

HUAWEI Sx700 Series Switches EIGRP Feature Replacement Technology White Paper

Issue 01
Date 2013-08-20

Copyright © Huawei Technologies Co., Ltd. 2015. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: <http://enterprise.huawei.com>

Contents

1 About This Document	1
1.1 Overview	1
1.2 Openness.....	1
1.3 Scalability	1
1.4 Others	2
2 Working Mechanism	4
2.1 Cisco EIGRP	4
2.1.1 Introduction to EIGRP	4
2.1.2 Advantages and Disadvantages of EIGRP	4
2.2 OSPF	6
2.2.1 Introduction to OSPF.....	6
2.2.2 Advantages and Disadvantages of OSPF	7
2.3 Comparison Between OSPF and EIGRP	8
3 Replacement Solution Design.....	10
3.1 Collect Live Network Information	10
3.2 Select a Replacement Solution	10
3.3 Network-Wide Replacement Solution	11
3.4 Asymptotic Replacement Solution	15
3.5 Solution Verification.....	19
4 References	20

1 About This Document

1.1 Overview

Enhanced Interior Gateway Routing Protocol (EIGRP) and Interior Gateway Routing Protocol (IGRP) are two Interior Gateway Protocols (IGPs) that are most frequently used in enterprise networks. The issue regarding which one of the protocols is more suited for enterprise networks has been discussed for a long time. However, the rapid development of the network technologies and the emergence of new applications drive users to pay more attention to openness and scalability of the IGP protocol and flexibility of business strategies. In the future-oriented enterprise networks, openness and scalability have become important indicators for selecting a protocol.

1.2 Openness

The EIGRP is a Cisco-proprietary protocol. Cisco is the protocol inventor and the only vendor that has rights to explain and modify the protocol. If users want to use the EIGRP protocol, they have to purchase the copyright from Cisco. In addition, Cisco has no obligation to inform any other vendor and users of any modification of the protocol. Open Shortest Path First (OSPF) is an open protocol, which is a standard issued by Internet Engineering Task Force (IETF). Mainstream network device vendors in the industry support the OSPF protocol, and thus interoperability and openness of this protocol can be ensured. It proves reasonable to use the EIGRP protocol before the OSPF protocol is rolled out, because other IGPs, for example, Routing Information Protocol (RIP), have many drawbacks. However, using the Cisco-proprietary EIGRP protocol as an IGP when standard and mature protocols such as OSPF and Intermediate System to Intermediate System (IS-IS) are widely used is not a good choice.

1.3 Scalability

Since the EIGRP is a Cisco-proprietary protocol, when users want to expand their networks deployed with this protocol, they have to purchase new Cisco devices. That is, if users have deployed the EIGRP protocol, they have no other choice but Cisco devices. Cloud computing technology has been widely used, and new network devices and architectures are surging. If users choose Cisco as the only vendor to provide devices for their future networks, potential security risks exist.

The network is end-to-end. In addition to routers and switches, there are other devices such as firewalls, load balancing devices, and content buffering devices, which use standard and open dynamic routing protocols such as OSPF and IS-IS. If the EIGRP protocol is used as the IGP on routers and switches, the firewalls, load balancing devices, and content buffering devices cannot interoperate with the routers and switches. As a result, end-to-end networks cannot be ensured.

1.4 Others

Multiprotocol Label Switching (MPLS) virtual private network (VPN) technology has been widely used in carrier networks and large enterprise networks. In the age of Big Data, MPLS traffic engineering (TE) technology has also been widely used in networks. The OSPF protocol that uses link state algorithms support the MLPS TE, whereas the EIGRP protocol that uses distance vector algorithms does not support the MLPS TE.






Intended Audience

This document is intended for:

- Network planning engineers
- Commissioning engineers
- Data configuration engineers
- Onsite maintenance engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows:

Symbol	Description
 DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
 CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
 NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
 NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Updates between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Issue 01 (2013-08-20)

This issue is the first official release.

2 Working Mechanism

2.1 Cisco EIGRP

2.1.1 Introduction to EIGRP

The EIGRP protocol and the earlier IGRP protocol were invented by Cisco, which are dynamic routing protocols that use distance vector algorithms. The EIGRP protocol is an enhanced version of the IGRP protocol and is a dynamic IGRP. It has some characteristics of link state routing protocols. Therefore, in some documents, the EIGRP protocol is also named "hybrid algorithm routing protocol." However, the EIGRP protocol is improved in terms of implementation. The convergence feature and operational efficiency of the EIGRP protocol have been significantly improved.

The convergence feature of the EIGRP protocol is based on the Distributed Update Algorithm (DUAL), which prevents path loops in route computation.

