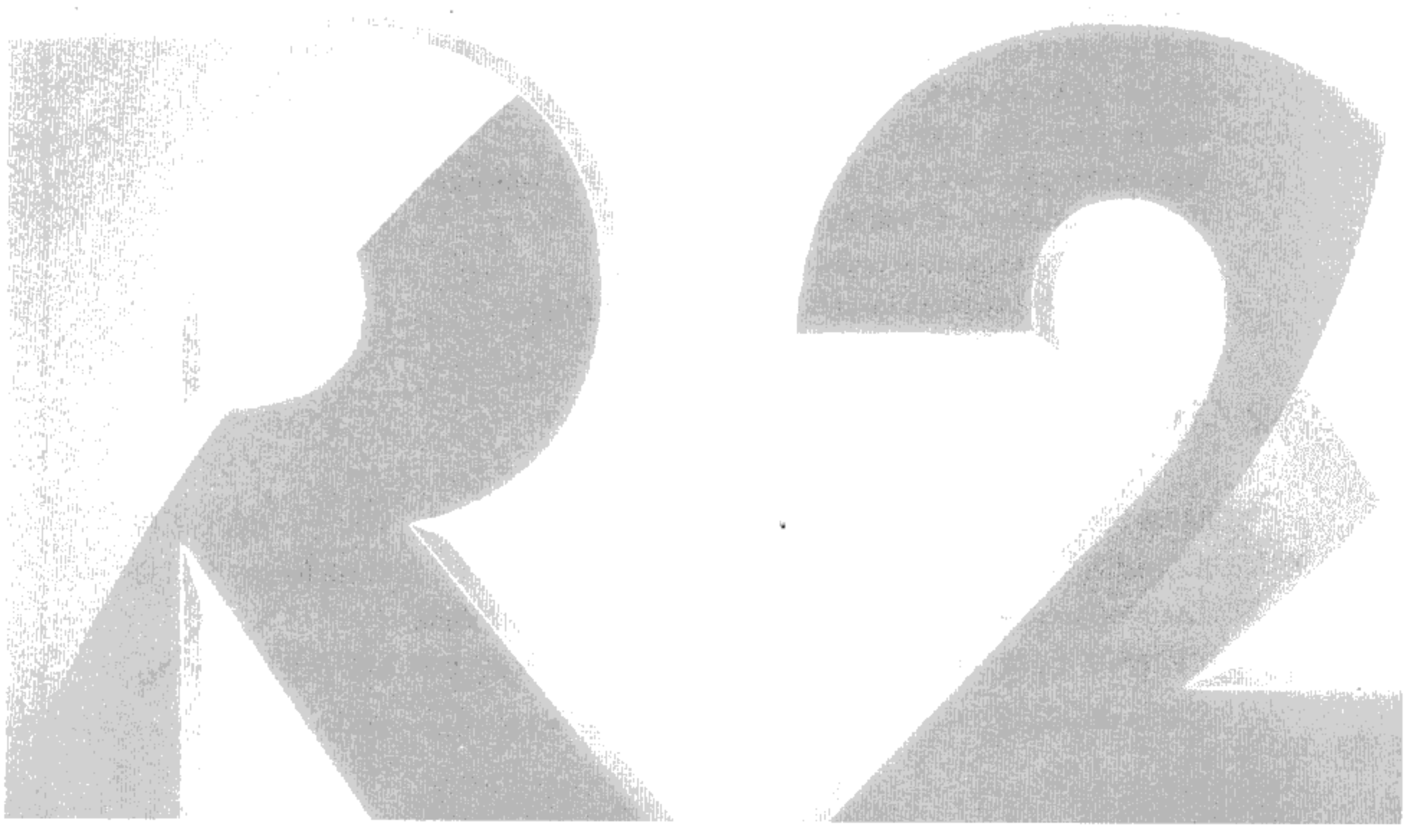
第 1 章

Windows Server 2008 R2基本网络概念

Windows Server 2008 R2提供了各种不同的网络解决方案，企业可以利用它来搭建各种不同的网络环境。本章我们将先简要介绍Windows Server 2008 R2的网络功能，随后我们将介绍在网络环境中不可或缺的TCP/IP协议，包括IPv4与IPv6。

- Windows Server 2008 R2的网络功能
- TCP/IP协议简介
- IPv6基本概念
- Windows Server 2008 R2的管理工具



1-1 Windows Server 2008 R2的网络功能

Windows Server 2008 R2支持多种不同的网络技术与服务，让您更容易地搭建各种不同架构的网络，例如您可以通过它们提供以下的网络环境：

- 企业内部网络（Intranet）：也就是一般公司内部的私有局域网（Local Area Network，LAN）。通过企业内部网络，用户可以将文件、打印机等资源共享给其他网络用户访问。由于因特网的蓬勃发展，因此一般企业内部网络会搭建各种与因特网技术有关的应用程序、服务，例如通过浏览器访问资源、通过电子邮件来传递信息等。
- 因特网（Internet）：通过因特网，让公司网络与全球提供Internet服务的网络串连在一起。用户可以通过浏览器访问Internet的资源、通过电子邮件传递信息，更为企业提供一个电子商务服务的网络环境。
- 企业外部网络（Extranet）：企业可以将其局域网与客户、供应商、合作伙伴的网络通过因特网技术串连成企业外部网络，以便相互共享资源。
- 远程访问：它让用户、系统管理员等可以通过远程访问技术，来连接、访问或管理公司内部局域网。企业内两个位于不同地点的局域网，也可通过虚拟专用网络（VPN）串连在一起，以便相互访问对方网络内的资源。

Windows Server 2008 R2提供了各种不同的技术和服务，让您来架构上述的网络环境，例如：

- 同时支持IPv4与IPv6
- DHCP服务器、DNS服务器、WINS服务器
- PKI（Public Key Infrastructure）与IPSec（Internet Protocol Security）
- 路由和远程访问、RADIUS服务器、DirectAccess与网络访问保护（NAP）
- 路由器、NAT与虚拟专用网（VPN）
- Quality of Service （QoS）
- Windows防火墙、802.1X无线网络、远程桌面服务、Windows部署服务
- IIS网站、SSL网站、FTP服务器、SSL FTP服务器
- Windows Server Update Services（WSUS）
- 网络负载均衡（Network Load Balancing）与Web Farm

1-2 TCP/IP协议简介

TCP/IP协议是目前最完整、被支持最广的协议，它可以让不同网络架构、不同操作系统的计算机之间相互通信，例如Windows Server 2008 R2、Linux主机等。它也是Internet的标准协议，更是Active Directory Domain Services（AD DS）所必须使用的协议。

在TCP/IP网络上，每一台连接在网络上的计算机（与部分设备）被称为是一台**主机**（host），

而这台主机必须正确配置TCP/IP属性，才可以与其他主机通信。

1-2-1 IP地址

每一台主机都有一个唯一的IP地址（其功能就好像是各家的门牌号码），IP地址不但可以用来标识每一台主机，其内也包含如何在网络之间发送数据的路径信息（routing information）。

IP地址占用32位（bit），一般是以4个十进制数来表示，每一个数字被称为一个octet。Octet与octet之间以点（dot）隔开，例如**192.168.1.31**。

> **提示**
>
> 这里所介绍的是目前使用最广泛的IPv4地址，它共占用32位，新版本的IPv6共占用128位（其相关说明请参考章节1-3）。

上述32位的IP地址中包含了**网络ID**（Network ID）与**主机ID**（Host ID）两部分数据：

- **网络ID**：每一个网络都有一个唯一的网络ID，换句话说同一个网络内的每一台主机都拥有相同的网络ID。
- **主机ID**：同一个网络内的每一台主机都有一个唯一的主机ID。

若网络需要与外界通信的话，则可能需要为此网络申请一个网络ID，整个网络内所有主机都使用这个网络ID，然后再分配给网络内每一台主机一个唯一的主机ID，因此网络上每一台主机就都会有一个唯一的IP地址（网络ID+主机ID）。您可以向Internet服务提供商（ISP）申请网络ID。

如果此网络并未与外部Internet连接在一起的话，则您可以自行选用任何一个可用的网络ID，不用申请，但是网络内各主机的IP地址不可相同。

1-2-2 IP 类

传统IP地址被分为A、B、C、D、E五大类，其中只有A类、B类、C类的IP地址可供一般主机使用（见表1-1），每类地址所支持的IP地址数量都不相同，以便满足各种不同规模的网络需求。D类和E类是特殊用途的IP地址。

