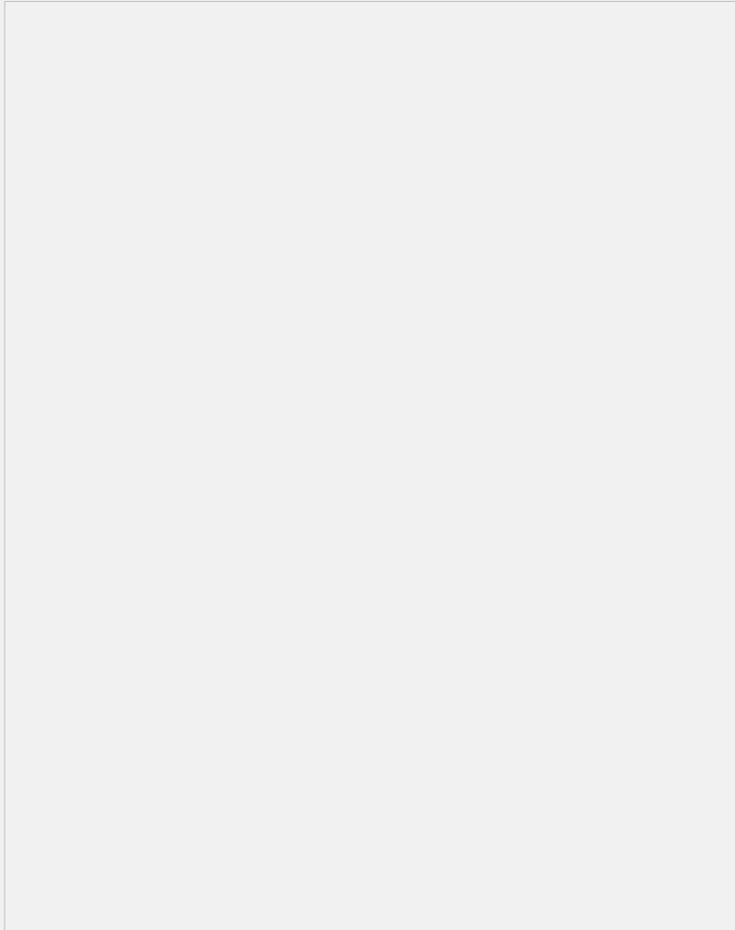


S7502与LanSec软件配合实现网络管理

一.组网需求:



二.问题描述

网络拓扑如上图所示,网管SERVER采用LanSec软件,用于认证服务器,其它计算机必须安装相应的客户端才能接入网络。所有计算机都接入S3600,网关在S7502。

对于没有按要求安装客户端的计算机,网管SERVER向其发送仿冒的ARP报文(包括仿冒网关以及仿冒此网段的其它PC的单播报文,目的MAC是这台没有安装客户端的PC MAC),使该PC不能上网,也不能访问LAN中的其它PC,达到非法计算机被隔离的效果。

但是,当非法计算机(192.168.5.7)从网络断开后,全网都无法正常访问网络。

三.过程分析

1. 查看S7502 ARP表项

断开非法计算机(192.168.5.7)前的正常表项:

```
<S7502_WLG>dis arp
Type: S-Static D-Dynamic
IP Address   MAC Address  VLAN ID  Port Name
192.168.5.250 0019-b947-123d 50    GigabitEthernet0/0/7
192.168.5.245 0014-2a9d-0812 50    GigabitEthernet0/0/7
192.168.5.7   001e-3786-4451 50    GigabitEthernet0/0/7
```

断开非法计算机(192.168.5.7)后的异常表项:

```
<S7502_WLG>dis arp
Type: S-Static D-Dynamic
IP Address   MAC Address  VLAN ID  Port Name   Aging Type
192.168.5.245 0030-1811-2233 50    GigabitEthernet0/0/7 20 D
192.168.5.250 002a-ca48-224e 50    GigabitEthernet0/0/7 20 D
192.168.5.7   002e-4886-4462 50    GigabitEthernet0/0/7 20 D
```

