任务 1

项目规划与设计

1.1 项目导引

新起点网络技术有限公司承接某城市城域网项目，项目要求通过给定的网络拓扑图选择能满足要求的设备，构建交换式局域网并且完成局域网之间的互联，针对安全性进行相关的访问控制，对整个网络中的所有设备进行安全的调试，并在发生故障时能进行故障的排查。

1.2 项目分析

根据与客户进行交流，要想达到客户的要求，必须首先要掌握各设备选用的理由和用途，这样才能选择出能满足要求的相关设备，在构建交换式局域网时要对地址进行相关的规划，以及对 VLAN 进行划分，通过静态路由或动态路由完成局域网之间的互联，可采用端口聚合等技术来优化网络，使用端口安全、访问控制来提高网络的安全性。

1.3 技术准备

1.3.1 知识点 1：网络拓扑分析

新起点网络技术有限公司网络设计人员根据客户提出的要求，考虑其业务目标和技术需求制定了相关的网络设计方案，在设计方案中设计人员列出了相关的业务目标以及这些目标的技术需求，从而绘制出了相关的拓扑结构以及选择了能满足需求的重要设备。网络拓扑结构如图 1-1所示。

在进行拓扑结构设计时，设计人员将设备自身的特点与客户的要求结合在一起，并根据城域网业务量分布，选择 2 个节点构成核心层；2 个主核心节点直接汇聚相关汇聚节点的流量，所

http://www.neubooks.com

有的流量都通过这两个主核心节点汇聚到骨干网。核心节点为全城域网范围的用户提供流量汇聚，并向核心出口路由器进行转发；设置多个汇聚节点，负责汇聚本地流量或者下级的汇聚节点的流量。结构是设计规划好了，下面紧接着就是选择能满足要求的路由器与交换机，网络中安装的硬件类型将影响应用程序性能，只有选择了合适的设备，才会给构建的网络带来卓越的性能与良好的安全保护。

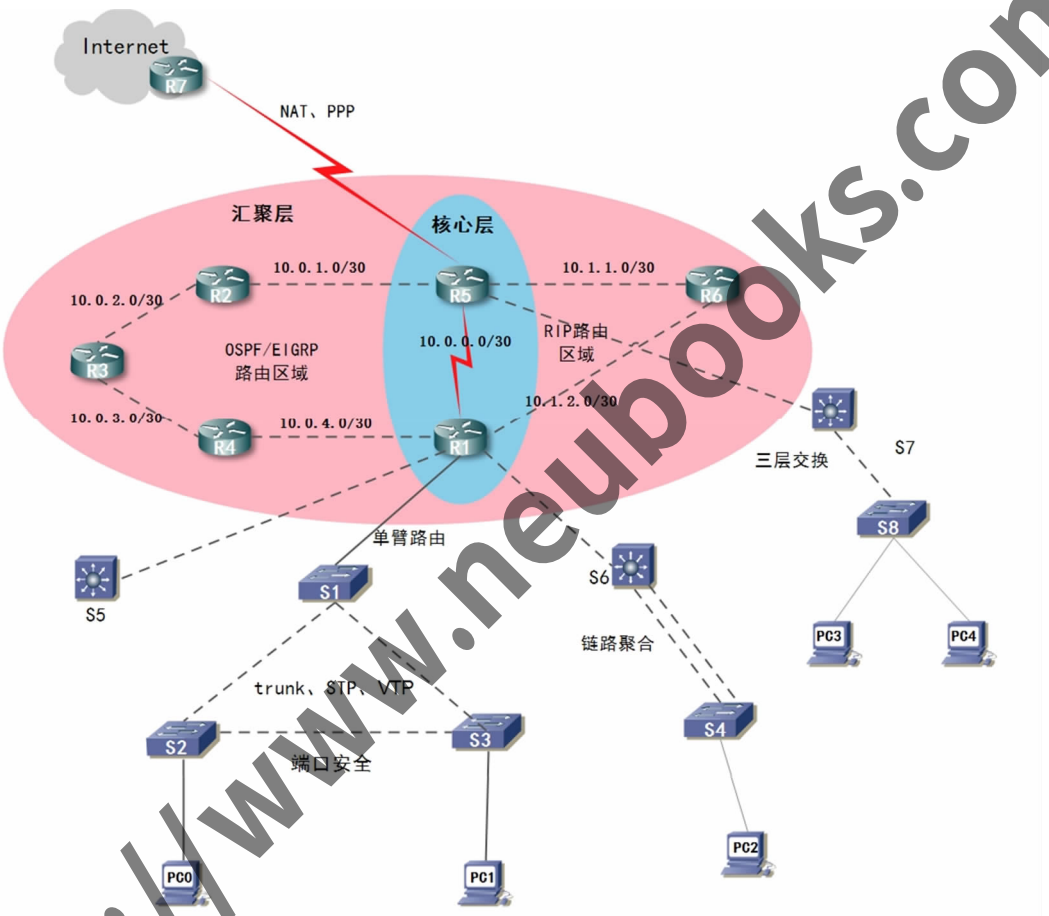

图 1-1　网络拓扑结构

1. 路由器选型

设计人员在进行路由器选型时，主要考虑以下四个方面：首先要有良好的性能，路由器的性能决定了路由器的工作效率，也决定了用户在建网时所考虑的数据承载量和应用；第二是可扩展性，路由器分为模块化结构与固定配置两类，模块化结构具有较大的灵活性，无论网络结构和接入方式如何变化，只需选择相关的模块即可适应各种复杂的网络情况；第三是冗余性和稳定性，完全冗余设计的路由器产品将大大提高设备运行的可靠性，同时，稳定的软件系统也确保了用户的应用；最后是安全性，没有安全的保障，一切都是空谈。企业出口网关既要连接内部分支机构，同时还要连接 Internet，因此作为进入企业网络的第一关，企业网关的安全性非常重要。综合以上各种因素的考虑，设计人员选用了 Cisco 3925/k9 系列集成多业务路由器。Cisco 3925/k9 系列集成多业务路由器如图 1-2 所示。

http://www.neubooks.com

图 1-2　Cisco 3925/k9 系列集成多业务路由器

Cisco 3900 系列以现有 Cisco 3800 系列集成多业务路由器为基础，提供两种平台：Cisco 3925和 Cisco 3945 集成多业务路由器。这两种 Cisco 3900 系列集成多业务路由器均提供嵌入式硬件加密加速、支持语音和视频的数字信号处理器(DSP)插槽、可选防火墙、入侵预防、呼叫处理、语音信箱以及应用程序服务。此外，这些平台还支持最广泛的有线和无线连接选项，如 T1/E1、T3/E3、xDSL、铜缆和光纤 GE，为从小型企业办公室到大型企业办公室的灵活网络部署提供出色的性能和灵活性。Cisco 3925 内置防火墙，支持 QoS、VPN，2 个服务模块插槽＋1 个双宽度服务模块插槽＋4 个 EHWIC 插槽数＋2 个双宽度 EHWIC 插槽＋1 个 ISM 插槽数＋4 个板载 DSP(PVDM)插槽。

