



第9章 网络安全 和网络管理

宁天桥

15820291950 / 661950

qq号: 930611

ntq@gcu.edu.cn

办公室: 行政楼 812

机器人工程学院
网络与通信技术



本章学习要求:

- ◆ 了解：网络安全与网络空间安全
- ◆ 掌握：OSI安全体系结构的内容
- ◆ 掌握：加密与认证的基本概念
- ◆ 掌握：网络安全协议的内容
- ◆ 掌握：防火墙的基本概念
- ◆ 了解：入侵检测的基本概念
- ◆ 了解：恶意代码发展及防护技术
- ◆ 掌握：网络管理的基本概念



9.4 网络安全协议



9.4.1 网络层安全与IPSec

- ◆ IPSec是IETF为网络层通信安全制订的一个协议集，目前已被广泛应用于VPN系统中。
- ◆ IPSec适用于各版本的IP协议（IPv4与IPv6），IPv4将IPSec作为一种可选的扩展协议，IPv6将IPSec作为组成部分来使用。
- ◆ IPSec设计目标是为IP分组传输提供安全服务，例如数据源身份认证、数据完整性认证与数据加密等。



IPSec组成部分

- ◆ **认证头 (AH, Authentication Header) : 提供数据源身份认证、数据完整性认证, 以及可选的抗重放数据包功能。**
- ◆ **封装安全负载 (ESP, Encapsulating Security Payload) : 提供AH协议的所有功能, 以及数据加密服务。**
- ◆ **密钥管理协议: 通信双方之间协商安全参数, 例如工作模式、认证或加密算法、密钥与生存期等。**



IPSec工作模式

- ◆ **传输模式 (Transport Mode) : 隧道两端分别位于两台IPSec主机, 提供主机到主机的安全服务。**
- ◆ **隧道模式 (Channel Mode) : 隧道两端分别位于两台IPSec网关, 提供子网到子网的安全服务。**
- ◆ **隧道模式会隐藏IP分组的路由信息, 可提供比传输模式更高的安全性。**

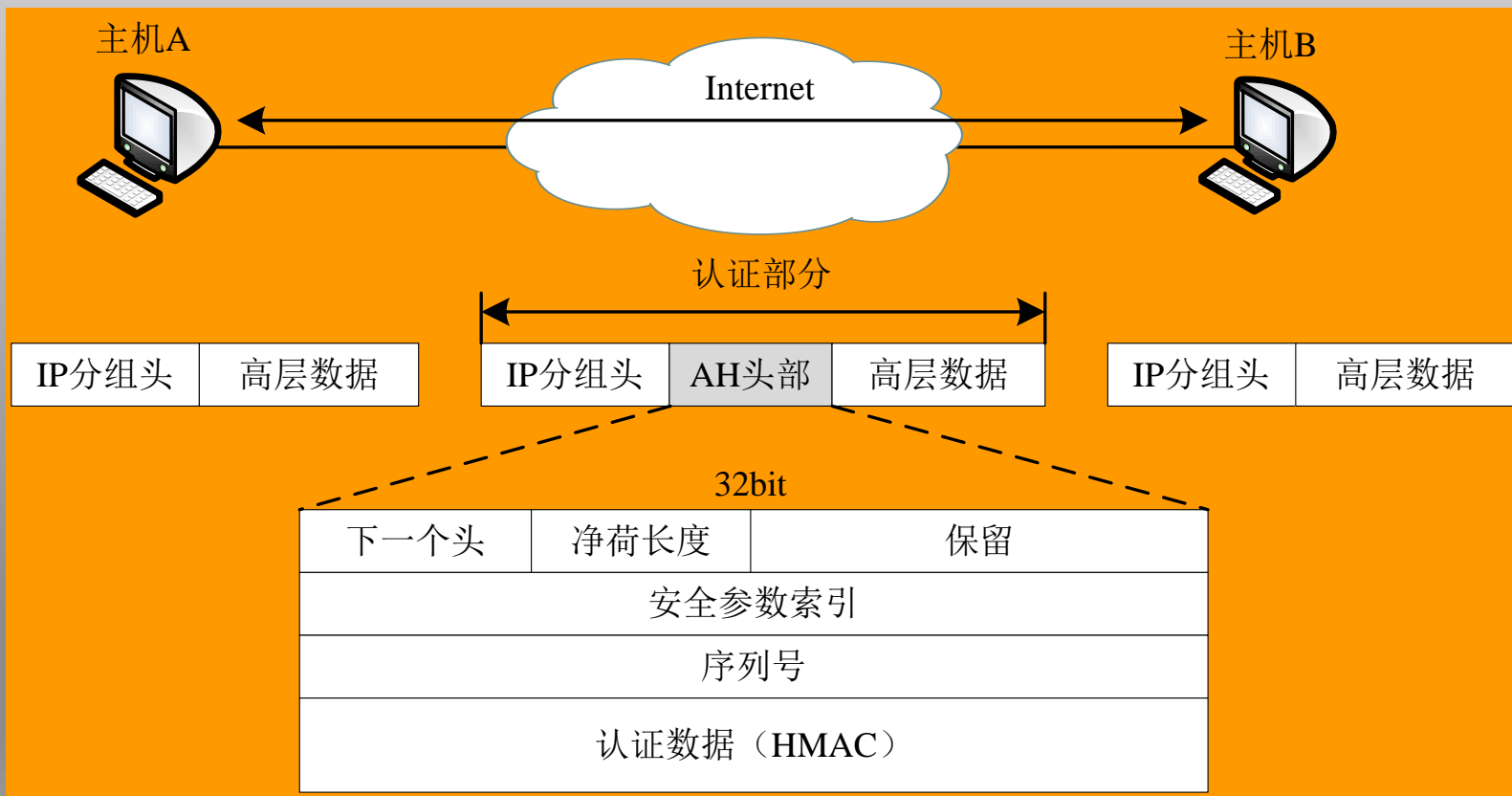


密钥管理协议

- ◆ 互联网安全关联与密钥管理协议 (ISAKMP, Internet Security Association and Key Management protocol)
- ◆ 互联网密钥交换 (IKE, Internet Key Exchange)
- ◆ Oakley协议



传输模式AH的工作原理





9.4.2 传输层安全与SSL

- ◆ Netscape公司提出用于Web应用的安全套接层（SSL, Secure Sockets Layer）协议。
- ◆ Microsoft公司开发类似的PCT（Private Communication Technology）协议。
- ◆ IETF发布传输层协议（TLS, Transport Layer Security），希望推动传输层安全协议标准化。



SSL协议的特点

- ◆ SSL可用于HTTP、FTP、Telnet等，但目前主要应用于HTTP协议，为基于Web服务的各种网络应用提供身份认证与安全传输服务。
- ◆ SSL处于端系统的应用层与传输层之间，在TCP上建立一个加密的安全通道，为TCP协议的数据传输提供安全保障。
- ◆ SSL握手协议实现通信双方的加密算法协商与密钥传递；SSL记录协议定义SSL数据传输格式，实现对数据的加密与解密操作。



