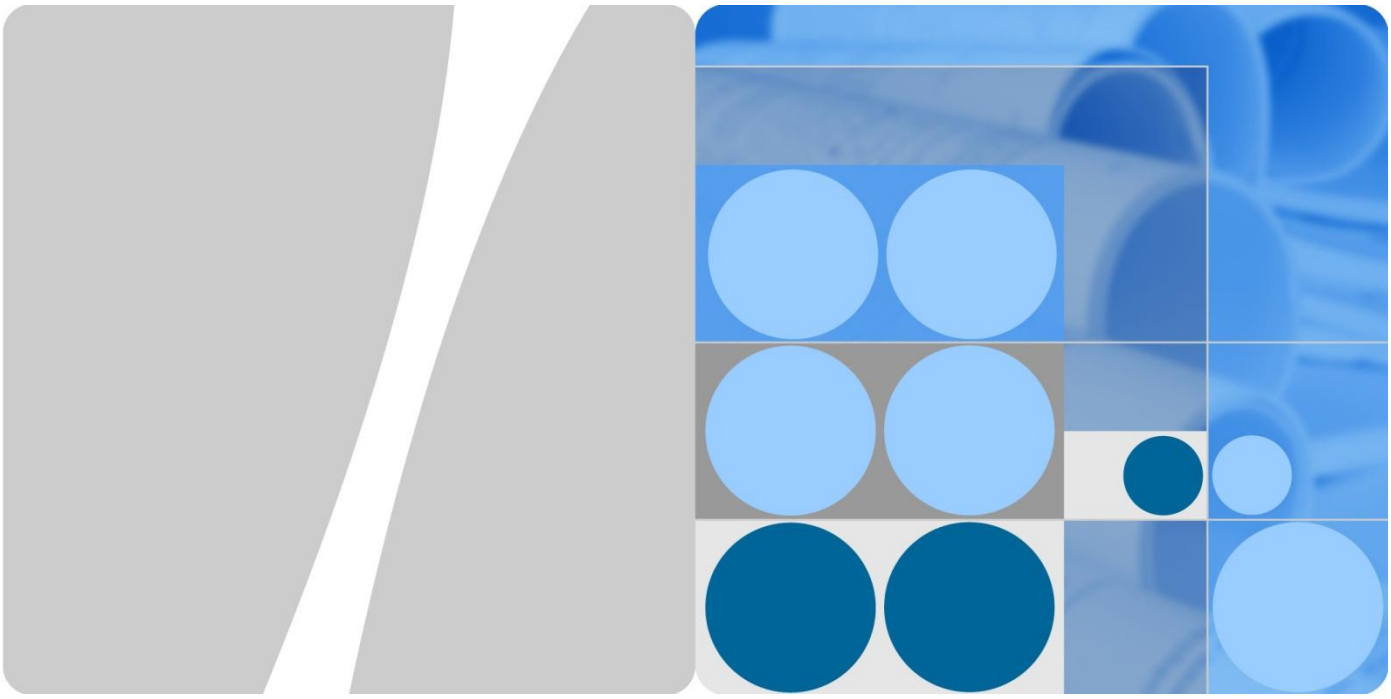


Security Technology White Paper

Issue 01

Date 2012-10-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://enterprise.huawei.com

About This Document

Abstract:

Simple and open Internet Protocol (IP) networks promote Internet development, but also bring security holes. Attacks on the IP networks have become easier over time. Attacking tools have become more automatic so that even people with little computer knowledge can initiate attacks on IP networks. Network attack types increase every year, causing increasing losses. The attacks affect many companies and even threaten information security of governments. Threats to network security hinder further development of the network.

Keywords:

Security, attack, DHCP snooping, DAI, IP source guard, MFF, NAC

Abbreviation list

Abbreviation	Full Name
DAI	Dynamic ARP Inspection
NAC	Network Access Control
URPF	Unicast Reverse Path Forwarding
MFF	MAC Force Forwarding

Contents

1 Overview

The basis of the Internet, IP network, raises issues of security, quality of service, and operation mode due to its openness and simplicity.

The simple and open IP network promotes development of the Internet, but the IP network also brings security threats. Fortunately, many useful methods are available to combat security threats. This white paper describes several of the most useful methods.

The technologies described in Table 1-1 help improve network security.

Table 1-1 IP network security methods

Switch Security Technology	Value
DHCP snooping	Prevents bogus DHCP server attacks, man-in-the-middle attacks, and IP/MAC spoofing attacks.
IP Source Guard	Prevents unauthorized users from accessing the network by using bogus IP addresses.
Dynamic ARP Inspection (DAI)	Prevents man-in-the-middle attacks.
MAC Force Forwarding (MFF)	Isolates client hosts at Layer 2 and enables them to communicate at Layer 3.
Unicast Reverse Path Forwarding (URPF)	Prevents unauthorized users from accessing the network by using bogus IP addresses.
Network Access Control (NAC)	Controls network access based on interfaces or users to prevent unauthorized hosts from accessing the network.

2 DHCP Snooping

2.1 Overview

DHCP snooping is a set of security methods used to protect the operation of DHCP. A switch creates and maintains the DHCP snooping binding table to filter out untrusted DHCP information, which is sent from untrusted zones. The DHCP snooping binding table contains the MAC address, IP address, lease, VLAN ID, interface number of each user in an untrusted zone.

