网络安全

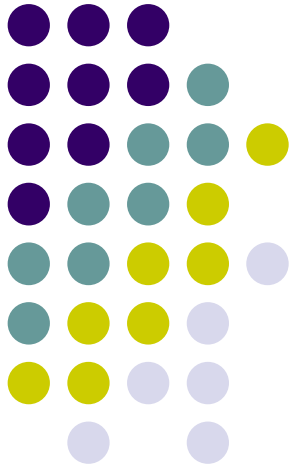
罗　敏

武汉大学计算机学院

mluo@whu.edu.cn

Tel: 13907125177

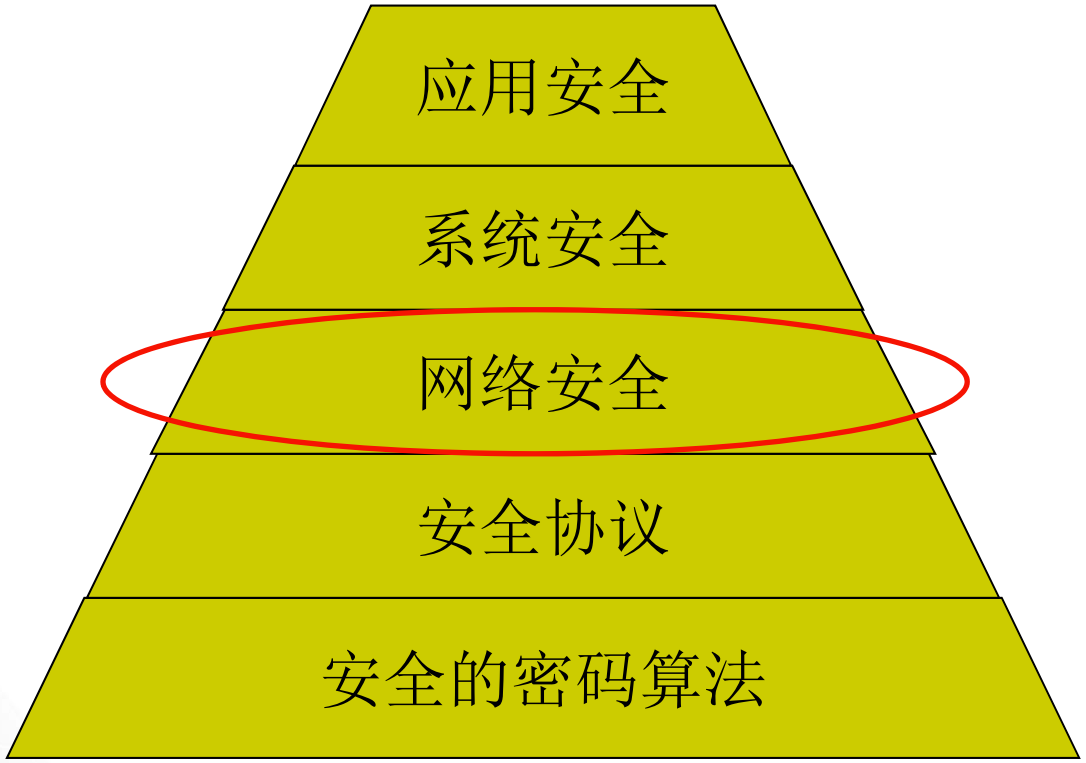
QQ：5118924



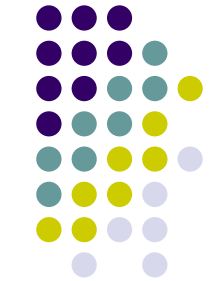
内容

- TCP/IP基础
- 防火墙
  - 防火墙的基本介绍
  - 几种防火墙的类型
  - 防火墙的配置
  - 防火墙技术的发展

安全层次

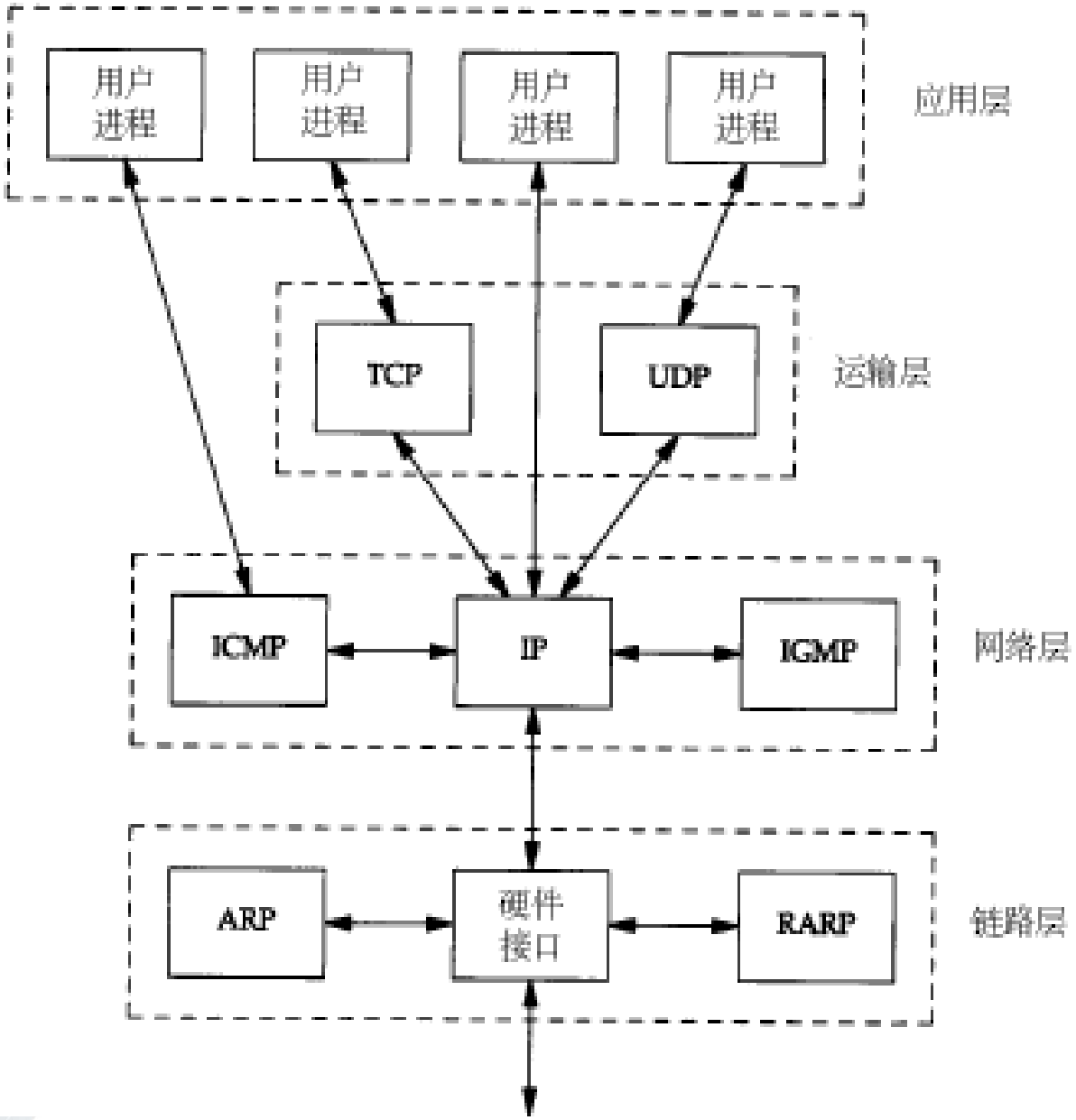


TCP/IP overview

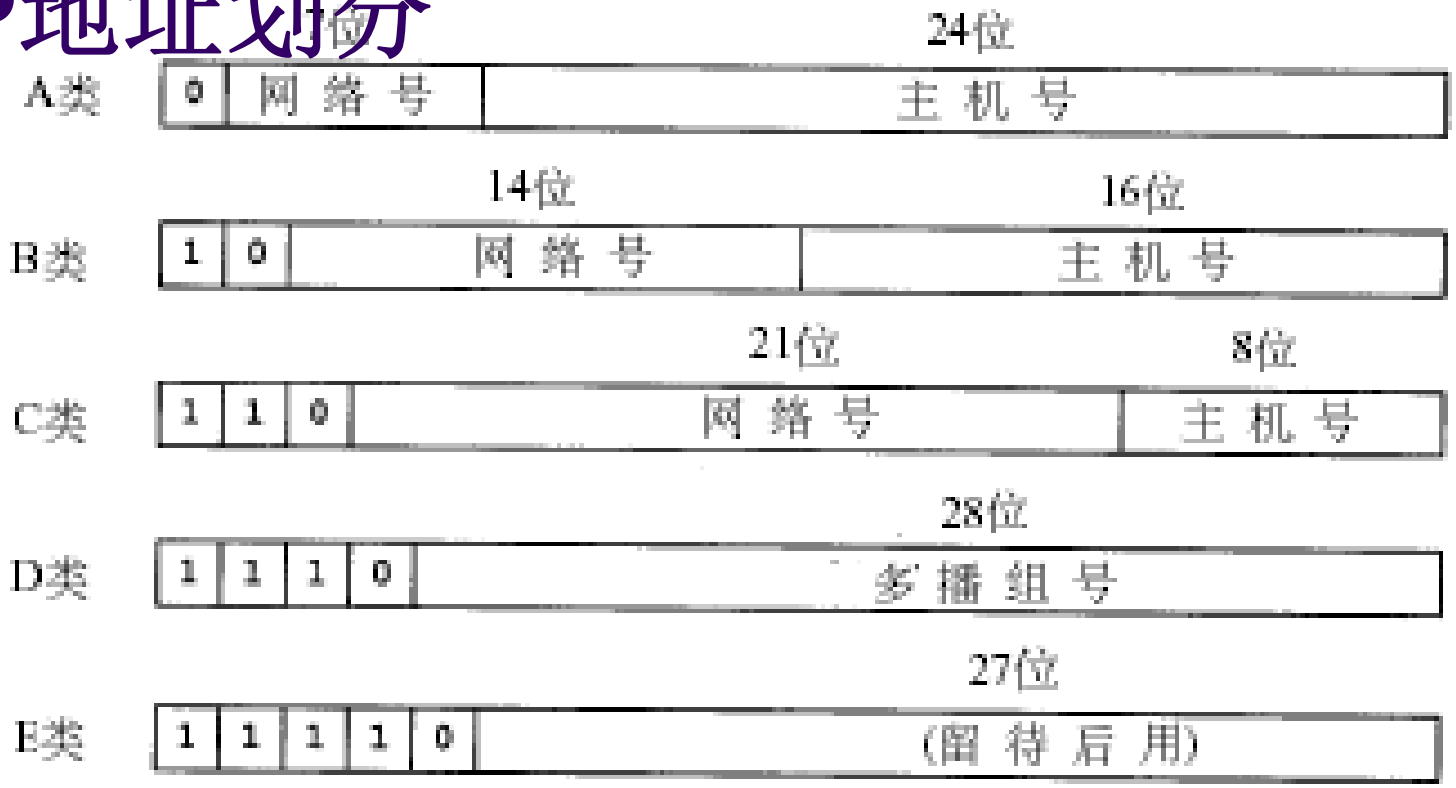


- 协议栈
- 一些数据包的格式
  - IP数据包
  - TCP/UDP数据包
- 常用的上层协议
- 几个常用工具

TCP/IP协议栈


用户进程
用户进程
用户进程
用户进程
应用层
TCP
UDP
运输层
ICMP
IP
IGMP
网络层
ARP
硬件接口
RARP
链路层

IP地址划分



- 保留私用的网络地址：
  - 10.0.0.0 - 10.255.255.255
  - 172.16.0.0 - 10.172.31.255.255
  - 192.168.0.0 - 192.168.255.255
- 还有一些具有特殊意义的网络地址，如广播地址和127.0.0.1地址等。

- 以ip地址为10.78.202.175　子网掩码为255.255.255.0

首先将这两个东西换算成二进制代码

ip地址：00001010.01001110.11001010.10101111

子网掩码：11111111.11111111.11111111.00000000

按位与之后得出网络地址：

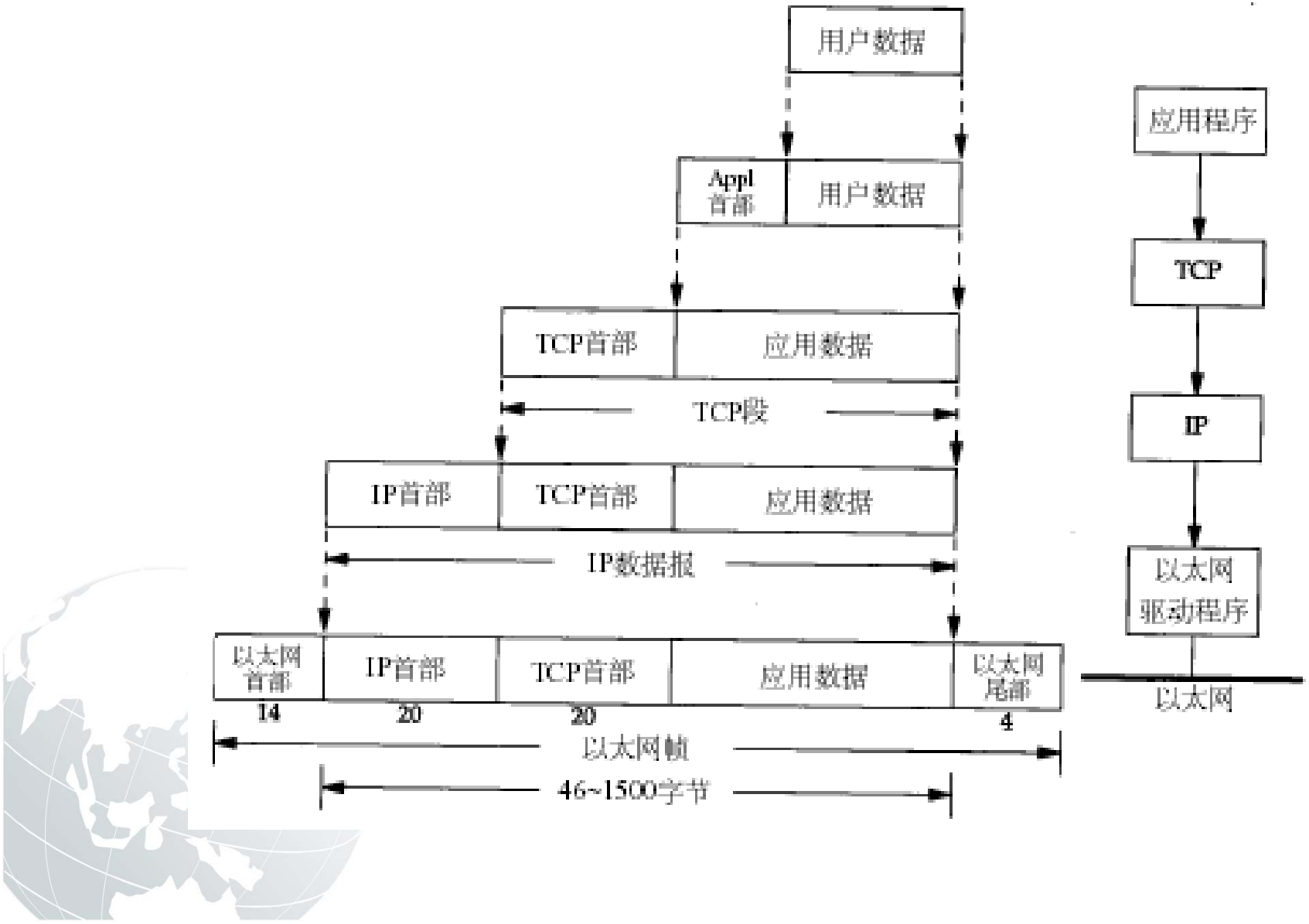
00001010.01001110.11001010.0000000

十进制表示就是10.78.202.0

这个网络地址理论上可以有255台主机，但是除去网络地址0和广播地址255之后，实际上只能有253台主机。那么我们可以知道175就是你这台机器的主机号，广播地址就是最大的主机号，也就是10.78.202.255。

