CEC中国电子 | MAIPU 迈普

路由器安全技术

课程目标

■熟练掌握ACL、NAT、DHCP协议原理

■熟练掌握上述协议配置应用及其使用场景

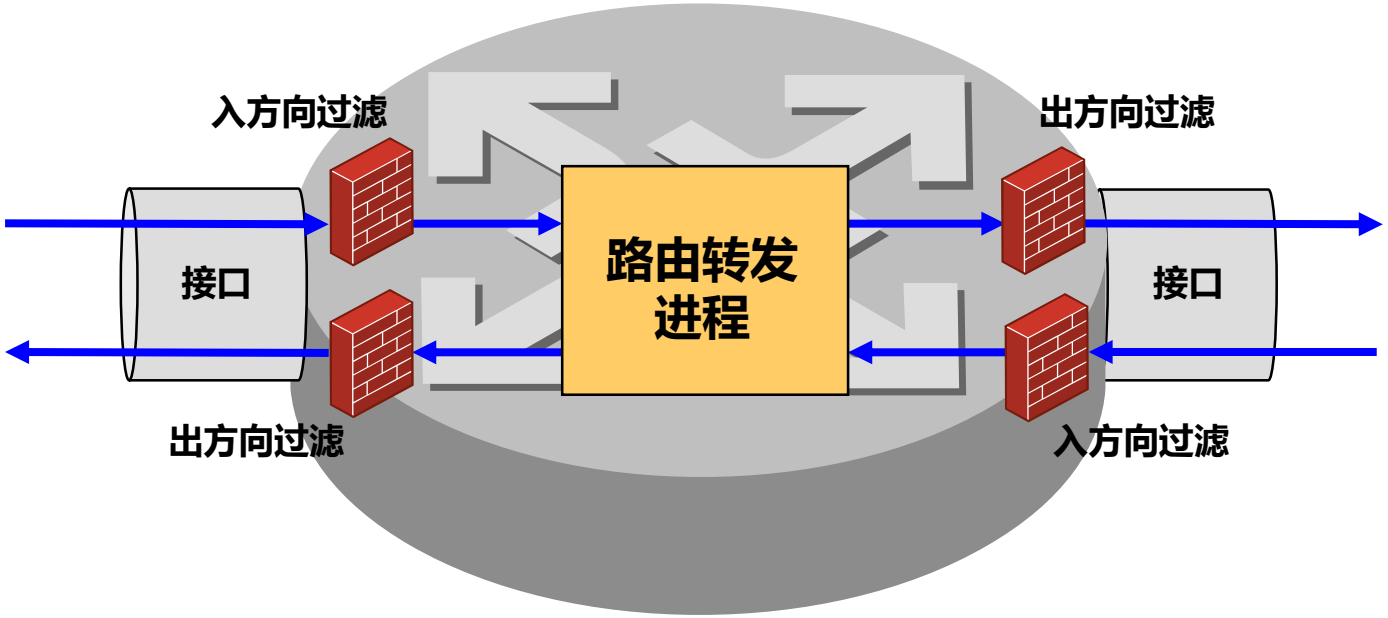
■掌握上述协议故障排查思路及方法

目录

ACL概述

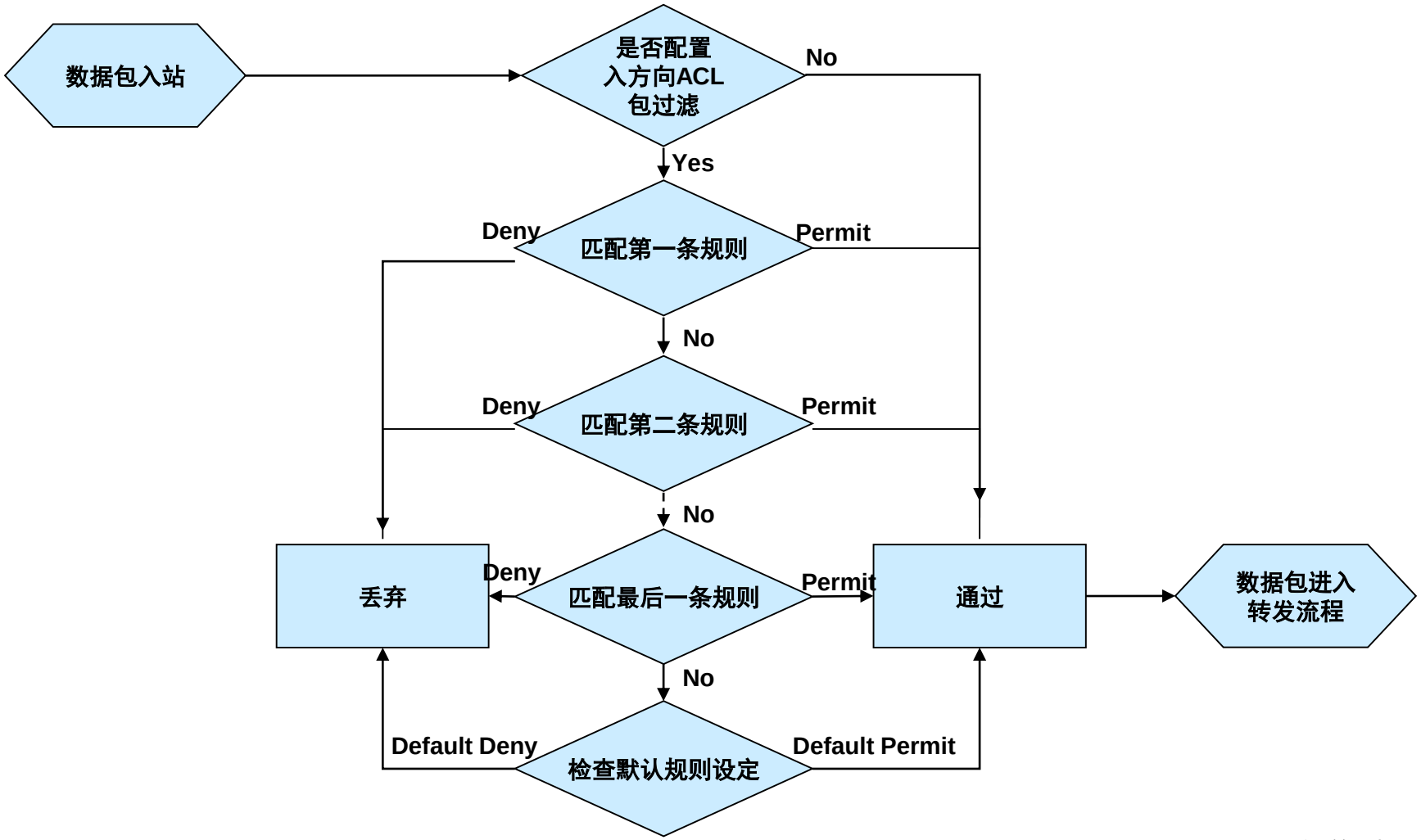
- **ACL（Access Control List，访问控制列表）是用来实现数据包识别功能的**
- **ACL可以应用于诸多方面**
  - 包过滤防火墙功能
  - NAT（Network Address Translation，网络地址转换）
  - 路由策略和过滤