表 1-1

类别	网络ID	主机识别码	W 值可为	可支持的网络数量	每个网络可支持的主机数量
A	W	X.Y.Z	1~126	126	16 777 214
B	W.X	Y.Z	128~191	16 384	65 534
C	W.X.Y	Z	192~223	2 097 152	254
D			224~239		
E			240~254		

在表中我们将IP地址的4个字节以W.X.Y.Z的形式来加以说明。

- **A类**：A类的IP地址适合于超大型网络，其网络ID占用一个字节W。W的范围为1到126，它可提供126个A类的网络ID。主机ID共占用X、Y、Z三个字节（24位），此24位可支持（2 ^ 24）－2＝16 777 214台主机（减2的原因后述）。
- **B类**：B类的IP地址适合于大中型网络，其网络ID占用两个字节W、X。W的范围为128到191，它可提供（191－128＋1）＊256＝16 384个B类的网络。主机ID共占用Y、Z两个字节，因此每个网络可支持（2 ^ 16）－2＝65 534台主机。
- **C类**：C类的IP地址适合于小型网络，其网络ID占用三个字节W、X、Y。W的范围为192到223，它可提供（223－192＋1）＊256＊256 ＝2 097 152个C类的网络。主机ID只占用一个字节Z，因此每个网络可支持（2^8）－2＝254台主机。
- **D类**：它是**组播**（multicast，或译为**多播**）所使用的组ID（group ID），这个组内包含着多台主机。其W的范围为224到239。
- **E类**：它保留给未来使用或供实验用途，其W的范围为240到254。

在设置主机的IP地址时请注意以下事项：

- **网络ID不可以是127**：网络ID127供**环回测试**（loopback test）使用，以便检查网卡与驱动程序是否可以正常工作。虽然您不可以将它分配给主机使用，不过一般来说127.0.0.1这个IP地址用来代表主机本身。
- **每一个网络的第1个IP地址代表网络本身、最后一个IP地址代表广播地址，因此实际可分配给主机的IP地址将少2个**：例如若您所申请到的网络ID为203.3.6，则共有203.3.6.0 到203.3.6.255的256个IP地址，但203.3.6.0是用来代表这个网络（因此我们一般会说此网络的网络ID为4个字节的203.3.6.0，而不是3个字节的203.3.6）；而203.3.6.255则保留给广播用途（255代表广播），例如若发送消息到203.3.6.255这个地址，表示将消息广播给网络ID为203.3.6.0网络内的所有主机。

图 1-1为一个C类的网络示例，其网络ID为192.168.1.0，图中5台主机的主机ID分别为1、2、3、21与22。

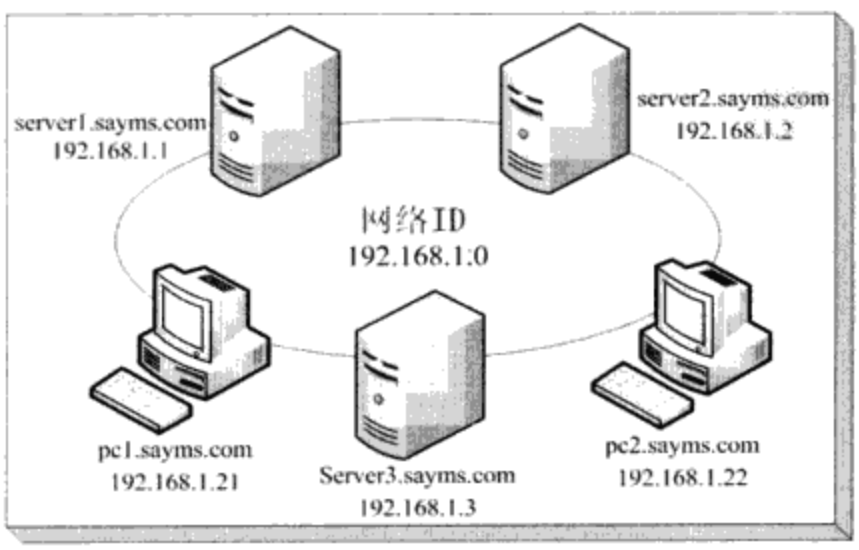


图 1-1

1-2-3 子网掩码

子网掩码也是占用32位，当IP网络上两台主机在相互通信时，它们利用子网掩码来得知对方的网络ID，进而得知彼此是否在相同网络内。

表1-2中为各类默认的子网掩码值，其中为1的位是用来算出网络ID，为0的位是用来算出主机ID，例如若某台主机的IP地址为192.168.1.3，转换为二进制值为11000000.10101000.00000001.00000011，而其子网掩码为255.255.255.0，转换为二进制值的话是11111111.11111111.11111111.00000000，则计算其网络ID的原则是：

表 1-2

Class	默认子网掩码（二进制）	默认子网掩码（十进制）
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

- 将IP地址与子网掩码相对应的位做AND逻辑运算（参见表1-3）。
- 将AND逻辑运算后的结果与子网掩码中的各位互相对应，只要在子网掩码中位值为1的，其所对应到的位，就是其网络ID，例如表1-3中有向上箭头符号的位。在IP地址中去除网络ID后，其余的部分就是主机ID。

表 1-3

192.168.1.3	→ 11000000	10101000	00000001	00000011
255.255.255.0	→ 11111111	11111111	11111111	00000000
AND后的结果	→ 11000000	10101000	00000001	00000000
	(192)	(168)	(1)	

因此IP地址192.168.1.3的网络ID就是192.168.1（有向上箭头符号的部分）。如前所述，用4个字节来表示网络ID的话，其网络ID为192.168.1.0，而主机ID就是3。

若A主机的IP地址为192.168.1.3，子网掩码为255.255.255.0，B主机的IP地址为192.168.1.5，子网掩码为255.255.255.0，则A主机与B主机的网络ID都是192.168.1.0，表示它们都是在同一个网络内，因此可以直接相互通信，不需要通过路由器（详见第11章）。

注意

如前所述的A类、B类、C类是分类的划分方式，不过目前普遍采用的是无类别的CIDR（Classless Inter-Domain Routing）划分方式，这种方式在表示IP地址与子网掩码时有所不同，例如网络ID为192.168.1.0、子网掩码为255.255.255.0，则一般我们会用192.168.1.0/24来代表此网络，其中的24代表子网掩码中值为1的位数有24个。

1-2-4 默认网关

假设有一个主机A要与同一个网络内的B主机通信（网络ID相同），可直接将数据发送到B主机；但是若要与不同网络内的C主机通信的话（网络ID不同），就需要将数据发送给一个路由器，再通过路由器发送给主机C。一般主机若要通过路由器来转发数据的话，只要事先将其**默认网关**配置成路由器的IP地址即可。

以图 1-2来说，图中甲乙两个网络是通过路由器来串连的。甲乙网络可通过路由器来实现相互间的通信。当甲网络的主机A要与乙网络的主机C通信时，由于主机A的IP地址为192.168.1.1、网络ID为192.168.1.0，而主机C的IP地址为192.168.2.10、网络ID为192.168.2.0，主机A可以判断出主机C是位于不同的子网内，因此会将数据发送给其默认网关，也就是IP地址为192.168.1.254的路由器，然后再由路由器将其发送到主机C。

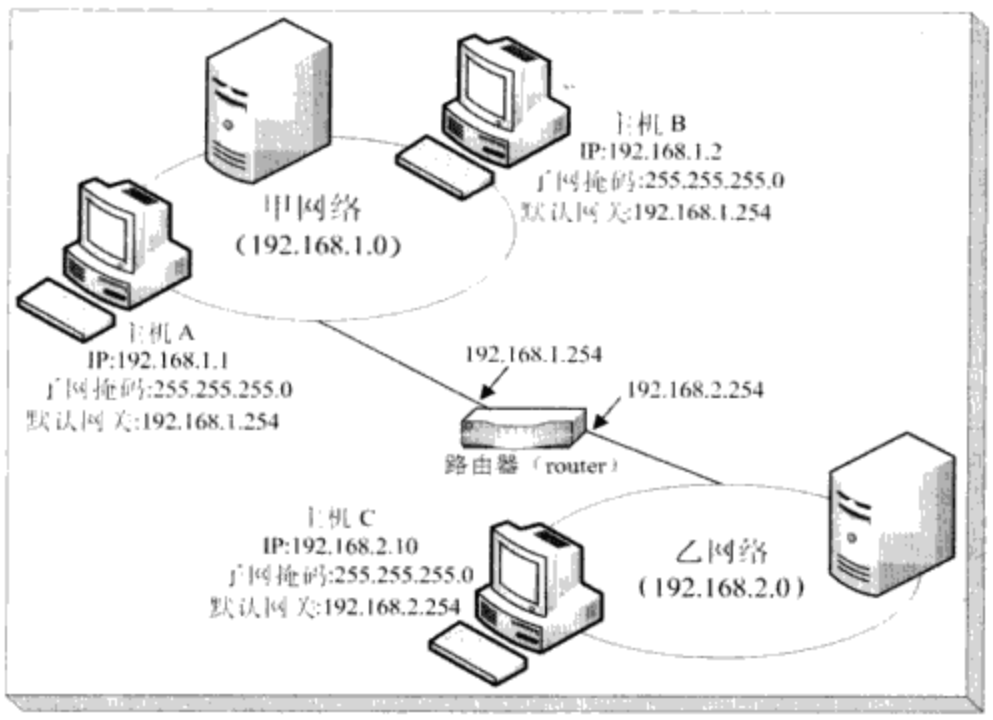


图 1-2

1-2-5 私有IP地址的使用

前面我们提到IP地址类中的A类、B类、C类是可供主机使用的IP地址，在这些IP地址中，有一些被分配为**私有IP**（private IP）（见表 1-4），各公司可以自行选择合适的**私有IP**，而且不需要申请，因此可以节省网络搭建成本。

