地址解析服务(ARP)检查在300系列被管理的交换机的属性配置

客观

地址解析服务(ARP)用于映射IP地址到MAC地址。ARP检查用于保护网络免受ARP攻击。ARP检查强化交通安全在成不信任被定义的接口在*Settings页的接口*信息包的检查。 当信息包在不信任的接口时到达， ARP检查查看信息包的IP原地址和MAC地址。 如果他们匹配IP地址，并且MAC地址在ARP访问控制规则查找，则转发信息包，否则信息包被丢弃。

此条款说明如何配置在300系列被管理的交换机的ARP检查。

可适用的设备

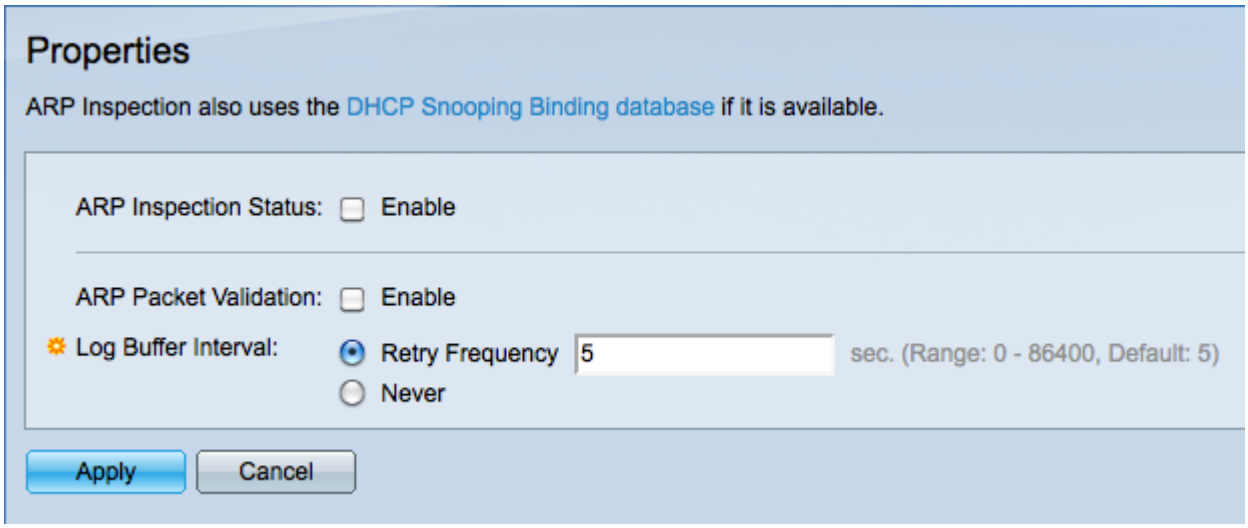
•SF/SG 300系列被管理的交换机

软件版本

•1.3.0.62

属性

步骤1.登陆到Web配置工具并且选择**安全> ARP检查>Properties**。*Properties页*打开：



Step 2.检查在ARP检查Status字段的**Enable复选框**对enable (event) ARP检查。

第3.步(可选的)检查在ARP信息包验证字段的**Enable复选框**对enable (event)以下验证。由ARP检查认为无效的信息包被记录并且被丢弃。

•源MAC —信息包的源MAC地址与发送方的MAC地址比较在ARP请求的。此检查为ARP请求和ARP响应被执行。

•目的地MAC —信息包的目的地MAC地址与接口的目的地MAC地址比较。此检查为ARP响应仅被执行。

•IP地址—比较无效的IP地址的ARP正文。这些地址包括0.0.0.0、255.255.255.255和所有IP组播地址。

步骤4.点击对应于在日志缓冲器间隔字段的期望选项的单选按钮。 如果流入信息包的IP原地址不可能由ARP检查找到，则信息包被丢弃，并且传送系统消息。日志缓冲器间隔是在系统消息之间的时间。

•重试次数频率—输入定义了频率(以秒钟) SYSLOG丢弃的数据包信息传送的值。

•从未—功能失效SYSLOG丢弃的数据包消息。

步骤5.点击**适用**保存更改或**取消**取消更改。