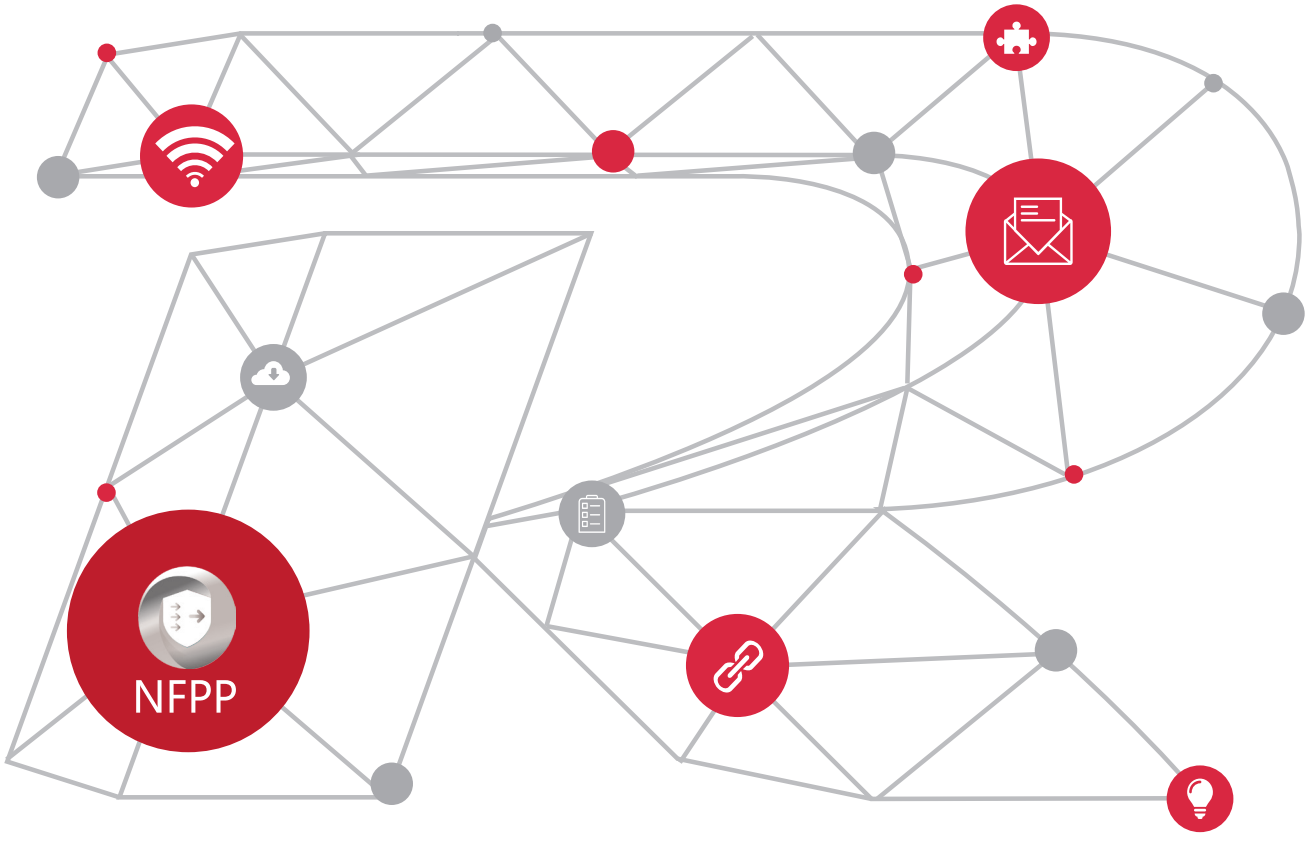
Ruijie Network Foundation Protection Policy

