

## 在 Oracle® Solaris 11.2 中规划网络部署

ORACLE®

文件号码 E53783  
2014 年 7 月

版权所有 © 2011, 2014, Oracle 和/或其附属公司。保留所有权利。

本软件和相关文档是根据许可证协议提供的，该许可证协议中规定了关于使用和公开本软件和相关文档的各种限制，并受知识产权法的保护。除非在许可证协议中明确许可或适用法律明确授权，否则不得以任何形式、任何方式使用、拷贝、复制、翻译、广播、修改、授权、传播、分发、展示、执行、发布或显示本软件和相关文档的任何部分。除非法律要求实现互操作，否则严禁对本软件进行逆向工程设计、反汇编或反编译。

此文档所含信息可能随时被修改，恕不另行通知，我们不保证该信息没有错误。如果贵方发现任何问题，请书面通知我们。

如果将本软件或相关文档交付给美国政府，或者交付给以美国政府名义获得许可证的任何机构，必须符合以下规定：

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

本软件或硬件是为了在各种信息管理应用领域内的一般使用而开发的。它不应被应用于任何存在危险或潜在危险的应用领域，也不是为此而开发的，其中包括可能会产生人身伤害的应用领域。如果在危险应用领域内使用本软件或硬件，贵方应负责采取所有适当的防范措施，包括备份、冗余和其它确保安全使用本软件或硬件的措施。对于因在危险应用领域内使用本软件或硬件所造成的一切损失或损害，Oracle Corporation 及其附属公司概不负责。

Oracle 和 Java 是 Oracle 和/或其附属公司的注册商标。其他名称可能是各自所有者的商标。

Intel 和 Intel Xeon 是 Intel Corporation 的商标或注册商标。所有 SPARC 商标均是 SPARC International, Inc 的商标或注册商标，并应按照许可证的规定使用。AMD、Opteron、AMD 徽标以及 AMD Opteron 徽标是 Advanced Micro Devices 的商标或注册商标。UNIX 是 The Open Group 的注册商标。

本软件或硬件以及文档可能提供了访问第三方内容、产品和服务的方式或有关这些内容、产品和服务的信息。对于第三方内容、产品和服务，Oracle Corporation 及其附属公司明确表示不承担任何种类的担保，亦不对其承担任何责任。对于因访问或使用第三方内容、产品或服务所造成的任何损失、成本或损害，Oracle Corporation 及其附属公司概不负责。

# 目录

---

使用本文档 .....	5
1 规划网络部署 .....	7
确定网络硬件 .....	7
网络拓扑概述 .....	8
在网络上使用子网 .....	10
IPv4 自治系统拓扑 .....	11
为网络规划路由器 .....	12
路由器如何传送包 .....	13
确定网络的 IP 地址寻址格式 .....	14
IPv4 地址 .....	14
专用地址 .....	15
DHCP 地址 .....	16
IPv6 地址 .....	16
文档前缀 .....	16
获取网络的 IP 号 .....	16
在网络上使用命名实体 .....	17
域名 .....	17
选择命名服务和目录服务 .....	17
管理主机名 .....	18
2 规划 IPv6 地址的使用 .....	19
IPv6 规划任务 .....	19
IPv6 网络拓扑概述 .....	20
确保硬件支持 IPv6 .....	22
准备 IPv6 寻址计划 .....	22
获取站点前缀 .....	23
制定 IPv6 编号方案 .....	23
配置网络服务以支持 IPv6 .....	24
▼ 如何准备网络服务以支持 IPv6 .....	24

▼ 如何准备 DNS 以支持 IPv6 .....	25
网络中使用隧道的规划 .....	26
IPv6 实现的安全注意事项 .....	26
索引 .....	29

## 使用本文档

---

- 概述 – 包括帮助您规划部署 IPv4 和 IPv6 网络的基本主题和任务。
- 目标读者 – 系统管理员。
- 必备知识 – 基本了解网络管理概念和做法。

## 产品文档库

有关本产品的最新信息和已知问题均包含在文档库中，网址为：<http://www.oracle.com/pls/topic/lookup?ctx=E56344>。

## 获得 Oracle 支持

Oracle 客户可通过 My Oracle Support 获得电子支持。有关信息，请访问 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>；如果您听力受损，请访问 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>。

## 反馈

请在 <http://www.oracle.com/goto/docfeedback> 提供有关本文档的反馈。



## 规划网络部署

---

本章介绍了规划 TCP/IP 网络部署时的各种注意事项。介绍的规划任务可以帮助您以有组织且经济有效的方式部署网络。请注意，本书并不详细讨论如何规划网络，只提供一般说明。本书还假定您熟悉基本网络概念和术语。

有关如何在 Oracle Solaris 中实现 TCP/IP 的说明以及此发行版中网络管理的概述，请参见《在 Oracle Solaris 11.2 中配置和管理网络组件》中的第 1 章“关于 Oracle Solaris 中的网络管理”。

对于规划站点的整体联网方案，要获得进一步帮助，请阅读《Oracle Solaris 11.2 中的网络管理策略》中的第 1 章“Oracle Solaris 网络管理摘要”中所述的联网策略。

本章包含以下主题：

- “确定网络硬件” [7]
- “网络拓扑概述” [8]
- “在网络上使用子网” [10]
- “IPv4 自治系统拓扑” [11]
- “为网络规划路由器” [12]
- “确定网络的 IP 地址寻址格式” [14]
- “获取网络的 IP 号” [16]
- “在网络上使用命名实体” [17]

## 确定网络硬件

您期望支持的系统数量影响网络配置方式。您的组织可能需要由某一建筑的同一楼层中几十个独立系统所组成的一个小型网络。或者，您可能需要设置一个网络，该网络由分布在多个建筑中的 1,000 多个系统组成。此设置要求您进一步将网络划分为多个称为子网的分区。

必须制定一些与硬件相关的规划决策，这包括：

- 网络硬件的网络拓扑、布局以及连接
- 网络可以支持的主机系统（包括服务器上可能需要的虚拟系统）的类型和数量

- 要安装在这些系统中的网络设备
  - 要使用的网络介质类型，如以太网等
  - 使用网桥、路由器和防火墙扩展网络介质或将本地网络连接到外部网络
- 有关网桥工作原理的信息，请参见《[在 Oracle Solaris 11.2 中管理网络数据链路](#)》中的“[桥接网络概述](#)”。
- 有关路由器如何运作的说明，请参见“[为网络规划路由器](#)” [12]。
- 有关防火墙的信息，请参见《[在 Oracle Solaris 11.2 中确保网络安全](#)》中的第 4 章“[关于 Oracle Solaris 中的 IP 过滤器](#)”。