2.1.2 Advantages and Disadvantages of EIGRP

Advantages

The EIGRP protocol has the following advantages:

- Accurate route cost calculation and support for multiple network protocols

The EIGRP protocol inherits the advantage of the IGRP protocol, that is, hybrid vector routing metric. The protocol must consider comprehensive factors such as network bandwidth, network latency, channel usage, and channel credibility. Therefore, the EIGRP's route calculation is more accurate and can reflect the real network status. In addition, the EIGRP protocol supports multiple network protocols, such as Internet Packet Exchange (IPX) and connectionless network protocol (CLNP).

- Low bandwidth usage

The EIGRP protocol is used to send small Hello packets at intervals between routers to ensure effectiveness of packets and reachability of neighbors. Route updates are sent using incremental sending methods, that is, only changed routes are sent each time. Route upgrade packets are sent using a reliable transmission mechanism. If no confirmation message is received, the packets are sent until a confirmation message is received. The EIGRP protocol can also control EIGRP packets that have been sent, reducing the occupancy of the EIGRP packets on port bandwidth. As a result, a large number of routing packets is prevented from affecting normal data services.

- Loop-free routing and fast route convergence
Loop-free routing and route convergence speed are important indicators of route calculation. The EIGRP protocol uses the DUAL, thus preventing loops during route calculation and ensuring fast route convergence. The enables the EIGRP protocol to re-calculate the changed routes during route calculation. As for a specific route, only the router that is affected by the route gets involved in the route re-calculation.
- Message digest algorithm 5 (MD5) authentication of protocol packets
To ensure accurate route obtaining, MD5 authentication can be configured between routers that run the EIGRP protocol progress. Unauthenticated packets are discarded to ensure secure route obtaining.
- Convergence of routes with any mask length
The EIGRP protocol supports convergence of EIGRP routes with any mask length through configurations, reducing the amount of route information that needs to be transmitted and saving bandwidth.
- Support for equal cost multipath (ECMP) load balancing and unequal cost multipath (UCMP) load balancing
The EIGRP protocol supports not only ECMP load balancing but also UCMP load balancing. This protocol can send traffic on links of different costs, increasing the link resource usage efficiency. The OSPF protocol does not support this function.
However, UCMP causes a certain pressure on routers and may result in routing loops. Therefore, users are not advised to use the EIGRP protocol.
- Simple protocol configuration
When the EIGRP protocol is used to build networks, router configuration is very simple without any complicated area settings. Users do not need to adopt different configuration methods according to different types of network ports. They only need to enable the EIGRP routing progress on the router and run the network command to enable ports on the network.

Disadvantages

The EIGRP protocol has the following disadvantages:

- The EIGRP protocol has no concept of area and is not applicable to hierarchical networks. In contrast, the OSPF protocol can divide areas to plan and restrict the network scale on large-sized networks. Therefore, the EIGRP protocol is applicable to small-sized networks, which is the drawback of distance vector routing algorithms (RIP uses these algorithms). Although the EIGRP protocol can divide an autonomous system (AS), this kind of networking solution is seldom used on live networks, and the effect is not as good as that of the OSPF's area division and the OSPF + Border Gateway Protocol (BGP) solution.
- The EIGRP protocol does not support DC expansion on dial-up links. Hello packets must be sent between routers running the EIGRP protocol at intervals to maintain the peer relationship. Even if the peer relationship exists on a dial-up network, Hello packets must be sent at intervals. As a result, on dial-on-demand networks, users cannot locate whether the packets are service packets or query packets sent by the EIGRP protocol at intervals and may trigger dial-on-demand networks to connect to each other, especially on backup networks. To avoid this problem, Dialer list and Dialer group must be configured on backup dial-up ports on routers that run the EIGRP protocol to filter out unnecessary packets. The TRIP can also be runner and, as a result, the cost of running routers. However, the OSPF protocol supports dial-on-demand, and a single routing protocol can meet the requirements for a variety of leased line and dial-up network applications.