表 1-4

网络ID	默认子网掩码	IP地址范围
10.0.0.0	255.0.0.0	10.0.0.1~10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1~172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1~192.168.255.254

不过**私有IP**只能够在公司内部的局域网使用，虽然它可以让内部计算机相互通信，但是无法直接与外界计算机通信。使用**私有IP**的计算机若要连接外网、收发电子邮件的话，需要通过具有NAT（Network Address Translation，网络地址转换）功能的设备，例如IP分享器、宽带路由器等。

其他不属于**私有IP**的IP地址被称为**公有IP**（public IP），例如220.135.145.145。使用**公有IP**的计算机可以直接在外网中通信，因此在这些计算机上可以架构商业网站，让外面的用户直接连接此商业网站。这些**公有IP**都必须预先申请。

如果Windows Server 2008 R2计算机因故无法拥有一个有效的IP地址时，则此计算机会通过Automatic Private IP Addressing（APIPA）机制为自己配置一个网络ID为169.254.0.0的临时IP地址，例如169.254.49.31，不过只能够用它来与同一个网络内也是使用169.254.*x*.*x* IP地址的计算机通信。

> **提示**
>
> 本书中的IPv4将利用**私有IP**来学习Windows Server 2008 R2网络。

1-3 IPv6基本概念

前面所介绍的IP地址等概念是属于IPv4的规范，在上世纪末业界曾经担心IPv4地址可能会不够使用，虽然后来利用无类别寻址（classless addressing）、NAT（Network Address Translation）等技术临时解决了问题，然而提供更多地址、效率更好、安全性更高的新版本协议的需求仍然亟切，IPv6也由此诞生了。

1-3-1 IPv6地址的语法

IPv6地址占用128位，它被分为8段，每段占用16位，段之间用冒号（:）隔开，然后以十六进制来表示每段内的数值，由于每段占用16位，因此每段共有4个十六进制的数值，举例来说，假设IPv6地址的二进制表示法为（128位）：

0010000000000001 0000000000000000 0100000100110110 1110001110001100
0001010011011001 0001001000100101 0011111101010111 1111011101011001

则其IPv6地址的十六进制表示为（参考图 1-3）：

2001:0000:4136:E38C:14D9:1225:3F57:F759

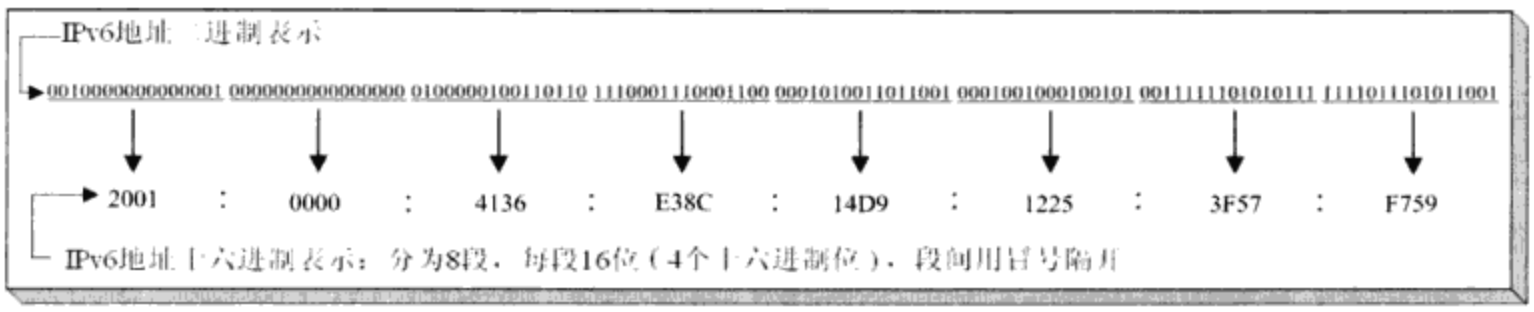


图 1-3

前面的0可以省略

为了简化IPv6地址的表示方式，因此可以省略某些数字为0的部分，例如图 1-4中的21DA:00D4:0000:E38C:03AC:1225:F570:F759可以被改写为21DA:D4:0:E38C:3AC:1225:F570:F759，其中的00D4被改写为D4、0000被改写为0、03AC被改写为3AC。

注意段中只有靠左边的0可以被省略，而靠右边或中间的0不可以省略，例如F570不可以改写为F57。

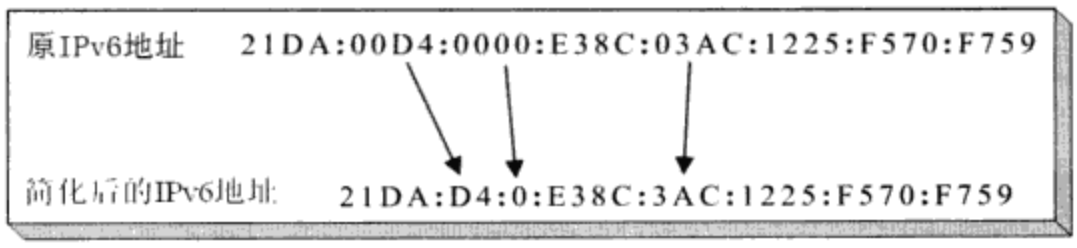


图 1-4

连续的0段可以缩写

如果有连续几个段都是0，则可以改用双冒号（::）来代表这些连续段，例如图 1-5中的FE80:0:0:0:10DF:D9F4:DE2D:369B可以被缩写为FE80::10DF:D9F4:DE2D:369B。

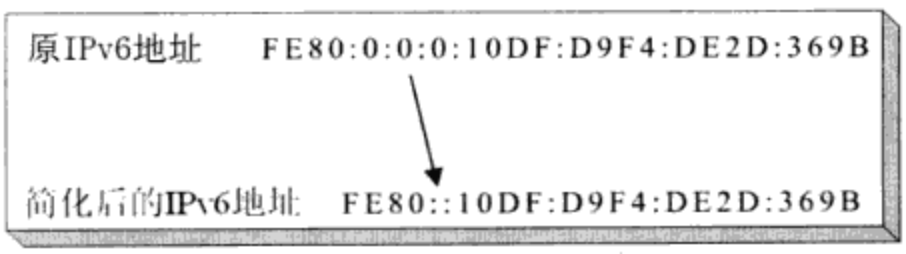


图 1-5

此示例将其中连续3个为0的段改用双冒号来表示。注意在一个IPv6地址中，这种缩写方式只能够使用一次，例如图 1-6的地址FE80:0:0:0:10DF:0:0:369B中有两个连续0段（0:0:0与0:0），则您可以将其中的0:0:0或0:0缩写，也就是此地址可用以下方式来表示：

