Cisco ios ospf configuration guide

This document applies to these Page 2 products This document applies to these Page 3 products Huawei uses machine translation in conjunction with a human corrector to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). This chapter describes how to set up ABR to improve network security and balance the load. This document applies to these Page 4 Huawei products uses machine translation in conjunction with a human proofer to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). This chapter introduces the IPv6 intermediate system (IS-IS) and describes its implementation and configuration. This document applies to these Page 5 products This document applies to these Products Page 6 Huawei uses machine translation in conjunction with human correcting to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). Conventional routers choose the shortest route as the main route, regardless of other factors such as bandwidth. Thus, traffic does not switch to other paths, even if the path is overloaded. MPLS Road Traffic (TE) has advantages in solving the problem of network congestion. With MPLS TE help, you can accurately monitor the trajectory and prevent traffic from passing through congested nodes. MPLS TE can reserve resources to ensure the quality of services when creating LSPs. c IS-IS TE is an extension of IS-IS to support MPLS TE and corresponds to RFC 5305. IS-IS TE identifies new TVs in IS-IS LSPs to transport TE information and flood LSPs to flood and synchronize TE information. It extracts TE information from all LSPs and then transmits TE information in a limited shortcut to the first (CSPF) MPLS module to calculate the tunnel path. IS-IS TE plays the role of porter in MPLS TE. Figure 8-28 shows the relationship between IS-IS TE, MPLS TE and CSPF. Figure 8-28 Relationships Between MPLS TE, CSPF, and IS-IS TE For In LSPs, IS-IS TE defines the following TVs in RFC 5305: Extended availability of IS TLV This TLV takes the place of availability of TLV IS and expands TLV formats with sub-TLV. Sub-TVs are implemented in TVs just as TVs are sold in LSPs. Currently, all sub-TVs identified in the RFC 5305 are supported. Table 8-7 Sub-TLVs identified in extended availability is IS TLV Length Type (Byte) Administrative Group Value 3 4 indicates an administrative group. IPv4 Interface Address 6 4 indicates the address of the IPv4 local interface. IPv4 Neighbor address 8 4 indicates the address of the neighbor's IPv4 interface. The maximum bandwidth of the 9 4 link indicates the maximum bandwidth of the link. The maximum reserved bandwidth of reference 10 4 indicates the maximum reserved bandwidth of the link. Unconditional bandwidth of 11 32 indicates unconditional bandwidth. The default metric of 18 3 indicates the default TE metric. The sub-TLV 22 36 bandwidth limit indicates TLV bandwidth limitations. Traffic Engineering router ID TLV It has a type of TLV 134, with a four-row router ID. It is used as an MPLS LSR ID. In MPLS TE, the router ID clearly identifies the router. Each router has a router ID. Extended availability of IP TLV This TLV takes the place of THE IP TLV and carries routing information. It extends the length of the route value field and carries sub-TLVs. Shared Risk Link Group TLV It has a type of TLV 138 and is used to carry information about the group of common risk links. This TLV can carry information about several common links, each of which is a 4-point positive integer. IS-IS TE is implemented in two phases: Answer to MPLS TE configurations. IS-IS TE only functions after MPLS TE is enabled. IS-IS TE updates TE information in IS-IS LSPs based on MPLS TE configurations. IS-IS TE transfers MPLS TE configurations to the CSPF module. Process TE information in LSPs. IS-IS TE extracts TE information from IS-IS LSPs and transmits TE information to the CSPF module. In typical applications, IS-IS TE helps MPLS TE set up te tunnels. As shown in Figure 8-29, the TE tunnel is installed between RouterA and RouterD. Figure 8-29 IS-IS TE Network Configuration is as follows: Turn on MPLS TE on RouterA, RouterB, RouterC, and RouterD and allow MPLS TE CSPF at RouterA to calculate the tunnel path. Start IS-IS and turn on IS-IS TE on RouterA, RouterB, RouterC and RouterD to connect the four routers. Once the previous IS-IS configuration has been completed on RouterA, RouterB, RouterC and RouterD sends LSPs with TE information, on every router. The router then receives TE information from RouterB, RouterC and RouterD from LSPs. the whole network. IS-IS Shortcut (AA) and IS-IS Advertise (FA) calculate routes through TE tunnel interfaces. For traffic transmitted on a particular route, MPLS guarantees a reliable distillation, while IP is less reliable. Rewind MPLS is achieved by setting up IS-IS Shortcut (AA) and IS-IS Advertise (FA), with TE tunnel interfaces involved in route calculation and defined as outgoing interfaces of specific routes. Figure 8-30 Principle IS-IS Shortcut (AA) and Advertising (FA) IS-IS Shortcut (AA) and IS-IS Advertising (FA) have the following differences: IS-IS Advertising (FA) advertises TE tunnel information for other ISs, while IS-IS Shortcut (AA) does not. As shown in Figure 8-30, if the TE tunnel is included with IS-IS Advertising (FA), RouterA advertises information that RouterC is its neighbor. Neighboring information is carried out in TLV Type 22 without sub-TLVs. That is, no TE information is kept. If the TE tunnel is enabled by IS-IS Shortcut (AA), RouterA does not advertise such information. Is-IS (FA) advertising affects the SPF tree of other routers, while IS-IS Shortcut (AA) does not affect. IS-IS Shortcut (AA) does not affect the original structure of the IS-IS SPF tree, regardless of whether the TE tunnel exists or not. Aside from a link from RouterA to RouterB, and that from RouterB to RouterC, a link marked shortcut from RouterA to RouterC is added. The link marked Shortcut is involved in the calculation of the route. If the TE tunnel is enabled with IS-IS Advertising (FA), RouterA advertises the message that RouterC is a neighbor of RouterA to other routers on the network. Other routers then consider RouterC a neighbor of RouterA and add RouterC to the SPF tree without not marking it with Shortcut. The IS-IS (FA) advertising does not support the relative metric, while is-IS Shortcut (AA) does. IS-IS Shortcut (AA) supports absolute metric and relative metric. If you use an absolute metric, the metric value of THE tunnels in IS-IS is fixed. If you use a relative metric, the metric cost of TE tunnels in IS-IS is the amount of physical connection cost and relative metric. As shown in Figure 8-30, if the relative