国家计算机软考职称
中级网络工程师培训

第23课：组网技术（四）

主讲：大涛

微信/QQ383419460，每周一三五 20:30-22:00， 全程录像网盘下载

上节课考点回顾

- 1、RIP与BFD联动实验
- 2、动态路由OSPF实验
- 3、动态路由IS-IS实验

微信扫码免费咨询报名考试
官方淘宝店：大涛网络学院
凡是其他联系方式均为盗版
官方微信/QQ：383419460

第23课：组网技术（四）

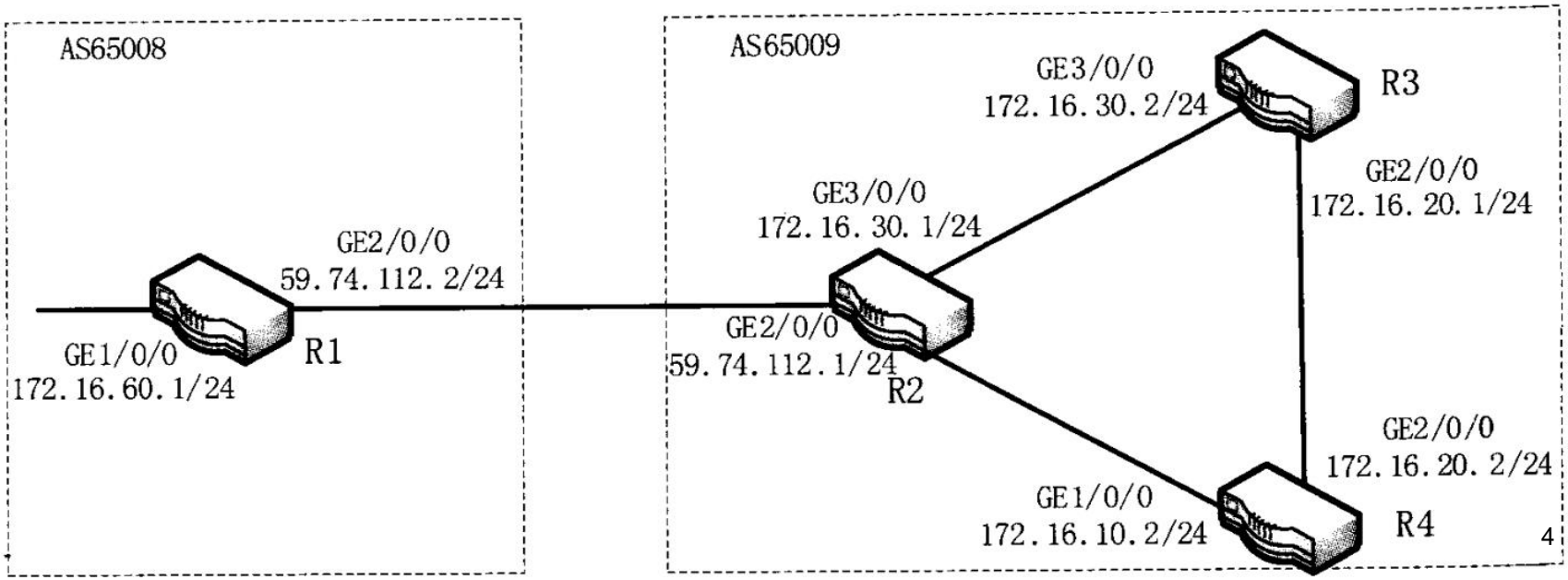
- ***1、动态路由BGP实验***
- 2、路由技术ACL实验
- 3、本节网工考题分析

微信扫码免费咨询报名考试
官方淘宝店：大涛网络学院
凡是其他联系方式均为盗版
官方微信/QQ：383419460

【章节】网工：10.5-10.8

第23课：组网技术（四）

- **考点01：**BGP：边界网关协议，在自制系统AS之间选择最佳路由，距离矢量。支持多出口大型网络。路由采用增量更新。除了下一跳还有经过的AS列表通过信息。允许CIDR和VLSM，支持鉴别、验证等。分为EBGP(外部)和IBGP(内部)。