基于ACL的包过滤技术

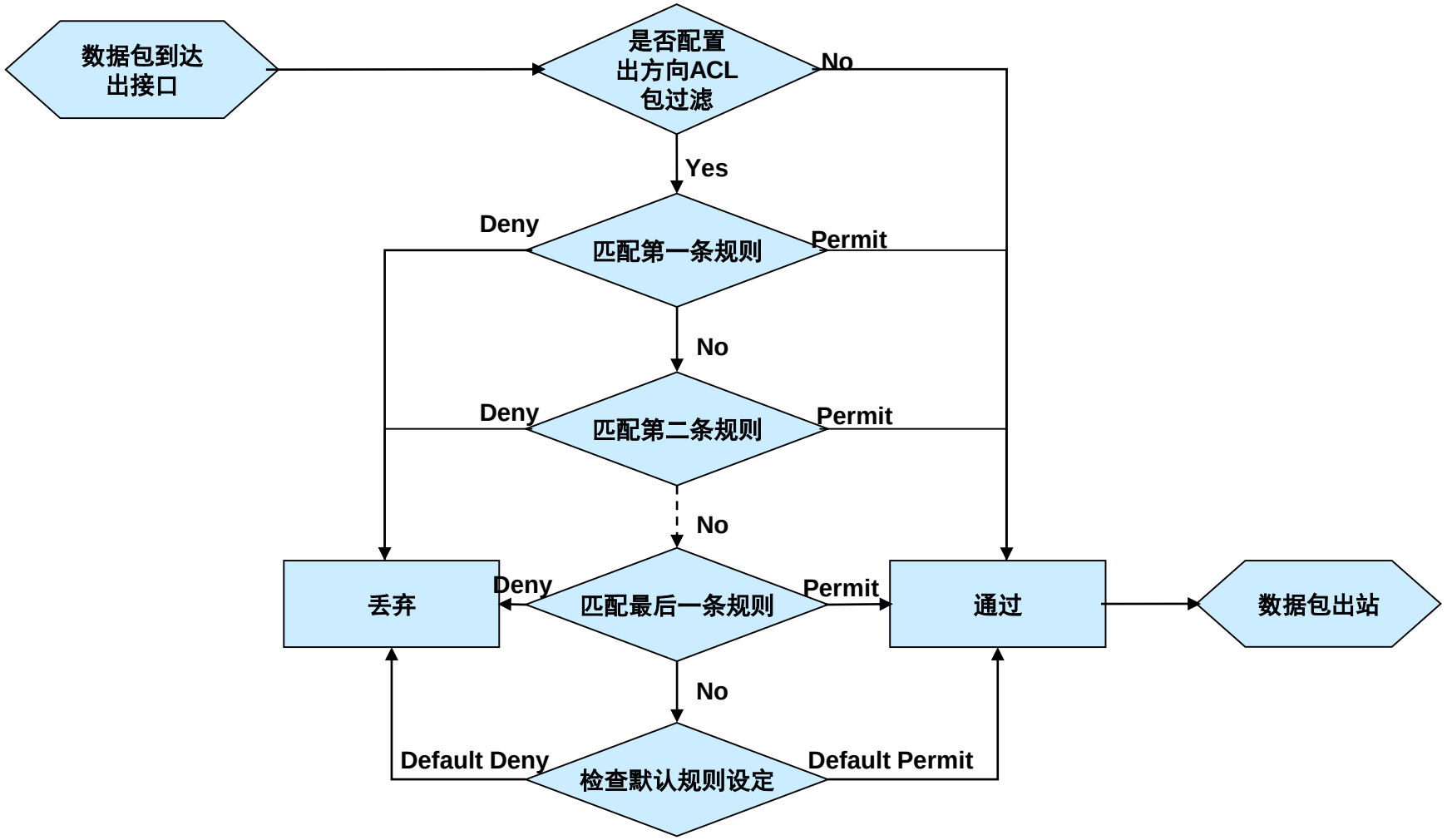


- 对进出的数据包逐个过滤，丢弃或允许通过
- ACL应用于接口上，每个接口的出入双向分别过滤
- 仅当数据包经过一个接口时，才能被此接口的此方向的ACL过滤
- 访问控制列表以IP包信息为基础，对IP源地址、IP目标地址、协议类型及各协议的字段（如：TCP、UDP的端口号，ICMP的类型、代码，IGMP的类型等）进行筛选；
- 访问列表根据过滤的内容可以分成2类，标准访问列表和扩展访问列表；

入站包过滤工作流程


数据包入站
是否配置
入方向ACL
包过滤
No
Yes
Deny
匹配第一条规则
Permit
No
Deny
匹配第二条规则
Permit
No
丢弃
Deny
匹配最后一条规则
Permit
通过
数据包进入
转发流程
No
Default Deny
检查默认规则设定
Default Permit

出站包过滤工作流程


数据包到达
出接口
是否配置
出方向ACL
包过滤
No
Yes
Deny
匹配第一条规则
Permit
No
Deny
匹配第二条规则
Permit
No
丢弃
Deny
匹配最后一条规则
Permit
通过
数据包出站
No
Default Deny
检查默认规则设定
Default Permit

通配符掩码

- 通配符掩码和IP地址结合使用以描述一个地址范围
- 通配符掩码和子网掩码相似，但含义不同
  - 0表示对应位须比较
  - 1表示对应位不比较

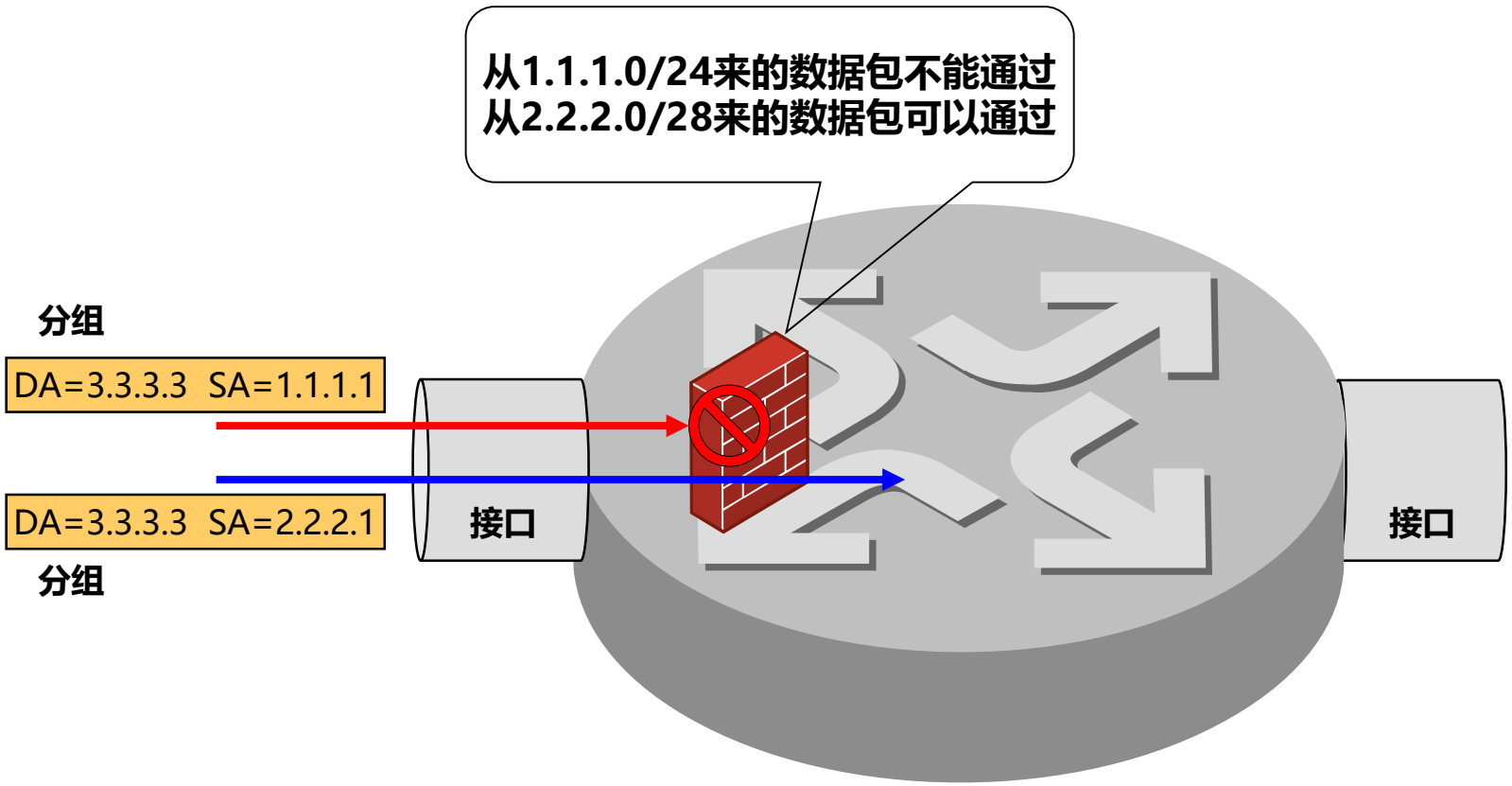
通配符掩码	含义
0.0.0.255	只比较前24位
0.0.3.255	只比较前22位
0.255.255.255	只比较前8位

通配符掩码的应用示例

IP地址	通配符掩码	表示的地址范围
192.168.0.1	0.0.0.255	192.168.0.0/24
192.168.0.1	0.0.3.255	192.168.0.0/22
192.168.0.1	0.255.255.255	192.0.0.0/8
192.168.0.1	0.0.0.0	192.168.0.1
192.168.0.1	255.255.255.255	0.0.0.0/0
192.168.0.1	0.0.2.255	192.168.0.0/24和192.168.2.0/24