metric is set at 1, the cost of the journey from RouterA to RouterC through the TE tunnel is 21 (10'10'1). If the relative metric is set at 0, the TE tunnel and physical connection have an equal cost to the outgoing interface. If the relative metric is less than 0, the TE tunnel interface is preferable to outgoing interfaces. Is-IS Advertise (FA) requires bidirectional TE tunnels, while IS-IS Shortcut (AA) requires only unidirectional tunnels. This document applies to these Page 7 huawei products uses machine translation in conjunction with a human proofer to translate this document into different languages to help you better understand the content of this Note: Even the most advanced machine translation are consistent with the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). Local multicast-topology IS-IS (MT) creates a separate multicast topology on a local device without affecting the protocol packages exchanged between devices so that both TE tunnels and multicast can be configured in the backbone network. The TE tunnel in question identifies the TE tunnel included from IGP Shortcut (AA). If you deploy multiplex and MPLS TE multiplex tunnels at the same time, the multicast function can be affected by the TE tunnel. This is because, after the TE tunnel is turned on with IS-IS Shortcut (AA), the outbound route interface calculated by IS is not an actual physical interface, but a TE tunnel interface. According to the unicast route to the multi-stationed original address, the router sends the Report message through the TE tunnel interface. Routers covered by the TE tunnel cannot feel the Report message, so multi-station rewinds cannot be created. The TE tunnel is one-way, so multi-station data packets sent by a multi-station source are sent to routers covered by the tunnel through appropriate physical interfaces. Routers don't have any multi-point rewind entry. In this way, multi-cast data packets are discarded. Figure 8-31 TE Tunnel Scenario As shown in Figure 8-31, RouterA, RouterB, RouterC, RouterD, and RouterE are Level-2 routers. Routers are operated by IS-IS to implement the accession. Multi-station services are normal. A single-directional MPLS TE tunnel is installed between RouterB and RouterD. The MPLS TE tunnel is enabled by IS-IS Shortcut (AA). When you view the multi-tissue routing table on routerC covered by the TE tunnel, you can't find a multi-taxi forward. In this way, multi-station services are interrupted. The process of transferring multicast packages between a client and a multi-frame server is this: to join a multi-point group, a customer sends a report message to RouterA. The routerA then sends a Message Join to RouterB. When the Join message reaches RouterB, RouterB uses the 1/0/0 tunnel as an RPF interface and sends a message to RouterC via GE 2/0/0 using the MPLS tag. The Join message is sent with the MPLS tag, so RouterC simply sends a message and doesn't create a multi-taxi routing record. In the topology shown in figure 8-31, RouterC is the penultimate jump forward of MPLS. RouterC pops out of the MPLS label and then sends a Join message to RouterD via GE 2/0/0. After receiving the Join message, RouterD creates a multi-cash reselling record. The incoming GE 2/0/0 interface and GE 1/0/0 interface. The router then sends a message to RouterE. SPT is set up. When a multi-cast source source routerD traffic will redirect traffic to RouterC. RouterC does not create any rewind recordings in advance. Thus, the traffic is discarded and the multi-cash service is interrupted. As described in the previous multicast package transfer process, the redirection of multicast packages depends on the unicast routing table, and the TE tunnel is one-way. In this way, multi-cast packages are discarded. This problem can be avoided with the following methods: Manual setting up static multi-cast routes to manage the re-typing of multi-office packages. Set up a bidirectional TE tunnel. In this case, returned multi-ticket packages can be sent through the same tunnel. Routers covered by the TE tunnel use a tunnel to transmit multi-station packages. Set up the Multicast Border Gateway Protocol (MBGP) for unicast topology from multi-tissue topology. MBGP provides a topology that does not contain a TE tunnel for a multi-cost individual. Multicast is used to test FIU on MBGP routes. Local MT Previous methods are used to prevent multicast services from being interrupted. The downside of the first three methods is that many manual configurations have to be made. As a result, if the network is complex, the planning, configuration, and maintenance tasks become more difficult. Therefore, in the previous network environment, you need to set up a local MT. Local MT creates a separate multicast topology on a local device without affecting the protocol packages exchanged between the devices. This ensures that multi-station services are still available when deploying both multi-station and MPLS TE tunnel with IGP Shortcut. After turning on the local MT router at the entrance to the TE tunnel, it creates a separate multi-station IGP (MIGP) routing table to store physical interfaces that match the TE tunnel. This ensures that multi-ticket protocols are sent correctly. Correct routing records are created in the multi-cast routing table (MRT). The implementation of the local MT can be divided into two stages: Create a MIGP routing table. Multicast protocol packages are redirected according to the unicast routing table. After turning on the local MT on RouterB RM, it creates separate MIGP routing tables for multi-taxi protocols. When the outgoing route interface is the TE tunnel interface, IGP calculates the actual physical outgoing route interface and adds an outgoing interface to the MIGP routing table. A guide to re-pumping multicast protocol packages. Before redirecting the multicast protocol package, the router needs to reach the unicast routing table. If the router finds that the next transition will be a TE tunnel, the router continues to search the MIGP routing table for physical interface to guide the distillation forward of the multi-cast protocol package. Figure 8-32 8-32 MT Topology As shown in Figure 8-32, if the outgoing multicast interface of multicast source 192.168.3.2/24 is a TE tunnel 1/0/0, the physical outgoing route interface calculated by IS-IS is GE 2/0/0. IS-IS sets the route to the MIGP routing table. Multi-taxi services are not affected by the TE tunnel. Multicast packages are redirected through physical outgoing interfaces according to the MIGP routing table for general IP redirection. Appropriate routing records are created in MRT. Multicast data packets are then