9.4.3 应用层安全与PGP、SET

- ◆ PGP (Pretty Good Privacy) 协议用于解决电子邮件安全问题，提供电子邮件的加密、身份认证、数字签名等功能。
- ◆ SET协议是目前公认、成熟的电子支付安全协议，使用对称加密与公钥加密体制，以及数字信封、信息摘要与双重签名技术。



9.5 防火墙技术

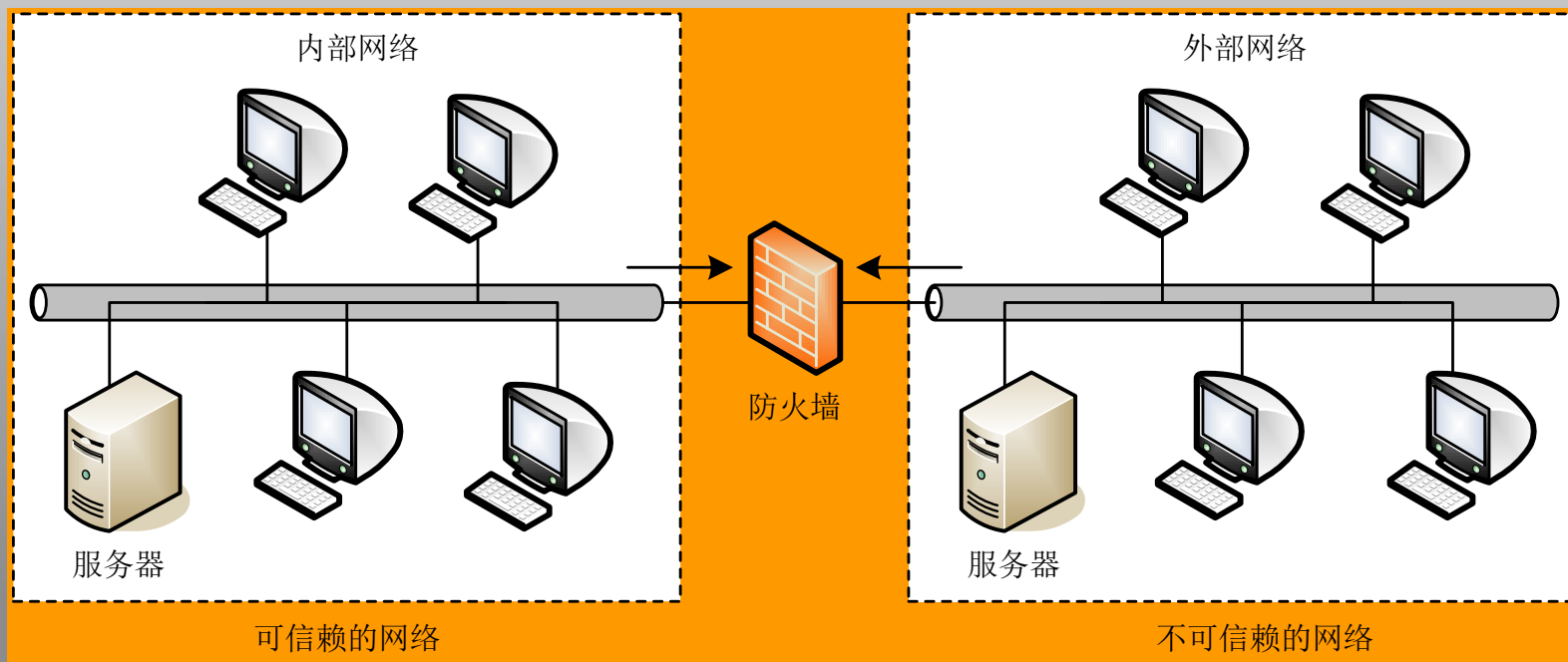


9.5.1 防火墙的基本概念

- ◆ **防火墙 (Firewall) 是在网络之间执行控制策略的系统，它包括硬件和软件。**
- ◆ **防火墙保护的内部网络是可信任网络，而外部网络是不可信任网络。**
- ◆ **防火墙用于保护内部网络的资源不被外部非授权用户使用，防止内部受到外部非法用户的攻击。**



防火墙的基本结构





防火墙的基本功能

- ◆ 检查所有从外部进入内部网络的数据包。
- ◆ 检查所有从内部网络流出外部的数据包。
- ◆ 执行安全策略，限制所有不符合安全策略的数据包通过。
- ◆ 具有防攻击能力，保证自身的安全性的能力。



9.5.2 防火墙的分类

- ◆ 防火墙系统的两个基本部件是：包过滤路由器（Packet Filtering Router）和应用级网关（Application Gateway）。
- ◆ 简单的防火墙由一个包过滤路由器组成，复杂的防火墙系统由包过滤路由器和应用级网关的组合。