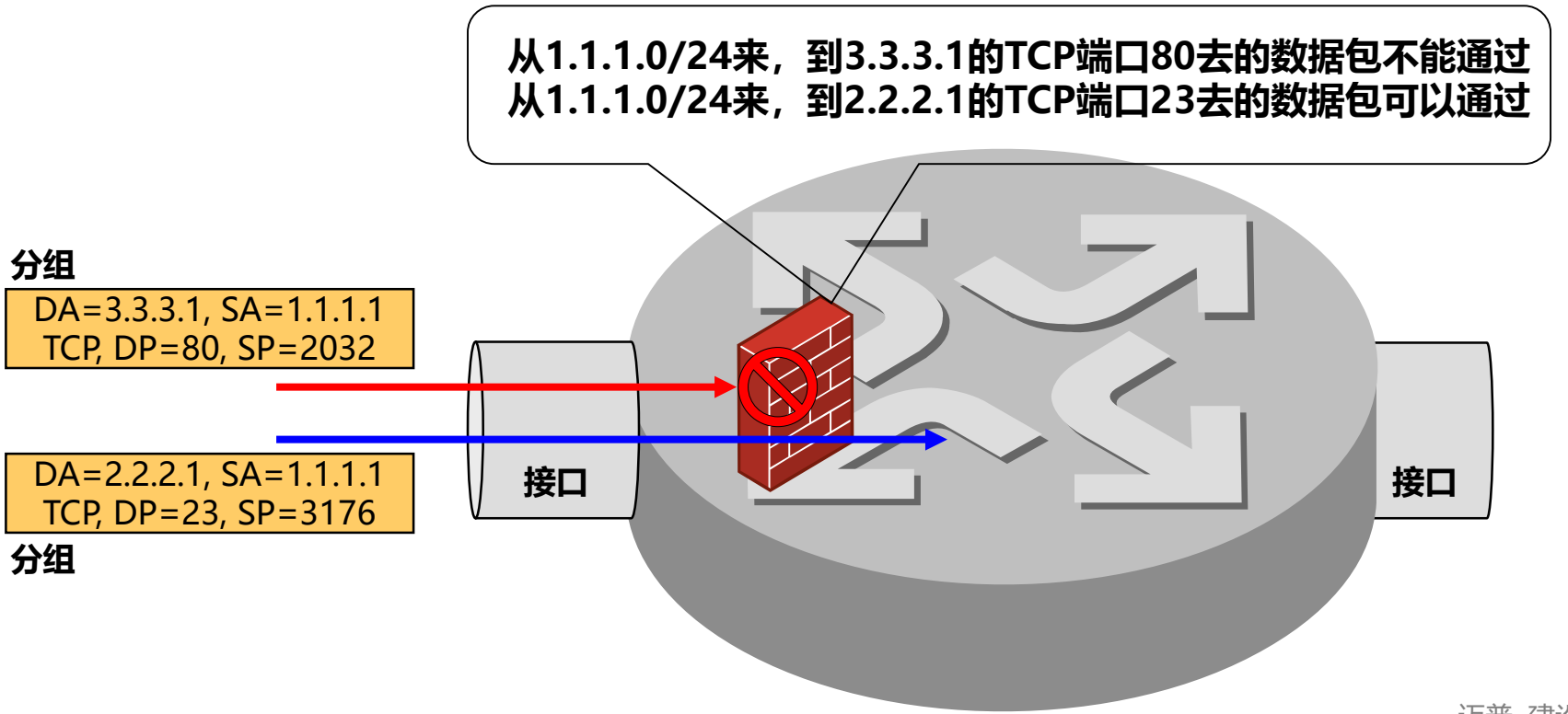
■ 基本访问控制列表

- 只根据报文的源IP地址信息制定规则



■ 高级访问控制列表

➢ 根据报文的源IP地址、目的IP地址、IP承载的协议类型、协议特性等三、四层信息制定规则



访问列表配置

■ 步骤一：创建访问列表

配置命令：ip access-list standard/extended list-num/list-name
【配置模式】全局配置模式。

语法	描述
standard	标准访问列表，仅解析数据包的源地址
extended	扩展访问列表，可解析数据包的源地址、目的地址、端口号等字段
list-num	访问列表编号，标准1-1000，扩展1001-2000
list-name	访问列表名称，支持字符命名

步骤二：定义访问列表条目

配置命令：permit/deny xxx
【配置模式】ACL配置模式

语法	描述
permit	允许条目
deny	拒绝条目 默认情况下ACL拒绝所有

■ 步骤三：接口上应用访问控制列表

- 若规则允许这个包，软件层面继续处理这个包；
- 若规则拒绝这个包，就会扔掉这个包，并向源地址发送ICMP管理状态不可达

语法：ip access-group list-num/list-name **in / out**

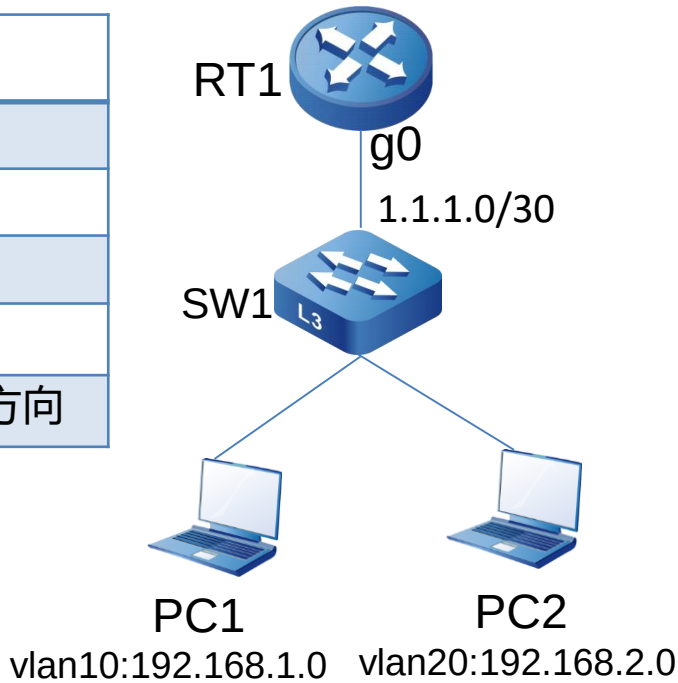
语法	描述
access-list-number	访问列表的编号，范围1-2000
access-list-name	访问列表的名称
in	过滤往内的包
out	过滤往出的包

访问列表配置实例-标准访问列表

■ 实例描述

如右图拓扑，vlan10能够访问RT1,vlan20不能访问RT1

命令	描述
RT1(config)#ip access-list standard 1	创建标准访问列表1
RT1(config-std-nacl)#deny 192.168.2.0 0.0.0.255	拒绝192.168.2.0/24网段
RT1(config-std-nacl)#permit any	允许所有网段
RT1(config)#interface g0	进入接口g0配置模式
RT1(config-if-fastethernet0/1)#ip access-list 1 in	将访问列表1应用于g0端口in方向