- The loop-free routing and fast route convergence of the EIGRP protocol are based on the distributed DUAL. This algorithm spreads an active route, that is, sending query packets to neighbors. After receiving reply packets from all neighbors, the algorithm converges routes. If neighbors are uncertain about reliability of the route information, the DUAL repeatedly spreads the active route. As a result, in some scenarios, the route may be always in active state (this route is named Route). In addition, if the metric of the successor of the active route changes during the DUAL calculation process, multiple calculations will be caused. This will slow down the route convergence speed of the DUAL. The OSPF protocol avoids this problem. Although the route convergence speed of the EIGRP protocol is almost the same as that of the OSPF protocol, the EIGRP protocol still has other disadvantages. For example, on a long and narrow network topology, if routes on a router are lost, the router will send query packets to all neighbors, and each neighbor will send query packets to all their own neighbors. It takes a long time to transmit route information changes on one router to the peer router and then converge the route from the peer router.
- On a shared network segment, every two routers running the EIGRP protocol exchange route information with each other. The OSPF elects the designated router (DR) and the backup designated router (BDR), so all routers exchange route information only with the DR and BDR. In this way, the EIGRP protocol uses more bandwidth to transmit protocol packets. When there is a large number of routers running the EIGRP protocol on a shared network segment, the protocol packets will occupy much bandwidth.
- The EIGRP is a Cisco-proprietary protocol. Cisco is the protocol inventor and the only vendor that has rights to explain and modify the protocol, and is not supervised by any third-party organization in the industry. Cisco has no obligation to notify any vendors or users who use the protocol of any modification of the EIGRP. Consequently, potential network security risks exist in network upgrade and expansion. Additionally, if users use this protocol for networking and select a single type of device, their network will be closed off like the system network architecture (SNA). As a result, their network construction and maintenance costs will be increased considerably. In contrast, the OSPF is an open protocol, which is a standard issued by IETF. Mainstream network device vendors in the industry support the OSPF protocol, and thus interoperability and openness of this protocol can be guaranteed. Using the OSPF protocol, users can control their network construction in a reasonable range. Moreover, with support from many device vendors, the OSPF protocol will become ever more mature.

2.2 OSPF

2.2.1 Introduction to OSPF

OSPF is an IETF-developed routing protocol that uses link state algorithms and applies in an AS. On the IP network, the OSPF protocol collects and transmits link state information of devices in an AS to dynamically discover and transmit routes.

Each router that runs the OSPF protocol describes the local network's connection state (for example, information about available interface information and reachable neighbors) using the link-state advertisement (LSA). The router also advertises the information to the entire AS. In this way, each router receives the LSA generated by all routers in the AS. Multiple LSAs form a link state database (LSDB). Each LSA is the description of the surrounding network topology of a router. The LSDB is the description of the network topology of the entire AS.

According to the LSDB, each router runs the shortest path first (SPF), creating a shortest path tree (SPT) rooted on the router. The SPT provides routes to each node in the AS. In the graph

theory, a "tree" is a loop-free connection diagram. Therefore, the route calculated by the OSPF protocol is loop-free.

To reduce its cost, the OSPF protocol puts forth the following concepts:

- **DR:** If there are two or more routers on a network that supports multiple access, a DR must be elected. The DR synchronizes the LSDB with all other routers in the same network segment. In this way, the LSDB is not synchronized between two non-DR routers, which reduces the bandwidth consumption due to protocol packets on the same network segment.
- **Area:** The OSPF protocol can divide an AS into different areas based on the topology and hierarchical management requirements. In this way, area border routers (ABRs) can generate LSAs by network segment when sending route information to other areas, reducing the number of LSAs in the AS and route calculation complexity.

The OSPF protocol uses the following types of routes in the sequence of priority:

- Intra-area routes
- Inter-area routes
- Type I external routes
- Type II external routes

Intra-area and inter-area routes describe the network structure of an AS. AS external routes describe how to select routes to destinations outside an AS. In general, the type I external routes are imported by the OSPF protocol from IGPs. The cost of this type of routes is almost the same as that of OSPF routes. The type II external routes are imported by OSPF from Exterior Gateway Protocols (EGPs). The cost of this type of route is far higher than that of OSPF routes. Therefore, only the cost of external routes is calculated.

2.2.2 Advantages and Disadvantages of OSPF

Advantages

OSPF is a mature protocol and many device vendors support this protocol. It has developed into one of the most widely used IGPs in the industry, especially for enterprise networks. The OSPF protocol is the only IGP recommended by IETF, which features the following advantages:

- The OSPF protocol is a loop-free routing protocol in the real sense: It uses link state and SPT algorithms.
- The OSPF protocol supports fast route convergence: It can transmit route changes to the entire AS and completes route recalculation in the shortest period of time.
- The OSPF protocol supports ECMP load balancing and improves the link resource usage efficiency.
- The OSPF protocol divides an AS into different areas and abstracts the routing information among the areas, substantially reducing the number of routes that need to be transmitted in the entire AS, lowering the requirements on the performance and management of routers, and preventing the routing information from surging with the increasing network size.
- The OSPF protocol is well-designed, minimizing the protocol packet cost. It uses the following technologies:
 - Hello packets that are sent at intervals to discover and maintain the neighbor relationship do not contain the routing information and are very short. Packets that contain the routing information are the mechanism that triggers the routing

information update (the packets are sent only when there are changes in routes). However, to enhance the robustness of the protocol, all the routing information is updated once every 1800 seconds.

