

Hillstone[®]
ARP防护
解决方案

山石网科通信技术(北京)有限公司
www.hillstonenet.com

Hillstone ARP防护

StoneOS保护MAC地址与ARP协议

1. 介绍

随着网络中交换机使用量的不断增加，我们的网络拓扑变得越来越扁平化。通用的网络部署是通过VLAN来划分交换网络，再使用三层交换或路由器为VLAN之间提供路由服务。VLAN的大量使用使得跨地域的客户机构可以存在于同一个广播网络中。在这样的网络中，基于数据链路层的攻击能够穿越没有进行有效防御的若干个二层设备并且有可能导致整个交换网络的瘫痪。

目前两种主要的二层攻击方法分别是ARP协议攻击和交换机MAC表攻击。

StoneOS提供了多种机制来抵御这些攻击：

- 客户端与网关之间的ARP验证
- IP地址与MAC地址静态绑定
- MAC地址与端口静态绑定
- 开启/关闭ARP学习功能
- 开启/关闭MAC学习功能
- 每MAC的IP地址数限制
- 自动免费ARP包
- 服务器的自动免费ARP包
- ARP反向查询
- 端口隔离
- ARP检查

2. ARP欺骗

ARP(Address Release Protocol)是将IP地址转换为链路层地址的网络协议。在以太网中，链路层的地址就是MAC地址。

传统方式下，需要得到IP地址对应MAC地址的主机通过向外发送ARP请求包的方式学习ARP。这个请求是广播信息，会被发送到以太网中的所有主机。拥有正确IP的主机向发送请求的主机发送一个ARP响应，该响应包含它的IP地址和MAC地址信息。这是一个单播信息。发送请求的主机将返回的IP地址与MAC地址信息对保存起来以备以后使用。

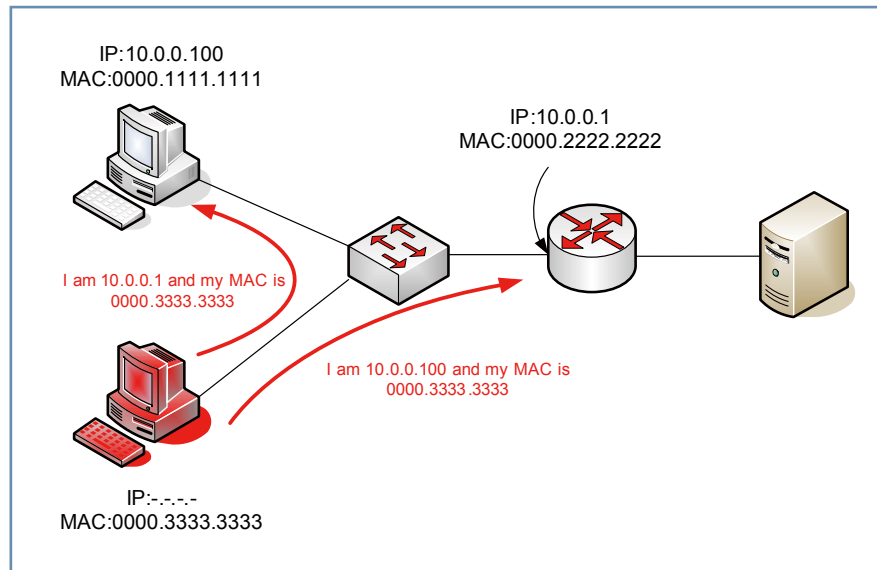
网络主机也可以发送免费ARP包。这个方法是用来探测网络中的冲突IP并且将IP地址变化通报给其它主机。

虽然ARP协议是请求/响应式，但ARP协议实现并不依赖于状态检测。所以，

主机会在未发送ARP请求的情况下收到主动ARP应答。

ARP欺骗（又名ARP缓存投毒）是利用ARP处理的无状态特性，主动的向受害站点发送虚假单播ARP应答包。

图1: ARP欺骗 ▶



如图1所示，攻击者向受害站点和受害网关两端发送ARP应答。如果攻击成功，站点10.0.0.100会认为攻击者（0000.3333.3333）是网关，网关会认为攻击者的IP地址是10.0.0.100并且会把所有从服务器到受害站点的返回流量发送给攻击者。