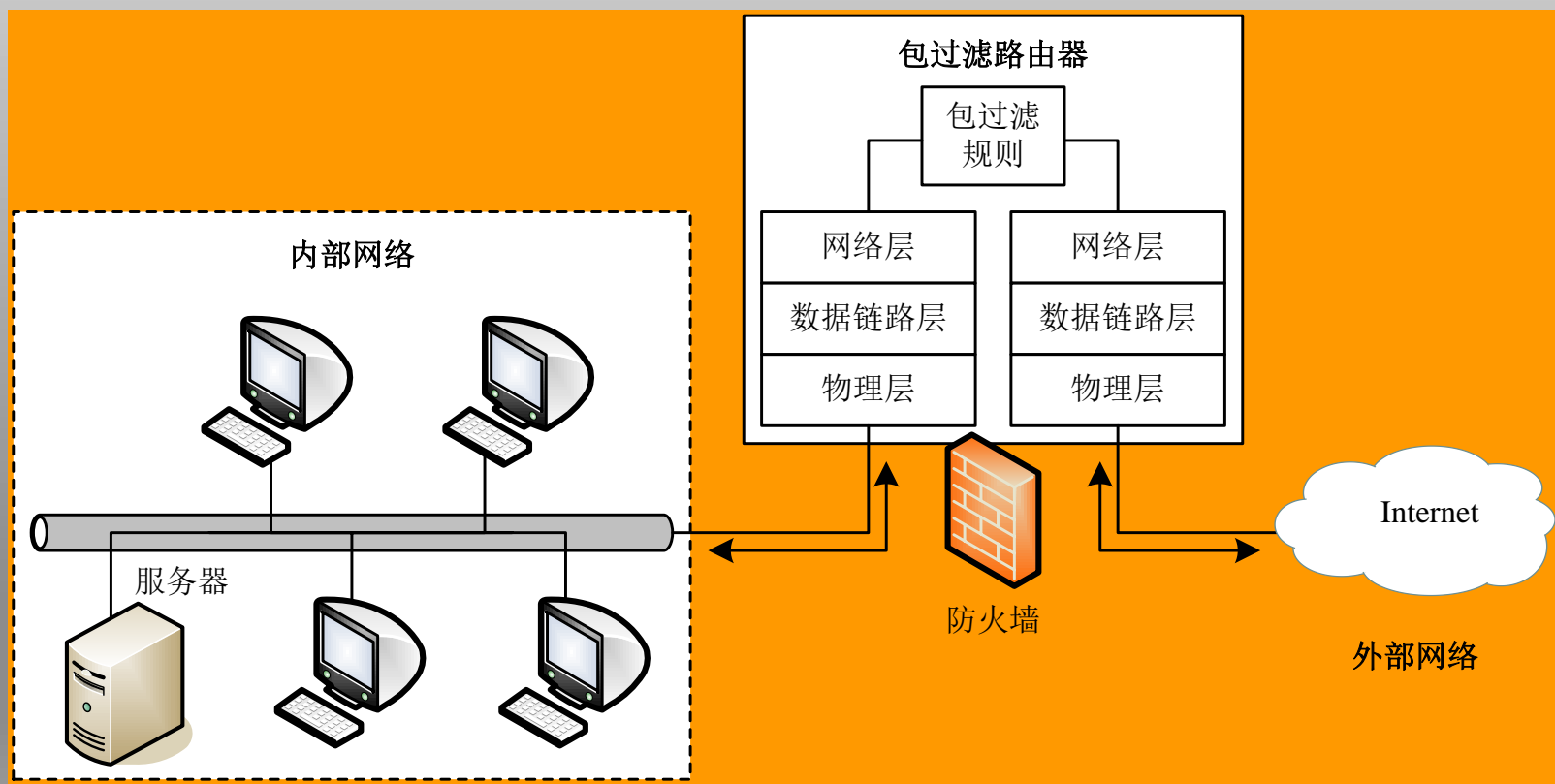


包过滤路由器的概念

- ◆ **包过滤路由器按系统内部设置的包过滤规则（即访问控制表），检查每个分组的源IP地址、目的IP地址，决定该分组是否应该转发。**
- ◆ **包过滤规则通常基于部分或全部报头内容。例如，TCP报头信息包括：源IP地址、目的IP地址、协议类型、IP选项内容、源TCP端口号、目的TCP端口号、TCP ACK标识等。**



包过滤路由器的工作原理



应用级网关

- ◆ 多归属主机又称为多宿主主机，它具有两个或两个以上的网络接口，每个网络接口与一个网络连接，具有在不同网络之间交换数据的能力。
- ◆ 通过应用程序访问控制规则，多归属主机可作为应用级网关，在应用层过滤进出内部网络特定服务的用户请求与响应。
- ◆ 应用代理是应用级网关的另一种形式，以存储转发方式检查和确定发送网络服务请求的用户身份，决定是否转发该服务请求。

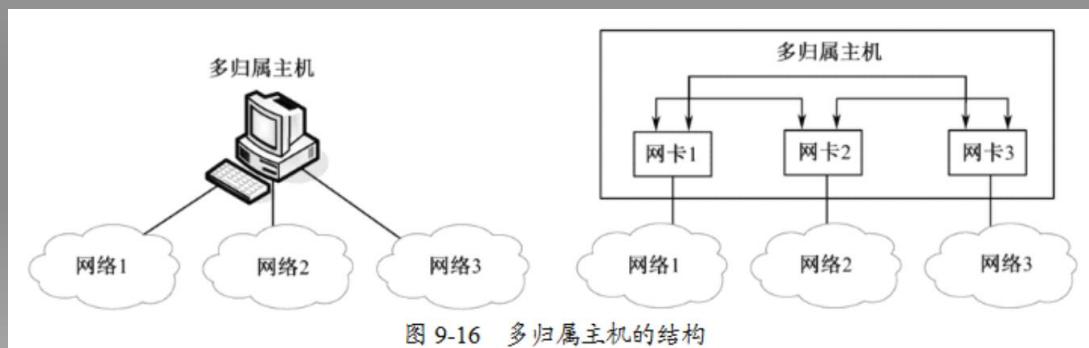
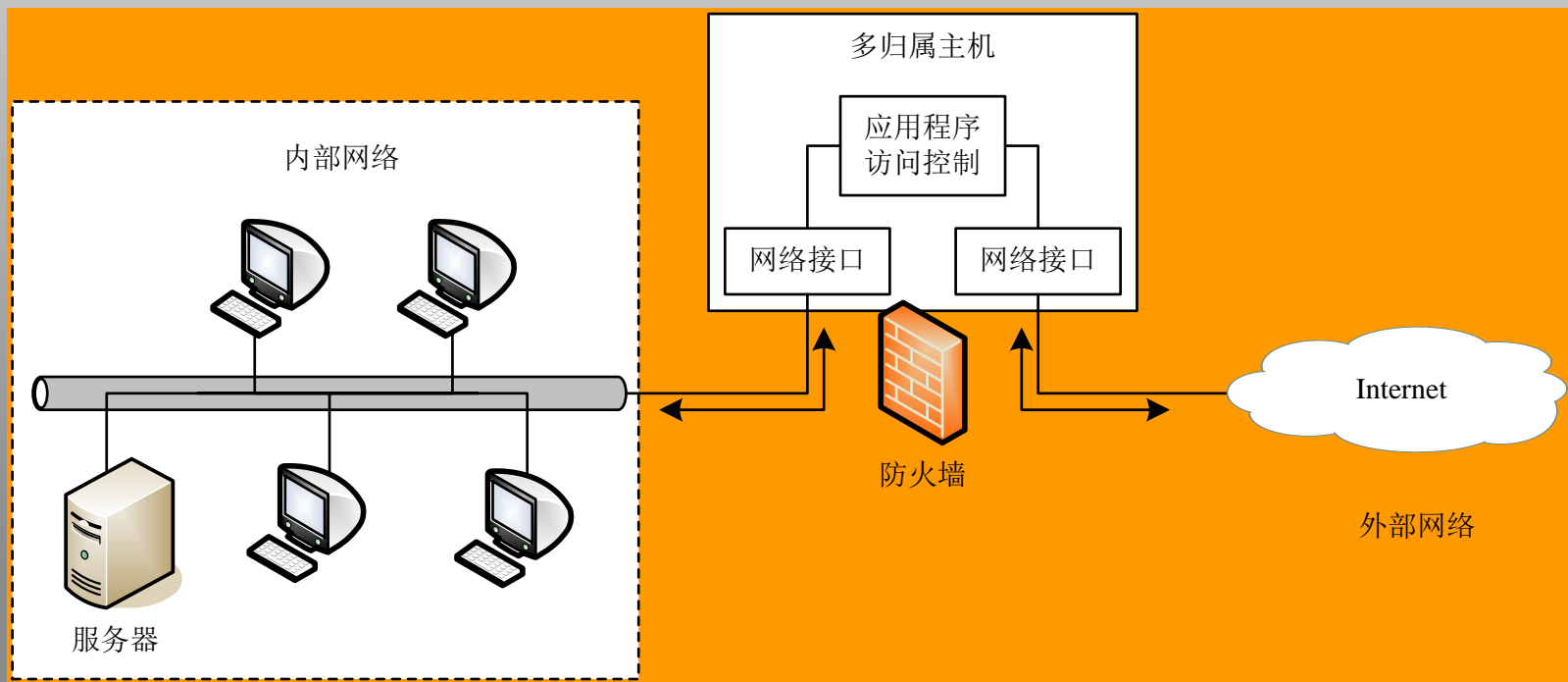


