第8章

访问控制

主要内容

- 访问控制概述
- 访问控制策略
- 网络访问控制的应用

8.1 访问控制的概念

- 访问控制是为了限制访问主体（或称为发起者，是一个主动的实体，如用户、进程、服务等）对访问客体（需要保护的资源）的访问权限，从而使计算机系统在合法范围内使用。访问控制机制决定用户及代表一定用户利益的程序能做什么，以及做到什么程度。

访问控制由两个重要过程组成

- 通过认证来检验主体的合法身份；
- 通过授权（Authorization）来限制用户对资源的访问级别。

访问控制的最基本概念

- 主体（Subject）
  - 访问的发起者，通常包括人、进程和设备。
  - 根据主体权限不同可以分为四类：特殊用户、一般用户、审计用户、作废的用户
- 客体（Object）
  - 接受访问的被动实体
  - 通常包括文件和文件系统、磁盘和磁带卷标、远程终端、信息管理系统的事务处理及其应用、数据库中的数据、应用资源等。

访问控制的最基本概念

- 访问（Access）
  - 使信息在主体和客体之间流动的一种交互方式。
- 访问许可（Access Permissions）
  - 决定了谁能够访问系统，能访问系统的何种资源以及如何使用这些资源。
- 控制策略
  - 控制策略是主体对客体的访问规则集，这个规则集直接定义了主体对客体的作用行为和客体对主体的条件约束。

- **访问控制**决定了谁能够访问系统，能访问系统的何种资源以及如何使用这些资源。

- 访问控制的手段包括用户识别代码、口令、登录控制、资源授权（例如用户配置文件、资源配置文件和控制列表）、授权核查、日志和审计。

访问控制策略

- 自主访问控制
- 强制访问控制
- 基于角色的访问控制
- 基于任务的访问控制
- 基于对象的访问控制

自主访问控制

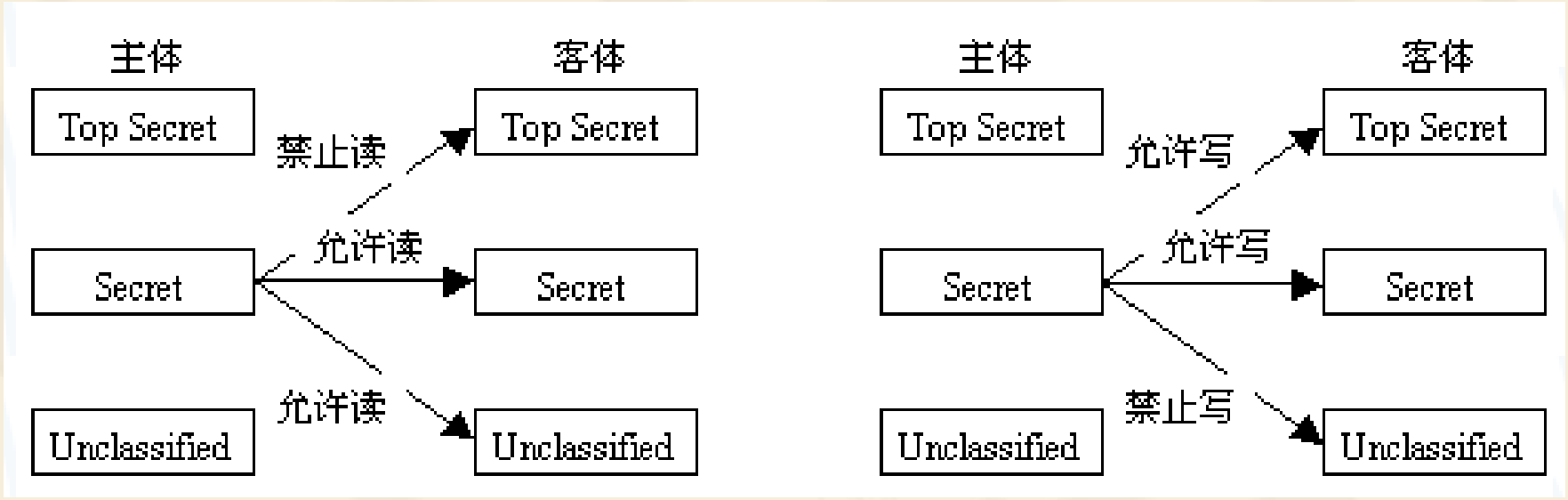
- 根据主体的身份及允许访问的权限进行决策。
- 如果一个主体拥有对某个客体的访问权，那么他可以自主地将这个访问权授予其它主体，也可以随时收回这个访问权。
- 灵活性高，被大量采用。
- 缺点：
  - 信息在移动过程中其访问权限关系会被改变。如用户**A**可将其对目标**O**的访问权限传递给用户**B,**从而使不具备对**O**访问权限的**B**可访问**O**。

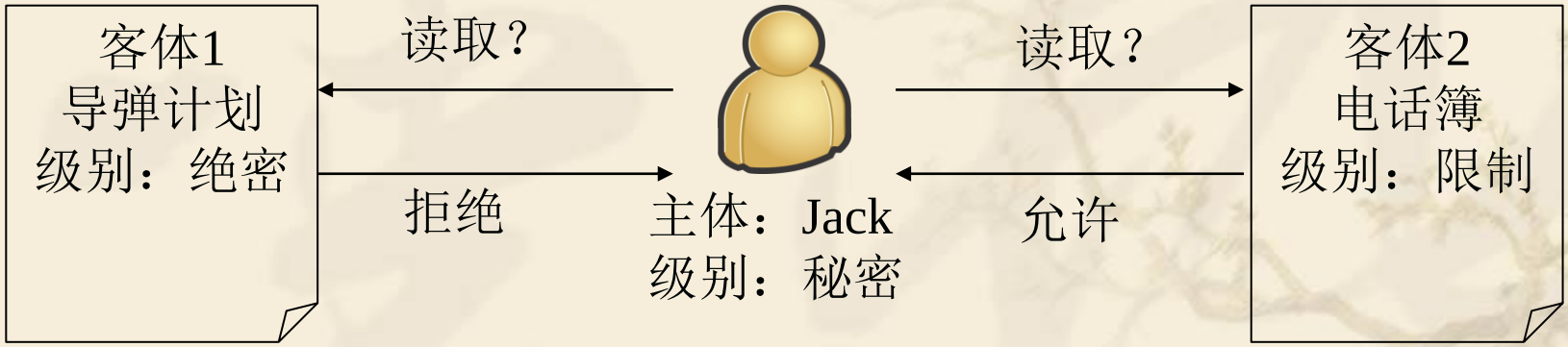
强制访问控制

- 每个用户及文件都被赋予一定的安全级别，用户不能改变自身或任何客体的安全级别，即不允许单个用户确定访问权限，只有系统管理员可以确定用户和组的访问权限。系统通过比较用户和访问的文件的安全级别来决定用户是否可以访问该文件。
- 安全级别一般有五级：绝密级（Top Secret，T）、秘密级（Secret，S）、机密级（Confidential，C）、限制级（Restricted，R）和无密级（Unclassified，U），其中T＞S＞C＞R＞U。

