高等学校计算机类国家级特色专业系列规划教材

网络安全协议分析与案例实践

赖英旭 田果 刘静 李健 刘丹宁 杨震 编著

清华大学出版社

高等学校计算机类国家级特色专业系列规划教材

网络安全协议分析与案例实践

赖英旭 田果 刘静 李健 刘丹宁 杨震 编著

清华大学出版社
北京

内 容 简 介

本书比较全面地介绍了网络安全协议的关键技术和主要应用模式。特别对 VPN 网络的特点、分类及应用模式等方面进行了比较深入的分析和探讨。

本书介绍数据链路层安全协议、网络层安全协议、传输层安全协议、会话层安全协议和应用层安全协议等方面的内容。本书重点阐述了三种常见的 VPN 网络应用模式，并比较详细地介绍了 VPN 网络的工作原理和配置。本书还介绍了网络协议安全性的测试工具，并以应用范例的方式介绍了测试工具的使用方法。

本书通俗易懂，注重可操作性和实用性。采用大量、真实案例讲解安全协议的应用，在真机实验设备上，分步介绍网络安全协议的环境搭建、命令配置、安全性测试等内容。使读者能够举一反三。

本书可作为广大计算机用户、计算机安全技术人员的技术参考书，特别是可用做信息安全、计算机与其他信息学科本科生的配套实验教材。同时，也可用做计算机信息安全职业培训的实验教材。

图书在版编目（CIP）数据

网络安全协议分析与案例实践/赖英旭等编著. —北京：清华大学出版社，2015
高等学校计算机类国家级特色专业系列规划教材
ISBN 978-7-302-42268-6

Ⅰ. ①网…　Ⅱ. ①赖…　Ⅲ. ①计算机网络－安全技术－通信协议－教材　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 283627 号

责任编辑：汪汉友　战晓雷
封面设计：傅瑞学
责任校对：梁　毅
责任印制：刘海龙

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn,010-62795954

印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：8.75　　**字　　数**：220 千字
版　　次：2015 年 12 月第 1 版　　**印　　次**：2015 年 12 月第1次印刷
印　　数：1～1000
定　　价：23.00 元

产品编号：060302-01

前　言

网络存在的目的就是为了能够让合法的用户访问相应的资源，但原有的网络协议存在太多的安全漏洞，在网络上传输的数据非常容易受到各种攻击。本书主要介绍了从数据链路层到应用层安全协议在保证数据传输安全性方面所采取的关键技术，使读者了解安全协议如何在原有协议基础上提供的安全保障。同时，本书作为《网络安全协议》一书的实验指导书，由北京工业大学计算机学院网络安全教学团队与 Yeslab 公司资深工程师共同编写，书中采用大量案例讲解安全协议的应用，同时，在真机实验设备上，分步介绍网络安全协议的环境搭建、命令配置、安全性测试等内容。

本书分为 7 章，具体内容如下：

第 1 章：基础知识与物理安全。主要介绍了信息安全的三个要点、网络拓扑常用模型、网络设备管理方法，以及物理安全的一些建议，使读者清晰地了解网络基础架构安全、网络协议安全的重要性。

第 2 章：数据链路层安全与相关特性。本章先介绍了原有数据链路层协议的安全问题，为了增强数据链路层协议的安全性，本章以应用实例着重介绍了局域网数据链路层安全威胁及防御方法。

第 3 章：网络层安全与 IPSec VPN。本章详细地介绍了网络安全协议 IPSec 的体系结构，IPSec 所包含的安全协议、安全联盟和密钥交换等关键技术。然后又以实例介绍了经典站点到站点 IPSec VPN、经典 DMVPN，给出了网络拓扑、实际接线图已经主要配置命令。

第 4 章：传输层安全与 SSL VPN。本章详细分析传输层安全协议 SSL 的握手协议和记录协议。介绍了 SSL VPN 的三种连接方式，并与 IPSec VPN 做了对比分析。最后，给出了经典瘦客户端 SSL VPN 的配置命令和测试步骤。

