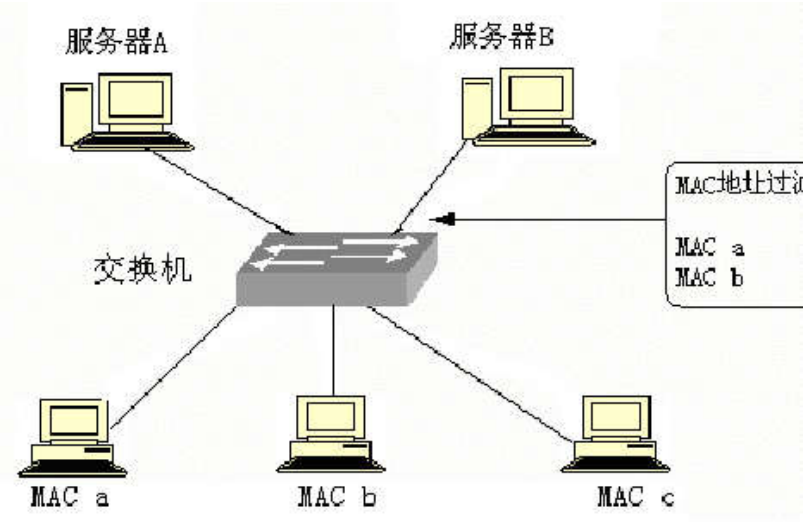
网络访问控制全解

目前进行网络访问控制的方法主要有：MAC地址过滤、VLAN隔离、IEEE802.1Q身份验证、基于IP地址的访问控制列表和防火墙控制等等。下面分别予以简单介绍。

1. MAC地址过滤法

MAC地址是网络设备在全球的唯一编号，它也就是我们通常所说的：物理地址、硬件地址、适配器地址或网卡地址。MAC地址可用于直接标识某个网络设备，是目前网络数据交换的基础。现在大多数的二层交换机都可以支持基于物理端口配置MAC地址过滤表，用于限定只有与MAC地址过滤表中规定的一些网络设备有关的数据包才能够使用该端口进行传递。通过MAC地址过滤技术可以保证授权的MAC地址才能对网络资源进行访问。

如下图所示，在服务器B所联接的交换机网络端口的MAC地址列表中上只配置了MAC a和MAC b两个工作站的MAC地址，因此只有这两台工作站可以访问服务器B，而MAC c就不能访问了，但是在服务器A中却没有配置MAC地址表，交换机就默认可以与所有同一网段的工作站连接，这样MAC a、MAC b、MAC c三个工作站都可以与服务器A连接了。



由于 MAC 地址过滤是基于网络设备唯一 ID 的，因此通过 MAC 地址过滤，可以从根本上限制使用网络资源的使用者。基于 MAC 地址的过滤对交换设备的要求不高，并且基本对网络性能没有影响，配置命令相对简单，比较适合小型网络，规模较大的网络不是适用。因为使用 MAC 地址过滤技术要求网络管理员必须明确网络中每个网络设备的 MAC 地址，并要根据控制要求对各端口的过滤表进行配置；且当某个网络设备的网卡发生变化，或是物理位置变化时要对系统进行重新配置，所以采用 MAC 地址过滤方法，对于网管员来说，其负担是相当重的，而且随着网络设备数量的不断扩大，它的维护工作量也不断加大。

另外，还存在一个安全隐患，那就是现在许多网卡都支持 MAC 地址重新配置，非法用户可以通过将自己所用网络设备的 MAC 地址改为合法用户 MAC 地址的方法，使用 MAC 地址“欺骗”，成功通过交换机的检查，进而非法访问网络资源。

