防火墙

定义

- 在计算机网络中是指设置在可信任的内部网络和不可信任的外界之间的屏障，通过强化边界控制保障内容安全，同时不妨碍内部对外部的访问。

作用

①强化网络安全策略：具有不同信任的互连网络

②防止网络故障蔓延

③对网络访问进行监控审核和报警

④提供流量控制（带宽管理）和计费

⑤利用IPSec实现VPN

⑥实现MAC与IP地址的绑定

局限性

①**防火墙可能被绕过**

②**无法抵御内部威胁**

③**不能防止对开放端口（服务）的攻击。**

④防火墙可以阻断攻击，但无法消除攻击源。

⑤防火墙自身也可能会受到攻击。

种类

包过滤型防火墙

- 最简单、最快的防火墙
- 任何防火墙系统的基础
- 检查每个IP数据包（没有上下文）按规则
- 允许或拒绝，查看的信息包括源IP地址、目的IP地址、TCP/UDP端口号、承载协议等
- 可能的默认策略：不指定允许的，都禁止；不指定禁止的，都允许

可能受到的攻击

- IP地址欺骗
- 源路由攻击
- 微小碎片攻击

代理防火墙

- 工作过程：
    1. 用户将请求的服务发送给代理防火墙
    2. 代理防火墙验证请求为合法后向网络应用服务器发送请求
    3. 网络应用服务器将服务数据发送给代理防火墙，代理防火墙将数据发送给用户
- **代理防火墙又包括应用级代理、电路级代理**
    - 应用级代理也被称作应用级网关，每个服务需要单独的代理服务，应用级网关可以在应用程序级别记录/审核流量
    - 电路级代理也被称作电路层网关，**工作在OSI模型的会话层**，维护一张合法的会话连接表，进行会话层过滤。一旦认为会话合法，就为双方建立连接，之后就作为数据的中转站，不再进行审查

状态检测防火墙

- 传统的包过滤不检查更高一层的语境，即匹配返回包和外向流
- 状态检测型防火墙扩展了包过滤防火墙，跟踪每个通过TCP连接的状态，将属于同一连接的所有包作为一个整体的数据流看待。
    - 跟踪客户机服务器会话
    - 检查每个包是否有效属于一个会话
- 因此，能够在上下文中更好地检测伪造包。甚至可能检查有限的应用程序数据

地址转换防火墙

- 网络地址转换（NAT）就是使用两套IP地址：内部IP地址（私有IP地址）和外部IP地址（公共IP地址）。
- 私有IP地址块：
    - A类：10.0.0.0~10.255.255.255
    - B类：172.16.0.0~172.31.0.0
    - C类：192.168.0.0~192.168.255.255
- 基本NAT的实现包括两种方法：
    - 静态NAT:私有IP地址与公共IP地址具有一对一关系。
    - 动态NAT:私有IP地址与公共IP地址具有动态（临时）一对一关系。全局地址放入NAT池。
- 网络地址端口转换（NAPT）：将内部地址映射到外部网络IP地址的不同端口上。

