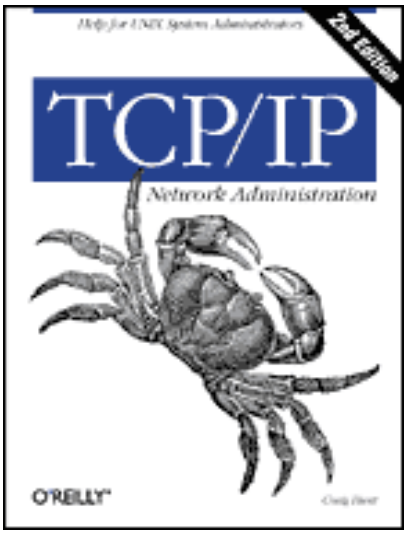
Top 10 công cụ giải quyết sự cố cho TCP/IP

5/12/2005 10:59:00 AM



Có rất nhiều công cụ phân tích mạng phức tạp và chuyên dụng nhưng thực ra chỉ có 10 công cụ chủ yếu để có thể giải quyết mọi sự cố trên mạng TCP/IP. Đó là những công cụ không phải là mạnh nhất nhưng lại được sử dụng thường xuyên nhất, bạn nên chắc chắn rằng trong bộ đồ nghề quản trị mạng của mình luôn sẵn sàng các công cụ này để phục vụ tốt nhất cho việc giải quyết sự cố.

1. Ping.

Ping là một ứng dụng kiểm tra kết nối giữa hai điểm trong mạng để xem chúng có thông suốt và hoạt động tốt ko, việc này được thực hiện bằng cách gửi và nhận một chuỗi các gói tin theo giao thức ICMP. Một trong những bước đầu tiên trong quy trình troubleshooting chính là một thao tác tưởng chừng đơn giản: ping địa chỉ loopback 127.0.0.1 để kiểm tra hoạt động của TCP/IP trong chính các local host.

2. Traceroute.

Traceroute được xây dựng trên nền tảng ứng dụng ping tuy nhiên nó không chỉ kiểm tra hoạt động của các tuyến đường mà còn xác định các chặng cần đi qua trên đường truyền và tính toán được thời gian gói tin được vận chuyển trên từng chặng. Ví dụ khi ta ping một thiết bị đầu xa và nhận thấy độ trễ của gói tin trả lời là rất lớn, muốn biết được gói tin bị trễ ở đâu, cần thực hiện lệnh traceroute.

3. Protocol analyzer/network analyzer.

Một bộ công cụ phân tích các giao thức (đôi khi còn gọi là các network analyzer) là một công cụ thiết yếu để admin theo dõi được hoạt động của mạng. Các công cụ này thực hiện công việc bắt các gói tin trên đường truyền (mặc định thường là bắt tất cả các gói, có thể cấu hình các bộ lọc để chỉ bắt một số gói nhất định).

Các gói tin này sẽ được lưu trong bộ đệm bắt gói, sau đó sẽ được phân tích các thông số trong gói và giải mã thông tin để hiển thị trên màn hình. Một số công cụ như Network Associates' Sniffer Pro còn có khả năng phát hiện ra tiến trình truyền nhận thông tin để phát hiện các động thái tấn công và xâm nhập để báo động với admin.

Một số các công cụ khác cũng khá phổ biến là: AG Group's EtherPeek, công cụ Network Monitor của WindowsNT.

4. Port scanner.

Công cụ quét cổng có thể phát hiện ra các dịch vụ nào đang hoạt động trên thiết bị đầu xa. Tuy nhiên quét cổng thường được xếp vào loại các hành động tấn công hoặc hành động xâm nhập và thường bị các mạng đầu xa chặn.

5. Nslookup/DIG.

Tiện ích nslookup cơ bản gửi các bản tin querry đến DNS server. Bản tin này sẽ nhờ server thực hiện một thao tác phân giải từ tên miền hoặc tên host sang địa chỉ IP tương ứng với nó. Domain Internet Grouper (DIG) là một công cụ tương tự như nslookup nhưng cung cấp nhiều thông tin về DNS hơn.

