. Series: Materials Science and Engineering **322** (2018) 072005 doi:10.1088/1757-899X/322/7/072005

gradually expand the scope and eventually reach the AS migration. In the internal network protocol migration, firstly, increase the AS value of OSPF, then enable ISIS on the device. After ISIS replaces OSPF, decrease the AS value of ISIS. After the ISIS finally takes effect, you can delete the OSPF protocol to achieve the migration of intranet protocol.

The overall design concept is as follows: First, configure ISIS on the entire network. Because the default management distance of ISIS is higher than that of OSPF, you can enable ISIS directly when the device runs, and then delete the OSPF protocol. In this case, the protocol does not take effect. Then two high performance routers are used as the Route Reflector of new AS[9].

Secondly, a OSPF area of the whole network is selected to complete the Loop-back change, BGP number change and IGP protocol change in the area. The AS is connected to the rest of the network area of the integrated data network through a word-shaped topology and is opened up using cross-domain technologies at both the IPV4 and VPN levels. At the IP level, the devices within the AS are interconnected through the ISIS protocol. To communicate outside the AS, it is done through EBGP cross-domain[10]. On the VPN level, the VPN routing reflection is performed between the devices within the AS through the new RR. If you need to communicate to outside of the AS, you can do it through option-B cross domain means[11]. In the process of transformation, the topological connection between the AS and the rest of the network area of the integrated data network does not need to be interrupted or dismantled.

Finally, the method of "gradual enlargement" is adopted to expand the scope of the area horizontally with the core nodes as the core. Each subsequent renovation will be modestly expanded on the basis of the original area until the changed area is expanded to the whole network. In this case, all the BGP numbers and IGP protocols in the entire network have been changed. The whole network RR also naturally migrate to the new RR.

3.3. Implementation steps of migration

The whole network is configured with ISIS protocol, and the management distance is the default value. In this case, the OSPF management distance is lower and the new IS-IS configuration does not take effect. Newly deployed Shunyi Company 2 in Shunyi District As the second core of Shunyi Company, two independent RRs were newly deployed and connected with Shunyi Company 1 and Shunyi Company 2 respectively.

The port, IGP, BGP configuration of the above three devices, in which the IGP protocol is configured as ISIS, BGP AS number is configured as 57580. Since independent RR is only used as routing control unit and is not used as data forwarding unit, the IGP metric between RR and PE should be increased.

Between RR1 and Shunyi Company 1, RR2 establishes an EBGP neighbor relationship with Tongzhou Company to make the four ASBRs form a word-shaped connection and provides structural support for the OPTION-B cross-domain as shown in figure 1.

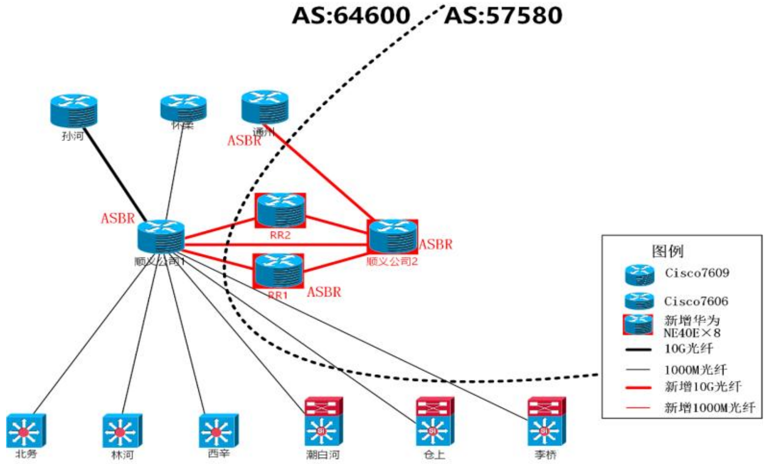

Figure 1. Mouth type graph.

In the remodeling window, all PE devices in Area (Area 22) governed by Shunyi Company are sequentially changed into AS 57580. Change the administrative distance of the ISIS agreement to 25 during the transformation to put it into effect. After ensuring that all the PE equipment in Area (Area 22) under Shunyi's operation is completely rebuilt, establish the EBGP neighbor relationship between Shunyi Company 1 and Sunhe to ensure that the word-type connection between the two ASs still exists.

Follow the above steps to repeat, with the backbone equipment as the core along the backbone of the link and gradually cut other areas of OSPF to AS 57580, until expanded to the entire network. In each implementation, the OSPF backbone device is modified first, and then the devices in the OSPF non-backbone area corresponding to the device are changed. After the whole network is changed to AS 57580, the RR2 on which Shunyi is located will be rerouted to the new RR at the front door.

First of all, in the current network equipment R3, add R4 as transfer after RR. R1 is used as the auxiliary cutting equipment and will be removed after the completion. Since the research is focused on the impact of the business on the cutover process, we directly discuss the topology after the R2--R10 cross-domain cutover is completed as shown in figure 2.