When DHCP snooping is enabled on a switch, the switch listens on DHCP messages and records the IP addresses and MAC addresses in the received DHCP Request messages or Ack messages.

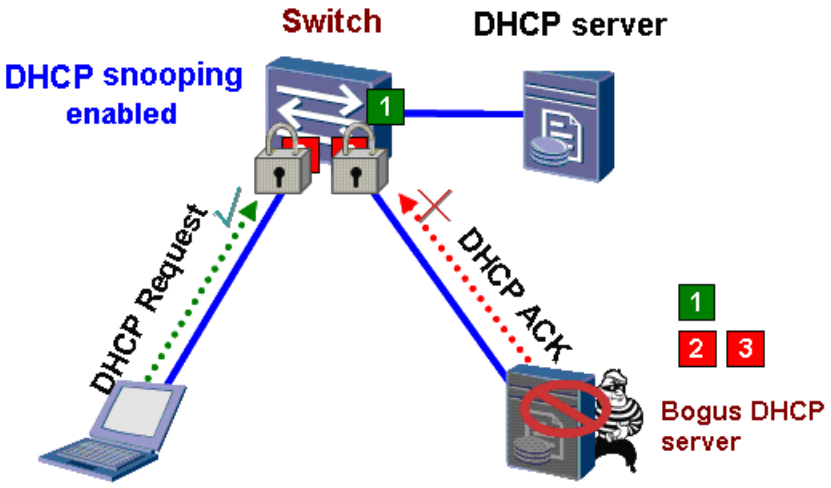
You can configure a physical interface as a trusted interface or an untrusted interface. A trusted interface can forward received DHCP Offer messages, whereas an untrusted interface discards the received DHCP Offer messages. Through DHCP snooping, the switch can shield bogus DHCP servers and ensure that clients obtain IP addresses from valid DHCP servers.

2.2 Implementation

DHCP snooping includes the following measures:

- An untrusted interface of a switch forwards only DHCP Request messages and discards all the other DHCP messages.
- Only the specified interface connected to the DHCP server or the upstream trusted interface can relay DHCP messages.
- The switch creates a mapping table containing the IP address, MAC address, interface number, and VLAN ID of each client for security functions such as IP source guard. This table is the DHCP snooping binding table.

Figure 2-1 Implementation of DHCP snooping

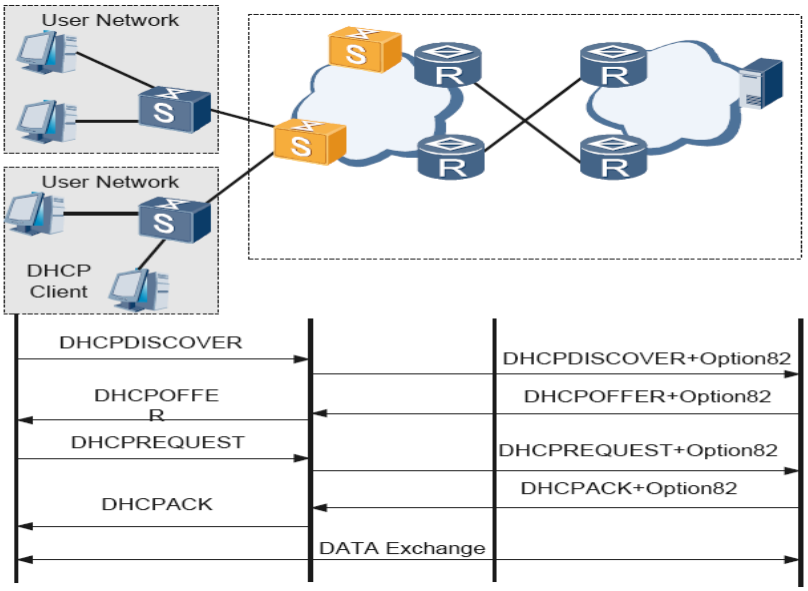


The DHCP snooping binding table contains dynamic binding entries and static binding entries.

- Dynamic DHCP snooping binding entries

  The switch generates the DHCP snooping binding entries according to the DHCP Ack messages received by the trusted interface.

Figure 2-2 Dynamically generating DHCP snooping binding entries



- Static DHCP snooping binding entries

  If a user accesses the network through a statically assigned IP address, the switch discards the packets of the user because the IP address matches no entries in the DHCP snooping binding table on the switch. You can configure a static DHCP snooping binding entry through commands. The IP address, MAC address, VLAN ID, and interface number of the user must be provided.

2.3 Value

DHCP snooping prevents the following attacks on DHCP applications:

- Bogus DHCP server attacks
- Man-in-the-middle attacks and IP/MAC spoofing attacks
- Denial of Service (DoS) attacks
- DoS attacks by changing the value of the Client Hardware Address (CHADDR)

3 Defense Against Address Scanning Attacks

3.1 Overview

An attacker initiates an address scanning attack by sending a large number of IP packets with different destination addresses to the target network. When the attacker scans the network segment that is directly connected to a network device, the network device generates ARP Miss messages. During this process, the network device sends ARP requests to each address on the network segment. If an address does not exist, the network device sends host unreachable messages to the attacker. If the directly connected network segment is large and the attack traffic is high, CPU and memory resources of the network device are occupied by the attack traffic, and the network services are interrupted.