第 5 章：会话层安全与 SSH。本章介绍了会话层安全协议 SSH 的主要安全机制、SSH 身份认证协议和 SSH 连接协议。为了使读者对 SSH 协议的应用理解得更加深入，还对 SSH 的典型应用案例进行了介绍。

第 6 章：通过 ASA 实现 VPN 连接。本章介绍如何通过实际设备 ASA 构建站点到站点 IPSec VPN，给出了实验拓扑和配置命令；如何通过 ASA 实现无客户端的 SSL VPN，给出了实验拓扑和配置命令。

第 7 章：AVISPA 安全协议分析工具分析。本章介绍了安全协议分析的重要工具——AVISPA。本章重点讲述了 AVISPA 的工具概述和使用方法，并根据范例介绍了分析工具的使用和结果分析。

本书由北京工业大学的赖英旭、刘静和 Yeslab 公司资深工程师田果、刘丹宁共同编写，其中第 1、3、7 章由赖英旭编写，第 4、5 章由田果编写，第 6 章由刘静编写，第 2 章由刘丹宁、杨震编写。全书最后由赖英旭和田果统稿，李健审定。

本书的研究和编写工作受到教育部“卓越工程师人才培养计划”资助。本书从各种论文、书刊、期刊以及互联网中引用了大量的资料，在文字的录入和整理中，得到了李健老师的帮助，在此谨向他们表示衷心感谢。

由于时间和水平有限，难免有误，恳请读者批评指正，使得本书得以改进和完善。

作　者

2015 年 8 月于北京

目　录

第 1 章　基础知识与物理安全

1.1　信息安全三要点

自从互联网延伸到最初的几所高校之外，针对它的恶意使用便层出不穷。在早期，由于网络的安全性问题尚未引起人们的广泛关注，因此很多与网络基础架构有关的协议并不具备相应的安全保护措施。最近几年，尽管已经没有人能够忽视网络安全的重要性，但伴随着移动时代和云时代的到来，信息所在的位置变得越来越模糊，因此，在边界部署安全策略这一传统做法就会显得捉襟见肘，于是，如何更好地保护无边界网络成为又一大困扰人们的课题。

网络的攻击方式固然林林总总，但信息安全的核心原则却可以概括为私密性（Confidentiality）、完整性（Integrity）与可用性（Availability）三点。有人取三个单词的英文首字母，将其称为信息安全的 CIA 三原则或 CIA 三要点，如图 1-1 所示。

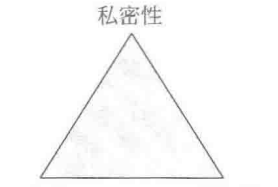

图 1-1　CIA 三原则

1.1.1　私密性

破坏信息的私密性是最为常见的攻击方式，这类攻击方式可以泛称为窃取。心怀鬼胎的人通过各种方式获取通信双方之间传递的敏感信息，并利用这些信息对信息的失窃者予取予夺，如图 1-2 所示。

图 1-2　窃取敏感信息

为了保障通信的私密性，最常见的手段是对穿越公共媒介的数据进行加密。这可以让敏感信息对非授权人员变得“不可读”，使非法窃取信息的人无从利用这些信息，如图 1-3 所示。

由于机密性在网络安全中扮演的角色极其重要，很多人甚至会认为实现了信息的机密性就等同于实现了网络安全，这种认识当然有失偏颇。从网络安全的核心原则来看，信息的完整性与可用性对于实现通信安全扮演着同样重要的角色。