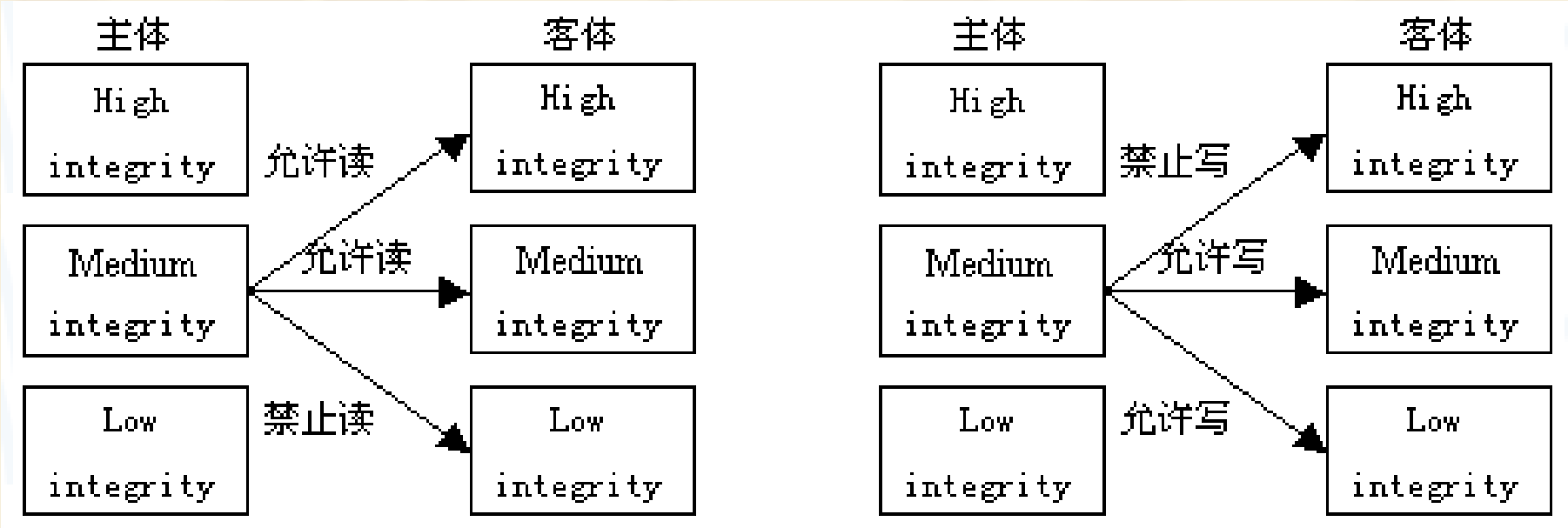
- 用户与访问的信息的读写关系将有四种，即：
  - 下读（read down）：用户级别大于文件级别的读操作。
  - 上写（write up）：用户级别低于文件级别的写操作。
  - 下写（write down）：用户级别大于文件级别的写操作。
  - 上读（read up）：用户级别低于文件级别的读操作。

Bell-Lapadula安全模型: 不上读/不下写





Biba安全模型: 不下读/不上写



基于角色的访问控制

- Role-based Access，RBAC
- 基本思想：将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。
- 角色由系统管理员定义，角色成员的增减也只能由系统管理员来执行，即只有系统管理员有权定义和分配角色。
- 用户与客体无直接联系，他只有通过角色才享有该角色所对应的权限，从而访问相应的客体。因此用户不能自主地将访问权限授给别的用户

基于任务的访问控制

- 前面几种访问控制没有时间限制，只要主体拥有对客体的访问权限，主体就可以无数次地执行该权限。
- 在基于任务的访问控制中，对象的访问权限控制并不是静止不变的，而是随着执行任务的上下文环境发生变化。
- TBAC从工作流中的任务角度建模，可以依据任务和任务状态的不同，对权限进行动态管理。因此，TBAC非常适合分布式计算和多点访问控制的信息处理控制以及在工作流、分布式处理和事务管理系统中的决策制定。

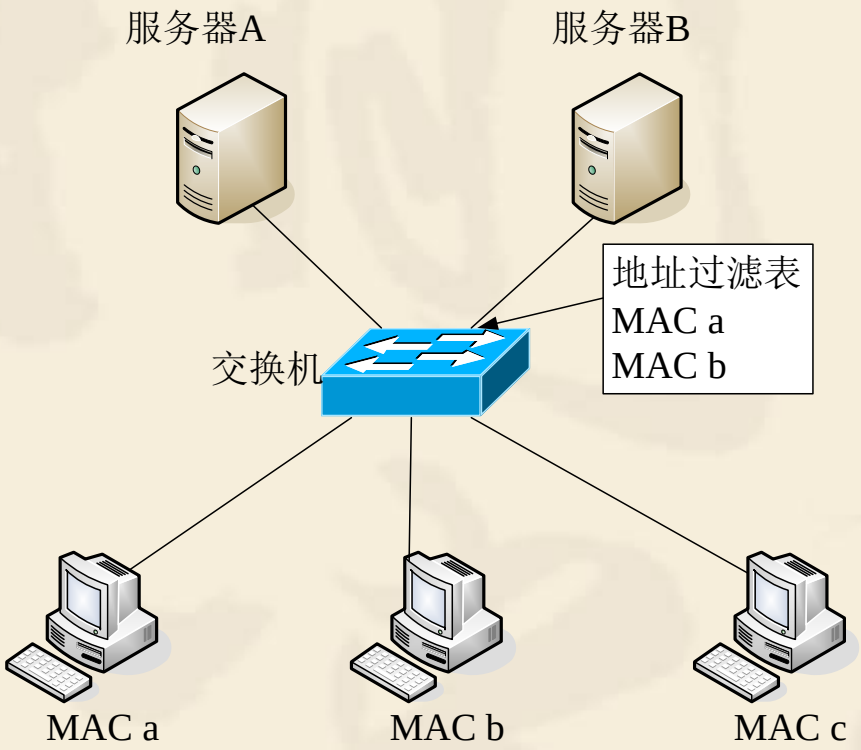
基于对象的访问控制

- Object-based Access Control，OBAC
- 将访问控制列表与受控对象或受控对象的属性相关联，并将访问控制选项设计成为用户、组或角色及其对应权限的集合
- 允许对策略和规则进行重用、继承和派生操作。派生对象可以继承父对象的访问控制设置
- 可以减轻由于信息资源的派生、演化和重组等带来的分配、设定角色权限等的工作量。

8.3 网络访问控制的应用

- MAC地址过滤
- VLAN隔离
- ACL访问控制列表
- 防火墙访问控制

MAC地址过滤



- a和b可以访问服务器B，c不能访问B
- a、b、c都可以访问A

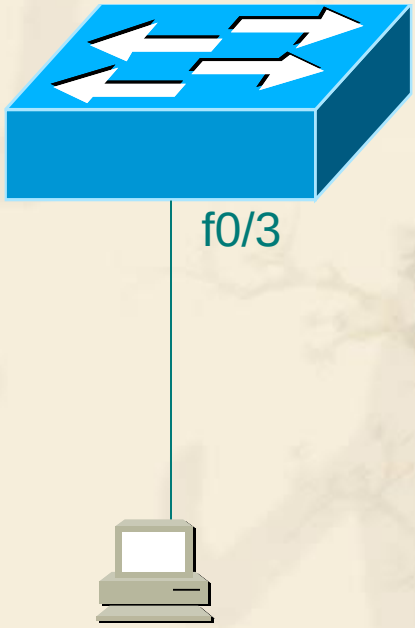
交换机的端口安全

- 交换机端口安全功能，是指针对交换机的端口进行安全属性的配置，从而控制用户的安全接入。
- 交换机端口安全功能包括：
  - 限制交换机端口的最大连接数
    - 控制交换机端口下连的主机数，并防止用户进行恶意的ARP欺骗。
  - 针对交换机端口进行MAC地址、IP地址的绑定。
    - 可以针对IP地址、MAC地址、IP+MAC进行灵活的绑定，实现对用户的严格控制，防止常见的内网攻击。

交换机端口安全配置

- 你是一个公司的网络管理员，公司要求对网络进行严格控制。为了防止公司内部用户的IP地址冲突，防止公司内部的网络攻击和破坏行为，为每一位员工分配了固定的IP地址，并且限制只允许公司员工主机可以使用网络，不得随意连接其他主机。
- 例如：某员工分配的IP地址是172.16.1.55，主机MAC地址是00-06-2B-DE-13-B4，该主机连接在1台交换机上。

- 某员工分配的IP地址是172.16.1.55，主机MAC地址是00-06-2B-DE-13-B4，该主机连接在1台交换机上。



步骤1 配置交换机端口的最大连接数

Switch# configure terminal
Switch(config)# interface range fastethernet 0/1-23
Switch(config-if-range)# switchport port-security
! 开启交换机的端口安全功能
Switch(config-if-range)# switchport port-security maximum 1
!配置端口的最大连接数为1
Switch(config-if-range)# switchport port-security violation shutdown
! 配置安全违例的处理方式为shutdown
查看交换机的端口安全配置：
Switch# show port-security

