

第1篇



园区网概述

第1章 园区网的网络模型发展历程

第2章 典型园区网的业务部署

园区网的网络模型发展历程

如同认识一个新生事物一样,对网络的认识也需要按照一定的认知方法,循序渐进地学习、掌握直至精通。本章将从园区网的发展历程入手,对网络的宏观面貌进行简要介绍,以便在掌握网络整体概况的基础上继续进行后续知识的学习。

1.1 本章目标

学习完本章,应该能够:

- 了解园区网发展历程;
- 了解扁平网络的缺点;
- 了解分层网络的优缺点;
- 掌握网络结构的核心层、汇聚层和接入层的功能和业务部署情况;
- 掌握局域网在园区网络中的应用。

1.2 小型局域网

局域网的典型代表以太网最初的发展实际上局限于在近距离的主机之间进行报文交付。而在其发展初期的典型网络设备则是目前已经淘汰的集线器。在此类网络中,所有网络主机在同一个冲突域内工作,冲突域内仅能同时允许一台主机发送报文。而今可见的典型小型局域网结构则如图 1-1 所示,主机之间的报文交互已经不再受冲突域的限制,从而可以同时进行。这也是交换网络带来的优势。

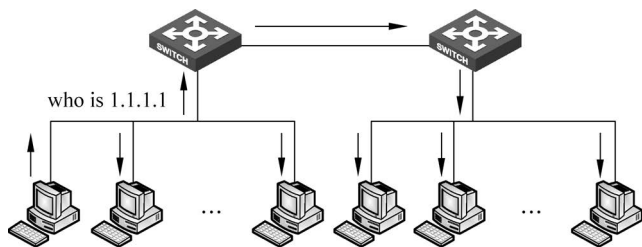


图 1-1 典型小型局域网结构

但是上述典型小型局域网仍然存在广播泛滥的问题。因为在此类网络中,主机发送的广播报文都将传播到网络的每个角落。而广播又是目前 IP 通信必不可少的手段之一,为了保证网络的效率,网络规模就必须限定在一定的范围内,而不是无止境地扩展。所以在小型局域网中,主机数量较少,只能适用于工作组应用。而且在交换网络产生的初期,网络本身没有安全机制,无法保障网络安全可靠地运行。

1.3 中型局域网

在小型局域网的基础上,如果用户数量进一步增加势必导致网络中的广播流量比例加大,网络传输效率降低,因此在如图 1-2 所示的典型中型局域网中将面临广播泛滥的问题。不得不采取有效的措施以限制广播流量的传播范围。现今广泛应用的 VLAN(虚拟局域网)技术正好在不需要额外增添网络设备的基础上可以很好地解决此问题。

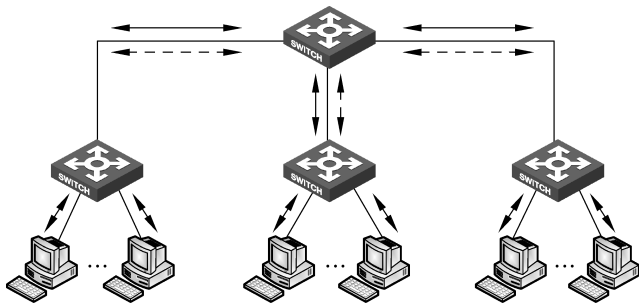


图 1-2 典型中型局域网

一方面,VLAN 利用特殊的报文头部特征对用户数据报文进行标识,从而可以将物理连接在一起的大型网络分割成逻辑上相互独立的多个小型局域网,这样在局域网上泛滥的广播流量将被限定在逻辑上相互独立的小型局域网内部。另一方面,VLAN 的 Trunk(干道)链路则给多个逻辑小型局域网带来了共享相同物理链路的便利性,降低了网络建设成本。

为了降低数据报文转发的开销,星形结构目前被广泛应用于中型网络中。网络以具有高转发性能的设备通过 Trunk 链路互联各个接入层二层交换设备,满足不同 VLAN 的用户分布于不同物理位置的需求,也满足多个 VLAN 共享同一物理链路的需求。

VLAN 的应用尽管解决了物理链路的共享、广播流量的泛滥等问题,但同时带来了一个新的问题,即各个 VLAN 之间的用户无法很好地互通。在 VLAN 应用初期,路由器被用来实现 VLAN 之间的互通,可是路由器的软件转发机制导致要么网络建设成本剧增,要么在路由器的转发上面形成瓶颈。

