IX的核心是具有大量高速以太网[①]端口的二层交换机（图4.28）[②]。二层交换机的基本原理和一般交换机相同，大家可以认为IX的核心就是大型的、高速的交换机。

接下来就是将各个运营商的路由器连接到IX核心交换机上，连接方法有几种。首先，当运营商NOC和IX位于同一幢大楼里时，只要从NOC中将光纤延长出来接到IX交换机就可以了（图4.28①）。这种情况和公司、家庭网络中的路由器与交换机的连接方法是相同的。这种方法很简单，但如果NOC和IX不在同一幢大楼里又该怎么办呢？我们可以用通信线路将路由器和交换机连起来。这种情况下有两种连法，一种是从路由器延伸出一根通信线路并连接到IX交换机上（图4.28②），另一种是将路由器搬到IX机房里，用通信线路将路由器和NOC连起来，再将路由器连到IX交换机上（图4.28③）。

以前IX交换机都是放在一个地方的，也就是呈点状分布的。现在这些点状设施已经逐步扩张，在数据中心等网络流量集中的地方一般都会设置IX终端交换机，各运营商的路由器在这里连接到终端交换机上（图4.28④）。IX已经从点扩张到线，甚至到面了。

下面我们来看一看网络包具体是如何传输的。其实这里并没有什么特别需要解释的，因为IX的交换机和一般的交换机在工作方式上没有区别，路由器发送网络包时，先通过ARP查询下一个路由器的MAC地址，然后将其写入MAC头部发送出去即可。只要填写了正确的MAC地址，就可以向任何运营商的路由器发送包。不过实际上，要成功发送包还需要正确的路由信息，对于没有进行路由交换的运营商，我们是无法向其发送包的。这需要运营商之间通过谈判签订合约，然后按照合约来交换路由信息，实现网络包的收发。

运营商之间可以直接连接，也可以通过IX连接，无论是哪种方式，

① 现在使用的是10 Gbit/s端口，如果将来出现更高速的以太网标准，在数据量大的地方应该就会升级到更高速的设备。

② 这种方式称为“二层方式”，在日本是主流方式，当然，也有采用其他方式的IX。

最终网络包都会到达服务器所在的运营商，然后通过 POP 进入服务器端的网络。后面的内容我们下一章继续讲。

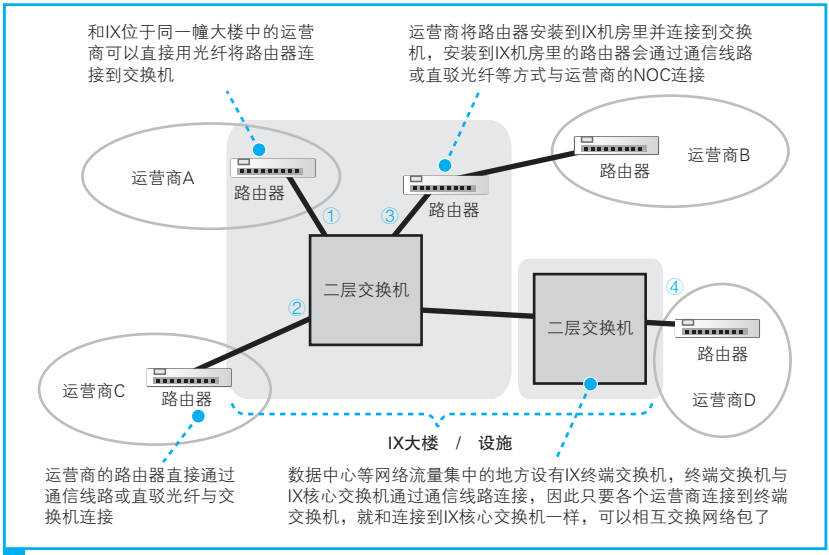



图 4.28 IX 的实体是高性能交换机

## 小测验

本章的旅程告一段落，我们为大家准备了一些小测验题目，确认一下自己的成果吧。

### 问题

1. 什么是接入网？
2. 要使用 ADSL 服务，需要安装一个将电话信号和 ADSL 信号分开的设备，这个设备叫什么名字？
3. 和电话局距离越远，ADSL 的通信速率越低，为什么？
4. BAS（宽带接入服务器）与一般的路由器有什么不同？
5. 将多个运营商汇聚在一起相互连接的设备叫什么？