步骤2 配置交换机端口的地址绑定

- 查计算机的MAC地址
- 配置交换机端口的地址绑定

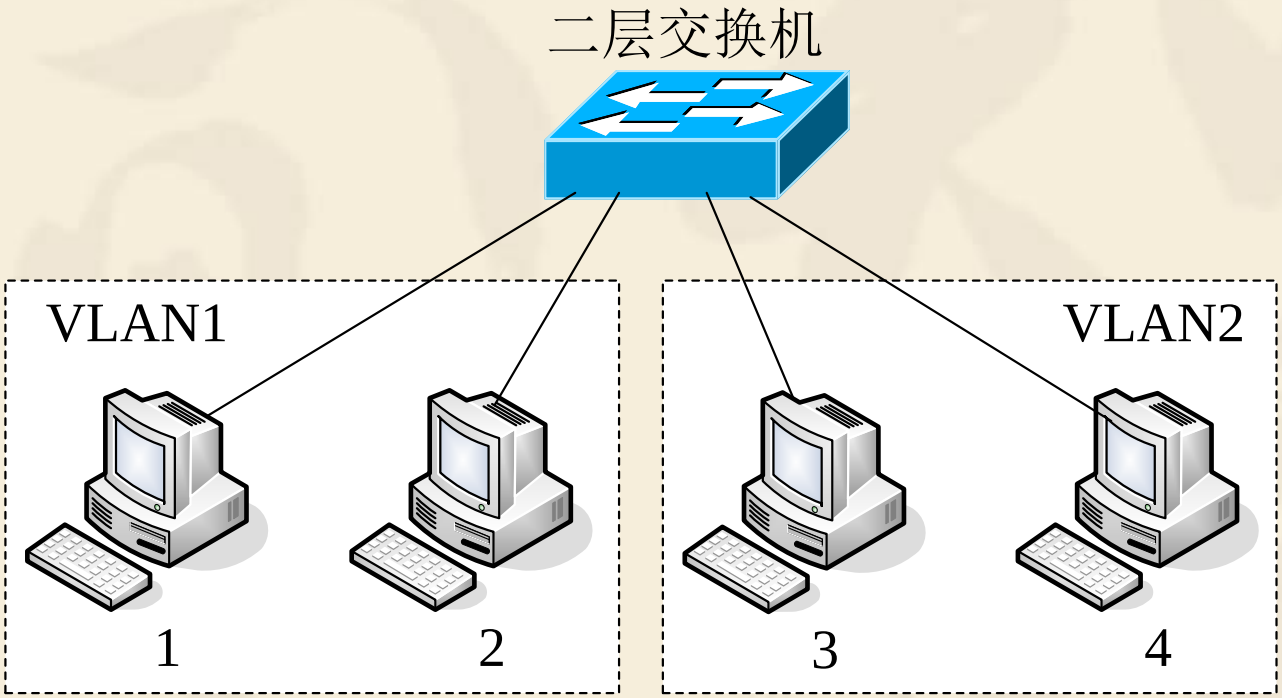
```
switch(config)# interface fastethernet 0/3
switch(config-if)# switchport port-security
switch(config-if)# switchport port-security mac-address
                    0006.2bde.13b4 ip-address 172.16.1.55
```

查看地址安全绑定配置：

```
Switch# show port-security address
```

8.3.2 VLAN隔离

- 通过VLAN技术，可以把一个网络系统中的众多网络设备分成若干个虚拟的“工作组”，组和组之间的网络设备在二层上互相隔离，形成不同的广播域，进而将广播流量限制在不同的广播域中。



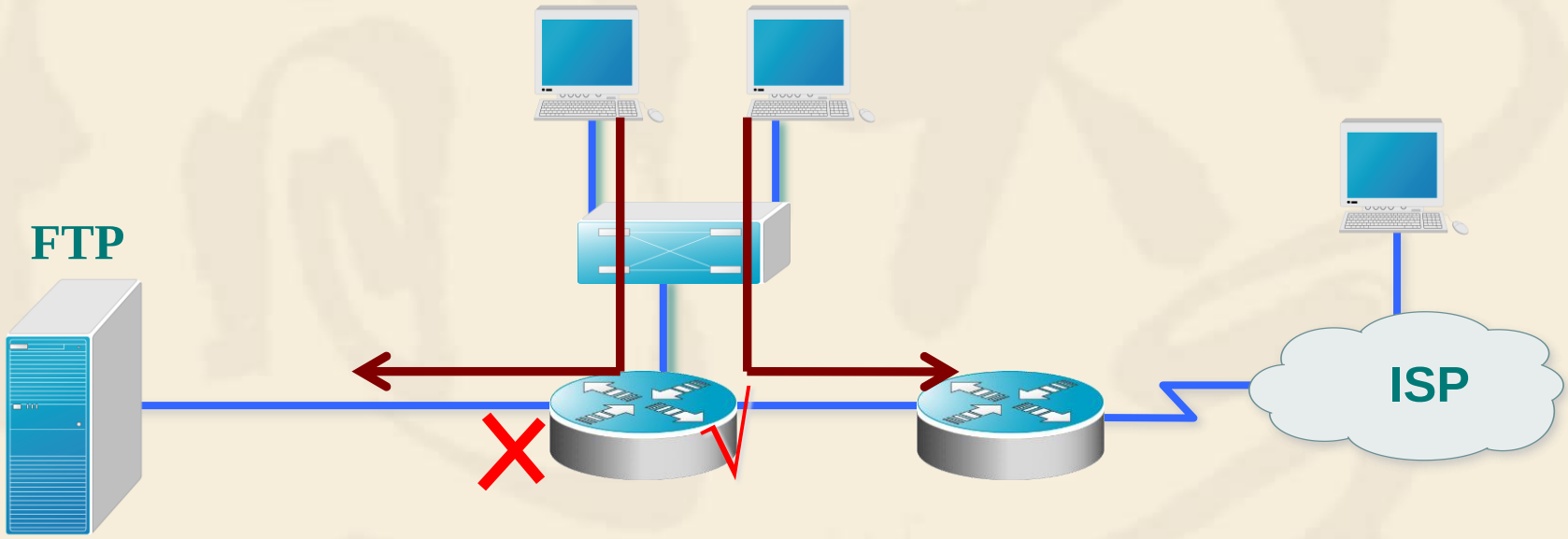
- 工作站1、2划分到VLAN1中，3、4划分到VLAN2中，这样1、2工作站之间可以相互通信，3、4工作站之间也可以相互通信，但两个组之间不可以直接通信

- VLAN技术可以保证网络设备间的隔离，但对于同一台服务器，只能做到同时向多个VLAN组全面开放或是只向某个VLAN组全面开放，而不能针对个别用户进行限制。而在通常情况下，一台服务器会提供多种服务，担当多种服务器角色，同时为多个VLAN组用户提供不同的服务，这样带来了一定的安全隐患。

