# 第3章 网络实体安全

**本章要点**

- 网络硬件系统的冗余；
- 网络机房设施与环境安全；
- 路由器安全；
- 交换机安全；
- 网络服务器和客户机安全。

计算机网络实体是网络系统的核心，它既是对数据进行加工处理的中心，也是信息传输控制的中心。计算机网络实体包括网络系统的硬件实体、软件实体和数据资源。因此，保证计算机网络实体安全，就是保证网络的硬件和环境、存储介质、软件和数据的安全。

很多行业和企业用户对网络系统的实时性要求都很高，他们的网络系统是不允许出现故障的，一旦出现故障，将带来非常巨大的经济损失和社会影响。但网络系统涉及的环节非常多，任何一个环节都有可能出现问题，一旦某个环节出现问题，可能会导致整个网络系统停止工作。因此，必须加强对网络系统硬件设备和软件设备的使用管理，坚持做好网络系统的日常维护和保养工作。

本章介绍网络硬件系统的冗余、网络机房设施与环境安全、路由器安全、交换机安全、服务器和客户机安全等内容。

## 3.1 网络硬件系统的冗余

如果在网络系统中有一些后援设备或后备技术等措施，在系统中某个环节出现故障时，这些后援设备或后备技术能够“站出来”承担任务，使系统能够正常运行下去。这些能提高系统可靠性、确保系统正常工作的后援设备或后备技术就是冗余设施。

### 3.1.1 网络系统的冗余

系统冗余就是重复配置系统的一些部件。当系统某些部件发生故障时，冗余配置的其他部件介入并承担故障部件的工作，由此提高系统的可靠性。也就是说，冗余是将相同的功能设计在两个或两个以上设备中，如果一个设备有问题，另外一个设备就会自动承担起正常工作。

冗余就是利用系统的并联模型来提高系统可靠性的一种手段。采用“冗余技术”是实现网络系统容错的主要手段。

冗余主要有工作冗余和后备冗余两大类。工作冗余是一种两个或两个以上的单元并行工作的并联模型,平时由各处单元平均负担工作,因此工作能力有冗余;后备冗余是平时只需一个单元工作,另一个单元是储备的,用于待机备用。

从设备冗余角度看,按照冗余设备在系统中所处的位置,冗余又可分为元件级、部件级和系统级;按照冗余设备的配备程度又可分为1∶1冗余、1∶2冗余、1∶n冗余等。在当前元器件可靠性不断提高的情况下,与其他形式的冗余方式相比,1∶1的部件级冗余是一种有效而又相对简单、配置灵活的冗余技术实现方式,如I/O卡件冗余、电源冗余、主控制器冗余等。

网络系统大多拥有"容错"能力,容错即允许存在某些错误,尽管系统硬件有故障或程序有错误,仍能正确执行特定算法和提供系统服务。系统的"容错"能力主要是基于冗余技术的。

系统容错可使网络系统在发生故障时,保证系统仍能正常运行,继续完成预定的工作。如在20世纪80～90年代风靡全球的NetWare操作系统,就提供了三级系统容错技术(System Fault Tolerant,SFT)。其第二级SFT采用了磁盘镜像(两套磁盘)措施,第三级SFT采取服务器镜像(配置两套服务器)措施实行"双机热备份"。

### 3.1.2 网络设备的冗余

网络系统的主要设备有网络服务器、核心交换机、供电系统、链接以及网络边界设备(如路由器、防火墙)等。为保证网络系统能正常运行和提供正常的服务,在进行网络设计时要充分考虑主要设备的冗余或部件的冗余。

**1. 网络服务器系统冗余**

由于服务器是网络系统的核心,因此为了保证系统能够安全、可靠地运行,应采用一些冗余措施,如双机热备份、存储设备冗余、电源冗余和网卡冗余等。

1) 双机热备份

对数据可靠性要求高的服务(如电子商务、数据库),其服务器应采用双机热备份措施。服务器双机热备份就是设置两台服务器(一个为主服务器,另一个为备份服务器),装有相同的网络操作系统和重要软件,通过网卡连接。当主服务器发生故障时,备份服务器接替主服务器工作,实现主、备服务器之间容错切换。在备份服务器工作期间,用户可对主服务器故障进行修复,并重新恢复系统。

2) 存储设备冗余

存储设备是数据存储的载体。为了保证存储设备的可靠性和有效性,可在本地或异地设计存储设备冗余。目前数据的存储设备多种多样,根据需要可选择刻录光驱、磁带机、磁盘镜像和独立冗余磁盘阵列(RAID)等。下面主要介绍磁盘镜像和RAID。

(1) 磁盘镜像。每台服务器都可实现磁盘镜像(配备两块硬盘),这样可保证当其中一块硬盘损坏时另一块硬盘可继续工作,不会影响系统的正常运行。

(2) RAID。RAID可采用硬件或软件的方法实现。磁盘阵列由磁盘控制器和多个磁盘驱动器组成,由磁盘控制器控制和协调多个磁盘驱动器的读写操作。可以这样来理解,RAID是一种把多块独立的硬盘(物理硬盘)按不同方式组合起来形成一个硬盘组(逻辑硬盘),从而提供比单个硬盘更高的存储性能和提供数据冗余的技术。组成磁盘阵列的不同方

式称为 RAID 级别。在用户看起来，组成的磁盘组就像是一个硬盘，用户可以对它进行分区、格式化等。总之，对磁盘阵列的操作与单个硬盘一样。不同的是，磁盘阵列的存储性能要比单个硬盘高很多，而且在很多 RAID 模式中都有较为完备的相互校检/恢复措施，甚至是直接相互的镜像备份，从而大大提高了 RAID 系统的容错度和系统的稳定冗余性。RAID 技术经过不断的发展，现在已拥有了六种级别。不同的 RAID 级别代表着不同的存储性能、数据安全性和存储成本。常用的 RAID 级别有 RAID0、RAID1、RAID5 等。

3）电源冗余

高端服务器普遍采用双电源系统（即服务器电源冗余）。这两个电源是负载均衡的，在系统工作时它们都为系统供电。当其中一个电源出现故障时，另一个电源就会满负荷地承担向服务器供电的工作。此时，系统管理员可以在不关闭系统的前提下更换损坏的电源。有些服务器系统可实现 DC（直流）冗余，有些服务器产品可实现 AC（交流）和 DC 全冗余。

4）网卡冗余

网卡冗余技术原为大、中型计算机上使用的技术，现在也逐渐被一般服务器所采用。网卡冗余是指在服务器上插两块采用自动控制技术控制的网卡。在系统正常工作时，双网卡将自动分摊网络流量，提高系统通信带宽；当某块网卡或网卡通道出现故障时，服务器的全部通信工作将会自动切换到无故障的网卡或通道上。因此，网卡冗余技术可保证在网络通道或网卡故障时不影响系统的正常运行。

**2. 核心交换机冗余**

核心交换机在网络运行和服务中占有非常重要的地位，在冗余设计时要充分考虑该设备及其部件的冗余，以保证网络的可靠性。

核心交换机中电源模块的故障率相对较高，为了保证核心交换机的正常运行，一般考虑在核心交换机上增配一块电源模块，实现该部件的冗余。为了保证核心交换机的可靠运行，可在本地机房配备双核心交换机或在异地配备双核心交换机，通过链路的冗余实行核心交换设备的冗余。同时针对网络的应用和扩展需要，还需在网络的各类光电接口以及插槽数上考虑有充分的冗余。

**3. 供电系统冗余**

电源是整个网络系统得以正常工作的动力源，一旦电源发生故障，往往会使整个系统的工作中断，从而造成严重后果。因此，采用冗余的供电系统备份方案，保持稳定的电力供应是必要的，因为供电系统的安全可靠是保证网络系统可靠运行的关键。

