TRIỂN KHAI, QUẢN TRỊ VÀ DUY TRÌ CƠ SỞ HẠ TẦNG MẠNG VỚI MICROSOFT WINDOWS SERVER 2003

HANỘI APTECH – 2006

MỤC LỤC

CHƯƠNG 1: TRIỂN KHAI DHCP 2
LỊCH SỬ SƠ LƯỢC CỦA DHCP 3
DHCP LÀ GÌ ?..... 4
DHCP HOẠT ĐỘNG NHƯ THẾ NÀO ? 6
ỦY QUYỀN MÁY CHỦ DHCP 19
CẤU HÌNH MỘT DHCP SCOPE (PHẠM VI DHCP)..... 23
CẤU HÌNH ĐỊA CHỈ DHCP DÀNH SẴN..... 27
CẤU HÌNH CÁC TÙY CHỌN CHO DHCP 29
CẤU HÌNH DHCP RELAY AGENT 31
TỔNG KẾT..... 40
BÀI TẬP 40
CÁC CÂU HỎI TỔNG KẾT..... 43
CÁC KỊCH BẢN TÌNH HUỐNG..... 43

CHƯƠNG 2: QUẢN TRỊ VÀ GIÁM SÁT DHCP 45
QUẢN TRỊ DHCP..... 45
HIỂU BIẾT CÁC CẬP NHẬT DNS ĐỘNG 46
QUẢN TRỊ CƠ SỞ DỮ LIỆU DHCP..... 55
GIÁM SÁT CSDL DHCP 63
SỬ DỤNG VIỆC CẤP ĐỊA CHỈ IP RIÊNG MỘT CÁCH TỰ ĐỘNG (APIPA) 75
TỔNG KẾT..... 79
BÀI TẬP 79
CÁC CÂU HỎI TỔNG KẾT..... 82
CÁC KỊCH BẢN TÌNH HUỐNG..... 84

CHƯƠNG 3: THỰC HIỆN VIỆC PHÂN GIẢI TÊN BẰNG DNS..... 85
TỔNG QUAN VỀ QUÁ TRÌNH PHÂN GIẢI TÊN 86
TỔNG QUAN VỀ DNS..... 86
CÀI ĐẶT DNS 90
CÁC VÙNG DNS..... 91
CÁC ROOT HINT (THÔNG TIN MỨC GỐC)..... 98
CÁC KIỂU MÁY CHỦ DNS..... 101
CÁC BẢN GHI TÀI NGUYÊN DNS 103
HIỂU BIẾT VỀ QUÁ TRÌNH TRUY VẤN DNS 115
ỦY QUYỀN CHO CÁC VÙNG 122
HIỂU BIẾT VỀ SỰ CHUYỂN GIAO VÙNG..... 126

HIỂU BIẾT VỀ SỰ CHUYỂN TIẾP (FORWARDING) 132
KẾT NỐI CÁC MẠNG NỘI BỘ RA INTERNET. 136
TỔNG KẾT 142
BÀI TẬP 144
CÁC CÂU HỎI TỔNG KẾT 148
CÁC KỊCH BẢN TÌNH HUỐNG 149

CHƯƠNG 4: QUẢN TRỊ VÀ GIÁM SÁT DNS 150
SỬ DỤNG CÁC CÔNG CỤ QUẢN TRỊ DNS 150
TÍCH HỢP CÁC VÙNG DNS VỚI WINS 165
QUẢN TRỊ DNS BẰNG CÁC THUỘC TÍNH NÂNG CAO CỦA MÁY CHỦ DNS 166
LÃO HÓA VÀ LOẠI BỎ CÁC BẢN GHI TÀI NGUYÊN (AGING AND SCAVENGING) 174
QUẢN LÝ BỘ ĐỆM PHÂN GIẢI TÊN DNS (DNS RESOLVER CACHE) 176
BẢO MẬT DNS 177
GIÁM SÁT VÀ GIẢI QUYẾT SỰ CỐ DNS 187
TỔNG KẾT 198
BÀI TẬP 199
CÁC CÂU HỎI TỔNG KẾT 201
CÁC KỊCH BẢN TÌNH HUỐNG 203

CHƯƠNG 5: BẢO MẬT TRONG MẠNG 205
THỰC HIỆN CÁC GIAO THỨC BẢO MẬT TRONG MẠNG 206
QUẢN LÝ CÁC QUYỀN CỦA NGƯỜI SỬ DỤNG (USER RIGHT) 206
THỰC HÀNH QUẢN TRỊ BẢO MẬT 213
SỬ DỤNG CÁC MẪU BẢO MẬT (SECURITY TEMPLATE) 219
QUẢN LÝ HỆ THỐNG FILE MÃ HÓA (EFS) 224
SỬ DỤNG CÁC CÔNG CỤ CẤU HÌNH BẢO MẬT 229
TỔNG KẾT 240
BÀI TẬP 240
CÁC CÂU HỎI KIỂM TRA 246
CÁC BÀI TẬP TÌNH HUỐNG 247

CHƯƠNG 6: BẢO MẬT LƯU THÔNG MẠNG VỚI IPSEC 248
MỤC ĐÍCH CỦA IPSEC 249
TÌM HIỂU IPSEC 251
TÌM HIỂU CÁC CHÍNH SÁCH BẢO MẬT IPSEC 268
TRIỂN KHAI CHÍNH SÁCH IPSEC 273

THỰC THI IPSEC SỬ DỤNG GIẤY CHỨNG NHẬN 276
SỬ DỤNG NAT VỚI IPSEC 278
QUẢN TRỊ VÀ THEO DÕI IPSEC 278
TỔNG KẾT 291
BÀI TẬP 292
CÂU HỎI ÔN TẬP 295
KỊCH BẢN TÌNH HUỐNG 298

CHƯƠNG 7: SỬ DỤNG RRAS ĐỂ CẤU HÌNH ĐỊNH TUYẾN 301
TỔNG QUAN VỀ DỊCH VỤ RRAS TRÊN WINDOWS SERVER 2003 303
CÁC LỰA CHỌN TRONG VIỆC CẤU HÌNH CHO CÁC MÁY CHỦ TRUY CẬP TỪ XA 306
LỰA CHỌN GIAO THỨC ĐỊNH TUYẾN 316
QUẢN TRỊ CÁC BẢNG ĐỊNH TUYẾN 319
LỌC GÓI TIN 324
CẤU HÌNH ĐỊNH TUYẾN QUAY SỐ THEO YÊU CẦU 327
ỦY QUYỀN CHO CÁC KẾT NỐI TRUY CẬP TỪ XA 331
ÁP DỤNG CÁC CHÍNH SÁCH TRUY CẬP TỪ XA 334
CẤU HÌNH MỘT CHÍNH SÁCH TRUY CẬP TỪ XA 335
QUẢN TRỊ XÁC THỰC TRUY CẬP MẠNG VÀ CÁC CHÍNH SÁCH 345
TỔNG KẾT 351
BÀI TẬP THỰ C HÀNH 352
CÂU HỎI ÔN TẬP 352
CÁC KỊCH BẢN TÌNH HUỐNG 354

CHƯƠNG 8: DUY TRÌ KIẾN TRÚC HẠ TẦNG MẠNG 355
SỬ DỤNG THẺ NETWORKING TRONG CÔNG CỤ TASK MANAGER 356
SỬ DỤNG MÀN HÌNH QUẢN TRỊ PERFORMANCE 360
GIÁM SÁT LƯU LƯỢNG MẠNG BẰNG CÔNG CỤ NETSTAT .. 368
SỬ DỤNG CÔNG CỤ GIÁM SÁT MẠNG NETWORK MONITOR 370
XỬ LÝ SỰ CỐ KẾT NỐI INTERNET 373
XỬ LÝ SỰ CỐ CÁC DỊCH VỤ TRÊN MÁY CHỦ 386
TỔNG KẾT 394
BÀI TẬP THỰC HÀNH 396
CÂU HỎI ÔN TẬP 398
CÁC KỊCH BẢN TÌNH HUỐNG 401

CHƯƠNG 1: TRIỂN KHAI DHCP

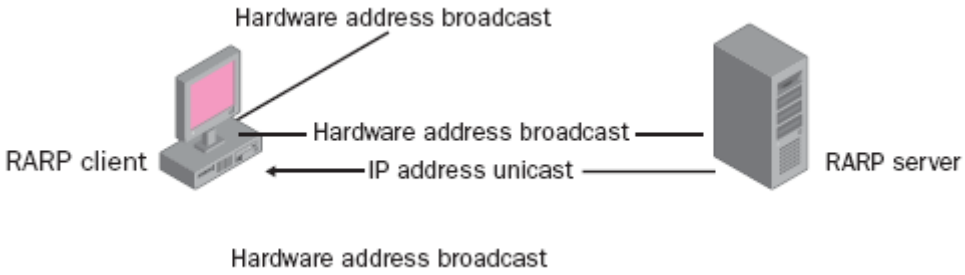
Sau khi hoàn thành chương này, bạn có thể:

- Mô tả mục đích của ***Dynamic Host Configuration Protocol*** (*Giao thức Cấu hình Động cho Máy trạm* - DHCP) và cách thức dịch vụ này tổ chức quản lý mạng thuận tiện hơn như thế nào.
- Giải thích quá trình dịch vụ DHCP cho thuê địa chỉ IP
- Ủy quyền cho một máy chủ DHCP và giải thích làm thế nào để ngăn không cho phép một máy chủ DHCP không được ủy quyền cấp địa chỉ IP không đúng cho các máy trạm DHCP
- Giải thích mục đích của ***multicasting*** (*Quảng bá có địa chỉ*)
- Cấu hình máy chủ DHCP bằng cách định nghĩa một ***scope*** (*phạm vi*) và một ***superscope*** (*siêu phạm vi*), tạo ra các địa chỉ dành sẵn cho máy khách DHCP và cấu hình các tùy chọn DHCP
- Giải thích mục đích và cấu hình của một ***DHCP relay agent*** (*phần tử chuyển tiếp DHCP*)

Các máy tính sử dụng **Giao thức Kiểm soát Truyền thông/Giao thức Internet (TCP/IP)** phải được cấu hình phù hợp để giao tiếp với các máy tính TCP/IP khác trong một hệ thống mạng. Mỗi máy tính phải có một địa chỉ IP và một ***subnet mask*** **(***mặt nạ mạng con***)** và nếu như các máy tính này truyền thông ra ngoài mạng con nội bộ, mỗi máy còn phải được cấu một ***default gateway*** **(***cổng ra mặc định***).** Mỗi địa chỉ IP phải hợp lệ và duy nhất trong toàn hệ thống mạng tương tác của máy tính đó. Yêu cầu này sẽ đem đến cho người quản trị mạng những thách thức lớn. Để đảm bảo rằng mỗi máy tính có một địa chỉ duy nhất, quá trình cấp phát, thay thế và cấp phát lại địa chỉ phải được giám sát một cách cẩn thận. Nếu điều này được thực hiện một cách thủ công, các bản ghi chép chính xác và kịp thời phải được giữ lại trong mỗi máy tính ghi lại nơi mà máy tính đó được đặt và địa chỉ IP nào, mặt nạ mạng con nào đã cấp phát cho máy đó. Nhiệm vụ này có thể trở nên rất đơn điệu và nhàm chán. Sẽ rất khó khăn khi quản lý các địa chỉ IP một cách thủ công đối với các doanh nghiệp có số lượng lớn các máy trạm yêu cầu địa chỉ IP. DHCP sẽ làm cho nhiệm vụ này trở nên đơn giản hơn bằng cách tự động cấp phát, theo dõi và tái cấp phát địa chỉ IP cho các máy trạm

LỊCH SỬ SƠ LƯỢC CỦA DHCP

Từ khi phát minh ra TCP/IP, một số giải pháp đã được nghiên cứu và phát triển để giải quyết vấn đề khó khăn của việc cấu hình các thiết lập TCP/IP cho một doanh nghiệp có một lượng lớn các máy trạm. Giao thức **Phân giải Địa chỉ Ngược (*Reverse Address Resolution Protocol* - RARP)** được thiết kế cho các máy trạm không có đĩa cứng nghĩa là không có phương tiện lưu trữ thường trực các thiết lập TCP/IP của chúng. RARP, theo như tên gợi ý, về cơ bản là ngược lại với **Giao thức Phân giải Địa chỉ (*Address Resolution Protocol* - ARP)**. Các máy trạm ARP sẽ quảng bá một địa chỉ IP để phát hiện ra địa chỉ **MAC (Media Access Control – Điều khiển truy cập thiết bị)** tương ứng (địa chỉ duy nhất của mỗi thành phần phần cứng). Các máy khách RARP sẽ quảng bá địa chỉ MAC (Thể hiện trên Hình 1-1). (***Quảng bá*** là một phương pháp truyền thông để gửi thông tin tới tất cả mọi phần tử trên một mạng máy tính một cách đồng thời). Một máy chủ RARP sau đó sẽ trả lời bằng cách truyền gửi địa chỉ IP cấp cho máy khách đó.



Hình 1-1. Máy trạm sử dụng RARP để nhận địa chỉ IP từ Máy chủ RARP khi phản hồi lại thông điệp quảng bá có chứa địa chỉ phần cứng của máy khách.

Bởi vì RARP không thể cung cấp các thiết lập bắt buộc phải có khác cho các máy khách, ví dụ như mặt nạ mạng con và cổng ra mặc định, nó sử dụng một giải pháp khác, đó là **Giao thức Bootstrap (BOOTP)**

BOOTP, hiện vẫn còn được sử dụng, cho phép một máy trạm TCP/IP nhận được các thiết lập cho các tất cả các tham số cấu hình mà nó cần để chạy, bao gồm địa chỉ IP, mặt nạ mạng con, cổng ra mặc định và địa chỉ **máy chủ DNS (Máy chủ Phân giải Tên miền).** Sử dụng Giao thức Truyền File Tối thiểu (***Trivial File Transfer Protocol*** – TFTP), máy trạm có thể tải về file thực thi mà có khả năng khởi động từ máy chủ BOOTP. Nhược điểm chính của BOOTP là người quản trị vẫn phải chỉ ra các thiết lập cho mỗi máy trạm trên máy chủ BOOTP. Một phương pháp tốt hơn để quản trị TCP/IP là tự động gán địa chỉ IP duy nhất trong khi ngăn không cho việc cấp phát trùng lặp xảy ra đồng thời cung cấp các thiết lập quan trọng khác như cổng ra mặc

định, mặt nạ mạng con, máy chủ DNS, máy chủ WINS, và các thông tin khác. Lý tưởng nhất là điều này được thực hiện mà không phải liệt kê mọi thiết bị trong mạng một cách thủ công. Đó chính là DHCP

DHCP dựa chủ yếu vào BOOTP, nhưng thay vì việc đẩy các tham số cấu hình sẵn đến đúng các máy khách, DHCP có thể tự động xác định địa chỉ IP từ một dải địa chỉ và sau đó đòi lại khi nó không còn cần thiết nữa. Bởi vì quá trình này là động nên không có việc trùng lặp khi cấp địa chỉ bằng máy chủ DHCP có cấu hình đúng và người quản trị có thể di chuyển các máy trạm giữa các mạng con với nhau mà không cần phải cấu hình lại. Hơn nữa, một số lượng lớn các tham số cấu hình chuẩn và tham số riêng biệt cho các phần cứng đặc biệt có thể được chỉ định và phân phối động đến các máy khách.

DHCP LÀ GÌ ?

DHCP là một giao thức mở, theo chuẩn công nghiệp sử dụng để làm giảm sự phức tạp của việc quản trị các mạng dựa trên nền TCP/IP. Nó được định nghĩa bởi các ***Requests for Comments*** (*Các Yêu cầu Giải thích* - RFCs) 2131 và 2132 của Tổ chức Ứng dụng Khoa học vào Internet (***Internet Engineering Task Force*** - IETF).

> ***THÔNG TIN THÊM. RFCs 2131 và 2132****. RFCs 2131 và 2132 DHCP là một chuẩn IETF dựa trên giao thức BOOTP và được định nghĩa trong RFC 2131 và 2132, các tài liệu này có thể được tìm thấy tại địa chỉ http://www.rfc-editor.org/rfcsearch.html*

Việc đánh địa chỉ IP là rất phức tạp bởi vì mỗi máy (máy tính, máy in hoặc các thiết bị khác có giao tiếp mạng) kết nối đến một mạng TCP/IP phải được cấp ít nhất một địa chỉ IP duy nhất và mặt nạ mạng con để có thể truyền thông trên mạng. Hơn nữa, hầu hết các máy đều yêu cầu các thông tin thêm như là địa chỉ IP hoặc cổng ra mặc định và máy chủ DNS. DHCP giải phóng người quản trị khỏi nhiệm vụ cấu hình trên mỗi máy trong mạng một cách thủ công. Hệ thống mạng càng lớn thì lợi ích của DHCP càng nhiều. Nếu không cấp phát địa chỉ động, mỗi máy phải cấu hình một cách thủ công và địa chỉ IP phải được quản lý cẩn thận để tránh việc trùng lặp hoặc cấu hình sai.

Quản lý địa chỉ IP và các tùy chọn cho máy sẽ dễ dàng hơn rất nhiều khi thông tin cấu hình có thể quản lý từ một địa điểm đơn hơn là kết hợp thông tin từ nhiều địa điểm. DHCP có thể cấu hình tự động một máy khi nó khởi động trên một mạng TCP/IP cũng như có thể thay đổi các thiết lập trong khi các máy đang kết nối đến mạng. Tất cả các việc này được thực hiện bằng cách sử dụng các thiết lập và thông tin từ một CSDL DHCP trung tâm. Bởi

vì các thiết lập và thông tin này được lưu một cách tập trung, bạn có thể nhanh chóng và dễ dàng thêm vào hoặc thay đổi các thiết lập máy trạm (ví dụ như địa chỉ IP của một máy chủ DNS thay thế) cho tất cả các máy trạm trong hệ thống mạng của bạn từ một địa điểm đơn. Nếu không có CSDL tập trung của các thông tin cấu hình này, rất khó khăn để duy trì hiện trạng của các thiết lập trên máy hoặc thay đổi chúng.

Tất cả các sản phẩm Microsoft Windows Server 2003 (Các phiên bản Standard Edition, Enterprise Edition, Web Edition, and Datacenter Edition) đều bao gồm dịch vụ DHCP Server, đó là một tùy chọn cài đặt. Mọi máy khách Microsoft Windows đều tự động cài đặt dịch vụ DHCP Client như là một thành phần của TCP/IP, bao gồm Windows Server 2003, Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows NT 4, Microsoft Windows Millennium Edition (Windows Me) và Microsoft Windows 98.

Nói ngắn gọn, DHCP cung cấp bốn lợi điểm quan trọng cho việc quản trị và duy trì một mạng TCP/IP:

- **Tập trung quản trị thông tin về cầu hình IP.** Thông tin cấu hình IP của DHCP có thể lưu trong một vị trí và cho phép người quản trị có thể tập trung quản lý tất cả các thông tin cấu hình IP. Một máy chủ DHCP sẽ theo dõi tất cả các địa chỉ IP đã cấp và địa chỉ IP dành riêng và liệt kê chúng trong bảng điều khiển DHCP. Bạn có thể sử dụng bảng điều khiển DHCP để xác định các địa chỉ IP của tất cả các thiết bị đã kích hoạt DHCP trong hệ thống mạng. Nếu không có DHCP, bạn không chỉ phải gán các địa chỉ một cách thủ công mà bạn còn phải nghĩ ra phương pháp để theo dõi và cập nhật chúng.

- **Cấu hình động các máy.** DHCP tự động thực hiện quá trình cấu hình động các tham số cấu hình quan trọng trong các máy. Điều này giảm thiểu nhu cầu cấu hình thủ công các máy riêng biệt khi TCP/IP lần đầu tiên được triển khai hoặc khi yêu cầu thay đổi cơ sở hạ tầng IP.

- **Cấu hình IP cho các máy một cách liền mạch.** Cách sử dụng DHCP đảm bảo rằng các máy trạm DHCP có thể nhận được các tham số cấu hình IP một cách chính xác và kịp thời, ví dụ như địa chỉ IP, mặt nạ mạng con, cổng ra mặc định, địa chỉ IP của máy chủ DNS và các tham số khác, mà không cần tác động của người dùng. Bởi vì cấu hình là tự động, việc giải quyết sự cố của việc cấu hình

sai, ví dụ như việc nhập các số không đúng kiểu, được giảm đáng kể.

- **Sự linh hoạt.** Sử dụng DHCP cho phép người quản trị mạng tăng sự linh hoạt, cho phép người quản trị mạng có thể thay đổi cấu hình IP một cách dễ dàng khi cơ sở hạ tầng thay đổi.

- **Khả năng mở rộng.** DHCP phù hợp từ mạng nhỏ đến mạng lớn. DHCP có thể phục vụ các mạng với chỉ 10 máy khách cũng như các mạng lớn với hàng ngàn máy khách. Đối với các mạng nhỏ, đơn độc, ta có thể sử dụng ***Automatic Private IP Addressing*** (APIPA). (APIPA sẽ được bàn đến trong phần sau của chương này)

DHCP HOẠT ĐỘNG NHƯ THẾ NÀO ?

Chức năng cốt lõi của DHCP là cấp phát địa chỉ. Như đã đề cập trước đây, điểm quan trọng then chốt của quá trình này là nó được thực hiện động. Điều có ý nghĩa đối với quản trị mạng là hệ thống mạng có thể được cấu hình để phân phát địa chỉ IP cho bất kỳ thiết bị nào kết nối tại bất kỳ đâu trong mạng. Việc phân phát các địa chỉ này được thực hiện bằng cách gửi các thông điệp lớp ứng dụng đến máy chủ DHCP và nhận các thông điệp lớp ứng dụng từ máy chủ DHCP. Mọi thông điệp DHCP được chứa trong các gói tin **User Datagram Protocol (Giao thức Gói tin Người sử dụng - UDP)** sử dụng các cổng đã dành trước là 67 (tại máy chủ) và 68 (tại máy khách)

> ***THÔNG TIN THÊM. Lớp ứng dụng***. *Lớp ứng dụng là một phần của mô hình tham chiếu* ***Open Systems Interconnection*** *(Kết nối các Hệ thống Mở - OSI) được định nghĩa bởi* ***International Organization for Standardization*** *(Tổ chức Quốc tế về chuẩn hóa - ISO) và* ***Telecommunication Standards Section of the International Telecommunications Union*** *(Hội Tiêu chuẩn Viễn thông của Hiệp hội Viễn thông Quốc tế ITU-T). Mô hình này được sử dụng để tham chiều và để giảng dạy. Nó chia chức năng mạng máy tính thành bảy lớp. Từ đỉnh xuống đến đáy, bảy lớp này là* ***application, presentation, session, transport, network, data-link,*** *và* ***physical*** *(Ứng dụng, Trình diễn, Phiên, Giao vận, Mạng, Liên kết dữ liệu và Vật lý). Để có thêm thông tin về mô hình tham chiếu OSI, hãy xem thêm sách* ***Network+ Certification Training Kit, Second Edition (Microsoft Press, 2001).***

Trước khi học về cách thức phân phát địa chỉ, bạn nên hiểu một số thuật ngữ: Máy khách DHCP, máy chủ DHCP và hợp đồng thuê địa chỉ. Các thuật ngữ này được định nghĩa trong các phần sau đây.

Máy chủ và máy khách DHCP

Một máy tính lấy các thông tin cấu hình của nó từ DHCP được gọi là một ***máy khách DHCP***. Máy khách DHCP giao tiếp với máy chủ DHCP để lấy địa chỉ IP và các thông tin cấu hình TCP/IP liên quan. Địa chỉ IP và các thông tin cấu hình mà máy chủ DHCP cung cấp cho các máy trạm được định nghĩa bởi người quản trị DHCP

Các hợp đồng thuê trong DHCP

Một hợp đồng thuê DHCP sẽ định nghĩa khoảng thời gian mà một máy chủ DHCP gán một địa chỉ IP cho một máy khách DHCP. Khoảng thời gian thuê có thể là bất kỳ khoảng thời gian nào từ 1 phút cho đến 999 ngày, hoặc nó có thể là không giới hạn. Khoảng thời gian thuê mặc định là 8 ngày.

Các kiểu thông điệp DHCP

Các thông điệp lớp ứng dụng trong quá trình giao tiếp giữa máy chủ DHCP/máy khách DHCP phải là một trong tám kiểu sau đây:

- **DHCPDISCOVER**. Gửi đi bởi máy khách thông qua cách gửi quảng bá để tìm máy chủ DHCP. Theo RFC 2131, thông điệp DHCPDISCOVER có thể bao gồm các lựa chọn gợi ý các giá trị cho địa chỉ mạng và khoảng thời gian thuê
- **DHCPOFFER**. Gửi đi bởi một hoặc nhiều máy chủ DHCP tới một máy khách DHCP để phản hồi lại thông điệp DHCPDISCOVER, đi kèm với các tham số cấu hình đề xuất.
- **DHCPREQUEST**. Được gửi đi bởi máy khách DHCP để báo hiệu rằng nó đã chấp nhận địa chỉ và các tham số mà máy chủ đề xuất cho nó. Máy khách tạo thông điệp DHCPREQUEST có chứa địa chỉ của máy chủ mà từ đó nó đã chấp nhận đồng thời gắn kèm với địa chỉ IP đã đề xuất. Bởi vì máy trạm chưa được tự cấu hình với các tham số đề xuất nên nó phát thông điệp DHCPREQUEST theo cách quảng bá. Thông điệp quảng bá này sẽ nhắc máy chủ rằng máy khách đã chấp nhận địa chỉ đề xuất và đồng thời nhắc tất cả các máy chủ khác trên mạng rằng máy khách sẽ từ chối các đề xuất khác.
- **DHCPDECLINE**. Được gửi đi bởi máy khách đến máy chủ DHCP, thông báo với máy chủ này rằng địa chỉ IP mà nó đề xuất là không được chấp nhận. Máy khách DHCP sẽ gửi một thông điệp

DHCPDECLINE nếu nó xác định được rằng địa chỉ đề xuất đó đã được sử dụng. Sau khi gửi đi DHCPDECLINE, máy khách bắt đầu lại quá trình đi hỏi thuê hoặc làm mới lần nữa.

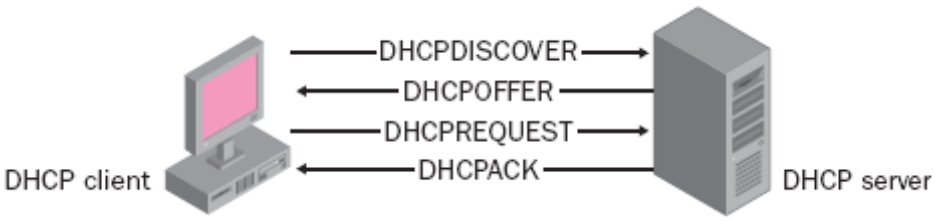
- **DHCPACK**. Gửi đi bởi máy chủ DHCP đến máy khách DHCP để xác nhận địa chỉ IP nó đã đề xuất cấp cho máy khách và được máy khách chấp nhận và để cung cấp cho máy khách các tham số cấu hình mà máy khách yêu cầu khi máy chủ đã được cấu hình để cung cấp các tham số đó.
- **DHCPNACK**. Gửi đi bởi máy chủ DHCP đến máy khách DHCP để từ chối thông điệp DHCPREQUEST của máy khách. Điều này có thể xảy ra nếu địa chỉ yêu cầu là không đúng bởi vì máy khách đã di chuyển sang một mạng con mới hoặc bởi vì thời hạn thuê của máy khách DHCP đã hết hạn và không thể làm mới được. Sau khi nhận được thông điệp DHCPNACK, máy khách bắt đầu lại quá trình đi hỏi thuê hoặc làm mới lần nữa
- **DHCPRELEASE**. Gửi đi bởi máy khách DHCP đến máy chủ DHCP để giải phóng một địa chỉ IP và hủy bỏ thời hạn thuê còn lại. Kiểu thông điệp này được gửi đến máy chủ cung cấp IP đang thuê.
- **DHCPINFORM**. Được gửi đi từ máy khách DHCP đến máy chủ DHCP để chỉ hỏi về các tham số cấu hình nội bộ bổ sung; máy khách đã được cấu hình địa chỉ IP rồi. Kiểu thông điệp này đồng thời sử dụng để phát hiện các máy chủ DHCP không được ủy quyền.

Cách thức máy khách có được một hợp đồng thuê ban đầu

Một máy khách thực hiện quá trình khởi tạo hợp đồng thuê trong các tình huống sau đây:

- Lần đầu tiên máy khách khởi động
- Sau khi nó giải phóng địa chỉ IP của mình
- Sau khi nó nhận được một thông điệp DHCPNACK, trả lời cho việc máy khách DHCP đó đang cố gắng làm mới lại một địa chỉ IP đã thuê từ trước.

Nếu thành công, quá trình khởi tạo hợp đồng thuê này là một chuỗi các trao đổi giữa máy khách DHCP và máy chủ DHCP bằng cách sử dụng bốn thông điệp sau: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST và DHCPACK. Quá trình trao đổi các thông điệp này được minh họa trong Hình 1-2:



Hình 1-2. Các thông điệp trao đổi với một máy chủ DHCP để có được một hợp đồng thuê

Định vị máy chủ.

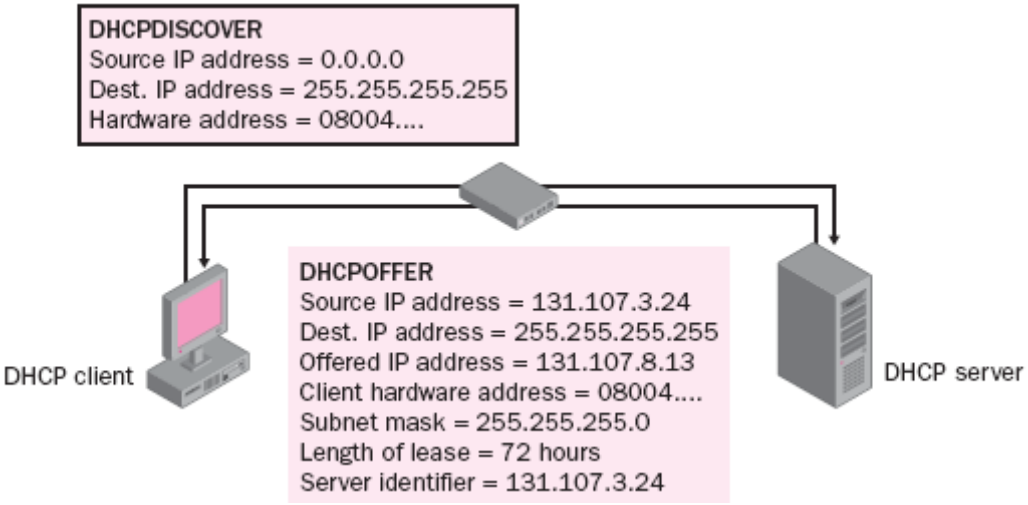
Máy khách quảng bá thông điệp DHCPDISCOVER để tìm kiếm máy chủ DHCP. Bởi vì máy khách chưa có một địa chỉ IP hoặc chưa biết địa chỉ IP của máy chủ DHCP nên thông điệp DHCPDISCOVER được gửi đi quảng bá trong toàn mạng nội bộ, với địa chỉ nguồn là 0.0.0.0 và địa chỉ đích là 255.255.255.255. Thông điệp DHCPDISCOVER là một lời yêu cầu về vị trí của máy chủ DHCP và thông tin địa chỉ IP. Yêu cầu này có chứa địa chỉ MAC của máy khách và tên máy tính để máy chủ DHCP biết rằng máy khách nào đã gửi yêu cầu.

Nhận địa chỉ đề xuất

Tất cả các máy chủ DHCP nhận được thông điệp DHCPDISCOVER, đồng thời đã được cấu hình đúng cho máy trạm, sẽ quảng bá thông điệp DHCPOFFER với các thông tin sau đây:

- Địa chỉ IP nguồn (Của máy chủ DHCP)
- Địa chỉ IP đích (Của máy khách DHCP)
- Địa chỉ IP đề xuất
- Địa chỉ phần cứng của máy khách
- Mặt nạ mạng con
- Thời hạn của hợp đồng thuê
- Thông tin nhận dạng máy chủ (địa chỉ IP của máy chủ DHCP đang đề xuất)

Như mô tả trên Hình 1-3, các thông điệp DHCPDISCOVER và DHCPOFFER đều là kiểu quảng bá.



Hình 1-3. Các thông điệp DHCPDISCOVER và DHCPOFFER đều là kiểu quảng bá.

Sau khi quảng bá thông điệp DHCPDISCOVER của mình, máy khách DHCP sẽ đợi lời đề xuất trong thời gian 1 giây. Nếu không nhận được một lời đề nghị nào, máy khách không có khả năng khởi tạo tiếp và nó sẽ phải gửi quảng bá lại yêu cầu ba lần (sau các khoảng thời gian 9, 13 và 16 giây cộng với một khoảng xê dịch giữa 1 miligiây và 1 giây). Nếu không nhận được một lời đề xuất nào sau bốn lần gửi, máy khách tiếp tục gửi lại với khoảng thời gian lặp lại là 5 phút. Nếu DHCP không thành công, các máy khách Windows XP, Windows Server 2003, Windows 98, Windows Me và Windows 2000 có thể sử dụng APIPA để lấy động được một địa chỉ IP và mặt nạ mạng con. Windows XP và Windows Server 2003 có thể sử dụng cấu hình thay thế, cấu hình này sẽ cấp động các thiết lập đã được định nghĩa trước nếu không tìm thấy một máy chủ DHCP nào. APIPA và cấu hình thay thế được mô tả trong phần "Cấu hình máy khách tự động" trong phần sau của chương.

Phản hồi lại địa chỉ đề xuất

Sau khi máy khách nhận được lời đề xuất từ ít nhất một máy chủ DHCP, nó quảng bá thông điệp DHCPREQUEST tới mọi máy chủ DHCP. Thông điệp quảng bá DHCPREQUEST này chứa các thông tin sau:

- Địa chỉ IP của máy chủ DHCP mà máy khách đã lựa chọn
- Địa chỉ IP đã yêu cầu của máy khách
- Một danh sách các tham số yêu cầu (mặt nạ mạng con, bộ định tuyến, danh sách các máy chủ DNS, tên miền, thông tin đặc thù về

nhà sản xuất, danh sách các máy chủ WINS, kiểu nút NetBIOS và phạm vi NetBIOS)

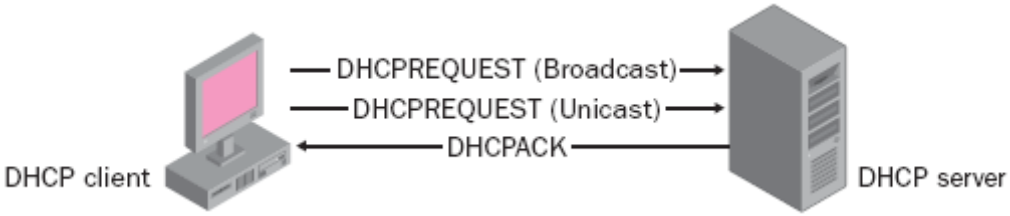
Khi các máy chủ DHCP mà có lời đề xuất không được chấp nhận, nhận được thông điệp DHCPREQUEST này, nó sẽ rút lại các đề xuất của mình.

Nhận lời xác nhận

Máy chủ DHCP mà có các đề xuất được chấp nhận sẽ gửi một xác nhận thành công đến máy khách dưới dạng một thông điệp DHCPACK. Thông điệp này có chứa một hợp đồng thuê hợp lệ của một địa chỉ IP, bao gồm cả các thời điểm làm mới (T1 và T2, sẽ được bàn đến trong phần sau, "DHCP làm mới một hợp đồng như thế nào") và khoảng thời gian của hợp đồng (tính bằng giây)

DHCP làm mới một hợp đồng như thế nào

Bởi vì các IP thuê có một thời gian tồn tại hữu hạn nên máy khách phải thường xuyên đều đặn làm mới hợp đồng thuê sau khi có được nó. Như Hình 1-4 thể hiện, máy khách Windows DHCP cố làm mới hợp đồng hoặc sau mỗi lần khởi đồng hoặc theo một khoảng thời gian đều đặn sau khi máy khách DHCP đã khởi tạo.



Hình 1-4. Các thông điệp trao đổi trong quá trình làm mới một hợp đồng

Như Hình 1-4 thể hiện, việc làm mới hợp đồng sẽ sử dụng chỉ hai thông điệp DHCPREQUEST (hoặc kiểu quảng bá hoặc kiểu đơn nhất) và DHCPACK. Nếu một máy khách DHCP làm mới hợp đồng khi nó khởi động lại, các thông điệp này được gửi đi thông qua các gói tin IP quảng bá. Nếu quá trình làm mới hợp đồng được thực hiện trong khi máy khách DHCP đang chạy, máy khách DHCP và máy chủ DHCP sẽ giao tiếp với nhau bằng các thông điệp đơn nhất. (Ngược lại với các thông điệp quảng bá, các thông điệp đơn nhất là các thông điệp điểm-tới-điểm giữa hai máy trong mạng)

Khi một máy khách có được hợp đồng thuê, DHCP cung cấp các giá trị cho các tùy chọn cấu hình mà máy khách DHCP yêu cầu và đã được cấu hình trên máy chủ DHCP. Bằng cách giảm thời hạn hợp đồng, người quản trị DHCP có thể bắt buộc các máy khách phải thường xuyên làm mới lại hợp

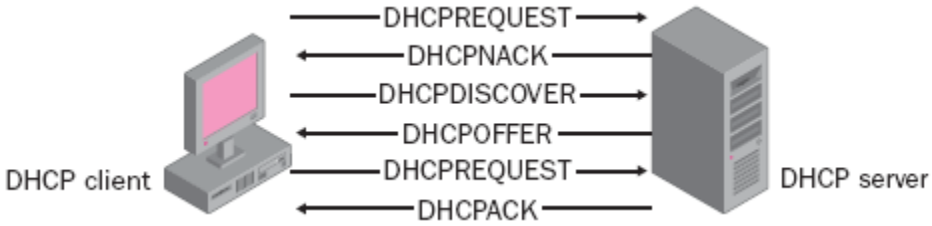
đồng thuê và lấy các thông tin chi tiết về cấu hinh cập nhật. Điều này có thể có lợi khi người quản trị muốn thay đổi phạm vi cấu hình hoặc muốn nhiều địa chỉ hơn cho các máy khách DHCP bằng cách thu hồi lại chúng nhanh hơn. Một ***phạm vi DHCP*** là một dải địa chỉ IP sẵn sàng để cho thuê hoặc gán cho các máy khách bằng dịch vụ DHCP. Một phạm vi có thể bao gồm một hoặc nhiều tùy chọn. ***Tùy chọn (Option)*** là các hạng mục cấu hình nhất định, ví dụ như mặt nạ mạng con hay địa chỉ IP cổng ra mặc định mà người quản trị DHCP muốn máy chủ DHCP cấp cho các máy khách DHCP

> ***LƯU Ý. Khi nào tăng hoặc giảm thời gian thuê DHCP****. Nếu các cấu hình mạng TCP/IP của bạn không thay đổi thường xuyên hoặc nếu bạn có nhiều địa chỉ IP hơn lượng địa chỉ cần thiết trong dải địa chỉ IP bạn đã gán, bạn có thể tăng thời gian thuê DHCP đáng kể dựa trên giá trị mặc định là tám ngày. Tuy nhiên, nếu cấu hình mạng của bạn thay đổi thường xuyên hoặc bạn có một lượng giới hạn các địa chỉ IP và phần lớn đều được sử dụng, bạn nên để chu kì dự trữ là ngắn, có thể là một ngày. Lý do là nếu dải địa chỉ IP sẵn sàng được sử dụng hết, các máy thêm vào hoặc di chuyển có thể không thể lấy được địa chỉ IP từ máy chủ DHCP và do đó không thể tham gia vào việc truyền thông trên mạng.*

Lần đầu tiên máy khách DHCP cố gắng làm mới lại hợp đồng thuê là khi đạt được một nửa thời gian thuê, được gọi là T1. Máy khách DHCP lấy giá trị T1 từ thông điệp DHCPACK khi xác nhận hợp đồng thuê. Nếu việc làm mới lại lại hợp đồng thuê không thành công tại thời điểm T1, máy khách DHCP tiếp tục cố gắng làm mới hợp đồng tại thời điểm 87.5% thời gian thuê, thời điểm này được gọi là T2. Giống như T1, T2 được xác định trong thông điệp DHCPACK. Nếu hợp đồng không được làm mới lại trước khi nó hết hạn (nếu ví dụ như không thể kết nối đến máy chủ DHCP được trong một khoảng thời gian nào đó), ngay khi hợp đồng bị hết hạn, máy khách lập tức giải phóng địa chỉ IP và cố gắng tìm kiếm một hợp đồng mới.

Thay đổi mạng con và các máy chủ DHCP

Nếu các máy khách DHCP yêu cầu một hợp đồng thuê bằng cách sử dụng thông điệp DHCPREQUEST mà máy chủ DHCP không thể đáp ứng được (ví dụ khi máy tính xách tay di chuyển sang một mạng con khác), máy chủ DHCP gửi một thông điệp DHCPNACK tới máy khách. Thông điệp này sẽ thông báo cho máy khách rằng địa chỉ IP yêu cầu thuê không được làm mới. Máy khách sau đó sẽ bắt đầu quá trình tìm kiếm tiếp bằng cách quảng bá một thông điệp DHCPDISCOVER. Hình 1-5 minh họa thứ tự của các thông điệp DHCP xảy ra khi một máy khách khởi động trong một mạng con mới.



Hình 1-5: Các thông điệp DHCP trao đổi khi một máy khách khởi động trong một mạng con mới

Khi một máy khách DHCP khởi động trong một mạng con mới, nó quảng bá một thông điệp để làm mới hợp đồng thuê của nó. Yêu cầu làm mới hợp đồng DHCP được quảng bá trong mạng con do đó tất cả mọi máy chủ DHCP mà cung cấp địa chỉ DHCP sẽ nhận được yêu cầu này. Máy chủ DHCP trả lời yêu cầu này lại nằm trong một mạng con mới, khác với máy chủ mà đã cung cấp hợp đồng thuê ban đầu. Khi máy chủ DHCP nhận được thông điệp quảng bá, nó sẽ so sánh địa chỉ mà máy khách DHCP yêu cầu với dải địa chỉ được cấu hình trên nó và trong mạng con. Nếu nó không thể đáp ứng yêu cầu của máy khách, máy chủ DHCP sẽ tạo ra một thông điệp DHCPNACK và máy khách bắt đầu lại quá trình tìm kiếm hợp đồng thuê địa chỉ IP.

Nếu máy khách không thể định vị bất kỳ một máy chủ DHCP nào khi khởi động lại, nó sẽ gửi đi một thông điệp quảng bá ARP đến cổng ra mặc định mà nó có được từ trước, nếu có. Nếu địa chỉ IP của cổng ra được phân giải thành công, máy khách DHCP giả định rằng nó vẫn nằm trong cùng một mạng mà từ đó nó có được bản hợp đồng thuê và tiếp tục sử dụng bản hợp đồng của nó. Trong trường hợp khác, nếu địa chỉ IP của cổng ra không được phân giải, máy khách giả định rằng nó đã được di chuyển đến một mạng khác mà không có máy chủ DHCP nào sẵn sàng (ví dụ như mạng tại nhà), và nó tự cấu hình bằng cách sử dụng APIPA hoặc một cấu hình thay thế. Khi nó tự cấu hình, máy khách DHCP cố gắng định vị một máy chủ DHCP sau mỗi 5 giây để cố gắng làm mới hợp đồng của nó.

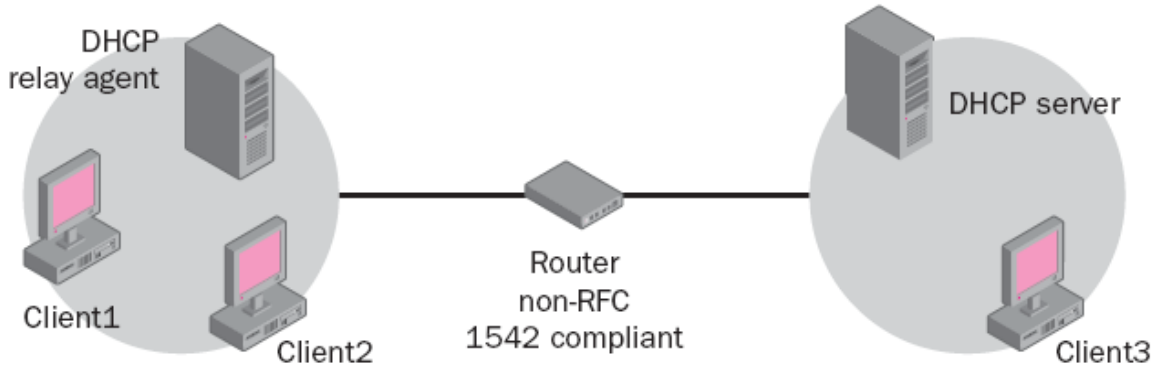
Sử dụng DHCP Relay Agent (Phần tử chuyển tiếp DHCP)

DHCP phụ thuộc rất lớn vào các thông điệp quảng bá. Các thông điệp quảng bá này thường được giới hạn trong mạng con mà nó sinh ra và không được chuyển tiếp đến các mạng con khác. Điều này sẽ dẫn đến một trục trặc nếu như máy khách nằm trong một mạng con khác mạng con của máy chủ DHCP. Một ***DHCP relay agent*** (phần tử chuyển tiếp DHCP) có thể là một máy hoặc một thiết bị định tuyến (***router***) mà lắng nghe các thông điệp DHCP (và BOOTP) từ máy khách đang quảng bá trong mạng con và chuyển

tiếp các thông điệp đó tới một máy chủ DHCP. Máy chủ DHCP sẽ gửi các thông điệp phản hồi lại cho ***relay agent*** và phần tử này này sẽ lại quảng bá chúng vào trong mạng con của các máy khách. Sử dụng ***DHCP relay agent*** sẽ giảm thiểu nhu cầu phải có một máy chủ DHCP trong mỗi mạng con.

Để hỗ trợ và sử dụng dịch vụ DHCP hoạt động trên nhiều mạng con, các thiết bị định tuyến kết nối các mạng con với nhau sẽ phải có tính năng hỗ trợ ***DHCP/BOOTP relay agent*** như mô tả trong RFC 1542. Để tuân theo chuẩn RFC 1542 này và cung cấp khả năng hỗ trợ ***relay agent***, mỗi thiết bị định tuyến phải có khả năng nhận biết các thông điệp của giao thức DHCP và BOOTP và chuyển tiếp chúng một cách thích hợp. Bởi vì các thiết bị định tuyến điển hình sẽ hiểu các thông điệp DHCP như là thông điệp BOOTP nên một thiết bị định tuyến chỉ cần có khả năng ***BOOTP relay agent*** sẽ chuyển tiếp được các gói tin DHCP và bất kỳ gói tin BOOTP nào gửi đi trong mạng.

DHCP relay agent được cấu hình với địa chỉ IP của máy chủ DHCP. ***DHCP relay agent*** sẽ lắng nghe các thông điệp DHCPDISCOVER, DHCPREQUEST và DHCPINFORM mà được quảng bá từ các máy khách. ***DHCP relay agent*** sau đó sẽ đợi trong một khoảng thời gian đã được cấu hình trước và nếu không phát hiện ra được phản hồi nào, nó sẽ gửi đi một thông điệp đơn nhất (***unicast***) đến máy chủ DHCP đã cấu hình sẵn. Máy chủ này sẽ tiếp nhận thông điệp và phản hồi trở lại cho ***DHCP relay agent***. Phần tử này sau đó sẽ quảng bá thông điệp này vào trong mạng con nội bộ, cho phép các máy khách DHCP nhận chúng. Các quá trình trên được mô tả trong Hình 1-6.



Hình 1-6. Các thông điệp DHCP được chuyển tiếp bởi DHCP relay agent

Quá trình trao đổi thông tin trong hình 1-6 được tiến hành theo các bước sau:

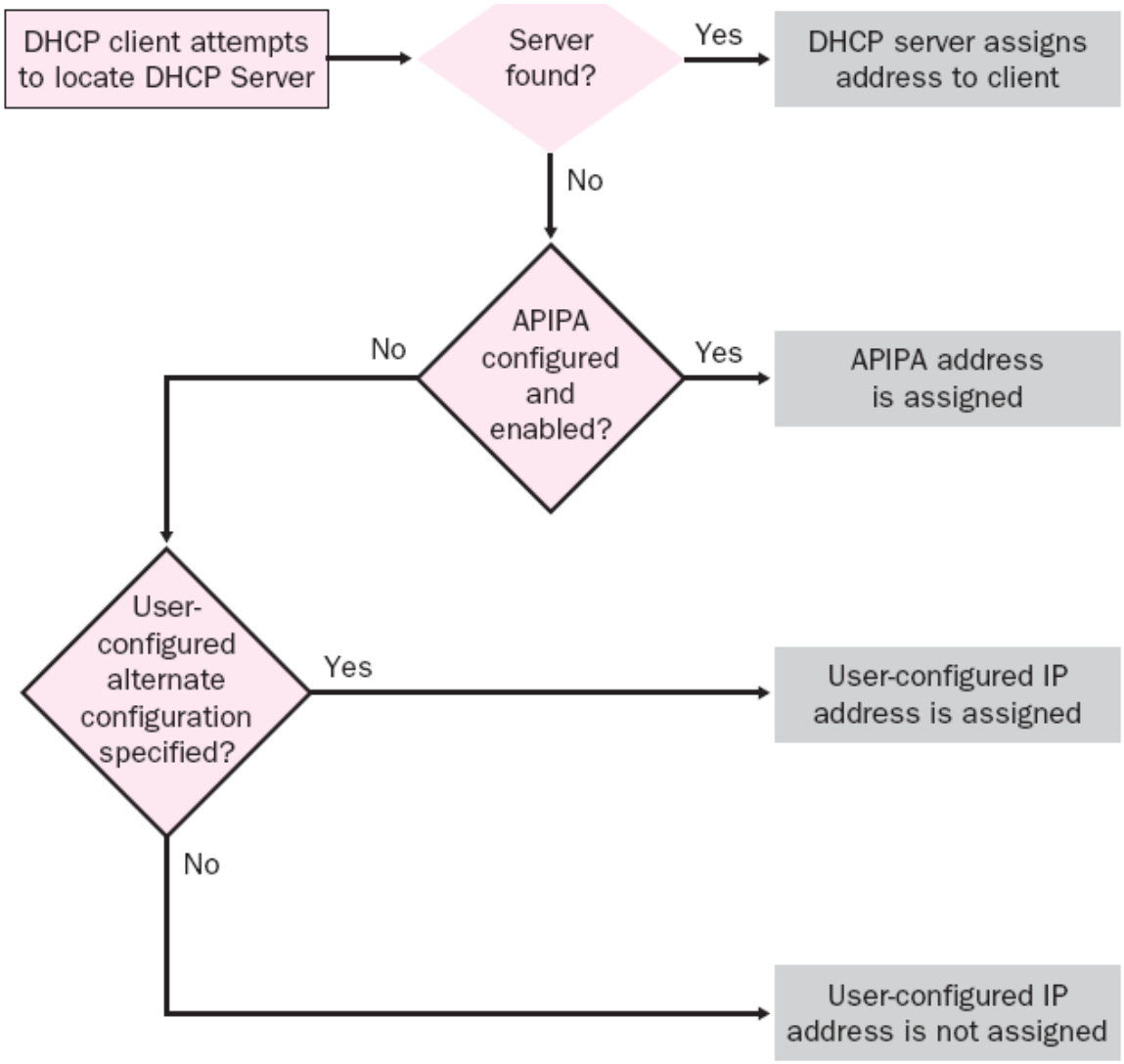
1. ***Client1*** quảng bá gói tin DHCPDISCOVER
2. ***Relay agent*** chuyển tiếp gói tin DHCPDISCOVER đến máy chủ DHCP

3. Máy chủ gửi gói tin DHCPOFFER đến ***DHCP relay agent***
4. ***Relay agent*** quảng bá gói tin DHCPOFFER
5. ***Client1*** quảng bá gói tin DHCPREQUEST
6. ***Relay agent*** chuyến tiếp gói tin DHCPREQUEST đến máy chủ DHCP
7. Máy chủ quảng bá gói tin DHCPACK và ***DHCP relay agent*** sẽ đón lấy gói tin đó
8. ***Relay agent*** quảng bá gói tin DHCPACK

Cấu hình máy khách tự động

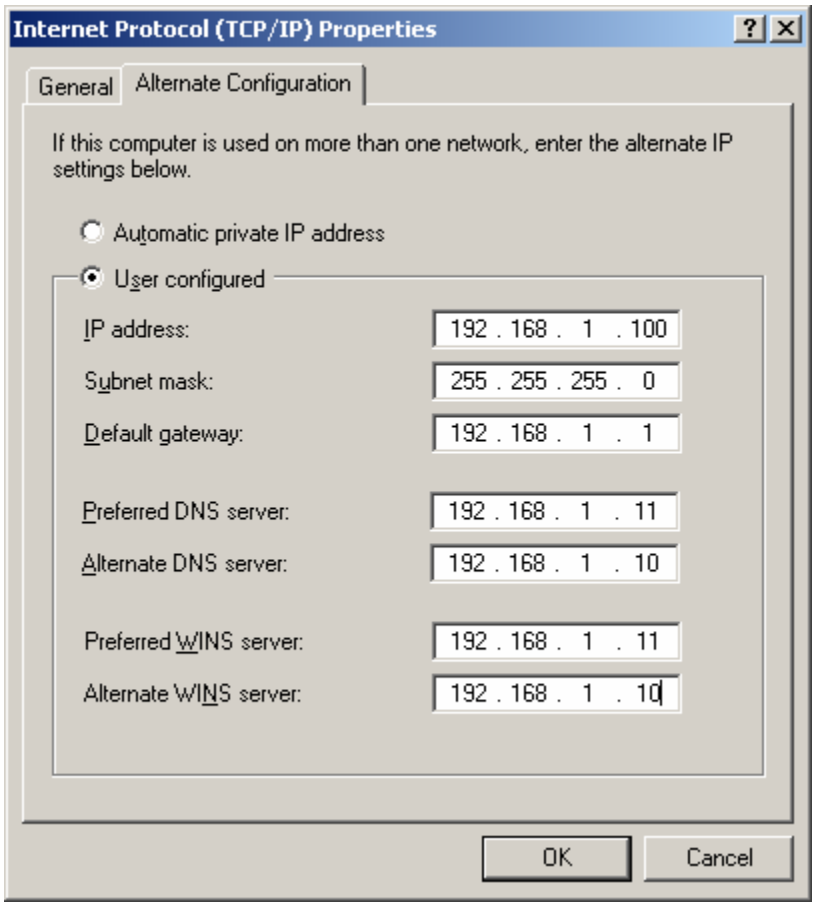
Trong hầu hết các trường hợp, các máy khách DHCP đều tìm thấy một máy chủ trong mạng con nội bộ hoặc thông qua ***relay agent***. Để cho phép hệ thống chạy bình thường khi máy chủ DHCP không hoạt động, Windows Server 2003, Windows XP, Windows 2000 và Windows 98 cung cấp tính năng APIPA. APIPA là một thành phần trong khi triển khai Windows TCP/IP cho phép một máy tính xác định được thông tin cấu hình IP khi không có một máy chủ DHCP nào hoặc chưa có cấu hình thủ công nào trước đó.

APIPA giúp một máy tính IP không bị sự cố vì không thể truyền thông khi máy chủ DHCP không hoạt động vì một lý do nào đó. Hình 1-7 thể hiện các chu trình gán địa chỉ IP khác nhau khi một máy khách DHCP tìm kiếm một máy chủ DHCP. Trong trường hợp không tìm thấy máy chủ DHCP và APIPA đã được cấu hình và kích hoạt, một địa chỉ APIPA sẽ được gán cho máy tính. APIPA có lợi trong các mạng làm việc nhỏ khi mà không triển khai máy chủ DHCP. Bởi vì việc cấu hình tự động không hỗ trợ cổng ra mặc định cho nên nó chỉ làm việc trên một mạng con và không thích hợp cho các mạng lớn.



Hình 1-7: Việc gán địa chỉ IP sử dụng APIPA hay Cấu hình Thay thế

Nếu máy khách DHCP không thể tìm thấy máy chủ DHCP và lại không được cấu hình thay thế (thể hiện trong Hình 1-8), máy tính đó sẽ tự cấu hình với một địa chỉ IP ngẫu nhiên lựa chọn từ giải dịa chỉ mạng lớp B 169.254.0.0 và với mặt nạ mạng con 255.255.0.0 đã được ***Internet Assigned Numbers Authority*** (*Tổ chức được chỉ định số cho Internet* - IANA) dự phòng trước. Máy tính được cấu hình tự động sẽ kiểm tra để xác nhận rằng địa chỉ IP mà nó chọn là chưa được sử dụng bằng cách dùng một quảng bá ARP. Nếu địa chỉ IP đã được sử dụng, máy tính sẽ lựa chọn địa chỉ ngẫu nhiên khác. Máy tính sẽ cố gắng thực hiện 10 lần để tìm ra địa chỉ IP mà nó có thể sử dụng.



Hình 1-8. Trang thuộc tính cấu hình thay thế

Khi một địa chỉ lựa chọn được xác nhận là có thể sử dụng, máy khách sẽ được cấu hình với địa chỉ đó. Máy khách DHCP sẽ tiếp tục âm thầm tìm kiếm một máy chủ DHCP cứ 5 phút một lần, và nếu tìm thấy máy chủ DHCP, cấu hình mà máy chủ DHCP đề xuất sẽ được sử dụng

Các máy khách Windows XP và Windows Server 2003 có thể được cấu hình để sử dụng một cấu hình thay thế, máy khách DHCP sẽ sử dụng cấu hình này nếu không thể liên lạc được với một máy chủ DHCP nào. Cấu hình thay thế bao gồm một địa chỉ IP, một mặt nạ mạng con, một cổng ra mặc định, các địa chỉ của máy chủ DNS và WINS.

Một mục đích của cấu hình thay thế chính là giải pháp cho các máy tính xách tay vì chúng luôn di chuyển giữa một mạng tích hợp có máy chủ DHCP và mạng gia đình trong đó địa chỉ IP tĩnh được sử dụng. Ví dụ, Janice có một máy tính xách tay mà cô ta sử dụng ở cả văn phòng làm việc và ở nhà. Tại văn phòng làm việc, máy tính của cô lấy địa chỉ IP từ máy chủ DHCP, nhưng cô ấy không có một máy chủ DHCP nào ở nhà cả. Janice có thể sử dụng cấu hình thay thế để giữ lại thông tin về địa chỉ IP, mặt nạ mạng

con, cổng ra mặc định và máy chủ DNS để khi cô ta kết nối máy xách tay của cô ấy ở mạng gia đình, nó sẽ được cấu hình một cách tự động.

Nếu bạn sử dụng DHCP với cấu hình thay thế và máy khách DHCP không thể tìm thấy máy chủ DHCP, cấu hình thay thế này sẽ được sử dụng để cấu hình giao tiếp mạng. Không cần phải thực hiện việc tìm kiếm thêm nào khác trừ trong các trường hợp sau:

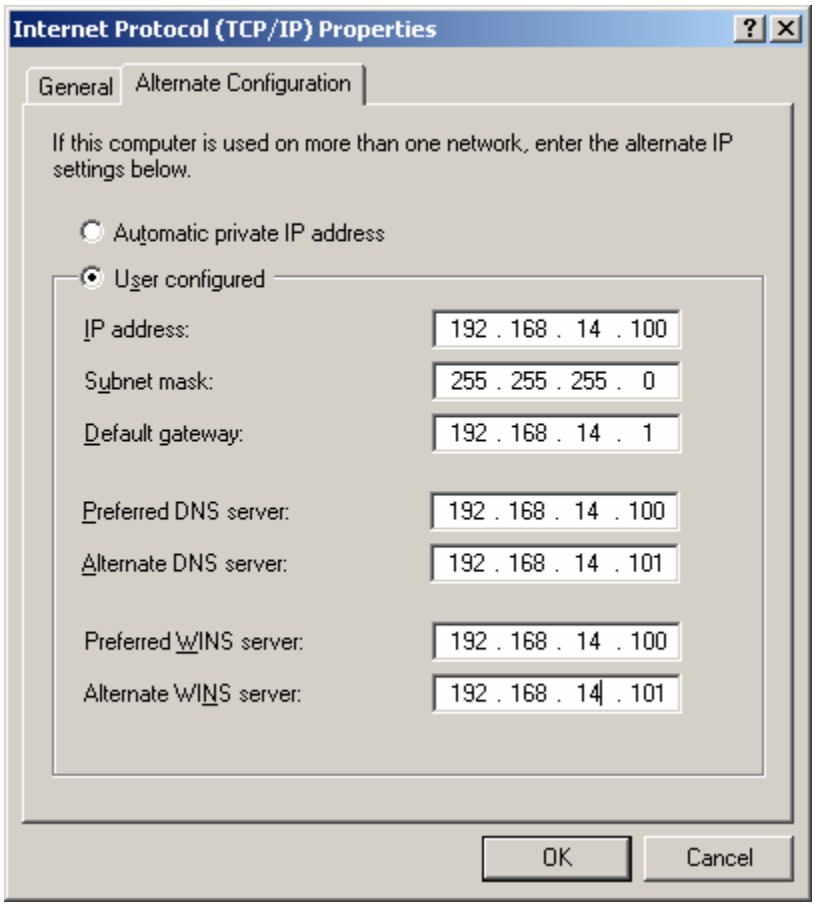
- Giao tiếp mạng bị vô hiệu hóa và sau đó được kích hoạt lại
- Thiết bị kết nối (ví dụ cáp mạng) bị ngắt ra và sau đó kết nối lại
- Các thiết lập TPC/IP cho giao tiếp mạng thay đổi và máy chủ DHCP vẫn còn hoạt động sau các thay đổi này.

Nếu máy chủ DHCP được tìm thấy, giao tiếp mạng sẽ được gán địa chỉ IP DHCP hợp lệ

- **Hiển thị thẻ Alternate Configuration (Cấu hình thay thế)**

Để hiển thị thẻ "***Alternate Configuration***" như thể hiện trong Hình 1-9, giao tiếp mạng phải được cấu hình để lấy địa chỉ IP một cách tự động. Để xem thẻ "***Alternate Configuration***", thực hiện theo các bước sau:

1. Mở Control Panel, và nhấn đúp vào phần Network Connections
2. Trong cửa sổ Network Connections, nhấn phải chuột vào Local Area Connection và chọn Properties
3. Trong trang Local Area Connection Properties, trỏ vào Internet Protocol (TCP/IP) và sau đó nhấn vào Properties
4. Trong thẻ "***Alternate Configuration***", nhập vào địa chỉ IP của bạn.



Hình 1-9. Thẻ Alternate Configuration của trang thuộc tính Internet Protocol (TCP/IP)

ỦY QUYỀN MÁY CHỦ DHCP

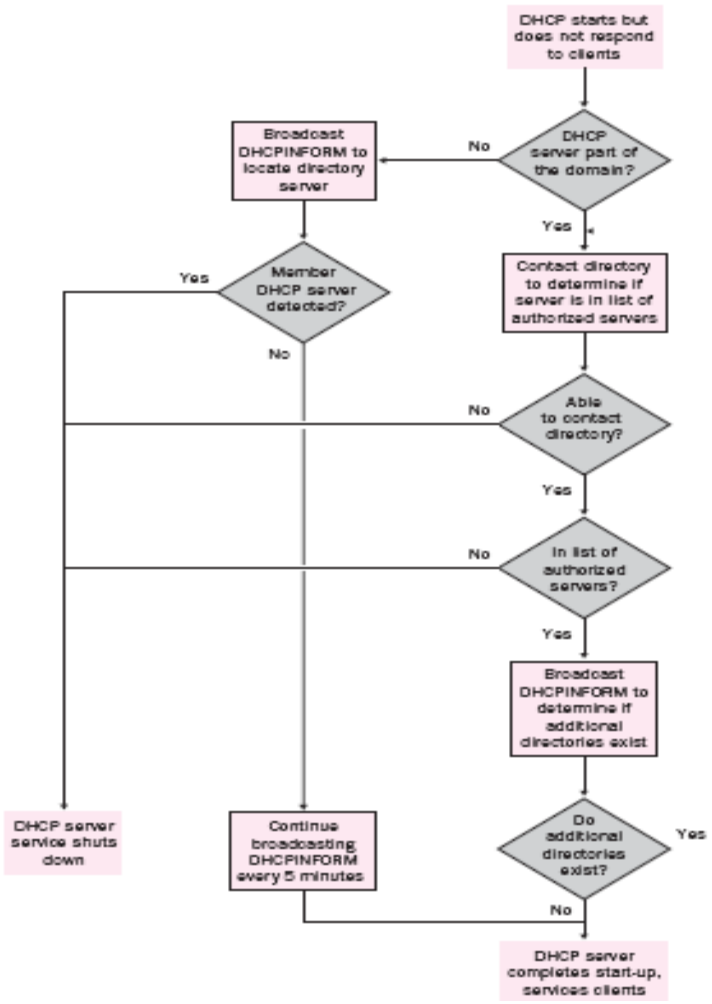
Khi triển khai DHCP trong các hệ điều hành trước Windows 2000, bất kỳ người dùng nào cũng có thể tạo ra một máy chủ DHCP trong mạng, một hành vi có thể gây ra sự xung đột trong việc cấp địa chỉ IP. Ví dụ nếu một máy khách có được hợp đồng thuê địa chỉ từ một máy chủ DHCP được cấu hình không chuẩn, máy khách có thể nhận được một địa chỉ IP không hợp lệ và sẽ không thể giao tiếp với các máy khác trên mạng. Điều này thậm chí còn có thể ngăn cản người dùng không đăng nhập được. Trong Windows Server 2000 và Windows Server 2003, một máy chủ DHCP ***chưa được ủy quyền*** (còn được gọi là một máy chủ DHCP giả mạo) đơn thuần là một máy chủ DHCP mà không được liệt kê trong dịch vụ thư mục sử dụng Active Directory như một máy chủ được ủy quyền. Bạn phải ủy quyền một máy chủ DHCP trong Active Directory trước khi máy chủ này có thể gán các địa chỉ cho các máy khách DHCP.

