1 因特网

对因特网由两种描述方式：具体构成描述、服务描述

1.1 从具体构成来描述

- 从构成因特网的部件的角度描述因特网
- 主要概念：
    1. **主机==端系统**：与因特网相连的设备。有时候分为客户和服务器
    2. **通信链路和分组交换机**：端系统通过它们连接在一起

        链路的传输速率：bit/s

        分组交换机：从通信链路接受分组，然后转发到另一条通信链路

        分组交换机的分类：**路由器**（位于网络核心）和**链路层交换机**（位于接入网）

        通过网络的**路径**：端与端传输中，一个分组经历的一系列通信链路和分组交换机
    3. **ISP**：网络服务提供商。端系统通过它接入因特网。

        ISP本身的组成：多台分组交换机和多段通信链路组成的网络
    4. **协议**：因特网部件都要运行一系列协议。

        RFC：因特网标准文档，定义了一些协议等。是*Request For Comment*（请求评论）的缩写。

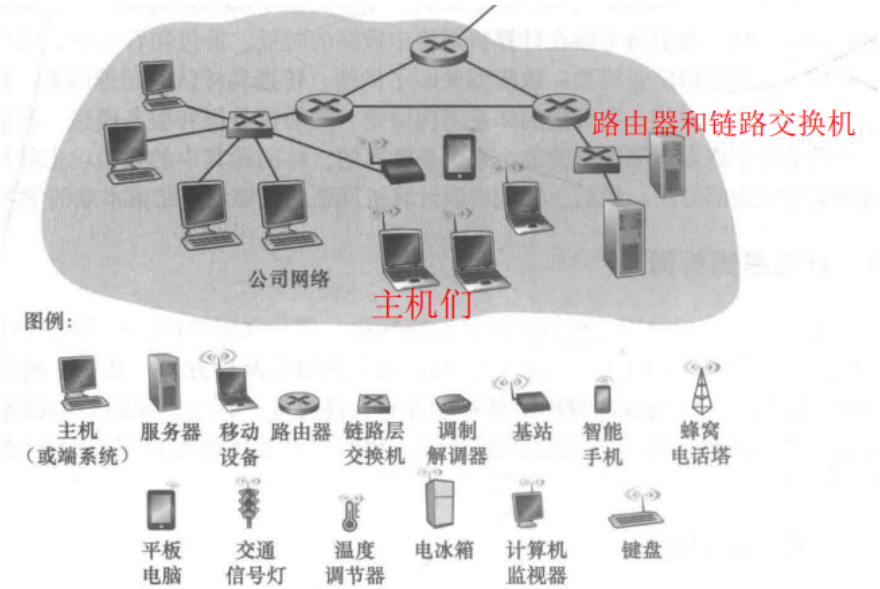


图 1-1　因特网的一些部件

1.2 从服务来描述

- 从因特网作为给应用程序提供服务的基础设施的角度来描述
- 主要概念：

    1.**因特网应用程序**：被称为分布式应用程序，运行在端系统上

    2.应用程序如何相互发消息：**套接字接口**定义了交付数据的方式

1.3 协议是什么

协议（protocol）定义了在两个或多个通信实体之间交换的报文的格式和顺序，以及报文发送和/或接收一条报文或其他事件所采取的动作。

2 网络边缘

2.1 接入网

- 定义：将端系统物理连接到其边缘路由器的网络。

  边缘路由器：端系统到任何其他远程端系统路径上的第一个路由器