8.3.3 ACL访问控制列表

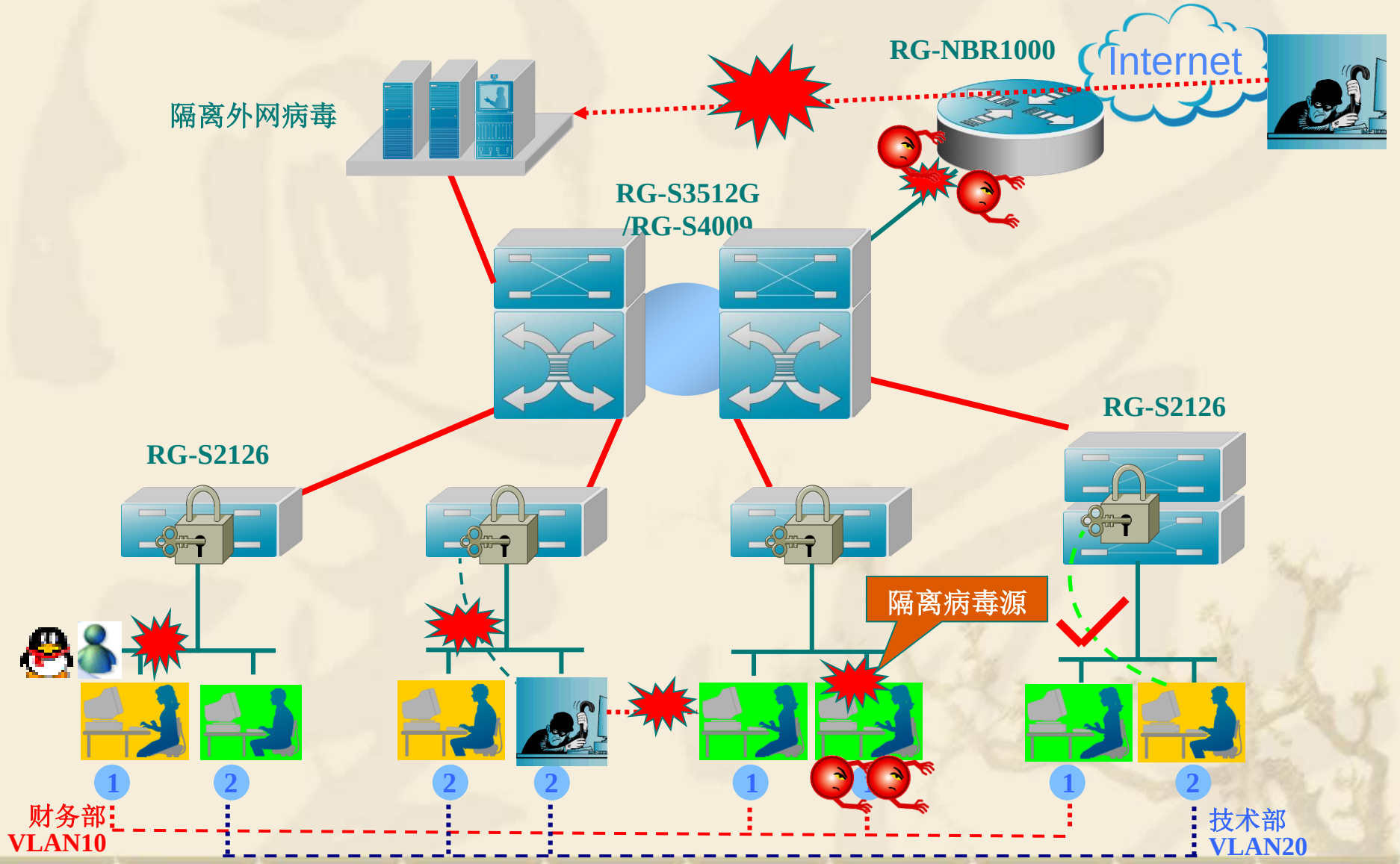
- 访问控制列表在路由器中被广泛采用，它是一种基于包过滤的流向控制技术。
- 通过把源地址、目的地址以及端口号作为数据包检查的基本元素，并可以规定符合检查条件的数据包是允许通过，还是不允许通过。
- 访问控制列表可以有效地在网络层上控制网络用户对网络资源的访问，它既可以细致到两台网络设备间的具体的网络应用，也可以按网段进行大范围的访问控制管理

1、什么是访问控制列表



- Access Control list：访问控制列表，简称ACL
- ACL就是对经过网络设备的数据包，根据一定的规则，进行数据包的过滤。

2、为什么要使用访问控制列表



不同部门所属VLAN不同

3、访问列表的组成

- 定义访问列表的步骤

  第一步：定义规则（哪些数据允许通过，哪些数据不允许通过）

  第二步：将规则应用在路由器（或交换机）的接口上

- 访问控制列表的分类：

  1、标准访问控制列表

  2、扩展访问控制列表

  3、命名的访问控制列表

  4、基于时间访问控制列表

  5、专家级访问控制列表

- 访问控制列表规则元素

  源IP、目的IP、源端口、目的端口、协议、服务

4、访问列表规则的应用

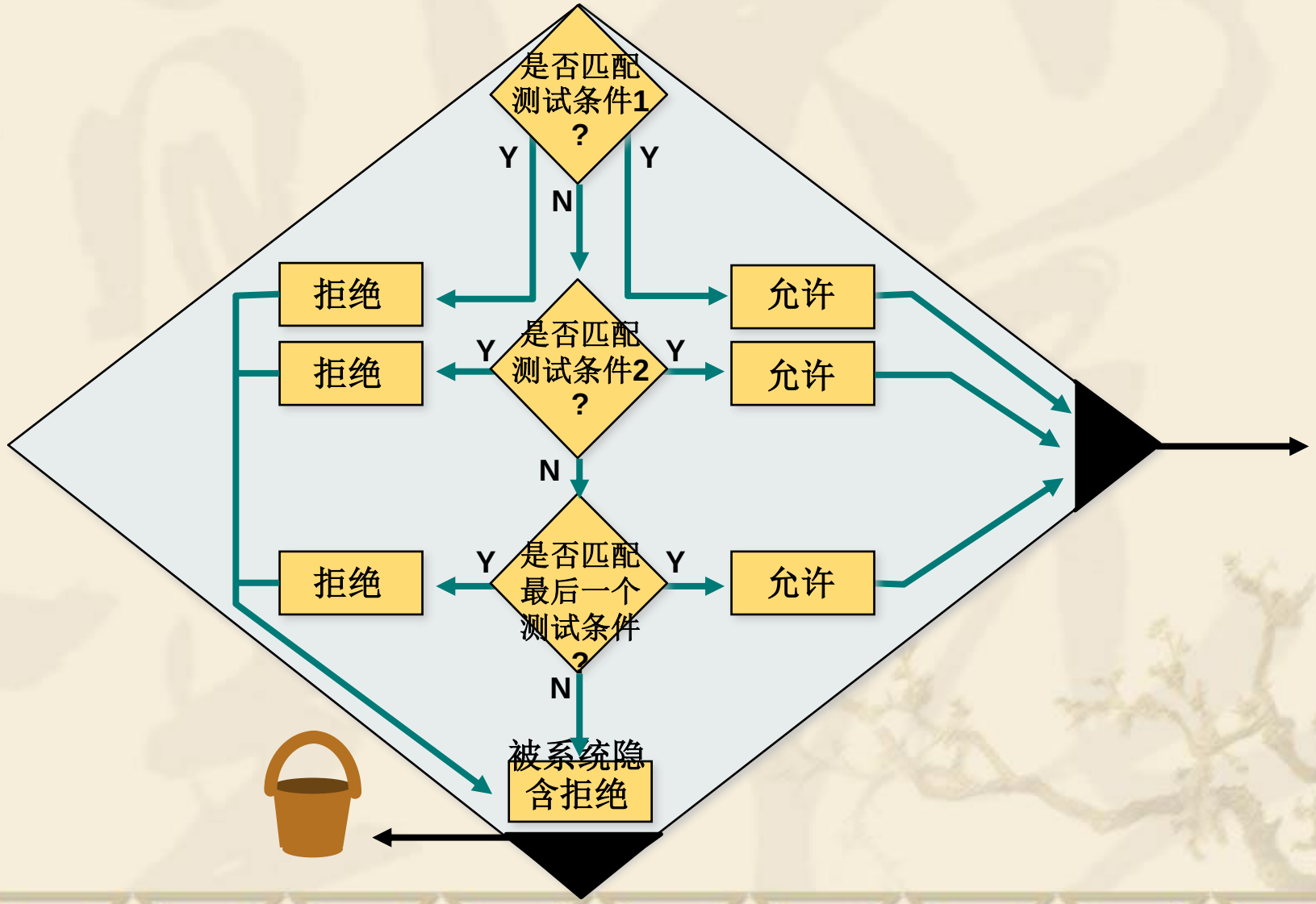
- 路由器应用访问列表，对流经接口的数据包进行控制：
  1. 入栈应用（in）
  2. 出栈应用（out） 缺省