三层交换机的诞生解决了性能瓶颈的难题。三层交换机实现了基于硬件快速转发的三层路由功能,既降低了成本又提升了三层转发性能。因此在应用三层交换机的情况下,网络结构变得更加清晰,网络也变得更加健壮。首先,可以从逻辑上将三层交换机所在的中心网络划分为核心层,而二层交换机所在的边缘网络为接入层。接入层的二层交换机利用已有的 VLAN 划分、安全接入认证等成熟技术保证网络的高效、安全运转。其次,核心层的三层交换机在满足各 VLAN 的互通的情况下,还可以采用 ACL 包过滤等机制实现 VLAN 之间的受控互访,增强安全性。由此可以形成新的局域网模型,如图 1-3 所示,中型局域网中的核心互联交换机升级为三层交换机并形成界限分明的核心层和接入层是当前中小规模三层交换机网络的典型应用。

但在应用三层交换机时,单个三层交换机处理的事务非常繁重,在网络规模增大的情况下,核心设备的性能可能会降低。另外,此类星形网络连接存在一个致命的故障风险,即核心设备的单点故障。一旦核心设备发生故障,整个网络将形成多个孤岛而无法互通。

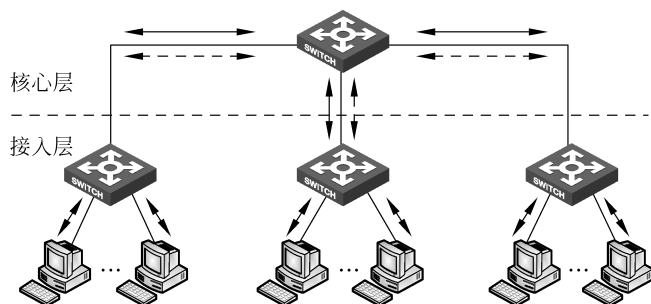


图 1-3 三层交换机局域网

1.4 大型局域网

大型企业从行政管理来看往往存在多级管理,首先整个企业被分为多个一级部门,如研发部、市场部、服务部等,而各一级部门会进一步划分成二级部门。中型局域网则仅仅适合大型企业的某个一级部门的管理结构。而各一级部门之间还需要额外的网络设备或网络来实现互联互通。因此最容易想到的是对中型局域网的结构进行扩展,在现有一级部门的星形结构的基础上,仍然采用星形结构将各一级部门进行互联。这样就形成了如图 1-4 所示的三级树状网络结构。

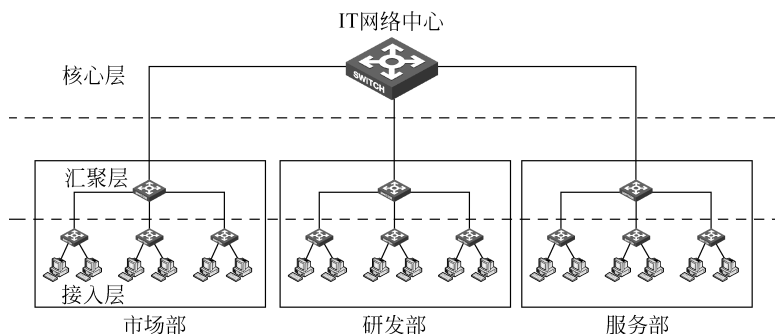


图 1-4 大型局域网锥形

如果将上述实际组网进行抽象形成一个简化模型,则可以表示为如图 1-5 所示的三层结构。这种三层结构是目前大型局域网的典型应用,各层次之间界线相对分明,功能相互独立。三个层次的网络位置和部署简述如下。

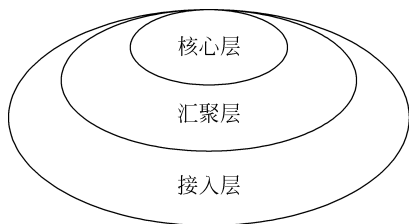


图 1-5 大型局域网分层结构

(1) 核心层处在网络的最核心位置,为来自汇聚层设备的数据提供高速转发,在某些情况下还直接接入服务器集群等核心资源。通常并不在核心层部署复杂的控制策略。

(2) 汇聚层处在网络的中间位置,对来自接入层的数据进行汇聚,以降低核心设备的压力。汇聚层设备往往作为网关存在,而且需要实施一定的控制策略以保证网络安全高效地运行。