White Paper



Contents

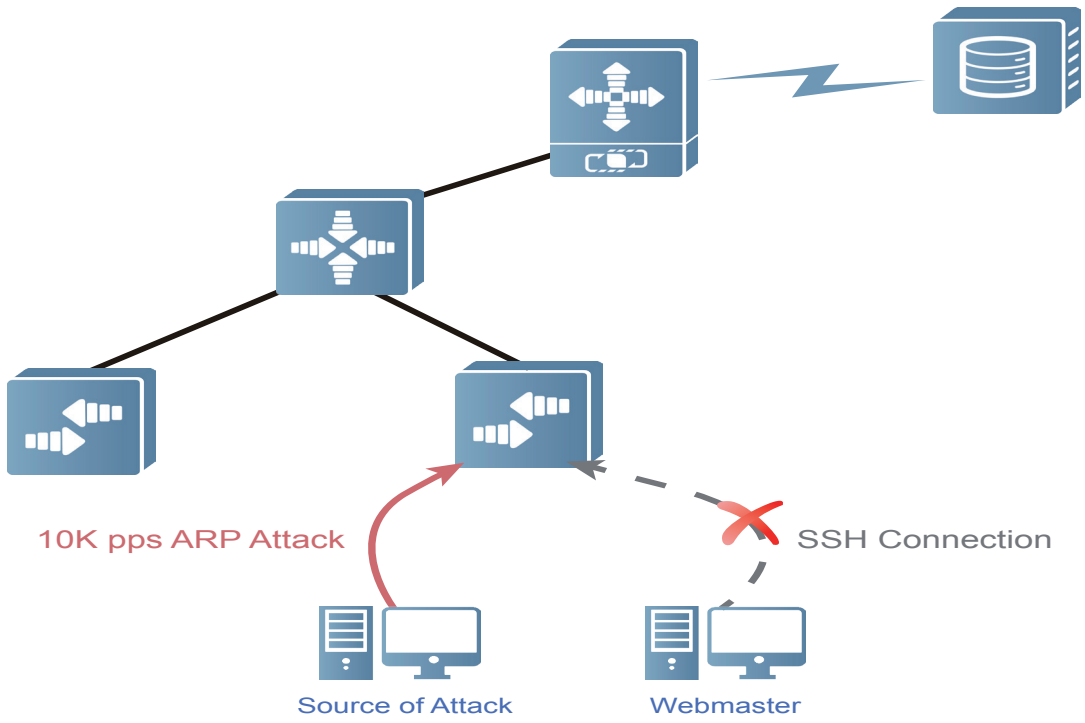
Introduction

The Network Foundation Protection Policy (NFPP) is a protection system for enhancing the anti-attack capability of a switch. When a switch encounters malicious attacks, NFPP employs a series of countermeasures, such as rate-limiting, identifying, and isolating the attack source, to ensure the normal control and management flows of the system, thereby protecting the computing and channel resources of the switch CPU.

• Attack Types Defended Against by NFPP

A network frequently encounters malicious attacks, among which one type of attacks causes excessive CPU usage of the switch and occupies much bandwidth of the CPU packet channel. Consequently, the CPU improperly processes the control and management flows and the switch system works abnormally.

Figure 1 uses the ARP attack as an example.



When the access switch receives specific ARP packets from the attack source at a rate of 10,000 pps, the packets are sent to the CPU through the CPU input channel. This process consumes a great number of computing resources; as a result, the Webmaster fails to connect to the device due to a denial of service (DoS).

Figure 1 shows a typical attack example of Webmaster crash caused by switch CPU overload. Similarly, the switch involves multiple types of packet flows destined for the CPU. These packet flows are generally controlled by the CPU and produce a small data throughput. According to RFC 3746, the control and forwarding planes of the switch are separated. On the forwarding plane, the sending and receiving of data flows are implemented by the ASIC chip, which features a large throughput. On the control plane, protocol interaction is processed and the operation of the forwarding unit is controlled. Logically, the switch is divided into the data plane, management plane, and control plane in terms of functions.

Table 1 describes functions of the preceding three planes.

Table 1: Functions of the Preceding Three Planes

Logical Plane	Function	Typical Data Flow
Management plane	Provides the network administrator with a management interface in Telnet, Web management, or SSH mode.	IPv4 or IPv6 packets with the destination IP address being the IP address of a local device
Data plane	Forwards data using the ASIC chip, instead of transmitting packets to the CPU.	Unknown IPv4 or IPv6 multicast packets, IPv4 or IPv6 packets with the destination IP address being the IP address of a non-local device, and non-IP packets
Control plane	Controls and manages the operation of all network protocols, enabling the switch to understand and maintain the devices, links, and interaction in the network.	The network protocols include but are not limited to: RLDP, RERP, BPDU, ISIS, DHCP, GVRP, RIP (ng), IGMP, MPLS, OSPF (v3), PIM (v6), and VRRP.