通常城市供电相对比较稳定，如果停电也是区域性停电，且停电时间不会很长，因此可考虑使用 UPS 作为备份电源，即采用市电＋UPS 后备电池相结合的冗余供电方式。正常情况下，市电通过 UPS 稳频稳压后，给网络设备供电，保证设备的电能质量。当市电停电时，网络操作系统提供的 UPS 监控功能，在线监控电源的变化，当监测到电源故障或电压不稳时，系统会自动切换到 UPS 给网络系统供电，使网络正常运行，从而保证系统工作的可靠性和网络数据的完整性。

**4. 链接冗余**

为避免由于某个端口、某台交换机或某块网卡的损坏导致网络链路中断，可采用网络链路冗余措施，每台服务器同时连接到两台网络设备，每条骨干链路都应有备份线路（冗余链路）。

**5. 网络边界设备冗余**

对于比较重要的网络系统或重要的服务系统,对路由器和防火墙等网络边界设备的可靠性要求也非常高,一旦该类设备出现故障则影响内部网和外部网的互联。因此,在必要时可对部分网络边界设备进行冗余设计。

## 3.2 网络机房设施与环境安全

保证网络机房的实体环境(即硬件和软件环境)安全是网络系统正常运行的重要保证。因此,网络管理部门必须加强对机房环境的保护和管理,以确保网络系统的安全。只有保障机房的安全可靠,才能保证网络系统的日常业务工作正常进行。

网络机房的设施与环境安全包括机房场地的安全,机房的温度、湿度和清洁度控制,机房内部的管理与维护,机房的电源保护,机房的防火、防水、防电磁干扰、防静电、防电磁辐射等。

### 3.2.1 机房的安全保护

**1. 机房场地的安全与内部管理**

通常,在选择网络机房环境及场地时,应采用以下安全措施。

(1) 为提高计算机网络机房的安全可靠性,机房应有一个良好的环境。因此,机房的场地选择应考虑避开有害气体来源以及存放腐蚀、易燃、易爆物品的地方,避开低洼、潮湿的地方,避开强振动源和强噪音源,避开电磁干扰源。

(2) 机房内应安装监视和报警装置。在机房的隐蔽地方安装监视器和报警器,用来监视和检测入侵者,预报意外灾害等。

同时,可采取以下机房及内部管理措施。

(1) 制定完善的机房出入管理制度,通过特殊标志、口令、指纹、通行证等标识对进入机房的人员进行识别和验证,对机房的关键通道应加锁或设置警卫等,防止非法人员进入机房。

(2) 外来人员(如参观者)要进入机房,应先登记申请进入机房的时间和目的,经有关部门批准后由警卫领入或由相关人员陪同。进入机房时应佩戴临时标志,且要限制一次性进入机房的人员数量。

(3) 机房的空气要经过净化处理,要经常排除废气,换入新风。

(4) 工作人员进入机房要穿着工作服,佩戴标志或标识牌,并要经常保持机房的清洁卫生。

(5) 要制定一整套可行的管理制度和操作人员守则,并严格监督执行。

**2. 机房的环境设备监控**

随着社会信息化程度的不断提高,机房计算机系统的数量与日俱增,其环境设备也日益增多,机房环境设备必须时时刻刻为网络系统提供正常的运行环境。因此,对机房设备及环境实施监控就显得尤为重要。

机房的环境设备监控系统主要是对机房设备(如供配电系统、UPS电源、防雷器、空调系统、消防系统、安保系统等)的运行状态、温度、湿度、洁净度,供电的电压、电流、频率,配电

系统的开关状态等进行实时监控并记录历史数据，为机房高效的管理和安全运行提供有力的保证。

**3. 机房的温度、湿度和洁净度**

为保证计算机网络系统的正常运行，对机房工作环境中的温度、湿度和洁净度都要有明确要求。为了使机房的这“三度”达到要求，机房应配备空调系统、去/加湿机、除尘器等设备。特殊场合甚至要配备比公用空调系统在加湿、除尘等方面有更高要求的专用空调系统。

机房的温度和湿度过高、过低或变化过快，都将对设备的元器件、绝缘件、金属构件以及信息存储介质产生不良影响，其结果不仅影响系统工作的可靠性，还会影响工作人员的身心健康。一般情况下，机房的温度应控制在 18～25℃，更严格的要求为 20℃±2℃，变化率为 2℃/h。机房的相对湿度应为 30%～80%，更严格的要求为 40%～65%，变化率为 25%/h。温度控制和湿度控制最好都与空调联系在一起，由空调集中控制。机房内应安装温度、湿度显示仪，随时观察和监测温度、湿度。

此外，机房灰尘会造成设备接插件的接触不良、发热元器件的散热效率降低、电子元件的绝缘性能下降、机械磨损增加、磁盘数据的读写出错且可能划伤盘片等危害。因此，机房必须有防尘和除尘设备及措施，保持机房内的清洁卫生，以保证设备的正常工作。通常，机房的洁净度要求灰尘颗粒直径小于 0.5$\mu$m，平均每升空气含尘量少于 18 000 粒。

**4. 机房的电源保护**

电源是计算机网络系统的命脉，电源系统的稳定可靠是网络系统正常运行的先决条件。电源系统电压的波动、电流浪涌或突然断电等意外事件的发生不仅可能使系统不能正常工作，还可能造成系统存储信息的丢失、存储设备损坏等。因此，电源系统的安全是网络系统安全的重要组成部分。电源系统安全包括外部供电线路的安全和电源设备的安全。

网络机房负载分为主设备负载和辅助设备负载。主设备负载指计算机及网络系统、计算机外部设备及机房监控系统，主设备的配电系统称为“设备供配电系统”，其供电质量要求高，应采用不间断电源(UPS)供电来保证主设备负载供电的稳定性和可靠性。

UPS 主要由 UPS 主机和 UPS 电池组构成。它能够提供持续、稳定、不间断的电源供应。当系统交流电网(市电)一旦停止供电时，UPS 就会立即启动，为系统继续供电，并保持一段时间的供电，使用户有充分的时间保存信息并正常关机。在 UPS 供电期间，还可启动备用发电机，以保证更长时间的不间断供电。此外，UPS 还有滤除电压的瞬变和稳压作用。按工作原理的不同可分为后备式、在线式和在线互动式 UPS。普通计算机可选用后备式 UPS，可靠性要求高或高端设备可选用在线式 UPS。一般情况下，UPS 的功率大小应为负载功率的 1.2～1.8 倍，其值越高可靠性越好。

**5. 机房的防火和防水**

机房发生火灾将会使网络机房建筑、计算机设备、通信设备及软件和数据备份等毁于一旦，造成巨大的财产损失。通常，在人们视觉不及的顶棚之上、地板之下及电源开关、插线板、插座等处往往是火灾的发源地。引起火灾的原因主要有：电器设备或电线起火、空调电加热器起火、人为事故起火或其他建筑物起火殃及机房等。机房火灾的防范要以预防为主、防消结合。平时加强防范，消除一切火灾隐患；一旦失火，要积极扑救；灾后做好弥补、恢复工作，减少损失。机房防火的主要措施有建筑物防火、设置报警系统及灭火装置和加强防火安全管理等。

机房一旦受到水浸,将使网络电缆和电气设备的绝缘性能大大降低,甚至不能工作。因此,机房应有相应的预防、隔离和排水措施。一般可采取的防水措施有:在机房地面和墙壁使用防渗水和防潮材料、在机房四周筑有水泥墙脚(防水围墙)、对机房屋顶进行防水处理、在地板下区域设置合适的排水设施、机房内或附近及楼上房间不应有用水设备、机房必须设置水淹报警装置等。

### 3.2.2 机房的静电和电磁防护

**1. 机房的静电防护**

静电是物体表面存在过剩或不足的静止电荷(留存在物体表面的电能),它是正、负电荷在局部范围内失去平衡的结果。静电具有高电位、低电量、小电流和作用时间短等特点。

静电是一种客观的自然现象,产生的方式有很多(如接触、摩擦等)。机房内的静电主要是两种不同起电序列的物体通过摩擦、碰撞、剥离等方式,在接触又分离后在一种物体上积聚正电荷,在另一种物体上积聚等量的负电荷而形成的。