(3) 接入层处在网络的边缘,其主要目的是实现业务的接入。可以在接入层部署安全认证等措施保证合法用户的正确接入,防范非法用户对网络资源的占用或者攻击网络。

大型局域网的核心层一旦发生故障将导致全网故障,因此保证核心层的健康稳定运行成为重中之重。因此核心层网络通常不采用存在单点故障的单核心网络,而常用双机主备互联、多机环网互联和多机 full-mesh 互联等具有冗余备份功能的组网。

双机主备互联是核心层建设最为主流和经济的方案之一。在核心层架设两个高性能的核心路由器或核心三层交换机,两个核心设备之间采用高速链路互联,汇聚层设备则采用常规的双归属接入方案同时接入核心层的主机和备机。

多机环网互联也是核心层建设的主流方案之一,它主要应用在规模巨大,核心设备数量较多的网络中。多机环网互联仅需要较少数量的高速链路即可在核心层设备间建立起备份路径,因此可以在不增加成本的情况下,实现一定的核心层设备和链路的冗余备份。多机环网互联拓扑如图 1-6 所示。

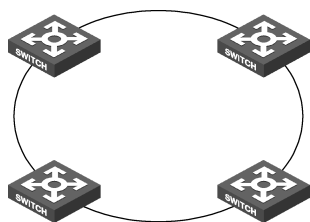


图 1-6 核心层互联之环网

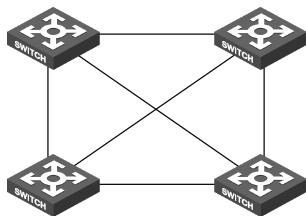


图 1-7 核心层互联之 full-mesh

为了实现核心层无单点故障,汇聚层也必须保证主备链路双归属接入核心层的两个不同的设备,防止核心层单个设备的故障导致业务中断。如图 1-8 所示,在核心层双机主备互联的情况下,汇聚层设备分别采用两条链路连接到核心层。当主机出现故障时可以快速切换到备机转发而不中断业务。在业务流量较大的网络中还可以实现主备链路的负载分担。

汇聚层与核心层之间的链路负载分担或主备备份既可以采取二层方案也可以采取三层方案。但为了降低核心设备的压力,通常采用三层方案,即将网关置于汇聚层,核心层和汇聚层设备运行动态路由协议,既可以实现负载分担,也可以实现冗余备份。

在接入层设备的基础上,汇聚层同时还实施复杂的控制策略,例如采用包过滤和策略路由等技术实现的访问控制、路由控制和流量控制。

接入层作为网络的边缘,主要任务是实现多业务的安全接入。根据接入业务的重要性,可以采用单链路上行或者双链路上行,如图 1-9 所示。

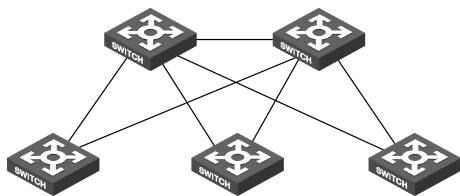


图 1-8 汇聚层网络连接

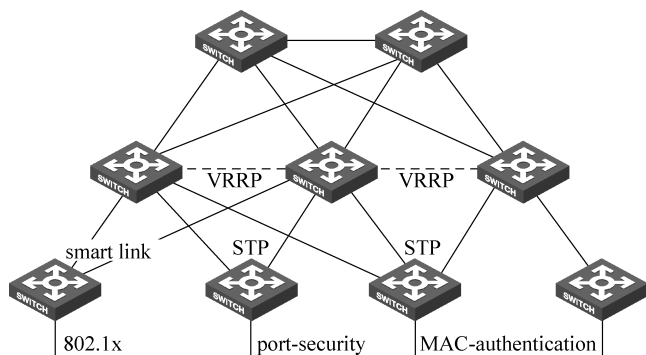


图 1-9 接入层网络连接

采用双链路上行时,需要根据实际情况选择恰当的负载分担和冗余备份技术。目前常用的备份技术有 VRRP、STP、smart link 等。VRRP 的真正实施在汇聚层网关上,接入层终端用户可以以 VRRP 的虚拟 IP 为网关,实现网关的备份。STP 可以选择单生成树实现链路的冗余备份,也可以选择多生成树实现链路的负载分担。smart link 则是双归属网络中针对 STP 的优化技术,可以实现更快的倒换收敛速度。

