 有台Cisco 2600，平时般用作互联网服务器。现在希望可以屏蔽某些特定网站，该怎么做呢？ 这不是个困难任务只要您知道Cisco IOS如何工作的。这里将指导您进行这项工作，并告诉您使这种方式应当注意些什么 。 步骤1：配置个DNS服务器 假设我们打算屏蔽个名www.badsite.com网站。我们并不知道该网站具体IP地址，而且们也不想知道。没问题Cisco IOS自己把地址找出并填上它。 要做到这点，们需至少在路由器上配置一台DNS服务器。若想配置一台DNS服务器，应使ip name-server命令。下面个例子： Router(config)# ip name-server 1.1.1.1 2.2.2.2 本例中，我们配置一个主DNS服务器1.1.1.1，以及个备DNS服务器2.2.2.2，以便路由器对域名进行解析。这不会影响路由器任何流量 。当我们需对某个域名进行Ping服务时，路由器将使用这些DNS服务器。以下是具体示例： Router# ping www.techrepublic.com Translating "www.techrepublic.com"...do main server (1.1.1.1) [OK] Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 216.239.113.101, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms Router# 在上述例子中，路由器使用了我们指定的域名服务器地址（1.1.1.1）来尝试解析域名。它成功的将域名www.techrepublic.com解析为对应IP 216.239.113.101。 如果我们不曾指定DNS服务器，那么路由器很可能返回下述这些反馈： Translating "www.techrepublic.com"...do main server

(255.255.255.255) % Unrecognized host or address, or protocol not running.（不认识主机或地址，或可能协议未运行） 步骤2：建立ACL 想真正阻止访问某个网站，我们必须建立一个存取控制列表（access control list，简称ACL）来具体定义们想阻止什么。下面举个例子： Router(config)# access-list 101 deny tcp any hostwww.badsite.com eq www Translating "www.badsite.com"...do main server (1.1.1.1) [OK] Router(config)# access-list 101 permit tcp any any eq www ! to allow all other web traffic 这个ACL拒绝了所有对特定网站www.badsite.com访问。在阻止访问该网站同时，它允许所有人访问其他任意网站。最后，由于ACL的隐含禁止，除WWW外所有其通信将全部被禁止。 如果您想知道到底哪些IP地址试图访问被阻止的网站，可以通过使LOG关键字，记录相关信息。下面是一个例子。 Router(config)# access-list 101 deny tcp any host www.badsite.com eq www log 步骤3：避免“ 遗漏 ”有一点需注意。们输入述ACL第一行后，留意路由器是如何使用DNS服务器来解析域名。然后它会用解析域名所得的IP地址替换掉ACL主机名。我们仔细看看配置： Router# sh run | inc access-list 101 access-list 101 deny tcp any host 66.116.109.62 eq www 这是个很好的功能，但是可能由于几个原因导致出现问题。首先，该IP仅仅是DNS服务器响应的第一个IP。如果这个大型网站，有多台服务器 （比如一个搜索引擎），而ACL却仅仅包含了DNS首先响应第一个IP您不得不手工屏蔽其余IP地址。下面是一个示例： C: 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com