Chapter 5
Outbound Link Load Balancing (LLB)

Training Team

HCSA-ADC Official Training

Integrative Cybersecurity

Visionary. AI-powered. Accessible.

Background Introduction

- With the rapid development of the internet, there is an increasing demand for internet access in various industries, and higher requirements for network quality and stability. The bandwidth limitations and unstable factors of single-operator links can no longer meet user needs, and single-operator links are gradually being replaced by multi-operator and multi-links.
- However, multi-operator and multi-link connections face new problems:
  - when internal personnel of an organization browse the internet, they inevitably encounter latency issues when accessing across different operators. Some users may access telecom resources but end up accessing them through Unicom links, resulting in poor access speed and stability. On the other hand, it is difficult to fully utilize multiple links deployed by the organization, and there are often situations where the telecom link is very busy while the Unicom link is idle, leading to resource waste.

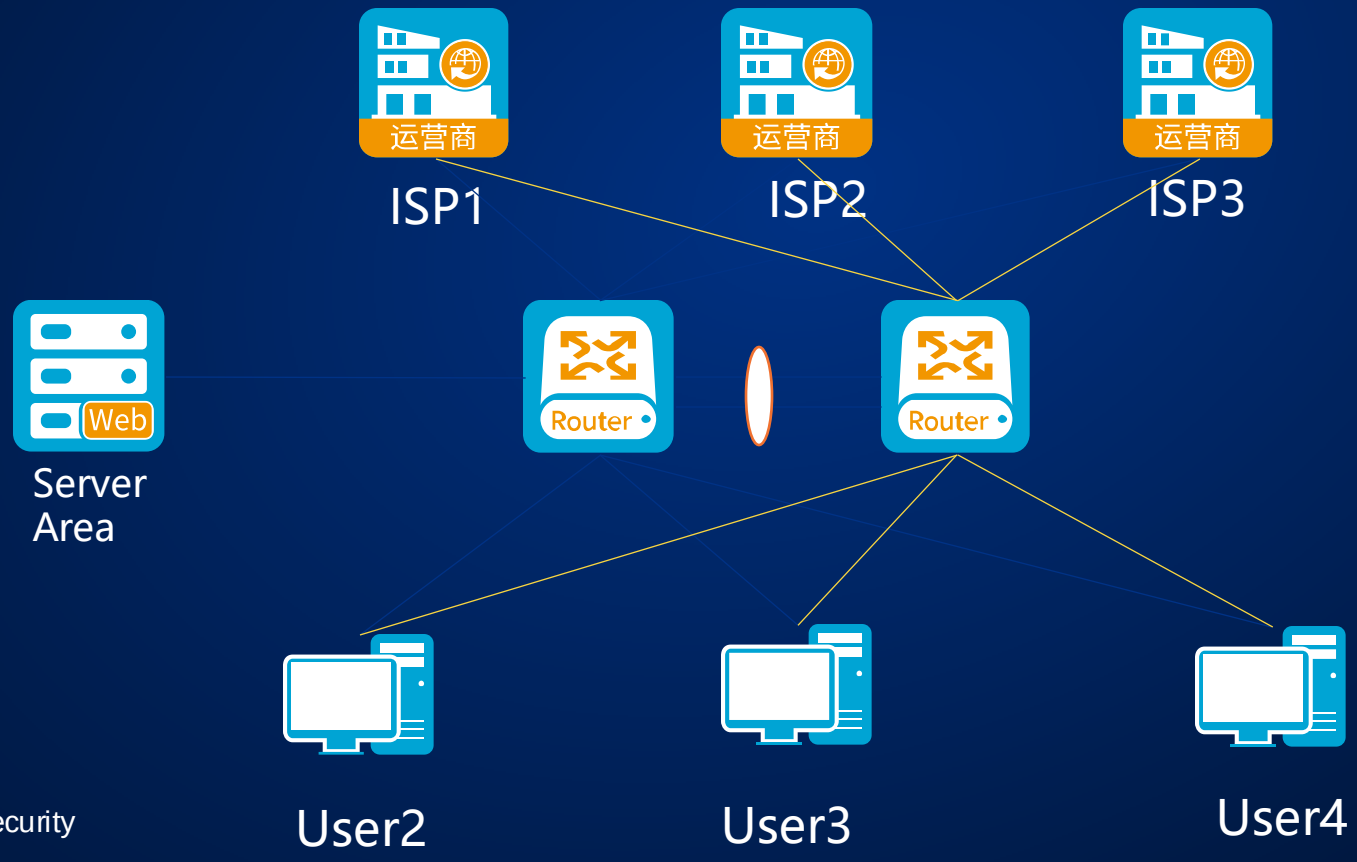
Agenda

- LLB Application Scenario
- LLB Implementation

1 LLB Application Scenario

Application Scenario