1.1.2　完整性

完整性是指信息在传输过程中没有遭到如图 1-4 所示的篡改。换言之，如果信息是完

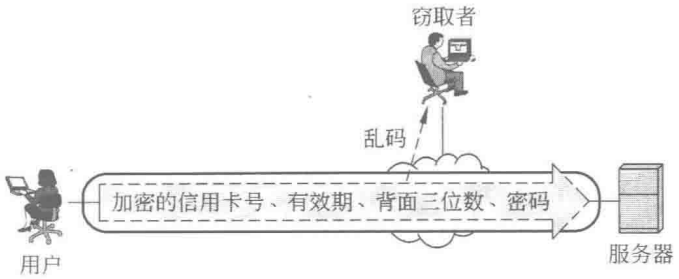

图 1-3　通过加密保障通信的私密性

整的，就表明信息接收者获得的信息与原始信息别无二致。

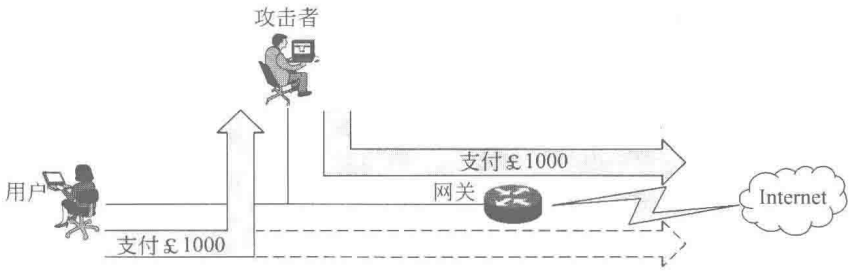

图 1-4　攻击者篡改通信信息

在图 1-4 中，攻击者借助中间人攻击截取了用户发往网关的信息，并对该信息进行了篡改（在第 2 章会介绍一些攻击者在局域网中创造中间人攻击环境的手段）。

为了保障接收到的信息是可靠的，通信双方可以对信息进行完整性校验。通过完整性校验，接收方可以发觉自己接收到的信息遭到了篡改，并立即采取措施。

1.1.3　可用性

网络存在的目的就是为了能够让合法的用户可以访问相应的资源，让合法用户无法访问数据的攻击方式一般称为拒绝服务（DoS）攻击。顾名思义，若网络由于攻击者发起的攻击而拒绝为合法用户提供服务，那么这个攻击者就破坏了网络的可用性。

实现拒绝服务攻击的方式有很多，除了设法耗尽资源之外，对通信的一方或双方进行欺骗，也是实现拒绝服务的一种常见方法。

表面上看，中断服务对用户造成的影响似乎并不如窃取或篡改用户信息造成的影响恶劣，但发起拒绝服务攻击的门槛较低，没有专业技能的人也可以轻易做到；此外，窃取和篡改信息往往是针对个别用户所进行的攻击，而拒绝服务攻击则往往会造成大量用户无法获取服务，进而对多项业务的开展造成严重影响，因此同样不可小觑。

1.2　常用基本概念

1.2.1　OSI 模型

OSI 模型是国际标准化组织提出的网络互联框架，全称为开放式系统互连参考模型。

由于 OSI 七层模型构成了本书的重要线索，因此有必要对其进行简要的回顾。

在 OSI 模型中，下层是上层的基础和依托，如果下层失效，上层便无法工作。OSI 七层模型如图 1-5 所示。

OSI 模型七层的功能在大量材料中都有提及，这里不再赘述。

1.2.2 网络拓扑与物理连接

在实施和维护网络时，必须使用相应网络的拓扑来开展工作。但网络的逻辑拓扑往往与物理连接方式不尽相同。由于高校相关课程往往侧重网络环境的逻辑层面，因此这一点必须特别注意。