Quá trình ủy quyền một máy chủ DHCP

Tại thời điểm khởi tạo, máy chủ DHCP liên hệ với Active Directory để xác định liệu nó có nằm trong danh sách các máy chủ hiện thời đang được ủy quyền để thực hiện nhiệm vụ trong mạng. Một trong các hành động sau đây sẽ xảy ra:

- Nếu máy chủ DHCP được ủy quyền, dịch vụ DHCP Server sẽ khởi động
- Nếu máy chủ DHCP chưa được ủy quyền, dịch vụ DHCP Server sẽ ghi một lỗi vào trong nhật ký sự kiện hệ thống rằng dịch vụ không khởi động và hiển nhiên là nó sẽ không phản hồi lại các yêu cầu của máy khách.

Hãy xem xét hai kịch bản sau. Trong kịch bản thứ nhất, máy chủ DHCP là một phần của miền và được ủy quyền. Trong kịch bản thứ hai, máy chủ DHCP không phải trong một miền và hiển nhiên là chưa được ủy quyền. Các kịch bản này được thể hiện rõ ràng trong hai phía trái và phải tương ứng của Hình 1-10:



Hình 1-10. Quá trình khởi tạo và ủy quyền một máy chủ DHCP

Trong kịch bản đầu tiên, máy chủ DHCP khởi tạo và xác định liệu nó có phải là một phần của miền hay không. Nếu đúng, nó sẽ liên hệ với dịch vụ thư mục để xác nhận xem nó có được ủy quyền hay không. Dịch vụ thư mục sẽ xác nhận rằng máy chủ được ủy quyền. Sau khi nhận được xác nhận này, máy chủ này sẽ quảng bá một thông điệp DHCPINFORM để xác định liệu các dịch vụ thư mục khác có sẵn sàng hay không và lặp lại quá trình ủy quyền với từng dịch vụ thư mục phản hồi với thông điệp đó. Sau khi quá trình này hoàn thành, máy chủ bắt đầu phục vụ các máy khách DHCP một cách chính thức.

Trong kịch bản thứ hai, máy chủ không nằm trong miền. Khi máy chủ khởi tạo, nó kiểm tra xem có máy chủ thành viên DHCP nào không. Nếu không có máy chủ DHCP thành viên nào được tìm thấy, máy chủ bắt đầu phục vụ các máy khách DHCP và tiếp tục kiểm tra xem có máy chủ thành viên nào không bằng cách gửi các thông điệp DHCPINFORM đi cứ 5 phút một lần.

Nếu một máy chủ DHCP thành viên được tìm thấy, máy chủ sẽ tắt dịch vụ DHCP và hiển nhiên là ngừng phục vụ các máy khách DHCP.

Active Directory phải hoạt động để ủy quyền cho máy chủ DHCP và ngăn chặn các máy chủ không được ủy quyền. Nếu bạn cài đặt một máy chủ DHCP trong mạng không có Active Directory thì cũng không phải thực hiện việc ủy quyền. Nếu sau đó bạn thêm Active Directory vào, máy chủ DHCP sẽ nhận biết được sự có mặt của Active Directory, và vì nó chưa được ủy quyền nên máy chủ đó sẽ tự tắt dịch vụ của nó. Máy chủ DHCP thông thường theo mặc định là không được ủy quyền và do vậy các máy chủ đó phải được ủy quyền một cách trực tiếp.

Bảo vệ hệ thống khỏi các máy chủ DHCP không được phép trong nhóm làm việc

Khi khởi tạo một máy chủ DHCP mà không phải là máy chủ thành viên của một miền (ví dụ như thành viên của một nhóm làm việc), các sự kiện sau xảy ra:

- Máy chủ sẽ quảng bá một thông điệp DHCPINFORM trong mạng
- Bất ký máy chủ nào nhận được thông điệp này sẽ phản ứng lại bằng một thông điệp DHCPACK và cung cấp tên của miền thư mục mà nó là thành viên.
- Nếu một máy chủ DHCP thuộc nhóm làm việc phát hiện ra máy chủ DHCP thành viên khác của một miền trong mạng, máy chủ DHCP thuộc nhóm làm việc này sẽ cho rằng nó chưa được ủy quyền trong mạng đó và tự tắt dịch vụ của nó.
- Nếu máy chủ DHCP thuộc nhóm làm việc phát hiện ra sự tồn tại của một máy chủ thuộc nhóm làm việc khác, nó sẽ không để ý đến máy chủ đó, điều này có nghĩa là nhiều máy chủ thuộc nhóm làm việc có thể được kích hoạt cùng một thời điểm mặc dù không có một dịch vụ thư mục nào.

Khi một máy chủ thuộc nhóm làm việc khởi tạo và được ủy quyền, (bởi vì không có máy chủ thành viên của miền hoặc máy chủ thuộc nhóm làm việc nào khác trong mạng), nó tiếp tục quảng bá thông điệp DHCPINFORM cứ sau mỗi 5 phút. Nếu một máy chủ DHCP thành viên của miền ủy quyền được khởi tạo sau đó, máy chủ thuộc nhóm làm việc sẽ trở thành không ủy quyền và sẽ ngừng phục vụ.

- **Ủy quyền dịch vụ DHCP Server**

Để ủy quyền cho một máy chủ DHCP trong Active Directory, thực hiện theo các bước sau đây:

1. Mở bảng điều khiển DHCP từ thực đơn ***Administrative Tools.***
2. Trong bảng điều khiển, nhấn phải chuột vào DHCP và sau đó nhấn vào "***Manage Authorized Servers***" (*Quản trị các máy chủ được ủy quyền*)
3. Trong hộp thoại Manage Authorized Servers, lựa chọn Authorize (Ủy quyền)
4. Trong hộp thoại ***Authorize DHCP Server (****Máy chủ DHCP được ủy quyền****)***, nhập vào tên hoặc địa chỉ IP của máy chủ DHCP cần ủy quyền và sau đó nhấn OK
5. Máy tính sẽ liệt kê tên đầy đủ và địa chỉ IP của máy tính và sau đó hỏi để xác nhận. Nhấn OK để tiếp tục.

Khi việc ủy quyền được hoàn thành, mũi tên trên biểu tượng máy chủ trong bảng điều khiển DHCP sẽ thay đổi từ đỏ sang xanh. Bạn có thể phải ***refresh*** (làm tươi) bảng điều khiển này.

> ***LƯU Ý. Ai có thể ủy quyền máy chủ DHCP****. Để ủy quyền một máy chủ DHCP, một người dùng phải là thành viên của nhóm* ***Enterprise Admins****, nhóm này có trong miền gốc (****root domain****) của rừng.*

CẤU HÌNH MỘT DHCP SCOPE (PHẠM VI DHCP)

Phạm vi sẽ xác định các địa chỉ IP nào sẽ sử dụng cho các máy khách. Bạn có thể cấu hình nhiều phạm vi trên một máy chủ DHCP mà cần cho môi trường mạng của bạn.

Phạm vi DHCP là gì ?

Một phạm vi DHCP, như đã đề cập đến trong phần trước, là một tập hợp các địa chỉ IP và các thông tin cấu hình được ấn định để cung cấp cho các máy trạm DHCP. Một phạm vi phải được định nghĩa và kích hoạt trước khi các máy khách DHCP có thể sử dụng máy chủ DHCP cho việc cấu hình động TCP/IP.

Người quản trị có thể tạo ra một hoặc nhiều phạm vi trên một hoặc nhiều máy chủ Windows Server 2003 chạy dịch vụ DHCP Server. Tuy nhiên, bởi vì các máy chủ DHCP không trao đổi các thông tin về phạm vi với nhau nên

người quản trị phải cẩn thận khi định nghĩa các phạm vi để nhiều máy chủ DHCP không gán cùng một địa chỉ IP cho các máy khách khác nhau hoặc gán các địa chỉ mà đã được đặt tĩnh cho các máy IP trước đó.

Các địa chỉ IP định nghĩa trong một phạm vi DHCP phải liên tục và được gắn với cùng một mặt nạ mạng con. Nếu các địa chỉ bạn muốn gán là không liên tục, bạn phải tạo ra một phạm vi bao hàm tất cả các địa chỉ mà bạn muốn gán và sau đó loại trừ các địa chỉ hoặc dải địa chỉ xác định ra khỏi phạm vi đó. Bạn chỉ có thể tạo ra một phạm vi trên một mạng con trong một máy chủ DHCP đơn. Để cho phép loại trừ khả năng một số địa chỉ IP trong phạm vi có thể đã được gán và đang sử dụng, người quản trị DHCP có thể chỉ định khoảng *ngoại lệ* (***Exclusion***) - một hoặc nhiều địa chỉ IP trong dải mà sẽ không gán cho các máy khách DHCP.

Dải địa chỉ

Khi mà phạm vi DHCP đã được định nghĩa và khoảng ngoại lệ được áp dụng, phần địa chỉ còn lại sẽ hình thành một dải địa chỉ sẵn sàng trong phạm vi đó. Các địa chỉ trong dải này có thể được cấp động cho các máy khách trong mạng.

Dải địa chỉ ngoại lệ

Một dải ngoại lệ là một dãy giới hạn các địa chỉ IP trong dải phạm vi mà sẽ được loại trừ khỏi danh sách đề xuất của máy chủ DHCP. Khi dải ngoại lệ được sử dụng, chúng đảm bảo rằng bất kỳ địa chỉ nào trong dải ngoại lệ được định nghĩa này sẽ không được máy chủ DHCP đề xuất cho các máy khách. Bạn có thể chỉ ra tất cả các địa chỉ IP đã được cấu hình tĩnh cố định vào trong dải ngoại lệ này.

- **Cấu hình một phạm vi DHCP**

Để cấu hình một phạm vi DHCP, thực hiện theo các bước sau:

1. Mở bảng điều khiển DHCP từ thực đơn ***Administrative Tools***

2. Trong bảng điều khiển, nhấn trái chuột và sau đó nhấn phải chuột vào máy chủ DHCP trong đó bạn muốn tạo ra một phạm vi DHCP mới và sau đó lựa chọn ***New Scope*** (*Phạm vi mới*)

3. Trong "***New Scope Wizard***" (*Trình tạo phạm vi mới*), nhấn ***Next***, nhập vào một tên và mô tả của phạm vi và sau đó nhấn ***Next***. Bạn có thể sử dụng bất kỳ tên nào bạn muốn, tuy nhiên nó nên đủ ý nghĩa để bạn có thể nhận biết được mục đích của phạm vi này

trong mạng của bạn. (Ví dụ bạn có thể sử dụng một tên như "Các địa chỉ cho máy khách trong tòa nhà quản lý")

4. Trong trang "***IP Address Range***" (*Khoảng địa chỉ IP*), nhập vào khoảng địa chỉ mà có thể được gán như là một phần của phạm vi này. (Ví dụ, sử dụng một dải địa chỉ IP từ địa chỉ khởi đầu 10.1.1.50 đến địa chỉ kết thúc 10.1.1.150). Bởi vì các địa chỉ này sẽ được gán cho các máy khách, chúng phải là các địa chỉ hợp lệ và hiện tại chưa được sử dụng trong mạng. Giá trị mặt nạ mạng con mặc định tương ứng với dải địa chỉ của bạn sẽ được gắn vào. Nếu bạn sử dụng một giá trị mặt nạ mạng con khác, nhập vào mặt nạ mạng con mới và sau đó nhấn ***Next***.

5. Trong trang "***Add Exclusions***" (*Thêm các ngoại lệ*), trong hộp ***Start***, nhập vào địa chỉ IP bắt đầu của dải mà bạn muốn loại trừ và trong hộp ***End***, nhập vào địa chỉ kết thúc của dải địa chỉ mà bạn muốn loại trừ. Để loại trừ một địa chỉ IP đơn, trong hộp ***Start***, nhập vào địa chỉ IP đó.

6. Nhấn ***Add*** để lặp lại Bước 5 cho tới khi bạn đã nhập vào tất cả các địa chỉ IP mà bạn muốn loại trừ. Bạn nên loại trừ bất kỳ địa chỉ nào mà bạn đã gán tĩnh. Nhấn ***Next***.

7. Trong trang "***Lease Duration***" (*Thời hạn thuê*), nhập vào số ngày, giờ và phút trước khi một địa chỉ IP đã gán từ phạm vi này bị hết hạn. Như đã đề cập đến trong phần trước, việc này sẽ xác định thời gian bao lâu một máy khách có thể giữ được một địa chỉ nhận được mà chưa cần làm mới nó. Giá trị khoảng thời gian mặc định của hợp đồng là tám ngày. Nhấn ***Next***.

8. Trong trang "**Configure DHCP Options**" (Cấu hình các tùy chọn DHCP), nhấn vào "**Yes, I Want To Configure These Options Now**" (Đúng, tôi muốn cấu hình các tùy chọn này ngay bây giờ) để sử dụng trình hướng dẫn này cấu hình các lựa chọn DHCP thông dụng nhất, ví dụ như địa chỉ IP của cổng ra mặc định, các thiết lập máy chủ DNS và WINS. Nhấn Next.

9. Trong trang "***Router (Default Gateway***)" (*Bộ định tuyến (Cổng ra mặc định*)), nhập vào địa chỉ IP cho cổng ra mặc định sẽ được sử dụng bởi các máy khách mà nhận được địa chỉ IP từ phạm vi này. Nhấn ***Add*** để đặt địa chỉ của cổng ra mặc định này trong danh sách và sau đó nhấn ***Next***.

10. Trong trang "***Domain Name And DNS Servers***" (*Tên miền và các máy chủ DNS*), nếu bạn đang sử dụng máy chủ DNS trong mạng của bạn, nhập vào tên miền của hệ thống trong hộp thoại "***Parent domain***" (*Tên miền mức cha*).

11. Trong trang "***Domain Name And DNS Servers***", nhập vào tên của máy chủ DNS của bạn và sau đó nhấn ***Resolve*** để đảm bảo rằng máy chủ DHCP có thể liên lạc với máy chủ DNS và xác định địa chỉ IP của nó.

12. Trong trang "***Domain Name And DNS Servers***", nhấn ***Add*** để thêm máy chủ đó vào trong danh sách của các máy chủ DNS mà gán cho các máy khách DHCP. Nhấn ***Next***.

13. Trong trang WINS, nhập vào địa chỉ IP của máy chủ WINS trong mạng của bạn và nhấn ***Add.*** Nếu bạn không biết địa chỉ IP, trong hộp ***Server name***, nhập vào tên của máy chủ WINS và nhấn ***Resolve.*** Sau khi thêm vào các máy chủ WINS, nhấn ***Next***

14. Trong trang "**Activate Scope**" (Kích hoạt phạm vi), nhấn "**Yes, I Want To Activate This Scope Now**" (Đúng, tôi muốn kích hoạt phạm vi này ngay lập tức), để kích hoạt phạm vi này và cho phép các máy khách lấy địa chỉ từ nó và sau đó nhấn **Next**

15. Trong trang **Completing The New Scope Wizard** (Hoàn thành việc tạo phạm vi mới), nhấn **Finish**.

Địa chỉ Multicast (Quảng bá có địa chỉ)

Máy chủ Microsoft DHCP đã được mở rộng để cho phép việc gán các địa chỉ ***Multicast*** (quảng bá có địa chỉ) bên cạnh các địa chỉ ***Unicast*** (đơn nhất). Một chuẩn do IETF đề xuất định nghĩa việc chỉ định các địa chỉ ***multicast***. Chuẩn đề xuất này đem lại lợi ích cho các quản trị mạng bằng cách cho phép các địa chỉ ***Multicast*** được gán trong cùng kiểu như các địa chỉ ***unicast***, cho phép sử dụng hoàn toàn nền tảng hạ tầng đã có.

Việc sử dụng các địa chỉ ***multicast*** có hai phần: (1) Việc triển khai phía máy chủ để cấp các địa chỉ ***multicast*** và (2) giao diện lập trình ứng dụng (API) phía máy khách mà các ứng dụng có thể sử dụng để yêu cầu, làm mới và giải phóng các địa chỉ ***multicast***. Để sử dụng các địa chỉ ***multicast***, người quản trị trước hết phải cấu hình các phạm vi ***multicast*** và các khoảng địa chỉ IP ***multicast*** tương ứng trên máy chủ thông qua snap-in. Các địa chỉ ***multicast*** sau đó có thể được quản lý giống như các địa chỉ IP thông thường. Các máy

khách có thể gọi các hàm API để yêu cầu địa chỉ ***multicast*** từ một phạm vi. Việc thi hành ngầm thế này sẽ sử dụng các định dạng gói tin kiểu giao thức DHCP giữa máy khách và máy chủ.

CẤU HÌNH ĐỊA CHỈ DHCP DÀNH SẴN

Sử dụng các dịa chỉ IP dành sẵn (***reservation***) cho các máy khách DHCP cần phải có địa chỉ IP tĩnh trong mạng. Ví dụ về các máy tính yêu cầu địa chỉ tĩnh trong mạng là các máy chủ Email và các máy chủ ứng dụng. Máy chủ File và In ấn cũng có thể yêu cầu địa chỉ IP tĩnh hoặc địa chỉ IP dành sẵn nếu chúng được truy cập bằng địa chỉ IP của chúng.

Sự dành sẵn DHCP là gì ?

Sự dành sẵn cho phép các hợp đồng thuê địa chỉ được gán lâu dài từ máy chủ DHCP. Khi sự dành sẵn được sử dụng, chúng đảm bảo rằng một thiết bị phần cứng cụ thể trong một mạng con có thể luôn sử dụng cùng một địa chỉ IP. Sự dành sẵn phải được tạo ra trong phạm vi và không bị loại trừ khỏi phạm vi đó. Các địa chỉ ngoại lệ sẽ không thể gán cho các máy khách cho dù nó được dành sẵn cho máy khách đó. Một địa chỉ IP được thiết lập dự phòng hoặc dành sẵn cho một thiết bị mạng có địa chỉ MAC gắn với địa chỉ IP đó. Do đó, khi tạo ra một sự dành sẵn, bạn phải biết được địa chỉ MAC của mỗi thiết bị mà bạn muốn dành sẵn một địa chỉ IP cho nó. Đối với Windows 98, Windows 2000, Windows XP và Windows Server 2003, địa chỉ MAC có thể được biết bằng cách nhập vào ***ipconfig /all*** tại giao diện dòng lệnh, việc này sẽ cho kết quả đầu ra tương tự hình sau đây:

Ethernet adapter:
Description.....:DECDC21140 PCI FastEthernet Adapter
PhysicalAddress….....:00-03-FF-F6-FF-FF
DHCPEnabled.....:Yes
IPAddress.....:169.254.150.72
SubnetMask…….....:255.255.0.0
DefaultGateway…….....:
DHCPServer.....:255.255.255.255
PrimaryWINSServer…...:
SecondaryWINSServer...:
LeaseObtained.....:0712036:11:42PM
LeaseExpires.....:
Địa chỉ MAC trong ví dụ này là 00-03-FF-F6-FF-FF

Cấu hình một sự dành sẵn trong DHCP như thế nào

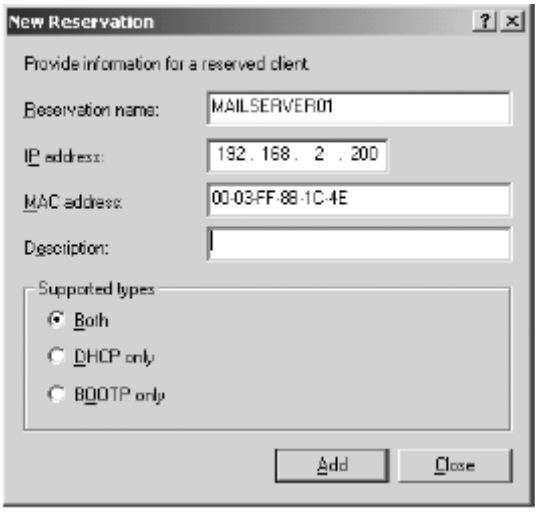
Để cấu hình một sự dành sẵn DHCP, thực hiện theo các bước sau:

1. Mở bảng điều khiển DHCP

2. Trong cây bảng điều khiển, nhấn vào ***Reservations***

3. Trong thực đơn ***Action***, nhấn vào ***New Reservation***

Hình 1-11 thể hiện một ví dụ của một trang thuộc tính ***New Reservation*** hoàn chỉnh



Hình 1-11. Một trang thuộc tính New Reservation DHCP

4. Trong hộp thoại ***New Reservation***, cung cấp các thông tin sau đây và sau đó nhấn ***Add***:

    a. Tên của việc dành sẵn này (ví dụ MailServer01)

    b. Địa chỉ IP

    c. Địa chỉ MAC

    d. Mô tả (Tùy ý, không bắt buộc)

    e. Kiểu hỗ trợ (Chỉ DHCP, Chỉ BOOTP, Cả hai)

Bạn có thể giới hạn kiểu máy khách có thể sử dụng sự dành sẵn này là DHCP hoặc BOOTP hoặc cho phép cả hai. Một số máy khách cũ mà chạy các hệ điều hành không phải Microsoft có thể sử dụng BOOTP cũ thay vì DHCP. Cũng như vậy, các máy khách Windows 2000 ***Remote Installation Services*** (RIS) sử dụng BOOTP khi chúng khởi tạo. Nhấn ***Both***, trừ khi bạn muốn cấu hình các máy trạm bị giới hạn sử dụng một giao thức cụ thể trong khi nhận sự dành sẵn DHCP này.

5. Để thêm sự dành sẵn cho máy khách vào phạm vi, nhấn ***Add***

6. Lặp lại hai bước trên cho bất kỳ sự dành sẵn nào khác mà bạn muốn thêm vào và nhấn ***Close***

CẤU HÌNH CÁC TÙY CHỌN CHO DHCP

Các tùy chọn DHCP là các tham số cấu hình máy khách bổ sung mà một máy chủ DHCP có thể gán khi phục vụ các máy khách DHCP. Các tùy chọn DHCP được cấu hình sử dụng bảng điều khiển DHCP và có thể được áp dụng cho nhiều phạm vi và sự dành sẵn. Ví dụ, các địa chỉ IP cho một thiết bị định tuyến hoặc cổng ra mặc định, máy chủ WINS hoặc máy chủ DNS thường xuyên được cung cấp cho một phạm vi đơn hoặc tổng quát cho tất cả các phạm vi được quản lý bởi máy chủ DHCP. Rất nhiều tùy chọn DHCP được định nghĩa trước trong RFC2132, nhưng máy chủ DHCP của Microsoft cũng cho phép bạn định nghĩa và thêm các tùy chọn tùy biến. Bảng 1-1 mô tả một số tùy chọn mà bạn có thể cấu hình.

Bảng 1-1: Các tùy chọn Phạm vi DHCP

Tùy chọn	Mô tả
Router (default gateway)	Địa chỉ của bất cứ cổng ra mặc định hay bộ định tuyến nào
Domain name	Tên miền DNS xác định miền mà máy khách sẽ phụ thuộc. Máy khách có thể sử dụng thông tin này dể cập nhật thông tin lên máy chủ DNS để các máy tính khác có thể tìm thấy nó.
DNS and WINS servers	Địa chỉ của bất cứ máy chủ DNS hay WINS nào mà máy khách có thể sử dụng trong liên lạc mạng.

Các phân lớp nhà cung cấp (*Vendor Classes*) và người dùng (*User classes*).

Các tùy chọn DHCP có thể được gán cho mọi phạm vi, một phạm vi cụ thể và tới một sự dành sẵn cho máy cụ thể nào đó. Có bốn loại tùy chọn DHCP trong Windows Server 2003:

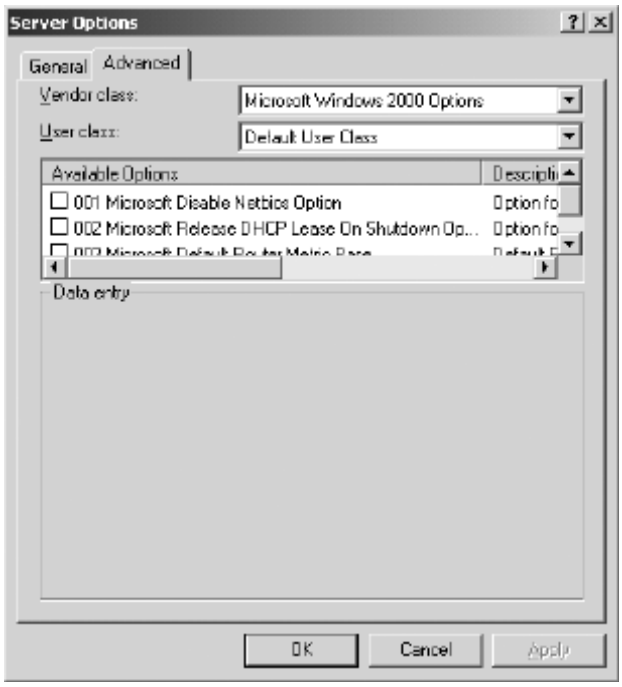
- **Server options (***Các tùy chọn cho máy chủ***)**. Các tùy chọn cho máy chủ sẽ áp dụng cho mọi máy khách của máy chủ DHCP đó. Sử dụng các tùy chọn này cho các tham số thường có trong tất cả các phạm vi trong máy chủ DHCP

- **Scope Options (***Các tùy chọn cho phạm vi*). Các tùy chọn cho phạm vi áp dụng cho tất cả các máy khách trong một phạm vi và là tập hợp các tùy chọn được sử dụng thường xuyên nhất. Các tùy chọn cho phạm vi sẽ có quyền ưu tiên cao hơn và phủ nhận các tùy chọn cho máy chủ.

- **Class Options (***Các tùy chọn cho phân lớp)*. Các tùy chọn cho phân lớp sẽ cung cấp các tham số DHCP cho các máy khách DHCP dựa trên kiểu- hoặc là các phân lớp nhà cung cấp (***Vendor Classes***) hoặc các phân lớp người dùng (***User classes***).

- **Client Options (***Các tùy chọn cho máy khách*). Các tùy chọn cho máy khách áp dụng cho từng máy khách riêng. Các tùy chọn cho máy khách có quyền ưu tiên cao nhất và phủ nhận các tùy chọn khác (máy chủ, phạm vi và phân lớp)

Các phân lớp người dùng được tạo ra theo ý riêng người quản trị DHCP. Các phân lớp nhà cung cấp được định nghĩa theo các nhà cung cấp máy tính và không thể thay đổi. Hình 1-12 thể hiện cách sử dụng của các phân lớp nhà cung cấp khi áp dụng tùy chọn 002 "***Microsoft Release DHCP Lease On Shutdown***" (Microsoft giải phóng hợp đồng DHCP khi tắt máy) vào các máy tính chạy Windows 2000. Sử dụng các phân lớp nhà cung cấp và người dùng, một quản trị có thể cấu hình máy chủ DHCP để gán các tùy chọn khác nhau, tùy thuộc vào kiểu máy khách tiếp nhận chúng. Ví dụ, một nhà quản trị có thể cấu hình máy chủ DHCP để gán các tùy chọn khác nhau dựa trên kiểu của máy khách, ví dụ máy để bàn hoặc máy xách tay. Tính năng này cho phép người quản trị mạng linh hoạt hơn trong khi cấu hình các máy khách. Nếu các phân lớp người dùng không được sử dụng, các thiết lập mặc định sẽ được gán vào.



Hình 1-12. Trang thuộc tính DHCP Server Options

> ***THÔNG TIN THÊM. Các phân lớp nhà cung cấp và các tùy chọn nhà cung cấp****. Phân lớn nhà cung cấp và các tùy chọn nhà cung cấp được mô tả trong trong RFC2132 và có thể tìm thấy tại địa chỉ* ***http://www.rfceditor.org/rfcsearch.html****.*

CẤU HÌNH DHCP RELAY AGENT

Khi máy khách DHCP và máy chủ DHCP trong cùng một mạng con, các thông điệp DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, and DHCPACK được gửi đi theo các hình thức quảng bá của mức MAC và mức IP. Khi máy chủ DHCP và máy khách không trong cùng một mạng con, các thiết bị định tuyến kết nối phải hỗ trợ việc chuyển tiếp các thông điệp DHCP giữa máy khách DHCP và máy chủ DHCP hoặc ***BOOTP/DHCP relay agent*** phải được cài đặt trong mỗi mạng con. Giao thức BOOTP và DHCP phụ thuộc vào các thông điệp quảng bá trên mạng để làm nhiệm vụ của chúng. Các bộ định tuyến trong môi trường định tuyến thông thường sẽ không tự động chuyển tiếp các thông điệp quảng bá từ một giao tiếp này đến giao tiếp khác.

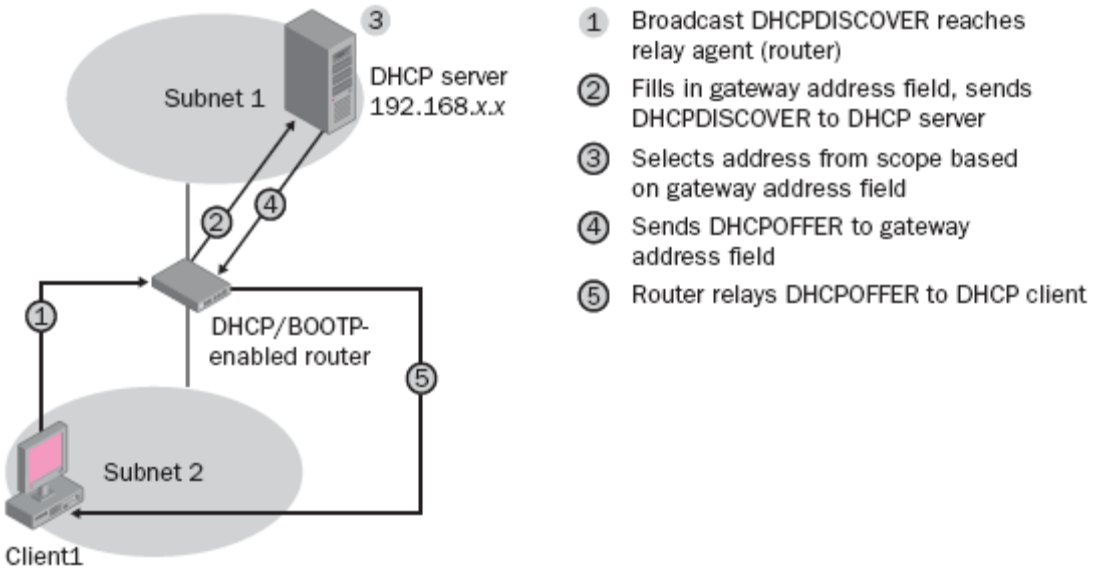
Có hai phương pháp cho phép bạn giải quyết giới hạn này. Cách thứ nhất, nếu bộ định tuyến phân cách máy chủ DHCP và máy khách là thiết bị tương thích RFC 1542, bộ định tuyến này có thể được cấu hình cho phép chuyển tiếp BOOTP. Bằng việc chuyển tiếp BOOTP, các bộ định tuyến chuyển tiếp các thông điệp quảng bá DHCP giữa các máy khách và các máy chủ và

thông báo cho các máy chủ trên mạng con phát sinh các yêu cầu của máy khách. Quá trình này cho phép các máy chủ DHCP gán các địa chỉ đến máy khách ở xa từ các phạm vi tương ứng.

Phương pháp thứ hai để cho phép truyền thông từ xa giữa máy chủ và máy khách DHCP là cấu hình ***DHCP relay agent*** trên mạng con mà có chứa các máy khách ở xa đó. ***DHCP relay agent*** sẽ chặn các gói tin DHCPDISCOVER và chuyển tiếp chúng tới một máy chủ DHCP mà địa chỉ đã được cấu hình sẵn. Một ***DHCP relay agent*** có thể là một bộ định tuyến hoặc một máy tính cấu hình để lắng nghe các thông điệp quảng bá DHCP/BOOTP và hướng chúng tới một hoặc nhiều máy chủ DHCP cụ thể. Sử dụng ***relay agent*** giảm thiểu sự cần thiết phải có một máy chủ DHCP trên mỗi phân đoạn mạng vật lý hoặc phải mua các bộ định tuyến tương thích RFC2131. Các ***relay agent*** không chỉ định hướng các yêu cầu của máy khách DHCP nội bộ đến các máy chủ DHCP mà còn trả các phản hồi của máy chủ DHCP về cho các máy khách DHCP. Mặc dù ***DHCP relay agent*** được cấu hình thông qua ***Routing And Remote Access*** (*Định tuyến và truy cập từ xa*), máy tính chứa ***relay agent*** này không cần thiết phải hoạt động như một bộ định tuyến thực sự giữa hai mạng con. Các bộ định tuyến tương thích theo chuẩn RFC 2131 (hoặc RFC 1542) có chứa các ***relay agent*** cho phép chúng chuyển tiếp các gói tin DHCP.

Relay agent làm việc như thế nào ?

Hình 1-13 và các danh sách đánh số sau đây thể hiện cách thức mà một máy khách DHCP trong mạng con 2 lấy được địa chỉ IP từ máy chủ DHCP trong mạng con 1.



Hình 1-13: Sử dụng Relay Agent

1. Máy khách DHCP quảng bá một thông điệp DHCPDISCOVER trong mạng con 2 như một gói dữ liệu UDP trên cổng UDP 67, đó là cổng dành riêng và chia sẻ cho các truyền thông của máy chủ BOOTP và DHCP.

2. ***Relay agent***, trong trường hợp này là một bộ định tuyến có khả năng chuyển tiếp DHCP/BOOTP, kiểm tra trường địa chỉ IP cổng ra trong ***header*** (tiêu đề) của thông điệp DHCP/BOOTP. Nếu trường này có giá trị 0.0.0.0, ***relay agent*** này sẽ điền giá trị địa chỉ của nó vào và chuyển tiếp thông điệp này vào mạng con 1, nơi có máy chủ DHCP.

3. Khi máy chủ DHCP trong mạng con 1 nhận được thông điệp DHCPDISCOVER, nó kiểm tra trường địa chỉ IP cổng ra của phạm vi DHCP để xác định liệu nó có thể cung cấp địa chỉ IP. Nếu máy chủ DHCP có nhiều phạm vi, địa chỉ trong trường địa chỉ IP cổng ra sẽ nhận biết phạm vi nào sẽ đề xuất các địa chỉ IP cho các máy khách.

   Ví dụ, nếu trường địa chỉ IP cổng ra có một địa chỉ IP là 192.168.45.2, máy chủ DHCP sẽ kiểm tra phạm vi DHCP của nó để tìm kiếm một khoảng phạm vi mà phù hợp với mạng IP lớp C mà bao gồm cả địa chỉ IP cổng ra của máy tính. Trong trường hợp này, máy chủ DHCP kiểm tra để xem phạm vi nào sẽ bao gồm khoảng địa chỉ 192.168.45.1 và 192.168.45.254. Nếu một phạm vi tồn tại mà có các thông tin phù hợp, máy chủ DHCP sẽ lựa chọn một địa chỉ cớ sẵn từ phạm vi phù hợp đó để sử dụng cho lời đề xuất cho thuê địa chỉ IP (DHCPOFFER) để phản hồi lại cho máy khách.

4. Máy chủ DHCP sẽ gửi đi một thông điệp DHCPOFFER trực tiếp đến ***relay agent*** mà nhận biết được trong trường địa chỉ IP cổng ra.

5. Bộ định tuyến sẽ chuyển tiếp thông điệp đề xuất địa chỉ (DHCPOFFER) đến máy khách DHCP như một thông điệp quảng bá vì địa chỉ IP của máy khách vẫn chưa xác định được.

   Sau khi máy khách nhận được thông điệp DHCPOFFER, một thông điệp DHCPREQUEST được chuyển tiếp từ máy khách tới máy chủ và một thông điệp DHCPACK sẽ được chuyển tiếp từ máy chủ đến máy khách như mô tả trong RFC1542.

- **Cài đặt một DHCP relay agent**

Để cài đặt một ***DHCP relay agent***, thực hiện theo các bước sau:

1. Trong thực đơn **Administrative Tools**, mở **Routing and Remote Access** (Định tuyến và truy cập từ xa)

2. Trong bảng điều khiển, mở rộng biểu tượng máy chủ và sau đó nhấn vào "***IP Routing***" (*Định tuyến IP*)

3. Trong khung chi tiết, nhấn phải chuột vào ***General*** và sau đó nhấn vào "***New Routing Protocol***" (*Giao thức định tuyến mới*)

4. Trong hộp thoại "***New Routing Protocol***", nhấn vào ***DHCP relay agent*** và nhấn ***OK***

5. Mở hộp thoại ***Properties*** của ***DHCP relay agent***. Trong hộp "***Server Address***" (*Địa chỉ máy chủ*), nhập vào địa chỉ IP của một máy chủ DHCP và sau đó nhấn ***Add.***

Sử dụng các Siêu phạm vi (Superscopes)

Một ***superscope*** là một cách nhóm các phạm vi theo mục đích quản trị, sử dụng để hỗ trợ đa mạng hoặc đa mạng con logic (phân đoạn con của một mạng IP) trong một đoạn mạng đơn (một phần của mạng kết nối IP mà bao bọc bởi các bộ định tuyến IP). Khái niệm đa mạng thường xuất hiện khi một số lượng các máy tính trong một đoạn mạng tăng dần vượt quá khả năng cung cấp của không gian địa chỉ gốc ban đầu. Bằng cách tạo ra một phạm vi thứ hai riêng biệt một cách logic và sau đó nhóm hai phạm vi này vào trong một ***superscope*** đơn, bạn có thể nhân đôi dung lượng đoạn mạng vật lý của bạn mà sẽ cấp địa chỉ. (Trong kịch bản đa mạng, định tuyến cũng được yêu cầu để kết nối các mạng con một cách logic). Theo cách này, máy chủ DHCP có thể cung cấp cho các máy khách trên một mạng vật lý các địa chỉ thuê từ nhiều hơn một phạm vi.

> ***LƯU Ý. Các superscope chỉ chứa danh sách các phạm vi thành viên***. *Các* ***superscope*** *chỉ chứa một danh sách các phạm vi thành viên hoặc phạm vi mức con mà có thể được kích hoạt đồng thời; chúng không phải là sử dụng để cấu hình các chi tiết khác về phạm vi sử dụng.*

- **Tạo superscope**

Để tạo ra ***superscope***, đầu tiên bạn phải tạo ra phạm vi. Sau khi bạn đã tạo ra một phạm vi, bạn có thể tạo ra một ***superscope*** bằng cách hoàn thành các bước sau:

1. Mở bảng điều khiển DHCP

2. Trong bảng điều khiển, lựa chọn máy chủ DHCP sẽ thực hành

3. Từ thực đơn **Action,** lựa chọn **New Superscope** (Siêu phạm vi mới)

4. Dòng lệnh thực đơn này chỉ xuất hiện nếu có ít nhất một phạm vi không phải là một phần trong một ***superscope*** nào khác mà đã được tạo ra trong máy chủ này.

5. Trong trang **Welcome To The New Superscope Wizard** (Chào mừng đến với trình hướng dẫn tạo siêu phạm vi mới), nhấn **Next**

6. Trong trang "***Superscope Name***" (*Tên Siêu phạm vi*), trong hộp Name, nhập vào tên của ***superscope*** và sau đó nhấn ***Next***

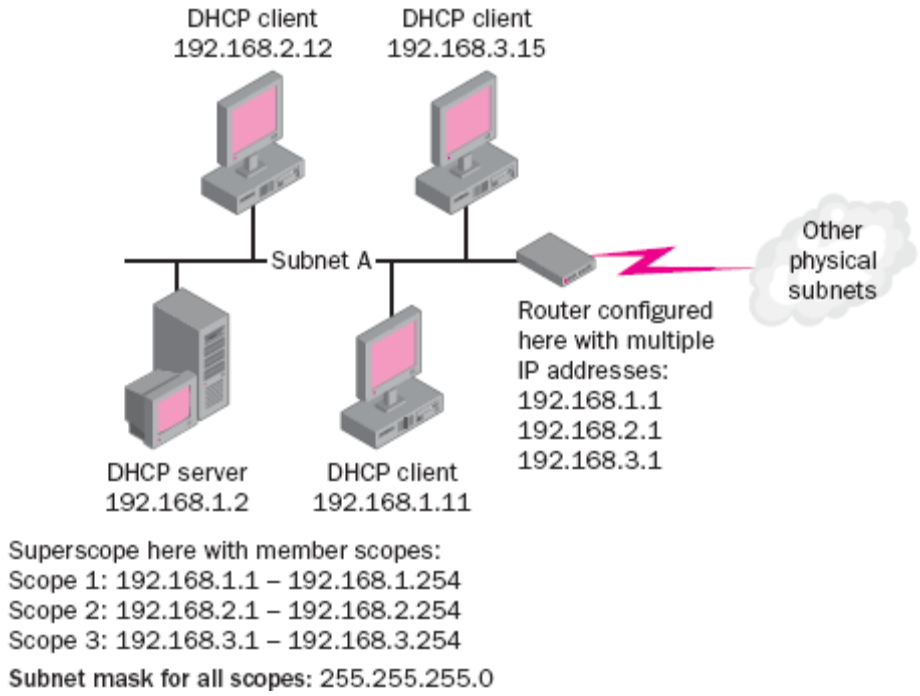
7. Trong trang "***Select Scopes***" (*Lựa chọn các phạm vi*), trong hộp ***Available Scopes*** (*Các phạm vi sẵn sàng*), lựa chọn một hoặc nhiều phạm vi từ danh sách để thêm vào ***superscope*** và sau đó nhấn ***Next***

8. Trong trang **Completing The New Superscope Wizard** (Hoàn thành trình hướng dẫn tạo siêu phạm vi mới), nhấn **Finish**.

Cấu hình superscope cho các đa mạng

Phần tiếp theo sẽ trình bày cách thức một mạng DHCP đơn giản có thể bao hàm một đoạn mạng vật lý và một máy chủ DHCP có thể được mở rộng bằng cách sử dụng các ***superscope*** để hỗ trợ các cấu hình đa mạng.

Superscope hỗ trợ đa mạng nội bộ. Hình 1-14 thể hiện đa mạng trong một mạng vật lý (Mạng con A) với một máy chủ DHCP đơn.

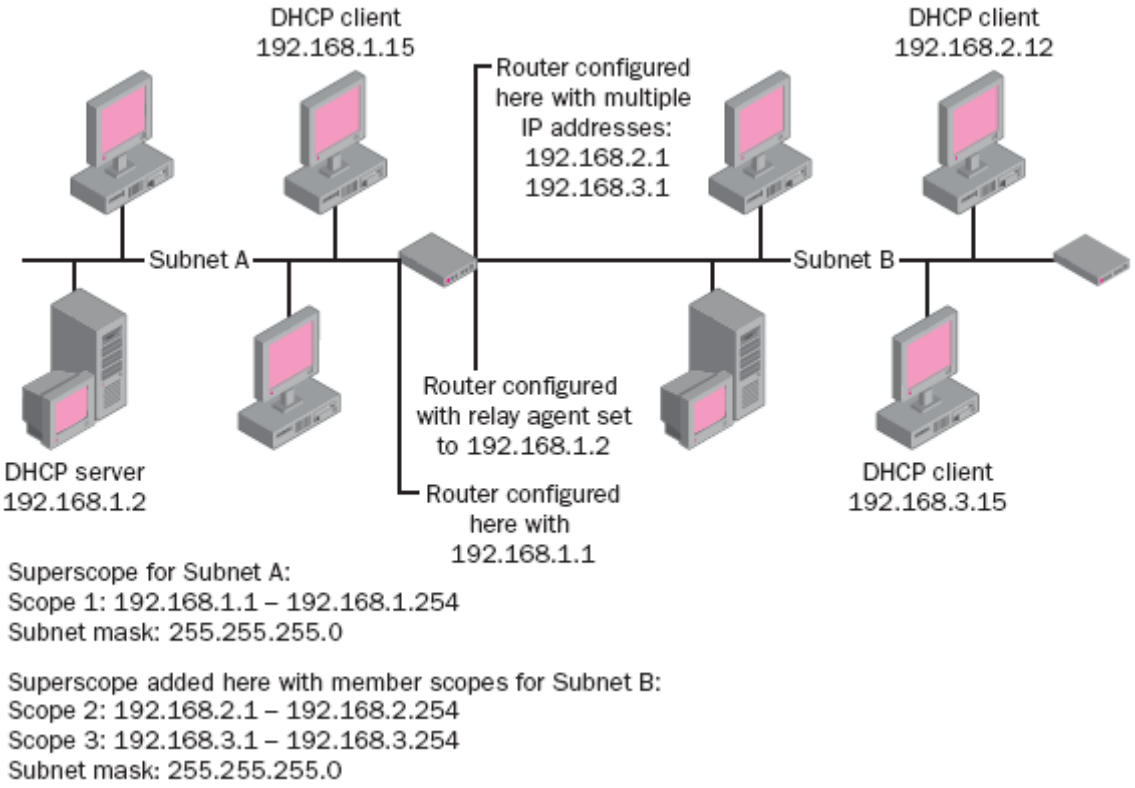


Hình 1-14. Đa mạng trong một đoạn mạng đơn

Để hỗ trợ kịch bản này, bạn có thể cấu hình một ***superscope*** mà bao hàm các thành viên của phạm vi gốc (Phạm vi 1) và các phạm vi bổ sung cho đa mạng logic mà bạn cần hỗ trợ. (Phạm vi 2 và 3)

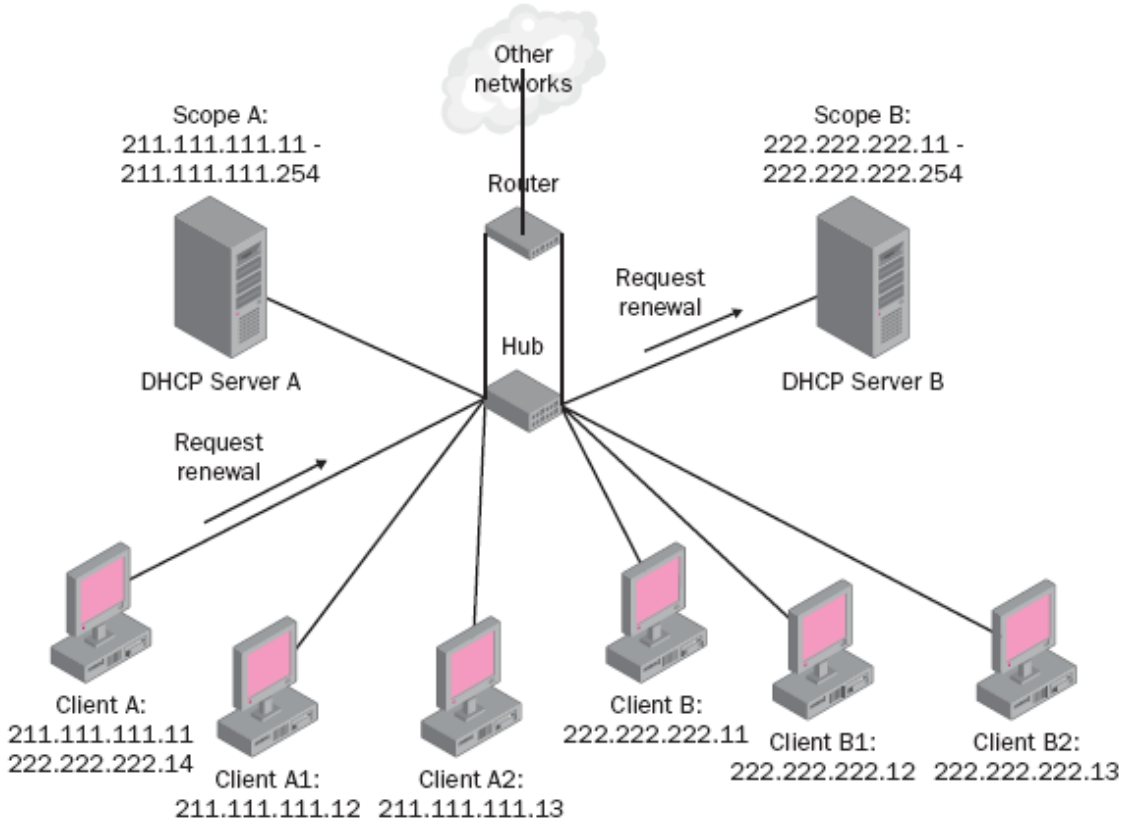
> ***LƯU Ý. Kết nối hai mạng con logic****. Khi hỗ trợ hai mạng con logic trong cùng một đoạn mạng vật lý, sử dụng một bộ định tuyến để kết nối lưu lượng từ một mạng con này sang mạng con khác.*

Superscope hỗ trợ đa mạng ở xa. Hình 1-15 thể hiện một cấu hình sử dụng để hỗ trợ đa mạng trong một mạng vật lý. (Mạng con B) mà được phân tách từ máy chủ DHCP. Trong kịch bản này, một ***superscope*** được định nghĩa trong máy chủ DHCP, kèm theo là một ***relay agent*** cấu hình trong bộ định tuyến, kết hợp các mạng con A và B vào trong một đa mạng, nơi mà các máy tính trong cả hai mạng con có thể giao tiếp với máy chủ DHCP trong mạng con A.



Hình 1-15. Đa mạng được định tuyến

Superscope hỗ trợ hai máy chủ DHCP nội bộ. Khi không có các ***superscope***, hai máy chủ DHCP là nơi cấp địa chỉ trên một đoạn mạng đơn có thể gây ra sự xung đội địa chỉ. Hình 1-16 thể hiện kịch bản này.



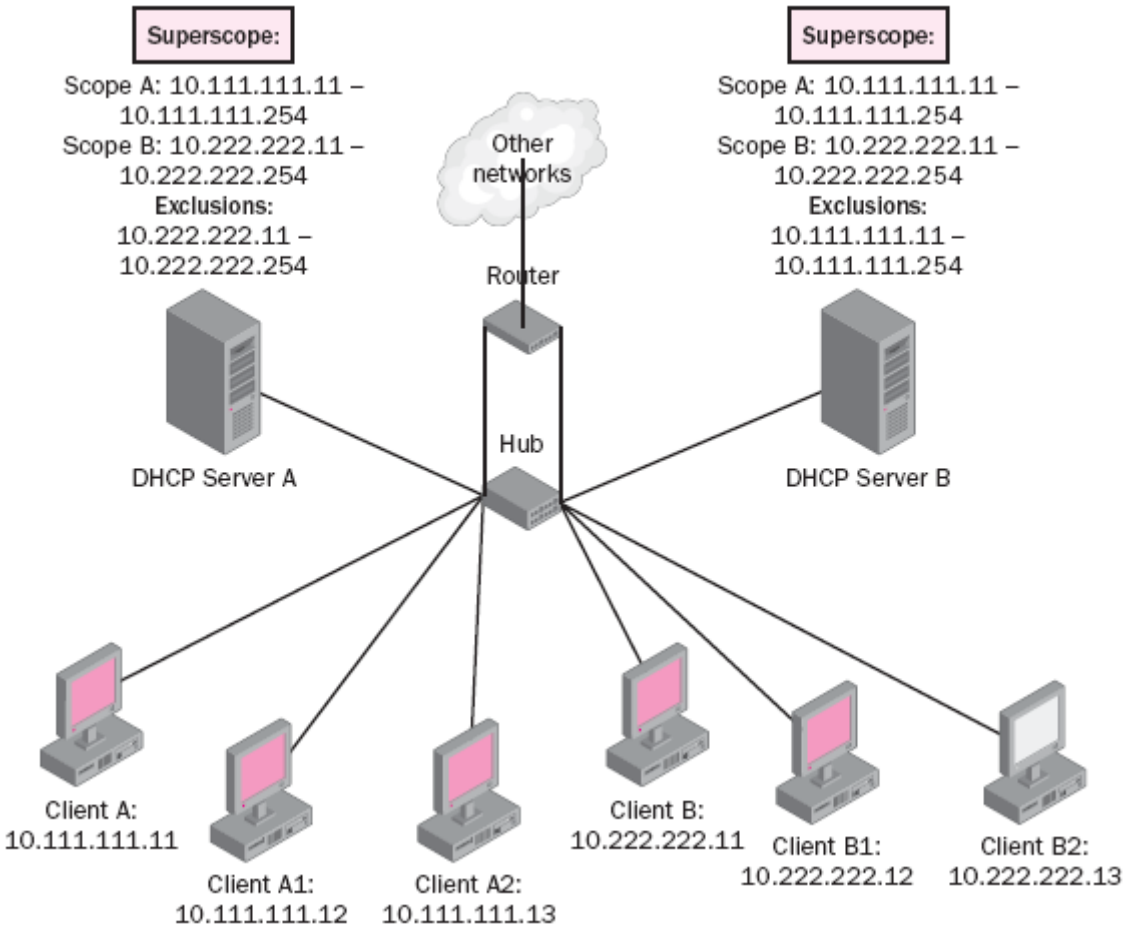
Hình 1-16. Xung đột trong mạng con hai máy chủ

Trong cấu hình này, máy chủ DHCP A quản lý một phạm vi địa chỉ khác so với máy chủ DHCP B và không có thông tin nào về các địa chỉ quản lý được trao đổi giữa hai máy tính. Sự cố xảy ra khi một máy khách, mà đã được đăng ký trước đó với máy chủ A, ví dụ, giải phóng tên của nó khi tắt và sau đó lại kết nối vào mạng.

Khi máy khách (máy A) khởi động lại, nó cố gắng làm mới địa chỉ mà nó có. Tuy nhiên, nếu máy chủ B phản hồi lại yêu cầu của máy khách A trước khi máy chủ A nhận được thì máy chủ B sẽ từ chối yêu cầu làm mới địa chỉ ngoại lai này bằng một thông điệp DHCPNACK. Kết quả của quá trình này là địa chỉ IP của máy khách A bị xóa bỏ và máy khách A bắt buộc phải tìm kiếm một địa chỉ IP mới. Trong quá trình tìm và lấy địa chỉ mới, máy khách A có thể được đề xuất một địa chỉ nào đó dẫn đến việc máy A nằm trong một mạng con logic không đúng nào đó.

Hình 1-17 thể hiện cách thức mà bạn có thể tránh các vấn đề này và quản lý hai phạm vi một cách thường xuyên đều đặn và hiệu quả bằng cách sử dụng các ***superscope*** trên cả hai máy chủ DHCP. Trong cấu hình này, cả hai máy chủ đều vẫn nằm trong cùng một mạng con vật lý. Một ***superscope*** được thêm vào trong cả hai máy chủ A và B mà thành viên là cả hai phạm vi được định nghĩa ở trong đoạn mạng vật lý. Để không cho các máy chủ này gán

các địa chỉ trong phạm vi kia, mỗi máy chủ sẽ loại trừ khoảng địa chỉ đầy đủ thuộc về máy chủ kia. Điều này thể hiện trong Hình 1-17.



Hình 1-17. Hai máy chủ sử dụng một siêu phạm vi

TỔNG KẾT

- DHCP là một giao thức chuẩn, đơn giản giúp cho người quản trị cấu hình mạng TCP/IP dễ dàng hơn rất nhiều bằng cách gán các địa chỉ IP một cách động và cung cấp các thông tin cấu hình bổ sung cho các máy khách một cách tự động.
- Các thông tin cấu hình bổ sung được cung cấp dưới dạng các tùy chọn và có thể gắn với các địa chỉ IP dành sẵn, cho các phân lớp người dùng hoặc nhà cung cấp, cho một phạm vi hoặc toàn bộ máy chủ DHCP

BÀI TẬP

QUAN TRỌNG. Hoàn thành tất cả các bài tập*. Nếu bạn có kế hoạch làm tất cả các bài tập trong sách của chương này, bạn phải thực hiện tất cả các bài tập để trả máy tính trở về trạng thái gốc của nó để chuẩn bị cho các bài tập thực hành sau này trong cuốn BÀI TẬP THỰC HÀNH.*

Bài tập 1-1. Cài đặt và ủy quyền máy chủ DHCP

1. Nhấn **Start** và trỏ vào "**Manage Your Server**" (Quản lý máy chủ của bạn)
2. Trong trang "**Manage Your Server**", nhấn vào "**Add Or Remove A Role**" (Thêm hoặc bớt một vai trò)
3. Trong trang "**Preliminary Steps Next**" (Chuẩn bị bước tiếp theo), nhấn **Next**
4. Trong trang "***Server Role***" (*Vai trò máy chủ*), nhấn vào "***DHCP Server***" và sau đó nhấn ***Next***
5. Trong trang "**Summary Of Selections**" (Tổng kết các lựa chọn), nhấn **Next**
6. Trong trang "**Welcome To The New Scope Wizard**" (Chào mừng đến với trình tạo phạm vi mới), nhấn **Cancel** (Bạn sẽ tạo ra một phạm vi trong Bài tập 1-2)
7. Trong trang "**Cannot Complete**" (Không thể hoàn thành), nhấn **Finish**
8. Nhấn ***Start***, trỏ vào ***Administrative Tools*** và sau đó chọn ***DHCP***

9. Trong bảng điều khiển DHCP, nhấn trái chuột và sau đó phải chuột vào máy chủ DHCP mà bạn muốn ủy quyền và sau đó nhấn ***Authorize*** (*Ủy quyền*)

10. Mở ***Event Viewer*** và kiểm tra nhật ký Hệ thống. tìm sự kiện thông tin mà nguồn là ***DHCPServer***, thông tin này hiển thị rằng máy chủ DHCP đã được ủy quyền một cách thành công.

11. Trong bảng điều khiển DHCP, nhấn phải chuột vào máy chủ mà bạn ủy quyền và sau đó nhấn ***Unauthorize***. Nhấn ***Yes*** để xác nhận việc dỡ bỏ máy chủ DHCP khỏi thư mục và sau đó ***refressh*** (*làm tươi*) bảng điều khiển này.

Bài tập 1-2. Cấu hình một phạm vi DHCP

1. Mở bảng điều khiển DHCP

2. Trong bảng điều khiển DHCP, nhấn phải chuột vào máy chủ DHCP mà bạn muốn cấu hình một phạm vi và sau đó nhấn "***New Scope***" (Phạm vi mới)

3. Trong trang ***Welcome***, nhấn ***Next***.

4. Trong trang "***Scope Name***", nhập vào tên và mô tả cho phạm vi này và sau đó nhấn ***Next***

5. Trong trang "***IP Address Range***" (*Dải địa chỉ IP*), nhập vào các thông tin sau đây và sau đó nhấn ***Next***

6. Địa chỉ IP bắt đầu: 10.1.1.50

7. Địa chỉ IP kết thúc: 10.1.1.100

8. Mặt nạ mạng con: 255.255.0.0

9. Trong trang "***Add Exclutions***" (*Thêm ngoại lệ*), loại bỏ dải từ 10.1.1.70 đến 10.1.1.75 ra khỏi khoảng phạm vi và nhấn ***Next***

10. Trong trang "***Lease Duration***" (*Thời hạn hợp đồng*), thiết lập khoảng hạn hợp đồng là 4 ngày và nhấn ***Next***

11. Trong trang "**Configure DHCP Options**" (Cấu hình các tùy chọn DHCP) nhấn "**Yes, I Want To Configure These Options Now**"(Đúng, tôi muốn cấu hình các tùy chọn này ngay bây giờ) và sau đó nhấn **Next**

12. Trong trang "***Router (Default Gateway)***" (*Bộ định tuyến (Cổng ra mặc định)*), nhập vào 10.1.1.1 là bộ định tuyến và sau đó nhấn ***Next***

13. Trong trang "***Domain Name and DNS Servers***" (*Tên miền và các máy chủ DNS*) trong hộp "***Parent domain***" *(miền mức cha*) nhập vào ACNA.com và trong mục ***IP address***, nhập vào 10.1.1.200. nhấn ***Add*** và sau đó nhấn ***Next***.

14. Trong trang "***WINS Servers***" (*Các máy chủ WINS*), trong mục **IP *Address***, nhập vào 10.1.1.200. Nhấn ***Add*** và sau đó nhấn ***Next***.

15. Trong hộp "**Active Scope**" (Kích hoạt phạm vi), nhấn "**No, I Will Activate This Scope Later**" (Không, tôi sẽ kích hoạt phạm vi sau này), nhấn **Next** vào sau đó nhấn **Finish**

16. Trong bảng điều khiển DHCP, kiểm tra phạm vi mà bạn vừa mới tạo ra.

Bài tập 1-3. Cấu hình một DHCP dành sẵn

1. Trong bảng điều khiển DHCP, mở rộng phạm vi mà bạn tạo ra trong bài tập 1-2. Nhấn phải chuột vào mục ***Reservations*** và lựa chọn ***New Reservation*** (*Sự dành sẵn mới*)

2. Trong trang thuộc tính ***New Reservation*** (*Sự dành sẵn mới*), nhập vào các giá trị sau đây, nhấn ***Add*** và sau đó nhấn ***Close***

3. Reservation Name: MailServer01

4. ***IP address***: 10.1.1.71

5. ***MAC address***: 00-53-45-0F-00-0A

Bài tập 1-4. Dỡ bỏ DHCP

Trong bài tập này, bạn sẽ hủy các thay đổi cấu hình mà bạn đã tạo ra trong các bài tập trước.

1. Nhấn Start và lựa chọn Manage Your Server

2. Trong trang "Manage Your Server", nhấn "Add or Remove a Role"

3. Trong trang "***Preliminary Steps***", nhấn ***Next***

4. Trong trang "***Server Role***", nhấn vào ***DHCP*** và sau đó nhấn ***Next***,

5. Lựa chọn hộp thoại "**Remove The DHCP Server Role**" (Hủy bỏ vai trò máy chủ DHCP) và sau đó nhấn **Next**

6. Trong trang "**DHCP Server Role Removed**" (Vai trò máy chủ DHCP đã được hủy bỏ), nhấn **Finish.**

CÁC CÂU HỎI TỔNG KẾT

1. Trong trường hợp nào mà một quản trị mạng nên sử dụng DHCP?

2. Đặt các kiểu thông điệp DHCP sau đây theo thứ tự mà một quá trình cấp địa chỉ IP thành công sử dụng chúng?

    a. DHCPACK

    b. DHCPOFFER

    c. DHCPREQUEST

    d. DHCPDISCOVER

3. Một máy khách DHCP phản hồi thế nào khi sự cố gắng làm mới địa chỉ IP của nó là không được và hợp đồng bị hết hạn?

4. Bạn cấu hình một phạm vi với dải địa chỉ từ 192.168.0.11 đến 192.168.0.254. tuy nhiên máy chủ DNS của bạn trong cùng một mạng con đã được gán một địa chỉ tĩnh là 192.168.0.200. Làm thế nào bạn có thể cho phép tương thích giữa địa chỉ máy chủ DNS và dịch vụ DHCP trong mạng con của bạn mà tốn ít công sức quản trị nhất?

5. Trong mỗi mạng con của bạn, bạn muốn 10 máy khách DHCP xác định (bên cạnh 150 tổng số máy trong mạng) sử dụng một máy chủ DNS thử nghiệm mà không gán thông tin này cho các máy tính khác cũng sử dụng DHCP. Làm thế nào bạn có thể đạt được mục tiêu này?

CÁC KỊCH BẢN TÌNH HUỐNG

Kịch bản tình huống 1-1: Nhận địa chỉ IP

Tháng trước, một máy chủ được cấu hình thành máy chủ DHCP và hoạt động bình thường. Năm ngày sau, một máy chủ thử nghiệm trong cùng một đoạn mạng được thăng chức thành máy chủ quản trị miền đầu tiên của mạng. Hôm nay một số người dùng trong cùng mạng với máy chủ DHCP phàn nàn

rằng họ không thể nhận được địa chỉ IP bằng phương thức DHCP. Đâu là lý do chính của việc người dùng không thể lấy được địa chỉ IP ?

a) Hợp đồng thuê địa chỉ IP của người dùng đã hết hạn
b) ***DHCP relay agent*** bị mất hoặc được cấu hình không chính xác
c) Có sự trùng lặp địa chỉ IP trong mạng
d) Máy chủ DHCP phải được ủy quyền và hiện nó chưa được ủy quyền.