接入层根据接入用户的安全性选择不同的接入认证方式,如 IEEE 802.1X 认证、端口安全等。IEEE 802.1X 认证是目前以太网中应用最为广泛的接入认证技术,而 MAC 认证则是 IEEE 802.1X 认证的一种变化,简化了客户端的操作。端口安全则是综合接入认证的典型代表,它是 IEEE 802.1X 认证、MAC 认证以及 voice VLAN 等应用的综合体,可以在同一端口实现多种认证方式的组合。

1.5 局域网应用

如图 1-10 所示为一个中型企业的办公楼。每个楼层都需要部署一定数量的信息接入点,整个大楼有将近 1000 个信息接入点。网络中心在大楼一层的 IT 机房。要求各业务部门之间的二层网络相互独立,业务部门之间的信息接入点互访必须通过网络中心的核心设备,在核心设备实施流量控制。

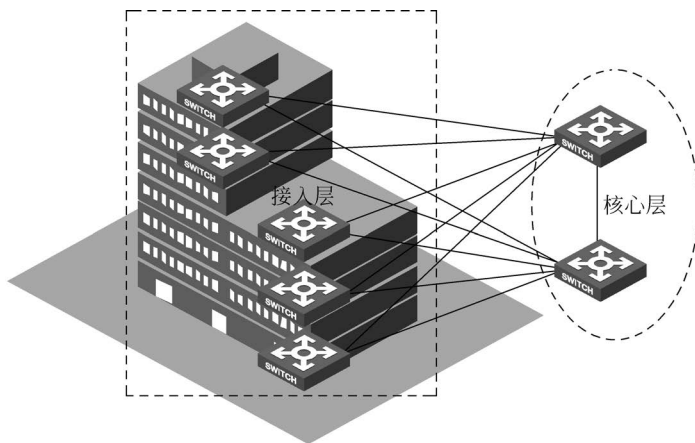


图 1-10 典型二层网络结构

针对上述需求,可以采用典型的中型局域网的拓扑结构来部署该企业的办公网络。在网络中心采用双机互联形成核心网络,各楼层根据信息点数量的需求决定选择一个或多个接入层交换机双上行连接到两核心设备。

核心设备必须选择具有路由功能的三层设备,推荐采用线速转发的高性能三层交换机实现无阻塞交换。同时还要求设备支持较强的 ACL 功能,可以灵活地部署 ACL 进行访问控制。另外需根据网络规模确定设备需要支持的路由、ARP 和 MAC 等规格。

接入设备建议选择具备 VLAN 划分、接入认证、STP 等功能的二层交换机。在业务接入端口采用接入认证并根据业务部门的要求进行 VLAN 划分。上行链路选择 smart link 或 STP 等冗余备份技术。

上述中型园区网适合大多数中小企业或者中小学校的网络建设。此类网络信息接入点的数量一般不多于 1000 个,要求实现一定的安全防范和可靠性,但对网络建设成本较为敏感。

与中小型企业网不同,大型企业园区办公网和高校校园网物理位置分布更加广泛,一般都分布在同一园区的多栋大楼内。图 1-11 所示即为一个典型的大型企业在一个园区内的网络分布情况。

