交换机应对网络攻击的安全防范措施简析

蔡周明

（长讯通信服务有限公司　广东　汕头　515021）

[摘　要]交换机作为我国网络中的硬件设备与我国网络的整体安全起着较为重要的影响，因此需要我国工作人员予以高度重视，更好的保护我国网络安全。因此，本文重点对于我国交换机存在的安全隐患进行分析与探讨，同时提出较为合理的解决对策，来帮助我国工作人员解决交换机在实际应用中出现的问题，来促进我国安全通信发展。

[关键词]交换机；网络攻击；安全防范措施

【DOI】10.12252/j.issn.2096-627X.2021.05.2025

一、阐述交换机概念

笔者通过调查了解到，交换机主要是利用我国通信设备所传达的信息需求来进行工作的，主要是将所传播的信息由人工或者自动化设备来进行路由转播的这类技术统称为交换机。并且据调查了解到，交换机的位置至关重要，他是我国一些网络攻击较为频发的位置，因此，为了更好的促进我国数据传播安全就要注重对于交换机的保护。与此同时，就需要工作人员予以高度重视。并且据调查了解到，为了更好地构建我国安全的计算机网络应用，以期可以更好的保障交换机可以安全有效运转，同时提升我国网络通讯安全可持续发展。

二、分析交换机的安全威胁

笔者通过对于我国交换机在实际的使用过程之中存在的安全威胁进行分析与探讨，了解到它主要包含以下几个方面内容，第一是它容易受到ARP攻击。它主要是是指地址解析协议。主要是对于一些地址信息和接口位置的映射。并且据调查了解到，我国ARP攻击主要是针对这类项目攻击的技术，他带来了巨大的负面影响。对于一些信息进行破坏，使得出现一些较大故障。从而致使所有的计算机无法正常有效连接。并且据调查了解到它主要包含两种类型的攻击，首先是洪泛攻击，其次是主要是欺骗。它的洪泛攻击主要是指攻击者伪造了映射，同时对于其在网络上与主机相关的数据产生一些拥堵，使得整个网络无法正常有效进行通讯工作。不仅如此，他的ARP欺骗主要是指伪装者伪装成网关网络中的某台主机，使得拦截整个网络中的数据包，以达到窃取目的。并且据调查了解到，如果局域网内出现了一些。 ARP攻击就会严重影响着主机与服务端的映射关系，从而导致整体通讯网络被控制，从而影响信息安全。

第二是DOS攻击。DOS主要是指拒绝服务，这类攻击行为被称为DOS攻击。并且据调查了解到，攻击者设法将目标主机进行停止服务，同时影响资源，即网络宽带等正常的用户访问，从而使得攻击目标无法正常有序工作。并且据调查了解到受网络宽带的影响，DOS攻击者可以采用分布式的攻击方法对同一个目标进行主动攻击，这样就会导致这段网络进行有效破坏，从而使得受害者无法及时接收并处理外界要求。

第三是MAC地址泛洪攻击。它主要是指数据被装成帧在网络上传输。并且在进入交换机时则会记录下原MAC地址，会产生一条与地址相关的关联记录，从而支持着MAC地址的信息流，只能通过该端口进行有线转发。并且如果恶意者有意识的向CAM发送大量伪造数据包，就会导致CAM被占满，从而导致整体网络受到严重威胁。

三、交换机的安全防范措施

据上述调查了解到，为了更好的保障，我国交换机可以正常安全有效地运转，就需要对于一些非法问题进行有效打击，同时采取较为合理的安全防范措施，加强我国交换机的安全配置，从而更好地促进我国网络安全。

第一针对ARP攻击防护。他主要要求工作人员可以配置交换机的端口的安全策略来进行有效防御。具体做法如下：第一步，要求工作人员在进行前期准备工作时，要先了解源MAC地址的阈值，并熟知交换机的安全策略设置位置，并安排一个合理的模式来进行信息传递和病毒监管。从而促进我国通信过程中的信息可以安全传递。并且当出现一些违反法律和出现一些意外时，就会产生一定的质量，对于一个攻击源进行及时的调查，及时关闭攻击源所连接的交换机端口，使得我国攻击源与其他网络逻辑断开。

与此同时，对于ARP欺骗攻击可以在网络中设计一定的监测点，以期能够更好的针对网络中的ARP数据包进行有效监听，根据真实网关和主机的映射，对于一些网络中的虚假包进行有效监管。以避免产生一些问题，从而影响到整体交换机端口的安全运转。

第二是针对DOS攻击防御。为了更好的促进DOS攻击防御工作开展，就需要采用交换机的控制列表功能，同时对于一些过滤数据包进行有效监管和控制，实现对于报文的过滤和控制工作。并且利用这类功能可以将未经授权用户的非法接入进行有效防止同时提升我国网络性能，有效抵制DOS攻击。

第三点是主要针对MAC地址泛洪问题。主要分为三种防御方法，首先是利用交换机的各个定对端口允许接入的计算机MAC地址设定，更好的绑定计算机。第2种方法主要是采用基于端口的访问控制协议方法，这也是一种连接入网的认证和授权手段，从而在端口上进行设备认证，通过授予合法用户，更好地保护我国网络安全。第3类主要是设置动态虚拟网络，这样可以更好的针对MAC地址划分对应的区域网，同时保持各部分的通讯安全。

第四交换机的VLAN划分计划。划分VLAN是交换机的一项重要安全功能，因此需要工作人员予以高度重视。它主要是指通过有限的广播，在二层或三层之上的交换机中得以具体开展，同时将网络划分为多个单独的区域，对于每个区域进行及时的控制与检测，更好地为我国通讯工作开展打下坚实基础。不仅如此，它可以结合一些MAC地址的绑定，对于网络用户的安全问题进行有效控制，以避免由于一些区域疏于管理而产生一些负面影响，同时它利于控制网络流量，降低我国广播流量的数量，减少了我国泄露机密信息的可能性。

结束语

综上所述，我们不难看出交换机作为我国网络中的核心节点，因此需要予以高度重视，以期可以利用各类交换机的安全保护措施来最大限度的管理我国网络中的违法问题，避免由于一些非法入侵行为，造成我国网络安全信息大量泄漏，从而引发通信安全问题。注重交换机的安全防范举措推进落实，更好的保障整个网络安全，为我国通信可持续健康发展打下坚实基础。

参考文献

[1]任文.浅析内网的网络攻击与安全防范[J].硅谷,2011,(9):185-185.

[2]王朝岗,韩珂.计算机在网络中安全防范措施分析[J].才智,2014,(34):338-338,341.

[3]方富贵.网络攻击与安全防范策略研究[J].软件导刊,2011,10(6):136-137.

[4]汤韬.探讨常见计算机网络攻击手段及安全防范措施[J].计算机光盘软件与应用,2014,(12):175-176.