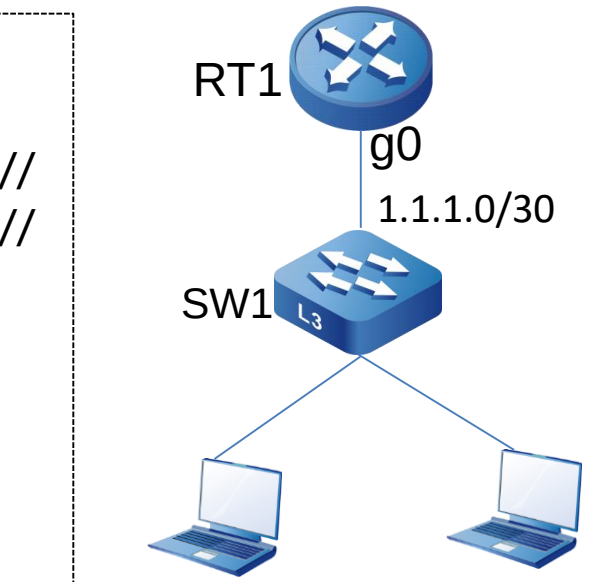
访问列表配置实例-扩展访问列表

■ 实例描述

如右图拓扑，vlan10与vlan20均能访问RT1,但vlan10与vlan20不能互访。

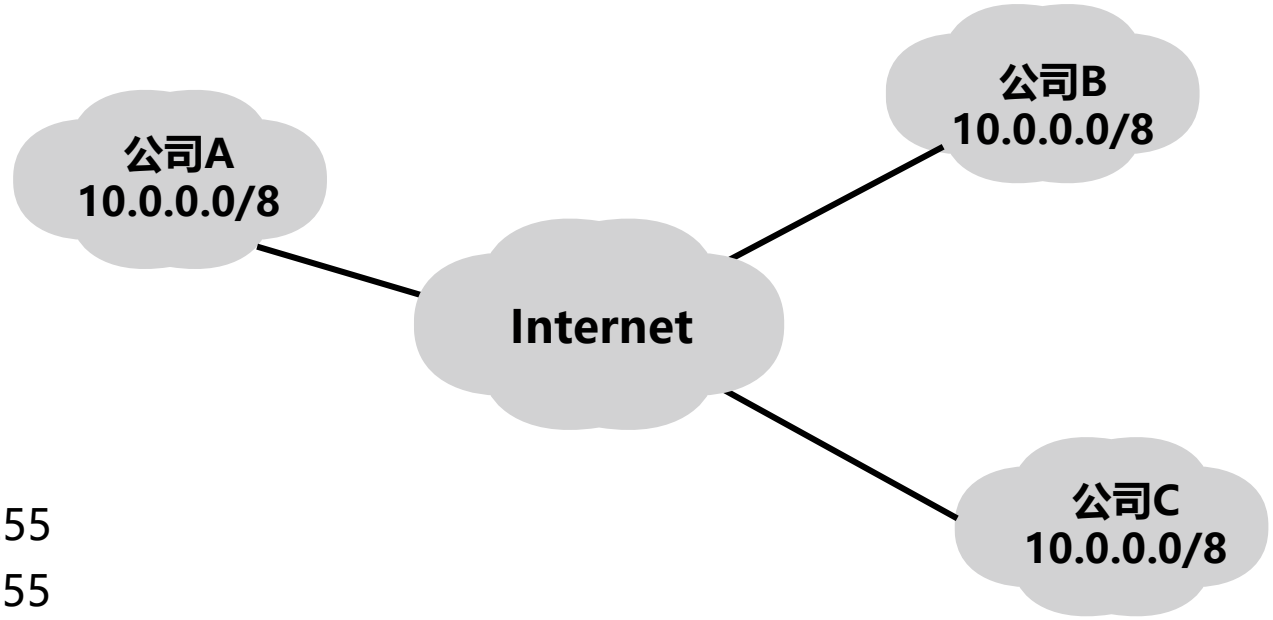
参考配置（**SW1)**

```
ip access-list extended 1001          //创建扩展访问列表1001//
deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255   //拒绝1.0网段访问2.0网段//
deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255   //拒绝2.0网段访问1.0网段//
permit ip any  any                    //允许所有到所有网段//
interface vlan 10                     //进入vlan10//
ip access-list 1001 in                //将扩展访问列表1001应用于vlan10 in方向//
interface vlan 20
ip access-list 1001 in
```



目录

公有地址和私有地址



私有地址范围：

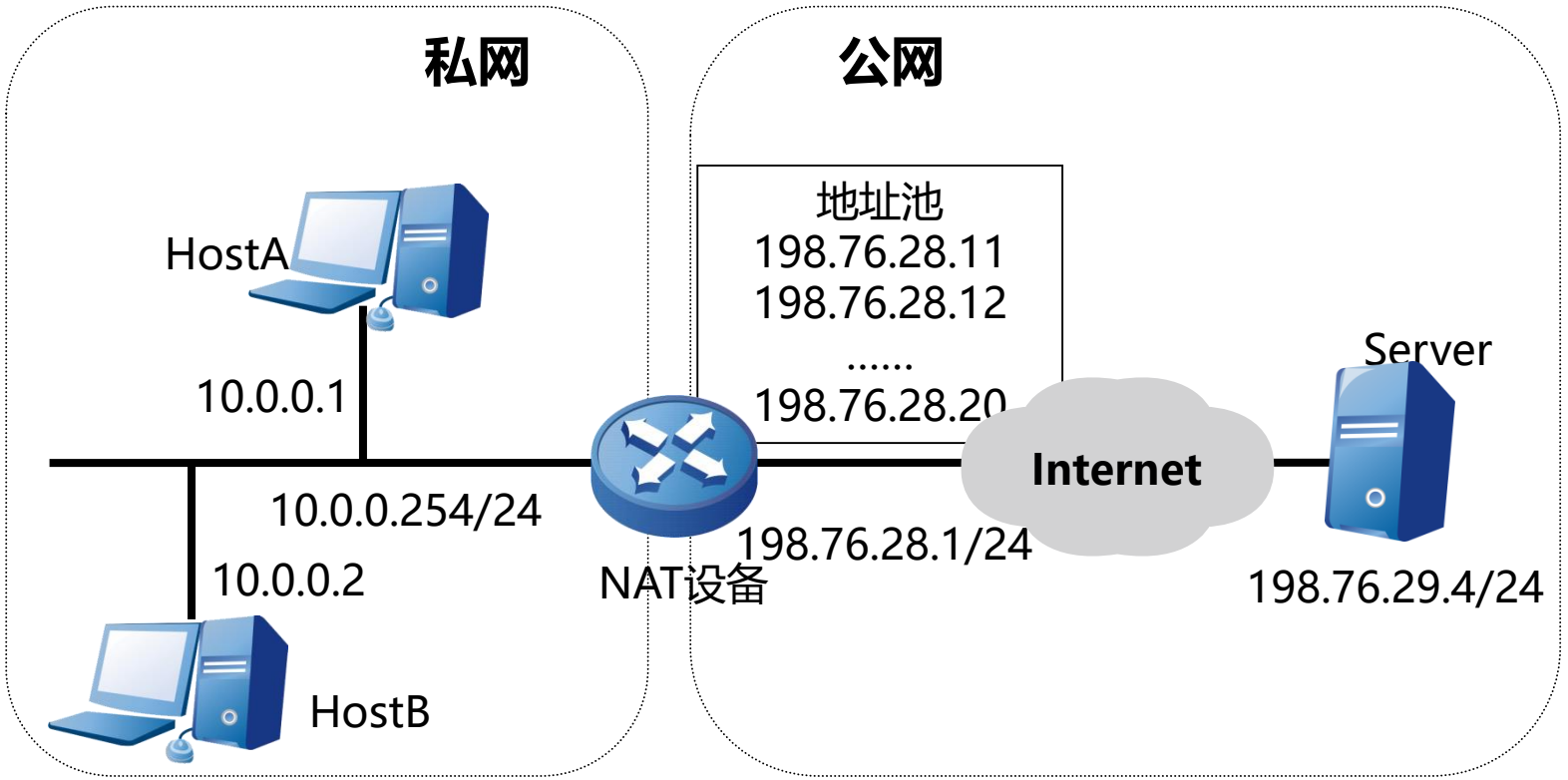
10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

- 任何组织都可以任意使用私有地址空间
- 私有地址在Internet上无法路由
- 如果采用私有地址的网络需要访问Internet，必须在出口处部署NAT设备

NAT组网和常用术语


私网
公网
地址池
198.76.28.11
198.76.28.12
.....
198.76.28.20
HostA
10.0.0.1
10.0.0.254/24
10.0.0.2
HostB
NAT设备
198.76.28.1/24
Internet
Server
198.76.29.4/24