图 9-16 多归属主机的结构



应用级网关的工作原理



9.5.3 防火墙系统结构

◆ 应用级网关结构的防火墙

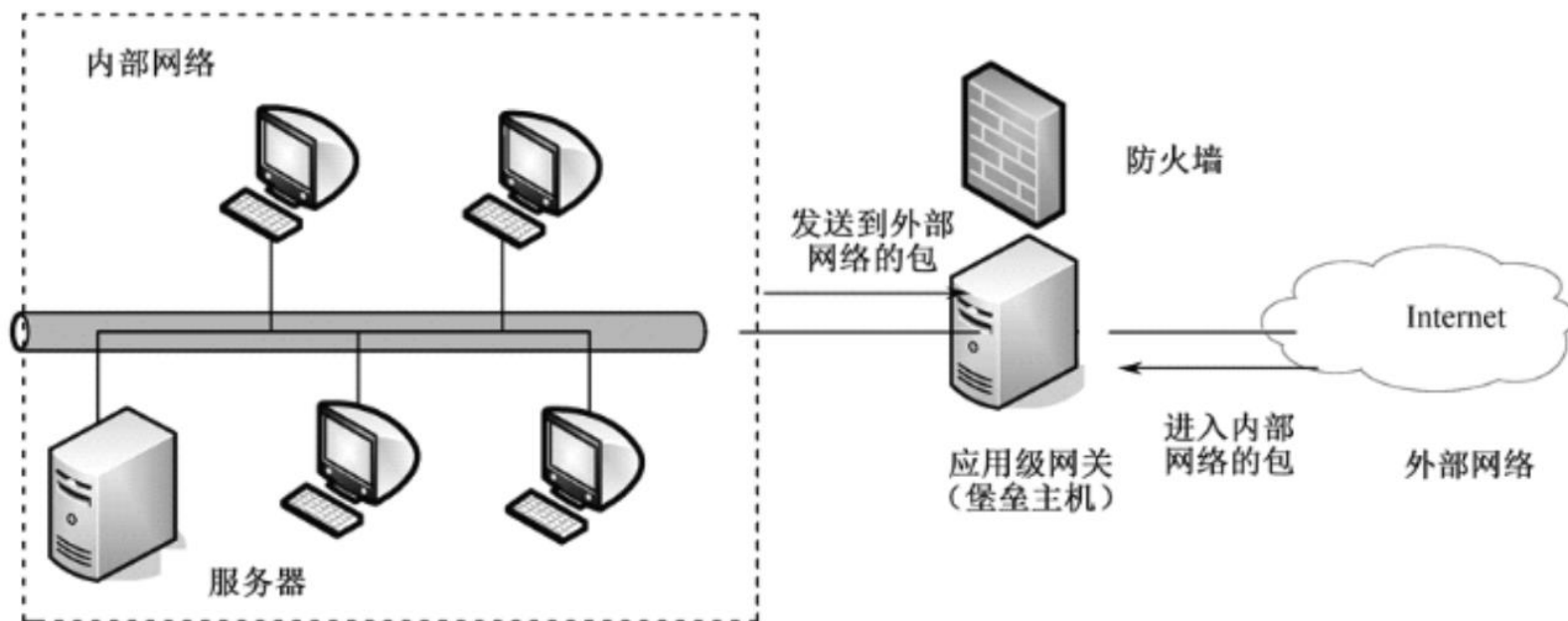
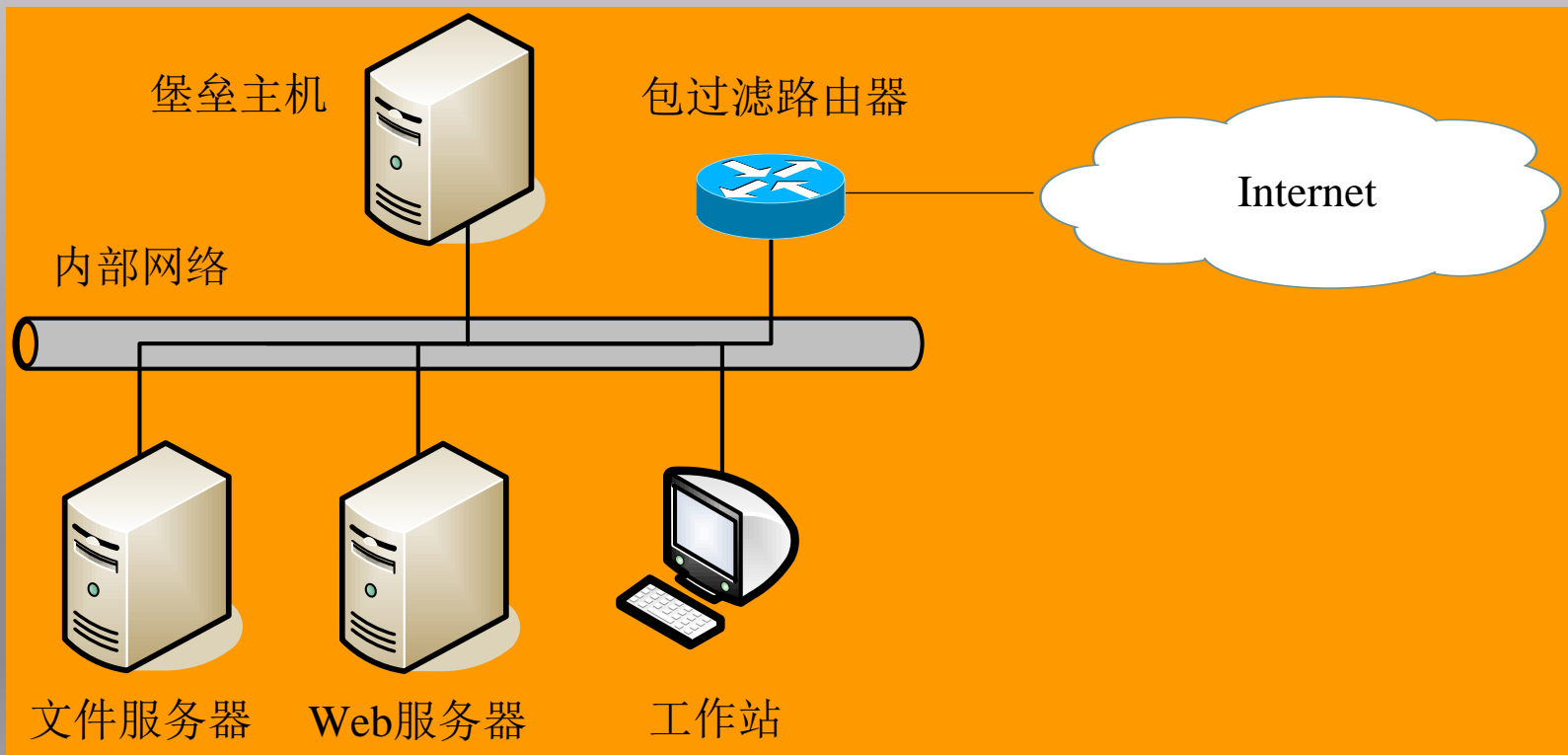