sent correctly. This document applies to these Page 8 Huawei products uses machine translation in conjunction with a human proofreader to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). IS is a dynamic communication state routing protocol originally developed by OSI. To support routing, IPv4 IS is applied to IPv4 networks and is called Integrated IS-IS. As IPv6 networks are built, IS-IS also needs to provide accurate routing information to re-route IPv6 packages. IS-IS is well scalable, supports IPv6 network protocols and is able to open, generate and re-mute IPv6 routes. Advanced IS-IS for IPv6 is defined in the project-ietf-isis-ipv6-05 IETF. IPv6 IS uses two new TVs and one network protocol ID (NLPID) to process and calculate routes. Two TVs: TLV 236 (IPv6 Reachability): describes network availability by determining the prefix and route metric. TLV 232 (IPv6 Interface Address): Similar to the IP interface address TLV IPv4, except that it changes the 32-bit IPv4 address to the 128-bit IPv6 address. NLPID is an 8-bit field that defines network layer protocol packages. NLPID IPv6 is 142 (0x8E). If IS-IS supports IPv6, it advertises routing information through the NLPID value. This document applies to these Page 9 Huawei products uses machine translation in conjunction with a human proofreader to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). This chapter describes THE routing of IP and how it is a core element of data networks. This document applies to these products Page 10 Huawei uses translation, combined with a human corrector to translate this document into various different different to help you better understand the contents of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). Table 10-5 lists all the common route attributes that influence route selection and the commands used to test them. Table 10-5 Teams used to test the attributes of the Team Attribute route, used to check the route Attribute PrefVal display bgp routing table - network - Local_Pref display bgp routing table -dining network AS_Path display bgp routing-table - network - Origin display bgp routing-table - network - MED display bgp routing-table - network - peer type of display bgp routing-table network I The NETWORK's e-table display IP routing table ip address mask length mask mask length verbose , in which the IP address is the following IP address hop route BGP Cluster_List display bgp routing network table Originator_ID display bgp routing the table network Router ID display bgp routing the table network Peer IP address display bgp routing network table next example describes How to check the BGP route attributes in the bgp display routing the team table output. <HUAWEI> display bgp routing-table BGP Local router ID is 192.168.2.2 Status codes: * - valid, > - best, d - damped, h - history, i - internal, s - suppressed, S - Stale Origin : i - IGP, e - EGP, ? - incomplete Total Number of Routes: 9 Network NextHop MED LocPrf PrefVal Path/Ogn *> 1.1.1.9/32 0.0.0.0 0 0 i *>i 2.2.2.7/32 10.1.1.2 0 100 0 (65001)i * i 10.1.3.1 0 100 0 (65011 65001)i *>i 2.2.2.8/32 10.1.2.2 0 100 0 (65011)i * i 10.1.3.2 0 100 0 (65001 65011)i *>i 2.2.2.9/32 10.1.4.2 0 100 0 (65001 65101)i * i 10.1.5.2 0 100 0 (65011 65101)i i 3.3.3.9/32 10.1.6.2 0 100 0 (65001 65101) 300i i 10.1.6.2 0 100 0 (65011 65001 65101) 300i Table 10-6 Description of the display bgp routing-table command output Item Description BGP Local router ID is 1.1.1.2 Router ID : 1.1.1.2, в том же формате, что и код статуса IPv4-адреса Status Codes Route displayed before each route record: : indicates a valid route with the address attainable following. The best route chosen by BGP indicates the best route chosen by BGP. g: points to a soaked route. h: indicates the route of history. i: indicates the route taken from the peer group IBGP. s: points to a depressed route. If certain routes to generalize the route are suppressed, s is displayed before each specific route. S: indicates the route in Stale status, and the route is removed. Such routes may occur during the BGP GR process. BGP damping measures the stability of the route penalty. The higher the penalty cost, the more stable the route. Every time the route slams occurs (the device is zlt;/HUAWEI)gt; withdrawal or upgrade package), BGP adds a penalty cost to the route carried in the package. When the route penalty exceeds the Value of the Suppression, BGP suppresses the route by replacing the route sign d or h. The route is ignored, and its upgrade packages are not advertised to other BGP colleagues until the penalty cost of the route is reduced to the reuse value. If d is displayed in front of the route, the route is in the upgrade package. If h is displayed in front of the route, the route is in the Withdraw package. The value of the fine does not increase after reaching the suppression threshold. The penalty cost of the depressed route is reduced by half after a period of semi-chilli. When the penalty value of a D route is reduced to reuse, the route becomes reusable, and BGP removes the D sign, adds a route to the IP routing table, and advertises the Upgrade package that carries the route to BGP colleagues. When the penalty value of a h route is reduced to 0, BGP removes that route from the BGP routing table. Origin Route Origin code displayed before each route record: IGP: indicates that routes are added to the BGP routing table using the network team (BGP). EGP: indicates that routes have been explored using the EGP protocol. Incomplete: indicates that routes are added to the BGP routing table using the import-route (BGP) command. The network address in bgP NextHop Next hop routing table address MED the value of the BGP route, similar to the cost of IGP LocPrf routes Local_Pref PrefVal PrefVal Path/Ogn AS_Path and Origin attributes information about Next_Hop, MED, Local_Pref, PrefVal, AS_Path and Origin can be displayed via the bgp display routing team. To check for information about route type, peer type, IGP cost, Cluster_List, router ID, and ip address, start bgp routing routing network command. <HUAWEI> display bgp routing-table 10.1.1.1 BGP local router ID : 192.168.2.2 Local AS number : 65001 Paths: 1 available, 1 best, 1 select BGP routing table entry information of 10.1.1.1/32: From: 10.1.3.1 (192.168.2.3) Route Duration: 05h35m04s Relay IP Nexthop: 0.0.0.0 Relay IP Out-Interface: GigabitEthernet1/0/4 Original nexthop: 10.1.3.1 Qos information : 0x0 AS-path Nil, origin incomplete, MED 1234, localpref 100, pref-val 0, valid, internal, best, select, active, pre 255, IGP cost 1 Not advertised to any peer yet Table 10-7 Description of the display bgp routing-table command output Item