详解加实例思科访问列表全接触 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/251/2021_2022__E8_AF_A6_E8_A7_A3_E5_8A_A0_E5_c101_251053.htm 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。 一、基本访问控制列表 （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： access-list 1 deny host 192.46.27.8 access-list 1 permit any access-list 1 deny any 在上述例子里面，由于访问列表中第2条语句明确允许任何数据包都通过，所以隐含的拒绝语句不起作用，但实际情况并不总是如此。例如，如果希望来自源地址为 192.46.27.8和192.46.27.12的数据包通过路由器的接口，同时阻止其他一切数据包通过，则访问列表的代码如下： access-list 1 permit host 192.46.27.8 access-list 1 permit host 192.46.27.12 注意，因为所有的访问列表会自动在最后包括该语句。 顺便讨论一下标准型IP访问列表的参数"log"，它起日志的作用。一旦访问列表作用于某个接口，那么包括关键字"log"的语句将记录那些满足访问列表中"permit"和"deny"条件的数据包。第一个通过接口并且和访问列表语句匹配的数据包将立即产生一个日志信息。后续的数据包根据记录日志的方式，或者在控制台上显示日志，或者在内存中记录日志。通过Cisco IOS的控制台命令可以选择记录日志方式。 二、扩展型IP访问列表 扩展型IP访问列表在数据包的过滤方面增加了不少功能和灵活性。除了可以基于源地址和目标地址过滤外，还可以根据协议、源端口和目的端口过滤，甚至可以利用各种选项过滤。这些选项能够对数据包中某些域的信息

进行读取和比较。扩展型IP访问列表的通用格式如下：access-list[list number][permit|deny] [protocol|protocol key word] [source address source-wildcard mask][source port] [destination address destination-wildcard mask] [destination port][log options] 和标准型IP访问列表类似，"list number"标志了访问列表的类型。数字100～199用于确定100个惟一的扩展型IP访问列表。"protocol"确定需要过滤的协议，其中包括IP、TCP、UDP和ICMP等等。 如果我们回顾一下数据包是如何形成的，我们就会了解为什么协议会影响数据包的过滤，尽管有时这样会产生副作用。图2表示了数据包的形成。请注意，应用数据通常有一个在传输层增加的前缀，它可以是TCP协议或UDP协议的头部，这样就增加了一个指示应用的端口标志。当数据流入协议栈之后，网络层再加上一个包含地址信息的IP协议的头部。 由于IP头部传送TCP、UDP、路由协议和ICMP协议，所以在访问列表的语句中，IP协议的级别比其他协议更为重要。但是，在有些应用中，您可能需要改变这种情况，您需要基于某个非IP协议进行过滤 为了更好地说明，下面列举2个扩展型IP访问列表的语句来说明。假设我们希望阻止TCP协议的流量访问IP地址为192.78.46.8的服务器，同时允许其他协议的流量访问该服务器。那么以下访问列表语句能满足这一要求吗？ access-list 101 permit host 192.78.46.8 access-list 101 deny host 192.78.46.12 回答是否定的。第一条语句允许所有的IP流量、同时包括TCP流量通过指定的主机地址。这样，第二条语句将不起任何作用。可是，如果改变上面2条语句的次序