2. 交换机选型

设计人员通过需求分析得知公司接入层需要为网络设备提供链接；需要通过创建 VLAN 将各种设备进行隔离；需要提供到分布层网络的冗余链路等，为了满足以上的需求，设计人员选择了 CISCO WS-C2960S-48TS-L 交换机作为其中的设备，这种设备是固定配置的 10/100 以太网交换机，具有可扩展性、可用性、安全性、易于管理性。

但是 2960 还存在一些局限性，因为 2960 是第二层交换机，只能在接入层提供第二层功能。但是对于分布层来说分布层负责在 VLAN 之间路由数据流，以及过滤不需要的数据流，那只使用 2960 是不能满足要求，为了满足要求，设计人员又选择了 CISCO WS-C3570X-24S-S 多层交换机来解决分布层的需求，多层交换机的端口密度很高，且支持所需的路由选择功能。对于核心层的首要目标是保证高可用性，设计人员需要采取一切措施提高可靠性和可用性，从设备的性能上来说 CISCO WS-C3570X-24S-S 也能满足这种要求，所以在整个方案中可采用 2 种型号的交换机来满足整个网络的需求。以下对两种不同型号交换机的性能进行介绍。

图 1-3　CISCO WS-C2960S-48TS-L

http://www.neubooks.com

CISCO WS-C2960S-48TS-L 以太网交换机机身以灰色外观设计，尺寸大小为 300mm×445mm×45mm，属于 Cisco 2960S 系列，是一款独立配置的机型，应用于二层交换。可提供桌面快速以太网和千兆以太网连接，并为分支机构网络实现高级局域网服务的固定配置独立式智能以太网，可提供集成安全性，包括网络准入控制(NAC)、高级服务质量(QoS)和为网络边缘提供智能服务的永续性。

CISCO WS-C2960S-48TS-L 以太网交换机还有较强的数据处理能力，其提供了 48 个以太网 10/100/1000 Mbps 端口，4 个 1G SFP 上行链路。背板带宽 88 Gbps，包转发率 77.4 Mbps，DRAM 内存为 128 MB，FLASH 内存为 64 MB。最大 VLAN 数为 255，VLAN ID 数为 4000。支持 IEEE 802.1D，IEEE 802.1p，IEEE 802.1Q，IEEE 802.1s，IEEE 802.1w，IEEE 802.1X，IEEE 802.1ab，IEEE 802.3ad，IEEE 802.3ah，IEEE 802.3 等网络标准。

图 1-4 CISCO WS-C3750X-24S-S

CISCO WS-C3750X-24S-S 采用最新的 CISCO StackWise 技术[①]，不但实现高达 32 Gbps 的堆叠互联，还从物理上到逻辑上使若干独立交换机在堆叠时集成在一起，便于用户建立一个统一、高度灵活的交换系统就好像是一整台交换机一样。

CISCO WS-C3750X-24S-S 可通过提供配置灵活性，支持融合网络模式，已经自动配置智能化网络服务，降低融合应用的部署难度，适应不断变化的业务需求；针对高密度千兆位以太网部署进行了专门的优化，其中包含多种可以满足接入、汇聚或者小型网络骨干网连接需求的交换机。

1.3.2 知识点 2：地址规划分析

如果将同一个 IP 地址分配给网络中的多台设备，将导致 IP 冲突。当网络中发生 IP 冲突时，分组便不能可靠地传输到该 IP 地址设计的设备，通过合理的网络规划，IP 编址方案可支持层次型路由选择并提供高效的第三层结构。设计人员规划的 IP 地址分配以实现如下目标：

- 防止地址重复；
- 提供和控制访问；
- 监视安全和性能；
- 支持模块化设计；

① CISCO StackWise 技术是一种针对千兆位以太网优化的、先进的堆叠架构。该技术的设计目的是及时地对设备添加、移除和重新部署做出反应，同时保持稳定的性能。利用特殊的堆叠互联电缆和堆叠软件，CISCO StackWise 技术最多可以将 9 台单独交换机连接到一个统一的逻辑单元中。

http://www.networks.com

◆ 支持使用路由汇总的可扩展解决方案。

整个网络的地址规划如图 1-1 所示，但是设计人员认为，网络的规模将在未来几年急剧增大，为了满足可扩展性的需要，设计人员提议使用层次性 IP 编址方案和无类路由选择协议。

1. 无分类编址 CIDR

在 IP 编址方案中，设计人员使用支持无类型域间路由选择 CIDR 的路由选择协议。

(1)CIDR 定义：无类型域间路由选择 CIDR(Classless Inter-Domain Routing)是一个在 Internet 上创建附加地址的方法，这些地址提供给服务提供商(ISP)，再由 ISP 分配给客户。CIDR 将路由集中起来，使一个 IP 地址代表主要骨干提供商服务的几千个 IP 地址，从而减轻 Internet 路由器的负担。

(2)CIDR 的应用：CIDR 技术能够很好的消除网络地址中类的概念，从而能够有效的分配 IPv4 地址，CIDR 用 13～27 位长的前缀取代了原来地址结构对地址网络部分的限制。(3 类地址的网络部分分别被限制为 8 位、16 位和 24 位)

CIDR 地址中包含标准的 32 位 IP 地址和有关网络前缀位数的信息，以 CIDR 地址 222.80.18.18/25 为例，其中“/25”表示其前面地址中的前 25 位代表网络部分，其余位代表主机部分。

CIDR 建立于“超级组网”的基础上，“超级组网”是“子网划分”的派生词，可看作子网划分的逆过程。子网划分时，从地址主机部分借位，将其合并进网络部分；而在超级组网中，则是将网络部分的某些位合并进主机部分。这种无类别超级组网技术通过将一组较小的无类别网络汇聚为一个较大的单一路由表项，减少了 Internet 路由域中路由表条目的数量。

2. 可变长子网掩码 VLSM5

为了有效地使用无类型域间路由和路由汇总来控制路由表的大小，网络管理员使用先进的 IP 寻址技术，可变长子网掩码 VLSM(Variable Length Subnet Mask)就是其中的常用方式。网络设计人员使用 VLSM 为网络制定子网划分方案，通过使用 VLSM，可以方便同一个父网的所有子网都有相同数量的主机地址和相同的前缀长度。VLSM 可更有效地利用 IP 地址空间，还让路由器能够在除分类网络边界外的其他地方汇总路由。

3. 子网划分

根据 IP 网络需求中的信息，网络设计人员确定每个网络区域所需 IP 地址块的大小，将需求相似的区域编组，以减少需要支持的子网掩码数量，如果所有设备都需要分配注册的公有 IP 地址，编组将毫无意义。通过减少子网数，设计人员可简化配置，这将简化网络工作人员的工作量和排除故障工作。