Description BGP local router ID Router ID of the local device, in the same format as an IPv4 address. Local number AS Local number AS. Information about the BGP Path route. BGP routing information entry table 10.1.1.1/32 Information on the BGP route 10.1.1.1/32: From IP address advertised route. In this example, 10.1.3.1 is the IP address of the interface used. BGP (peer-to-peer IP address) and 192.168.2.3 is a peer-to-peer router ID. The duration of the route. Rebroadcast the IP Nexthop IP address of the route by which the BGP route is edified. Rebroadcast IP Out-Interface The Out-Interface Out Route Interface to which the BGP route is routeed. The original nexthop Original next IP Hop address. Sos information zos information. AS-way AS_Path attribute. If Nil is displayed, AS_Path attribute is zero. Origin: Origin: IGP: indicates that routes are added to the BGP routing table using the Network Command (BGP). EGP: indicates that routes have been explored using the EGP protocol. Incomplete: indicates that routes are imported using the import-route (BGP) command. MED MED is the value of the BGP route, similar to the cost of IGP routes. localpref Local_Pref pref-val PrefVal a valid valid route with an achievable following hop address. the inner type of peer from which the route is learned. External: indicates that the route learn from peer EBGP. Internal: indicates that the route learn from the peer-to-peer IBGP. the best optimal route. Select the route you choose to deliver to the IP routing table. NOTE: According to BGP selection rules, BGP selects only one optimal route, and this route is marked by the best. In load balancing scenarios or FRR, you need to add multiple routes to the IP routing table, and each route is marked with a choice. Thus, the number of best-marked routes is 1, and the number of routes marked by choice is the actual number of routes added to the IP routing table. active active route. Up to 255 Protocol priority route: 255 IGP cost IGP cost. Not advertised for any peer yet the itinerary is not advertised for any peer yet. The bgp display routing network - mask-length mask - longer prefixes - the team's output varies depending on route generation mode and transmission mode, and not all BGP attributes are necessarily displayed. In the previous example, the route type is not displayed because route 10.1.1.1/32 is the IBGP route. For example: zlt;HUAWEI:mapping bgp routing table 10.0.0.0 BGP local router ID: 192.168.2.4 Local AS Number : 200 Ways: 1 Available, 1 Best, 1 Choice BGP Routing Table Entry Information 10.0.0/8: Aggregate Route. Duration: 04h50m46s Direct exit interface: NULL0 Original nexthop: 127.0.0.0.1 Pet Information : 0x0 AS-way (65001 10 1000), Origin incomplete, pref-val 0, valid, local, best, pick, active, up to 255 aggregator: AS 200, Aggregator ID 192.168.2.4, Atomic Unit 3 knots: 10.1.7.2 172.16.1.2 192.168.1.2 Route 10.0.0.0/8 was manually summarized using an aggregated command. This way, the aggregated route is displayed in the team's output. The route type changes as follows: If the route is automatically added up with a consolidated automatic command, the Summary of the route is a total of The route will be displayed. If the route is imported by a network command, the network route will be displayed. If the route is imported with the import-route command, the import route will be displayed. The following example is RR and cluster. Thus, Cluster_List attribute is displayed in the network routing-table display bgp - mask, mask-length - longer prefixes - output of the team. BGp display routing table 10.2.1.0 BGP local router ID : 4.4.4.4 Local NUMBER AS : 65010 Ways: 1 available, 0 best, 0 Select login information to BGP routing table 10.2.1.0/24: From: 10.1.4.1 (2.2.2.2) Duration: 0 Relay IP Nexthop: 0.0.0.0 Relay IP Out-Interface: Original nexthop: 10.1.1.2 zos Info : 0x0 AS-way Neal, Origin igp, MED 0, localpref 100, pref-val 0, internal, pre 255 Originator: 1.1.1.1 Cluster list: 0.0.0.0.1 Is not advertised to any peer, but this document applies to these Page 11 products Huawei uses machine translation in conjunction with human adjustment to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). HEALTH BGP provides rapid detection of link malfunctions to accelerate network convergence. When there is a malfunction on communications between BGP colleagues who have BGP tracking configured, BGP tracking can quickly detect peer inaccessibility and instruct the routing control module to notify BGP of a malfunction, achieving a rapid network convergence. Compared to BFD, BGP tracking is easy to set up because it only needs to be configured on a local device. BGP tracking is a mechanism for detecting faults at the routing level, while BFD is a mechanism for detecting faults on the link layer. The convergence of BGP routes on the network where BGP tracking is configured is slower than in the network where the BFD is configured. Thus, BGP tracking is not suitable for voice services that require rapid convergence. Figure 10-12, RouterA and RouterB, and RouterB and RouterC establish IGP connections. RouterA and RouterC establish peer-to-peer IBGP relationships. THE BGP is set up on RouterA. When there is an error in communication between RouterA and RouterB, IGP performs a rapid convergence. BgP tracking subsequently detects the route's inaccessibility to RouterC and notifies the BGP malfunction on RouterA, which then interrupts the BGP connection to RouterC. Figure 10-12 Network Tracking Chart BGP If establishing a relationship between peers IBGP requires IGP routes, and you need to set the interval between detecting peer inaccessibility and interrupting a connection. This interval should be longer than the IGP.co., huawei. time of convergence. Otherwise, before the IGP route slamming caused by the transitional interruption, the link between BGP's peer-to-peer communications may have been interrupted, causing unnecessary BGP convergence. This document applies to these Page 12 products Huawei uses machine translation in conjunction with a human proofer to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). BGP graceful restart (GR) are high-availability solutions that minimize the impact of device failures on user services. BGP GR ensures that the readmily plane continues to send a re-adhesive of data during the restart of the device or active/backup switching. Operations on the control plane, such as restoring peer relationships and calculating the route, do not affect the plane of re-entry. This mechanism prevents service interruptions caused by the slamming of the route and improves network reliability. The GR concept is: a GR rebooting device