NAT的相关术语

■ 内部地址

- 分配给内部网络中的主机的IP地址

■ 外部地址

- 合法的外部IP地址（由NIC或ISP分配的）

■ 静态转换

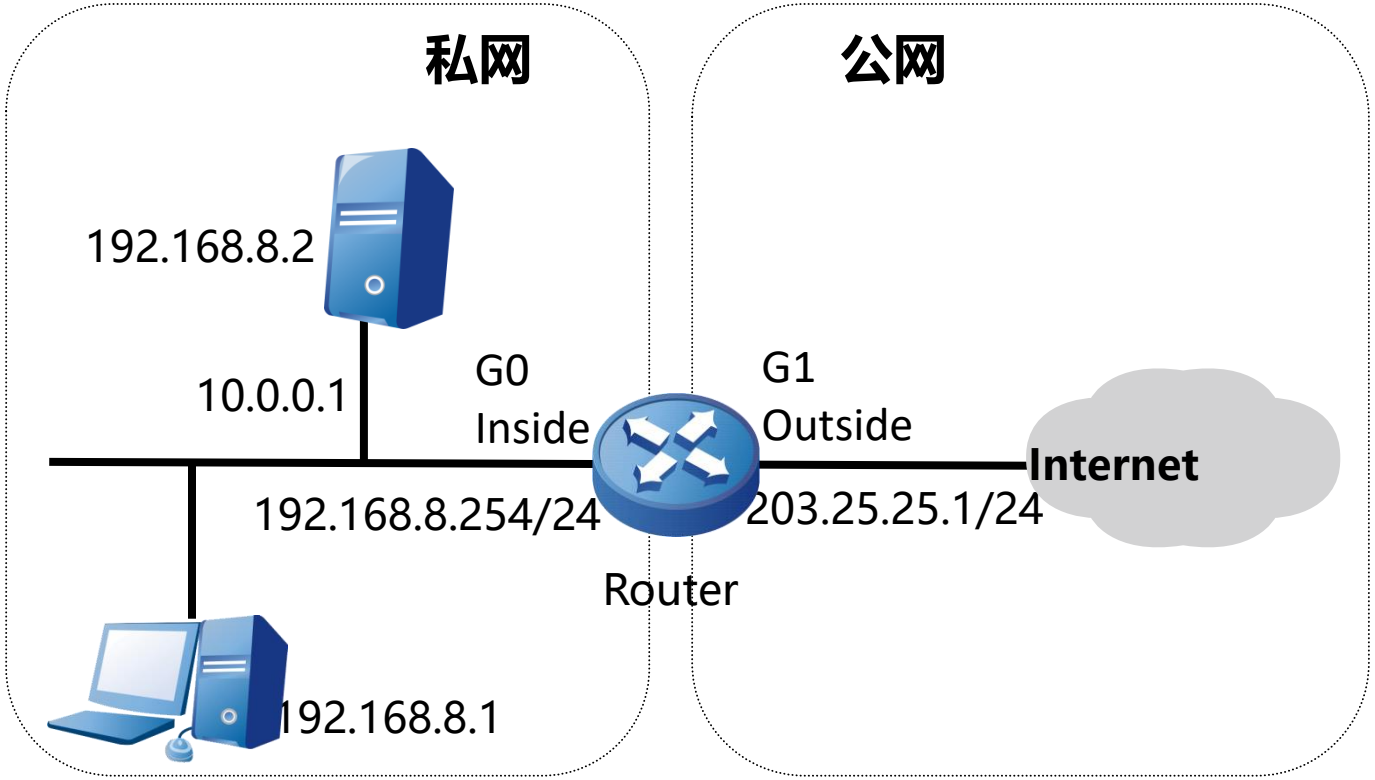
- 在内部本地地址与内部全局地址之间建立一个一对一的映射

■ 动态转换

- 在一个内部本地地址与一个全局地址池之间建立一个映射

内部源地址转换

- 转换内部源地址把内部IP地址转换成外部IP地址。
- 可以采用静态转换或者动态转换

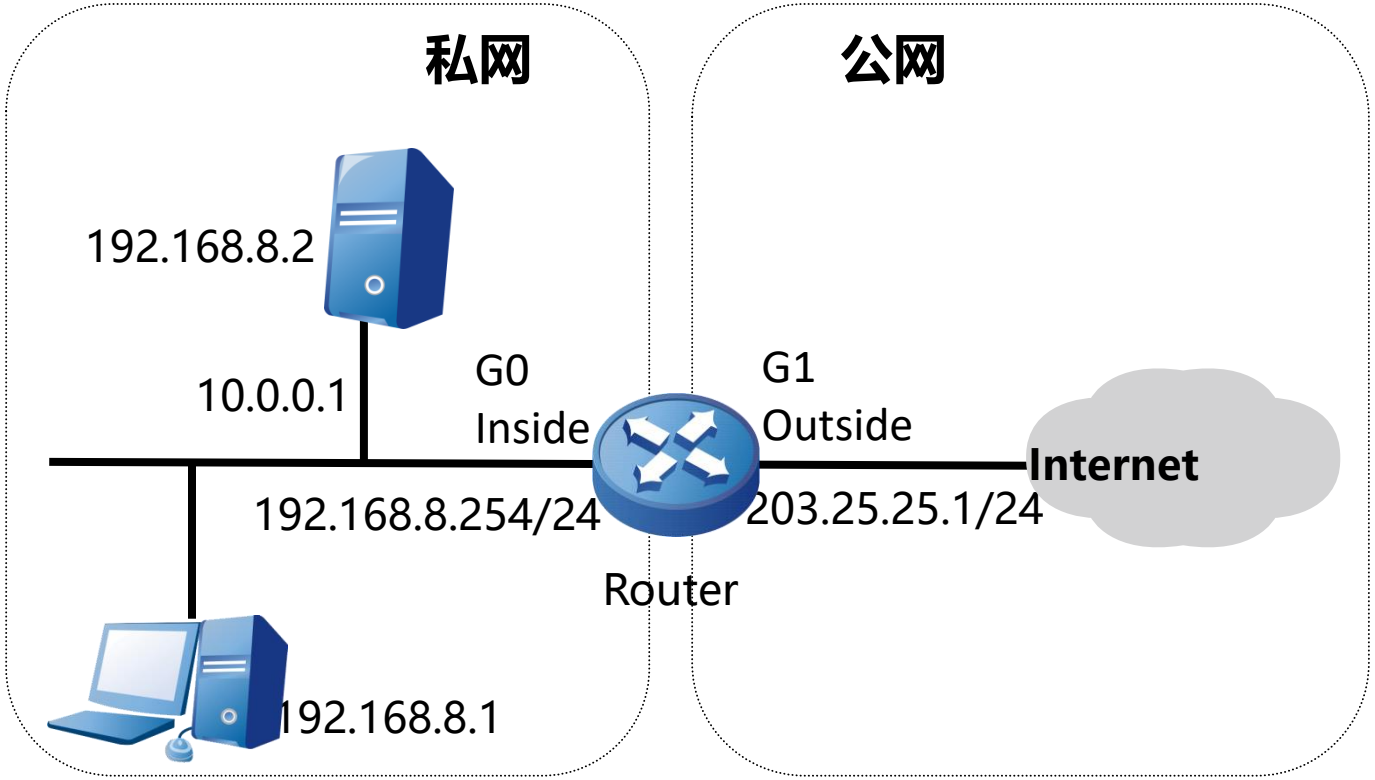


静态转换内部源地址

- 静态转换实现内外部地址的**一对一**
- 动态转换可实现多对多

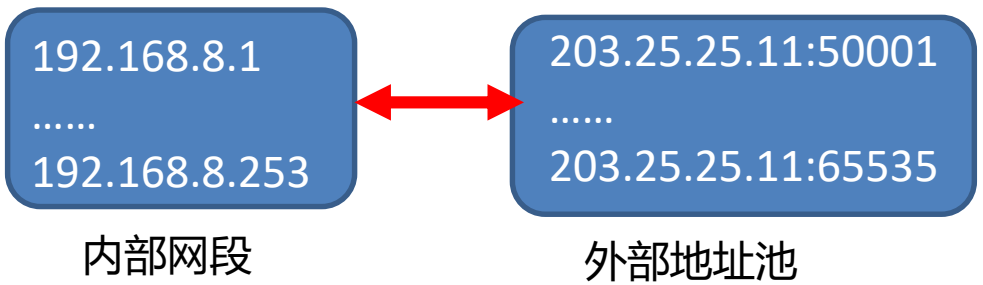
静态

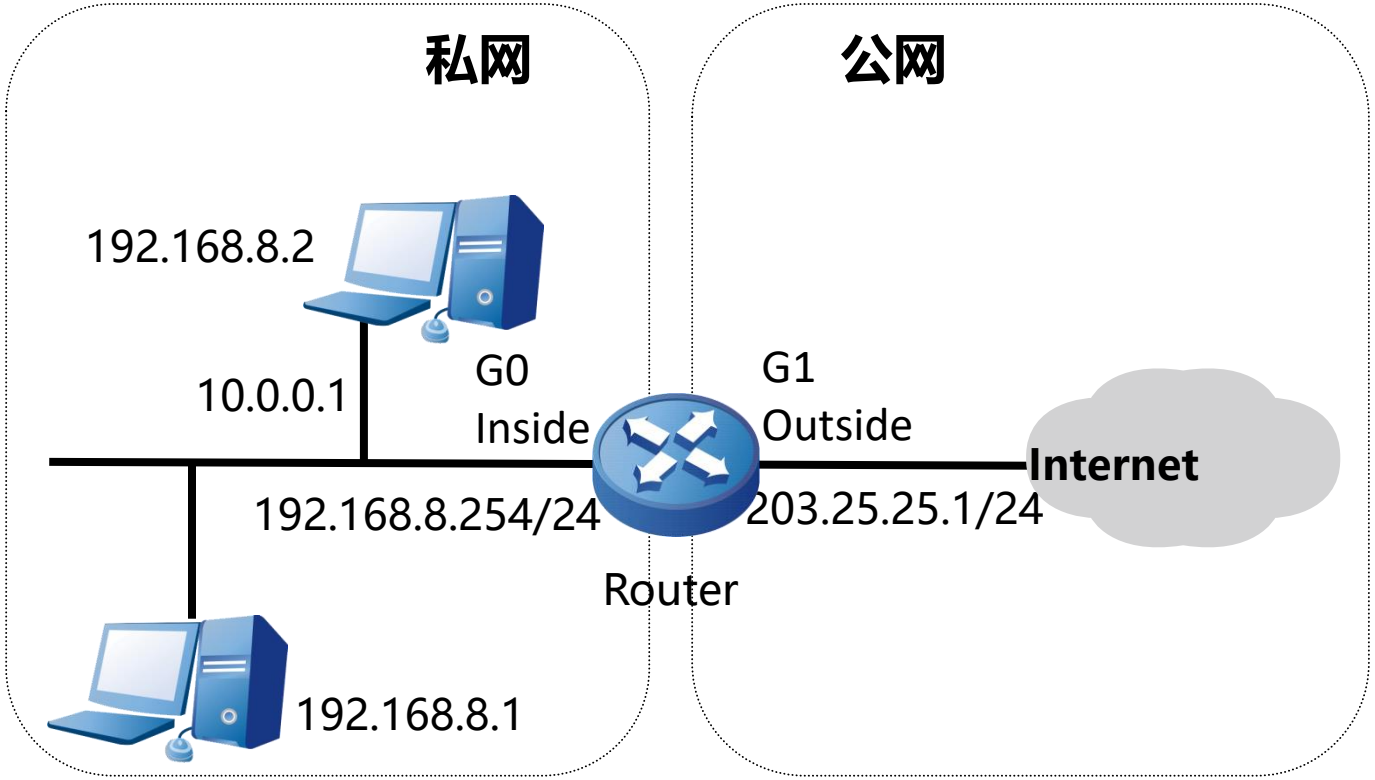