FE80::10DF:0:0:369B 或 FE80:0:0:0:10DF::369B

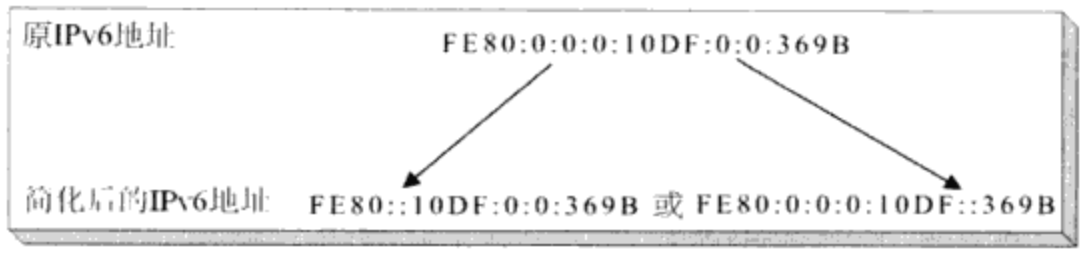


图 1-6

但是不可以同时将0:0:0与0:0都缩写，也就是此地址不可以写成：

FE80::10DF::369B

因为将无法判断其中两个双冒号::各自代表着多少个0段。

IPv6的前缀（prefix）

前缀是IPv6地址的一部分，用来表示IP地址中某些位是固定的值，或用来反映其所代表的子网，前缀的表示方式与IPv4的CIDR表示方式相同。IPv6地址的前缀表示法为 ***地址/前缀长度***，例如21DA:D3:0:2F3B::/64就是一个IPv6地址的前缀，也就是IPv6地址中最左边64个位固定为21DA:D3:0:2F3B。IPv4中使用的子网掩码，在IPv6中已经不支持。

1-3-2 IPv6地址的分类

IPv6支持3种类型的地址，它们分别是unicast地址（单点广播地址）、multicast地址（多点广播地址）与anycast地址（任意点广播地址）。表 1-5列出IPv4地址与其对应的IPv6地址。

表 1-5

IPv4地址	IPv6地址
Internet地址按类别分类	不分类
Public IP地址	Global unicast地址
Private IP地址（10.0.0.0/8，172.16.0.0/12与192.168.0.0/16）	Site-local地址（FEC0::/10）
APIPA自动配置的IP地址（169.254.0.0/16）	Link-local地址（FE80::/64）
Loopback地址为127.0.0.1	Loopback地址为::1
未分配地址为0.0.0.0	未分配地址为::
广播地址	不支持广播
多点广播地址（224.0.0.0/4）	IPv6多点广播地址（FF00::/8）

Unicast地址（单点广播地址）

Unicast地址用来代表单一网络接口，例如每一块网卡可以有一个unicast地址，当数据包目标是unicast地址时，该数据包将被发到拥有此unicast地址的网络接口。IPv6的unicast地址包含以下几种类型：

- Global unicast地址
- Link-local地址
- Site-local地址
- 特殊地址（special IPv6 address）
- 兼容地址（compatibility address）

Global unicast地址（全局单点广播地址）

IPv6的global unicast地址相当于IPv4的public IP地址，它们可以被路由与连接到Internet。图 1-7为global unicast地址的结构图，它包含以下四个字段：

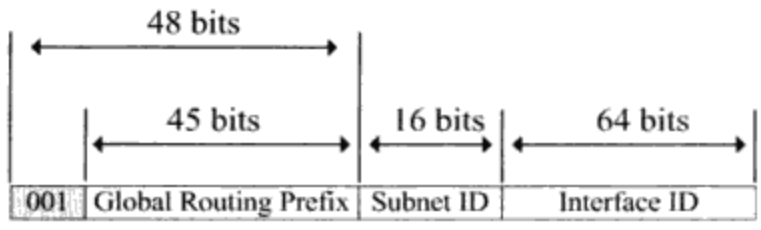


图 1-7

- 最左边3位固定为001（参考图 1-7）。Global unicast地址的前缀为**2000::/3**，其中最左边的2的二进制为0010，其左边的3位就是001。
- Global Routing Prefix（全局路由前缀）是公司网络所在地（site，以下将其称为**站点**）的路由前缀，它类似于IPv4的网络ID（network ID）。3个固定为001的前缀加上45位的Global Routing Prefix，一共48位被用来分配给公司的站点，Internet网络上的IPv6路由器在收到前缀符合这48位格式的数据包时，就会将此数据包路由到拥有此前缀的站点。
- Subnet ID（子网ID）用来区分站点内的子网，通过这16位的Subnet ID，可以让公司在一个站点内创建最多65536个子网。
- Interface ID（接口ID）用来表示子网内的一个网络接口（例如网卡），它相当于IPv4中的主机ID（host ID）。Interface ID可以通过以下两种方式中的一种来产生：
  - **根据网卡的MAC地址生成Interface ID**：如图 1-8中的1号箭头所示，先将MAC地址（物理地址）转换成标准的EUI-64（Extended Unique Identifier-64）地址，然后再修改此EUI-64地址，也就是如2号箭头所示将图中的0改为1（此位在标准的IEEE 802网卡中为0），最后将此修改过后的EUI-64地址当作IPv6的Interface ID。Windows Server 2003与Windows XP所自动配置的IPv6地址，默认是用此方法生成Interface ID。

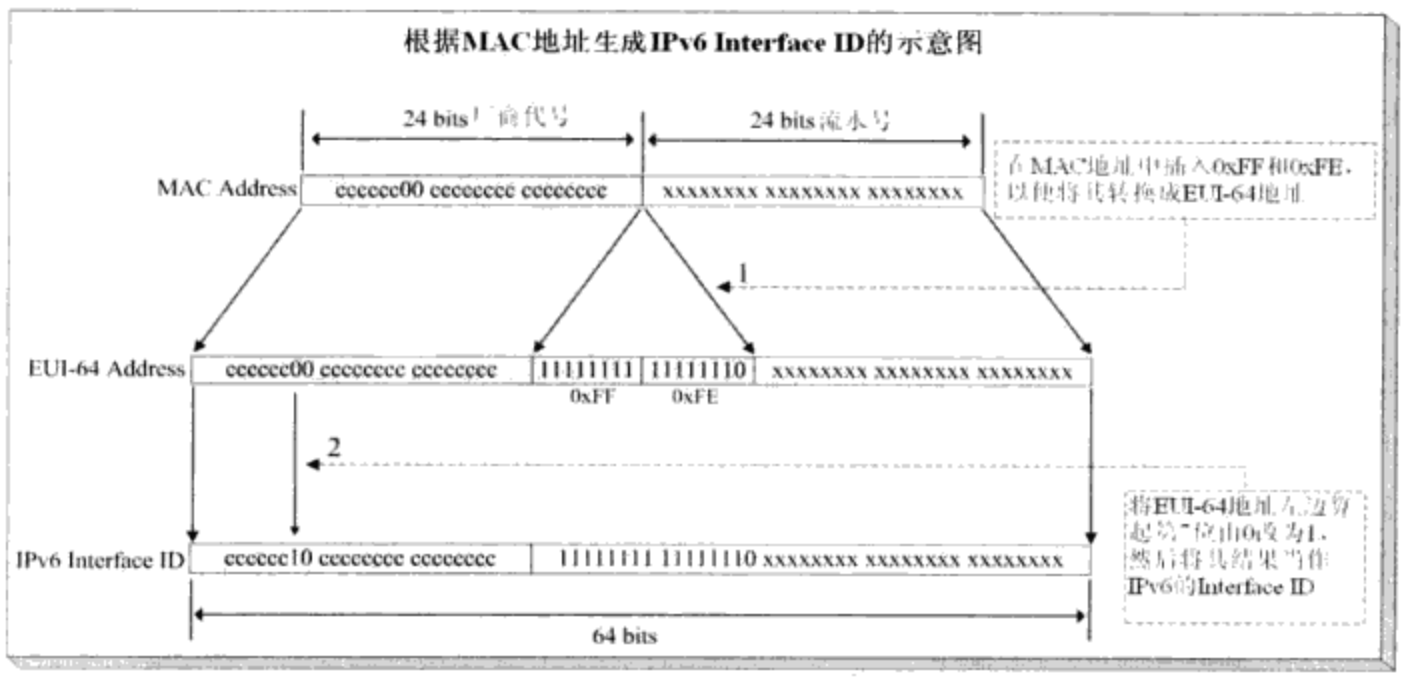


图 1-8

■ **随机数生成Interface ID**：Windows Server 2008 R2、Windows Server 2008、Windows 7与Windows Vista自动配置的IPv6地址，默认是用此方法生成Interface ID。

Link-local地址（本地链接地址）

拥有link-local地址的节点使用此地址与同一**链接**上的邻近节点通信（见附注），IPv6节点（例如Windows Server 2008 R2主机）会自动配置link-local 地址。Link-local地址相当于IPv4中利用Automatic Private IP Addressing机制获取的IP地址169.254.0.0/16。Link-local地址的使用范围是该节点所连接的本地链接（local link）之内，也就是利用此地址来与同一个链接内的节点通信。图 1-9为link-local地址的结构图。