第23课：组网技术（四）

- **第一步：**配置R1到R4接口IP的基本配置(略)。
- **第二步：**配置IBGP：R2、R3、R4如下配置。

```
[R2] bgp 65009                                  //启动BGP及AS号
[R2-bgp] router-id 2.2.2.2                      //配置BGP的RouterID
[R2-bgp] peer 9.1.1.2 as-number 65009           //配置BGP对等体
[R2-bgp] peer 9.1.3.2 as-number 65009
```

```
[R3] bgp 65009
[R3-bgp] router-id 3.3.3.3
[R3-bgp] peer 9.1.3.1 as-number 65009
[R3-bgp] peer 9.1.2.2 as-number 65009
[R3-bgp] quit
```

第23课：组网技术（四）

```
[R4] bgp 65009
[R4-bgp] router-id 4.4.4.4
[R4-bgp] peer 9.1.1.1 as-number 65009
[R4-bgp] peer 9.1.2.1 as-number 65009
[R4-bgp] quit
```

- 第三步：配置EBGP：R1、R2如下配置。

```
[R1] bgp 65008
[R1-bgp] router-id 1.1.1.1
[R1-bgp] peer 59.74.112.1 as-number 65009

[R2-bgp] peer 59.74.112.2 as-number 65008
```

第23课：组网技术（四）

- **第四步：**配置R1发布路由，如下配置。

```
[R1-bgp] ipv4-family unicast      //进入IPV4地址族视图
[R1-bgp-af-ipv4] network 172.16.60.0 255.255.255.0
[R1-bgp-af-ipv4] quit
```

- **第五步：**配置R2引入路由，如下配置。

```
[R2-bgp] ipv4-family unicast
[R2-bgp-af-ipv4] import-route direct      //引入路由表
```

- **第六步：**验证BGP用到的命令。

dis bgp peer、dis bgp routing、dis cu、ping。

第23课：组网技术（四）

- 1、动态路由BGP实验
- ***2、路由技术ACL实验***
- 3、本节网工考题分析

微信扫码免费咨询报名考试
官方淘宝店：大涛网络学院
凡是其他联系方式均为盗版
官方微信/QQ：383419460

【章节】网工：10.5-10.8

软考IT专业培训，大涛微信/QQ：383419460 http://dtwlxy.taobao.com

第23课：组网技术（四）

- 考点02：ACL：访问控制列表，可以根据源地址、目标地址、源端口、目标端口、协议信息对数据包进出过滤控制。
- 两个方向：入口inbound是指数据流进入路由器(进门)、出口outbound是指数据流从路由器流出(出门)。两种动作：允许permit、拒绝deny。

分类	规则定义描述	编号范围
基本 ACL	仅使用报文的源 IP 地址、分片信息和生效时间段信息来定义规则	2000～2999
高级 ACL	既可使用 IPv4 报文的源 IP 地址，也可使用目的 IP 地址、IP 协议类型、ICMP 类型、TCP 源/目的端口、UDP 源/目的端口号、生效时间段等来定义规则	3000～3999
二层 ACL	使用报文的以太网帧头信息来定义规则，如根据源 MAC（Media Access Control）地址、目的 MAC 地址、二层协议类型等	4000～4999
用户 ACL	既可使用 IPv4 报文的源 IP 地址，也可使用目的 IP 地址、IP 协议类型、ICMP 类型、TCP 源端口/目的端口、UDP 源端口/目的端口号等来定义规则	6000～6031

第23课：组网技术（四）

- **考点03：**基本ACL：编号2000~2999

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule permit source 172.16.10.3 0
```

命令 动作 源地址 IP 反掩码

1
2
3

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule permit source 172.16.10.3 0
[Huawei-acl-basic-2001] rule deny source 172.16.10.0 0.0.0.255
[Huawei-acl-basic-2001] description Permit only 172.16.10.3 through
```