Then, after the completion of the topological transformation, the region is divided into the BGP AS2 area. In order to ensure that the service data is not interrupted during the cutover, the two main lines are cut using R5 - R1 and R2 - R1. The idea is: R1 and R2 use cross-domain technology, and R2 and R1 use Option-B cross-domain technology for redundancy to prevent single point of failure. All ISIS configurations are configured to the core. Because the IS value of IS-IS is greater than the AD value of OSPF, IS-IS does not take effect when OSPF co-exists with IS-IS. In this case, the entire network still runs under OSPF.

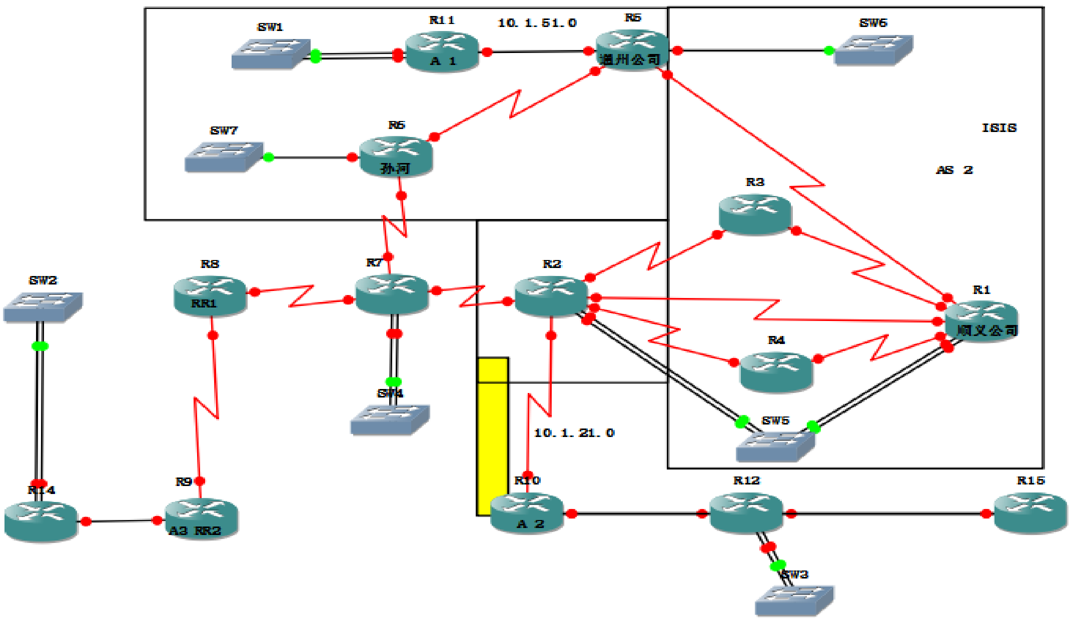

Figure 2. AS migration.

Finally, the main structure of the network is as follows: The IP address is configured on the network interface, ISIS and MPLS are enabled, and the ISIS calculation route and MPLS label distribution are implemented. Each device needs to be configured with a unique ISIS NET-ID, which, once repeated, can cause the entire network to fail. To save the number of configuration commands, you can use the BGP group command[12] to configure [instead of using one by one configuration. In the configuration process should pay attention to the RR, as well as sending and receiving community attributes and other matters.

3.4. The testing of Cut-over
This paper mainly tests the window service and recovery time. First, the business of testing non-secant Windows. As shown in figure 3 below, the business traffic of the non-secant window is normal.

```
R14#ping vrf 1 172.16.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.6.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 216/276/380 ms
```

Figure 3. the business of testing non-secant windows.

Second, it is the business of testing the window. When you upgrade R12, determine its impact on other node businesses. You can test it by long ping, and you can see from figure 4 that there is no drop after the upgrade completing. Therefore, it indicates that the upgrade process does not affect the business of non-cutover nodes.

```
R14#ping vrf 1 172.16.6.6 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 172.16.6.6, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Figure 4. the business of testing the window.

Finally, the test was cut-over the equipment after the completion of a cut-over its business recovery time: in the cut-over at the same time open two login window, upgrade the modification window, another window test business, the following figure 5 below.

```
R12#ping vrf 1 172.16.6.6 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 172.16.6.6, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
*Mar  1 00:07:42.431: %BGP-5-ADJCHANGE: neighbor 8.8.8.8 Down BGP protocol initialization
*Mar  1 00:07:42.431: %BGP-5-ADJCHANGE: neighbor 9.9.9.9 Down BGP protocol initialization.
..
*Mar  1 00:08:02.803: %BGP-5-ADJCHANGE: neighbor 3.3.3.3 Up .....
*Mar  1 00:08:11.059: %BGP-5-ADJCHANGE: neighbor 4.4.4.4 Up .!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Figure 5. the business recovery time of testing.

The following topology diagram is shown in figure 6. The cut-over is completed and the topology structure is as follows: at this point, the R8, and R9 has lost the function of the RR, RR has a smooth migration to the R3 and R4, at the same time IGP has changed to ISIS, BGP has also changed to 2. The transformation completed successfully.