Kịch bản tình huống 1-2: Tối ưu thời hạn hợp đồng khả thi

Bạn đang cấu hình các tùy chọn cho một phạm vi DHCP cho công ty ACNA,Ltd. Công ty có một lượng giới hạn địa chỉ IP cho các máy khách và muốn cấu hình DHCP để tối ưu thời hạn thuê. Lựa chọn tất cả các hành động sau đây để hoàn thành mục tiêu này:

a) Thiết lập khoảng thời hạn thuê dài
b) Thiết lập khoảng thời hạn thuê ngắn
c) Cấu hình các lựa chọn DHCP để tự động giải phóng một địa chỉ IP khi mà máy tính tắt
d) Tạo ra các địa chỉ DHCP dành sẵn cho tất cả các máy tính xách tay.

CHƯƠNG 2: QUẢN TRỊ VÀ GIÁM SÁT DHCP

Sau khi hoàn thành chương này, bạn có khả năng:

- Mô tả sự quan trọng và các **kỹ năng** thực hành để quản trị một máy chủ DHCP
- Quản trị CSDL DHCP bằng việc thực hiện các tác vụ sau: Sao lưu và khôi phục, **nén** CSDL DHCP và thống nhấn CSDL DHCP
- Giám sát CSDL DHCP bằng cách tạo và xem các nhật ký kiểm soát DHCP, tạo ra mức **hiệu năng cơ sở** DHCP, xem các thông số thống kê của phạm vi và máy chủ DHCP**,** và tạo ra các cảnh báo hiệu năng DHCP.

Sau khi bạn cài đặt và cấu hình thành công DHCP trên máy chủ Microsoft Windows Server 2003, bạn phải quản lý và giám sát những hoạt động đang diễn ra tại máy chủ đó. Hệ thống của bạn càng không ổn định (việc không ổn định có thể là kết quả của việc thêm vào, xóa bớt hoặc thay đổi mục đích sử dụng của các máy chủ) thì việc quản trị và giám sát máy chủ DHCP của bạn càng quan trọng. Độ ổn định của hệ thống mạng của bạn sẽ xác định cả tần suất của việc quản trị và giám sát máy chủ mà bạn sẽ phải làm.

Mục đích của việc quản trị và giám sát máy chủ DHCP giúp cho ta ngăn cản các sự cố, đảm bảo rằng máy chủ thực hiện đúng chức năng mà bạn đã gán cho nó và để đảm bảo rằng máy chủ thực hiện chức năng của nó ở mức hiệu năng có thể chấp nhận được. Việc giám sát máy chủ một cách hiệu quả cho phép bạn nhận biết và thực hiện các biện pháp cứu chữa xu hướng mà có thể dẫn đến việc máy chủ ngừng hoạt động hoặc giảm hiệu năng. Chương này sẽ trình bày các phương pháp mà bạn có thể quản trị và giám sát máy chủ DHCP

QUẢN TRỊ DHCP

DHCP đóng vai trò quan trọng trong cơ sở hạ tầng mạng của doanh nghiệp. Như đã bàn đến trong chương 1, "Triển khai DHCP", một doanh nghiệp sử dụng DHCP để cung cấp các thiết lập kết nối bắt buộc (Địa chỉ IP và mặt nạ mạng con). Các máy chủ DHCP cũng cung cấp các địa chỉ IP cho các tài nguyên quan trọng như máy chủ DNS và máy chủ WINS. Nếu không thể truy cập đến một máy chủ DHCP, các máy khách sẽ mất hoàn toàn kết nối

mạng. Do đó, cũng giống như các tài nguyên then chốt khác trong doanh nghiệp của bạn, bạn phải quản trị máy chủ DHCP một cách cẩn thận. Việc quản trị máy chủ DHCP một cách đúng đắn sẽ giúp bạn tránh các thời gian chết của máy chủ và hỗ trợ bạn nhanh chóng phục hồi lại sau sự cố. Bảng 2-1 sẽ liệt kê các tác vụ quản trị DHCP khi nào các tác vụ này thường xuyên tiến hành.

Bảng 2-1. Các tác vụ quản trị DHCP

Tác vụ Quản trị	Thời điểm thực hiện
Cấu hình và thay đổi Phạm vi	Tại thời điểm cài đặt hoặc khi thêm các máy khách nằm ngoài các Phạm vi hiện tại
Cấu hình và thay đổi các tùy chọn	Khi thêm hay thay đổi các máy chủ dịch vụ mạng.
Cấu hình *DHCP relay agent*	Khi thêm mạng con mới
Sao lưu CSDL DHCP	Mỗi giờ, theo mặc định
Khôi phục CSDL DHCP	Khi CSDL bị hỏng
Nén CSDL DHCP	Khi cần thiết, để tránh các ảnh hưởng do việc CSDL phát triển
Thống nhất các Phạm vi DHCP	Khi tìm thấy các xung đột

HIỂU BIẾT CÁC CẬP NHẬT DNS ĐỘNG

Windows Server 2003 DNS hỗ trợ giao thức **Cập nhật DNS Động** (RFC 2136), cho phép các máy khách DNS cập nhật động các bản ghi tài nguyên của nó trong vùng DNS. Bạn có thể chỉ định rằng máy chủ DHCP trong mạng của bạn cập nhật động DNS khi nó cấu hình các máy khách DHCP. Điều này sẽ giảm thời gian quản trị cần thiết khi quản trị thủ công các bản ghi vùng. Bạn có thể sử dụng các cập nhật động khi máy tính giải phóng hoặc cập nhật địa chỉ IP.

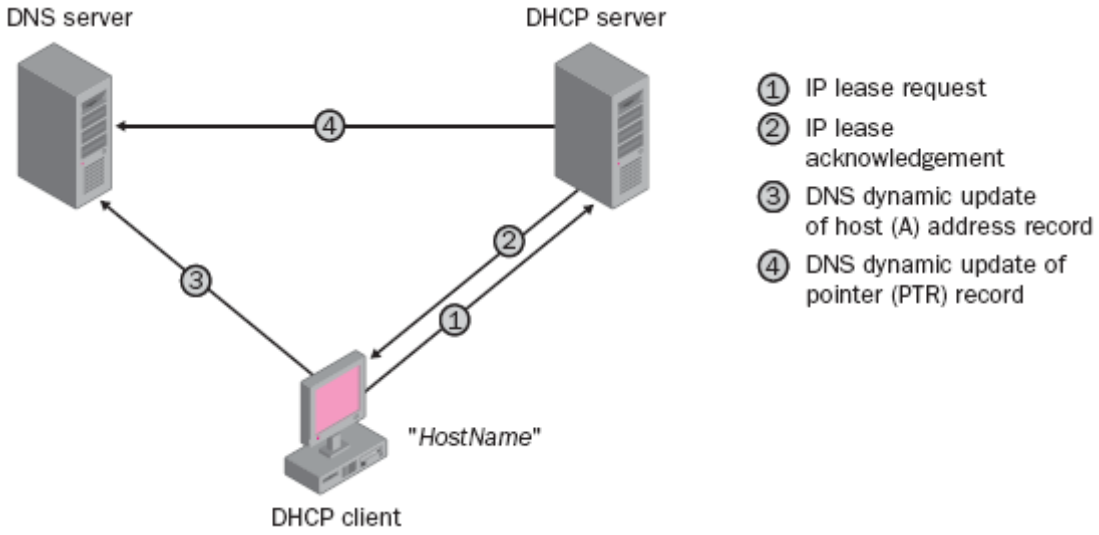
Trên máy chủ DHCP, bạn chỉ định các vùng DNS mà máy chủ DHCP này chịu trách nhiệm cập nhật tự động. Trên máy chủ DNS, bạn chỉ định máy chủ DHCP là máy tính duy nhất mà được ủy quyền để cập nhật các mục trong DNS.

Nếu bạn sử dụng nhiều máy chủ Windows Server 2003 DHCP trong mạng và bạn cấu hình các vùng của bạn để cho phép chỉ các cập nhật động bảo mật, bạn phải sử dụng ***Active Directory User And Computers*** để thêm máy chủ DHCP của bạn vào nhóm bảo mật ***DnsUpdateProxy***. Điều này cho phép máy chủ DHCP của bạn thực hiện việc cập nhật thay mặt cho các máy khách DHCP.

Bạn phải thực hiện cập nhật DNS động từ máy chủ DHCP nếu:

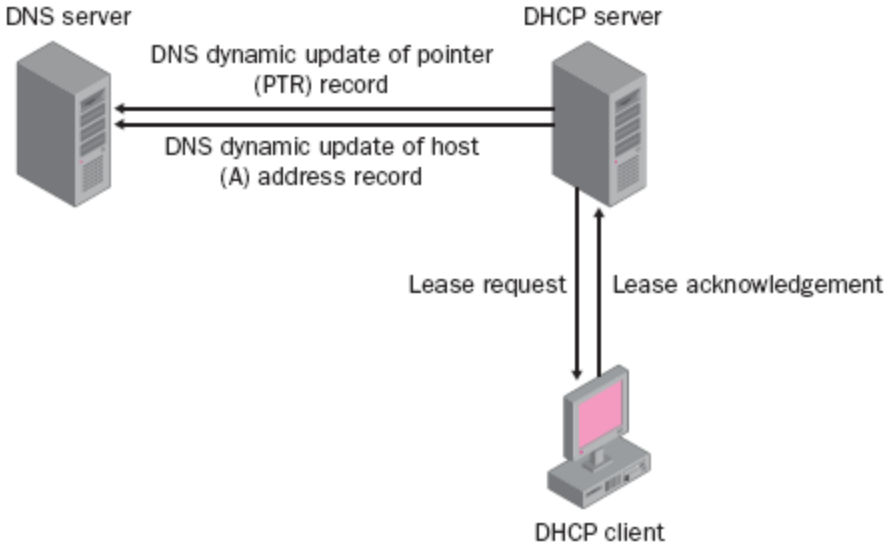
- Hệ điều hành máy khách DNS không phải là Microsoft Windows Server 2000, Microsoft Windows XP hoặc Windows Server 2003
- Việc gán các Cấp phép, cho phép mỗi máy tính, nhóm hoặc người dùng cập nhật các mục vào tương ứng trong DNS, là không thể quản lý được.
- Việc cho phép các máy khách DNS riêng lẻ cập nhật các mục vào DNS sẽ gây ra các nguy cơ bảo mật mà có thể dễ dẫn đến các máy tính không ủy quyền sẽ đóng giả các máy tính đã được ủy quyền.

Các máy khách chạy Windows 2000 hoặc cao hơn thực hiện việc cập nhật các **Bản ghi Tài nguyên Địa chỉ** (***address (A) resource records***) một cách trực tiếp, nhưng chúng lại sử dụng máy chủ DHCP để cập nhật động các **Bản ghi Tài nguyên Con trỏ (*Pointer Resource Records* - PTR)** của chúng, thể hiện trong Hình 2-1 (lưu ý rằng bước 3 và 4 có thể được đặt trước). Một bản ghi **A** phân giải tên máy sang địa chỉ IP và một bản ghi **PTR** lại phân giải địa chỉ IP sang tên máy. Khi có cả hai loại bản ghi, máy chủ DNS có thể thực hiện việc phân giải xuôi và phân giải ngược.



Hình 2-1. Quá trình cập nhật động cho các máy khách Windows 2000 hoặc các hệ điều hành sau Windows 2000.

Các máy khách sử dụng DHCP chạy các phiên bản trước đây của hệ điều hành Microsoft sẽ không thể cập nhật hoặc đăng lý các bản ghi tài nguyên DNS một cách trực tiếp. Các máy khách DHCP này phải sử dụng dịch vụ DHCP cung cấp trong Windows Server 2003 để đăng ký và cập nhật cả bản ghi tài nguyên A và bản ghi PTR. Hình 2-2 thể hiện quá trình này.



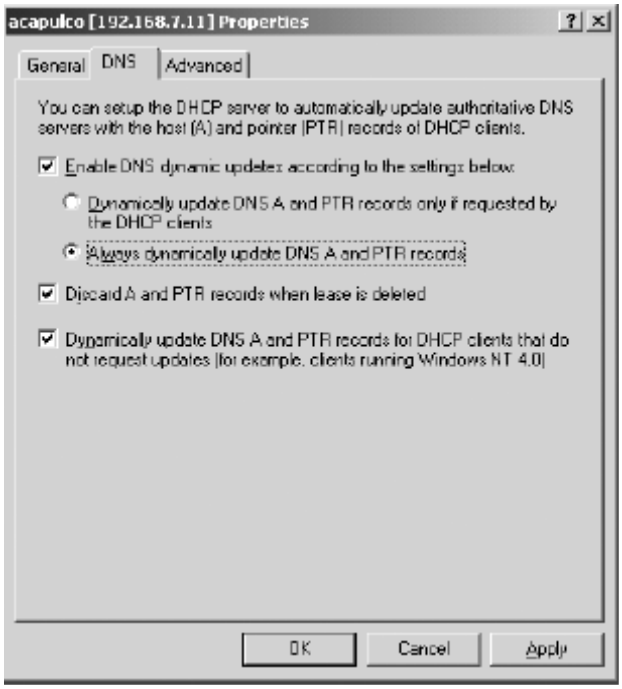
Hình 2-2. Quá trình cập nhật động cho các máy khách mà chạy hệ điều hành Microsoft trước Windows 2000.

Bạn có thể chỉnh sửa cách thực hiện mặc định này theo nhiều cách khác nhau bằng cách cấu hình các thiết lập cập nhật DNS trong máy chủ DHCP. Điều này sẽ được bàn đến trong phần tiếp sau.

Cấu hình các thiết lập cập nhật động DNS trên máy chủ DHCP

Để kích hoạt khả năng cập nhật động, trong trang thuộc tính của máy chủ DHCP, lựa chọn "***Enable DNS Dynamic Updates According To The Settings Below***" (*Kích hoạt việc cập nhật động DNS theo các thiết lập sau đây*). Lựa chọn này và lựa chọn "***Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients***" (*Cập nhật động DNS các bản ghi A và bản ghi PTR chỉ khi các máy khách DHCP yêu cầu*) đều được chọn theo mặc định. Khi các lựa chọn mặc định này được sử dụng, và máy khách DHCP yêu cầu máy chủ cập nhật bản ghi tài nguyên PTR của nó, máy chủ DHCP sẽ thực hiện chỉ yêu cầu đó. Để cấu hình máy chủ DHCP cập nhật cả bản ghi A và bản ghi PTR, sử dụng bảng điều khiển ***DHCP Manager*** để hiển thị thuộc tính của máy chủ DNS và chỉnh sửa các thiết lập trong thẻ DNS như thể hiện trong Hình 2-3. Để cập nhật DNS cho các máy khách chạy các hệ điều hành trước đây của Windows, ví dụ như Microsoft Windows 98 và Windows NT, lựa chọn "***Dynamically Update DNS A And***

PTR Records For DHCP Clients That Do Not Request Updates" (*Cập nhật động DNS các bản ghi A và bản ghi PTR cho các máy khách DHCP không yêu cầu cập nhật*), thể hiện trong Hình 2-3.



Hình 2-3. Kích hoạt máy chủ DHCP để cập nhật các bản ghi A và bản ghi PTR

> ***LƯU Ý. Cấu hình thuộc tính của phạm vi****. Các cập nhật động DNS cũng được cấu hình tại mức phạm vi bằng cách sử dụng hộp thoại* ***Scope Properties*** *hoặc cho máy khách có địa chỉ IP dành sẵn trong hộp thoại thuộc tính của địa chỉ dành sẵn đó*

Nếu bạn không thể bảo mật việc cập nhật động, bạn có thể vô hiệu hóa các cập nhật động DNS. Để không cho máy chủ DHCP thực hiện việc cập nhật động thay mặt cho các máy khách Windows 2000, Windows XP hoặc Windows Server 2003, bạn hãy bỏ lựa chọn "***Enable DNS Dynamic Updates According To The Settings Below***" (*Kích hoạt việc cập nhật động DNS theo các thiết lập sau đây*)

Thông thường, không có lý do gì để duy trì các thông tin về một máy khách DNS đã bị xóa. Lựa chọn "***Discard A And PTR Records When Lease Is Deleted***" (*Loại bỏ bản ghi DNS và bản ghi PTR khi hợp đồng bị xóa bỏ*) sẽ xóa các bản ghi tài nguyên của máy khách đó khỏi DNS khi hợp đồng thuê địa chỉ IP bị xóa.

Các thiết lập cập nhật động cuối cùng mà mà bạn có thể cấu hình trong thẻ DNS sẽ xác định liệu máy chủ DHCP có cung cấp dịch vụ cập nhật động

DNS thay mặt cho các máy khách DHCP không có khả năng thực hiện cập nhật động hay không, ví dụ như các máy tính chạy Microsoft Windows NT4. Theo mặc định, máy chủ DHCP Windows Server 2003 không thực hiện việc cập nhật động thay mặt cho các máy khách. Để kích hoạt máy chủ DHCP Windows Server 2003 thực hiện việc cập nhật động thay mặt cho các máy khách, lựa chọn "***Dynamically Update DNS A And PTR Records For DHCP Clients That Do Not Request Updates***" (*Cập nhật động DNS các bản ghi A và bản ghi PTR cho các máy khách DHCP không yêu cầu cập nhật*)

Sử dụng các cập nhật động bảo mật

Mặc dù các cập nhật động cho phép các máy khách cập nhật các bản ghi tài nguyên, đây không phải là một cách làm an toàn. Một cách bảo mật hơn để cập nhật các bản ghi tài nguyên DNS là sử dụng các cập nhật động bảo mật. Máy chủ sẽ thực hiện cập nhật nếu như máy khách có thể đưa ra thông tin nhận dạng của nó và có các thông số đúng đắn để thực hiện việc cập nhật. Việc thực hiện cập nhật động bảo mật sẽ thực hiện được chỉ thông qua dịch vụ thư mục Active Directory và khi DNS tích hợp Active Directory được kích hoạt. (Để có thêm thông tin, xem Chương 3, "Triển khai việc phân giải tên sử dụng DNS")

Cấu hình cập nhật động bảo mật. Theo mặc định, các vùng tích hợp Active Directory (***Active Directory–integrated***) sẽ cho phép sự cập nhật động bảo mật và thiết lập này có thể được chỉnh sửa khi bạn tạo ra vùng này. Nếu bạn tạo ra vùng là vùng chính tiêu chuẩn (***Standard Primary***) và sau đó chuyển đổi nó sang vùng tích hợp Active Directory, nó sẽ giữ nguyên các cấu hình cập nhật động của vùng chính tiêu chuẩn và có thể được thay đổi bằng cách sử dụng bảng điều khiển DNS.

- **Cấu hình cập nhật động bảo mật.**

  Các thao tác sau đây sử dụng bảng điều khiển DNS để xác nhận một vùng sẽ sử dụng các cập nhật động. Để khẳng định các thiết lập cập nhật động, làm theo các bước sau:

1. Trong bảng điều khiển DNS, nhấn phải chuột vào vùng mà bạn muốn cấu hình cập nhật động và lựa chọn ***Properties***
2. Trong danh sách sổ xuống ***Dynamic Updates***, xác nhận rằng ***Secure Only*** (xem Hình 2-4) được lựa chọn

Hình 2-4. Vùng DNS được cấu hình chỉ cho phép cập nhật động bảo mật

Theo mặc định, khi dịch vụ DHCP máy khách đăng ký các bản ghi tài nguyên cho một tên DNS, nó sẽ thực hiện kiểu cập nhật động chuẩn trước tiên. Nếu thao tác cập nhật động này không thành, máy khách sẽ thu xếp một cập nhật động bảo mật. Bạn có thể cấu hình các máy khách luôn luôn thực hiện cập nhật động chuẩn hoặc cập nhật động bảo mật bằng cách thêm vào trong ***registry*** mục vào ***UpdateSecurityLevel*** trong khóa con sau đây:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Giá trị của ***UpdateSecurityLevel*** có thể được thiết lập các giá trị 0, 16 hoặc 256 với các giá trị cấu hình bảo mật như sau:

- **0** Chỉ định việc sử dụng các cập nhật động bảo mật khi việc cập nhật động chuẩn bị từ chối. Đây là giá trị mặc định
- **16** Chỉ định việc chỉ sử dụng kiểu cập nhật động chuẩn
- **256** Chỉ định việc chỉ sử dụng kiểu cập nhật động bảo mật

Sử dụng Nhóm Bảo mật DnsUpdateProxy . Sử dụng các cập nhật động bảo mật có thể dẫn đến tình huống trong đó các bản ghi có thể không được cập nhật. Khi sử dụng các cập nhật động bảo mật, các máy khách đã đăng ký, và chỉ các máy khách đã đăng ký, là có thể chỉnh sửa tên đó. Ví dụ, hãy xem xét một máy chủ DHCP mà đăng ký một bản ghi cho máy khách sử dụng hệ điều hành trước Windows 2000. Sau đó, máy khách này nâng cập lên Windows XP và hiện tại có khả năng tự cập nhật bản ghi tài nguyên DNS của chính nó. Bởi vì sử dụng các cập nhật động bảo mật yêu cầu đối tượng sở hữu (trong trường hợp này là máy chủ DHCP) của bản ghi tài nguyên thực hiện việc cập nhật cho bản ghi này nên máy trạm đã nâng cấp

mới này không thể cập nhật bản ghi của chính nó. Tương tự, nếu máy chủ DHCP thứ cấp của bạn đăng ký một tên và sau đó lại ở trạng thái không kết nối (***offline***), tên đó sẽ không thể được cập nhật động nữa cho đến khi máy chủ thứ cấp đó trở lại trạng thái kết nối (***online***).

Để giải quyết vấn đề này, Active Directory trong Windows Server 2003 cung cấp một nhóm bảo mật có sẵn gọi là ***DnsUpdateProxy***. Các đối tượng được tạo ra bởi nhóm này là không bảo mật. Và do vậy, ban dầu đối tượng không có chủ sở hữu, do vậy mà máy chủ hoặc máy khách DHCP không tạo ra nó, thậm chí trong các vùng yêu cầu cập nhật bảo mật, có thể cập nhật nó. Tuy nhiên, như với mọi bản ghi khác, ngay sau khi máy chủ hoặc máy khách DHCP đầu tiên, không phải là thành viên của nhóm bảo mật ***DnsUpdateProxy***, chỉnh sửa bản ghi, máy chủ hoặc máy khách đó sẽ trở thành chủ sở hữu của bản ghi này. Tại thời điểm này, chỉ chủ sở hữu mới có thể cập nhật cho bản ghi này trong vùng mà yêu cầu cập nhật bảo mật. Do đó, nếu mọi máy chủ DHCP đăng ký các bản ghi tài nguyên cho các máy khách cũ hơn là thành viên của nhóm bảo mật này và bản thân các máy khách không phải là thành viên của nhóm này, vấn đề bàn đến trong phần trước đã được loại trừ. Để tránh các trục trặc có thể xẩy ra, bạn nên cân nhắc việc thêm các máy chủ DHCP vào trong nhóm bảo mật ***DnsUpdateProxy***.

Thêm các đối tượng máy tính vào trong nhóm bảo mật DnsUpdateProxy. Bạn có thể thêm các đối tượng máy tính vào trong nhóm bảo mật ***DnsUpdateProxy*** thông qua bảng điều khiển ***Active Directory Users and Computer***.

- **Thêm các đối tượng máy tính vào trong nhóm bảo mật DnsUpdateProxy.**

  Để thêm một máy chủ DHCP vào trong nhóm bảo mật ***DnsUpdateProxy***, thực hiện theo các bước sau:

1. Nhấn ***Start***, trỏ vào ***All Programs***, trỏ đến ***Administrative Tools*** và sau đó nhấn vào ***Active Directory Users and Computer***.
2. Mở rộng ***contoso.com*** và nhấn vào thư mục chứa ***Users***
3. Nhấn phải chuột vào ***DnsUpdateProxy*** và sau đó lựa chọn ***Properties***.
4. Trong thẻ ***Member***, nhấn ***Add***
5. Trong hộp lựa chọn ***Enter The Object Names To Select***, nhập vào tên của máy chủ thành viên hoặc máy chủ quản trị miền mà thực hiện nhiệm vụ DHCP

6. Nhấn vào ***Check Names*** và sau đó đóng trang thuộc tính bằng cách nhấn ***OK***.

LƯU Ý. Thêm các máy chủ DHCP vào trong nhóm bảo mật DnsUpdateProxy*. Nếu bạn đang sử dụng nhiều máy chủ DHCP để chống lỗi và các cập nhật động bảo mật được yêu cầu cho các vùng được các máy chủ DHCP này phục vụ, hãy chắc chắn thêm tất cả các máy chủ DHCP chạy Windows Server 2003 vào trong nhóm bảo mật* ***DnsUpdateProxy***

Các vấn đề liên quan đến bảo mật. Mặc dù việc thêm tất cả các máy chủ DHCP vào trong nhóm bảo mật có sẵn ***DnsUpdateProxy*** sẽ hỗ trợ cho một số vấn đề về việc duy trì các cập nhật động DNS, giải pháp này cũng gây nên một số nguy cơ bảo mật khác.

Ví dụ, bất kỳ tên miền DNS nào đăng ký bởi các máy tính chạy dịch vụ ***DHCP Server*** là không bảo mật. Bản ghi tài nguyên A cho máy chủ DHCP là một ví dụ của một bản ghi như thế. Để bảo vệ hệ thống khỏi nguy cơ này, bạn có thể cấu hình chỉ định một chủ sở hữu khác một cách thủ công cho bất kỳ bản ghi DNS nào gắn với máy chủ DHCP. Tuy nhiên, một vấn đề bảo mật có ý nghĩa lớn hơn sẽ xuất hiện nếu máy chủ DHCP, là thành viên của nhóm bảo mật ***DnsUpdateProxy***, lại cũng đồng thời là máy chủ quản trị miền. Trong trường hợp này, các Bản ghi Tài nguyên Định vị Dịch vụ (SRV), Bản ghi Địa chỉ Máy tính (A) và Bản ghi Tên Qui chuẩn (CNAME) được đăng ký bởi dịch vụ ***Netlogon*** cho Máy chủ Quản trị Miền là không bảo mật. Để giảm thiểu vấn đền này, bạn không nên cài đặt một máy chủ DHCP trên một máy chủ quản trị miền khi sử dụng các cập nhật bảo mật.

CẢNH BÁO. Thêm các máy chủ DHCP vào trong nhóm bảo mật DnsUpdateProxy*. Đối với Windows Server 2003, việc sử dụng các cập nhật động bảo mật có thể bị ảnh hưởng do việc chạy máy chủ DHCP trên Máy chủ Quản trị Miền khi dịch vụ DHCP được cấu hình để thực hiện các đăng ký các bản ghi DNS thay mặt cho các máy khách DHCP. Để tránh vấn đề này, hãy cài đặt các máy chủ DHCP và các máy chủ quản trị miền trên các máy tính khác nhau.*

Giải quyết sự cố cập nhật động

Trong một thời điểm nào đó, có thể bạn gặp các sự cố với các cập nhật động hay các cập nhật động bảo mật. Phần sau đây sẽ giúp bạn nhận dạng và giải quyết các sự cố cập nhật động.

Nếu các cập nhật động không đăng ký đúng tên hoặc địa chỉ IP, các thao tác sau đây sẽ giúp bạn trong việc chẩn đoán và giải quyết vấn đề:

- Kiểm tra nhật ký hệ thống trên máy trạm có các lỗi cụ thể đó.
- Bắt các máy khách làm mới các đăng ký của nó bằng cách nhập ***ipconfig /registerdns*** tại dấu nhắc dòng lệnh.
- Kiểm tra xem liệu các cập nhật động có được kích hoạt hay không đối với vùng được ủy quyền cho tên mà máy trạm thực hiện việc cập nhật
- Để **phát hiện ra qui luật cho** các sự cố **khác**, kiểm tra xem liệu các máy khách cập nhật động có liệt kê máy chủ DNS chính trong vùng là máy chủ DNS **ưa** thích của nó hay không. Để xác định máy chủ DNS ưa thích cho một máy khách, kiểm tra cấu hình địa chỉ IP trong phần thuộc tính TCP/IP của kết nối mạng trong máy khách hoặc tại giao diện dòng lệnh, nhập vào ***ipconfig /all***
- Nếu máy khách liệt kê máy chủ ưa thích không phải là máy chủ DNS chính trong vùng, các cập nhật động vẫn có thể hoạt động đúng, tuy nhiên **vẫn có** các vấn đề khác có thể gây nên sự cố, ví dụ như vấn đề về kết nối mạng giữa hai máy chủ hoặc một sự tra cứu đệ qui kéo dài đối với máy chủ **DNS** chính trong vùng.
- Nếu vùng là tích hợp Active Directory, bất kỳ máy chủ DNS **có** chứa một bản sao tích hợp Active Directory của vùng **đều** có thể thực hiện việc cập nhật.
- Kiểm tra xem liệu danh sách điều khiển truy cập (ACL) của bản ghi tài nguyên có cấu hình cho phép các cập nhật động hay không. Nếu vùng được cấu hình các cập nhật động, việc cập nhật có thể thất bại nếu các thiết lập bảo mật của bản ghi không cho phép các máy khách thực hiện việc thay đổi các bản ghi này hoặc việc cập nhật có thể không thành nếu máy khách này không sở hữu tên mà nó đang cập nhật. Để xác định liệu các cập nhật có phải thất bại vì một trong những lí do trên, kiểm tra ***Event Viewer*** trên máy khách.

Việc cho phép cập nhật động bảo mật có thể ngăn cản không cho một máy khách tạo, chỉnh sửa hoặc xóa các bản ghi tùy vào ACL cho vùng và tên đó. Theo mặc định, các cập nhật động bảo mật sẽ không cho máy khách tạo, xóa hay chỉnh sửa một bản ghi nếu như máy khách không phải là đối tượng tạo ra tên đó. Ví dụ, nếu hai máy tính có cùng một tên và cả hai đều cố gắng đăng ký tên của chúng trong DNS, việc cập nhật động có thể không thành đối với một máy khách đăng ký sau.

Nếu máy khách thất bại trong việc cập nhật tên trong vùng đã cấu hình cập nhật động bảo mật, một trong các điều kiện sau đây có thể là nguyên nhân của thất bại đó:

- Thời gian hệ thống trong máy khách DNS và thời gian hệ thống trong máy chủ DNS không được đồng bộ
- Bạn đã chỉnh sửa trong ***registry***, mục ***UpdateSecurityLevel***, ngăn cản việc sử dụng các cập nhật động bảo mật trong máy trạm
- Vùng đó bị khóa. **M**áy chủ DNS **sẽ** khóa vùng trước khi thực hiện việc chuyển vùng lớn. Khi vùng bị khóa, các máy khách không thể cập nhật tên.
- Máy khách không có đủ quyền để cập nhật bản ghi tài nguyên. Bạn có thể xác nhận điều này bằng cách kiểm tra ACL gắn với tên cập nhật. Nếu máy khách không có đủ quyền để cập nhật bản ghi tài nguyên, hãy kiểm tra xem máy chủ DHCP đăng ký tên của máy khách đó và kiểm tra xem máy chủ DHCP có phải là chủ sở hữu của đối tượng ***dnsNode*** tương ứng. Nếu thế, bạn có thể phải nghĩ đến việc đặt máy chủ DHCP trong nhóm bảo mật ***DnsUpdateProxy***. Tuy nhiên, việc sử dụng lại bất kỳ đối tượng nào đã được tạo ra bởi thành viên của nhóm bảo mật ***DnsUpdateProxy*** là không an toàn.

QUẢN TRỊ CƠ SỞ DỮ LIỆU DHCP

Hệ thống mạng của bạn liên tục thay đổi. Các máy chủ mới được thêm vào và các máy chủ cũ thay đổi vai trò của nó hoặc bị gỡ bỏ hoàn toàn ra khỏi mạng. Như đã nói trước, bởi vì hệ thống mạng của bạn liên tục thay đổi nên bạn phải giám sát và quản trị dịch vụ DHCP để đảm bảo rằng nó đáp ứng được yêu cầu của doanh nghiệp. Đặc biệt, bạn phải quản trị cơ sở dữ liệu DHCP bằng cách thực hiện các nhiệm vụ sau đây đối với CSDL:

- Sao lưu và khôi phục
- Thống nhất CSDL
- Nén CSDL
- Dỡ bỏ CSDL

CSDL DHCP là gì ?

CSDL của máy chủ DHCP là một CSDL động, đó là một kho dữ liệu lưu được cập nhật khi các máy khách DHCP được gán hoặc khi chúng giải phóng các tham số cấu hình TCP/IP. Bởi vì CSDL DHCP không phải là một CSLD phân bố giống như CSDL trong máy chủ DNS nên việc duy trì các CSDL DHCP không phức tạp bằng. DNS được lưu một cách có cấu trúc phân cấp trên rất nhiều máy chủ khác nhau mà mỗi máy chủ lưu một phần của CSDL tổng thể. Ngược lại, DHCP được lưu trong một số file trên một máy chủ.

CSDL trong máy chủ DHCP trong họ hệ điều hành Windows Server 2003 sử dụng cơ chế lưu trữ ***Joint Engine Technology*** (JET). Khi bạn cài đặt dịch vụ DHCP, các file thể hiện trong Bảng 2-2 được tạo ra một cách tự động trong thư mục ***%systemroot%\System32\Dhcp***

Bảng 2-2: các file CSDL dịch vụ DHCP

File	Mô tả
Dhcp.mdb	File CSDL DHCP máy chủ
Temp.edb	File được CSDL DHCP sử dụng như là nơi lưu tạm trong khi CSDL thực hiện việc duy trì chỉ mục. File này đôi khi xuất hiện trong thư mục *%systemroot%\System32\Dhcp* sau khi hệ thống bị lỗi.
J50.log và J50#####.log	Tệp nhật ký của tất cả các giao dịch CSDL. CSDL DHCP sử dụng các file này để khôi phục dữ liệu khi cần.
J50.chk	File *kiểm tra* chỉ ra vị trí của thông tin cuối cùng đã được ghi thành công từ file nhật ký vào CSDL. Trong kịch bản phục hồi dữ liệu, File *Kiểm tra* chỉ ra vị trí mà việc phục hồi hay thực hiện lại dữ liệu sẽ bắt đầu. File *Kiểm tra* sẽ được cập nhật sau khi dữ liệu đã được ghi thành công vào CSDL (*Dhcp.mdb*)
Res*.log	Các tệp nhật ký dự phòng sẽ được sử dụng trong trường hợp hệ thống bị thiếu khoảng trống trên đĩa

> ***CẢNH BÁO. Dỡ bỏ hoặc thay thế các file CSDL****. không nên dỡ bỏ hoặc thay thế các file* ***J50.log, J50#####.log, Dhcp.mdb*** *và* ***Dhcp.tmp****. Việc thay thế các file này có thể gây nên hậu quả là máy chủ DHCP của bạn bị lỗi.*

Không có giới hạn số lượng các bản ghi trong kho lưu trữ của máy chủ DHCP. Kích thước của CSDL tăng dần theo thời gian bởi vì các máy khách gia nhập và rời mạng. Microsoft gợi ý rằng một Máy chủ chạy dịch vụ DHCP không nên có quá 10000 máy khách và 1000 phạm vi.

Kích thước của CSDL DHCP không tỷ lệ một cách trực tiếp với số lượng các mục vào của các máy khách đang hoạt động. Theo thời gian, một số mục vào máy khách DHCP trở nên lỗi thời hoặc bị xóa mất. Không gian lưu trữ không được phục hồi lại do đó một số vùng lưu trữ vẫn không được sử dụng.

Để phục hồi lại các vùng lưu trữ không sử dụng này, CSDL DHCP sẽ được nén. Việc nén CSDL động được thực hiện trên máy chủ DHCP như là một tiến trình tự động thực hiện ở mức nền của Windows trong thời gian nghỉ hoặc sau khi CSDL được cập nhật.

Sao lưu và khôi phục cấu hình máy chủ DHCP

Các máy chủ Windows Server 2003 DHCP hỗ trợ việc sao lưu tự động và thủ công. Để cung cấp khả năng chống lỗi trong trường hợp sự cố, việc sao lưu CSDL DHCP là rất quan trọng. Điều này sẽ cho phép bạn khôi phục CSDL từ các bản sao lưu nếu như phần cứng bị hỏng. Khi bạn thực hiện sao lưu, toàn bộ CSDL DHCP sẽ được sao lưu lại, bao gồm các thành phần sau đây:

- Các phạm vi, bao gồm các siêu phạm vi và các đa phạm vi
- Các địa chỉ dành sẵn
- Các hợp đồng thuê địa chỉ
- Các lựa chọn, bao gồm lựa chọn máy chủ, lựa chọn cho phạm vi, lựa chọn cho các địa chỉ dành sẵn và các lựa chọn cho phân lớp.

> ***CẢNH BÁO. Các thông số bảo mật****. Lưu ý rằng các thông số bảo mật không nằm trong danh sách này. Không có các tiến trình sao lưu các thông số bảo mật dù là tự động hoặc thủ công. Bạn phải cấu hình lại các thông số này sau khi khôi phục CSDL DHCP.*

Tự động sao lưu CSDL DHCP

Theo mặc định, dịch vụ DHCP sẽ tự động sao lưu CSDL DHCP và các mục trong ***registry*** có liên quan vào một thư mục sao lưu trên đĩa cứng cục bộ. Quá trình này sẽ xảy ra cứ 60 phút một lần. Cũng theo mặc định, các bản sao lưu tự động sẽ được lưu vào thư mục ***%systemroot%\System32\Dhcp\Backup***. Người quản trị có thể thay đổi địa

điểm lưu bản sao lưu. Các bản sao lưu tự động chỉ sử dụng khi phục hồi tự động (việc phục hồi tự động được thực hiện bởi dịch vụ DHCP khi nó phát hiện ra có sự sai hỏng trong CSDL)

Thực hiện sao lưu CSDL thủ công.

Bạn có thể sao lưu CSDL DHCP một cách thủ công. Theo mặc định, việc sao lưu thủ công được lưu trong thư mục ***%systemroot%\System32\Dhcp\Backup***. Người quản trị có thể thay đổi địa điểm lưu các bản sao lưu này. Các bản sao lưu thủ công sẽ được khôi phục thủ công. Bạn có thể thực hiện việc sao lưu một cách thủ công CSDL DHCP trong khi dịch vụ DHCP vẫn đang chạy. Nơi lưu các bản sao lưu phải là đĩa cứng cục bộ, các đường dẫn đến máy tính ở xa là không được phép và thư mục sao lưu sẽ được tạo ra một cách tự động. (nếu như nó chưa tồn tại). Người quản trị có thể sao chép các file sao lưu DHCP sang một thiết bị lưu trữ không kết nối (***Offline***) (như băng từ hoặc đĩa)

Tự động khôi phục CSDL DHCP

Khi dịch vụ DHCP khởi động, nếu nó không thể nạp CSDL DHCP được thì nó sẽ tự động khôi phục từ thư mục chứa bản sao lưu trên đĩa cứng nội bộ. Nếu CSDL DHCP bị hỏng, người quản trị có thể lựa chọn hoặc khôi phục từ thư mục sao lưu trên đĩa cứng cục bộ hoặc nếu như không có, hệ thống sẽ khôi phục từ một thiết bị sao lưu không kết nối.

Nếu phần cứng máy chủ bị hư hỏng và không có các bản sao lưu cục bộ, người quản trị chỉ có thể khôi phục từ các thiết bị sao lưu không kết nối.

Khôi phục CSDL DHCP thủ công.

Bạn có thể khôi phục CSDL từ một thư mục sao lưu trên đĩa cứng nội bộ. Nếu việc khôi phục CSDL DHCP từ thư mục sao lưu trên đĩa cứng nội bộ là không thành, bạn phải khôi phục CSDL DHCP từ một thiết bị lưu trữ không kết nối.

- **Cấu hình đường dẫn sao lưu CSDL DHCP**

  Để cấu hình đường dẫn sao lưu CSDL DHCP, thực hiện theo các bước sau:

  1. Trong bảng điều khiển DHCP, lựa chọn máy chủ DHCP tương ứng
  2. Trong thực đơn ***Action***, nhấn vào ***Properties***
  3. Trong thẻ ***Advanced***, trong mục ***Backup Path***, nhập vào đường dẫn sao lưu tương ứng và sau đó nhấn ***OK***

- **Thực hiện sao lưu CSDL DHCP thủ công.**

  Để sao lưu CSDL DHCP một cách thủ công vào thư mục sao lưu trên đĩa cứng nội bộ, thực hiện theo các bước sau:

  1. Trong bảng điều khiển DHCP, lựa chọn máy chủ DHCP tương ứng
  2. Trong thực đơn ***Action***, lựa chọn ***Backup***
  3. Trong hộp thoại ***Browse For Folder***, lựa chọn thư mục tương ứng để lưu bản sao lưu và nhấn ***OK***

- **Khôi phục CSDL DHCP một cách thủ công**

  Để khôi phục một CSDL DHCP một cách thủ công từ thư mục sao lưu trên đĩa cứng nội bộ, thực hiện theo các bước sau:

  1. Trong bảng điều khiển DHCP, lựa chọn máy chủ DHCP tương ứng
  2. Trong thực đơn ***Action***, lựa chọn ***Restore***
  3. Trong hộp thoại ***Browse For Folder***, lựa chọn thư mục đang chứa bản sao lưu và nhấn ***OK***
  4. Trong hộp thoại DHCP, nhấn ***Yes*** để dừng và khởi động lại dịch vụ
  5. Nếu như trạng thái của dịch vụ không được cập nhật, nhấn ***F5*** để làm tươi bảng điều khiển DHCP

Thống nhất CSDL DHCP

Thống nhất là quá trình xác nhận các giá trị CSDL DHCP với các giá trị của DHCP trong ***registry***. Bạn có thể thống nhất CSDL DHCP của bạn trong các kịch bản sau đây:

- Các giá trị CSDL DHCP được cấu hình chuẩn xác tuy nhiên chúng lại không hiển thị một cách chính xác trong bảng điều khiển DHCP
- Sau khi bạn khôi phục một CSDL DHCP, nhưng CSDL DHCP mà khôi phục lại không **có** các giá trị mới nhất.

Ví dụ giả định rằng CSDL đã có của bạn bị xóa mất và bạn phải khôi phục lại một phiên bản trước đó của CSDL này. Nếu bạn khởi động DHCP và mở bảng điều khiển, bạn sẽ thấy rằng các phạm vi và lựa chọn được hiển thị, tuy nhiên các hợp đồng đang có lại không thấy đâu. Việc thống nhất sẽ phổ biến các thông tin về hợp đồng thuê của máy khách từ ***registry*** tới CSDL DHCP

Thống nhất CSDL DHCP như thế nào ?

Khi bạn thống nhất một máy chủ hoặc một phạm vi, dịch vụ DHCP sử dụng cả các thông tin tổng hợp trong ***registry*** và các thông tin chi tiết trong CSDL DHCP để tái xây dựng lại các giá trị gần nhất của dịch vụ DHCP. Bạn có thể lựa chọn để thống nhất tất cả các phạm vi trên máy chủ bằng cách lựa chọn máy chủ DHCP hoặc bạn có thể thống nhất chỉ một phạm vi bằng cách chỉ lựa chọn phạm vi tương ứng.

Trước khi sử dụng tính năng Thống nhất để xác nhận các thông tin về máy khách trong một phạm vi DHCP từ ***registry***, máy chủ cần phải đảm bảo thoả mãn các thông số sau:

- Bạn phải khôi phục lại các giá trị khóa trong ***registry*** của máy chủ DHCP hoặc chúng phải được duy trì nguyên vẹn từ lần hoạt động gần nhất trên máy chủ.

- Bạn phải tạo ra một bản sao mới của các file CSDL trong máy chủ DHCP trong thư mục ***%systemroot%\System32\Dhcp***

  - **Tạo ra một bản sao mới của CSDL máy chủ DHCP**

    Bạn có thể tạo ra một bản sao mới của CSDL máy chủ DHCP theo các bước sau:

    1. Xác nhận rằng bạn có một bản sao lưu của CSDL DHCP, bao gồm tất cả các file và các thư mục con yêu cầu
    2. Ngừng dịch vụ ***DHCP Server***
    3. Xóa tất cả các file CSDL trong đường dẫn thư mục CSDL hiện tại
    4. Khởi động lại máy chủ DHCP

    Khi ***registry*** và CSDL có thông tin phù hợp với các thông số trước, bạn có thể khởi động lại dịch vụ DHCP. Sau khi mở bảng điều khiển DHCP, bạn có thể lưu ý rằng các thông tin phạm vi hiện ra nhưng không có hợp đồng hiện tại nào hiện ra cả. Để lấy lại các hợp đồng thuê hiện tại của các phạm vi, sử dụng tính năng Thống nhất

  - **Thống nhất tất cả các phạm vi trong CSDL DHCP**

    Để thống nhất tất cả các phạm vi trong CSDL DHCP, thực hiện theo các bước sau:

    1. Trong bảng điều khiển DHCP, lựa chọn máy chủ DHCP

2. Trong thực đơn ***Action***, lựa chọn ***Reconcile All Scopes***.
3. Trong hộp thoại ***Reconcile All Scopes***, nhấn vào ***Verify***
4. Trong hộp thoại DHCP, nhấn ***OK***

■ **Thống nhất phạm vi trong CSDL DHCP**

Để thống nhất phạm vi trong CSDL DHCP, thực hiện các bước sau:

1. Trong bảng điều khiển DHCP, lựa chọn phạm vi tương ứng trong cây điều khiển
2. Trong thực đơn ***Action***, lựa chọn ***Reconcile***.
3. Trong hộp thoại ***Reconcile***, nhấn vào ***Verify***
4. Trong hộp thoại DHCP, nhấn ***OK***

Khi xem các thuộc tính của các máy khách riêng lẻ hiển thị trong danh sách các hợp đồng hiện tại, bạn có thể thấy các thông tin máy khách hiện ra không được chính xác. Khi các máy khách trong phạm vi làm mới hợp đồng thuê địa chỉ, ***DHCP Manager*** sẽ thực hiện việc chuẩn hóa và cập nhật các thông tin này.

Nén CSDL DHCP

Để lấy lại không gian lưu trữ không sử dụng, CSDL DHCP cần phải được nén. Windows Server 2003 nén động CSDL trong một chu trình tự động ở mức nền của hệ điều hành trong thời gian nghỉ sau khi cập nhật CSDL. Mặc dù việc nén động này giảm thiểu nhu cầu của việc thực hiện việc nén khi không kết nối, nó sẽ không hoàn toàn thay thế được điều này. Việc nén khi không kết nối sẽ lấy lại các không gian một cách hiệu quả hơn. Bạn nên thực hiện điều này ít nhất một lần trong một tháng đối với một hệ thống mạng lớn không ổn định với 1000 hoặc nhiều hơn các máy khách DHCP. Đối với các mạng nhỏ hơn, việc nén thủ công sẽ yêu cầu thực hiện chỉ một lần trong vài tháng.

Windows Server 2003 có sẵn tiện ích ***Jetpack.exe***, nó sẽ nén thủ công các ***CSDL DHCP*** và ***CSDL Jet*** khác (ví dụ như WINS). Sử dụng ***Jetpack.exe*** để nén ***CSDL Jet*** một cách định kỳ khi nào mà CSDL tăng trưởng lớn hơn 30MB hoặc nhiều hơn. Như đã đề cập đến trong phần trước, đối với Windows Server 2003, dịch vụ DHCP thực hiện việc nén động đối với CSDL trong máy chủ DHCP khi máy chủ này đang hoạt động trên mạng. Điều này sẽ làm giảm, nhưng không loại trừ, nhu cầu sử dụng ***Jetpack.exe*** để nén CSDL khi không kết nối.

Xem xét các lệnh sau đây khi sử dụng với ***Jetpack.exe***:

jetpack dhcp.mdb tmp.mdb

Cú pháp của lệnh này như sau:

Jetpack.exe <database name> <temp database name>

Khi dùng lệnh này, ***Jetpack.exe*** sử dụng ***Tmp.mdb*** để nén. ***Tmp.mdb*** là một CSDL tạm thời mà được ***Jetpack.exe*** sử dụng khi nén ***DHCP.mdb***. ***DHCP.mdb*** là một file CSDL DHCP. ***Jetpack.exe*** sẽ nén CSDL DHCP bằng cách sao chép các thông tin CSDL vào ***Tmp.mdb***, xóa file CSDL DHCP gốc ***DHCP.mdb*** và sau đó đổi tên file CSDL tạm thời thành tên của file gốc, ***DHCP.mdb***

Kích hoạt khả năng phát hiện xung đột dựa trên máy chủ

Máy chủ Windows Server 2003 DHCP cung cấp khả năng phát hiện xung đột dựa trên máy chủ, nó sẽ ***ping*** một địa chỉ IP trước khi gán nó cho một máy khách để đảm bảo rằng địa chỉ IP này không đang được sử dụng. Windows Server 2003, Windows XP và Windows 2000 sẽ tự động xác nhận rằng địa chỉ IP mà đề xuất bởi máy chủ DHCP sẽ có thể dùng được trước khi chấp nhận nó, do đó việc phát hiện xung đột là rất hữu ích chỉ cho các máy khách sử dụng hệ điều hành trước Windows 2000. Tính năng Phát hiện Xung đột dựa trên Máy chủ có thể được kích hoạt trong thẻ ***Advance*** của trang thuộc tính của máy chủ DHCP. Để tránh các lưu lượng mạng không cần thiết, hãy để nó trong trạng thái bị vô hiệu hóa trừ khi việc cấp trùng địa chỉ IP cho các máy khách sử dụng hệ điều hành trước Windows 2000 xảy ra nhiều lần.

Dỡ bỏ vai trò của máy chủ DHCP

Việc dỡ bỏ vai trò DHCP từ một máy chủ còn được gọi là *giáng cấp*. Khi bạn dỡ bỏ DHCP, các file DHCP sẽ bị xóa khỏi máy chủ, trừ các file chương trình đang được sử dụng. Để xoa bỏ các file chương trình này, bạn phải khởi động lại hệ thống.

- **Dỡ bỏ vai trò DHCP**

  Để dỡ bỏ hoặc gỡ cài đặt DHCP, thực hiện theo các bước sau:

  1. Trong thực đơn ***Start***, nhấn vào ***Manage Your Server***
  2. Trong trang ***Manage Your Server***, nhấn vào ***Add Or Remove A Role***.
  3. Trong trang ***Preliminary***, nhấn ***Next***,

4. Trong trang ***Server Role***, trỏ vào máy chủ DHCP và sau đó nhấn ***Nex***t.
5. Trong trang ***Role Removal Confirmation***, nhấn vào ***Remove The DHCP Server Role*** và sau đó nhấn ***Next***
6. Trong trang DHCP ***Server Role Removed***, nhấn ***Finish***

Thực hành quản trị một CSDL DHCP

Khi sao lưu và khôi phục CSDL DHCP, hãy áp dụng các bài thực hành sau đây:

■ Sao lưu thủ công CSDL DHCP vào một nơi nào đó khác *%systemroot%\System32\Dhcp\Backup*, đó là thư mục mặc định cho việc sao lưu tự động. Nếu bạn lưu một bản sao lưu CSDL DHCP, mà được tạo ra một cách thủ công, trong cùng thư mục với bản sao được tạo ra bởi cách tự động, dịch vụ DHCP sẽ không hoạt động một cách đúng đắn.

■ Duy trì một bản sao của CSDL DHCP mà đã sao lưu **không kết nối** (ví dụ giữ một bản sao trên băng từ hoặc đĩa). Bởi vì dịch vụ DHCP tự động sao lưu một bản sao của CSDL DHCP vào một thư mục trên đĩa cứng nội bộ, bạn có thể mất cả CSDL DHCP gốc và bản sao CSDL DHCP nếu như phần cứng máy chủ bị hỏng.

GIÁM SÁT CSDL DHCP

Giám sát dịch vụ DHCP yêu cầu bạn thu thập và xem các dữ liệu về dịch vụ DHCP. Bạn cần phải giám sát cả các máy khách DHCP và máy chủ DHCP. Bạn cũng có thể phải giám sát các dịch vụ liên quan, ví dụ như DNS và WINS. Phần này sẽ tập trung vào các vấn đề phát sinh khi giám sát máy chủ DHCP

Thiết lập mức hiệu năng cơ sở (*Performance Baseline*)

Giám sát hiệu năng của máy chủ DHCP một cách hiệu quả yêu cầu việc xác định mức hiệu năng chấp nhận được và không chấp nhận được của một máy chủ DHCP. Để nhận biết sớm việc hiệu năng DHCP giảm đột ngột, bạn phải nhận biết trạng thái "bình thường" của hiệu năng DHCP. Nhận biết mức hiệu năng bình thường trong hệ thống và máy chủ DHCP của bạn yêu cầu bạn phải thiết lập một mức hiệu năng cơ sở. Mức hiệu năng cơ sở là mức hiệu năng hệ thống mà bạn quyết định rằng nó còn chấp nhận được. Bạn nên thiết lập hoặc tạo ra mức hiệu năng cơ sở khi máy chủ đang chạy với mức tải điển hình. Khi bạn có mức hiệu năng cơ sở, việc nhận biết các vấn đề hiệu năng là rất dễ dàng bởi vì bạn có thể so sánh qui luật của các tài nguyên then

chốt khi chúng hiện đang hoạt động với giá trị của mức hiệu năng cơ sở. Sự sai lệch đáng kể khỏi mức hiệu năng cơ sở thường chứng tỏ rằng hệ thống có vấn đề.

Mức hiệu năng cơ sở cũng rất có giá trị khi bạn lập kế hoạch cho việc thay đổi và bổ sung cho hệ thống mạng. Sử dụng mức hiệu năng cơ sở và các dữ liệu thu thập được theo thời gian sẽ cho phép bạn ước tính được thông lượng của một máy chủ DHCP dựa trên một lượng người dùng nhất định. Dựa trên dữ liệu giám sát DHCP, bạn có thể tính toán được kết quả của việc bổ sung thêm người dùng và ước tính được các tài nguyên bổ sung cần thiết nếu có.

Khi giám sát một máy tính được cấu hình thành một máy chủ DHCP, bạn phải xem xét các chức năng khác mà máy chủ này phải đảm nhiệm như sau:

- Liệu nó có phải là một máy chủ quản trị miền, máy chủ file và in ấn hoặc máy chủ thư điện tử bên cạnh vai trò một máy chủ DHCP hay không ?
- Mức sử dụng tổng thể của tài nguyên máy chủ là bao nhiêu ? Các vai trò bổ sung của máy chủ DHCP ảnh hưởng đến hiệu năng tổng thể của máy chủ này như thế nào?
- Xem xét thời gian trong ngày mà bạn thu thập dữ liệu: Liệu nó có phải trong thời điểm nhiều người dùng đăng nhập nhất (mức đỉnh)
- Các chu trình đã được lập lịch khác ví dụ như sao lưu, có chạy vào cùng thời điểm ?
- Bao nhiêu người dùng truy cập máy chủ mà sử dụng chức năng khác ngoài DHCP trong khi bạn đang thu thập dữ liệu cho mức **hiệu năng cơ sở** của bạn.

Dịch vụ DHCP sử dụng các phân hệ bộ nhớ, bộ vi xử lý, đĩa và mạng. Mặc dù các phân hệ này là quan trọng với dịch vụ DHCP để nó hoạt động một cách tối ưu, bạn còn có thể có được nhiều thuận lợi hơn nữa nếu bạn giám sát hiệu năng của các phân hệ mạng.

Nơi chứa dữ liệu về DHCP

Bốn công cụ cung cấp dữ liệu về DHCP: Bảng điều khiển DHCP, Nhật ký Kiểm soát DHCP, ***Event Viewer*** và ***bảng điều khiển Performance***. Mỗi công cụ cung cấp các thông tin như mô tả trong Bảng 2-3

Bảng 2-3: Các công cụ dữ liệu DHCP

Công cụ	Mô tả	Ví dụ về các thông tin được cung cấp
Bảng điều khiển DHCP	Sử dụng bảng điều khiển DHCP để hiển thị các thông số thống kê của máy chủ DHCP. Các số liệu có thể được thu thập tại mức Máy chủ hay mức Phạm vi kể từ khi dịch vụ DHCP khởi động lần cuối	■ Thời gian dịch vụ DHCP khởi động hay dừng ■ Số địa chỉ IP có trong phạm vi ■ Số các hợp đồng thuê địa chỉ hiện có trong Phạm vi ■ Số các máy khách đang sử dụng dịch vụ
DHCP audit log/Event Viewer	Hai công cụ nay thực hiện cùng một chức năng. Chúng cung cấp các thông tin về các sự kiện DHCP. Thông tin bao gồm các sự kiện xẩy ra hoặc trong hệ thống hoặc trong ứng dụng mà cần thông báo với người dùng hay cần ghi thêm vào nhật ký.	■ Khi dịch vụ khởi động hay dừng, và do ai thực hiện ■ Các lỗi dịch vụ DHCP ■ Các sự ủy quyền dịch vụ DHCP
Performance console	Công cụ này cung cấp các dữ liệu hiệu năng DHCP. Dịch vụ DHCP bao gồm một tập các biến đếm hiệu năng mà quản trị mạng có thể sử dụng để theo dõi nhiều hoạt động khác nhau của máy chủ	■ Số các hợp đồng được làm mới trong một khoảng thời gian cho trước ■ Số các gói tin DHCPACK hay DHCPNACK trong một khoảng thời gian cho trước ■ Dung lượng đĩa CSDL DHCP sử dụng ■ Số địa chỉ IP xung đột

Sử dụng các thông số thống kê DHCP để giám sát máy chủ DHCP

Các thông số thống kê bao gồm các dữ liệu thu thập được ở mức máy chủ hoặc mức phạm vi kể từ lần khởi động gần đây nhất của dịch vụ DHCP.

Các thông số thống kê cung cấp một cách nhìn thời gian thực mà bạn có thể sử dụng để kiểm tra trạng thái của máy chủ DHCP hoặc các phạm vi. Bạn có thể lấy các thông số thống kê của riêng một phạm vi hoặc ở mức máy chủ, ở mức này sẽ thể hiện các giá trị trung bình của tất cả các phạm vi mà máy chủ quản lý.

Sử dụng bảng điều khiển DHCP, bạn có thể xem các thông số thống kê DHCP cho một máy chủ hoặc một phạm vi như liệt kê trong bảng 2-4.

Bảng 2-4: các thông số thống kê DHCP

Các thông số thống kê DHCP	Mô tả	Các thông số thống kê Máy chủ	Các thông số thống kê Phạm vi
Start Time	Thời điểm dịch vụ DHCP khởi động	X	
Up Time	Thời gian dịch vụ DHCP hoạt động	X	
Discovers	Số các thông điệp DHCPDISCOVER máy khách mà máy chủ đã nhận được	X	
Offers	Số các thông điệp DHCPOFFER đã gửi	X	
Requests	Số các thông điệp DHCPREQUEST nhận được	X	
Acks	Số các thông điệp DHCPACK đã gửi	X	
Nacks	Số các thông điệp DHCPNACK đã gửi	X	
Declines	Số các thông điệp DHCPDECLINE đã nhận	X	
Releases	Số các thông điệp DHCPRELEASE đã nhận	X	
Total Scopes	Tổng số các Phạm vi trên máy chủ DHCP	X	
Total Addresses	Tổng số các địa chỉ IP được cấu hình cho máy khách	X	X
In Use	Tổng số các địa chỉ IP hiện đang được thuê	X	X
Available	Tổng số các địa chỉ IP còn lại có thể cho thuê	X	X

Xem các thông số thống kê DHCP

Bạn có thể xem các thông số thống kê DHCP cho cả máy chủ và phạm vi. Để xem các thông số thống kê của DHCP một cách dễ dàng nhất, bạn có thể cấu hình cho phép các thông số thống kê của máy chủ DHCP được làm tươi một cách tự động, điều này cho phép các thông số thống kê của phạm vi DHCP được làm tươi một cách tự động.

- **Cấu hình tự động làm tươi các thông số thống kê DHCP.**

  Để cấu hình tự động làm tươi các thông số thống kê DHCP, thực hiện theo các bước sau:

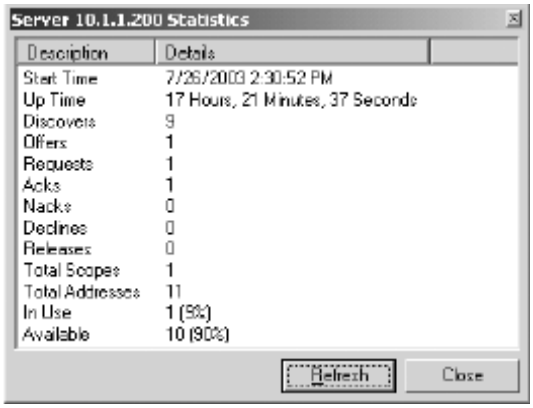
  1. Trong bảng điều khiển DHCP lựa chọn máy chủ DHCP tương ứng.
  2. Trong thực đơn ***action***, nhấn vào ***properties***.

3. Trong thẻ ***general*** lựa chọn hộp chọn ***Automatically Update Statistics Every***, cấu hình các trường ***Hours*** và ***minute*** tướng ứng và sau đó nhấn ***OK***

■ **Xem các thống số thống kê của máy chủ DHCP**

Để xem các thống số thống kê của máy chủ DHCP, thực hiện theo các bước sau:

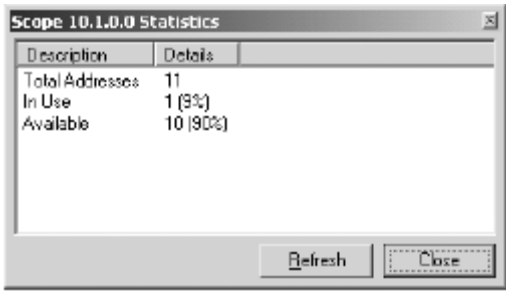
1. Trong bảng điều khiển DHCP lựa chọn máy chủ DHCP tương ứng.
2. Trong thực đơn ***Action***, lựa chọn ***Display Statistics***. Hình 2-5 hiện ra.



Hình 2-5: các thông số thống kê Máy chủ DHCP

■ **Xem các thông số thống kê của phạm vi DHCP**

1. Trong bảng điều khiển DHCP, lựa chọn phạm vi DHCP tương ứng
2. Trong thực đơn ***Action***, lựa chọn ***Display Statistics***. Hình 2-6 hiện ra.



Hình 2-6: Các thông số thống kê Phạm vi DHCP

Sử dụng các nhật ký kiểm soát DHCP để giám sát máy chủ DHCP

Ghi nhật ký dữ liệu máy chủ DHCP cho phép bạn thu thập các thông tin về dịch vụ ***DHCP Server*** khi nó hoạt động trong mạng. Bạn có thể xem các file nhật ký theo từng ngày để biết các thông tin hoặc bạn có thể thu thập các file nhật ký trên các máy chủ riêng biệt để phân tích dữ liệu máy chủ DHCP trong một khoảng thời gian dài. Các thông tin này rất hữu ích khi quyết định bổ sung thêm các máy chủ DHCP hoặc khi giải quyết các sự cố của máy chủ DHCP. Một điều rất quan trọng là bạn phải hiểu các chu trình nhật ký kiểm soát bởi vì có nhiều khi việc ghi nhật ký bị dừng lại và các file nhật ký có thể bị ghi đè. Việc hiểu về các chu trình này sẽ cho phép bạn thu thập các thông tin thống kê DHCP cần thiết để duy trì hiệu năng tối ưu cho máy chủ DHCP của bạn.

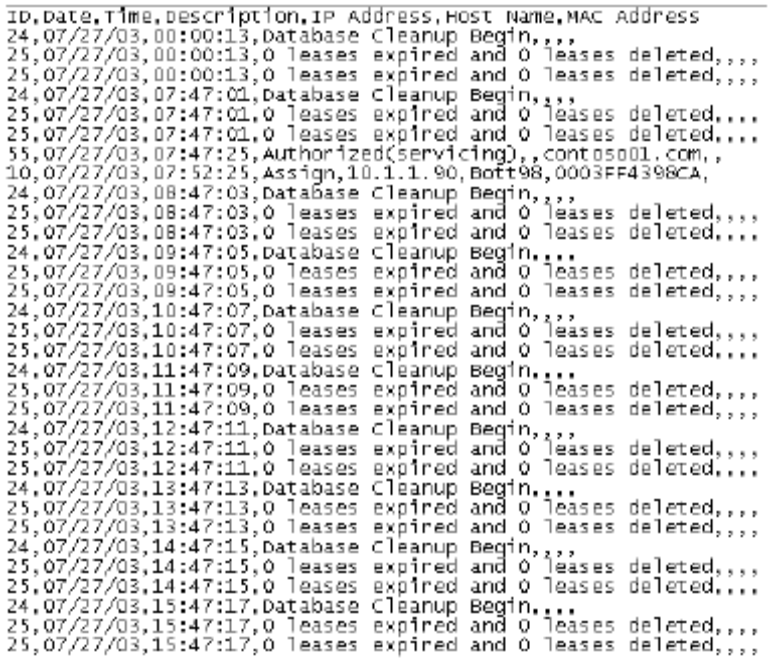
Nhật ký kiểm soát DHCP cho phép người quản trị có thể thu thập các sự kiện DHCP hàng ngày. Nhật ký kiểm soát DHCP cung cấp cho bạn các thông tin mà bạn có thể cần cho giám sát máy chủ DHCP của bạn. Bạn có thể sử dụng nhật ký kiểm soát DHCP để xem các hoạt động trong một ngày cụ thể nào đó hoặc bạn có thể thu thập các nhật ký để phân tích các hoạt động của máy chủ DHCP trong một khoảng thời gian dài.