工作模式

防火墙的工作模式包括3种

①路由模式：防火墙以第3层对外连接（接口具有IP地址）。

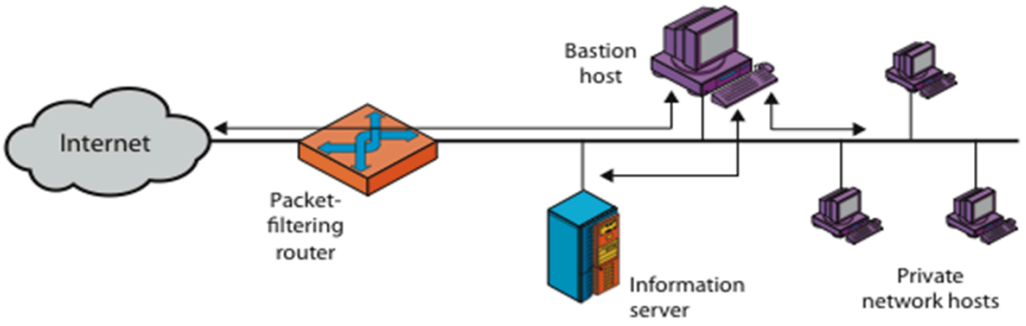
②透明模式：防火墙以第2层对外连接（接口无IP地址）。

③混合模式：若防火墙既存在工作在路由模式的接口也存在工作在透明模式的接口。

部署（随便看看）

屏蔽路由器和屏蔽主机(Screened Host)

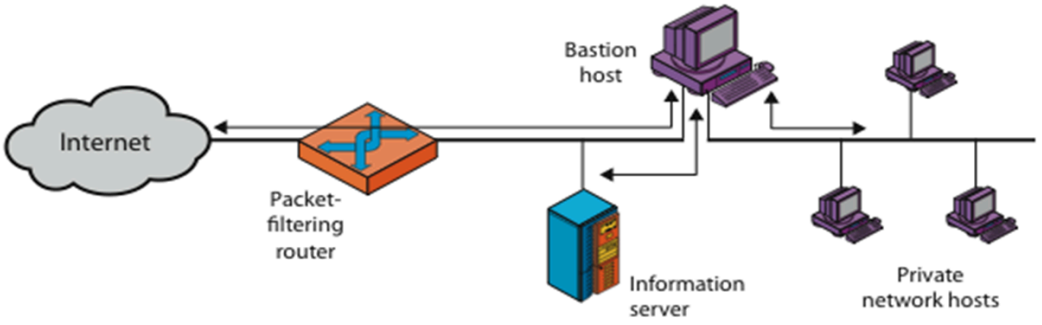
具有数据包过滤功能的路由器叫屏蔽路由器，具有数据包过滤功能的主机叫屏蔽主机



(a) Screened host firewall system (single-homed bastion host)

双宿/多宿主机(Dual-Homed /Multi-Homed Host Firewall)

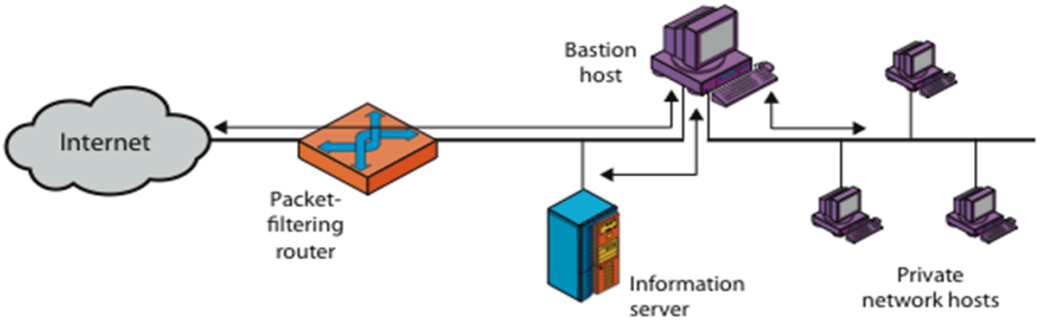
有两个网络接口的计算机系统，一个接口连接内部网，一个接口连接外部网



(b) Screened host firewall system (dual-homed bastion host)

堡垒主机（Bastion Host)