that is restarted by an administrator or caused by a glitch to perform a GR. A neighbor's GR assistant that helps the GR reboot to perform GR. GR is the time during which the GR assistant retains information about the readmilyst after discovering a reboot or active/backup switching GR reboot. The BGP GR process is this: using the BGP capability negotiation mechanism, gr-reboot and assistant, we know each other's GR capabilities and create a gr session. If you find a restart or an active/backup restart switch, the GR assistant waits for the BGP connection to be restored with the GR restart. It does not delete routing information or re-ad GR restart records or notify other neighbors of restart or switching. The GR restart restores neighbors' relationships with all GR assistants before GR expires. This document applies to these Page 13 products Huawei uses machine translation in conjunction with human correcting to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). Rapid IP redirection (FRR) is a method that implements a quick backup of a route. This allows the router to use the backup to rewind packages if the router detects a malfunction on the physical or data reference level. With IP FRR the router also reports a malfunction of routing the top layer of the layer In traditional IP networks, when an error occurs on the lower layer of the rewinding link, the physical interface on the router gets down. Once the router detects a malfunction, it informs the top routing system to recalculate routes and then update the routing information. Typically, it takes a few seconds for the routing system to re-select an available route. Second-level convergence is not acceptable for services sensitive to delay and loss of packages, as this can lead to a interruption in service. For example, Voice through Internet Protocol (VoIP) services are tolerated only for millisecond interruptions. IP FRR solves this problem by ensuring that the over-the-top system quickly detects a link malfunction and then uses the backup route to restore services as soon as possible. IP FRR, which is designed for routes in IP networks, is classified by IP FRR on public networks and IP FRR in private networks. IP FRR in public networks protects routers in public networks. IP FRR in private networks protects the edges of customers (CEs). IP FRR implemented as follows: If the main link is available, you can set up an IP FRR policy to provide information about the route of rewinding to the distillation engine. If the advanced engine detects a major connection malfunction, the engine uses a backup link to rewind traffic before the routes on the control plane converge. In the example shown in Figure 2-3, IP FRR is configured to improve network reliability. CE1 is a dual home for PE1 and PE2 and has two outgoing interfaces and the next two hops are configured. That is, Link B functions as a backup link A. When the link fails, traffic can be quickly switched to link B. Figure 2-3 IP FRR This document applies to these Products Page 14 Huawei uses machine translation in conjunction with a human proofer to translate this document into different languages to help you better understand the contents of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). The IP prefix list may contain several index records, each of which complies with the filtering rule. In figure 11-4, the system coincides with the routes on which the upstream number of indices is in order. If the route corresponds to the entry permit, this route is allowed. If the route corresponds to the denial of entry, this route is denied. If the route does not match any entry in the IP prefix list, this route is denied. Figure 11-4 Compliance with the principles of the IP Prefix List Route Of the IP List Rules includes: match, unique match, and deny by default. Consecutive match: Routes coincide with records in the order of the index's ascending number. If different numbers of indices are configured for multiple entries in the Ip prefix list, various filtering results can be obtained. Therefore, when setting up index numbers, be careful. Unique match: If the route matches one entry, it no longer tries to match other records. Ban by default: By default, all routes that do not match any entry are denied. Thus, once one or more denial records are created in the IP prefix list, one entry must be created to allow all other routes. One of the advantages of the IP prefix list over the ACL is that the routes can be comparable to their mask. The following example shows the ip-prefix command used to set up the list of iPv4 prefixes: ip-prefix ip-prefix-name - index-number - permission to refuse the length of the ipv4-address mask - the more-equal equal value - less equal value - less equal value - in this command, ipv4-address mask-length - more-equal value - less equal value - determines the network ID and the range of routes that should be filtered. Table 11-3 describes the parameters of this team. Table 11-3 Address Range in ip prefix Description of the ipv4 address defines the network ID. The length of the mask determines the length of the mask for the exact match. a more equal value indicates that the length of the mask should be larger or equal to the greater equal value. less equal to the equal value indicates that the length of the mask should be smaller or less equal to the equivalent value. When the filtering route corresponds to the network ID, the length of the mask can be accurate or within the specified length of the mask. If the team is not configured as more equal or less equal, the exact match is performed on the routes. That is, only routes coincide with the specified length of the mask. If the team is only more equal, the range of mask length used to match routes is a greater equal value, 32. If the team is only less tuned, the range of mask length used to map routes is mask length, less than equal value. If the team is configured to be both more equal and less equal, the range of length of the mask used to match routes is greater equal value, less equal value. You can use both ip and ACL prefixes as a route filter. ACLs can only match the network ID, but not the mask (the length of the prefix), but the list of IP prefixes is more flexible than the ACLs, because it can fit both the network ID and the mask, improving the accuracy of the route of conformity. The following two examples can help differentiate the list of ACL and IP prefixes. Figure 11-5 Using IP prefix list to filter import routes in Figure 11-5, SwitchB has two route, but only the static route 192.168.0.0/16 must be imported into OSPF. Check the IP SwitchB routing table. The team's next exit shows that it has two static routes 192.168.0/16 and 192.168.0.0/24. Now only route 192.168.0.0/16 must be re-announced in the OSPF. (SwitchB) IP display routing table Route flags: flags: - relay, D - download to fib ------------------------------------------------------------------------------ Routing Tables: Public Destinations : 6 Routes : 6 Destination/Mask Proto Pre Cost Flags NextHop Interface 10.10.12.0/24 Direct 0 0 D 10.10.12.1 Vlanif10 10.10.12.1/32 Direct 0 0 D 127.0.0.1 Vlanif10 127.0.0.0/8 Direct 0 0 D 127.0.0.1 InLoopBack0 127.0.0.1/32 Direct 0 0 D 127.0.0.1 InLoopBack0 192.168.0.0/16 Static 60 0 D 0.0.0.0 NULL0 192.168.0.0/24 Static 60 0 D 0.0.0.0 NULL0 First, use an ACL to meet this requirement. 