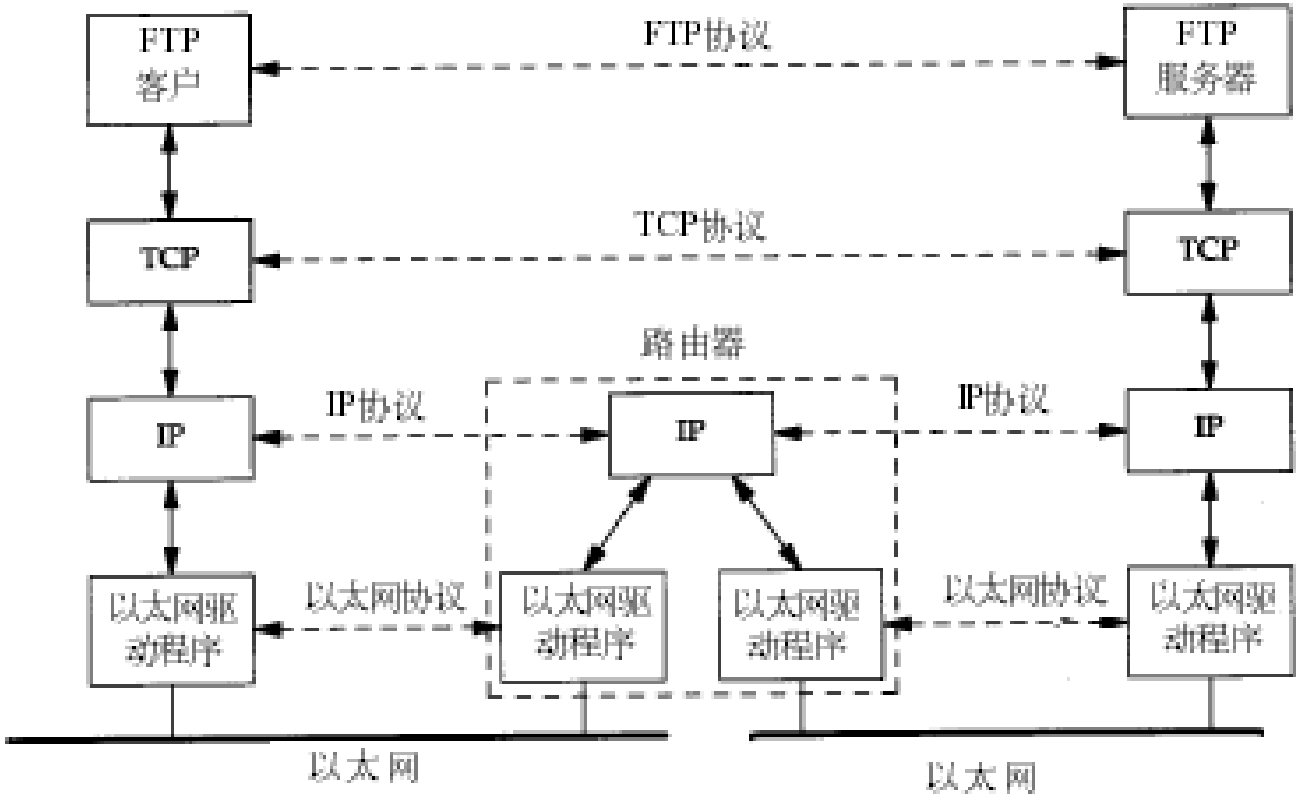
255.255.255.255 合法的广播地址 ？

协议栈各层数据包的结构

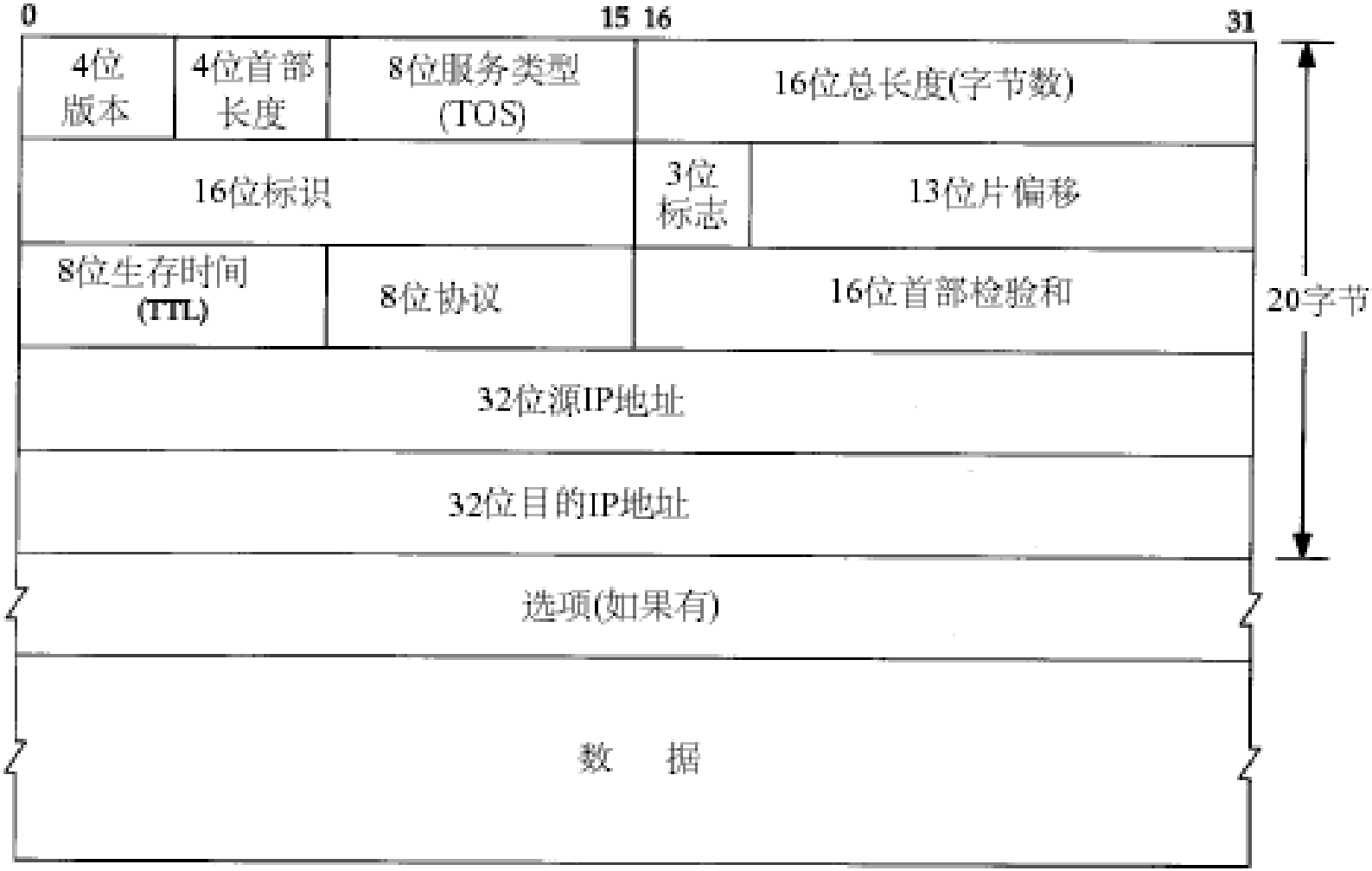


IP网络互连的原理

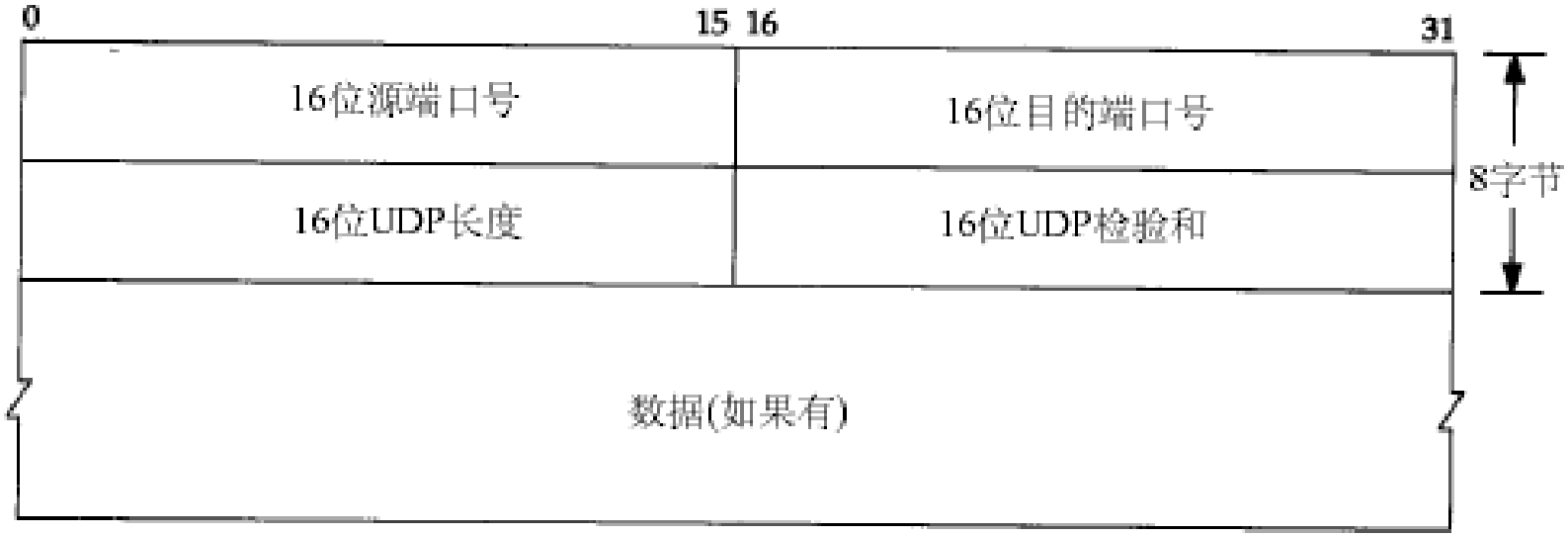
- 广播子网内部
  - ARP地址解析
    - 从MAC地址到IP地址之间的解析
- 以太网络间路由



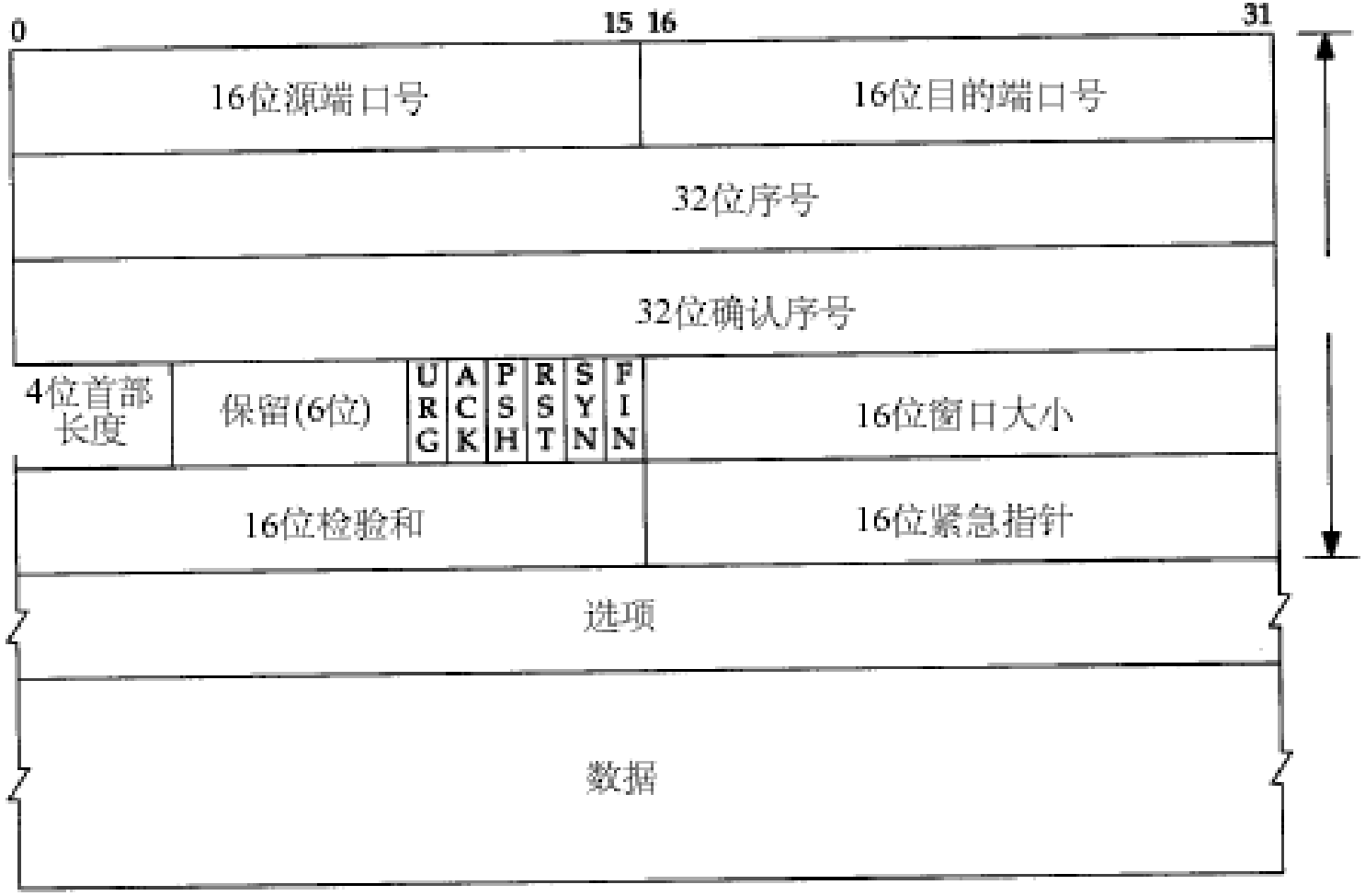
IP数据包格式


0
15 16
31
4位
版本
4位首部
长度
8位服务类型
(TOS)
16位总长度(字节数)
16位标识
3位
标志
13位片偏移
8位生存时间
(TTL)
8位协议
16位首部检验和
20字节
32位源IP地址
32位目的IP地址
选项(如果有)
数　据