静电是机房发生最频繁、最难消除的危害之一。静电对网络设备的影响主要表现为两点,一是可能造成元器件(中大规模集成电路、双极性电路)损坏,二是可能引起计算机误操作或运算错误。静电放电会造成电路的潜在损伤使其参数变化、品质劣化、寿命降低。静电可使设备在运行一段时间后,随温度、时间、电压的变化出现各种故障,影响系统的正常运行(如误码率增大、设备误动作等)。静电对计算机的外部设备也有明显的影响,如带阴极射线管的显示设备受到静电干扰时,会引起图像紊乱、模糊不清。静电还会造成 Modem、网卡、Fax 等工作失常,打印机的打印不正常等故障。此外,静电还会影响机房工作人员的工作和身心健康。

静电问题很难查找,有时会被认为是软件故障。对静电问题的防护,不仅涉及网络的系统设计,还与网络机房的结构和环境条件有很大关系。

通常,机房采取的防静电措施有:

- 机房建设时,在机房地面铺设防静电地板。
- 工作人员在工作时穿戴防静电衣服和鞋帽。
- 工作人员在拆装和检修机器时应在手腕上佩戴防静电手环(该手环可通过柔软的接地导线放电)。
- 保持机房内相应的温度和湿度。

**2. 机房的电磁干扰防护**

电磁干扰和电磁辐射不是一回事。电磁干扰是系统外部电磁场(波)对系统内部设备及信息的干扰;而电磁辐射是电的基本特性,是系统内部的电磁波向外部的发射。电磁辐射出的信息不仅容易被截收并破译,而且当发射频率高到一定程度时还会对人体有害。

网络机房周围电磁场的干扰会影响系统设备的正常工作,而计算机和其他电气设备的组成元器件容易受电磁干扰的影响。电磁干扰会增加电路的噪声,使机器产生误动作,严重时将导致系统不能正常工作。

电磁干扰主要来自计算机系统外部。系统外部的电磁干扰主要来自无线电广播天线、雷达天线、工业电气设备、高压电力线和变电设备,以及大自然中的雷击和闪电等。另外,系统本身的各种电子组件和导线通过电流时,也会产生不同程度的电磁干扰,这种影响可在机

器制作时采用相应的工艺来降低和解决。

通常可采取将机房选择在远离电磁干扰源的地方、建造机房时采用接地和屏蔽等措施防止和减少电磁干扰的影响。

**3. 机房的电磁辐射防护**

电磁辐射是网络设备在工作时通过地线、电源线、信号线等将所处理的信息以电磁波或谐波形式放射出去而形成的。

电磁辐射会产生两种不利因素：一是由电子设备辐射出的电磁波通过电路耦合到其他电子设备中形成电磁波干扰，或通过连接的导线、电源线、信号线等耦合而引起相互间的干扰，当这些电磁干扰达到一定程度时，就会影响设备的正常工作；二是这些辐射出的电磁波本身携带有用信号，如这些辐射信号被截收，再经过提取、处理等过程即可恢复出原信息，造成信息泄露。

利用网络设备的电磁辐射窃取机密信息是国内外情报机关截获信息的重要途径，因为用高灵敏度的仪器截获计算机及外部设备中辐射的信息，比用其他方法获得的情报更准确、可靠和及时，而且隐蔽性好，不易被对方察觉。

为了防止电磁辐射引起有用信息的扩散，通常是在物理上采取一定的防护措施以减少或干扰辐射到空间中的电磁信号。

对电磁辐射的保护可按设备防护、建筑物防护、区域防护、通信线路防护和 TEMPEST（电磁辐射防护和抑制技术）防护几个层次进行。

通常，可采取抑源法、屏蔽法和噪声干扰法等措施防止电磁辐射。抑源法是从降低电磁辐射源的发射强度出发，对计算机设备内部产生和运行串行数据信息的部件、线路和区域采取电磁辐射抑制措施和传导发射滤波措施，并视需要在此基础上对整机采取整体电磁屏蔽措施，以减小全部或部分频段信号的传导和辐射。电磁屏蔽技术包括设备屏蔽和环境屏蔽，它是从阻断电磁辐射源辐射的角度采取措施，将涉密设备或系统放置在全封闭的电磁屏蔽室内，采用的屏蔽材料为金属板和金属网，目前已有满足不同防护需求的屏蔽机柜、屏蔽舱和屏蔽包等产品。噪声干扰法是在信道上增加噪声，降低接收信号的信噪比，使其难以将辐射信息还原。可见，抑源法通过降低或消除计算机电磁辐射源的辐射从根本上解决问题，屏蔽法通过阻断发射和传导途径来达到电磁辐射防护的目的，而噪声法则是通过添加与信息相关的噪声，增大接收辐射信息还原的难度。

## 3.3 路由器安全

路由器是网络的神经中枢，是众多网络设备的重要一员，它担负着网间互联、路由走向、协议配置和网络安全等重任，是信息出入网络的必经之路。广域网就是靠一个个路由器连接起来组成的，局域网中也已经普遍应用到了路由器，在很多企事业单位，已经用路由器来接入网络进行数据通信，可以说，路由器现在已经成为大众化的网络设备了。

路由器在网络的应用和安全方面具有极重要的地位。随着路由器应用的广泛普及，它的安全性也成为一个热门话题。路由器的安全与否，直接关系到网络是否安全。

### 3.3.1 路由协议与访问控制

路由器是网络互连的关键设备,其主要工作是为经过路由器的多个分组寻找一个最佳的传输路径,并将分组有效地传输到目的地。路由选择是根据一定的原则和算法在多结点的通信子网中选择一条从源结点到目的结点的最佳路径。当然,最佳路径是相对于几条路径中较好的路径而言的,一般是选择时延小、路径短、中间结点少的路径作为最佳路径。通过路由选择,可使网络中的信息流量得到合理的分配,从而减轻拥挤,提高传输效率。

**1. 路由选择及协议**

路由算法包括静态路由算法和动态路由算法。静态路由算法很难算得上是算法,只不过是开始路由前由网管建立的映射表。这些映射关系是固定不变的。使用静态路由的算法较容易设计,在简单的网络中使用比较方便。由于静态路由算法不能对网络改变做出反应,因此其不适用于现在的大型、易变的网络。动态路由算法根据分析收到的路由更新信息来适应网络环境的改变。如果分析到网络发生了变化,路由算法软件就重新计算路由并发出新的路由更新信息,这样就会促使路由器重新计算并对路由表做相应的改变。

在路由器上利用路由选择协议主动交换路由信息,建立路由表并根据路由表转发分组。通过路由选择协议,路由器可动态适应网络结构的变化,并找到到达目的网络的最佳路径。静态路由算法在网络业务量或拓扑结构变化不大的情况下,才能获得较好的网络性能。在现代网络中,广泛采用的是动态路由算法。在动态路由选择算法中,分布式路由选择算法是很优秀的,并且得到了广泛的应用。在该类算法中,最常用的是距离向量路由选择(DVR)算法和链路状态路由选择(LSR)算法。前者经过改进,成为目前应用广泛的路由信息协议(RIP),后者则发展成为开放式最短路径优先(OSPF)协议。

**2. ACL**

ACL(路由器访问控制列表)是 Cisco IOS 所提供的一种访问控制技术,初期仅在路由器上应用,近些年来已经扩展到三层交换机,部分最新的二层交换机也开始提供 ACL 支持。在其他厂商的路由器或多层交换机上也提供类似技术,但名称和配置方式可能会有细微的差别。

ACL 技术在路由器中被广泛采用,它是一种基于包过滤的流控制技术。ACL 在路由器上读取第三层及第四层包头中的信息(如源地址、目的地址、源端口、目的端口等),根据预先定义好的规则对包进行过滤,从而达到访问控制的目的。ACL 增加了在路由器接口上过滤数据包出入的灵活性,可以帮助管理员限制网络流量,也可以控制用户和设备对网络的使用。它根据网络中每个数据包所包含的信息内容决定是否允许该信息包通过接口。

