
Tedu.cn
达内教育
企业级网络架构
NSD NETWORK
DAY03

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	OSPF
	10:30 ~ 11:20	
	11:30 ~ 12:00	
下午	14:00 ~ 14:50	传输层
	15:00 ~ 15:50	ACL
	16:10 ~ 17:00	
	17:10 ~ 18:00	总结和答疑

OSPF

Tedu.cn 达内教育

动态路由

Tedu.cn 达内教育

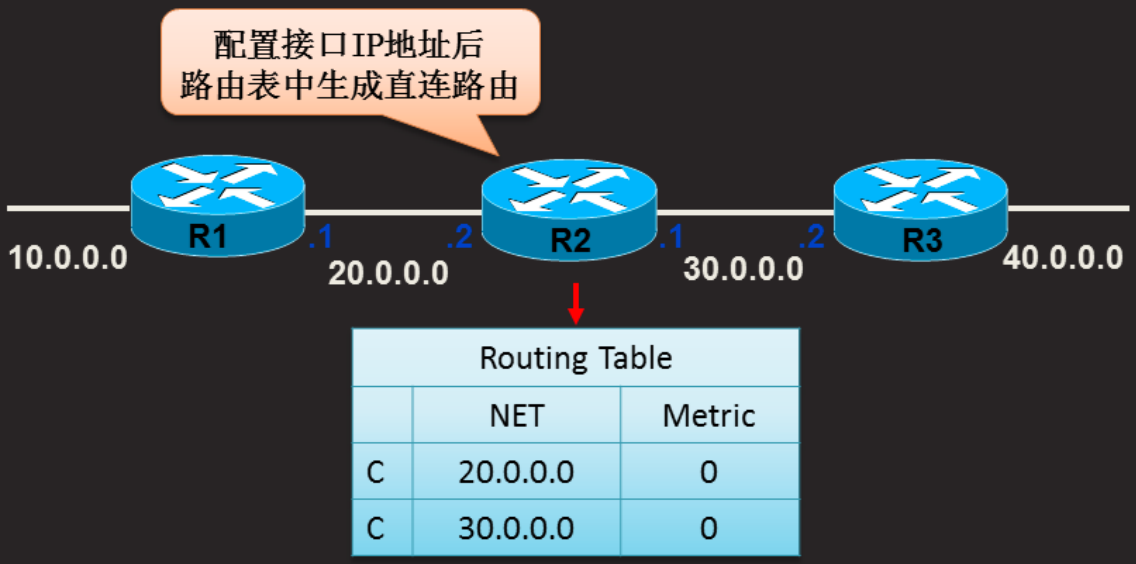
动态路由概述

知识讲解

- 动态路由
  - 基于某种路由协议实现
- 动态路由特点
  - 减少了管理任务
  - 占用了网络带宽

动态路由概述（续1）

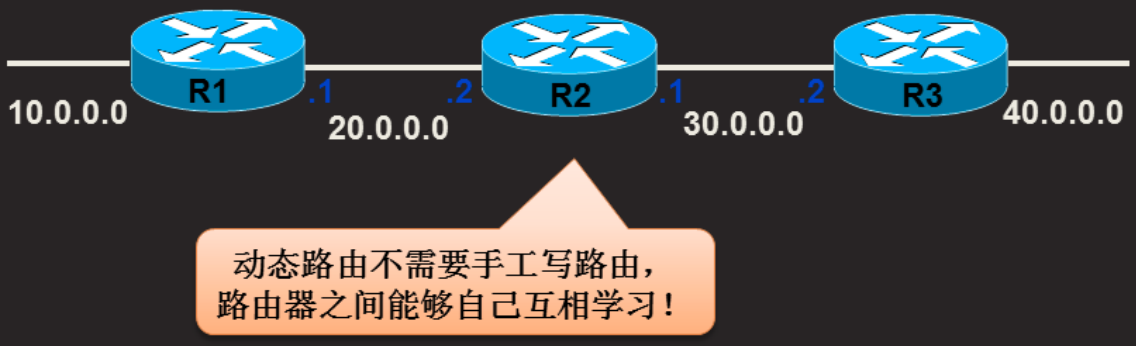
知识讲解



Routing Table		
	NET	Metric
C	20.0.0.0	0
C	30.0.0.0	0

动态路由概述（续2）

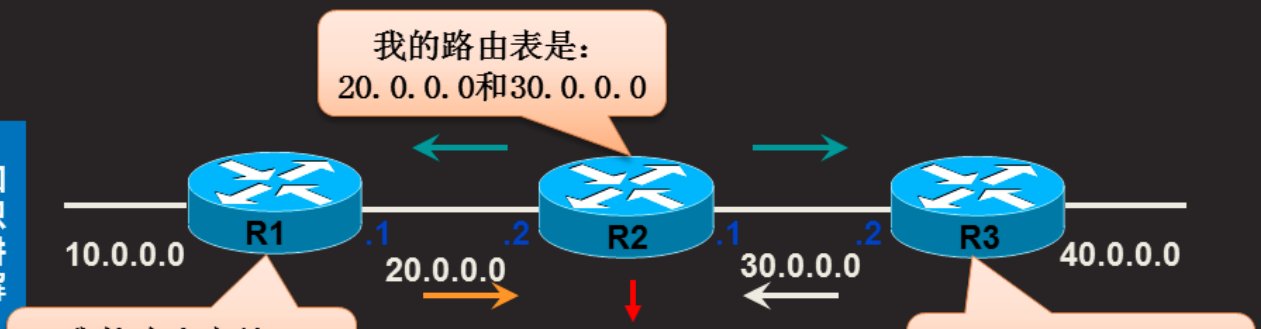
知识讲解



动态路由概述（续3）

Tedu.cn 达内教育

知识讲解

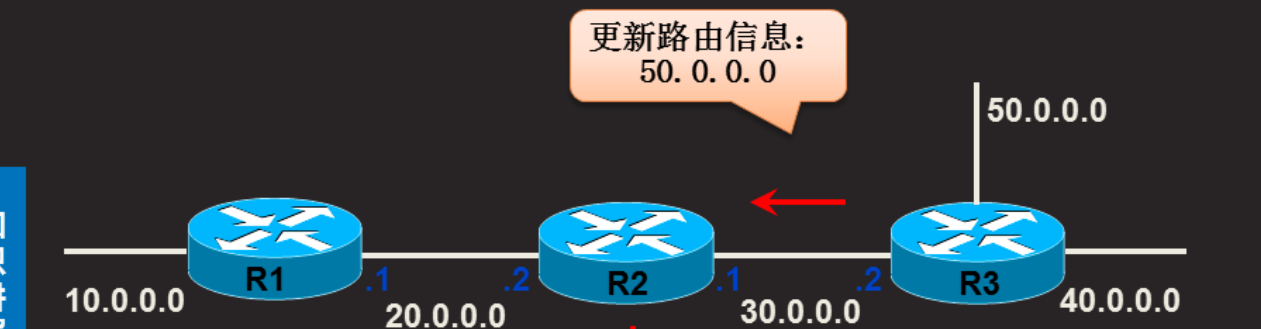


Routing Table		
	NET	Metric
C	20.0.0.0	0