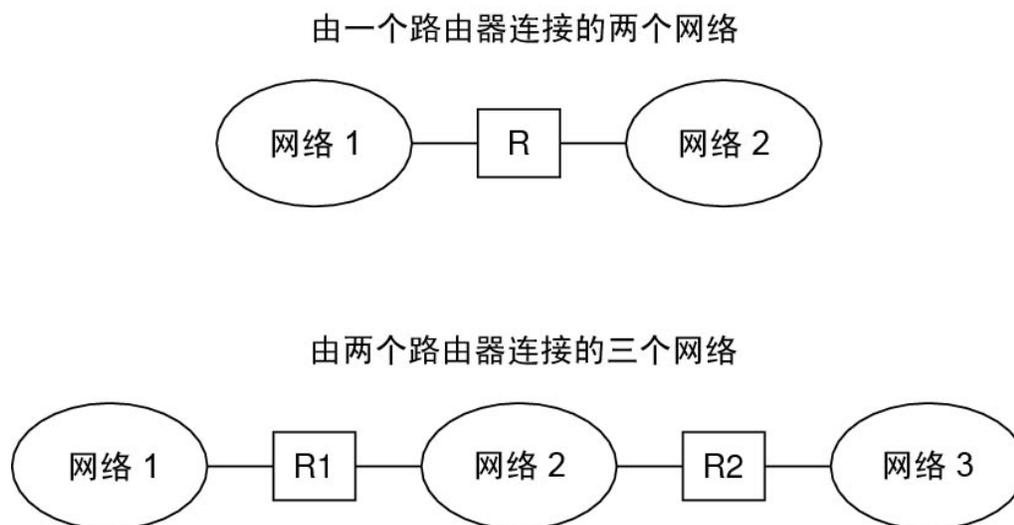
## 网络拓扑概述

网络拓扑描述了网络如何结合在一起。路由器是指将网络相互连接的实体。路由器是指任何一台具有两个或更多网络接口并实现 IP 转发的计算机。但是，系统必须进行正确配置之后才能作为路由器运行，如《[将 Oracle Solaris 11.2 系统配置为路由器或负载均衡器](#)》中的第 2 章“[将系统配置为路由器](#)”中所述。

路由器可连接两个或更多网络以形成更大的互连网络。必须配置路由器，使其能在两个相邻网络间传送包。通过将包转发到与相邻网络连接的其他路由器，路由器还应该可以将包传送到相邻网络以外的网络。

下图显示了网络拓扑的基本部分。本图的上面部分显示由单个路由器连接的两个网络的简单配置。本图的下面部分显示由两个路由器互连的三个网络的配置。在第一个示例中，路由器 R 将网络 1 和网络 2 连接成一个大互连网络。在第二个示例中，路由器 R1 连接网络 1 和 2。路由器 R2 连接网络 2 和 3。这些连接形成了一个包括网络 1、2 和 3 的网络。

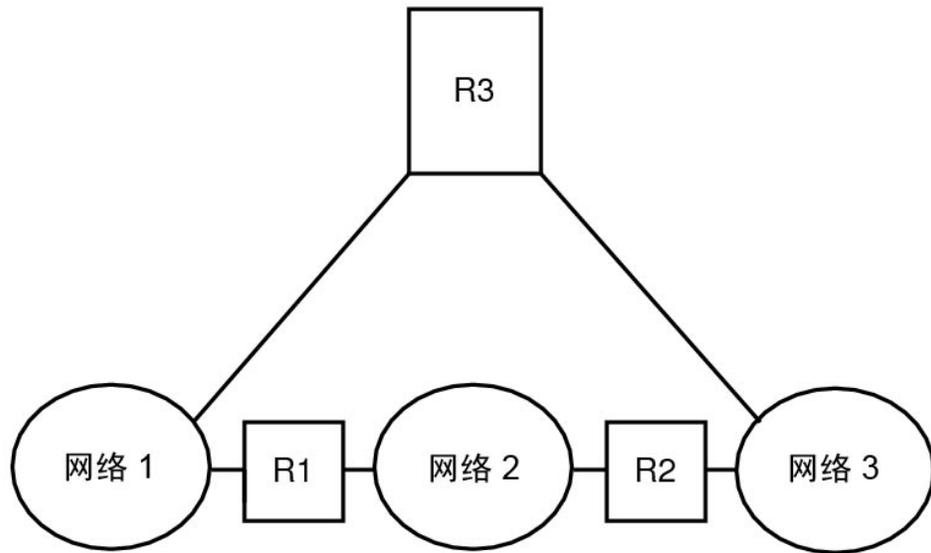
图 1-1 基本网络拓扑



除了将网络连接成互连网络之外，路由器还会在基于目标网络地址的网络间路由包。随着互连网络的日益复杂，每个路由器制定的有关包目标地址的决定也越来越多。

下图显示了较复杂的情况。路由器 R3 直接连接网络 1 和 3。冗余性提高了可靠性。如果网络 2 关闭，则路由器 R3 仍会在网络 1 和 3 之间提供路由。您可以互连许多网络。但是，这些网络必须使用相同的网络协议。

图 1-2 在网络间提供其他路径的网络拓扑



[“为网络规划路由器” \[12\]](#)中对路由器进行了更详细的论述。

## 在网络上使用子网

使用子网与需要进行管理细分以解决大小和控制问题有关。网络中包含的主机和服务器越多，管理任务就会越复杂。通过创建管理分区和使用子网，管理复杂网络变得更容易。

有关为网络设置管理分区的决定由以下因素确定：

- 网络大小  
即使是在规模相对较小的网络（其分区位于广泛的地理区域）中，子网也是很有用的。
- 用户组共有的公共需求

例如，您的网络可能局限在一栋建筑物内，支持相对较少的计算机。这些计算机划分在多个子网中。每个子网都支持有不同需求的用户组。在本示例中，您可能需要针对每个子网使用一个管理分区。

- 安全性

您可能需要将关键任务服务器、桌面系统和面向 Internet 的 Web 服务器分离到不同的子网中，可以在这些子网之间建立防火墙。

## IPv4 自治系统拓扑

具有多个路由器和网络的站点通常将其网络拓扑作为单个路由域或自治系统 (autonomous system, AS) 进行管理。图 1-3 “具有多个 IPv4 路由器的自治系统” 展示了一个 AS，它分成了三个本地网络：10.0.5.0、172.20.1.0 和 192.168.5.0。

该网络由以下类型的系统组成：

- 路由器

路由器使用路由协议管理网络包如何从其源定向或路由至本地网络中的目标，或者定向或路由至外部网络。有关 Oracle Solaris 中支持的路由协议的信息以及将系统配置为路由器的说明，请参见《将 Oracle Solaris 11.2 系统配置为路由器或负载均衡器》中的“路由协议”。