图 1-6 展示了一个网络的逻辑拓扑。

图 1-5 OSI 七层模型

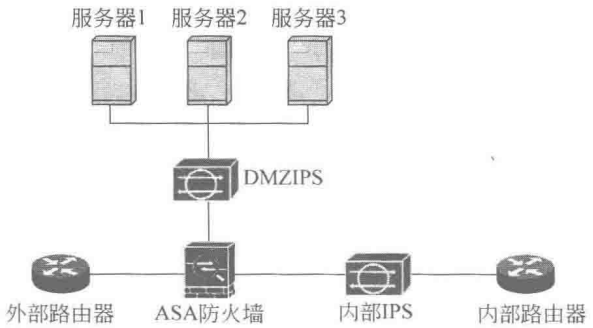

图 1-6 一个网络的逻辑拓扑

这个网络的实际物理连接有可能与逻辑拓扑相去甚远，如图 1-7 所示。

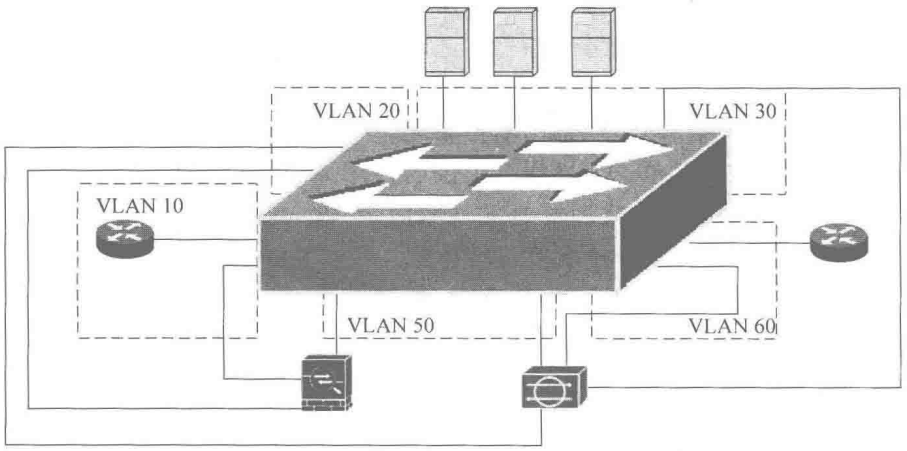

图 1-7 一个网络的物理连接

如图 1-7 所示，逻辑拓扑中的所有设备可能都物理地连接在一台 2 层交换机上，并通过划分 VLAN 的方式形成了图 1-6 所示的逻辑网络，但逻辑拓扑中并不会包含这台 2 层交换机。此外，逻辑拓扑中的两台 IPS 也有可能是同一台设备在不同网段中的复用。

在对网络进行安全性设计时，应该参照 1.2.1 节中的 OSI 模型，按照自顶向下的方式，先根据需求设计出逻辑拓扑，然后再根据逻辑拓扑决定设备的实际连接方式。在实施项目

时，则必须采取自底向上的方式，先搭建物理连接，然后创建出逻辑拓扑的环境，然后再实施相应的网络需求。

1.2.3 设备的管理方式

管理网络设备有两种方式，即本地管理和远程管理。

1. 本地管理

本地管理要求管理员能够在物理上接触到网络设备。管理的方式是将管理设备的计算机与被管理设备的管理端口直接物理相连，然后使用计算机上的虚拟终端程序对设备进行配置。图 1-8 为使用 Console 连接线连接笔记本电脑和交换机，以对交换机进行管理的示意图。

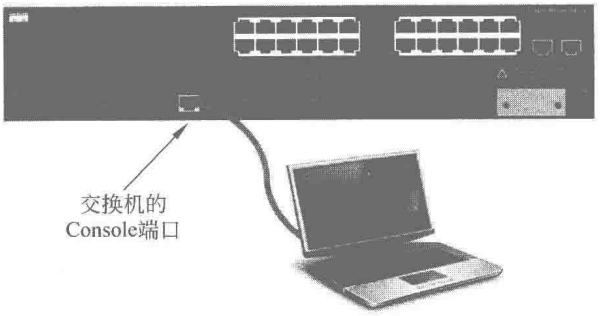

图 1-8 使用笔记本电脑对交换机进行本地管理

在管理思科网络设备时，传统上，管理员可以通过一根 Console 连接线连接电脑的串行接口，然后依次选择“开始”→“程序”→“附件”→“通讯”→“超级终端”，打开 Windows 自带的虚拟终端程序，然后选择与网络设备相连的串口，再按照图 1-9 所示设置该串口属性即可。