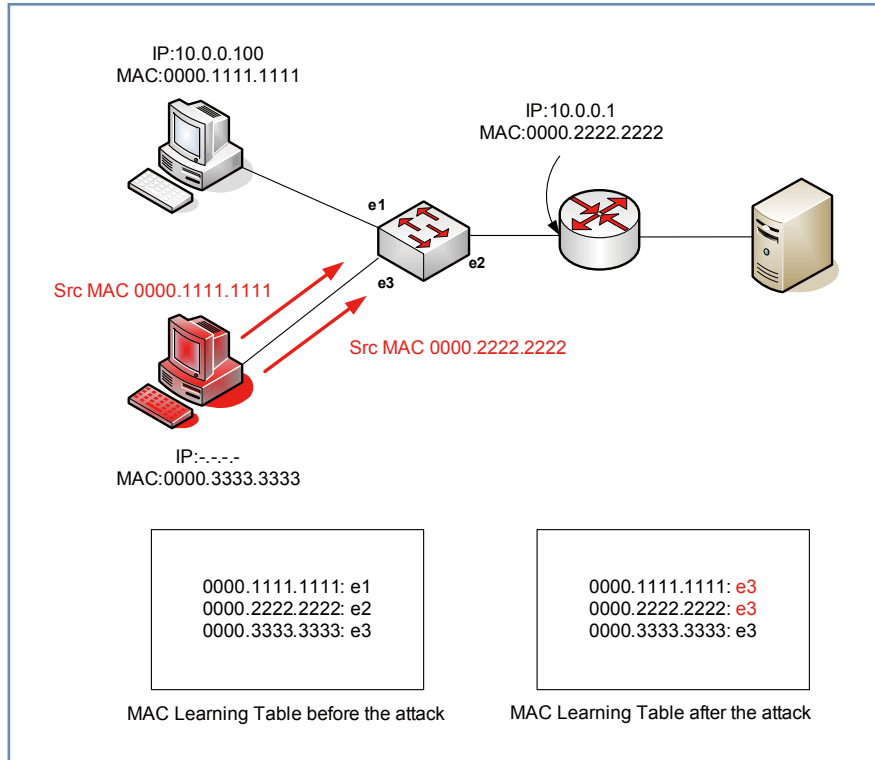
除了拒绝服务，ARP欺骗还可以造成非常危险的中间人攻击。

3. MAC地址/CAM表攻击

二层交换机的基本功能是透过端口获得站点的MAC地址，避免了像网络集线器那样，向所有端口发送不必要的洪水流量。攻击者可以利用这个技术来实现流量重定向和拒绝服务攻击。