ACL 有标准 ACL 和扩展 ACL 两种。标准 ACL 把源地址、目的地址及端口号作为数据包检查的基本元素,并规定符合条件的数据包是否允许通过,其使用的局限性大,其序列号是 1～99。扩展 ACL 能够检查可被路由的数据包的源地址和目的地址,同时还可以检查指定的协议、端口号和其他参数,具有配置灵活、控制精确的特点,其序列号是 100～199。

这两种类型的 ACL 都可以基于序列号和命名进行配置。最好使用命名方法配置 ACL,这样对以后的修改是很方便的。配置 ACL 要注意两点:一是 ACL 只能过滤流经路由器的流量,对路由器自身发出的数据包不起作用;二是一个 ACL 中至少有一条允许

语句。

ACL 的主要作用就是一方面保护网络资源，阻止非法用户对资源的访问，另一方面限制特定用户所能具备的访问权限。它通常应用在企业内部网的出口控制上，通过实施 ACL，可以有效地部署企业内部网的出口策略。随着企业内部网资源的增加，一些企业已开始使用 ACL 来控制对企业内部网资源的访问，进而保障这些资源的安全性。

**3. 路由器安全**

1）用户口令安全

路由器有普通用户和特权用户之分，口令级别有十多种。如果使用明码在浏览或修改配置时容易被其他无关人员窥视到。可在全局配置模式下使用 service password-encryption 命令进行配置，该命令可将明文密码变为密文密码，从而保证用户口令的安全。该命令具有不可逆性，即它可将明文密码变为密文密码，但不能将密文密码变为明文密码。

2）配置登录安全

路由器的配置一般有控制口（Console）配置、Telnet 配置和 SNMP 配置三种方法。控制口配置主要用于初始配置，使用中英文终端或 Windows 的超级终端；Telnet 配置方法一般用于远程配置，但由于 Telnet 是明文传输的，很可能被非法窃取而泄露路由器的特权密码，从而会影响安全；SNMP 的配置则比较麻烦，故使用较少。

为了保证使用 Telnet 配置路由器的安全，网络管理员可以采用相应的技术措施，仅让路由器管理员的工作站登录而不让其他机器登录到路由器，可以保证路由器配置的安全。

使用 IP 标准访问列表控制语句，在路由器的全局配置模式下，输入：

```
#access-list 20 permit host 192.120.12.20
```

该命令表示只允许 IP 为 192.120.12.20 的主机登录到路由器。为了保证 192.120.12.20 这一 IP 地址不被其他机器假冒，可以在全局配置模式下输入：

```
#arp 192.120.12.20 xxxx.xxxx.xxxx arpa
```

此命令可将该 IP 地址与其网卡物理地址绑定，xxxx.xxxx.xxxx 为机器的网卡物理地址。这样就可以保证在用 Telnet 配置路由器时不会泄露路由器的口令。

3）路由器访问控制安全策略

在利用路由器进行访问控制时可考虑如下安全策略。

（1）严格控制可以访问路由器的管理员；对路由器的任何一次维护都需要记录备案，要有完备的路由器的安全访问和维护记录日志。

（2）建议不要远程访问路由器。若需要远程访问路由器，则应使用访问控制列表和高强度的密码控制。

（3）要严格地为 IOS 做安全备份，及时升级和修补 IOS 软件，并迅速为 IOS 安装补丁。

（4）要为路由器的配置文件做安全备份。

（5）为路由器配备 UPS 设备，或者至少要有冗余电源。

（6）为进入特权模式设置强壮的密码，可采用 enable secret（不要采用 enable password）命令进行设置，并且启用 Service password-encryption，操作如下。

```
Router(config)#service password-encryption
```

```
Router(config)#enable secret
```

(7) 如果不使用 AUX 端口,则应禁止该端口,使用如下命令即可(默认时未被启用)。



```
Router(config)#line aux 0
Router(config-line)#transport input none
Router(config-line)#no exec
```

(8) 若要对权限进行分级,采用权限分级策略,可进行如下操作。

```
Router(Config)#username test privilege 10 xxxx
Router(Config)#privilege EXEC level 10 telnet
Router(Config)#privilege EXEC level 10 show ip access-list
```

## 3.3.2 VRRP

**1. VRRP 协议概述**

VRRP (Virtual Router Redundancy Protocol,虚拟路由器冗余协议)是一种选择性协议,它可以把一个虚拟路由器的责任动态分配到局域网上 VRRP 路由器。控制虚拟路由器 IP 地址的 VRRP 路由器称为主路由器,它负责转发数据包到虚拟 IP 地址上。一旦主路由器不可用,这种选择过程就会提供动态的故障转移机制,这就允许虚拟路由器的 IP 地址可以作为终端主机的默认第一跳路由器。使用 VRRP 的优点是有更高默认路径的可用性而无须在每个终端主机上配置动态路由或路由发现协议。

使用 VRRP 可以通过手动或 DHCP 设定一个虚拟 IP 地址作为默认路由器。虚拟 IP 地址在路由器间共享,其中一个指定为主路由器而其他的则为备份路由器。如果主路由器不可用,这个虚拟 IP 地址就会映射到一个备份路由器的 IP 地址(该备份路由器就成为了主路由器)。

**2. VRRP 协议原理**

通常,一个网络内的所有主机都设置一条默认路由(如图 3.3.1 所示,10.100.10.1),这样主机发出的目的地址不在本网段的报文将被通过默认路由发往路由器 RouterA,从而实现主机与外部网络的通信。当路由器 RouterA 故障时,本网段内所有以 RouterA 为默认路由下一跳的主机将断掉与外部的通信。

VRRP 是一种容错协议,它是为解决上述问题而提出的,如图 3.3.2 所示。VRRP 将局域网的一组路由器(包括一个 Master 路由器和若干个 Backup 路由器)组织成一个虚拟路由器,称为一个备份组。该虚拟路由器拥有自己的 IP 地址 10.100.10.1(该 IP 地址可以和备份组内的某路由器接口地址相同),备份组内的路由器也有自己的 IP 地址(如 Master 路由器的 IP 地址为 10.100.10.2,Backup 路由器的 IP 地址为 10.100.10.3)。局域网内的主机仅仅知道这个虚拟路由器的 IP 地址 10.100.10.1,而不知道 Master 路由器的 IP 地址和 Backup 路由器的 IP 地址,它们将自己的默认路由下一跳地址设置为该虚拟路由器的 IP 地址 10.100.10.1。于是,网络内的主机就通过该虚拟路由器与其他网络进行通信。如果备份组内的 Master 路由器出现故障,Backup 路由器将会通过选举策略选出一个新的 Master 路由器,继续向网络内的主机提供路由服务,从而实现网络内的主机不间断地与外部网络进行通信。