图 9-19 应用级网关结构的防火墙



9.5.3 防火墙系统结构

◆ S-B1防火墙系统



9.5.3 防火墙系统结构

◆ 多级结构防火墙系统

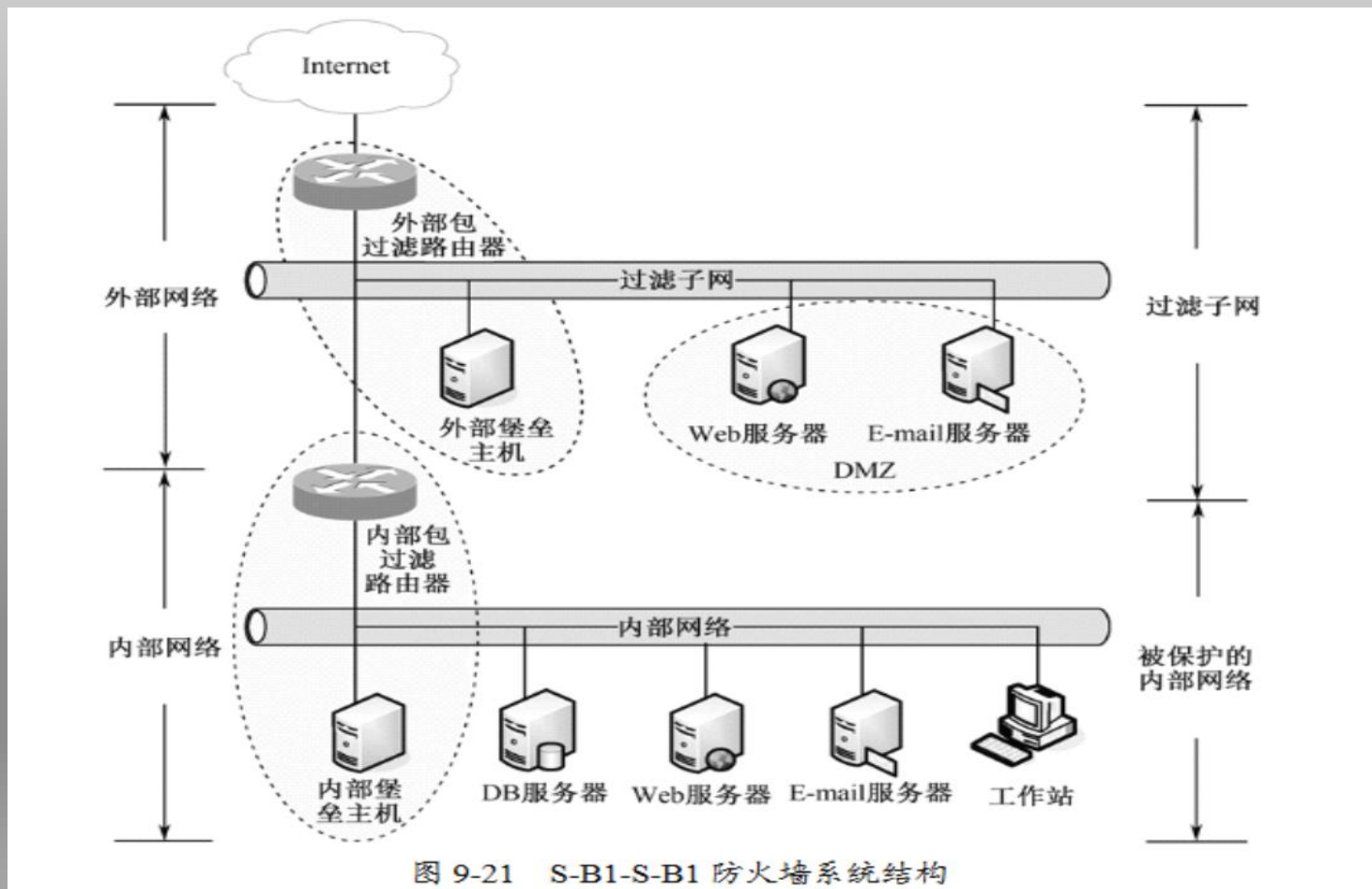


图 9-21 S-B1-S-B1 防火墙系统结构



9.6 入侵检测技术

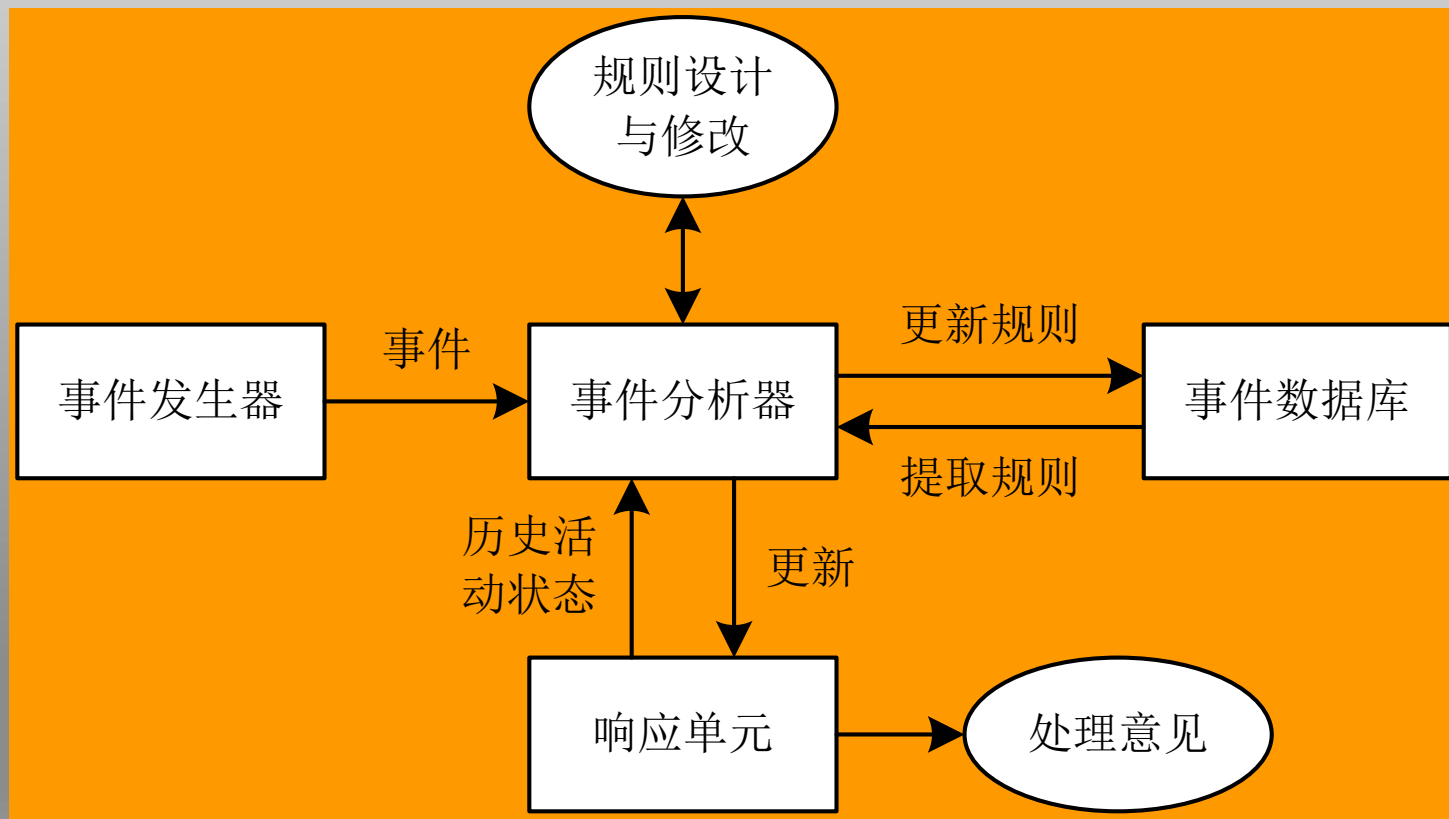


9.6.1 入侵检测的概念

- ◆ **入侵检测系统 (IDS, Intrusion Detection System)** 是识别对计算机和网络资源的恶意使用行为的系统。