(1)定义

子网划分是通过借用 IP 地址的若干位主机位来充当子网地址从而将原网络划分为若干子网而实现的。

(2)步骤

①确定要划分的子网数。

②求出子网数目对应二进制数的位数 N 及主机数目对应二进制数的位数 M。

③对该 IP 地址的原子网掩码，将其主机地址部分的前 N 位置取 1 或后 M 位置取 0 即得出该 IP 地址划分子网后的子网掩码。

http://www.neubooks.com

(3)举例

以C类网络为例,原有8位主机位,2的8次方即256个主机地址,默认子网掩码255.255.255.0。借用1位主机位,产生2个子网,每个子网有126个主机地址;借用2位主机位,产生4个子网,每个子网有62个主机地址……每个网中,第一个IP地址(即主机部分全部为0的IP)和最后一个IP(即主机部分全部为1的IP)不能分配给主机使用,所以每个子网的可用IP地址数为总IP地址数量减2;根据子网ID借用的主机位数,我们可以计算出划分的子网数、掩码、每个子网主机数,如下所示:

①划分子网数 ②子网位数 ③子网掩码(二进制) ④子网掩码(十进制) ⑤每个子网主机数

①1～2 ②1 ③11111111.11111111.11111111.10000000 ④255.255.255.128 ⑤126

①3～4 ②2 ③11111111.11111111.11111111.11000000 ④255.255.255.192 ⑤62

①5～8 ②3 ③11111111.11111111.11111111.11100000 ④255.255.255.224 ⑤30

①9～16 ②4 ③11111111.11111111.11111111.11110000 ④255.255.255.240 ⑤14

①17～32 ②5 ③11111111.11111111.11111111.11111000 ④255.255.255.248 ⑤6

①33～64 ②6 ③11111111.11111111.11111111.11111100 ④255.255.255.252 ⑤2

如上所示的C类网络中,若子网占用7位主机位时,主机位只剩一位,无论设为0还是1,都意味着主机位是全0或全1。由于主机位全0表示本网络,全1留作广播地址,这时子网实际没有可用主机地址,所以主机位至少应保留2位。

1.3.3 知识点3:VLAN规划分析

设计人员通过对公司需求分析和对地址规划得知,有领导办公室和职工办公室,并且他们有相同的网络地址,公司要求同一部门之间可以进行通信,但是职工办公室里的机器不可以跟领导办公室通信。根据需求我们将领导办公室设置成一个VLAN,将职工们按照所在部门设置成对应的VLAN。我们使用子网划分可节约IP地址和方便各个部门工作,但如果需要调集各个部门的精英协同完成一项工作的话,就不方便,正是由于以上各种的需求才使用了VLAN,可以动态的管理网络。

1. VLAN规划目的

VLAN即虚拟局域网技术,是一种将实际的物理设备划分到逻辑的几个区域内,使其具有自己独立的功能和作用,实际还是在一个局域网内,VLAN封装遵循IEEE802.1Q标准。同一个VLAN中的成员能够实现通信,不同VLAN间的信息不能通信,这样,VLAN将整个网络分割成多个独立的逻辑区域,避免了广播风暴的几率,而且有利于网络的管理,流量的控制,提高了网络的安全性。若需要通信必须要借助于三层设备来实现VLAN间的通信。

2. VLAN划分技术

(1)根据端口来划分VLAN

许多VLAN厂商都利用交换机的端口来划分VLAN成员。被设定的端口都在同一个广播域中。这样做允许各端口之间的通讯,并允许共享型网络的升级。但是,这种划分模式将虚拟网限制在了一台交换机上。

第二代端口VLAN技术允许跨越多个交换机的多个不同端口划分VLAN,不同交换机上的若干个端口可以组成同一个虚拟网。

以交换机端口来划分网络成员,其配置过程简单明了。因此,从目前来看,这种根据端口来

http://www.neubooks.com

划分 VLAN 的方式仍然是最常用的一种方式。

(2)根据 MAC 地址划分 VLAN

这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分,即对每个 MAC 地址的主机都配置它属于哪个组。这种划分 VLAN 方法的最大优点就是当用户物理位置移动时,即从一个交换机换到其他的交换机时,VLAN 不用重新配置,所以,可以认为这种根据 MAC 地址的划分方法是基于用户的 VLAN,这种方法的缺点是初始化时,所有的用户都必须进行配置,如果有几百个甚至上千个用户的话,配置是非常累的。而且这种划分的方法也导致了交换机执行效率的降低,因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员,这样就无法限制广播包了。另外,对于使用笔记本电脑的用户来说,他们的网卡可能经常更换,这样,VLAN 就必须不停地配置。

(3)根据网络层地址划分 VLAN

这种划分 VLAN 的方法是根据每个主机的网络层地址或协议类型(如果支持多协议)划分的,虽然这种划分方法是根据网络地址,比如 IP 地址,但它不是路由,与网络层的路由毫无关系。

这种方法的优点是用户的物理位置改变了,不需要重新配置所属的 VLAN,而且可以根据协议类型来划分 VLAN,这对网络管理者来说很重要,这种方法不需要附加的帧标签来识别 VLAN,这样可以减少网络的通信量。

这种方法的缺点是效率低,因为检查每一个数据包的网络层地址是需要消耗处理时间的(相对于前面两种方法),一般的交换机芯片都可以自动检查网络上数据包的以太网帧头,但要让芯片能检查 IP 帧头,需要更高的技术,同时也更费时。

(4)根据 IP 组播划分 VLAN

IP 组播实际上也是一种 VLAN 的定义,即认为一个组播组就是一个 VLAN,这种划分的方法将 VLAN 扩大到了广域网,因此这种方法具有更大的灵活性,而且也很容易通过路由器进行扩展,但是这种方法不适合局域网,主要是效率不高。

3. VLAN 划分实例讲解

根据实际情况将属于同一功能区的放在同一个 VLAN ,根据 VLAN 中终端数量的多少划分 IP 地址。

例:某公司现在有工程部、销售部、财务部、业务部、客户服务部……多个部门通过以太网连接,每个部门的计算机只可以访问各自的网段。工程部有 200 台电脑,销售部有 100 台电脑,财务部有 20 台电脑,业务部有 40 台电脑,客户服务部有 300 台电脑。

VLAN 的划分:工程部 VLAN10、销售部 VLAN20、财务部 VLAN30、业务部 VLAN40、客户服务部 VLAN50。

1.3.4　知识点 4:局域网互联分析

网络设计人员需要选择能满足公司需求的路由选择协议:

- 支持 VLSM 的无类路由选择协议;
- 路由选择更新较小且不频繁,以减少数据流;
- 网络在出现故障时能快速汇聚;

http://www.neubooks.com

◆ 易于排除故障和重新配置。

综合以上的要求设计人员选择了 3 种的路由协议，即 RIP 和 OSPF/EIGRP。

路由协议用于路由器动态寻找网络最佳路径，保证所有路由器拥有相同的路由表，决定数据包在网络上的行走路径。路由选择协议消息在路由器之间传送，允许路由器与其他路由器通信来修改和维护路由选择表。