（图）

- 主要概念

  1. 家庭接入：使用数字用户线（DSL）和电缆

     数字用户线：从本地电话公司获得DSL。家庭电话线同时承载数据和传统的电话信号

     电缆因特网接入：利用有线电视公司现有的电视基础设施。使用光缆和同轴电缆--混合光纤同轴。

  2.企业（和）家庭接入（略）

  3.广域无线接入（略）

图中粗的线是接入链路：

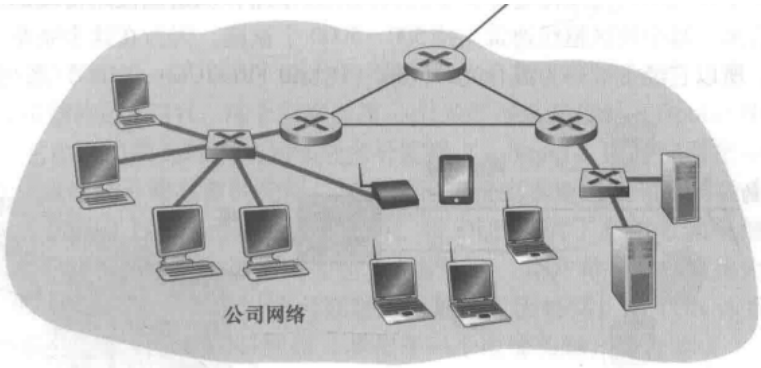


图 1-4　接入网

2.2 物理媒体

- 举例：光缆和同轴电缆（HFC使用的），双绞铜线（DSL和以太网使用的，两根线绞合，来减少临近类似双绞线的电器干扰），同轴电缆（两个同心的铜导体），多模光纤缆.....
- 作用：每个发射源-接收器通过跨越**物理媒体**传播电磁波或光脉冲来发送比特。
- 分类：**导引型媒体**（电波沿着固体前行：如光缆、双绞铜线、同轴电缆）

  非导引型媒体（电波在空气或外层空间中传播）

3 网络核心

通过网络链路和交换机移动数据有两种方法：分组交换，电路交换

图中粗的线是网络核心：

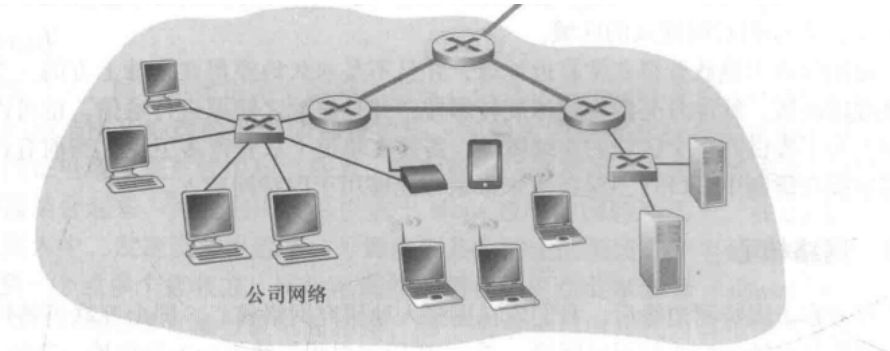


图 1-10　网络核心

3.1 分组交换

- 分组交换机定义：见1.2
- 主要概念：

  端系统彼此交换**报文**，发送源将报文划分为较小的数据块--**分组**

  分组传输速率：分组以链路最大的传输速率通过通信链路。公式：$传输时间 = \frac{L(比特数)}{R(链路传输速率)}$

  储存转发传输：交换机必须接受到整个分组才开始传输

3.2 电路交换

- 特点：在电路交换中，会预留端系统沿路通信需要的所有资源，在发送方和接收方之间建立实在的端到端连接，以确保的恒定速率传数据
- 电路交换中的网络复用：频分和时分复用

