技术经验：访问控制列表 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/462/2021_2022__E6_8A_80_E6_9C_AF_E7_BB_8F_E9_c101_462126.htm 简介：CISCO路由器中的access-list（访问列表）最基本的有两种，分别是标准访问列表和扩展访问列表，二者的区别主要是前者是基于目标地址的数据包过滤，而后者是基于目标地址、源地址和网络协议及其端口的数据包过滤... CISCO路由器中的access-list（访问列表）最基本的有两种，分别是标准访问列表和扩展访问列表，二者的区别主要是前者是基于目标地址的数据包过滤，而后者是基于目标地址、源地址和网络协议及其端口的数据包过滤。 （1）标准型IP访问列表的格式 标准型IP访问列表的格式如下： access-list[list number][permit |deny][source address] [address][wildcard mask][log] 下面解释一下标准型IP访问列表的关键字和参数。首先，在access和list这2个关键字之间必须有一个连字符"-"；其次，list number的范围在0～99之间，这表明该access-list语句是一个普通的标准型IP访问列表语句。因为对于Cisco IOS，在0～99之间的数字指示出该访问列表和IP协议有关，所以list number参数具有双重功能：（1）定义访问列表的操作协议；（2）通知IOS在处理access-list语句时，把相同的list number参数作为同一实体对待。正如本文在后面所讨论的，扩展型IP访问列表也是通过list number（范围是100～199之间的数字）而表现其特点的。因此，当运用访问列表时，还需要补充如下重要的规则：在需要创建访问列表的时候，需要选择适当的list number参数。 （2）允许/拒绝数据包通过 在标准型IP访问列表中，使

用permit语句可以使得和访问列表项目匹配的数据包通过接口，而deny语句可以在接口过滤掉和访问列表项目匹配的数据包。source address代表主机的IP地址，利用不同掩码的组合可以指定主机。 为了更好地了解IP地址和通配符掩码的作用，这里举一个例子。假设您的公司有一个分支机构，其IP地址为C类的192.46.28.0。在您的公司，每个分支机构都需要通过总部的路由器访问Internet。要实现这点，您就可以使用一个通配符掩码 0.0.0.255。因为C类IP地址的最后一组数字代表主机，把它们都置1即允许总部访问网络上的每一台主机.因此，您的标准型IP访问列表中的access-list语句如下： access-list 1 permit 192.46.28.0 0.0.0.255 注意，通配符掩码是子网掩码的补充。因此，如果您是网络高手，您可以先确定子网掩码，然后把它转换成可应用的通配符掩码。这里，又可以补充一条访问列表的规则5。 （3）指定地址 如果您想要指定一个特定的主机，可以增加一个通配符掩码0.0.0.0.例如，为了让来自IP地址为192.46.27.7的数据包通过，可以使用下列语句： Access-list 1 permit 192.46.27.7 0.0.0.0 在Cisco的访问列表中，用户除了使用上述的通配符掩码0.0.0.0来指定特定的主机外，还可以使用"host"这一关键字。例如，为了让来自IP地址为192.46.27.7的数据包通过，您可以使用下列语句： Access-list 1 permit host 192.46.27.7 除了可以利用关键字"host"来代表通配符掩码0.0.0.0外，关键字"any"可以作为源地址的缩写，并代表通配符掩码0.0.0.0 255.255.255.255。例如，如果希望拒绝来自IP地址为192.46.27.8的站点的数据包，可以在访问列表中增加以下语句： Access-list 1 deny host 192.46.27.8 Access-list 1 permit any 注意上述2条访问列表语句的次序。第1

条语句把来自源地址为192.46.27.8的数据包过滤掉，第2条语句则允许来自任何源地址的数据包通过访问列表作用的接口。如果改变上述语句的次序，那么访问列表将不能够阻止来自源地址为192.46.27.8的数据包通过接口。因为访问列表是按从上到下的次序执行语句的。这样，如果第1条语句是：Access-list 1 permit any 的话，那么来自任何源地址的数据包都会通过接口。（4）拒绝的奥秘 在默认情况下，除非明确规定允许通过，访问列表总是阻止或拒绝一切数据包的通过，即实际上在每个访问列表的最后，都隐含有一条"deny any"的语句。假设我们使用了前面创建的标准IP访问列表，从路由器的角度来看，这条语句的实际内容如下：