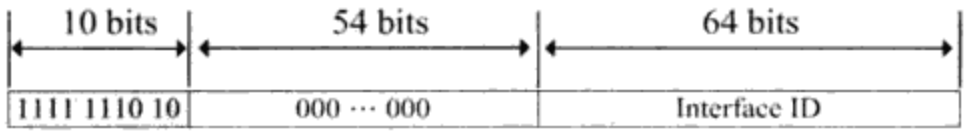


图 1-9

提示

什么是节点（node）？任何一个拥有IP地址的设备都可称为节点，例如计算机、打印机、路由器等。

一个站点（site）内包含着一或多个子网，这些子网通过路由器等设备连接在一起。每一个子网内包含着多个节点，这些节点通过网络接口（network interface，例如网卡）连接在这个子网上，也就是说这些节点是在同一个**链接**（link）上。

Link-local地址以**FE80**开头，其前缀为**FE80::/64**。IPv6路由器在收到目的地为link-local地址的数据包时，绝对不会将其路由到本地链接之外的其他链接。图 1-10中右边倒数第1个箭头所指处就是一个link-local地址，此界面是通过运行**netsh interface ipv6 show address**命令得到的。图中link-local地址（**FE80::**开始）最后**%**后面的数字11是网络接口索引（interface index），例如若在此主机上用**Ping FE80::10DF:D9F4:DE2D:369B%11**命令来与另外一台IPv6主机通信时，它表

示是要通过接口索引为11的这个网络接口来将数据包发出。其实%之后的数字应该称为Zone ID：若是link-local地址的话，此Zone ID就是接口索引，若是site-local地址的话，Zone ID就是site ID。

为何link-local与site-local地址需要Zone ID? 因为它们的前缀可以重复使用，因而会造成使用上的混淆，以link-local地址来说（Zone ID为接口索引），若您的主机有两块网卡，分别连接到A与B链接，每块网卡都自动分配到一个FE80::开头的link-local地址，假设有一台主机位于B链接，其link-local地址也是FE80::开头，若您的主机要与该主机通信的话，由于您的两块网卡地址都是FE80::开头，此时该由哪一块网卡发出数据包呢? 所以，只要在IP地址后面加上网络接口索引，就可以知道是要通过拥有此接口索引的网卡发出。每一台主机各有自己的接口索引，并不一定会相同。

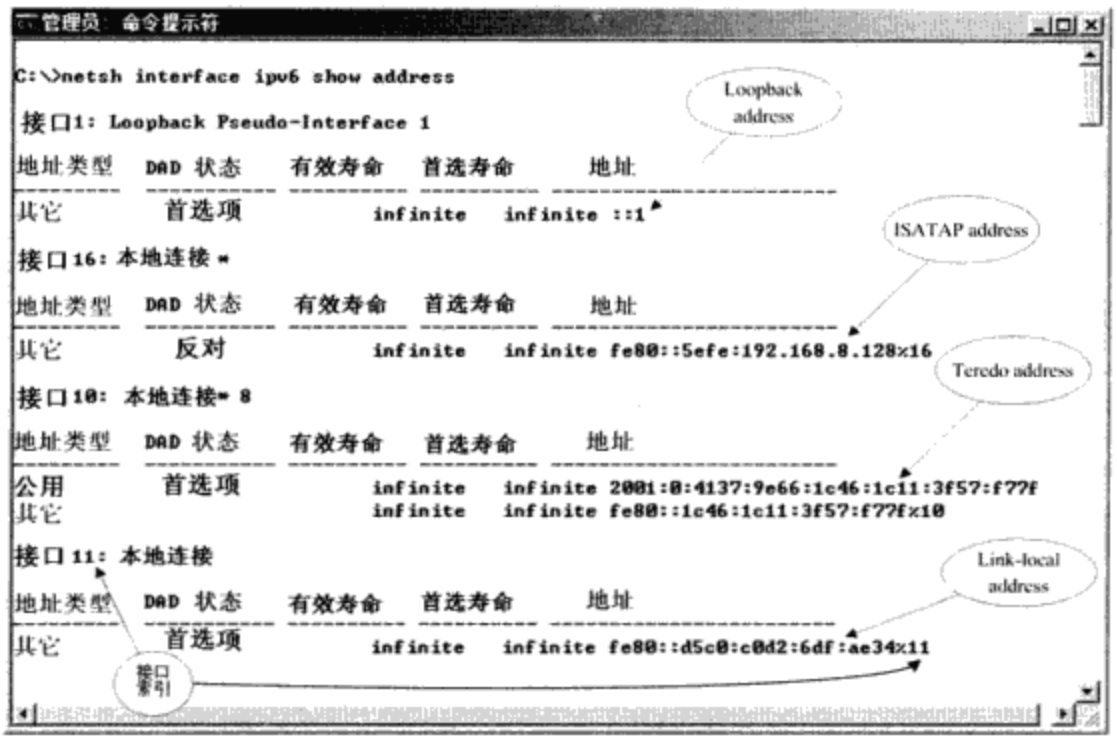


图 1-10

同理，每一台主机也可能有多块网卡分别连接到多个站点（site），因此也需通过Zone ID来区分（此时它被称为Site ID）。每一台主机各有自己的Site ID，并不一定会相同。若您的主机只连接到1 个站点，则其Site ID为1。

您也可以如图 1-11所示用**ipconfig**或**ipconfig /all**命令获得一些IPv6的相关信息。

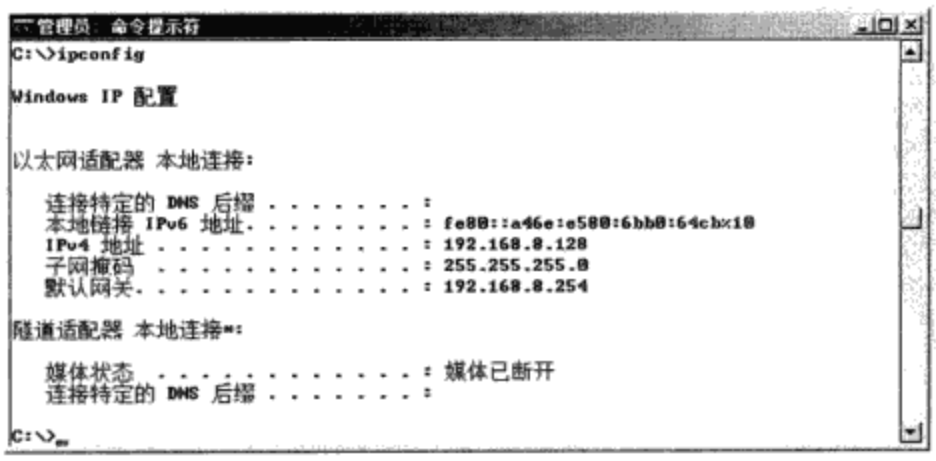


图 1-11

Site-local地址（本地站点地址）

Site-local地址相当于IPv4中的private IP地址（10.0.0.0/8，172.16.0.0/12与192.168.0.0/16），site-local地址的使用范围是该节点所链接的站点（local site）之内，也就是用来与同一站点内的节点通信。路由器不会将使用site-local地址的数据包转发到其他站点，因此一个站点内的节点无法使用site-local地址与其他站点内的节点通信。IPv6节点并不会自动配置site-local地址，而是通过路由器或DHCPv6服务器来配置。

图 1-12为site-local地址的结构图。Site-local地址的前缀占用10位，其前缀为**FEC0::/10**。每一个站点可以通过占用16位的Subnet ID来划分子网。IPv6路由器在收到目的地为site-local地址的数据包时，并不会将其路由到区域站点（local site）之外的其他站点。

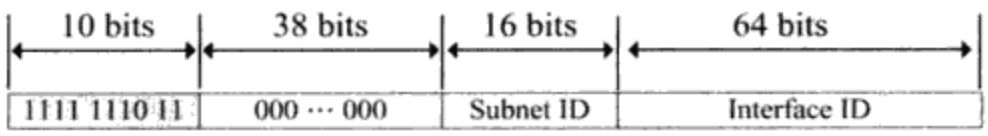


图 1-12

注意

RFC 3879内已经不赞成在新搭建的IPv6网络使用site-local地址，但是现有IPv6环境可以继续使用site-local地址。

特殊地址

以下是两个特殊的IPv6地址：

- **未分配地址（unspecified address）**：也就是**0:0:0:0:0:0:0:0**或**::**，它相当于IPv4的0:0:0:0，它并不会被用来分配给网络接口，也不会被当作数据包的目的地址。当节点要确认其网络接口所获取的临时地址（tentative address）是否唯一时，其所发出的确认数据包的来源地址就是使用**未分配地址**。
- **环回地址（loopback address）**：也就是**0:0:0:0:0:0:0:1**或**::1**（参考图 1-10中的示例），它相当于IPv4的127.0.0.1。我们可以通过环回地址来进行环回测试，以便检查网卡与驱动程序是否可以正常工作。发送到此地址的数据包并不会被发送到**链接**（link）上。

