WX系列AC实现ARP防攻击功能的配置

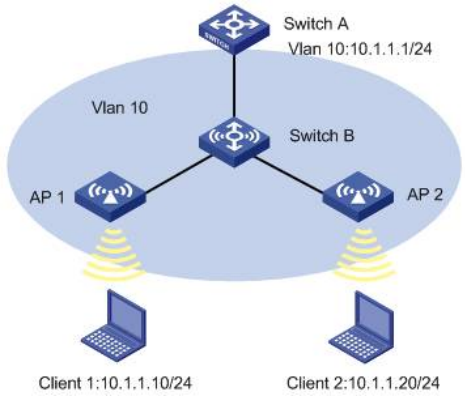
攻击检测及防范 ARP 宋斌 2011-12-01 发表

WX系列AC实现ARP防攻击功能的配置

一、 组网需求：

三层交换机、WX系列AC、FIT AP、交换机、便携机（安装有无线网卡）

二、 组网图：



Switch A作为网关设备，可以配置ARP源MAC地址固定攻击检查、源MAC一致性检查、主动确认等功能实现对网关设备的保护。

Switch B作为接入设备(以WX3024为例)，可以配置ARP Detection，同时配置DHCP Snooping，或者静态绑定网关或重要服务器IP和MAC，对转发的ARP进行侦听检查，对于不合法的报文进行丢弃处理。

三、 特性介绍：

ARP防攻击结合网关单机防御和整网防御两种防御方式，可以有效防御仿冒网关、仿冒用户和泛洪攻击等攻击行为。

从单机防御上看，源MAC地址固定攻击检查、源MAC一致性检查和主动确认等机制结合原有的ARP限速功能、接口ARP学习个数限制等功能可以有效保护网关设备。

从整网防御看，ARP Detection结合DHCP Snooping、静态绑定IP和MAC表项等手段，可以有效防御仿冒网关、仿冒用户等ARP攻击行为。

ARP的主动确认功能主要应用于网关设备上，防止攻击者仿冒用户欺骗网关设备。

源MAC地址固定攻击检查、源MAC一致性检查和主动确认等机制可以独立存在，不依赖于其它特性。

结合DCHP Snooping安全表项的ARP Detection应用在接入设备上，依赖于通过DHCP分配地址的组网方式，且要求在接入设备上启用DHCP Snooping。

l ARP主动确认功能简介

使能ARP主动确认功能之后，当收到的ARP报文中的源MAC地址和对应ARP表项中的不同时，设备首先判断ARP表项刷新时间是否超过1分钟，如果没有超过1分钟，则不更新ARP表项。否则向ARP表项对应的源发送一个单播ARP请求报文，如果在随后的5秒内收到ARP应答报文，则忽略之前收到的ARP攻击报文；如果没有收到ARP应答报文，则向之前收到的ARP报文对应的源发送一个单播ARP请求报文，如果在随后的5秒内收到了ARP应答报文，则根据之前收到的ARP报文更新ARP表项，否则ARP表项不会被修改。

l 源MAC地址固定的ARP攻击检测功能

本特性根据ARP报文的源MAC地址进行统计，在5秒内，如果收到同一源MAC地址的ARP报文超过一定的阈值，则认为存在攻击，打印对应的告警信息，并对此源MAC地址对应的用户进行限制。

只对上送CPU的ARP报文进行统计。

l ARP报文源MAC一致性检查功能

ARP报文源MAC一致性检查功能主要应用于网关设备上，防御以太网数据帧首部中的源MAC地址和ARP报文中的源MAC地址不同的ARP攻击。

在ARP Detection中也对源MAC一致性进行了检查，但这两者功能不同。ARP Detection

中的源MAC一致性检查，是在接入设备上使能ARP Detection，对上送的ARP报文进行源MAC一致性的检查。而这里的源MAC一致性检查，是网关设备在学习ARP之前，对要被学习的ARP报文进行检查。

四、 主要配置步骤：

配置组网图中所有端口属于VLAN 及Switch A对应VLAN接口的IP地址（略）。

Switch A配置源MAC固定攻击检测。

进入系统视图。

```
system-view
```

使能源MAC固定攻击检查，并选择过滤模式。

```
[switchA] arp anti-attack source-mac filter
```

配置源MAC固定攻击检测保护MAC地址。

```
[switchA] arp anti-attack source-mac exclude-mac 0000-5619-0000
```

配置防攻击表项老化时间。

```
[switchA] arp anti-attack source-mac aging-time 600
```

配置防攻击检测阈值。

```
[switchA] arp anti-attack source-mac threshold 30
```

Switch A配置ARP主动确认功能。

使能ARP主动确认功能。

```
[switchA] arp anti-attack active-ack enable
```

Switch A配置ARP报文源MAC一致性检查。

使能ARP报文源MAC一致性检查。

```
[switchA] arp anti-attack valid-check enable
```

配置Switch B的无线特性。

```
system-view
[switchB] interface WLAN-ESS 1
[switchB-WLAN-ESS1] port access vlan 10
[switchB-WLAN-ESS1] quit
[switchB] wlan service-template 1 clear
[switchB-wlan-st-1] ssid abc
[switchB-wlan-st-1] bind wlan-ess 1
[switchB-wlan-st-1] authentication-method open-system
[switchB-wlan-st-1] service-template enable
[switchB-wlan-st-1] quit
```

配置AP 1提供WLAN服务。

```
[switchB] wlan ap ap1 model WA2100
[switchB-wlan-ap-ap1] serial-id SZ001
[switchB-wlan-ap-ap1] radio 1 type dot11g
[switchB-wlan-ap-ap1-radio-1] service-template 1
[switchB-wlan-ap-ap1-radio-1] radio enable
```

配置AP 2提供WLAN服务。

```
[switchB] wlan ap ap2 model WA2100
[switchB-wlan-ap-ap2] serial-id SZ002
[switchB-wlan-ap-ap2] radio 1 type dot11g
[switchB-wlan-ap-ap2-radio-1] service-template 1
[switchB-wlan-ap-ap2-radio-1] radio enable
[switchB-wlan-ap-ap2-radio-1] return
```

Switch B配置ARP Detection特性相关功能。

进入系统视图。

```
system-view
```

配置ARP Detection检查模式，这里启用静态IP、MAC绑定两种检查模式。

```
[switchB] arp detection mode static-bind
[switchB] arp detection static-bind 10.1.1.1 000f-e212-0101
```

进入VLAN视图。

```
[switchB] vlan 10
```

VLAN内使能ARP Detection特性。

```
[switchB-vlan10] arp detection enable
```

显示使能ARP Detection的VLAN ID。

```
[switchB-vlan10] display arp detection
ARP Detection is enabled in the following VLANs:10
```

端口状态缺省为非信任状态，上行端口设置为信任状态，下行端口按缺省设置。

```
[switchB] interface GigabitEthernet 1/0/1
[switchB-GigabitEthernet1/0/1] arp detection trust
[switchB-GigabitEthernet1/0/1] quit
```

Switch B配置报文上送限速。

进入端口视图。

```
[switchB] interface WLAN-ESS 1
```

端口设置报文上送限制速度。

```
[switchB-WLAN-ESS1] arp rate-limit rate 15 drop
[switchB-WLAN-ESS1] quit
```