- On a broadcast network, multicast addresses (not broadcast addresses) are used to send packets, reducing interference from other network devices that do not run the OSPF protocol.
- On networks that support multiple access, for example, broadcast and non-broadcast multiple access (NBMA) networks, the number of times of route exchange (or synchronization) between routers on the same segment from O (N*N) to O (N).
- The OSPF protocol uses the concept of stub area, preventing the stub area from importing routes outside the OSPF protocol and controlling the importing of LSAs in other areas.
- ABRs support route aggregation, thus reducing the routing information that needs to be transmitted among different areas.
- OSPF over On Demand Circuits is configured on point-to-point (P2P) ports to allow the SPF not to send Hello packets or update the routing information, reducing bandwidth consumption on low-speed links. The update information can be sent only when the network topology changes.
- Routes are strictly divided into four levels to provide more reliable route selection.
- The OSPF protocol supports port-based plain-text and MD5 protocol packet verification, preventing malicious attacks and configuration errors.
- The OSPF protocol is also applicable to networks of all sizes and is able to support thousands of devices through proper planning.
- The OSPF protocol can perceive the global network topology information, which is supported by link-state routing protocols. It can also be expanded to support TE, maximizing the backbone network usage efficiency.

Disadvantages

The OSPF protocol has the following disadvantages:

- **Complex configuration:** Network analysis personnel must have adequate network knowledge to configure and manage the OSPF network because network area division and network attributes are complex. As a matter of fact, most of network administrators are familiar with the OSPF protocol as this protocol is widely used.
- **Comparatively poor route load balancing capability:** Although the OSPF protocol can automatically generate port route costs based on information such as the port bandwidth, it selects only the optimal path to forward (supporting ECMP) routes of different costs destined to the same destination. The OSPF protocol cannot implement load balancing of routes of different costs. However, the EIGRP can configure a range to send traffic in proportion based on different link costs.

2.3 Comparison Between OSPF and EIGRP

Table 2-1 lists the comparison between the OSPF and EIGRP protocols.

Table 2-1 Comparison between OSPF and EIGRP

Comparison Item	OSPF	EIGRP
Protocol standard	IETF's standard protocol, which is well-designed and supported by the majority of device vendors Networking is not restricted by device vendor selection.	As a Cisco-proprietary protocol, it cannot interoperate with protocols from other vendor for networking and is not as mature as the OSPF protocol. Protocol implementation is being optimized based on utilization experience, for example, stub processing is added.
Deployment scope	IGP recommended by IETF and most widely used routing protocol in the world	Only few networks use this protocol.
Core algorithm	SPF, supporting fast route convergence and loop-free routing	Uses the distributed DUAL. The intermediate status is unpredictable and is likely to enter the SIA status. Query may be spread to the entire network.
Support for network topologies	Supports hierarchical network topologies and has good manageability and scalability.	Does not support hierarchical network topologies.
Support for new technologies	Can be expanded to support OSPF-TE.	Cannot be expanded to support TE. If the EIGRP protocol is used as the IGP on large-sized networks, the TE deployment will be restricted.

3 Replacement Solution Design

This chapter provides the low level design (LLD) for two replacement solutions, which can be selected according to the live network situation. Perform operations according to the replacement procedure during replacement.

3.1 Collect Live Network Information

Collect live network information before performing the replacement to conduct an appropriate plan for the network after the replacement is complete.

3.2 Select a Replacement Solution

There are multiple solutions for replacing the EIGRP protocol with the OSPF protocol. Table 3-1 lists the two most frequently used replacement solutions.

Table 3-1 Replacement solution

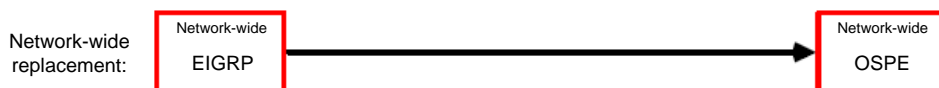
Replacement Solution	Description	Network Type
Solution 1: network-wide replacement solution	Network-wide replacement indicates replacing all routing devices that run the EIGRP protocol with new devices that run the OSPF protocol at a time. After the replacement is complete, the entire network is deployed with routing devices that run the OSPF protocol.	This solution is suited for small-sized networks that have a clear service traffic model.

Replacement Solution	Description	Network Type
Solution 2: asymptotic replacement solution	Asymptotic replacement indicates replacing the EIGRP protocol on border networks with the OSPF protocol (the replacement operation can be performed simultaneously on multiple branch networks) when the size of networks is large. After that, replace the EIGRP protocol with the OSPF protocol on the backbone network. Finally, replace the EIGRP protocol with the OSPF protocol on the entire network.	This solution is applicable to networks of complex topologies and service traffic models. The replacement can be completed through two steps. NOTE This solution is applicable to a new branch network that uses the OSPF protocol. The new border network that uses the OSPF protocol as the IGP is connected to the original EIGRP network.