5、ACL的基本准则

- 一切未被允许的就是禁止的。
- 按规则链来进行匹配

  使用源地址、目的地址、源端口、目的端口、协议、时间段进行匹配
- 从头到尾，至顶向下的匹配方式
- 匹配成功马上停止
- 立刻使用该规则的“允许、拒绝……”

6、一个访问列表多个测试条件



7、ACL分类

- 标准访问列表

  根据数据包源IP地址进行规则定义

- 扩展访问列表

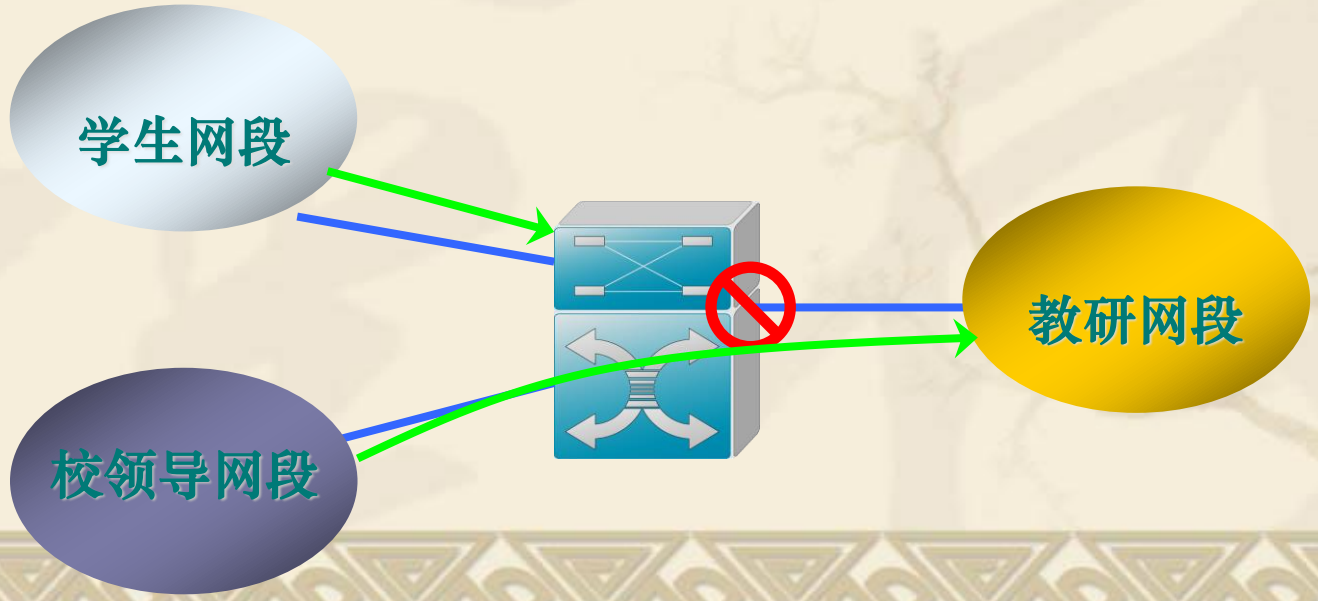
  根据数据包中源IP、目的IP、源端口、目的端口、协议进行规则定义

8、标准访问列表规则的定义（1）

- 标准的访问列表

  只能根据源IP地址，进行数据包的过滤。

  例：在校园网中，学生网段不可以访问教研网段，但校领导网段可以访问教研网段



标准访问列表（2）

1、定义标准ACL

Router(config)# access-list <1-99> { permit |deny } 源地址 [反掩码]

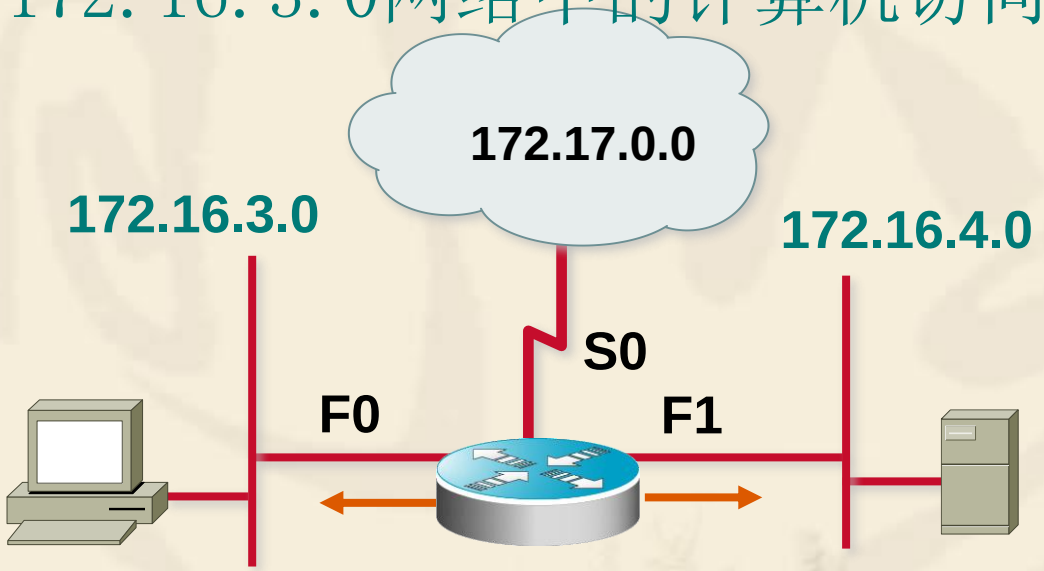
2、应用ACL到接口

Router(config-if)#ip access-group <1-99>|{name} { in | out }

in和out参数可以控制接口中不同方向的数据包，如果不配置该参数，缺省为out。

IP标准访问列表配置（3）

只允许172.16.3.0网络中的计算机访问互联网络

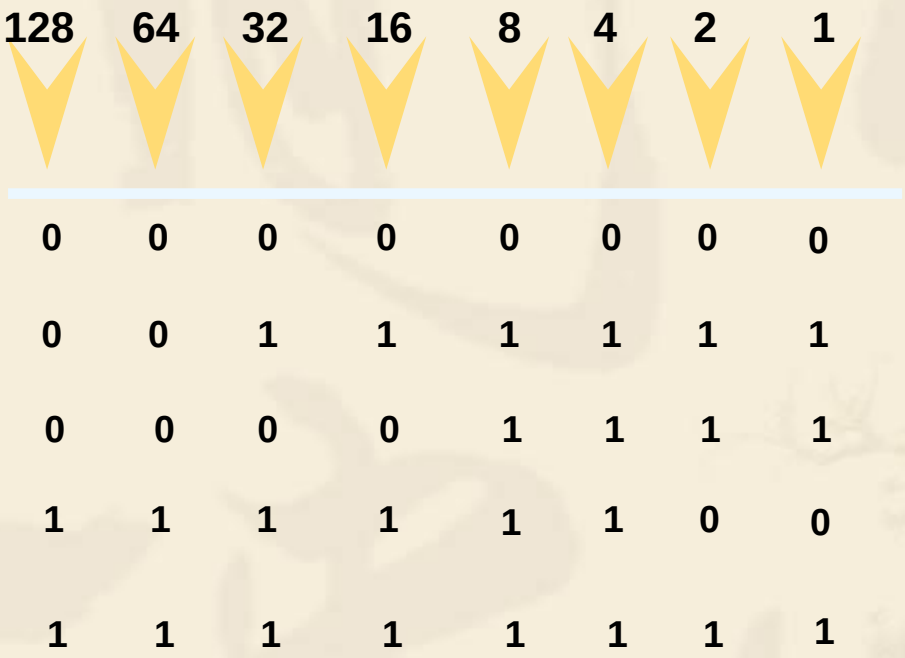



```
access-list 1 permit 172.16.3.0   0.0.0.255
access-list 1 deny 0.0.0.0   255.255.255.255

interface serial 0
ip access-group 1 out
```

配置中的反掩码（通配符）技术

通配符掩码是一个32比特位。在通配符掩码位中，0表示“检查相应的位”，1表示“不检查相应的位”。通配符掩码与IP地址是成对出现 .