File nhật ký kiểm soát DHCP

Một file nhật ký kiểm soát DHCP là một nhật ký các sự kiện liên quan đến dịch vụ, ví dụ các sự kiện sau:

- Khởi động và dừng dịch vụ
- Xác nhận việc ủy quyền
- Cấp phát, làm mới và từ chối địa chỉ IP

Khi bạn kích hoạt tính năng ghi nhật ký, máy chủ DHCP sẽ tạo ra các file nhật ký tên là ***DhcpSrvLog-day.log***, trong đó ***day*** là ba ký tự viết tắt thể hiện ngày mà nhật ký được tạo ra; ví dụ một nhật ký được tạo ra trong ngày Chủ nhật sẽ có tên ***DhcpSrvLog-Sun.log***. Máy chủ DHCP lưu các file này trong thư mục CSDL DHCP. Hình 2-7 thể hiện một file nhật ký mẫu



```
ID,Date,Time,Description,IP Address,Host Name,MAC Address
24,07/27/03,00:00:13,Database Cleanup Begin,,,,
25,07/27/03,00:00:13,0 leases expired and 0 leases deleted,,,,
25,07/27/03,00:00:13,0 leases expired and 0 leases deleted,,,,
24,07/27/03,07:47:01,Database Cleanup Begin,,,,
25,07/27/03,07:47:01,0 leases expired and 0 leases deleted,,,,
25,07/27/03,07:47:01,0 leases expired and 0 leases deleted,,,,
55,07/27/03,07:47:25,Authorized(servicing),,contoso01.com,,
10,07/27/03,07:52:25,Assign,10.1.1.90,Bott98,0003FF4398CA,
24,07/27/03,08:47:03,Database Cleanup Begin,,,,
25,07/27/03,08:47:03,0 leases expired and 0 leases deleted,,,,
25,07/27/03,08:47:03,0 leases expired and 0 leases deleted,,,,
24,07/27/03,09:47:05,Database Cleanup Begin,,,,
25,07/27/03,09:47:05,0 leases expired and 0 leases deleted,,,,
25,07/27/03,09:47:05,0 leases expired and 0 leases deleted,,,,
24,07/27/03,10:47:07,Database Cleanup Begin,,,,
25,07/27/03,10:47:07,0 leases expired and 0 leases deleted,,,,
25,07/27/03,10:47:07,0 leases expired and 0 leases deleted,,,,
24,07/27/03,11:47:09,Database Cleanup Begin,,,,
25,07/27/03,11:47:09,0 leases expired and 0 leases deleted,,,,
25,07/27/03,11:47:09,0 leases expired and 0 leases deleted,,,,
24,07/27/03,12:47:11,Database Cleanup Begin,,,,
25,07/27/03,12:47:11,0 leases expired and 0 leases deleted,,,,
25,07/27/03,12:47:11,0 leases expired and 0 leases deleted,,,,
24,07/27/03,13:47:13,Database Cleanup Begin,,,,
25,07/27/03,13:47:13,0 leases expired and 0 leases deleted,,,,
25,07/27/03,13:47:13,0 leases expired and 0 leases deleted,,,,
24,07/27/03,14:47:15,Database Cleanup Begin,,,,
25,07/27/03,14:47:15,0 leases expired and 0 leases deleted,,,,
25,07/27/03,14:47:15,0 leases expired and 0 leases deleted,,,,
24,07/27/03,15:47:17,Database Cleanup Begin,,,,
25,07/27/03,15:47:17,0 leases expired and 0 leases deleted,,,,
25,07/27/03,15:47:17,0 leases expired and 0 leases deleted,,,,
```

Hình 2-7: Ví dụ của File nhật ký kiểm soát DHCP

File nhật ký là các file văn bản phân tách bởi dấu phẩy có chứa các mục vào nhật ký thể hiện trong một dòng văn bản đơn. Một file nhật ký kiểm soát DHCP bao gồm các trường thể hiện trong Bảng 2-5.

Bảng 2-5: các trường của file nhật ký kiểm soát DHCP

Trường	Mô tả
ID	Mã nhận dạng sự kiện DHCP server
Date	Ngày sự kiện được ghi vào nhật ký
Time	Thời gian sự kiện được ghi vào nhật ký
Description	Mô tả của sự kiện
IP Address	Địa chỉ IP của máy khách DHCP
Host Name	Tên của máy khách DHCP
MAC Address	Địa chỉ MAC của cạc mạng máy khách

Các file nhật ký kiểm soát của máy chủ DHCP sử dụng các mã sự kiện ID dành riêng để cung cấp thông tin về kiểu của sự kiện máy chủ hoặc các hành động đã được ghi lại. Bảng 2-6 mô tả các mã sự kiện DHCP mà có thể xuất hiện trong file nhật ký

Bảng 2-6: Mã nhận dạng sự kiện DHCP và các mô tả tương ứng

Sự kiện	Mô tả
00	Khởi tạo việc ghi nhật ký.
01	Dừng việc ghi nhật ký.
02	Việc ghi nhật ký tạm dừng do thiếu không gian đĩa.
10	Máy khách thuê địa chỉ IP mới.
11	Máy khách làm mới hợp đồng thuê.
12	Máy khách chấm dứt hợp đồng thuê.
13	Địa chỉ IP được phát hiện là đang được sử dụng trên mạng.
14	Yêu cầu thuê không được thỏa mãn do vùng địa chỉ cho thuê của Phạm vi đã cạn.
15	Hợp đồng thuê bị từ chối.
20	Máy khách thuê địa chỉ BOOTP

Nhật ký kiểm soát DHCP làm việc như thế nào

Chu trình sau đây mô tả cách thức mà nhật ký kiểm soát khởi động, thực hiện và kết thúc trong một ngày 24 giờ:

1. Một file nhật ký mới được tạo ra khi một trong các sự kiện sau đây xảy ra: Máy chủ DHCP khởi động hoặc thời gian cục bộ vượt qua 12:00 A.M
2. Tùy thuộc vào liệu file nhật ký kiểm soát đã từng được tạo ra trong 24 giờ trước hay chưa, các hành động sau đây xảy ra:
   a) Nếu như file đã tồn tại trước đó mà không bị sửa chữa trong khoảng thời gian hơn 1 ngày, nó sẽ bị ghi đè
   b) Nếu như file đã tồn tại nhưng đã bị sửa chữa trong vòng 24 giờ trước, nó không bị ghi đè. Thay vào đó, các hoạt động mới sẽ được ghi tiếp vào cuối file đã có đó. Đây là trường hợp mà hoặc hệ thống hoặc dịch vụ DHCP Server bị khởi động lại.
3. Máy chủ sẽ ghi một thông điệp tiêu đề vào trong file nhật ký kiểm soát, thể hiện rằng việc ghi nhật ký đã khởi động.
4. Trong quá trình ghi nhật ký kiểm soát, máy chủ DHCP thực hiện rất nhiều việc kiểm tra ổ đĩa logic để đảm bảo rằng không gian đĩa sử dụng bởi nhật ký vẫn còn trong giới hạn đã thiết lập trong ***registry***. Kiểm tra đĩa được thực hiện vào các thời điểm có sự kiện hoặc khi đồng hồ máy tính chỉ 12:00 A.M. theo mặc định, các đĩa sẽ được coi là đầy khi dung lượng đĩa trống là dưới 20 MB hoặc file nhật ký kiểm soát hiện tại có dung lượng lớn hơn 1/7 của không gian đĩa tối đa đã phân chia cho tổng

kích thước của tất cả các file nhật ký kiểm soát lưu trong máy tính. Không gian tối đa theo mặc định là 70 MB

5. Nếu việc kiểm tra đĩa cho thấy đĩa đã bị đầy, việc ghi nhật ký sẽ bị ngừng lại nhưng việc kiểm tra đĩa vẫn còn tiếp tục. Nếu có nhiều hơn không gian đĩa được giải phóng và có thể sử dụng, việc ghi nhật ký sẽ lại tiếp tục.
6. Vào 12:00 A.M, file nhật ký ngày hiện tại được đóng lại và quá trình ghi nhật ký sẽ bắt đầu lại

> ***LƯU Ý. Giữ các file nhật ký lâu hơn 7 ngày****. Để giữ các thông tin nhật ký kiểm soát trong khoảng thời gian lâu hơn một tuần, hãy chuyển các file nhật ký kiểm soát đó khỏi thư mục trước khi file nhật ký của tuần tới có thể ghi đè nó.*

■ **Kích hoạt và cấu hình việc ghi nhật ký kiểm soát DHCP**

Để kích hoạt và cấu hình việc ghi nhật ký kiểm soát DHCP, thực hiện theo các bước sau:

1. Trong bảng điều khiển DHCP, lựa chọn máy chủ DHCP tương ứng
2. Trong thực đơn ***Action***, lựa chọn ***Properties***
3. Trong thẻ ***Genera***l, xác nhận rằng tùy chọn ***Enable DHCP Audit Logging*** được lựa chọn
4. Trong thẻ ***Advance***, trong trường ***Audit Log File Path***, nhập vào đường dẫn của file nhật ký kiểm soát tương ứng và sau đó nhấn ***OK***
5. Trong hộp thoại DHCP, nhấn ***Yes*** để ngừng và khởi động lại dịch vụ.

Xem nhật ký kiểm soát DHCP

Do nhật ký kiểm soát DHCP được kích hoạt theo mặc định, ngay sau khi DHCP được cài đặt và cấu hình, bạn có thể xem các nhật ký kiểm soát DHCP để xem các thông tin mà bạn cần để giám sát máy chủ DHCP của bạn. Sử dụng Windows Explorer, tìm đến thư mục nơi mà bạn lưu file nhật ký kiểm soát, nhấn đúp vào file nhật ký tương ứng đó.

> ***LƯU Ý. Các file nhật ký của dịch vụ DHCP được lưu ở đâu****. Theo mặc định, dịch vụ DHCP lưu các file nhật ký kiểm soát của nó trong thư mục **%systemroot%\System32\Dhcp**. Một file nhật ký kiểm soát chứa các ID của sự kiện và nghĩa của chúng trong file. Các nhật ký kiểm soát được đặt tên theo mẫu **DhcpSrvLog-day.log** trong đó day*

là ba ký tự viết tắt của ngày trong tuần. Ví dụ, file nhật ký kiểm soát cho ngày thứ Tư sẽ là ***DhcpSrvLog-Wed.log***

Sử dụng bảng điều khiển Performance để giám sát DHCP

Có một tiện ích quản trị gọi là ***bảng điều khiển Performance***, bạn có thể sử dụng để giám sát hiệu năng của máy chủ DHCP. Khi bạn mở ***bảng điều khiển Performance***, bảng này sẽ có một cây gồm hai nút. Nút đầu tiên là ***System Monitor*** và nút thứ hai là ***Performance Logs And Alerts***

System Monitor (Giám sát hệ thống)

Bạn có thể thêm các đối tượng và biến đếm hiệu năng vào bất kỳ kiểu nào trong ba màn hình đồ họa: Đồ thị, biểu đồ và báo cáo. Để xem các cách này một cách riêng lẻ, nhấn phải chuột vào cách xem mà bạn muốn và nhấn vào ***New Window From Here***. Bạn có thể xem các dữ liệu đã được ghi lại. Nếu bạn thêm vào một một biến đếm mà có nhiều hơn một trường hợp riêng, bạn sẽ có khả năng lựa chọn biến đếm cho từng trường hợp riêng. Ví dụ, nếu như máy tính của bạn đang giám sát có hai giao tiếp mạng, khi bạn lựa chọn đối tượng hiệu năng ***Network Interface***, bạn có thể lựa chọn một hoặc cả hai giao tiếp mạng này để giám sát. Một đối tượng hiệu năng là một tập hợp logic của các biến đếm mà gắn với một tài nguyên hoặc dịch vụ mà có thể giám sát được. Một biến đếm hiệu năng là một mục dữ liệu mà gắn với một đối tượng hiệu năng. Đối với mỗi biến đếm được lựa chọn, ***System Monitor*** hiển thị giá trị tương ứng với một khía cạnh cụ thể nào đó của hiệu năng mà đã định nghĩa cho đối tượng hiệu năng đó. Một ***performance object instance*** (*trường hợp riêng của đối tượng hiệu năng*) là một thuật ngữ sử dụng để phân biệt các đối tượng hiệu năng của cùng một kiểu trong máy tính.

Các biến đếm hiệu năng thông thường. Bảng 2-7 cung cấp một mẫu các biến đếm hiệu năng thông dụng, đi kèm với lời giải thích về ý nghĩa dữ liệu của các dữ liệu này (Đối tượng hiệu năng là máy chủ DHCP)

Bảng 2-7: Các Biến dếm Hiệu năng thông dụng

Performance Counter	**Dữ liệu được thu thập**	**Ý nghĩa của dữ liệu**	**Việc cần theo dõi sau khi thiết lập mức hiệu năng cơ sở**
Packets received/ second	Số các gói thông điệp máy chủ DHCP đã nhận trong một giây	Giá trị này lớn chứng tỏ các lưu thông liên quan đến DHCP tới máy	Theo dõi các sự tăng giảm đột ngột của tham số này có thể phát hiện được nguyên nhân gây

		chủ là nặng	nên tải DHCP lớn, chẳng hạn như mất kết nối…
Requests/ second	Số các thông điệp yêu cầu thuê địa chỉ DHCP máy chủ nhận trong một giây	Việc tăng đột ngột hay không bình thường của tham số này chứng tỏ có một số lượng lớn các máy khách tiến hành làm mới hợp đồng thuê. Nó có thể chỉ ra rằng thời hạn hợp đồng thuê đã được cấu hình cho Phạm vi là quá ngắn	Theo dõi việc tăng hay giảm đột ngột của tham số này có thể giúp ta phát hiện nguyên nhân, như mất kết nối mạng…
Active queue length	Chiều dài hàng đợi hiện tại của các thông điệp DHCP. Đây cũng chính là số các thông điệp chưa được máy chủ DHCPxử lý.	Giá trị lớn của tham số này chứng tỏ máy chủ DHCP không đáp ứng được với các tải hiện tại	Theo dõi việc tăng đột ngột hay liên tục sẽ phát hiện được việc tăng tải trên hệ thống hay khả năng của máy chủ bị giảm.
Duplicates dropped/second	Số các gói tin trùng lặp mà máy chủ loại bỏ trong một giây	Số này có thể bị ảnh hưởng do có nhiều *DHCP relay agents* hay giao tiếp mạng cùng gửi một gói tin đến máy chủ. Giá trị lớn của tham số này chứng tỏ máy chủ đáp ứng không đủ nhanh hay ngưỡng thời gian khởi động của *relay agen* không đặt dủ lớn.	Theo dõi biến đếm này đối với bất kỳ hành động nào có hơn một yêu cầu được các *Relay Agent* thay mặt cho máy khách gửi tới máy chủ. Giá trị lớn của biến đếm này chứng tỏ ngưỡng thời gian đặt tại máy khách là quá ngắn, hay máy chủ đáp ứng không đủ nhanh

Tạo các cảnh báo hiệu năng trong DHCP

Các biến đếm có thể sử dụng cho đối tượng hiệu năng máy chủ DHCP cũng được sử dụng trong việc tạo ra các cảnh báo. Nếu bạn biết mức chấp nhận được mà một biến đếm có thể cao hoặc thấp hơn trước khi sự cố xảy đến, bạn có thể tạo ra một cảnh báo để đồng thời thông báo cho bạn và chạy một chương trình hoặc kịch bản. Cảnh báo là tính năng phát hiện khi biến đếm định nghĩa trước có giá trị vượt quá hoặc thấp hơn một mức thiết lập cụ thể. Thiết lập cụ thể cho một biến đếm là mức ngưỡng cảnh báo. Ví dụ, nếu mức hiệu năng cơ sở của độ dài hàng đợi hoạt động DHCP luôn luôn thấp hơn 3, thiết lập một mức ngưỡng cảnh báo có giá trị 6 hoạc 7. Một sự tăng đột ngột trong độ dài hàng đợi hoạt động DHCP có thể cho bạn biết rằng mức tải yêu cầu đang quá nhiều đối với máy chủ DHCP này.

Kinh nghiệm thực tiễn khi tạo ra các cảnh báo DHCP

Khi bạn tạo ra các cảnh báo cho máy chủ DHCP, thực hiện theo các gợi ý đề xuất như sau:

- Định nghĩa mức chấp nhận được mà một biến đếm DHCP có thể vượt quá hoặc thấp hơn trước khi tạo ra một cảnh báo. Để làm điều này, bạn ghi nhật ký biến đếm DHCP trong một khoảng thời gian xác định để tạo ra mức **hiệu năng cơ sở**. Sử dụng mức **hiệu năng cơ sở** này, bạn có thể tìm hiểu chắc chắn khoảng hoạt động thông thường của một biến đếm DHCP cho trước và sau đó tạo ra các cảnh báo để thông báo cho bạn khi hoạt động của biến đếm DHCP này nằm ngoài khoảng hoạt động thông thường.

- Sử dụng các *scripts* (kịch bản) với các cảnh báo. Sử dụng lệnh *Nesh* của DHCP trong các kịch bản để **đáp** ứng lại cảnh báo

> ***THÔNG TIN THÊM. Sử dụng lệnh Nesh**. Để có nhiều thông tin thêm về cách sử dụng lệnh **Nesh**, xem trong **Microsoft Knowledgebase** bài viết 242468 "Làm thế nào để sử dụng công cụ **Nesh.exe** và các khóa chuyển dòng lệnh". Để tìm kiếm bào viết này, hãy truy cập trang http://support.microsoft.com và nhập vào số của bài viết trong hộp thoại **Search The Knowledge Base***

Kinh nghiệm thực tiễn khi giám sát DHCP

Xem xét các bài thực hành hữu ích sau đây khi giám sát hiệu năng của một máy chủ DHCP

- Tạo ra mức hiệu năng cơ sở cho dữ liệu hiệu năng trên máy chủ DHCP. Bạn có thể so sánh mức **hiệu năng cơ sở** với các biến **đếm** mà có thể cho

biết liệu máy chủ DHCP có đang quá tải hay không hoặc mạng đang gửi quá nhiều các yêu cầu DHCP đến máy chủ

- Kiểm tra các biến đếm chuẩn dùng để đo hiệu năng máy chủ (như mức sử dụng bộ vi xử lý, trang bộ nhớ, hiệu năng đĩa và mức sử dụng mạng). Bởi vì DHCP thường được cài đặt trong một máy chủ mà đồng thời có các dịch vụ hoặc ứng dụng khác, việc phải hiểu tổng mức tải của tất cả các ứng dụng và dịch vụ trên máy chủ và cách thức mà mức tải trên máy chủ ảnh hưởng đến hoạt động của dịch vụ *DHCP Server* như thế nào.

- Quan sát các biến đếm máy chủ DHCP, ví dụ như *Acks/sec*, để tìm kiếm sự suy giảm hoặc tăng đáng kể thể hiện sự thay đổi trong lưu lượng DHCP. Một sự tăng đột ngột các hoạt động có thể do việc thêm các máy khách DHCP hoặc nó có thể cho thấy sự thay đổi thời hạn thuê ngắn hơn. Một sự giảm đột ngột trong các hoạt động có thể cho thấy thời hạn thuê đã dài hơn, một sự cố trong mạng đã làm cho các yêu cầu DHCP không được truyền đi, hoặc máy chủ DHCP có sự cố khi xử lý các yêu cầu DHCP.

SỬ DỤNG VIỆC CẤP ĐỊA CHỈ IP RIÊNG MỘT CÁCH TỰ ĐỘNG (APIPA)

Như đã nói đến trong Chương 1, "Triển khai DHCP", Việc cấp Địa chỉ IP Riêng một cách Tự động (APIPA) là một tính năng đánh địa chỉ IP cho các mạng đơn giản mà chỉ chứa một đoạn mạng đơn. Bất cứ khi nào máy tính chạy Windows Server 2003 đươc cấu hình để lấy IP tự động và không có một máy chủ DHCP nào hoặc không có cấu hình thay thế, máy tính sẽ sử dụng APIPA để gán cho chính nó một địa chỉ riêng trong dải từ 169.254.0.1 đến 169.254.255.254

Để xác định rằng liệu APIPA hiện có đang được kích hoạt và hoạt động hay không, nhập vào ***ipconfig /all*** tại dấu nhắc dòng lệnh. Dữ liệu văn bản hiện ra cho biết địa chỉ IP và các thông tin khác. Nếu như dòng ***Autoconfiguration Enabled*** hiện giá trị ***Yes*** và địa chỉ IP trong dải từ 169.254.0.1 đến 169.254.255.254, APIPA đang hoạt động

Tính năng cấp địa chỉ tự động chỉ làm việc trên các máy tính trong một đoạn mạng đơn mà không thể lấy được địa chỉ IP bằng các phương pháp khác. Nếu máy chủ DHCP sau đó hoạt động trở lại và một máy khách trước đó đã tự được gán địa chỉ APIPA, nó sẽ thay đổi địa chỉ IP của nó sang một địa chỉ IP mà được cấp từ máy chủ DHCP. Các máy tính sử dụng địa chỉ APIPA chỉ có thể trao đổi với các máy tính cũng sử dụng địa chỉ APIPA trong cùng một

đoạn mạng, chúng không thể kết nối trực tiếp từ Internet. Lưu ý rằng mặc dù sử dụng APIPA, bạn không thể cấu hình một máy tính với địa chỉ máy chủ DNS, địa chỉ cổng ra mặc định hoặc một địa chỉ máy chủ WINS. Nếu bạn muốn một máy tính lấy địa chỉ tự động nhưng muốn chỉ định một địa chỉ khi mà không tìm thấy một máy chủ DHCP nào, bạn có thể chỉ định nó sử dụng cấu hình thay thế. Để có thêm thông tin về cấu hình thay thế, xem trong Chương 1 ”Triển khai DHCP”

APIPA có trong các máy tính chạy Windows 98, Microsoft Windows Millennium Edition (Me), Windows 2000, Windows XP và Windows Server 2003.

Vô hiệu hóa APIPA

Nếu bạn muốn đảm bảo rằng APIPA không được sử dụng, bạn có thể cấu hình một địa chỉ thay thế trong thuộc tính của địa chỉ IP của kết nối hoặc vô hiệu hóa tính năng địa chỉ tự động bằng cách chỉnh sửa lại ***registry***. Lưu ý rằng để vô hiệu hóa APIPA cho một giao tiếp mạng và vô hiệu hóa APIPA cho tất cả các giao tiếp mạng, bạn phải chỉnh sửa các khóa khác nhau trong ***registry***.

- **Vô hiệu hóa APIPA trong một giao tiếp đơn.**

  Để vô hiệu hóa APIPA trên một giap tiếp mạng bằng cách chỉnh sửa ***registry***, thực hiện theo các bước sau:

1. Sử dụng trình soạn thảo registry ***regedit.exe*** để thêm mục vào ***IPAutoconfigurationEnabled*** với giá trị 0 (kiểu dữ liệu REG_DWORD) trong khóa con sau đây:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\interface

2. Khởi động lại máy tính

- **Vô hiệu hóa APIPA trên nhiều giao tiếp mạng**

  Để vô hiệu hóa APIPA trên nhiều giao tiếp mạng bằng cách chỉnh sửa ***registry***, thực hiện theo các bước sau:

1. Thiết lập giá trị của ***IPAutoconfigurationEnabled*** là 0 (kiểu dữ liệu REG_DWORD) trong khóa con sau đây:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

2. Khởi động lại máy tính

Giải quyết sự cố APIPA

Đối với các máy tính chạy bất kỳ phiên bản nào của hệ điều hành Windows từ Windows 98 trở đi, địa chỉ APIPA là địa chỉ mặc định. Điều đó có nghĩa là chúng được gán cho các máy tính mà các cấu hình mạng của chúng chưa được thay thế kể từ khi hệ điều hành được cài đặt. Trong một hệ thống mạng nhỏ hơn, bạn có thể muốn để các máy tính với các địa chỉ IP mặc định này để đơn giản hóa việc giao tiếp trên mạng và quản trị. Nếu thế, bạn có thể chạy lệnh ***ipconfig /all*** trên các máy tính nối mạng để xác định liệu địa chỉ gán cho mỗi máy tính trong mạng nội bộ có nằm trong khoảng địa chỉ APIPA từ 169.254.0.1 đến 169.254.255.254 hay không.

Nếu như lệnh ***ipconfig /all*** không trả kết quả cho bạn một địa chỉ APIPA, kết quả đầu ra sẽ cho biết một trong ba tình huống sau: không địa chỉ và không có thông báo lỗi nào, một địa chỉ toàn zero hoặc một địa chỉ IP không phải toàn zero mà nằm ngoài dải địa chỉ APIPA

Khi không có địa chỉ IP nào được gán cho một máy tính, một thông báo lỗi có thể cung cấp cho ta biết nguyên nhân cụ thể. Ví dụ, kết quả đầu ra của ***ipconfig /all*** có thể thông báo với bạn rằng phương tiện (cách gọi khác là dây cáp mạng) đã bị ngắt kết nối. Tại thời điểm này, bạn có thể kiểm tra dây nối mạng và chạy lệnh ***ipconfig /renew*** để lấy địa chỉ IP bằng tính năng APIPA. Nếu cách này không thể cấp cho bạn một địa chỉ IP mới, bạn nên tiến hành chẩn đoán sự cố phần cứng như lỗi cáp mạng, hub hoặc switch.

Thỉnh thoảng kết quả của lệnh ***ipconfig /all*** không cung cấp một nguyên nhân rõ ràng cho việc lấy địa chỉ IP không thành của một máy tính. Nếu thế, có thể dự đoán sự cố là do giao tiếp mạng. Xác nhận rằng máy tính có phần cứng giao tiếp mạng được cài đặt tốt, cùng với trình điều khiển thiết bị tương ứng có phiên bản mới nhất. sau đó chạy lệnh ***ipconfig /renew*** để cố gắng lấy địa chỉ IP một lần nữa. Nếu sự cố vẫn còn, bạn nên tiến hành chẩn đoán các phần cứng.

Một địa chỉ toàn zero thông thường có nghĩa là TCP/IP đã khởi tạo thành công trên máy tính nhưng chưa lấy được địa chỉ từ máy chủ DHCP. Ví dụ, nếu máy tính của bạn đã lấy thành công địa chỉ IP từ máy chủ DHCP và bạn nhập vào ***ipconfig /release*** để giải phóng địa chỉ này, địa chỉ IP sẽ hiện ra là 0.0.0.0

Đối với các máy tính hoạt động tốt trong một mạng mà không chủ định sử dụng APIPA cho cấu hình mạng, chúng ta mong muốn địa chỉ nhận được sẽ không phải toàn zero và đồng thời nằm ngoài dải APIPA. Ví dụ thông thường của kiểu địa chỉ này bao gồm một loạt các địa chỉ IP dành sẵn của

LANA cho các hệ thống mạng riêng (từ 10.0.0.0 đến 10.255.255.255, từ 172.16.0.0 đến 172.31.255.255 và từ 192.168.0.0 đến 192.168.255.255)

TỔNG KẾT

- Bạn có thể cấu hình DHCP để cập nhật động DNS. Nếu bạn lựa chọn cập nhật động các bản ghi tài nguyên DNS, bạn nên xem xét sử dụng các cập nhật động bảo mật.
- Bởi vì DHCP là một thành phần quan trọng trong hệ thống của bạn, bạn phải quản trị và giám sát nó
- Việc quản trị DHCP bao gồm việc sao lưu và khôi phục CSDL cũng như thống nhất, **nén** và trong một số trường hợp, dỡ bỏ CSDL
- Bạn có thể giám sát DHCP bằng cách sử dụng *Performance Monitor*, các file nhật ký kiểm soát DHCP, *Event Viewer* và các thông số thống kê máy chủ và phạm vi DHCP
- APIPA là rất hữu ích cho việc cung cấp các địa chỉ cho một mạng đơn không có máy chủ DHCP

BÀI TẬP

***QUAN TRỌNG. Hoàn thành tất cả các bài tập**. Nếu bạn có kế hoạch làm các bài tập trong sách lý thuyết trong chương này, bạn phải làm tất cả các bài tập trong chương để cho máy tính trở lại trạng thái gốc của nó trước khi làm các bài tập trong sách BÀI TẬP THỰC HÀNH. Lưu ý rằng các bài tập sau đâ yêu cầu cài đặt DNS và DHCP, đó là trạng thái của máy tính học viên sau khi hoàn thành Bài tập Thực hành 1 trong sách BÀI TẬP THỰC HÀNH*

Bài tập 2-1: Cấu hình cập nhật DNS động

Để cấu hình cập nhật động DNS, thực hiện theo các bước sau:

1. Mở bảng điều khiển DNS
2. Nhấn phải chuột vào vùng mà bạn muốn cấu hình cập nhật DNS động, và lựa chọn ***Properties***
3. Trong thẻ ***General,*** trong danh sách ***DNS Updates***, lựa chọn ***Nonsecure And Secure*** và sau đó nhấn ***OK***

Bài tập 2-2: Thực hiện sao lưu CSDL DHCP thủ công

Để sao lưu CSDL DHCP trong máy chủ nguồn, hoàn thành các bước sau:

1. Mở bảng điều khiển DHCP

2. Trong bảng điều khiển, lựa chọn máy chủ DHCP mà bạn muốn sao lưu
3. Trong thực đơn ***Action***, lựa chọn ***Backup***. Hộp thoại ***Browse For Folder*** mở ra.
4. Lựa chọn thư mục sẽ chứa bản sao lưu CSDL DHCP và sau đó nhấn OK
5. Bạn phải lựa chọn đĩa cứng nội bộ để chọn thư mục lưu bản sao lưu CSDL DHCP

Bài tập 2-3: Thống nhất một CSDL DHCP

Để thống nhất CSDL DHCP, thực hiện theo các bước sau:

1. Mở bảng điều khiển DHCP
2. Thực hiện một trong các bước sau đây và sau đó nhấn ***Verify***:
    a. Để thống nhất một phạm vi xác định, lựa chọn phạm vi đó và nhấn ***Reconcile***
    b. Để thống nhất tất cả các phạm vi, phải chuột vào máy chủ DHCP và sau đó nhấn ***Reconcile All Scopes***
3. Nếu việc thống nhất thành công, một hộp thoại DHCP xuất hiện nói rằng CSDL đã ở trong trạng thái thống nhất.

Bài tập 2-4: Thực hiện sắp xếp gọn một CSDL DHCP thủ công

Để nén một CSDL DHCP một cách thủ công, thực hiện theo các bước sau:

1. Tại máy chủ DHCP, mở cửa sổ dấu nhắc lệnh
2. Để chuyển đến thư mục DHCP, tại dấu nhắc dòng lệnh, nhập vào "***cd %systemroot%\system32\dhcp"*** và sau đó nhấn ***Enter***
3. Để ngừng dịch vụ DHCP, tại dấu nhắc lệnh, nhập vào: ***net stop dhcpserver***, sau đó nhấn ***Ente***r
4. Để nén CSDL DHCP, tại dấu nhắc dòng lệnh, nhập vào "***jetpack dhcp.mdb"*** và sau đó nhấn ***Enter***
5. Một thông báo hiển thị trạng thái bao lâu nó sẽ thực hiện xong việc nén CSDL, rằng CSDL được di chuyển từ file tạm sang ***dhcp.mdb*** và sau đó quá trình kết thúc thành công.
6. Để khởi động dịch vụ DHCP, tại dấu nhắc dòng lệnh, nhập vào "***net start dhcpserver"*** rồi nhất ***Enter***

Bài tập 2-5: Cấu hình và xem các nhật ký kiểm soát DHCP

Để cấu hình và xem các nhật ký kiểm soát DHCP, thực hiện theo các bước sau:

1. Mở bảng điều khiển DHCP
2. Trong bảng điều khiển, chọn máy chủ DHCP mà bạn muốn kích hoạt tính năng nhật ký kiểm soát
3. Trong thực đơn ***Action***, lựa chọn ***Properties***
4. Trong thẻ ***General***, lựa chọn hộp chọn ***Enable DHCP Audit Logging*** và nhấn ***OK***
5. Trong thẻ ***Advance***, trong hộp ***Audit Log File Path***, nhập vào ***c:\textbook\exercises\chapter02***.
6. Bạn sẽ được hỏi liệu bạn có muốn khởi động dịch vụ DHCP để áp dụng các thay đổi này không. Lựa chọn ***Yes***
7. Duyệt đến thư mục ***c:\textbook\exercises\chapter02*** và nhấn đúp chuột vào file ***DhcpSrvLog-day.log*** (trong đó day là 3 ký tự viết tắt của ngày tạo ra bản nhật ký này)

Bài tập 2-6: Tạo ra các Cảnh báo cho một máy chủ DHCP

Để tạo ra cảnh báo cho máy chủ DHCP, thực hiện theo các bước sau:

1. Trong bảng điều khiển hiệu năng, trong mục ***Performance Logs And Alerts***, lựa chọn ***Alerts***
2. Trong thực đơn ***Action***, nhấn vào ***New Alert Settings***
3. Trong hộp thoại ***New Alert Settings***, trong hộp ***Name***, nhập vào ***DHCP Renew Alert*** và sau đó nhấn ***OK***
4. Trong Thẻ ***General***, trong hộp thoại ***DHCP Renew Alert***, trong trường ***Comment***, nhập vào ***Alert When DHCP Client Renews IP Lease***, sau đó nhấn ***Add***
5. Trong hộp thoại ***Add Counters,*** trong trường ***Performance Object***, lựa chọn máy chủ DHCP và biến đếm ***Acks/sec***, sau đó nhấn ***Close***
6. Trong thẻ ***General***, trong hộp thoại ***DHCP renew Alert***, trong trường ***Interval***, nhập vào ***5***
7. Trong thẻ ***Action***, lựa chọn ***Send A Network Message To,*** và nhập vào ***Administrator***
8. Khi cảnh báo được kích hoạt, một hộp thoại sẽ hiện ra

9. Trong thẻ ***Schedule***, trong mục ***Start Scan***, xác nhận rằng ***Manually*** (***Using The Shortcut Menu***) được lựa chọn và sau đó nhấn ***OK***

CÁC CÂU HỎI TỔNG KẾT

1. Bạn có một máy khách Windows NT 4 trong đó bạn muốn kích hoạt tính năng cập nhật động. Bạn muốn máy chủ DHCP tự động cập nhật cả bản ghi A và bản ghi PTR. Bạn phải làm gì để hoàn thành việc này?
   a) Không làm gì cả. Việc cập nhật các bản ghi A và bản ghi PTR sẽ được thực hiện theo mặc định
   b) Trong thẻ DNS của hộp thoại thuộc tính máy chủ DHCP, lựa chọn ***Dynamically Update DNS A And PTR Records For DHCP Clients That Do Not Request Updates***.
   c) Tại thẻ DNS trong hộp thoại ***DHCP server properties***, lựa chọn ***Always Dynamically Update DNS A And PTR Records***
   d) Đăng ký máy khách như là một máy tính động với máy chủ DHCP
2. Bạn không chỉnh sửa các thiết lập mặc định cho DNS trên máy chủ hay máy khách DHCP. Bản ghi máy khách nào sau đây mà máy chủ DHCP sẽ cập nhật trong DNS (Giả định rằng các máy khách đều chạy Windows XP)
   a) Bản ghi tài nguyên PTR
   b) Bản ghi tài nguyên A
   c) Cả hai Bản ghi tài nguyên PTR và A
   d) Không phải Bản ghi tài nguyên PTR hay A
3. Đối với một vùng mà bạn chỉ cho phép cập nhật động bảo mật, bạn cấu hình máy chủ DHCP để thực hiện việc cập nhật động thay mặt cho các máy khách Windows NT 4. Các thiết lập DNS động khác trên máy chủ DHCP có các giá trị mặc định. Sau khi bạn nâng cấp máy khách lên Windows XP, bạn thấy rằng bản ghi tài nguyên A không còn được cập nhật nữa. Bạn giải thích điều này như thế nào ?
4. Đúng hay Sai: Nếu một vùng DNS chỉ chấp nhận các cập nhật động bảo mật và máy chủ DHCP là thành viên của nhóm bảo mật ***DnsUpdateProxy***, các bản ghi tài nguyên tạo ra bởi dịch vụ ***Netlogon*** cho máy chủ quản trị miền có phải là không bảo mật hay không ? Giải thích câu trả lời.
5. Việc sao lưu tự động và thủ công CSDL DHCP được thực hiện thành công. Bạn muốn khôi phục lại các đối tượng sau đây: Tất cả các phạm vi,

các dành sẵn, các hợp đồng thuê, các lựa chọn và các thông số bảo mật. Bạn phải làm gì ?

a) Khôi phục từ bản sao lưu tự động

b) Khôi phục từ bản sao lưu thủ công

c) Khôi phục từ bản sao lưu không kết nối

d) Khôi phục từ bản sao lưu tự động hoặc thủ công, sau đó cấu hình lại các thông số bảo mật một cách thủ công

6. Bạn vừa hoàn thành việc khôi phục một CSDL DHCP. Bạn khởi động bảng điều khiển DHCP đẻ xác nhận việc khôi phục là thành công. Bạn thấy rằng phạm vi và lựa chọn đều hiển thị, tuy nhiên các hợp đồng hiện tại lại không hiện ra. Bạn nên làm gì để các bản hợp đồng hiện tại này hiện ra?

   a) Việc khôi phục là không thành. Thực hiện khôi phục lại một lần nữa

   b) Việc khôi phục là không thành bởi vì bản sao lưu bị hỏng. Tìm một bản sao lưu tốt và sử dụng nó để thực hiện khôi phục lại CSDL DHCP

   c) Sử dụng bảng điều khiển DHCP, thực hiện việc thống nhất CSDL

   d) Xóa file ***Tmp.mdb*** và sau đó khởi động lại dịch vụ DHCP

7. Bạn đang giám sát một máy chủ DHCP và bạn muốn lưu các nhật ký kiểm soát mà được tạo ra trong thứ Ba tuần trước. Hôm nay là thứ Hai. Bạn phải làm gì ?

   a) Không làm gì cả; máy chủ DHCP tự động lưu các nhật ký sau khi ghi vào nó.

   b) Xóa bỏ các file nhật ký khỏi thư mục

   c) Thay đổi địa điểm lưu của file nhật ký

   d) Vào thứ Tư, ngừng và khởi động lại dịch vụ DHCP Server

8. Bạn muốn xác định bao nhiêu địa chỉ IP có khả năng sử dụng để cho thuê trong tất cả các phạm vi. Công cụ nào mà bạn sử dụng để thực hiện điều đó ?

   a) Nhật ký sự kiện hệ thống

   b) Các thông số thống kê phạm vi DHCP

   c) Các thông số thống kê máy chủ DHCP

   d) Nhật ký kiểm soát DHCP

CÁC KỊCH BẢN TÌNH HUỐNG

Kịch bản tình huống 2-1: Giám sát các yêu cầu DHCP

Bạn đang giám sát hoạt động của máy chủ DHCP bằng cách sử dụng ***System Monitor***. Bạn đã từng xem biến đếm ***Discovers/sec***. Bạn quan sát thấy sự tăng đột ngột số lượng các yêu cầu DHCP. Nguyên nhân nào sau đây có thể giải thích việc tăng đột ngột này?

a. Một lượng lớn máy khách đang khởi tạo một cách đồng thời và đang cố gắng tìm kiếm máy chủ DHCP

b. Một lượng lớn máy khách đang tắt một cách đồng thời và đang giải phóng các địa chỉ IP mà chúng đã thuê

c. Thời hạn của các hợp đồng phạm vi quá ngắn, gây ra việc tăng các thông điệp DHCPACK

d. Hai máy chủ DHCP đã được cài đặt trong mạng và đang truy vấn dịch vụ thư mục để tìm kiếm gốc của hệ thống.

Kịch bản tình huống 2-2: Giám sát lưu lượng DHCP trên mạng

Gần đây, người dùng hay phàn nàn rằng hệ thống mạng chậm vào các thời điểm khác nhau trong tuần. Bạn nghi ngờ rằng lưu lượng DHCP quá lớn là một phần của nguyên nhân. Khi lưu lượng DHCP tăng nhiều hơn thông thường, bạn muốn có một cảnh báo về điều này. Làm thế nào để bạn có thể làm điều này ?

CHƯƠNG 3: THỰC HIỆN VIỆC PHÂN GIẢI TÊN BẰNG DNS

Sau khi hoàn thành chương này, bạn có khả năng:

- Mô tả các quá trình của việc phân giải tên và lý do tại sao nó lại quan trọng với doanh nghiệp của bạn
- Cài đặt và cấu hình Hệ thống tên miền (***Domain Name System*** – DNS)
- Mô tả và cấu hình các vùng chính (***Primary Zone***), vùng thứ cấp (***Secondary Zone***), vùng ***in-addr.arpa*** và vùng cụt (***Stub Zone***)
- Tạo một vùng tích hợp Active Directory (***Integrated Active Directory Zone***) và giải thích lợi điểm của việc tạo ra vùng này này
- Mô tả các dạng khác nhau của máy chủ DNS và chức năng mà chúng thực hiện
- Giải thích lợi ích của việc ủy quyền cho một vùng và tạo một vùng được ủy quyền
- Mô tả quá trình chuyển giao vùng

Chương này giới thiệu các khái niệm cơ bản liên quan đến việc phân giải tên DNS trong Microsoft Windows Server 2003. Chương này cũng đồng thời giải thích các khái niệm DNS then chốt, ví dụ như Không gian Tên DNS, các Vùng DNS, các dạng Máy chủ DNS, các Bản ghi Tài nguyên DNS và việc phân giải tên DNS. Đồng thời, chương này còn thảo luận về quá trình cấu hình các máy chủ DNS, các kiểu và chu trình truy vấn DNS và sự chuyển tiếp. Bởi vì DNS đóng vai trò then chốt trong Windows Server 2003 nên việc hiểu kỹ càng các khái niệm, chu trình và phương pháp cấu hình nó là điều rất quan trọng. Nếu không có DNS, hệ thống mạng của bạn có thể không hoạt động đúng chức năng, các máy trạm thậm chí không thể phân giải được từ tên sang địa chỉ IP. Hơn nữa, các máy khách sử dụng dịch vụ thư mục Active Directory lại dùng DNS để định vị các máy chủ quản trị miền nên việc bạn hiểu rõ các khái niệm DNS then chốt và cách thức để cấu hình DNS một cách đúng đắn cho hệ thống mạng của bạn là yếu tố quyết định.

TỔNG QUAN VỀ QUÁ TRÌNH PHÂN GIẢI TÊN

Đối với các thiết bị mạng, ví dụ như các máy tính hoặc các máy in, để giao tiếp với nhau trên Internet hoặc trong nội bộ hệ thống mạng của doanh nghiệp, chúng phải có khả năng định vị được nhau. Trong hệ thống mạng Windows Server 2003, phương tiện chính để định vị các thiết bị mạng và dịch vụ mạng là thông qua việc sử dụng DNS

Ví dụ, để máy tính A giao tiếp được với máy tính B bằng giao thức TCP/IP, máy tính A phải có được địa chỉ IP của máy tính B. Quá trình tìm kiếm một địa chỉ IP cho một tên máy tính nào đó (ví dụ máy tính A) được gọi là quá trình phân giải tên. Việc phân giải tên sử dụng DNS và WINS (Hệ thống tên Internet của Windows) là các chu trình phần mềm riêng biệt của việc chuyển đổi giữa các tên, mà để cho người dùng dễ nhớ, và các địa chỉ IP số hóa, tuy khó khăn hơn cho người dùng nhưng lại cần thiết cho việc truyền thông bằng TCP/IP.

TỔNG QUAN VỀ DNS

Trước khi ARPANET phát triển thành hệ thống mà ngày nay chúng ta gọi là Internet, các file văn bản sẽ thực hiện việc phân giải tên. Các file văn bản liệt kê tên của các máy và địa chỉ IP tương ứng của nó (file ***HOSTS.txt***). Bất cứ khi nào một máy được thêm vào mạng, file HOSTS.txt này được cập nhật với tên và địa chỉ IP của máy đó. Theo lịch đều đặn, các người dùng ARPANET sẽ tải về và sử dụng file ***HOSTS.txt*** được cập nhật này. Bởi vì file ***HOSTS.txt*** này là file có cấu trúc phẳng (***flat***) nên tất cả các tên máy trong file này là duy nhất. Không có phương pháp nào để tạo ra các không gian tên ví dụ như các miền

Một vấn đề khác là kích thước của CSDL và sự bất lực trong việc phân phối mức tải khi rất nhiều máy tính cùng truy cập file này. Các file ***HOSTS.txt*** liệt kê tất cả các máy có trong mạng, điều này có nghĩa là mỗi máy tính phân tích file ***HOSTS.txt*** sẽ dành 100% công việc để phân giải các tên máy khách sang địa chỉ IP. Rõ ràng điều này là không hiệu quả và một hệ thống phân giải tên tốt hơn đã được phát minh ra.

Năm 1984, khi số lượng các máy trong mạng ARPANET đạt đến 1000, DNS đã được giới thiệu. Bởi vì DNS được thiết kế như một CSDL phân tán với cấu trúc có phân cấp, nó có thể đóng vai trò là nền tảng cho việc phân giải tên các máy trong một mạng TCP/IP kích thước bất kỳ, bao gồm cả Internet. Khả năng phân phối của DNS cho phép mức tải của việc phân giải tên được chia sẻ giữa rất nhiều máy tính. Ngày nay, hầu hết các phần mềm

làm việc trên Internet, ví dụ như các chương trình thư điện tử hoặc các trình duyệt Web, đều sử dụng DNS làm phương pháp phân giải tên cho nó.

Lợi điểm của DNS

Mặc dù DNS hầu như chỉ gắn với Internet, các mạng riêng cũng có thể sử dụng DNS bởi vì các lợi điểm sau đây:

- **Khả năng mở rộng.** Bởi vì DNS có khả năng phân phối mức tải giữa các CSDL trên nhiều máy tính, nó có thể được mở rộng để phục vụ bất kỳ mức phân giải tên nào yêu cầu**.**
- **Tính bất biến.** Các tên máy sẽ được duy trì không đổi thậm chí cả khi các địa chỉ IP gắn với nó thay đổi, điều này làm cho việc định vị các tài nguyên dễ dàng hơn.
- **Dễ dàng sử dụng.** Người dùng truy cập các máy tính bằng các tên dễ nhớ ví dụ ***www.microsoft.com*** hơn là các địa chỉ IP bằng số, ví dụ như là 192.168.1.100
- **Tính đơn giản.** Người dùng chỉ cần phải biết một qui ước tên để tìm các tài nguyên hoặc trên mạng Internet hoặc trong mạng Intranet

DNS là gì ?

Để hiểu được tầm quan trọng của DNS và cách thức nó hoạt động trong môi trường mạng Windows Server 2003, bạn phải hiểu các thành phần sau đây của DNS

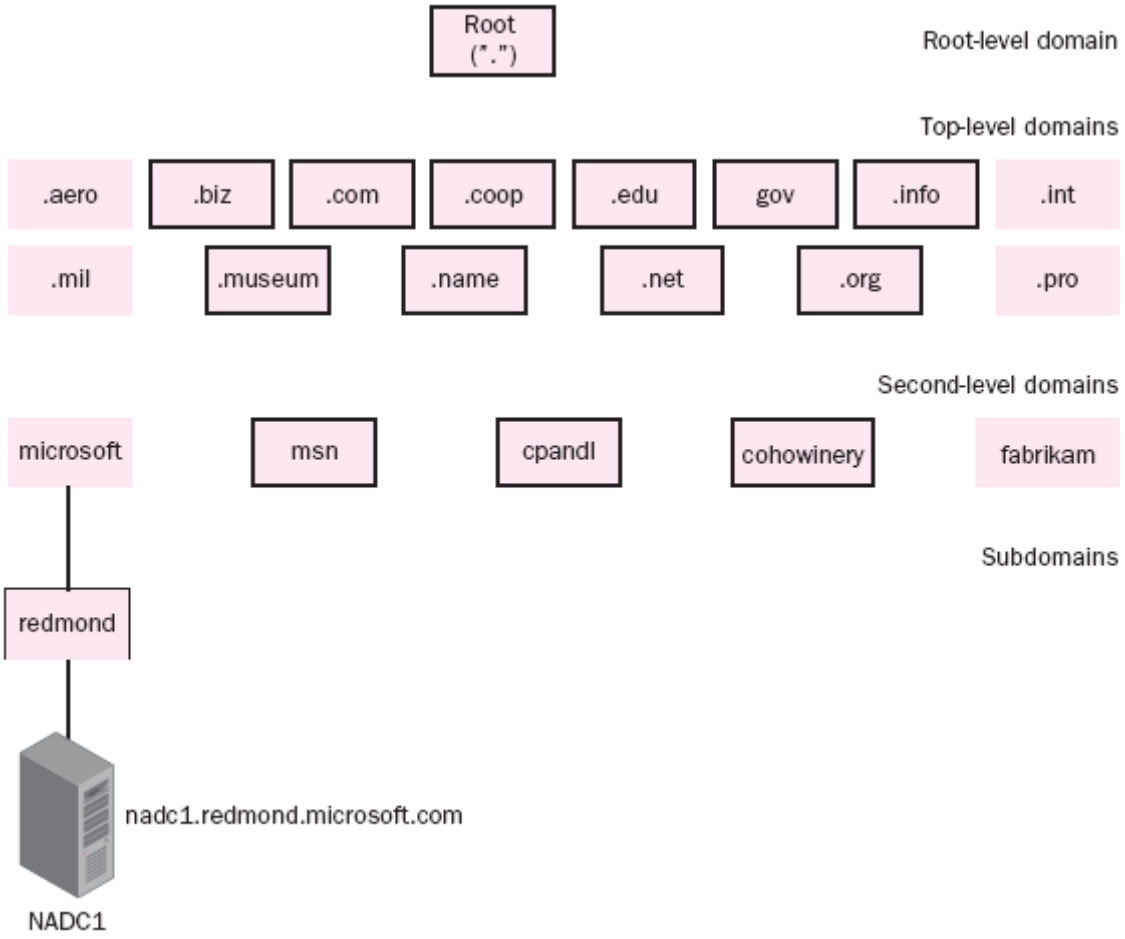
- Không gian tên DNS
- Các vùng DNS
- Các kiểu máy chủ tên DNS
- Các bản ghi tài nguyên DNS

Các phần sau đây sẽ thảo luận về các thành phần này.

Không gian tên miền

Không gian tên miền là một không gian tên phân cấp, có cấu trúc hình cây, khởi đầu từ một gốc không tên (root) được sử dụng cho mọi hoạt động DNS. Trong không gian tên DNS, mỗi đối tượng nút và đối tượng lá trong cây không gian tên miền hình cây sẽ thể hiện một miền đã được đặt tên. Mỗi

miền có thể có nhiều miền con bổ sung. Hình 3-1 thể hiện cấu trúc của một không gian tên miền Internet.



Hình 3-1. Không gian tên DNS của Internet

Không gian tên DNS có cấu trúc phân cấp và mỗi **tên miền DNS** là duy nhất. Trong Hình 3-1, tại đỉnh của không gian tên DNS Internet là miền gốc (***root***). Miền gốc được thể hiện bởi "**.**" (Dấu chấm). Dưới miền gốc DNS, các **miền mức-đỉnh (top-level domains)**, hay còn gọi là các **miền mức-đầu tiên** là các loại tổ chức khác nhau như ***.org, .com*** và ***.edu.*** Có ba kiểu của các miền mức-đỉnh là:

- ***Generic*** (Chung). Xem Bảng 3-1 để biết các ví dụ của các tên miền mức-đỉnh chung
- ***Country code*** (Mã quốc gia). Ví dụ của các tên miền kiểu mã quốc gia là .uk, .jp và us
- ***Infrastructure domain*** (Miền hạ tầng) ***.arpa*** là một tên miền kiểu hạ tầng

Cộng đồng Internet sẽ tạo ra các miền chung. Mỗi quốc gia riêng lẻ sẽ sử dụng tên miền kiểu mã quốc gia nếu cần thiết. Tổ chức có Thẩm quyền Gán Số Internet (IANA) sẽ cấp các tên miền mức-đỉnh. Bảng 3-1 liệt kê các tên miền mức-đỉnh và cách sử dụng chúng.

Bảng 3-1: Các tên miền mức-đỉnh kiểu tổng quan

Tên miền	Sử dụng
.aero	Loại ra để dành riêng cho các tổ chức hàng không
.biz	Miền mức-đỉnh dành cho các công ty lớn và nhỏ trên thế giới
.com	Các tổ chức thương mại, ví dụ như microsoft.com là của Tập đoàn Micrsoft
.coop	Miền mức-đỉnh dành cho các tập đoàn
.edu	Các viện giáo dục, hiện tại chính là để cho các trường đại học và cao đẳng 4 năm ví dụ như wustl.edu là của đại học Washington ở St. Louis
.gov	Đại diện của chính phủ liên bang Mỹ, ví dụ như fbi.gov là của Cục điều tra liên bang Mỹ
.info	Một miền không giới hạn để cung cấp thông tin tiêu dùng toàn cầu
.int	Các tổ chức thành lập bởi các Hiệp Ước quốc tế, ví dụ như nato.int
.mil	Quân đội Mỹ, ví dụ như af.mil là của Không lực Mỹ
.museum	Một miền giới hạn cho các nhà thờ và các tổ chức và cá nhân liên quan
.name	Một miền toàn cầu dành cho các cá nhân có khả năng phát triển vào hệ thống nhận dạng số toàn cầu của người dùng
.net	Các tổ chức hoặc các nhà cung cấp máy tính, mạng chuyên biệt cho Internet, các nhà cung cấp dịch vụ Internet (ISP) và tương tự, ví dụ như internic.net là của Trung tâm thông tin mạng Internet (InterNIC)
.org	Miền mức đỉnh cho các nhóm mà không phù hợp với các tên miền trên, ví dụ như các tổ chức phi chính phủ hoặc phi lợi nhuận (ví dụ w3.org là của cộng đồng WWW)
.pro	Miền mức đỉnh cho các chuyên gia ví dụ như các bác sĩ, luật sư hoặc kế toán

DNS sử dụng **Tên Miền Tiêu chuẩn Đầy đủ (FQDN)** để ánh xạ một tên máy sang một địa chỉ IP. Một FQDN mô tả chính xác mối liên hệ giữa một máy và miền DNS của nó. Ví dụ, ***computer1.sales.microsoft.com*** thể hiện một tên máy, ***computer1*** trong miền ***sales*** trong miền mức-thứ hai ***microsoft*** và trong miền mức-đỉnh ***.com***. Hình 3-2 thể hiện một FQDN

Hình 3-2. Phân tích một tên FQDN

Các tên miền DNS mức-thứ hai được đăng ký cho các cá nhân riêng rẽ hoặc cho các tổ chức, ví dụ như ***microsoft.com***, tên miền của Tập đoàn Microsoft, hoặc ***wustl.edu***, đó là Đại học Washington trong miền St.Louis; hoặc ***gov.au***, miền của chính phủ Australian. Các miền DNS mức-thứ hai có thể có rất nhiều miền con và bất kỳ miền nào cũng có các trạm (***host***). Một trạm (***host***) là một máy tính hoặc một thiết bị mạng cụ thể nào đó trong một miền, ví dụ như ***computer1*** trong miền con ***sales*** của miền ***microsoft.com***

Một lợi điểm của cấu trúc phân cấp của DNS là nó cho phép tồn tại hai trạm có cùng tên trạm nhưng lại nằm tại hai vị trí khác nhau trong cấu trúc phân cấp đó. Ví dụ, hai máy có tên ***conputer1***: ***computer1.sales.microsoft.com*** và ***computer1.cpandl.microsoft.com***-có thể đồng thời tồn tại mà không có xung đột bởi vì chúng khác nhau về vị trí trong không gian tên phân cấp.

Như đã đề cập trong phần trước, lợi ích khác của cấu trúc phân cấp là mức tải của việc phân giải tên được phân phối trên nhiều tài nguyên khác nhau.

Các vùng DNS, các máy chủ tên và các bản ghi tài nguyên sẽ được bàn luận đến trong phần sau của chương này.

CÀI ĐẶT DNS

Để biết được các lợi điểm của DNS, tất nhiên là bạn phải cài đặt DNS. Trước khi bạn cài đặt DNS, có lời khuyên là bạn nên cấu hình máy tính của bạn có địa chỉ IP tĩnh. Nếu máy chủ DNS được gán địa chỉ từ máy chủ DHCP, địa chỉ IP của nó có thể thay đổi. Nếu địa chỉ IP của máy chủ DNS thay đổi, các truy vấn gửi đến bởi máy khách DNS mà cấu hình với địa chỉ IP cũ sẽ không thành. Windows Server 2003 cung cấp một số trình hướng dẫn và các công cụ khác để cài đặt DNS nhanh chóng và dễ dàng. Một phương pháp cài đặt DNS là sử dụng trang "***Manage Your Server***" (*Quản trị máy chủ của bạn*). Trang "***Manage Your Server***" cho phép bạn thêm hoặc bớt các vai trò cho máy chủ, ví dụ như máy chủ file, máy chủ in ấn,

máy chủ DHCP và máy chủ DNS. Các thao tác sau đây giải thích cách sử dụng trang "***Manage Your Server***" để thêm vào vai trò của máy chủ DNS.

- **Thêm vai trò máy chủ DNS.**

  Để thêm vai trò của máy chủ DNS, thực hiện theo các bước sau:

  1. Nhấn ***Start***, trỏ vào ***Administrative Tools*** và sau đó lựa chọn "***Manage Your Server***"

  2. Trong trang "**Manage Your Server**", lựa chọn "**Add Or Remove A Role**" (Thêm hoặc bớt một vai trò)

  3. Trong trang "**Preliminary Steps**" (Các bước mở đầu), nhấn **Next**

  4. Trong trang "***Server Role***" (*Vai trò máy chủ*), nhấn vào "***DNS Server***" và sau đó nhấn ***Next***

  5. Trong trang "**Summary Of Selections**" (Bảng tổng kết các lựa chọn), nhấn **Next**

  6. Trong trang "**Welcome To The Configure A DNS Server Wizard**" (Chào mừng đến với trình cấu hình một máy chủ DNS), nhấn **Next**

  7. Trong trang "**Select Configuration Action**" (Lựa chọn cấu hình), nhấn vào **Configure Root Hints Only (Recommended For Advanced Users Only)** (Chỉ cấu hình các **Root Hints** (Khuyến nghị chỉ dành cho người dùng có trình độ cao)) và sau đó nhấn **Next**

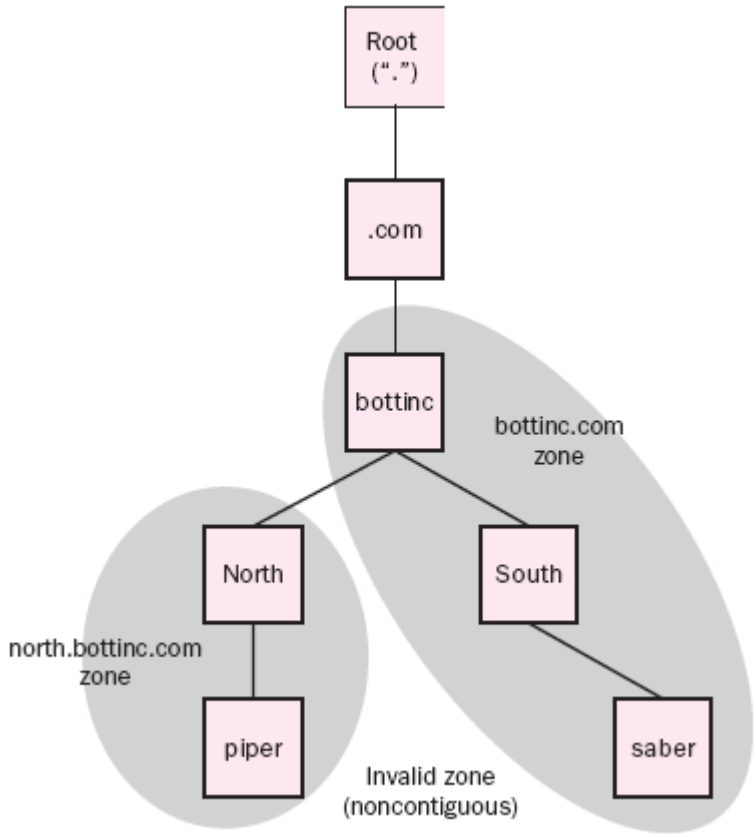
  8. Trong trang "**Completing The Configure A DNS Server Wizard**" (Hoàn thành cấu hình máy chủ DNS), nhấn **Finish**

  9. Trong trang "**This Server Is Now A DNS Server**" (Máy chủ bây giờ là máy chủ DNS), nhấn **Finish**

CÁC VÙNG DNS

Với mục đích quản trị, các miền DNS có thể được tổ chức thành các vùng. Một vùng là một tập hợp các ánh xạ tên máy tính – địa chỉ IP cho các máy trong một vùng tiếp giáp nhau của không gian tên DNS, như thể hiện trong Hình 3-3. Một vùng có thể chứa các bản ghi tài nguyên cho một miền hoặc nó có thể chứa các bản ghi tài nguyên cho nhiều miền. Một vùng có thể chứa

nhiều hơn một miền chỉ khi các miền đó là tiếp giáp nhau-có nghĩa là chúng có mối quan hệ cha-con trực tiếp với nhau. Một lý do để phân chia các không gian tên thành các vùng là để ủy quyền cho từng phần của nó. Các miền lớn có thể rất khó khăn khi quản trị.



Hình 3-3. Hai vùng hợp lệ và một vùng không hợp lệ, có không gian tên không tiếp giáp nhau

Đối với mỗi tên miền DNS có trong một vùng, vùng đó trở thành nguồn được ủy quyền của các thông tin về miền đó. Khi một vùng được ủy quyền trên một phần của không gian tên có nghĩa là nó sẽ chứa các bản ghi tài nguyên cho phần không gian tên đó. Tuy nhiên, điều này không có nghĩa là máy chủ đó có thể cập nhật hoặc thay đổi vùng này.

Các vùng được phân loại theo các thông số như địa điểm mà chúng được lưu, liệu chúng có thể ghi không và phân loại theo các thông tin nào mà chúng nhận được và trả lại. Các vùng có thể được lưu trong các file văn bản hoặc trong Active Directory.

Các máy chủ DNS được phân loại theo kiểu của vùng mà nó phục vụ. Một máy chủ DNS có thể phục vụ các vùng chính, các vùng thứ cấp, các vùng cụt hoặc không phục vụ vùng nào cả. Một máy chủ DNS được gọi là **máy**

chủ tên chính thức cho các vùng chính mà nó chứa và là **máy chủ tên thứ cấp** cho các vùng thứ cấp mà nó chứa. Một máy chủ chỉ-đệm (caching-only) sẽ không chứa vùng nào cả.

Tóm lại, dữ liệu vùng được duy trì trên một máy chủ DNS và được lưu trong một hoặc hai cách sau đây:

- Như là một vùng dữ liệu phẳng chứa một danh sách các ánh xạ
- Trong một CSDL Active Directory

Nếu phân loại theo kiểu của các truy vấn, mỗi vùng có thể là một **vùng phân giải xuôi** hoặc **vùng phân giải ngược**. Một vùng phân giải xuôi hay ngược có thể là một trong ba kiểu sau đây:

- Chính (***Primary***)
- Thứ cấp (***Secondary***)
- Cụt (***Stub***)

Khi bạn cấu hình một máy chủ DNS, bạn có thể cấu hình nó hoặc với một vài kiểu vùng hoặc không kiểu nào cả, tùy thuộc vào vai trò của máy chủ DNS đó trong hệ thống mạng.

Bằng cách sử dụng các vùng khác nhau, bạn có thể cấu hình giải pháp DNS của bạn phù hợp nhất với nhu cầu. Ví dụ, bạn nên cấu hình một vùng chính và một vùng thứ cấp trên các máy chủ DNS khác nhau để cung cấp khả năng chống lỗi khi một máy chủ bị hỏng. Bạn có thể cấu hình một vùng cụt nếu như vùng này được duy trì trên một máy chủ DNS riêng rẽ.