- ◆ **入侵检测监测和发现可能存在的攻击行为，包括来自系统外部的入侵行为，以及来自内部用户的非授权行为，并采取相应的防护手段。**

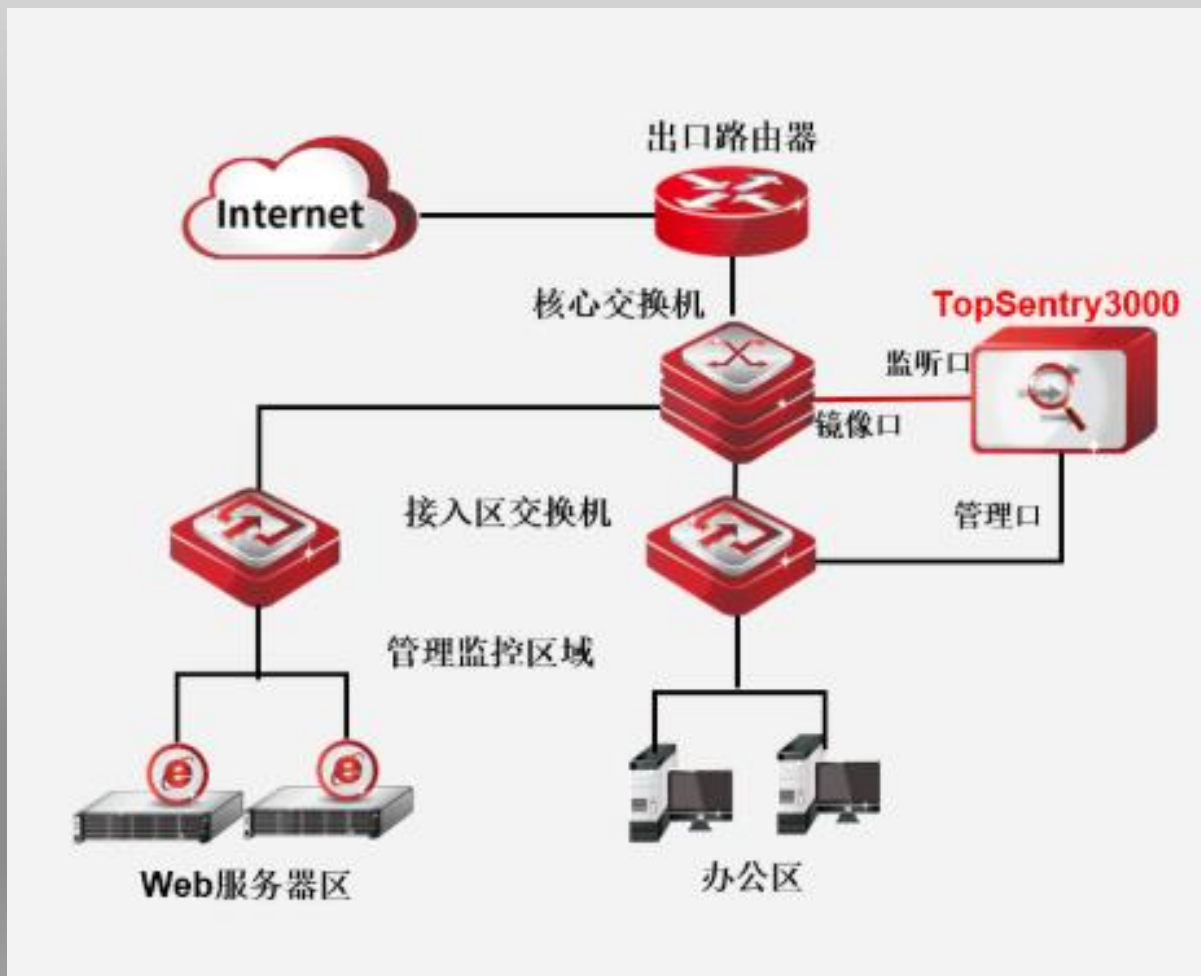


入侵检测系统的框架结构





入侵检测系统在网络中部署





9.6.2 入侵检测的分类

- ◆ 按照采用的检测方法，入侵检测系统可分为：异常检测、误用检测，以及两种方法结合。
- ◆ 按照检测对象和基本方法，入侵检测系统可分为：基于主机的入侵检测系统、基于网络的入侵检测系统与分布式入侵检测系统。