# Column
# 网络术语其实很简单

## 名字叫服务器，其实是路由器

**探索队员：**BAS 其实是路由器对吧？

**探索队长：**是呢，它也是路由器的一种。不过它有一些一般路由器没有的功能，算是加强版的路由器吧。

**队员：**可是，为什么它要叫服务器呢？

**队长：**你的关注点怎么总是这么奇怪？

**队员：**是吗？难道只有我觉得这个名字很怪吗？

**队长：**好吧好吧，其实 BAS 是从 RAS 发展而来的，一开始叫 B-RAS，意思是用于宽带网络的 RAS，后来缩略成了 BAS。

**队员：**RAS 也是路由器的一种吗？

**队长：**是啊。

**队员：**那 RAS 又为什么叫服务器呢？太奇怪了吧？

**队长：**其实也没什么可奇怪的。

**队员：**这话怎么说？

**队长：**以前和现在不一样，大部分情况下，RAS 是用一台服务器里面装上 RAS 软件来实现的，所以叫服务器是很正常的。

**队员：**咦？服务器也可以当路由器来用吗？

**队长：**这有什么大惊小怪的，只要有相应的软件，计算机什么都能干。

**队员：**这么说好像挺有道理的。

**队长：**所以说，只要安装了路由器软件，计算机也可以当路由器来用。

**队员：**原来是这样啊。

**队长：**其实以前的路由器也不是专门的设备，都是在计算机上安装相应的软件当成路由器来用的。

**队员：**真的吗？

**队长：**当然。现在的计算机也可以当路由器用哦。Linux 等 UNIX 系操作系统都内置了路由功能，Windows Server 版本也具有路由功能。

**队员：**这样啊，学到了。

**队长：**不过，以前和现在不一样，以

前的计算机可是很贵的，最少也要几百万日元，高性能的型号要几亿日元呢。

**队员：**好像听说过这事。

**队长：**这么贵的东西，只是拿来转发网络包，未免太浪费了对吧。

**队员：**我还以为转发网络包是个很复杂的工作呢。

**队长：**不不，跟数据库、业务系统相比，转发包算是简单的工作了。

**队员：**这样啊。

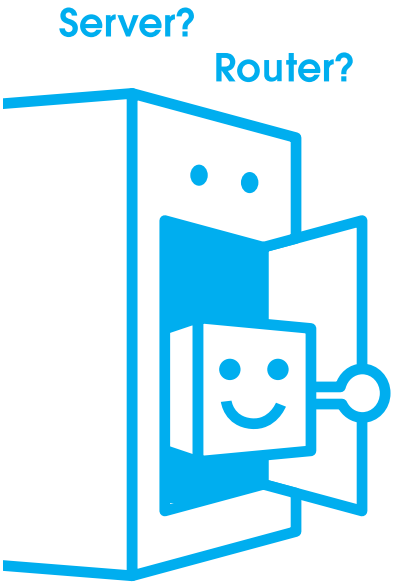
**队长：**是啊，让昂贵的计算机做这么简单的事太浪费了，有人就想，如果设计一种专用设备，是不是能节省成本呢？于是就有了路由器。

**队员：**原来是这样啊。

**队长：**不过，这是以前的事了，现在情况又不一样了。现在使用专用硬件不是为了降低成本，而是为了提高性能。

**队员：**这话怎么说？

**队长：**计算机需要用软件来处理网络包的转发对吧？




**队员：**是啊。

**队长：**专用硬件可以通过芯片实现非常快速的处理，因此性能更好。

**队员：**原来如此。

**小测验答案**

1. 用于连接网络运营商的线路（参见【4.1.2】）
2. 分离器（参见【4.2.4】）
3. 因为离电话局越远，信号越弱（参见【4.2.3】）
4. BAS 具有身份认证、向客户端下发 IP 地址等配置信息的功能（参见【4.3.1】）
5. IX（Internet eXchange，互联网交换中心）（参见【4.4.4】）