Hai phần sau đây sẽ thảo luận về các cách khác nhau trong đó dữ liệu vùng được lưu trữ: trong các vùng chuẩn và các vùng tích hợp Active Directory.

Các vùng chuẩn (*Standard Zone*)

Có rất nhiều lựa chọn cho việc tối ưu hóa cấu hình cho máy chủ DNS, dựa trên kiến trúc mạng, nhu cầu quản trị và kích thước của không gian tên. Hoạt động của các máy chủ DNS điển hình sẽ dựa trên ba vùng chuẩn (Chính, thứ cấp và in-addr.arpa). Windows Server 2003 cung cấp một tùy chọn thứ tư là các vùng cụt. Mỗi vùng chuẩn sẽ được thảo luận trong các phần sau đây.

Các vùng chính chuẩn (standard primary zone)

Một vùng chính chuẩn (***standard primary zone***) chứa một bản sao có thể ghi/đọc của một vùng DNS mà các bản ghi tài nguyên được tạo ra và quản trị. Chỉ một máy chủ có thể chứa và nạp bản ghi tài nguyên chính của vùng,

không máy chủ chính nào khác của vùng đó được cấp quyền này và chỉ máy chủ phục vụ vùng chính mới được phép chấp nhận các cập nhật động và xử lý việc thay đổi vùng. Khi thiết lập các máy chủ DNS để phục vụ các vùng của một miền, máy chủ chính thường được đặt ở nơi mà có thể truy cập được để quản trị các file của vùng.

Các vùng thứ cấp chuẩn (Standard Secondary Zone)

Một bản sao file của vùng có thể được lưu trên một hoặc nhiều máy chủ để cân bằng mức tải trên mạng, cung cấp khả năng chống lỗi hoặc tránh việc ép buộc các truy vấn phải thực hiện trên các kết nối WAN tốc độ thấp. Một vùng thứ cấp chuẩn là một bản sao chỉ đọc của vùng DNS chính chuẩn. Việc chuyển giao vùng, được thực hiện bằng cách đơn giản là sao chép file của vùng từ máy chủ chính sang máy chủ thứ cấp, sẽ tạo ra một vùng thứ cấp. Khi một vùng thứ cấp được tạo ra, bạn phải chỉ định địa chỉ IP của một hoặc nhiều các máy chủ DNS chủ mà bạn muốn sao chép vùng từ đó. Các bản sao chép này sẽ tham chiếu như là các file CSDL của vùng thứ cấp. Các file CSDL của vùng thứ cấp này được cập nhật đều đặn từ CSDL của vùng chính.

Các vùng in-addr.arpa

Hầu hết các truy vấn gửi đến máy chủ DNS đều là các truy vấn xuôi, có nghĩa là chúng yêu cầu một địa chỉ IP dựa trên một tên DNS. DNS cũng cung cấp chu trình phân giải ngược, tính năng này cho phép một máy có thể xác định tên của một máy khác dựa trên địa chỉ IP của nó. Ví dụ, truy vấn sẽ tương đương như một câu hỏi "tên miền DNS của một máy có địa chỉ IP 192.168.100.1 là gì ?"

Để trả lời truy vấn này, miền ***in-addr.arpa*** sẽ được tra cứu kết hợp với địa chỉ IP trong câu hỏi đó. Như khi bạn đọc địa chỉ IP từ trái sang phải, phần địa chỉ mạng là một số bit bên trái và phần địa chỉ máy là một số bit bên phải, dựa trên mặt nạ mạng con. Ví dụ, 192.168.100.2, với mặt nạ mạng con mặc định là 255.255.255.0 có nghĩa là phần địa chỉ mạng là 192.168.100 còn phần địa chỉ máy là 2. Bởi vì mức cao hơn (chi tiết hơn) của địa chỉ nằm ở phía bên phải, nó nhất thiết phải được đảo lại khi xây dựng cây của miền. Nói một cách ngắn gọn, bởi vì FQDN đi từ cụ thể đến tổng quan và một địa chỉ IP lại đi từ tổng quan đến cụ thể nên để thực hiện việc phân giải ngược, địa chỉ IP phải được đảo khi bị ràng buộc trong miền in-addr.arpa. Ví dụ, vùng phân giải ngược cho mạng con 192.168.100.0 là 100.168.192.in-addr.arpa. Cây của miền ***in-addr.arpa*** sẽ sử dụng bản ghi tài nguyên kiểu con trỏ (PTR), nó được sử dụng để gắn một địa chỉ IP với tên của máy. Quá

trình phân giải sẽ trỏ tương ứng đến một bản ghi tài nguyên địa chỉ (A) của máy trong vùng phân giải xuôi.

Các truy vấn phân giải ngược thường được sử dụng bởi các ứng dụng để xác nhận hơn là để nhận biết hoặc như một công cụ để giám sát và giải quyết sự cố của dịch vụ DNS.

> ***LƯU Ý. In-addr.arpa và mạng dựa trên nền IPv4****. Miền in-addr.arpa được sử dụng chỉ cho các mạng dựa trên nền giao thức Internet phiên bản 4 (IPv4). Trong bảng điều khiển DNS của Windows Server 2003, trình hướng dẫn tạo vùng mới của máy chủ DNS sử dụng miền này khi tạo ra một vùng phân giải ngược. Các vùng phân giải ngược dựa trên nên giao thức Internet phiên bản 6 (IPv6) sẽ dựa vào miền* ***ip6.arpa***

Các vùng phân giải ngược có cùng một bản ghi tài nguyên Khởi tạo Ủy quyền (***Start of Authority*** - SOA) và bản ghi tài nguyên Máy chủ Tên (**Name Server** - NS) như là vùng phân giải xuôi. Bạn có thể đồng thời cấu hình các vùng phân giải ngược thành các vùng chính hoặc thứ cấp hoặc tích hợp Active Directory. Các vùng phân giải ngược tích hợp Active Directory sẽ được đồng bộ giống như các vùng phân giải xuôi tích hợp Active Directory.

Các vùng cụt (Stub Zone)

Một máy chủ DNS chạy Windows Server 2003 cũng hỗ trợ một kiểu vùng mới được gọi là vùng cụt. Một vùng cụt là một bản sao của một vùng mà chỉ chứa các bản ghi tài nguyên cần thiết để nhận biết các máy chủ DNS được ủy quyền cho vùng đó. Một vùng cụt là một con trỏ trỏ đến máy chủ DNS mà được ủy quyền cho vùng đó và được sử dụng để duy trì hoặc cải tiến việc phân giải tên sao cho hiệu quả.

Một vùng cụt có chứa một tập hợp con của dữ liệu vùng có chứa một bản ghi SOA, một bản ghi NS và một bản ghi A. Cũng giống như vùng thứ cấp chuẩn, các bản ghi tài nguyên trong vùng cụt không thể được chỉnh sửa, chúng phải được chỉnh sửa trong vùng chính.

Các vùng cụt cho phép một máy chủ DNS thực hiện sự truy vấn đệ qui bằng cách sử dụng danh sách của các máy chủ tên trong vùng cụt mà không cần phải truy vấn máy chủ Internet hoặc máy chủ gốc nội bộ để có thông tin về không gian tên DNS. Sử dụng các vùng cụt trong cơ sở hạ tầng của bạn cho phép bạn có thể phân phối một danh sách của các máy chủ DNS được ủy quyền cho một vùng mà không cần sử dụng các vùng thứ cấp. Tuy nhiên, các vùng cụt không thể đáp ứng hiệu quả giống như là các vùng thứ cấp và không thể sử dụng được khi muốn cung cấp khả năng dự phòng và cân bằng tải.

Các vùng tích hợp Active Directory.

Lưu các vùng trong Active Directory là một phương pháp độc quyền của Microsoft để quản trị, bảo mật và đồng bộ các thông tin về vùng DNS. Một vùng tích hợp Active Directory là một vùng DNS được chứa trong Active Directory. Các vùng được lưu trong các file văn bản thông thường được gọi là các vùng chuẩn hoặc vùng gói trong file và các vùng được lưu trong Active Directory được gọi là các vùng tích hợp Active Directory. Lưu một vùng trong Active Directory có các lợi điểm sau đây:

- **Khả năng chống lỗi**. Thông tin được lưu trong nhiều máy chủ
- **Bảo mật**. Các vùng DNS lưu trong Active Directory có thể sử dụng các tính năng bảo mật tăng cường bằng cách chỉnh sửa danh sách điều khiển truy cập khi cần (**discretionary access control list -**DACL). Các DACL cho phép bạn chỉ định người dùng nào và nhóm nào có thể chỉnh sửa các vùng DNS.
- **Các vùng là đa chủ**. Điều này có nghĩa là các vùng này có thể được cập nhật trên nhiều nơi. Mọi máy chủ quản trị miền, nơi mà vùng được lưu, đều có thể chỉnh sửa vùng. Các thay đổi với vùng sau đó sẽ được đồng bộ tới các máy chủ quản trị miền mà có chứa các file của vùng.
- **Đồng bộ hiệu quả**. Việc chuyển giao vùng có thể được thay thế hiệu quả hơn bằng việc đồng bộ trong Active Directory. Điều này có thể đặc biệt quan trọng trên các hệ thống mạng kết nối tốc độ chậm bởi vì các dữ liệu được nén lại khi đồng bộ trong Active Directory có thể được trao đổi giữa các site.
- **Các vùng thứ cấp.** Các vùng lưu trong Active Directory có thể được chuyển giao sang các máy chủ thứ cấp chuẩn để tạo ra các vùng thứ cấp giống như cách mà các vùng gói trong file được chuyển giao.

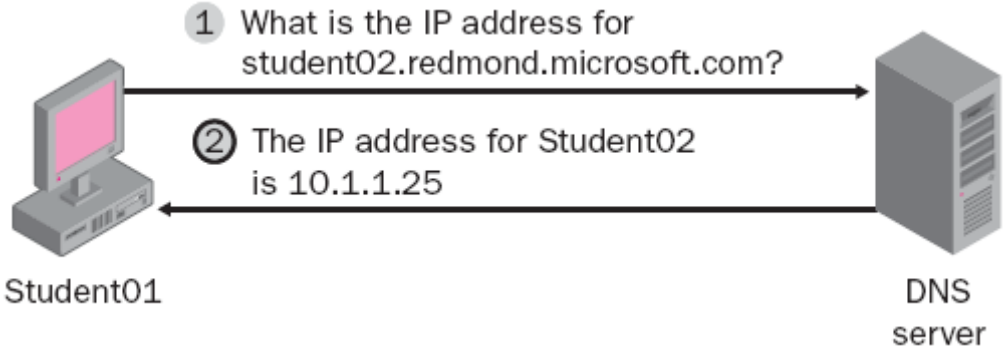
Windows Server 2003 cung cấp một phương pháp hiệu quả hơn để đồng bộ các thông tin trong vùng DNS hơn Microsoft Windows Server 2000. Trong Windows Server 2000, các cập nhật cho các vùng Active Directory được đồng bộ đến tất cả các máy quản trị miền trong miền đó, không cần biết đó có phải là các máy chủ DNS hay không. Trong Windows Server 2003, các vùng tích hợp Active Directory có thể được đồng bộ theo ba cách:

- Với tất cả các máy chủ quản trị miền trong miền (giống như trong Windows Server 2000)
- Với tất cả các máy chủ quản trị miền là máy chủ DNS trong miền cục bộ
- Với tất cả các máy chủ quản trị miền mà đồng thời là máy chủ DNS trong toàn bộ rừng.

Bạn có thể tạo ra hai kiểu vùng tích hợp Active Directory: Các vùng phân giải xuôi và các vùng phân giải ngược. Các vùng này được thảo luận trong phần sau

Các vùng phân giải xuôi

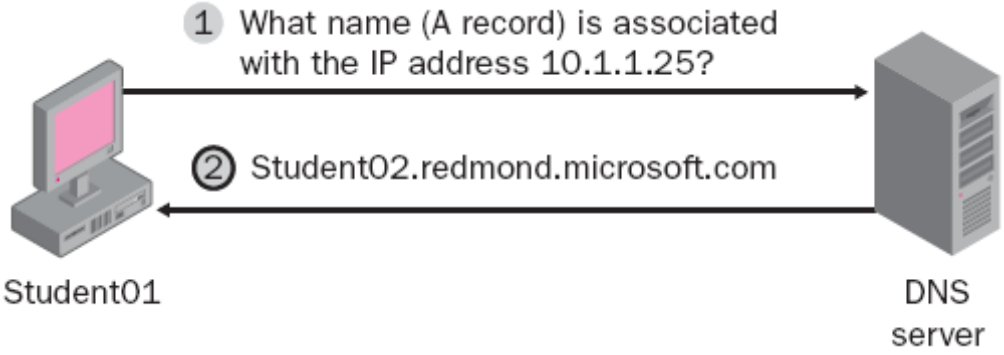
Một vùng phân giải xuôi tích hợp Active Directory tương tự như một vùng chính chuẩn. Không có Active Directory, các máy chủ chính và thứ cấp đều cần thiết bởi vì chúng theo mô hình cập nhật kiểu đơn chủ. Chỉ có một máy chủ chứa bản sao có thể ghi được của CSDL vùng. Tuy nhiên, các vùng tích hợp Active Directory lại theo một mô hình cập nhật đa chủ, có nghĩa là các vùng tích hợp Active Directory đều chứa một bản sao có thể ghi/đọc của vùng và có thể thay đổi các thông tin trong vùng. Do đó, việc phân biệt chính và thứ cấp là không cần thiết. Một vùng phân giải xuôi lưu các bản ghi để trả lời cho các truy vấn xuôi ví dụ như thể hiện trong Hình 3-4.



Hình 3-4: Truy vấn xuôi

Các vùng phân giải ngược

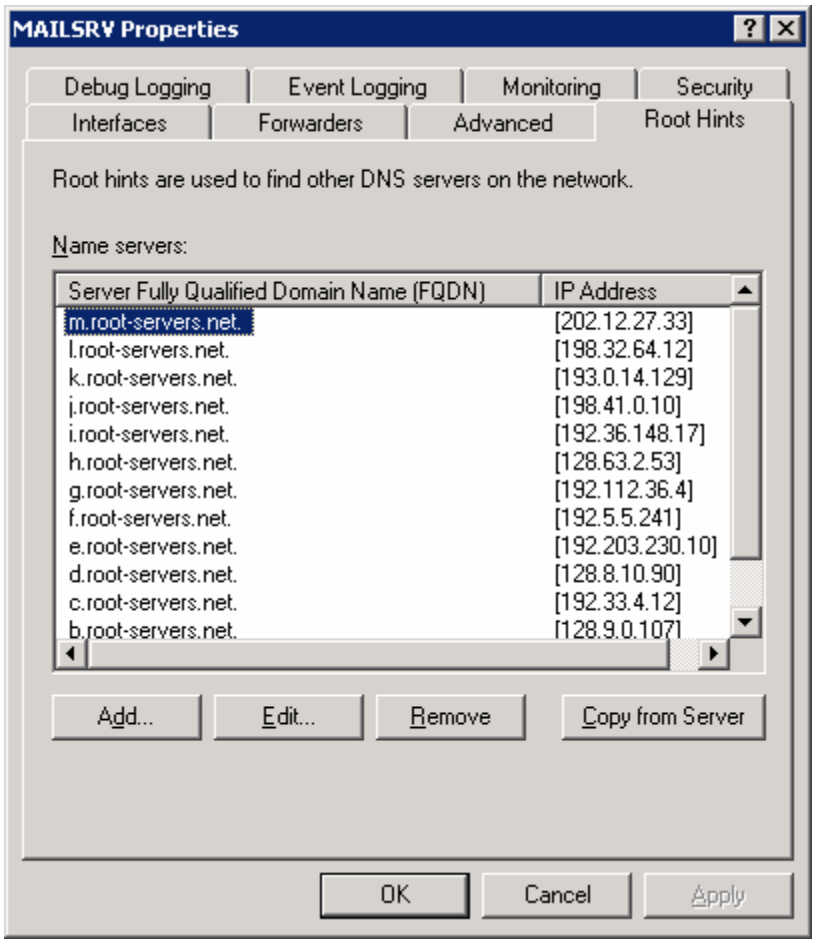
Một vùng phân giải ngược được sử dụng để phân giải một địa chỉ IP sang một tên và tương tự như vùng ***in-addr.arpa*** chuẩn. Vùng phân giải ngược được lưu và cập nhật giống như các vùng phân giải xuôi tích hợp Active Directory. Một vùng phân giải ngược lưu các bản ghi để trả lời cho các truy vấn phân giải ngược ví dụ như trong Hình 3-5.



Hình 3-5: Truy vấn ngược

CÁC ROOT HINT (THÔNG TIN MỨC GỐC)

Các máy chủ DNS phân giải các truy vấn DNS bằng cách sử dụng các dữ liệu ủy quyền cục bộ hoặc dữ liệu lưu đệm (cache). Nhưng nếu như máy chủ không chứa các dữ liệu yêu cầu và không được ủy quyền của tên có trong truy vấn, nó có thể thực hiện phương pháp **phân giải đệ qui** hoặc trả lại một tham chiếu đến các máy chủ DNS khác tùy thuộc vào liệu máy khách có yêu cầu đệ qui hay không. Dịch vụ DNS Server phải được cấu hình với các **root hint (thông tin mức gốc)** để phân giải các truy vấn cho các tên mà nó không được ủy quyền. ***Root hint*** có chứa các tên và địa chỉ IP của các máy chủ DNS được ủy quyền cho các vùng gốc. Bạn có thể sử dụng bảng điều khiển DNS để quản trị một danh sách các máy chủ gốc như thể hiện trong Hình 3-6



Hình 3-6. Trang thuộc tính root hint DNS

Theo mặc định, các máy chủ DNS sử dụng một file ***root hint*** là ***cache.dns***. File ***cache.dns*** được lưu trong thư mục ***%systemroot%\System32\Dns*** trên máy chủ. Khi máy chủ khởi động, ***cache.dns*** được nạp sẵn vào trong bộ nhớ máy chủ. Bằng cách sử dụng các ***root hint*** để tìm các máy chủ gốc, một máy chủ DNS có khả năng hoàn thành các truy vấn đệ qui. Quá trình này được thiết kế để cho phép bất kỳ máy chủ DNS nào cũng có thể định vị các máy chủ mà được ủy quyền cho bất kỳ một tên miền DNS nào mà sử dụng tại bất cứ mức nào trong cây không gian tên.

Khi trình hướng dẫn cấu hình một máy chủ DNS (***Configure A DNS Server Wizard***) được sử dụng để cấu hình một máy chủ DNS, nó gửi một truy vấn NS tìm miền gốc (.) đến các máy chủ DNS ưa thích và máy chủ DNS thay thế (***preferred*** và ***alternative DNS servers***). Các trả lời cho truy vấn này được lưu tại ***root hint*** của máy chủ DNS. Nếu không có máy chủ mức gốc nào được phát hiện, trình này sẽ gửi truy vấn giống như vậy đến các máy chủ DNS nằm trong file ***cache.dns*** mà tương ứng với các máy chủ mức gốc trên Internet. Nếu không phát hiện ra máy chủ mức gốc nào, trình này sẽ nhắc người dùng hoặc là tạo ra một máy chủ gốc hoặc chỉ định thủ công các

root hint. Việc cập nhật các ***root hint*** cho phép máy chủ hoạt động một cách hiệu quả hơn. Bạn nên cập nhật các ***root hint*** bất cứ khi nào một máy chủ mới được thêm vào hoặc thay đổi.

- **Cập nhật các root hint trong máy chủ DNS**

Để cập nhật các root hint trong máy chủ DNS, thực hiện theo các bước sau:

1. Mở bảng điều khiển DNS
2. Nhấn phải chuột vào máy chủ DNS tương ứng và nhấn vào ***Properties***
3. Nhấn vào thẻ ***Root Hints***

Chỉnh sửa các máy chủ ***root hint*** như sau:

- Để thêm một máy chủ gốc vào trong danh sách, nhấn ***Add*** và sau đó nhập vào tên và địa chỉ IP của máy chủ sẽ thêm vào trong danh sách máy chủ ***root hint***.
- Để chỉnh sửa một máy chủ trong trong danh sách, nhấn ***Edit*** và sau đó nhập vào tên và địa chỉ IP của máy chủ sẽ được chỉnh sửa trong danh sách
- Để xóa một máy chủ gốc trong danh sách, lựa chọn nó trong danh sách và sau đó nhấn ***Remove***

Bên cạnh việc bổ sung hoặc xóa bỏ danh sách các máy chủ gốc, bạn còn có thể sử dụng phím ***Copy From Server*** như thể hiện trong Hình 3-6. Cách này cho phép bạn chỉ định một địa chỉ IP của một máy chủ DNS khác mà từ đó máy chủ DNS của bạn có thể sao chép các ***root hint***.

Bạn còn có thể sử dụng dòng lệnh ***dnscmd*** để thêm hoặc xóa một máy chủ từ danh sách ***root hint***. ***Dnscmd*** được thảo luận trong Chương 4, "Quản trị và giám sát DNS". Trong ví dụ sau đây, máy chủ 10.1.1.200 được thêm vào trong danh sách của các máy chủ gốc tại máy chủ tên ***ns1.eu.reskit.com***:

C:\Windows>dnscmd ns1.eu.reskit.com. /RecordAdd /roothints @ ns 10.1.1.200

Command completed successfully.

> ***THÔNG TIN THÊM. Lệnh dnscmd***. ***Dnscmd*** *không được cài đặt theo mặc định, nó phải được thêm vào. Cũng giống như các công cụ khác, dòng lệnh* ***dnscmd*** *có thể được cài đặt từ đĩa cài đặt Microsoft Windows Server 2003 từ thư mục sau:* ***\Support\Tools\Suptools.msi.***

Trong Windows Server 2003, đối với dịch vụ ***DNS Server*** chạy trong máy chủ quản trị miền, các ***root hint*** được lưu trong phân vùng thư mục ứng dụng toàn miền

> ***LƯU Ý. Sử dụng các root hint đối với các máy chủ gốc nội bộ****. Nếu bạn có một máy chủ gốc DNS nội bộ trong cơ sở hạ tầng DNS của bạn, cấu hình các* ***root hint*** *của các máy chủ DNS nội bộ để trỏ vào chỉ máy chủ DNS chứa miền gốc và không phải là máy chủ DNS chứa miền Internet gốc. Điều này sẽ ngăn không cho máy chủ DNS nội bộ của bạn gửi các thông tin cá nhân ra ngoài Internet khi thực hiện việc phân giải tên.*

Dỡ bỏ vùng DNS gốc.

Một máy chủ DNS Windows Server 2003 sẽ theo các bước sau trong quá trình phân giải tên của nó: Máy chủ DNS đầu tiên sẽ truy vấn bộ nhớ lưu đệm của nó, sau đó kiểm tra các bản ghi vùng của nó và sau nữa gửi các yêu cầu đến các máy chủ chuyển tiếp (***forwarders***) và tiếp theo nó sẽ cố gắng phân giải bằng cách sử dụng các máy chủ gốc.

Theo mặc định, một máy chủ Microsoft DNS kết nối đến Internet để xử lý các yêu cầu DNS mà cần phải phân giải tên mức gốc. Khi bạn sử dụng công cụ ***dcpromo*** để thăng cấp một máy chủ thành máy chủ quản trị miền, máy chủ quản trị miền sẽ yêu cầu DNS. Nếu bạn cài đặt DNS trong quá trình thăng cấp, một vùng gốc sẽ được tạo ra. Vùng gốc này chỉ định máy chủ DNS của bạn rằng nó cũng chính là máy chủ Internet gốc. Do đó, máy chủ DNS của bạn không sử dụng các máy chủ chuyển tiếp hoặc các ***root hint*** trong quá trình phân giải tên và có thể gây ra việc phân giải tên không thành. Để giải quyết vấn đề này, hãy dỡ bỏ vùng gốc ra khỏi máy chủ DNS của bạn.

- **Dỡ bỏ vùng DNS gốc.**

1. Nhấn ***Start***, trỏ vào ***Administrative Tools*** và sau đó nhấn ***DNS***
2. Mở rộng tên máy chủ và sau đó mở rộng ***Forward Lookup Zones***
3. Nhấn phải chuột vào vùng "**.**" và sau đó nhấn ***delete***

CÁC KIỂU MÁY CHỦ DNS

Các kiểu máy chủ DNS được xác định bởi kiểu của vùng hoặc các vùng mà máy chủ đó chứa và bởi chức năng mà chúng đảm nhận. Một máy chủ DNS có thể chứa một vùng chính hoặc vùng thứ cấp hoặc cả hai. Trong cùng một thời điểm một máy chủ có thể là một máy chủ tên chính, đó là một máy chủ

chịu trách nhiệm cập nhật các máy chủ khác. Nếu máy chủ không chứa một vùng nào, nó được gọi là máy chủ chỉ-đệm dự trữ. Bốn kiểu máy chủ sau được hỗ trợ trong Windows Server 2003 và được thảo luận trong các phần sau đây.

Máy chủ tên chính (*Primary Name Server*)

Các máy chủ tên chính chứa một hoặc nhiều hơn các vùng chính. Khi có một sự thay đổi trong dữ liệu vùng, ví dụ như là thêm các bản ghi tài nguyên vào vùng, sự thay đổi này phải được thực hiện trên máy chủ chính của vùng đó. Các thay đổi sau đó sẽ được phân phối đến các máy chủ tên thứ cấp. Máy chủ tên chính cũng đồng thời phục vụ các truy vấn của các máy trạm.

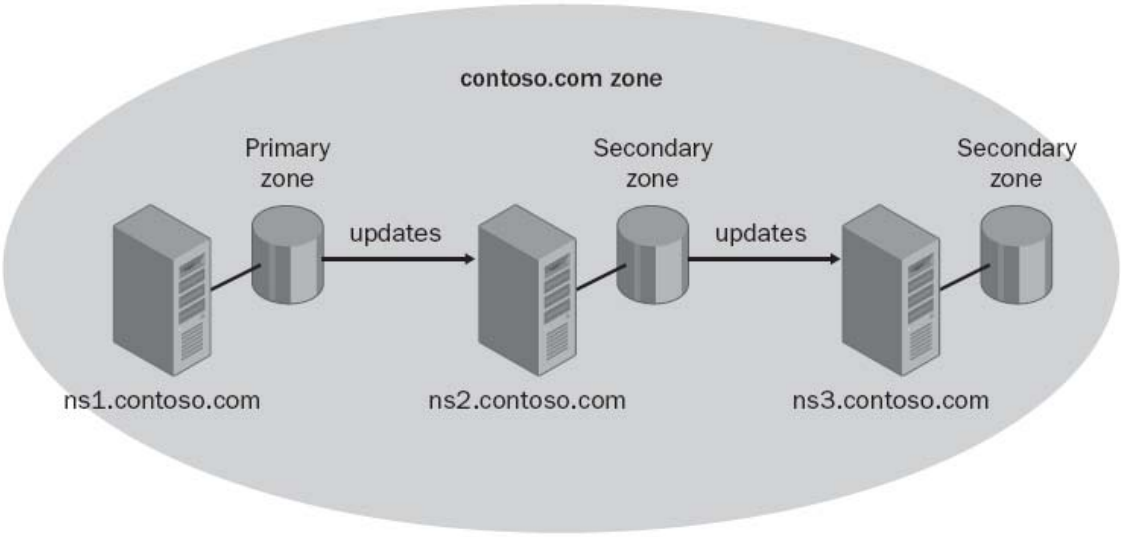
Máy chủ tên thứ cấp (*Secondary Name Server*)

Máy chủ tên thứ cấp chứa một hoặc nhiều các CSDL vùng thứ cấp. Bởi vì sự chuyển vùng được thực hiện để tạo ra một vùng thứ cấp, máy chủ tên chính và vùng phải đã tồn tại để tạo ra một máy chủ tên thứ cấp.

Máy chủ tên chủ đạo (*Master Name Server*)

Máy chủ tên là máy chủ tên chủ đạo khi nó chịu trách nhiệm gửi các bản sao cập nhật của CSDL đến các máy chủ tên khác. Một máy chủ tên chủ đạo có thể chứa các bản sao chính hoặc thứ cấp của CSDL của vùng. Điều này có nghĩa là một máy chủ tên chủ đạo có thể là một máy chủ tên chính hoặc một máy chủ tên thứ cấp. trong hình 3-7:

- ***ns1.contoso.com*** là máy chủ tên chính và chủ đạo cho ***ns2.contoso.com***
- ***ns2.contoso.com*** là máy chủ thứ cấp, nhận bản cập nhật từ ***ns1*** và là máy chủ tên chủ đạo của ***ns3***
- ***ns3.contoso.com*** là máy chủ thứ cấp và nhận các cập nhật từ ***ns2***



Hình 3-7. Các vùng chính và thứ cấp đóng vai trò như máy chủ tên chủ đạo

Máy chủ chỉ-đệm (*Caching-Only Server*)

Các máy chủ chỉ-đệm không chứa bất kỳ một vùng nào và không được ủy quyền cho một miền nào cả. Các máy chủ DNS chỉ-đệm khởi đầu với một bộ nhớ đệm trống và dần thêm vào các mục bản ghi tài nguyên mà máy chủ sử dụng để phục vụ các yêu cầu của máy khách. Các thông tin này sau đó sẽ sẵn sàng phục vụ từ bộ đệm của nó khi trả lời các truy vấn sau đó của máy khách. Một máy chủ DNS chỉ-đệm sẽ rất có giá trị trong một site khi chức năng DNS là cần thiết trong nội bộ nhưng việc tạo ra một miền hoặc vùng riêng biệt là không yêu cầu.

CÁC BẢN GHI TÀI NGUYÊN DNS

Một ***bản ghi tài nguyên*** là thông tin liên quan đến một miền DNS; ví dụ, bản ghi trạm xác định một địa chỉ IP của trạm. Các bản ghi tài nguyên được thể hiện bằng định dạng nhị phân trong các gói tin khi mà các truy vấn và các phản hồi được tạo ra trong DNS. Tuy nhiên trong file của vùng DNS, các bản ghi tài nguyên lại được thể hiện như các mục văn bản. Hầu hết các bản ghi tài nguyên đều được thể hiện là các mục vào kiểu dòng văn bản đơn. Nếu một mục có thể mở rộng thành hơn một dòng, bạn có thể sử dụng các dấu ngoặc đơn để đóng gói các thông tin. Trong rất nhiều hệ thống sử dụng DNS, chỉ có bản ghi SOA là có thể có nhiều dòng văn bản. Để có thể đọc được, các dòng trống và chú giải thường được chèn vào trong các file của vùng và thường được máy chủ DNS bỏ qua. Các chú thích luôn bắt đầu với một dấu phẩm phẩy (**;**) và kết thúc với một dấu xuống dòng.

Các bản ghi tài nguyên có cú pháp như sau:

Owner [TTL] Class Type RDATA

Bảng 3-2 mô tả các tập hợp thông tin thông thường trong các bản ghi tài nguyên.

Bảng 3-2. Các trường trong các bản ghi tài nguyên điển hình

Tên	Mô tả
Owner (Chủ sở hữu)	Nhận diện các máy hoặc các miền DNS mà các bản ghi tài nguyên này là sở hữu của nó
TTL (*Thời gian sống*)	Một số nguyên 32 bit thể hiện thời gian tối đa tính bằng giây mà một máy chủ hoặc máy trạm DNS có thể lưu đệm bản ghi này trước khi nó bị hủy bỏ. Trường này là tùy chọn, và nếu nó không được chỉ định cụ thể, máy khách sẽ sử dụng giá trị TTL tối thiểu có trong bản ghi SOA
Class (Phân lớp)	Định nghĩa các giao thức quen thuộc sử dụng, ví dụ như IN là cho hệ thống Internet
Type (Kiểu)	Nhận diện các kiểu bản ghi tài nguyên. Ví dụ kiểu A là thể hiện đó là bản ghi tài nguyên lưu các thông tin địa chỉ máy
RDATA (Dữ liệu bản ghi tài nguyên)	Chứa RDATA. Trường RDATA là một trường có độ dài biến đổi thể hiện các thông tin sẽ mô tả bởi bản ghi tài nguyên. Ví dụ, trong một bản ghi tài nguyên A, dữ liệu có trong trường này là địa chỉ IP 32 bit của máy có tên trong mục Owner

Các kiểu bản ghi tài nguyên.

CSDL DNS chứa rất nhiều bản ghi tài nguyên có liên quan đến các thông tin khác nhau về các tên trong CSDL. Một bản ghi tài nguyên cho một tên DNS có thể nhận biết một tài nguyên đơn trong một hệ thống mạng, ví dụ như một máy tính mạng sử dụng tên đó hoặc một dịch vụ chạy trong máy tính mạng đó, ví dụ như thư điện tử.

Các kiểu khác nhau của các bản ghi tài nguyên cung cấp dữ liệu DNS về các máy tính trong một mạng TCP/IP. Các bản ghi tài nguyên thông thường được mô tả trong Bảng 3-3 và chi tiết ở các phần sau đây. Các thảo luận trong phần này sẽ bao gồm các bản ghi tài nguyên cụ thể cho việc triển khai DNS trong Windows 2000 và Windows Server 2003

Bảng 3-3. Các kiểu bản ghi tài nguyên

Mô tả	Phân loại	TTL	Kiểu	Dữ liệu
Khởi đầu ủy quyền	Internet (IN)	60 phút	SOA	Tên chủ sở hữu, tên FQDN của máy chủ tên, số thứ tự, khoảng thời gian làm tươi, khoảng thời gian thử lại, thời gian hết hạn, và giá trị TTL tối thiểu
Trạm	Internet (IN)	TTL của SOA trong cùng vùng	A	Tên chủ sở hữu (tên DNS của máy) và địa chỉ IPv4 của máy
Máy chủ Tên	Internet (IN)	TTL của SOA trong cùng vùng	NS	Tên chủ sở hữu và tên DNS của máy chủ
Trao đổi thư	Internet (IN)	TTL của SOA trong cùng vùng	MX	Tên chủ sở hữu, tên DNS của máy chủ trao đổi thư (MX), và số thứ tự ưu tiên
Tên quy chuẩn (Bí danh)	Internet (IN)	TTL của SOA trong cùng vùng	CNAME	Tên chủ sở hữu (tên bí danh) và tên DNS của máy

Bản ghi tài nguyên Khởi tạo Ủy quyền (Start of Authority - SOA)

Mỗi vùng đều chứa một bản ghi tài nguyên SOA ở phần đầu file của vùng. Một bản ghi tài nguyên SOA chỉ định điểm khởi đầu hoặc điểm khởi nguồn của việc ủy quyền cho các thông tin lưu trong một vùng. Nó chứa tất cả các thông tin cụ thể của vùng để máy chủ DNS sử dụng khi duy trì vùng này. Bản ghi tài nguyên SOA là bản ghi tài nguyên đầu tiên được tạo ra khi tạo ra một vùng mới.

Trường RDATA trong bản ghi tài nguyên SOA chứa các trường thể hiện trong Bảng 3-4.

Bảng 3-4. Trường RDATA trong bản ghi tài nguyên SOA

Trường RDATA	Mô tả
Authoritative Server ***(****Máy chủ có thẩm quyền)*	Chứa tên của máy chủ DNS chính thức có thẩm quyền của vùng

Responsible Person *(Người chịu trách nhiệm)*	Thể hiện địa chỉ Email của người quản trị chịu trách nhiệm của vùng. Trường này sử dụng dấu chấm (.) thay cho dấu (@)
Serial number (*Số thứ tự*)	Chỉ ra số lần mà vùng được cập nhật. Khi máy chủ thứ cấp của vùng liên lạc với máy chủ chủ đạo để xác định liệu nó có cần phải khởi tạo một sự chuyển giao vùng hay không, nó sẽ so sánh số thứ tự của nó với số thứ tự của máy chủ chủ đạo. Nếu số thứ tự của máy chủ chủ đạo cao hơn, máy chủ thứ cấp sẽ khởi tạo một sự chuyển giao vùng
Refresh (*Làm tươi*)	Chỉ ra tần suất mà máy chủ thứ cấp của vùng kiểm tra để xem liệu dữ liệu của vùng có bị thay đổi hay không
Retry (*Thử lại*)	Sau khi gửi di một yêu cầu chuyển giao vùng, số này thể hiện khoảng thời gian tính bằng giây mà máy chủ thứ cấp của vùng sẽ đợi trước khi gửi đi một yêu cầu khác
Expire (*Hết hạn*)	Sau khi chuyển giao vùng, số này thể hiện khoảng thời gian tính bằng giây mà máy chủ thứ cấp của vùng tiếp tục phản hồi lại các truy vấn về vùng trước khi loại bỏ vùng mà nó chứa vì không hợp lệ nữa
Minimum TTL (*Thời gian sống tối thiểu*)	Áp dụng cho tất các bản ghi tài nguyên trong vùng bất cứ khi nào giá trị TTL không được chỉ định rõ trong các bản ghi tài nguyên hoặc có nhưng lại ngắn hơn giá trị TTL tối thiểu chỉ định trong bản ghi tài nguyên SOA. Bất cứ khi nào máy khách DNS truy vấn máy chủ, máy chủ sẽ gửi ngược lại bản ghi tài nguyên mà chứa giá trị TTL xác định của bản ghi hoặc giá trị TTL tối thiểu. Các phản hồi từ chối sẽ được lưu đệm với thời gian bằng giá trị TTL tối thiểu có trong bản ghi tài nguyên SOA của vùng có thẩm quyền

Các thông tin sau đây là một ví dụ của một bản ghi tài nguyên SOA:

na.contoso.com. IN SOA (
nadc1.na.contoso.com.; authoritative server for the zone
administrator.na.contoso.com. ; zone admin e-mail
; (responsible person)
5099 ; serial number
3600 ; refresh (1 hour)
600 ; retry (10 mins)
86400 ; expire (1 day)
60) ; minimum TTL (1 min)

Bản ghi tài nguyên Tên Máy chủ (Name Server - NS)

Bản ghi tài nguyên NS nhận biết một máy chủ DNS mà được ủy quyền cho một vùng. Tên của máy chủ DNS mà được ủy quyền cho một vùng sẽ được lưu trong trường RDATA. Các bản ghi tài nguyên NS được sử dụng để nhận biết cả các máy chủ DNS chính và thứ cấp cho một vùng chỉ định trong bản ghi tài nguyên SOA và để chỉ định các máy chủ DNS cho bất kỳ vùng được cấp quyền nào. Nếu một vùng có nhiều máy chủ được ủy quyền (ví dụ một máy chủ chính và một hoặc nhiều máy chủ thứ cấp), bạn cần phải có một bản ghi NS cho mỗi máy chủ. Dịch vụ Windows Server 2003 DNS Server tự động tạo ra bản ghi NS đầu tiên cho một vùng khi vùng đó được tạo ra. Bạn có thể thêm các bản ghi tài nguyên NS bổ sung bằng bảng điều khiển DNS Manager hoặc sử dụng công cụ dòng lệnh Dnscmd.

> ***LƯU Ý. Các vùng và các bản ghi NS****. Mỗi vùng chứa ít nhất một bản ghi NS.*

Ví dụ, nếu một người quản trị của ***contoso.com*** cấp quyền quản trị miền con ***na.contoso.com*** cho máy chủ ***nadc1.na.contoso.com***, dòng sau đây sẽ được thêm vào các vùng ***contoso.com*** và ***ns.contoso.com***

na.contoso.com. IN NS nadc1.na.contoso.com.

Bản ghi tài nguyên địa chỉ trạm (A)

Bản ghi tài nguyên địa chỉ trạm (A) sẽ ánh xạ một tên FQDN đến một địa chỉ IP. Ví dụ, bản ghi tài nguyên A sau đây được đặt trong vùng ***na.contoso.com*** và ánh xạ FQDN của một máy chủ đến địa chỉ IP của nó:

nadc1.na.contoso.com. IN A 172.16.48.1

Bản ghi tài nguyên A chứa các trường sau đây:

- Các trường ***Owner*** (Đối tượng sở hữu), TTL, ***Class*** (Phân lớp) và ***Type*** (Kiểu), các trường này được mô tả trong Bảng 3-2 "Các

trường trong các bản ghi tài nguyên điển hình" có trong phần sau của chương.

- Trường ***RDATA*** là địa chỉ ***IP*** của đối tượng sở hữu.

Bản ghi tài nguyên PTR

Bản ghi tài nguyên PTR thực hiện thức năng ngược với bản ghi A bằng cách ánh xạ một địa chỉ IP sang một FQDN. Ví dụ, bản ghi tài nguyên PTR sau đây sẽ ánh xạ địa chỉ IP 172.16.48.1 của ***nadc1.na.contoso.com*** đến FQDN của nó.

1.48.16.172.in-addr.arpa. IN PTR nadc1.na.contoso.com.

Bản ghi tài nguyên PTR chứa các trường sau đây:

- Các trường ***Owner*** (Đối tượng sở hữu), ***TTL***, ***Class*** (Phân lớp) và ***Type*** (Kiểu), các trường này được mô tả trong Bảng 3-2 "Các trường trong các bản ghi tài nguyên điểm hình", có trong phần sau của chương.

- Trường ***RDATA*** là tên máy của máy mà có địa chỉ IP có trong trường ***Owner***

Bản ghi tài nguyên tên qui chuẩn (CNAME)

Bản ghi tài nguyên tên quy chuẩn (CNAME) tạo ra một biệt danh cho một FQDN cụ thể. Bạn có thể sử dụng bản ghi tài nguyên CNAME để che giấu các thông tin chi tiết của mạng của bạn khi các máy khách kết nối đến nó.

Ví dụ nếu bạn muốn đặt một máy chủ FPT (*Giao thức truyền file*) tên là ***ftp1.na.contoso.com*** trong miền con ***na.contoso.com***, nhưng bạn lại biết rằng trong sáu tháng sau bạn có thể phải chuyển nó sang một máy tính có tên ***ftp2.na.contoso.com*** và bạn lại không muốn người dùng phải biết được sự thay đổi đó, hãy làm như sau: Tạo ra một biệt danh là ***ftp.na.contoso.com*** mà trỏ đến ***ftp1.na.contoso.com***. Khi bạn chuyển máy tính của bạn, bạn cần phải thay đổi chỉ bản ghi CNAME để trỏ vào ***ftp2.na.contoso.com***. Ví dụ, bản ghi tài nguyên CNAME sau đây sẽ tạo ra một biệt danh cho ***ftp1.na.contoso.com***

ftp.na.contoso.com. IN CNAME ftp1.na.contoso.com.

Sau khi các máy khách DNS truy vấn tên của ***ftp.na.contoso.com***, máy chủ DNS sẽ tìm bản ghi tài nguyên CNAME, phân giải truy vấn tên của ***ftp1.na.contoso.com*** và trả lại cả bản ghi tài nguyên A và CNAME cho máy khách.

LƯU Ý. CNAME và các biệt danh trong một vùng. *Nếu một bản ghi tài nguyên CNAME lại thể hiện một nút (tên DNS), không bản ghi tài nguyên nào khác của cùng tên đó có thể tồn tại trong vùng. Điều này để đảm bảo rằng dữ liệu cho một CNAME và biệt danh của nó không thể khác nhau. Theo RFC 2181, một biệt danh có thể chỉ có thể có một tên qui chuẩn.*

Bản ghi tài nguyên CNAME chứa các trường sau đây:

- Các trường ***Owner*** (Đối tượng sở hữu), *TTL*, ***Class*** (Phân lớp) và ***Type*** (Kiểu). Trường ***Owner*** của bản ghi CNAME chính là biệt danh
- Trường ***RDATA*** là tên của máy mà biệt danh đó trỏ vào.

Bản ghi tài nguyên trao đổi thư điện tử (Mail Exchanger - MX)

Bản ghi tài nguyên trao đổi thư điện tử (MX) chỉ định một máy chủ sẵn sàng làm nhiệm vụ như một máy chủ thư điện tử cho một tên DNS. Máy chủ thư mà nhận biết trong một bản ghi MX là một máy chủ hoặc xử lý hoặc chuyển tiếp các thư điện tử cho một tên miền DNS. Việc xử lý thư có nghĩa là hoặc đưa nó đến đúng địa chỉ hoặc chuyển nó sang một dạng khác của việc vận chuyển thư. Việc chuyển tiếp thư có nghĩa là gửi nó đến máy chủ đích cuối cùng, gửi nó bằng cách sử dụng ***Simple Mail Transfer Protocol*** (*giao thức chuyển thư đơn giản* - SMTP) đến một máy chủ trao đổi thư khác mà gần đích đến cuối cùng hơn, hoặc xếp nó vào hàng đợi trong một khoảng thời gian.

Để cải tiến độ tin cậy của dịch vụ thư trong một miền, bạn có thể thiết kế các máy chủ thư thứ cấp mà có thể lưu thư của miền. Nếu máy chủ thư chính ngừng hoạt động, máy chủ thư thứ cấp có thể chứa các thư và sau đó chuyển tiếp nó khi mà máy chủ thư chính hoạt động trở lại. Một ***SMTP smart host*** (*Trạm SMTP thông minh*, có khả năng sử dụng các bản ghi MX) sẽ sử dụng nhiều máy chủ thư, cho phép bạn cấu hình nhiều bản ghi tài nguyên MX.

Ví dụ sau đây sẽ cho ta biết các bản ghi tài nguyên cho các máy chủ thư của miền ***na.contoso.com***

@ IN MX 5 mailserver1.na.contoso.com.
@ IN MX 10 mailserver2.na.contoso.com.
@ IN MX 20 mailserver3.na.contoso.com.

Bản ghi tài nguyên MX chứa các trường sau đây:

- Các trường ***Owner*** (Đối tượng sở hữu), ***TTL***, ***Class*** (Phân lớp) và ***Type*** (Kiểu), các trường này được mô tả trong Bảng 3-2 "Các

trường trong các bản ghi tài nguyên điển hình", có trong phần sau của chương.

- Các dữ liệu sau đây được lưu trong trường ***RDATA*** của bản ghi tài nguyên ***MX***:
  - Bốn trường trong bản ghi ***MX*** là giá trị máy chủ thư ưa thích. Giá trị máy chủ thư ưa thích chỉ định sự ưu tiên cho một bản ghi ***MX*** giữa các bản ghi ***MX*** khác. Các bản ghi với số thứ tự ưu tiên thấp (nhưng thực sự lại có độ ưu tiên cao hơn) là được ưa thích hơn. Do đó, khi một máy khách thư cần phải gửi thư đến một miền DNS nào đó, đầu tiên nó phải liên lạc với một máy chủ DNS của miền đó và nhận về tất cả các bản ghi ***MX***. Sau đó nó sẽ liên hệ với máy chủ thư với giá trị ưa thích thấp nhất

THÔNG TIN THÊM. Việc định tuyến thư và hệ thống miền. *Để có thêm thông tin về cách thức định tuyến thư điện tử trong hệ thống các miền, xem RFC 974, tài liệu này có thể tìm tại địa chỉ http://www.rfc-editor.org/rfcsearch.html.*

  - Trường cuối cùng là tên của máy chủ thư để liên hệ

Ví dụ, giả sử Holly Holt gửi một thông điệp thư điện tử đến ***loviatt@na.contoso.com*** vào một ngày mà máy chủ thư ***mailserver1*** bị hỏng nhưng máy chủ ***mailserver2*** vẫn hoạt động. Máy trạm (còn gọi là máy khách thư điện tử - ***email client***) của cô ấy cố gắng chuyển thông điệp thư đến ***mailserver1*** bởi vì máy chủ này có giá trị ưa thích thấp nhất, nhưng không thể được vì máy chủ này đang bị hỏng. Trong trường hợp này, máy trạm của Holly lựa chọn máy chủ thư ***mailserver2*** bởi vì giá trị ưa thích của nó là thấp thứ hai. Nếu máy chủ ***mailserver2*** hoạt động, thư sẽ được gửi thành công đến ***mailserver2.***

Để tránh vòng lặp thư, nếu như phần mềm trao đổi email lại nằm trên một máy mà được liệt kê như một MX cho máy đích, phần mềm trao đổi email này có thể chỉ chuyển email tới một MX với giá trị ưa thích thấp hơn giá trị của chính nó. Nếu một máy chủ thư nhận được nhiều bản ghi MX với độ ưu tiên ngang nhau, lựa chọn bản ghi MX nào được sử dụng sẽ tùy thuộc vào việc triển khai hệ thống như thế nào.

Bản ghi Tài nguyên Định vị Dịch vụ (Service Locator - SRV)

Các bản ghi tài nguyên định vị dịch vụ (SRV) cho phép bạn chỉ định địa chỉ của các máy chủ cung cấp một dịch vụ mạng xác định nào đó cho một giao thức xác định và trong một miền xác định. Các bản ghi SRV cho phép bạn

có một số máy chủ cung cấp một dịch vụ mạng và bạn có thể chuyển các dịch vụ này giữa các máy chủ mà không cần phải thay đổi cấu hình của các máy khách. Ví dụ, nếu bạn có hai máy chủ ứng dụng trong miền của bạn, bạn có thể tạo ra các bản ghi tài nguyên SRV trong DNS chỉ định máy nào sẽ hoạt động như là máy chủ ứng dụng. Các ứng dụng trên máy khách có hỗ trợ các bản ghi SRV sẽ sử dụng DNS để phục hồi các bản ghi tài nguyên của các máy chủ ứng dụng.

Active Directory là một ví dụ về một ứng dụng phụ thuộc vào các bản ghi tài nguyên SRV. Một ví dụ của một ứng dụng mà được hỗ trợ bản ghi tài nguyên SRV là dịch vụ ***Netlogon*** trong Windows 2000 và Windows Server 2003. Trong Windows 2000, Microsoft Windows XP và Windows Server 2003, các máy khách sử dụng bản ghi tài nguyên SRV để định vị các máy chủ quản trị miền của một miền và gia nhập miền Active Directory đó.

Định dạng của một bản ghi SRV như sau:

_Service_Protocol.Name [TTL] Class SRV Priority Weight Port Target

Bảng 3-5 cho biết các trường của bản ghi tài nguyên SRV.

Bảng 3-5 Các trường của bản ghi tài nguyên SRV

Tên trường	Mô tả
Service (*Dịch vụ*)	Chỉ định tên của dịch vụ, ví dụ như ***http*** hoặc ***telnet***
Protocol (*Giao thức*)	Chỉ định giao thức, ví dụ như TCP hoặc UDP
Name (*Tên*)	Chỉ định tên miền mà bản ghi tài nguyên này trỏ đến
TTL (*Thời gian sống****)***	Sử dụng một số nguyên 32 bit để thể hiện thời gian tối đa tính bằng giây và máy chủ hoặc máy khách DNS lưu đệm mục này trước khi nó bị hủy bỏ. Trường này là tùy chọn, và nếu nó không được chỉ định, máy khách sẽ sử dụng giá trị TTL tối thiểu trong bản ghi tài nguyên SOA
Class (*Lớp)*	Định nghĩa các giao thức thông thường sử dụng, nó thường là ***IN*** cho các hệ thống Internet. Các giá trị khác được định nghĩa trong RFC 1034 là ***CH*** cho các hệ thống ***Chaos***, (một hệ thống được sử dụng để làm thí nghiệm trong Học viện công nghệ Massachusetts

Bảng 3-6 mô tả các dữ liệu có trong trường RDATA của bản ghi tài nguyên SRV:

Bảng 3-6. Các trường RDATA của bản ghi SRV:

Tên trường	Mô tả
Priority *(Thứ tự ưu tiên)*	Chỉ định thứ tự ưu tiên của máy. Các máy khách cố gắng liên lạc với máy mà có số thứ tự ưu tiên thấp nhất

Weight (*Trọng số*)	Thực hiện việc cân bằng tải. Khi giá trị trong trường ***Priority*** giống nhau trong hai hoặc nhiều bản ghi tài nguyên trong cùng một miền, các máy khách sẽ phải thử các bản ghi có trọng số cao thường xuyên hơn, chỉ trừ khi các máy khách có hỗ trợ một số kỹ thuật cân bằng tải nào khác
Port (*Cổng*)	Chỉ ra cổng của dịch vụ trên máy
Target *(Mục tiêu)*	Chỉ ra tên FQDN của máy cung cấp dịch vụ

Các ví dụ sau đây cho biết các bản ghi tài nguyên của hai máy chủ quản trị miền:

_ldap._tcp.contoso.com. IN SRV 0 0 80 dc1.contoso.com.

_ldap._tcp.contoso.com. IN SRV 10 0 80 dc2.contoso.com.

Ví dụ này không chỉ định một TTL. Do đó, các máy khách DNS sử dụng giá trị TTL nhỏ nhất được chỉ định trong bản ghi tài nguyên SOA.

Nếu máy tính cần thiết phải định vị một máy chủ ***Lightweight Directory Access Protocol*** (*Giao thức truy cập thư mục dựa trên trọng số nhẹ* - LDAP) trong miền ***contoso.com***, các máy khách DNS sẽ gửi một truy vấn SRV với tên sau:

_ldap._tcp.contoso.com.

Máy chủ DNS sẽ phản hồi lại với bản ghi SRV liệt kê trong ví dụ trước. Máy khách DNS sau đó sẽ lựa chọn giữa máy chủ DC1 và DC2 bằng cách nhìn vào giá trị ưu tiên của chúng. Bởi vì DC1 có giá trị ưu tiên thấp hơn, máy khách LDAP sẽ lựa chọn DC1. Trong ví dụ này, nếu giá trị ưu tiên là giống nhau, nhưng giá trị trọng số lại khác nhau, máy khách sẽ lựa chọn máy chủ quản trị miền một cách ngẫu nhiên với xác suất tương ứng với giá trị của trường ***Weight*** (*Trọng số*).

Tiếp theo, máy khách DNS sẽ yêu cầu một bản ghi A của ***DC1.contoso.com*** và máy chủ DNS sẽ gửi lại bản ghi A. Cuối cùng, máy khách sẽ cố gắng liên hệ với máy chủ quản trị miền sử dụng địa chỉ IP trong bản ghi A

Các máy tính chạy Windows 2000, Windows XP và Windows Server 2003 hỗ trợ RFC 2782, sẽ sử dụng bản ghi tài nguyên DNS để xác định địa chỉ của các dịch vụ (DNS SRV)

Các kiểu bản ghi tài nguyên khác

Bảng 3-7 thể hiện các bản ghi tài nguyên bổ sung và các RFC định nghĩa chúng. Rất nhiều bản ghi tài nguyên này chỉ được coi là thử nghiệm nên rất hiếm khi được sử dụng. Họ hệ điều hành Windows Server 2003 cung cấp hỗ trợ cho việc định nghĩa, lưu trữ và phục hồi lại các bản ghi tài nguyên này.

Để có thêm thông tin về mỗi kiểu bản ghi tài nguyên này, hãy xem các RFC tương ứng. (Xem ***http://www.rfc-ditor.org/rfcsearch.html*** để có thêm thông tin về các RFC)

Bảng 3-7 Các kiểu bản ghi tài nguyên khác hỗ trợ bởi Windows Server 2003.

Kiểu bản ghi	RFC
AAAA	**1886**
AFSDB	**1183**
HINFO	**1035**
ISDN	**1183**
KEY	**2535**
MB	**1035**
MG	**1035**
MINFO	**1035**
MR	**1035**
NXT	**2535**
OPT	**2671**
RP	**1183**
RT	**1183**
SIG	**2535**
TXT	**1035**
WKS	**1035**
X25	**1183**

Các bản ghi tài nguyên không định nghĩa trong RFC

Bên cạnh các kiểu bản ghi tài nguyên liệt kê trong RFC, Windows Server 2003 còn sử dụng các kiểu bản ghi tài nguyên thể hiện trong Bảng 3-8.

Bảng 3-8: Các loại Bản ghi Tài nguyên khác được Windows Server 2003 hỗ trợ

Tên	Mô tả
WINS	Bản ghi tài nguyên WINS chứa địa chỉ IP của các máy chủ WINS mà máy chủ DNS phải truy vấn để phân giải các truy vấn về bản ghi A. Máy chủ DNS trong Microsoft Windows NT, Windows 2000 hoặc Windows 2003 có thể sử dụng máy chủ WINS để tra cứu phần tên trạm (***Host***) của tên DNS không tồn tại trong vùng DNS có thẩm quyền của tên đó. Nếu một máy chủ DNS có thẩm quyền trong một vùng nhưng không có đủ các bản ghi A cần thiết, máy chủ DNS sẽ chỉ truy vấn máy chủ WINS
WINS-R	Bản ghi tài nguyên WINS tra cứu ngược (WINS-R) được sử dụng trong vùng tra cứu ngược để tìm phần tên máy trong tên DNS của một địa chỉ IP cụ thể. Máy chủ DNS sẽ gửi một truy vấn trạng thái NetBIOS của cạc mạng đến địa chỉ IP được chỉ định trong truy vấn nếu như vùng có thẩm quyền của địa chỉ IP được truy vấn không chứa bản ghi có địa chỉ IP này mà lại chứa bản ghi tài nguyên WINS-R
ATMA	Bản ghi tài nguyên Địa chỉ Chế độ Chuyển giao Không đồng bộ (A***synchronous Transfer Mode Address -*** ATMA), được định nghĩa bởi Diễn đàn ATM, được sử dụng để ánh xạ các tên miền DNS sang các địa chỉ ATM

Các bản ghi ủy thác và bản ghi gắn kết

Bản ghi ủy thác và bản ghi gắn kết là các bản ghi tài nguyên mà bạn thêm vào trong một vùng để ủy thác, giao phó một miền con cho một vùng riêng biệt nằm trên máy chủ DNS khác. Một ***bản ghi ủy thác*** được thể hiện bởi một bản ghi NS trong vùng mức cha trong đó liệt kê các máy chủ DNS có thẩm quyền chứa vùng mức con của miền con được ủy quyền đó. Một ***Bản ghi gắn kết*** là một bản ghi A trong vùng cha chỉ định việc ủy quyền một máy chủ DNS phục vụ một vùng con có chứa miền con được ủy thác

Ví dụ, máy chủ DNS mà chứa vùng của miền ***contoso.com*** sẽ ủy thác miền con ***na.contoso.com*** cho máy chủ DNS ***ns2.na.contoso.com***, đó là nơi mà vùng của miền ***na.contoso.com*** được lưu. Để tạo ra sự ủy quyền này, các bản ghi sau đây được thêm vào trong miền mức cha của ***contoso.com***

na.contoso.com. IN NS ns2.na.contoso.com
ns2.na.contoso.com. IN A 172.16.54.1

Khi một máy khách DNS gửi truy vấn cho một tên trong vùng mức con đến máy chủ DNS có thẩm quyền của vùng mức cha, máy chủ DNS có thẩm quyền của vùng mức cha sẽ kiểm tra vùng này. Bản ghi tài nguyên ủy quyền nói rằng máy chủ DNS nào đã được ủy quyền cho vùng mức con đó. Máy

chủ DNS có thẩm quyền của vùng mức cha sau đó có thể trả lại một tham chiếu trong đó chứa bản ghi ủy quyền đến máy khách DNS.

Một bản ghi gắn kết là cần thiết trong ví dụ này bởi vì ***ns2.na.contoso.com*** là thành viên của miền được ủy quyền ***na.contoso.com***. Tuy nhiên, nếu nó là thành viên của một miền khác, ví dụ như ***microsoft.com***, máy khách DNS có thể thực hiện việc phân giải tên chuẩn để phân giải tên của máy chủ DNS có thẩm quyền sang địa chỉ IP, đó là trường hợp không cần thiết phải có một bản ghi gắn kết. Chúng ta thường ít gặp các cấu hình miền tách biệt như vậy.

Việc ủy thác không đúng có thể là nguồn gốc của việc không thể phân giải tên trong DNS bởi vì một sự ủy thác không đúng có thể xóa bỏ một nhánh của cây không gian tên DNS, và các nút khác trong cây không thể định vị các tên DNS trong và dưới nhánh đó. Với lý do này, bạn nên xác nhận các sự ủy thác này một cách đều đặn và các cán bộ quản trị chịu trách nhiệm về các vùng mức cha và mức con phải trao đổi nếu như có bất kỳ sự chỉnh sửa nào mà có ảnh hưởng đến việc ủy thác.

Các Bản ghi Tài nguyên Đại diện (Wildcard Resource Record)

Trong một số bản thiết kế DNS, bạn có thể cần phải sử dụng một lượng lớn các bản ghi tài nguyên trong một vùng, tuy nhiên, bạn có thể thấy khó khăn khi phải thực hiện việc thêm các bản ghi tài nguyên một cách thủ công. Trong các trường hợp như vậy, bạn có thể định nghĩa một Bản ghi Tài nguyên DNS Đại diện

Sau đây là một ví dụ về địa chỉ đại diện từ miền ***contoso.com***

**** IN A 172.16.54.1***

Nếu bản ghi A trên có trong DNS, mọi truy vấn về một trạm trong miền ***contoso.com***, mà không được định nghĩa tường minh trong file của vùng, sẽ nhận được một phản hồi với địa chỉ 172.16.54.1. DNS trong Windows 2000 và Windows Server 2003 hỗ trợ bản ghi tài nguyên DNS đại diện.

HIỂU BIẾT VỀ QUÁ TRÌNH TRUY VẤN DNS

Khi một máy khách DNS cần tra cứu một tên để có được địa chỉ IP tương ứng, nó hình thành nên một truy vấn DNS chứa các thông tin sau đây:

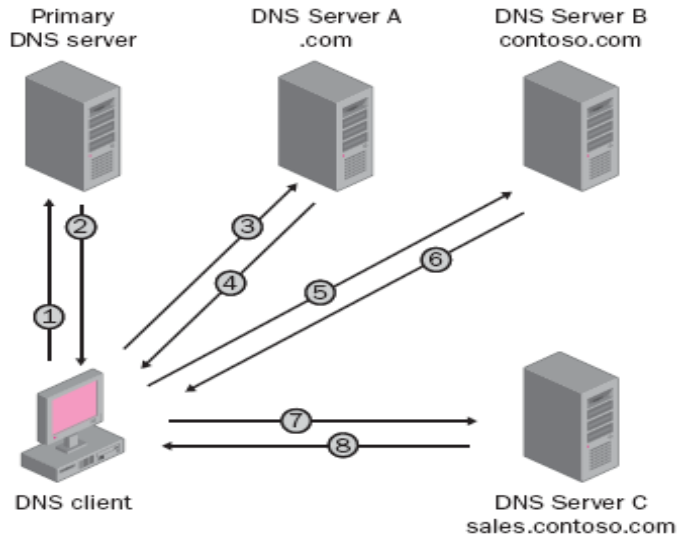
- *Tên miền DNS* dưới dạng một FQDN
- *Kiểu truy vấn* - chỉ định bản ghi tài nguyên sẽ được trả lại (A, SRV, ..vv..)
- *Phân lớp tên miền DNS*, đó là ***IN*** nếu như muốn trỏ ra Internet

Đầu tiên, truy vấn sẽ được chuyển đến dịch vụ phân giải tên DNS nội bộ trên máy khách để phân giải tên. Nếu như truy vấn này không thể được phân giải trong nội bộ, nó sẽ được gửi đến máy chủ DNS chính

Nếu như truy vấn không khớp với bất cứ mục nào trong bộ đệm dữ trữ, quá trình phân giải sẽ tiếp tục với việc máy khách sẽ truy vấn một máy chủ DNS để phân giải tên này. Các truy vấn từ máy khách hoặc máy chủ có thể thực hiện dưới hai định dạng: Lặp lại và đệ qui

Các truy vấn lặp

Một **truy vấn lặp** là một truy vấn DNS gửi đến một máy chủ DNS trong đó máy khách thực hiện truy vấn sẽ yêu cầu máy chủ trả về một câu trả lời tốt nhất mà nó có thể cung cấp, bằng cách sử dụng thông tin của nó mà không tìm kiếm sự trợ giúp nào từ các máy chủ DNS khác. Ví dụ, trong Hình 3-8, một máy trạm truy vấn máy chủ DNS chính, máy chủ này sẽ kiểm tra các bản ghi của nó và hướng máy khách đến một Máy chủ A. Máy chủ A sẽ kiểm tra bộ nhớ đệm tên của nó, không tìm thấy câu trả lời và gửi lại một tham chiếu thay thế đến máy chủ B. Máy khách nhận được phản hồi và gửi một truy vấn đến máy chủ B, máy chủ này trả lại một tham chiếu đến máy chủ C. Máy khách tiếp tục truy vấn máy chủ C và nhận được một phản hồi khác.



Hình 3-8. Quá trình truy vấn lặp

Như thể hiện trên hình 3-8, máy khách truy vấn sẽ có trách nhiệm thực hiện các truy vấn bổ sung cho đến khi nó nhận được câu trả lời cuối cùng. Trong ví dụ đó, máy khách này thực hiện ba truy vấn trước khi nhận được thông tin mà nó yêu cầu. Quá trình này như sau:

1. Bước đầu tiên của quá trình truy vấn là chuyển đổi tên yêu cầu thành một truy vấn và chuyển nó đến dịch vụ ***DNS Client*** để phân giải bằng cách sử dụng các thông tin trong bộ nhớ đệm. Nếu truy vấn này có thể trả lời được từ bộ nhớ đệm nội bộ, quá trình này hoàn thành. Nếu không, máy khách sẽ gửi một truy vấn lặp đến một máy chủ DNS chính của nó.