兼容地址与自动隧道

目前绝大多数网络是使用IPv4，而要将这些网络转移到IPv6是一个漫长且具有很高挑战性的工作，为了让转移工作能够更加顺利，IPv6提供了若干个自动隧道技术（automatic tunneling technology）与兼容IP地址来帮助从IPv4转移到IPv6。

自动隧道不需要您手动创建，而是由系统自动创建此隧道。如图 1-13所示两台同时支持IPv6与IPv4的主机如果要利用IPv6来通信的话，由于它们之间的网络为IPv4架构，此网络无法发送IPv6数据包，此时可以在两台主机之间通过隧道来发送IPv6数据包，也就是将IPv6数据包封装到IPv4数据包内，然后通过IPv4网络来发送。

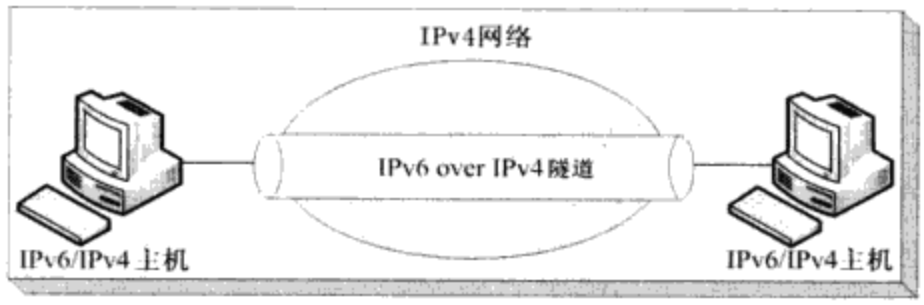


图 1-13

IPv6支持多个兼容地址，以便隧道两端的主机（或路由器）可用它们来通信：

- **ISATAP地址**：ISATAP（Intra-Site Automatic Tunnel Addressing Protocol）地址是主机-主机、主机-路由器、路由器-主机之间通过隧道通信时所使用的IPv6地址，它让两台同时支持IPv6与IPv4的主机之间可以在IPv4 Intranet网络上用IPv6来通信。
  ISATAP 地址的Interface ID格式为**::0:5EFE:w.x.y.z**，其中**w.x.y.z**为unicast IPv4地址（public或private）。任何一个可用在unicast地址的64位前缀，都可以当作是ISATAP地址的前缀，包括link-local地址（FE80::/64），例如FE80::5EFE:192.168.8.128就是一个link-local ISATAP 地址。Windows Server 2008 R2的每一个IPv4网络接口都有一个虚拟ISATAP隧道接口（tunneling pseudo-interface），而系统默认会为此接口配置一个link-local ISATAP 地址（可参考图 1-10中的示例），拥有link-local ISATAP 地址的两台主机，可以各自使用其ISATAP地址通过IPv4网络通信。
- **6to4地址**：6to4地址是路由器-路由器、主机-路由器、路由器-主机之间通过隧道通信时所使用的IPv6地址，它可以让IPv6主机通过IPv4 Internet来连接IPv6站点。6to4地址属于global unicast地址，其前缀为**2002:wwxx:yyzz::/48**，其中的**wwxx:yyzz** 是获取自unicast public IPv4地址（w.x.y.z）。
- **Teredo地址**：Teredo是给IPv6使用的NAT-T。若一台同时支持IPv6与IPv4的主机位于IPv4的NAT之后，则当它要在IPv4的因特网上使用IPv6时，就可以使用Teredo地址。早期Teredo 地址的前缀尚未定义出来时，Microsoft为Windows XP与Windows Server 2003所设置的前缀为**3FFE:831F::/32**，不过现在定义在RFC4380的标准前缀为**2001::/32**，因此Windows Server 2008 R2、Windows Server 2008、Windows 7与Windows Vista都采用标准的**2001::/32**（可参考图 1-10中的示例），Windows XP与Windows Server 2003必须安装更新程序后才会改用标准的前缀（参考Microsoft安全性公告MS06-064）。
- **IPv4-compatible地址**：两台同时支持IPv6与IPv4的主机要相互使用IPv6通信时，如果它们之间需要经过使用public地址的IPv4网络的话，便可以使用IPv4-compatible地址从而通过自动隧道通信。
  IPv4-compatible地址的格式为**0:0:0:0:0:0:w.x.y.z**或**::w.x.y.z**，其中**w.x.y.z**为unicast public IPv4地址，例如某台主机的IPv4地址为220.14.10.11，则其IPv4-compatible地址为**0:0:0:0:0:0:220.14.10.11**或**::220.14.10.11**。

- **6over4地址**：6over4被又称为**IPv4组播隧道**，它是主机-主机、主机-路由器、路由器-主机之间通过隧道通信时所使用的IPv6地址。它让IPv6主机之间可以在IPv4 Intranet网络上利用unicast与multicast IPv6来通信。
  任何一个可用在unicast地址的64位前缀，都可以当作是6over4地址的前缀，而其Interface ID格式为**::wwxx:yyzz**，其中的**wwxx:yyzz**同样获取自unicast IPv4地址（w.x.y.z）。6over4主机默认会为其每一个6over4网络接口配置一个link-local地址FE80::wwxx:yyzz。

Multicast地址（多点广播地址）

IPv6 multicast地址与IPv4一样是用来代表一组网络接口，也就是多个节点可加入到同一multicast组，它们都可通过共同的multicast地址来监听multicast请求。一个节点也可以加入多个multicast组，也就是它可以同时通过多个multicast地址来监听multicast的流量。图 1-14为multicast地址的结构图。

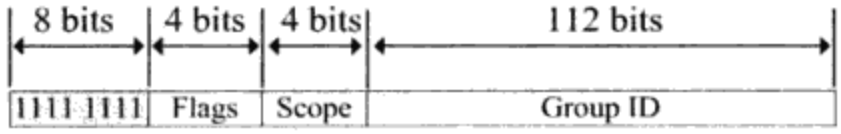


图 1-14

- 其最高8位固定为11111111，也就是十六进制的FF。
- **Flags**：它目前有以下两个值：
  - **0000**：表示它是由IANA组织（Internet Assigned Numbers Authority）固定分配给well-known multicast地址的地址。
  - **0001**：表示它尚未被IANA固定分配使用，是一个临时multicast地址。
- **Scope**:用来表示此multicast地址可发送的范围，当路由器收到multicast地址的数据包时，它可以根据scope来决定是否要路由此数据包。Scope最常见的值为1(表示node-local scope。node-local：发送给节点自己)、2（表示link-local scope）与5（表示site-local），举例来说如果路由器收到一个要发送至FF02::2的数据包时，由于此数据包的范围为link-local，因此路由器并不会将此数据包发送到超出此本地链接（local link）以外的链接。
- **Group ID**：用来代表此组的唯一组ID，它占用112位，不过RFC 3513建议只使用最低的32位，其余的填0。

从FF01::到FF0F::是保留的well-known multicast地址，例如：

- FF01::1（node-local scope all-nodes multicast address）
- FF02::1（link-local scope all-nodes multicast address）
- FF01::2（node-local scope all-routers multicast address）
- FF02::2（link-local scope all- routers multicast address）

- FF05::2（site-local scope all- routers multicast address）

Solicited-node multicast地址

在IPv4中是利用**ARP request**来进行IP地址解析工作（解析物理层的地址，以Ethernet网络来说就是MAC地址），由于它是MAC-level的广播数据包，因此会干扰到网段内的所有节点。在IPv6中通过发出**Neighbor Solicitation**信息来进行IP地址解析工作，而且为了减少对链接内所有节点的干扰，因此信息目的地址不是采用link-local scope all-nodes multicast地址，而是solicited-node multicast地址，此地址是从网络接口的unicast地址转换而来，如图 1-15所示，其前缀为**FF02::1:FF00:0/104**，最后的24位是获取自unicast地址的Interface ID的最右24位。