With the rapid development of the internet, operators, broadcasting and television entities, universities, government, and enterprises have gradually become important broadband service providers, offering internet access services to a large number of users. These three types of customers share many common characteristics and needs in the management of network traffic.



Network Features and Requirements

Network Features

- Huge number of users and complex Internet traffic: As a broadband provider, it carries a large number of Internet users, and users have different Internet habits, and various application traffic is mixed.
- Using multiple exit links: To balance the purchase cost and link quality, multiple exit links with different operators, different bandwidths, and different quality are often introduced.
- Control operating costs and ensure user experience: In order to ensure profitability, it is necessary to balance cost and experience, and ensure users' online experience to the greatest extent while reasonably controlling cost investment.

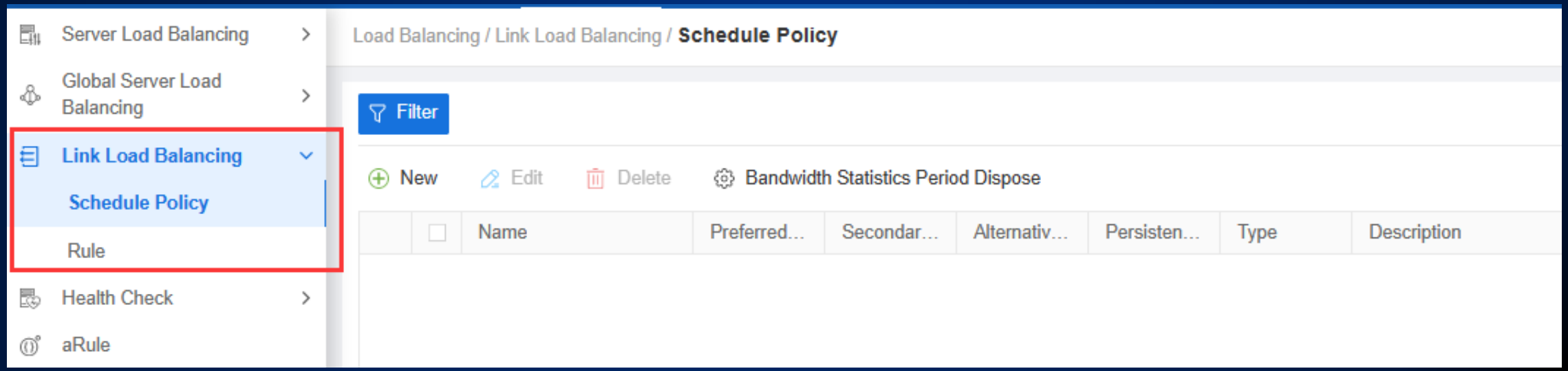
Management Needs

- Application level dynamic management - we must make full and reasonable use of the resources of each exit link, and dynamically adjust the traffic forwarding strategy according to the different link states and applications, so as to achieve better link balancing effect.