路由器类型包括以下各项：

- 边界路由器 – 用于将本地网络（如 10.0.5.0）以外部方式连接到服务提供商。
- 缺省路由器 – 用于管理本地网络中的包路由，本地网络本身可能包含多个本地网络。例如，在图 1-3 “具有多个 IPv4 路由器的自治系统” 中，路由器 1 充当 192.168.5 的缺省路由器。同时，路由器 1 还连接到 10.0.5.0 内部网络。路由器 2 的接口连接到 10.0.5.0 和 172.20.1.0 内部网络。
- 包转发路由器 – 用于转发内部网络之间的包，但不运行路由协议。在图 1-3 “具有多个 IPv4 路由器的自治系统” 中，路由器 3 是一个包转发路由器，具有到 172.20.1 和 192.168.5 网络的连接。

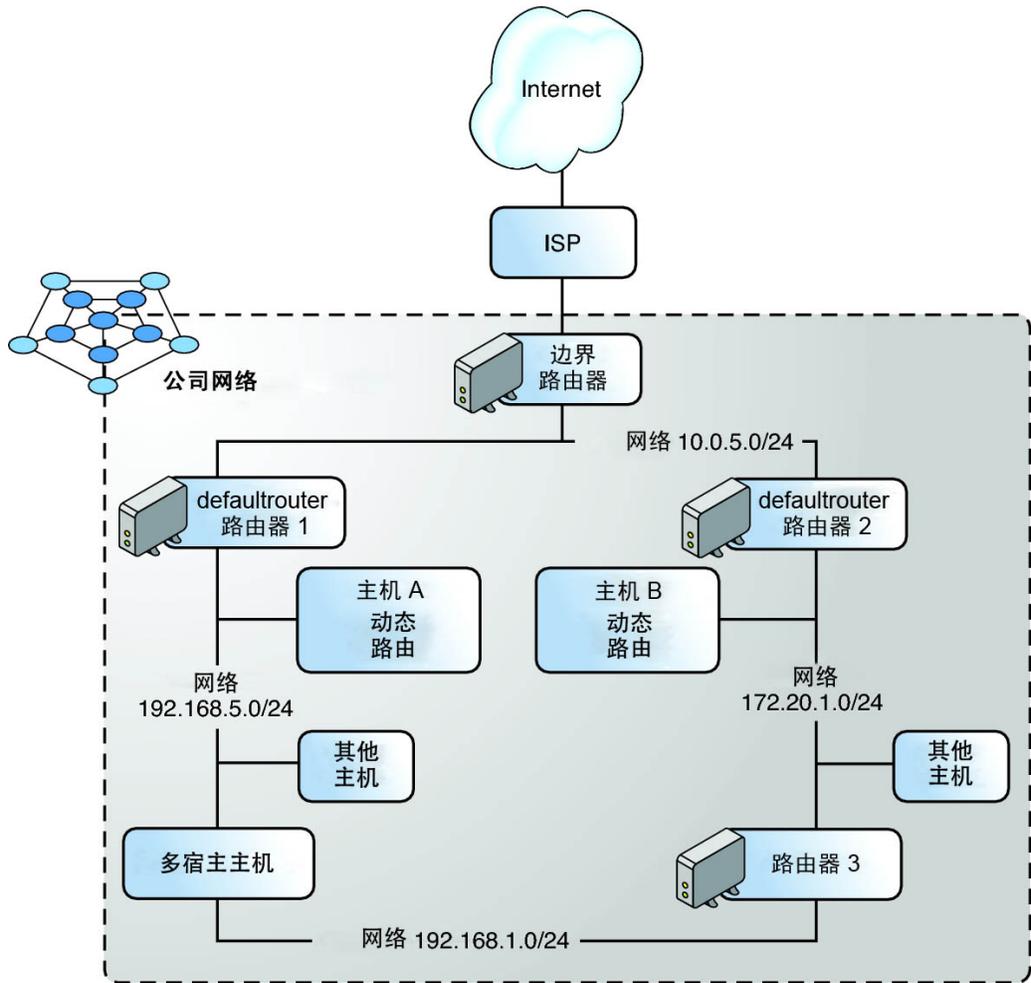
- 客户机系统

- 多宿主系统或具有多个 NIC 的系统。在 Oracle Solaris 中，这些系统缺省情况下可以将包转发到同一网络段中的其他系统。
- 单接口系统依赖于本地路由器进行包转发和接收配置信息。

有关与任务相关的信息，请参见《在 Oracle Solaris 11.2 中配置和管理网络组件》中的第 3 章“在 Oracle Solaris 中配置和管理 IP 接口和地址”。

配置其他网络组件时使用下图作为参考。

图 1-3 具有多个 IPv4 路由器的自治系统



## 为网络规划路由器

回顾使用 TCP/IP 的情形，网络中有两种类型的实体：主机和路由器。所有网络都必须包含主机，不过并非所有网络都需要路由器。网络的物理拓扑可确定是否需要路由器。本节介绍了网络拓扑和路由的概念。在决定将其他网络添加到现有网络环境中时，这些概念非常重要。

注 - 有关在 IPv4 和 IPv6 网络中配置路由器的全部详细信息和任务，请参见《将 Oracle Solaris 11.2 系统配置为路由器或负载均衡器》中的第 2 章“将系统配置为路由器”。

## 路由器如何传送包

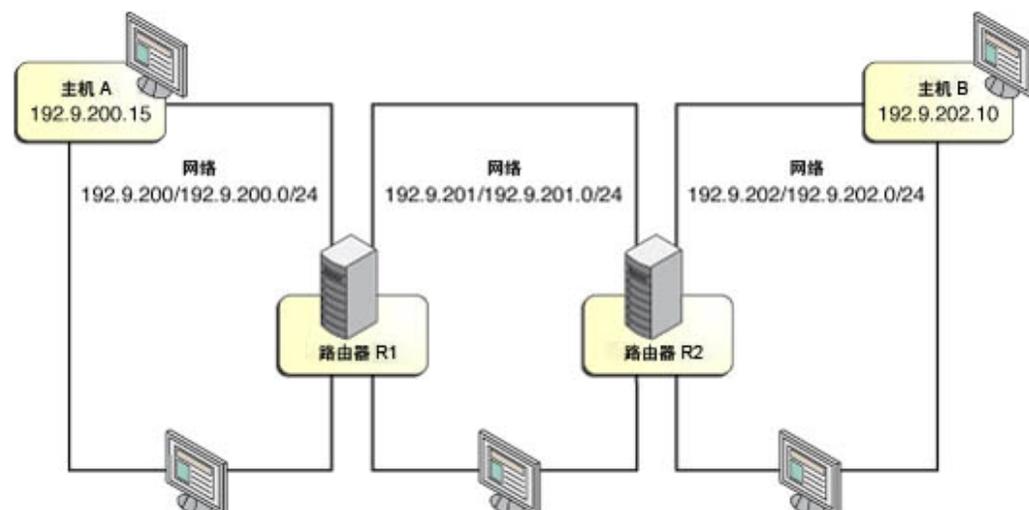
路由器以下面的方式传送包：

- IP 网络上的所有节点维护路由表中的路由信息。这些表包含有关如何访问与本地和远程网络连接的系统的信息。路由表是从本地配置信息以及与相邻系统交换的路由协议消息生成的。
- 主机系统最初发送包时，它在自己的路由表中查找包的目标地址，以便确定该目标是否位于本地网络上。如果是，该包直接转至具有该 IP 地址的主机。如果不是，该包转至本地网络上的路由器。
- 路由器收到包时会检查其路由表，以确定目标地址是否属于与它相连的一个网络上的系统，或者确定是否必须通过其他路由器来转发该消息。然后，它会将该消息发送到目标的路径中的下一个系统。
- 此过程将在收到该消息的每个路由器上重复，直到该消息到达目标系统。