典型的路由选择方式有两种：静态路由和动态路由。

1. 静态路由

静态路由是在路由器中设置固定的路由表。除非网络管理员干预，否则静态路由不会发生变化。由于静态路由不能对网络的改变作出反映，一般用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。在所有的路由中，静态路由优先级最高。当动态路由与静态路由发生冲突时，以静态路由为准。大型和复杂的网络环境通常不宜采用静态路由。一方面，网络管理员难以全面地了解整个网络的拓扑结构；另一方面，当网络的拓扑结构和链路状态发生变化时，路由器中的静态路由信息需要大范围地调整，这一工作的难度和复杂程度非常高。

2. 动态路由

动态路由是网络中的路由器之间相互通信，传递路由信息，利用收到的路由信息更新路由器表的过程。它能实时地适应网络结构的变化。如果路由更新信息表明发生了网络变化，路由选择软件就会重新计算路由，并发出新的路由更新信息。这些信息通过各个网络，引起各路由器重新启动其路由算法，并更新各自的路由表以动态地反映网络拓扑变化。动态路由适用于网络规模大、网络拓扑复杂的网络。当然，各种动态路由协议会不同程度地占用网络带宽和 CPU 资源，在网络拓扑发生变化时，路由更新会消耗带宽，随着路由表的增大，需要消耗更多的 CPU 资源，并消耗了内存。

3. 静态路由和动态路由的适用情形

静态路由和动态路由有各自的特点和适用范围，因此在网络中动态路由通常作为静态路由的补充。当一个分组在路由器中进行寻径时，路由器首先查找静态路由，如果查到则根据相应的静态路由转发分组；否则再查找动态路由。

4. 动态路由协议

根据是否在一个自治域内部使用，动态路由协议分为内部网关协议(IGP)和外部网关协议(EGP)。这里的自治域指一个具有统一管理机构、统一路由策略的网络。自治域内部采用的路由选择协议称为内部网关协议，常用的有 RIP、OSPF；外部网关协议主要用于多个自治域之间的路由选择，常用的是 BGP 和 BGP-4。下面分别进行简要介绍。

(1)RIP 路由协议

RIP 协议最初是为 Xerox 网络系统的 Xerox parc 通用协议而设计的，是 Internet 中常用的路由协议。RIP 采用距离矢量算法，即路由器根据距离选择路由，所以也称为距离矢量协议。路由器收集所有可到达目的地的不同路径，并且保存有关到达每个目的地的最少站点数的路径信息，除到达目的地的最佳路径外，任何其他信息均予以丢弃。同时路由器也把所收集的路由信息用 RIP 协议通知相邻的其他路由器。这样，正确的路由信息逐渐扩散到了全网。

RIP 使用非常广泛，它简单、可靠，便于配置。但是 RIP 只适用于小型的同构网络，因为它

http://www.neubooks.com

允许的最大站点数为 15，任何超过 15 个站点的目的地均被标记为不可达。而且 RIP 每隔 30s 一次的路由信息广播也是造成网络的广播风暴的重要原因之一。

(2)OSPF 路由协议

20 世纪 80 年代中期，RIP 已不能适应大规模异构网络的互连，OSPF 随之产生。它是网间工程任务组织(IETF)的内部网关协议工作组为 IP 网络而开发的一种路由协议。

OSPF 是一种基于链路状态的路由协议，需要每个路由器向其同一管理域的所有其他路由器发送链路状态广播信息。在 OSPF 的链路状态广播中包括所有接口信息、所有的量度和其他一些变量。利用 OSPF 的路由器首先必须收集有关的链路状态信息，并根据一定的算法计算出到每个节点的最短路径。而基于距离向量的路由协议仅向其邻接路由器发送有关路由更新信息。

与 RIP 不同，OSPF 将一个自治域再划分为区，相应地即有两种类型的路由选择方式：当源和目的地在同一区时，采用区内路由选择；当源和目的地在不同区时，则采用区间路由选择。这就大大减少了网络开销，并增加了网络的稳定性。当一个区内的路由器出了故障时并不影响自治域内其他区路由器的正常工作，这也给网络的管理、维护带来方便。

(3)BGP 和 BGP-4 路由协议

BGP 是为 TCP/IP 互联网设计的外部网关协议，用于多个自治域之间。它既不是基于纯粹的链路状态算法，也不是基于纯粹的距离向量算法。它的主要功能是与其他自治域的 BGP 交换网络可达信息。各个自治域可以运行不同的内部网关协议。BGP 更新信息包括网络号/自治域路径的成对信息。自治域路径包括到达某个特定网络须经过的自治域串，这些更新信息通过 TCP 传送出去，以保证传输的可靠性。

为了满足 Internet 日益扩大的需要，BGP 还在不断地发展。在最新的 BGP4 中，还可以将相似路由合并为一条路由。

1.3.5　知识点 5：网络优化与安全管理

设计人员发现在进行网络访问时有时会存在访问瓶颈的问题，在网络出现故障或其他原因断开其中一条或多条链路时，剩下的链路不可以工作，流量在某些端口上无法自动进行负载均衡，想达到更高的数据传输率但是成本太高等等，要想消除这些现象可采用端口聚合技术，这样就可解决相关问题的出现了。

网络虽然得到相应的优化了，公司员工可以更好地去使用网络了，但是现今网络的威胁形式变化多样，可能来自内部，也可能来自外部。仅在企业边缘部署防火墙并不能保证网络的安全。设计人员必须确定可能受到的威胁的数据和通信以及潜在的攻击源，以防范可能发生的攻击。网络安全从保护网络设备开始，这就包括路由器、交换机和设备免受直接或间接攻击。这种保护有助于确保网络可用于传输数据，常用的基础设施保护包括：关闭不需要的服务、关闭所有未用的端口和接口、为 VTY、控制台和 AUX 端口设置超时和 ACL 等。

1. 提高链路带宽——端口聚合

(1)定义

端口聚合是将多物理连接当作一个单一的逻辑连接来处理，它允许两个交换器之间通过多个端口并行连接同时传输数据以提供更高的带宽、更大的吞吐量和可恢复性的技术。

http://www.neubooks.com

(2)实现

这一技术是以较低的成本通过捆绑多端口提高带宽,而其增加的开销只是连接用的普通五类网线和多占用的端口,它可以有效地提高子网的上行速度,从而消除网络访问中的瓶颈。另外 Trunk 还具有自动带宽平衡,即容错功能:即使 Trunk 只有一个连接存在时,仍然会工作,这无形中增加了系统的可靠性。

(3)端口聚合方式

静态聚合:双方系统间不使用聚合协议来协商链路信息。

动态聚合:双方系统间使用聚合协议来协商链路信息。

2. 提高局域网安全——端口安全

(1)定义

端口安全是连接到交换机端口与以太网 MAC 地址绑定。

(2)安全实现

任何其他 MAC 地址试图通过此端口通信,端口安全特性会阻止它。使用端口安全特性可以防止某些设备访问网络,并增强安全性,当主机 MAC 地址与绑定的端口不一致,则端口将自动关闭,从而实现了对网内主机的保护,从而实现了端口的安全设置。