0表示检查相应的地址比特

1表示不检查相应的地址比特

通配符掩码与子网掩码工作原理是不同的。在IP子网掩码中，数字1和0用来决定是网络，还是主机的IP地址。如表示172.16.0.0这个网段，使用通配符掩码应为0.0.255.255。

在通配符掩码用255.255.255.255表示所有IP地址，全为1说明所有32位都不检查相应的位，这是可以用any来取代。

0.0.0.0的通配符掩码则表示所有32位都要进行匹配，这样只表示一个IP地址，可以用host表示。

IP标准访问列表配置技术（4）

host/any----host和any分别用于指定单个主机和所有主机。

host表示一种精确的匹配，其屏蔽码为0.0.0.0。

假定我们希望允许从198.78.46.8来的报文，则使用标准的访问控制列表语句如下:

access-list 1 permit 198.78.46.8 0.0.0.0

如果采用关键字host，也可以用下面的语句来代替：

access-list 1 permit host 198.78.46.8

any是0.0.0.0 255.255.255.255的简写

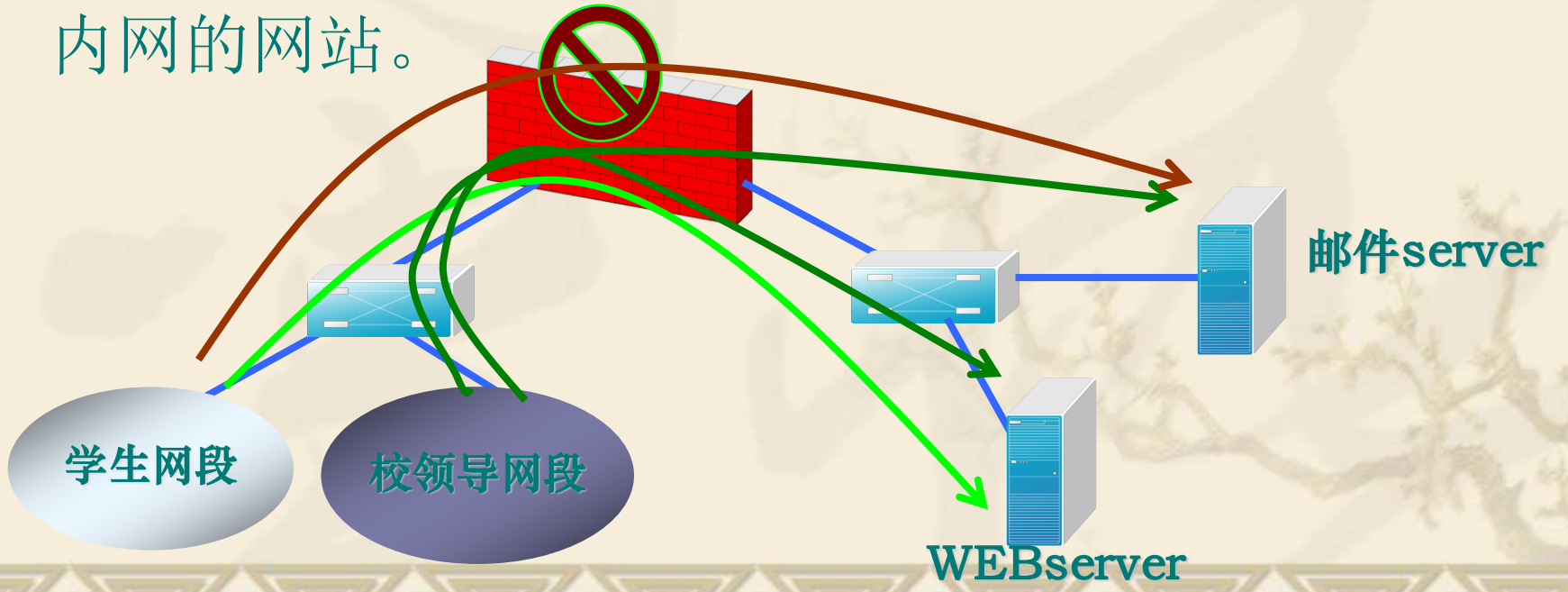
IP标准访问列表配置技术（4）

假使在我们的网络管理过程中，要阻止网络中地址为192.168.0.45的一台主机通过E0访问网络，而允许其他的机器访问网络，可以通过如下操作

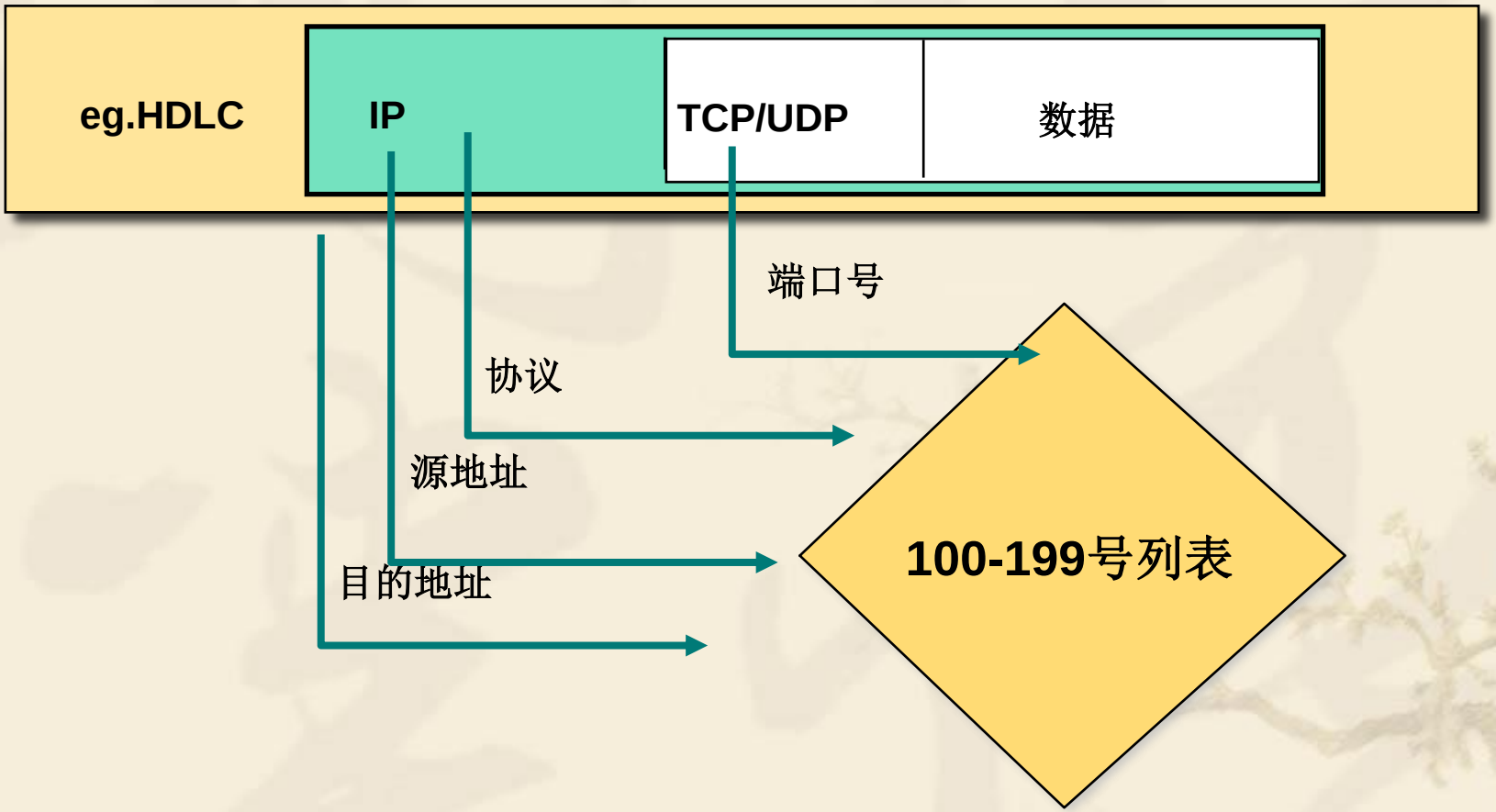
```
Router（config） # access-list 1 deny host
  192.168.0.45
Router（config） # access-list 1 permit any
Router（config） # interface ethernet 0
Router（config-if） # ip access-group 1 in
```