请参阅《将 Oracle Solaris 11.2 系统配置为路由器或负载均衡器》中的第 2 章“将系统配置为路由器”。

下图中显示了由两个路由器连接的三个网络的网络拓扑。

图 1-4 具有三个互连网络的网络拓扑



路由器 R1 连接网络 192.9.200.0/24 和 192.9.201.0/24。路由器 R2 连接网络 192.9.201.0/24 和 192.9.202.0/24。

如果网络 192.9.200.0/24 中的主机 A 向网络 192.9.202 中的主机 B 发送消息，则会发生以下事件：

1. 主机 A 在其路由表中检查指向 192.9.202.10 的路径。本地网络地址范围不包括此地址，但是存在先前通过包括该地址的路由器 R1 获悉的缺省路由。因此，主机 A 将包发送到路由器 R1。
2. 路由器 R1 检查其路由表。任何本地网络的地址范围均不包括该目标地址，但是存在通过包括该地址的路由器 R2 到网络 192.9.202.0/24 的已知路由，路由器 R1 将包发送到路由器 R2。
3. 路由器 R2 直接连接到网络 192.9.202.0/24。在执行路由表查找之后显示 192.9.202.10 位于所连接的网络上。路由器 R2 直接将包发送到主机 B。

## 确定网络的 IP 地址寻址格式

当您规划网络寻址方案时，请考虑以下因素：

- 要使用的 IP 地址类型：IPv4 或 IPv6
- 网络中可能有的系统的数量
- 多宿主系统或路由器的数量，这些需要多个网络接口卡 (network interface card, NIC)，每个网络接口卡具有单独的 IP 地址
- 是否在网络中使用专用地址
- 是否拥有一个用来管理 IP 地址池的 DHCP 服务器

## IPv4 地址

这是 TCP/IP 网络上使用的原始地址格式。IPv4 地址的长度为 32 位。IPv4 地址最初分配给 A 类连续地址块（包含 16777216 个地址）、B 类连续地址块（包含 65536 个地址）或 C 类连续地址块（包含 256 个地址）中的各个组织。请求地址块的每个组织会收到固定地址前缀和隐含的前缀掩码，它们都以点分十进制表示法来指定。例如，Internet 编号分配机构 (Internet Assigned Numbers Authority, IANA) 将 A 类地址块 156.0.0.0 网络掩码 255.0.0.0 分配给了美国 Internet 编号注册机构 (American Registry for Internet Numbers, ARIN)。第一个字节等于 156 的所有地址都位于此地址块内。ARIN 将其 A 类地址块中的 B 类地址块 156.151.0.0 网络掩码 255.255.0.0 通过子分配操作分配给 Sun Microsystems（现在为 Oracle）。

随后，Internet 工程任务组 (Internet Engineering Task Force, IETF) 开发了无类域间路由 (Classless Inter-Domain Routing, CIDR) 地址，作为解决 IPv4 地址缺乏和全局 Internet 路由表容量受限的临时补救方法。在最满足组织要求的位边界上细分 CIDR 地

址分配。地址块按如下形式指定：先是点分十进制 IPv4 地址，后跟一条斜杠和以位为单位的地址前缀长度。

有关更多信息，请参阅以下资源：

- [Internet Protocol DARPA Internet Program Protocol Specification \(http://tools.ietf.org/html/rfc791\)](http://tools.ietf.org/html/rfc791) (Internet 协议 DARPA Internet 程序协议规范)
- [Classless Inter-domain Routing \(CIDR\): The Internet Address Assignment and Aggregation Plan \(http://tools.ietf.org/html/rfc4632\)](http://tools.ietf.org/html/rfc4632) (无类域间路由 (Classless Inter-domain Routing, CIDR) : Internet 址分配和聚合计划)

下表提供了 CIDR 表示法和点分十进制格式的子网长度规范示例，以及可能位于具有该前缀长度的网络上的主机总数。

表 1-1 CIDR 前缀及其等效的十进制值

CIDR 网络前缀长度	相应的点分十进制子网掩码	可用 IP 地址
/19	255.255.224.0	8,192
/20	255.255.240.0	4,096
/21	255.255.248.0	2,048
/22	255.255.252.0	1,024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32

## 专用地址

IANA 已保留了 IPv4 地址块。这些专用地址用于专用网络中的网络通信流量。从其 Internet 服务提供商请求 IPv4 地址块的组织不可能收到足够的分配，因此其每个系统无法具有唯一地址。组织通常向其内部网络上的系统分配专用地址。其系统可以使用网络地址转换器 (Network Address Translator, NAT) 以及使用应用程序代理服务器与 Internet 上的其他站点通信，从而有效共享 Internet 服务器提供商 (Internet Service Provider, ISP) 提供的有限地址。

下表列出了 IPv4 专用地址的范围及其相应的掩码。

网络前缀/长度	IPv4 地址范围
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/125	172.16.0.0 - 172.31.255.25
192.168.0.0/16	192.168.0.0 - 192.168.255.255

## DHCP 地址

通过动态主机配置协议 (Dynamic Host Configuration Protocol, DHCP), 系统可在引导过程中从 DHCP 服务器接收配置信息 (包括 IP 地址)。DHCP 服务器维护 IP 地址池, 通过该地址池可为 DHCP 客户机指定地址。使用 DHCP 的站点所用的 IP 地址池可以小于为所有客户机指定永久性 IP 地址时所需的 IP 地址数, 前提是这些客户机不连续连接。在这种情况下, 您可以在客户机之间共享地址, 从而减少所需的 IP 地址总数。但是, 如果您没有足够的客户机往来, 您最终将需要相同数量的 IP 地址。使用 DHCP 地址更普遍的优势是您无需执行与单个主机一样多的配置, 因为您使用配置详细信息设置 DHCP 服务器。这样, 主机将需要极少手动配置, 甚至不需要手动配置。您可以设置 DHCP 服务来管理站点的 IP 地址或部分地址。有关更多信息, 请参阅《[在 Oracle Solaris 11.2 中使用 DHCP](#)》。