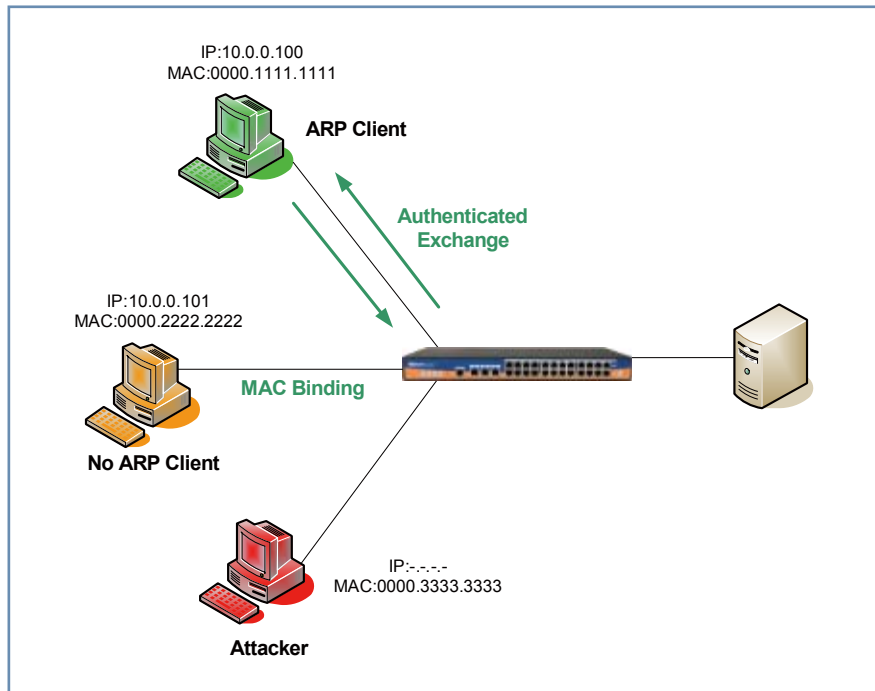
如下图2所示的虽然是一个简单得令人吃惊的攻击，但现在许多网络却不能防御这种攻击。攻击者首先利用ARP来扫描网络从而获得当前站点的IP和MAC地址，然后攻击者简单地向交换器发送伪造的源MAC地址，这样交换机的MAC学习会受到混淆。如果攻击者以足够短的间隔向外发送这种类型的流量，那么这些流量将淹没其它合法的流量，交换机会将以后发往这些MAC地址的流量转发给攻击者。通常情况下，这会引入网络的拒绝服务。

图2: 二层交换机攻击 ▶



4. StoneOS解决方案

图3: Hillstone集成网关: 集成防火墙、交换机和路由器的功能 ▶



Hillstone设备集成防火墙、路由器和交换机功能于一体，提供一整套丰富、完善的方案保卫网络、防护二层攻击。

4.1 Hillstone ARP客户端

事实表明，在一些Windows平台上，即使是静态绑定的ARP条目仍然可以被ARP攻击改变。StoneOS支持一个专有的协议来认证ARP请求和响应。对于那些很难做静态绑定或者不能做静态绑定的网络环境来说，这是一个最好的解决方案。

装有Hillstone ARP客户端的PC会与Hillstone设备进行基于身份认证的ARP协议通讯（见图3），这就保证每台安装客户端的PC能够获得来自于Hillstone设备认证过的设备MAC地址。这个交换使用公钥基础设施（PKI）来确保ARP信息的真实性。该协议执行强大的反伪造和防重放机制，使系统免受各种攻击，包括伪造的ARP包和重放的ARP包。

ARP客户端还可以监控PC的可疑二层行为并阻断受感染的PC对同一局域网内的其他PC或网络设备发动ARP攻击。

此外，StoneOS可以探测客户端是否安装了ARP验证工具并且在客户端安装该工具之前拒绝其访问Internet。这一功能帮助管理员强制部署ARP防护策略。这个协议和工具能够向下兼容传统的ARP协议。因此，如果策略允许，将不会出现跟原有设备/客户端的互操作问题。

ARP客户端不需要任何设置。每一台PC只需要执行一次安装，之后不需要任何操作，十分简便。

4.2 无客户端ARP与二层防护

- 静态IP/MAC绑定：静态IP/MAC绑定是防ARP欺骗攻击的最有效的方法之一。静态绑定的IP和MAC地址条目不会被ARP请求和响应改变，这种方法的缺点是它需要极高的管理维护成本。StoneOS通过“实时扫描加静态绑定”功能来减轻管理负担，容易操作。这一功能允许管理员扫描网络中的所有站点并且自动执行静态绑定功能。该功能还可以和“开启/关闭ARP学习”结合使用，实现更理想的安全防护。

- 静态MAC/端口绑定：和静态IP/MAC绑定相同，静态MAC/端口绑定可以防御以上描述的MAC地址表攻击。如果MAC地址已经与端口静态绑定，交换机将忽略学习到的MAC，MAC/端口信息与设备中静态绑定的MAC/端口信息不一致的数据包将会被丢弃。该功能可以与“开启/关闭MAC学习”功能相结合使用，实现更理想的安全防护。StoneOS将MAC/端口绑定功能集成到“扫描加绑定”功能中，使MAC/端口绑定功能的实现变得简单。管理员仅仅需要点击一个按钮，就可以同时启动静态IP/MAC绑定功能和静态MAC/端口绑定功能。

