

# ACL

## 层面

- 控制层面 ⊖ 路由
- 转发层面 ⊖ 数据

## 作用

- 过滤\抓取数据
- 动作 ⊖
  - 允许 ⊖ permit
  - 拒绝 ⊖ deny

## 数据

- 网络接口 ⊖
  - 收
  - 发
- 用户 ⊖
  - 下载 ⊖
    - 下行带宽
    - 宽带200m
  - 上传 ⊖ 上行带宽

## 类型

- 标准 ⊖ 只能匹配源地址
- 扩展 ⊖
  - SIP
  - DIP
  - sport
  - dport
  - 协议
  - ...

## 奇偶

- 正掩码 ⊖
  - 1代表唯一匹配
  - 0代表任意匹配
  - 必须连续
- 反掩码通配符 ⊖
  - 1代表任意匹配
  - 0代表唯一匹配
  - 不要求连续
- 172.16.10.0/24网段, 偶数不能访问114.114.114.114 其他都可以
- 匹配网段10.0/24 ⊖ 172.16.10.0 0.0.0.255
- 匹配网段10.0/24偶数 ⊖
  - 172.16.10.0 0.0.0.254
  - IP172.16.10.0000 0000
  - 反0.0.0. 1111 1110
  - 子主题
- 匹配网段10.0/24奇数 ⊖
  - 172.16.10.1 0.0.0.254
  - IP172.16.10.0000 0001
  - 反0.0.0. 1111 1110
  - 172.16.10.3 0.0.0.254
  - 子主题

## 配置

- config ⊖
  - ip access-list extended guolv
  - 10 permit ip 172.16.10.1 0.0.0.0 114.114.114.114 0.0.0.0
  - 20 deny ip host 172.16.10.2 host 114.114.114.114
  - 垫底策略 拒绝所有 ⊖ 思科
  - 垫底策略 允许所有 ⊖ 华为
  - ACL的配置的rule seq配置步进10
- 查看 ⊖ sh ip access-lists
- 调用 ⊖ 哪个接口 ⊖
  - 发
  - 收
- 测试