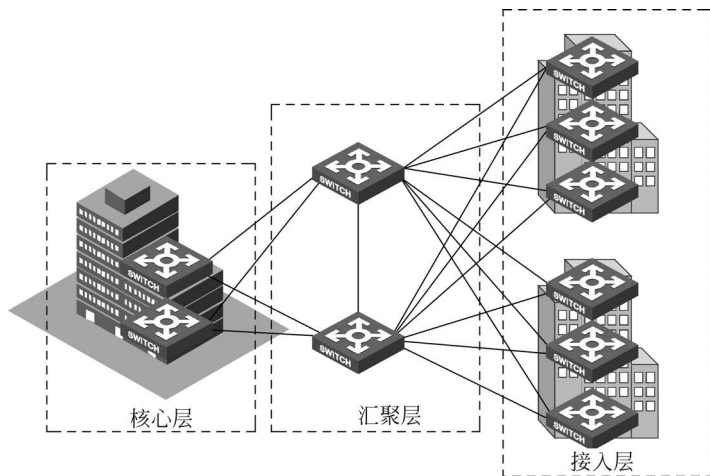


图 1-11 典型三层网络结构

按照办公楼的分布情况,将物理位置相对处于中心的大楼选为网络核心层所在地,可以更大幅度地降低传输线路的建设成本。而在网络核心层,根据企业对网络可靠性的要求选择核心网常见组网结构中的恰当类型,如最为常见的双机主备互联。在网络核心层所在大楼和其他办公大楼再以双机热备的形式组建汇聚层网络,最后将接入层设备按照双归属或者单上行的方案就近接入本大楼的汇聚设备,从而形成典型的三层网络结构。

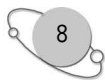
核心层设备作为全网核心和高速交换中心,必须保证设备自身具备高可靠性,关键部件具备冗余备份功能。设备转发性能具备可扩展性,网络建设初期其实际被耗用的性能占其当前最大性能的 50% 为宜,便于后期网络的扩容改造。

汇聚层设备与中小型网络的核心层设备相当,因此同样具备一定的设备级可靠性和相应的硬件性能规格,如 ARP 表项、MAC 地址表项、路由表项等规格应该能够满足当前及后期网络扩容需求。除此之外还必须具备各种冗余备份技术的能力,对上层和核心层设备实现三层的冗余备份。对下层和接入层设备实现二层的冗余备份。

接入层设备则与中小型网络的接入层设备要求相当,或者根据企业的安全性和可靠性要求适当提升设备性能和业务支撑能力。但冗余备份和安全接入等基本技术采取相同的策略和部署原则。

1.6 本章总结

- (1) 局域网的发展历史和典型的扁平、星形和树状结构。
- (2) 局域网的核心层、汇聚层和接入层的划分和功能。
- (3) 典型二层网络结构的应用。
- (4) 典型三层网络结构的应用。



1.7 习题和答案

1. 习题

- (1) 当前构建局域网主要采用的设备是()。
- A. 集线器 B. 交换机 C. 路由器 D. 服务器
- (2) 大型局域网通常分为()。
- A. 核心层 B. 汇聚层 C. 接入层 D. 网络层
- (3) 大型局域网的核心层网络常见的组网结构有()。
- A. 单核心组网 B. 双机主备互联
C. 多机环网互联 D. full-mesh 互联
- (4) 大型局域网中常见的冗余备份技术有()。
- A. VRRP B. MSTP C. smart link D. 动态路由协议
- (5) 接入层网络的常用安全接入认证技术有()。
- A. IEEE 802.1X 认证 B. MAC 集中认证
C. 端口安全 D. voice VLAN
- (6) 大型园区网的网络结构必须采用常见的树状结构。()
- A. 正确 B. 错误

2. 习题答案

- (1) B (2) ABC (3) BCD (4) ABCD (5) ABC (6) B

典型园区网的业务部署

在网络的各层次采取何种技术来满足网络需求,需要细致地分析才能得出最佳的解决方案。

本章从网络的业务需求、可靠性需求以及管理需求等多方面阐述各种网络技术的应用场景和应用优势,以利于对园区网内主要业务类型的部署形成整体认识。

2.1 本章目标

学习完本章,应该能够:

- 熟悉园区网的集中常见业务;
- 了解园区网常见的冗余备份技术;
- 了解组网业务的相关技术和协议类型;
- 了解常见的安全接入认证技术;
- 了解常见的网络管理和维护技术。

2.2 高可靠冗余网络

如图 2-1 所示的树状拓扑网络中,如果核心设备宕机或者掉电,将导致全网故障。因为各汇聚层设备被分割开来,相互独立而无法互通。这是星形和树状网络存在的典型缺陷——单点故障。显而易见,一个需要 $7\times 24\text{h}$ 不间断服务的网络是不允许存在单点故障缺陷的。因此对于高可靠性网络的建设首先需要考虑的是避免单点故障或者降低单点故障发生时网络业务受影响的范围和程度。