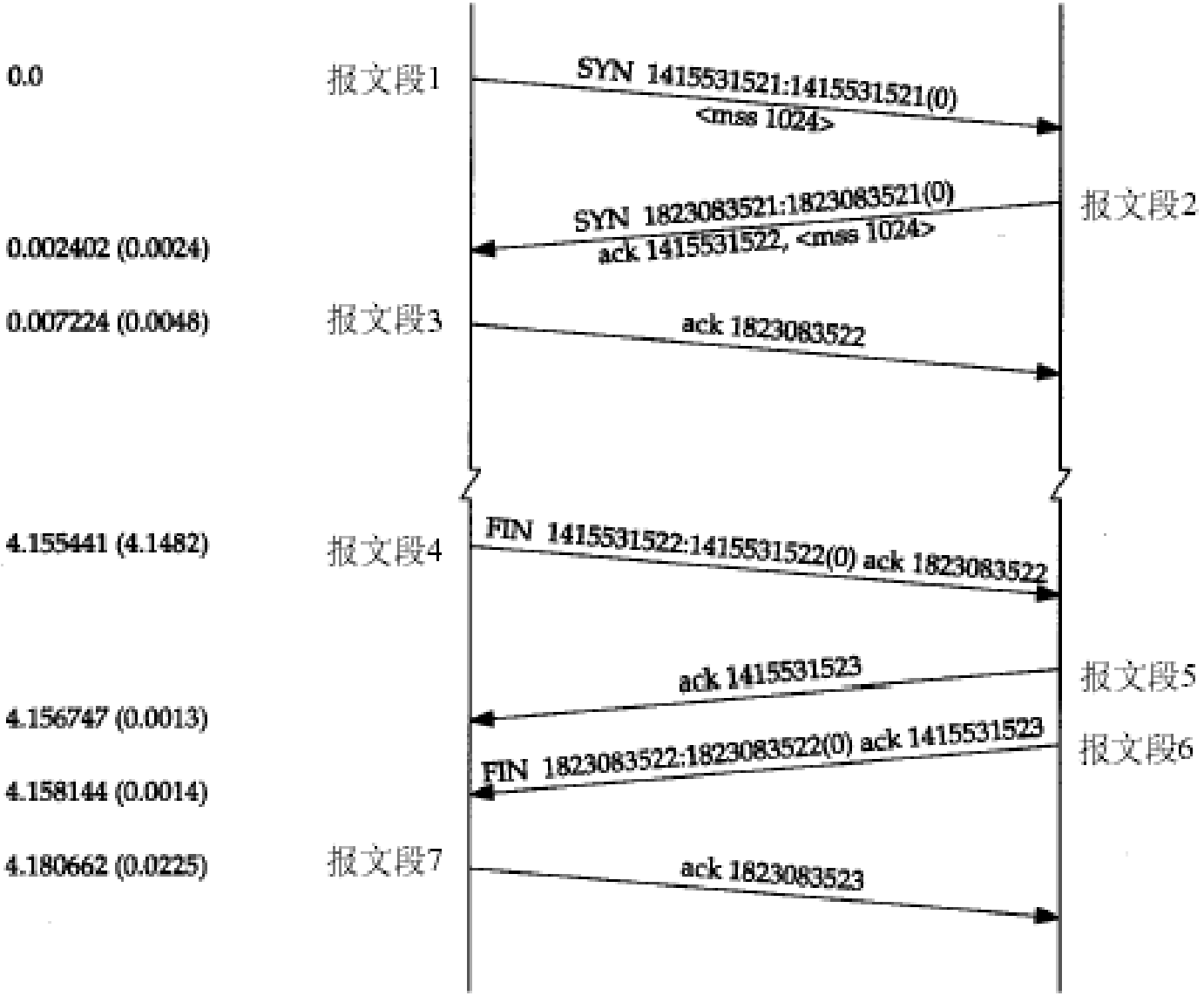
UDP数据包格式



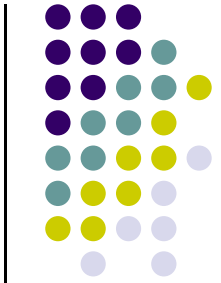
TCP数据包格式


0
15 16
31
16位源端口号
16位目的端口号
32位序号
32位确认序号
4位首部长度
保留(6位)
URG
ACK
PSH
RST
SYN
FIN
16位窗口大小
16位检验和
16位紧急指针
选项
数据

TCP连接的建立和终止时序图



常用的上层协议



- DNS: 53/tcp,udp
- FTP: 20,21/tcp,udp
- telnet: 23/tcp,udp
- HTTP: 80/tcp,udp
- NNTP: 119/tcp,udp
- SMTP: 25/tcp,udp
- POP3: 110/tcp,udp
- 参考：IANA提供的port-numbers.txt

常用的网络工具

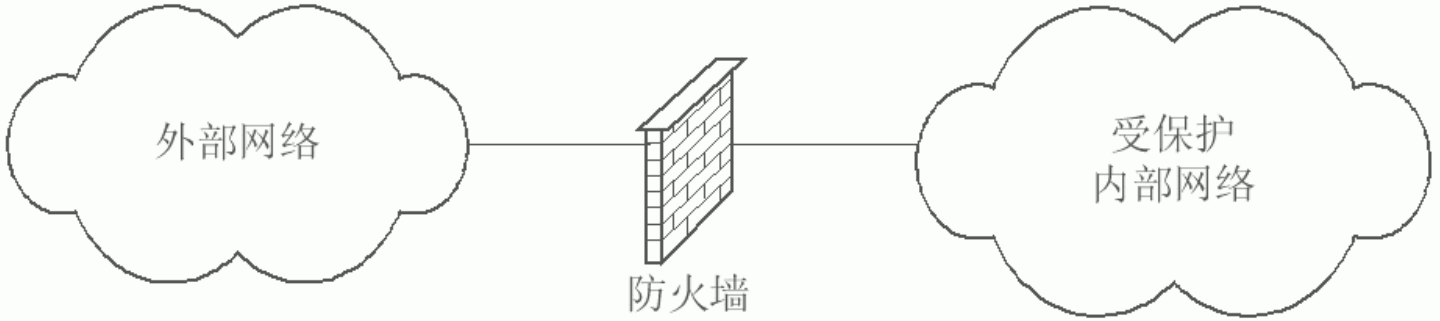
- Netstat
- Ipconfig/ifconfig
- Ping
- Tracert
- ……

防火墙技术

- 本章详细介绍防火墙技术，包括防火墙分类、体系结构，讲解如何根据实际的网络需求构建防火墙，最后介绍了两种典型防火墙产品的使用方法。

10.1 防火墙技术概述

- 在网络中防火墙主要用于逻辑隔离外部网络与受保护的内部网络



10.1 防火墙技术概述

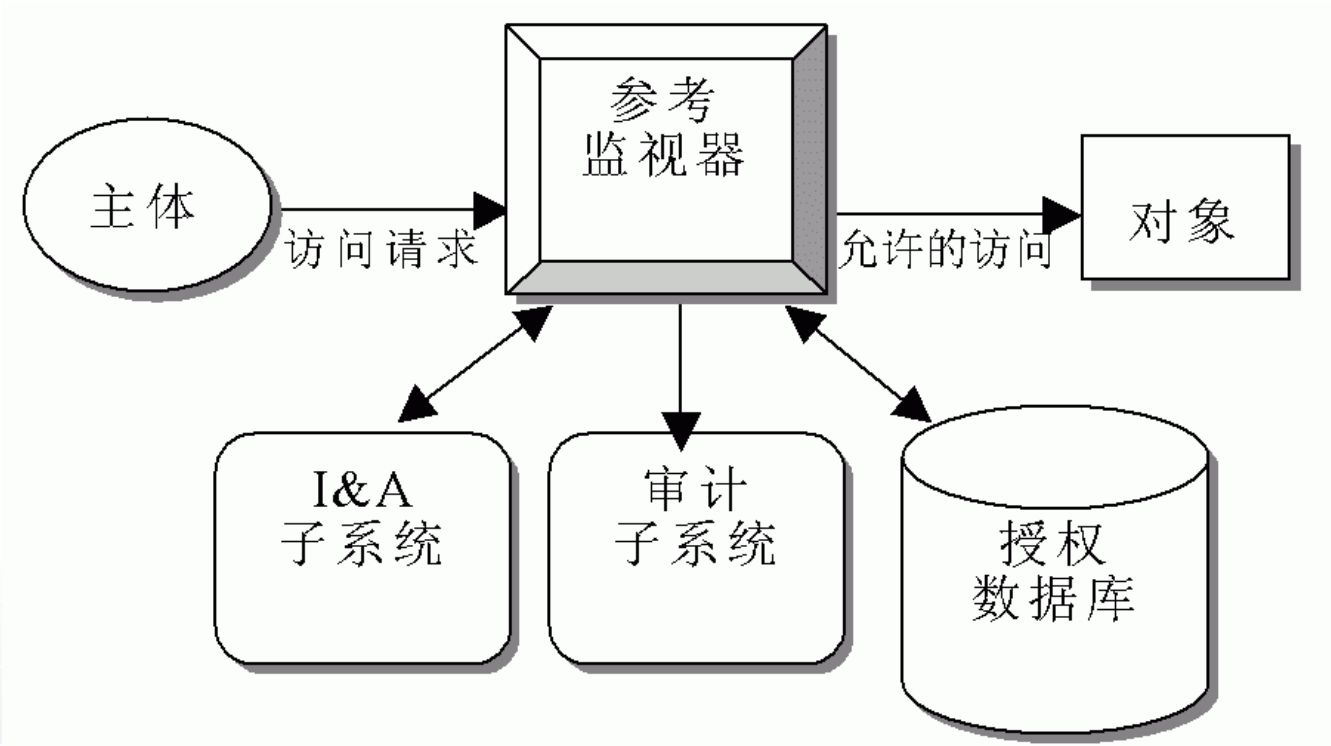
- 防火墙技术属于典型的静态安全技术，该类技术用于逻辑隔离内部网络与外部网络
- 通过数据包过滤与应用层代理等方法实现内外网络之间信息的受控传递，从而达到保护内部网络的目的

10.1 防火墙技术概述

- 经典安全模型
- 防火墙规则
- 匹配条件
- 防火墙分类

10.1 防火墙技术概述

- 经典安全模型



10.1 防火墙技术概述

- 防火墙规则
  - 防火墙的基本原理是对内部网络与外部网络之间的信息流传递进行控制
  - 控制的功能是通过在防火墙中预先设定一定的安全规则（也称为安全策略）实现的

10.1 防火墙技术概述

- 防火墙规则
  - 防火墙的安全规则由匹配条件与处理方式两个部分共同构成
  - 其中匹配条件是一些逻辑表达式，根据信息中的特定值域可以计算出逻辑表达式的值为真（True）或假（False）
  - 如果信息使匹配条件的逻辑表达式为真，则说明该信息与当前规则匹配

10.1 防火墙技术概述

- 防火墙规则
  - 信息一旦与规则匹配，就必须采用规则中的处理方式进行处理
  - 处理方式主要包括
    - Accept：允许数据包或信息通过
    - Reject：拒绝数据包或信息通过，并且通知信息源该信息被禁止
    - Drop：直接将数据包或信息丢弃，并且不通知信息源

10.1 防火墙技术概述

- 防火墙规则
  - 基本原则
    - “默认拒绝”原则
    - “默认允许”原则
  - 现有的防火墙产品大多基于第一种规则

10.1 防火墙技术概述

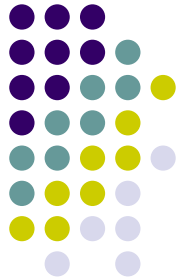
- 匹配条件
  - 网络层
    - IP源地址、IP目的地址、协议
  - 传输层
    - 源端口 、目的端口
  - 应用层
    - 根据各种具体应用而定
  - 基于信息流向的匹配条件
    - 向内、向外

10.1 防火墙技术概述

- 防火墙分类
  - 按防范领域分类
    - 个人防火墙
      - 禁止Internet文件共享、隐藏端口、过滤IP信息流、控制Internet应用程序、警告和日志、漏洞检查
    - 网络防火墙
      - 对网络数据流进行分析，并按照规则进行过滤。

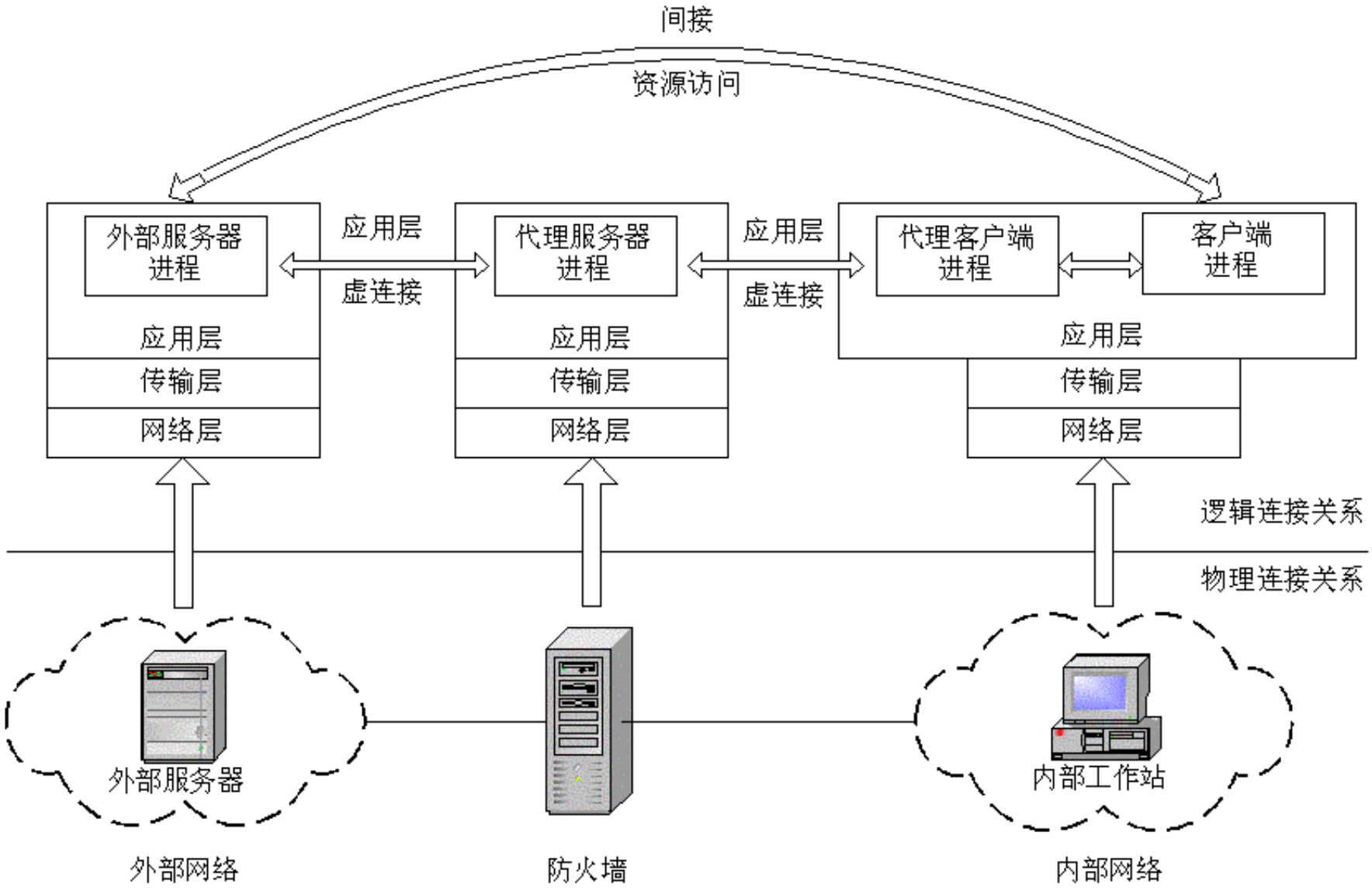
10.1 防火墙技术概述

- 防火墙分类
  - 按实现的方式分类
    - 软件防火墙
    - 硬件防火墙



10.1 防火墙技术概述

- 防火墙分类
  - 按实现技术分类
    - 数据包过滤
      - 在系统进行IP数据包转发时设置访问控制列表，访问控制列表主要由各种规则组成。
      - 数据包过滤的规则主要采用网络层与传输层匹配条件
    - 应用层代理
      - 应用层代理是指运行在防火墙主机上的特殊应用程序或者服务器程序
      - 这些程序根据安全策略接受用户对网络的请求，并在用户访问应用信息时依据预先设定的应用协议安全规则进行信息过滤


间接
资源访问
外部服务器进程
应用层
虚连接
代理服务器进程
应用层
虚连接
代理客户端进程
客户端进程
应用层
传输层
网络层
应用层
传输层
网络层
应用层
传输层
网络层
逻辑连接关系
物理连接关系
外部服务器
内部工作站
外部网络
防火墙
内部网络

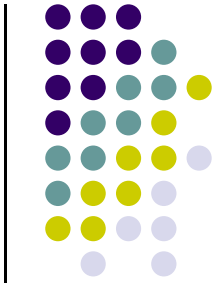
10.1 防火墙技术概述

- 技术方案对比
  - 数据包过滤
    - 服务无关、对用户透明
    - 过滤规则复杂 、正确性难以检测、容易形成瓶颈
  - 应用层代理
    - 内网安全性较高 、Cache机制可以提高信息访问效率、支持用户认证 、支持基于内容的信息过滤
    - 必须对每种应用提供代理服务和代理客户端、实时性差

状态检测

- 状态检测技术是防火墙近几年才应用的新技术。
- 传统的包过滤防火墙只是通过检测IP包头的相关信息来决定数据流的通过还是拒绝，
- 状态检测技术采用的是一种基于连接的状态检测机制，将属于同一连接的所有包作为一个整体的数据流看待，构成连接状态表，通过规则表与状态表的共同配合，对表中的各个连接状态因素加以识别。
- 这里动态连接状态表中的记录可以是以前的通信信息，也可以是其他相关应用程序的信息
- 与传统包过滤防火墙的静态过滤规则表相比，状态检测技术具有更好的灵活性和安全性。