3.2 Implementation

A switch prevents address scanning attacks by monitoring and changing problematic routes. After receiving a packet whose destination IP address is on the directly-connected network segment, the switch checks whether the route to the destination IP address exists. If the route does not exist, the switch sends an ARP request packet and generates a drop entry of the next hop address to prevent subsequent packets from continuously affecting the CPU. If the switch receives an ARP reply packet, it deletes the drop entry immediately and adds a normal routing entry. If the switch does not receive any ARP reply packet, it deletes the drop entry. The switch can prevent scanning of the directly-connected network segment and ensure normal service provisioning.

A switch that supports the address scanning attack defense also allows users to set the maximum rate of ARP Miss messages on an interface. When the rate of ARP Miss messages generated on an interface exceeds the maximum, the switch directly discards excess ARP Miss messages on the interface.

If a user initiates an address scanning attack by sending packets with the same source IP address, the switch can count the ARP Miss messages triggered by the source IP address. If the rate of ARP Miss messages triggered by the source IP address exceeds the maximum, the switch delivers an ACL to discard the excess packets with this source IP address.

4 Man-in-the-Middle and IP/MAC Spoofing Attacks

4.1 Overview

When users obtain IP addresses through DHCP, the switch is open to man-in-the-middle attacks. The attacker (the man in the middle) sends a packet carrying its own MAC address and the IP address of the DHCP server to the client. The client learns the IP and MAC addresses of the attacker and considers the attacker as the DHCP server. The packets sent from the client to the DHCP server pass the attacker.

The attacker then sends a packet carrying its own MAC address and the IP address of the client to the DHCP server. This action causes the DHCP server to learn the IP and MAC address of the attacker and consider the attacker as the client. Then all the packets sent from the DHCP server to the client pass the attacker.

The attacker also sends a packet carrying the valid IP and MAC addresses of a client to the DHCP server. The DHCP server now misidentifies the attacker as a valid client and learns the IP and MAC addresses. The actual valid client, however, cannot access the service provided by the DHCP server. In this case, an IP/MAC spoofing attack is initiated.

4.2 Implementation

DHCP snooping can prevent man-in-the-middle attacks and IP/MAC spoofing attacks.

When the switch receives an IP packet on an interface, the switch matches the source IP address and source MAC address of the packet with entries in the DHCP snooping binding table. When the strong policy is configured, the switch discards the IP packet if no matching entry is found. When the weak policy is configured, the switch forwards the IP packet even if no matching entry is found.

The switch discards IP packets sent from the DHCP clients configured with static IP addresses, because such DHCP clients have no DHCP snooping binding entries. This prevents unauthorized users from accessing the network.

When an unauthorized user uses the IP address of an authorized user but not an IP address obtained by sending a DHCP request message, the MAC address and interface number of the unauthorized user do not match the DHCP snooping binding entry of the authorized user. The switch discards IP packets sent by the attacker to protect the network.

5 IP source Guard

5.1 Overview

IP source guard is a technology used to filter traffic on a port based on IP and MAC addresses. IP source guard can prevent IP address spoofing attacks on a local area network (LAN). A switch maintains an IP source binding table to check the data packets received on each port. The switch forwards received data packet only in the following conditions:

- The data packet matches a port/IP/MAC entry in the IP source binding table.
- The data packet is a DHCP data packet. Other data packets are discarded.

The IP source binding table can be configured manually or learned by the switch through DHCP snooping.

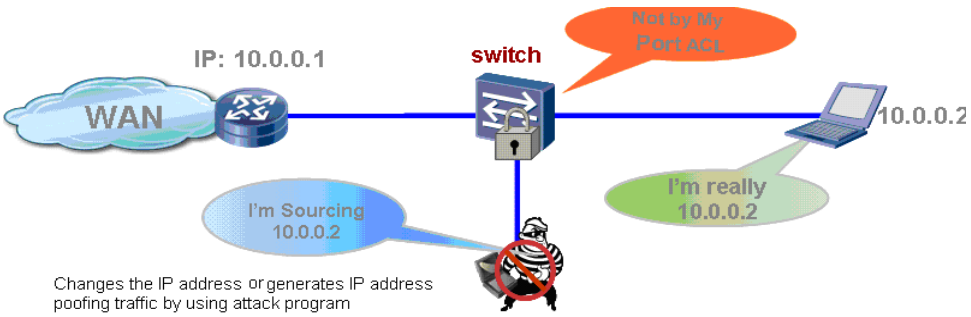
5.2 Implementation

DHCP snooping binds user information such as the IP address, MAC address, port number, and VLAN ID.

The switch generates a port-based ACL and adds the IP address and MAC address of a user to the ACL.

When the lease of the IP address expires, the switch deletes the MAC address of the host and the ACL to release resources. This prevents data interception and anonymous attacks.

Figure 5-1 Implementation of IP source guard



5.3 Value

IP source guard prevents unauthorized users from accessing the network by using bogus IP addresses, protecting network resources of the customer.

6 DAI

6.1 Overview

Dynamic ARP Inspection (DAI) dynamically sets up binding between IP addresses and MAC addresses.

6.2 Implementation

The DAI function is implemented using the DHCP snooping binding table. If a host does not use the DHCP server, you can add a static ARP access list for the host. DAI applies to VLANs. You can choose to enable or disable DAI on all the ports in a VLAN. DPI controls the number of ARP requests on each port. This technology prevents man-in-the-middle attacks.