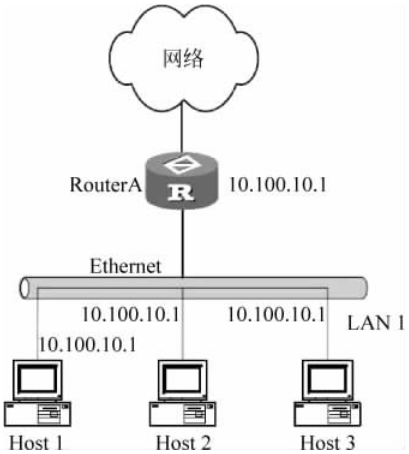


图 3.3.1　单出口路由网络结构

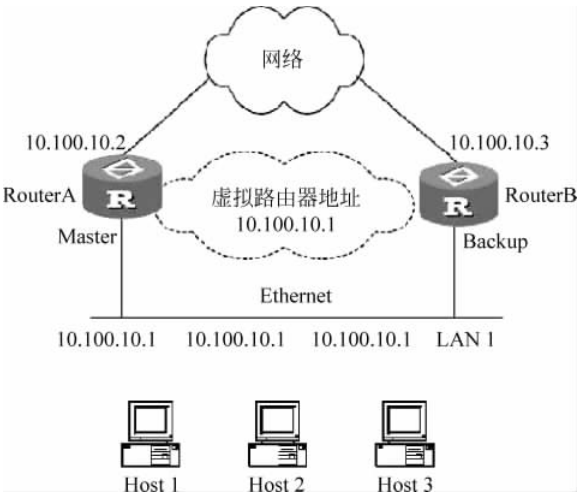


图 3.3.2　应用 VRRP 协议路由网络结构

在 VRRP 路由器组中，按优先级选举主控路由器，VRRP 协议中的优先级范围是 0～255。若 VRRP 路由器的 IP 地址和虚拟路由器的接口 IP 地址相同，则称该虚拟路由器为 VRRP 组中的 IP 地址所有者，IP 地址所有者自动具有最高优先级(255)。优先级的配置原则可以依据链路速度和成本、路由器性能和可靠性以及其他管理策略设定。在主控路由器选举中，高优先级的虚拟路由器将获胜，因此，如果在 VRRP 组中有 IP 地址所有者，则它总是作为主控路由的角色出现。对于相同优先级的候选路由器，则按照 IP 地址的大小顺序选举。为了保证 VRRP 协议的安全性，提供了明文认证和 IP 头认证两种安全认证措施。明文认证要求在加入一个 VRRP 路由器组时，必须同时提供相同的 VRID 和明文密码。IP 头认证提供了更高的安全性，能够防止报文重放和修改等攻击。

VRRP 协议的工作机理与 Cisco 公司的 HSRP(Hot Standby Routing Protocol)协议有许多相似之处。但二者之间的主要区别是在 Cisco 的 HSRP 中，需要单独配置一个 IP 地址作为虚拟路由器对外体现的地址，这个地址不能是组中任何一个成员的接口地址。

使用 VRRP 协议，不用改造目前的网络结构，从而最大限度地保护了当前投资，只需最少的管理费用，却大大提升了网络性能，具有重大的应用价值。

## 3.4　交换机安全

交换机是一种基于 MAC(网卡的硬件地址)识别，能完成封装转发数据包功能的网络设备。交换机可以“学习”MAC 地址，并把其存放在内部地址表中，通过在数据帧的源发送者和目标接收者之间建立临时的交换路径，使数据帧由源地址到达目的地址。

### 3.4.1　交换机功能与安全

交换机在内部网中占有重要的地位，通常是整个网络的核心所在。在这个黑客入侵成风、病毒肆虐的网络时代，作为网络核心的交换机也理所当然地要承担起网络安全的一部分责任。传统交换机主要用于数据包的快速转发，强调转发性能。交换机作为网络环境中重

要的转发设备,其原来的安全特性已经无法满足现在的安全需求,所以要求交换机应有专业安全产品的性能,因此安全交换机便应运而生。在安全交换机中集成了安全认证、ACL、防火墙、入侵检测、防攻击、防病毒等功能。

**1. 交换机功能**

传统以太网交换机是第二层交换机,第二层交换机是一个可以将发送端地址与接收端地址连接起来的网络设备。该设备根据数据帧中的头信息,将来自一个或多个输入端口的帧发送到一个或多个端口,完成数据交换。交换技术是为向共享式局域网提供有效的网段划分解决方案而出现的,它可以使每个用户都尽可能地分享到最大带宽。交换机工作在OSI模型中的数据链路层,因此交换机对数据包的转发是建立在MAC地址基础之上的,对于IP网络协议来说,它是透明的,即交换机在转发数据包时,不知道也无须知道信源机和信宿机的IP地址,只需知其物理地址(MAC地址)即可。显然,这种交换机的最大优点是数据交换快。因为它仅需要识别数据帧中的MAC地址,而直接根据MAC地址产生选择转发端口,算法十分简单。第二层交换机虽然也支持子网的划分和广播限制等基本功能,但控制能力较小。

交换机在操作过程中会不断地收集信息去建立MAC地址表。MAC地址表说明了某个MAC地址是在哪个端口上被发现的,所以当交换机收到一个TCP/IP数据包时,会查看该数据包的目的MAC地址,然后核对自己的MAC地址表以确认应该从哪个端口把数据包发出去。此功能由按特定用户要求和特定电子系统的需要而设计、制造的专用集成电路ASIC完成,因此速度相当快,一般只需要几十微秒,交换机便可决定一个IP数据包该往哪里送。

交换机可看作是一个具有流量控制的网桥,它是由背板、端口、缓冲区、逻辑控制单元和交叉矩阵等部件组成的。

**2. 交换机安全**

1) 安全交换机的三层含义

交换机最重要的作用就是转发数据,在黑客攻击和病毒侵扰下,交换机要能够继续保持其高效的数据转发速率,不受到攻击的干扰,这就是交换机所需的最基本的安全功能。同时,交换机作为整个网络的核心,应该能对访问和存取网络信息的用户进行区分和权限控制。更重要的是,交换机还应该配合其他网络安全设备,对非授权访问和网络攻击进行监控和阻止。

2) 802.1x安全认证

在传统的局域网环境中,只要有物理的连接端口,未经授权的网络设备就可以接入局域网,或者未经授权的用户就可以通过连接到局域网的设备进入网络,这样就造成了潜在的安全威胁。另外,在学校和智能小区的网络中,由于涉及网络的计费,所以验证用户接入的合法性也显得非常重要。IEEE 802.1x正是解决这个问题的良方,目前已经被集成到二层智能交换机中,用以完成对用户的接入安全审核。

802.1x协议是基于端口的访问控制协议。它能够在利用IEEE 802局域网优势的基础上提供一种对连接到局域网的用户进行认证和授权的手段,达到接受合法用户接入,保护网络安全的目的。802.1x协议与LAN是无缝融合的。802.1x利用了交换式LAN架构的物理特性,实现了LAN端口上的设备认证。在认证过程中,LAN端口要么充当认证者,要么

扮演请求者。在作为认证者时，LAN 端口在需要用户通过该端口接入相应的服务之前，首先进行认证，如若认证失败则不允许接入；在作为请求者时，LAN 端口则负责向认证服务器提交接入服务申请。基于端口的 MAC 锁定只允许信任的 MAC 地址向网络中发送数据。来自任何“不信任”的设备的数据流都会被自动丢弃，从而最大限度地确保安全性。

3）流量控制

安全交换机的流量控制技术把流经端口的异常流量限制在一定的范围内，以避免交换机的带宽被无限制滥用。安全交换机的流量控制功能能够实现对异常流量的控制，以避免网络堵塞。

4）防范 DDoS 攻击

企业网一旦遭到分布式拒绝服务（DDoS）攻击，就会影响大量用户的正常使用，严重时甚至造成网络瘫痪。安全交换机采用专门技术来防范 DDoS 攻击，它可以在不影响正常业务的情况下，智能地检测和阻止恶意流量，从而防止网络受到 DDoS 攻击的威胁。

5）虚拟局域网 VLAN

虚拟局域网是安全交换机必不可少的功能。VLAN 可以在二层或三层交换机上实现有限的广播域。它可把网络分成一个个独立的区域，并控制这些区域是否可以通信。VLAN 可能会跨越一个或多个交换机，设备之间好像在同一个网络间通信一样，而与它们的物理位置无关。VLAN 可在各种形式上形成，如端口、MAC 地址、IP 地址等。VLAN 限制了各个不同 VLAN 之间的非授权访问，并且可以设置 IP/MAC 地址绑定功能限制用户的非授权访问网络。