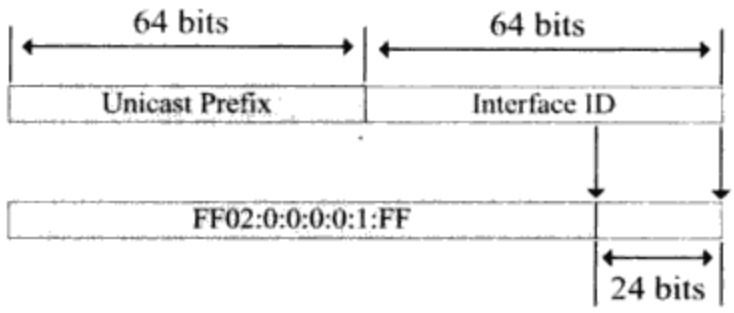


图 1-15

提示

IPv6不再使用广播地址，所有原先在IPv4中使用广播地址的方式，在IPv6中都改用multicast地址。

例如某台主机的网络接口的link-local IPv6地址为FE80::10DF:D9F4:DE2D:369B，由于其最右边24位为2D:369B，故其solicited-node multicast地址为FF02::1:FF2D:369B，该主机会注册并拥有此地址，并通过此地址来监听IP地址解析请求。

Anycast地址（任意点广播地址）

Anycast地址可以被分配给多个网络接口（通常是位于不同的节点上），发送到anycast地址的数据包，并不是被发送到拥有此anycast地址的所有节点，而只会被发送到其中一个节点，它是距离最近的节点（指路由距离）。

Anycast地址目前只能够用在数据包的目的地地址，而且只能够分配给路由器来使用。Anycast地址是来自unicast地址，因此它的表示法与unicast没有差别，且它的发送范围与所使用的unicast地址一样。

在Anycast地址中有一个提前定义好的地址：Subnet-Router anycast地址，它是路由器必须支持的地址，发送给Subnet-Router anycast的数据包，会被发送到该子网中的一个路由器。Subnet-Router地址的格式如图 1-16所示，其中的**subnet prefix**表示网络接口所在的链接（link，也可以说是**子网**），其长度视不同的unicast地址而有所不同，后面剩下的位都是0。

图 1-16

1-3-3 IPv6地址的自动设置

IPv6最好用的功能之一就是IPv6主机能够自动设置自己的IPv6地址，而且可以不需要通过DHCPv6协议的帮助。

自动设置IPv6地址的方法

IPv6主机默认会自动为每一个网络接口设置一个link-local地址，除此之外，如果IPv6主机能够找到路由器的话，还可以根据路由器内的设置来获得更多的IPv6地址与参数，然后利用这些地址来连接因特网（如果是global地址的话）或连接同一个站点内的其他子网（如果是site-local地址的话）。IPv6主机是通过发出Router Solicitation信息来寻找路由器，路由器会回应Router Advertisement信息，此信息内包含以下信息：

- **一或多个附加的前缀**：IPv6主机会根据这些附加的前缀（可能是global或local前缀）另外创建一或多个IPv6地址。
- **Managed Address Configuration（M）标志**：若此标志被设置为1的话，表示要使用DHCPv6来获取IPv6地址。
- **Other Stateful Configuration（O）标志**：若此标志被设置为1的话，表示要使用DHCPv6来获取其他参数，例如DNS服务器的IPv6地址。

若路由器所回复的信息内包含一或多个前缀，但是M与O标志都被设为0，此时IPv6主机会根据前缀来创建一或多个IPv6地址，但是不会通过DHCPv6来获取其他IPv6地址与参数，这种自动设置被称为**无状态自动配置**（Stateless Autoconfiguration）；若路由器所回复的信息内没有前缀，但是M或O标志被设为1，此时IPv6主机只会通过DHCPv6来获取其他IPv6地址或参数，这种自动设置被称为**全状态自动配置**（Stateful Autoconfiguration）；若路由器有回复前缀，且M或O标志被设置为1的话，则IPv6主机会同时采用以上两种自动设置的方式来获取IPv6地址与参数。

> **提示**
>
> 若M标志与O标志都为1的话，在Windows Server 2008 R2内的DHCP服务器将其称为**DHCPv6全状态模式**；若M标志为0、O标志为1，则将其称为**DHCPv6无状态模式**。

自动设置的IPv6地址的状态分类

无论是IPv6主机自动设置的link-local地址或用路由器回复的前缀所创建的global或local地

址、还是通过DHCPv6获取的任何一个IPv6地址，这些IP地址在不同的时间有着不同状态，如图 1-17所示：

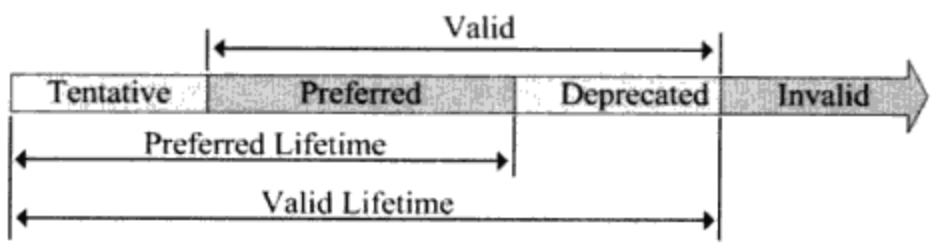


图 1-17

- **Tentative（临时性）**：当产生一个新IPv6地址时，它是处于tentative（临时性）状态，此时IPv6主机会通过发出Neighbor Solicitation信息来运行DAD （Duplicate Address Detection）程序，以便监测此地址是否已被使用。若收到Neighbor Advertisement回应信息的话，就将其标识为**已被重复使用**。
- **Preferred（首选的）**：如果确认了此IP地址的唯一性（IPv6主机未收到Neighbor Advertisement回应信息），就将此地址的状态改为Preferred，而从现在开始它就是一个有效的（valid）IPv6地址，IPv6主机可以用此地址来接收与发送数据包。
- **Deprecated（已超时）**：一个状态为Preferred的IPv6地址有一定的使用时限，时限过后，其状态就会被改为Deprecated，它还是一个有效的地址，现有的连接可以继续使用Deprecated地址，不过新的连接不应该使用Deprecated地址。
- **Invalid（无效的）**：处于Deprecated状态的地址在经过一段时间后就会变成无效的（invalid）地址，此时就不可以再通过此地址来接收与发送数据包。

在图 1-18中运行**netsh interface ipv6 show address**命令后，可以看到有几个处于不同状态的IPv6地址。

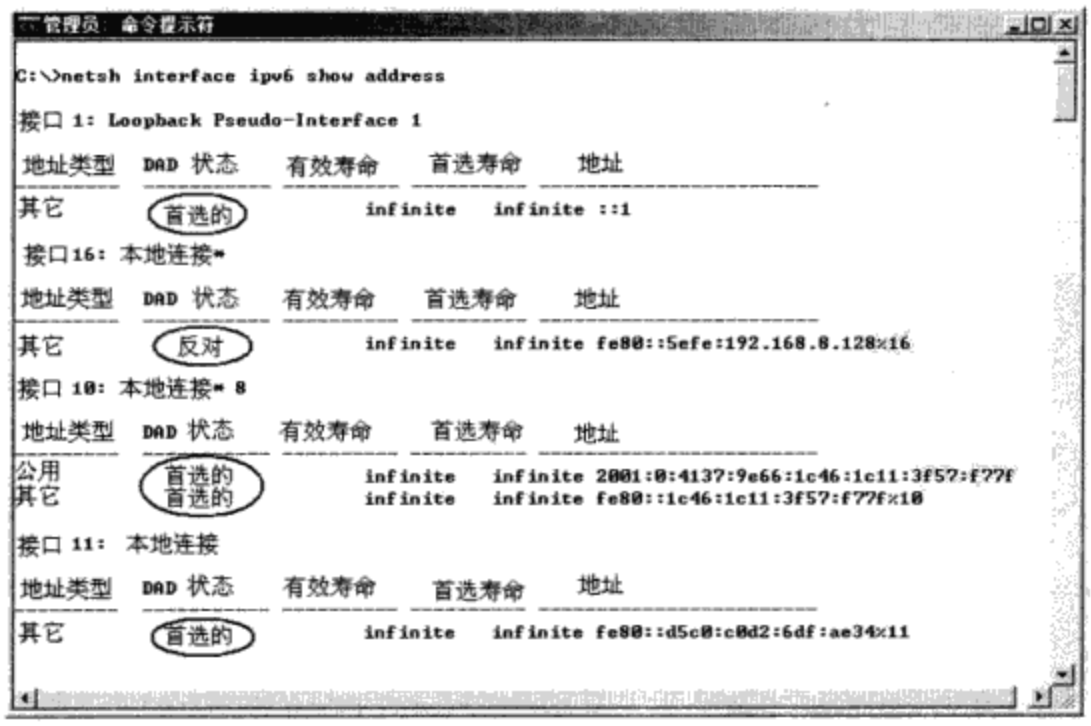


图 1-18

另外图最左边可看到**地址类型**字段出现**公用**（Public）这个词，这是因为IPv6的地址又可

被分类为公用、临时与其他地址。其中公用与临时地址的说明如下：

- **公用IPv6地址（public IPv6 address）**：它是一个global地址，主要用来接收传入连接（incoming connection），例如用在网站，这个地址应该要在DNS服务器内注册。公用IPv6地址的interface ID可以是EUI-64地址（参见前面“Global unicast地址”的说明）或用随机生成的。
- **临时IPv6地址（temporary IPv6 address）**：此地址主要是客户端应用程序在初始连接时使用，例如网页浏览器就可以使用此地址连接外部网站，此地址不需在DNS服务器内注册。临时IPv6地址的interface ID是随机生成的，这是为了安全考虑，因为是随机生成的，故每次IPv6协议启动时，其IPv6地址都不一样，如此可避免用户的上网行为被追踪。