# 第5章 服务器端的局域网中有什么玄机

## 热身问答

在开始探索之旅之前，我们准备了一些和本章内容有关的小题目，请大家先试试看。

这些题目是否答得出来并不影响接下来的探索之旅，因此请大家放轻松。


下列说法是正确的（√）还是错误的（×）？

1. 当使用浏览器访问 Web 服务器时，浏览器的通信对象不仅限于 Web 服务器。
2. 没有防火墙就不能连接到互联网。
3. 也有防火墙无法抵御的攻击。

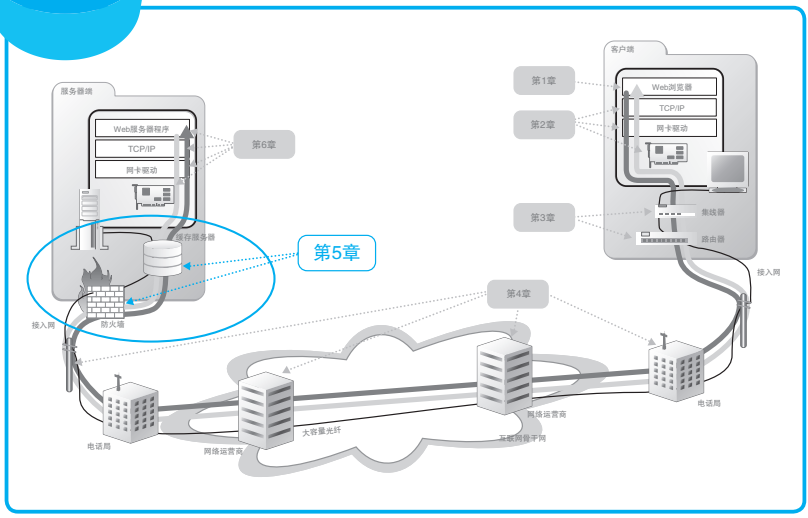
## 答案

1. √。浏览器有时候是和 Web 服务器通信，有时候是和缓存服务器以及负载均衡器等进行通信。
2. ×。防火墙并不是必需的，但是没有防火墙会增加风险。
3. √。防火墙不会检查通信数据的具体内容，因此无法抵御隐藏在通信数据内容中的攻击。

## 前情提要

上一章，我们探索了网络包在进入互联网之后，通过通信线路和运营商网络到达服务器 POP 端的过程。接下来，网络包将继续朝服务器前进，并通过服务器前面的防火墙、缓存服务器、负载均衡器等。本章我们将对这一部分进行探索。

## 探索之旅的看点




### (1) Web 服务器的部署地点

客户端计算机一般都放在家庭、公司网络上，但服务器的部署不仅限于家庭和公司中。那么服务器到底放在哪里呢？这是我们的第一个看点。

### (2) 防火墙的结构和原理

一般在 Web 服务器前面都会部署防火墙，那么防火墙是通过怎样的机制保护服务器的呢？这是我们的第二个看点。

### （3）通过将请求平均分配给多台服务器来平衡负载

随着访问量的增加，Web 服务器的处理能力会不够用，对于访问量很大的大型网站来说，必须要考虑到这一点。如何应对这个问题，也是我们的看点之一。有很多方案可以应对这个问题，我们先介绍其中一种方法，即通过多台 Web 服务器来分担负载。

### （4）利用缓存服务器分担负载

另一种减轻 Web 服务器负担的方法是将访问过的数据保存在缓存服务器中，当再次访问时直接使用缓存的数据。除了在服务器端部署缓存服务器之外，在客户端也可以部署缓存服务器，缓存服务器有各种用法，这也是我们的看点之一。

### （5）内容分发服务

内容分发服务是从缓存服务器发展而来的，它在互联网中部署很多缓存服务器，并将用户的访问引导到最近的缓存服务器上。那么如何才能找到离用户最近的缓存服务器呢？如何将用户的访问引导到这台服务器上呢？内容分发服务的结构还是非常耐人寻味的。

# 5.1 Web 服务器的部署地点

## 5.1.1 在公司里部署 Web 服务器

网络包从互联网到达服务器的过程，根据服务器部署地点的不同而不同。最简单的是图 5.1（a）中的这种情况，服务器直接部署在公司网络上，并且可以从互联网直接访问。这种情况下，网络包通过最近的 POP 中的路由器、接入网以及服务器端路由器之后，就直接到达了服务器。其中，路由器的包转发操作，以及接入网和局域网中包的传输过程都和我们之前讲过的内容没有区别[①]。

以前这样的服务器部署方式很常见，但现在已经不是主流方式了。这里有几个原因。第一个原因是 IP 地址不足。这样的方式需要为公司网络中的所有设备，包括服务器和客户端计算机，都分配各自的公有地址。然而现在公有地址已经不够用了，因此采用这种方式已经不现实了。