状态检测（续）



- **通信信息：**即所有7层协议的当前信息。
  - 防火墙的检测模块位于操作系统的内核，在网络层之下，能在数据包到达网关操作系统之前对它们进行分析。
  - 防火墙先在低协议层上检查数据包是否满足企业的安全策略，对于满足的数据包，再从更高协议层上进行分析
  - 它验证数据的源地址、目的地址和端口号、协议类型、应用信息等多层的标志，因此具有更全面的安全性。

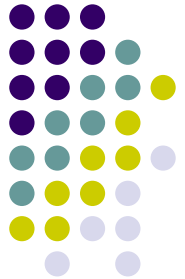
状态检测（续）

- **通信状态：**即以前的通信信息。
  - 状态检测防火墙在状态表中保存以前的通信信息，记录从受保护网络发出的数据包的状态信息
  - 然后，防火墙根据该表内容对返回受保护网络的数据包进行分析判断，这样，只有响应受保护网络请求的数据包才被放行。这里，对于UDP或者RPC等无连接的协议，检测模块可创建虚会话信息用来进行跟踪。

状态检测（续）

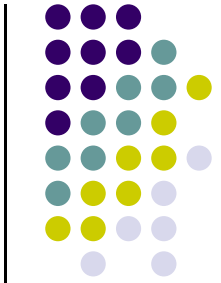
- 应用状态：即其他相关应用的信息。
  - 状态检测模块能够理解并学习各种协议和应用，以支持各种最新的应用；
  - 并且，它能从应用程序中收集状态信息存入状态表中，以供其他应用或协议做检测策略。

状态检测（续）



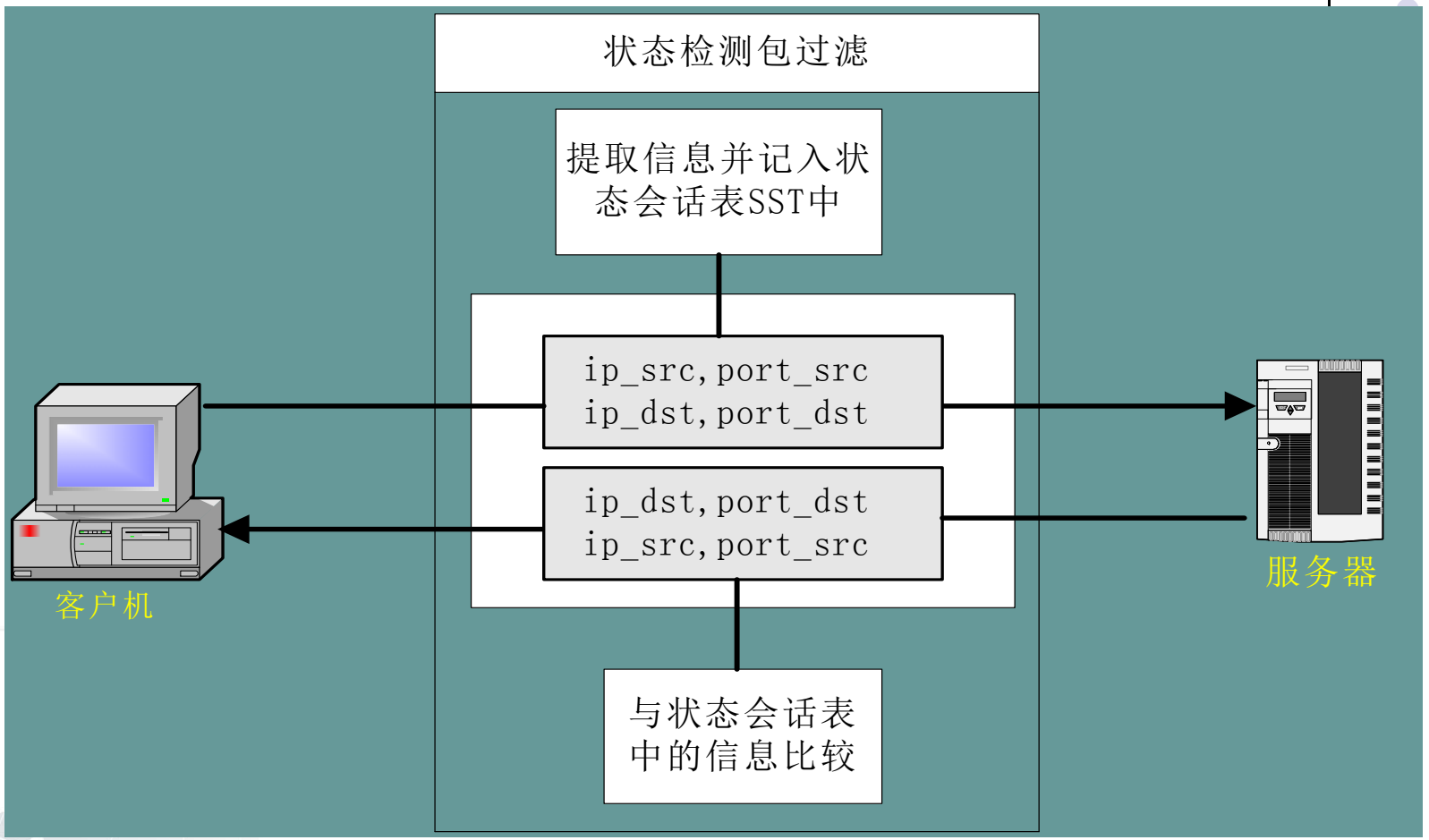
- **操作信息：**即在数据包中能执行逻辑或数学运算的信息。
  - 状态监测技术，采用强大的面向对象的方法，基于通信信息、通信状态、应用状态等多方面因素，利用灵活的表达式形式，结合安全规则、应用识别知识、状态关联信息以及通信数据，构造更复杂的、更灵活的、满足用户特定安全要求的策略规则

状态检测（续）

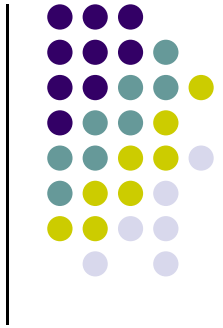


- 工作在TCP/IP各层，检查由防火墙转发的包，并创建相应的结构记录连接的状态。
- 它的检查项包括链路层、网络层、传输层、应用层的各种信息，并根据规则表或状态表来决定是否允许转发包通过。

状态检测原理

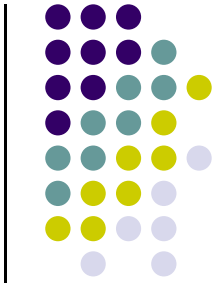

状态检测包过滤
提取信息并记入状态会话表SST中
ip_src,port_src
ip_dst,port_dst
ip_dst,port_dst
ip_src,port_src
与状态会话表中的信息比较
客户机
服务器

状态检测（续）



- 数据链路层
  - 在数据包到达IP层以前进行检测，如果不满足安全策略，数据包被抛弃

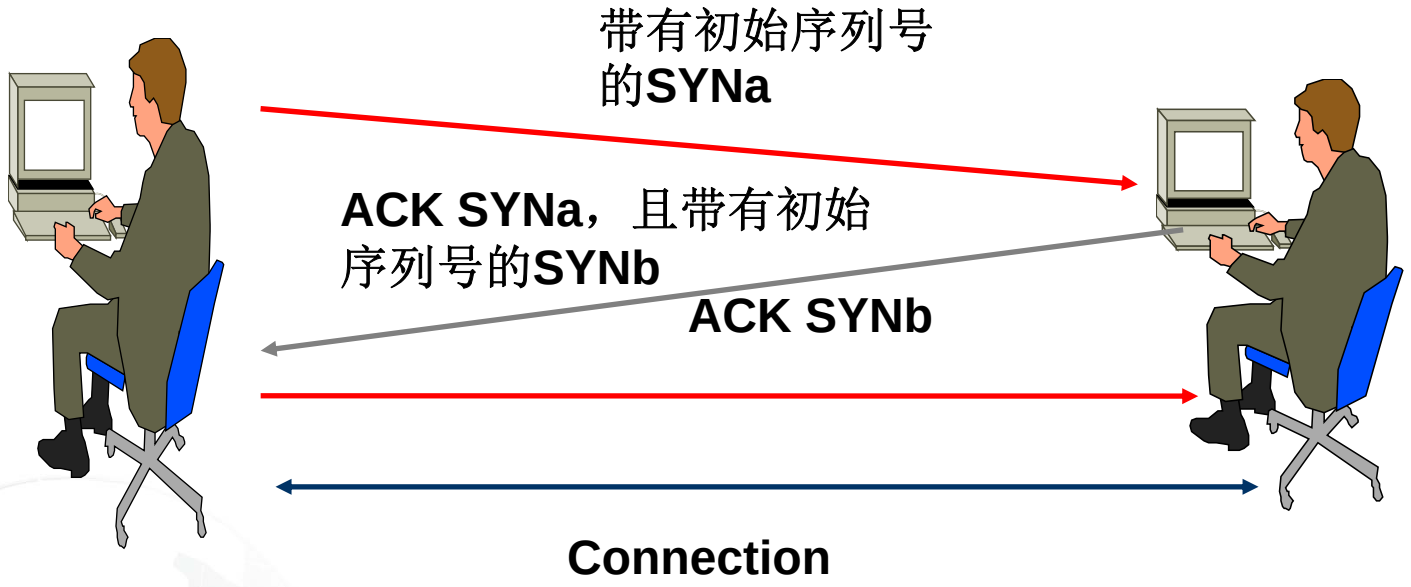
状态检测（续）



- **IP层**
  - 协议、地址和端口（如 TCP协议，UDP协议等）
  - IP分片
  - ICMP协议检测

状态检测（续）

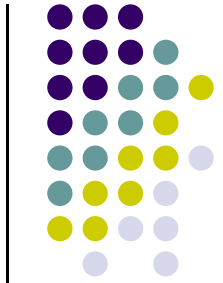
- TCP



状态检测（续）

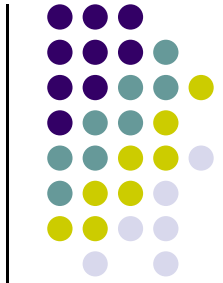
- TCP数据包的状态
  - **SYN：初始化**
  - **ACK：确认**
  - **RST 连接复位**
  - **FIN ：关闭连接**
  - **STN：同步序列号**
  - **URG:紧急数据**
  - **……**

状态检测（续）



- UDP协议
  - 超时检测
  - 是否有以前的UDP数据包

状态检测（续）



- 应用层
  - **FTP**
  - **HTTP**
  - 用户认证等

状态检测（续）

- 数据包过滤规则

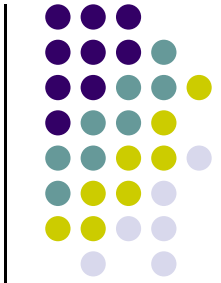
行为	源地址	目的地址	协议	源端口	目的端口	码子位
允许	内部网络地址	外部网络地址	**TCP**	任意	**80**	任意
允许	外部网络地址	内部网络地址	**TCP**	**80**	**1023**	**ACK**
拒绝	所有	所有	所有	所有	所有	所有

状态检测（续）

- 状态数据包过滤规则

行为	规则
允许	数据包是先前连接的一部分
允许	先前有出站数据包
拒绝	其他

状态检测（续）



状态表示例：

	源地址	目的地址	协议	源端口	目的端口	超时（秒）	码字位
	10.1.1.20	**10.34.12.11**	**TCP**	**2341**	**80**	**60**	
	10.1.1.34	**10.22.11.45**	**TCP**	**32141**	**80**	**1.5**	
	202.115.2.1	**10.22.11.46**	**UDP**	**33222**	**21**	**20**	

状态检测（续）

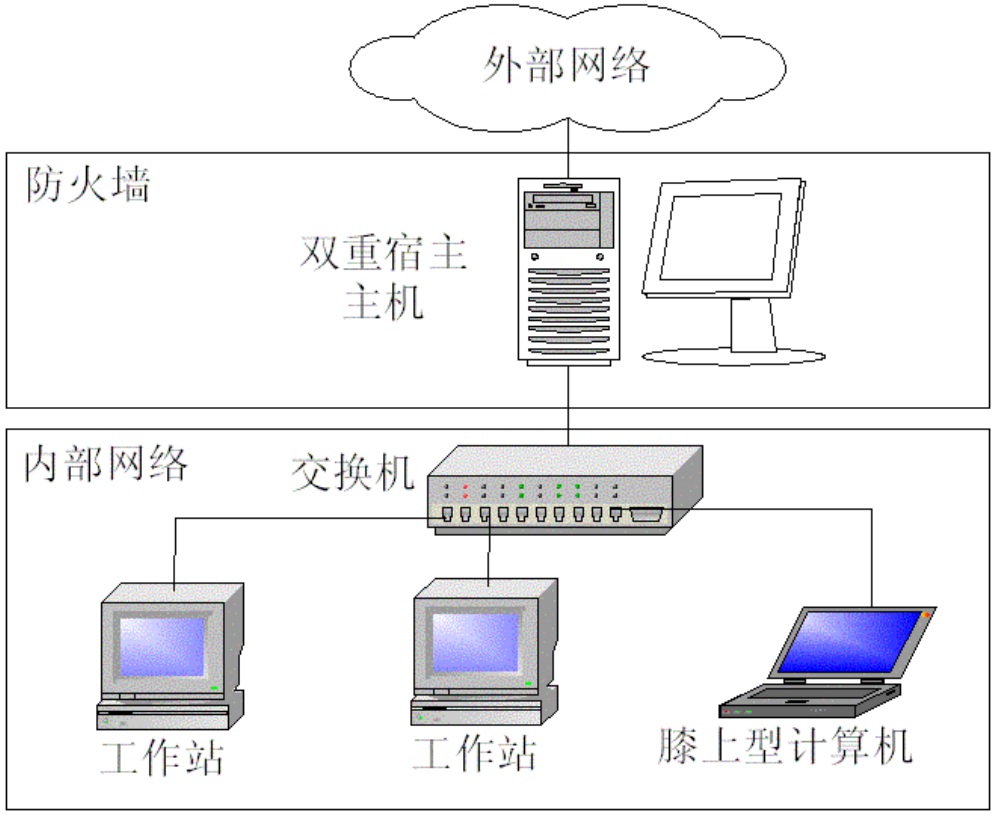
- 优点
  - 安全强度高
  - 配置灵活
- 缺点：
  - 速度慢
  - 管理复杂