3.3 Network-Wide Replacement Solution

The network-wide replacement solution requires that the EIGRP protocol be replaced with the OSPF protocol on all routers over the entire network. Figure 3-1 shows the replacement model. The core idea of this solution is adjusting the management distance (also known as the route priority) of the EIGRP to enable both EIGRP and SPF to run the same device while only one protocol takes the role of forwarding service traffic.

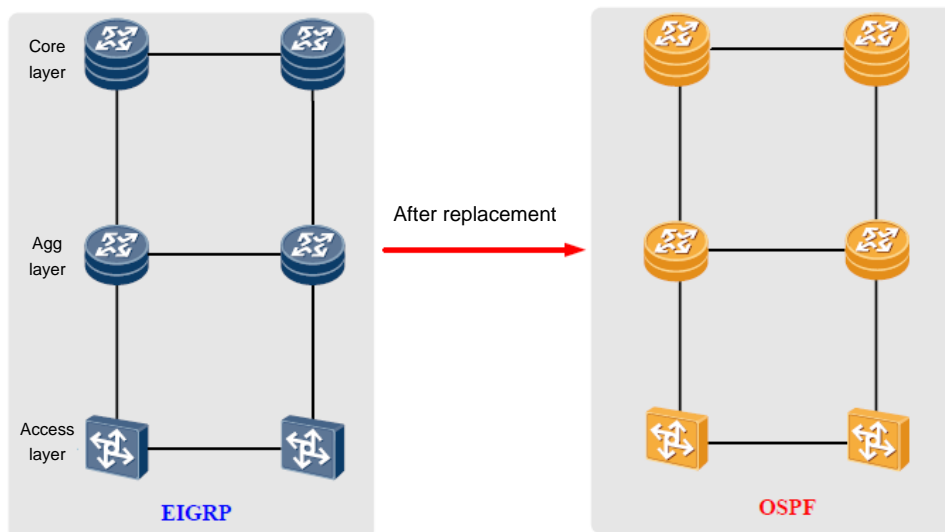
Figure 3-1 Network-wide replacement model



In actual operations, adjust the EIGRP route priority to higher than the OSPF route priority to ensure the EIGRP protocol takes the role of service traffic forwarding. After the OSPF configuration is complete, modify the EIGRP priority to lower than the OSPF route priority to enable the OSPF protocol to take the role of service traffic forwarding. After services on the live network have run properly for a certain period of time, delete the EIGRP configurations, so that the entire network is an OSPF network.

Figure 3-2 shows the typical network-wide replacement model. Prior to the replacement, all core, aggregation, and access layer devices on the network run the EIGRP.

Figure 3-2 Networking diagram



The EIGRP protocol on all devices on the entire network can be replaced with the OSPF protocol through the following procedure:

Step 1 Save and back up data

Save the live network configuration data in the memory of devices and back up the data in a local PC for fault location and data rollback if a problem occurs during replacement.

Collect key data such as information about the routing table and forwarding information table (FIB), the number of routes, and link bandwidth usage on devices. Back up the data in a local PC. After the replacement is complete, compare the key data to ensure that services can run properly.

Step 2 Modify the EIGRP route priority.

The purpose of modifying the EIGRP route priority is to ensure the EIGRP route priority is higher than the OSPF route priority, so that the EIGRP protocol takes the role of service traffic forwarding. Table 3-2 lists the route priorities of routing protocols on Cisco devices. By default, the internal and external EIGRP route priority values are 90 and 170 respectively, while the OSPF route priority value is 110.

Table 3-2 Route priority

Protocol Type	Route Priority
Connected	0
Static	1
Internal EIGRP routes	90
OSPF	110

Protocol Type	Route Priority
IS-IS	115
RIP	120
External EIGRP routes	170

The external EIGRP route priority value can be modified to 95, which is higher than the OSPF route priority value.

distance eigrp 90 95



NOTE

A smaller route priority value indicates a higher priority.

Step 3 Configure the OSPF protocol.

OSPF configuration must be planned based on the collected live network information, for example, area planning, ABR planning, autonomous system boundary router (ASBR) planning, and route aggregation planning.



CAUTION

If route aggregation exists on the original EIGRP network, advertise aggregation routes first and then advertise specific routes on connected network segments during OSPF configuration to prevent the OSPF's specific routes and the EIGRP's aggregation routes from taking effect.



CAUTION

After the OSPF configuration is complete, compare the current routing table information and the number of routes with the collected data to check whether the OSPF routes can fully cover the EIGRP routes. If not, check and modify the OSPF configuration until the OSPF routes fully cover the EIGRP routes. The EIGRP protocol coexists with the OSPF protocol on all devices over the entire network. The devices select the EIGRP routes for data forwarding because the priority of the EIGRP routes is higher than that of the OSPF routes. The OSPF protocol is in backup state but does not instruct data forwarding.