3. 园区网内访问控制——ACL

公司管理的安全策略制定了用户和用户组访问资源的权限。设计人员应遵守服务器操作系统厂商推荐的做法,这种做法有助于识别并过滤已知的恶意数据流。设计 ACL 时,通常的策略是拒绝所有这样的数据流,即没有明确授权,也不是对允许查询的响应。

(1)定义

访问控制列表(Access Control List,ACL)是通过设置权限,用来控制端口进出的数据包。

(2)ACL 访问安全控制

一个端口执行哪条 ACL,这需要按照列表中的条件语句执行顺序来判断。如果一个数据包的报头跟表中某个条件判断语句相匹配,那么后面的语句就将被忽略,不再进行检查。数据包只有在跟第一个判断条件不匹配时,它才被交给 ACL 中的下一个条件判断语句进行判断,数据会立即发送到目的接口。如果所有的 ACL 判断语句都检测完毕,仍没有匹配的语句出口,则该数据包将视为被拒绝而被丢弃。注意:ACL 不能对本路由器产生的数据包进行控制。

4. 接入 Internet 访问控制(NAT)

(1)定义

NAT(Network Address Translation,网络地址转换)是将 IP 数据包头中的 IP 地址转换为另一个 IP 地址的过程。NAT 主要用于实现私有网络访问公共网络的功能。这种通过使用少量的公有 IP 地址代表较多的私有 IP 地址的方式,将有助于减缓可用 IP 地址空间的枯竭。

(2)NAT 技术实现方式

NAT 的实现方式有三种,即静态转换 Static Nat、动态转换 Dynamic Nat 和端口多路复用 OverLoad。

静态转换是指将内部网络的私有 IP 地址转换为公有 IP 地址,IP 地址对是一对一的,是一成不变的,某个私有 IP 地址只转换为某个公有 IP 地址。借助于静态转换,可以实现外部网络对内部网络中某些特定设备(如服务器)的访问。

http://www.neubooks.com

动态转换是指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址是不确定的，是随机的，所有被授权访问上 Internet 的私有 IP 地址可随机转换为任何指定的合法 IP 地址。也就是说，只要指定哪些内部地址可以进行转换，以及用哪些合法地址作为外部地址时，就可以进行动态转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时。可以采用动态转换的方式。

端口多路复用(Port Address Translation，PAT)是指改变外出数据包的源端口并进行端口转换，即端口地址转换。采用端口多路复用方式，内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自 Internet 的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

1.4　项目实施

当接手一个网络项目时一般都按照以下步骤进行实施。

1. 网络结构设计

首先进行网络结构设计，在网络结构设计方面，将完成如下工作：网络层次划分、核心节点设计、汇聚节点设计以及接入层设计。

(1)网络层次划分

按照网络扁平化设计原则，对网络进行统一规划、统一建设、统一管理。将整个网络划分为核心层、汇聚层、接入层。

(2)核心层设计

根据网络业务量分布，选择两个节点构成核心层；两个主核心节点直接汇聚相关汇聚节点的流量，所有的流量都通过这两个主核心节点汇聚到骨干网。核心节点为全网范围的用户提供流量汇聚，并向核心出口路由器进行转发。

(3)汇聚层设计

根据网络地域特性和具体地理分布的情况，设置多个汇聚节点，负责汇聚本地流量或者下级的汇聚节点的流量，根据流量增长，可以利用开销的流量负载均衡等，提高链路带宽利用率并提高网络的可靠性。

(4)接入层设计

根据拓扑图的设计要求选用 NAT 或者 PPP 的方式接入到外部的 Internet 中去。

2. 相关设定

当相关的设计完成后将进行设备命名、接口参数以及地址规划的设定。

3. 网络路由部署

根据拓扑图的要求进行网内各区域的路由部署。

4. IP 地址规划

IP 地址的合理分配是保证网络顺利运行和网络资源有效利用的关键。对网络的 IP 地址分配应该尽可能地利用申请到的地址空间，充分考虑到地址空间的合理使用，保证实现最佳的

http://www.neubooks.com

网络内地址分配及业务流量的均匀分布。同时，根据网络的业务发展计划，用户数量将大量膨胀，因此必然需要申请新的地址空间，满足业务发展的需求。

IP 地址空间的分配与合理使用与网络拓扑结构、网络组织及路由政策有非常密切的关系，将对全网的可用性、可靠性与有效性产生显著影响，应充分考虑不同用户对 IP 地址的需求，以满足未来业务发展对 IP 地址的需求。

5. VLAN 规划

通过划分 VLAN，可以实现流量和用户的隔离。通过把不同的流量映射到不同的 VLAN 中并分配相应的优先级，可以为用户提供不同优先级别的服务质量保证。但是，VLAN 的划分必须进行合理的规划，首先，二层网络的范围不宜过大，过大的二层网络将导致大量的 STP 计算，使设备的性能下降并降低网络的效率；其次，VLAN ID 资源有限，每台交换机全局支持 4096 个 802.1q VLAN ID，每台交换机能同时支持的 STP 实例也是有限的。

6. 设备安全设置

网络的安全性在很大程度上取决于网络设备的安全性，设备的安全方面的配置，是尤为重要的。一般针对网络设备本身的安全，做好如下配置：

在网络设备上关闭不必要的服务，如 Finger、Bootp、Http 等。

缺省情况下，从任何地方都可以登录网络设备。为了增加网络设备的安全性，需要对远程登录的范围进行限制。通常使用访问控制列表(ACL)限制登录主机的源地址，只有具有符合条件的主机能够登录到该网络设备上。配置分为两步：

- 定义访问控制列表(ACL)；
- 应用访问控制列表(ACL)。

定义好 ACL 后，将 ACL 应用到 VTY 端口即可对能够登录设备的主机进行限制。另外需要对能够登录网络设备的用户进行管理，对网络设备有可配置权限的用户尤其要严格控制。建议采用分区分权管理，不要使对于网络拥有可配置权限的用户名/口令系统让太多的管理人员涉及，应该紧收；对于一般可操作权限的用户/口令系统可以适当的放的松些。

7. 设备的调试与故障排除

最后可进行设备连接的调试，一般采用常用的设备调试命令进行调试。当出现问题时要对出现的故障进行排除，最后达到稳定性和可靠性。

1.5 技术拓展

(1)IP 分配应考虑近期和远期的发展，减少在网络发展过程中因地址重新规划而对业务造成的影响。

(2)根据 APNIC 地址申请原则，IP 地址的规划应立足近期，并根据业务发展需要做 6 个月到 1 年的地址需求预测。

(3)IP 地址的分配必须采用 VLSM 技术，保证 IP 地址的利用效率。

(4)采用 CIDR 技术，这样可以减小路由器路由表的大小，加快路由器路由的收敛速度，也可以减小网络中广播的路由信息的大小。

http://www.neubooks.com

(5)地址分配应该考虑使用的路由协议,便于路由表的汇聚和控制,应尽可能连续分配。

(6)所有 Internet 用户采用公有 IP 地址,避免使用 NAT 设备以便保证未来基于 H.323 或 NGN 技术的业务顺利开展;如必需使用 NAT,则建议将 NAT 设备尽可能部署在用户侧或边缘接入层次。

(7)将城域网的 IP 地址资源分块,并分到核心层、汇聚层节点,其中一段地址作为核心、汇聚层设备互联之用;其余各节点分配到的地址按照用户地址与网络互联地址两种应用,以背对背的方式,分别"从前向后",和"从后向前"的形式进行规划和使用。

1.6　本章小结

通过本章的学习,可以掌握项目分析的基本过程,即从网络设备的选型、拓扑结构的选择、子网划分、子网地址的规划选择、VLAN 的规划、路由的部署、到网络的优化以及安全管理,后面的章节将详细介绍每一部分的具体设置步骤。

1.7　强化练习

1.已知 172.31.128.255/18,试计算:

(1)子网数目;

(2)网络号;

(3)主机号;

(4)广播地址;

(5)可分配 IP 的起止范围。

2.划分 VLAN 的方法都有哪些?