10、ACL分类（2）-扩展的访问列表

- 扩展的访问列表
- 扩展ACL可以根据数据包内的源、目的地址，应用服务进行过滤。例如教师网段可以访问内网的邮件服务器，而学生网不可以访问，但可以访问内网的网站。



IP扩展访问列表（1）



IP扩展访问列表的配置（2）

1、定义扩展的ACL

Router(config)# access-list <100-199> { permit /deny }
协议 源地址 反掩码 [源端口] 目的地址 反掩码
[目的端口]

- 协议项定义了需要被过滤的协议，例如IP、TCP、UDP、ICMP等等
- 端口号可以用几种不同的方法来指定
  - 显式地指定 :www,http,stmp…
  - 使用数字:80,21
  - 操作符:eq,gt,lt,neq,range port1 port2
  - access-list 101 permit tcp any host 198.78.46.8 eq smtp
    允许来自任何主机的TCP报文到达特定主机198.78.46.8的smtp服务端口(25);
  - access-list 101 permit tcp any host 198.78.46.3 eq www
    允许任何来自任何主机的TCP报文到达指定的主机198.78.46.3的www或http服务端口(80)

2、应用ACL到接口

Router(config-if)#ip access-group <100-199> |{name}
{ in | out }

IP扩展访问列表配置实例（3）

创建一条Extended IP ACL，允许网络192.168.0.0内所有主机，可以访问HTTP服务器172.168.12.3。

Switch (config)# access-list 111 permit tcp 192.168.0.0 0.0.255.255 any host 172.168.12.3 eq www

11、ACL分类（3）---命名访问控制列表

1、定义命名的扩展ACL

- ip access-list extended name

{ deny | permit } protocol {source wildcard [operator port] destination wildcard [operator port]

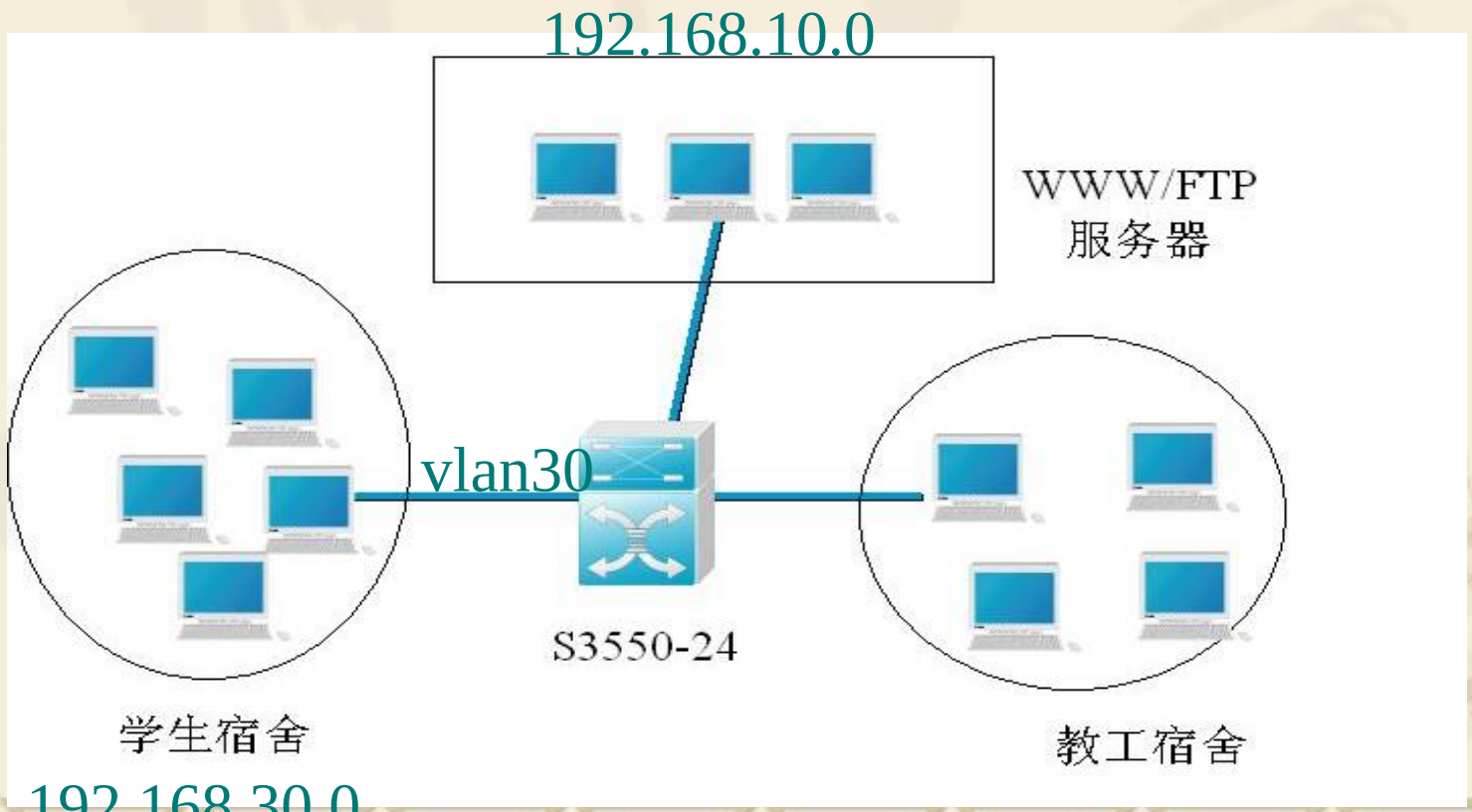
2、应用ACL到接口

Router(config-if)#ip access-group name { in | out }

也可以用命名来定义标准访问控制列表

ip access-list standard name

在3550-24交换机上连着学校提供WWW和FTP的服务器，另外还连接着学生宿舍楼和教工宿舍楼，学校规定学生只能对服务器进行FTP访问，不能进行WWW访问，教工则没有此限制。



☼ 配置命名扩展IP访问控制列表

3550-24(config) # ip access-list extended denystudentwww
!定义命名扩展访问列表

3550-24(config-ext-nacl)# deny tcp 192.168.30.0 0.0.0.255
192.168.10.0 0.0.0.255 eq www
! 禁止WWW服务

3550-24(config-ext-nacl)# permit ip any any
!允许其他服务

☼ 把访问控制列表在接口下应用

3550-24(config)# int vlan 30
3550-24(config-if)# ip access-group denystudentwww in

12、ACL分类（4）-- 基于时间访问控制列表

☼ 基于时间的访问列表:是指在标准或扩展的访问列表的基础上，增加时间段的应用规则。

☼ **Time-range** 时间段分为两种：绝对性时间段和周期性时间段。

在周期时间段里有一些常见参数:

weekdays表示每周的工作日（周一至周五）

weekend表示周末（周六、日）

daily表示每天。

- 基于时间的访问控制列表的格式：

第一部分：定义时间段

第二部分：定义扩展访问控制列表规则

第三部分：将ACL添加到相应的端口中

定义时间段

time-range 时间段名称

absolute start [小时：分钟] [日 月 年] [end] [小时：分钟] [日 月 年]

