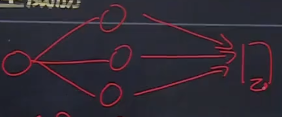
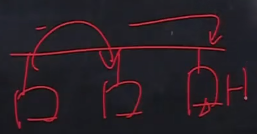
第八章网络安全基础：网络安全概述，数据加密，消息完整性与数字签名，身份认证，密钥分发中心与证书认证，防火墙与入侵检测系统，网络安全协议

网络安全概述

1. 基本概念

网络安全通信所需要的基本属性：

1. 机密性：不会被非授权人看到
2. 消息完整性：不会被非授权人修改
3. 可访问与可用性：防火墙，备用设备
4. 身份认证
5. 网络安全威胁
6. 窃听：电脑屏幕、电信号
7. 插入：完整性的破坏
8. 假冒：诈骗电话，邮件的发件人信息
9. 劫持：截获信息可以进行篡改
10. 拒绝服务DoS和分布式拒绝服务DDoS：网络层ICMP（Ping命令）->Ping of death->蓝屏，或者大量给你发送信息，分布式：大量计算机给一台计算机发送信息（一台计算机可以控制成千上万、上百万、上千万台计算机->僵尸网络）
11. 映射：给你每个端口发信息->扫描你的计算机提供了什么服务->端口扫描
12. 嗅探：和窃听相似，比如在广播线上，在公共网络不要发送敏感信息
13. IP欺骗：也是一种假冒，为了使用内部资源改变IP地址