## IPv6 地址

这些 128 位 IPv6 地址提供的地址空间大于 IPv4 可提供的地址空间。IPv6 地址显示为八组, 每组包含四个十六进制数字, 各组之间用冒号隔开。可以隐藏每组中的前导零。如果一个或多个连续组中都是零, 可以由双冒号替换, 如以下示例中所示:

```
2001:db8:2f32:27:214:4fff:fe4a:9926
```

与 CIDR 格式的 IPv4 地址一样, IPv6 地址是无类的并使用前缀来指定用于定义站点网络的地址部分, 如以下示例中所示:

```
2001:db8:2f32::/48
```

有关 IPv6 寻址的详细信息, 请参见 [IP Version 6 Addressing Architecture \(http://tools.ietf.org/html/rfc4291\)](http://tools.ietf.org/html/rfc4291) (IP 版本 6 寻址体系结构)。

## 文档前缀

对于 IPv6 地址, 前缀 2001:db8::/32 是专用于文档示例的特殊 IPv6 前缀。本书中的示例使用专用 IPv4 地址和保留的 IPv6 文档前缀。

## 获取网络的 IP 号

IPv4 网络通过 IPv4 网络号加上网络的掩码或网络掩码的组合来定义。IPv6 网络通过其站点前缀定义; 如果使用子网, 则通过其子网前缀定义。

要使用网络能够与 Internet 中的外部网络通信, 必须从相应的组织为网络获取一个已注册的 IP 号。此地址会成为 IPv4 寻址方案的网络号或 IPv6 寻址方案的站点前缀。

ISP 可为网络提供 IP 地址，其定价基于不同的服务级别。了解各个 ISP 可确定哪一个提供商可提供最好的网络服务。ISP 通常向企业提供动态分配的地址或静态 IP 地址。某些 ISP 同时提供 IPv4 和 IPv6 地址。

如果您的站点是一个 ISP，则可通过您语言环境的 Internet 注册机构 (Internet Registry, IR) 获取用户的 IP 地址块。IANA 最终负责将注册的 IP 地址授予世界各地的 IR。每个 IR 都拥有由其提供服务的语言环境的注册信息和模板。有关 IANA 及其 IR 的信息，请参阅 [IANA 的 IP 地址服务页面 \(http://www.iana.org/ipaddress/ip-addresses.htm\)](http://www.iana.org/ipaddress/ip-addresses.htm)。

## 在网络上使用命名实体

TCP/IP 协议使用系统的 IP 地址在网络中查找系统。但是，与 IP 地址相比，主机名使您可以更容易标识系统。

从 TCP/IP 角度来说，网络是一组命名的实体。主机是具有名称的实体，路由器是具有名称的实体，网络也是具有名称的实体。也可以为安装有网络的组或部门指定名称，这与可为部门、区域或公司指定名称一样。理论上，可用于标识网络的名称分层结构实际没有限制。

## 域名

许多网络会将其主机和路由器组织为管理域的分层结构。如果使用网络信息服务 (Network Information Service, NIS) 或域名系统 (Domain Name System, DNS) 命名服务，则必须为组织选择一个全球唯一的域名。要确保域名是唯一的，应向 *InterNIC* 注册此域名。如果您计划允许 Internet 上的其他站点通过 DNS 定位您的系统，则需要唯一域名。

位于另一个域下的域名通常称为子域。域名结构是分层的。新域通常位于现有的相关域的下方。例如，分公司的域名可位于父公司域名的下方。如果域名没有其他关系，则组织可以直接将其域名放置在某一个现有顶级域的下方，例如 .com、.org、.edu、.gov 等。

## 选择命名服务和目录服务

在 Oracle Solaris 中，您可以从以下三种类型的命名服务中进行选择：本地文件、NIS 和 DNS。命名服务维护有关网络中的计算机的重要信息，例如主机名、IP 地址等。除命名服务以外，您也可以使用 LDAP 目录服务来代替命名服务。LDAP 是用来访问目录服务器以使用分布式命名和其他目录服务的安全网络协议。该基于标准的协议支持一个分层次的数据库结构。在 UNIX 和多平台环境中都可以使用同一协议来提供命名服务。有关 Oracle Solaris 中的命名服务的介绍，请参阅《[使用 Oracle Solaris 11.2 目录和命名服务：DNS 和 NIS](#)》中的第 1 章“关于命名和目录服务”。

网络数据库的配置非常关键。因此，需要在网络规划期间确定要使用的命名或目录服务。此外，决定是否使用命名服务还会影响是否将网络组织为管理域。

对于命名或目录服务，可以从以下各项中选择：

- NIS 或 DNS – NIS 和 DNS 命名服务维持网络中多个服务器上的网络数据库。《[使用 Oracle Solaris 11.2 目录和命名服务：DNS 和 NIS](#)》介绍了这些命名服务并说明了如何配置数据库。此外，该指南还详细说明了名称空间和管理域的概念。
- LDAP – 除命名服务以外，您也可以使用 LDAP 目录服务来代替命名服务。LDAP 是用来访问目录服务器以使用分布式命名和其他目录服务的安全网络协议。
- 本地文件 – 如果您未实现 NIS、DNS 或 LDAP，网络将使用本地文件提供命名服务。“本地文件”一词是指 /etc 目录中由网络数据库使用的一系列文件。除非另行指明，否则，本书中的过程将假定您使用本地文件作为命名服务。

---

注 - 如果决定使用本地文件作为网络的命名服务，则以后可以设置其他命名服务。

---

## 管理主机名

为构成网络的系统规划命名方案。网络上的每台计算机应该具有与其主网络接口上的 IP 地址对应的 TCP/IP 主机名。主机名在系统的子域内必须唯一。就像物理计算机一样，虚拟系统也应该具有唯一 IP 地址和主机名。

系统可以具有以下内容：

- 映射到系统 IP 地址的多个主机名。例如，`systema.mycompany.com` 也称为 `www.mycompany.com`。
- 对于 IPv4 和 IPv6 地址相同的主机名。
- 在某个期间配置有相同主机名的新 IP 地址和旧的过时 IP 地址，以支持网络重新编号。
- 不同子网上的多个网络接口，每个具有唯一 IP 地址和主机名。

规划网络时，请创建一个包含 IP 地址及其关联的主机名的列表，以便在设置过程中轻松访问它们。此列表可以帮助检验所有主机名是否唯一。

---

注 - 主接口的 TCP/IP 主机名是一个与系统主机名不同的实体，后者是使用 `hostname` 命令设置的。虽然 Oracle Solaris 并不要求对这两者使用相同的名称，不过这是通常的做法。某些网络应用程序依赖于这一约定。有关更多信息，请参见 [hostname\(1\)](#) 手册页。

---

## 规划 IPv6 地址的使用

---

本章是第 1 章 [规划网络部署](#) 的补充，介绍了决定在网络上使用 IPv6 地址时，需要考虑的其他注意事项。

如果除了使用 IPv4 地址外，还计划使用 IPv6 地址，请确保当前的 ISP 支持这两种地址类型

有关 IPv6 概念的介绍，请参阅 [Internet Protocol, Version 6 \(IPv6\) Specification \(http://www.ietf.org/rfc/rfc2460.txt\)](http://www.ietf.org/rfc/rfc2460.txt) (Internet 协议版本 6 (IPv6) 规范)。