另一个原因是安全问题。这种方式中，从互联网传来的网络包会无节制地进入服务器，这意味着服务器在攻击者看来处于“裸奔”状态。当然，我们可以强化服务器本身的防御来抵挡攻击，这样可以一定程度上降低风险。但是，任何设置失误都会产生安全漏洞，而裸奔状态的服务器，其安全漏洞也都会暴露出来。人工方式总会出错，安全漏洞很难完全消除，因此让服务器裸奔并不是一个稳妥的办法。

因此，现在我们一般采用图 5.1（b）中的方式，即部署防火墙[②]。防火墙的作用类似于海关，它只允许发往指定服务器的指定应用程序的网络包通过，从而屏蔽其他不允许通过的包。这样一来，即便应用程序存在安全漏

① 路由器的包转发参见第 3 章，接入网参见第 4 章，局域网参见第 3 章。

② 防火墙：一种抵御外部网络攻击的机制，也是最早出现的一种防御机制。现在已经出现了很多可以绕过防火墙的攻击方法，因此防火墙一般需要和反病毒、非法入侵检测、访问隔离等机制并用。我们将在 5.2 节详细介绍。

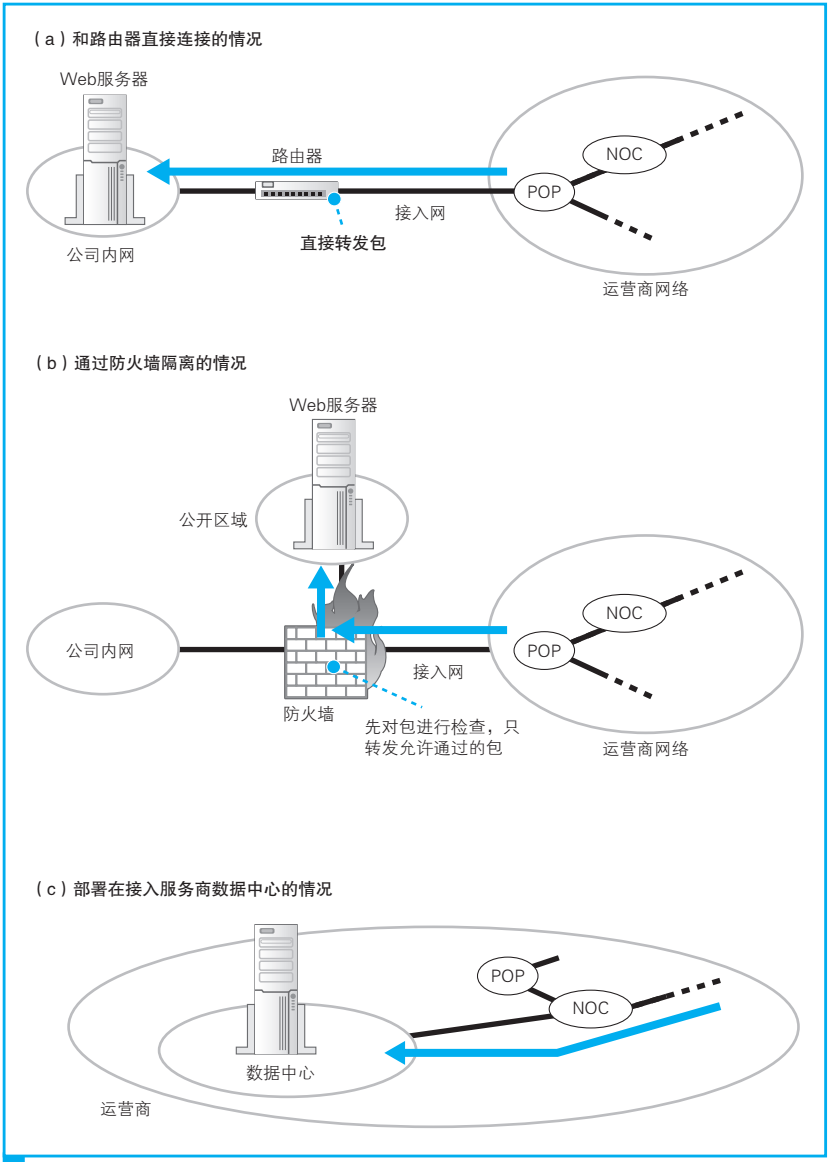

（a）和路由器直接连接的情况
Web服务器
路由器
NOC
POP
接入网
直接转发包
公司内网
运营商网络
（b）通过防火墙隔离的情况
Web服务器
公开区域
公司内网
NOC
POP
接入网
防火墙
先对包进行检查，只
转发允许通过的包
运营商网络
（c）部署在接入服务商数据中心的情况
POP
NOC
数据中心
运营商