2. VLAN 隔离法

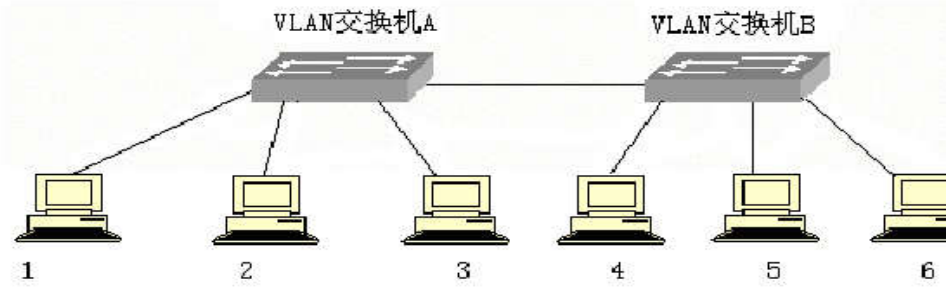
VLAN（虚拟局域网）技术是为了避免当一个网络系统中网络设备数量增加到一定程度后，众多的网络广播报文消耗大量的网络带宽，使得真正的数据传递受到很大的影响；确保部分安全性比较敏感的部门数据不被随意访问浏览而采用

一种划分相互隔离子网的方法。在此仅对 VLAN 技术实现访问控制的一些基本方面作一简单介绍。

通过 VALN 技术，可以把一个网络系统中的众多网络设备分成若干个虚拟的“工作组”，组和组之间的网络设备在二层上互相隔离，形成不同的广播域，进而将广播流量限制在不同的广播域中。

由于 VALN 技术是基于二层和三层之间的隔离技术，被广泛应用于网络安全方面，可以通过将不同的网络用户与网络资源进行分组，通过支持 VLAN 的交换机阻隔不同组内网络设备间的数据交换来达到网络安全的目的。该方式允许同一 VLAN 上的用户互相通信，而处于不同 VLAN 的用户之间在链路层上是断开的，只能通过三层路由器才能访问。

如下图所示，右从左至右工作站的编号为 1~6。在该图中将编号为 1、3、5 的工作站划分到一个 VLAN 中，将编号为 2、4、6 的工作站划分到另一个 VLAN 中，这样编号为 1、3、5 的工作站之间可以相互通信，编号为 2、4、6 的工作站之间也可以相互通信，但两个组之间不可以直接通信，这样可以确保本组资源只能由本组用户访问。



目前基于 VLAN 隔离方式的访问控制方法，在一些中小型企业中也得到广泛应用。如企业中的人事部和财务部等部门都是相对来说安全性要求更高一些的，通常不允许其它部门用户随意访问、查阅相关资料，通过 VLAN 方式划分后，两

个部门的网络数据就不会被其他用户访问了，虽然他们与其它部门一样同处一个网络。还有一点要注意的是，虽然别的用户不能随意访问 VLAN 组用户，但 VLAN 组用户却可随意访问其它非 VLAN 组用户，除非也做了访问限制配置。

不同的交换机 VLAN 划分的方法不尽相同，可以分别基于端口、MAC、IP 地址进行，具体因篇幅关系，在此不作详细介绍。

虽然我们说 VLAN 隔离方式具有比较明显的优点，但同时也有一个非常明显的缺点，那就是要求网络管理员必须明确交换机每一物理端口上所联接的设备的 MAC 地址或是 IP 地址，并要根据不同的工作组对交换机进行 VLAN 配置。当某一网络终端的网卡、IP 地址或是物理位置发生变化时，需要对整个网络系统中的多个相关的网络设备进行重新配置，这同样对于网管来说负担是相当重的，所以只适用于在小型网络中使用。

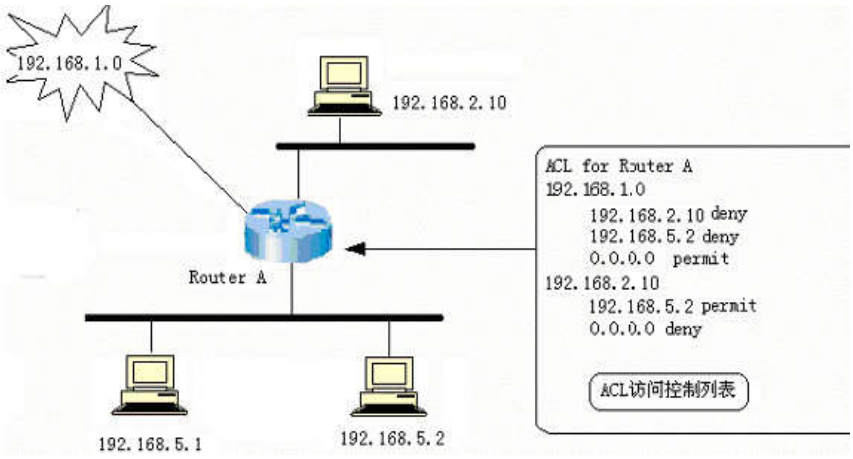
在安全性方面也存在隐患，VLAN 技术可以保证网络设备间的隔离，但对于同一台服务器，只能做到同时向多个 VLAN 组全面开放或是只向某个 VLAN 组全面开放，而不能针对个别用户进行限制。而在通常情况下，一台服务器会提供多种服务，担当多种服务器角色，同时为多个 VLAN 组用户提供不同的服务，这样带来了一定的安全隐患。例如一个数据库服务器中可能存有财务数据，也可能同时担当市场部电子商务中服务器角色，存有客户的数据，这样这台服务器就得同时向财务人员与市场人员开放，单纯采用 VLAN 技术就无法避免市场人员查看财务数据的情况发生。当然这种安全隐患可通过其它途经来解决。