7 MFF

7.1 Overview

In traditional Ethernet solutions, VLANs are usually configured on switches to implement Layer 2 isolation and Layer 3 interconnection between clients. When many users need to be isolated on Layer 2, a large number of VLANs are required. In addition, to enable the clients to communicate on Layer 3, each VLAN must be assigned an IP network segment and each VLANIF interface needs an IP address. This use of VLANs therefore wastes IP addresses..

The MAC-Forced Forwarding (MFF) technology provides a solution to this problem and implements Layer 2 isolation and Layer 3 interconnection between clients in a broadcast domain. MFF intercepts ARP request packets from users and sends ARP reply packets containing the MAC address of the gateway through the proxy ARP mechanism. In this manner, MFF forces users to send all traffic (including the traffic on the same subnet) to the gateway so that the gateway can monitor data traffic. This prevents malicious attacks and improves network security.

7.2 Implementation

7.2.1 Proxy ARP

Proxy ARP ensures Layer 3 interconnection between users and reduces broadcast packets transmitted between the network and users.

The MFF module processes ARP packets as follows:

- Responds to ARP requests of users. The MFF module substitutes for the gateway to respond to ARP requests of users so that packets of users are all forwarded on Layer 3 by the gateway. A user may send an ARP request containing the IP address of the gateway or another user.
- Responds to ARP requests of the gateway. The MFF module substitutes for user hosts to respond to ARP requests of the gateway. If the ARP entry mapping the request of the gateway exists on the MFF module, the MFF module returns a response with the requested MAC address to the gateway. If the mapping ARP entry does not exist, the MFF module forwards the request. This reduces broadcast packets on the network.
- Forwards ARP reply packets sent from user hosts and the gateway.
- Listens on ARP packets on the network. Updates the mapping between the IP address and MAC address of the gateway.

7.2.2 Automatically Obtaining the IP Address and MAC Address of the Switch

If users obtain IP addresses from the DHCP server, you need to enable DHCP snooping before enabling MFF. The MFF module listens on the DHCP Ack message sent from the DHCP server to a user host and analyzes the Option 3 and Option 121 fields in the DHCP Ack message. Then the MFF module records the IP address of the switch that the user host accesses and the IP and MAC addresses of the user host. After dynamic MFF is enabled, the MFF module sends an ARP request immediately to probe the switch MAC address. In the ARP request, the SMAC and SIP fields are respectively set to the MAC address and IP address of the first host recorded in the user information list in the VLAN. After receiving a response from the AR, the MFF module records the MAC address of the switch in the mapping table. If the periodical probe function is enabled, the MFF module sends probe packets to the gateway at a specified interval. The default probe interval is 30s. The ARP probe packet is a bogus ARP packet, and the source IP and MAC addresses in the packet are the IP and MAC addresses of a user recorded in the user information list. The MFF module selects the IP and MAC addresses of the first user in the list. If the entry of this user is deleted, the MFF module selects the IP and MAC addresses of another user to forge the ARP probe packet. If the gateway does not have any matching user information after the user entry is deleted, the MFF module deletes probe information.

7.2.3 Static Gateway Address

If user hosts use static IP addresses, you need to configure the IP address of the switch when enabling MFF on the EAN. The EAN listens on the ARP responses that the switch sends to users to obtain the MAC address of the switch. Then the EAN creates a mapping table between the switch and user hosts. In static configuration, each VLAN supports one switch address.

Two types of interfaces are involved in the MFF function: network interface and user interface.

A user interface is directly connected to users. MFF processes packets on a user interface as follows:

- MFF allows protocol packets to pass through.
- MFF sends ARP and DHCP packets to the CPU.
- If the interface has learned the gateway MAC address, MFF allows the unicast packets with the destination MAC address as the gateway MAC address to pass through and discards other packets. If the interface does not learn the gateway MAC address, MFF discards all packets.
- MFF rejects multicast data packets and broadcast packets.

A network interface is connected to another network device, for example, an access switch, an aggregate switch, or a gateway. MFF processes packets on a network interface as follows:

- MFF allows multicast and DHCP packets to pass through.
- MFF sends ARP packets to the CPU.
- MFF rejects other broadcast packets.

8 NAC - 802.1X

8.1 Overview

802.1x is an IEEE standard for port-based network access control (NAC).

Use of 802.1x provides good service continuity and expansibility, high security, and flexibility. The standard can be implemented at low cost.

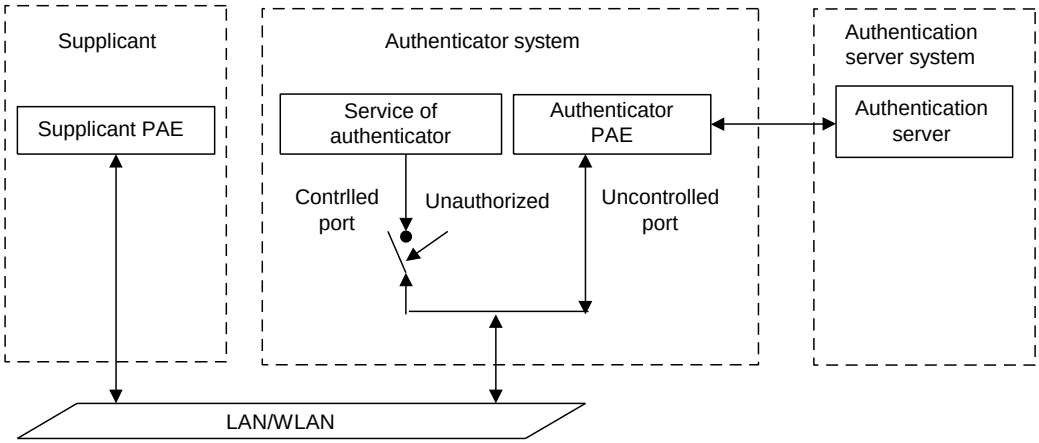
LANs that comply with the IEEE 802 protocol do not include access authentication, and users can access the devices or resources on the LANs directly. In the scenarios such as telecom access, LANs in office buildings, and mobile offices, network administrators need to control user access and configure the access control function. In this case, port-based network access control such as that provided by 802.1x is required.