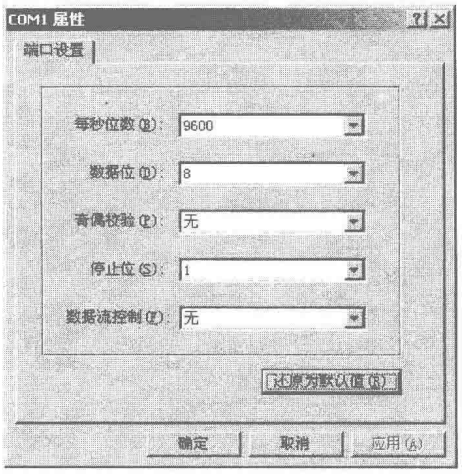

图 1-9 串行端口的设置

但是近来多数超薄笔记本电脑都已不再装配宽大的串行端口，最新的 Windows 操作系统也取消了自带的超级终端程序。在这种情况下，要通过连接网络设备的 Console 端口来对其进行本地管理，就需要购入 USB 转串行端口（RS 232 端口）的转接口，并安装相应的驱动程序，然后再自行下载虚拟终端程序。

2. 远程管理

远程管理是指通过远程管理协议对设备发起管理访问。为了实现远程管理，必须先让管理设备能够与被管理设备的管理地址进行通信，而这需要先通过本地管理对被管理设备执行初始化配置。

最为常用的远程管理协议是 Telnet 协议，但是 Telnet 协议只能提供用户认证，却无法对设备之间的管理信息提供私密性保护。因此，在通过不安全媒介对设备发起远程管理访问时，应先对被管理设备进行预配置，使其只能接受通过安全外壳协议（SSH）发起的安全远

程管理访问。关于 SSH 协议，将在第 5 章详细介绍。

大多数思科设备都可以通过两种类型的界面进行管理，即命令行界面(CLI)和图形化(GUI)界面。本书只介绍通过命令行界面管理设备的方式。

1.3 物理安全建议

在一般的网络安全策略中，相比远程管理用户，本地管理用户需要提供的身份认证往往要少一些。而且，为了避免合法的用户因为忘记密码而无法管理设备，网络设备大都为那些能够在物理上接触到设备的用户提供了密码恢复的机制。

注意：在有些思科公司生产的设备上，可以通过命令 no service password-recovery 禁止用户通过冷启动设备进入 ROMMON 模式，并修改寄存器值的方式来重设 enable 密码。这种做法虽然可以在一定程度上提高安全性，但管理员一旦忘记 enable 密码需要付出的代价则惨痛得多。权衡利弊，建议不要轻易使用这条命令。提高物理环境的安全性，让恶意用户无法接近设备方为上上之策。

除了设备之外，线缆安全同样值得关注。具备窃听工具的入侵者如果能够接触到线缆(无论非屏蔽双绞线还是光纤)，就可以对其中的信息进行窃听。当然，从介质的传输原理也不难发现，相比双绞线，窃听光纤的难度要大得多，而且会造成正常传输数据的中断，因此窃听行为也更容易被发现。

即使入侵者不具备任何技术能力，他/她只要能够在物理上接触到设备，就可以绕过逻辑层面，直接对设备发起“物理攻击”(哪怕只是拔掉设备的数据线或电源线，造成的“拒绝服务”攻击也比通过泛洪数据包要有效和直接得多)。总之，通过物理方式造成的破坏，是用任何逻辑策略都无法消弭的。因此，只要入侵者能够轻易地摸到设备外面的那层铁壳，许多逻辑层面的安全技术也就形同虚设。尽管物理安全与网络技术关系不大，但物理安全绝对是网络安全的基本前提。

综上所述，为了让恶意用户难于接触到网络设备，应该对设备所在的机房安装指纹认证系统。这可以防止居心叵测之徒通过窃取机房的钥匙或门禁卡进入机房。如果不具备安装指纹系统的条件，至少要选择安装门禁卡。门禁卡比门锁更可靠，因为一旦有员工离职，离职的员工在交还钥匙之前有可能为自己配一把钥匙，有了门禁卡即使离职的员工未交还钥匙，也无法再顺利进入机房。

此外，虽然很少有机房做到这一点，但最理想的做法是在机房安装感应式闸门或十字转门，否则指纹认证和门禁卡都无法防止有人尾随合法用户进入机房。

保障网络基础设施的物理安全是一项繁杂而艰巨的工作，方式方法不胜枚举，也难以在书中一一尽数，因此这里仅提供有限的几点参考意见，希望能够抛砖引玉，让物理安全得到重视。