9.6.3 蜜罐的概念

- ◆ 蜜罐 (Honey-pot) 是一个包含漏洞的诱骗系统，通过模拟主机、服务器或其他网络设备，为攻击者提供一个容易攻击的目标，诱骗攻击者对它发起攻击。
- ◆ 从应用目标的角度，蜜罐系统分为两类：研究型蜜罐与实用型蜜罐。从系统功能的角度，蜜罐系统分为三类：端口监控器、欺骗系统与多欺骗系统等。



9.7 恶意代码及防护技术



9.7.1 恶意代码的演变

- ◆ **恶意代码 (Malicious Code) 是在计算机之间或网络之间传播的程序，目的是在用户和网络管理员不知情的情况下故意修改系统。**
- ◆ **恶意代码具有三个共同特征：恶意的目的，本身是程序，通过执行产生作用。**
- ◆ **恶意代码早期的主要形式是计算机病毒。目前，恶意代码主要包括：计算机病毒、网络蠕虫、特洛伊木马、脚本攻击代码、垃圾邮件、流氓软件等。**



9.7.2 计算机病毒的概念

- ◆ **计算机病毒 (Computer Virus) 是指侵入计算机或网络系统，具有感染性、潜伏性与破坏性等特征的程序。**
- ◆ **从计算机病毒产生至今，其主要传播途径有2种：移动存储介质与计算机网络。**
- ◆ **计算机病毒生命周期通常分为4个阶段：休眠、传播、触发与执行阶段。**



9.7.3 网络蠕虫的概念

- ◆ **网络蠕虫 (Network Worm) 在设计上与计算机病毒类似，有时被认为是计算机病毒的一个子类。**
- ◆ **网络蠕虫的权威定义：一种无须用户干预、依靠自身复制能力、自动通过网络传播的恶意代码。**
- ◆ **网络蠕虫的最大优势表现在：自我复制与大规模传播能力。**



9.7.4 木马程序的概念

- ◆ 特洛伊木马 (Trojan Horse) 通常简称 “木马”，后来被引用为后门程序的代名词，特指为攻击者打开计算机后门的程序。
- ◆ 木马的权威定义：伪装成合法程序或隐藏在合法程序中的恶意代码，这些代码本身可能执行恶意行为，或者为非授权访问系统的提供后门。
- ◆ 木马程序通常不感染其他文件，它只是伪装成一种正常程序，并随着其他程序安装在计算机中，但是用户不知道该程序的真实功能。



9.7.5 网络防病毒技术

- ◆ 网络防病毒需要从两方面入手：工作站与服务器。
- ◆ 为了防止病毒从工作站侵入，可以采取以下措施：使用无盘工作站、带防病毒芯片的网卡、单机防病毒卡或网络防病毒软件。
- ◆ 网络防病毒系统通常包括以下几个部分：客户端防毒软件、服务器端防毒软件、针对邮件的防毒软件、针对黑客的防毒软件。



9.8 网络管理技术



9.8.1 网络管理的概念

- ◆ **网络管理是指用于运营、管理与维护一个网络，以及提供网络服务所需的各种活动的总称。**
- ◆ **网络提供：通过提供新服务类型增加网络服务，或通过增加新设备提高网络性能。**
- ◆ **网络维护：通过性能监控、故障诊断与恢复等，保证网络可靠与连续运行。**
- ◆ **网络处理：通过分析网络通信量、设备利用率等，优化网络资源使用效率。**

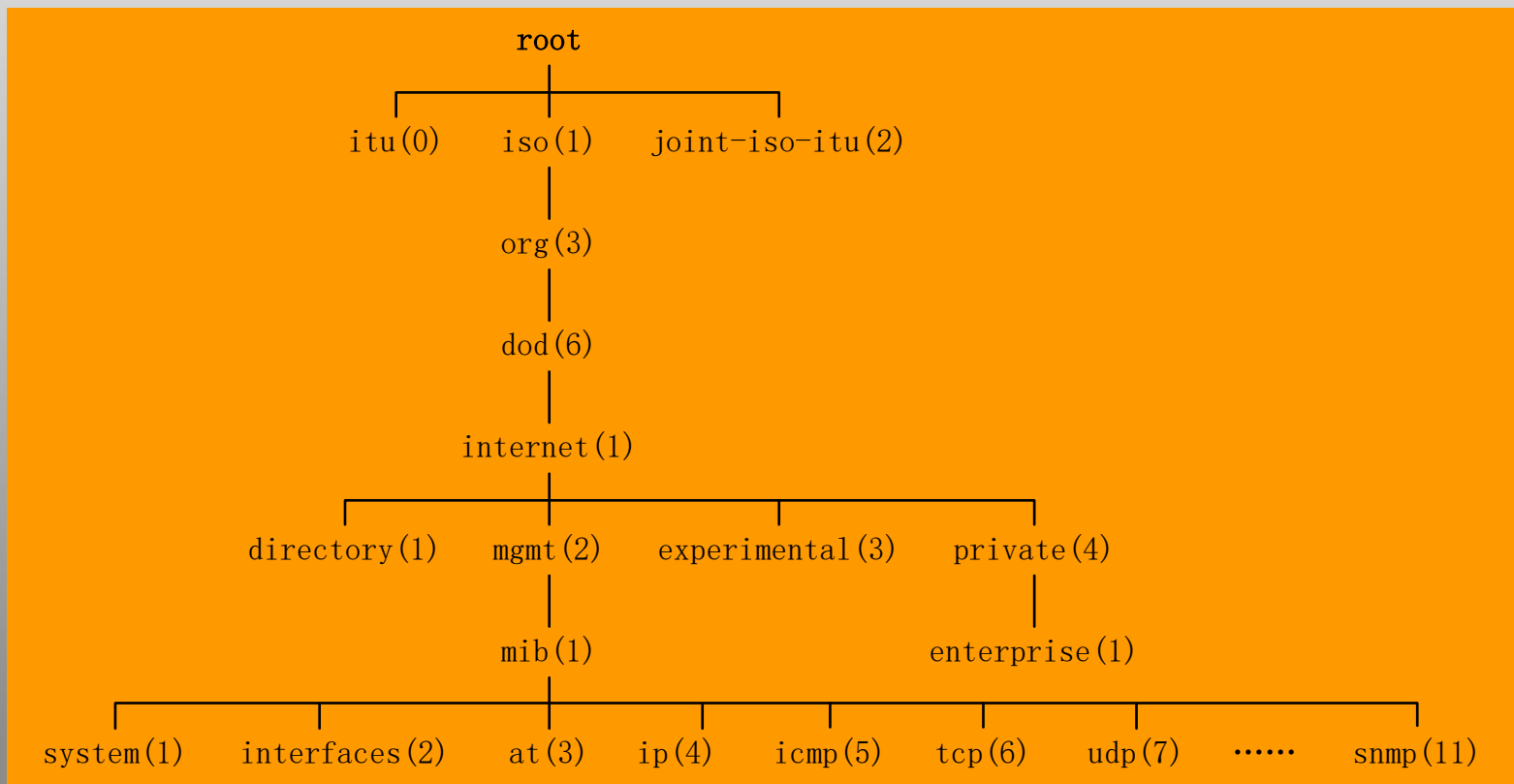


ISO定义的网管模型

- ◆ **组织模型：描述网管系统的组成与结构。**
- ◆ **信息模型：描述网管系统的对象命名。**
- ◆ **通信模型：描述网管系统使用的管理协议。**
- ◆ **功能模型：描述网管系统的主要功能。**