  频分复用FDM：每个电台分配特定的频段

  时分复用TDM：时间被划分为帧，帧被划分为固定数量的时隙
- **二者对比**

  分组交换缺点：由于时延不可预测，不适合实时服务（电话、视频）

  优点：比电路交换简单有效

  现在更趋近于使用分组交换

3.3 对网络的网络的理解

- 因特网用户过多，ISP必须互联。所以**网络的网络**是指作为网络的ISP也需要互联形成网络。
- 为了详细说明，对网络结构进行探讨：

  网络结构1：单一的全球传输ISP（作为提供商）互联所有接入ISP（作为客户）

  网络结构2：两层结构，全球传输提供商ISP（此时有多个）位于顶层，接入ISP（数以万计）位于底层

  网络结构3：多层ISP：第一层ISP--区域ISP--接入ISP。

  如今的因特网：在结构3上增加以下结构：

  存在点（PoP）：存在点存在于各个层次

  多宿：除了第一层ISP，任何ISP可以和两个或更多提供商ISP连接

  对等：位于相同等级的邻近一对ISP剋直接将网络俩在一起，不经过上有ISP，通常不进行收费

  因特网交换点IXP：多个ISP在IXP（是一个汇合点）对等

ISP互联即是上述提到的结构。

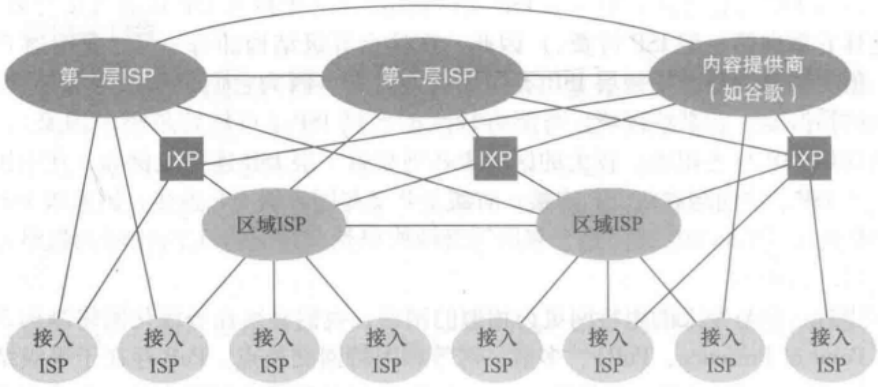


图 1-15　ISP 的互联

总结一下，今天的因特网是一个网络的网络，其结构复杂，由十多个第一层 ISP 和数十万个较低层 ISP 组成。ISP 覆盖的区域多种多样，有些跨越多个大洲和大洋，有些限于狭窄的地理区域。较低层的 ISP 与较高层的 ISP 相连，较高层 ISP 彼此互联。用户和内容提供商是较低层 ISP 的客户，较低层 ISP 是较高层 ISP 的客户。近年来，主要的内容提供商也已经创建自己的网络，直接在可能的地方与较低层 ISP 互联。

4 分组交换网中的时延、丢包和吞吐量

4.1 时延

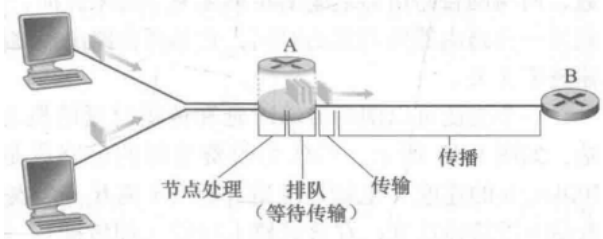


图 1-16　路由器 A 的节点时延

- $d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$
- d_{nodal}：总时延
- d_{proc}：处理时延：如检查分组首部、比特级别差错
- d_{queue}：**排队时延**：在交换机等待被发送
  - 排队时延取决于流量到达队列的速率、链路传输速率、到达流量的性质（突发or均匀）
  - 举例：

    假设分组长度 L 比特
    a 表示分组到达队列的平均速率（单位是分组/秒，即 pkt/s）
    R是传输速率，即从队列中推出比特的速率（以 bps 即 b/s为单位）
    假定所有分组都是由 L 比特组成的，比特到达队列的平均速率是 La bps（分组到达时就看作分组的L比特全都一起到达，所以比特到达速率=分组长度*分组速率）。

比率La/R 被称为**流量强度**（traffic intensity），如果 La/R>1，则比特到达队列的平均速率超过从该队列传输出去的速率。在这种不幸的情况下，该队列趋向于无限增加，并且排队时延将趋向无穷大。所以设计系统时流量强度不能大于1。

现在考虑La/R≤1 时的情况。这时，到达流量的性质影响排队时延。例如，如果分组周期性到达，即每L/R秒到达一个分组，则每个分组将到达一个空队列中，不会有排队时延。另一方面，如果分组以突发形式到达而不是周期性到达，则可能会有很大的平均排队时延。

- d_{trans}：传输时延 $d_{trans}=\frac{L(\text{分组长度，单位}bit)}{R(\text{两个路由器之间的连读传输速率，单位}bps=>bit/s)}$
- d_{prop}：传播时延 $d_{prop}=\frac{d(\text{两路由器之间的距离})}{s(\text{链路的传播速率})}$
- 分组交换和电路交换：
  - 电路交换：总时延=电路的建立时延+报文长度/数据率+链路总长度/传播速率

    电路交换是以电路连接为目的的交换方式。通信之前要在通信两方之间建立一条被两方独占的物理通道。电路交换没有存储转发，并且一直占有线路，**所以没有处理时延和排队时延。**注意："报文长度/数据率"不需要乘以节点数，因为电路交换是直接建立连接，没有中间节点的发送。
  - 分组交换