From the logical perspective, NFPP defends against attacks on the management plane and control plane, because the packets on the two planes are processed by the CPU and involve the occupation of the CPU input channel bandwidth and computing resources. When malicious attacks occur on the two planes, much bandwidth of the CPU input channel is occupied, leading to the loss of non-attack packets. At the same time, a great number of resources (such as the memory, clock cycle, and computing unit) are consumed to process the attack packets, leading to flapping or DoS of the management and control flows and seriously affecting the switch work. Table 2 describes the typical attacks.

Table 2: Typical Attacks on the Control Plane and Management Plane

Attack Type	Attack Means	Impact
ARP	The attack source sends a great number of invalid ARP packets to the gateway.	The gateway incurs a DoS to normal ARP flows.
IP scanning	The attack source sends the scanning attack packets with changing destination IP addresses to the switch at a high speed, such as the Blaster virus.	The IP packets with the unknown destination IP address need to be transmitted to the CPU for processing ("one-time routing" process of the switch), causing overload of the CPU routing module.
ICMP flooding	The attack source sends an ICMP echo request to the switch for an echo reply.	Excessive ICMP requests lead to the huge consumption of CPU resources.
DHCP depletion	The attack source broadcasts DHCPv4 or DHCPv6 requests with forged the MAC addresses.	The DHCP service addresses of the switch may quickly be depleted in the case of a great number of requests with forged addresses, and the switch fails to respond to the requests with normal IP addresses.
ND	The attack source sends a great number of neighbor discovery packets.	The switch load incurred from IPv6 address resolution, route discovery, prefix discovery, and redirection bursts leads to enormous resource consumption.

Besides the attack means listed in Table 2, the attack packets on the control plane and management plane occur in various other forms and means.

• Existing Industrial Anti-attack Functions

Currently, the industry emphasizes the security of switches and launches a variety of anti-attack functions, such as ACL, QoS, uRPF, SysGuard, and CPP. These anti-attack functions are decentralized, and do not form a unified system framework, or integrate resources for the locating and advertisement of attack sources and scheduling of isolation and locating time. For example, the ACL is used for isolation, and the QoS is used for rate limiting. In this case, the existing anti-attack functions can hardly provide comprehensive and systematic protection in the attack scenarios, and may confuse users due to complex configuration.

• Anti-attack Mode of Ruijie NFPP

To defend against attacks on the control plane and management plane, NFPP builds a complete and multi-dimensional network foundation protection system for the switch, covering attack identification and advertisement, rate limiting on specific packet flows, and attack isolation. NFPP has the following features:

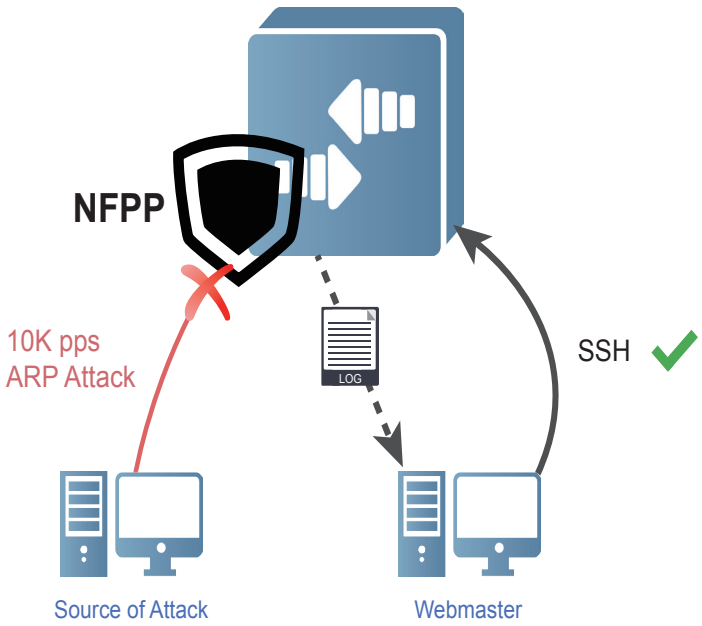
* **Supports the integrated defense with attack identification, bandwidth rate-limiting, and attack isolation.**