对于 IPv6 配置任务，请参见《[在 Oracle Solaris 11.2 中配置和管理网络组件](#)》中的“[配置 IPv6 接口](#)”。

有关 IPv6 网络故障排除的信息，请参见《[在 Oracle Solaris 11.2 中排除网络管理问题](#)》中的“[排除 IPv6 部署问题](#)”。

本章包含以下主题：

- “[IPv6 规划任务](#)” [19]
- “[IPv6 网络拓扑概述](#)” [20]
- “[确保硬件支持 IPv6](#)” [22]
- “[准备 IPv6 寻址计划](#)” [22]
- “[配置网络服务以支持 IPv6](#)” [24]
- “[网络中使用隧道的规划](#)” [26]
- “[IPv6 实现的安全注意事项](#)” [26]

### IPv6 规划任务

下表介绍了计划在网络上实现 IPv6 时需要考虑的各种事项。如果您正从现有 IPv4 网络迁移到 IPv6 网络，请参见《[在 Oracle Solaris 11.2 中配置和管理网络组件](#)》中的“[从 IPv4 网络迁移到 IPv6 网络](#)”了解其他说明。

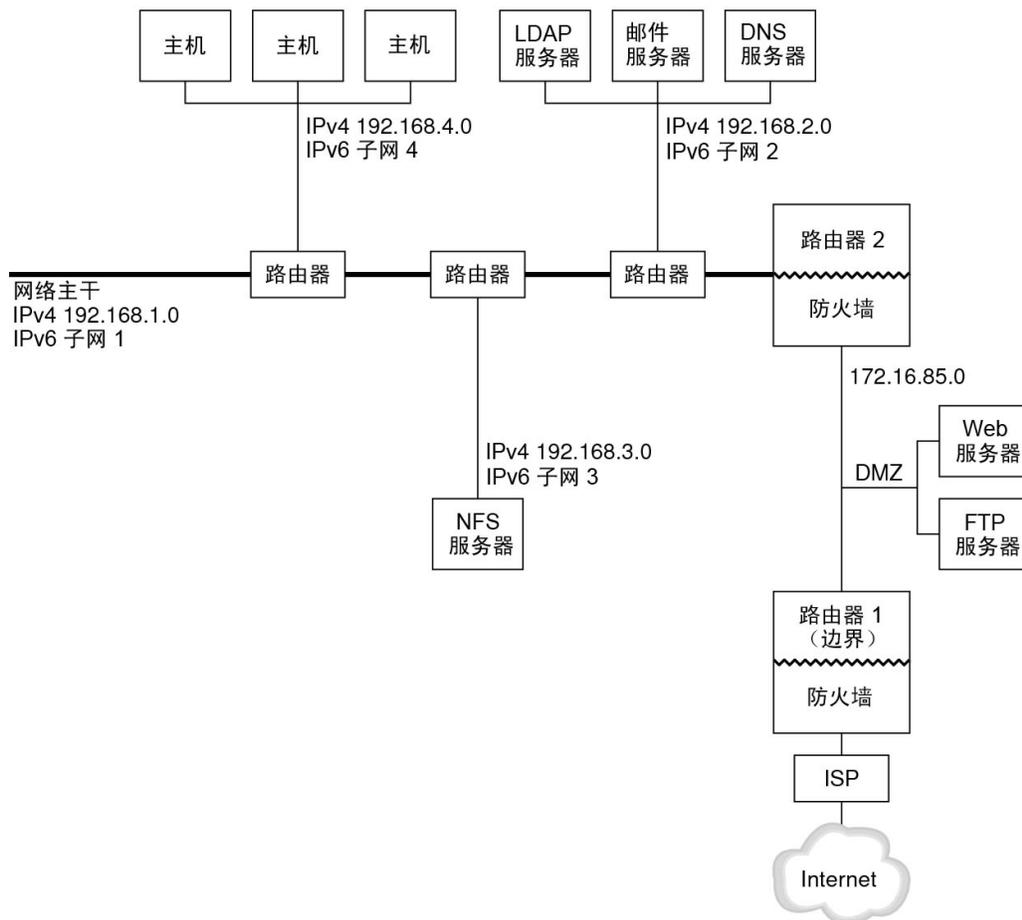
任务	说明	参考
准备硬件以支持 IPv6。	确保硬件可以升级到 IPv6。	<a href="#">“确保硬件支持 IPv6” [22]</a>

任务	说明	参考
确保应用程序能够支持 IPv6。	验证应用程序是否可以在 IPv6 环境中运行。	<a href="#">“配置网络服务以支持 IPv6” [24]</a>
制定隧道使用计划。	确定应当使用哪些路由器来建立与其他子网或外部网络连接的隧道。	<a href="#">“网络中使用隧道的规划” [26]</a>
计划如何保证网络安全并制定 IPv6 安全策略。	出于安全方面的考虑，在配置 IPv6 之前，需要为 DMZ 及其实体制定寻址计划。  决定实现安全的方式，例如使用此发行版的 IP 过滤器、IP 安全体系结构 (IPsec)、Internet 密钥交换 (Internet Key Exchange, IKE) 和其他安全功能。	<a href="#">“IPv6 实现的安全注意事项” [26]</a>  <a href="#">《在 Oracle Solaris 11.2 中确保网络安全》</a>
为网络上的系统制定寻址计划。	在配置 IPv6 之前，应当先制定好服务器、路由器和主机的寻址计划。此步骤包括获取网络的站点前缀以及规划 IPv6 子网（如果需要）。	<a href="#">“为节点制定 IPv6 寻址计划” [23]</a>

## IPv6 网络拓扑概述

通常，IPv6 用于也使用 IPv4 的混合网络拓扑中，如下图所示。下图用作本章中说明 IPv6 配置任务的参考。

图 2-1 IPv6 网络拓扑方案



图中所示的企业网络方案由五个具有现有 IPv4 地址的子网组成。网络的链路直接对应于管理子网。四个内部网络以 RFC 1918 样式的专用 IPv4 地址表示，这是在缺少 IPv4 地址时的常见解决方案。

这些内部网络使用以下地址方案：

- 子网 1 是内部网络主干 192.168.1。
- 子网 2 是具有 LDAP、sendmail 和 DNS 服务器的内部网络 192.168.2。
- 子网 3 是具有企业 NFS 服务器的内部网络 192.168.3。
- 子网 4 是包含企业员工主机的内部网络 192.168.4。