802.1x is widely used on broadband MANs and intranets of enterprises or campuses. In broadband network construction, 802.1x and its extended features become a key differentiator when similar services are provided on the networks.

8.2 Implementation

Figure 8-1 shows the system architecture of IEEE 802.1x. The 802.1x system consists of three entities: supplicant, authenticator system, and authentication server system.

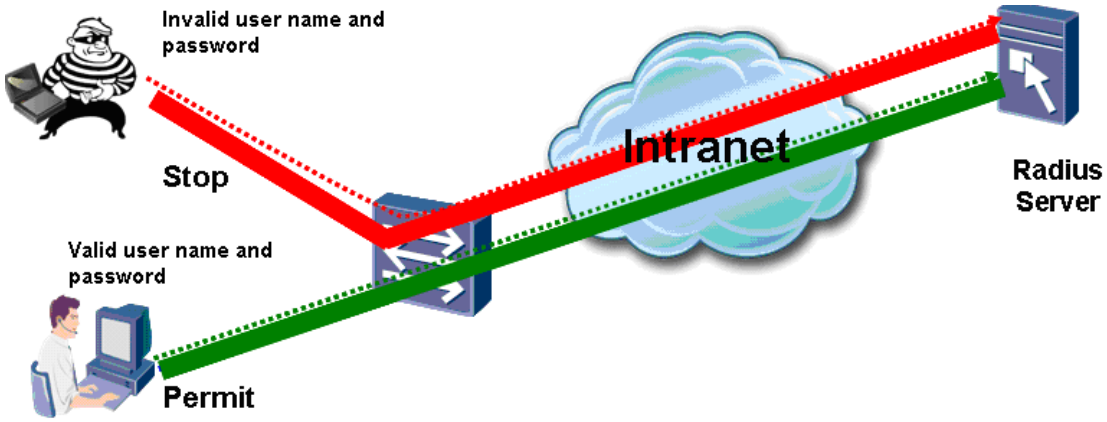
Figure 8-1 System architecture of the IEEE 802.1x authentication system



The supplicant is an entity on one end of a point-to-point LAN network segment and is usually a user terminal. The supplicant is authenticated by the device on the other end of the link. The user starts client software to initiate 802.1x authentication. The supplicant must support the EAP over LAN (EAPoL) protocol.

As mentioned, the authenticator system is an entity on the other end of a point-to-point LAN network segment. The authenticator system is generally a network device supporting the 802.1x protocol and provides a port for the supplicant to access the LAN. The port can be a physical port (for example, an Ethernet port or an AP access channel of an Ethernet switch) or a logical port (for example, the MAC address or VLAN ID of the user).

Figure 8-2 Implementation of 802.1x authentication



Before authentication, the user host cannot access the resources on the access switch. The host needs to send the user name and password to the RADIUS server for authentication.

After being authenticated, the user can access the network services on the access switch.

8.3 Value

802.1x authentication prevents unauthorized hosts from accessing the network.

9 Broadcast, Multicast, and Unknown Unicast Packets Suppression

When a large number of broadcast, multicast, or unknown unicast packets are transmitted on a network, these packets may occupy high bandwidth and affect forwarding performance of network devices. If loops exist on a network device, a great number of broadcast, multicast, and unknown unicast packets are generated, which may make the entire network break down.

Huawei switches have powerful capabilities to filter broadcast, multicast, and unknown unicast packets. A Huawei switch can limit the absolute rate or rate percentage of broadcast, multicast, or unknown unicast packets.

10 URPF

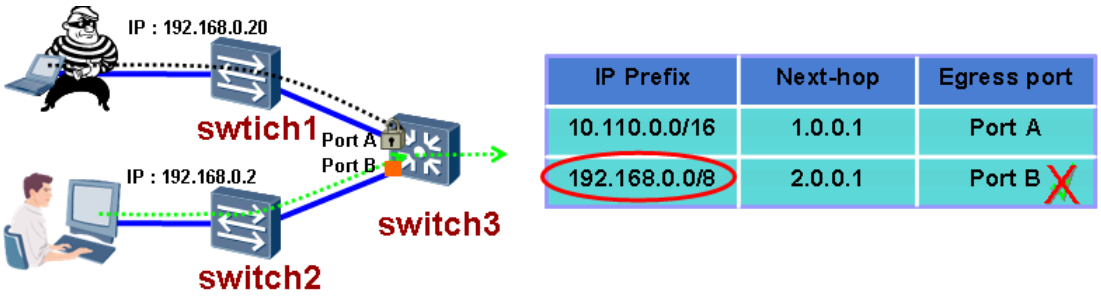
10.1 Overview

Unicast Reverse Path Forwarding (URPF) can prevent source address spoofing on networks.