C	30.0.0.0	0
?	10.0.0.0	?
?	40.0.0.0	?

动态路由概述（续4）

Tedu.cn 达内教育

知识讲解



Routing Table		
	NET	Metric
C	20.0.0.0	0
C	30.0.0.0	0
	10.0.0.0	
	40.0.0.0	
	50.0.0.0	

根据拓扑变化做出及时反映

动态路由协议OSPF

Tedu.cn 达内教育

知识讲解

- 全称为Open Shortest Path First（开放式最短路径优先）
- 适合大中型网络使用

动态路由协议OSPF（续1）

Tedu.cn 达内教育

知识讲解

- OSPF区域
  - 为了适应大型的网络，OSPF在网络内部划分多个区域
  - 每个OSPF路由器只维护所在区域的完整链路状态信息
- 区域ID
  - 区域ID可以表示成一个十进制的数字
  - 也可以表示成一个IP
- 骨干区域Area 0
  - 负责区域间路由信息传播

OSPF基本配置

知识讲解

- 启动OSPF路由进程并进入首个区域

```
[Huawei]ospf 1
[Huawei-ospf-1]area 0
```

宣告所在的网段

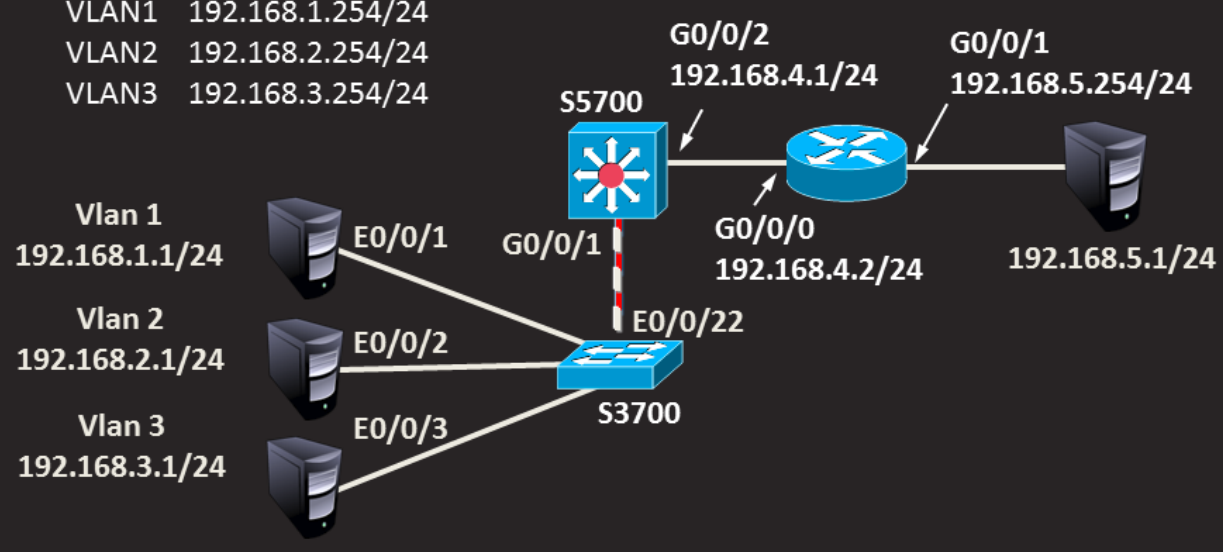
```
[Huawei-ospf-1-area-0.0.0.0]network  192.168.0.0 0.0.0.255
```