CAUTION

The OSPF routes fully cover the EIGRP routes: The next-hop IP address and the outbound port of the same destination network in the OSPF routing table are the same as that in the EIGRP routing table. This is prerequisite of replacement implementation.

Step 4 Modify the EIGRP route priority again.

Modify the EIGRP route priority to ensure the EIGRP route priority is lower than that of the OSPF protocol, so that the OSPF takes the role of service traffic forwarding. The EIGRP protocol is in backup state. The internal and external EIGRP route priority values can be modified to 130 and 170.

distance eigrp 130 170

 **TIP**

You are advised to modify the EIGRP route priority on border devices first and then on core devices. During the route priority modification, the EIGRP routes take effect on some devices and the OSPF routes take effect on some devices. As a result, loops may exist on the network. To avoid this problem, this step must be quickly performed. You are advised to modify the route priority in batches using configuration scripts through a network management system (NMS).

Step 5 Verify the result.

After the OSPF routes take effect, check whether the live network services run properly. Pay attention to the following points during actual verification:

- Routing table entries before the replacement are the same as that after the replacement.
- There is little difference between the link bandwidth usage before the replacement and that after the replacement.
- Access to specific services is normal after the replacement.

Step 6 Delete EIGRP configurations.

After the OSPF network runs properly for a certain period of time and the service traffic forwarding is normal, delete the EIGRP configuration.

----**End**

After the EIGRP protocol is replaced with the OSPF protocol on network-wide devices, the entire network is an OSPF network.

Related Configuration Information

EIGRP configuration is simple. If the EIGRP routes advertised in network mode, no mask needs to be configured. The EIGRP routes are automatically aggregated and advertised based on the network types (A, B, and C). This is a big difference between EIGRP configuration and OSPF configuration. Table 3-3 lists the commands for EIGRP and OSPF configurations.

Table 3-3 Commands for EIGRP and OSPF configurations

Command	Description
router eigrp 1	Configures the EIGRP process.
router ospf 1	Configures the OSPF process.
network 10.0.0.0	Enables the EIGRP network segment.
network 10.4.4.13 0.0.0.0 area 2	Enables the OSPF network segment in areas.
redistribute static/RIP/OSPF	Imports external routes.
show ip route	Displays routing table entries.

Command	Description
show ip eigrp topology summary	Displays the EIGRP topology summary.
distance eigrp 90 95	Configures the priorities of internal and external EIGRP routes.
show ip ospf neighbor	Displays the OSPF neighbor information.
show ip ospf database	Displays the OSPF routing database information.
show ip ospf data database-summary	Displays the OSPF routing database summary information.

3.4 Asymptotic Replacement Solution

Asymptotic replacement indicates replacing the EIGRP protocol on border networks with the OSPF protocol (the replacement operation can be performed simultaneously on multiple branch networks) when the size of networks is large. After that, replace the EIGRP protocol with the OSPF protocol on the backbone network. Finally, replace the EIGRP protocol with the OSPF protocol on the entire network. Figure 3-3 shows the asymptotic replacement model.