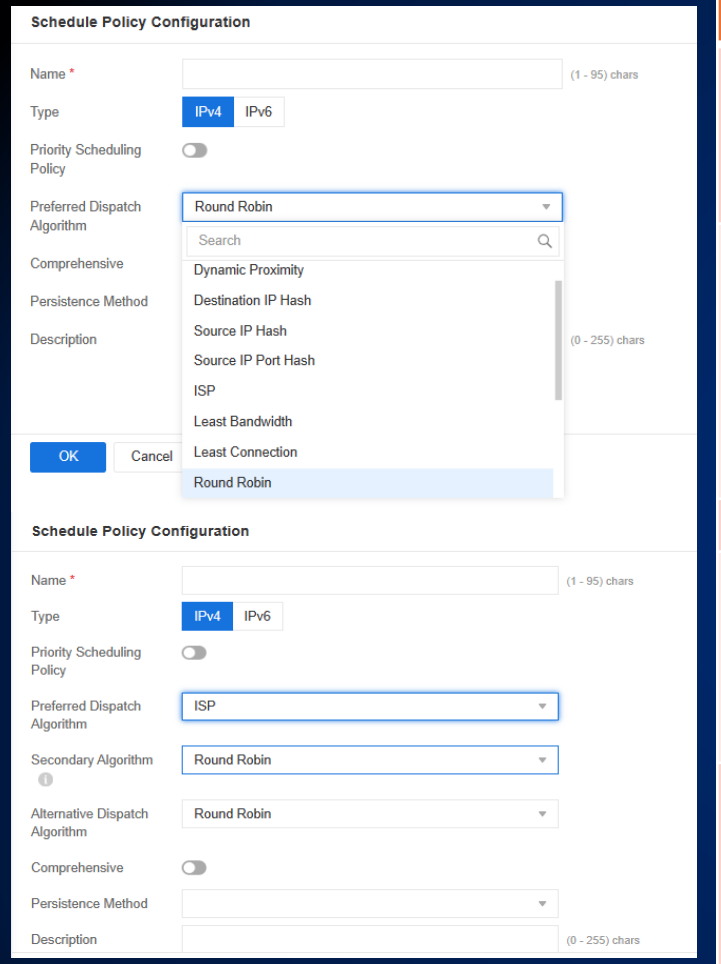
2 LLB Implementation

Link Load Balancing

- The configuration of link load balancing can be divided into rules and schedule policies:
  - Schedule policy: configuring balancing algorithms, and session persistence, etc.;
  - Rule: apply scheduling policies and configuring routing related settings.