为了安全起见，Windows Server 2008 R2、Windows Server 2008、Windows 7与Windows Vista默认是用随机数来生成unicast地址的Interface ID[包含global（public）地址]。您可以通过以下命令来禁用随机生成Interface ID：

```
netsh interface ipv6 set global randomizeidentifiers=disabled
```

或要重新启用的话，只要将disabled改为enabled即可。

可以通过netsh interface ipv6 show global命令来查看目前系统是否使用随机数来生成interface ID，如图 1-19所示为已经启用。

图 1-19

1-4 Windows Server 2008 R2的管理工具

Windows Server 2008 R2可扮演很多角色，例如DNS服务器、DHCP服务器等，在您安装这些角色后，系统会自动创建用来管理这些角色的工具，它们位于【开始➲管理工具】内。您也可通过【开始➲管理工具➲服务器管理器】或单击左下角的**服务器管理器**图示来管理这些角色。

如果您要在Windows Server 2008 R2计算机上管理远程Windows Server 2008 R2计算机内的

角色与功能，但是要使用的管理工具却没有出现在【开始➲管理工具】内的话，此时可以通过【打开**服务器管理器**➲单击**功能**➲添加功能➲远程服务器管理工具➲在图 1-20中选择所需角色或功能的管理工具】，之后便可以在【开始➲管理工具】中来选择这些管理工具。

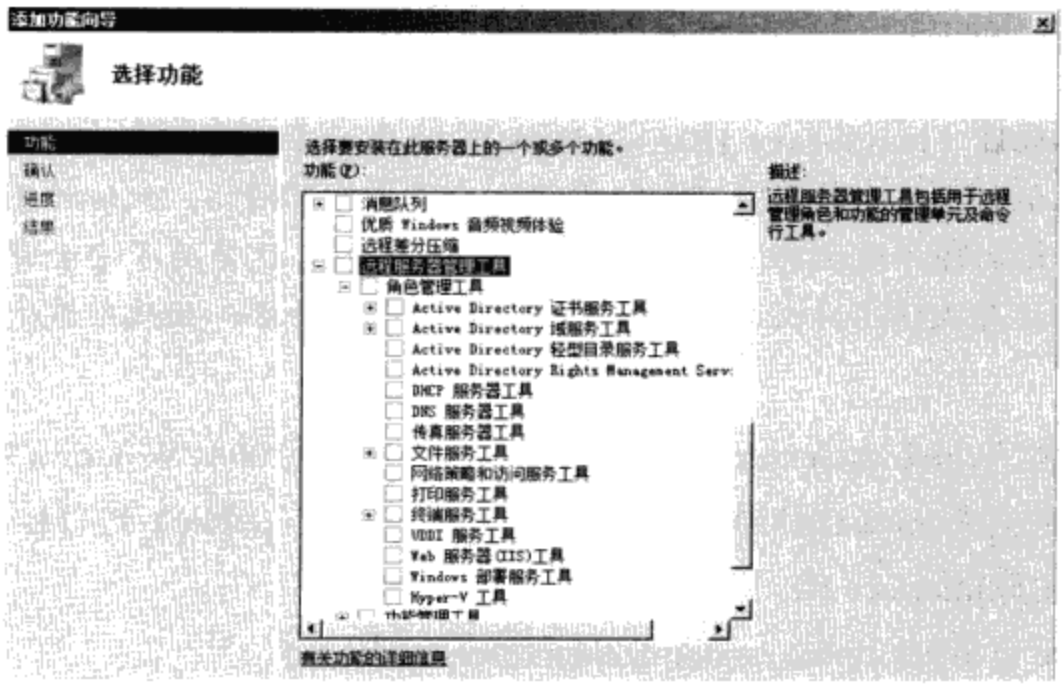


图 1-20

若要在Windows 7计算机上管理Windows Server 2008 R2角色与功能的话，请到微软网站下载与安装Remote Server Administration Tools for Windows 7工具（Windows 7的远程服务器管理工具），安装完成之后选择【开始➲控制面板➲单击最下方的**程序**➲单击最上方的**打开或关闭Windows功能**➲在图 1-21中选择要使用的角色管理工具、功能管理工具或服务器管理器】，之后便可以在【开始➲管理工具】中选择这些管理工具。

图 1-21

若在**开始菜单**中没有**管理工具**快捷方式的话，请通过以下方法添加：【对着屏幕左下角**开始**图形按右键➲属性➲如图 1-22所示单击 **「开始」菜单**右边的自定义➲选择系统**管理工具**处的**在“所有程序”菜单和「开始」菜单上显示】**，接着就可以在【开始➲管理工具】中选择管理工具了。

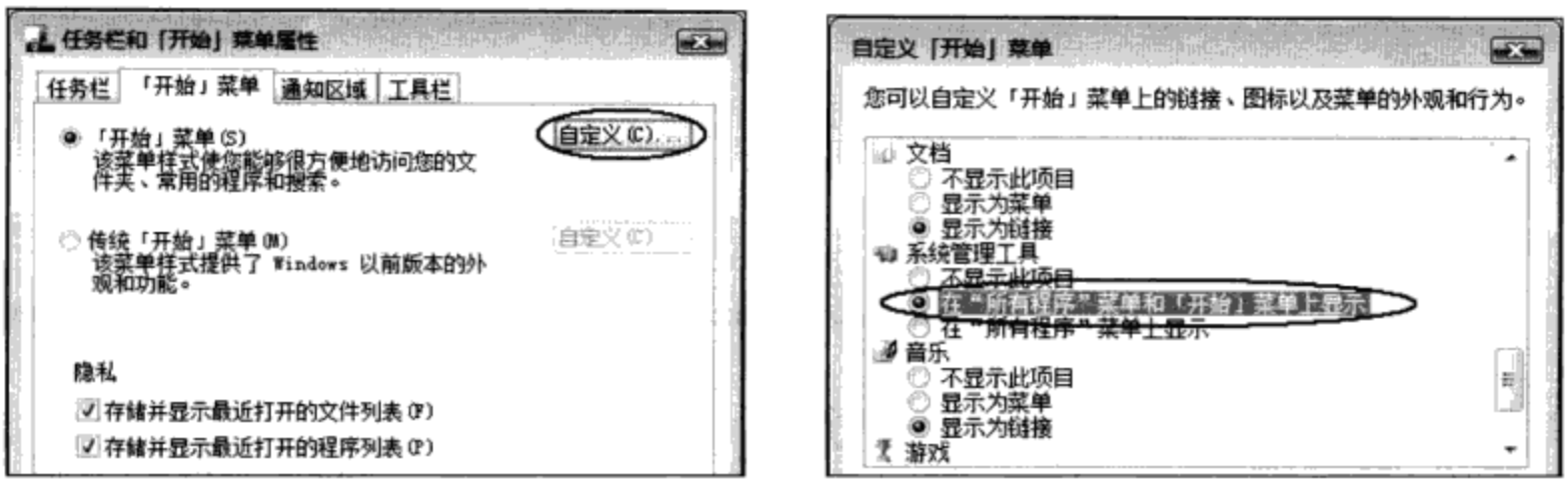


图 1-22

提示

您可以通过Windows Server 2008 R2 Hyper-V所提供的虚拟机器来架构本书中所有的演练环境，如此只要准备一台实际的计算机就可以了。Windows Server 2008 R2 Hyper-V的详细说明可参考笔者这一系列的《**Windows Server 2008 R2安装与管理**》这本书。