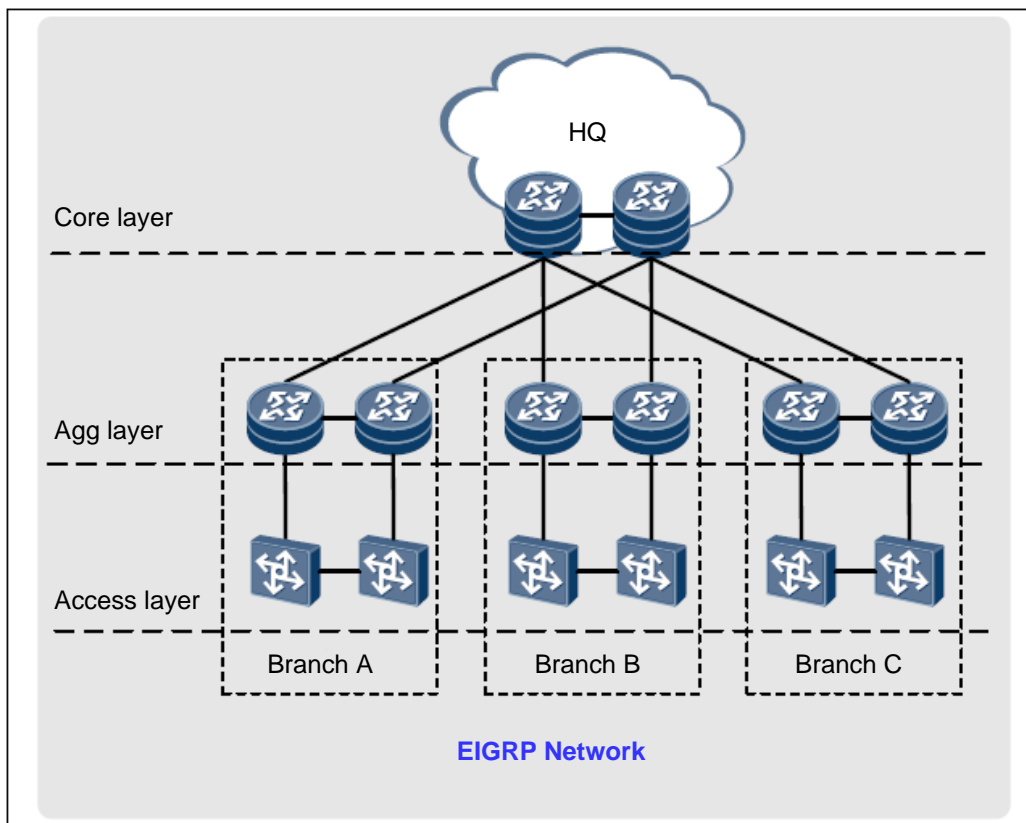
Figure 3-3 Asymptotic replacement model



There is an intermediate state in the asymptotic replacement solution: The EIGRP protocol that is not replaced with the OSPF protocol on some devices still takes the role of service traffic forwarding, and the OSPF protocol takes the role of service traffic forwarding after the replacement is complete. In this intermediate state, part of network is an EIGRP network and part of the network is an OSPF network. To enable the EIGRP network to communicate with the OSPF network, bidirectional redistribution of the EIGRP and OSPF routes must be implemented on border devices (running EIGRP and OSPF simultaneously) on the EIGRP and OSPF networks.

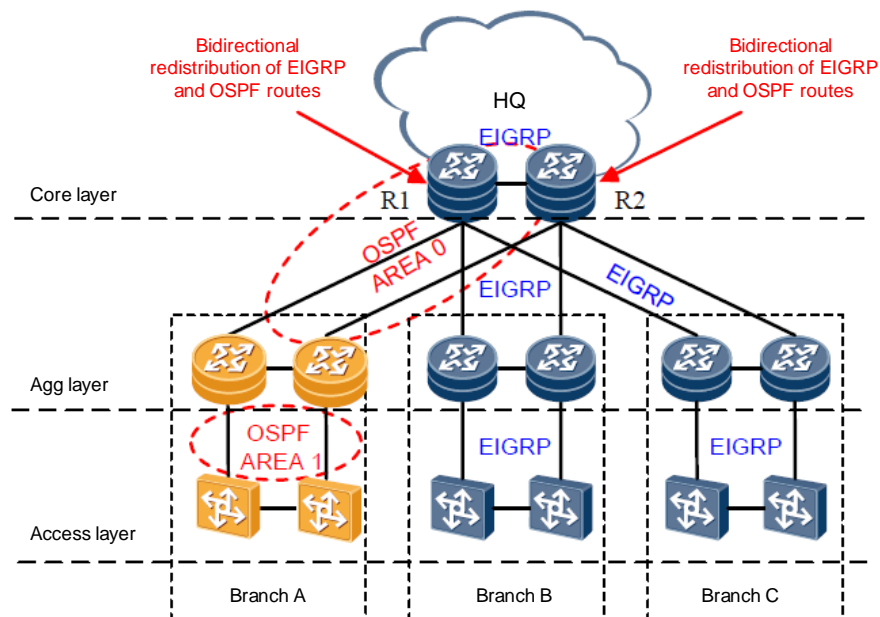
As shown in Figure 3-4, an enterprise network is composed of a headquarters (HQ) network and branch networks. All devices on the entire network run the EIGRP. The enterprise plans to replace the EIGRP protocol with the OSPF protocol. Regarding the large size of the enterprise network and the heavy difficulty in replacing the EIGRP protocol with the OSPF protocol at a time, the asymptotic replacement solution is recommended.

Figure 3-4 Pre-replacement networking diagram



To meet the enterprise's requirements for asymptotic replacement, the EIGRP protocol on routing devices on Branch A network is replaced with the OSPF protocol. Figure 3-5 shows the post-replacement networking model.

Figure 3-5 Post-replacement networking diagram of Branch A



NOTE

This networking model is used as an example to describe how to implement asymptotic replacement. In actual projects, the planning of network size and OSPF, for example, area planning, must be conducted based on the live network situation and the target network.

The asymptotic replacement procedure is as follows:

Step 1 Save and back up data.

Save the live network configuration data in the memory of devices and back up the data in a local PC for fault location and data rollback if a problem occurs during replacement.

write

Collect key data such as information about the routing table and FIB, the number of routes, and link bandwidth usage on devices. Back up the data in a local PC. After the replacement is complete, compare the key data to ensure that services can run properly.