思 考 题

1. 请尝试使用 Microsoft Visio 画出图 6-5 所示的逻辑拓扑在实验室环境中可能的物理拓扑结构。

2. 请通过查询相关资料，简述在本地恢复某型号网络设备密码的步骤，不限设备厂商。并请尽可能创造条件，通过实验对这一过程进行测试。

第 2 章　数据链路层安全与相关特性

2.1　局域网中常见的二层威胁与防御技术

在数据传输的过程中，数据链路层下启物理层，上承网络层，重要性不言而喻。然而，由于数据链路层看似总是能够正常工作，因此这一层的安全性常常为人们所忽视，这使得数据链路层成为网络中安全性最薄弱的环节，针对这一层的攻击方式也层出不穷。作为 OSI 模型中的第二层，网络层及更高层的信息都需要封装进某种二层数据帧中，因此如果数据链路层不能得到有效的保护，让攻击者可以干扰二层数据的转发，那么网络层及以上无论采取什么安全策略也都无济于事。

根据美国联邦调查局 2005 年发布的一份与计算机犯罪和安全有关的报告，在所有针对企业网络的攻击中，有 70%来自内部网络。但现状是，企业针对网络安全的投资大都用于防护来自公共网络的攻击，更为重要的内部网络安全反而成为人们的盲点。

由于网络层及以上的安全技术多用于防御来自公共网络的攻击，而针对数据链路层的攻击却几乎都是在局域网中发起的，因此本章对局域网中一些常见的数据链路层攻击进行介绍，并推荐一些思科交换机上能够缓解这些攻击的安全特性。

2.1.1　CAM 表溢出攻击与端口安全

1. CAM 表简述

交换机可以将数据帧通过与其目的 MAC 地址设备相连的那个端口转发出去。这一点与集线器只能将数据通过其所有的接口广播出去的行为明显不同。

交换机这种有针对性的转发行为需要依赖 CAM 表来实现。在初始状态下，这张转发表为空，此时，交换机并不知道各个设备与端口的连接关系。而当与交换机相连的设备向交换机发送数据帧时，交换机就会立刻将数据帧的源 MAC 地址与接收到该数据帧的端口作为一个条目保存到 CAM 表中。图 2-1 和图 2-2 分别为 CAM 表的初始状态和交换机接收到第一个数据帧之后 CAM 表的状态。

一旦交换机拥有了图 2-2 中的 CAM 表条目，它就会在该条目失效之前，将目的 MAC 地址为 A 的数据帧通过端口 Fa0/3 转发出去。

2. CAM 表溢出攻击

显然，CAM 表需要占用交换机的内存资源，因此它的容量不可能是无限的，一般来说，CAM 表能够保存的条目为数千条到数十万条不等。当 CAM 表中保存的条目已满时，如果交换机接收到了以 CAM 表中没有记录的 MAC 地址作为目的地址的数据包，它就会像集线器一样将该数据帧通过(该 VLAN 内的)所有端口进行泛洪。因此，如果攻击者想要接收自己所在 VLAN 中的所有数据帧，只需设法用不同的 MAC 地址将 CAM 填满即可，如图 2-3 所示。