3. ACL 访问控制列表法

访问控制列表在路由器中被广泛采用，它是一种基于包过滤的流向控制技术。标准访问控制列表通过把源地址、目的地址以及端口号作为数据包检查的基本元

素，并可以规定符合检查条件的数据包是允许通过，还是不允许通过。访问控制列表通常应用在企业网络的出口控制上，例如企业通过实施访问控制列表，可以有效地部署企业网络出网策略。如控制哪些员工可以访问 Internet；员工可以访问哪些 Internet 站点；员工可以在什么时候访问 Internet；员工可以利用 Internet 收发电子邮件而不可以进行其它活动等。从而保证宝贵的网络资源不至于被浪费，而且使员工在上班时精力集中。

随着局域网内部网络资源的增加，一些企业已经开始使用访问控制列表来控制对局域网内部资源的访问能力，进而来保障这些资源的安全性。如图所示的就是一个应用 ACL 访问控制列表的示意图。如在路由器 A 中配置一个访问控制列表，ACL 访问控制列表配置允许 IP 地址为 192.168.2.10 的工作站通过它访问其它网络 IP 地址为 192.168.5.2 的主机，而子网 192.168.1.0 不能与 192.168.2.10 及 192.168.5.2 通信。



访问控制列表可以有效地在三层上控制网络用户对网络资源的访问，它既可以细致到两台网络设备间的具体的网络应用，也可以按网段进行大范围的访问控制管理，可以说是为网络应用提供了一个有效的安全手段。

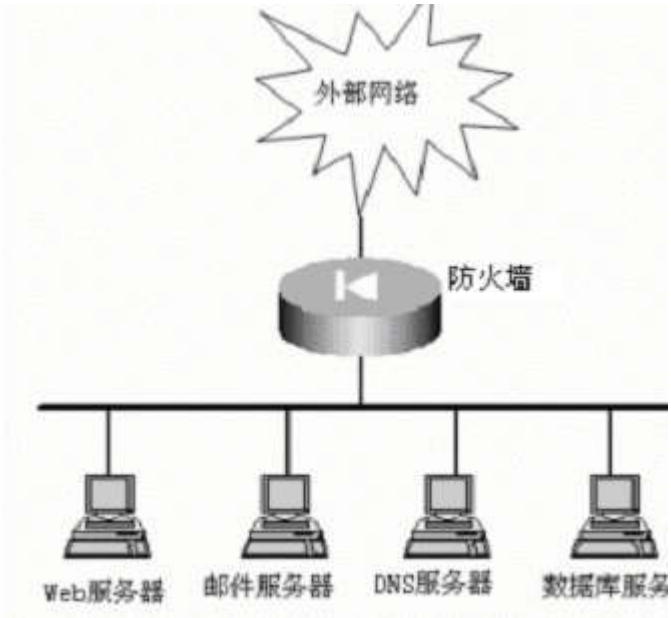
访问控制列表如果广泛用于局域网内部的访问控制，可能最终会变为一种较为“粗犷”型的管理手段。因为采用这种技术，网络管理员需要明确每一台主机

及工作站所在的 IP 子网，并确认它们之间的访问关系，对于网络终端数量有限的网络而言，这不成问题，但对于具有大量网络终端的网络而言，为了完成某些访问控制甚至不得不浪费很多的 IP 地址资源，同时巨大的网络终端数量，同样会使得管理的复杂性和难度十分巨大。