Generally, a routing switch searches for a route according to the destination IP address of a packet. If a matching route is found, the routing switch forwards the packet; otherwise, the switch discards the packet.

After URPF is enabled on the routing switch, the routing switch obtains the source IP address and inbound interface of a packet, and then searches for the route in which the destination address is the source address of the packet. If the outbound interface of the route is not the inbound interface of the packet, the switch considers the source IP address of the packet as a spoofing address and discards the packet. In this way, the switch can protect the network against attacks initiated by changing the source address.

Figure 10-1 Implementation of URPF



As shown in Figure 10-1, switch 3 obtains the source IP address of a received packet, and then searches the FIB for the route in which the destination IP address is the source IP address of the packet. If the outbound interface of the route is not the inbound interface of the packet, switch 3 considers the packet as an IP address spoofing packet and discards the packet.

10.2 Value

URPF can prevent unauthorized users from accessing the network by using bogus IP addresses.

11 Attack Defense

11.1 Overview

Network attacks are initiated in the following ways:

- The network attacker intrudes in or destroys a network server or a host to intercept sensitive data or to interrupt the services of the server.
- The network attacker directly destroys network devices, which results in network service exceptions or even service interruption.

The switch can identify various network attacks and protect itself and the Intranet against malicious attacks to ensure normal operation of the network.

Networks are subject to three types of attacks:

- DoS attacks

  An attacker initiates a Denial of Service (DoS) attack by sending a large number of data packets to the system. As a result, the system cannot receive requests from authorized users or is suspended. The system therefore cannot work normally. DoS attacks include SYN flood, Land, Smurf, and ICMP flood attacks.

  Different from other types of attacks, the DoS attacker prevents legitimate users from accessing resources or the switch instead of searching for the ingress of the Intranet.

- Scanning and snooping attacks

  An attacker initiates a scanning and snooping attack by sending a large number of ping packets (ping sweep, including ICMP sweep and TCP sweep). The attacker can locate the latent targets using ping packets, and identify the type of an operating system and the latent service type by scanning TCP and UDP ports.

  By scanning and snooping, an attacker can know the service type and security vulnerability of the system and prepare for further intrusion.

- Malformed/Bogus packet attacks

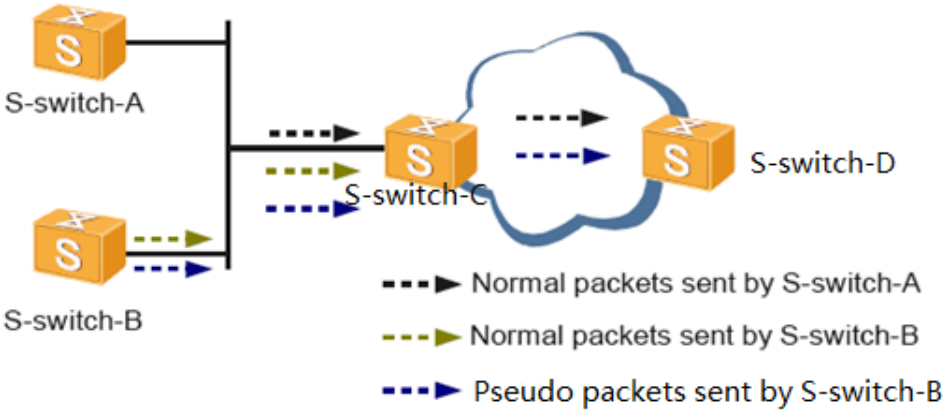
  An attacker initiates a malformed packet attack by sending malformed IP packets to the target system. The system may crash when processing such packets. Typical malformed packet attacks include Ping of Death and Teardrop packets. The bogus packet attack is initiated by sending bogus packets to the target system to intrude in or control the target system. IP spoofing attack is a typical bogus packet attack.

11.2 Attack Description

11.2.1 IP Spoofing Attack

In an IP spoofing attack, an attacker forges a packet carrying a valid source IP address to access a target system. In this way, the attacker snoops in or controls the system. As shown in Figure 11-1, a rule is configured on S-switch-C to allow packets from S-switch-A to pass through. The rule rejects packets from S-switch-B. S-switch-B forges a packet by using the IP address of S-switch-A as the source IP address. The forged packet can go through S-switch-C and arrive at S-switch-D.

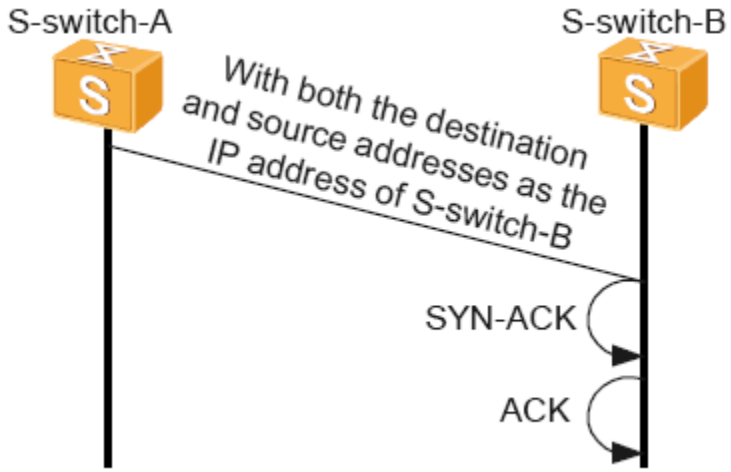
Figure 11-1 IP address spoofing



11.2.2 Land Attack

In a Land attack, an attacker sets both the source and destination addresses of a TCP SYN packet as the IP address of the target device. Then the target device sends a SYN-ACK packet to itself, and then responds with an ACK packet, establishing an empty connection. Each empty connection is kept until it times out. Excess empty connections affect normal running of the S-switch. Figure 11-2 illustrates the Land attack.