外部的公共网络 172.16.85 充当企业的 DMZ（隔离区）。此网络中包含 Web 服务器、匿名 FTP 服务器以及企业为外界提供的其他资源。路由器 2 使用防火墙并将公共网络 172.16.85 与内部主干分开。在隔离区 (Demilitarized Zone, DMZ) 的另一端，路由器 1 使用防火墙并充当企业的边界服务器。

在图 2-1 “IPv6 网络拓扑方案”中，公共 DMZ 具有 RFC 1918 专用地址 172.16.85。在实际应用中，公共 DMZ 必须具有已注册的 IPv4 地址。大多数 IPv4 站点都使用公共地址和 RFC 1918 专用地址的组合。但是，在引入 IPv6 时，公共地址和专用地址的概念发生了变化。因为 IPv6 具有大得多的地址空间，所以，可以将公共 IPv6 地址同时用于专用网络和公共网络。

Oracle Solaris 双协议栈支持同时执行 IPv4 操作和 IPv6 操作。在您的网络上部署 IPv6 期间及之后，您可以成功运行与 IPv4 相关的操作。在已使用 IPv4 的操作网络上部署 IPv6 时，请确保不要中断正在进行的操作。

## 确保硬件支持 IPv6

可以就下列类别的硬件，查阅制造商的文档，确定是否已经针对 IPv6 做好准备：

- 路由器
- 防火墙
- 服务器
- 交换机

---

注 - 本书中的所有过程都假定您的设备（尤其是路由器）可以升级到 IPv6。但是，某些型号的路由器无法升级到 IPv6。有关更多信息和解决方法，请参阅《在 Oracle Solaris 11.2 中排除网络管理问题》中的“无法将 IPv4 路由器升级到 IPv6”。

---

## 准备 IPv6 寻址计划

从 IPv4 到 IPv6 的主要部分转换包括制定寻址计划，其中包括以下准备工作：

- “获取站点前缀” [23]
- “制定 IPv6 编号方案” [23]

对于实际迁移任务，请参见《在 Oracle Solaris 11.2 中配置和管理网络组件》中的“从 IPv4 网络迁移到 IPv6 网络”。

## 获取站点前缀

在配置 IPv6 之前，必须获取站点前缀。站点前缀用于派生 IPv6 实现中所有节点的 IPv6 地址。

支持 IPv6 的任何 ISP 都可以为贵工作单位提供 48 位 IPv6 站点前缀。如果当前的 ISP 仅支持 IPv4，则可以使用另一个 ISP 来支持 IPv6，同时保留当前的 ISP 来支持 IPv4。在这种情况下，您可以使用多种解决方法之一。有关更多信息，请参见《在 Oracle Solaris 11.2 中排除网络管理问题》中的“当前的 ISP 不支持 IPv6”。

如果贵组织是 ISP，则可以从相应的 Internet 注册机构获取客户的站点前缀。有关更多信息，请参见 [Internet Assigned Numbers Authority \(IANA\) \(http://www.iana.org\)](http://www.iana.org) (Internet 编号分配机构)。

## 制定 IPv6 编号方案

除非建议的 IPv6 网络是全新的网络，否则请将现有的 IPv4 拓扑用作 IPv6 编号方案的基础。

## 为节点制定 IPv6 寻址计划

对于大多数主机，采用无状态自动配置为其接口配置 IPv6 地址是恰当的省时策略。当主机从离其最近的路由器接收到站点前缀时，相邻节点搜索会自动为主机上的每个接口生成 IPv6 地址。

服务器需要具有稳定的 IPv6 地址。如果您未手动配置服务器的 IPv6 地址，那么，更换服务器上的 NIC 卡时，系统会自动配置一个新的 IPv6 地址。

在为服务器创建地址时，请记住以下提示：

- 为服务器提供有意义的稳定接口 ID。一个策略就是针对接口 ID 使用连续编号方案。例如，图 2-1 “IPv6 网络拓扑方案”中 LDAP 服务器的内部接口可能会变为 2001:db8:3c4d:2::2。
- 或者，如果您不定期为 IPv4 网络重新编号，请考虑使用路由器和服务器现有的 IPv4 地址作为其接口 ID。在图 2-1 “IPv6 网络拓扑方案”中，假定路由器 1 的 DMZ 接口具有 IPv4 地址 192.168/16。可以将 IPv4 地址转换为十六进制地址，并将结果用作接口 ID。新的接口 ID 将为 ::7bc8:156F。

只有当您拥有已注册的 IPv4 地址（而不是从 ISP 获取的地址）时，才使用此方法。如果使用由 ISP 提供给您的 IPv4 地址，则会产生依赖性，而这在更换 ISP 时会造成问题。

由于可用的 IPv4 地址的数量有限，因此，在过去，网络设计者必须考虑在何处使用全局已注册地址和专用 RFC 1918 地址。但是，全局和专用 IPv4 地址的概念并不适用于

IPv6 地址。可以在网络的所有链路（包括公共 DMZ）上使用全局单播地址（包括站点前缀）。

## 为子网制定编号方案

在制定编号方案时，应首先将现有的 IPv4 子网映射到等效的 IPv6 子网。例如，请考虑图 2-1 “IPv6 网络拓扑方案”中所示的子网。子网 1–4 除了用数字 1–4 来指示子网以外，还使用所指定的 RFC 1918 IPv4 专用地址作为其地址的前 16 位。为了进行说明，假定已将 IPv6 前缀 2001:db8:3c4d/48 指定给该站点。

下表说明了如何将专用的 IPv4 前缀映射到 IPv6 前缀。

IPv4 子网前缀	等效的 IPv6 子网前缀
192.168.1.0/24	2001:db8:3c4d:1::/64
192.168.2.0/24	2001:db8:3c4d:2::/64
192.168.3.0/24	2001:db8:3c4d:3::/64
192.168.4.0/24	2001:db8:3c4d:4::/64

## 配置网络服务以支持 IPv6

下列典型的 IPv4 网络服务还可以支持 IPv6：

- DNS
- HTTP（Apache 2 发行版或 Orion）
- LDAP
- NFS
- sendmail

IMAP（Internet 消息访问协议）邮件服务仅适用于 IPv4。

针对 IPv6 配置的节点可以运行 IPv4 服务。在打开 IPv6 时，并非所有的服务都能够接受 IPv6 连接。已经移植到 IPv6 的服务将能够接受连接。尚未移植到 IPv6 的服务将继续使用协议栈的 IPv4 部分。

在将服务升级到 IPv6 之后，可能会出现一些问题。有关详细信息，请参见《在 Oracle Solaris 11.2 中排除网络管理问题》中的“将服务升级到支持 IPv6 时遇到问题”。