* **Supports multiple types of basic attack flows and customizes attack packet types.**

* **Provides convenient management and an attack alarm mechanism; adjusts the isolation and identification periods as required; and supports configuration of the blacklist, whitelist, and privileged users.**

* **Supports the sequential and rate-limited packet dispatching, and allocates the bandwidth for different service types by weight to ensure normal running of high-priority services.**

Figure 2: NFPP Anti-attack

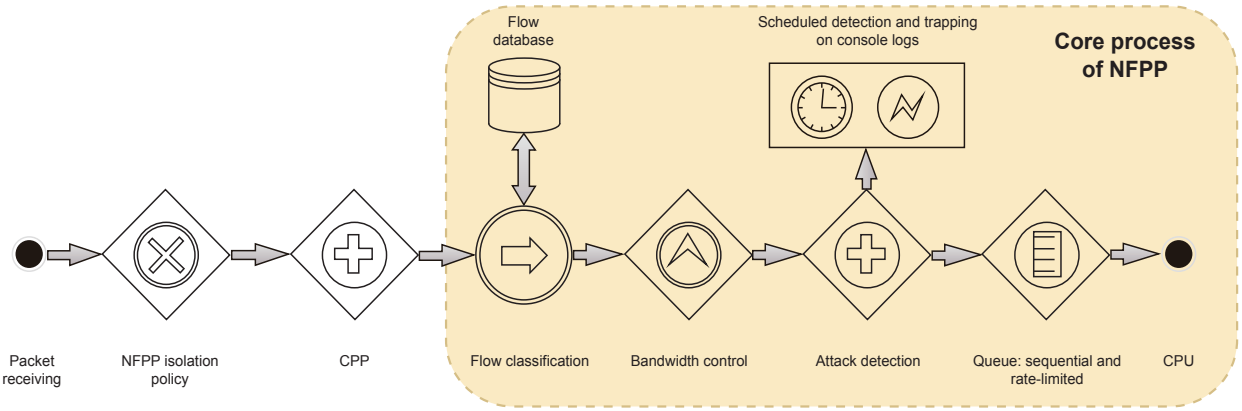


Concepts

• Working Process of NFPP

Figure 3 shows the simplified working process of NFPP.

Figure 3: Simplified Working Process of NFPP



*** CPP: Classifies the packets destined for the CPU and limits the traffic at the hardware layer.**

*** Flow classification: Reads the classification information from the flow database, including the type and rate statistics, and classifies the packet flows by the management plane, data plane, and control plane based on the information.**

*** Bandwidth control: Dynamically adjusts the packet traffic bandwidth of all types of flows based on the CPU processing capability.**

*** Attack detection: If the traffic of a specific type of packets transmitted to the CPU exceeds the attack threshold, the system advertises the syslogs and SNMP traps of the attack source based on the user-defined detection time.**

*** NFPP isolation: Isolates all attack packets sent by the attack source within a specific period of time.**

*** Sequential and rate-limited packet dispatching: Adjusts the bandwidth proportion of various types of packet flows based on the user-defined weights and schedules all the packet flows to a same queue for CPU processing, to prevent a specific type of packet flows exclusively occupying the queue resources.**

• Working Principle of NFPP

Flow Classification

NFPP must first detect the type of corresponding packets before taking anti-attack measures based on the flow policies of the packet type.

Flow classification is to identify the packets that meet a type of characteristics based on certain rules, and includes fixed classification and custom classification. The fixed classification implements the corresponding anti-attack functions for protocols such as IP, ARP, ICMP, DHCP, and DHCPv6. The custom classification supports the user-defined classification keywords to meet the anti-attack requirements in different environments.