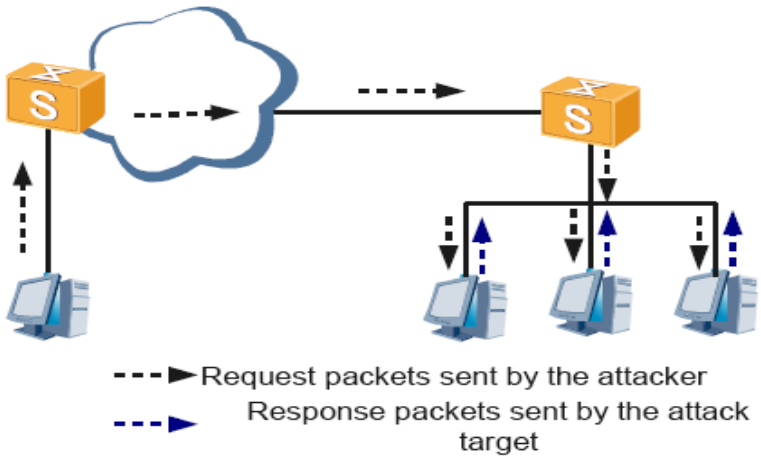
Figure 11-2 Land attack



11.2.3 Smurf Attack

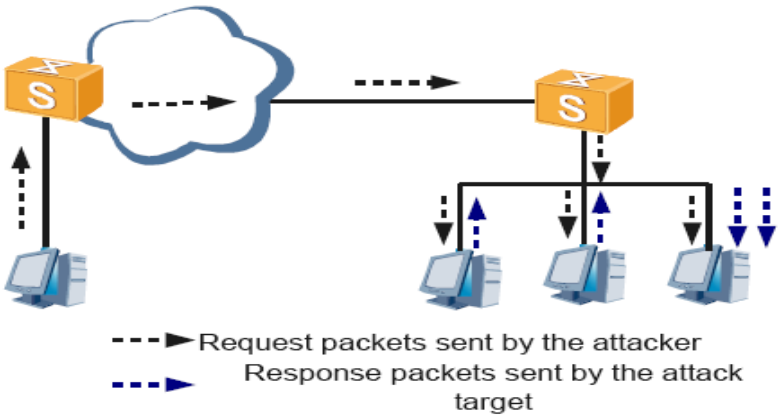
A simple Smurf attack targets a network. An attacker sends an ICMP Echo message to the broadcast address of the target network. All the hosts on the network then respond to the ICMP Echo message. The network is congested. Figure 11-3 illustrates the simple Smurf attack.

Figure 11-3 Simple Smurf attack



An advanced Smurf attack targets hosts. An attacker sends an ICMP Echo message to the network where the target host is located. The destination IP address of the message is set to the IP address of the target host; therefore, all ICMP Echo Reply messages are sent to the target host. This slows down the packet processing on the target host or even makes the host crash. Figure 11-4 illustrates the advanced Smurf attack. The attack is damaging when the traffic of the attack packets is heavy and lasts for a long time.

Figure 11-4 Advanced Smurf attack



11.2.4 SYN Flood Attack

The SYN flood attack takes advantage of the vulnerability of three-way handshake of TCP. An attacker sends a SYN packet to the target device to initiate a TCP connection but does not respond to the SYN-ACK sent from the device. If the target device receives no ACK packet from the attacker, the device keeps waiting for the ACK packet. A half-open connection is therefore generated. The attacker keeps sending SYN packets, so many half-open connections are set up on the target device. These connections waste a large number of resources. When the resources of the target device are used up, the device responds to access requests of users very slowly. Therefore, authorized users cannot access the network.

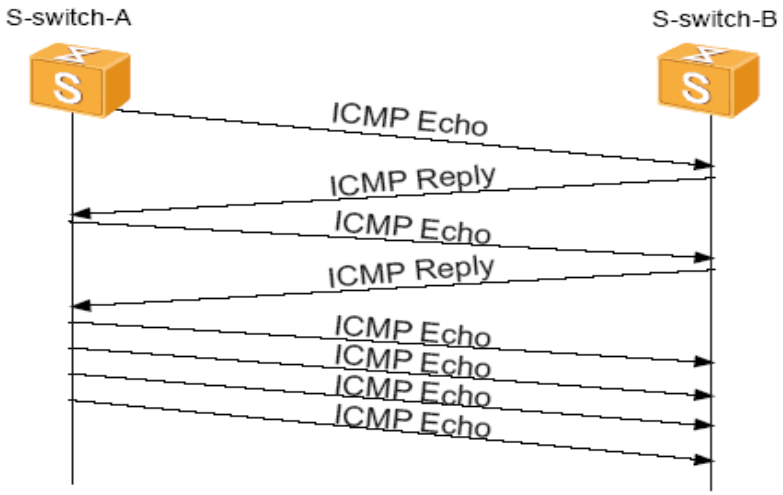
11.2.5 ICMP Flood Attack

Generally, a network administrator monitors a network and rectifies network faults with the ping tool as follows:

1. The source host sends an ICMP Echo message to the destination host.
2. When receiving the ICMP Echo message, the destination host sends an ICMP Echo Reply message to the source host.