图 2-3 为一个 CAM 表容量为 8000 个条目的交换机遭到了 CAM 表溢出攻击的情形。

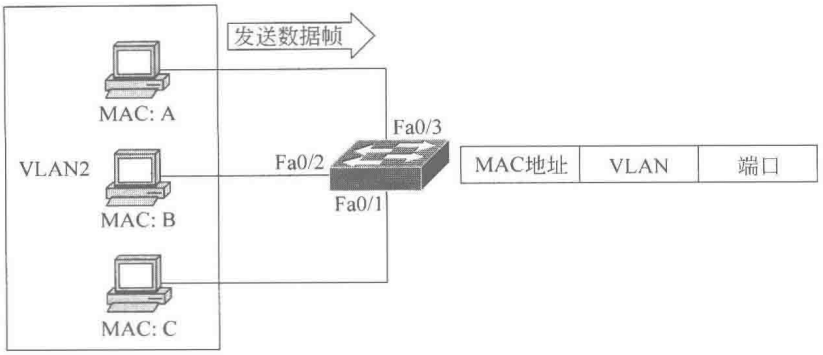

图 2-1　CAM 表初始状态

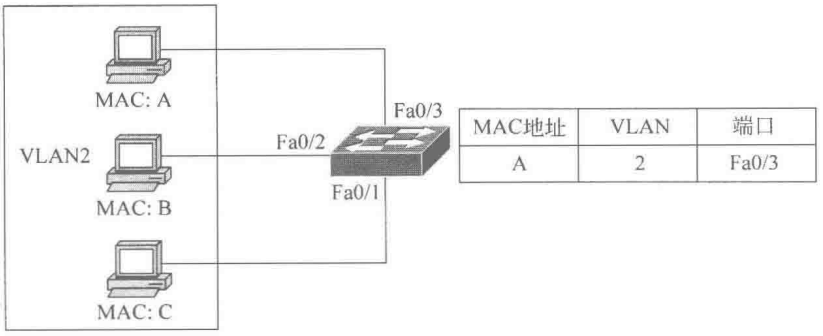

图 2-2　交换机接收到一个数据帧后的 CAM 表状态

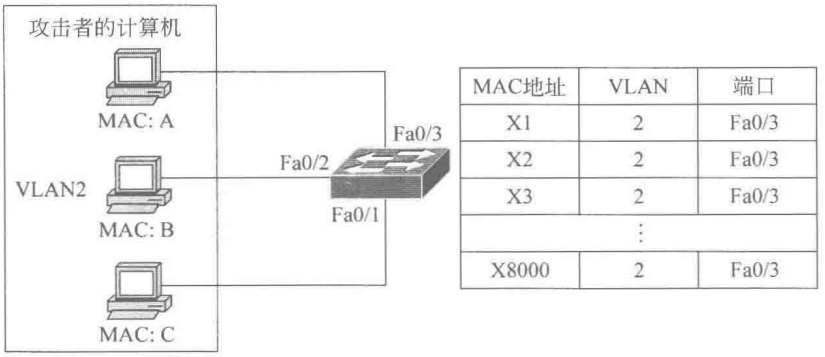

图 2-3　CAM 表溢出

此时，若 MAC 地址为 C 的计算机向 MAC 地址为 B 的计算机发送数据帧，攻击者的计算机也可以接收到这个数据帧，这是因为交换机 CAM 表中并没有保存与 MAC 地址 B 相对应的端口，因此交换机会在该 VLAN 的所有端口泛洪这个数据帧，如图 2-4 所示。

注意：虽然交换机不会跨 VLAN 泛洪数据帧，但一旦交换机的 CAM 表被攻击者伪造的 MAC 地址占满，交换机也就无法通过属于其他 VLAN 的接口学习其相连设备的 MAC 地址信息。因此，一个 VLAN 遭到 CAM 表溢出攻击，也会导致交换机在其他 VLAN 中泛洪本 VLAN 的数据帧。

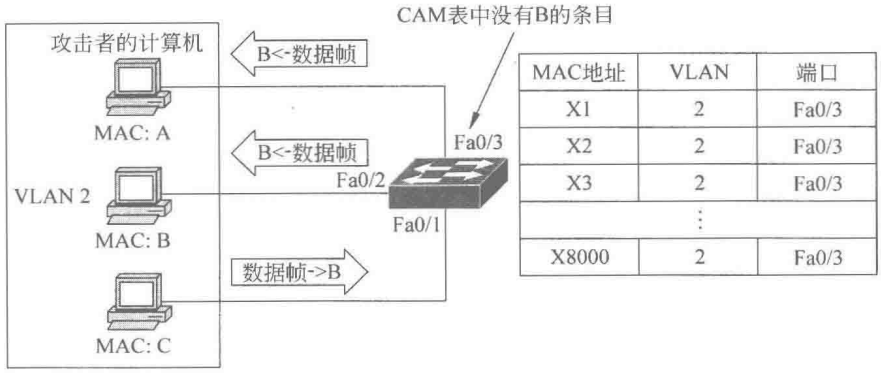

图 2-4　交换机泛洪数据帧

3. 防御策略

Cisco 交换机所提供的一种称为端口安全的(port security)特性可以有效地防止这种攻击,这种特性可以限制交换机通过一个端口接收到的源 MAC 地址数量,其命令如例 2-1 所示。