- 1、进入系统　　2、配置编号　　3、ACL列表
- 基本ACL，基于源地址，放置到目的端路由器。

第23课：组网技术（四）

- **考点04：**基本ACL命令规则：编号2000~2999

acl [number] *acl-number* [match-order { auto | config }]

命令 可选 编号 匹配 排序 排序 顺序

acl name *acl-name* { basic | *acl-number* } [match-order { auto | config }]

rule [rule-id] { deny | permit } [source

命令 步长数字 拒绝 允许 源地址

{ source-address source-wildcard | any }

源IP 反掩码 任何

| [fragment | none-first-fragment] | logging

分片 不分片 日志

| time-range time-name]

时间 名称

第23课：组网技术（四）

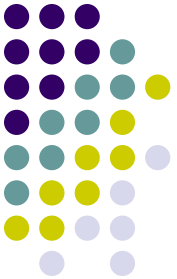
```
<Huawei> system-view
[Huawei] time-range working-time 8:00 to 18:00 working-day
[Huawei] acl name work-acl basic
[Huawei-acl-basic-work-acl] rule deny source 172.16.10.0
                                0.0.0.255 time-range working-time

<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule deny source 172.16.10.0
                                0.0.0.255 none-first-fragment
```

- 善用**Tab**键补全命令和问号**?**键帮助命令。

第23课：组网技术（四）

- **考点05：**ACL几个重点知识：
- ACL执行原则：①自上而下排序原则。②先匹配原则（特例在前，其他在后）。③默认丢弃原则（deny any）。
- 反掩码：0.0.0.0，单个主机，同host，如：192.168.1.1 0.0.0.0 = host 192.168.1.1
- 反掩码：255.255.255.255，任意主机，同any，通常与0.0.0.0一起使用，例如：0.0.0.0 255.255.255.255 = any



第23课：组网技术（四）

- **考点06：**高级ACL：编号3000~3999

```
<Huawei> system-view
[Huawei] acl 3001
[Huawei-acl-adv-3001] rule permit icmp source 172.16.10.3 0
                      destination 172.16.20.0 0.0.0.255
```

命令 动作 协议 源端 IP

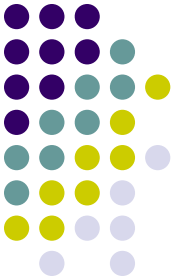
目的 IP 反掩码

```
1 <Huawei> system-view
2 [Huawei] acl name deny-telnet
3 [Huawei-acl-adv-deny-telnet] rule deny tcp destination-port eq telnet
                      source 172.16.10.3 0 destination 172.16.20.0 0.0.0.255
```

命令 动作 协议 目的端口 等于 23

源端 IP 反掩码 目的 IP 反掩码

- 高级ACL，基于目的，放置到源端的路由器。



第23课：组网技术（四）

- **考点08：**高级ACL命令规则：编号3000~3999

rule [*rule-id*] { deny | permit }{ *protocol-number* | udp }
命令 步长数字 拒绝 允许 协议号 协议

[destination { *destination-address* *destination-wildcard* | any } |
目的 IP 反掩码 任何

destination-port {eq | gt | lt *port* | range *port-start port-end* } | *source*
目的端口 等于 端口号 范围 开始端口 结束端口 源

{*source-address* *source-wildcard* | any } | source-port {eq | gt | lt *port*
IP 反掩码 任何 源端口 等于 端口号

| range *port-start port-end* } | logging | time-range *time-name*]
范围 开始端口 结束端口 日志 时间 名称