If an attacker sends many ICMP Echo messages to the target host, an ICMP flood attack occurs. The target host is busy with these Echo messages and cannot process other data packets. Therefore, normal services are affected. Figure 11-5 illustrates the ICMP Flood attack.

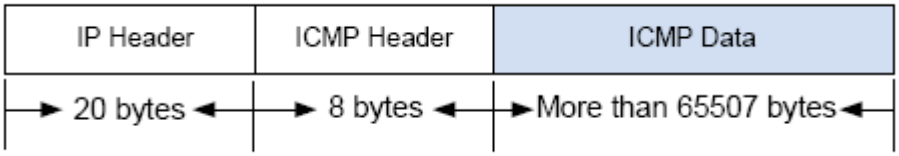
Figure 11-5 ICMP Flood attack



11.2.6 Ping of Death Attack

In a Ping of Death attack, an attacker intrudes in a system by sending oversized ICMP packets. The length field of an IP packet is 16 bits, so the maximum length of an IP packet is 65535 bytes. If the length of an ICMP packet is greater than 65507 bytes, the total length of the packet is longer than 65535 bytes (ICMP data + IP header (20) + ICMP header (8) > 65535). Some systems or devices cannot process oversized ICMP packets. If they receive such packets, they may stop responding, crash, or restart. Figure 11-6 shows an oversized ICMP packet.

Figure 11-6 Oversized ICMP packet

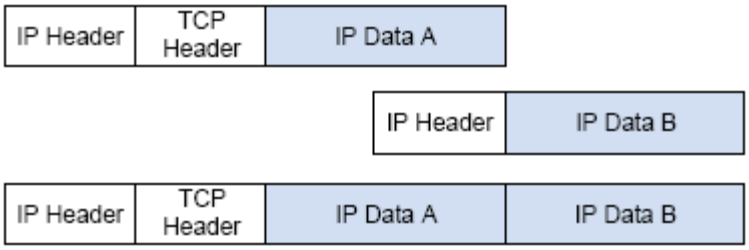


11.2.7 Teardrop Attack

During packet transmission, when an IP packet is longer than the maximum transmission unit (MTU) of the link layer, the IP packet must be fragmented. The IP packet header contains an offset field and an MF field. The MF field set to 1 indicates that the IP packet is a fragment of a large packet. The offset field indicates the location of this fragment in the whole IP packet. The receiver can reassemble the IP packet based on the information carried in the IP packet header.

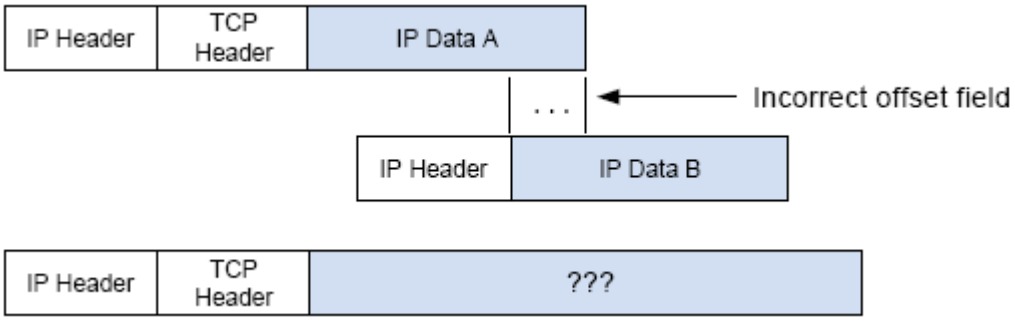
For example, if a large packet is transmitted over a link with a smaller MTU, the packet is fragmented into two IP packets. The receiver then reassembles the two IP packets into the original IP packet, as shown in Figure 11-7.

Figure 11-7 Normal segmentation and reassemble of an IP packet



If an attacker sets an incorrect value for the offset field, the receiver cannot correctly reassemble packets. Some TCP/IP protocol stacks may crash when they receive such bogus fragments containing overlapping offset values. This is a Teardrop attack. Figure 11-8 shows a Teardrop attack packet.

Figure 11-8 Teardrop attack packet



11.2.8 DoS/DDoS Attack

A DoS attack aims to occupy resources of a device by sending many connection requests. As a result, the device cannot function properly and may crash. DoS attacks usually target a server. In this case, the server deny requests of authorized users.

A Distributed Denial of Service (DDoS) attack is a more intense form of the DoS attack. An attacker initiates DoS attacks from multiple hosts, causing more damages.

Huawei switches can defend against common DoS attacks such as IP spoofing, Land, and Smurf. When a protocol is attacked, the attack defense function helps ensure normal running of other protocols and forwarding of service packets. When an attacker initiates a DoS attack to the server connected to a switch, for example, an S9300, the S9300 can deliver a specified ACL rule to filter attack packets. Therefore, the hosts and server connected to the S9300 can run properly.