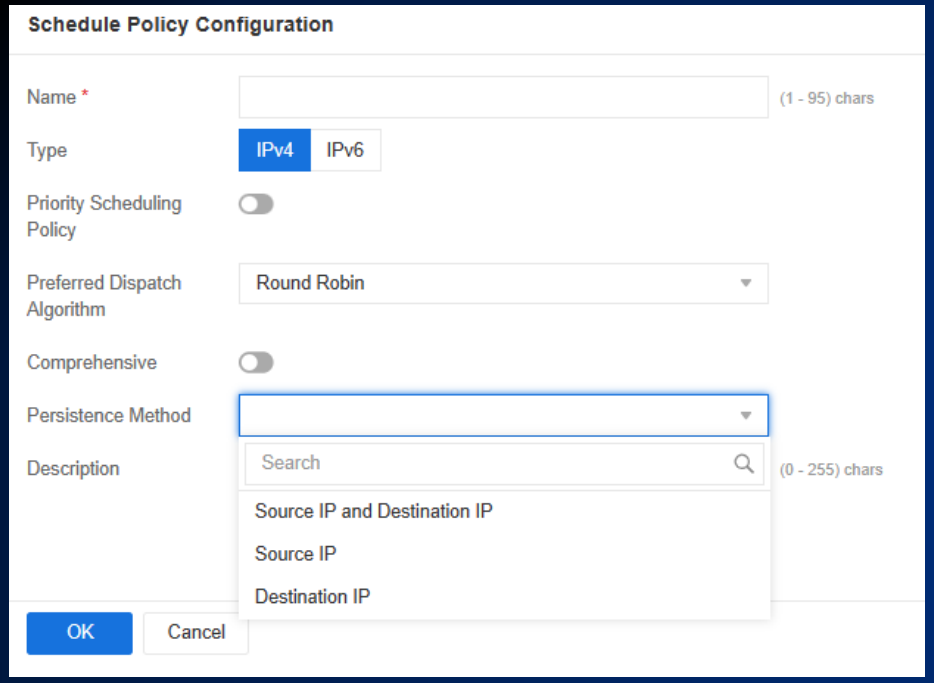


Schedule Policy



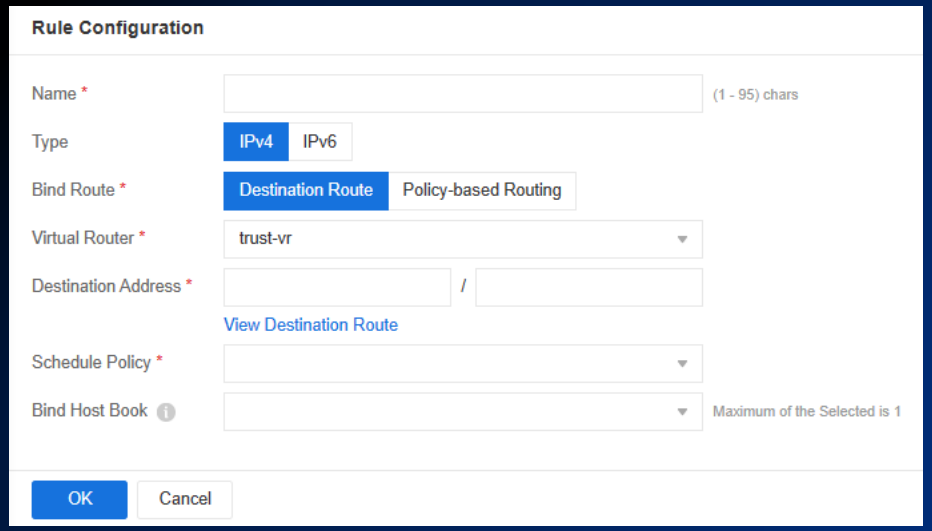
Balancing Algorithm	Descriotion
Round Robin/Weighted Round Robin	The client's requests/connections are scheduled in turn to each available link. Weighting simply means that different links have different weights, with larger weights having a greater chance of being scheduled. For example, if link 1 has a weight of 50 and link 2 has a weight of 100, then when sufficiently balanced, the probability of scheduling to link 2 is twice that of link 1. Weight is configured on the router.
IP Hash/Weighted IP Hash	Hash value is calculated based on the source IP/destination IP, and the link is selected based on the hash value. When the number of source IPs/destination IPs is small, the calculated hash value changes little, which may result in an unbalanced schedule. As the number of source IPs/destination IPs increases, the range of hash value changing becomes larger, gradually achieving balance. When session persistence is not configured and there is no link state change, all requests from a source IP/destination IP can be scheduled to the same link. However, when there is a link state change, all requests will be scheduled to the new link, breaking the client's stickiness to the previous link. The larger the weight is, the greater the probability of being scheduled.
Least Connection	Schedule requests/connections to the link with the minimum number of connections.
Least Bandwidth/Weighted Least Bandwidth	The device will record the upstream bandwidth, downstream bandwidth, or total bandwidth of upstream and downstream on each link. When new outbound traffic arrives, the device will choose the link with the minimum bandwidth or minimum total bandwidth to forward the traffic. Weight is configured in Router, and the larger the weight is, the more opportunities for scheduling. The total bandwidth will be proportionally distributed to each link according to their weight, and business requests will be forwarded to each link for processing.
ISP	It will match the destination address of the traffic with the ISP information of the system and select the route based on the matching result. After the ISP algorithm is selected, there will be a secondary algorithm and a backup balancing algorithm. The secondary algorithm: When there are multiple links within the same operator, the ISP algorithm cannot select a specific link, so the secondary algorithm is used to balance the multiple links within the same operator. The backup balancing algorithm: When the destination address of the business request (e.g., Ali Cloud address) cannot be matched with the ISP information database of the operator, the backup balancing algorithm is used to select an available link to ensure normal business forwarding.