10.2 防火墙的结构

- 经典防火墙体系结构
  - 双重宿主主机体系结构
  - 被屏蔽主机体系结构
  - 被屏蔽子网体系结构

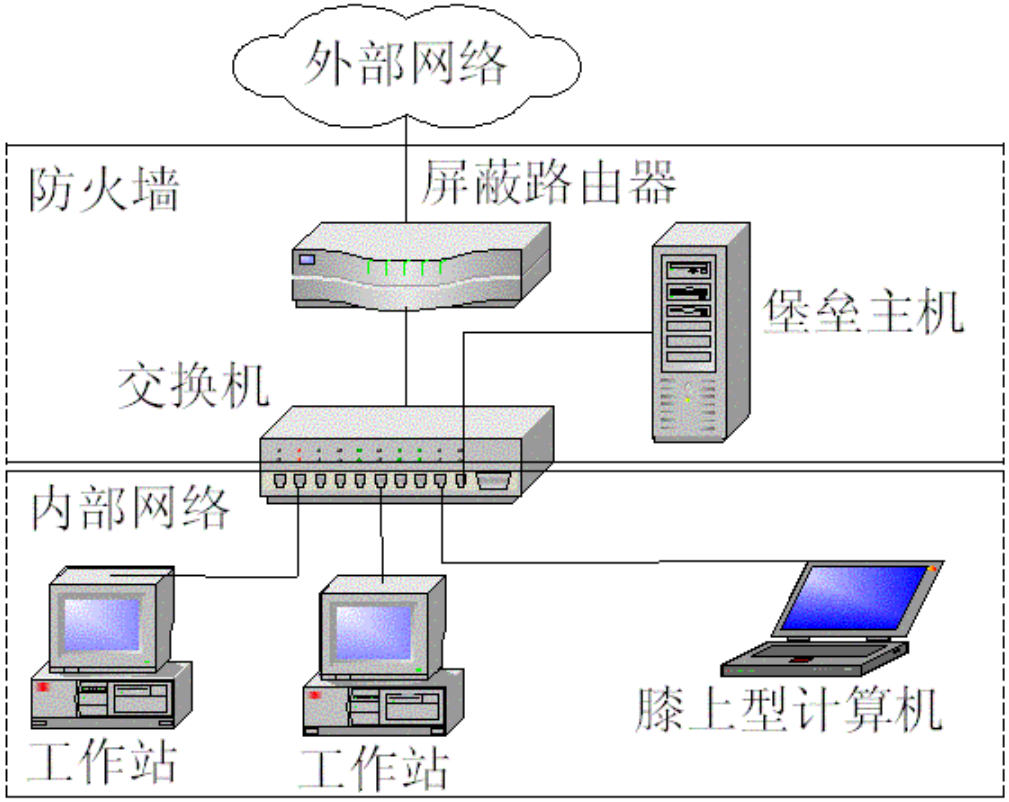
10.2 防火墙的结构

- 双重宿主主机体系结构



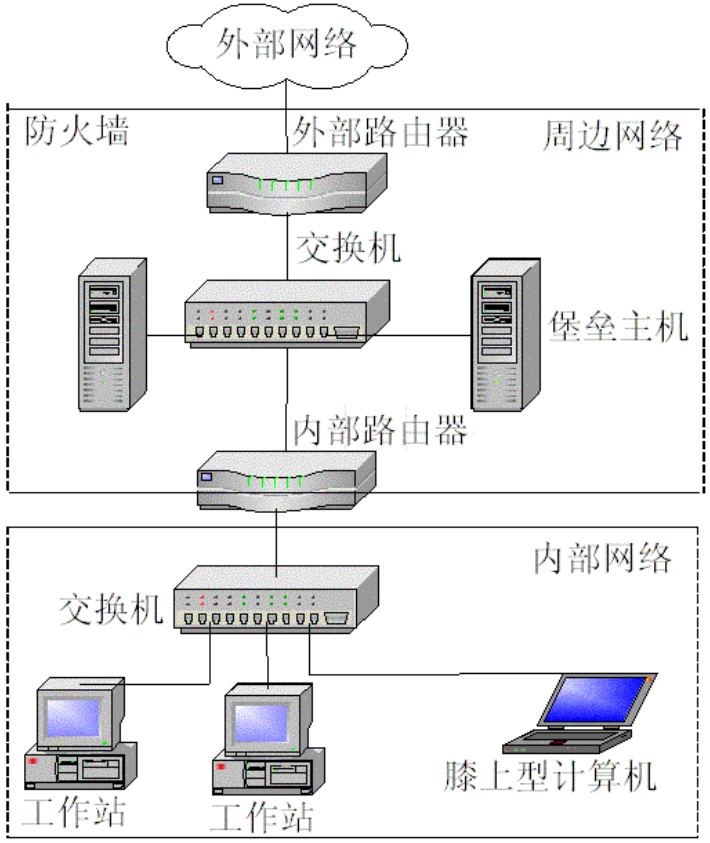
10.2 防火墙的结构

- 被屏蔽主机体系结构



10.2 防火墙的结构

- 被屏蔽子网体系结构

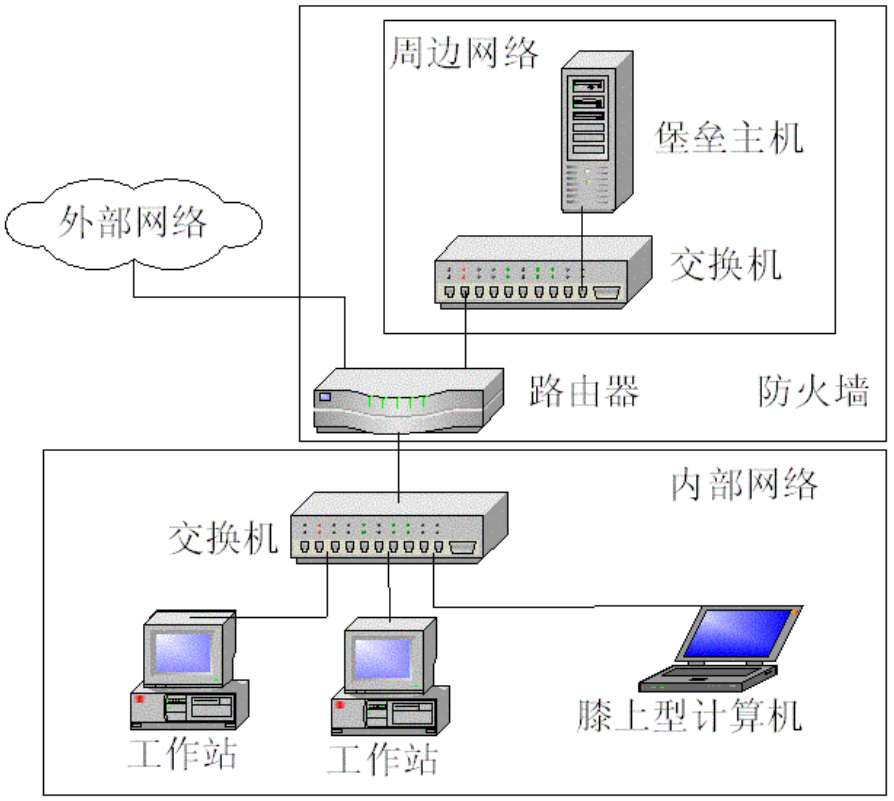


10.2 防火墙的结构

- 其他体系结构
  - 合并内部和外部路由器
  - 合并堡垒主机和外部路由器
  - 合并堡垒主机和内部路由器
  - 多台内部路由器
  - 多台外部路由器
  - 多个周边网络