3.常见的链路状态路由协议有(　　)。

A. RIP　　B. BGP　　C. IS-IS　　D. OSPF

4.常见的 IGP 路由协议包括(　　)。

A. RIP　　B. OSPF　　C. IS-IS　　D. BG

5.RIP 协议路由表的更新报文发送周期是(　　)秒。

A. 5　　B. 30　　C. 60　　D. 180

6.关于 RIP 协议下列说法正确的有(　　)。

A. RIP 协议是一种 IGP

B. RIP 协议是一种 EGP

C. RIP 协议是一种距离矢量路由协议

D. RIP 协议是一种链路状态路由协议

7.NAT 技术的实现方式有哪些?

8.端口聚合的方式有哪些?

http://www.neubooks.com

任务 2

网络搭建与设备互联

2.1 项目导引

新起点网络技术有限公司承接的某城市城域网建设项目，前期已完成了项目分析与规划设计，接下来要进行的工作就是对项目的实施，在该项目的实施过程中，需要先对网络设备进行连接，完成网络拓扑硬件搭建，并对网络设备进行基本配置。

2.2 项目分析

首先对该城域网项目进行了分析，对网络搭建与设备互联任务进行细化，可将项目分解为以下任务：

(1)网络设备互联：了解网络设备互联采用的各类线缆和路由器的接口类型等网络设备互联的基本知识。

(2)设备基本配置：了解路由器、交换机的内部构造及启动顺序，能够对交换机、路由器这些网络设备进行基本配置，配置网络设备的 console、telnet、enable 密码，根据地址规划表为各路由器、交换机配置正确的地址信息。

2.3 技术准备

2.3.1 知识点 1：网络设备互联

1. 网络设备互联采用的线缆

要将网络设备连接并接入网络需要不同类型的线缆，我们要根据设备的类型以及所具有接口的不同类型来进行选择。现代网络主要使用三种介质来连接设备并提供传输数据的途径：内含铜质导线的电缆、玻璃或塑料纤维(光缆)、无线传输。

http://www.neubooks.com

(1)双绞线

双绞线(TP)是一种铜质电缆,分为屏蔽双绞线和非屏蔽双绞线两种类型。用来连接 LAN 接口的连接器中,最为常见的是用于非屏蔽双绞线(UTP)电缆的 RJ-45 水晶头,如图 2-1 所示。

双绞线整体效果如图 2-2 所示。

图 2-1　RJ-45 水晶头

图 2-2　双绞线

双绞线由 8 根具有绝缘保护层的铜导线组成,每两根铜导线按一定密度互相绞在一起,每一根导线在传输中辐射出来的电波会被另一根线上发出的电波抵消,有效降低信号干扰的程度,双绞线的两端按照布线标准安装 RJ-45 水晶头。EIA/TIA 的布线标准中规定了两种双绞线的线序 T-568A 与 T-568B。T-568A 的排线顺序从左到右依次为:绿白、绿、橙白、蓝、蓝白、橙、棕白、棕;T-568B 的排线顺序从左到右依次为:橙白、橙、绿白、蓝、蓝白、绿、棕白、棕。如果线缆两端的线序不同,即一端是 568A 标准,另一端是 568B 标准的双绞线,称为交叉线;如果线缆两端的线序相同,即两端都是 568A 或都是 568B 标准的双绞线,称为直通线。如图 2-3 所示。

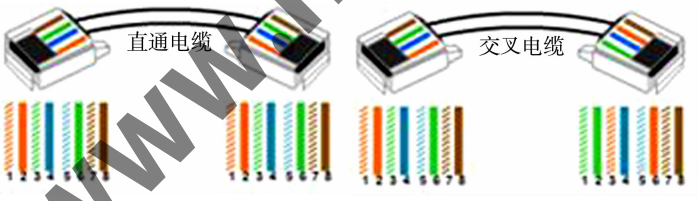

图 2-3　直通线与交叉线

直通线与交叉线应用的场景不同,直通电缆可用于:交换机至路由器、交换机至 PC、集线器至 PC、集线器至服务器等,交叉电缆可用于:交换机至交换机、PC 至 PC、交换机至集线器、集线器至集线器、路由器至路由器、路由器至服务器等。有的网络设备已经带有智能分辨功能,这时直通线和交叉线都可以正常使用,否则信号无法传输。

(2)串口线缆

串行接口(Serial Interface)是指数据一位一位地顺序传送,其特点是通信线路简单,只要一对传输线就可以实现双向通信,从而大大降低了成本,特别适用于远距离通信,但传送速度较慢。这种接口是现在最常见的网络设备广域网接口,俗称“串口”。Cisco 路由器支持EIA/TIA-232、EIA/TIA-449、V.35、X.21 等串行连接标准。常见的路由器串口线缆有:RS-232 电缆、V.35 电缆、X.21 电缆、RS-449 电缆等。

目前,随着宽带模拟调制解调器应用的逐渐减少,V.35 被常用于支持 DTE 和新兴的数字传输设施不同类型数据服务单元(DSU)连接之间的接口。由此,在对最初的 V.35 建议进行多次修订后,成为当前通信设备中流行的、用于连接远程的高速同步接口。大多数的服务单元,如

http://www.neubooks.com

分组交换机、路由器、远程网桥和网关都带有 V.35 接口。在 V.35 的标准中，线缆有两类，一类是 DTE，一类是 DCE，DTE 是公头，DCE 是母头，插头上是针的为公头，如图 2-4 所示，插头上是孔的为母头，如图 2-5 所示，这样两种接口才能接在一起。

DCE 端需要设置时钟，提供了一个用于同步 DCE 设备和 DTE 设备之间数据传输的时钟信号。

图 2-4 V.35 线缆公头

图 2-5 V.35 线缆母头

(3)Console 线

Console 线一般叫做配置线，对网络设备进行初始化配置，或者设备无法通过网络访问时，通常会使用 Console 口进行设备配置。在使用 Console 口连接配置设备时需要使用专用的设备配置线。配置线外形上看，一边是 RJ-45 接头，用于连接网络设备的 Console 接口，另一头的 COM(DB9)接头用于连接计算机的 COM 口，通过超级终端来配置设备。Console 线如图 2-6 所示。