1. Set up a basic ACL 2001. SwitchB acl 2001 (SwitchB-acl-basic-2001) rule allows source 192.168.0.0 0.0.255.5.5 255 SwitchB-acl-basic-2001 left The Node Node 10 in route-policy RP, to allow a route corresponding to the basic ACL 2001 and to deny all unrivalled routes. SwitchB route-policy RP permission of node 10 SwitchB-route-policy if-match acl 2001 SwitchB-route-policy to exit Import static route, permitted route-policy RP in OSPF. SwitchB ospf SwitchB-ospf-1 import-route static route-policy RP SwitchB-ospf-1 to come out After the completion of previous configurations, check the routing table IP SwitchC. <SwitchC> дисплей IP маршрутизации таблицы Маршрут флаги: R - реле, D - скачать на fib ------------------------------------------------------------------------------ Маршрутные таблицы: Общественные направления : 6 Маршруты : 6 Назначения / Маска Прото Предварительная стоимость флаги NextHop Интерфейс 10.10.12.0/24 Прямая 0 0 D 10.10.12.2 Vlanif10 10 .10.12.2/32 Прямая 0 0 D 127.0.0.1 Vlanif10 127.0.0.0/8 Прямая 0 0 D 127.0.0.1 InLoopBack 0 127.0.0.1/32 Прямая 0 0 D 127.0.0.1 BLoopBack0 192.168.0.0/16 O_ASE 150 1 D 10.10.12.1 Vlanif10 192.168.0.0/24 O_ASE 150 1 D 10.10.12.1 Vlanif10 Выход команды показывает, что два маршрута до 192.168.0.0 были импортированы. This is because in rule ACL 2001 the resolution source 192.168.0.0 0.255.255, 0.0.255.255 indicates the wildcard, but not the length of the mask. Once the wildcard is converted to a binary number, 0 indicates that the routes must match this ACL, while 1 indicates that the routes do not. For example, 192.168.0.0 0 0.0.255.255 determines the route prefix range: 192.168.0.0 to 192.168.255.255. The two routes are 192.168.0.0/16 and 192.168.0.0/24 both correspond to the ACL 2001. Thus, the two routes coincide with node 10 in the RP route policy and both are imported into OSPF. ACLs cannot guarantee that only Route 192.168.0/16 or 192.168.0.0/24 corresponds, because ACLs can only match the network ID, but not the mask. The following use the IP prefix list to filter imported routes. Check if the IP prefix list can ensure that route 192.168.0/16 is imported and route 192.168.0/24 Set up a list of IP huawei prefixes and set up Node 10 to allow route 192.168.0/16. The Huawei 10 ip-prefix 10 index allows 192.168.0.0 16 to customize the RP route and set up a 10 node to allow the route to be routed by the zlt/SwitchC.gt; meets the IP prefix list huawei and deny all unbeatable routes. The SwitchB route-policy RP permission node 10 SwitchB-route-policy if-match IP-prefix huawei SwitchB-route-policy to exit Import static route, permitted route-policy RP in OSPF. SwitchB ospf SwitchB-ospf-1 import-route static route-policy RP SwitchB-ospf-1 to come out After the completion of previous configurations, check the routing table IP SwitchC. The next team exit shows that only route 192.168.0.0/16 is imported into OSPF. <SwitchC> дисплей IP маршрутизации таблицы Маршрут флаги: R - реле, D - скачать на fib ------------------------------------------------------------------------------ Маршрутные таблицы: Общественные направления : 5 Маршруты : 5 Назначения / Маска Прото Предварительная стоимость флаги NextHop Интерфейс 10.10.12.0/24 Прямая 0 0 0 D 10.10.12.2 Vlanif10 10.10.12.2/32 Прямая 0 0 D 127.0.0.1 Vlanif10 127.0.0.0/8 Прямая 0 0 D 12 7.0.0.1 InLoopBack0 127.0.0.1/32 Прямая 0 0 D 127.0.0.1 InLoopBack0 192.168.0.0/16 O_ASE 6 150 1 D 10.10.12.1 Vlanif10 Технологический форум Huawei S Серия переключает маршрутизацию Политики Этот документ применяется к этим продуктам Страница 15 Huawei использует машинный перевод в сочетании с человеческим корректором для перевода этого документа на разные языки, чтобы помочь вам лучше понять содержание этого документа. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). This section describes BGP concepts that will help you better understand BGP's features. An autonomous system (AS) is a group of Internet Protocol (IP) networks that are controlled by one organization, usually an IsP, and have the same routing policy. Each AS is assigned a unique AS number that identifies AS on the BGP network. Two types of AS rooms are available: 2 AS rooms and 4 AS rooms. Number 2-byte AS ranges from 1 to 65535, and the number of AS 4-byte ranges from 1 to 4294967295. Devices that support 4-byte AS numbers are compatible with devices that support 2-byte AS numbers. Figure 10-1, BGP is classified into two types depending on where it operates: Internal BGP (IBGP) and External BGP (EBGP). Figure 10-1 BGP EBGP EBGP works between ASs. To prevent routing cycles between ASs, bgP discards routes with a local AS number when you receive routes from EBGP nodes. IBGP IBGP operates within AS. To prevent routing cycles in AS, BGP does not advertise routes extracted from peer-to-peer ibGP to other IBGP colleagues, and establishes full network connections with all colleagues Route Reflector and BGP Confederation are used to solve too many IBGP links between ibGP colleagues. If the BGP device needs to be advertised, it's a switchC. The route received from the EBGP peer outside AS through another BGP device, IBGP is recommended. There are two roles in BGP messaging: the speaker device that sends BGP messages is the BGP speaker. BgP receives and generates new routes, as well as touts routes to other BGP speakers. THE peer-to-peer BGP speakers that exchange messages with each other are a peer-to-peer BGP group. A group of BGP colleagues who share the same policies can form a group of peers. The BGP router ID is a 32-bit value that is often presented by the IPv4 address to identify the BGP device. It is carried out in an open message sent during the creation of the BGP session. When two BGP colleagues need to create a BGP session, each requires a unique router ID. This document applies to these Page 16 products Huawei uses machine translation in conjunction with human correcting to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). BGP uses