分组是特殊类型的 IP 数据报就可以了。）幸运的是，这种大规模攻击所带来的损害很小，对用户的因特网体验几乎没有或根本没有影响。攻击者的确成功地将大量的分组指向了根服务器，但许多 DNS 根服务器受到了分组过滤器的保护，配置的分组过滤器阻挡了所有指向根服务器的 ICMP ping 报文。这些被保护的服务器因此未受伤害并且与平常一样发挥着作用。此外，大多数本地 DNS 服务器缓存了顶级域名服务器的 IP 地址，使得这些请求过程通常绕过了 DNS 根服务器。

对 DNS 的潜在更为有效的 DDoS 攻击将是向顶级域名服务器（例如向所有处理.com 域的顶级域名服务器）发送大量的 DNS 请求。过滤指向 DNS 服务器的 DNS 请求将更为困难，并且顶级域名服务器不像根服务器那样容易绕过。但是这种攻击的严重性通过本地 DNS 服务器中的缓存技术可将部分地被缓解。

DNS 能够潜在地以其他方式被攻击。在中间人攻击中，攻击者截获来自主机的请求并返回伪造的回答。在 DNS 毒害攻击中，攻击者向一台 DNS 服务器发送伪造的回答，诱使服务器在它的缓存中接收伪造的记录。这些攻击中的任一种，都能够将满怀信任的 Web 用户重定向到攻击者的 Web 站点。然而，这些攻击难以实现，因为它们要求截获分组或扼制住服务器［Skoudis 2006］。

另一种重要的 DNS 攻击本质上并不是一种对 DNS 服务的攻击，而是充分利用 DNS 基础设施来对目标主机发起 DDoS 攻击（例如，你所在大学的邮件服务器）。在这种攻击中，攻击者向许多权威 DNS 服务器发送 DNS 请求，每个请求具有目标主机的假冒源地址。这些 DNS 服务器则直接向目标主机发送它们的回答。如果这些请求能够精心制作成下述方式的话，即响应比请求（字节数）大得多（所谓放大），则攻击者不必自行产生大量的流量就有可能淹没目标主机。这种利用 DNS 的反射攻击至今为止只取得了有限的成功［Mirkovic 2005］。

总而言之，DNS 自身已经显示了对抗攻击的令人惊讶的健壮性。至今为止，还没有一个攻击已经成功地妨碍了 DNS 服务。已经有了成功的反射攻击；然而，通过适当地配置 DNS 服务器，能够处理（和正在处理）这些攻击。

2.6 P2P 应用

在目前为止本章中描述的应用（包括 Web、电子邮件和 DNS）都采用了客户 - 服务器体系结构，极大地依赖于总是打开的基础设施服务器。2.1.1 节讲过，使用 P2P 体系结构，对总是打开的基础设施服务器有最小的（或者没有）依赖。与之相反，成对间歇连接的主机（称为对等方）彼此直接通信。这些对等方并不为服务提供商所拥有，而是受用户控制的桌面计算机和膝上计算机。

在本节中我们将研究两种不同的特别适合于 P2P 设计的应用。第一种应用是文件分发，其中应用程序从单个源向大量的对等方分发一个文件。文件分发是开始研究 P2P 的良好起点，因为它清晰地揭示了 P2P 体系结构的自扩展性。作为文件分发的一个特定的例子，我们将描述流行的 BitTorrent 协议。我们将研究的第二种 P2P 应用是分布在大型对等方社区中的数据库。对于这个应用，我们将探讨**分布式散列表**（Distributed Hash Table，DHT）的概念。