案例1：使用动态路由连接网络

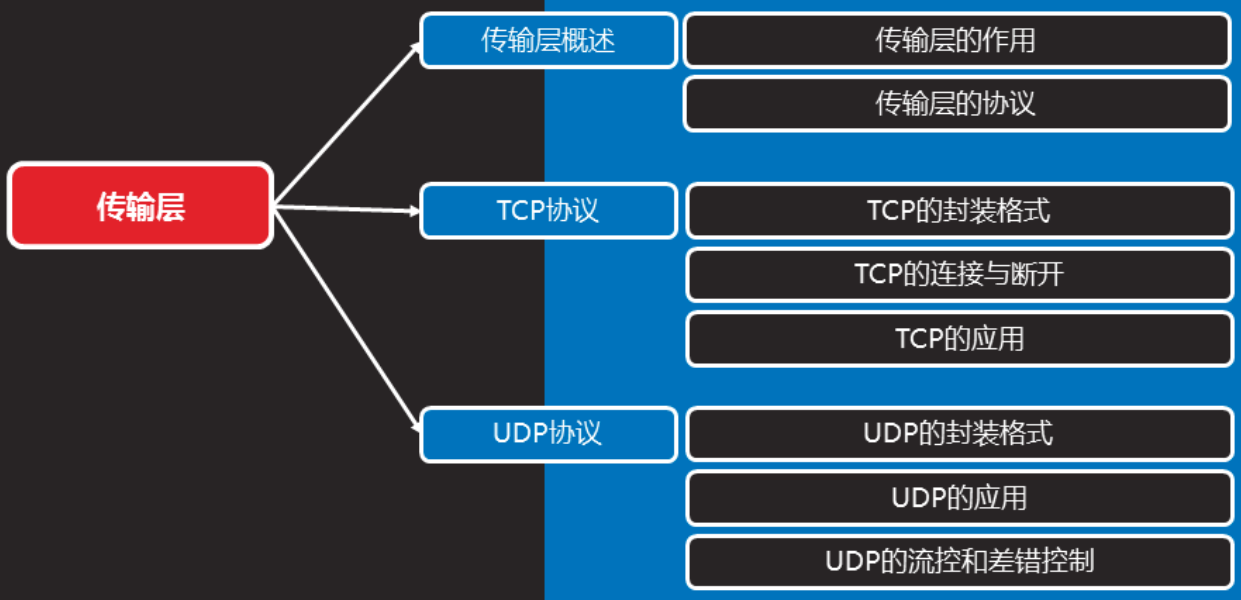
课堂练习

- 配置动态路由协议ospf使全网互通

SVI地址：
VLAN1　192.168.1.254/24
VLAN2　192.168.2.254/24
VLAN3　192.168.3.254/24



传输层



Tedu.cn
达内教育

传输层概述

传输层的作用

- 网络层提供点到点的连接
- 传输层提供端到端的连接

知识讲解

传输层的协议

- TCP（Transmission Control Protocol）
  - 传输控制协议
  - 可靠的、面向连接的协议
  - 传输效率低

- UDP（User Datagram Protocol）
  - 用户数据报协议
  - 不可靠的、无连接的服务
  - 传输效率高

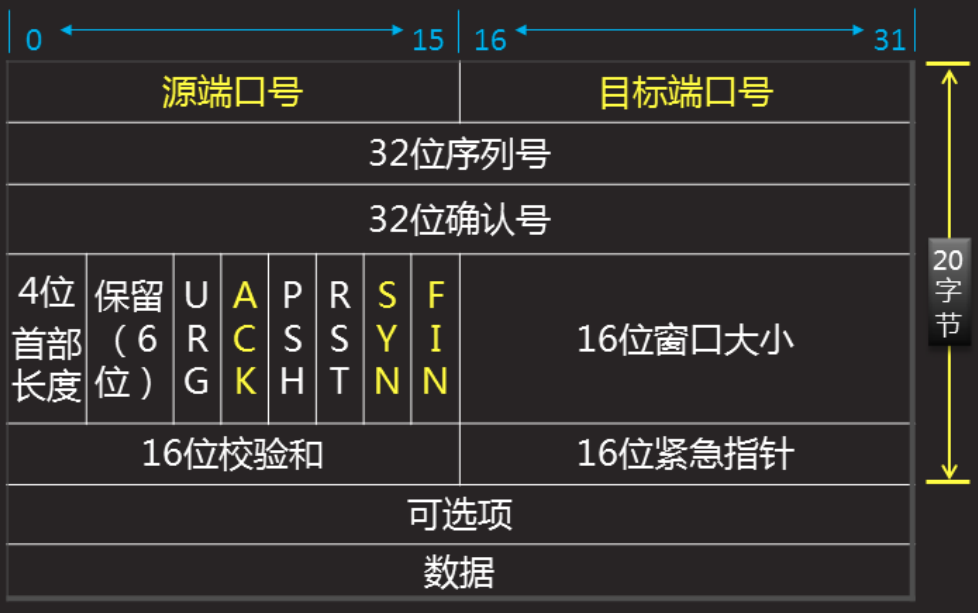
Tedu.cn 达内教育