6）基于 ACL 的防火墙功能

安全交换机采用了访问控制列表（ACL）来实现包过滤防火墙的安全功能和增强安全防范能力。ACL 通过对网络资源的访问控制，确保网络设备不被非法访问或被用作攻击跳板。ACL 是一张规则表，交换机按照顺序执行这些规则，并且处理每一个进入端口的数据包。每条规则根据数据包的属性（如源地址、目的地址和协议）允许或拒绝数据包通过。由于规则是按照一定顺序处理的，因此每条规则的相对位置对于确定允许和不允许什么样的数据包通过网络是至关重要的。ACL 以前只在核心路由器中才有使用。在安全交换机中，访问控制过滤措施可以基于源/目标交换槽、端口、源/目标 VLAN、源/目标 IP、TCP/UDP 端口、ICMP 类型或 MAC 地址来实现。

7）IDS 功能

安全交换机的入侵检测系统（IDS）功能可以根据上报信息和数据流内容进行检测，在发现网络安全事件时，进行有针对性的操作，并将这些对安全事件反应的动作发送到交换机上，由交换机来实现精确的端口断开操作。实现这种联动，需要交换机支持认证、端口镜像、强制流分类、进程数控制、端口反向查询等功能。

**3. 交换机的基本配置**

配置交换机使网络对可访问站点进行控制，从而实现对自身的保护。如果用户的工作站是固定的，那么往往可以通过 MAC 地址与相同接入层的交换机端口连接。如果工作站是移动的站点，也可以动态地获得其 MAC 地址并将该地址加入到一个地址列表中，以实现与交换机端口的连接。

端口安全（port-secure）命令定义了一个最大值，即在 MAC 地址表中与交换机端口相

联系的所允许的最多的 MAC 地址。最大计数值范围为 1～132,默认值为 132,即最多可有 132 个目的 MAC 地址。

用 port-secure 命令设置端口安全性后,该端口所对应的地址就会出现在 MAC 地址表中,而不会以动态类型出现。因为若该端口对应的静态 MAC 地址数未达到最大计数值,且交换机又从端口的帧流量源地址中学到了新的地址,则将该地址自动转变成永久 MAC 地址并存入 MAC 地址表中。一旦永久或静态 MAC 地址数达到 count 值,则不再接受新的地址,这种方式称为 Sticky-Learns(记忆性学习)。该方式解决了未经允许而多人共用一台集线器接入交换机的一个端口所造成的不安全因素。

1) MAC 地址表及相关信息

MAC 地址表对于交换机而言如同路由表对于路由器。因此,对 MAC 地址表的配置也尤为重要。

(1) 显示 MAC 地址表。

MAC 地址表中的地址由永久地址、限制性静态地址和动态地址三种地址组成。

在 Switch# show MAC-address-table 命令中即可看到 MAC 地址表。

MAC 地址表由地址、源端口表、目的端口和类型组成。地址是指目的 MAC 地址;源端口表是可以向目的端口转发帧的源端口集合;目的端口是转发数据帧的端口;类型是指动态地址,其意味着 MAC 地址表中的地址是通过学习流入该端口的数据帧的帧头中的源端 MAC 地址得来的。

(2) 设置永久地址。

若设置了永久地址的目的 MAC 地址及其转发端口,则该地址永久不会超时,所有的端口均可以转发帧给它。设置永久地址的命令如下。

```
Switch(config)#MAC-address-table permanent[MAC Address][type slot/port]
```

(3) 设置限制性静态地址。

限制性静态地址不但继承了永久地址的所有特性,更进一步严格地限制了源端口,安全性得到进一步地增强。设置限制性静态地址的命令如下。

```
Switch(config)#MAC-address-table restricted static[MAC address][type slot/port][source
interface list]
```

(4) 删除表项。

如果不需要某条 MAC 地址表项,则可将其删除,删除表项的命令如下。

```
Switch#clear MAC-address-table[dynamic|permanent|restricted]
```

2) 交换机端口安全

(1) 认证端口。

可以给交换机端口配置增加一个文本描述来帮助认证配置,这个描述仅仅意味着一个注释域,作为端口使用的一条记录或者其他唯一的信息。为了给端口分配一个注释或描述,在接口配置模式下输入如下命令。

```
Switch(config-if)#description description-string
```

执行接口配置命令 no description 时会删除一个注释或描述。

(2) 端口速度。

可以通过交换机配置命令给交换机端口指定一个特殊的速度,快速以太网 10/100 端口可以为自协商模式设置速度为 10、100 或 Auto(默认)。使用如下命令可在一个特殊的以太网端口上指定端口速度。

```
Switch(config-if)#speed{10 | 100 | auto}
```

(3) 端口模式。

可以为一个以太网交换机端口指定一个特殊的连接模式,使端口在半双工、全双工或自协商模式下操作。在接口配置模式下输入如下命令可在交换机端口上设置连接模式:

```
Switch(config-if#duplex{auto | full | half}
```

在接口配置模式下执行 description 命令,可配置描述信息。

3) 交换机口令安全

通常,网络设备应该配置为对于未被授权的访问是安全的。Cisco 交换机通常提供一个简单安全的形式,通过设置密码来限制注册到用户接口的人。交换机有用户执行模式和特权模式两种可用的用户访问级别。用户执行模式是访问的第一级密码,它允许访问基本的端口。特权模式是第二级密码,它允许设置或改变交换机的操作参数和配置。

(1) 密码设置。

为用户模式设置注册密码,需要在全局配置模式下输入下列命令。

```
Switch(config)#line con 0
Switch(config-line)#password password
Switch(config-line)#login
Switch(config-1)#line vty 0 15
Switch(config-line)#password password
Switch(config-line)#login
```

登录密码可防止未授权用户登录。启用密码可防止未授权用户修改配置。

当进入全局配置模式后,可使用 enable password 命令配置登录密码和启用密码。

```
(config)#enable password?
level Set exec level password
(config)#enable password level
<1-15>Level Number
```

Level l 为登录密码,Level 15 为启用密码,密码长度是 4～8 个字符,如果超过此范围,系统则提示密码长度无效,如:

```
(config)#enable password level l nocoluvsnoko
Error: Invalid password length.
Password must be between 4 and 8 characters
```

(2) 重配置并验证。

```
(config)#enable password level 1 noco
(config)#enable password level 15 noko
```

```
(config)#exit
#exit
```



## 3.4.2 交换机端口汇聚与镜像

**1. 交换机端口汇聚**

1) 端口汇聚的概念

端口聚合也称以太通道(ethernet channel),主要用于交换机之间的连接。简单来讲,端口聚合就是将多个物理端口合并成一个逻辑端口。利用端口汇聚技术,交换机会把一组物理端口联合起来,作为一个逻辑通道,也就是 channel-group。这时,交换机会认为这个逻辑通道为一个端口。

端口汇聚将多个端口聚合在一起形成一个汇聚组,以实现出负荷在各成员端口中的分担,同时也提供了更高的连接可靠性。端口汇聚可以分为手工汇聚、动态 lacp 汇聚和静态 lacp 汇聚。同一个汇聚组中端口的基本配置应该保持一致,即如果某端口为 trunk 端口,则其他端口也配置为 trunk 端口;如果该端口的链路类型改为 access 端口,则其他端口的链路类型也改为 access 端口。

2) 交换机端口汇聚技术的实现(以 H3C 交换机为例)

交换机端口汇聚结构如图 3.4.1 所示,这样可增加 SwitchA 的 SwitchB 的互联链路的带宽,实现链路备份。SwitchA 的端口 E0/1 和 E0/2 分别与 SwitchB 的端口 E0/1 和 E0/2 互连。当交换机之间互联时,配置端口汇聚会将流量在多个端口上进行分担,即采用端口汇聚可以完成增加带宽、负载分担和链路备份的效果。