In terms of the technical implementation of flow classification, NFPP fully considers the maintenance of the classification database and the stability and execution efficiency of flow query.

Maintenance of the Classification Database

The maintenance of the classification database has the following characteristics:

* **Uses the improved high-efficiency adjacency linked list to store instance nodes. The fixed classification and custom classification perform addressing independently, imposing no impact on each other and ensuring the accuracy.**

* **Uses the adjacency linked list in coordination with the linear speedup algorithm to avoid the complex algorithm logic after a new flow type is added, improving the setting efficiency. In addition, the linear speedup algorithm supports the hash and mask processing of variable-length keywords to flexibly store the similar hash keys, ensuring the accuracy of classification.**

* **Efficiently processes the flow type subset relationship. The following takes three flow types as an example:**

```
IP: etype=0x0800;

UDP: etype=0x0800,protocol=17;

RIP: etype=0x0800,protocol=17,dest-port=520;
```

A RIP packet simultaneously complies with the preceding three types. Performance issues may occur if you query the types in sequence. To process the protocol subset relationship, NFPP always keeps the types in the subnet in the uppermost position of the hash bucket when configuring the flow classification. In this case, the algorithm complexity of classification operations remains at O(n), with n being the number of protocol subnet relationships under a single bucket. This feature guarantees the efficient execution of flow classification.

* **Efficiently processes unclassified flows. When the unclassified flows pass through NFPP, NFPP also maintains them to the database. According to the principle of locality, a large number of packets of the same type may continue passing through NFPP. When unclassified packets hit the database, subsequent processing of NFPP for these packets is directly skipped, ensuring efficient transmission of packets to the CPU.**

* **Supports node aging. NFPP supports high-level interrupt service routine (HISR) to trigger the aging operation for nodes with unclassified packets, and can trigger to release storage and computing resources of the nodes, ensuring the memory efficiency.**

System Protection Policy of NFPP

The anti-attack policy of NFPP is called flow table. Based on the policy type, the flow table falls into the port-based policy and host-based policy. Based on the policy behavior, the flow table falls into the software protection policy and hardware isolation policy.

After the flow classification is completed, packets are scheduled to the corresponding queues based on their types, and the elements in each queue contain the policy information of such traffic. NFPP executes the corresponding protection measures based on the traffic and policy information of the current type:

* **Software protection: If the traffic of a type of packets exceeds the anti-attack threshold within the specified period of time, NFPP identifies the attack source based on the flow policy of this type and advertises the software syslogs and SNMP traps to users. In addition, NFPP triggers hardware protection and isolation.**

* **Hardware isolation: When executing the policy for software protection, NFPP delivers the policies for hardware traffic-limiting and attack source isolation as required. Traffic-limiting proactively limits the attack traffic at the hardware layer, without occupying CPU resources; attack source isolation isolates all packets of the required type sent by the attack source within a specified period of time.**

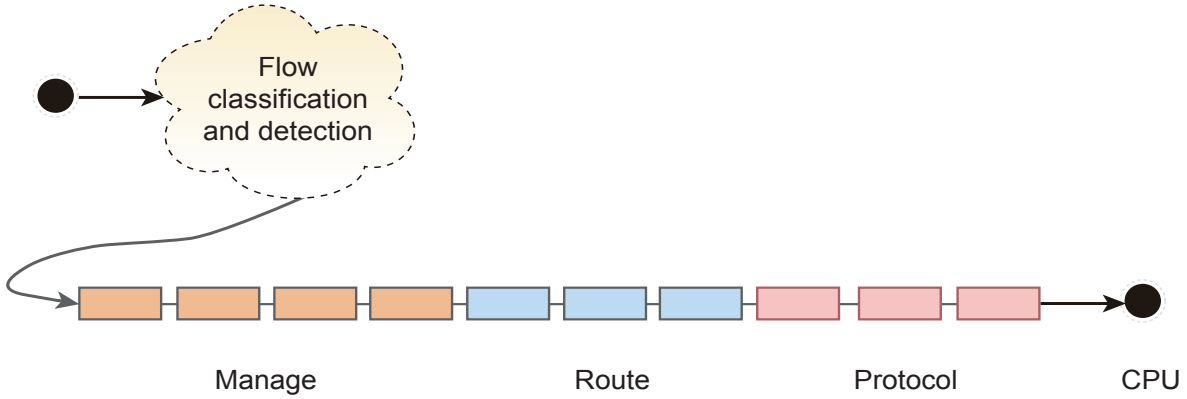
The NFPP is a high-priority security application and can deliver isolation entries to the hardware to restrict packet forwarding and transmission to the CPU, thereby ensuring that the system works properly and efficiently even upon attacks.