从表项可以看到，S7502学习到仿冒网段的错误ARP表项，造成整个网段的IP地址ARP表项完全错误，所有计算机都无法正常访问网络。

2. 抓包分析

在上联S7502端口抓包发现：

1	0.000000	192.168.5.245	00:1e:37:86:44:51	ARP	v
2	0.001127	192.168.5.250	00:1e:37:86:44:51	ARP	v
3	0.002212	192.168.5.254	00:1e:37:86:44:51	ARP	v
4	0.003295	192.168.5.7	00:1e:37:86:44:51	ARP	v
5	0.004843	JetwayIn_33:22:11	00:1e:37:86:44:51	ARP	v

```
Frame 1 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:30:18:11:22:33, Dst: 00:1e:37:86:44:51
  Destination: 00:1e:37:86:44:51 (00:1e:37:86:44:51)
  Source: 00:30:18:11:22:33 (192.168.5.245)
  Type: ARP (0x0806)
  Trailer: 0000000000000000000000000000000000000000
Address Resolution Protocol (request)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (0x0001)
  Sender MAC address: 00:30:18:11:22:33 (192.168.5.245)
  Sender IP address: 192.168.5.245 (192.168.5.245)
  Target MAC address: 00:1e:37:86:44:51 (00:1e:37:86:44:51)
  Target IP address: 192.168.5.7 (192.168.5.7)
```

LanSec软件通过单播的方式发向非法用户（001e-3786-4451）发送虚假ARP表项报文（真IP，假MAC），使非法用户学习到错误ARP表项。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.5.245	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Tell 192.168.5.245
2	0.001127	192.168.5.250	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Tell 192.168.5.250
3	0.002212	192.168.5.254	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Tell 192.168.5.254
4	0.003295	192.168.5.7	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Gratuitous ARP
5	0.004843	JetwayIn_33:22:11	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Tell 192.168.5.254
6	0.010295	Hangzhou_1f:9b:99	Broadcast	ARP	192.168.5.254 is at 00:0f:e2:1f:9b:99
7	0.016880	Hangzhou_1f:9b:99	Broadcast	ARP	192.168.5.254 is at 00:0f:e2:1f:9b:99
8	2.000004	192.168.5.245	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Tell 192.168.5.245
9	2.001266	192.168.5.250	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Tell 192.168.5.250
10	2.002382	192.168.5.254	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Tell 192.168.5.254
11	2.003454	192.168.5.7	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Gratuitous ARP
12	2.004786	JetwayIn_33:22:11	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Tell 192.168.5.254
13	2.005501	Hangzhou_1f:9b:99	Broadcast	ARP	192.168.5.254 is at 00:0f:e2:1f:9b:99
14	2.013701	Hangzhou_1f:9b:99	Broadcast	ARP	192.168.5.254 is at 00:0f:e2:1f:9b:99
15	3.999982	192.168.5.245	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Tell 192.168.5.245
16	4.001140	192.168.5.250	00:1e:37:86:44:51	ARP	who has 192.168.5.7? Tell 192.168.5.250

```
Frame 1 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:30:18:11:22:33, Dst: 00:1e:37:86:44:51
  Destination: 00:1e:37:86:44:51 (00:1e:37:86:44:51)
  Source: 00:30:18:11:22:33 (192.168.5.245)
  Type: ARP (0x0806)
  Trailer: 0000000000000000000000000000000000000000
Address Resolution Protocol (request)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (0x0001)
  Sender MAC address: 00:30:18:11:22:33 (192.168.5.245)
  Sender IP address: 192.168.5.245 (192.168.5.245)
  Target MAC address: 00:1e:37:86:44:51 (00:1e:37:86:44:51)
  Target IP address: 192.168.5.7 (192.168.5.7)
```

当断开非法用户后，交换机S3600找不到非法用户的MAC地址，于是把此报文作为未知单播进行泛洪。

此报文到达S7502后，S7502会更新自己ARP表项，造成学习到错误ARP表项。

四. 解决办法：

1. 在S7502静态绑定网关和合法用户的ARP表项。
 2. 有些交换机可以抑制未知单播，例如：75E，36等。75不能抑制未知单播。
- 进入相应以太网端口视图，`unicast-suppression { ratio / pps max-pps }`