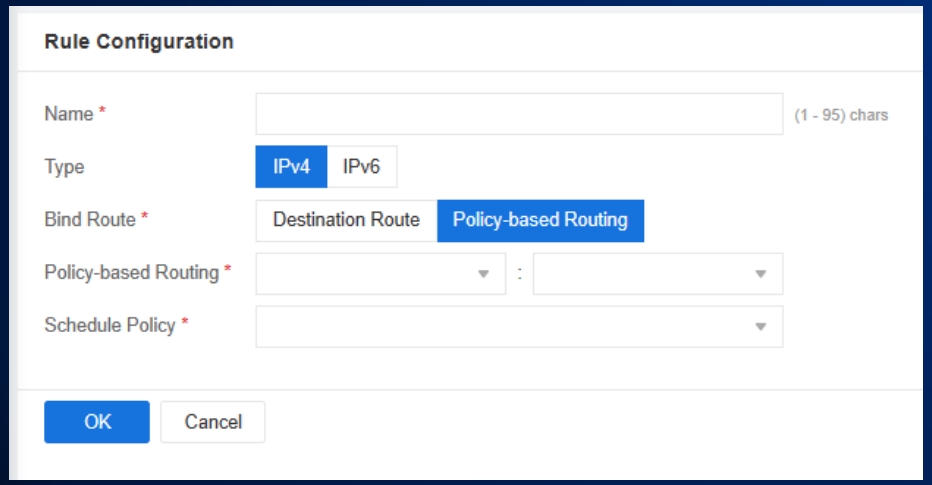
Schedule Policy – Session Persistence



Session Persistence	Description
Source IP and Destination IP	Establish session persistence table entries based on the client address and the destination address of the requested business, to ensure that requests from the same client to the same destination are allocated to the same link, preventing interruptions in different businesses due to load balancing across different links.
Source IP	Establish a session table based on the source IP address to ensure that requests from the same source IP are allocated to the same link, preventing interruptions in business due to scheduling across different links. Note: If there is a device doing SNAT in front of the ADC device, it may result in few source addresses. In this case, using source address session persistence may lead to uneven link distribution.
Destination IP	Establish a session table entry based on the destination address of the request, to allocate subsequent requests to the same destination address to the same link.
Timeout	The timeout of the session persistence table, after the timeout, the session persistence will no longer take effect, and new requests will be scheduled again based on the load balancing algorithm.

Rule





Options	Description
Schedule Policy	Call the configured schedule policy
Bind Route	ADC supports to binding destination route and policy-based route. Destination route requires specifying the virtual router to which the destination route belongs and the segment of the destination address. Note that the network segment of the destination address needs to be the same as the segment of the ECMP route in the routing module. If the segment of the address is different, it will result in the inability to hit the LLB process. Policy routing involves binding LLB to policy based route and corresponding rules. The link load balancing function is only effective when multiple links are available. If two links are used for load balancing and one of them goes down, the link load balancing function will be disabled. Once the link is restored, the link load balancing will be resumed. Fine-grained control can be achieved by creating LLB rules by using policy based routing, such as based on application, service, domain, etc.