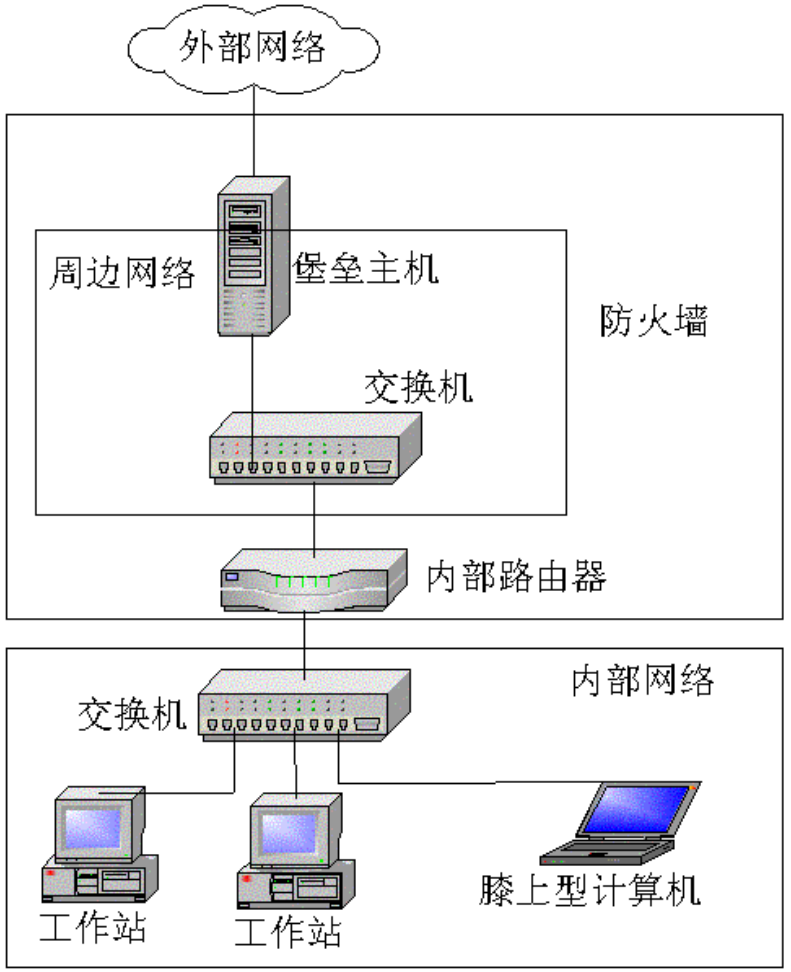
10.2 防火墙的结构

- 其他体系结构
  - 合并内部和外部路由器



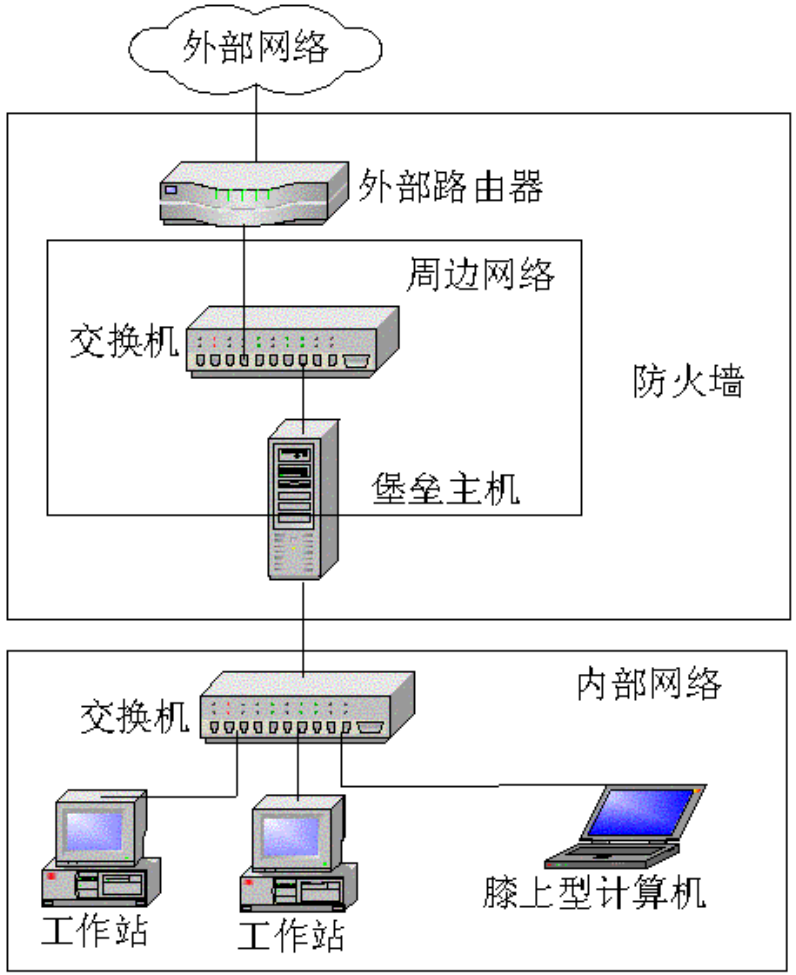
10.2 防火墙的结构

- 其他体系结构
  - 合并堡垒主机和外部路由器



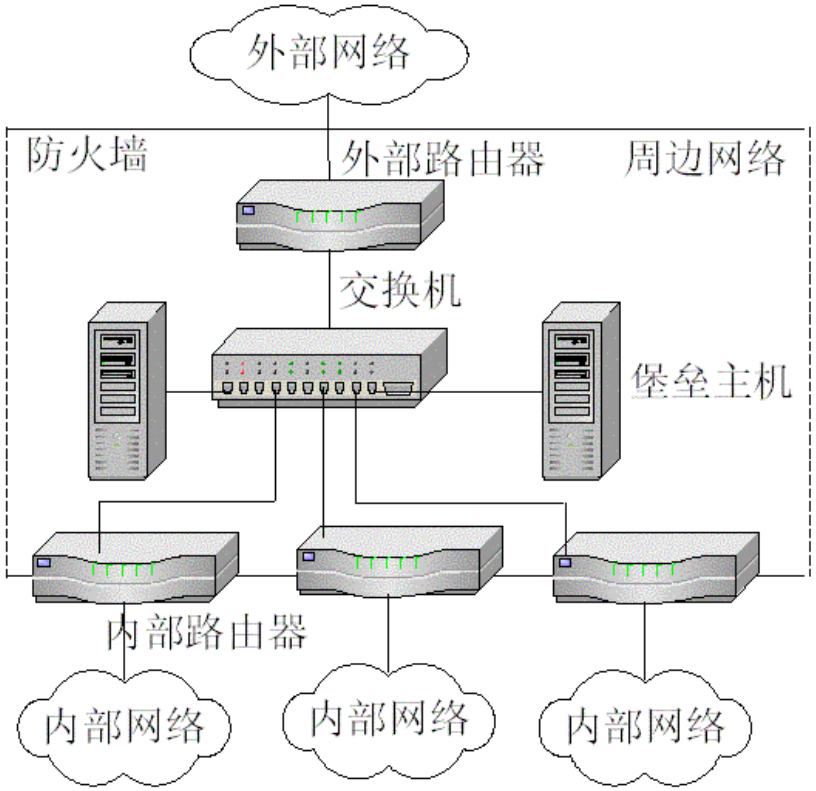
10.2 防火墙的结构

- 其他体系结构
  - 合并堡垒主机和内部路由器



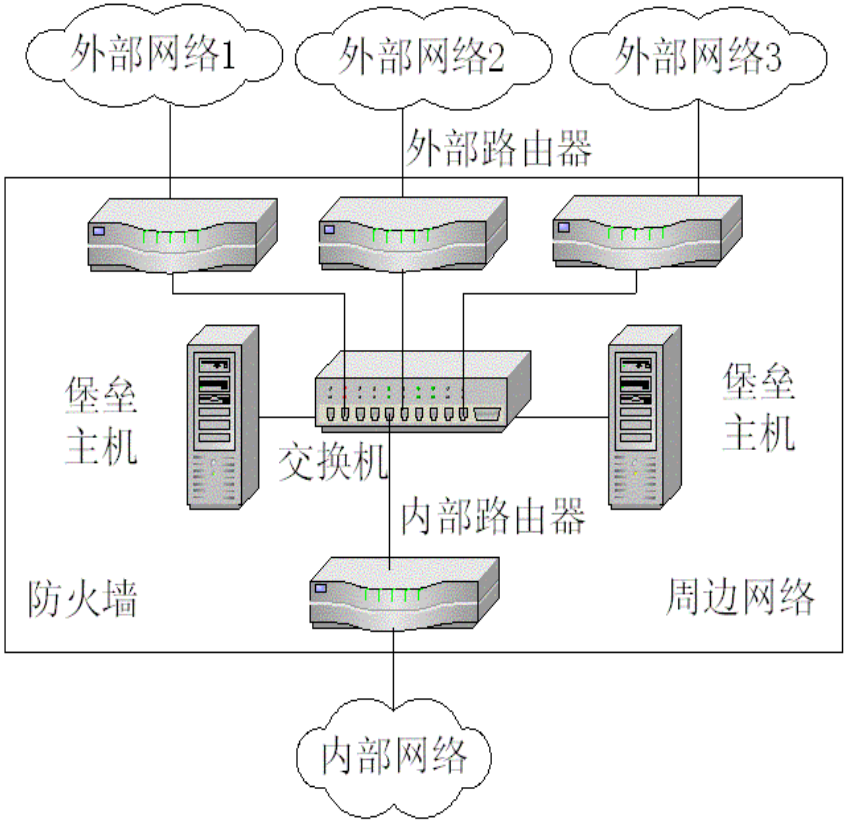
10.2 防火墙的结构

- 其他体系结构
  - 多台内部路由器



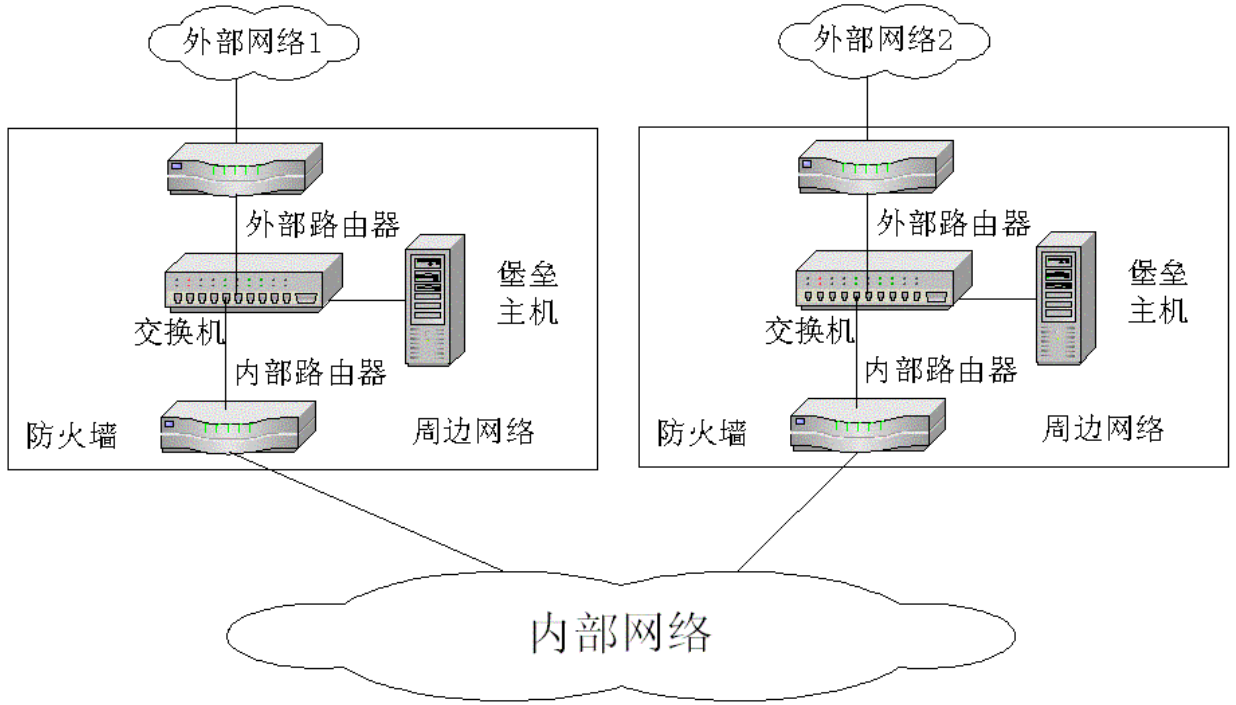
10.2 防火墙的结构

- 其他体系结构
  - 多台外部路由器



10.2 防火墙的结构

- 其他体系结构
  - 多个周边网络



10.3 构建防火墙

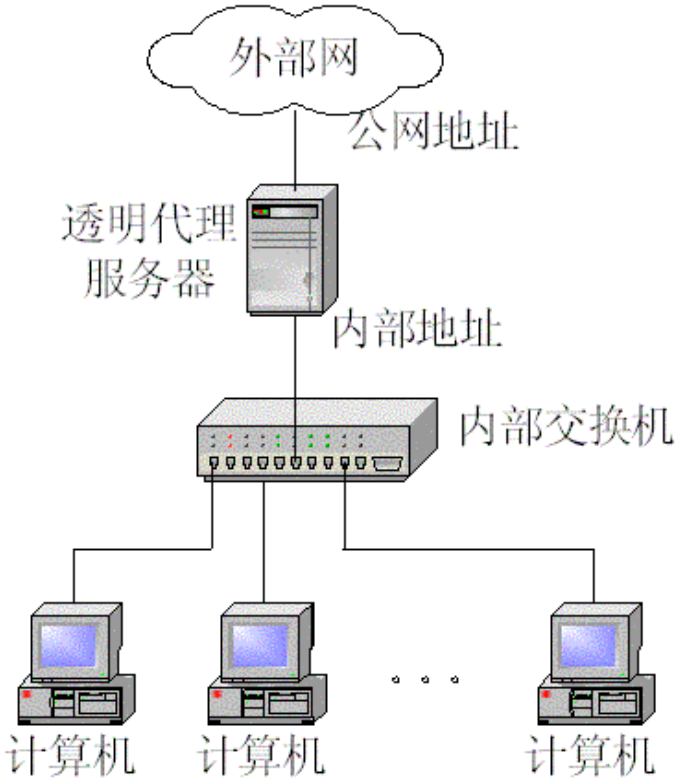
- 选择防火墙体系结构
- 安装外部路由器
- 安装内部路由器
- 安装堡垒主机
- 设置数据包过滤规则
- 设置代理系统
- 检查防火墙运行效果

10.3 构建防火墙

- 选择防火墙体系结构
  - 小型网络
  - 中型网络
  - 大型网络

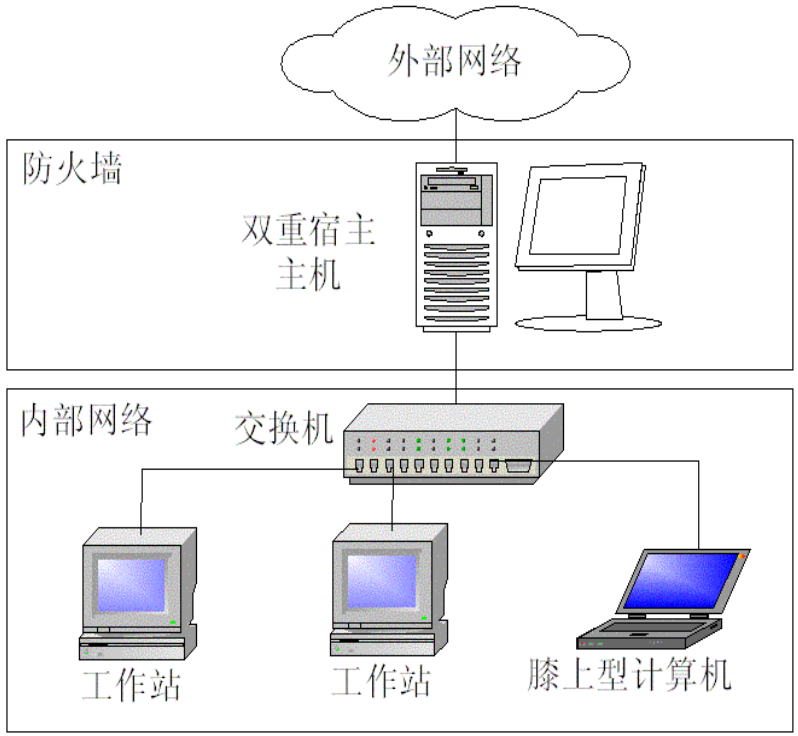
10.3 构建防火墙

- 选择防火墙体系结构
  - 小型网络
    - 透明代理



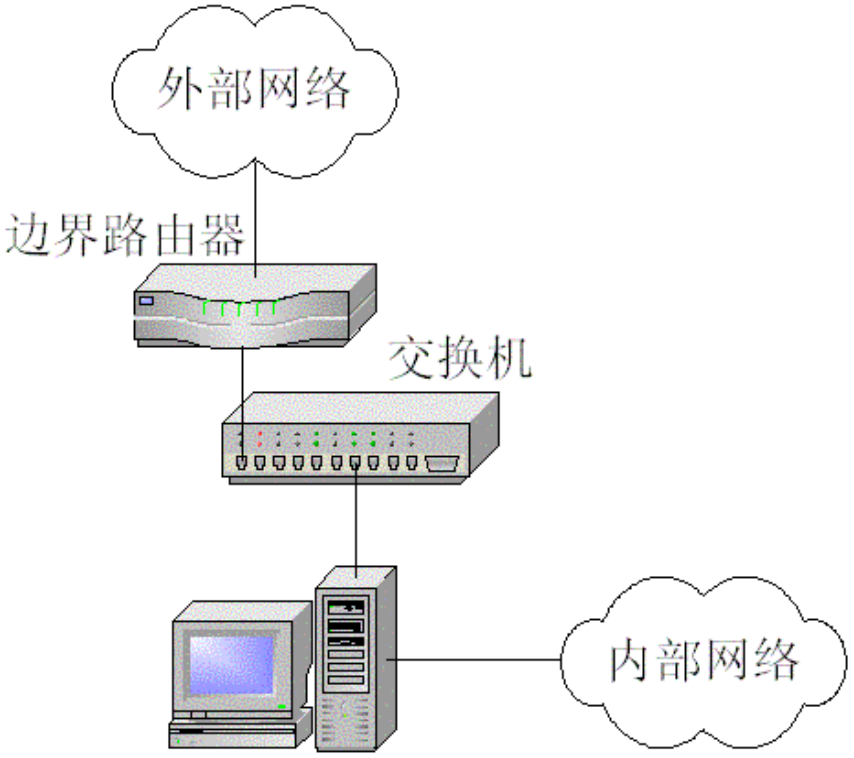
10.3 构建防火墙

- 选择防火墙体系结构
  - 小型网络
    - 透明代理
    - 双重宿主主机



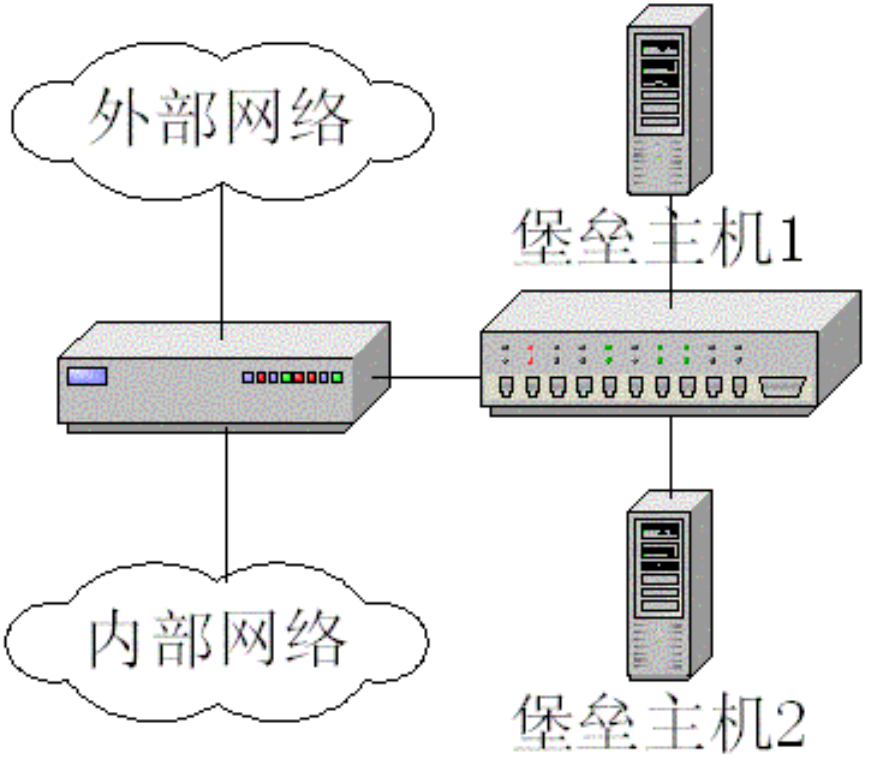
10.3 构建防火墙

- 选择防火墙体系结构
  - 中型网络
    - 软件防火墙



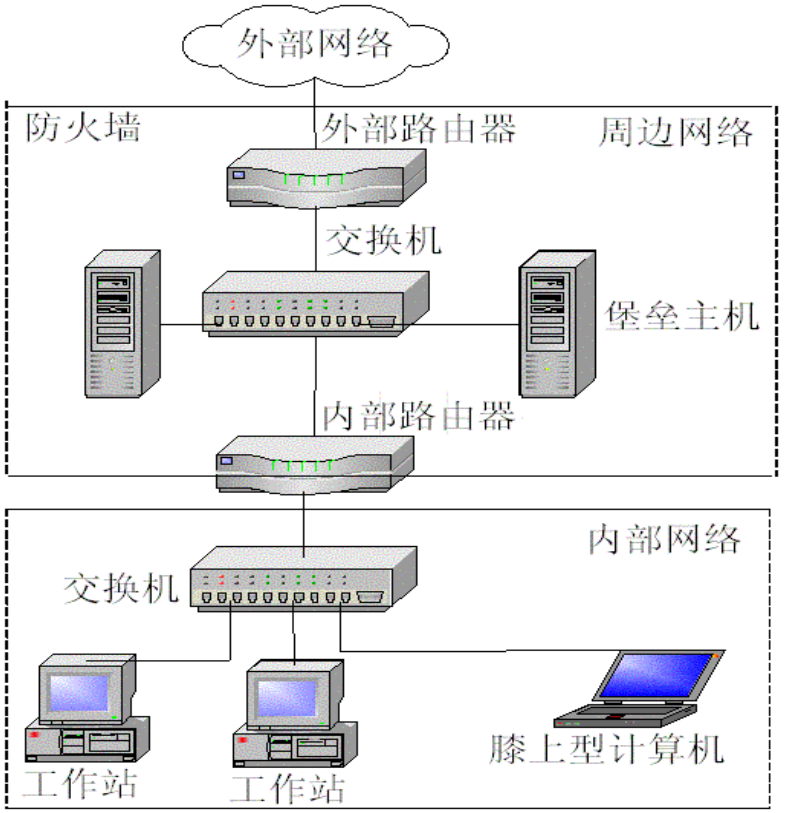
10.3 构建防火墙

- 选择防火墙体系结构
  - 中型网络
    - 软件防火墙
    - 硬件防火墙



10.3 构建防火墙

- 选择防火墙体系结构
  - 大型网络
    - 被屏蔽子网



10.3 构建防火墙

- 安装外部路由器
  - 连接线路
  - 配置网络接口
  - 测试网络连通性
  - 配置路由算法
  - 路由器的访问控制

10.3 构建防火墙

- 安装外部路由器
  - 连接线路
    - 保证设备与外部网络、周边网络（或内部网络）的线路连接正常
    - 由于外部路由器的外部网络接口一般较为复杂，可能会使用XDSL、ISDN、ATM等广域网、城域网协议与接口，必须首先完成线路申请、线路连接等前期工作

10.3 构建防火墙

- 安装外部路由器
  - 配置网络接口
    - 配置网络接口的工作主要包括IP地址、子网掩码、开启网络接口等
    - 在配置完毕后需要进行网络接口连通性测试，必需保证路由器上的测试程序可以通过外部网络接口访问外部网络，通过内部网络接口可以访问周边网络（或内部网络）

10.3 构建防火墙

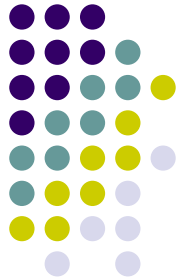
- 安装外部路由器
  - 测试网络连通性
    - 在不添加访问控制规则的情况下，用户应该能够通过路由器从周边网络访问外部网络，同样从外部网络访问周边网络

10.3 构建防火墙

- 安装外部路由器
  - 配置路由算法
    - 为让外部路由器能够参与外部网络的路由运算，必需在外部路由器上配置相应的动态路由算法或静态路由，同时将外部网络访问内部网络的下一跳地址指向内部路由器或双重宿主主机

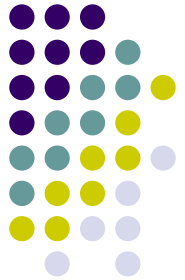
10.3 构建防火墙

- 安装外部路由器
  - 路由器的访问控制
    - 在路由算法配置完毕后，需要配置针对路由器自身的访问控制，限制路由器对外部提供Telnet等服务，将这些服务的服务范围限制在内部网络中的管理员使用的计算机



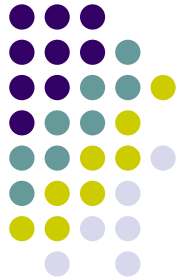
10.3 构建防火墙

- 安装内部路由器
  - 连接线路
    - 内部网络一般比较单纯，多局限于以太系列网络，线路连接较为简单
  - 配置路由算法
    - 内部路由器不参与外部路由算法，也不参与内部网络中各子网间的路由转发，因此只需要通过静态路由配置外部网络、内部网络、周边网络之间的数据包转发



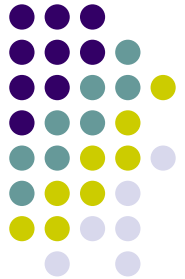
10.3 构建防火墙

- 安装堡垒主机
  - 选择合适的物理位置
    - 要求堡垒主机必须存放在安全措施完善的机房内部，同时要保证机房的供电、通风、恒温、监控条件良好
  - 选择合适的硬件设备
    - 选择堡垒主机一定要以满足服务性能需求作为最终依据，过高、过低的配置都是不合时宜的