TCP协议

Tedu.cn 达内教育

TCP的封装格式

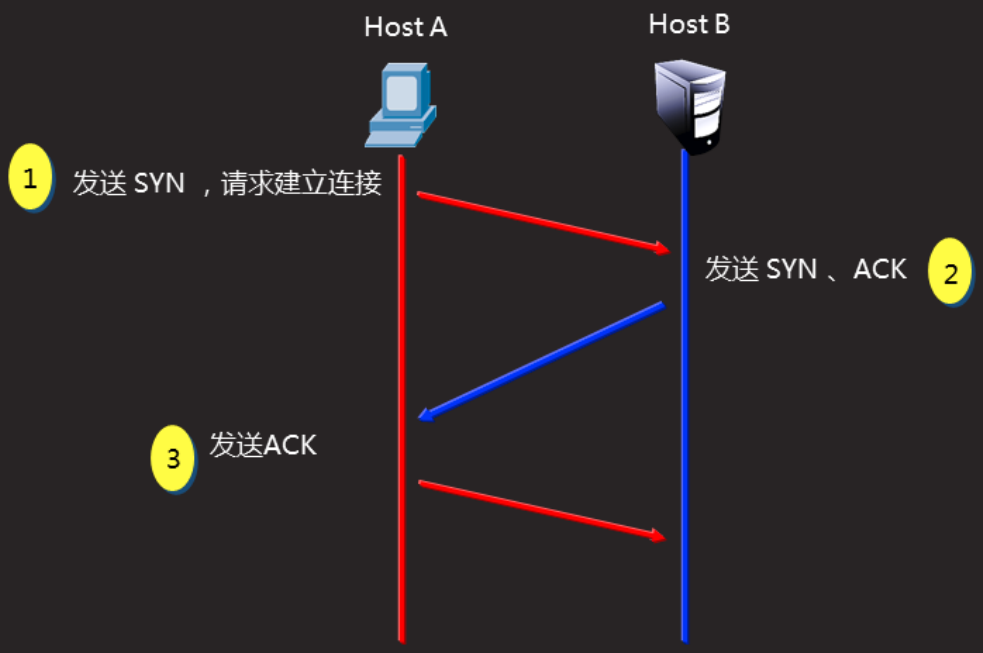
知识讲解



TCP的连接与断开

- TCP的连接 - 三次握手

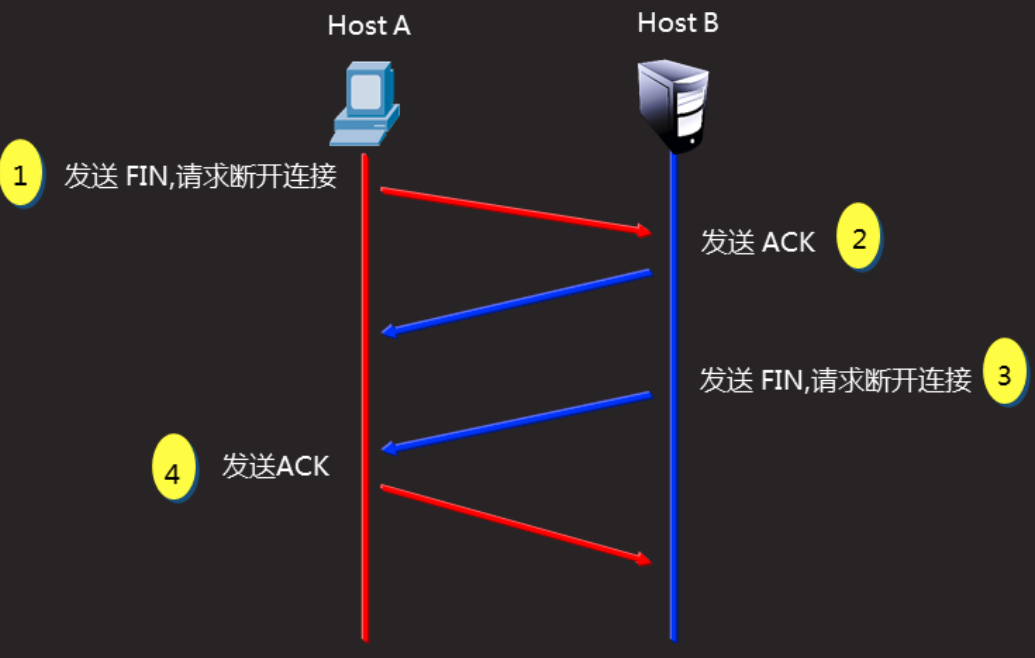
知识讲解



TCP的连接与断开（续1）

- TCP的四次断开

知识讲解



TCP的应用

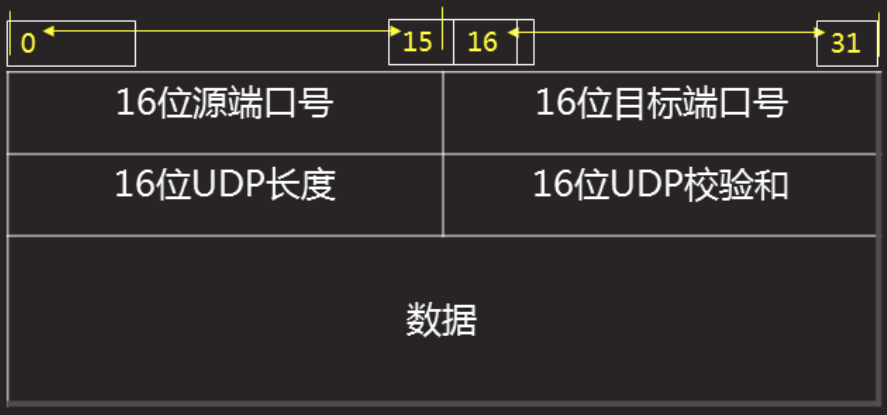
知识讲解

端口	协议	说明
21	FTP	文件传输协议，用于上传、下载
23	Telnet	用于远程登录，通过连接目标计算机的这一端口，得到验证后可以远程控制管理目标计算机
25	SMTP	简单邮件传输协议，用于发送邮件
53	DNS	域名服务，当用户输入网站的名称后，由DNS负责将它解析成IP地址，这个过程中用到的端口号是53
80	HTTP	超文本传输协议，通过HTTP实现网络上超文本的传输