Link Busy Protection

- "Link Busy Protection" is designed to address the issue where strict adherence to scheduling algorithms can lead to a deteriorating link and ultimately poor user experience due to factors such as large flows or significant traffic fluctuations. Here are a few common examples:

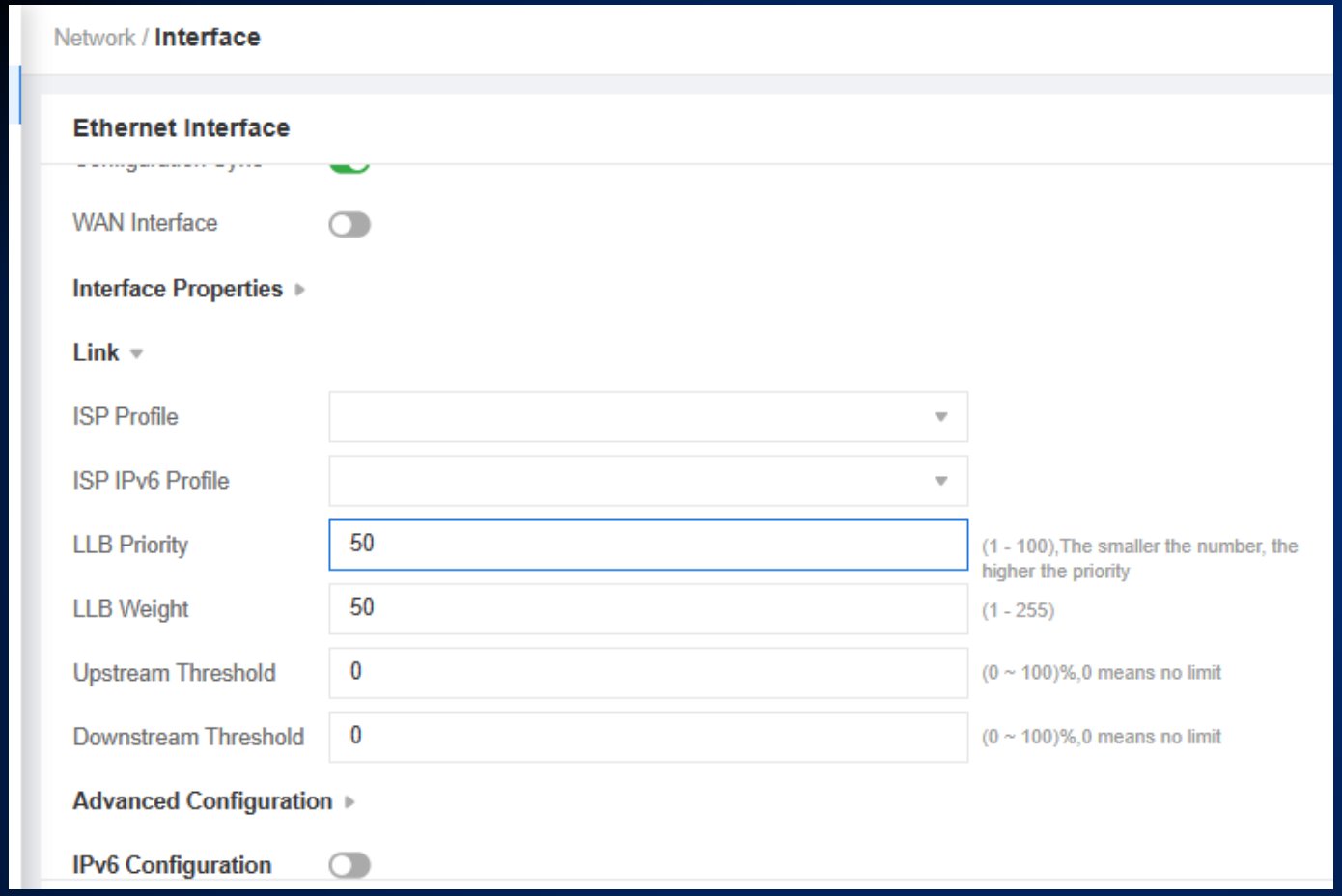
  - Example 1: Suppose there are two links from the same operator, referred to as Link 1 and Link 2, with equal bandwidth and quality. These links use round-robin scheduling for traffic distribution. Without considering session persistence, new sessions are sequentially scheduled on Link 1 and Link 2. However, during a certain period, several sessions on Link 1 generate particularly large traffic, causing high utilization of Link 1, while Link 2 remains relatively idle. If traffic distribution still follows round-robin scheduling, the user experience for sessions on Link 1 will be very poor.