第23课：组网技术（四）

● 考点09：几个重要参数

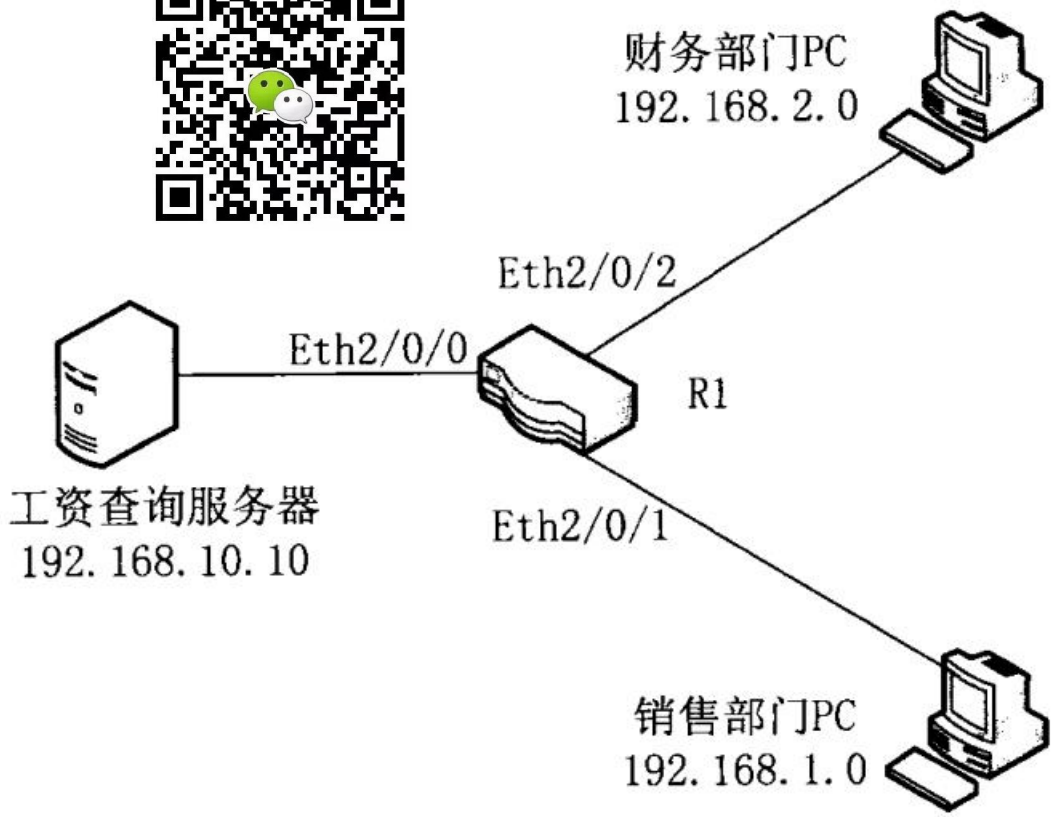
操作符	解释	操作符	解释
lt	小于	neq	不等于
gt	大于	range	指定范围
eq	等于		

传输协议	上层协议	端口号	命令参数关键字
TCP	文件传输协议——数据	20	ftp-data
TCP	文件传输协议——控制	21	ftp
TCP	远程连接	23	telnet
TCP	简单邮件传输协议	25	smtp
UDP	域名服务	53	dns
UDP	简单文件传输协议	69	tftp
TCP	超文本传输协议	80	www
UDP	简单网络管理协议	161	snmp
UDP	简单网络管理协议	162	snmp-trap
UDP	路由信息协议	520	rip

第23课：组网技术（四）

- **考点10：**高级ACL实验一：限制用户在特定时间访问特定服务器。

- 要求禁止销售部门在上班时间（8:00-18:00)访问工资查询服务器，财务部门不受限制，可以随时访问，如图。



第23课：组网技术（四）

- **第一步：**配置IP、配置VLAN、VLANIF等。

以E2/0/1口为例

```
<Huawei> system-view
[Huawei] sysname R1
[R1] vlan batch 10 20 100
[R1] interface ethernet 2/0/1
[R1-Ethernet2/0/1] port link-type trunk
[R1-Ethernet2/0/1] port trunk allow-pass vlan 10
[R1-Ethernet2/0/1] quit
[R1] interface vlanif 10
[R1-Vlanif10] ip address 192.168.1.1 255.255.255.0
[R1-Vlanif10] quit
```