2. Máy chủ DNS chính kiểm tra để xem liệu nó có được ủy quyền cho miền đó không. Trong ví dụ này, nó không được ủy quyền nhưng nó lại chứa thông tin mà trỏ đến các máy chủ DNS của miền mức-đỉnh ***.com***. Máy chủ chính này sẽ phản hồi lại cho máy trạm với tham chiếu đến máy chủ miền mức-đỉnh ***.com***.

3. Máy khách DNS sẽ gửi một truy vấn lặp đến máy chủ DNS A

4. Máy chủ DNS A phản hồi với tham chiếu đến máy chủ DNS B

5. Máy khách gửi một truy vấn lặp đến máy chủ DNS B về miền ***sales.contoso.com***.

6. Máy chủ DNS B phản hồi với tham chiều đến máy chủ DNS C

7. Máy khách DNS sẽ gửi một truy vấn lặp đến máy chủ DNS C.

8. Máy chủ DNS C được ủy quyền cho miền ***sales.contoso.com*** và phản hồi lại một câu trả lời cuối cùng cho truy vấn của máy khách (trong trường hợp này là bản ghi A cho ***sales.contoso.com***)

Tính chất lặp lại được sử dụng trong các tình huống:

- Máy khách yêu cầu việc sử dụng đệ qui nhưng đệ qui lại không được kích hoạt trong máy chủ DNS

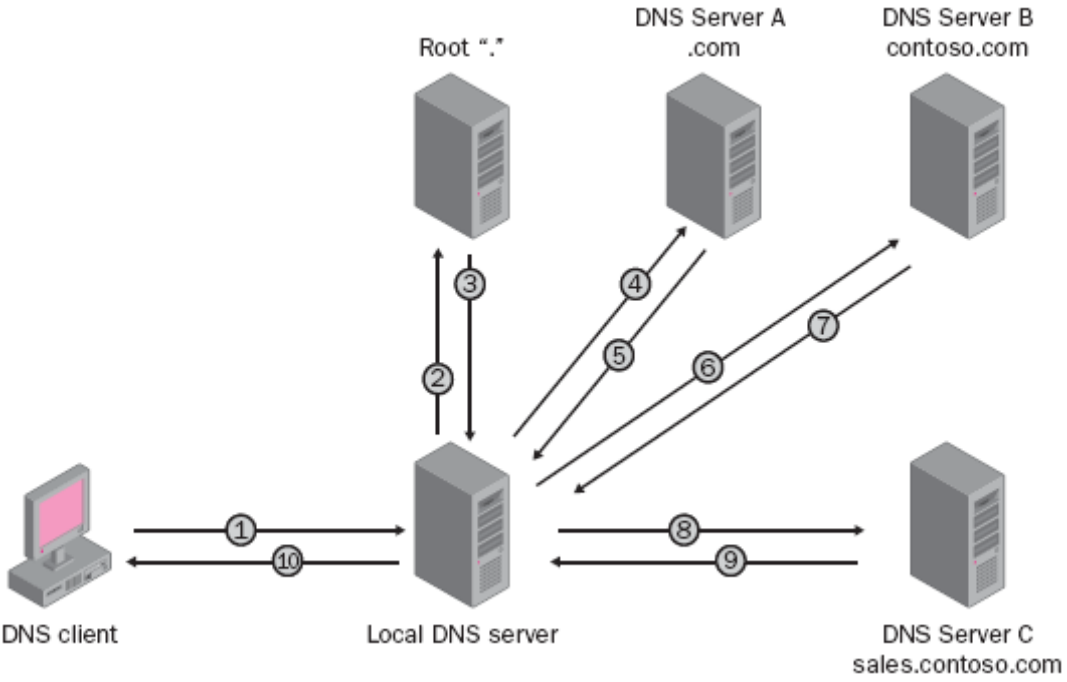
- Máy khách không yêu cầu sử dụng đệ qui khi truy vấn máy chủ DNS

- Yêu cầu truy vấn lặp từ máy khách thông báo cho máy chủ DNS rằng máy khách kỳ vọng câu trả lời tốt nhất mà máy chủ DNS có thể được cung cấp ngay lập tức mà không cần phải liên hệ với các máy chủ DNS khác.

Các truy vấn đệ qui

Một ***truy vấn đệ qui*** là một truy vấn DNS gửi đến một máy chủ DNS trong đó máy khách truy vấn sẽ yêu cầu máy chủ DNS cung cấp một câu trả lời

cuối cùng cho truy vấn đó, điều này có nghĩa là máy chủ DNS thậm chí phải liên hệ với các máy chủ khác để có thể cung cấp câu trả lời. Khi gửi đi một truy vấn đệ qui, máy chủ DNS sẽ truy vấn lặp các máy chủ khác để có thể có được câu trả lời. Trong Hình 3-9, máy khách truy vấn sẽ chỉ đưa ra một truy vấn trước khi nhận được thông tin mà nó yêu cầu.



Hình 3-9. Quá trình truy vấn đệ qui

Để tập trung mức tải và giảm lưu lượng mạng, các máy khách thông thường sẽ gửi các truy vấn đệ qui đến các máy chủ DNS. Một mạng với 1000 máy khách gửi truy vấn lặp đến các máy chủ DNS sẽ không hiệu quả bằng việc tập trung các truy vấn vào một máy chủ trung tâm nào đó. Việc tập trung các truy vấn có nghĩa là mỗi máy khách sẽ gửi đi một truy vấn đệ qui hơn là mỗi máy khách sẽ gửi đi nhiều truy vấn lặp. Các máy chủ DNS thông thường sẽ đưa ra các truy vấn lặp đến các máy chủ DNS khác nếu chúng không thể đưa ra câu trả lời cho truy vấn đệ qui từ thông tin có trong bộ nhớ đệm của nó. Bằng cách sử dụng các truy vấn đệ qui, mức tải của việc phân giải tên DNS có thể được tập trung vào một số máy chủ và do đó hệ thống có thể hoạt động hiệu quả hơn. Hình 3-9 thể hiện việc máy khách gửi một truy vấn đệ qui và nhận được một câu trả lời cuối cùng. Quá trình đó như sau:

1. Bước đầu tiên của quá trình truy vấn là chuyển đổi một yêu cầu tên sang một truy ván và sau đó chuyển nó tới dịch vụ DNS client để phân giải tên sử dụng các thông tin bộ đệm dữ trữ nội bộ. Nếu như có thể

trả lời được truy vấn này bằng bộ đệm dữ trữ, quá trình sẽ kết thúc. Nếu không, truy vấn này sẽ được chuyển đến máy chủ DNS nội bộ.

2. Máy chủ tên nội bộ kiểm tra xem liệu nó có được ủy quyền cho miền đó không. Trong ví dụ này, nó không được ủy quyền nhưng nó lại có chứa các ***root hint***. Máy chủ tên nội bộ sử dụng các ***root hint*** để bắt đầu tìm kiếm máy chủ tên mà được ủy quyền cho miền ***sales.contoso.com***. Nó sau đó sẽ truy vấn máy chủ tên mức gốc.

3. Máy chủ tên gốc sẽ gửi địa chỉ IP của các máy chủ tên của miền mức đỉnh ***.com*** trả lại cho máy chủ DNS nội bộ.

4. Máy chủ DNS nội bộ sẽ gửi một truy vấn lặp lại đến máy chủ DNS A (***.com***) của miền ***sales.contoso.com***

5. Máy chủ DNS A sẽ trả lời với tham chiếu đến máy chủ tên ***contoso.com***, máy chủ DNS B

6. Máy chủ DNS nội bộ sẽ gửi một truy vấn lặp lại khác đến máy chủ DNS B. ***contoso.com***

7. Máy chủ DNS B sẽ phản hồi với địa chỉ IP của máy chủ được ủy quyền, máy chủ DNS C

8. Máy chủ DNS nội bộ sẽ gửi một truy vấn lặp đến máy chủ DNS C

9. Máy chủ DNS C sẽ phản hồi bằng câu trả lời cuối cùng (trong trường hợp này là bản ghi A)

10. Máy chủ DNS nội bộ sẽ phản hồi với máy khách DNS bằng một câu trả lời cuối cùng.

11. Theo đúng như mong muốn của máy khách, một yêu cầu được gửi đi và được giải đáp bởi máy chủ DNS nội bộ. Thông tin có được bởi máy chủ DNS nội bộ sẽ được lưu vào bộ đệm dữ trữ để có thể trả lời các truy vấn sau đó.

Định thời gian truy vấn đệ qui. Theo mặc định, các máy chủ DNS sử dụng bộ định thời để xác định các khoảng thời gian lặp lại và khoảng thời gian hết hạn. Các giá trị này như sau:

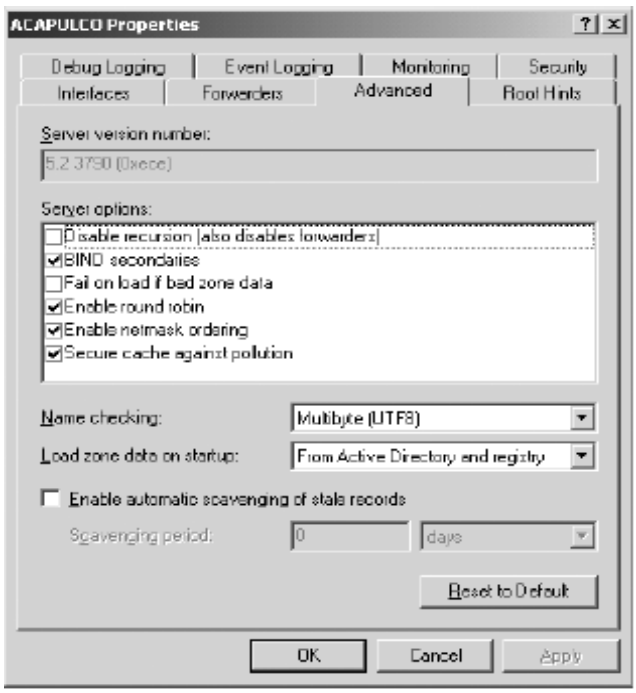
- Khoảng thời gian chờ thực hiện lại của truy vấn đệ qui là 3 giây. Đó là khoảng thời gian mà dịch vụ DNS sẽ đợi trước khi cố gắng tạo ra một truy vấn mới trong quá trình phân giải kiểu đệ qui.

- Khoảng thời gian hết hạn của một truy vấn đệ qui là 15 giây. Đó là khoảng thời gian mà dịch vụ DNS đợi trước khi xác định một phân giải đệ qui là không thành công sau khi đã cố gắng thực hiện.

Trong hầu hết các trường hợp, các tham số này không cần thiết phải chỉnh sửa. Tuy nhiên, nếu bạn đang sử dụng các tra cứu đệ qui trên một đường truyền WAN tốc độ chậm, bạn có thể cải thiện hiệu năng máy chủ và quá trình hoàn thành các truy vấn bằng cách điều chỉnh một chút các thiết lập này.

Việc vô hiệu hóa cách sử dụng truy vấn đệ qui trên một máy chủ DNS thông thường được thực hiện khi các máy khách DNS bị giới hạn chỉ phân giải tên bằng các máy chủ DNS xác định, ví dụ như máy chủ nằm trong mạng intranet nội bộ của bạn. Việc đệ qui có thể bị vô hiệu hóa trong trường hợp máy chủ DNS không có khả năng phân giải các tên DNS bên ngoài và các máy khách cũng mong muốn có thể được chuyển sang một máy chủ DNS khác để phân giải các tên này khi không thực hiện được trên máy này.

Bạn có thể vô hiệu hóa việc sử dụng đệ qui bằng cách cấu hình các thuộc tính trong trang ***Advance*** của bảng điều khiển DNS, như thể hiện trong Hình 3-10.



Hình 3-10. Trang thuộc tính Advance của DNS

> ***LƯU Ý. Vô hiệu hóa Đệ qui trong một máy chủ DNS****. Nếu bạn vô hiệu hóa đệ qui trong một máy chủ DNS, bạn sẽ không thể sử dụng các* ***forwarders*** *trên máy chủ này.*

Các phản hồi cho truy vấn

Hai ví dụ của các truy vấn DNS trên đây cho thấy quá trình được kết thúc bằng một phản hồi tin cậy, chắc chắn để trả lại cho máy khách. Tuy nhiên, các truy vấn có thể phản hồi lại bằng các câu trả lời khác nữa. Các câu trả lời sau đây là thông thường nhất:

- **Một câu trả lời có thẩm quyền**. Một câu trả lời được có thẩm quyền là một câu trả lời khẳng định để trả lại cho một máy khách và được chuyển đi với tập hợp các bit có thẩm quyền trong thông điệp DNS để thể hiện rằng câu trả lời là có từ một máy chủ có thẩm quyền trực tiếp của tên truy vấn đó.

- **Một câu trả lời tích cực.** Một câu trả lời tích cực có thể chứa bản ghi tài nguyên được truy vấn hoặc một danh sách các bản ghi tài nguyên (còn gọi là tập hợp các bản ghi tài nguyên) mà đáp ứng được tên miền DNS cần truy vấn và kiểu bản ghi có trong thông điệp truy vấn. Các câu trả lời có thể là có thẩm quyền hoặc không.

- **Một câu trả lời tham chiếu.** Một câu trả lời tham chiếu chứa các bản ghi tài nguyên bổ sung mà tên hoặc kiểu của nó không có trong truy vấn. Kiểu trả lời này được sử dụng để trả lời các máy trạm nếu không hỗ trợ kiểu truy vấn đệ qui. Các bản ghi này có ý nghĩa là một câu trả lời tham chiếu hữu ích cho máy khách tiếp tục quá trình truy vấn bằng sử dụng các truy vấn lặp.

  Một câu trả lời tham chiếu chứa các dữ liệu bổ sung, ví dụ như các bản ghi tài nguyên hơn là các kiểu truy vấn. Ví dụ, nếu tên máy khách được truy vấn là "***www***" và không bản ghi tài nguyên A nào của tên này được tìm thấy trong vùng này, tuy nhiên một bản ghi tài nguyên CNAME cho "***www***" lại được tìm thấy, máy chủ DNS có thể thêm các thông tin này vào câu trả lời khi gửi đến cho các máy khách.

  Nếu như máy khách sử dụng truy vấn lặp, nó có thể thực hiện các truy vấn bổ sung bằng cách sử dụng các thông tin tham chiếu có được trong một truy vấn nào đó để có thể phân giải tên một cách đầy đủ.

- **Một câu trả lời tiêu cực.** Một câu trả lời tiêu cực từ một máy chủ có thể biểu hiện của việc đã nhận được một trong hai kết quả tích cực có thể xảy ra sau khi máy chủ cố gắng xử lý và phân giải đệ qui truy vấn một cách đầy đủ và có ủy quyền.

- ❖ Máy chủ được ủy quyền báo cáo rằng tên được truy vấn không tồn tại trong không gian tên miền DNS.
- ❖ Máy chủ được ủy quyền báo cáo rằng tên đang truy vấn tồn tại nhưng không có bản ghi nào của kiểu xác định tồn tại cho tên đó.

Trình phân giải tên sẽ chuyển phản hồi cho truy vấn đó ngược lại cho chương trình đã yêu cầu và lưu phản hồi này vào bộ đệm dữ trữ.

Máy chủ tên lưu đệm (Name Server Caching)

Khi các máy chủ DNS tạo các truy vấn đệ qui thay mặt cho các máy khách, chúng sẽ lưu đệm tạm thời các bản ghi tài nguyên. Các bản ghi tài nguyên được lưu đệm sẽ chứa các thông tin lấy được từ các máy chủ DNS có thẩm quyền đối với các tên vùng, thông tin này có được trong quá trình tạo các truy vấn lặp để tìm kiếm và trả lời đầy đủ cho các truy vấn đệ qui thay cho các máy khách. Sau đó, khi máy khách khác gửi các truy vấn mới mà yêu cầu các thông tin của bản ghi tài nguyên trùng với các bản ghi tài nguyên có trong bộ đệm dữ trữ, máy chủ DNS có thể sử dụng các thông tin bản ghi tài nguyên lưu trong bộ đệm để trả lời chúng. Việc lưu đệm cung cấp một giải pháp để tăng hiệu năng của việc phân giải tên DNS đối với các truy vấn tuần tự của các tên thông dụng, trong khi dần dần giảm lưu lượng mạng của các truy vấn liên quan đến DNS trong hệ thống mạng.

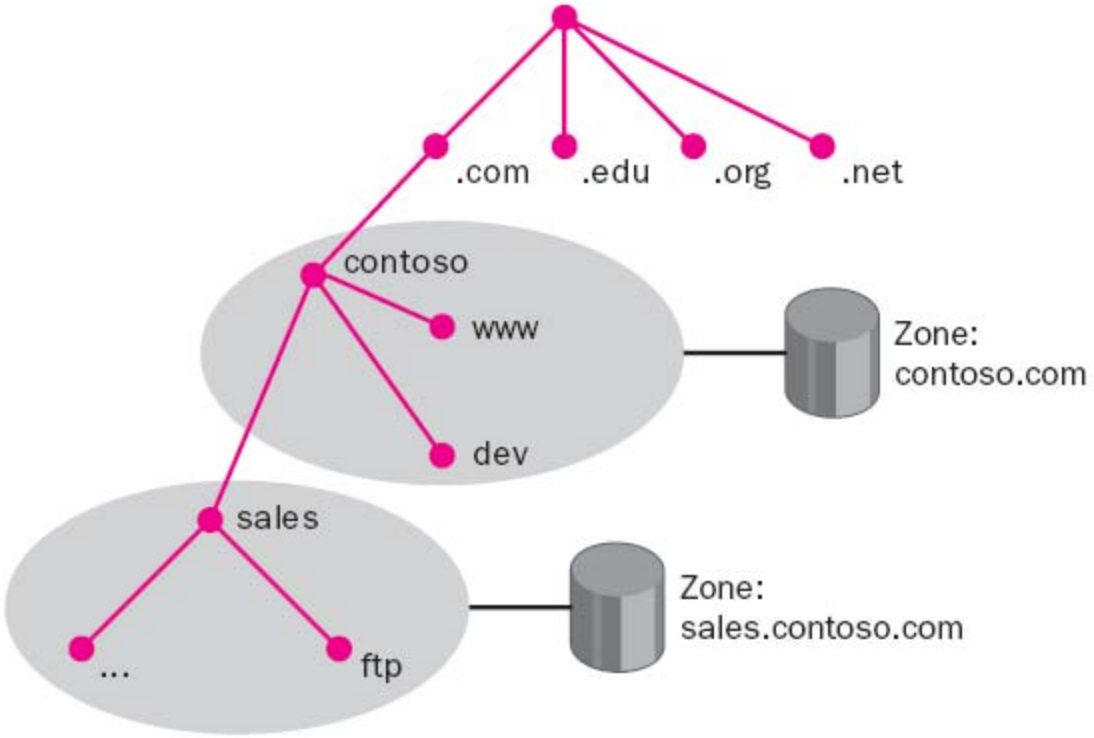
Khi các thông tin được lưu đệm, giá trị TTL sẽ áp dụng cho tất cả các bản ghi tài nguyên được lưu đệm. Khi TTL cho một bản ghi tài nguyên lưu đệm chưa hết hạn, máy chủ DNS có thể tiếp tục lưu đệm và sử dụng các bản ghi tài nguyên đó khi trả lời cho các truy vấn của các máy khách mà khớp với các bản ghi tài nguyên này. Các giá trị TTL lưu đệm sử dụng bởi các bản ghi tài nguyên trong hầu hết các cấu hình vùng đều được gán giá trị TTL tối thiểu (mặc định), giá trị này được thiết lập trong bản ghi tài nguyên SOA của vùng. Theo mặc định, giá trị TTL tối thiểu là 3600 giây (1 giờ) nhưng có thể được điều chỉnh hoặc nếu cần, các giá trị TTL lưu đệm riêng lẻ có thể được thiết lập trong mỗi bản ghi tài nguyên.

ỦY QUYỀN CHO CÁC VÙNG

Khởi đầu, một vùng chỉ lưu các thông tin về một tên vùng DNS đơn. Khi các miền khác được thêm vào, bạn phải quyết định về việc liệu miền thêm vào có là một phần của cùng một vùng đó hay không. Nếu bạn lựa chọn thêm một miền con, bạn có thể:

- Quản trị miền con như là một phần của vùng khởi đầu.
- Ủy quyền quản trị miền con cho một vùng khác.

Ví dụ, Hình 3-11 thể hiện miền ***contoso.com***, trong đó chứa tên miền của công ty ***Contoso, Ltd.*** Khi miền ***contoso.com*** được khởi tạo trên một máy chủ đơn, nó được cấu hình như là một vùng đơn cho tất cả không gian tên DNS của ***Contoso***. Tuy nhiên nếu miền ***contoso.com*** cần các miền con, các miền con phải được thêm vào trong vùng hoặc được ủy quyền sang vùng khác.



Hình 3-11. Sử dụng miền con để phân đoạn các vùng

Trong ví dụ này, miền ***contoso.com*** có một miền con mới - miền ***sales.contoso.com*** – được ủy thác khỏi vùng ***contoso.com*** và được quản trị trong vùng riêng của nó. Tuy nhiên, vùng ***contoso.com*** cần chứa một số bản ghi tài nguyên để cung cấp các thông tin ủy thác mà tham chiếu đến các máy chủ DNS được ủy quyền để quản trị miền con được ủy thác ***sales.contoso.com***.

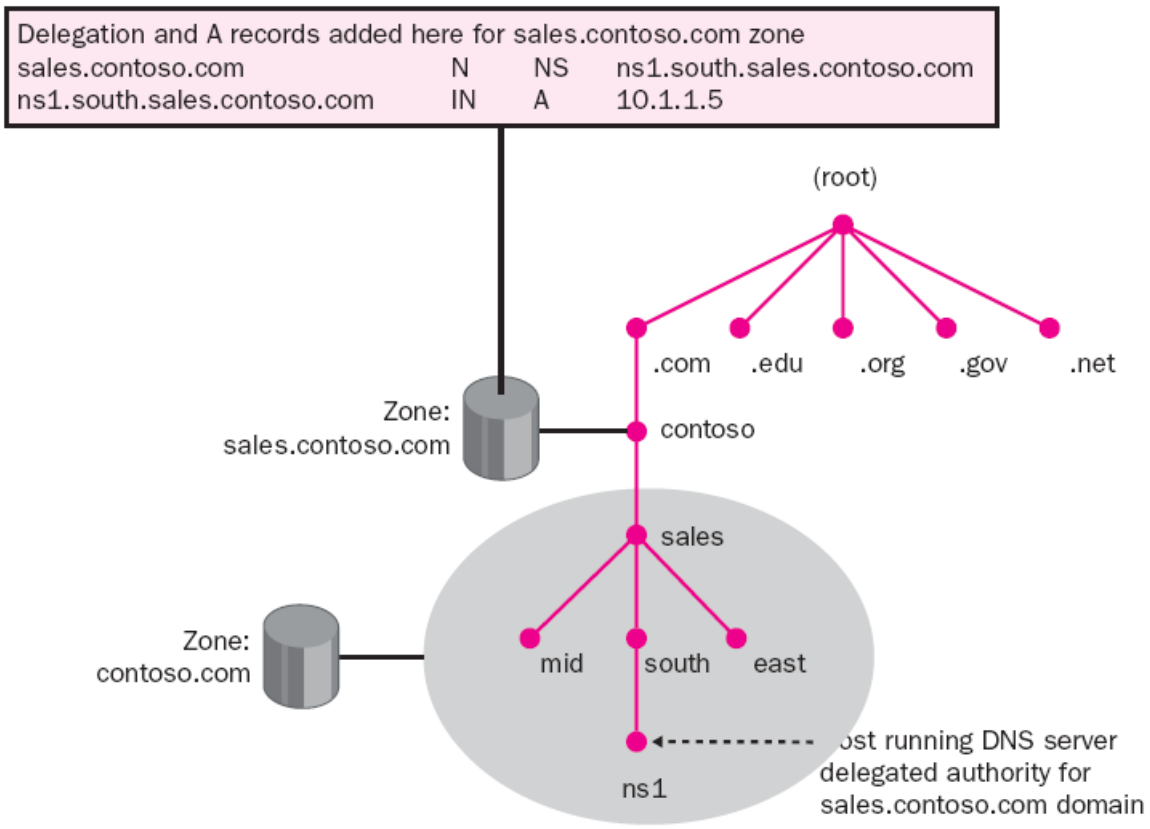
Nếu vùng ***contoso.com*** không sử dụng sự ủy thác đối với miền con, dữ liệu cho miền con vẫn là một phần của vùng ***contoso.com***. Ví dụ, miền con ***dev.contoso.com*** không được ủy thác, do vậy, chúng được quản trị bởi vùng ***contoso.com***.

Như đã thảo luận ở trên, các không gian tên có thể được phân chia thành một hoặc nhiều vùng. Các vùng có thể được lưu, phân phối và đồng bộ với các máy chủ DNS khác. Trước khi tạo ra thêm các vùng mới, hãy xác định xem liệu có các nhu cầu nào là đúng trong doanh nghiệp của bạn:

- Doanh nghiệp của bạn có nhu cầu ủy thác quản trị một phần không gian tên DNS cho vị trí khác hoặc phòng/ban khác.
- Bạn muốn cung cấp một môi trường DNS có khả năng chống lỗi tốt hơn
- Bạn muốn cải thiện hiệu năng của việc phân giải tên DNS bằng cách phân chia một vùng lớn thành nhiều vùng nhỏ, do đó phân phối mức tải giữa vài máy chủ.
- Doanh nghiệp của bạn đã mở một văn phòng chi nhánh mới hoặc địa điểm mới và bạn muốn mở rông không gian tên DNS bằng cách thêm vào rất nhiều miền con.

Nếu một trong các lý do kể trên là đúng đối với doanh nghiệp của bạn, việc ủy thác các vùng có thể đem lại nhiều lợi ích cho bạn. Khi xây dựng cấu trúc các vùng, hãy sử dụng một bản thiết kế phản ánh đúng cấu trúc của doanh nghiệp của bạn. Đồng thời, hãy lưu ý rằng đối với mỗi vùng mà bạn tạo ra, bạn cần các bản ghi ủy thác trong các vùng khác mà trỏ đến các máy chủ DNS được ủy quyền cho vùng mới. Điều này là cần thiết cho cả việc chuyển giao thẩm quyền và đồng thời cung cấp các tham chiếu đúng đắn đến các máy chủ và các máy khách DNS khác của máy chủ mới mà đang được ủy quyền cho vùng mới đó.

Hình 3-12 thể hiện sự ủy thác từ một vùng mức cha cho một vùng mới được tạo ra cho một miền con, ***sales.contoso.com***



Hình 3-12. Ủy thác một miền con cho một vùng mới

Trong Hình 3-12, máy chủ DNS có thẩm quyền của miền con mới được ủy thác là ***sales.contoso.com*** sẽ được đặt tên dựa vào các miền con phát sinh thêm trong vùng mới (***ns1.south.sales.contoso.com***). Để máy chủ này có thể biết đến các vùng mới được ủy thác khác bên ngoài, hai bản ghi tài nguyên trong vùng ***microsoft.com*** là cần thiết để hoàn thành việc cấp quyền cho vùng mới này:

- Một bản ghi tài nguyên NS là cần thiết để cho việc ủy thác này có hiệu quả. Bản ghi tài nguyên này được sử dụng để quảng bá rằng máy chủ có tên ***ns1.south.sales.contoso.com*** là máy chủ có thẩm quyền của miền con được ủy thác trên.

- Một bản ghi tài nguyên A (bản ghi gắn kết) cũng là cần thiết để phân giải tên của máy chủ trong bản ghi tài nguyên NS nói trên sang địa chỉ IP của nó. Quá trình phân giải tên máy trong bản ghi tài nguyên này thành máy chủ DNS được cấp quyền trong bản ghi NS đôi khi còn được gọi là sự *gắn kết theo* (***glue chasing***)

HIỂU BIẾT VỀ SỰ CHUYỂN GIAO VÙNG

Sự chuyển giao vùng là một quá trình chuyển giao hoàn toàn hoặc một phần của tất cả các dữ liệu trong một vùng từ một máy chủ DNS chính đang phục vụ vùng đó sang một máy chủ DNS thứ cấp chứa một bản sao của vùng đó. Bản sao của vùng được lưu trên máy chủ DNS thứ cấp cũng được khởi tạo bằng quá trình chuyển giao vùng. Khi có sự thay đổi trong vùng trên máy chủ DNS chính, máy chủ DNS chính sẽ thông báo các máy chủ DNS thứ cấp rằng có sự thay đổi xảy ra và các thay đổi này sẽ được đồng bộ tới tất cả các máy chủ DNS thứ cấp của vùng bằng cách sử dụng sự chuyển giao vùng.

Trong các qui định đầu tiên về DNS, chỉ có một kiểu chuyển giao vùng là có thể được thực hiện, đó là việc chuyển giao toàn bộ vùng (***Full zone transfer***). RFC 1995 đã bàn đến một kiểu bổ sung của việc chuyển giao vùng, đó là chuyển giao phần tăng thêm của vùng (***incremental zone transfer***). Windows Server 2003 hỗ trợ các chuyển giao phần tăng của vùng này. Phần này sẽ mô tả các kiểu chuyển giao vùng cũng như quá trình thông báo còn được gọi là Tin báo DNS

Các sự kiện sau đây sẽ kích hoạt việc chuyển giao vùng:

- Sự chuyển vùng được khởi tạo thủ công tại bảng điều khiển trên máy chủ thứ cấp
- Khoảng thời gian làm tươi vùng bị hết hạn
- Dịch vụ DNS Server khởi động tại máy chủ thứ cấp
- Máy chủ chính thông báo cho máy chủ thứ cấp về các thay đổi trong vùng.

Việc chuyển giao vùng luôn được khởi tạo tại máy chủ thứ cấp của vùng và gửi đến các máy chủ chủ đạo có trong cấu hình của nó, đóng vai trò là nguồn của vùng. Các máy chủ chủ đạo có thể là bất kỳ máy chủ DNS nào chứa vùng, ví dụ có thể là máy chủ chính của vùng hoặc các máy chủ thứ cấp khác. Khi máy chủ chủ đạo nhận được các yêu cầu về vùng này, nó có thể phản hồi bằng một sự chuyển vùng đầy đủ (IXFR) hoặc chuyển vùng phần tăng thêm (AXFR) cho máy chủ thứ cấp

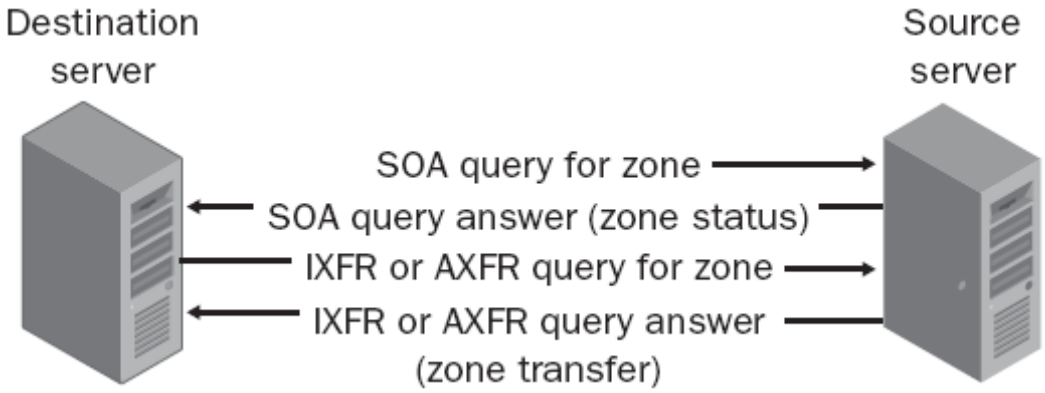
Trong chuyển vùng đầy đủ, máy chủ DNS chính có chứa vùng chính sẽ chuyển giao một bản sao của toàn bộ CSDL vùng sang máy chủ DNS thứ cấp mà chứa bản sao cũ của vùng. Dù trong chuyển giao vùng đầy đủ hay phần tăng thêm, quá trình được thực hiện đều giống như thể hiện trong Hình 3-13.

1. Khi giá trị của trường ***Refresh*** trong bản ghi tài nguyên SOA của vùng được chứa trong máy chủ DNS thứ cấp bị hết hạn, máy chủ DNS thứ cấp sẽ truy vấn máy chủ DNS chính về bản ghi tài nguyên SOA của vùng chính

2. Máy chủ DNS chính của vùng sẽ phản hồi lại truy vấn bằng một bản ghi tài nguyên SOA

3. Máy chủ DNS thứ cấp của vùng sau sẽ so sánh số thứ tự trong bản ghi SOA nhận được với số thứ tự trong bản ghi SOA của bản sao nội bộ của vùng. Nếu số thứ tự gửi bởi máy chủ DNS chính của vùng lớn hơn số thứ tự của vùng nội bộ của nó, vùng này cần được cập nhật và máy chủ DNS thứ cấp sẽ gửi một yêu cầu AXFR (một yêu cầu cho việc chuyển giao vùng đầy đủ) tới máy chủ DNS chính.

4. Máy chủ DNS chính sẽ nhận được yêu cầu cho việc chuyển giao vùng và sẽ gửi một bản CSDL vùng đầy đủ đến máy chủ DNS thứ cấp, về bản chất là tái tạo lại bản sao của vùng trong khi duy trì tất cả các thiết lập vùng



Hình 3-12. Quá trình chuyển giao vùng

Nếu máy chủ DNS chính của vùng không phản hồi lại yêu cầu về việc chuyển giao vùng gửi đi từ máy chủ DNS thứ cấp, máy chủ DNS thứ cấp sẽ tiếp tục cố gắng gửi lại sau khoảng thời gian chỉ định trong trường ***Retry*** của bản ghi tài nguyên SOA của vùng. Nếu vẫn không có câu trả lời sau khoảng thời gian chỉ định trong trường ***Expire*** trong bản ghi tài nguyên SOA của vùng, máy chủ DNS thứ cấp sẽ loại bỏ vùng của nó.

Chuyển giao vùng kiểu phần tăng.

Chuyển giao phần tăng thêm của vùng được thiết kế để giảm lưu lượng trên mạng gây ra bởi việc chuyển giao vùng đầy đủ. Thay vì việc gửi đi một bản sao của toàn bộ file của vùng, một sự chuyển giao phần tăng của vùng sẽ chỉ

gửi đi các bản ghi mà thay đổi từ lần cập nhật lần cuối cùng. Cả Windows 2000 và Windows Server 2003 đều hỗ trợ việc chuyển giao phần tăng của vùng.

Mặc dù các chuyển giao phần tăng của vùng sẽ tiết kiệm băng thông của mạng, nó sử dụng nhiều không gian đĩa trên máy chủ để ghi lại lịch sử của các phiên bản. Máy chủ DNS chính của vùng duy trì một lịch sử các phiên bản gần đây của vùng, nó theo dõi bất kỳ bản ghi nào đã thay đổi xảy ra trong các phiên bản được cập nhật gần đây nhất của vùng. Để giữ gìn không gian đĩa, các máy chủ DNS chỉ lưu các bản cập nhật gần nhất. Dịch vụ Windows Server 2003 DNS Server lưu các bản cập nhật này trong một file nhật ký nằm trong thư mục ***%systemroot%\System32\Dns***. File nhật ký này được đặt tên bằng cách sử dụng các tên của file của vùng với phần đuôi ***.log***. Ví dụ, nếu file của vùng của miền ***contoso.com*** được lưu thành ***contoso.com.dns***, file nhật ký sẽ được đặt tên là ***contoso.com.dns.log***

Một chuyển giao phần tăng thêm của vùng sẽ sử dụng quá trình như sau:

1. Khởi đầu, khi máy chủ thứ cấp được cấu hình lần đầu tiên, nó gửi một yêu cầu chuyển giao vùng đầy đủ (AXFR) đến máy chủ DNS chủ đạo. Máy chủ chủ đạo (nguồn) sẽ phản ứng bằng cách gửi một bản sao đầy đủ của vùng cho máy chủ thứ cấp (đích)

2. Mỗi lần chuyển giao vùng sẽ được đánh dấu bởi một phiên bản, thể hiện bằng một số thứ tự trong thuộc tính của bản ghi tài nguyên SOA và một khoảng thời gian làm tươi (theo mặc định là 900 giây). Khoảng thời gian làm tươi sẽ chỉ định khoảng thời gian mà máy chủ thứ cấp sẽ lại yêu cầu một bản sao khác của vùng từ máy chủ nguồn.

3. Khi khoảng thời gian này bị hết, máy chủ đích sẽ gửi đi một truy vấn SOA để yêu cầu một sự chuyển giao vùng kiểu phần tăng thêm.

4. Máy chủ nguồn sẽ trả lời truy vấn này bằng cách gửi đi bản ghi SOA của nó trong đó chứa số thứ tự đã đề cập ở trên.

5. Máy chủ đích sẽ so sánh số thứ tự trong bản ghi SOA này với số thứ tự nội bộ hiện tại của nó. Nếu hai số này là bằng nhau, không có chuyển giao vùng nào được yêu cầu và khoảng thời gian làm tươi sẽ bị xóa.

6. Nếu giá trị số thứ tự trong phản hồi SOA lớn hơn số thứ tự nội bộ hiện tại, các bản ghi của nguồn là mới hơn so với bản ghi nội bộ và một yêu cầu IXFR được gửi đến máy chủ nguồn. Truy vấn này bao gồm số

thứ tự nội bộ do đó máy chủ nguồn có thể xác định bản ghi nào mà máy chủ đích cần đến.

7. Tùy thuộc vào một vài yếu tố, máy chủ nguồn sẽ phản hồi bằng một sự chuyển giao vùng đầy đủ hoặc phần tăng thêm. Máy chủ DNS chính của vùng không được yêu cầu thực hiện một sự chuyển giao phần tăng của vùng. Nó có thể lựa chọn để thực hiện một chuyển giao vùng đầy đủ nếu trong các điều kiện sau đây:

   - ❖ Máy chủ DNS chính không hỗ trợ kiểu chuyển giao phần tăng thêm của vùng
   - ❖ Máy chủ DNS chính không có đủ dữ liệu cần thiết để thực hiện một chuyển giao phần tăng thêm của vùng.
   - ❖ Một chuyển giao phần tăng thêm của vùng sử dụng nhiều băng thông hơn một chuyển vùng đầy đủ.

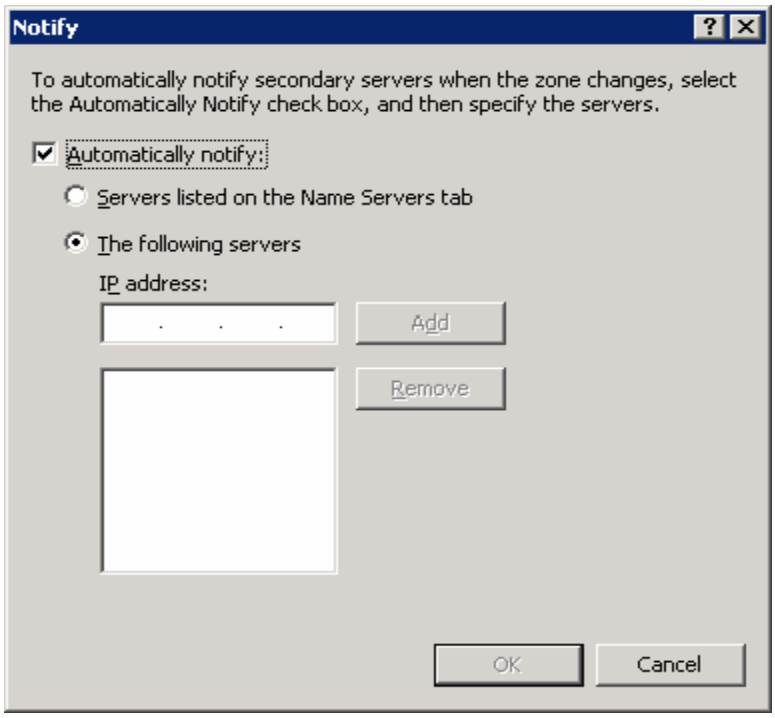
8. Khi máy chủ DNS thứ cấp nhận được một chuyển giao phần tăng thêm của vùng, nó tạo ra một phiên bản mới của vùng và bắt đầu thay thế các bản ghi tài nguyên lỗi thời bằng các bản ghi tài nguyên dược cập nhật từ máy chủ nguồn, áp dụng từ cũ nhất sang mới nhất. Khi tất cả các cập nhật được hoàn thành, máy chủ DNS thứ cấp thay thế phiên bản cũ của nó bằng phiên bản mới của vùng.

Thông báo DNS

Các máy chủ DNS dựa trên Windows hỗ trợ *Thông báo DNS*, một sự cập nhật cho giao thức DNS gốc, cho phép tạo thông báo đến các máy chủ thứ cấp khi có sự thay đổi vùng (RFC1996). Các máy chủ được thông báo sau đó có thể khởi tạo một chuyển giao vùng được mô tả trong phần trước để yêu cầu các thay đổi vùng từ máy chủ chủ đạo và cập nhật các bản sao nội bộ của vùng nó chứa. Quá trình này cải thiện việc đồng nhất trong dữ liệu của vùng.

Một danh sách các máy chủ DNS thứ cấp mà máy chủ DNS chính sẽ thông báo được duy trì trong *danh sách thông báo*, đó là một danh sách các địa chỉ IP của các máy chủ thứ cấp này. Khi vùng được cập nhật, máy chủ DNS chính của vùng chỉ thông báo các máy chủ DNS trong danh sách thông báo đó. Để các máy chủ DNS thứ cấp nhận được thông báo bởi máy chủ DNS mà đóng vai trò là máy chủ nguồn cấu hình của một vùng, mỗi máy chủ thứ cấp này phải có địa chỉ IP của mình trong danh sách thông báo của máy chủ nguồn. Trong DNS của Windows Server 2003, bạn có thể sử dụng hộp thoại

DNS Notify, truy cập từ bảng điều khiển DNS, thể hiện trong Hình 3-14, để thiết lập danh sách thông báo.



Hình 3-14. Hộp thoại DNS Notify

- **Tạo Danh sách thông báo của một vùng**

  Để tạo ra một danh sách thông báo của một vùng, thực hiện theo các bước sau:

  1. Nhấn ***Start***, trỏ vào ***Administrative Tools*** và sau đó nhấn ***DNS***
  2. Trong bảng điều khiển, nhấn vào vùng cần thực hiện
  3. Trong thực đơn ***Action***, nhấn vào ***Properties***
  4. Trong thẻ ***Zone Transfer***, nhấn vào ***Notify***
  5. Xác nhận rằng hộp thoại ***Notify Automatically*** được lựa chọn
  6. Lựa chọn phương pháp sẽ sử dụng để tạo ra một danh sách để thông báo các máy chủ khác khi trong vùng có sự thay đổi. Lựa chọn của bạn là như sau:
  7. Sử dụng tùy chọn "***Servers Listed On The Name Servers***" (Danh sách các máy chủ trong thẻ Name Servers) để cho phép chỉ các

máy chủ xuất hiện trong bảng địa chỉ IP trong thẻ ***Name Server*** được thêm vào trong danh sách thông báo.

8. Sử dụng tùy chọn "***The Following Servers***" nếu bạn muốn chỉ định một danh sách thông báo khác sẽ được sử dụng thay thế.

9. Nếu bạn lựa chọn "***The Following Servers***" trong bước trước, thêm hoặc bớt các địa chỉ IP máy chủ để tạo nên một danh sách thông báo khi cần:

10. Để thêm một máy chủ vào danh sách thông báo, nhập vào địa chỉ IP trong trường địa chỉ IP và sau đó nhấn ***Add***

11. Để bỏ một máy chủ trong danh sách thông báo, nhấn vào địa chỉ IP máy chủ trong hộp danh sách và sau đó nhấn ***Remove***

Ngoài việc thông báo các máy chủ trong danh sách, bảng điều khiển khiển DNS cho phép bạn sử dụng nội dung của danh sách thông báo như là một phương tiện để hạn chế hoặc giới hạn việc chuyển giao vùng chỉ truy cập các máy chủ thứ cấp trong danh sách này. Điều này có thể giúp ta ngăn chặn các truy cập không mong muốn bởi các máy chủ DNS không rõ nguồn gốc hoặc chưa được ủy thác để lấy hoặc yêu cầu các cập nhật của vùng.

Khi một vùng trong một máy chủ DNS được cập nhật, sự kiện sau đây xảy ra:

- Trường ***Serial Number*** (Số thứ tự) trong bản ghi SOA được cập nhật để thể hiện rằng một phiên bản mới của vùng đang được ghi vào đĩa

- Máy chủ DNS chính gửi một thông điệp thông báo đến các máy chủ DNS có trong danh sách thông báo của nó

- Một máy chủ DNS thứ cấp của vùng đó nhận được thông điệp thông báo sẽ phản hồi bằng cách gửi lại một truy vấn kiểu SOA đến máy chủ DNS chính mà đã thông báo để xác định liệu vùng trong máy chủ DNS chính có phải là bản mới hơn bản sao của vùng hiện đang lưu trong máy chủ DNS thứ cấp hay không.

- Nếu máy chủ thứ cấp được thông báo xác định rằng số thứ tự chỉ định trong bản ghi SOA của vùng trên máy chủ DNS chính là lớn hơn số thứ tự chỉ định trong bản ghi SOA của bản sao vùng hiện tại (vùng mà chứa nhiều bản ghi cập nhật gần đây hơn), máy chủ

DNS thứ cấp được thông báo sẽ yêu cầu một sự chuyển giao vùng (AXFR hoặc IXFR).

LƯU Ý. Các thông báo DNS trong các vùng tích hợp Active Directory*. Để đồng bộ các vùng tích hợp Active Directory, các thông báo DNS là không cần thiết. Đó là bởi vì các máy chủ DNS nạp vùng từ Active Directory sẽ tự động truy vấn thư mục (theo chỉ định bởi khoảng thời gian lặp trong bản ghi tài nguyên SOA) để cập nhật và làm tươi vùng này. Trong các trường hợp này, việc cấu hình một danh sách thông báo có thể làm giảm hiệu năng hệ thống do các yêu cầu chuyển giao thêm vào là không cần thiết đối với các vùng đã được cập nhật.*

HIỂU BIẾT VỀ SỰ CHUYỂN TIẾP (FORWARDING)

Một trạm chuyển tiếp (**forwarder)** là một máy chủ DNS trong mạng được sử dụng để chuyển tiếp các truy vấn DNS về các tên DNS bên ngoài đến một máy chủ DNS ngoài mạng. Một *chuyển tiếp có điều kiện* sẽ chuyển tiếp các truy vấn tùy vào các tên miền cụ thể.

Chuyển tiếp chuẩn

Như đã đề cập trước đây, một máy chủ DNS trên mạng được thiết kế là một máy chủ chuyển tiếp bằng cách cho phép các máy chủ DNS khác trong mạng chuyển tiếp các truy vấn mà chúng không thể phân giải nội bộ được đến máy chủ DNS đó. Bằng cách sử dụng máy chủ chuyển tiếp, bạn có thể quản trị việc phân giải tên cho các tên nằm ngoài hệ thống mạng của bạn, ví dụ như các tên trên Internet, và bạn sẽ cải thiện hiệu năng của việc phân giải tên cho các máy tính trong mạng của bạn. Ví dụ, để sử dụng các máy chủ chuyển tiếp để quản lý lưu lượng DNS giữa hệ thống mạng của bạn và Internet, cấu hình tường lửa trong mạng của bạn cho phép chỉ một máy chủ DNS có thể giao tiếp ra ngoài Internet. Khi bạn cấu hình các máy chủ DNS khác trong mạng chuyển tiếp các truy vấn mà chúng không thể phân giải nội bộ đến máy chủ DNS đó, nó sẽ đóng vai trò là một máy chủ chuyển tiếp của bạn.

Bởi vì các lưu lượng mạng ra ngoài đi qua một máy chủ DNS đơn, máy chủ đó sẽ phải có một lượng bộ nhớ đệm lớn của các dữ liệu DNS và do đó, theo thời gian, sẽ làm giảm lưu lượng Internet và cung cấp thời gian phản hồi nhanh hơn đế các máy khách.

Nếu không có một máy chủ DNS xác định đóng vai trò như một máy chủ chuyển tiếp, mọi máy chủ DNS khác có thể gửi các truy vấn ra ngoài mạng bằng cách sử dụng các root hints của nó. Kết quả là rất nhiều các thông tin DNS nội bộ, có thể là các thông tin rất quan trọng, có thể bị lộ ra ngoài Internet. Bên cạnh vấn đề bảo mật và kín đáo này, phương pháp phân giải này còn có thể tạo ra lượng lớn lưu lượng ra ngoài vừa đắt vừa không hiệu quả cho một hệ thống mạng có đường truyền Internet chậm hoặc một công ty phải trả chi phí Internet cao.

Một máy chủ mà được cấu hình như một máy chủ chuyển tiếp sẽ hoạt động khác một máy chủ DNS thông thường mà không phải là máy chủ chuyển tiếp. Một máy chủ DNS được cấu hình sử dụng một máy chủ chuyển tiếp sẽ hoạt động như sau:

- Khi máy chủ DNS nhận được một truy vấn, nó cố gắng phân giải truy vấn này bằng cách sử dụng các vùng chính và thứ cấp mà nó chứa và bằng cách sử dụng bộ nhớ đệm
- Nếu như truy vấn này không thể phân giải được bằng các dữ liệu nội bộ này, nó chuyển tiếp truy vấn này đến máy chủ mà có chức năng của một máy chủ chuyển tiếp
- Máy chủ DNS này sẽ đợi câu trả lời từ máy chủ chuyển tiếp trong một thời gian ngắn trước khi cố gắng liên hệ với các máy chủ chỉ định trong root hints.
- Thay vì gửi đi một truy vấn lặp chuẩn, khi một máy chủ DNS chuyển một truy vấn đến một máy chủ chuyển tiếp, theo mặc định nó sẽ gửi đi một truy vấn đệ qui đến máy chủ chuyển tiếp.

Chuyển tiếp có điều kiện

Việc chuyển tiếp có điều kiện sẽ cho phép một máy chủ DNS có thể chuyển tiếp các truy vấn đến các máy chủ DNS khác dựa trên tên miền DNS trong truy vấn đó. Với việc sử dụng các chuyển tiếp có điều kiện, một máy chủ DNS có thể được cấu hình chuyển tiếp tất cả các truy vấn mà nó nhận được cho các tên kết thúc bằng research.wingtiptoys.com đến một địa chỉ IP máy chủ DNS xác định hoặc tới một địa chỉ IP của nhiều máy chủ DNS.

Ví dụ, khi hai công ty, fabrikam.com và wingtiptoys.com, sát nhập hoặc cộng tác với nhau, họ có thể cho phép các máy khách từ không gian tên nội bộ của một công ty này có thể phân giải tên của các máy khách từ không gian tên của công ty kia.

Người quản trị của một công ty (fabrikam.com) có thể thông báo cho người quản trị mạng của công ty kia (wingtiptoys.com) một loạt các máy chủ DNS mà họ có thể sử dụng để gửi các truy vấn DNS đến để phân giải tên trong nội bộ không gian tên của công ty đầu tiên (fabrikam.com). Trong trường hợp này, các máy chủ DNS trong wingtiptoys.com sẽ được cấu hình để chuyển tiếp tất cả các truy vấn về tên kết thúc bởi fabrikam.com đến máy chủ DNS được ủy nhiệm chính của miền đó.

> ***LƯU Ý. Cách thức chuyển tiếp của máy chủ DNS ủy quyền***. *Các máy chủ DNS đã được ủy quyền không thể chuyển tiếp các truy vấn tùy vào tên miền mà chúng được ủy quyền. Ví dụ, máy chủ DNS được ủy quyền của vùng* ***widgets.microsoft.com*** *không thể chuyển tiếp các truy vấn về tên miền* ***widgets.microsoft.com***. *Nếu máy chủ DNS được cho phép làm điều đó thì nó sẽ vô hiệu hóa khả năng của máy chủ khi trả lời các truy vấn về tên miền* ***widgets.microsoft.com***. *Máy chủ DNS được ủy quyền của* ***widgets.microsoft.com*** *có thể chuyển tiếp các truy vấn cho các tên DNS mà kết thúc bởi* ***hr.widgets.microsoft.com*** *nếu miền* ***hr.widgets.microsoft.com*** *đã được ủy quyền cho máy chủ DNS khác.*

Các thiết lập cho máy chủ chuyển tiếp có điều kiện sẽ bao gồm các mục sau đây:

- Các tên miền mà máy chủ DNS sẽ chuyển tiếp các truy vấn
- Một hoặc nhiều địa chỉ IP của máy chủ DNS cho từng tên miền xác định

➢ **Cấu hình chuyển tiếp**

Để cấu hình chuyển tiếp, thực hiện theo các bước sau:

1. Mở DNS
2. Trong bảng điều khiển, nhấn vào máy chủ DNS cần cấu hình
3. Trong thực đơn ***Action***, nhấn vào ***Properties***.
4. Trong thẻ ***Forwarders***, để thực hiện chuyển tiếp có điều kiện, nhập vào tên miền; để thực hiện việc chuyển tiếp thông thường, lựa chọn ***All Other DNS Names***
5. Trong danh sách ***Selected Domain's Forwarder IP Address***, nhập vào địa chỉ ***IP*** của máy chủ chuyển tiếp và nhấn ***Add***

Thứ tự chuyển tiếp

Mỗi tên miền sử dụng để chuyển tiếp trong một máy chủ DNS sẽ được gắn với các địa chỉ IP của một hoặc nhiều máy chủ DNS. Một máy chủ DNS được cấu hình để chuyển tiếp sẽ sử dụng danh sách máy chủ chuyển tiếp của nó sau khi nó xác định rằng nó không thể phân giải truy vấn bằng cách sử dụng các dữ liệu mà nó có thẩm quyền (các dữ liệu của vùng chính hoặc vùng thứ cấp) hoặc các dữ liệu trong bộ đệm của nó. Nếu máy chủ không thể phân giải một truy vấn bằng cách sử dụng các máy chủ chuyển tiếp, nó có thể cố gắng gửi các truy vấn đệ qui đến các máy chủ ***root hint.***

Thứ tự của các địa chỉ IP liệt kê sẽ xác định thứ tự mà các địa chỉ IP đó được sử dụng. Sau khi máy chủ DNS chuyển các truy vấn đến máy chủ chuyển tiếp bằng địa chỉ IP đầu tiên gắn với tên miền, nó sẽ đợi câu trả lời trong một khoảng thời gian ngắn từ máy chủ chuyển tiếp (tùy thuộc vào thiết lập thời gian hết hạn trên máy chủ DNS) trước khi thực hiện chuyển lại lần nữa đến địa chỉ IP tiếp theo mà gắn với tên miền đó. Nó sẽ tiếp tục quá trình này đến khi nó nhận được câu trả lời khẳng định từ một máy chủ chuyển tiếp hoặc cho đến khi nó đã thử hết tất cả các địa chỉ trong danh sách đó.

Khi một máy chủ DNS mà cấu hình sử dụng chuyển tiếp có điều kiện nhận được một truy vấn về một tên miền, nó sẽ so sánh tên miền đó với danh sách các tên miền điều kiện và sử dụng các tên miền điều kiện dài nhất mà phù hợp với tên miền trong truy vấn. Ví dụ, một máy chủ DNS nhận được một truy vấn về ***www.qualitycontrol.research.wingtiptoys.com***.

Nó sẽ so sánh tên miền đó với cả ***wingtiptoys.com*** và ***research.wingtiptoys.com.*** Máy chủ DNS sẽ xác định rằng ***research.wingtiptoys.com*** là tên miền gần nhất với tên trong truy vấn ban đầu.

Máy chủ chỉ chuyển tiếp

Một máy chủ DNS có thể được cấu hình không thực hiện đệ qui sau khi việc chuyển tiếp không thành; nếu nó không nhận được một phản hồi thành công cho truy vấn đó từ bất kỳ một máy chủ nào mà cấu hình như máy chủ chuyển tiếp, nó sẽ gửi một phản hồi tiêu cực đến máy khách DNS.

Tùy chọn để ngăn cản việc đệ qui có thể được thiết lập cho từng máy chủ chuyển tiếp có điều kiện trong Windows Server 2003. Ví dụ, một máy chủ DNS có thể được cấu hình để thực hiện đệ qui cho tên miền ***research.wingtiptoys.com,*** nhưng không thực hiện đệ qui cho tên miền ***wingtiptoys.com***.

***LƯU Ý. Vô hiệu hóa đệ qui**. Nếu bạn vô hiệu hóa đệ quy trong thẻ **Advance** trong trang thuộc tính của máy chủ DNS, bạn sẽ không thể sử dụng các máy chủ chuyển tiếp trên cùng một máy chủ.*

KẾT NỐI CÁC MẠNG NỘI BỘ RA INTERNET.

Mặc dù có thể cấu hình các máy chủ DNS bên trong tường lửa của bạn để sử dụng cùng tên DNS như khi sử dụng để truy cập chúng từ bên ngòai tường lửa, tuy nhiên điều này là không được khuyến khích. Để sử dụng không gian tên khác cho mạng nội bộ của bạn, ta nên thêm vào một hậu tố "***.local***" vào tên miền của bạn (ví dụ ***example contoso.local***) hơn là sử dụng không gian tên bên ngòai của bạn (ví dụ ***contoso.com***)

Chúng ta sẽ xem xét ba cách mà một tên DNS được phân giải khi các khuyến cáo trên được sử dụng; phân giải một tên miền DNS nội bộ cho doanh nghiệp này, phân giải một tên DNS ngoài cho doanh nghiệp mà không sử dụng máy chủ proxy và phân giải một tên DNS ngoài cho doanh nghiệp mà có sử dụng máy chủ proxy. Trong kịch bản sau đây, Contoso, Ltd được cấu hình với mạng ngoài của nó sử dụng tên ***contoso.com*** và mạng trong của nó sử dụng tên ***contoso.local***. Hai vùng này sẽ được phân tách với nhau bởi tường lửa và bên ngòai tường lửa, máy chủ DNS sẽ được cung cấp bởi ISP của công ty Contoso, Ltd

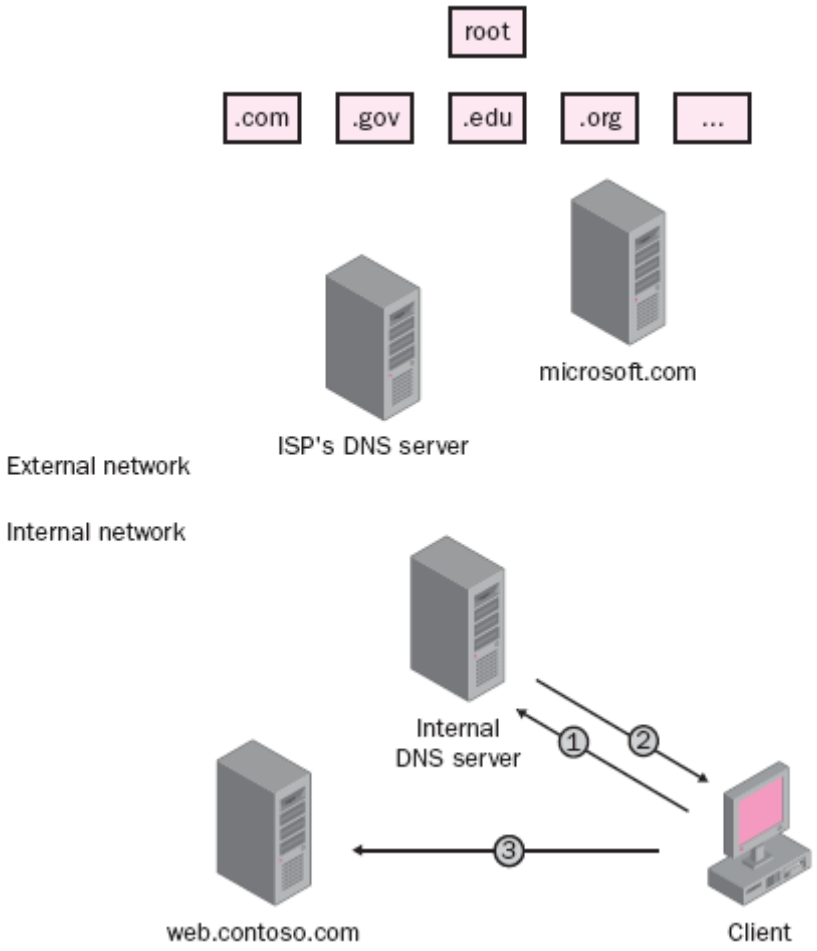
Phân giải các tên nội bộ

Một máy khách muốn truy cập Web site nội bộ, ***web.contoso.local***. Quá trình phân giải tên diễn ra như sau: (Xem Hình 3-15)

1. Máy khách gửi một truy vấn về tên ***web.contoso.local*** đến máy chủ DNS nội bộ

2. Máy chủ DNS nội bộ phân giải tên ***web.contoso.local*** sang địa chỉ IP và gửi kết quả lại cho máy trạm

3. Máy khách khởi tạo một kết nối đến ***web.contoso.local***



Hình 3-15. Phân giải các tên nội bộ

Phân giải tên ngoài khi không có máy chủ Proxy

Các máy chủ DNS nội bộ của Contoso, Ltd được cấu hình chuyển tiếp các yêu cầu về địa chỉ IP đến các máy chủ DNS bên ngoài cung cấp bởi ISP. Trong kịch bản này, một máy khách cần truy cập trang ***support.microsoft.com***. Quá trình phân giải tên diễn ra như sau: (Xem Hình 3-16).

12. Máy khách gửi một truy vấn về ***support.microsoft.com*** đến máy chủ DNS nội bộ

13. Máy chủ DNS nội bộ chuyển tiếp truy vấn này đến máy chủ DNS bên ngoài mà ISP cung cấp

14. Máy chủ DNS bên ngoài lại không được ủy quyền của miền này nên nó kiểm tra bộ nhớ đệm của nó. Nếu không tìm thấy mục nào

về tên ***support.microsoft.com*** này, nó sẽ chuyển tiếp truy vấn này đến miền gốc mức đỉnh (***top-level root domain***)

15. Máy chủ ***top-level root*** phản hồi lại cho máy chủ DNS bên ngoài một danh sách của các máy chủ ***.com***

16. Máy chủ DNS bên ngoài chuyển tiếp truy vấn về ***microsoft.com*** đến máy chủ ***.com***

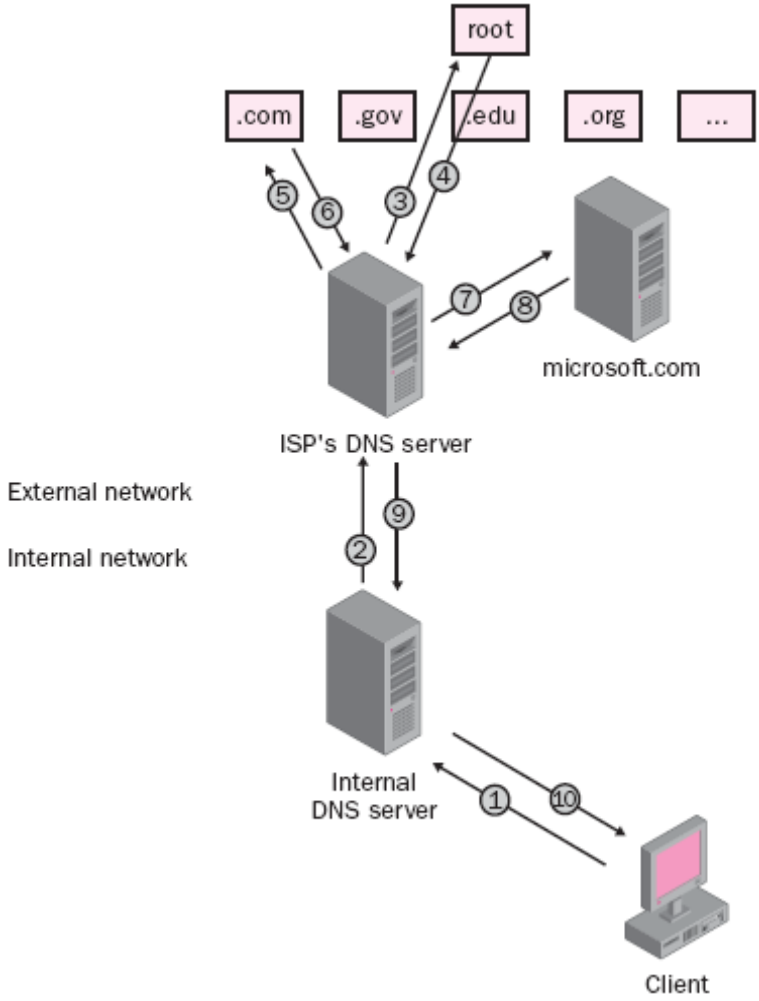
17. Máy chủ ***.com*** phản hồi lại cho máy chủ DNS bên ngoài với địa chỉ IP của ***microsoft.com***

18. Máy chủ DNS bên ngoài chuyển tiếp truy vấn về ***support.microsoft.com*** đến máy chủ ***microsoft.com***

19. Máy chủ ***microsoft.com*** phản hồi lại cho máy chủ DNS bên ngoài với địa chỉ của địa chỉ của ***support.microsoft.com***

20. Máy chủ DNS bên ngòai này lại chuyển tiếo địa chỉ này đến máy chủ DNS nội bộ

21. Máy chủ DNS nội bộ chuyển tiếp thông tin yêu cầu đến máy khách.



Hình 3-16. Phân giải các tên bên ngoài

Phân giải tên ngoài bằng cách sử dụng một proxy

Để phân giải ***support.microsoft.com*** bằng cách sử dụng máy chủ proxy, quá trình truy vấn như sau: (Xem Hình 3-17).