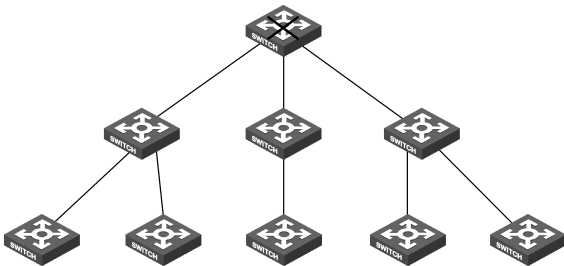


图 2-1 树状拓扑网络

避免单点故障最常见的方法就是在各设备之间采用更多的冗余物理链路进行连接。如图 2-2 所示,在核心层采用多台设备进行全互联防止单点故障,而在汇聚层和接入层则采用双归属甚至环形连接来达到上行链路的负载分担和冗余备份。不过在此类网络中,一个数据报文从一个终端转发到另一个终端可能有多条路径,如果每条路径都转发一份报文,则目的终端

将收到大量重复的报文。广播报文也会在网络中被不断复制,最终形成广播风暴。因此不得不采用一定的算法来计算并选择终端之间的唯一转发路径。最先被开发设计来解决此问题的当属 STP(spanning tree protocol,生成树协议)。

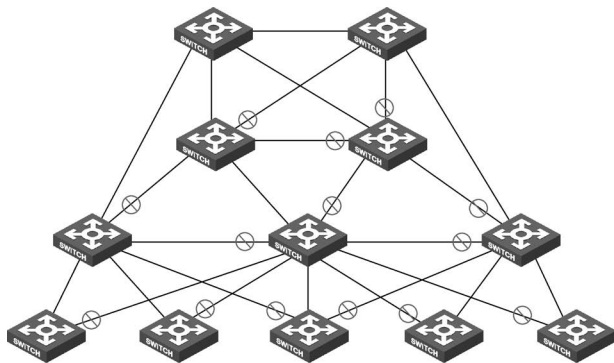


图 2-2 网状网络

STP 的计算将错综复杂的物理网络整理成一棵逻辑转发树,将那些当前没有必要使用的链路进行逻辑阻塞,从而避免网络环路。而当某些当前在用的链路出现故障时,STP 又可以快速启用那些曾经被阻塞的链路来代替它,从而恢复网络的连通性。

全网状或半网状的网络采用大量的冗余物理链路来实现网络的不间断转发或者快速恢复,其建设成本则相对高昂。在一定条件下,网络对可靠性和快速自愈能力的要求可以适当降低,因此可以根据需要适当裁剪部分冗余链路而形成更为简洁经济的网络拓扑。如图 2-3 所示的环形网络就是典型代表之一。

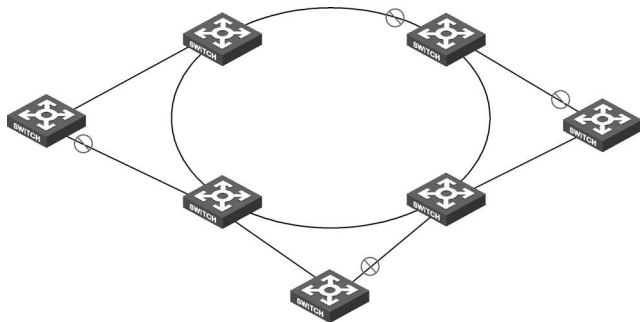


图 2-3 环形网络

环形网络常常通过多个核心设备形成核心环网,每个核心设备再根据需要单链路或双链路接入接入层网络。在此类网络中部署 STP 仍然是解决环路行之有效的方法之一。但在环形网络中,STP 并不是最佳选择,RRPP(rapid ring protection protocol,快速环网保护协议)在上述拓扑中显得更加高效快捷。

RRPP 是专门针对环形网络拓扑开发设计的协议,它利用少量的冗余链路来完成环网上的冗余备份。RRPP 的核心思想是在正常情况下阻塞环上的某个链路,并通过协议报文的交互来监控其余链路的工作状态,一旦发现某链路发生故障,将快速恢复被阻塞的链路。相对于 STP,RRPP 具有更小的资源开销和更快的收敛速度。但由于实际物理冗余链路的匮乏,其可靠性在一定程度上有所损失,若环上同时发生了两个链路的故障,将导致网络被分割。

根据实际情况,边缘接入层则可以继续选择 RRPP 协议运行子环,或者选择其他针对性的冗余备份协议。