内部地址		外部地址
192.168.8.1	⟷	203.25.25.11
192.168.8.2	⟷	203.25.25.12



动态转换内部源地址

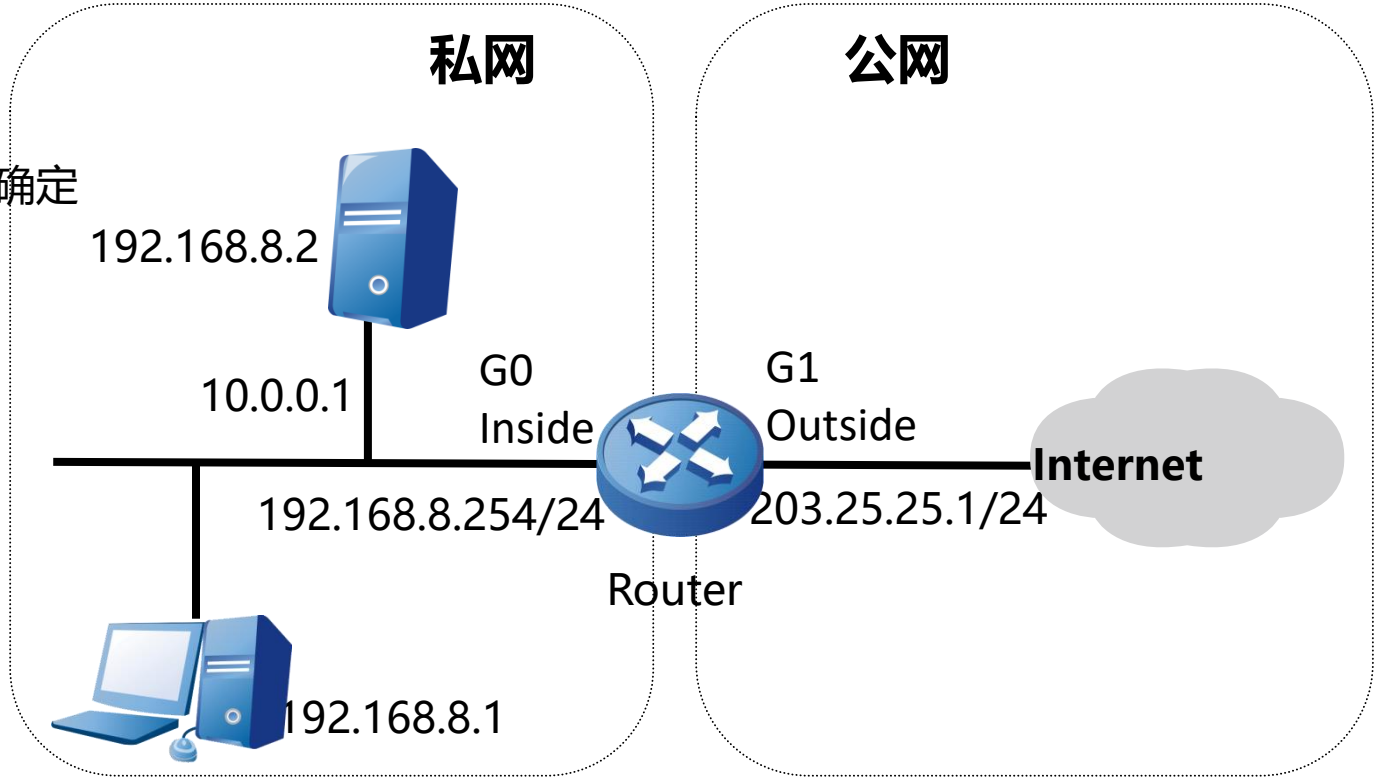
- 外部地址的TCP/UDP端口对应内部IP
- 动态转换可实现**一对多**





NAT配置思路

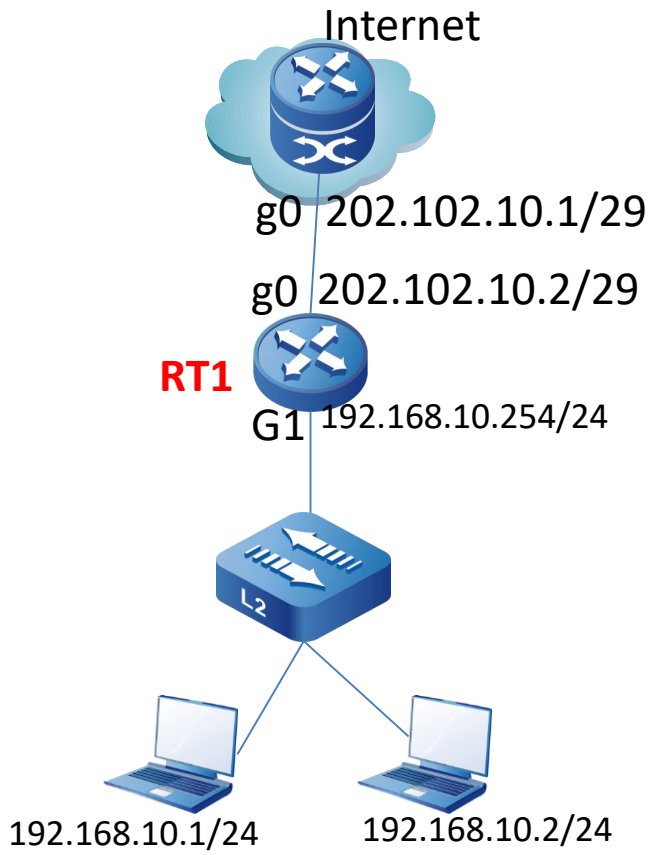
- **确定内部需要转换的地址**
  - 若需要转换的为地址范围，则需要通过标准ACL确定
- **确定外部地址资源**
- **确认NAT应用中的内外部接口**
  - 连接外部网络的接口为outside
  - 连接内部网络的接口为inside
- **根据上述内容进行配置**
  - 根据需要用标准ACL选定内部需转换地址
  - 配置内外部地址对应关系
  - 设置NAT应用中的内外部接口