Step 2 Modify the EIGRP route priority on the routing devices of Branch A network and the routing devices (R1 and R2, border devices on the EIGRP and OSPF networks) that connect the HQ to the Branch A.

The purpose of modifying the EIGRP route priority is to ensure the EIGRP route priority is higher than the OSPF route priority, so that the EIGRP protocol takes the role of service traffic forwarding. By default, the internal and external EIGRP route priority values are 90 and 170 respectively, while the OSPF route priority value is 110. The external EIGRP route priority value can be modified to 95, which is higher than the OSPF route priority value.

distance eager 90 95



NOTE

A smaller route priority value indicates a higher priority.

Step 3 Configure the OSPF protocol on the routing devices on Branch A network and R1 and R2.

OSPF configuration must be planned based on the collected live network information, for example, area planning, ABR planning, autonomous system boundary router (ASBR) planning, and route aggregation planning.

You are advised to plan set the OSPF area of branch networks as the stub area and deliver default routes through OSPF backbone devices to divert upstream traffic. This avoids the operation of redistributing the EIGRP routes to the OSPF routes on border devices.



WARNING

If route aggregation exists on the original EIGRP network, advertise aggregation routes first and then advertise specific routes on connected network segments during OSPF configuration to prevent the OSPF's specific routes and the EIGRP's aggregation routes from taking effect.



WARNING

After the OSPF configuration is complete, compare the current routing table information and the number of routes with the collected data on the routing devices of Branch A network to check whether the OSPF routes can fully cover the EIGRP routes. If not, check and modify the OSPF configuration until the OSPF routes fully cover the EIGRP routes. The EIGRP coexists with the OSPF on the routing devices of Branch A network and R1 and R2. The routing devices of Branch A network and R1 and R2 select the EIGRP routes for data forwarding because the priority of the EIGRP routes is higher than that of the OSPF routes. The OSPF protocol is in backup state but does not instruct data forwarding.



WARNING

The OSPF routes fully cover the EIGRP routes: The next-hop IP address and the outbound port of the same destination network in the OSPF routing table are the same as that in the EIGRP routing table. This is prerequisite of replacement implementation.

Step 4 Configure bidirectional redistribution of the EIGRP and OSPF routes on border devices R1 and R2.

R1 and R2 are border devices of the EIGRP and OSPF networks. To enable the EIGRP network to communicate with the OSPF network, bidirectional redistribution of the EIGRP and OSPF routes must be configured on R1 and R2.



NOTE

Configure bidirectional redistribution of the EIGRP and OSPF routes on border devices first, and then modify the EIGRP route priority on the routing devices of Branch A network to reduce traffic loss during priority modification.

If the OSPF area of Branch A network is the stub area, you only need to configure bidirectional redistribution of the EIGRP and OSPF routes on R1 and R2.

Step 5 Modify the EIGRP route priority on the routing devices of Branch A network to ensure the route priority of the EIGRP protocol is lower than that of the OSPF protocol, so that the OSPF protocol takes the role of service traffic forwarding. The EIGRP protocol is in backup state. The internal and external EIGRP route priority values can be modified to 130 and 170.

distance eigrp 130 170

 **TIP**

You are advised to modify the EIGRP route priority on access layer devices first and then on aggregation layer devices.

During the route priority modification, the EIGRP routes take effect on some devices and the OSPF routes take effect on some devices. As a result, loops may exist on Branch A network. To avoid this problem, this step must be quickly performed. You are advised to modify the route priority in batches using configuration scripts through an NMS.

Step 6 Verify the result.

After the OSPF routes take effect, check whether the live network services run properly. Pay attention to the following points during actual verification:

- On the routing devices of Branch A network, routing table entries before the replacement are the same as that after the replacement.
- On the routing devices of Branch A network, there are few differences between the link bandwidth usage before the replacement and that after the replacement.
- Branch A network can communicate with the EIGRP network on which the EIGRP protocol has not been replaced with the OSPF protocol.

Step 7 Delete EIGRP configurations on Branch A network.

After the OSPF network runs properly on Branch A network for a certain period of time and the service traffic forwarding is normal, delete EIGRP configurations on Branch A network.

----**End**

Replace the EIGRP protocol with the OSPF protocol on other branch networks by referring to Branch A network. After the EIGRP protocol is replaced with the OSPF protocol on all branch networks, only the backbone network at the HQ runs the EIGRP. Then, replace the EIGRP protocol with the OSPF protocol on the backbone network and delete configurations of bidirectional redistribution of EIGRP and OSPF routes on border devices. Finally, the entire network becomes an OSPF network.

3.5 Solution Verification

The two replacement solutions have been verified on actual networks.

4 References

RFC2281: <http://www.rfc-editor.org/info/rfc2281>

RFC2338: <http://www.rfc-editor.org/info/rfc2338>