authentication and a generalized TTL (GTSM) security mechanism to ensure the security of exchange between BGP colleagues. BGP authentication includes Message Digest 5 (MD5) authentication and key fob authentication, which improves communication security between BGP colleagues. In MD5 authentication, you can only set an authentication password for a TCP connection. When you authenticate a key fob, you can set the authentication password to connect to TCP and verify the authenticity of BGP messages. BGP GTSM checks whether the time for life (TTL) is in the IP package header in a predetermined range. It allows or discards packages with TTL values beyond the predetermined range to protect services above the IP level. BGP GTSM improves system security. Suppose the range of TTL values from BGP peers is set at 254-255. When an attacker forge actual BGP packages and continues to send these packages to attack the device, the TTL values of these packages are less than 254. If BGP GTSM is not enabled on the device, the device detects that these packages are for itself and sends packages into the control plane for processing. The level of control must then handle a large number of such attack packages, causing high CPU usage. If BGP GTSM is enabled on the device, the system checks TTL values in all BGP packages and discards attack packages with TTL values less than 254. This prevents the use of packages attacks on CPU resources. This document applies to these products Page 17 Huawei uses machine translation in conjunction with a human proofer to translate this document to another other to help you better understand the contents of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). You must enable RIP before any RIP configurations are performed. The RIP configurations in the interface view will not take effect until RIP is enabled. You run the system view Display system. Running Rip (process-id) - vpn-instance vpn-instance-name RIP is on, the RIP process is created, and the RIP view is displayed. If you specify a VPN, the RIP process belongs to that VPN. If you don't specify a VPN, the RIP process belongs to a public network instance. (Optional) This document applies to these Page 18 products Huawei uses machine translation in conjunction with human correcting to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). OSPFv3 supports multiple processes on the switch. These processes are differentiated by andD processes. The process ID is set when OSPFv3 is turned on and is only only locally valid. This does not affect the exchange of packages with other switches. A router ID is a 32-bit unsigned integer that uniquely identifies the switch in AS. This is expressed in the IPv4 address format. The OSPFv3 router's ID version must be manually installed. If the router ID is not installed, OSPFv3 cannot function properly. Make sure the iD memory of the switch router in AS is all different. When you turn on multiple processes on the switch, specify a unique route ID for each process. Plan your router's IEDs and set them up manually to ensure OSPFv3 works smoothly. Here's what you do on the switch that works OSPFv3. You run the system view Display system. Launch ospfv3 - process-id - vpn-copy vpn-name - OSPFv3 is enabled, and the OSPFv3 view is displayed. The router-ID router-ID router ID is installed. When you set up your router ID, make sure your router ID is unique in AS. You can choose the IP address of the interface as a router ID. If the router's ip addresses contradict the OSPFv3 process, routers can't establish relationships between OSPFv3 neighbors, and routing information If there is a router ID conflict, do one of the following: Reconfiguring the router ID. Run undo ospfv3 router-ID automatic recovery disable command to turn on the switch to automatically change the conflicted router router ID your own IP address. After the automatic recovery of the ospfv3 router is automatically restored, a conflicting router ID will be launched. After the router ID is changed, if the new router ID still conflicts with the other, the switch can reconfigure one maximum three times. This document applies to these Page 19 Huawei products uses machine translation in conjunction with human correcting to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). You run the system view Display system. You run ospf - process-ID-router-id-id-vpn-instance vpn-instance-name - osPF process is launched, and the OSPF view is displayed. You'll run the frr Displayed OSPF IP FRR view. Running without a series of alternative OSPF IP FRR is enabled to create a non-loop backup link. This feature is disabled by default. OSPF can only create a back-up link when the OSPF IP FRR traffic protection disparity is satisfied. In the following description, the Distance_opt (X, Y) indicates the shortest link from X to Y. S means the original node, E for the faulty node, N for the backup link and D for the destination node. Link protection takes effect when traffic that is protected flows through the specified link and the cost of communication corresponds to inequality: Distance_opt (N, D) zlt; Distance_opt (N, S) and Distance_opt (S, D). The site and link protection takes effect when traffic that is protected flows through the specified link and nodes, and fulfills the following conditions: communication costs correspond to inequality: Distance_opt (N, D) zlt; Distance_opt (N, S) and Distance_opt (S, D). The cost of the interface is in line with the inequality: Distance_opt (N, D) zlt; Distance_opt (N, E) and Distance_opt (E, D). The static low-science Loop-Free Alternates (LFA) algorithm is used to calculate the next and outgoing interfaces for backup links. The next and outgoing interface of the free OSPF backup link can be obtained using any of the following methods: for static backup links, after the IP FRR is enabled with the ip frr command in the presentation of the system or the presentation of a VPN instance, set up the nexthop and outgoing interface for static backup links. For dynamic backup, once the OSPF IP FRR is enabled with an alternative team cycle, allow the device to use the LFA algorithm to calculate the next and outgoing interface for dynamic backup By default, static backup links prefer dynamic backup links when choosing a route. However, static backup links are less flexible than dynamic backup links. If a link fails, static backup links Update automatically, but dynamic backup links can. So to provide an automatic link update, run a frr-priority static low command to allow dynamic backup links to take precedence over static backup links, so that the LFA algorithm is used to calculate the nexthop and outgoing