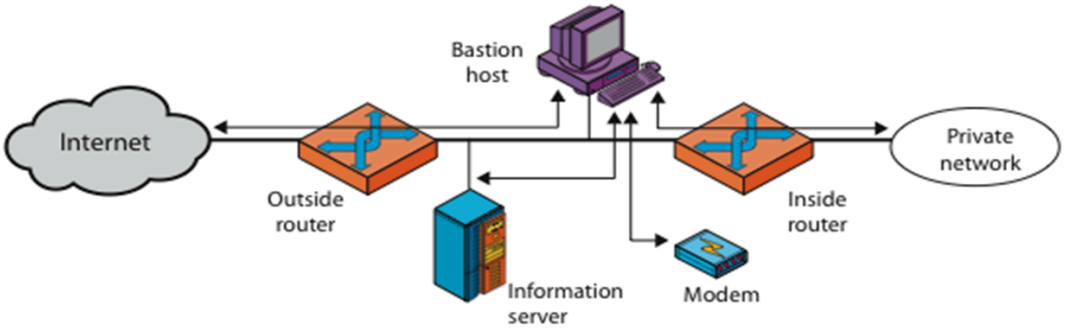
堡垒主机是一种配置了安全防范措施的网络上的计算机，堡垒主机为网络之间的通信提供了一个阻塞点，也就是说如果没有堡垒主机，网络之间将不能相互访问。可以配置成过滤型、代理型或混合型



(b) Screened host firewall system (dual-homed bastion host)

屏蔽子网防火墙(Screened Subnet Firewall)

