

Anatomy Of An Access List

List No.	Rule	Pattern Definition						
access-list xxx (100-199)	permit or deny	IP or ICMP	Source IP address xxx.xxx.xxx.xxx	Source IP address mask xxx.xxx.xxx.xxx	Destination IP address xxx.xxx.xxx.xxx	Destination IP address mask xxx.xxx.xxx.xxx	eq=equal gt=greater than lt=less than neq=not equal	TCP or UDP destination port no.
		TCP or UDP		255=ignore 0=apply		255=ignore 0=apply		
1	2	3	4	5	6	7	8	9
<p>1) Every extended access list has a number from 100 to 199, which identifies the list in two places. When building the list, every line must be labeled with the same access list number. When you apply the list to an interface on the router, you must reference it by the same number. Version 11.2 of the IOS allows you to use a name for the list instead of a number.</p> <p>2) A permit or deny rule has to be applied to every line or statement on the list.</p> <p>3) If you are only filtering on IP address, you will specify IP (or ICMP for pings and trace routes) as the protocol. This means that only the IP address is considered for a match. If you are also filtering on UDP or TCP port, you must specify TCP or UDP.</p> <p>4) Every line in the list must have a source address.</p>		<p>5) Every IP source address in the list must have a mask. The mask lets you determine how much of the preceding IP address to apply to the filter. In most cases, you will simply want to put a 255 corresponding to every octet in the IP address that you want to ignore, and 0 for every octet that you want the packet match to apply to.</p> <p>6) Every line in the list must have a destination address.</p> <p>7) Every IP destination address in the list must have a mask. See 5 above.</p> <p>8) This applies to the TCP or UDP port that you are filtering on. In most cases, you will use the eq, which means equals. This gives you the ability to permit or deny TCP or UDP ports equal to the port specified. There are cases, however, where you will want to apply a range of port numbers, which is where the gt, greater than, or lt, less than, will come in handy.</p> <p>9) If you have defined the pattern as a TCP or UDP packet, you will have to have an associated port number.</p>						
<p>Required</p>		<p>Optional</p>						