  - Example 2: In a backup link scenario, after all active links are heavily utilized, if traffic continues to be scheduled according to the scheduling algorithm, high-priority links will be heavily loaded while low-priority links remain idle, resulting in a poor network experience.

- By configuring link busy protection, it is possible to effectively avoid situations where some links are heavily utilized while others remain idle. When link utilization exceeds a certain threshold, new connections will not be scheduled on the busy link until the utilization falls below a certain threshold.

- To configure link busy protection, set the uplink and downlink thresholds in the network -> interface -> link configuration. The threshold is the critical point that triggers link busy protection, and new business will no longer be distributed to the link once bandwidth utilization exceeds the threshold.
- Note: link busy protection requires configuring the uplink and downlink bandwidth to match the actual business bandwidth to avoid wasting customer bandwidth or overloading the device.

Link Busy Protection Configuration

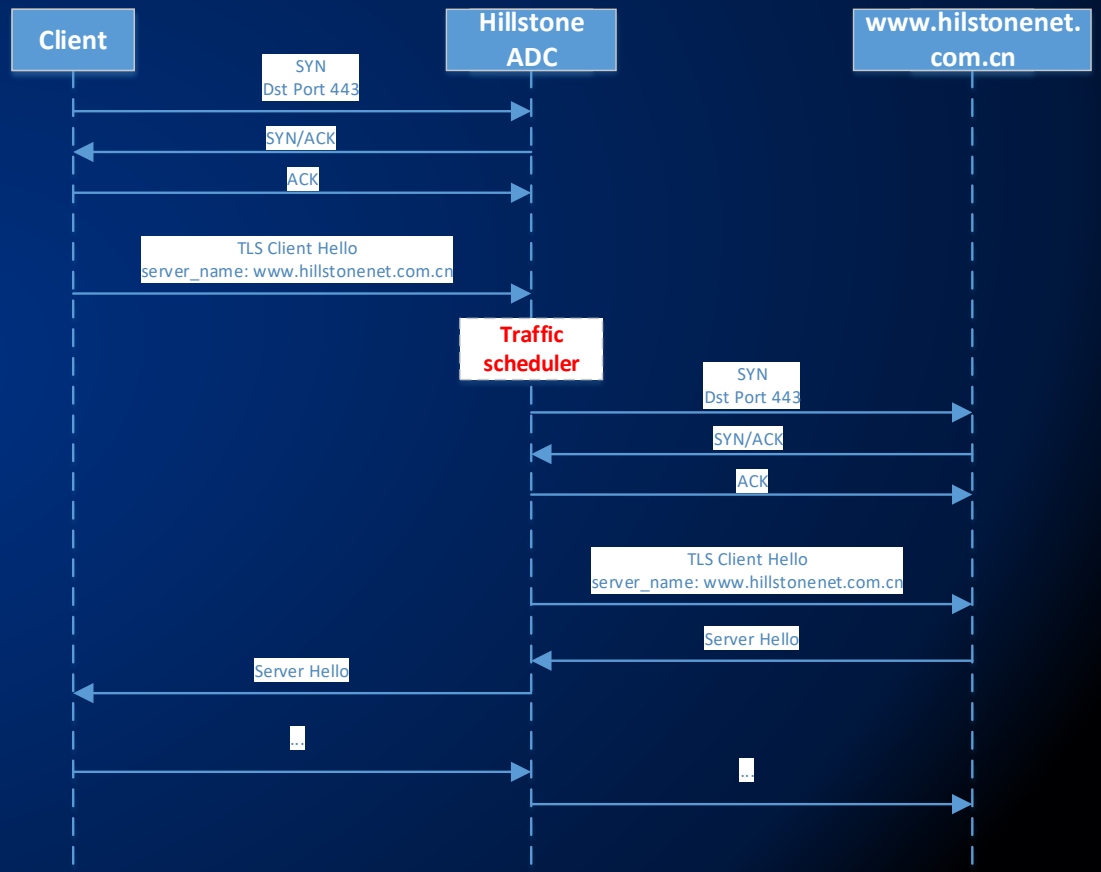


Domain Name based Load Balancing – Other Venders' Solution

- Competitor Vendor plan one: Translate domain names into IP addresses
  - Principle: This plan is easy to understand. When configuring traffic scheduling policies, the domain name is translated into an IP address for policy issuance, and the domain name is periodically resolved. When there are changes, the scheduling policy is updated. The implementation is relatively simple.
  - Shortcoming 1: Many websites are published through CDN or have multiple ISPs access, resulting in many IP addresses. The IP address resolved by the client is highly likely to be inconsistent with the IP address resolved by the gateway, resulting in inaccurate policy issuance, which may lead to traffic scheduling based on domain names for some clients.
  - Shortcoming 2: Since the IP address resolved by the gateway often changes, frequent updates to the scheduling policy will incur high system overhead to rebuild the system's scheduling policy table. If session rematch needs to be done in certain scenarios, it may have catastrophic consequences for the system, greatly increasing the instantaneous load on the system, and in severe cases, may affect normal traffic forwarding due to high system load.
- Competitor Vendor plan two: Translate domain names into IP addresses with DNS traffic sniffing