NAT配置案例：静态转换

■ 实例描述

某实验网络中，RT1作为互联网接入路由器，通过NAT实现内部主机访问外部网络



- **步骤一：用标准ACL选定内部需转换地址**

ip access-list 1001

Permit 192.168.10.0 0.0.0.255

- **步骤二：根据需要配置ip nat pool**

ip nat pool test 202.102.10.3 202.102.10.6

- **步骤三：配置内外部地址对应关系**

Ip nat inside source list 1001 pool test

- **步骤四：设置接口在NAT应用中的工作位置**

interface g0

ip nat outside

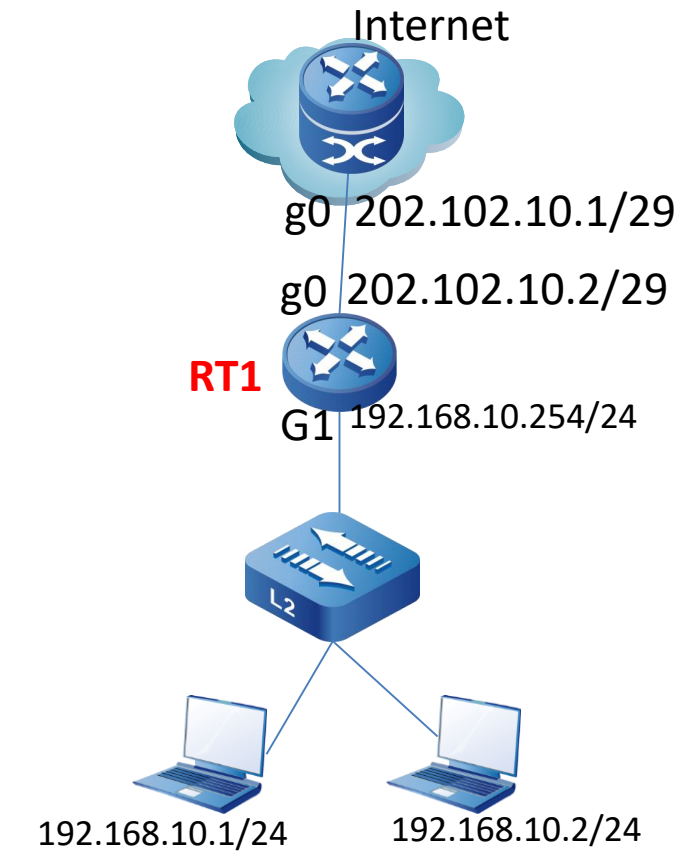
interface g1

ip nat inside

NAT配置案例：动态转换

■ 实例描述

某园区网络中，RT1作为互联网接入路由器，通过NAT实现局域网访问互联网



➢ **步骤一：用标准ACL选定内部需转换地址**

ip access-list 1001

Permit 192.168.10.0 0.0.0.255

➢ **步骤二：根据需要配置ip nat pool**

为节省公网地址，直接采用g0口地址

Ip nat inside source list 1001 interface g0 **overload**

➢ **步骤四：设置接口在NAT应用中的工作位置**

interface g0

ip nat outside

interface g1

ip nat inside

NAT监控与维护

- **show ip nat translation**

显示激活的NAT转换表条目

- **show ip nat statistics**

显示NAT统计数据

- **clear ip nat statistics**

清除NAT统计数据

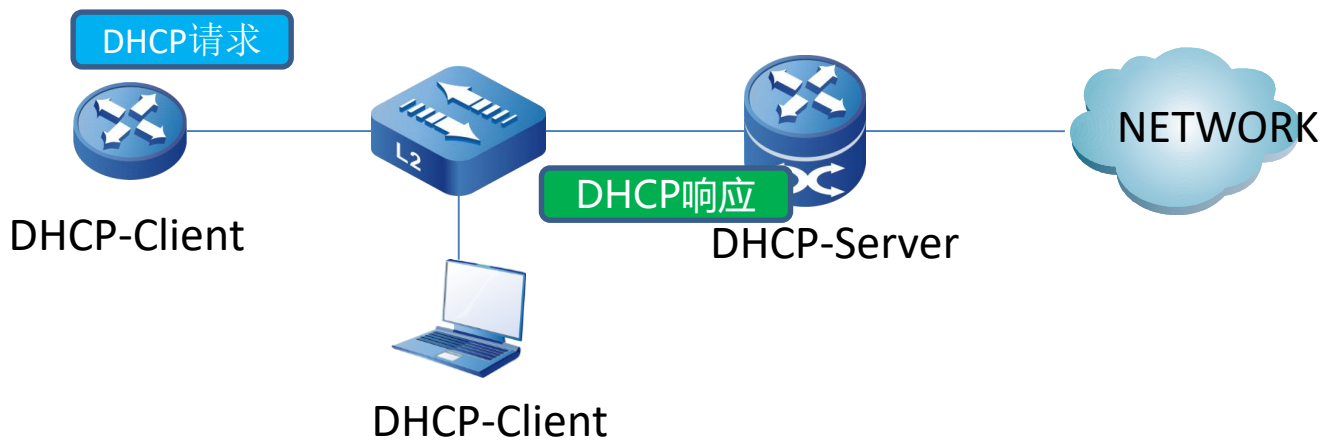
- **clear ip nat translation all**

清除NAT转换表

目录

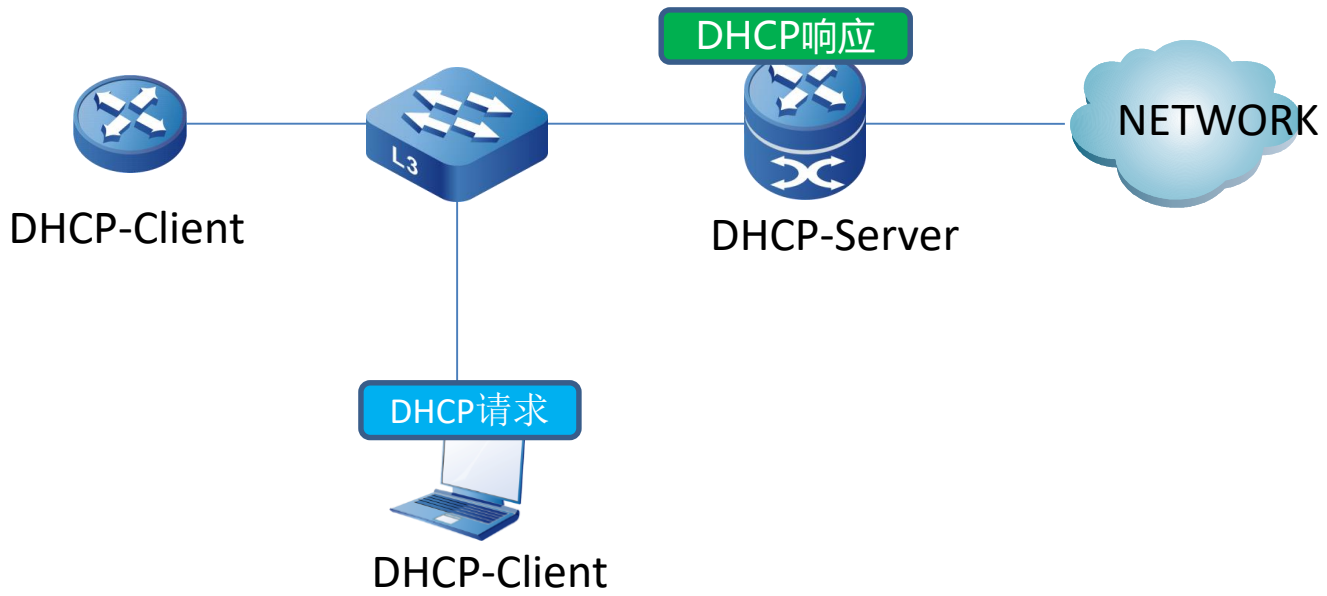
DHCP协议简介

- 解决主机规模大难以管理的问题
- DHCP采用**客户端/服务器模式**
  - 交互报文以广播方式为主，只能在广播域里传播
- 自动为主机分配IP协议相关参数
  - IP地址
  - 缺省网关
  - DNS服务等



DHCP协议中继代理

- DHCP报文无法直接跨越广播域
- 使用中继代理方式对DHCP报文进行转换
  - 客户端将DHCP报文发给中继器
  - 中继器收到后转发给DHCP服务器
- 中继代理一般在最末端网关设备上开启