它是在被保护网络和Internet之间设置了一个独立的子网作为防火墙

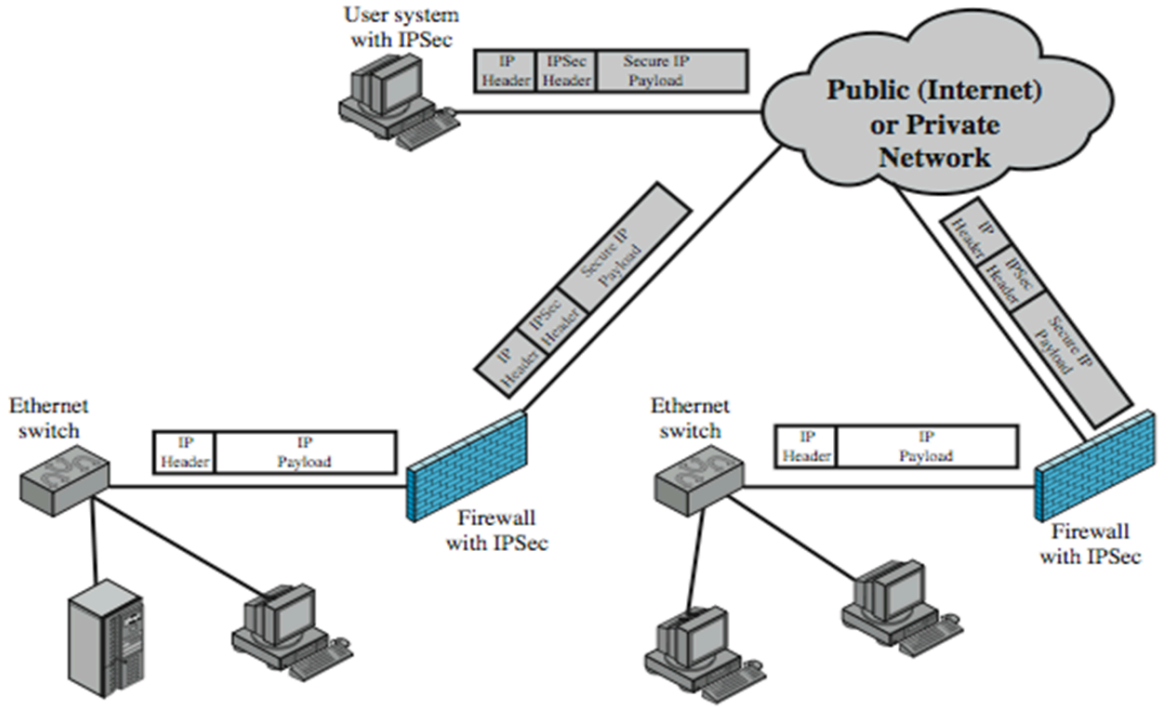


(c) Screened-subnet firewall system

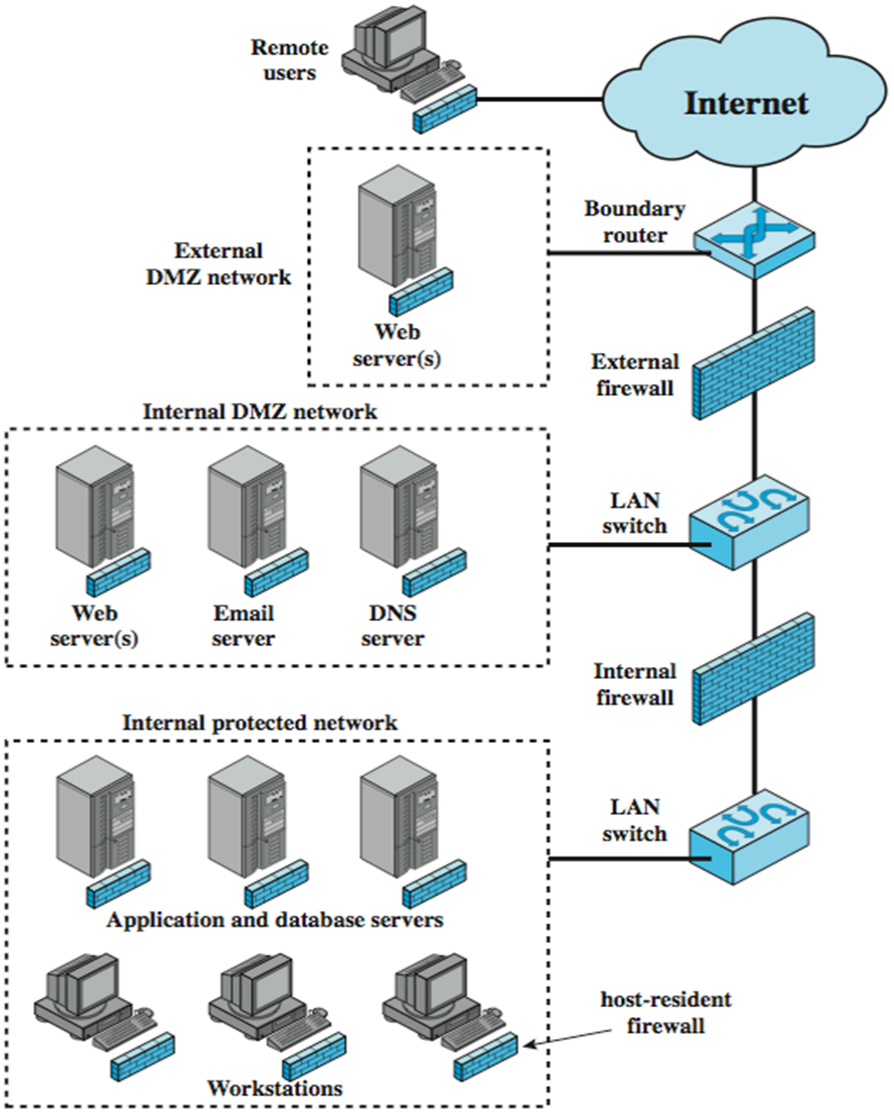