  - Principle: This plan is an evolution of the above plan, partially addressing the shortcomings of plan one. This plan does not use the DNS module to resolve the domain name but translates the domain name into an IP address by sniffing the DNS query response message passing through the gateway device.
  - Shortcoming 1: In some scenarios, there are multiple WAN gateway accesses, and some clients' DNS requests do not pass through the gateway, so it is impossible to obtain the client's DNS traffic and translate it.
  - Shortcoming 2: In practice, there are many situations where a domain name corresponds to a large number of IP addresses. It is common for many large websites to resolve several dozen or even hundreds of IP addresses. This requires the gateway to record all the IP addresses corresponding to these domain names. When there are many target websites, the system's memory overhead will be relatively large. When there are too many domain names, it may lead to the problem of being unable to translate correctly due to insufficient capacity.
  - Shortcoming 3: Most importantly, Shortcoming 2 of plan one still exists. Whenever the IP address corresponding to this domain name changes (increases or decreases), it is necessary to re-issue and construct the scheduling policy table.

Domain Name based Load Balancing – Hillstone's Solution

- Hillstone Solution: Access through proxy, as shown on the right:
  - Hillstone Network's ADC modifies the normal session creation process and does not perform traffic scheduling when receiving SYN packets. For HTTPS traffic, after seeing the Client Hello, the server_name in the TLS extension can be viewed, which identifies the domain name which is being accessed, allowing for more natural domain-based traffic scheduling.
  - For HTTP web traffic, the processing principle is similar to HTTPS; HTTP traffic needs to obtain the domain name information through the Host field in the request, while HTTPS traffic obtains the domain name information through the server_hello extension in the TLS Client Hello.
  - After obtaining the domain name, ADC obtains the corresponding IP address from the configured DNS server, and then retrieves the client request content and returns it to the client.



Hillstone NETWORKS

Integrative Cybersecurity

Visionary. AI-powered. Accessible.

+1 408 508 6750
inquiry@hillstonenet.com
5201 Great America Pkwy, #420
Santa Clara, CA 95054
www.hillstonenet.com