例 2-1　端口安全的配置

```
Switch(config)# int fa 0/3
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

端口安全默认的最大 MAC 地址数量为 1,管理员可以通过命令 switchport port-security maximum *number* 手动修改最大 MAC 地址数量,如果管理员手动指定的数量也是 1,那么在运行配置中就看不到这条命令。

如果网络中出现了违背(violation)端口安全策略的行为,交换机可以执行以下 3 种行为:

- protect:交换机会丢弃所有源 MAC 地址未知的数据帧,但不会为此发送任何通告消息。
- restrict:交换机会丢弃所有源 MAC 地址未知的数据帧,同时发送 SNMP trap 消息,并将 violation counter(违背计数器)的数量加 1。
- shutdown:交换机让该端口进入 err-disabled 状态。此时,相应端口不会再收发任何数据帧,设备上相应端口的 LED 灯也会熄灭,同时交换机会发送 SNMP trap 消息,并将 violation counter(违背计数器)的数量加 1。

交换机行为的配置命令为 switchport port-security violation <action>,在上述 3 个行为中,交换机默认的行为是 shutdown。

例 2-2 为设置交换机的违背行为。

例 2-2　设置端口安全的违背行为

```
Switch(config-if)# switchport port-security violation protect
```

安全端口特性支持在交换机端口上向 CAM 表中静态配置 MAC 地址,也支持动态学习 MAC 地址。在默认情况下,静态配置的 MAC 地址不仅会保存进 CAM 表中,同时也会

记录到配置文件中；而动态学习的 MAC 地址则只会保存进 CAM 表中，一旦交换机重启，就需要重新学习这些 MAC 地址。如果管理员希望动态学习的 MAC 地址也被保存进交换机的运行配置中，可以使用命令 switchport port-security mac-address sticky 来实现这一功能。

在默认情况下，安全地址列表中的 MAC 地址是不会老化的（无论是通过动态还是静态获得的安全 MAC 地址），但是管理员可以通过 switchport port-security aging 命令来修改这种行为，这条命令可以使用以下关键字：

(1) time：设定这个端口安全 MAC 地址老化的时间，范围是 0～1440 分钟。若设置为 0，表示该端口的安全 MAC 地址不会老化。

(2) type：设定地址老化的方式。地址老化有两种类型：

- absolute：若类型设置为 absolute，那么安全 MAC 地址在经过这一段时间后就会老化。
- inactivity：若类型设置为 inactivity，那么安全 MAC 地址只有在超过这一段时长没有发起流量时才会老化。

(3) static：设定这个端口下静态配置的安全地址会老化。

例 2-3 为地址老化的配置示例，在这个示例中，管理员规定了安全地址超过 5 分钟没有发送流量就会老化，同时静态配置的安全地址也会老化。

例 2-3 安全地址老化的配置

```
Switch(config-if)# switchport port-security aging time 5
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

命令 show port-security 可以查看与端口安全有关的信息，如例 2-4 所示。

例 2-4 查看端口安全汇总信息

```
Switch# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
             (Count)      (Count)      (Count)
------------------------------------------------------------------------
   Fa0/3        5            5            0          Protect
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port):     4
Max Addresses limit in System (excluding one mac per port): 5120
```

此外，如果希望查看某个特定端口下的端口安全信息，可以使用命令 show port-security interface 来实现，如例 2-5 所示。

例 2-5 查看某个端口与端口安全有关的信息

```
Switch# show port-security interface fastEthernet 0/3
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 5 mins
```