另外，维护访问控制列表不仅耗时，而且较大程度上增加了路由器开销。访问控制列表的策略性非常强，并且与网络的整体规划有很大的关系，因此，它的使用对策略制定及网络规划的人员要求比较高，所以是否采用访问控制列表以及在多大程度上利用它，只能是管理效益与网络安全之间的一个权衡。

4. 防火墙控制法

防火墙技术首先将网络划分为内网与外网，它通过分析每一项内网与外网通信应用的协议构成，得出主机 IP 地址及 IP 上联端口号，从而规划出业务流，对相应的业务流进行控制。如下图所示的是一个利用防火墙控制内、外网络通信的基本网络结构。



在图中，通过对防火墙的配置可以对外界开放 Web 服务器的 80 端口，因为 80 号端口是 Web 应用的 HTTP 协议使用的端口，这样就可使得任何用户都可以

访问公司的网站。而在邮件服务器及 DNS 服务器上也开放相应的 IP 上联端口(如 POP 的 23 号端口和 SMTP 的 25 号端口)，在保证相应功能实现的同时，也确保这些主机不会受到恶意的攻击。而对于数据库服务器来说，外界对它的访问将受到严格的限制，多是以 VPN 或是加密传输的专线方式进行。

防火墙技术在最大限度上限制了源 IP 地址、目的 IP 地址、源上联端口号、目的上联端口号的访问权限，从而限制了每一业务流的通断。它要求网络管理员明确每一业务的源及目标地址、以及该业务的协议甚至上联端口。在一个庞大的网络中构造一个有效的防火墙，也需要相当大的工作量与技术水平。同时，防火墙设备如果要达到很高的数据吞吐量，其设备造价将会非常高，通常在企业应用中都只能用于整个企业的出口安全，在企业网内部的安全保护方面使用较少。

支持 VPN 通信的防火墙支持如 DES、3DES、RC4 以及国内专用的数据加密标准和算法。加密除用于保护传输数据以外，还应用于其他领域，如身份认证、报文完整性认证，密钥分配等。支持的用户身份认证类型是指防火墙支持的身份认证协议，一般情况下具有一个或多个认证方案，如 RADIUS、Kerberos、TACACS/TACACS + 、 口令方式、数字证书等。防火墙能够为本地或远程用户提供经过认证与授权的对网络资源的访问，防火墙管理员必须决定客户以何种方式通过认证。

还可对通过防火墙的包过滤规则进行设置。包过滤防火墙的过滤规则集由若干条规则组成，它应涵盖对所有出入防火墙的数据包的处理方法，对于没有明确定义的数据包，应该有一个缺省处理方法；过滤规则应易于理解，易于编辑修改；同时应具备一致性检测机制，防止冲突。

防火墙中的 IP 包过滤依据主要是 IP 包头部信息，如源地址和目的地址。如

IP 头中的协议字段封装协议为 ICMP、TCP 或 UDP，则再根据 ICMP 头信息（类型和代码值）、TCP 头信息（源端口和目的端口）或 UDP 头信息（源端口和目的端口）执行过滤，其他的还有 MAC 地址过滤。应用层协议过滤要求主要包括 FTP 过滤、基于 RPC 的应用服务过滤、基于 UDP 的应用服务过滤要求以及动态包过滤技术等。

以上几种访问控制方式的比较如下表所示。

比较项	MAC 过滤	VLAN 隔离	访问控制列表	防火墙控制
复杂度	低	较低	较高	高
配置工作量	大	大	较大	中
灵活性	差	较差	中	中
与网络规划关系	不密切	较密切	密切	密切
设备造价	低	较低	较高	高
网络层面	二层	一至三层	三至四层	三层以上
资源安全共用	不能	不能	可以	可以
防伪造能力	低	较低	较低	较低

由上表中的比较可以看出，几种访问控制方式各有优缺点，由于它们采用的技术以及所要解决问题的方向相差较大，所以在现实的网络安全管理中，通常都是几种甚至是全部技术的组合，从而对网络安全管理人员的要求非常高。但全面掌握这些网络安全技术的管理人员相对较少，特别是一些中小企业中，这样就使得众多企业不能有效利用这些技术来充分保障企业网内部网络资源的安全。