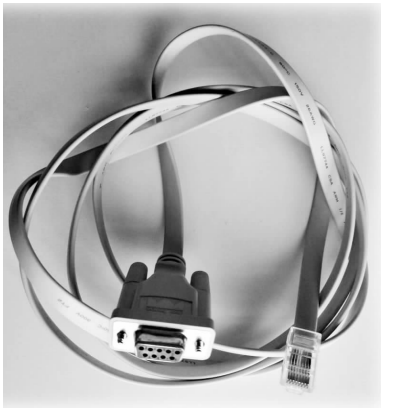

图 2-6 Console 线

2. 路由器的接口

路由器包含用于管理路由器的物理接口，这些接口也称为管理端口，与以太网接口和串行接口不同，管理端口不用于转发数据包。最常见的管理端口是控制台端口，控制台端口用于连接终端(多数情况是运行终端模拟器软件的 PC)，从而在无需通过网络访问路由器的情况下配置路由器。对路由器进行初始配置时，必须使用控制台端口。另一种管理端口是辅助端口，并非所有路由器都有辅助端口，有时，辅助端口的使用方式与控制台端口类似，此外，此端口也可用于连接调制解调器。如图 2-7所示是路由器的接口外观。

图 2-7 路由器接口外观

接口一词在 Cisco 路由器中表示主要负责接收和转发数据包的路由器物理接口。路由器有多个接口，用于连接多个网络。通常，这些接口连接到多种类型的网络，也就是说需要各种不同类型的介质和接口。例如，路由器一般具有快速以太网接口，用于连接不同的 LAN；还具有各种类型的 WAN 接口，用于连接多种串行链路(其中包括 T1、DSL 和 ISDN)。

http://www.neubooks.com

与大多数网络设备一样，Cisco 路由器使用 LED 指示灯提供状态信息。接口上的 LED 会指示对应接口的活动情况。如果接口为活动状态而且连接正确，但 LED 不亮，则表示该接口可能存在故障。如果接口繁忙，则其 LED 会一直亮起。

路由器上的每个接口都是不同 IP 网络的成员或主机，每个接口必须配置一个 IP 地址以及对应网络的子网掩码，Cisco IOS 不允许同一路由器上的两个活动接口属于同一网络。

路由器接口主要可分为两组：

LAN 接口——如以太网接口和快速以太网接口。

WAN 接口——如串行接口、ISDN 接口和帧中继接口。

(1)LAN 接口

顾名思义，LAN 接口用于将路由器连接到 LAN，如同 PC 的以太网网卡用于将 PC 连接到以太网 LAN 一样。类似于 PC 以太网网卡，路由器以太网接口也有第 2 层 MAC 地址，且其加入以太网 LAN 的方式与该 LAN 中任何其他主机相同。例如，路由器以太网接口会参与该 LAN 的 ARP 过程。路由器会为对应接口提供 ARP 缓存、在需要时发送 ARP 请求，以及根据要求以 ARP 回复作为响应。

路由器以太网接口通常使用支持非屏蔽双绞线 (UTP) 网线的 RJ-45 接口。当路由器与交换机连接时，使用直通电缆。当两台路由器直接通过以太网接口连接，或 PC 网卡与路由器以太网接口连接时，使用交叉电缆。

(2)WAN 接口

WAN 接口用于连接路由器与外部网络，这些网络通常分布在距离较为遥远的地方。WAN 接口的第 2 层封装可以是不同的类型，如 PPP、帧中继和 HDLC(高级数据链路控制)。与 LAN 接口一样，每个 WAN 接口都有自己的 IP 地址和子网掩码，这些可将接口标识为特定网络的成员。

2.3.2　知识点 2：设备基本配置

1. 互联网操作系统 IOS

Cisco 设备采用的操作系统软件称为 Cisco Internetwork Operating System(IOS)。与计算机上的操作系统一样，Cisco IOS 会管理路由器或交换机的硬件和软件资源，Cisco IOS 属于多任务操作系统，集成了路由、交换、网际网络及电信等功能。

虽然许多路由器中的 Cisco IOS 看似相同，但实际却是不同类型的 IOS 映像。IOS 映像是一种包含相应路由器完整 IOS 的文件，Cisco 根据路由器型号和 IOS 内部的功能，创建了许多不同类型的 IOS 映像。通常，IOS 内部的功能越多映像就越大，因此就需要越多的闪存和 RAM 来存储和加载 IOS。例如，某些功能包括了运行 IPv6 的能力，或者能让路由器执行 NAT(网络地址转换)。

与其他操作系统一样，Cisco IOS 也有自己的用户界面，命令行界面(CLI)是配置 Cisco 设备的最常用方法。

2. 网络设备的结构与启动顺序

(1)路由器的结构与启动顺序

路由器其实也是计算机，它的组成结构类似于任何其他计算机(包括 PC)，图 2-8 是某路由

http://www.neubooks.com

器的外观。

图 2-8 ISR 系列 1841 型

尽管路由器类型和型号多种多样，但每种路由器都具有相同的通用硬件组件，与 PC 一样，路由器也包含中央处理器(CPU)、随机访问存储器(RAM)、只读存储器(ROM)。CPU 执行操作系统指令，如系统初始化、路由功能和交换功能。RAM 存储 CPU 所需执行的指令和数据，包括操作系统、运行配置文件、IP 路由表、ARP 缓存、数据包缓冲区。ROM 是一种永久性存储器，使用的是固件，Cisco 设备使用 ROM 来存储 bootstrap 指令、基本诊断软件、精简版 IOS，如果路由器断电或重新启动，ROM 中的内容不会丢失。闪存是非易失性计算机存储器，可以电子的方式存储和擦除，闪存用作操作系统 Cisco IOS 的永久性存储器，在大多数 Cisco 路由器型号中，IOS 是永久性存储在闪存中的，可以通过升级这些卡来增加闪存的容量，如果路由器断电或重新启动，闪存中的内容不会丢失。NVRAM(非易失性 RAM)在电源关闭后不会丢失信息，这与大多数普通 RAM(如 DRAM)不同，后者需要持续的电源才能保持信息。NVRAM 被 Cisco IOS 用作存储启动配置文件(startup-config)的永久性存储器，要保存这些更改以防路由器重新启动或断电，必须将 running-config 复制到 NVRAM，并在其中存储为 startup-config 文件。

路由器启动过程主要有四个阶段。

①执行 POST

加电自检(POST)几乎是每台计算机启动过程中必经的一个过程，POST 过程用于检测路由器硬件。当路由器加电时，ROM 芯片上的软件便会执行 POST，在这种自检过程中，路由器会通过 ROM 执行诊断，主要针对包括 CPU、RAM 和 NVRAM 在内的几种硬件组件。