- time-range softer ！定义了一个时间段，名称为softer

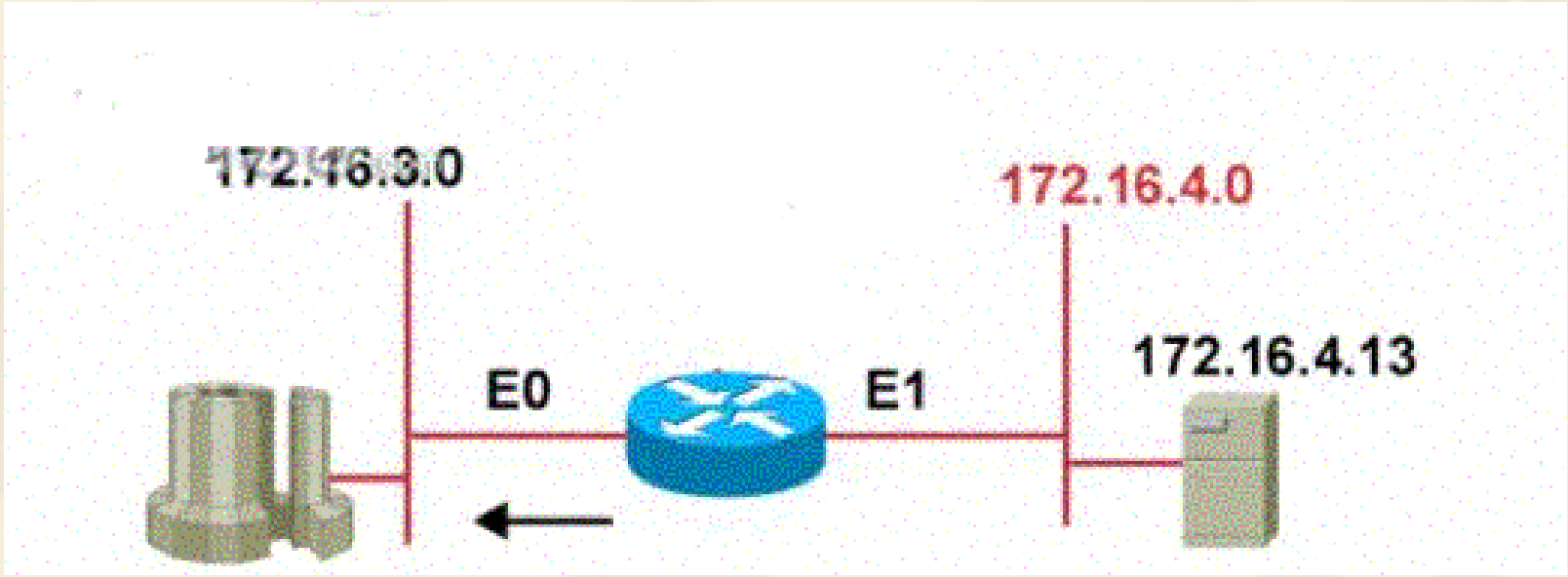
absolute start 0:00 1 may 2005 end 12:00 1 june 2005

！起始时间为2005年5月1日零点,结束时间为6月1日中午12点

- time-range softer ！定义时间段名称为softer

periodic weekend 00:00 to 23:59

！定义具体时间范围，为每周周末（6，日）的0点到23点59分。



172.16.3.0网段的用户，在周末时间不许访问172.16.4.13上的FTP资源，在工作时间能下载该FTP资源。

time-range softer ！定义时间段名称为softer
periodic weekend 00:00 to 23:59
！定义时间范围每周周末（6，日）0点到23点59分

access-list 101 deny tcp any 172.16.4.13 0.0.0.0
eq ftp time-range softer
！禁止时间段softer范围内访问172.16.4.13的FTP服务
access-list 101 permit ip any any
！容许其他时间段和其他条件下的正常访问

int ethernet 1 ！进入E1端口。
ip access-group 101 out ！应用ACL 101

13、ACL分类（5）-专家级访问控制列表

专家级访问控制列表，可以利用MAC地址、IP地址、VLAN号、传输端口号、协议类型、时间ACL等元素进行灵活组合，定义规则。从而更加灵活地控制网络的流量，保证网络的安全运行。

✡ 在S2126G上配置专家级访问控制列表

Switch(config)# expert access-list extended test1

!定义专家级访问列表test1

Switch(config-ext-nacl)# deny ip host 172.16.1.1 host 00e0.9823.9526 host 160.16.1.1 any

! 禁止IP地址为172.16.1.1 和MAC地址00e0.9823.9526 的主机访问IP地址为160.16.1.1 的主机

Switch(config-ext-nacl)# permit any any any any

Switch (config)# interface fastethernet 0/1

!进入接口F0/1配置模式

Switch (config-if)# expert access-group test1 in

!在接口F0/1的入方向上应用专家级访问列表test1

访问列表的验证

- 显示全部的访问列表
  - Router#show access-lists
- 显示指定的访问列表
  - Router#show access-lists <1-199>
- 显示接口的访问列表应用
  - Router#show ip interface <接口名称> <接口编号>

访问列表的注意事项

1、在进行规则匹配时，从上至下，匹配成功马上停止，不会继续匹配下面的规则。

2、所有访问列表默认规则是拒绝所有数据包

3、处理方式只有允许通过和拒绝通过

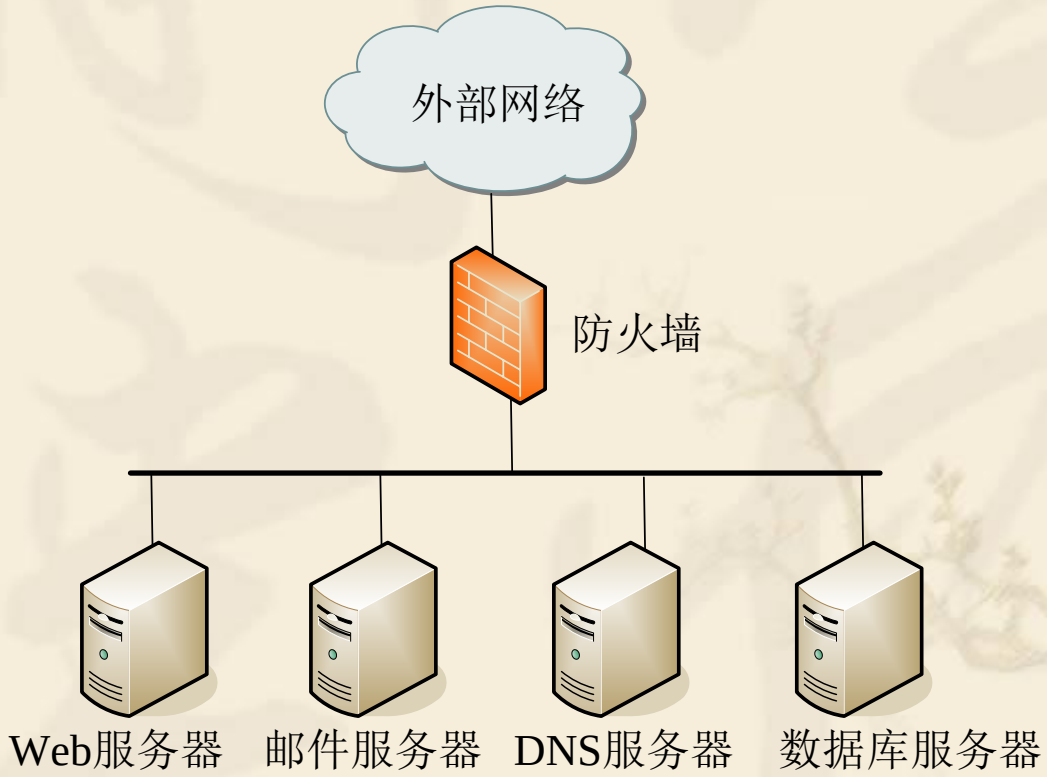
4、锐捷路由器只能编写编号方式的规则

5、锐捷交换机只能编写命名方式的规则

6、一个端口在某一方向只能应用一组访问列表

8.3.4 防火墙访问控制

- 将网络划分为内网与外网，它通过分析每一项内网与外网通信应用的协议构成，得出主机IP地址及端口号，从而规划出业务流，对相应的业务流进行控制。



结论

- 各种访问控制方式各有优缺点，由于它们采用的技术以及所要解决问题的方向相差较大，所以在现实的网络安全管理中，通常都是几种甚至是全部技术的组合。