10.3 构建防火墙

- 安装堡垒主机
  - 选择合适的操作系统
    - 堡垒主机操作系统的选择必须考虑到安全性、高效性等方面的因素
  - 注意堡垒主机的网络接入位置
    - 堡垒主机应该放置于不涉及敏感信息的位置
    - 不应该采用集线器这样的共享设备

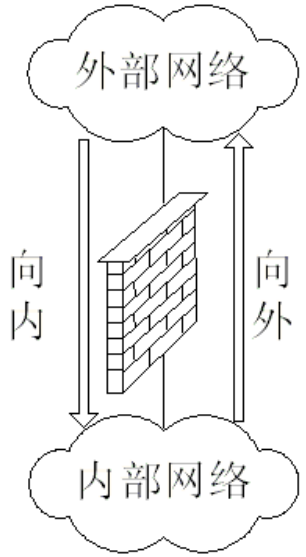


10.3 构建防火墙

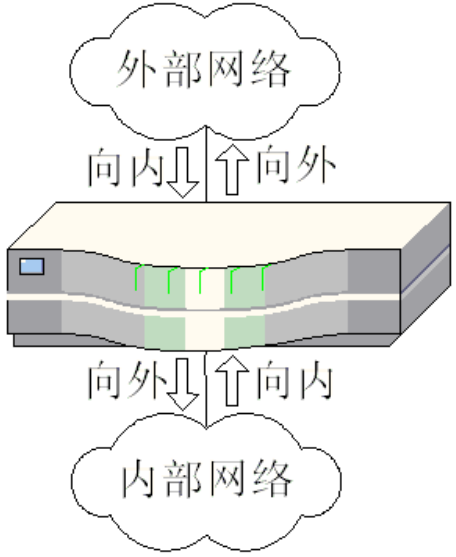
- 安装堡垒主机
  - 设置堡垒主机提供的服务
    - 关闭不需要的服务
    - 对提供的服务需要添加一定的安全措施，包括用户IP限制、DOS攻击屏蔽等
    - 在堡垒主机上禁止使用用户账号
  - 核查堡垒主机的安全保障体制
    - 核查的手段主要是在主机上运行相应的安全分析软件或者漏洞扫描程序，在发现堡垒主机的安全漏洞后应该及时排除
  - 维护与备份

10.3 构建防火墙

- 设置数据包过滤规则
  - 首先需要确定设置数据包过滤规则设备对“向内”与“向外”的具体概念
    - 要尽 限制
    - 采用
    - 脱机



（a）采用软件、硬件防火墙或堡垒主机



（b）采用路由器
向内=接收、向外=发送

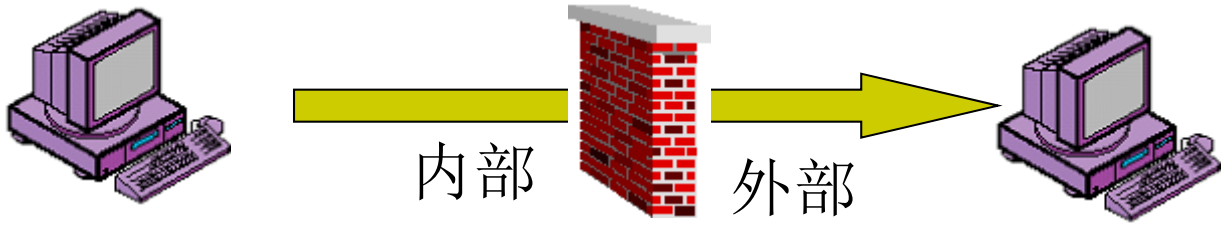
10.3 构建防火墙

- 设置数据包过滤规则
  - 数据包过滤的方式
    - 堡垒主机

序号	流向	源地址	目的地址	动作
1	向内	202.102.0.0/255.255.0.0	203.104.64.0/255.255.240.0	Accept
2	向外	203.104.64.0/255.255.240.0	202.102.0.0/255.255.0.0	Accept
3	向内	0.0.0.0/0.0.0.0	203.104.64.0/255.255.255.0	Accept
4	向外	203.104.64.0/255.255.255.0	0.0.0.0/0.0.0.0	Accept
5	向内	0.0.0.0/0.0.0.0	203.104.65.0/255.255.255.0	Accept
6	向外	203.104.65.0/255.255.255.0	0.0.0.0/0.0.0.0	Accept
7	--	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	Reject

包过滤防火墙的设置(1)

- 从内往外的telnet服务



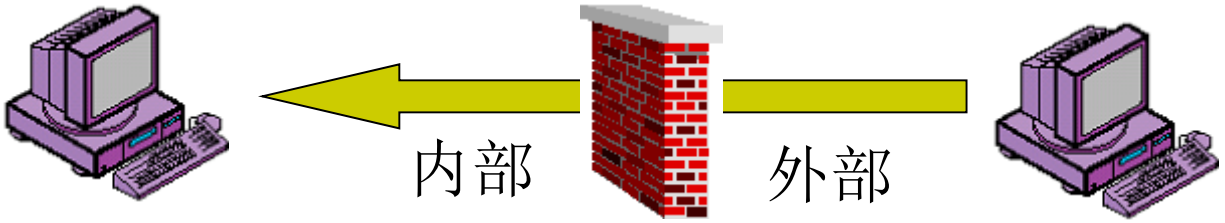
Client

TCP
1234

Server
TCP23

包过滤防火墙的设置(1)

- 从外往内的telnet服务



Server

TCP

23

Client

TCP

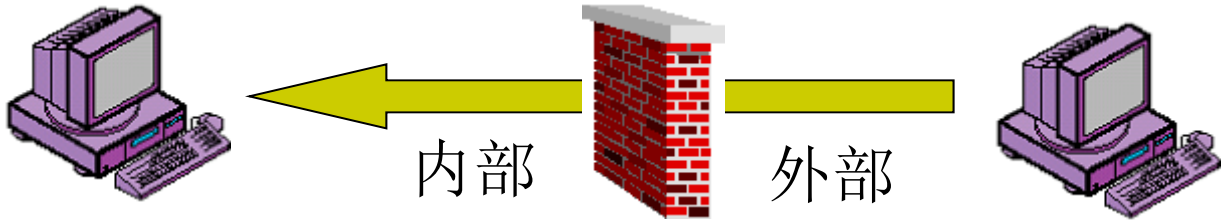
1234

针对telnet服务的防火墙规则

规则	包方向	源地址	目标地址	包类型	目标端口	动作
A	输入	外部	内部	TCP	25	允许
B	输出	内部	外部	TCP	>1023	允许
C	输出	内部	外部	TCP	23	允许
D	输入	外部	内部	TCP	>1023	允许
E	入/出	任意	任意	任意	任意	拒绝

包过滤防火墙的设置(1)

- 从外往内的telnet服务



10.0.0.2

TCP

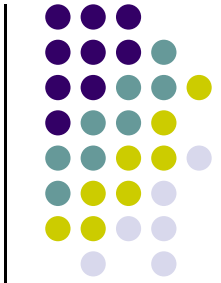
6000

202.114.106.10

TCP

5000

针对telnet服务的防火墙规则



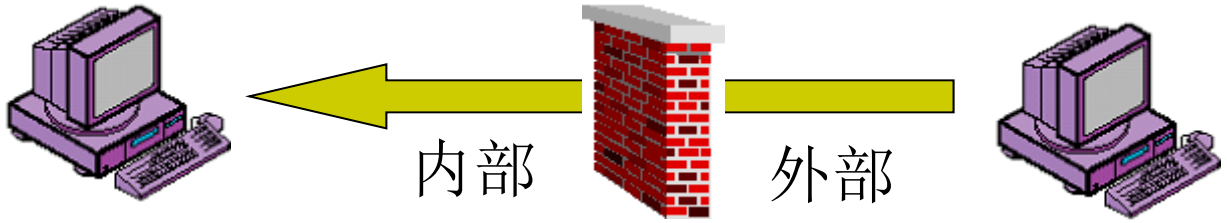
	包方向	源地址	目标地址	包类型	目标端口	动作	规则
1	输入	外部	内部	TCP	6000	允许	D
2	输出	内部	外部	TCP	5000	允许	B

针对telnet服务的防火墙规则

规则	包方向	源地址	目标地址	包类型	源端口	目标端口	动作
A	输入	外部	内部	TCP	>1023	23	允许
B	输出	内部	外部	TCP	23	>1023	允许
C	输出	内部	外部	TCP	>1023	23	允许
D	输入	外部	内部	TCP	23	>1023	允许
E	入/出	任意	任意	任意	任意	任意	拒绝

包过滤防火墙的设置(1)

- 从外往内的telnet服务



10.0.0.2

TCP

6000

202.114.106.10

TCP

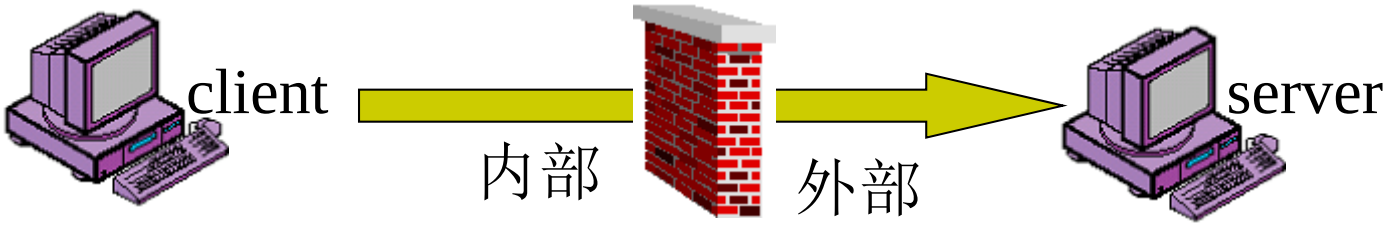
23

针对telnet服务的防火墙规则

	包方向	源地址	目标地址	包类型	源端口	目标端口	动作	规则
1	输入	外部	内部	TCP	23	6000	允许	D
2	输出	内部	外部	TCP	6000	23	允许	B

包过滤防火墙的设置(1)

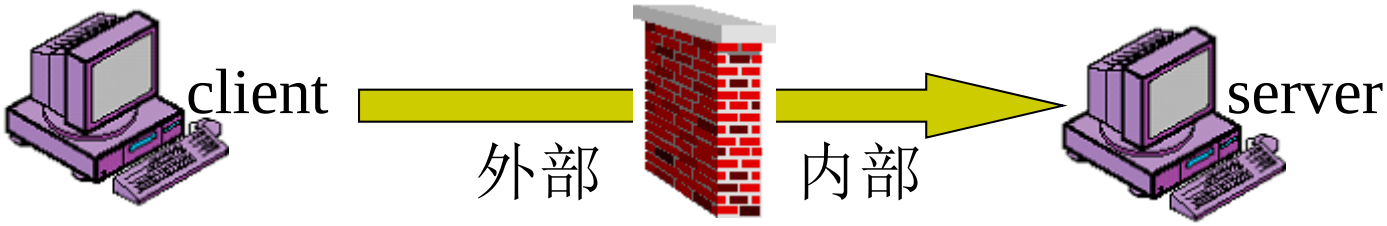
- 从内往外的telnet服务



- 往外包的特性(用户操作信息)
  - IP源是内部地址
  - 目标地址为server
  - TCP协议，目标端口23
  - 源端口>1023
  - 连接的第一个包ACK=0，其他包ACK=1
- 往内包的特性(显示信息)
  - IP源是server
  - 目标地址为内部地址
  - TCP协议，源端口23
  - 目标端口>1023
  - 所有往内的包都是ACK=1

包过滤防火墙的设置(2)

- 从外往内的telnet服务



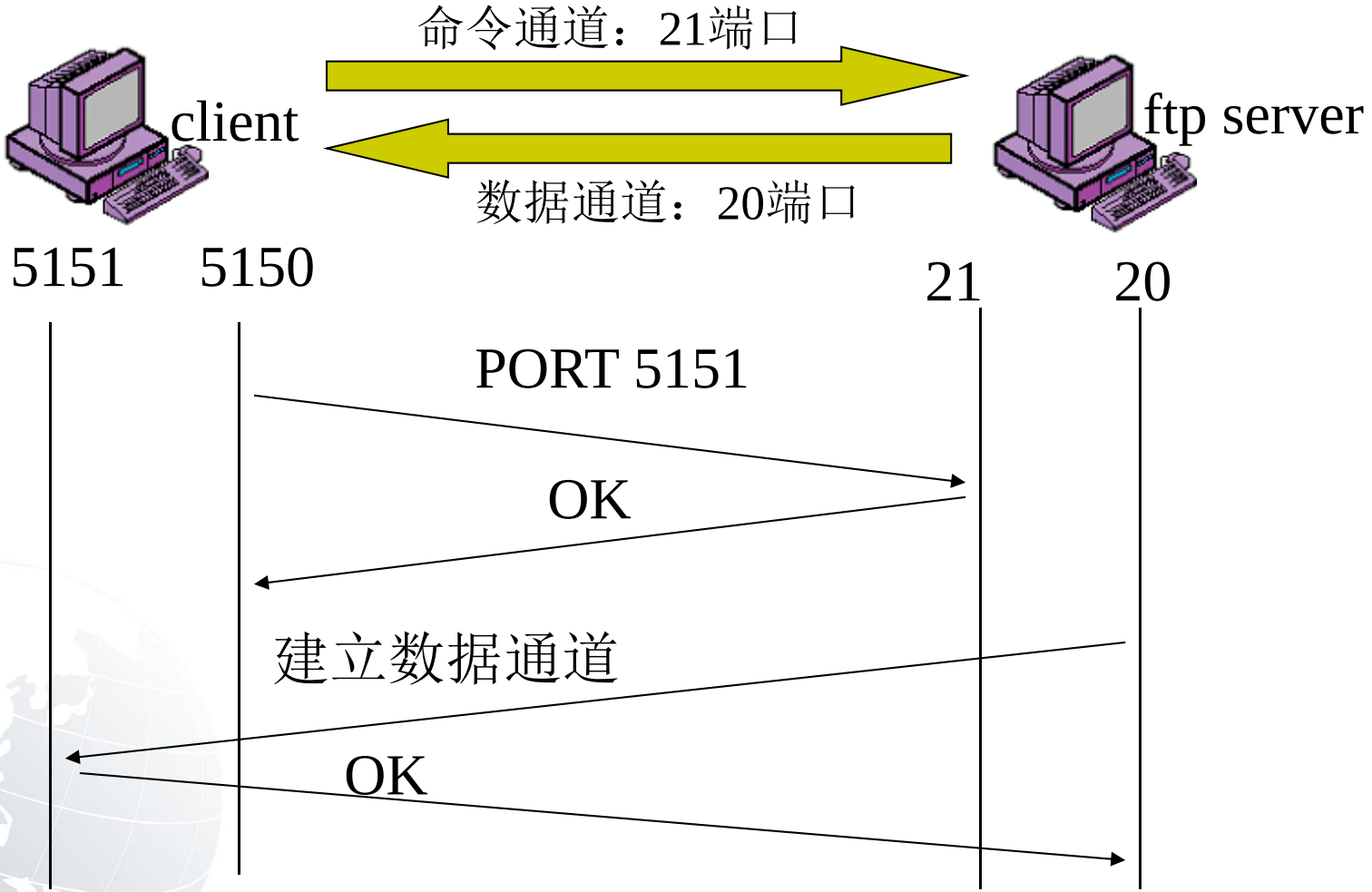
- 往内包的特性(用户操作信息)
  - IP源是外部地址
  - 目标地址为本地server
  - TCP协议，目标端口23
  - 源端口>1023
  - 连接的第一个包ACK=0，其他包ACK=1
- 往外包的特性(显示信息)
  - IP源是本地server
  - 目标地址为外部地址
  - TCP协议，源端口23
  - 目标端口>1023
  - 所有往内的包都是ACK=1