- 开启/关闭ARP学习：关闭ARP学习意味着除了与IP地址作了静态绑定的那些MAC地址，所有使用其它MAC地址的主机将不能通过Hillstone进行路由。

- 开启/关闭MAC学习：关闭MAC学习功能意味着除了与端口作了静态绑定的那些MAC地址，所有使用其它MAC地址的主机将不能通过Hillstone设备进行交换。

- ARP欺骗探测：当两个MAC地址通告使用同一个IP地址时，Hillstone设备会报告地址冲突，此时表明网络中出现了ARP欺骗。

2007-11-28 09:56:38	警告	网络：MAC地址001c.5400.0900的IP地址10.160.65.51与接口ethernet0/0的IP地址冲突
2007-12-06 14:40:02	警告	数据流：ARP欺骗攻击：警告！MAC地址0013.c36b.0e80和0090.fb0a.2763在接口ethernet0/1上有同样的IP地址10.160.33.149

- 每MAC的IP地址数限制：StoneOS能够限制每个MAC地址相对应的IP地址数。将该数值设置为1能够有效限制ARP欺骗和避免中间人攻击。

- 自动免费ARP包：StoneOS能够周期性地发送免费ARP包来防御那些伪装成Hillstone设备IP地址的攻击者。

- 服务器的自动免费ARP包：StoneOS能够帮助服务器发送免费ARP包来防御那些伪装成服务器IP地址的攻击者。

- ARP反向查询：当收到ARP请求/响应和免费ARP包时，Hillstone设备记录发送者的MAC地址并且向发送者发出ARP请求，然后检测返回的结果是否与储存的MAC地址相匹配，如果不匹配，Hillstone设备将忽略此ARP包，防止受到欺骗。

- 端口隔离：StoneOS提供该功能使每一个端口形成自己单独的广播域，从而进行网络保护。它能够保护从一个域的分支到另一个域的跨域二层攻击。

- ARP检查：Hillstone产品的透明模式和混合模式都能够支持ARP检查。Hillstone设备会对所有通过设备的ARP包进行本地静态IP/MAC绑定检查。

5. 结论

Hillstone的StoneOS是一个专业的安全操作系统，它将安全防护与传统的路由和交换等网络功能相结合，并引进一系列安全防护特性，对ARP和二层攻击进行了广泛而有效的防护。这些安全防护机制能够保护ARP学习表和MAC学习表，有效防御了来自内部和外部的攻击。



山石网科通信技术(北京)有限公司

www.hillstonenet.com

北京总部

地 址: 北京市海淀区上地七街1号
汇众大厦3层
邮 编: 100085
电 话: +86(10)8289 7229
传 真: +86(10)8289 9814

上海办事处

地 址: 上海市陕西北路1388号
银座企业中心1721室
邮 编: 200060
电 话: +86(21)6149 8205
传 真: +86(21)6149 8001

成都办事处

地 址: 成都市总府路2号
时代广场A座26层2625
邮 编: 610016
电 话: +86(28)6606 7115
传 真: +86(28)6606 7199

广州办事处

地 址: 广州市天河区天河路208号
粤海天河城大厦13层1363室
邮 编: 510620
电 话: +86(20)2826 1950
传 真: +86(20)2826 1999

服务热线: 400-650-0259

Copyright © 2008, Hillstone Networks, Inc. 版权所有，保留所有权利。

Hillstone Networks、Hillstone Networks标识、Hillstone、Hillstone标识、StoneOS、StoneManager、Hillstone SA-2003、Hillstone SA-2005、Hillstone SA-2010、Hillstone SA-5020、Hillstone SA-5040、Hillstone SA-5050、Hillstone SR-330、Hillstone SR-530和Hillstone SR-550为Hillstone公司的商标。所有其他商标和注册商标均为本公司的财产。

本文所包含信息可能会有所修改，恕不另行通知。