②加载 bootstrap 程序

POST 完成后，bootstrap 程序将从 ROM 复制到 RAM，进入 RAM 后，CPU 会执行 bootstrap 程序中的指令。bootstrap 程序的主要任务是查找 Cisco IOS 并将其加载到 RAM。此时，如果有连接到路由器的控制台，会看到屏幕上开始出现输出内容。

③查找并加载 Cisco IOS

IOS 通常存储在闪存中，但也可能存储在其他位置，如 TFTP(简单文件传输协议)服务器上。如果不能找到完整的 IOS 映像，则会从 ROM 将精简版的 IOS 复制到 RAM 中。这种版本的 IOS 一般用于帮助诊断问题，也可用于将完整版的 IOS 加载到 RAM。有些较早的 Cisco 路由器可直接从闪存运行 IOS，但现今的路由器会将 IOS 复制到 RAM 后由 CPU 执行。

④查找并加载配置文件

IOS 加载后，bootstrap 程序会搜索 NVRAM 中的启动配置文件(也称为 startup-config)，此文件含有先前保存的配置命令以及参数，其中包括接口地址、路由信息、口令和网络管理员保存的其他配置。如果在 NVRAM 中找到启动配置文件，则 IOS 会将其加载到 RAM 作为 running-config，并以一次一行的方式执行文件中的命令。running-config 文件包含接口地址，并可启动路由过程以及配置路由器的口令和其他特性。如果不能找到启动配置文件，路由器会

http://www.neubooks.com

提示用户进入设置模式。设置模式包含一系列问题，提示用户一些基本的配置信息。设置模式不适于复杂的路由器配置，网络管理员一般不会使用该模式，当启动不含启动配置文件的路由器时，会在 IOS 加载后看到以下问题：

```
Would you like to enter the initial configuration dialog? [yes/no]:no
```

当提示进入设置模式时，回答 no。如果回答 yes 并进入设置模式，可随时按【Ctrl＋C】终止设置过程。不使用设置模式时，IOS 会创建默认的 running-config。默认 running-config 不包含任何接口地址、路由信息、口令或其他特定配置信息。

一旦显示提示符，路由器便开始以当前的运行配置文件运行 IOS。而网络管理员也可开始使用此路由器上的 IOS 命令。

(2)交换机的组成与启动顺序

思科交换机的硬件结构包括 CPU、接口系统、存储介质、电源，存储介质包含 ROM、Flash、NVRAM、DRAM，其中 ROM 用来存放引导程序，Flash 存储 IOS，NVRAM 存储 startup-config 启动配置文件，DRAM 用于存储 running-config 运行配置文件。在 Cisco 交换机开启之后，它将经过以下启动顺序：

①首先，交换机加载存储在 ROM 中的加电自检(POST)程序。POST 对系统进行自检，会检查 CPU 子系统，测试 CPU、DRAM 以及构成闪存文件系统的闪存设备部分。接下来交换机加载启动加载器软件。启动加载器是存储在 ROM 中并在 POST 成功完成后立即运行的小程序。

②启动加载器执行低级 CPU 初始化，引导运行 Flash 中的 IOS。启动加载器初始化 CPU 寄存器，寄存器控制物理内存的映射位置、内存量以及内存速度。启动加载器初始化系统主板上的闪存文件系统，引导运行 Flash 中的 IOS，并将默认 IOS 操作系统软件镜像加载到内存。

③NVRAM(或 Flash)中寻找交换机的配置文件。

④将初始配置装入 DRAM 中运行，即 running-config。

3. 交换机的工作原理

交换机使用其 MAC 地址表来确定如何处理传入的数据帧，交换机通过记录与其每一个端口相连的节点的 MAC 地址来构建其 MAC 地址表。当某个特定端口上的某个特定节点的 MAC 地址记录到地址表之后，交换机就可以知道在后续传输中，应将目的地为该特定节点的流量从与该节点对应的端口上发出。

当交换机收到传入的数据帧，而地址表中没有该帧的目的 MAC 地址时，交换机将把该帧从除接收该帧的端口之外的所有端口转发出去。当目的节点响应时，交换机从响应帧的源地址字段中获得的该节点的 MAC 地址，并将其记录在地址表中。在多台交换机互联的网络中，连接其他交换机的端口在 MAC 地址表中记录有多个 MAC 地址，用来代表远端节点。通常，用于互联两台交换机的交换机端口在 MAC 地址表中记录了多个 MAC 地址。

图 2-9　交换机与 PC 连接拓扑图

根据图 2-9 所示网络拓扑，可以把交换机 MAC 寻址工作过程总结如下：

http://www.neubooks.com

步骤 1:交换机在端口 1 上收到来自 PC1 的广播帧。

步骤 2:交换机将源 MAC 地址以及接收该帧的交换机端口输入地址表。

步骤 3:由于目的地址为广播,因此交换机将该帧泛洪发送到所有端口(接收该帧的端口除外)。

步骤 4:目的设备为了响应广播,发出目标地址为 PC1 的单播帧。

步骤 5:交换机将 PC2 的源 MAC 地址和接收该帧的交换机端口的端口号输入地址表。帧的目的地址及其关联的端口可在 MAC 地址表中找到。

步骤 6:交换机现在无需泛洪即可在源设备和目的设备之间转发帧,因为地址表中已经有了标识关联端口的条目。

4. 网络设备配置模式

(1)配置模式

Cisco IOS 软件将路由器、交换机的工作模式设为用户模式、特权模式、全局配置模式以及一些其他配置模式。

用户模式只允许用户访问有限量的基本监视命令。用户执行模式是在从 CLI 登录到 Cisco 交换机后所进入的默认模式。用户执行模式由>提示符标识。

特权模式允许用户访问所有设备命令,如用于配置和管理的命令,特权执行模式可采用口令加以保护,使得只有获得授权的用户才能访问设备。特权执行模式由 # 提示符标识。要从用户执行模式切换到特权执行模式,输入 enable 命令。

全局配置模式用于配置全局交换机参数(例如用于交换机管理的交换机主机名或交换机 IP 地址)。要访问全局配置模式,在特权执行模式下输入 configure terminal 命令。提示符将更改为(config)#。

要从全局配置模式下访问接口配置模式,输入 interface<interface name>命令。提示符将更改为(config-if)#。

要退出到上一级模式,使用 exit 命令,使用 end 直接退至特权模式。

```
Switch>
Switch>enable
Switch#configure terminal
Switch(config)#interface f0/1
Switch(config-if)#exit
Switch(config)#end
Switch#
```

(2)使用控制台帮助

Cisco IOS CLI 提供了两种类型的帮助。

①词语帮助:如果记不起完整命令,但是记得开头几个字符,则可以按顺序先输入这几个字符,然后再输入一个问号(?),问号前面不要加入空格。以输入的字符开头的一系列命令将随即显示,例如,输入 sh? 将返回以 sh 字符序列开头的所有命令的列表。

②命令语法帮助:如果不熟悉在 Cisco IOS CLI 的当前上下文中可以使用哪些命令,或者不知道要使给定命令完整需要哪些参数或可以使用哪些参数,则可以输入? 命令。

http://www.neubooks.com