Ví dụ: một thao tác **nslookup** đơn giản cho www.ipmac.com.vn sẽ trả về những thông tin sau:
> www.ipmac.com.vn

Name: ipmac.com.vn
Address: 64.235.234.141
Aliases: www.ipmac.com.vn

Trong khi đó với cùng thao tác trên DIG trả về các thông tin trên cộng với phần sau:
Name servers: ns1.lunarpage.com
IP address: 69.25.27.170
ns1.lunarpage.com
IP address: 66.150.161.141

6. ARP.

Công cụ này cho phép theo dõi các địa chỉ IP trên mạng và các địa chỉ vật lý tương ứng với nó. Bằng công cụ này, admin có thể hiển thị ra bảng ARP để biết được địa chỉ vật lý của thiết bị thực hiện việc gửi nhận thông tin qua mạng. Việc này đóng vai trò khá quan trọng vì chỉ bằng cách xem địa chỉ vật lý (là địa chỉ duy nhất định danh cho thiết bị mạng) admin mới phát hiện được chính xác một host vì địa chỉ IP chỉ là địa chỉ logic, nó hoàn toàn có thể bị thay đổi.

7. Route.

Là công cụ cho phép hiển thị và thao tác với bảng định tuyến trong thiết bị.

8. Các công cụ SNMP.

Các công cụ quản trị trên nền SNMP cho phép thu thập thông tin trong các bản tin Management Information Base (MIB) được phát đi bởi những thiết bị hỗ trợ SNMP. Có thể theo dõi các thiết bị SNMP bằng một hệ thống thông báo/báo động có khả năng báo cáo cho SNMP ngay lập tức về các action vượt qua giới hạn đã được cấu hình trước trên các thiết bị. Tuy nhiên một trở ngại đối với SNMP là hiện có rất ít các sản phẩm có khả năng chạy trên nhiều nền tảng thiết bị của các hãng khác nhau.

9. Bộ test Cable.

Đây là một công cụ không thể thiếu để kiểm tra sự chính xác trong hoạt động của hệ thống dây dẫn. Công cụ phổ biến là Microtest's OmniScanner được trang bị các chức năng test độ toàn vẹn và độ nhiễu của dây dẫn. Bộ kiểm tra cáp có khả năng làm những việc sau: báo cáo về tổng chiều dài dây dẫn, kết quả kiểm tra các thông số, độ nhiễu xuyên âm, độ suy hao đường truyền, trở kháng và nhiều thông số khác nữa.

Một số công cụ kiểm tra cáp còn cung cấp khả năng theo dõi traffic trên mạng.

10. Các công cụ tổ hợp.

Ngòai các công cụ trên còn một số công cụ giải quyết sự cố khác bao gồm NetScanTools Pro 2000 và AG Group’s NetTools. Các công cụ này thuận tiện ở chố nó là những phần mềm tổ hợp của các tiện ích port scan, ping, traceroute và thực hiện được cả thao tác nslookup, tiết kiệm đáng kể cho admin thời gian troubleshoot cho một mạng. Trong hai công cụ tổng hợp trên NetTools có giá thành rẻ hơn tuy nhiên các tiện ích của nó chỉ là một phần nhỏ so với NetScanTools Pro 2000.

Admin cũng có thể sử dụng các tiện ích cung cấp thông tin và cấu hình cơ bản được tích hợp sẵn trong Windows như WINIPCFG, IPCONFIG và netstat. Một phần mềm tính toán địa chỉ IP đôi khi cũng trở thành một công cụ thuận lợi để tiết kiệm thời gian, có rất nhiều phần mềm loại này,các admin có thể download miễn phí trên mạng.
Việc lựa chọn các công cụ thích hợp sẽ giúp giảm nhẹ và đơn giản hóa công việc giải quyết sự cố cho

các mạng TCP/IP.

IPMAC Networking Academy