DMZ网络

DMZ一般指两台包过滤防火墙之间的区域，称为非军事区

虚拟私人网络



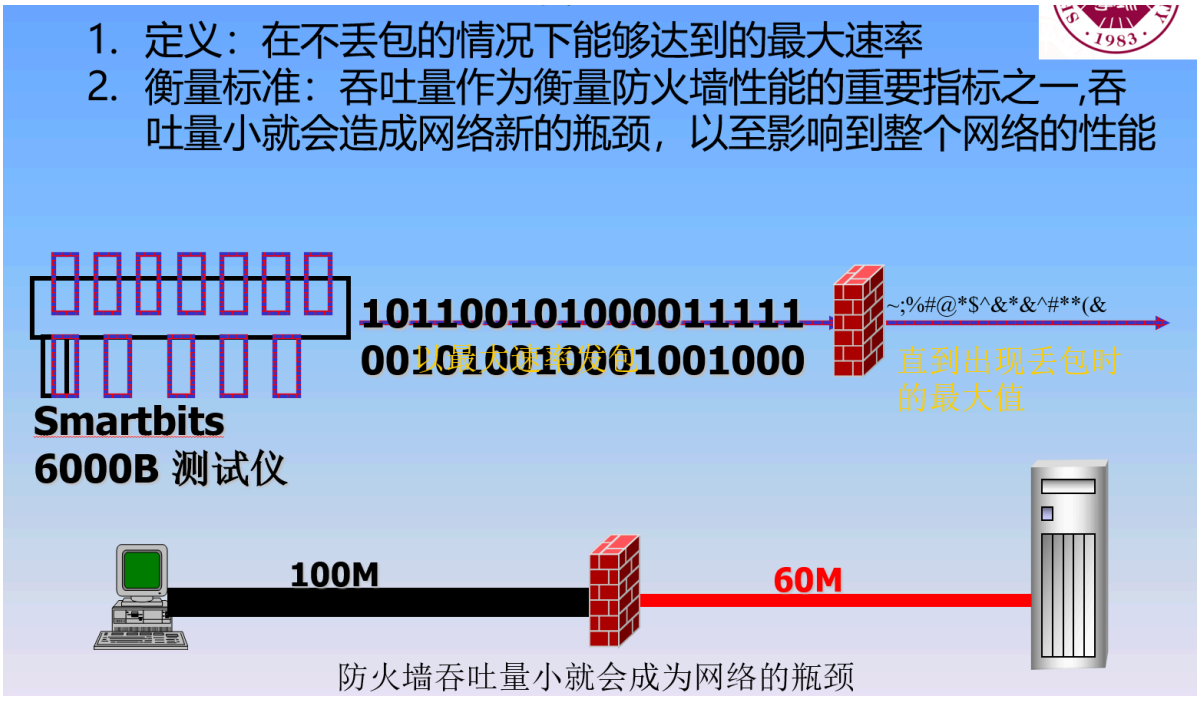
分布式防火墙



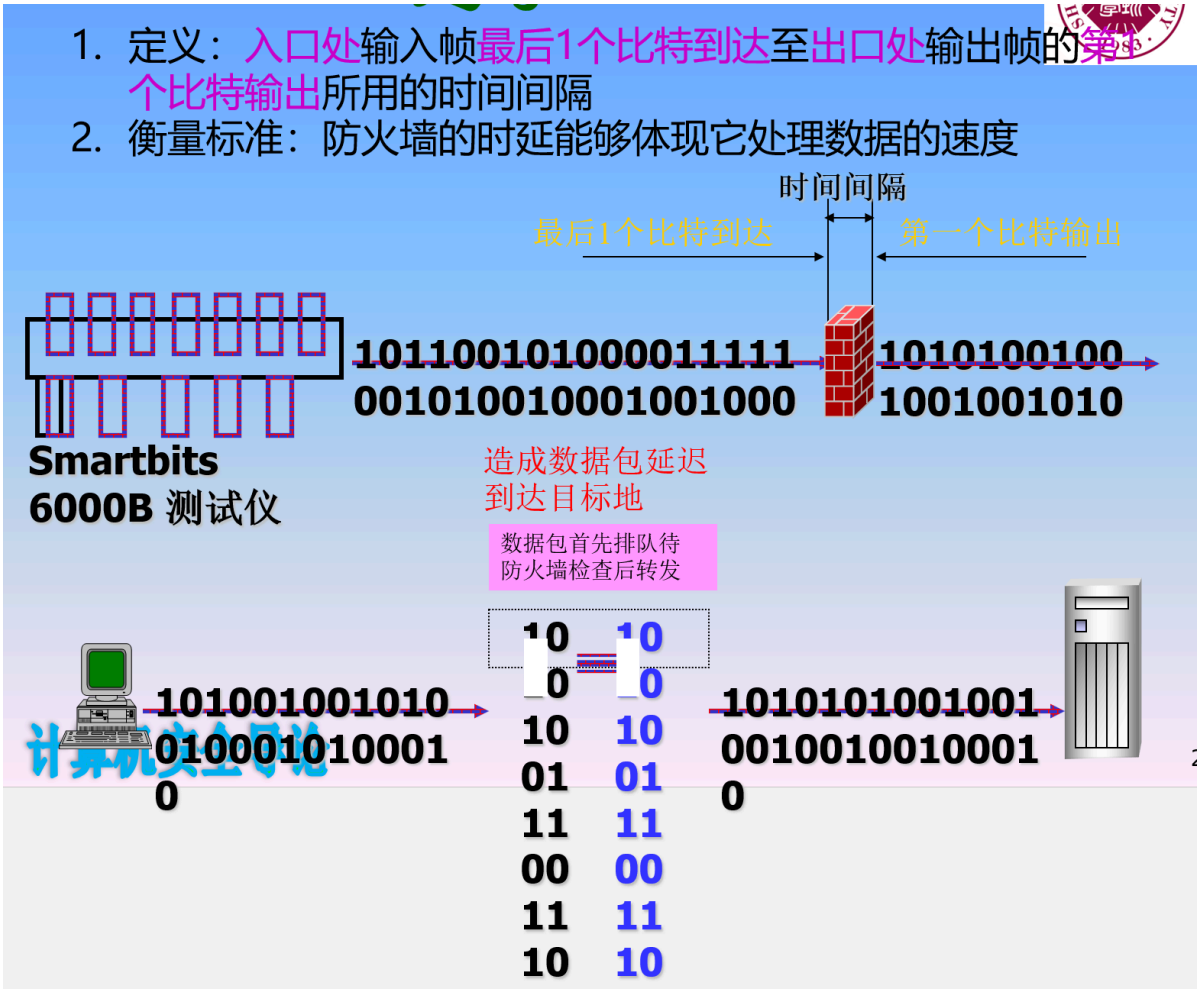