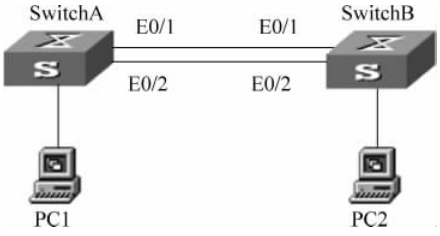


图 3.4.1 交换机端口汇聚结构

SwitchA 交换机的端口汇聚配置如下。

(1) 进入端口 E0/1。

```
[SwitchA]interface ethernet 0/1
```

(2) 汇聚端口必须工作在全双工模式。

```
[SwitchA-ethernet0/1]duplex full
```

(3) 汇聚的端口速率要求相同,但不能是自适应。

```
[SwitchA-ethernet0/1]speed 100
```

(4) 进入端口 E0/2,其他配置类同。

```
[SwitchA]interface ethernet 0/2
```

```
[SwitchA - ethernet0/2]duplex full
[SwitchA - ethernet0/2]speed 100
```

(5) 根据源和目的 MAC 进行端口选择汇聚。

```
[SwitchA]link - aggregation ethernet 0/1 to ethernet 0/2 both
```

SwitchB 的相关配置与 SwitchA 的配置顺序及内容相似。

```
[SwitchB]interface ethernet 0/1
[SwitchB - ethernet0/1]duplex full
[SwitchB - ethernet0/1]speed 100
[SwitchB]interface ethernet 0/2
[SwitchB - ethernet0/2]duplex full
[SwitchB - ethernet0/2]speed 100
[SwitchB]link - aggregation ethernet 0/1 to ethernet 0/2 both
```

配置端口汇聚时可使用参数 ingress 或 both。两者的区别是：前者表示端口汇聚组中各成员端口仅根据源 MAC 地址对出端口的流量进行负荷分担；后者表示端口汇聚组中各成员端口根据源、目的 MAC 地址对出端口的流量进行负荷分担。只有数目较多的主机进行访问时，才能观测出负载的效果。

**2. 交换机端口镜像**

通过交换机端口的镜像功能，使用服务器对两台 PC 的业务报文进行监控。按照镜像的不同方式有基于端口的镜像配置和基于流的镜像配置。如图 3.4.2 所示，将 PC1 接在交换机 E0/1 端口，IP 地址为 1.1.1.1/24；PC2 接在交换机 E0/2 端口，IP 地址为 2.2.2.2/24；Server 接在交换机 E0/8 端口，该端口作为镜像端口；E0/24 为交换机上行端口。

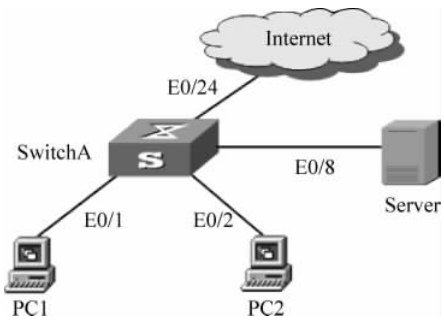


图 3.4.2　交换机端口镜像配置

基于端口的镜像是把被镜像端口的进出数据完全复制一份到镜像端口，这样可进行流量观测或故障定位。基于流镜像的交换机针对某些流进行镜像，每个连接都有两个方向的数据流，这两个数据流是分开镜像的。

下面以 S8016 交换机为例介绍基于端口的镜像配置，以 S3026 交换机为例介绍基于三层流的镜像和基于二层流的镜像。

1) 基于交换机端口的镜像配置

(1) 假设 S8016 交换机镜像端口为 E1/0/15，被镜像端口为 E1/0/0，设置端口 E1/0/15 为端口镜像的观测端口。

```
[SwitchA] port monitor ethernet 1/0/15
```

(2) 设置端口 E1/0/0 为被镜像端口，对其输入输出数据都进行镜像。

```
[SwitchA] port mirroring ethernet 1/0/0 both ethernet 1/0/15
```

也可以通过两个不同的端口，对输入和输出的数据分别镜像。

(3) 设置 E1/0/15 为镜像观测端口。

```
[SwitchA] port monitor ethernet 1/0/15
```

(4) 设置端口 E1/0/0 为被镜像端口,分别使用 E1/0/15 和 E2/0/0 对输入和输出数据进行镜像。

```
[SwitchA] port mirroring gigabitethernet 1/0/0 ingress ethernet 1/0/15
[SwitchA] port mirroring gigabitethernet 1/0/0 egress ethernet 2/0/0
```

2) 基于三层流的镜像配置

(1) 定义一条扩展 ACL。

```
[SwitchA]acl num 100
```

(2) 定义一条报文源地址为 1.1.1.1/24 去往所有目的地址的规则。

```
[SwitchA-acl-adv-101]rule 0 permit ip source 1.1.1.1 0 destination any
```

(3) 定义一条报文源地址为所有源地址、目的地址为 1.1.1.1/24 的规则。

```
[SwitchA-acl-adv-101]rule 1 permit ip source any destination 1.1.1.1 0
```

(4) 将符合上述 ACL 规则的报文镜像到 E0/8 端口。

```
[SwitchA]mirrored-to ip-group 100 interface ethernet 0/8
```

3) 基于二层流的镜像配置

(1) 定义一个 ACL。

```
[SwitchA]acl num 200
```

(2) 定义一个从 E0/1 发送数据包至其他端口(如 E0/2)的规则。

```
[SwitchA]rule 0 permit ingress interface ethernet 0/1 egress interface ethernet 0/2
```

(3) 定义一个从其他端口(如 E0/2)发送数据包到 E0/1 端口的规则。

```
[SwitchA]rule 1 permit ingress interface ethernet 0/2 egress interface ethernet 0/1
```

(4) 将符合上述 ACL 的数据包镜像到 E0/8。

```
[SwitchA]mirrored-to link-group 200 interface ethernet 0/8
```

## 3.5 服务器与客户机安全

### 3.5.1 服务器安全

**1. 网络服务器**

网络服务器(硬件)是一种高性能计算机,再配以相应的服务器软件系统(如操作系统)就构成了网络服务器系统。网络服务器系统的数据存储和处理能力均很强,是网络系统的灵魂。在基于服务器的网络中,网络服务器担负着向客户机提供信息数据、网络存储、科学

计算和打印等共享资源和服务，并负责协调管理这些资源。由于网络服务器要同时为网络上所有的用户服务，因此，要求网络服务器具有高可靠性、高吞吐能力、大内存容量和较快的处理速度等性能。

根据网络的应用和规模，网络服务器可选用高档微机、工作站、PC 服务器、小型机、中型机和大型机等担任。按照服务器用途，服务器可分为文件服务器、数据库服务器、Internet/Intranet 通用服务器、应用服务器等。

Internet 上的应用服务器又有 HDCP 服务器、Web 服务器、FTP 服务器、DNS 服务器和 STMP 服务器等。上述服务器主要用于完成一般网络和 Internet 上的不同功能。应用服务器用于在通用服务器平台上安装相应的应用服务软件并实现特定的功能，如数据中间件服务器、流式媒体点播服务器、电视会议服务器和打印服务器等。

**2. 服务器的安全策略**

(1) 对服务器进行安全设置(包括 IIS 的相关设置、Internet 各服务器的安全设置、MySQL 安全设置等)，提高服务器应用的安全性。

(2) 进行日常的安全检测(包括查看服务器状态、检查当前进程情况、检查系统账号、查看当前端口开放情况、检查系统服务、查看相关日志、检查系统文件、检查安全策略是否更改、检查目录权限、检查启动项等)，以保证服务器正常、可靠地工作。

(3) 加强服务器的日常管理(包括服务器的定时重启、安全和性能检查、数据备份、监控、相关日志操作、补丁修补和应用程序更新、隐患检查和定期的管理密码更改等)。

(4) 采取安全的访问控制措施，保证服务器访问的安全性。

(5) 禁用不必要的服务，提高安全性和系统效率。

(6) 修改注册表，使系统更强壮(包括隐藏重要文件/目录，修改注册表实现完全隐藏、启动系统自带的 Internet 连接防火墙、防止 SYN 洪水攻击、禁止响应 ICMP 路由通告报文、防止 ICMP 重定向报文攻击、修改终端服务端口、禁止 IPC 和建立空连接、更改 TTL 值、删除默认共享等)。