    1.发送时延=报文长度/数据率+结点数（即链路数减一）*单个分组长度/数据率

    2.传播时延=（分组总数n减一）*单个分组长度/传播速率+链路数k*单个链路长度d/传播速率

    注：考虑第一个分组经过了所有链路（耗时：链路数k*单个链路长度d/传播速率），终于来到了终点。但是前面还有其他n-1个分组，它们还差点到，所以加上"*分组总数n减一）*单个分组长度/传播速率*"。此外可能需要考虑储存转发：中间节点数(k-1)*报文长度/传播速度，这是因为每个分组在每个节点都有储存，就相当于整个报文在每个节点都有储存

    3.排队时延=仅仅需要计算最后一个分组的排队时延即可，前面分组的排队时延不用看

    4.处理时延=

    分组交换是以分组为单位进行传输和交换的，它是一种存储——转发交换方式。即将到达交换机的分组先送到存储器临时存储和处理，等到对应的输出电路有空暇时再送出。

4.2 丢包

当排队队列满了，新到的分组只有被丢弃

4.3 吞吐量

- 瞬时吞吐量（instantaneous throughput）：主机B接收到该文件的速率（以bps 计）。
- 平均吞吐量：如果该文件由F比特组成，主机 B接收到所有F比特用去T秒，则文件传送的平均吞吐量（average throughput）是F/Tbps
- 例子：

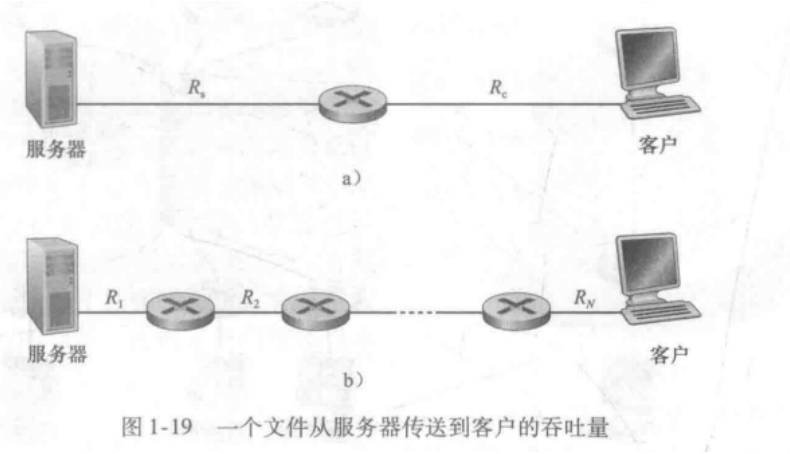


图 1-19　一个文件从服务器传送到客户的吞吐量

  - 图a)：

    令R_s表示服务器与路由器之间的链路速率

    令R_c表示路由器与客户之间的链路速率。

对于这种简单的两链路网络，其吞吐量是 $min\{R_c, R_s\}$，它是瓶颈链路（bottleneck link）的传输速率。

- 图b)：

  令这 N条链路的传输速率分别是 $R_1, R_2, \ldots R_N$

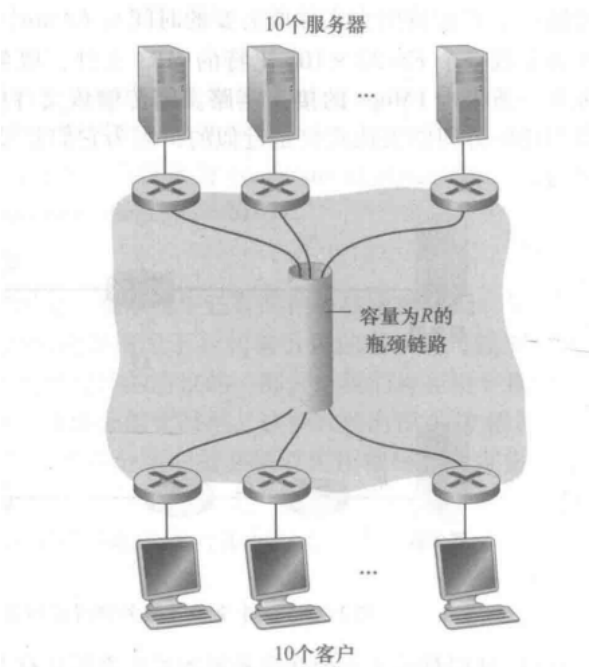
  吞吐量是 $min\{R_1 \ldots R_N\}$，这同样仍是沿着服务器和客户之间路径的瓶颈链路的速率