DHCP配置思路与步骤

■ 确定分配的IP协议信息

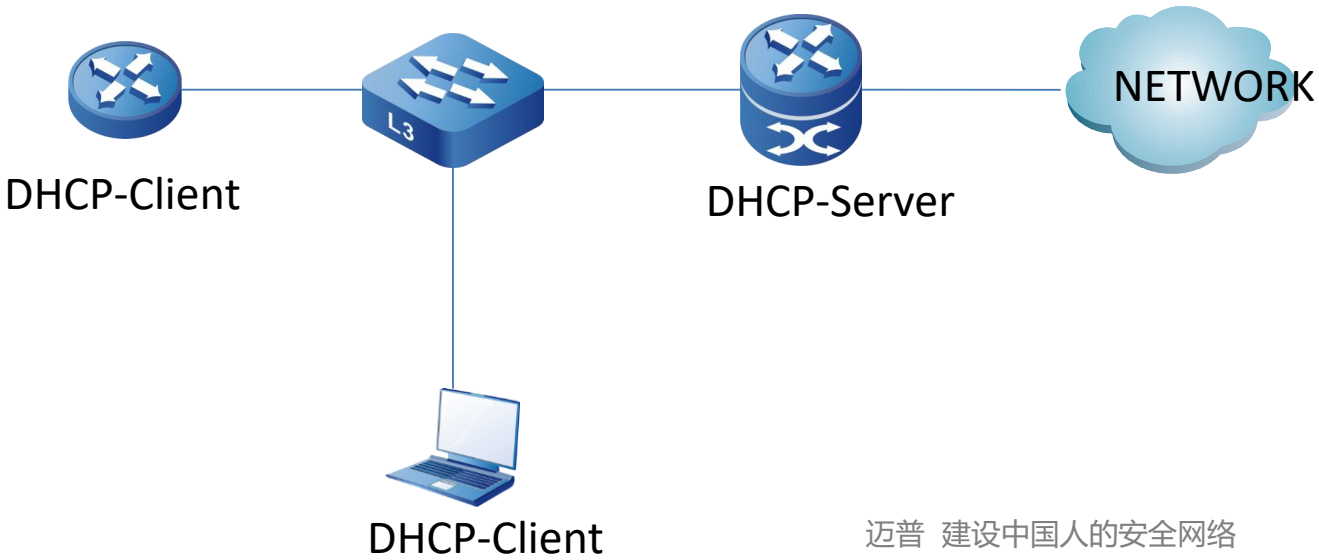
- 分配的IP地址范围及保留地址
- 对应确定网关
- DNS服务器（含备份服务器）

■ 确定其他需求

- IP地址租期，默认为30小时
- IP与MAC绑定信息等

■ 根据上述内容进行配置

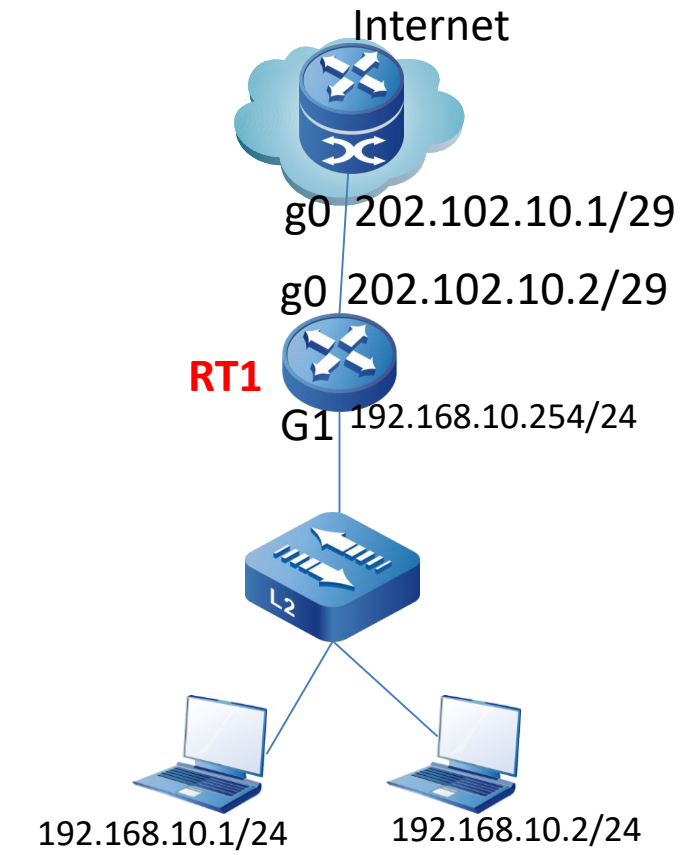
- 创建dhcp-pool
- 配置IP地址分配范围
- 配置缺省网关
- 配置DNS
- 配置其他参数
- 若有中继代理，则在中继设备上进行配置



DHCP配置案例:直接获取

■ 实例描述

某实验网络中，RT1作为互联网接入路由器，为简化局域网IP地址设置，启用DHCP协议自动分配IP地址。



- **第一步:创建dhcp-pool**

ip dhcp pool test

- **第二步:配置IP地址分配范围**

network 192.168.10.0 255.255.255.0

或range 192.168.10.1 192.168.10.253 255.255.255.0

- **第三步:配置缺省网关**

default-route 192.168.10.254

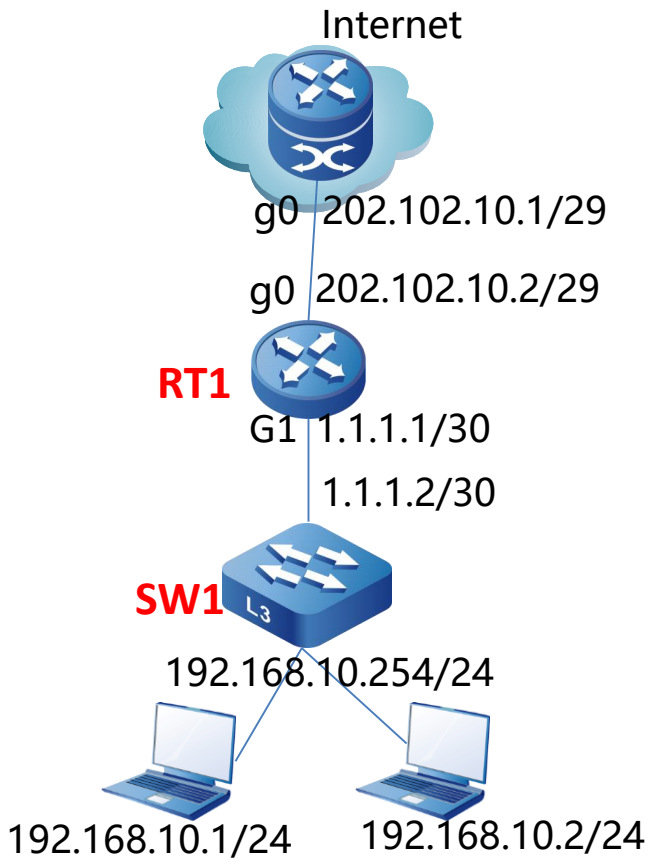
- **第四步:配置DNS**

dns-server 61.139.2.69 4.4.4.4

DHCP配置案例:中继代理

■ 实例描述

某园区网络中，RT1作为互联网接入路由器，为简化局域网IP地址设置，启用DHCP协议自动分配IP地址。要求192.168.10.99地址保留不做分配



- **第一步:创建dhcp-pool**

ip dhcp pool test

- **第二步:配置IP地址分配范围**

network 192.168.10.0 255.255.255.0

ip dhcp excluded-address 192.168.10.99 //须在全局配置//

- **第三步:配置缺省网关**

default-route 192.168.10.254

- **第四步:配置DNS**

dns-server 61.139.2.69 4.4.4.4

- **第五步:配置中继代理**

ip dhcp-server 1.1.1.1 //在SW1上配置//

DHCP监控命令

- **show ip dhcp binding**

显示系统中IP、MAC绑定的数目

- **show ip dhcp lease**

显示DHCP客户端的租约信息

- **clear ip dhcp binding**

清除DHCP服务器中的地址绑定

- **clear ip dhcp relay statistics**

清除中继服务器上的统计信息

CEC 中国电子 | MAIPU 迈普

迈普 建设中国人的安全网络