(7) 正确划分文件系统格式，选择稳定的操作系统安装盘。

(8) 正确设置磁盘的安全性(包括系统盘权限设置、网站及虚拟机权限设置、数据备份盘和其他方面的权限设置)。

## 3.5.2 客户机安全

在企业、单位的内部网络中，除了一些提供网络服务的服务器外，应用更多的是客户机。网络管理人员可以考虑制定标准的客户机安全政策，利用一些安全设定与保护机制来管理这些有潜在风险的客户机系统。

客户机是对企业网络进行内部攻击的最常见的攻击源头，其对系统安全管理员的工作构成了挑战：一是因为网络中客户机的数量很多；二是因为许多用户没有接受过网络安全教育，或不关心网络安全问题。虽然阻止外部对网络内部客户机的访问相对容易，但要防止内部的攻击却困难得多。

**1. 客户机的安全策略**

网络安全管理员为客户机制订合理的、切实可行的安全策略，利用相关的安全产品，提高客户机的安全性是非常必要的。

1) 客户机系统安全

(1) 下载安装软件开发厂商提供的补丁程序,并执行修补作业。

(2) 安装防毒软件并定期更新病毒码。

(3) 定期执行文件和数据的备份。

(4) 关闭或移除不必要的应用程序。

(5) 合理使用客户机管理程序。

(6) 不随意下载或执行来源不明的文档或程序。

2) 客户机安全设定

(1) 设定使用者授权机制。在企业、单位内部网络环境里,可以明确唯有授权的使用者方可使用内部网的客户机。另外,使用者可以启动屏幕保护程序来限制非授权人的使用,以保护客户机中所存放的数据。

(2) 设定访问控制权限。对于客户机中机密或重要的文档/目录进行权限控制,非授权人无法读取重要的文件或利用密码保护功能进行控制。

(3) 设定安全的远程管理。

Windows Server 2003 及以上版本都支持远程桌面控制功能,都提供远程对服务器和客户机的安全管理工具,用户只需简单设定一下即可。

**2. 客户机的风险防护**

1) 对身份认证风险的防护

从操作系统安全方面来看,身份认证是最先考虑的环节,获得一个用户的身份就掌握了所登录计算机的所有资源,同时也很容易获得各应用系统的使用权限,因此身份认证方式的安全有效是非常重要的。目前,从技术上看身份认证主要有用户名+复杂口令、电子密钥+PIN 码和人体生理特征识别三种方式。

通常情况下,主机采用用户名和设置复杂口令的身份认证方式。该方式一般要求的口令位数为 12 位或更多,由字母、数字、特殊符号混合组成,并定期更换。但这种方式的缺点是系统的口令容易被破解,且终端用户在口令更换周期、口令复杂性等方面很难严格执行,日常管理难度较大。对于 Windows 7 客户机操作系统,可以使用组策略管理方法,由网络管理员直接配置系统密码策略和账户锁定策略,对密码长度、更换周期、锁定时长和无效登录阈值等进行具体限制。利用组策略管理器管理密码的方法参见 9.2.1 节介绍。

电子密钥和 PIN 码的身份认证方式是在电子密钥中存入数字证书等身份识别文件,定期更换 PIN 值(类似动态口令卡),PIN 值一般设为 6 位或更多,用户只有在同时拥有电子密钥和知道 PIN 值的情况下才能登录系统。数字证书是目前在网上银行、政府部门等应用比较广泛的技术手段,其安全性优于用户名+复杂口令方式。数字证书身份认证方式需要购买相应的软硬件产品。

以个人生理特征进行验证时,可有多种技术为验证机制提供支持,如指纹识别、声音识别、血型识别、视网膜识别等。个人生理特征识别方法的安全性最好,但验证系统也最复杂。指纹识别是常用于客户机的生理特征识别方法。指纹识别技术基于人体生理特征,安全性相对较高,但缺点是成本高,每台客户机均要安装指纹传感器及相应软件。对于非常重要的客户机可以采取生理特征识别+复杂口令的技术措施来保证安全。

2）对信息泄露风险的防护

根据网络模式、安全保密需求等具体情况的不同，用户权限的管理在各应用场合的要求也不同。在安全保密要求较高的部门，客户机的 I/O 端口应该是受到控制的。通常可利用相关安全产品对客户机的光驱、USB 口、COM 口、LPT 口以及打印机（本地打印机和网络打印机）等 I/O 端口进行使用权限控制。同时出于安全性和保护内部机密的需要，要求相关安全产品提供审计功能以加强对内部网络中客户机的监控和管理。就审计功能而言，可以有如下审计内容。

- 审计客户机的身份认证内容，如每天用户登录尝试次数、登录时间等信息。
- 审计客户机与移动存储设备间的文件操作，包括复制、删除、剪切、粘贴、文件另存为等。
- 审计客户机的打印机使用情况，记录打印文件名称、打印时间、打印页数等信息。
- 禁止客户机以无线方式接入互联网，并部署审计策略记录客户机未成功的联网行为。

3）对内部攻击风险的防护

对于来自内部网络的攻击，除了加强口令强度预防外，还应采取及时安装系统补丁、进行策略设置和安装病毒防护系统等安全措施。

4）对移动存储介质风险的防护

为了降低移动存储介质带来的安全风险，应在企业内部对所有移动存储介质进行统一管理。对不同的存储介质采取不同的技术和管理措施。通过技术手段使外来移动存储介质无法接入企业内部网，内部网中认证过的移动存储介质也仅能在授权的客户机上使用，对涉密的移动存储介质应采取加密等技术使其在授权之外的计算机上无法使用，以降低因介质丢失或管理不严带来的安全风险。

## 习题和思考题

**一、简答题**

1. 解释网络系统安全中冗余的含义及冗余的目的。
2. 什么是服务器镜像？什么是端口汇聚？
3. 网络设备冗余有哪些措施？
4. 简述路由器访问控制的安全策略。
5. 简述服务器的安全策略。
6. 简述客户机实体安全和系统安全策略。
7. 列举几种网络上常用的服务器。
8. 简述机房环境及场地的选择考虑。
9. 简述机房的防火和防水。
10. 简述机房的静电防护。
11. 简述机房的电磁干扰和电磁辐射的概念和二者之间的区别。
12. 什么是 NAT？简述 NAT 的应用。
13. 什么是 VRRP？它的作用是什么？

14. 客户机的安全策略有哪些?

**二、填空题**

1. 网络服务器冗余措施有(　　)冗余、(　　)冗余和(　　)冗余等。

2. 网络设备的冗余措施有(　　)冗余、(　　)冗余、(　　)冗余和(　　)冗余等。

3. 网络机房的保护通常包括机房的(　　)、(　　)、防雷和接地、(　　)、防盗、防震等措施。

4. 一般情况下,机房的温度应控制在(　　)℃,机房相对湿度应为(　　)%～(　　)%。

5. 冗余就是(　　),以保证系统更加可靠、安全地工作。

6. 网络系统的主要设备有(　　)、(　　)、(　　)和(　　)等。

7. 路由选择算法可分为(　　)路由选择算法和(　　)路由选择算法两大类。

8. 网络服务器有(　　)、(　　)、(　　)和(　　)服务器等。

9. Interent 应用服务器有(　　)、(　　)、(　　)和(　　)等。

**三、选择题**

1. 双机热备份是采用了两个(　　)。

A. 服务器互为备份　　B. 硬盘互为镜像

C. 磁盘互为镜像　　D. 客户机互为备份

2. 以下(　　)是网络供电系统的冗余措施。

A. WPS　　B. PGP　　C. USB　　D. UPS

3. 触摸机器时人手会有一种麻酥酥的感觉,这是由(　　)现象引起的。

A. 电磁辐射　　B. 静电　　C. 电磁干扰　　D. 潮湿

4. (　　)是网络系统的互联设备。

A. 服务器　　B. 交换机　　C. 路由器　　D. 客户机