第23课：组网技术（四）

- 第二步：配置基于时间的ACL访问规则等。

```
#配置 8:00 至 18:00 的周期时间段
[R1] time-range satime 8:00 to 18:00 working-day

#配置销售部门到工资查询服务器的访问规则
[R1] acl 3001
[R1-acl-3001] rule deny ip source 192.168.1.0 0.0.0.255
      destination 192.168.10.10 0.0.0.0 time-range satime
```

- Mon(周一)、Tue(周二)、Wed(周三)、Thu(周四)、Fri(周五)、Sat(周六)、Sun(周日) 、working-day(周一到周五)、off-day(周六周日)daily(周一到周日)、数字0-6(每周几)。

第23课：组网技术（四）

- 第三步：配置基于ACL的流分类策略。

#配置流分类 c_xs，对匹配 ACL 3001 的报文进行分类

[R1] traffic classifier c_xs

[R1-classifier-c_xs] if-match acl 3001

[R1-classifier-c_xs] quit

#配置流行为 b_xs，动作为拒绝报文通过

[R1] traffic behavior b_xs

[R1-behavior-b_xs] deny

[R1-behavior-b_xs] quit

第23课：组网技术（四）

- **第四步：**应用基于ACL的流策略。

#配置流策略 p_xs，将流分类 c_xs 与流行为 b_xs 关联

[R1] traffic policy p_xs

[R1-trafficpolicy-p_xs] classifier c_xs behavior b_xs

[R1-trafficpolicy-p_xs] quit

#由于销售部门访问服务器的流量从接口 Eth2/0/1 进入 Router，所以可以在 Eth2/0/1 接口的入方向应用流策略 p_xs

[R1] interface ethernet2/0/1

[R1-Ethernet2/0/1] traffic-policy p_xs inbound

[R1-Ethernet2/0/1] quit

第23课：组网技术（四）

- 1、动态路由BGP实验
- 2、路由技术ACL实验
- ***3、本节网工考题分析***

【章节】网工：10.5-10.8

例题01

- 下面ACL语句中，表达“禁止外网和内网之间互相ping”的是（　　）。

  A. rule 100 permit any any

  B. rule 100 permit icmp any any

  C. rule 100 deny any any

  D. rule 100 deny icmp any any

例题02

- 每一个访问控制列表(ACL)最后都隐含着一条(　　)语句。　A. deny any　　B. deny all

  C. permit any　　D. permit all

例题03

- 关于访问控制列表编号 下面描述正确的是（ ）

A. 基本的访问控制列表编号范围是1000-2999

B. 高级的访问控制列表编号范围是3000-3999

C. 基本的访问控制列表编号范围是4000-4999

D. 基本的访问控制列表编号范围是1000-2000

例题04

- 下列哪项参数不能用于高级访问控制列表？

A. 物理接口　　B. 目的端口号

C. 协议号　　D. 时间范围

例题05

- 下列静态路由配置不正确的是（ ）。

A. ip route-static 129.1.0.0 16 serial 0
B. ip route-static 10.0.0.2 16 129.1.0.0
C. ip route-static 129.1.0.0 16 10.0.0.2
D. ip route-static 129.1.0.0 255.255.0.0 10.0.0.2

例题06

- 在系统视图下键入什么命令可以切换到用户视图？

A. system-view
B. router
C. quit
D. user-view

例题答案

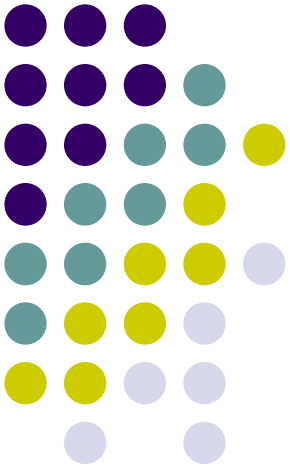
- 例题01：D。
- 例题02：A。
- 例题03：B。
- 例题04：A。
- 例题05：B。
- 例题06：C。

- **作业：01号题库23（海量题库班级号127166）**

获取考试咨询帮助加老师
微信/QQ 383419460

大涛网络学院 出品

UU教育 2018.03月



微信/QQ383419460，每周一三五 20:30-22:00， 全程录像网盘下载