针对telnet服务的防火墙规则

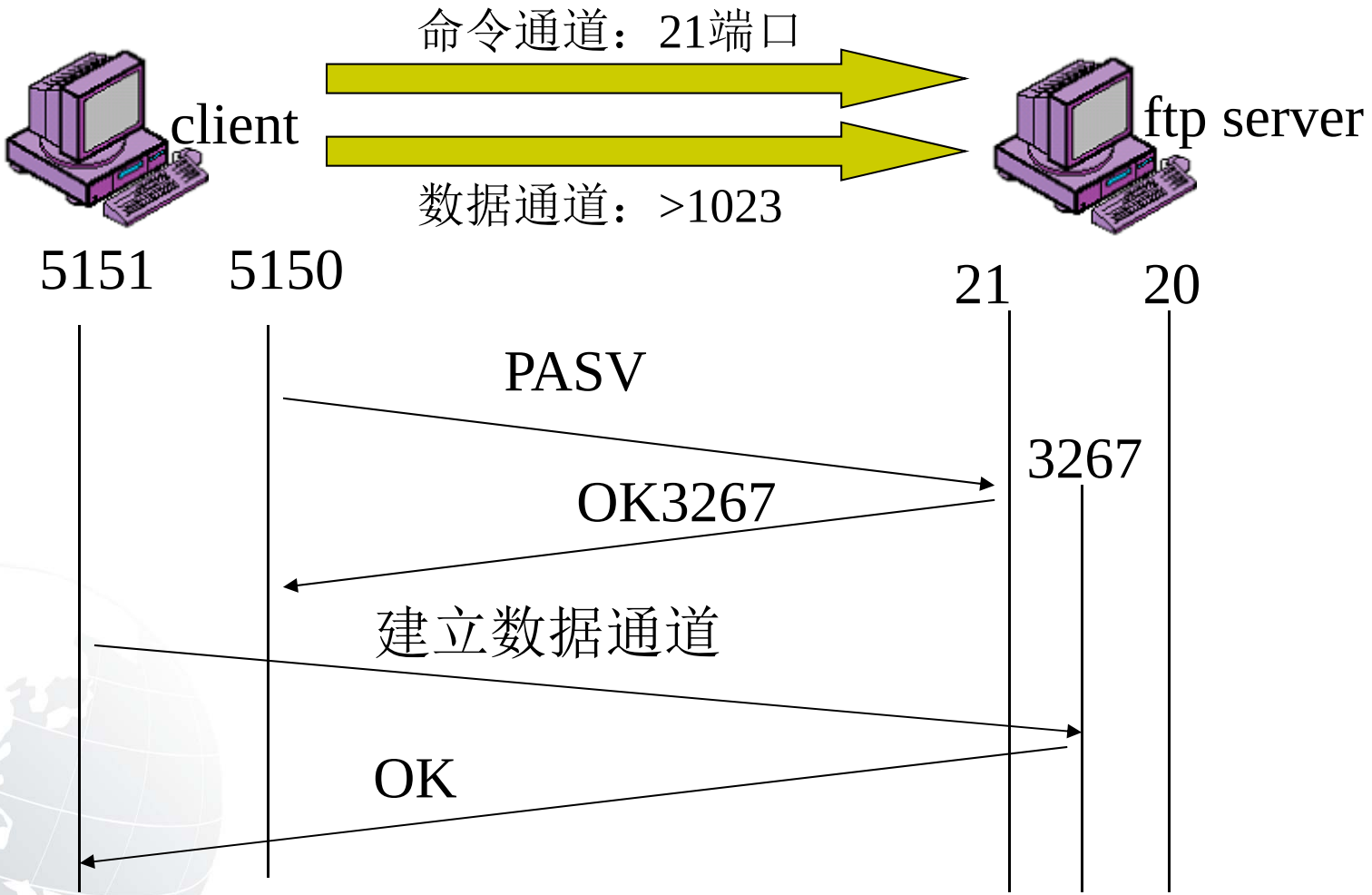
服务方向	包方向	源地址	目标地址	包类型	源端口	目标端口	ACK
往外	外	内部	外部	TCP	>1023	23	*
往外	内	外部	内部	TCP	23	>1023	1
往内	外	外部	内部	TCP	>1023	23	*
往内	内	内部	外部	TCP	23	>1023	1

*: 第一个ACK=0, 其他=1

Ftp文件传输协议


命令通道：21端口
client
ftp server
数据通道：20端口
5151
5150
21
20
PORT 5151
OK
建立数据通道
OK

Ftp文件传输协议(续)


命令通道：21端口
client
ftp server
数据通道：>1023
5151
5150
21
20
PASV
3267
OK3267
建立数据通道
OK

针对ftp的包过滤规则注意事项

- 建立一组复杂的规则集
  - 是否允许正常模式的ftp数据通道？
  - 有些ftp client不支持pasv模式
- 动态监视ftp通道发出的port命令
  - 有一些动态包过滤防火墙可以做到
- 启示
  - 包过滤防火墙比较适合于单连接的服务(比如smtp, pop3)，不适合于多连接的服务(比如ftp)

10.3 构建防火墙

- 设置数据包过滤规则
  - 数据包过滤的方式
    - 服务过滤规则

序号	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	向内	0.0.0.0/0.0.0.0	203.104.64.32	TCP	>1023	21	Accept
2	向外	203.104.64.32	0.0.0.0/0.0.0.0	TCP	21	>1023	Accept
3	向内	0.0.0.0/0.0.0.0	203.104.64.100	TCP	>1023	20	Accept
4	向外	203.104.64.32	0.0.0.0/0.0.0.0	TCP	20	>1023	Accept
5	向内	0.0.0.0/0.0.0.0	203.104.64.100	TCP	>1023	80	Accept
6	向外	203.104.64.100	0.0.0.0/0.0.0.0	TCP	80	>1023	Accept
7	向内	202.102.22.66	203.104.64.2	UDP	53	53	Accept
8	向外	203.104.64.2	202.102.22.66	UDP	53	53	Accept
9	--	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject

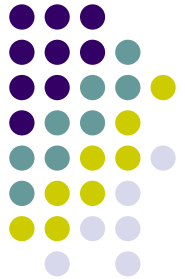
10.3 构建防火墙

路由器外部接口				
序号	流向	源地址	目的地址	动作
1	向内	202.102.0.0/255.255.0.0	203.104.64.0/255.255.240.0	Accept
2	向内	0.0.0.0/0.0.0.0	203.104.64.0/255.255.255.0	Accept
3	向内	0.0.0.0/0.0.0.0	203.104.65.0/255.255.255.0	Accept
4	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	Reject
路由器外部接口				
1	向内	203.104.64.0/255.255.240.0	202.102.0.0/255.255.0.0	Accept
2	向内	203.104.64.0/255.255.255.0	0.0.0.0/0.0.0.0	Accept
3	向内	203.104.65.0/255.255.255.0	0.0.0.0/0.0.0.0	Accept
4	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	Reject

路由器外部接口							
序号	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	向内	0.0.0.0/0.0.0.0	203.104.64.32	TCP	>1023	21	Accept
2	向内	0.0.0.0/0.0.0.0	203.104.64.100	TCP	>1023	20	Accept
3	向内	0.0.0.0/0.0.0.0	203.104.64.100	TCP	>1023	80	Accept
4	向内	202.102.22.66	203.104.64.2	UDP	53	53	Accept
5	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject
路由器内部接口							
序号	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	向内	203.104.64.32	0.0.0.0/0.0.0.0	TCP	21	>1023	Accept
2	向内	203.104.64.32	0.0.0.0/0.0.0.0	TCP	20	>1023	Accept
3	向内	203.104.64.100	0.0.0.0/0.0.0.0	TCP	80	>1023	Accept
4	向内	203.104.64.2	202.102.22.66	UDP	53	53	Accept
5	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject

10.3 构建防火墙

- 设置数据包过滤规则
  - 注意包过滤规则的顺序
    - 获得更高的过滤效率
    - 避免出现漏洞
  - 设置网络服务
    - 对外提供正常的服务

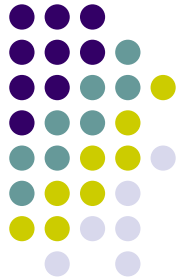


10.3 构建防火墙

- 设置代理系统
  - 可以直接访问外部网络，又可以通过代理访问
  - 设置代理服务器
    - 尽量选择较为成熟、稳定的产品或版本
    - 尽量避免根据用户账号提供代理服务的方式
    - 应该只对一定IP地址范围内的主机提供服务
    - 禁用远程配置，只允许在本机实施配置
    - 定期升级，并通过相应的扫描软件及早发现代理服务配置的漏洞

10.3 构建防火墙

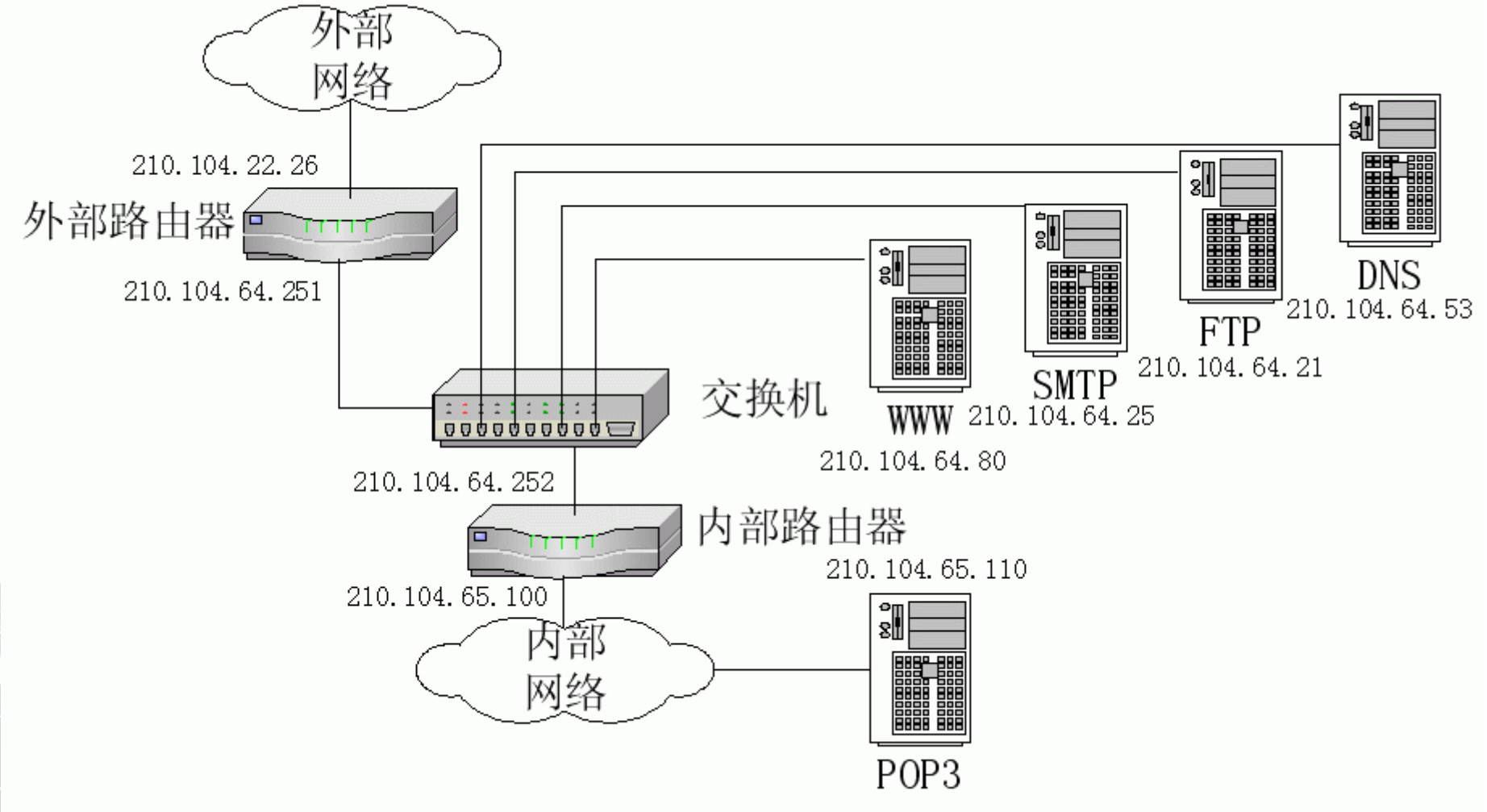
- 设置代理系统
  - 设置代理客户端
    - 使用定制客户端软件
    - 使用定制的用户过程



10.3 构建防火墙

- 检查防火墙运行效果
  - 检查的内容包括
    - 对外提供的服务
      - WWW、FTP、BBS、EMAIL
    - 对内提供的服务
      - DNS等
    - 网络访问
      - 检查过滤规则是否生效，并及早发现规则中存在的漏洞

10.3 构建防火墙


外部
网络
210.104.22.26
外部路由器
210.104.64.251
交换机
210.104.64.252
内部路由器
210.104.65.100
210.104.65.110
内部
网络
WWW
210.104.64.80
SMTP
210.104.64.25
FTP
210.104.64.21
DNS
210.104.64.53
POP3

10.3 构建防火墙

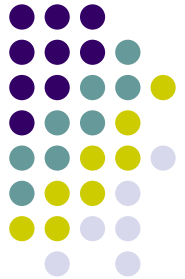
序号	路由器	接口	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.80	TCP	>1023	80	Accept
2	外部	内网	向内	210.104.64.80	0.0.0.0/0.0.0.0	TCP	80	>1023	Accept
3	内部	内网	向内	210.104.65.0/ 255.255.255.0	210.104.64.80	TCP	>1023	80	Accept
4	内部	外网	向内	210.104.64.80	210.104.65.0/ 255.255.255.0	TCP	80	>1023	Accept

10.3 构建防火墙

序号	路由器	接口	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.21	TCP	>1023	21	Accept
2	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.21	TCP	>1023	20	Accept
3	外部	内网	向内	210.104.64.21	0.0.0.0/0.0.0.0	TCP	21	>1023	Accept
4	外部	内网	向内	210.104.64.21	0.0.0.0/0.0.0.0	TCP	20	>1023	Accept
5	内部	内网	向内	210.104.65.0/ 255.255.255.0	210.104.64.21	TCP	>1023	21	Accept
6	内部	内网	向内	210.104.65.0/ 255.255.255.0	210.104.64.21	TCP	>1023	20	Accept
7	内部	外网	向内	210.104.64.21	210.104.65.0/ 255.255.255.0	TCP	21	>1023	Accept
8	内部	外网	向内	210.104.64.21	210.104.65.0/ 255.255.255.0	TCP	20	>1023	Accept

10.3 构建防火墙

序号	路由器	接口	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.25	TCP	25	25	Accept
2	外部	内网	向内	210.104.64.25	0.0.0.0/0.0.0.0	TCP	25	25	Accept
3	内部	外网	向内	210.104.64.25	210.104.65.110	TCP	25	25	Accept
4	内部	内网	向内	210.104.65.110	210.104.64.25	TCP	25	25	Accept
5	内部	内网	向内	210.104.65.0/255.255.255.0	210.104.64.25	TCP	>1023	25	Accept
6	内部	外网	向内	210.104.64.25	210.104.65.0/255.255.255.0	TCP	25	>1023	Accept



10.3 构建防火墙

- 防
-

序号	路由器	接口	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.53	UDP	53	53	Accept
2	外部	内网	向内	210.104.64.53	0.0.0.0/0.0.0.0	UDP	53	53	Accept
3	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.53	UDP	>1023	53	Drop
4	外部	内网	向内	210.104.64.53	0.0.0.0/0.0.0.0	UDP	53	>1023	Drop
5	内部	内网	向内	210.104.65.0/ 255.255.255.0	210.104.64.53	UDP	>1023	53	Accept
6	内部	外网	向内	210.104.64.53	210.104.65.0/ 255.255.255.0	UDP	53	>1023	Accept

10.3 构建防火墙

序号	路由器	接口	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	外部	外网	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject
2	外部	内网	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject
3	内部	外网	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject
4	内部	内网	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject

第10章 防火墙技术

- 防火墙技术概述
- 防火墙的结构
- 构建防火墙
- 防火墙产品

第10章 防火墙技术

- 课后习题
  - 防火墙规则的处理方式中，“Reject”与“Drop”的区别是什么？
  - 使用应用层代理访问外部Web站点时，会出现访问某些经典网站的响应速度较快，而其他站点响应速度较慢，原因何在？
  - 如果防火墙允许周边网络上的主机访问内部网络上的任何基于TCP协议的服务，而禁止外部网络访问周边网络上的任何基于TCP协议的服务，给出实现的思路？