### ▼ 如何准备网络服务以支持 IPv6

1. 更新以下网络服务以支持 IPv6：

- 邮件服务器
- NIS 服务器
- NFS

---

注 - LDAP 无需执行特定于 IPv6 的配置任务即可支持 IPv6。

---

2. 检验防火墙硬件是否能够支持 IPv6。  
有关说明，请参阅与防火墙有关的文档。
3. 检验网络上的其他服务是否已移植到 IPv6。  
有关更多信息，请参阅软件的营销宣传材料和相关文档。
4. 如果您的站点部署了下列服务，请确保已经针对这些服务采取了相应的措施：
  - 防火墙 - 考虑增强用于 IPv4 的策略来支持 IPv6。有关更多的安全注意事项，请参见[“IPv6 实现的安全注意事项” \[26\]](#)。
  - 邮件 - 在 DNS 的邮件交换器记录 (mail exchanger record, MX record) 中，考虑添加您的邮件服务器的 IPv6 地址。
  - DNS - 有关 DNS 特定的注意事项，请参见[如何准备 DNS 以支持 IPv6 \[25\]](#)。
  - IPQoS - 在主机上使用先前用于 IPv4 的同一 *Diffserv* 策略。
5. 在将某个节点转换为支持 IPv6 以前，审计由该节点提供的任何网络服务。

## ▼ 如何准备 DNS 以支持 IPv6

Oracle Solaris 在客户端和服务端均支持 DNS 解析。要使 DNS 服务支持 IPv6，请使用以下过程进行准备。

有关 DNS 支持 IPv6 的更多相关信息，请参阅 [《使用 Oracle Solaris 11.2 目录和命名服务：DNS 和 NIS》](#)。

1. 确保执行递归名称解析的 DNS 服务器是双栈 (IPv4 和 IPv6) 服务器或者仅包含 IPv4。
2. 在 DNS 服务器上，使用转发区域中相关的 IPv6 数据库 AAAA 记录填充 DNS 数据库。

---

注 - 需要特别注意那些运行多个关键服务的服务器。确保网络正常工作，还要确保所有的关键服务都已经移植到 IPv6。然后，将服务器的 IPv6 地址添加到 DNS 数据库中。

---

3. 向反向区域中添加与 AAAA 记录相关联的 PTR 记录。

4. 向描述区域的 NS 记录中仅添加 IPv4 数据或者同时添加 IPv6 和 IPv4 数据。

## 网络中使用隧道的规划

在将网络迁移到 IPv4 和 IPv6 的混合网络时，IPv6 实现支持将许多隧道配置作为转换机制。隧道可以使隔离的 IPv6 网络能够进行通信。因为大多数 Internet 都运行 IPv4，所以，来自您的站点的 IPv6 包需要借助于通往目标 IPv6 网络的隧道在 Internet 上传播。

下面是在 IPv6 网络拓扑中使用隧道的一些主要方案：

- 从其购买 IPv6 服务的 ISP 允许您建立一个从您的站点的边界路由器到 ISP 网络的隧道。图 2-1 “IPv6 网络拓扑方案”显示了这样的隧道。在这种情况下，需要建立 IPv6 over IPv4 手动隧道。
- 管理具有 IPv4 连通性的大型分布式网络。要连接使用 IPv6 的分布式站点，可以从每个子网的边界路由器建立 6to4 自动隧道。
- 有时，基础结构中的某个路由器无法升级到 IPv6。在这种情况下，可以建立将两个 IPv6 路由器作为端点且经由 IPv4 路由器的手动隧道。

有关配置隧道的过程，请参阅《在 Oracle Solaris 11.2 中管理 TCP/IP 网络、IPMP 和 IP 隧道》中的第 5 章“管理 IP 隧道”。有关隧道的概念性信息，请参阅《在 Oracle Solaris 11.2 中管理 TCP/IP 网络、IPMP 和 IP 隧道》中的“IP 隧道功能摘要”。

## IPv6 实现的安全注意事项

在现有网络中引入 IPv6 时，必须注意不要危及站点的安全性。

在分阶段实现 IPv6 时，需要注意以下安全问题：

- 对于 IPv6 包和 IPv4 包，需要相同的过滤量。
- 通常，IPv6 包通过防火墙进行隧道传送。  
因此，您应当实现下列任一方案：
  - 让防火墙在隧道内部执行内容检查。
  - 在隧道的另一个端点设置一个具有相似规则的 IPv6 防火墙。
- 在 IPv4 隧道上存在某些使用基于用户数据报协议 (User Datagram Protocol, UDP) 的 IPv6 的转换机制。这些机制能够绕过防火墙，因此被认为可能存在问题。
- IPv6 节点可从企业网络外部进行全局访问。如果安全策略禁止公共访问，则必须为防火墙制定更严格的规则。例如，考虑配置有状态的防火墙。

本书包括有关以下安全功能的信息，这些功能可在 IPv6 实现中使用：

- IP 安全体系结构 (IPsec) 功能允许您为 IPv6 包提供加密保护。有关更多信息，请参阅《在 Oracle Solaris 11.2 中确保网络安全》中的第 6 章“关于 IP 安全体系结构”。
- Internet 密钥交换 (Internet Key Exchange, IKE) 功能自动进行 IPsec 的密钥管理。有关更多信息，请参阅《在 Oracle Solaris 11.2 中确保网络安全》中的第 8 章“关于 Internet 密钥交换”。



# 索引

---

## A

安全注意事项

启用了 IPv6 的网络，26

A、B 和 C 类网络号，14

## B

包

传送

路由器，13

包转发路由器，11

本地文件

选作命名服务，18

边界路由器，11

## C

CIDR 表示法，14

## D

多宿主系统

定义，11

## H

互联网络

冗余和可靠性，9

定义，8

拓扑，8，9

通过路由器传送包，13

## I

IP 地址

CIDR 表示法，14

网络类

网络号管理，14

设计地址方案，14

IPQoS

启用了 IPv6 的网络的策略，25

IPv6

DNS 支持准备，25

安全注意事项，26

寻址计划，23

## L

路由器

传送包，13

包转发路由器，11

添加，12

网络拓扑，8，9

## M

命名服务

选择，17

## N

NIS

选作命名服务，18

## Q

缺省路由器

定义，11

## R

- 任务列表
  - IPv6
    - 规划, 19

## S

- 设计网络
  - IP 寻址方案, 14
  - 命名主机, 18
  - 域名选择, 17
- 隧道
  - 规划, 对于 IPv6, 26

## T

- 拓扑, 8, 9

## W

- 网络管理
  - 主机名, 18
- 网络规划
  - IP 寻址方案, 14
  - 注册网络, 16
  - 添加路由器, 12
- 网络拓扑, 8, 9
  - 自治系统, 12

## Y

- 域名
  - 选择, 17
- 域名系统 (Domain Name System, DNS)
  - 选作命名服务, 18
- 域名系统 (domain name system, DNS)
  - 准备, IPv6 支持, 25

## Z

- 站点前缀, IPv6
  - 如何获取, 23
- 主机

- 主机名
  - 管理, 18
- 注册
  - 网络, 16
- 自治系统 (autonomous system, AS) 见 网络拓扑子网, 10
  - IPv6
    - 编号建议, 24