UDP协议

UDP的封装格式

知识讲解



UDP的应用

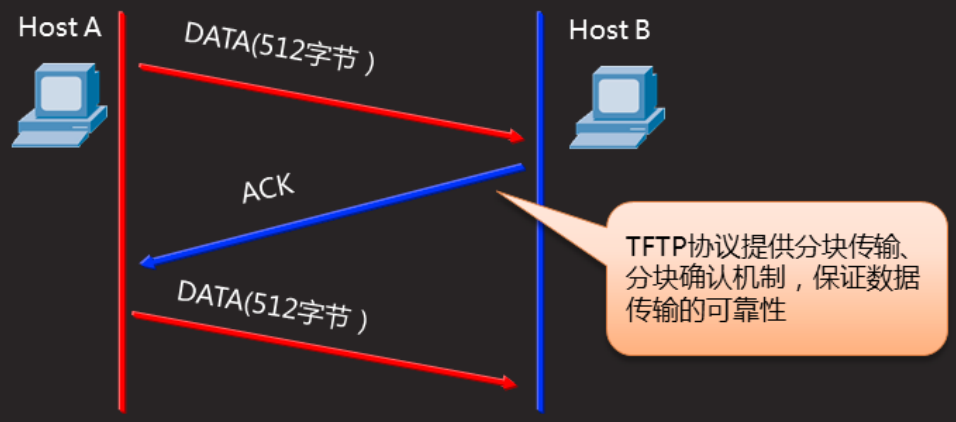
知识讲解

端 口	协 议	说 明
69	TFTP	简单文件传输协议
53	DNS	域名服务
123	NTP	网络时间协议

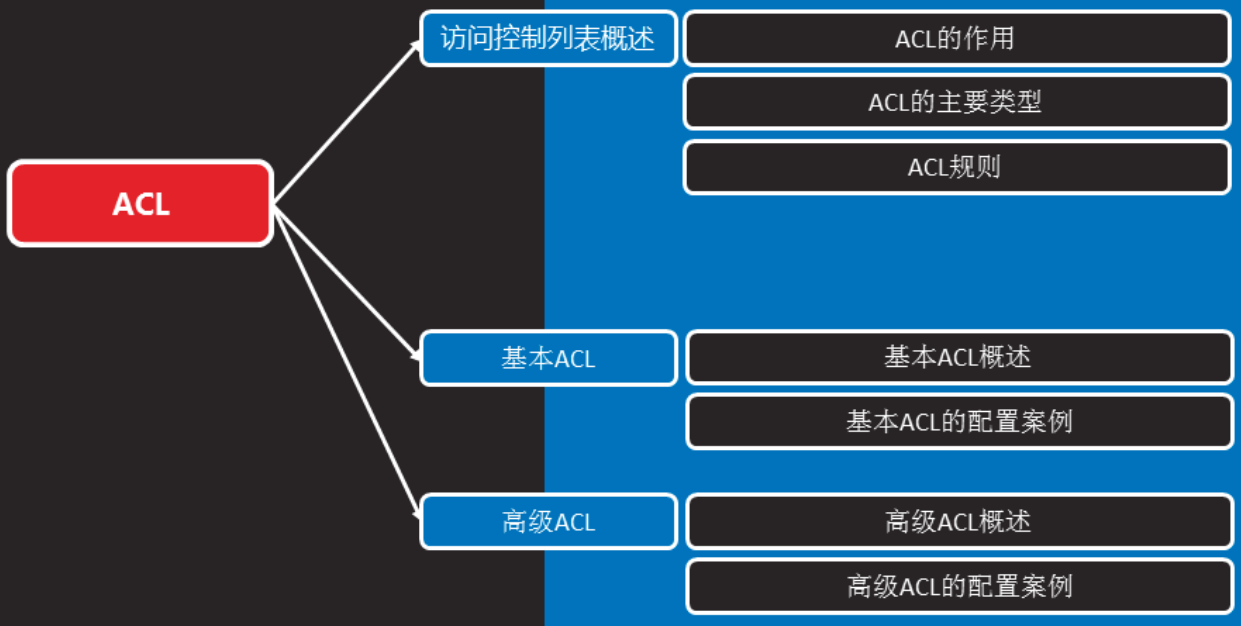
UDP的流控和差错控制

- UDP缺乏可靠机制
- UDP只有校验和来提供差错控制
  - 需要上层协议来提供差错控制：例如TFTP协议

知识讲解



ACL



Tedu.cn 达内教育

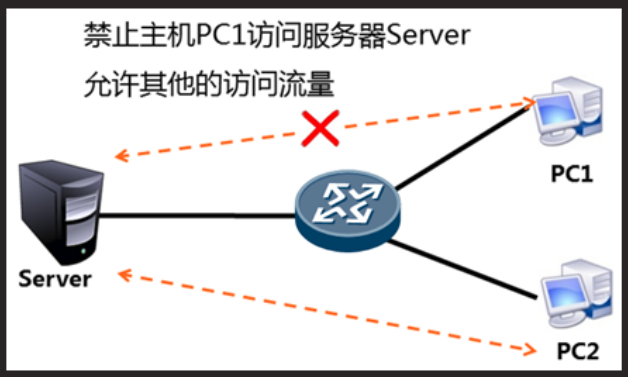
访问控制列表概述

Tedu.cn 达内教育

ACL的作用

- 访问控制列表（Access Control List，ACL）是应用在路由器接口的指令列表（即规则）

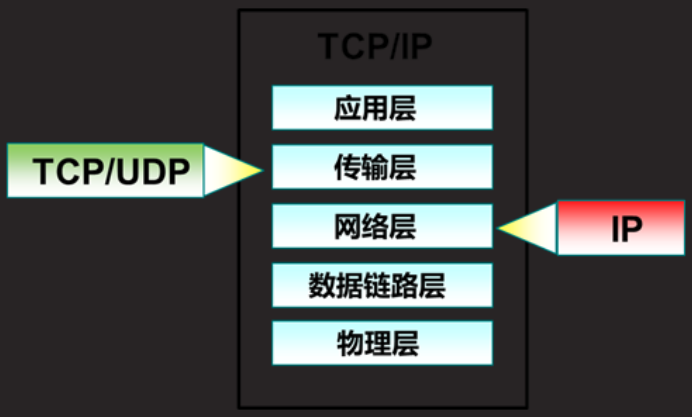
知识讲解



ACL的作用（续1）

知识讲解

- 读取第三层、第四层报文头信息
- 根据预先定义好的规则对报文进行过滤



ACL的主要类型

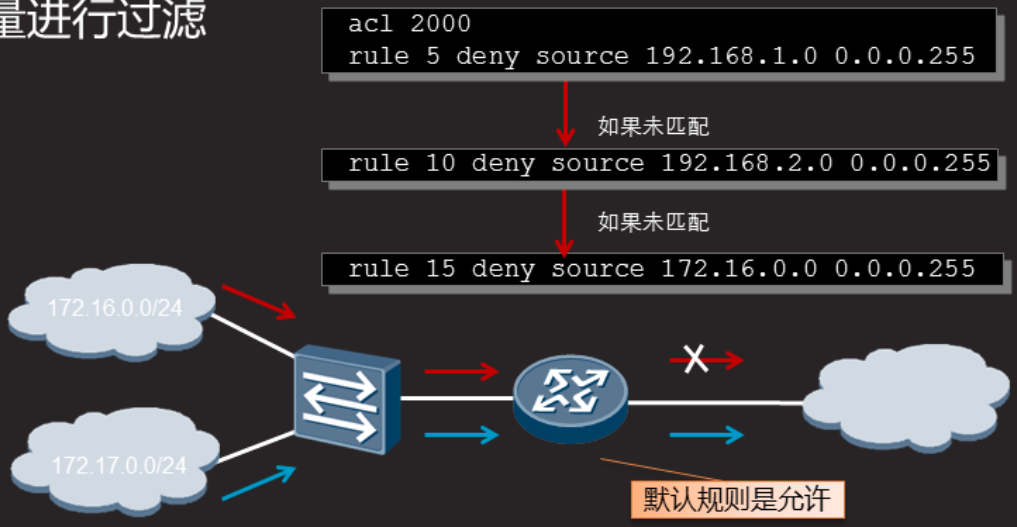
知识讲解

分类	编号范围	参数
基本ACL	2000-2999	源IP地址
高级ACL	3000-3999	源IP地址、目的IP地址、 源端口、目的端口、协议