interface. (Optional) The frr-policy route-policy of the ROUTE-policy of the NAME OSPF IP FRR route is set up. Once the OSPF IP FRR filtering policy has been set up, only OSPF backup routes that meet the filtering conditions can be delivered to the distillation table. To protect traffic along a specific OSPF route, you can set up a filtering policy that matches the OSPF route to ensure that the route can be added to the distillation table. If this route fails, OSPF can quickly switch traffic to a backup link. This document applies to these Page 20 Huawei products uses machine translation in conjunction with a human proofer to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). The restart of the IS-IS switches causes the network to rupture temporarily as the adjaction relationship between the switch and its neighbor has been demolished. Switch LSPs are removed, making the route calculation inaccurate. Thus, the packages are lost. You can set up IS-IS GR to solve this problem. After turning on IS-IS GR, the switch notifies the neighbor of the restart status and restores the adjaction relationship with its neighbor without interrupting the redirect. The GR interval is set as Holdtime in IS-IS Hello PDU. Thus, the adjaction ratio is not ripped off when the switch restarts. You run the system view Display system. You run isis - process-id - displayed the view of IS-IS. Running a graceful IS-IS GR reboot is on. Is-IS GR is disabled by default. Running a graceful reboot without the impact of holding Neighbor's retention time IS-IS is set to stay unchanged in IS-IS GR mode. (Optional) You run a gracefully restarting interval value set up for the T3 timer during IS-IS GR. The T3 timer indicates the longest time gr lasts. The router disables the T3 timer after the LSDB sync is over in all areas. If the LSDB is not yet in sync after the T3 timer expires, GR fails. The default T3 timer is 300 seconds. It's a good idea to keep the default. During GR Neighbor IS-IS sets the T3 timer value for the time of the hold of the neighboring relationship between them, which prevents the recalculation of routes as a whole due to a neighbor's outage during GR. (Optional) Running a graceful reboot of Suppression-sa Restart GR is set to suppress suppression-advertising (SA) a bit of a TLV reboot. By default, the SA bit is not suppressed. You will launch the display isis gracefully-reboot status - level-1, level-2 - process-ID, vpn-copy-copy-name- team to check the status of IS-IS GR. This document applies to these Page 21 Huawei products uses machine translation in conjunction with a human corrector to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). Creating an S-IS process is a prerequisite for an IS-IS configuration. You run the system view Display system. You run isis - process-id - creates an IS-IS process, shows the representation of the IS-IS process. The process ID defines the IS-IS process ID. Process ID 1. (Optional) Provide a description Description For the IS-IS process set up. (Optional) Turn on IS-IS to add POI and host name TLV to clean LSPs. Running clearing-creator-identification allow always - IS-IS has the ability to determine whether to add a POI TLV and a host name TLV to clean LSPs based on the authentication configuration. If the initiator-identification team is up and any authentication is configured, LSPs Purge generated does not carry a POI TLV or a TLV host name. If the initiator-identification team is up and the authentication is not configured, LSPs Purge generated carry a POI TLV or a TLV host name. If the re-in-identification cleaning setup always works, LSPs Purge generated carry POI TLV and host name TLV, regardless of whether the authentication is configured. This document applies to these Page 22 products Huawei uses machine translation in conjunction with a human proofer to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). Creating IS-IS processes is a prerequisite for IS-IS configurations. You run the system view Display system. You run isis - process-id - vpn-instance vpn-instance-name - created the PROCESS IS-IS, displayed a representation of the IS-IS process. The process ID defines the IS-IS process ID. If The process is not Process identifier 1 by default. To link the IS-IS process to a VPN instance, please provide the name of a VPN instance. (Optional) Description of the LaunchInscript Description is set up for the IS-IS process. (Optional) Turn on IS-IS to add POI and host name TLV to clean LSPs. Running clearing-creator-identification allow always - IS-IS has the ability to determine whether to add a POI TLV and a host name TLV to clean LSPs based on the authentication configuration. If the creator-identification cleaning team is up and the send-only option is specified when you set up the authentication, the LSPs Purge generated does not carry a POI TLV or a TLV host name. If the initiator-identification cleaning team is up and running MD5 or HMAC-MD5 authentication, LSPs Purge generated do not carry POI TLV or host name TLV. If the initiator-identification cleaning team is up and running and is configuring another type of authentication or is not configured authentication, the LSPs generated by Purge carry POI TLV and the TLV host name. If the identification of the cleaning originator always allows you to perform, LSPs Purge generated carry POI TLV and host name TLV, regardless of whether the authentication is configured or the option is only sent when the authentication is set up. This document applies to these Page 23 Huawei products uses machine translation in conjunction with a human proofer to translate this document into different languages to help you better understand the contents of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). This document applies to these Page 24 products Huawei uses machine translation in conjunction with a human proofer to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). This document applies to these Page 25 products Huawei uses machine translation in conjunction with a human proofer to translate this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). This document applies to these page 26 products Huawei uses machine translation in conjunction with adjust the translation of this document into different languages to help you better understand the content of this document. Note: Even the most advanced machine translation cannot match the quality of professional translators. Huawei is not responsible for the accuracy of the translation, and it is recommended to refer to the English document (the link to which was provided). This document applies to these products cisco ios xe ip routing ospf configuration guide