- 图1-20b:

  其中有10台服务器和10个客户与某计算机网络核心相连。

  假定R_s=2Mbps，R_c=1Mbps，R=5Mbps，并且公共链路为10个下载平等划分它的传输速率。

  这时每个下载的瓶颈不再位于接入网中，而是位于核心中的共享链路了，该瓶颈仅能为每个下载提供500kbps 的吞吐量。因此每个下载的端到端**吞吐量现在减少到 500kbps。**



b）10个客户从10个服务器下载文件

图 1-20　端到端吞吐量

5 协议层层次及其服务模型

5.1 协议分层

- 优点：概念化和结构化。分层提供了一种结构化方式来讨论系统组件。模块化使更新系统组件更为容易。
- 缺点：
  1. 一层可能冗余较低层的功能。例如，许多协议栈在基于每段链路和基于端到端两种情况下，都提供了差错恢复。
  2. 某层的功能可能需要仅在其他某层才出现的信息（如时间戳值），这违反了层次分离的目标。
- 主要概念

  各层的所有协议被称为**协议栈**（protocol stack）

  （1）应用层：分组称为**“报文”**

  - 应用层是网络应用程序及它们的应用层协议存留的地方。

- 包括的协议：

  HTTP（它提供了Web 文档的请求和传送）

  SMTP（它提供了电子邮件报文的传输）

  FTP（它提供两个端系统之间的文件传送）

  DNS（域名系统）

（2）运输层：分组称为**报文段**（segment）。

- 运输层在应用程序端点之间传送应用层报文。
- 两种运输协议，即 TCP 和 UDP

  TCP ：特点：面向连接，可以确保传递，提供流量控制（即发送方/接收方速率匹配），将长报文划分为短报文，提供拥塞控制机制。

  UDP：提供无连接服务，没有可靠性，没有流量控制，也没有拥塞控制。

（3）网络层：分组称为**数据报**（datagram）

- 作用：将数据包从一台主机移动到另一台主机。
- 协议：网际协议 **IP**，该协议定义了在数据报中的各个字段以及端系统和路由器如何作用于这些字段。
- 通常把网络层简单地称为 IP层

（4）链路层：分组称为**帧**（frame）。

- 作用：将分组从一个节点（主机或路由器）移动到路径上的下一个节点
- 协议：某些协议基于链路提供可靠传递，从传输节点跨越一条链路到接收节点。注意：这里的可靠传递和TCP不一样，TCP是确保程序到程序的可靠，

  包括以太网、WiFi和电缆接入网的 DOCSIS 协议

（5）物理层：

- 作用：将该帧中的一个个比特从一个节点移动到下一个节点。
- 协议 : 一个是关于双绞铜线的，另一个是关于同轴电缆的，还有一个是关于光纤的，等等。

（6）OSI中表示层和会话层

- **表示层**的作用是使通信的应用程序能够解释交换数据的含义。这些服务包括**数据压缩和数据加密**（它们是自解释的）以及**数据描述**（这使得应用程序不必担心在各台计算机中表示/存储的内部格式不同的问题）。
- **会话层**提供了**数据交换**的定界和同步功能，包括了建立检查点和恢复方案的方法。

- 注意：

  1.运输层：是程序到程序传输

  2.网络层：是主机到主机

  3.数据链路层：是链路上节点到节点

  4.物理层：是节点到节点间的比特传输

  5.链路层中"可靠"传输不同于TCP的可靠传输，TCP是程序之间的可靠，链路层是链路上相邻节点之间的可靠，可能下一个节点就不是可靠协议了。某条链路上用可靠的链路协议，不代表对话主机间的整条路径是可靠的。

5.2 封装

封装的体现：

- 在发送主机端，一个应用层报文（**图中的M**）被传送给运输层。
- 运输层收取到报文并附上附加信息（**图中的**H_t），应用层报文和运输层首部信息一起构成了运输层报文段。运输层报文段因此**封装**了应用层报文。
- 运输层向网络层传递该报文段，网络层增加了如源和目的端系统地址等网络层首部信息（**图中的**H_n）生成了网络层数据报。该数据报接下来被传递给链路层
- 链路层增加它自己的链路层首部信息并生成链路层帧。
- 在每一层，一个分组具有两种类型的字段：首部字段和有效载荷字段。有效载荷通常是来自上一层的分组。