ACL规则

- 每个ACL可以包含多个规则，路由器根据规则对数据流量进行过滤

知识讲解



基本ACL

基本ACL概述

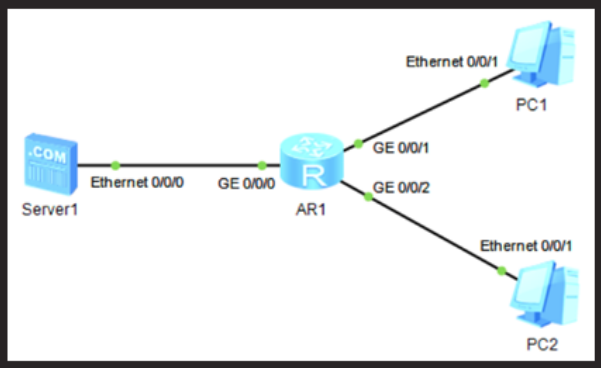
知识讲解

- 华为基本ACL
  - 基于源IP地址过滤数据包
  - 列表号是2000～2999

基本ACL的配置案例

知识讲解

- 需求描述
  - 禁止PC1网络访问服务器Server1
  - 允许其他所有的访问流量



192.168.1.0/24

192.168.100.0/24

192.168.2.0/24

基本ACL的配置案例（续1）

知识讲解

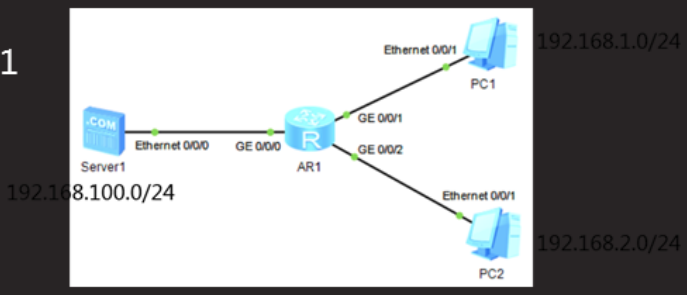
- 需求描述
  - 禁止PC1访问服务器Server1
  - 允许其他所有的访问流量

```
[Huawei]acl 2000
[Huawei-acl-basic-2000]rule 5 deny source 192.168.1.1 0
[Huawei-acl-basic-2000]rule 10 permit source any
[Huawei-acl-basic-2000]quit
[Huawei]int g0/0/1
[Huawei-GigabitEthernet0/0/1]traffic-filter inbound acl 2000
```