1. Máy khách proxy gửi một truy vấn về ***Microsoft.com*** đến máy chủ proxy

2. Máy chủ proxy xác định đây là một địa chỉ ngoài và chuyển tiếp yêu cầu này đến máy chủ DNS ngoài mà nó đã được cấu hình

3. Máy chủ DNS bên ngoài kiểm tra bộ đệm của nó về địa chỉ này và nếu nó không tìm thấy nó sẽ gửi một yêu cầu đến máy chủ mức đỉnh của miền ***.com***

4. Máy chủ mức đỉnh của miền ***.com*** sẽ gửi địa chỉ của miền ***.com*** đến máy chủ DNS bên ngoài

5. Máy chủ DNS bên ngoài chuyển tiếp yêu cầu về ***microsoft.com*** đến miền ***.com***

6. Miền ***.com*** gửi địa chỉ cỉa ***microsoft.com*** đến máy chủ DNS bên ngòai

7. Máy chủ DNS bên ngòai sẽ chuyển tiếp yêu cầu đến máy chủ DNS của ***Microsoft.com***

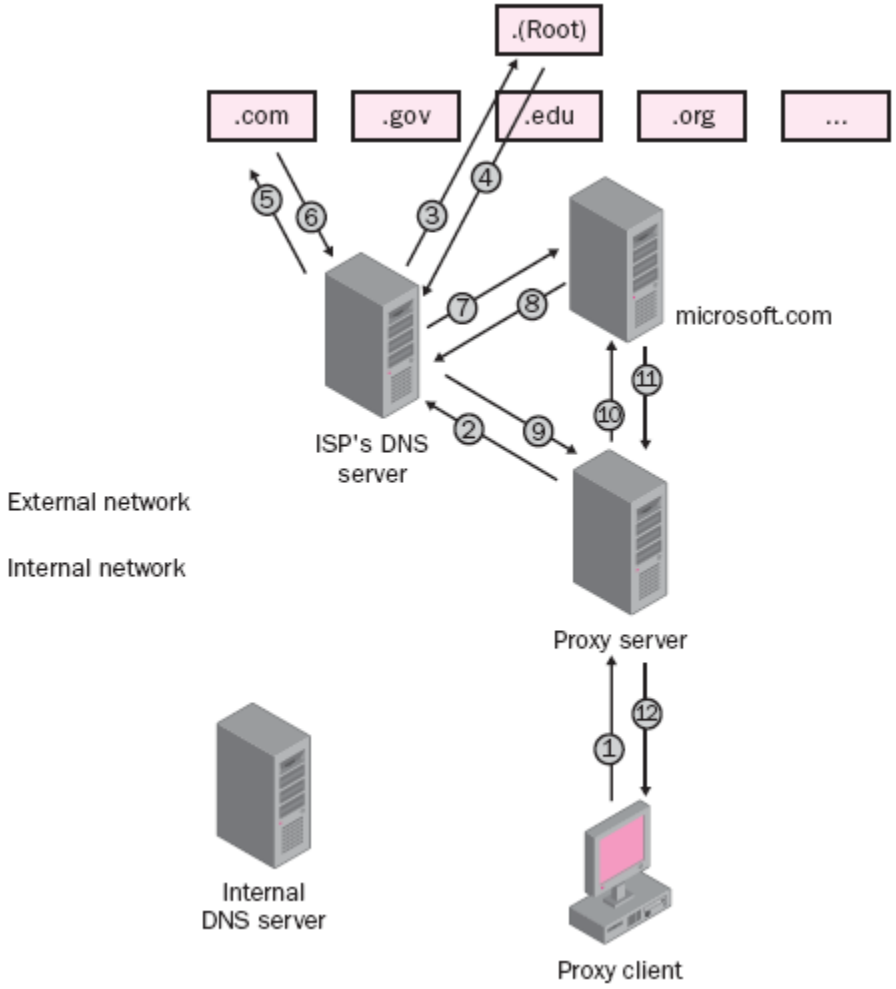
8. Máy chủ DNS của ***Microsoft.com*** phân giải truy vấn và phản hồi lại cho máy chủ DNS bên ngoài

9. Máy chủ DNS bên ngoài chuyển tiếp phản hồi này lại cho máy chủ proxy.

10. Sau khi máy chủ proxy nhận được phản hồi từ máy chủ DNS bên ngoài, nó truy vấn trực tiếp ***microsoft.com*** về địa chỉ của ***support.microsoft.com***

11. Máy chủ DNS của ***Microsoft.com*** sẽ phản hồi lại yêu cầu này và gửi các thông tin yêu cầu đến máy chủ proxy

12. Máy chủ proxy gửi phản hồi lại cho máy khách.



Hình 3-17. Phân giải các tên bên ngoài sử dụng máy chủ proxy

TỔNG KẾT

- Các tên DNS và giao thức DNS được yêu cầu cho các miền dựa trên Active Directory và để tương thích với Internet

- Không gian tên DNS có tính chất phân cấp và dựa trên một gốc duy nhất mà có thể có rất nhiều miền con. Một FQDN là một tên của một máy DNS trong không gian tên này thể hiện vị trí của máy này trong sự liên hệ với gốc của miền DNS hình cây. Một ví dụ của một FQDN là host1.subdomain.microsoft.com

- Một vùng DNS là một phần liên tục của một không gian tên mà trong đó một máy chủ có thẩm quyền. Một máy chủ có thể có thẩm quyền trong một hoặc nhiều vùng, và một vùng có thể chứa một hoặc nhiều miền liên tục. Một máy chủ gọi là có thẩm quyền cho một vùng nếu nó chứa vùng đó trong vai trò là máy chủ DNS chính hoặc thứ cấp. Mỗi vùng DNS chứa các bản ghi tài nguyên mà nó cần để trả lời các truy vấn về phần của nó trong không gian tên DNS

- Có một số kiểu máy chủ DNS: chính (***Primary***), thứ cấp (***Secondary***), tên chủ (***Master Name***) và chỉ đệm (***Caching Only***)
  - Một máy chủ DNS mà chứa một vùng DNS chính sẽ được gọi là máy chủ DNS chính. Các máy chủ DNS chính lưu các dữ liệu nguồn gốc cho các vùng đó. Với Windows Server 2003, bạn có thể triển khai các vùng chính theo một trong hai cách sau: Như một vùng chính chuẩn, trong đó các dữ liệu của vùng được lưu trong một file văn bản, hoặc như một vùng tích hợp Active Directory, trong đó dữ liệu của vùng được lưu trong CSDL Active Directory.
  - Một máy chủ DNS mà chứa một vùng DNS thứ cấp sẽ được gọi là máy chủ DNS thứ cấp. Các máy chủ DNS thứ cấp là máy chủ dự phòng có thẩm quyền của máy chủ chính. Các máy chủ mà từ đó máy chủ thứ cấp yêu cầu các thông tin của vùng sẽ được gọi là các máy chủ tên chủ đạo (***Master***).
  - Một máy chủ tên chủ đạo (***Master***) có thể là máy chủ chính hoặc máy chủ thứ cấp

- ❖ Máy chủ chỉ-đệm chuyển tiếp các yêu cầu đến các máy chủ DNS khác và không chứa một vùng nào cả, nhưng lại có một bộ đệm của các bản ghi thường xuyên được yêu cầu.

- Đệ qui là một hoặc nhiều kiểu quá trình phân giải tên DNS. Một máy khách DNS sẽ yêu cầu một máy chủ DNS cung cấp một câu trả lời hoàn chỉnh cho một truy vấn mà không bao gồm việc trỏ đến các máy chủ DNS khác, hiệu quả trong việc phân chia mức tải của việc phân giải tên từ máy khách đến máy chủ DNS. Để các máy chủ DNS thực hiện đệ qui một cách đúng đắn, máy chủ cần biết nó phải bắt đầu tìm tên ở đâu trong không gian tên DNS. Thông tin này được cung cấp bởi file ***root hint***, ***cache.dns*** được lưu trong máy chủ.

- Một máy chủ DNS trong mạng được thiết kế như một máy chủ chuyển tiếp khi các máy chủ DNS khác trong mạng chuyển các truy vấn mà chúng không phân giải nội bộ được đến máy chủ DNS đó. Việc chuyển tiếp có điều kiện cho phép một máy chủ DNS chuyển các truy vấn đến các máy chủ DNS khác dựa trên tên miền DNS trong các truy vấn đó.

BÀI TẬP

***QUAN TRỌNG. Hoàn thành tất cả các bài tập**. Nếu bạn có kế hoạch làm tất cả các bài tập trong sách lý thuyết trong chương này, bạn phải làm tất cả các bài tập trong chương rồi khôi phục máy tính trở lại trạng thái gốc của nó trước khi làm các bài tập trong sách BÀI TẬP THỰC HÀNH. Lưu ý rằng các bài tập sau đâ yêu cầu cài đặt DNS và DHCP, đó là trạng thái của máy tính học viên sau khi hoàn thành Bài tập Thực hành 3-1 trong sách BÀI TẬP THỰC HÀNH*

Bài tập 3-1. Thêm vai trò máy chủ DNS

Trong bài tập này, bạn sẽ sử dụng trang "***Manage Your Server***" (Quản trị máy chủ của bạn) để thêm vào vai trò máy chủ DNS.

1. Nhấn Start, trỏ vào Administrative Tools, và sau đó lựa chọn Manage Your Server
2. Trang ***Manage Your Server*** sẽ tự động khởi tạo theo mặc định sau khi đăng nhập
3. Trong trang ***Manage Your Server***, nhấn vào ***Add/Remove A Role***
4. Trong trang ***Preliminary Steps***, nhấn ***Next***
5. Trong trang ***Server Roles***, nhấn vào ***DNS Server*** và sau đó nhấn ***Next***
6. Trong trang ***Summary Of Selections,*** nhấn ***Next***
7. Trong trang ***Welcome To The Configure A DNS Server Wizard***, nhấn ***Next***
8. Trong trang ***Select Configuration Action***, nhấn vào ***Configure Root Hints Only (Recommended For Advanced Users Only)*** và sau đó nhấn ***Next***
9. Trong trang ***Completing The Configure A DNS Server Wizard***, nhấn ***Finish***
10. Trong trang ***This Server Is Now A DNS Server,*** nhấn ***Finish***

Bài tập 3-2. Thêm một vùng phân giải xuôi chính thức chuẩn

Trong bài tập này bạn sẽ sử dụng bảng điều khiển DNS để thêm vào một vùng phân giải xuôi chính chuẩn

1. Nhấn ***Start***, trỏ vào ***Administrative Tools***, và sau đó lựa chọn ***DNS***
2. Trong bảng điều khiển, chọn sau đó nhấn phải chuột vào ***ComputerName*** (trong đó ***ComputerName*** là tên máy tính của bạn) và sau đó nhấn ***New Zone***
3. Trong trang ***Welcome To The New Zone Wizard***, nhấn ***Next***
4. Trong trang ***Zone Type***, nhấn vào ***Primary Zone*** và xóa lựa chọn ***Store The ZoneIn Active Directory (Available Only If DNS Server Is A Domain Controller)*** rồi nhấn ***Next***.
5. Trong trang ***Forward Or Reverse Lookup Zone,*** nhấn vào ***Forward Lookup Zone*** và sau đó nhấn ***Next***.
6. Trong trang ***Zone Name,*** trong hộp thoại ***Zone Name,*** nhập vào ***computername.contoso.com***, và sau đó nhấn ***Next***
7. Trong trang ***Zone File,*** xác nhận rằng hộp chọn ***Create A New File With This File Name*** được lựa chọn và tên ***computername.contoso.com.dns*** được hiển thị trên hộp và sau đó nhấn ***Next***
8. Trong trang ***Dynamic Update,*** xác nhận rằng hộp chọn ***Do Not Allow Dynamic Updates*** được lựa chọn và nhấn ***Next***
9. Trong trang Completing The New Zone Wizard, nhấn Finish

Bài tập 3-3. Chuyển sang vùng tích hợp Active Directory

Trong bài tập này, bạn sẽ chuyển một vùng chuẩn sang vùng chính tích hợp Active Directory

1. Nhấn ***Start***, trỏ vào ***Administrative Tools***, và sau đó lựa chọn ***DNS***
2. Trong bảng điều khiển, chọn sau đó nhấn phải chuột vào ***ComputerName*** (trong đó ***ComputerName*** là tên máy tính của bạn), mở rộng ***Forward Lookup Zones***, nhấn phải chuột vào ***computername.contoso.com***, và sau đó nhấn vào ***Properties***

3. Trong thẻ ***General***, nhấn vào ***Change***

4. Trong cửa sổ Change Zone Type, lựa chọn Store The Zone In Active Directory (Available Only If DNS Server Is A Domain Controller), và sau đó nhấn OK

5. Khi bạn được hỏi rằng liệu bạn có muốn vùng này trở thành vùng ***tích hợp Active Directory*** không, nhấn ***Yes.***

6. Để đóng cửa sổ trang Properties của computername.contoso.com, nhấn OK

7. Trong bảng điều khiển, nhấn vào ***Forward Lookup Zones***, và trong khung chi tiết, lưu ý rằng bây giờ, kiểu của vùng ***computername.contoso.com*** đã chuyển thành vùng tích hợp Active Directory

Bài tập 3-4. Tạo ra vùng phân giải ngược

Trong bài tập này, bạn sẽ tạo ra một vùng phân giải ngược

1. Nhấn ***Start***, trỏ vào ***Administrative Tools,*** và sau đó lựa chọn ***DNS***

2. Trong bảng điều khiển, chọn sau đó nhấn phải chuột vào ***ComputerName*** (trong đó ***ComputerName*** là tên máy tính của bạn), mở rộng ***Reverse Lookup Zones***, nhấn phải chuột vào ***computername.contoso.com,*** và sau đó nhấn vào ***Properties***

3. Trong trang Welcome To The New Zone Wizard, nhấn Next

4. Trong trang Zone Type, xác nhận rằng Primary Zone được lựa chọn và xác nhận rằng hộp chọn Store The Zone In Active Directory (Available Only If DNS Server Is A Domain Controller) được lựa chọn rồi nhấn Next.

5. Trong trang Active Directory Zone Replication Scope, xác nhận rằng hộp chọn To All Domain Controllers In The Active Directory Domain Contoso.com được lựa chọn và sau đó nhấn Next

6. Trong trang ***Reverse Lookup Zone Name***, trong hộp ***Network ID,*** nhập vào ***10.1.1*** và sau đó nhấn ***Next***.

7. Trong trang ***Dynamic Update***, xác nhận rằng hộp chọn ***Allow Only Secure Dynamic Updates*** (***Recommended For Active Directory***) được lựa chọn và sau đó nhấn ***Next***.

8. Trong trang Completing The New Zone Wizard, nhấn Finish.

9. Trong bảng điều khiển, nhấn vào ***Reverse Lookup Zones*** và trong khung chi tiết, xác nhận rằng vùng có tên ***10.1.1.x Subnet*** (trong đó x là số của máy tính của bạn) hiển thị với kiểu là ***Active Directory–Integrated Primary***

Bài tập 3-5. Định vị bản ghi tài nguyên DNS

Bài tập 3-5 hướng dẫn bạn cách sử dụng bảng điều khiển DNS để nhận biết ba kiểu bản ghi tài nguyên khác nhau

1. Nhấn ***Start***, trỏ vào ***Administrative Tools***, và sau đó lựa chọn ***DNS***

2. Trong bảng điều khiển, mở rộng ***Forward Lookup Zones*** và sau đó nhấn vào ***domain.contoso.com*** (trong đó ***domain*** là tên miền của bạn).

3. Tìm các bản ghi ***SOA***, ***NS***, ***A*** trong khung chi tiết

Bài tập 3-6. Dỡ bỏ vai trò của máy chủ DNS

Để chuẩn bị cho các Bài tập Thực hành đi kèm trong chương này (sách BÀI TẬP THỰC HÀNH, chương 3), bài tập này hướng dẫn bạn cách dỡ bỏ vai trò của máy chủ DNS.

1. Nhấn Start, trỏ vào Administrative Tools, và sau đó lựa chọn Manage Your Server

2. Trang ***Manage Your Server*** sẽ tự động khởi tạo theo mặc định sau khi đăng nhập

3. Trong trang ***Manage Your Server***, nhấn vào ***Add/Remove A Role***

4. Trong trang ***Preliminary Steps,*** nhấn ***Next***

5. Trong trang ***Server Roles,*** nhấn vào ***DNS Server*** và sau đó nhấn ***Next***

6. Trong trang ***Role Removal Confirmation***, nhấn vào hộp chọn R***emove The DNS Server Rol***e và sau đó nhấn ***Next***

7. Trong trang ***DNS Server Role Removed***, nhấn ***Finish***

CÁC CÂU HỎI TỔNG KẾT

1. Mô tả quá trình trong đó các máy chủ thứ cấp xác định liệu việc chuyển giao vùng có nên được khởi tạo hay không.

2. Nêu sự khác nhau giữa một truy vấn IXFR và một truy vấn AXFR

3. Bạn nhận thấy rằng một quản trị mạng đã chỉnh sửa giá trị TTL mặc định cho vùng DNS chính của công ty của bạn là 5 phút. Sự thay đổi đó ảnh hưởng nhiều nhất đến điều gì sau đây:

   a. Các máy chủ chính khởi tạo một quá trình chuyển giao vùng cứ sau 5 phút

   b. Các máy khách DNS phải truy vấn máy chủ thường xuyên hơn để phân giải các tên mà máy chủ đó có thẩm quyền xử lý.

   c. Các máy chủ thứ cấp khởi tạo một sự chuyển giao vùng cứ sau mỗi 5 phút

   d. Các máy DNS đăng ký các bản ghi thường xuyên hơn.

4. Liên quan đến các vùng gói-trong-file, việc lưu các vùng DNS trong Active Directory sẽ đem lại kết quả gì trong các ý sau đây:

   a. Việc chuyển giao thông tin sẽ ít thường xuyên hơn

   b. Tăng nhu cầu quản trị

   c. Ít suy hao nhất đến băng thông mạng

   d. Khả năng thực hiện các cập nhật động bảo mật

5. Bạn muốn đồng nhất các lưu lượng DNS giữa mạng của bạn và Internet, Làm thế nào để bạn có thể sử dụng một máy chuyển tiếp để thực hiện điều đó

6. Vì các lý do nào mà một máy chủ nguồn có thể phản hồi lại bằng một kiểu chuyển giao AXFR trong khi nhận được yêu cầu chuyển giao IXFR?

7. **Đúng hay sai**: Một máy chủ chính luôn khởi tạo một sự chuyển giao vùng?

CÁC KỊCH BẢN TÌNH HUỐNG

Kịch bản tính huống 3-1: Tối ưu hóa lưu lượng và quản trị DNS

Contoso, Ltd. có một văn phòng chi nhánh kết nối đến văn phòng trung ương bằng một đường kết nối WAN tốc độ thấp. công ty muốn tối thiểu lưu lượng phát sinh bởi máy chủ DNS nội bộ trên đường kết nối này và cũng muốn giảm thiểu việc quản trị DNS tại văn phòng chi nhánh.

Bạn sẽ cấu hình máy chủ DNS như thế nào để đạt được các mục đích trên?

a. Vô hiệu hóa các cơ chế Round-Robin (trả kết quả luân phiên) và Netmask Ordering (trả kết quả theo trật tự mạng con)
b. Giảm thời gian nghỉ giữa các lần làm tươi trong bản ghi tài nguyên SOA của vùng chính
c. Không cấu hình bất kỳ vùng phân giải xuôi hay ngược nào nhưng cấu hình máy chủ trở thành một máy chủ chuyển tiếp
d. Cấu hình vùng phân giải xuôi trên với bản ghi phân giải WINS và giảm giá trị thời gian hết hạn của bộ nhớ đệm.

Kịch bản tính huống 3-2: Giải quyết sự cố khi truy cập đến các tài nguyên bên ngoài.

Bạn là quản trị mạng của công ty Contoso Ltd. người dùng trong công ty phàn nàn rằng họ không thể truy cập các tài nguyên bên ngoài từ trong mạng nội bộ. Bạn đã giảm thiểu các vấn đề liên quan đến kết nối tới máy chủ DNS và hạn chế các sự cố của việc phân giải tên. Sử dụng ping.exe, bạn có khả năng phân giải thành công tên nội bộ nhưng không thể phân giải các tên bên ngoài từ trong mạng nội bộ. Đâu là nguyên nhân có thể nhất của vấn đề này?

a. Máy chủ DNS nội bộ là không có thẩm quyền đối với tên miền DNS trên Internet.
b. Các truy vấn lặp bị vô hiệu hóa trên máy chủ DNS
c. Các truy vấn đệ quy bị vô hiệu hóa trên máy chủ DNS
d. Các root hint DNS bị thiếu hoặc bị cấu hình sai

CHƯƠNG 4: QUẢN TRỊ VÀ GIÁM SÁT DNS

Sau khi hoàn thành chương này, bạn có khả năng:

- Sử dung các công cụ quản trị để cấu hình **Hệ thống tên miền (DNS)** bao gồm ***Nslookup***, ***DNSLint*** và ***Dnscmd***
- Định nghĩa việc tích hợp DNS và **WINS (Dịch vụ tên Internet trên Windows)** và giải thích cách thức các tên máy và các **hệ thống mạng vào/ra cơ bản (NetBIOS)** có thể phù hợp với việc tích hợp DNS và WINS như thể nào
- Cấu hình các tùy chọn có thể trong thẻ Advance của hộp thoại ***DNS Server Properties***
- Giải thích cách thức các bản ghi tài nguyên hết hạn bị lão hóa và loại bỏ và khởi tạo quá trình lão hóa và loại bỏ như thế nào.
- Hiển thị và xóa bộ đệm **phân giải tên** DNS
- Bảo mật các đối tượng DNS trong dịch vụ thư mục sử dụng **Active Directory**
- Sử dụng Nhật ký sự kiện (***Event Log***), nhật ký gỡ rối (***debug log***) DNS và trình giám sát đồng bộ Active Directory (***Active Directory Replicate Monitor***) để giám sát và giải quyết sự cố DNS.

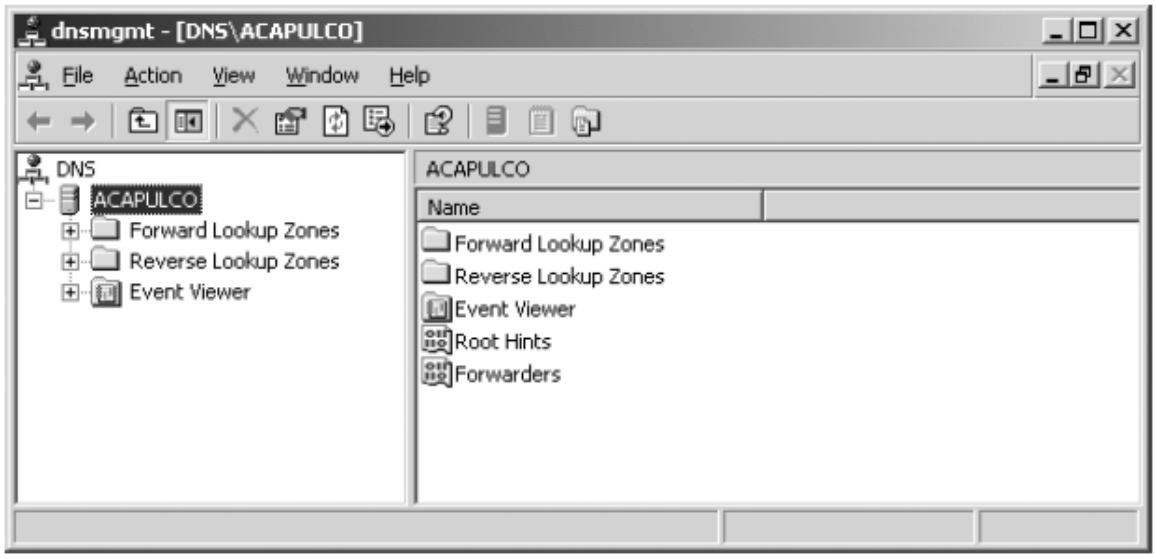
DNS là dịch vụ quan trọng then chốt trong hệ thống mạng sử dụng Microsoft Windows Server 2003. Nếu DNS không hoạt động, các máy trạm thường xuyên không thể kết nối đến Internet hoặc đến các máy trạm khác và Active Directory cũng không hoạt động được. Các thủ tục quản trị và giám sát hiệu quả sẽ làm giảm nguy cơ máy chủ DNS không hoạt động.

Chương này giới thiệu bạn các công cụ, khái niệm, và các thủ tục cần thiết để quản trị và giám sát việc phân giải tên DNS. Các chủ đề trong chương này bao gồm bảo mật DNS, giám sát và xử lý sự cố DNS bằng các công cụ như nhật ký sự kiện và nhật ký gỡ rối DNS và sử dụng các công cụ như ***nslookup***, ***Replication Monitor*** và ***Dnscmd***

SỬ DỤNG CÁC CÔNG CỤ QUẢN TRỊ DNS

Một số công cụ rất hữu ích để quản trị và giám sát dịch vụ DNS. Các công cụ này bao gồm như sau:

- Bảng điều khiển DNS, nó là một phần trong ***Administrative Tools***. Bảng điều khiển DNS là công cụ chính thức để cấu hình DNS. Nó được hiển thị trong Hình 4-1.



Hình 4-1. Bảng điều khiển DNS

- ***Nslookup***, có thể sử dụng để truy vấn các thông tin về vùng DNS để xác nhận các bản ghi tài nguyên đã tồn tại và đã được cấu hình trước.
- ***DNSLint***, một công cụ để xác nhận sự thống nhất của một tập xác định các bản ghi DNS tên nhiều máy chủ DNS
- Tính năng ghi nhật ký, ví dụ như nhật ký máy chủ DNS mà bạn có thể xem trong ***bảng điều khiển DNS*** hoặc ***Event Viewer.*** Các nhật ký viết vào file này có thể sử dụng tạm thời như một tùy chọn gỡ rối nâng cao để ghi nhật ký và theo dõi các sự kiện dịch vụ xác định.
- ***Dnscmd***, cho phép bạn sử dụng giao diện dòng lệnh để thực hiện hầu hết các tác vụ mà bạn có thể thực hiện trong bảng điều khiển DNS

Sử dụng bảng điều khiển DNS để giám sát các máy chủ DNS

Bạn có thể sử dụng bảng điều khiển DNS để kiểm tra các máy chủ DNS tự động hoặc thủ công bằng cách thực hiện hai kiểu truy vấn khác nhau:

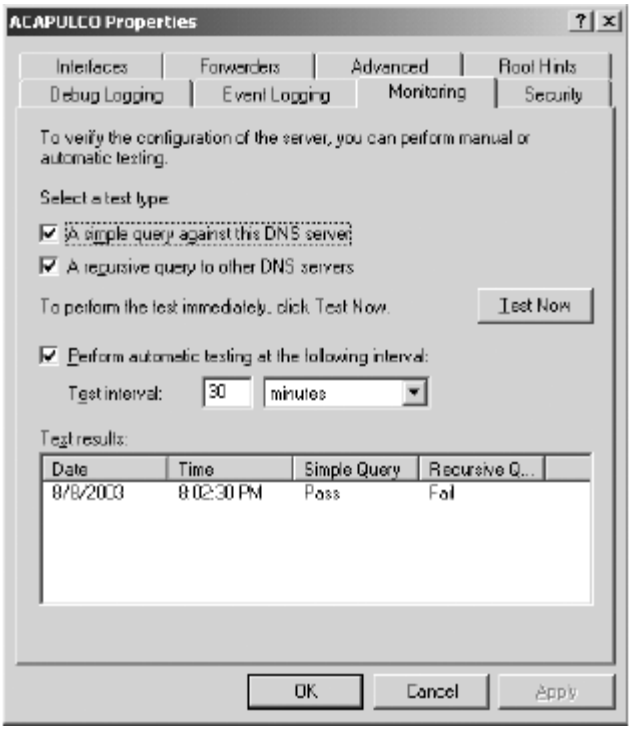
- Một truy vấn đơn giản, hay một **truy vấn lặp**. Thành phần phân giải tên DNS trên máy chủ (đóng vai trò máy khách) sẽ truy vấn chính các máy chủ DNS nội bộ, dù chúng đều nằm trên cùng một máy tính.
- Một **truy vấn đệ quy** đến các máy chủ DNS khác. Thành phần phân giải tên DNS trên máy chủ (đóng vài trò máy khách) truy vấn máy chủ DNS nội bộ, nhưng thay vì gửi đi một truy vấn lặp, nó sẽ gửi một truy vấn đệ quy. Trong trường hợp đặc biệt, máy khách sẽ yêu cầu máy

chủ sử dụng đệ quy để phân giải một truy vấn kiểu tên máy chủ (NS) về gốc của không gian tên miền DNS. Kiểu truy vấn này thường yêu cầu các quá trình xử lý đệ quy bổ sung khác và có thể có ích khi muốn xác nhận các máy chủ root hints hoặc xác nhận việc ủy quyền các vùng đã được thiết lập một cách đúng đắn.

Các thiết lập này được truy cập bằng cách nhấn vào thẻ Monitoring trong cửa sổ trang thuộc tính của máy chủ DNS. Bạn có thể thực hiện việc kiểm tra bằng cách nhấn vào phím Test Now hoặc chỉ định một khoảng thời gian lặp để thực hiện việc kiểm tra này.

Kết quả của cả hai việc kiểm tra tự động và thủ công sẽ được hiển thị trên hộp danh sách ***Test Results*** thể hiện trong Hình 4-2. Các thông tin này bao gồm:

- Thời gian và ngày tháng khi mà truy vấn được gửi đi
- Các kết quả trạng thái bổ sung của lần kiểm tra xác định nào đó, ví dụ như đó là các truy vấn đơn giản hay đệ quy, thành công hay thất bại



Hình 4-2. Hộp danh sách Test Result

Truy vấn DNS bằng Nslookup

Nslookup là một công cụ dòng lệnh kèm theo giao thức TCP/IP và có trong Windows Server 2003, công cụ này thực hiện truy vấn DNS và cho phép kiểm tra thành phần của file của vùng trên các máy chủ nội bộ và ở xa.

Nslookup thường xuyên được sử dụng để xác nhận cấu hình của các vùng DNS, để chẩn đoán và giải quyết sự cố của việc phân giải tên. Nslookup có thể thực hiện tại dấu nhắc dòng lệnh (trong chế độ dấu nhắc dòng lệnh) hoặc như một chương trình mà tiếp nhận các chuỗi dòng lệnh và truy vấn kế tiếp nhau (trong chế độ tương tác). Để tìm một tên máy đơn, bạn chỉ cần nhập vào một dòng lệnh đơn tại dấu nhắc dòng lệnh. Ví dụ, thực hiện lệnh sau đây tại dấu nhắc dòng lệnh sẽ trả về một địa chỉ IP gắn với tên FQDN của www.microsoft.com (kết quả đầu ra có thể thay đổi):

C:\>nslookup www.microsoft.com
Server: bottincdc1.bottinc.com
Address: 192.168.0.100
Non-authoritative answer:
Name: www.microsoft.akadns.net
Addresses: 207.46.134.155, 207.46.134.190, 207.46.249.222, 207.46.249.27
207.46.249.190
Aliases: www.microsoft.com

Để phân giải truy vấn này, tiện ích ***nslookup*** sẽ gửi tên cần truy vấn đến máy chủ DNS mà đã được chỉ định trong kết nối chính thức của máy trạm nội bộ. Máy chủ DNS này có thể trả lời truy vấn từ bộ nhớ đệm của nó hoặc thông qua đệ quy.

Nếu bạn gửi đi một truy vấn về một tên máy không tồn tại, bạn sẽ nhận được phản hồi như sau:

C:\>nslookup thisdoesnotexist.bottinc.com
Server: bottincdc1.bottinc.com
Address: 192.168.0.100

****** bottincdc1.bottinc.com can't find thisdoesnotexist.bottinc.com:***
Non-existent domain

Nếu bạn đang xử lý sự cố cho một máy chủ DNS cụ thể nào đó mà không phải là máy chủ chính thức chỉ định trong cấu hình máy trạm nội bộ, bạn có thể chỉ định máy chủ đó trong lệnh nslookup. Ví dụ, dòng lệnh thực thi trong dấu nhắc dòng lệnh sau đây sẽ truy vấn về tên www.microsoft.com bằng cách sử dụng máy chủ DNS có địa chỉ 207.46.138.20.

C:\>nslookup www.microsoft.com 207.46.138.20

Bạn còn có thể sử dụng nslookup để phân giải địa chỉ IP sang tên máy. Ví dụ, dòng lệnh sau đây thực hiện tại dấu nhắc dòng lệnh sẽ trả lại một tên FQDN gắn với địa chỉ IP 207.46.249.222, thể hiện trong kết quả như sau:

C:\>nslookup 207.46.249.222

Server: localhost
Address: 127.0.0.1

Name: www.microsoft.com
Address: 207.46.249.222

Cú pháp của nslookup

Sử dụng cú pháp sau đây của nslookup trong chế độ dấu nhắc dòng lệnh:

nslookup [-opt. ...] [{Host|[Server]}]

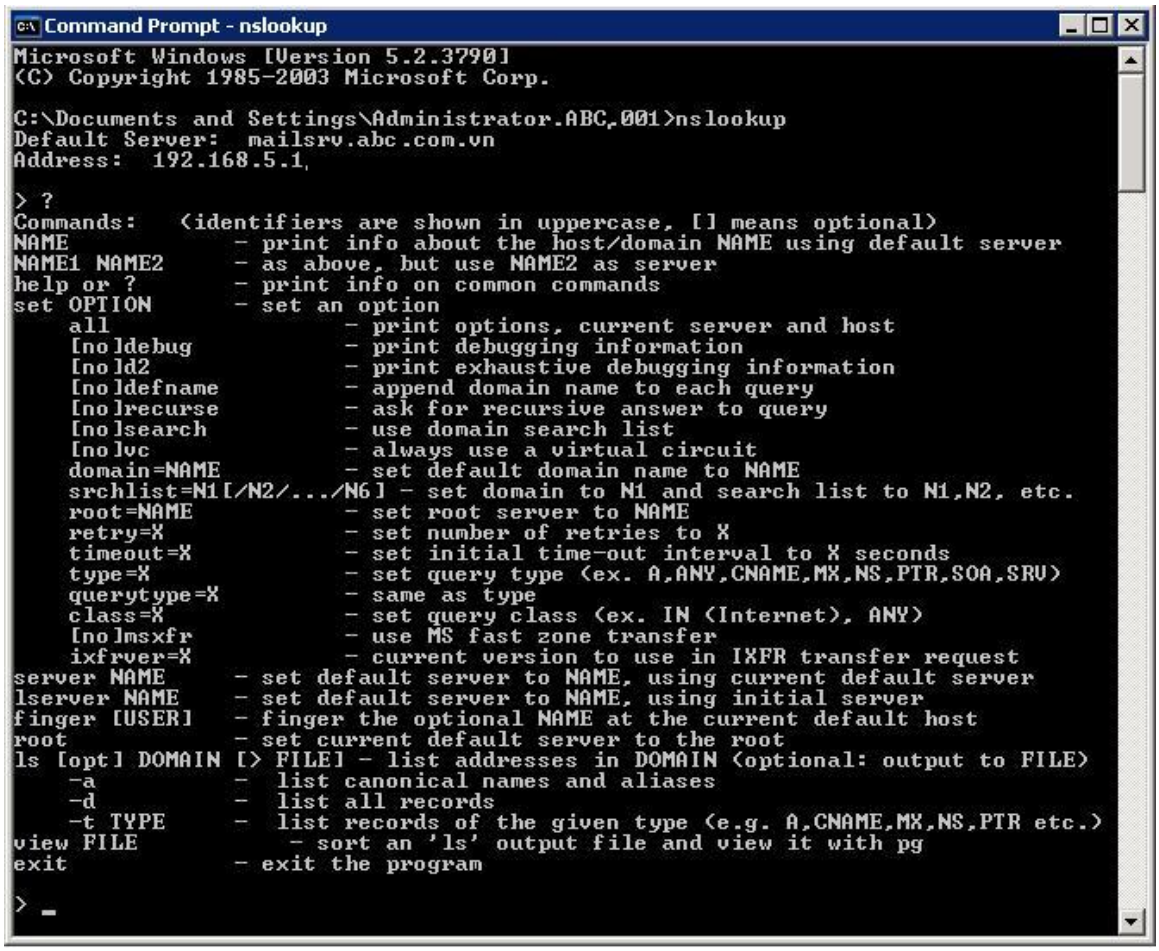
Dòng lệnh ***nslookup*** sử dụng cú pháp trên với các tham số sau đây:

- **-opt.** Chỉ định một hoặc nhiều lệnh con của ***nslookup*** như là tùy chọn của dòng lệnh
- **Host**. Tìm kiếm thông tin về trạm bằng cách sử dụng máy chủ tên DNS (NS) mặc định hiện tại, nếu như không chỉ định rõ một máy chủ nào khác. Để tìm kiếm một máy tính mà không có trong **miền DNS** hiện tại, bạn phải gắn thêm vào các dấu chấm trong tên.
- **Server.** Chỉ định sử dụng máy chủ này như là máy chủ tên DNS. Nếu bạn bỏ qua tham số này, máy chủ tên DNS mặc định sẽ được sử dụng.

Sử dụng Chế độ tương tác

Khi muốn sử dụng nhiều lệnh Nslookup, việc thực hiện nslookup trong chế độ tương tác sẽ đem lại hiệu quả tốt hơn. Để vào chế độ tương tác, mở một dấu nhắc dòng lệnh, nhập vào **nslookup** và nhấn Enter.

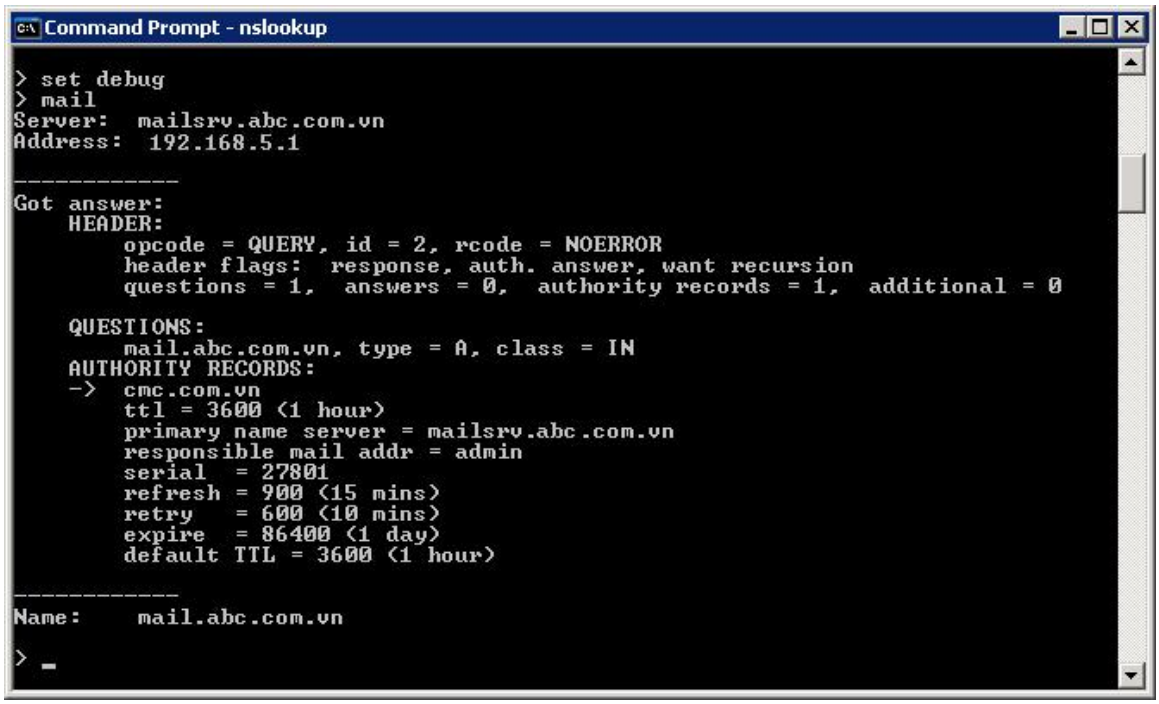
Trong chế độ tương tác, nslookup chấp nhận các lệnh và cho phép chương trình thực hiện rất nhiều chức năng, ví dụ như hiển thị các nội dung đặc biệt của các thông điệp có trong các trao đổi DNS, giả lập một quá trình **chuyển giao vùng** hoặc tìm kiếm các bản ghi có kiểu xác định trên một máy chủ nào đó. Các lệnh này có thể hiển thị bằng cách nhập vào lệnh help hoặc ? như thể hiện trong Hình 4-3.



Hình 4-3. Các lệnh trong Nslookup

Khám phá các tùy chọn trong Nslookup

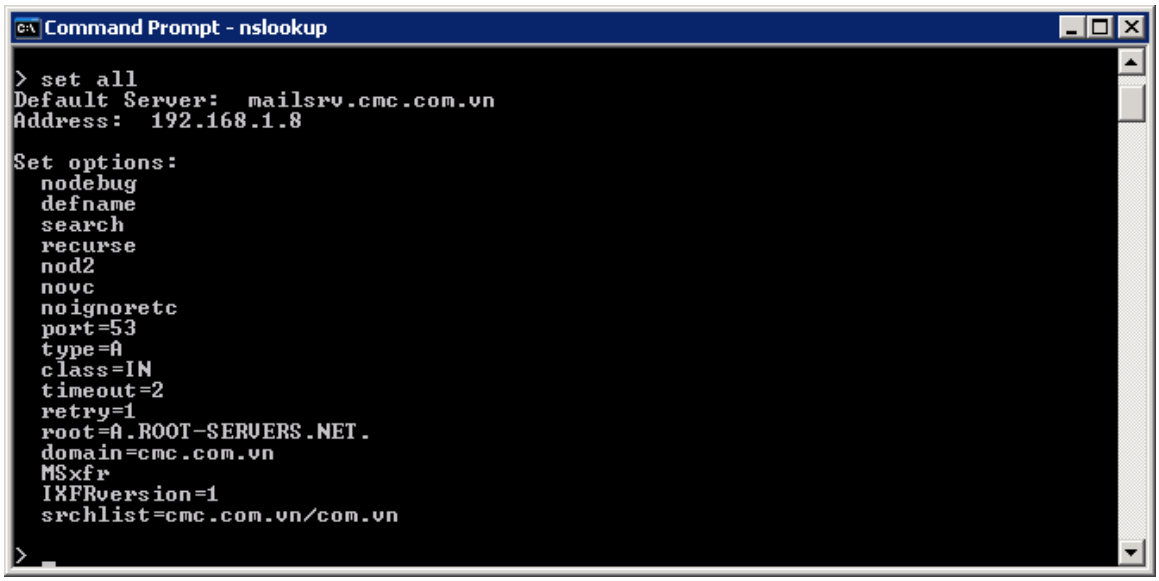
Khi bạn đang ở trong chế độ tương tác, bạn có thể sử dụng lệnh Set để cấu hình các tùy chọn của nslookup để xác định cách thức phân giải các truy vấn. Một tùy chọn là sử dụng lệnh ***debug***. Theo mặc định, ***nslookup*** được thiết lập là ***Nodebug***. Nhập vào **set debug** khi đang trong chế độ tương tác sẽ chuyển sang chế độ gỡ rối, chế độ này cho phép ***nslookup*** hiển thị các thông điệp phản hồi DNS trong quá trình trao đổi với máy chủ DNS như thể hiện trong Hình 4-4.



Hình 4-4. Nslookup trong chế độ gỡ rối

> ***LƯU Ý. Các lệnh Nslookup đều phân biệt chữ hoa, thường***. *Các lệnh nslookup được nhập vào trong chế độ tương tác đều phân biệt chữ hoa và chữ thường và phải được nhập vào trong kiểu chữ thường.*

Bạn có thể xem các tùy chọn hiện tại đang được cấu hình cho ***nslookup*** bằng cách chạy lệnh ***Set All,*** thể hiện trong Hình 4-5.



Hình 4-5. Hiển thị các tùy chọn của Nslookup

Bảng 4-1 mô tả các tùy chọn thông dụng nhất cấu hình bằng lệnh Set

Bảng 4-1. Các tùy chọn dòng lệnh đi kèm với lệnh Set

Các tùy chọn	Mục đích	Ví dụ
Set all	Hiển thị các trạng thái cấu hình của các tùy chọn	>set all
set [no]debug	Đặt Nslookup trong chế độ gỡ rối. Khi chế độ gỡ rối được bật lên, nhiều thông tin được in ra hơn về các gói tin gửi đến máy chủ và kết quả của câu trả lời	>set debug hoặc set nodebug
set [no]d2	Đặt Nslookup trong chế độ gỡ rối diễn giải dài do đó bạn có thể kiểm tra truy vấn và các gói tin phản hồi giữa bộ phận phân giải và máy chủ	>set d2 hoặc set nod2
set domain=<*domain name*>	Thông báo bộ phận phân giải rằng tên miền nào sẽ được gắn vào các truy vấn chưa chứng nhận (ví dụ Sales là một truy vấn chưa được chứng nhận của sales.fabrikam.com) bao gồm tất cả các tên truy vấn mà không có dấu chấm đi kèm trong phần hậu tố của tên	>set domain =bottinc.com
set timeout=<*time-out value*>	Thông báo bộ phận phân giải về giá trị thời gian hết hạn được sử dụng, tính bằng giây. Tùy chọn này có ích nếu đường truyền chậm mà trên đó các truy vấn hay bị hết hạn và thời gian chờ đợi luôn phải kéo dài	>set timeout=5
set type=<*record type*> hoặc set querytype=<*record type*> hoặc set q=<*record type*>	Thông báo bộ phận phân giải về kiểu bản ghi tài nguyên nào sẽ được tìm kiếm (ví dụ các bản ghi A, PTR, SRV). Nếu bạn muốn bộ phận phân giải truy vấn tất cả các kiểu bản ghi tài nguyên, nhập vào set type=all	>set type=A >set q=MX

Phần sau đây sẽ mô tả cách thức thực hiện các tác vụ thông thường bằng cách sử dụng nslookup trong chế độ tương tác.

Tìm kiếm các kiểu dữ liệu khác nhau

Theo mặc định, các tên được truy vấn trong lệnh nslookup sẽ chỉ trả lại các bản ghi tài nguyên địa chỉ máy (A) phù hợp. Để tìm kiếm các kiểu dữ liệu khác nhau trong không gian tên miền, sử dụng lệnh Set Type hoặc lệnh Set Querytype (Set Q) tại dấu nhắc dòng lệnh. Ví dụ, để chỉ truy vấn đến bản ghi tài nguyên trao đổi thư điện tử (MX) thay vì các bản ghi tài nguyên A, nhập vào set q=mx như thể hiện dưới đây:

C:\>nslookup
Default Server: bottincdc1.bottinc.com
Address: 192.168.0.100
> set q=mx
> microsoft.com
Server: bottincdc1.bottinc.com

Address: 192.168.0.100
Non-authoritative answer:
microsoft.com MX preference = 10, mail exchanger = maila.microsoft.com
microsoft.com MX preference = 10, mail exchanger = mailb.microsoft.com
microsoft.com MX preference = 10, mail exchanger = mailc.microsoft.com
maila.microsoft.com internet address = 131.107.3.124
maila.microsoft.com internet address = 131.107.3.125
mailb.microsoft.com internet address = 131.107.3.122
mailb.microsoft.com internet address = 131.107.3.123
mailc.microsoft.com internet address = 131.107.3.121
mailc.microsoft.com internet address = 131.107.3.126
>

> ***LƯU Ý. Truy vấn một bản ghi thuộc kiểu bất kỳ****. Để truy vấn một bản ghi kiểu bất kỳ, thực hiện lệnh nslookup sau: Set q=any*

Lần đầu tiên một truy vấn được tạo ra để tìm kiếm một tên ở xa, câu trả lời là có thẩm quyền, tuy nhiên các truy vấn tiếp sau là không có thẩm quyền. Cách thức này là bởi các lý do sau đây: lần đầu tiên một máy ở xa được truy vấn, máy chủ DNS nội bộ sẽ liên lạc với máy chủ DNS mà có thẩm quyền của miền đó. Máy chủ DNS nội bộ sau đó sẽ lưu đệm các thông tin đó lại do đó các truy vấn tiếp sau sẽ được trả lời một cách không có thẩm quyền bằng các thông tin có trong bộ đệm của máy chủ.

Truy vấn các máy chủ tên khác một cách trực tiếp

Để truy vấn các máy chủ tên khác một cách trực tiếp, sử dụng lệnh Server hoặc Lserver để chuyển sang máy chủ tên đó. Lệnh Lserver sử dụng máy chủ tại chỗ để lấy địa chỉ của máy chủ mà nó sẽ chuyển tới trong đó lệnh Server sử dụng máy chủ mặc định hiện tại để lấy địa chỉ.

Sau khi bạn thực thi bất kỳ một lệnh nào trong các lệnh trên, tất cả các tìm kiếm tiếp theo trong phiên nslookup hiện tại sẽ được thực hiện trên máy chủ chỉ định ở trên cho đến khi bạn chuyển sang máy chủ khác.

Cú pháp sau đây minh họa các thông tin mà bạn nhập vào để khởi tạo việc chuyển máy chủ.

C:\> nslookup
Default Server: nameserver1.contoso.com
Address: 10.0.0.1
> server nameserver2
Default Server: nameserver2.contoso.com
Address: 10.0.0.2

Sử dụng các lệnh phụ Ls trong nslookup để xem dữ liệu của vùng

Bạn có thể sử dụng lệnh phụ Ls của nslookup để liệt kê các thông tin về một miền DNS. Khi bạn sử dụng lệnh nslookup với phụ lệnh Ls, bạn thực tế đang yêu cầu một sự chuyển giao vùng. Cú pháp của lệnh Ls như sau:

ls [-a|d|ttype] domain. [> filename]

Bảng 4-2 liệt kê các tùy chọn hợp lệ

Bảng 4-2. Các tùy chọn Ls trong Nslookup

Các tùy chọn	Mục đích	Ví dụ
- t *QueryType*	Liệt kê tất cả các bản ghi của kiểu xác định	>ls -t cname contoso.com
- a	Liệt kê các biệt danh của các máy tính trong một miền DNS (tương đương với -t CNAME)	>ls -a contoso.com
- d	Liệt kê tất cả các bản ghi trong một miền DNS (tương đương với -t ANY)	>ls -d contoso.com
- h	Liệt kê tất cả các thông tin về CPU và hệ điều hành trong một miền DNS (tương đương với -t HINFO)	>ls -h contoso.com
- s	Liệt kê các dịch vụ đã biết của các máy tính trong một miền DNS (tương đương với -t WKS)	>ls -s contoso.com

Các thông tin đầu ra sau đây sẽ hiển thị cách sử dụng lệnh Ls trong chế độ tương tác.

>ls contoso.com
[nameserver1.contoso.com]
nameserver1.contoso.com. NS server = ns1.contoso.com
nameserver2.contoso.com NS server = ns2.contoso.com
nameserver1 A 10.0.0.1
nameserver2 A 10.0.0.2
>

Theo mặc định, dịch vụ DNS Server cho phép các thông tin của vùng chỉ được chuyển giao đến các máy chủ liệt kê trong các bản ghi tài nguyên tên máy chủ (NS) của một vùng. Mặc dù đây là một thiết lập bảo mật, bạn nên tăng cường sự bảo mật bằng cách chỉ cho phép chuyển giao vùng đến các địa chỉ IP xác định. Bạn cũng có thể tùy chọn cho phép chuyển giao vùng đến máy chủ bất kỳ. Đây là thiết lập không được khuyến khích và nó có thể làm lộ diện dữ liệu DNS của bạn với các kẻ tấn công và chúng có thể nhận biết hệ thống mạng của bạn để phục vụ cho các quá trình tấn công lớn hơn. Thông báo lỗi sau đây được trả về nếu việc chuyển giao vùng bảo mật được thiết lập:

****** Can't list domain <example>.: Query refused***

Sử dụng DNSLint

DNSLint là một công cụ dòng lệnh DNS có trong Windows Server 2003 để xác nhận sự đồng nhất của một tập hợp cá biệt của các bản ghi DNS trên nhiều máy chủ DNS. Nó cũng có thể giúp đỡ trong việc chẩn đoán và giải quyết lỗi gây ra bởi việc bản ghi DNS thiếu hoặc không đúng. DNSLint biên dịch các kết quả vào trong một file Hypertext Markup Language (HTML) có tên theo mặc định là ***DNSLint.html.*** File này được lưu trong cùng thư mục mà từ đó bạn thực hiện lệnh ***DNSLint*** này.

Ví dụ, ***DNSLint*** có thể trợ giúp bạn khi các máy khách gặp phải sự cố trong khi phân giải các **tên NetBIOS** hoặc giúp bạn xác nhận rằng các bản ghi SRV (mà các máy khách có thể sử dụng để tìm kiếm các máy chủ WINS) đều có sẵn và chứa thông tin chính xác. ***DNSLint*** có thể trợ giúp bạn trong việc xác định chắc chắn liệu DNS có gây ra sự cố nào không.

Bạn có thể sử dụng DNSLint để giải quyết sự cố các vấn đề về việc đồng bộ Active Directory liên quan đến DNS. Đặc biệt, sử dụng DNSLint còn để xác định các vấn đề sau:

- Liệu tất cả các máy chủ DNS, được cho là có thẩm quyền đối với root của một rừng Active Directory, có đủ các bản ghi DNS cần thiết để đồng bộ các phân vùng thư mục một cách thành công giữa các máy chủ quản trị miền trong một rừng Active Directory hay không.

- Liệu một máy chủ quản trị miền Active Directory cụ thể nào đó có thể phân giải các bản ghi DNS cần thiết để đồng bộ các phân vùng thư mục một cách thành công giữa các máy chủ quản trị miền trong một rừng Active Directory hay không. DNSLint nhận biết các bản ghi DNS nào không thể phân giải được bằng máy chủ quản trị miền đang được kiểm tra.

  THÔNG TIN THÊM. Sử dụng DNSLint để giải quyết sự cố đồng bộ Active Directory. *Xem Microsoft Knowledge Base bài viết 321046, "LÀM THẾ NÀO: Sử dụng DNSLint để giải quyết sự cố đồng bộ Active Directory" Để tìm bài viết này, truy cập trang http://support.microsoft.com và nhập vào số thứ tự của bài viết trong hộp thoại* ***Search The Knowledge Base***

Trong kịch bản khác, bạn có khả năng gửi email nhưng không nhận được. Một trong những nguyên nhân có thể là cấu hình DNS không đúng. Để xác định liệu DNS có bị cấu hình sai hay không, sử dụng DNSLint để xác nhận

sự đúng đắn các bản ghi DNS trong máy chủ DNS sử dụng để phân giải địa chỉ IP của máy chủ Email.

Cú pháp của DNSLint và các chức năng.

Cú pháp của DNSLint như sau:

dnslint /d domain_name. |/ad [LDAP_IP_address] | /ql input_file.
[/c [smtp,pop,imap]] [/no_open] [/r report_name]
[/t] [/test_tcp] [/s DNS_IP_address] [/v] [/y]

DNSLint thực hiện một trong ba chức năng sau và sau đó sinh ra một báo cáo HTML.

- **./d** Khóa chuyển ***/d*** (kiểm tra tên miền) được sử dụng để kiểm tra một tên miền DNS cụ thể. Khóa chuyển này được sử dụng để trợ giúp trong việc chẩn đoán vấn đề "ủy quyền không đúng" và các vấn đề khác liên quan đến DNS. Việc *ủy quyền không đúng* xảy ra khi một vùng được ủy quyền cho một máy chủ mà chưa được cấu hình đúng đắn để có thẩm quyền của vùng đó hoặc một máy chủ có thẩm quyền cho một vùng lại có một bản ghi NS trỏ đến máy khác trong khi máy này không có thẩm quyền đối với vùng đó.

- **./ad** Khóa chuyển ***/ad*** (kiểm tra việc đồng bộ Active Directory) sử dụng để kiểm tra các bản ghi DNS mà chịu trách nhiệm cho việc đồng bộ rừng Active Directory. Hình 4-6 thể hiện kết quả của các báo cáo ***DNSLint*** khi thực hiện với lệnh ***/ad /s localhost /v***

Hình 4-6: Trang kết quả của DNSint

- **/ql** Khóa chuyển ***/ql*** (kiểm tra Danh sách truy vấn) được sử dụng để kiểm tra các bản ghi DNS chỉ định trong một file văn bản.

  THÔNG TIN THÊM. Sử dụng DNSLint*. Xem Microsoft Knowledge Base bài viết 321045 "Mô tả tiện ích DNSLint". Để tìm bài viết này, truy cập trang http://support.microsoft.com và nhập vào số của bài viết trong hộp thoại Search The Knowledge Base*

Các thủ tục sau đây mô tả cách thức sử dụng các tham số tự động tạo ra với khóa chuyển /ql để sinh ra một file mà bạn có thể tùy biến nó.

➢ **Tạo ra một file đầu vào cho DNSLint**

Để tạo ra một báo cáo ***DNSLint***, thực hiện theo các bước sau:

1. Mở cửa sổ dấu nhắc dòng lệnh
2. Duyệt đến thư mục chứa ***Dnslint.exe.***
3. Tại dấu nhắc dòng lệnh, nhập vào **dnslint /ql autocreate**
4. Khi các tham số tự động tạo ra được them vào trong khóa chuyển ***/ql***, một file văn bản truy vấn mẫu được tạo ra.
5. Tại dấu nhắc dòng lệnh, nhập vào **notepad in-dnslint.txt**

6. Trong Microsoft Notepad, trong dòng thư bảy tính từ dưới lên, thay thế từ ***dns1.cp.msft.net*** thành *ComputerName*.**northwindtraders.msft**
7. Trong ***Notepad***, trong bốn dòng cuối cùng của file, thay đổi bất cứ trường hợp nào của địa chỉ 207.46.197.100 thành địa chỉ IP của máy chủ DNS mà bạn muốn sử dụng để truy vấn
8. Trong Notepad, lưu file thành ***Dnslintquery.txt*** trong cùng thư mục mà chứa ***In-dnslint.txt*** và sau đó đóng Notepad lại.
9. Tại dấu nhắc dòng lệnh, nhập vào **dnslint /ql dnslintquery.txt /v**. Khóa chuyển /ql sẽ yêu cầu các truy vấn từ danh sách đặc biệt (Dnslintquery.txt). Khóa chuyển ***/v*** sẽ yêu cầu các phản hồi giải thích chi tiết
10. Khi báo cáo HTML mở ra, xác nhận nội dung và sau đó đóng báo cáo
11. Đóng dấu nhắc dòng lệnh

Sử dụng Dnscmd

Bạn có thể sử dụng công cụ dòng lệnh Dnscmd để thực hiện hầu hết các tác vụ mà bạn thực hiện tại bảng điều khiển DNS. Công cụ này có thể sử dụng để tạo các file kịch bản script, để trợ giúp trong việc tự động quản trị và cập nhật các cấu hình máy chủ DNS sẵn có hoặc để thực hiện cài đặt và cấu hình các máy chủ DNS. Ví dụ, bạn có thể làm các việc sau đây:

- Tạo, xóa và xem các vùng và các bản ghi
- Khởi tạo lại các thuộc tính của máy chủ và vùng
- Thực hiện công việc bảo dưỡng vùng ví dụ như cập nhật vùng, nạp lại vùng, làm tươi vùng, ghi vùng vào trong file hoặc Active Directory, và tạm ngừng hoặc tiếp tục lại một vùng.
- Xóa bộ nhớ đệm
- Ngừng và khởi động dịch vụ DNS
- Xem các thông số thống kê

Dnscms được trang bị như là một công cụ dòng lệnh để quản trị các máy chủ DNS. Để sử dụng ***Dnscmd***, bạn phải cài đặt ***Windows Support Tools***.

➢ **Cài đặt Windows Support Tools.**

Để cài đặt Windows Support Tools, thực hiện theo các bước sau:

1. Đưa đĩa CD Windows Server 2003 vào trong ổ đĩa CD-ROM
2. Chuyển đến thư mục ***\Support\Tools***
3. Nhấn đúp vào ***supports.msi***
4. Khi trang ***Welcome To The Windows Support Tools Setup Wizard*** xuất hiện, nhấn ***Next***
5. Trong trang ***End User License Agreement,*** nhấn ***I Agree*** và sau đó nhấn ***Next***
6. Trong trang ***User Information,*** cung cấp tên của bạn và tên của doanh nghiệp của bạn và sau đó nhấn ***Next***
7. Trong trang ***Destination Directory***, nhập vào đường dẫn nơi mà sẽ cài đặt ***Windows Support Tools*** vào đó và sau đó nhấn ***Install Now***
8. Trong trang ***Completing The Windows Support Tools,*** nhấn ***Next.***

➢ **Hiển thị danh sách hoàn chỉnh của các vùng**

Để hiển thị một danh sách hoàn chỉnh của các vùng được cấu hình trên một máy chủ DNS bằng cách sử dụng ***Dnscmd***, tại dấu nhắc dòng lệnh, nhập vào ***dnscmd [ComputerName] /enumzones.***

Thực hiện Dnscmd với localhost sẽ cho ra kết quả như sau:

C:\>dnscmd localhost /enumzones
Enumerated zone list:
Zone count = 5
Zone name Type Storage Properties
. Cache AD-Legacy
_msdcs.contoso01.com Primary AD-Forest Secure
1.1.10.in-addr.arpa Primary AD-Legacy Secure Rev
computer01.contoso.com Primary AD-Legacy
contoso01.com Primary AD-Domain Secure
Command completed successfully.

➢ **Hiển thị các thông tin vùng đặc biệt**

Để hiển thị các thông tin về một vùng đặc biệt mà được cấu hình trên một máy chủ DNS bằng cách sử dụng Dnscmd, tại dấu nhắc dòng lệnh, nhập vào như sau:

dnscmd [ComputerName] /zoneinfo [zone]

Thực hiện lệnh sau đây sẽ cho ra kết quả giống như sau đây:

C:\>dnscmd localhost /zoneinfo contoso01.com

Zone query result:
Zone info:
Ptr = 00083050
zone name = contoso01.com
zone type = 1
update = 2
DS integrated = 1
data file = (null)
using WINS = 0
using Nbstat = 0
aging = 0
refresh interval = 168
no refresh = 168
scavenge available = 3529116
Zone Masters
NULL IP Array.
Zone Secondaries
NULL IP Array.
secure secs = 3
directory partition = AD-Domain flags 00000015
zone DN =DC=contoso01.com,cn=MicrosoftDNS, DC=DomainDnsZones, DC=contoso01,DC=com
Command completed successfully.