Sequential and Rate-limited Packet Dispatching

When normal services incur heavy traffic, the CPU may constantly stay in a high-load state. As a result, the network administrator may fail to manage devices or the device protocol may fail to work properly. NFPP employs sequential and rate-limited packet dispatching to increase the priorities of some flow types.

NFPP differentiates the Manage, Route, and Protocol packets when applying sequential and rate-limited packet dispatching, and guarantees separate bandwidth for each type of packets. Packets whose traffic exceeds the bandwidth threshold will be discarded. This feature takes effect to attack flows and assigns a weight to the normal Manage packets, ensuring that advanced system services always run properly.

Figure 4 Packet Queue with Sequential and Rate-limited Packet Dispatching



Reliability

NFPP guarantees system reliability in many aspects to ensure system robustness:

*** VDU framework support: The VDU divides the system into multiple virtual domains, assigns ports to each virtual domain, and adds the domain-based NFPP policies. After the division, NFPP independently runs in each domain and the domains do not affect each other.**

*** Aggregation port change: After a port joins an aggregation port (AP), the AP can automatically switch to the monitoring and protection policies of the new port.**

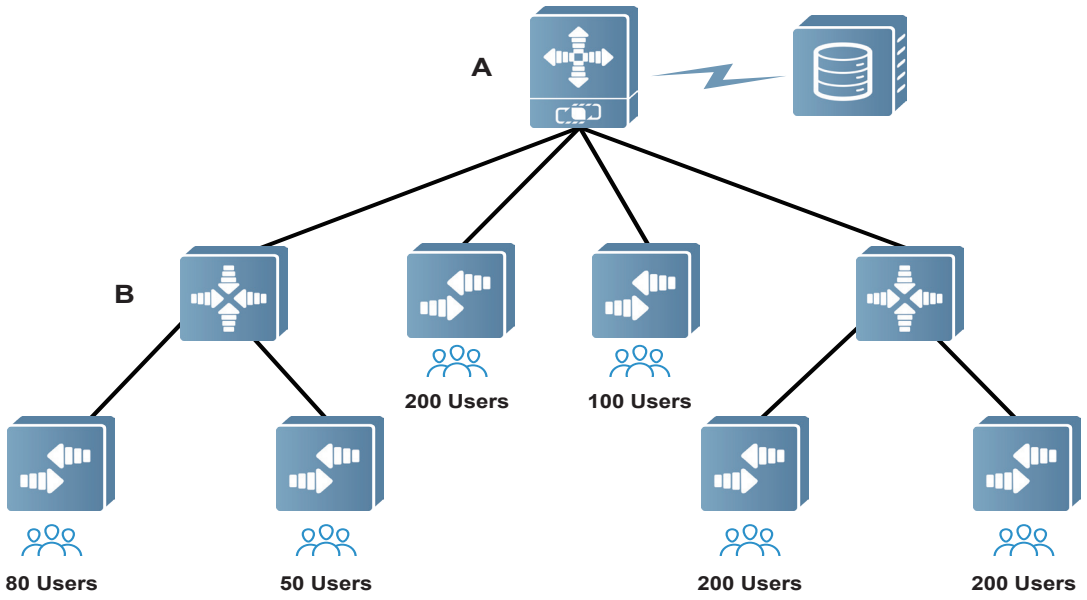
*** VLAN change: The normal monitoring behavior is not affected when a VLAN is created or deleted or a port joins or exits an AP.**

