 ISP 所面临的最大的挑战之一是跟踪和阻止denial of service(DoSattacks）. 对付DoS attack 有三个步骤: intrusion detection, source tracking,and blocking. 本命令是针对source tracking。 1、配置举例： 本例说明怎样在路由器上所有line cards/port adapters , 为了让每块line card or port adapter收集到主机 100.10.0.1（被攻击的机器） 的数据流。两分钟后生成 log日志. 记录在log的数据包和流每60秒向GRP/RSP 导出以方便察看. Router# configure interface Router(config)# ip source-track 100.10.0.1 Router(config)# ip source-track syslog-interval 2 Router(config)# ip source-track export-interval 60 显示到达源端口的攻击包的源地址及流量： Router# show ip source-track Address SrcIF Bytes Pkts Bytes/s Pkts/s 10.0.0.1 PO2/0 0 0 0 0 192.168.9.9 PO1/2 131M 511M 1538 6 192.168.9.9 PO2/0 144G 3134M 6619923 143909 显示所有攻击源条目： Router# show ip source-track summary Address Bytes Pkts Bytes/s Pkts/s 10.0.0.1 0 0 0 0 100.10.1.1 131M 511M 1538 6 192.168.9.9 146G 3178M 6711866 145908 2、Cisco IOS feature 配置 TCP Intercept (防止 Denial-of-Service Attacks) 配置路由器以保护服务器免收 TCP SYN-flooding attacks。 以下配置定义了一个扩展access list 101,保护192.168.1.0/24网段的服务器: ip tcp intercept list 101 access-list 101 permit tcp any 192.168.1.0 0.0.0.255 show tcp intercept connections 显示不完全和已建TCP连接 