性能指标

①吞吐量

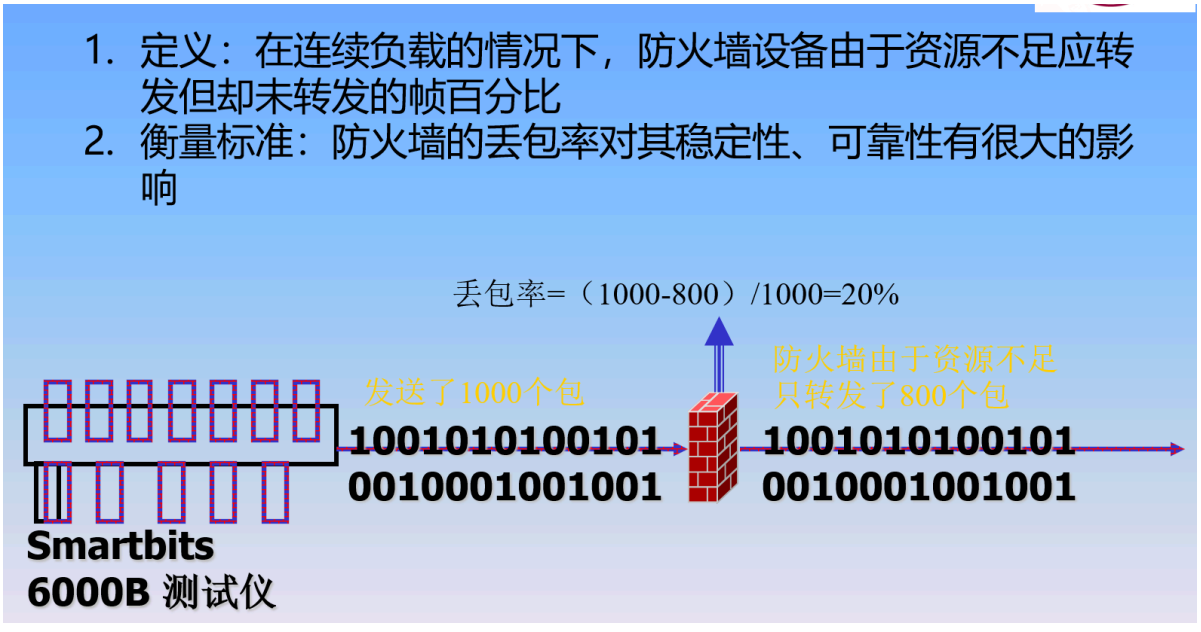
1. 定义：在不丢包的情况下能够达到的最大速率
2. 衡量标准：吞吐量作为衡量防火墙性能的重要指标之一,吞吐量小就会造成网络新的瓶颈，以至影响到整个网络的性能



