Access Control Lists introduction

Written on by Puran S Rawat at PSR|Technosol

Access Control Lists are used to control traffic into and out of your network based on a given criteria. An ACL consists of a sequence of permit or deny statements that apply to network layer or upper layer protocols. Most often Access Control Lists are used for security reasons to filter traffic.

Access lists are aplied per interface as:

- Inbound ACL – where packets are processed before they are routed;
- Outbound ACL – packets are routed to outbound interface, and then processed by ACL;

Take note that ACLs do not act on packets that were originated from the router itself. At the end of every access list is an "implicit deny any" statement. Therefore, if a packet doesn't match any of the ACL statements, it is automatically denied.

Cisco ACLs can be of two types, standard and extended.

Standard ACLs

Standard ACLs enable you to permit or deny traffic from source IP addresses. The destination of the packet and the port doesn't matter.

Extended ACLs

Extended ACLs are more advanced and filter IP packets based on several criteria, for example, protocol type, source or destination IP address, source or destination of TCP or UDP ports.

Both ACLs types can be Numbered or Named (starting with Cisco IOS Release 11.2). In table below you can find what numbers are used for both IP ACLs types.

Numbers used by ACLs

Standard ACLs	1 to 99	1300 to 1999
Extended ACLs	100 to 199	2000 to 2699

That's all for time being, I hope you enjoyed this brief ACLs intro. Browse throughout this section to find out more about ACLs.