基本ACL的配置案例（续2）

知识讲解

- 需求描述
  - 禁止PC1访问服务器Server1
  - 允许其他所有的访问流量



查看ACL

```
[Huawei] display acl 2000
```

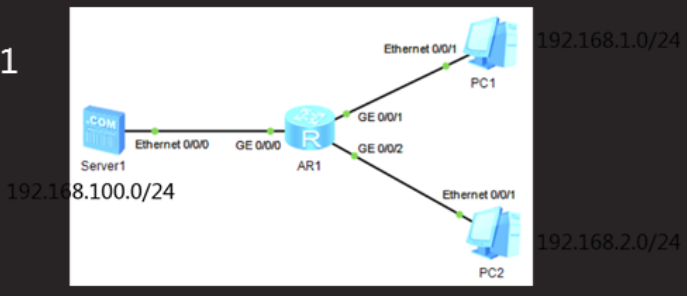
或

```
[Huawei] display acl all
```

基本ACL的配置案例（续3）

知识讲解

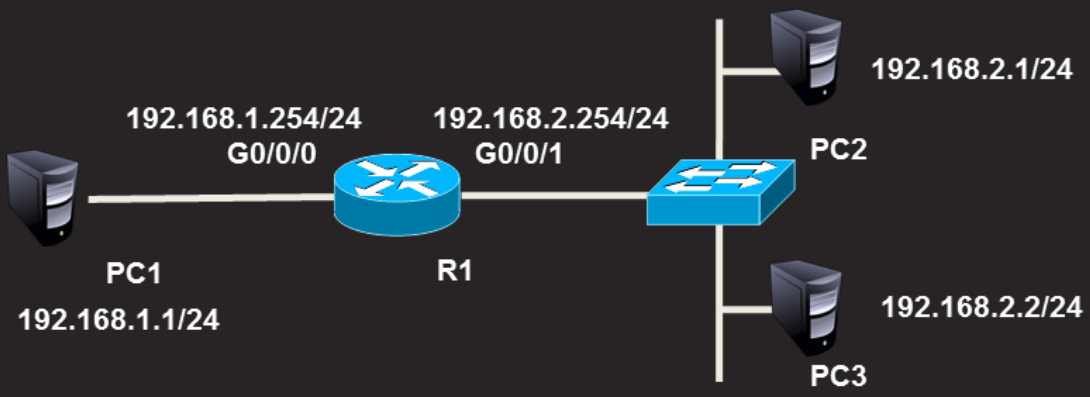
- 需求描述
  - 禁止PC1访问服务器Server1
  - 允许其他所有的访问流量
- 测试
  - PC1不能ping通Server1
  - PC2可以ping通Server1



案例2：基本ACL的配置（1）

- 需求描述
  - 禁止主机PC2与PC1通信，而允许所有其他的流量

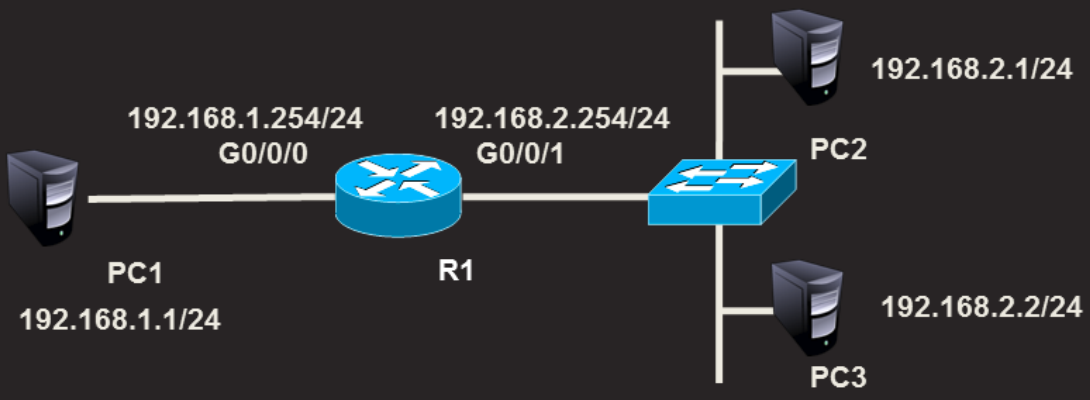
课堂练习



案例3：基本ACL的配置（2）

- 需求描述
  - 允许主机pc2与pc1互通，而禁止其他设备访问pc1

课堂练习



高级ACL

高级ACL概述

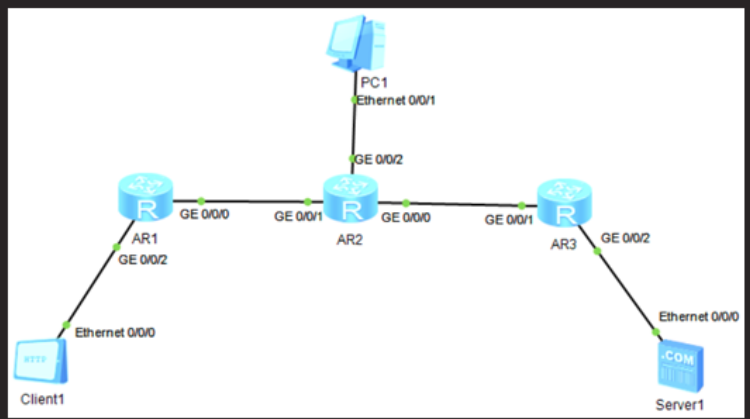
知识讲解

- 华为高级ACL
  - 基于源IP地址、目的IP地址、源端口、目的端口、协议过滤数据包
  - 列表号是3000～3999

高级ACL的配置案例

知识讲解

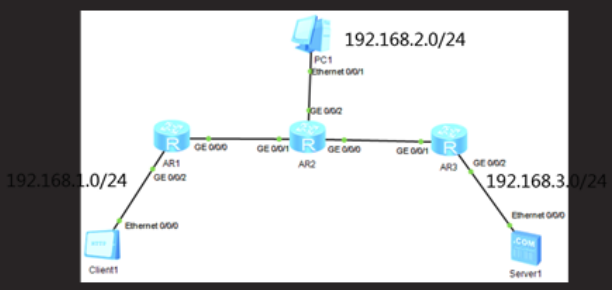
- 需求描述
  - 允许Client1访问Server1的Web服务
  - 允许Client1访问网络192.168.2.0/24
  - 禁止Client1访问其它网络