②延时

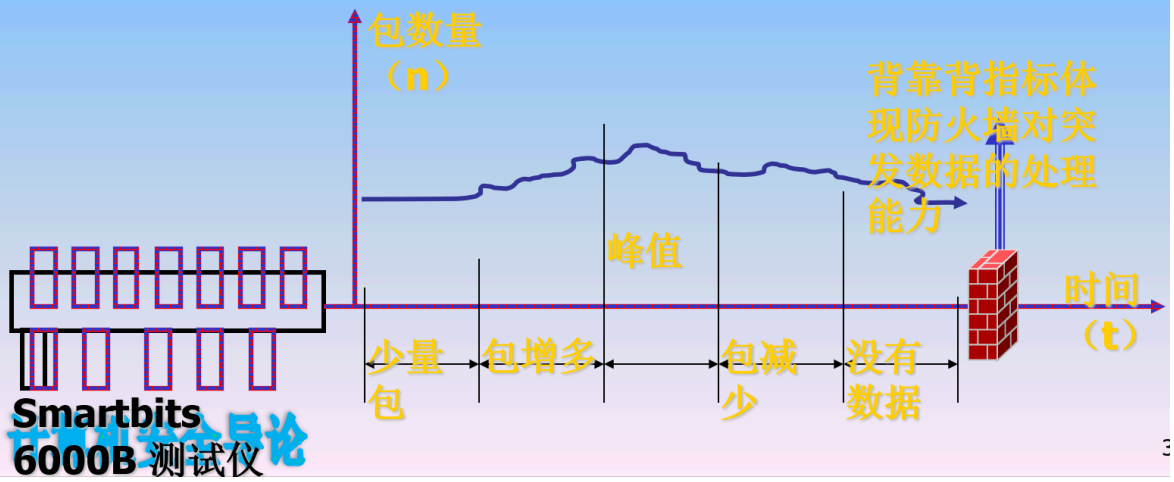


③丢包率



④背靠背

1. 定义：从空闲状态开始，以达到传输介质最小合法间隔极限的传输速率发送相当数量的固定长度的帧，当出现第一个帧丢失时，发送的帧数。
2. 衡量标准：背靠背包的测试结果能体现出被测防火墙的缓冲容量，网络上经常有一些应用会产生大量的突发数据包（例如：备份，路由更新等），而且这样的数据包的丢失可能会产生更多的数据包，强大缓冲能力可以减小这种突发对网络造成的影响



⑤最大并发连接数

⑥最大并发连接建立速率

⑦最大策略数

⑧平均无故障间隔时间

⑨支持的最大用户数