(MIT) 管理信息树



1.3.6.1 表示 Internet, 1.3.6.1.2.1表示MIB,
1.3.6.1.2.1.11表示 SNMP



9.8.2 网络管理功能域

- ◆ 配置管理 (Configuration Management)
- ◆ 故障管理 (Fault Management)
- ◆ 性能管理 (Performance Management)
- ◆ 安全管理 (Security Management)
- ◆ 记账管理 (Accounting Management)



9.8.3 网络管理系统的概念

- ◆ **管理对象 (Managed Object)** 是经过抽象的网络元素，对应网络中具体可操作的数据。
- ◆ **管理进程 (Manager Process)** 是对网络设备进行管理与监控的软件，它安装在网络中的网管工作站与各种网络设备中。
- ◆ **管理协议 (Management Protocol)** 负责在网管工作站与网络设备的管理进程之间通信

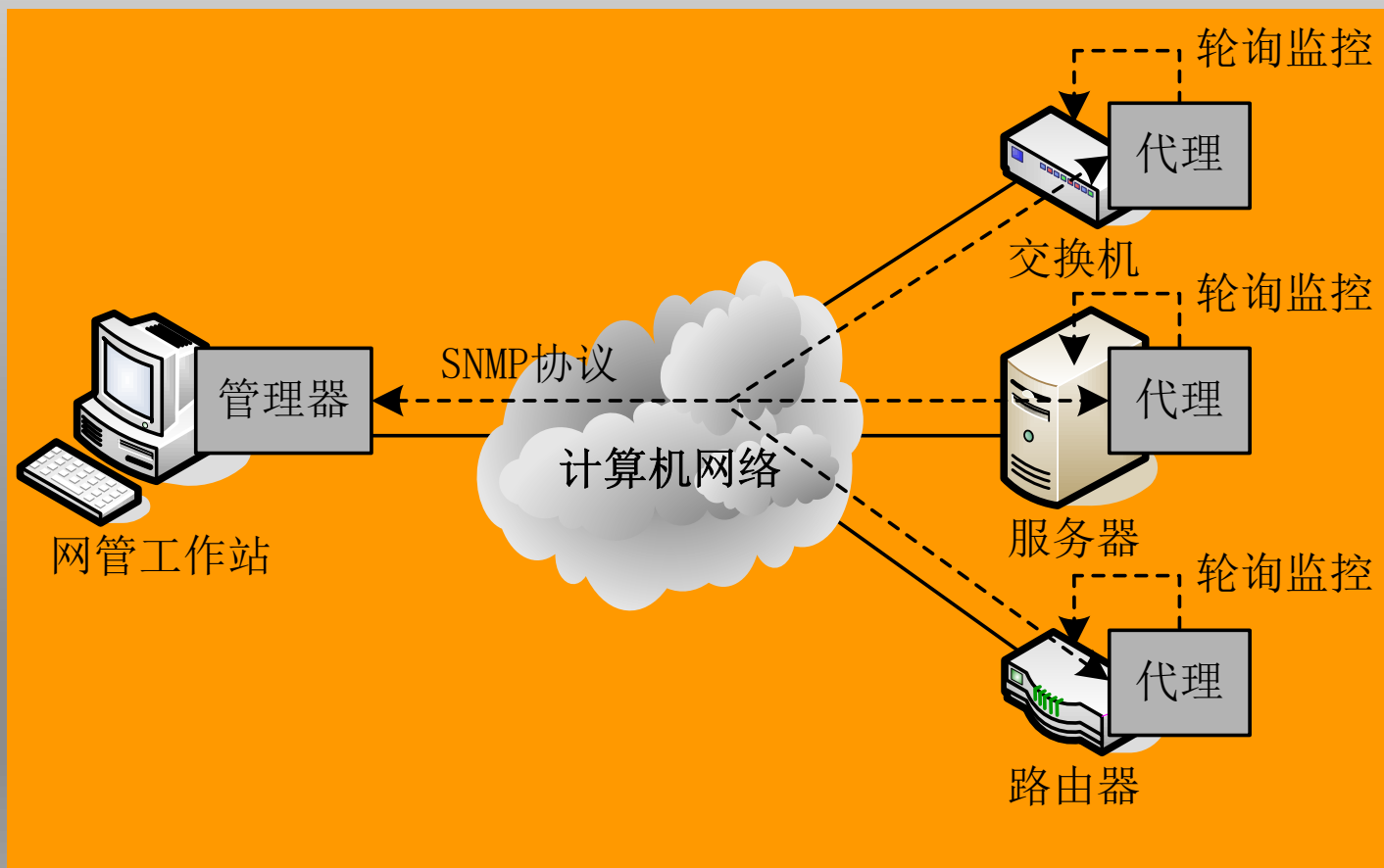


9.8.4 简单网络管理协议

- ◆ SNMP是一种面向Internet的网管协议，针对的管理对象主要是网络设备，例如交换机、路由器等。
- ◆ 1989年，IETF制定SNMPv1，它是一种设计简单、易于实现的协议。
- ◆ 1993年，IETF制定SNMPv2，增加操作类型与支持多种传输层协议。
- ◆ 1998年，IETF制定SNMPv3，提供安全性与改进的框架结构。



SNMP系统的基本结构





有用的网络测试工具

请同学们结合视频讲解和工具自带的帮助学习使用下列工具

◆ 操作系统中自带的工具 (windows/linux)

- 设置和查看网络接口配置信息: ipconfig
(linux: ifconfig)
- 测试网络联通状态工具: ping
- 查看协议包经过的路径工具 (查看路由) : tracert
- 查看网络状态工具: netstat (linux: ss -ant)
- 查看和设置路由表的工具: route
- 查看域名工具: nslookup

◆ 一个开源免费的非常好用的网络测试工具

- tcping (直接下载 tcping.exe 可执行文件, 放到系统目录中即可)



THANKS