图 5.1　服务器的所在地

洞，也可以降低相应的风险。因为防火墙屏蔽了不允许从外部访问的应用程序，所以即便这些程序存在安全漏洞，用于攻击的网络包也进不来[①]。当然，即便如此风险也不会降到零，因为如果允许外部访问的应用程序中有安全漏洞，还是有可能遭到攻击的[②]，但怎么说也远比完全暴露安全漏洞的风险要低得多。这就是防火墙的作用。

### 5.1.2 将 Web 服务器部署在数据中心

图 5.1（a）和图 5.1（b）都是将 Web 服务器部署在公司里，但 Web 服务器不仅可以部署在公司里，也可以像图 5.1（c）这样把服务器放在网络运营商等管理的数据中心里，或者直接租用运营商提供的服务器。

数据中心是与运营商核心部分 NOC 直接连接的，或者是与运营商之间的枢纽 IX 直接连接的。换句话说，数据中心通过高速线路直接连接到互联网的核心部分，因此将服务器部署在这里可以获得很高的访问速度[③]，当服务器访问量很大时这是非常有效的。此外，数据中心一般位于具有抗震结构的大楼内，还具有自主发电设备，并实行 24 小时门禁管理，可以说比放在公司里具有更高的安全性。此外，数据中心不但提供安放服务器的场地，还提供各种附加服务，如服务器工作状态监控、防火墙的配置和运营、非法入侵监控等，从这一点来看，其安全性也更高。

如果 Web 服务器部署在数据中心里，那么网络包会从互联网核心部分直接进入数据中心，然后到达服务器。如果数据中心有防火墙，则网络包会先接受防火墙的检查，放行之后再到达服务器。无论如何，网络包通过

① 在设计防火墙机制的那个年代，还没有特别恶劣的攻击方式，因此只要服务器管理员正确配置应用程序，就可以防止出现漏洞。当时的设计思路就是对于允许外部访问的应用程序进行正确配置，防止出现漏洞，而对于其他应用程序则用防火墙来进行屏蔽保护。

② 因此管理员必须注意两点：1. 更新应用程序修补安全漏洞；2. 正确配置应用程序避免出现漏洞。

③ 将服务器部署在公司里时，只要提高接入网的带宽，就可以让访问速度变得更快。

路由器的层层转发，最终到达服务器的这个过程都是相同的。

## 5.2 防火墙的结构和原理

### 5.2.1 主流的包过滤方式

无论服务器部署在哪里，现在一般都会在前面部署一个防火墙，如果包无法通过防火墙，就无法到达服务器。因此，让我们先来探索一下包是如何通过防火墙的。

防火墙的基本思路刚才已经介绍过了，即只允许发往特定服务器中的特定应用程序的包通过，然后屏蔽其他的包。不过，特定服务器上的特定应用程序这个规则看起来不复杂，但网络中流动着很多各种各样的包，如何才能从这些包中分辨出哪些可以通过，哪些不能通过呢？为此，人们设计了多种方式[①]，其中任何一种方式都可以实现防火墙的目的，但出于性能、价格、易用性等因素，现在最为普及的是包过滤方式。因此，我们的探险之旅就集中介绍一下包过滤方式的防火墙是怎样工作的。

### 5.2.2 如何设置包过滤的规则

网络包的头部包含了用于控制通信操作的控制信息，只要检查这些信息，就可以获得很多有用的内容。这些头部信息中，经常用于设置包过滤规则的字段如表 5.1 所示。不过，光看这张表还是难以理解过滤规则是如何设置的，所以我们来看一个具体的例子[②]。