高级ACL的配置案例（续1）

知识讲解

- 需求描述
  - 允许Client1访问Server1的Web服务
  - 允许Client1访问网络192.168.2.0/24
  - 禁止Client1访问其它网络

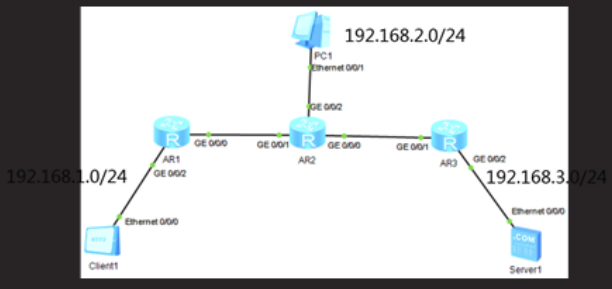



```
[AR1]acl 3000
[AR1-acl-adv-3000]rule 5 permit tcp source 192.168.1.1 0 destination 192.168.3.1
 0 destination-port eq 80
[AR1-acl-adv-3000]rule 10 permit ip source 192.168.1.1 0 destination 192.168.2.0
 0.0.0.255
[AR1-acl-adv-3000]rule 15 deny ip source any
[AR1-acl-adv-3000]quit
[AR1]int g0/0/2
[AR1-GigabitEthernet0/0/2]traffic-filter inbound acl 3000
```

高级ACL的配置案例（续2）

知识讲解

- 需求描述
  - 允许Client1访问Server1的Web服务
  - 允许Client1访问网络192.168.2.0/24
  - 禁止Client1访问其它网络

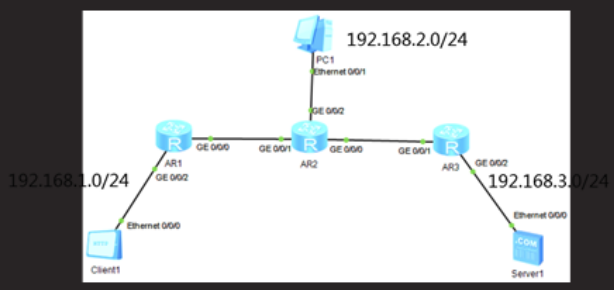


查看ACL
[AR1] display acl 3000
或
[AR1] display acl all

高级ACL的配置案例（续3）

知识讲解

- 需求描述
  - 允许Client1访问Server1的Web服务
  - 允许Client1访问网络192.168.2.0/24
  - 禁止Client1访问其它网络

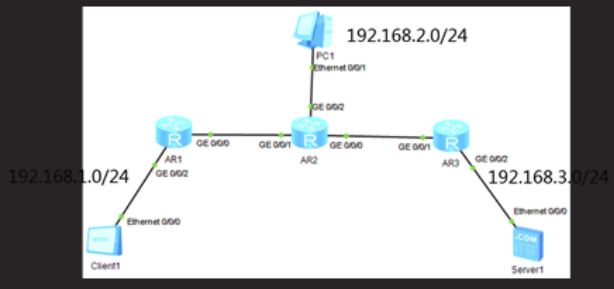



```
[AR1]ip route-static 0.0.0.0 0.0.0.0 192.168.12.2
[AR3]ip route-static 0.0.0.0 0.0.0.0 192.168.23.2
[AR2]ip route-static 192.168.1.0 255.255.255.0 192.168.12.1
[AR2]ip route-static 192.168.3.0 255.255.255.0 192.168.23.3
```

高级ACL的配置案例（续4）

知识讲解

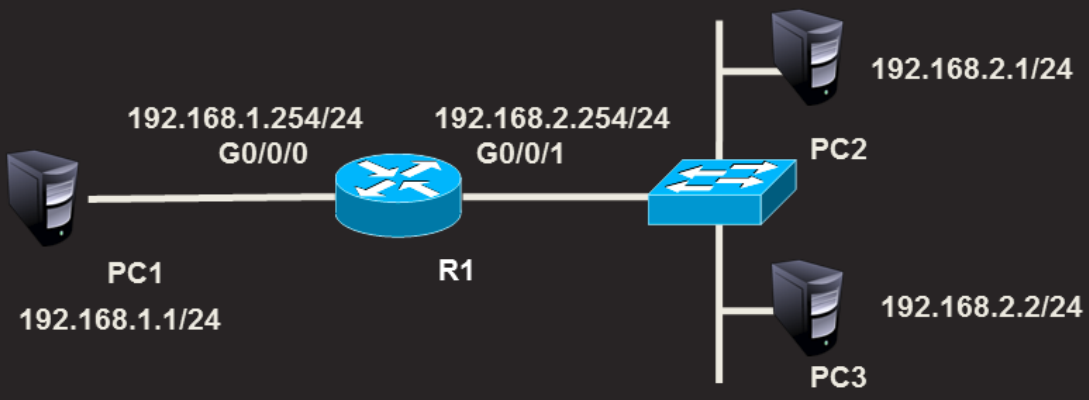
- 需求描述
  - 允许Client1访问Server1的Web服务
  - 允许Client1访问网络192.168.2.0/24
  - 禁止Client1访问其它网络
- 测试
  - Client1可以访问Server1的Web服务
  - Client1可以ping通网络192.168.2.0/24
  - Client1不能ping通网络192.168.3.0/24



案例4：高级ACL的配置

- 通过配置高级acl禁止pc2访问pc1的ftp服务，禁止pc3访问pc1的www服务器，所有主机的其他服务不受限制

课堂练习



总结和答疑