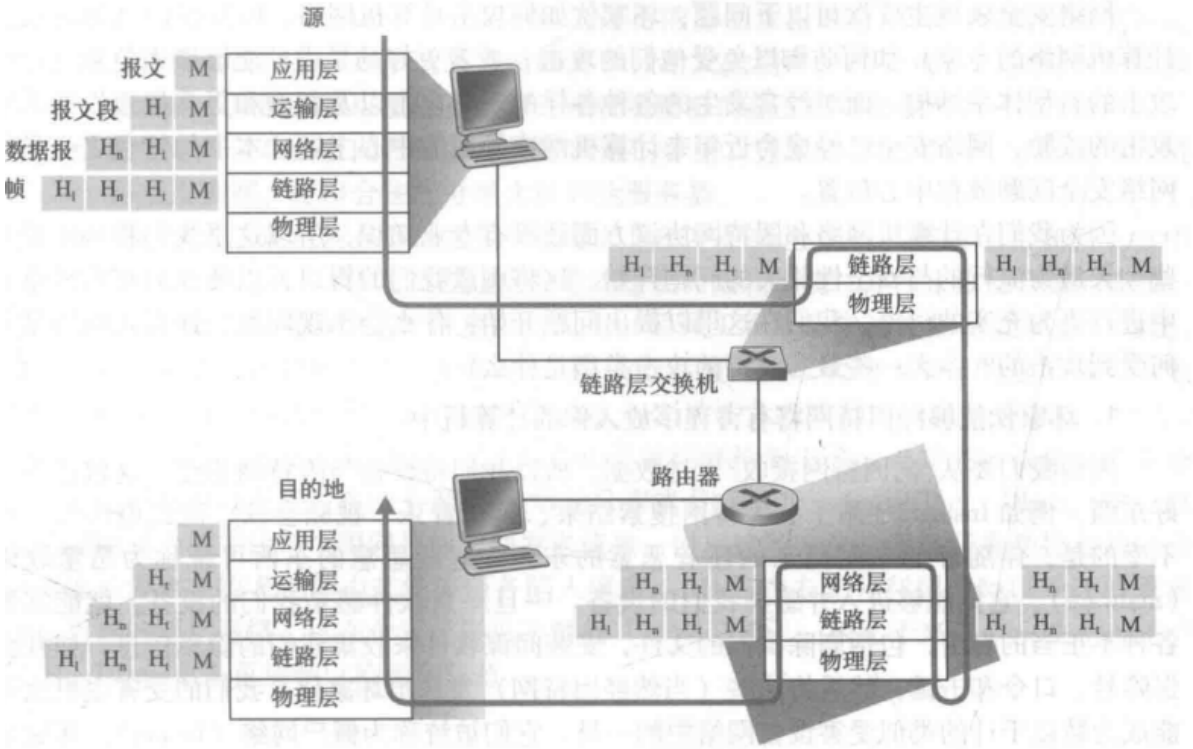


图 1-24　主机、路由器和链路层交换机，每个包含了不同的层，反映了它们的功能差异

6 面对攻击的网络

主要概念：

- 恶意软件统称为僵尸网络

  病毒：需要利用用户交互来感染用户，如利用发邮件将程序发给其他用户，点击即启动。

  蠕虫：无需明显的用户交互，如可以通过被感染的用户扫描他所在的因特网，感染其他用户。

- 拒绝服务攻击：
  - **弱点攻击。**向一台目标主机上运行的易受攻击的应用程序或操作系统发送制作精细的报文。如果适当顺序的多个分组发送给一个易受攻击的应用程序或操作系统，该服务器可能停止运行，或者更糟糕的是主机可能崩溃。
  - **带宽洪泛。**攻击者向目标主机发送大量的分组，分组数量之多使得目标的接入链路变得拥塞，使得合法的分组无法到达服务器。
  - **连接洪泛。**攻击者在目标主机中创建大量的半开或全开 TCP连接，该主机因这些伪造的连接而陷入困境，并停止接受合法的连接。
- 分组嗅探器

记录每个流经的分组副本的被动接收机被称为**分组嗅探器（packet sniffer）**。原理：在无线传输设备的附近放置一台被动的接收机，该接收机就能得到传输的每个分组的副本。