*** Hot backup: In the modular software, NFPP can periodically perform data synchronization and backup of the active and standby supervisor modules on the chassis-type switch, and the active/standby data synchronization and backup on the VSU, ensuring the security of monitoring data and eliminating data loss. In addition, the Smart NFPP is supported so that the dynamic configuration (non-user configuration) of NFPP is cleared when the hot-backup switchover occurs, further decreasing the CPU usage in hot backup mode.**

*** Hot swapping: When line cards are hot swapped on the modular chassis-type switch, NFPP automatically delivers the related policies to ensure the timely validation of NFPP.**

NFPP Application Instance

Figure 5: Application Topology



As shown in Figure 5, aggregation switch B is connected to a maximum of 80 clients through one port and 50 clients through another port; core switch A is connected to 4000 clients (excluding the clients connected to aggregation switch B), with one port connected to a maximum of 400 clients. Table 3 and Table 4 describe the typical configurations of NFPP for defending against ARP attacks in this scenario.

Table 3: Typical Configurations of Aggregation Switch B

Configuration	Description
arp-guard rate-limit 3 per-src-mac arp-guard rate-limit 3 per-src-ip	Configures the client rate limit, in the recommended range of 2–6 pps.
arp-guard rate-limit 80 per-port	Sets the maximum number of clients on each port to 80.
arp-guard attack-threshold 6 per-src-mac arp-guard attack-threshold 6 per-src-ip arp-guard attack-threshold 160 per-port	Sets the attack threshold.
arp-guard scan-threshold 15	Configures the anti-ARP scanning threshold.

Table 4: Typical Configurations of Core Switch A

Configuration	Description
arp-guard rate-limit 3 per-src-mac arp-guard rate-limit 3 per-src-ip	Configures the client rate limit.
arp-guard rate-limit 400 per-port	Sets the maximum number of clients on each port to 400.
arp-guard attack-threshold 6 per-src-mac - arp-guard attack-threshold 6 per-src-ip arp-guard attack-threshold 460 per-port arp-guard	Sets the attack threshold.
arp-guard scan-threshold 15	Configures the anti-ARP scanning threshold.

Table 5 shows performance comparison between NFPP-supported and NFPP-unsupported devices after the preceding configurations are applied.

Table 5: Device Performance Under NFPP Application

Attack Type	Attack Characteristic	Performance of NFPP-unsupported Devices	Performance of NFPP-supported Devices
ARP traffic attack	Valid ARP packets at a high rate	Without a rate limit, if the ARP traffic attack rate reaches 1000 pps, the ARP packet learning convergence time of the switch increases or even the ARP packet learning process is not converged. Because the traffic attack packets occupy all the bandwidth of the CPU input channel, valid ARP packets cannot be transmitted to the CPU.	The isolation function is enabled using the arp-guard command, and the ARP packet learning convergence time is not affected regardless of the ARP traffic attack rate.
		Without a rate limit, ARP packets are transmitted at the line rate. The Telnet or ping operation fails and the protocol fails to work properly, but the forwarding plane of the ASIC chip is not affected.	ARP packets are transmitted at the line rate. The Telnet or ping operation succeeds, the protocol works properly, and the forwarding plane of the ASIC chip is not affected.
Conclusion	When a client encounters ARP traffic attacks, if no NFPP is configured, the ARP packet learning process cannot be converged (that is, the client cannot be connected to the network) and the management plane works improperly. If NFPP is configured, the device stability can be enhanced. When a plane is attacked, NFPP guarantees the normal work of other planes, and rate-limits and isolates the invalid packets, ensuring that valid clients have sufficient bandwidth and all clients can be connected to the network properly.		

Conclusion

When a switch encounters malicious attacks, NFPP employs a series of countermeasures, such as rate-limiting, identifying, and isolating the attack source, to ensure the normal control and management flows of the system, thereby protecting the computing and channel resources of the switch CPU and greatly improving the security protection capability of the switch.

In the future, NFPP will continuously develop to defend against more types of attacks, improve the anti-attack capability of the switch, and evolve towards integrated functions at lower configuration costs and more centralized anti-attack functions. In addition, NFPP can coordinate with Ruijie's new-generation IPFIX traffic monitoring technology to develop a security solution with security policies associated throughout the network, avoiding attacks and guaranteeing the security of the whole network.