① 防火墙可分为包过滤、应用层网关、电路层网关等几种方式。

② 要理解包过滤的设置需要深入理解包是如何在网络中传输的，这些内容在第 2 章有详细的讲解，请大家复习一下。

表 5.1 地址转换和包过滤中用于设置规则的字段

| 头部类型 | 规则判断条件 | 含义 | |
|---|---|---|---|
| MAC 头部 | 发送方 MAC 地址 | 路由器在对包进行转发时会改写 MAC 地址，将转发目标路由器的 MAC 地址设为接收方 MAC 地址，将自己的 MAC 地址设为发送方 MAC 地址。通过发送方 MAC 地址，可以知道上一个转发路由器的 MAC 地址 | |
| IP 头部 | 发送方 IP 地址 | 发送该包的原始设备的 IP 地址。如果要以发送设备来设置规则，需要使用这个字段 | |
| | 接收方 IP 地址 | 包的目的地 IP 地址，如果要以包的目的地来设置规则，需要使用这个字段 | |
| | 协议号 | TCP/IP 协议为每个协议分配了一个编号，如果要以协议类型来设置规则，需要使用这个编号。主要的协议号包括 IP：0；ICMP：1；TCP：6；UDP：17；OSPF：89 | |
| TCP 头部或 UDP 头部 | 发送方端口号 | 发送该包的程序对应的端口号。服务器程序对应的端口号是固定的，因此根据服务器返回的包的端口号可以分辨是哪个程序发送的。不过，客户端程序的端口号大多是随机分配的，难以判断其来源，因此很少使用客户端发送的包的端口号来设置过滤规则 | |
| | 接收方端口号 | 包的目的地程序对应的端口号。和发送方端口号一样，一般使用服务器的端口号来设置规则，很少使用客户端的端口号 | |
| | TCP 控制位 | TCP 协议的控制信息，主要用来控制连接操作 | |
| | | ACK | 表示接收数据序号字段有效，一般用于通知发送方数据已经正确接收 |
| | | PSH | 表示发送方应用程序希望不等待发送缓冲区填充完毕，立即发送这个包 |
| | | RST | 强制断开连接，用于异常中断 |
| | | SYN | 开始通信时连接操作中发送的第一个包中，SYN 为 1，ACK 为 0。如果能够过滤这样的包，则后面的操作都无法继续，可以屏蔽整个访问 |
| | | FIN | 表示断开连接 |
| | 分片 | 通过 IP 协议的分片功能拆分后的包，从第二个分片开始会设置该字段 | |

（续）

| 头部类型 | 规则判断条件 | 含　义 | |
|---|---|---|---|
| ICMP 消息（非头部）的内容 | ICMP 消息类型 | ICMP 消息用于通知包传输过程中产生的错误，或者用来确认通信对象的工作状态。ICMP 消息主要包括以下类型，这些类型可以用来设置过滤规则 | |
| | | 0 | 针对 ping 命令发送的 ICMP echo 消息的响应。将这种类型的消息和下面的类型 8 消息屏蔽后，ping 命令就没有响应了。一般在发动攻击之前会通过 ping 命令查询网络中有哪些设备，如果屏蔽 0 和 8，就不会响应 ping 命令，攻击者也就无法获取网络中的信息了。不过，ping 命令也可以用来查询设备是否在正常工作，如果屏蔽了 0 和 8 的消息，可能别人会误以为设备没有在工作 |
| | | 8 | 这个类型的消息叫作 ICMP echo，当执行 ping 命令时，就会发送 ICMP echo 消息 |
| | | 其他 | ICMP 消息除了 0 和 8 以外还有其他一些类型，但其中有些消息被屏蔽后会导致网络故障，因此如果要屏蔽 0 和 8 以外的消息必须十分谨慎 |

假设我们的网络如图 5.2 所示，将开放给外网的服务器和公司内网分开部署，Web 服务器所在的网络可以从外网直接访问。现在我们希望允许从互联网访问 Web 服务器（图 5.2 ①），但禁止 Web 服务器访问互联网（图 5.2 ②）。以前很少禁止 Web 服务器访问互联网，但现在出现了一些寄生在服务器中感染其他服务器的恶意软件，如果阻止 Web 服务器访问互联网，就可以防止其他服务器被感染。要实现这样的要求，应该如何设置包过滤的规则呢？我们就用这个例子来看一看包过滤的具体思路。

在设置包过滤规则时，首先要观察包是如何流动的。通过接收方 IP 地址和发送方 IP 地址，我们可以判断出包的起点和终点。在图 5.2 ①的例子中，包从互联网流向 Web 服务器，从互联网发送过来的包其起点是不确定的，但终点是确定的，即 Web 服务器。因此，我们可以按此来设定规则，允许符合规则的包通过。也就是说，允许起点（发送方 IP 地址）为任意，