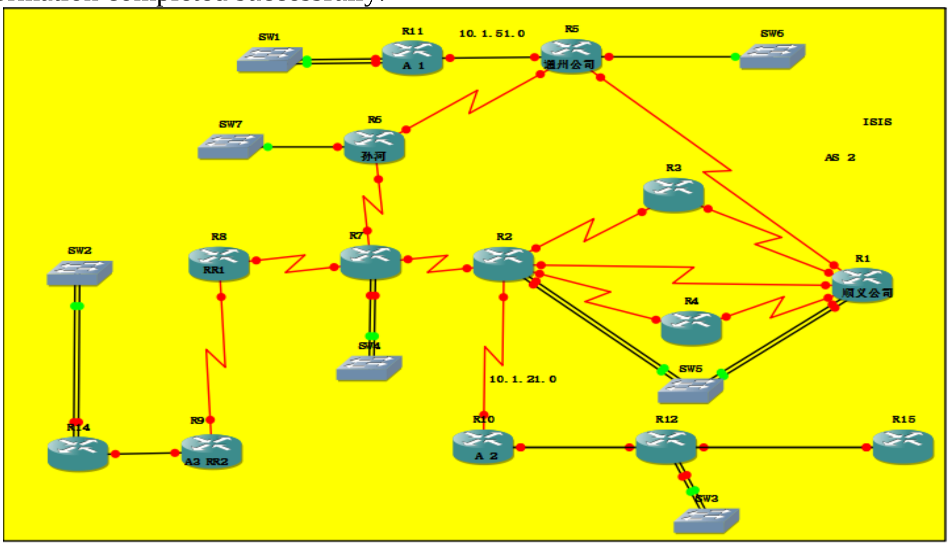

Figure 6. cut-over completed.

4. Conclusion
In the transformation of the Beijing electric power data network, through continuous exploration and practice, the network structure of electric power integrated data network is optimized, the network performance is improved to forward, effectively strengthen the robustness of the network and the

operation and maintenance costs are obtained Lower, and ultimately to achieve the user's requirements. The AS migration of large networks and the migration of Intranet protocols will almost cover the entire network, so the reasonable implementation scheme is very important for the success of migration. This paper analyzes the successful implementation of AS and Intranet protocols in the power system and ensures the normal operation of business data during the migration process.

Acknowledgments
This work was financially supported by the following fund projects:：2017 CERNET next generation of Internet technology innovation project（No.NGII20170307）； 2016 Hubei Province outstanding young and middle-aged science and technology innovation team planning project（No.T201633）； 2016 Qilin Education Research Institute Education and Teaching Research Project（No.2016-3-20）.

References
[1] Doyle J. OSPF and IS-IS: Choosing an IGP for Large-Scale Networks[M]. Addison-Wesley Professional, 2005.
[2] Dogan I, Bostanci E. Analysing Performances of Dynamic Routing Protocols on Various Network Topologies[J]. Journal of Advances in Computer Networks, 2016, 4(2).
[3] JDey G K, Ahmed M M, Ahmmed K T. Performance analysis and redistribution among RIPv2, EIGRP & OSPF Routing Protocol[C]// International Conference on Computer and Information Engineering. IEEE, 2016:21-24.
[4] Kaur V. Behavior Analysis of OSPF and ISIS Routing Protocol with Service Provider Network[J]. International Journal of Advanced Trends in Computer Science & Engineering, 2016.
[5] Filsfils C, Nainar N K, Pignataro C, et al. The Segment Routing Architecture[C]// IEEE Global Communications Conference. IEEE, 2015:1-6.
[6] Dijkstra's Algorithm. DIJKSTRA'S ALGORITHM[J]. Encyclopedia of Operations Research\s&\smanagement Science, 2012:273-315.
[7] Ahmed F, Butt Z U, Siddiqui U A. MPLS based VPN Implementation in a Corporate Environment[J]. Journal of Information Technology & Software Engineering, 2016, 6(5): 1-7.
[8] Patota F, Chiaraviglio L, Bella F, et al. DAFNES: A distributed algorithm for network energy saving based on stress-centrality[J]. Computer Networks, 2016, 94:263-284.
[9] Gutierrez E, Agriel D, Saenz E, et al. RRLOC: A tool for iBGP Route Reflector topology planning and experimentation[C]// Network Operations and Management Symposium. IEEE, 2014:1-4.
[10] Li Z, Jingming Y U, Qu D. Virtual Private Network Implementation Method and System Based on Traffic Engineering Tunnel: U.S. Patent Application 14/252,055[P]. 2014-4-14.
[11] Marrin D, Berbrick W. US Naval War College Global 2013 Game Report[R]. Naval War College Newport United States, 2014.
[12] Model F B R I B D. I2RS working group S. Hares Internet-Draft Huawei Intended status: Standards Track R. White Expires: October 6, 2016 LinkedIn April 4, 2016[J]. 2016.