


IES ACL 应用及配置

ACL (Access Control List, 访问控制列表) 是用来实现流识别功能的。网络设备为了过滤报文, 需要配置一系列的匹配条件对报文进行分类, 这些条件可以是报文的源地址、目的地址、端口号等。

当设备的端口接收到报文后, 即根据当前端口上应用的 ACL 规则对报文的字段进行分析, 在识别出特定的报文之后, 根据预先设定的策略允许或禁止该报文通过。

 注意: IES 系列交换机只能对入端口报文进行规则匹配。

配置 ACL 规则

ACL 匹配顺序

一个 ACL 中可以包含多个规则, 而每个规则都指定不同的报文匹配选项, 当这些规则出现矛盾的时候, 设备将采用配置规则的先后顺序进行规则匹配, 既先配置先执行规则。

配置二层 ACL 规则

二层 ACL 根据报文的源 MAC 地址、目的 MAC 地址制定匹配规则, 对报文进行相应的分析处理。

配置步骤:

操作步骤	命令	功能
步骤1	<code>enable</code>	进入配置模式
步骤2	<code>config access-list service [enable/disable]</code>	ACL服务使能
步骤3	<code>access-list <1-5000> {permit deny} mac destination [<dst_mac> any] source [<src_mac> any]</code>	创建ACL并定义规则
步骤4	<code>show access-list <1-5000></code>	显示ACL列表信息

配置高级 ACL 规则

高级 ACL 可以使用报文的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性 (例如 TCP 或 UDP 的源端口、目的端口, TCP 标记等) 等信息来制定匹配规则


配置步骤:

操作步骤	命令	功能
步骤1	<code>enable</code>	进入配置模式
步骤2	<code>config access-list service [enable/disable]</code>	ACL服务使能
步骤3	<code>access-list <1-5000> {permit deny} {tcp udp ip icmp} dip [<A. B. C. D/M> any] dst-port [<0-65535> any] sip [<A. B. C. D/M> any] src-port [<0-65535> any]</code>	创建ACL并定义规则
步骤4	<code>show access-list <1-5000></code>	显示ACL列表信息

删除 ACL 规则

配置步骤:

操作步骤	命令	功能
步骤1	enable	进入配置模式
步骤2	no access-list <1-5000>	删除ACL规则
步骤3	show access-list <1-5000>	显示ACL列表信息

 注意: 已经绑定到端口的 acl 列表不能被取消, 需要先取消端口的绑定后再取消列表

ACL 规则绑定到端口

将 ACL 规则绑定到指定端口


配置步骤:

操作步骤	命令	功能
步骤1	enable	进入配置模式
步骤2	interface ethernet <port>	进入到指定端口
步骤3	access-list <1-5000>	将规则绑定到端口
步骤4	show access-list <1-5000>	显示ACL列表信息

将 ACL 规则绑定到所有端口

配置步骤:

操作步骤	命令	功能
步骤1	enable	进入配置模式
步骤2	access-list global <1-5000>	将规则绑定到所有端口
步骤3	show access-list <1-5000>	显示ACL列表信息

 注意: 已经绑定到其它端口的 acl 列表不能绑定到所有端口

配置案例

禁止指定源 IP 的报文通过

配置交换机 port1 端口, 禁止源 IP 为 10.10.10.1/24 的报文通过

操作步骤	命令
步骤1	进入配置模式 IES>enable
步骤2	使能ACL服务 IES(config)#config access-list service enable
步骤3	创建ACL, 禁止源IP为10.10.10.1/24的报文通过 IES(config)#access-list 1 deny ip dip any sip 10.10.10.1/24
步骤4	进入到port1端口模式 IES(config)#interface ethernet 1

步骤5	将ACL规则与端口绑定 IES(if-eth1)#access-list 1
步骤6	显示ACL列表信息 IES(if-eth1)#show access-list ===== Interface-Ethernet: 1 Access-list number bound: 1 Access-list index: 1 =====