TÍCH HỢP CÁC VÙNG DNS VỚI WINS

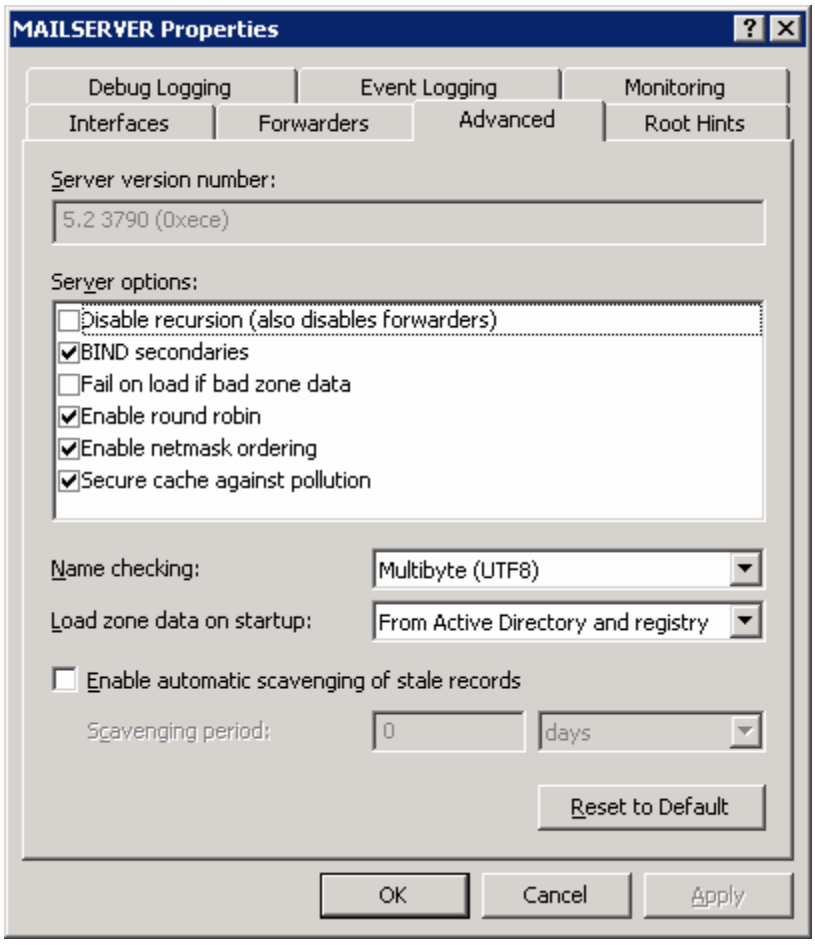
DNS và WINS tích hợp với nhau là một quá trình trong đó DNS sử dụng WINS để phân giải các tên sang địa chỉ IP. DNS được sử dụng để phân giải các tên máy và các dịch vụ sang địa chỉ IP và WINS được sử dụng để phân giải các tên NetBIOS sang địa chỉ IP. Bạn có thể cấu hình thủ công các ánh xạ tên NetBIOS sang địa chỉ IP trên máy chủ DNS hoặc bạn có thể cấu hình máy chủ DNS chuyển tiếp các tên truy vấn sang máy chủ WINS để phân giải. Việc tích hợp DNS và WINS cho phép các máy khách DNS sử dụng các tên NetBIOS có sẵn trong WINS để tra cứu tên máy. Dịch vụ DNS cung cấp khả năng sử dụng các máy chủ WINS để tra cứu các tên mà không có trong không gian tên DNS bằng cách kiểm tra không gian tên NetBIOS mà WINS quản lý.

Khi bạn cấu hình tra cứu bằng WINS cho một vùng phân giải xuôi, một bản ghi tài nguyên WINS trỏ đến máy chủ WINS, mà bạn chỉ định trong thẻ WINS, sẽ được thêm vào trong CSDL của vùng. Khi bạn cấu hình tra cứu WINS-R cho một vùng phân giải ngược, một bản ghi tài nguyên tương ứng WINS-R sẽ được thêm vào trong CSDL của vùng.

Các tên máy và tên NetBIOS có thể giống nhau trong Microsoft Windows Server 2000 hoặc Microsoft Windows Server 2003, điều này cho phép DNS và WINS có thể kết hợp với nhau để phân giải các tên. Trong một số trường hợp, việc các doanh nghiệp sử dụng CSDL WINS có sẵn để phục vụ việc tra cứu các tên sẽ tốt hơn là cấu hình từng máy trạm trong CSDL của WINS sang CSDL của DNS.

QUẢN TRỊ DNS BẰNG CÁC THUỘC TÍNH NÂNG CAO CỦA MÁY CHỦ DNS

Các thuộc tính nâng cao của máy chủ DNS là các thiết lập mà có thể được cấu hình trong thẻ ***Advance*** của hộp thoại ***DNS Server Properties*** (Thể hiện trong Hình 4-7). Các thuộc tính này liên hệ đến các tính năng đặc biệt của máy chủ, ví dụ như vô hiệu hóa đệ quy, tiến hành phân giải các máy nhiều giao tiếp mạng và có thể tương thích với các máy chủ DNS không phải là của Microsoft.



Hình 4-7. Thẻ Advance trong hộp thoại DNS Server Properties

Các thiết lập khi cài đặt máy chủ bao gồm sáu tùy chọn máy chủ, trong đó có giá trị ***on*** hoặc ***off*** và ba tính năng khác của máy chủ với rất nhiều lựa chọn để cấu hình. Bảng 4-3 thể hiện các thiết lập mặc định cho cả 9 tính năng này.

Bảng 4-3. Các thiết lập cài đặt DNS

Thuộc tính	**Thiết lập**
Disable Recursion	Off
BIND Secondaries	On
Fail On Load If Bad Zone Data	Off
Enable Round Robin	On
Enable Netmask Ordering	On
Secure Cache Against Pollution	On
Name Checking	Multibyte (UTF-8)

Load Zone Data On Startup	Lấy từ Active Directory và ***Registry***
Enable Automatic Scavenging Of Stale Records	Off (yêu cầu cấu hình khi kích hoạt)

Trong hầu hết các trường hợp, các cài đặt mặc định này được chấp nhận và không yêu cầu chỉnh sửa. Tuy nhiên, khi cần thiết, bạn có thể sử dụng bảng điều khiển DNS để chỉnh sửa các tham số nâng cao này và áp dụng cho các trường hợp và nhu cầu triển khai đặc biệt nào đó.

Bạn có thể khôi phục lại các thiết lập mặc định này vào bất cứ lúc nào bằng cách sử dụng thẻ ***Advanced***. Việc này thực hiện đơn giản bằng cách nhấn vào phím ***Reset To Default***.

Các phần sau đây sẽ mô tả các tùy chọn cài đặt có thể một cách chi tiết hơn.

Vô hiệu hóa đệ quy

Tùy chọn ***Disable Recursion*** trên máy chủ bị vô hiệu hóa theo mặc định (có nghĩa là có thể thực hiện đệ quy). Khi tùy chọn ***Disable Recursion*** được kích hoạt, dịch vụ DNS Server sẽ không trả lời các truy vấn mà nó không có thẩm quyền hoặc các truy vấn mà nó chưa từng trả lời và chưa có trong bộ đệm của nó. Thay vào đó, dịch vụ DNS Server sẽ cung cấp cho máy khách các *tham chiếu*, đó là các bản ghi tài nguyên mà cho phép một máy khách DNS thực hiện các truy vấn lặp để phân giải một tên FQDN. Không nên vô hiệu hóa đệ quy trên một máy chủ nếu các máy chủ tên khác sử dụng nó như một máy chủ chuyển tiếp. Vô hiệu hóa đệ quy khi bạn muốn tạo ra chỉ một máy chủ tên và ngăn cản việc làm hư hỏng bộ đệm. Do máy chủ này không truy vấn các máy chủ tên khác, nó sẽ không duy trì bộ đệm và do đó sẽ khó khăn để giả mạo (làm hư hại đến bộ đệm)

BIND thứ cấp (BIND Secondaries)

Tùy chọn BIND ***Secondaries*** sẽ điều khiển liệu định dạng ***chuyển giao vùng nhanh*** có được sử dụng trong quá trình chuyển giao vùng DNS hay không. ***Berkeley Internet Name Domain*** (BIND) là một phương pháp triển khai thông thường của DNS được thực hiện trên hầu hết các phiên bản hiện có của hệ điều hành UNIX. Định dạng ***chuyển giao vùng nhanh*** là một phương thức hữu hiệu của việc chuyển giao các dữ liệu vùng có cung cấp khả năng nén dữ liệu và cho phép nhiều bản ghi có thể được chuyển giao trong một thông điệp TCP (***Transmission Control Protocol***). Việc chuyển giao vùng nhanh luôn được sử dụng giữa các máy chủ DNS sử dụng Windows, do đó tùy chọn ***BIND Secondaries*** không ảnh hưởng đến việc truyền thông giữa

các máy chủ Windows với nhau.Tuy nhiên, chỉ có BIND phiên bản 4.9.4 và sau đó mới có thể thực hiện việc chuyển giao vùng nhanh được.

Đối với các phiên bản BIND trước 4.9.4, các máy chủ DNS chạy Windows Server 2003 có thể được cấu hình để chuyển giao vùng sử dụng một định dạng chuyển giao vùng chậm và không có nén dữ liệu. Khi bạn lựa chọn hộp chọn ***BIND Secondaries*** trong thẻ ***Advanced*** của hộp thoại ***Server Properties***, sẽ không có chuyển giao vùng nhanh nào được thực hiện cả.

Nếu bạn biết các máy chủ DNS sẽ thực hiện việc chuyển vùng với các máy chủ DNS sử dụng BIND phiên bản 4.9.4 hoặc mới hơn, bạn có thể vô hiệu hóa tùy chọn này để cho phép việc chuyển giao vùng nhanh được thực hiện. (BIND 9.2 được phát hành ngày 17 tháng 1 năm 2001)

Fail On Load If Bad Zone Data (Không nạp nếu dữ liệu vùng bị hỏng)

Các máy chủ DNS chạy Windows Server 2003 theo mặc định sẽ nạp một vùng ngay cả khi vùng đó có chứa lỗi. Trong các tính huống như thế, các lỗi sẽ được ghi nhật ký lại và được bỏ qua. Việc kích hoạt "Fail On Load If Bad Zone Data" (Không nạp nếu dữ liệu vùng bị hỏng) sẽ ngăn cản không cho nạp một vùng nếu nó có lỗi.

Sắp xếp lại tập các kết quả

Các *máy tính đa hướng* (***Multihomed computers*** - các máy tính có nhiều hơn 1 bộ giao tiếp mạng hoặc một giao tiếp mạng nhưng lại có nhiều địa chỉ IP) thông thường sẽ đăng ký nhiều bản ghi tài nguyên địa chỉ máy (A) cho cùng một tên máy. Khi một máy trạm thực hiện việc phân giải tên của một máy đa hướng bằng cách liên lạc với máy chủ DNS, máy chủ DNS sẽ trả lại một danh sách phản hồi đến máy trạm, còn gọi là danh sách trả lời, danh sách này có các bản ghi tài nguyên đáp ứng yêu cầu của máy trạm. Sau khi nhận được danh sách phản hồi này từ máy chủ DNS, máy trạm DNS sẽ cố gắng liên lạc với máy đích bằng địa chỉ IP đầu tiên trong danh sách. Nếu việc này không thành, máy trạm sẽ cố gắng liên lạc với địa chỉ IP thứ hai và cứ thế tiếp tục. Tùy chọn "***Enable Netmask Ordering***" (Sắp xếp theo mặt nạ mạng) và "***Enable Round Robin***" (Luân chuyển quay vòng) sẽ được sử dụng để thay đổi thứ tự của các bản ghi tài nguyên mà được trả về trong danh sách phản hồi này.

Kích hoạt Round Robin (Luân chuyển quay vòng)

Round robin là một kỹ thuật cân bằng tải sử dụng bởi các máy chủ DNS để chia sẻ và phân bố mức tải tài nguyên mạng. Nếu nhiều bản ghi tài nguyên đều thỏa mãn với truy vấn, bạn có thể sử dụng ***round robin*** để quay vòng thứ tự các kiểu bản ghi tài nguyên này khi trả về cho máy trạm

Theo mặc định DNS sử dụng round robin để quay vòng thứ tự sắp xếp của các dữ liệu bản ghi tài nguyên trong câu trả lời cho một truy vấn, trong đó có nhiều bản ghi tài nguyên cùng kiểu của một tên miền DNS. Tính năng này cho ta một phương pháp đơn giản để cân bằng mức tải khi các máy khách truy cập các máy chủ Web cũng như thường xuyên thực hiện các truy vấn khác đến các máy tính đa hướng. Khả năng thực hiện quay vòng round robin trên tất cả các kiểu bản ghi tài nguyên là tính năng mới có trong Windows Server 2003

> ***LƯU Ý. Thứ tự ưu tiên mặt nạ mạng (Netmask Ordering).*** *Độ ưu tiên mạng con nội bộ (**Netmask Ordering**) là lớn hơn và sẽ thay thế việc sử dụng quay vòng round-robin đối với các máy tính đa hướng. Do đó khi được kích hoạt, round robin chỉ được sử dụng như là phương pháp thứ hai để sắp xếp các bản ghi trả lại trong danh sách phản hồi*

Ví dụ về round Robin. Máy chủ Web tên là server1.contoso.com có ba giao tiếp mạng và có 3 địa chỉ IP riêng biệt. Trong vùng được lưu trữ, (hoặc trong file của vùng hoặc trong Active Directory), ba bản ghi tài nguyên A sẽ ánh xạ tên máy đến từng địa chỉ IP xuất hiện theo thứ tự cố định như sau:

server1 IN A 10.0.0.1
server1 IN A 10.0.0.2
server1 IN A 10.0.0.3

Máy trạm DNS đầu tiên-client1- mà truy vấn máy chủ để phân giải tên máy này - sẽ nhận được danh sách này theo thứ tự mặc định. Tuy nhiên, khi máy trạm thứ hai-client2-gửi đi một truy vấn tiếp theo để phân giải tên máy chủ này, danh sách này đã được quay vòng như sau:

server1 IN A 10.0.0.2
server1 IN A 10.0.0.3
server1 IN A 10.0.0.1

Vô hiệu hóa round robin . Khi bạn xóa hộp chọn Enable Round Robin, round robin sẽ bị vô hiệu hóa. Nếu ***round robin*** bị vô hiệu hóa trên một máy chủ DNS, thứ tự của các phản hồi cho các truy vấn sẽ dựa trên thứ tự gán tĩnh của các bản ghi tài nguyên trong danh sách trả lời như khi chúng lưu trong vùng (hoặc trong file của vùng hoặc trong Active Directory)

Kích hoạt Thứ tự mặt nạ mạng (Nestmask Ordering). Thứ tự mặt nạ mạng là một phương pháp mà DNS sử dụng để sắp xếp thứ tự và độ ưu tiên cho các địa chỉ IP trong cùng một mạng khi một máy khách truy vấn một tên máy mà có nhiều bản ghi tài nguyên A. Phương pháp này được thiết kế cho phép các chương trình máy khách có thể kết nối đến một máy bằng cách sử dụng địa chỉ IP gần nhất (và do đó được dự kiến là nhanh nhất) có thể.

Khi trả về nhiều hơn một địa chỉ IP cho máy khách, nếu ***Nestmask Ordering*** được kích hoạt, các địa chỉ IP phù hợp nhất với mặt nạ mạng của máy khách sẽ được đặt trên đầu tiên trong danh sách phản hồi. Tùy chọn kích hoạt ***Nestmask Ordering*** được lựa chọn theo mặc định. Ví dụ, một máy tính đa hướng, ***server1.contoso.com*** có ba bản ghi tài nguyên A cho ba địa chỉ IP trong vùng ***contoso.com***. Ba bản ghi tài nguyên này xuất hiện theo thứ tự sau trong vùng-hoặc trong file của vùng hoặc trong Active Directory:

server1 IN A 192.168.1.27
server1 IN A 10.0.0.14
server1 IN A 172.16.20.4

Khi một máy khách DNS có địa chỉ IP là 10.4.3.2 truy vấn máy chủ về địa chỉ IP của máy ***server1.comtoso.com***, dịch vụ ***DNS*** Se***r***ver nhận thấy rằng địa chỉ IP gốc của mạng của máy khách (10.0.0.0) sẽ phù hợp nhất với ID mạng (lớp A) của địa chỉ 10.0.0.14 trong danh sách trả lời của các bản ghi tài nguyên. Dịch vụ DNS Server sau đó sẽ xác định lại thứ tự của các địa chỉ này trong danh sách phản hồi như sau:

server1 IN A 10.0.0.14
server1 IN A 192.168.1.27
server1 IN A 172.16.20.4

Nếu như ID mạng của địa chỉ IP của máy khách truy vấn không phù hợp với bất kỳ ID của mạng nào có trong các bản ghi tài nguyên trong danh sách trả lời, danh sách này sẽ không bị sắp xếp thứ tự lại.

Trong mạng mà có sử dụng việc phân đoạn mạng con IP (IP subnetting - không sử dụng mặt nạ mạng con mặc định), lần đầu máy chủ DNS sẽ trả về một địa chỉ IP mà phù hợp với cả ID mạng và ID của mạng con của máy khách trước khi trả về bất kỳ một địa chỉ IP nào mà chỉ phù hợp với ID mạng của máy khách.

Ví dụ, một máy tính đa hướng server1.contoso.com, có 4 bản ghi tài nguyên A tương ứng với từng địa chỉ IP trong vùng contoso.com. Hai trong số các địa chỉ IP này thuộc về các mạng khác riêng biệt. Hai địa chỉ còn lại cùng chung một địa chỉ mạng IP thông thường, nhưng bởi vì mặt nạ mạng tùy chọn 255.255.248.0 được sử dụng, các địa chỉ IP là nằm trong các mạng con khác nhau. Các bản ghi tài nguyên ví dụ này xuất hiện theo thứ tự sau đây trong vùng, có thể trong file của vùng hoặc trong Active Directory:

server1 IN A 192.168.1.27
server1 IN A 172.16.22.4
server1 IN A 10.0.0.14
server1 IN A 172.16.31.5

Nếu địa chỉ IP của máy khách thực hiện truy vấn là 172.16.22.8, cả hai địa chỉ IP mà cùng trong mạng IP với máy khách, mạng 172.16.0.0, sẽ được trả về cho máy khách và sẽ được nằm trên đầu của danh sách trả về. Tuy nhiên, trong ví dụ này, địa chỉ 172.16.22.4 sẽ được đặt trên địa chỉ 172.16.31.5 bởi vì nó gần hơn với địa chỉ mạng IP của máy khách.

Thứ tự của danh sách trả về bởi dịch vụ DNS như sau:

server1 IN A 172.16.22.4
server1 IN A 172.16.31.5
server1 IN A 192.168.1.27
server1 IN A 10.0.0.14

LƯU Ý. Các thiết lập LocalNetPriority và thứ tự mặt nạ mạng. Thứ tự mặt nạ mạng thường được gọi là thiết lập ***LocalNetPriority***. Tên này xuất phát từ tùy chọn ***LocalNetPriority*** tương ứng mà sử dụng trong tiện ích dòng lệnh ***Dnscmd***.

Bảo mật bộ đệm khỏi bị sai hỏng

Theo mặc định, tùy chọn ***Secure Cache Against Pollution*** (Bảo mật bộ đệm khỏi bị sai hỏng) sẽ được kích hoạt. Thiết lập này cho phép máy chủ DNS bảo vệ bộ đệm của nó khỏi các tham chiếu mà các tham chiếu này thường làm sai hỏng hoặc không bảo mật nó. Khi thiết lập này được kích hoạt, máy chủ sẽ chỉ lưu đệm các bản ghi có tên tương ứng với miền mà tên miền này có trong truy vấn tạo ra. Bất kỳ tham chiếu nào nhận được từ các máy chủ DNS khác đi kèm trong một truy vấn phản hồi sẽ bị từ chối.

Ví dụ, nếu một truy vấn về tên example.microsoft.com được tạo ra và một câu trả lời tham chiếu cung cấp một bản ghi về tên không phải trong cây tên miền ***microsoft.com*** (ví dụ ***msn.com***), tên đó sẽ bị từ chối khi tùy chọn ***Secure Cache Against Pollution*** được kích hoạt. Thiết lập này cho phép ngăn ngừa, không cho các máy tính chưa xác thực giả mạo các máy chủ mạng khác.

Khi tùy chọn này được bỏ kích hoạt, tuy nhiên, máy chủ sẽ lưu đệm tất cả mọi bản ghi tài nguyên nhận được khi trả lời cho các truy vấn DNS-thậm chí khi bản ghi đó không tướng ứng với tên miền có trong truy vấn.

Kiểm tra tên

Theo mặc định, hộp danh sách xổ xuống ***Name Checking*** trong thẻ ***Advance*** của hộp thoại thuộc tính ***Server Properties*** được thiết lập là ***Multibyte*** (***UTF-8***). Do đó dịch vụ DNS, theo mặc định, sẽ xác nhận rằng mọi tên miền mà dịch vụ này thực hiện sẽ tương thích với Định dạng Chuyển đổi UCS (UCF). Unicode là một lược đồ mã hóa 2 byte, tương thích với định dạng 1 byte **American Standard Code for Information Interchange (ASCII)**

truyền thống, điều này cho phép thể hiện dạng nhị phân hầu hết các ngôn ngữ của con người. Bảng 4-4 liệt kê và mô tả bốn phương pháp kiểm tra tên

Bảng 4-4. Các phương pháp kiểm tra tên

Phương pháp	Mô tả
Strict RFC (***American Standard Code for Information Interchange [ASCII]***)	Sử dụng phương pháp kiểm tra tên chặt chẽ. Các hạn chế này, thiết lập trong RFC 1123, bao gồm việc giới hạn các tên chỉ bao gồm các ký tự viết hoa và thường (A-Z,a-z), các số (0-9) và dấu gạch ngang (-). Ký tự đầu tiên của tên DNS có thể là một số
Non RFC (ANSI)	Cho phép các tên không chuẩn và không theo các đặc tả về tên máy Internet trong RFC 1123
Multibyte (UTF-8)	Cho phép nhận biết các ký tự khác ngoài ASCII, bao gồm Unicode, thông thường được mã hóa với độ dài lớn hơn 1 octet. Với tùy chọn này, các ký tự đa byte có thể được chuyển đổi và biểu hiện bằng cách sử dụng hỗ trợ UTF-8, hình thức này được cung cấp sẵn trong Windows Server 2003. Các tên mã hóa trong định dạng UTF-8 phải không vượt quá kích thước giới hạn chỉ định trong RFC 2181, đặc tả này qui định tối đa 63 octet trên một nhãn và 255 octet trên một tên. Việc đếm ký tự là không thích hợp để xác định kích thước tên do một số ký tự UTF-8 có độ dài vượt quá một octet. tùy chọn này cho phép các tên miền sử dụng bảng chữ cái không phải tiếng Anh
All Name (Tất cả mọi tên)	Cho phép bất kỳ hình thức đặt tên nào

Mặc dù phương pháp kiểm tra tên theo chuẩn UTF-8 có tính linh hoạt cao nhưng bạn nên xem xét việc thay đổi tùy chọn ***Name Checking*** sang ***Strict RFC*** khi các máy chủ DNS của bạn thực hiện việc chuyển giao vùng với các máy chủ không phải là Windows mà không nhận biết được mã ***UTF-8***. Mặc dù máy chủ DNS mà không nhận biết UTF-8 có thể chấp nhận việc chuyển giao vùng chứa các tên mã hóa UTF-8, các máy chủ này có thể không ghi lại các tên này vào trong file của vùng hoặc nạp các tên này từ file của vùng.

Bạn chỉ nên sử dụng hai tùy chọn kiểm tra tên khác, ***Non RFC*** và ***All Names***, chỉ khi các ứng dụng đặc biệt yêu cầu chúng.

Nạp dữ liệu của vùng khi khởi động

Theo mặc định, đặc tính "***Load Zone Data On Startup***" (Nạp dữ liệu của vùng khi khởi động) được thiết lập là lựa chọn "***From Active Directory And Registry***" (Từ Active Directory và từ Registry). Do đó, theo mặc định, các máy chủ DNS trong Windows Server 2003 sẽ khởi tạo với các thiết lập chỉ định trong CSDL Active Directory và ***registry*** của máy chủ

Bạn còn có thể nạp dữ liệu vùng bằng cách sử dụng hai thiết lập khác: Từ Registry và Từ file. Tùy chọn Từ Registry sẽ bắt các máy chủ DNS khởi tạo bằng cách đọc các tham số lưu trong registry của Windows. Tùy chọn Từ File sẽ bắt máy chủ DNS khởi tạo bằng cách đọc các tham số lưu trong file khởi động. File khởi động phải là một file văn bản tên là Boot đặt trong thư mục ***%systemroot%\System32\Dns*** trên máy tính nội bộ.

Khi file khởi động được sử dụng, các thiết lập trong file sẽ áp dụng trong máy chủ và ghi đè các thiết lập lưu trong registry của máy chủ DNS. Tuy nhiên, đối với các tham số mà không thể được cấu hình bởi các định hướng trong file khởi động, các thiết lập mặc định trong registry (hoặc đã được cấu hình lại và lưu trong các thiết lập máy chủ) sẽ được áp dụng bởi dịch vụ DNS Server.

> ***THÔNG TIN THÊM. Cấu trúc file khởi động DNS***. *Xem thêm trong Microsoft Knowledge Base Article 194513, "Cấu trúc của một file khởi động DNS" Để tìm chủ đề này, hãy đến http:// support.microsoft.com và nhập vào số thứ tự bài viết trong hộp văn bản Search The Knowledge Base.*

LÃO HÓA VÀ LOẠI BỎ CÁC BẢN GHI TÀI NGUYÊN (AGING AND SCAVENGING)

Thông thường, người quản trị DNS sẽ thực hiện thủ công việc thêm hoặc xóa các bản ghi tài nguyên khỏi file của vùng DNS nếu cần. Với tính năng cập nhật động, các máy tính và dịch vụ riêng lẻ sẽ có khả năng tự động thêm, cập nhật và xóa các bản ghi tài nguyên DNS. Ví dụ, dịch vụ ***DNS Client*** trong Windows Server 2003 và Windows Server 2000 sẽ đăng ký bản ghi tài nguyên A và PTR của chúng với DNS khi khởi động và cứ tiếp tục sau mỗi 24 giờ. Việc cập nhật động đảm bảo rằng các bản ghi luôn là mới nhất, và bảo vệ DNS khi người quản trị vô tính xóa bất kỳ bản ghi tài nguyên nào

Theo thời gian, các bản ghi tài nguyên cũ sẽ chồng chất bên trong CSDL DNS. Các bản ghi sẽ trở nên cũ, ví dụ như khi máy tính của các người dùng hay di chuyển bị ngắt khỏi mạng một cách bất thường. Các bản ghi cũ sẽ cung cấp các thông tin lỗi thời và không chính xác cho máy khách, chiếm các không gian đĩa không cần thiết và có thể làm giảm hiệu năng của máy chủ. Windows Server 2003 cung cấp một kỹ thuật để loại bỏ các bản ghi kiểu này.

Windows Server 2003 sẽ gắn một tem định thời vào trong các bản ghi tài nguyên mà được tự động thêm vào trong các vùng chính thức nếu các vùng này đã được kích hoạt tính năng lão hóa (***aging***) và loại bỏ (***scavenging***). Các bản ghi được thêm vào một cách thủ công sẽ được gắn một tem định thời với giá trị là 0, điều này thể hiện các bản ghi này là ngoại lệ và không bị ảnh hưởng bởi quá trình lão hóa và loại bỏ. Khi các máy chủ tên thứ cấp nhận được một bản sao chỉ-đọc của dữ liệu của vùng từ máy chủ tên chính thức, chỉ các vùng chính thức mới có khả năng tham gia quá trình này. Các máy chủ có thể được cấu hình để tự động thực hiện việc loại bỏ theo định kỳ hoặc bạn có thể khởi tạo việc loại bỏ một cách thủ công và ngay lập tức trên máy chủ này.

- **Khởi tạo việc loại bỏ.**

Để khởi tạo việc loại bỏ, thực hiện theo các bước sau đây:

1. Mở bảng điều khiển quản trị DNS
2. Trong bảng điều khiển, nhấn phải chuột vào máy chủ DNS tương ứng và sau đó nhấn vào ***Set Aging/Scavenging For All Zones.*** (Thiết lập Lão hóa/Loại bỏ Cho Tất Cả Các Vùng)
3. Trong hộp thoại "***Server Aging/Scavenging Properties***" (Các thuộc tính Lão hóa/Loại bỏ của máy chủ), lựa chọn hộp chọn "***Scavenge Stale Resource Records***" (Loại bỏ các bản ghi tài nguyên lỗi thời), thiết lập một, không hoặc cả hai lựa chọn sau đây và nhấn ***OK.***

- **No-Refresh Interval**. Khoảng thời gian giữa thời điểm gần đây nhất thực hiện làm tươi tem định thời trong bản ghi và thời điểm mà tem định thời sẽ tiếp tục được làm tươi.
- **Refresh Interval**. Khoảng thời gian giữa thời điểm xa nhất mà tem định thời trong bản ghi có thể được làm tươi và thời điểm xa nhất khi một bản ghi có thể bị loại bỏ. Khoảng thời gian giữa các lần làm tươi phải dài hơn chu kỳ làm mới tối đa của bản ghi.

4. Trong hộp thoại ***Server Aging/Scavenging Confirmation*** (Xác nhận thiết lập Lão hóa/Loại bỏ của máy chủ), lựa chọn "***Apply These Settings To The Existing Active Directory–Integrated Zones***" (Áp dụng các thiết lập này vòa các vùng tích hợp Active Directory đã tồn tại) và nhấn ***OK***

CẢNH BÁO. Cấu hình lão hóa và loại bỏ một cách thích hợp*. Theo mặc định các kỹ thuật loại bỏ bị vô hiệu hóa. Bạn không nên kích hoạt việc loại bỏ các bản ghi tài nguyên DNS trừ khi bạn hoàn toàn đảm bảo rằng bạn đã hiểu hết các tham số và đã từng cấu hình chúng một cách đúng đắn. Nếu không, bạn có thể vô tình cấu hình cho phép máy chủ xóa đi các bản ghi mà đúng ra nó phải được giữ lại. Nếu một tên bị vô tình xóa đi, không chỉ người dùng không thể phân giải tên đó mà các người dùng khác còn có thể tạo ra và sở hữu tên đó, thậm chí ngay cả trong trường hợp các vùng được cấu hình chỉ cho phép các cập nhật bảo mật.*

QUẢN LÝ BỘ ĐỆM PHÂN GIẢI TÊN DNS (DNS RESOLVER CACHE)

Bộ phân giải tên DNS (***DNS resolver***) là một thành phần của dịch vụ DNS Client được cài đặt theo mặc định trong Windows Server 2003. Nó hoạt động cùng với tiến trình ***SVCHOST***

THÔNG TIN THÊM. SVCHOST là gì*? Xem thêm Bài viết 250320 trong Microsoft Knowledge Base "Mô tả svchost.exe trong Windows 2000". Để tìm bài viết này, hãy vào http://support.microsoft.com và nhập vào số thứ tự bài viết trong hộp văn bản* ***Search The Knowledge Base.***

Để giảm lưu lượng mạng đến các máy chủ DNS, bộ phân giải tên DNS sẽ lưu đệm các bản ghi tài nguyên có được trong các quá trình phản hồi lại các truy vấn. Các bản ghi tài nguyên này được sử dụng để phân giải các truy vấn lặp đi lặp lại từ máy khách và giảm các truy vấn dư thừa đến máy chủ DNS. Mỗi mục vào trong bộ đệm có một giá trị TTL xác định, thông thường được chỉ định bởi phản hồi truy vấn. Khi giá trị TTL này hết hạn, mục này sẽ bị xóa khỏi bộ đệm.

Khi bộ phân giải này không thể trả lời các truy vấn bằng cách sử dụng bộ đệm của nó, bộ phân giải này sẽ gửi truy vấn đến một hoặc nhiều máy chủ DNS được cấu hình trong trang thuộc tính của máy chủ này. Nếu nhu file ***Hosts*** được cấu hình trên các máy khách, nó sẽ được nạp sẵn trước vào trong bộ đệm phân giải.

Để xem bộ đệm, nhập vào dòng sau đây trong dấu nhắc dòng lệnh:

ipconfig /displaydns

Để xóa bộ đệm, nhập vào dòng sau đây trong dấu nhắc dòng lệnh:

ipconfig /flushdns

BẢO MẬT DNS

DNS là một giao thức mở và do đó nó có thể bị tổn thương bởi các kẻ tấn công. Windows Server 2003 cung cấp khả năng trợ giúp ngăn cản các cuộc tấn công vào cơ sở hạ tầng DNS của bạn thông qua các tính năng bảo mật bổ sung.

Phần này sẽ mô tả các nguy cơ thông thường của việc bảo mật DNS và cách thức để xác định các mức bảo mật DNS trong doanh nghiệp của bạn. Các thiết lập bảo mật mặc định và các tính năng bảo mật cũng sẽ được thảo luận.

Các nguy cơ bảo mật DNS.

Bảng 4-5 mô tả các phương thức điển hình trong đó cơ sở hạ tầng DNS bị de dọa bởi các kẻ tấn công.

Bảng 4-5. Các mối đe dọa thông thường đến an toàn DNS

Các mối đe dọa	Mô tả
Footprinting *(Lấy dấu vết)*	Là quá trình trong đó các dữ liệu của vùng DNS, bao gồm các tên miền, các tên máy tính và các địa chỉ IP của các tài nguyên mạng cơ bản bị kẻ tấn công lấy được. Một kẻ tấn công thông thường bắt đầu tấn công bằng cách sử dụng các dữ liệu DNS này để dựng lại sơ đồ, hay dấu vết cảu hệ thống mạng. Để dễ dàng nhận dạng, miền DNS và các tên máy tính thông thường có tên thể hiện chức năng hoặc vị trí của một máy chủ quản trị miền hoặc máy tính. Kẻ tấn công sẽ lợi dụng các ưu điểm của cách đặt tên này nhằm xác định các tài nguyên chính trong hệ thống mạng
Denial of service *(Từ chối Dịch vụ)*	Một cuộc tấn công kiểu Từ chối Dịch vụ (***Denial of Service*** - DoS) là một cuộc công kích, thường là có kế hoạch trước, tìm mọi cách để phá hủy tính năng của hệ thống. Một cuộc tấn công DoS sẽ làm tràn ngập tài nguyên mạng bằng các yêu cầu giả mạo mà không thể hoàn thành được. Theo cách đó, nó làm cho hệ thống trở nên luôn luôn bận rộn vì phải đáp ứng các yêu cầu giả mạo và không thể phục vụ các yêu cầu chính đáng khác. Trong ngữ cảnh của DNS, một cuộc tấn công DoS sẽ cố gắng làm một hoặc nhiều máy chủ DNS bị quá tải bằng cách làm chúng ngập tràn với các truy vấn đệ quy. Điều này sẽ làm cho CPU luôn hoạt động ở 100% hiệu suất và làm cho máy chủ gần như không thể đáp ứng các truy vấn hợp lệ khác

Chỉnh sửa dữ liệu	Một nỗ lực của kẻ tấn công (sau khi đã hoàn thành việc tấn công ***Footprint***) sử dụng các địa chỉ IP hợp lệ trong các gói tin IP mà kẻ tấn công tạo ra, do đó các gói tin này giống như là xuất phát từ một địa chỉ IP hợp lệ trong mạng. Cách này thường còn được gọi là ***IP spoofing*** - *Giả mạo IP*. Với địa chỉ IP hợp lệ này (một địa chỉ IP nằm trong dải địa chỉ của mạng con), kẻ tấn công có thể truy cập vào hệ thống mạng và phá hủy các dữ liệu hoặc tiến hành các cuộc tấn công khác.
Định hướng lại.	Là hình thức tấn công trong đó kẻ tấn công có khả năng định hướng lại các truy vấn về các tên DNS đến các máy chủ nằm thuộc quyền kiểm soát của kẻ tấn công. Một phương pháp định hướng lại là làm sai hỏng bộ đệm DNS của một máy chủ DNS bằng cách dữ liệu DNS không chuẩn mà có thể dẫn hướng các truy vấn tiếp theo sang các máy chủ thuộc quyền kiểm soát của kẻ tấn công.Ví dụ, nếu một truy vấn được tạo ra để truy vấn về tên ***example.microsoft.com*** và câu trả lời tham chiếu cung cấp một bản ghi về một tên nằm ngoài miền ***microsoft.com***, ví dụ như ***malicious-user.com***, máy chủ DNS sẽ sử dụng các dữ liệu bộ đệm của ***malicious-user.com*** để phân giải truy vấn về tên đó. Việc định hướng có thể được thực hiện bất cứ khi nào kẻ tấn công có khả năng truy cập và ghi được vào dữ liệu của DNS, ví dụ như các cập nhật động không bảo mật

Các mức bảo mật DNS

Việc triển khai bảo mật DNS có thể được tổng hợp trong ba mức sau: thấp, trung bình và cao. Xem qua các đặc tính của các mức để xác định mức nào phù hợp nhất với mức độ bảo mật của hệ thống DNS của bạn và các đặc tính nào sẽ được áp dụng khi triển khai cho hệ thống DNS của bạn.

Bảo mật mức thấp. Bảo mật mức thấp là một tiêu chuẩn triển khai DNS mà không có cấu hình bảo mật phòng ngừa trước nào cả. Chỉ triển khai mức bảo mật DNS này trong hệ thống mạng mà bạn không phải lo lắng gì về tính toàn vẹn của các dữ liệu DNS hoặc các mạng cá nhân riêng nơi không có sự đe dọa nào từ các kết nối bên ngoài. Bảo mật mức thấp có các đặc tính sau đây:

- Nếu có kết nối đến Internet, cơ sở hạ tầng DNS của doanh nghiệp của bạn sẽ có thể bị phơi bày hoàn toàn trên Internet.
- Các phân giải tên DNS chuẩn được thực hiện bởi tất cả các máy chủ DNS trong mạng của bạn
- Mọi máy chủ DNS đều được cấu hình với ***root hint*** trỏ đến các máy chủ mức gốc trên Internet.

- Mọi máy chủ DNS đều cho phép chuyển giao vùng đến bất kỳ máy chủ nào
- Mọi máy chủ DNS đều cấu hình để lắng nghe trên mọi địa chỉ IP của nó.
- Sự ngăn ngừa việc làm sai hỏng bộ đệm bị vô hiệu hóa trên tất cả các máy chủ DNS
- Các cập nhật động không bảo mật được cho phép đối với tất cả các vùng DNS
- Cổng 53 của giao thức TCP và UDP được mở trên các tường lửa trong hệ thống mạng của bạn cho cả các địa chỉ nguồn và địa chỉ đích

Bảo mật mức trung bình. Bảo mật mức trung bình sử dụng các tính năng bảo mật DNS có sẵn mà không nhất thiết các máy chủ DNS phải nằm trên các máy chủ quản trị miền hoặc lưu các vùng DNS trong Active Directory. Bảo mật mức trung bình có các đặc tính sau đây:

- Nếu có kết nối đến Internet, cơ sở hạ tầng DNS của doanh nghiệp của bạn sẽ bị phơi bày hay lộ ra một cách hạn chế
- Tất cả mọi máy chủ DNS được cấu hình sử dụng các ***forwarder*** để trỏ đến một danh sách xác định gồm các máy chủ DNS nội bộ khi chúng không thể tự phân giải các tên.
- Mọi máy chủ DNS đều giới hạn việc chuyển giao vùng đến các máy chủ liệt kê trong các bản ghi tài nguyên NS trong các vùng của chúng
- Các máy chủ DNS được cấu hình để lắng nghe trên các địa chỉ IP xác định
- Sự ngăn ngừa việc làm hư hỏng bộ đệm sẽ được kích hoạt trên tất cả các máy chủ DNS
- Các cập nhật động sẽ không được phép trên bất kỳ vùng DNS nào
- Các máy chủ DNS nội bộ sẽ trao đổi thông tin với các máy chủ DNS bên ngoài thông qua tường lửa, với một danh sách hạn chế các địa chỉ nguồn và đích được cho phép.
- Các máy chủ DNS bên ngoài mà nằm trước tường lửa của bạn sẽ được cấu hình với ***root hint*** mà trỏ đến các máy chủ mức gốc trên Internet.

- Tất cả các phân giải tên DNS đều được thực hiện thông qua máy chủ ***proxy*** và các ***gateway***.

Bảo mật mức cao. Bảo mật mức cao sử dụng cùng cấu hình giống như trong bảo mật mức trung bình nhưng đồng thời sử dụng các tính năng bảo mật có sẵn trong các máy chủ DNS mà đồng thời là máy chủ quản trị miền cũng như trong các vùng được lưu trong Active Directory. Hơn nữa, bảo mật mức cao sẽ hoàn toàn hạn chế việc trao đổi thông tin DNS với Internet. Đây không phải là một cấu hình thông dụng, nhưng cấu hình này được khuyến cáo là nên áp dụng khi mà không yêu cầu phải có kết nối ra Internet. Đặc tính của bảo mật mức cao như sau:

- Cơ sở hạ tầng DNS của doanh nghiệp của bạn sẽ không trao đổi thông tin với Internet thông qua các máy chủ DNS nội bộ
- Hệ thống mạng của bạn sử dụng một DNS root và không gian tên nội bộ; mọi thẩm quyền của các vùng DNS này đều là nội bộ.
- Các máy chủ DNS được cấu hình với các forwarder mà chỉ sử dụng địa chỉ của các máy chủ DNS nội bộ
- Mọi máy chủ DNS đều giới hạn việc chuyển giao vùng đến các địa chỉ IP xác định.
- Các máy chủ DNS được cấu hình để lắng nghe trên các địa chỉ IP xác định
- Sự ngăn ngừa việc làm hư hỏng bộ đệm sẽ được kích hoạt trên tất cả các máy chủ DNS
- Các máy chủ DNS nội bộ sẽ được cấu hình với root hint trỏ đến các máy chủ DNS nội bộ mà chứa vùng root của không gian tên nội bộ của bạn.
- Mọi máy chủ DNS đều chạy trên các máy chủ quản trị miền. Một Danh sách Điều khiển Truy cập Khi cần (**Discretionary Access Control List -** DACL) được cấu hình với dịch vụ ***DNS Server*** để chỉ cho phép các tài khoản cụ thể được thực hiện các tác vụ quản trị trên máy chủ DNS.
- Các vùng DNS được lưu trong Active Directory. DACL được cấu hình để chỉ cho phép một số tài khoản xác định có khả năng tạo, xóa hoặc chỉnh sửa các vùng DNS.

- Cập nhật động bảo mật được cấu hình trên các vùng DNS ngoại trừ các vùng mức đỉnh và mức gốc, hai vùng này không cho phép bất kỳ một sự chuyển giao vùng nào.

Các đối tượng DNS trong Windows Server 2003 Active Directory

Bên cạnh việc **đối tượng chứa (container object)** ***MicrosoftDNS*** nằm trong phân vùng miền (***domain partition***), có hỗ trợ trong cả Windows 2000 và Windows Server 2003, đối tượng ***MicrosoftDNS*** còn được đặt trong tất cả các phân vùng thư mục ứng dụng DNS (***DNS application directory partition***). Một *phân vùng thư mục ứng dụng DNS* là một kiểu mới của các phân vùng thư mục trong Windows Server 2003. Nó có thể được sử dụng bởi các ứng dụng để lưu các dữ liệu xác định của ứng dụng mà phạm vi áp dụng của nó không vượt quá ra ngoài toàn bộ rừng hoặc miền. Dữ liệu này có thể có các đặc điểm như thường xuyên thay đổi (động) hoặc có một thời hạn sử dụng ngắn (không ổn định). Ví dụ, Windows Server 2003 DNS có thể sử dụng các phân vùng thư mục ứng dụng để lưu các dữ liệu được cập nhật động của vùng DNS chỉ trên các máy chủ quản trị miền đồng thời là máy chủ DNS thay cho việc thực hiện chúng trên tất cả các máy chủ quản trị miền trong miền, đây là yêu cầu của các vùng tích hợp Active Directory trong Windows 2000.

Đối tương chứa ***MicrosoftDNS*** là một đối tượng mức cha của tất các các vùng trong miền hoặc trong phạm vi đồng bộ, điều này được chỉ định bởi phân vùng thư mục ứng dụng DNS. Một người dùng không có quyền đọc và ghi trên đối tượng chứa này sẽ không có khả năng cập nhật vùng hoặc tạo ra các vùng và bản ghi mới trong các vùng của phân vùng đó.

Mỗi vùng DNS được thể hiện trong Active Directory bởi một đối tượng ***dnsZone***. Các đối tượng vùng là đối tượng mức con của đối tượng ***MicrosoftDNS*** trong miền hoặc trong phân vùng thư mục ứng dụng. Các đối tượng vùng lưu các thông tin cấu hình trong thuộc tính ***dnsProperty***. Danh sách điều khiển truy cập DACL trên đối tượng vùng sẽ điều khiển việc tạo ra các bản ghi trong vùng đó, và các bản ghi đã có trong vùng cũng có thể thừa hưởng các hiệu ứng này. Việc quản trị các vùng, ví dụ như chỉnh sửa các tham số của vùng, sẽ yêu cầu một người dùng có quyền ***Full Control*** đối với đối tượng vùng trong đối tượng chứa ***MicrosoftDNS*** của Active Directory.

Tất cả tập hợp các bản ghi mà thuộc về một tên miền DNS đơn sẽ được lưu trong Active Directory trong một đối tượng ***dnsNode*** đơn. Danh sách điều khiển truy cập ACL trên đối tượng này sẽ điều khiển việc truy cập của máy khách.

Bảo mật dịch vụ DNS Server

Dịch vụ ***DNS server*** có thể chạy trên một máy chủ thành viên hoặc trên một máy chủ quản trị miền. Khi dịch vụ này chạy trên máy chủ quản trị miền, các tùy chọn bảo mật của nó sẽ có nhiều tính năng nâng cao hơn các tùy chọn có khi nó chạy trên một máy chủ thành viên.

Bảo mật một máy chủ DNS chạy trên một máy chủ thành viên. Bảng 4-6 sẽ mô tả các tùy chọn cấu hình dịch vụ ***DNS Server*** mà có các tính năng liên quan đến bảo mật khi dịch vụ ***DNS Server*** chạy trên máy chủ thành viên hoặc trên máy chủ quản trị miền

Bảng 4-6. Các thiết lập của dịch vụ DNS Server liên quan đến bảo mật

Các thiết lập	Mô tả
Các giao diện	Theo mặc định, dịch vụ DNS chạy trên máy tính đa hướng sẽ được cấu hình để lắng nghe các truy vấn DNS trên tất các địa chỉ IP của nó. Chỉ giới hạn các địa chỉ IP mà máy chủ DNS lắng nghe trên đó, đó sẽ là các địa chỉ IP mà các máy khách sẽ cấu hình là máy chủ DNS ưa thích của chúng
Secure Against Cache Pollution (*Bảo mật chống lại việc làm sai hỏng bộ đệm*)	Tùy chọn " ***Secure Against Cache Pollution***" sẽ ngăn cản một kẻ tấn công có thể làm sai hỏng bộ đệm của một máy chủ DNS bằng các bản ghi tài nguyên mà máy chủ DNS không yêu cầu. Việc thay đổi các thiết lập mặc định này sẽ làm giảm tính toàn vẹn của các phản hồi cung cấp bởi dịch vụ DNS Server.
Disable Recursion (*Vô hiệu hóa đệ quy)*	Đệ quy có thể được sử dụng bởi kẻ tấn công để từ chối dịch vụ ***DNS Server***; do đó nếu một máy chủ DNS trong hệ thống mạng của bạn không có ý định nhận hoặc thực hiện các truy vấn đệ quy, việc đệ quy nên bị vô hiệu hóa. Lưu ý rằng việc ***forwarding*** chính là thực hiện đệ quy.
Các ***root hint***	Nếu bạn có một DNS gốc nội bộ trong cơ sở hạ tầng mạng của bạn, hãy cấu hình các ***root hint*** trên các máy chủ nội bộ của bạn chỉ trỏ đến các máy chủ mà chứa miền gốc nội bộ chứ không phải là các máy chủ chứa miền gốc trên Internet. Điều này sẽ ngăn cản các máy chủ DNS nội bộ của bạn không gửi các thông tin cá nhân ra ngoài Internet trong quá trình phân giải các tên.

Các thiết lập điều khiển truy cập Active Directory. Danh sách DACL được sử dụng bởi dịch vụ ***DNS Server*** khi nó chạy trên máy chủ quản trị miền sẽ cho phép bạn quản lý quyền điều khiển dịch vụ ***DNS Server*** của các người dùng và nhóm trong Active Directory.

LƯU Ý. Tính sẵn sàng của các tính năng bảo mật Active Directory*. Các tính năng bảo mật Active Directory sẽ có trong dịch vụ DNS Server khi nó chạy trên máy chủ quản trị miền và không có trong dịch vụ* ***DNS Server*** *chạy trên các máy chủ Windows Server 2003 thành viên hoặc các máy chủ Web chạy hệ điều hành Windows Server 2003 bởi vì các cấu hình này không chứa trong Active Directory.*

- **Cấu hình các thiết lập bảo mật DNS cho dịch vụ DNS Server.**

Để đặt các cấu hình bảo mật DNS cho dịch vụ DNS Server, thực hiện theo các bước sau:

1. Mở bảng điều khiển ***DNS***
2. Trong bảng điều khiển, nhấn phải chuột vào máy chủ tương ứng và lựa chọn ***Properties***
3. Trong thẻ ***Security***, chỉnh sửa danh sách của các người dùng hoặc nhóm thành viên được phép quản trị máy chủ ***DNS*** và ***reset*** lại các quyền này nếu cần.

LƯU Ý. Quyền áp dụng cho dịch vụ DNS Server*. Các thiết lập bảo mật sẽ xác định ai có thể quản trị dịch vụ DNS Server nhưng chúng không ảnh hưởng đến DACL của các vùng và bản ghi tài nguyên lưu trên máy chủ này.*

Bảo mật các vùng gói trong file.

Bảo mật DNS cho các vùng được gói trong file sẽ yêu cầu việc quản trị quyền truy cập hệ thống file NTFS trên các file của vùng lưu trên máy chủ Windows Server 2003 thành viên.

- **Thiết lập quyền trên file của vùng được gói trong file.**

Để thiết lập quyền trên file của vùng được gói trong file thực hiện theo các bước sau:

1. Mở ***Windows Explorer***, và sau đó tìm đến file của vùng hoặc thư mục DNS trong đó file của vùng được lưu (theo mặc định, tất cả các file của vùng được lưu trong thư mục %***systemroot***%***System32\Dns***)

2. Nhấn phải chuột vào file của vùng hoặc thư mục đó, nhấn vào ***Properties*** và sau đó nhấn vào thẻ ***Security***

3. Trong cửa sổ thuộc tính của file hoặc thư mục, thực hiện một trong các bước sau đây:

- Để thiết lập quyền cho một nhóm hoặc người dùng mà không có trong hộp ***Group Or User Names***, nhấn vào ***Add***. Nhập vào tên của nhóm hoặc người dùng mà bạn muốn thiết lập cấp phép và sau đó nhấn ***OK***

- Để thay đổi hoặc dỡ bỏ cấp phép của một nhóm hoặc người dùng, nhấn vào tên của người dùng hoặc nhóm

4. Trong khi vẫn đang ở trong trang thuộc tính của thư mục hoặc file, thực hiện một trong các bước sau đây:

- Để cho phép hoặc không cho phép một quyền nào đó, trong hộp ***Permissions For Object***, lựa chọn hộp chọn ***Allow*** hoặc ***Deny***.

- Để loại bỏ nhóm hoặc người dùng từ hộp ***Group Or User Names***, nhấn vào ***Remove***.

Bảo mật các vùng DNS tích hợp Active Directory

Bảo mật vùng DNS tích hợp Active Directory sẽ yêu cầu các tùy chọn bảo mật bổ sung của việc cập nhật động bảo mật và điều khiển truy cập.

Theo mặc định, các thiết lập cập nhật động bảo mật là ***Secure Only***. Thiết lập mặc định này là thiết lập bảo mật nhất bởi vì nó ngăn cản các kẻ tấn công có thể cập nhật các vùng DNS, nhưng thiết lập này cũng có thể không cho bạn có được sự tiện lợi khi quản trị mà việc cập nhật động cung cấp. Cập nhật động bảo mật sẽ hạn chế các vùng DNS được cập nhật chỉ bởi các máy tính đã xác thực và gia nhập vào miền Active Directory mà máy chủ DNS này là thành viên và thỏa mãn các thiết lập bảo mật xác định có trong DACL của vùng DNS đó.

- **Chỉ cho phép các cập nhật động bảo mật**

Để chỉ cho phép các cập nhật động bảo mật, thực hiện theo các bước sau:

1. Mở bảng điều khiển ***DNS***
2. Trong bảng điều khiển, nhấn phải chuột vào vùng cần cấu hình và sau đó chọn ***Properties***

3. Trong thẻ ***General***, xác nhận rằng kiểu của vùng được thiết lập là ***Active Directory–Integrated.***

4. Trong mục ***Dynamic Updates***, lựa chọn ***Secure Only***

Danh sách DACL sử dụng bởi dịch vụ DNS Server khi nó chạy trên máy chủ quản trị miền cho phép bạn quản lý quyền truy cập của các người dùng và nhóm trong Active Directory khi họ muốn điều khiển vùng DNS này.

- **Đặt các thiết lập bảo mật DNS cho vùng DNS**

Để cấu hình các thiết lập bảo mật cho vùng DNS, thực hiện theo các bước sau:

1. Mở bảng điều khiển ***DNS***

2. Trong bảng điều khiển, nhấn phải chuột vào vùng cần cấu hình và sau đó chọn ***Properties***

3. Trong thẻ ***General***, xác nhận rằng kiểu của vùng được thiết lập là ***Active Directory–Integrated***.

4. Trong thẻ ***Security***, chỉnh sửa danh sách các người dùng hoặc nhóm thành viên mà được phép cập nhật bảo mật vùng này và ***reset*** các quyền của họ nếu cần

Bảo mật quá trình chuyển giao vùng

Theo mặc định, dịch vụ DNS Server trong Windows Server 2003 cho phép các thông tin của vùng được chuyển giao chỉ đến các máy chủ được liệt kê trong các bản ghi tài nguyên NS của một vùng. Đây là cấu hình bảo mật, nhưng để tăng cường tính bảo mật, thiết lập này nên được thay đổi sang tùy chọn cho phép chỉ chuyển giao vùng đến các địa chỉ IP xác định.

- **Chỉnh sửa các thiết lập chuyển giao vùng.**

Để chỉnh sửa các thiết lập chuyển giao vùng, thực hiện theo các bước sau:

1. Mở bảng điều khiển ***DNS***

2. Trong bảng điều khiển, nhấn phải chuột vào vùng cần cấu hình và sau đó chọn ***Properties***

3. Trong thẻ ***Zone transfer***, thực hiện một trong các tác vụ sau:

- Để vô hiệu hóa việc chuyển giao vùng, xóa hộp chọn ***Allow Zone Transfers***

- Để cho phép chuyển giao vùng, lựa chọn hộp chọn ***Allow Zone Transfers***

4. Nếu bạn cho phép chuyển giao vùng, thực hiện một trong các bước sau:

■ Để cho phép chuyển giao vùng đến bất kỳ máy chủ nào, nhấn vào "***To Any Server***".

■ Để cho phép chỉ chuyển giao vùng đến các máy chủ DNS liệt kê trong thẻ ***Name Servers***, nhấn vào "***Only To Servers Listed On The Name Servers***" (Chỉ cho phép đến các máy chủ liệt kê trong danh sách các máy chủ tên).

■ Để cho phép chỉ chuyển giao vùng đến các máy chủ DNS xác định, nhấn vào "***Only To The Following Servers***" (Chỉ cho phép đến các máy chủ sau đây), sau đó thêm vào một hoặc nhiều địa chỉ IP của các máy chủ DNS này.

LƯU Ý. Các thiết lập chuyển giao vùng không bảo mật*. Thay đổi các thiết lập vùng để cho phép chuyển giao vùng "**To Any Server**" sẽ dẫn đến việc có thể các dữ liệu DNS của bạn có nguy cơ bị tấn công và kẻ tấn công có thể tìm dấu vết (**footprint**) hệ thống mạng của bạn.*

Bảo mật các bản ghi tài nguyên DNS

Việc điều khiển truy cập các bản ghi tài nguyên lưu trong Active Directory sẽ được quản lý bởi các DACL. DACL được áp dụng trên các bản ghi tài nguyên sẽ cho phép bạn quản trị các quyền của các người dùng hoặc nhóm Active Directory, có thể là quyền điều khiển các bản ghi tài nguyên DNS.

- **Cấu hình các thiết lập bảo mật DNS cho các bản ghi tài nguyên DNS**

Để cấu hình thiết lập bảo mật DNS cho các bản ghi tài nguyên DNS, thực hiện theo các bước sau:

1. Mở bảng điều khiển DNS

2. Trong bảng điều khiển, nhấn phải chuột vào vùng cần cấu hình tương ứng

3. Trong khung chi tiết, nhấn phải chuột vào bản ghi mà bạn muốn cấu hình các thuộc tính bảo mật của nó, và sau đó nhấn Properties

4. Trong thẻ Security, chỉnh sửa danh sách của các nhóm hoặc người dùng thành viên mà được phép cập nhật bảo mật vùng này và reset lại các quyền của họ nếu cần

Bảo mật dịch vụ DNS Server

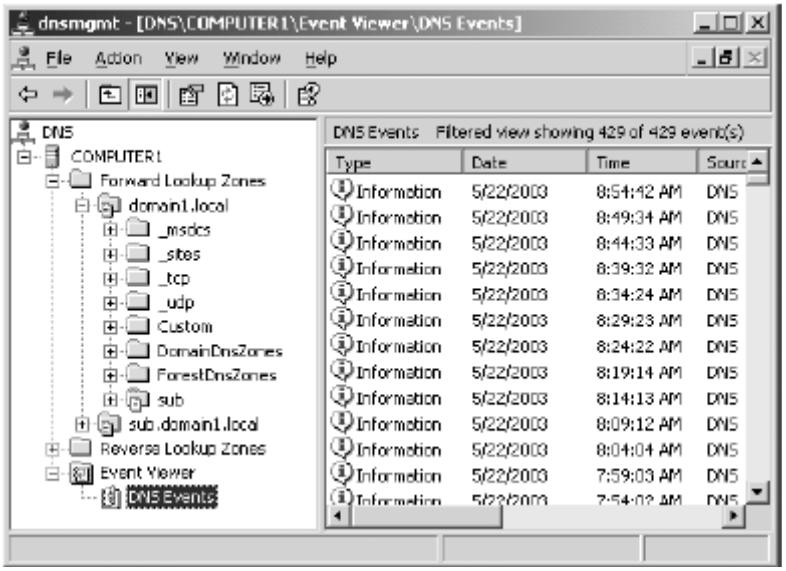
Nếu có thể, bạn nên chỉ định một địa chỉ IP tĩnh cho các máy chủ DNS ưa thích và thay thế để các máy khách DNS có thể sử dụng. Nếu một máy khách DNS được cấu hình để có được địa chỉ các máy chủ DNS một cách tự động, nó sẽ lấy các thông tin này từ máy chủ DHCP. Mặc dù phương pháp lấy địa chỉ các máy chủ DNS này là khá bảo mật, tuy nhiên nó chỉ bảo mật khi máy chủ DHCP được bảo mật. Bằng cách cấu hình các máy khách DNS với các địa chỉ IP tĩnh trong các mục máy chủ DNS ưa thích và thay thế, bạn đã giảm thiểu nguy cơ bị tấn công.

GIÁM SÁT VÀ GIẢI QUYẾT SỰ CỐ DNS

Trong phần này, hai công cụ ghi nhật ký và ***Replication Monitor*** sẽ được giới thiệu. Các công cụ này có thể sử dụng để cả giám sát và giải quyết sự cố DNS

Xem các nhật ký sự kiện DNS

Windows Server 2003 duy trì một nhật ký riêng cho các sự kiện máy chủ DNS mà có thể xem được trong ***Event Viewer*** và từ bảng điều khiển DNS, như thể hiện trong Hình 4-8

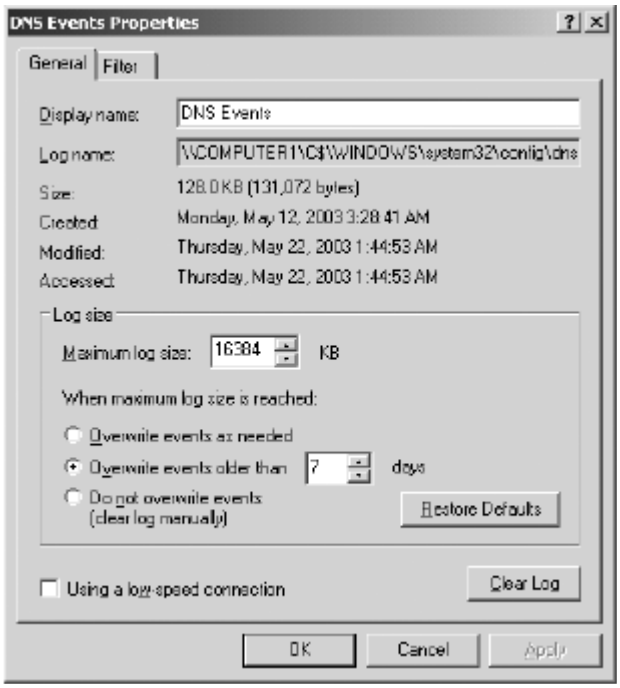


Hình 4-8. Xem DNS Event Log

Nếu bạn có trục trặc với DNS, xem ***DNS Server Events Log*** để phán đoán các sự kiện. Giao diện đồ họa người dùng (GUI) trong Windows Server 2003 đã được nâng cấp (xem Hình 4-9) để bạn có thể dễ dàng hơn trong việc cấu hình các mức ghi nhật ký.

Hình 4-9. Cấu hình các mức ghi nhật ký sự kiện DNS

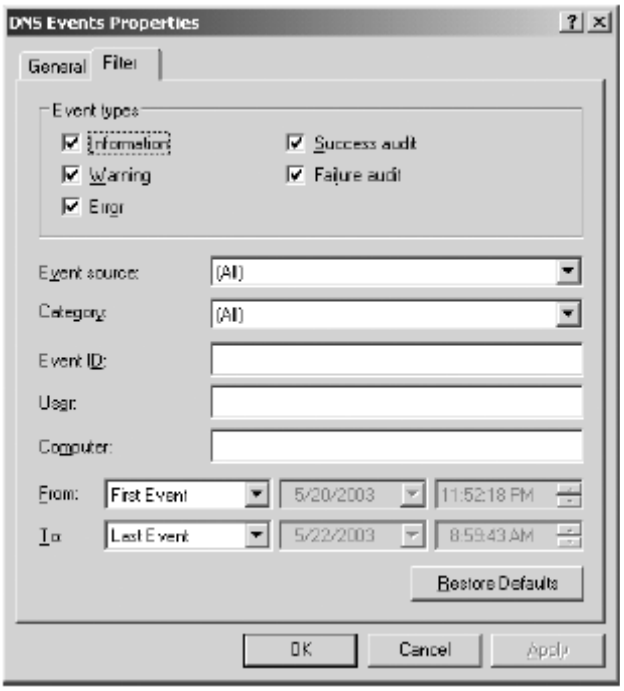
Để mở hộp thoại ***DNS Events Properties***, nhấn phải chuột vào mục DNS Events Log trong bảng điều khiển DNS và sau đó nhấn Properties. Hộp thoại ***DNS Events Properties*** có chứa thẻ ***General*** và thẻ ***Filter***. Trong thẻ ***General***, như thể hiện trong Hình 4-10, cho phép bạn cấu hình các tên hiển thị trong nhật ký, kích thước tối đa của file nhật ký và các hành động khi kích thước file nhật ký đạt đến giá trị tối đa của nó.



Hình 4-10. Thẻ General của hộp thoại DNS Events Properties

Theo mặc định, ***DNS Events Log*** sẽ hiển thị tất cả các sự kiện DNS. Trong thẻ ***Filter***, như thể hiện trong Hình 4-11, bạn có thể được phép hạn chế hiển

thị các sự kiện trong ***DNS Events Log*** theo kiểu sự kiện, nguồn gốc sự kiện, ID của sự kiện, ngày và các tham số khác.



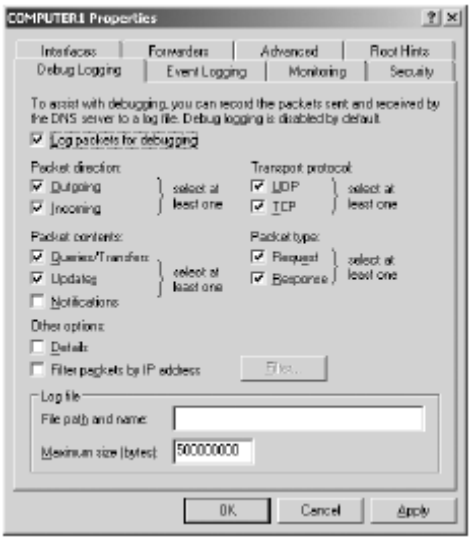
Hình 4-11. Lọc các nhật ký sự kiện DNS

Giải quyết sự cố DNS với DNS Debug Log

Bên cạnh ***DNS Events Log***, dịch vụ ***DNS Server*** còn duy trì một nhật ký riêng sử dụng để gỡ rối gọi là ***DNS Debug Log***. Nhật ký ***DNS Debug Log*** này là một file có tên ***Dns.log***, file này được lưu trong thư mục ***WINDOWS\System32\Dns***. Hơn nữa, bởi vì định dạng tự nhiên của file ***Dns.log*** là ***Rich Text Format*** (RTF), bạn nên sử dụng ***Microsoft WordPad*** để xem nội dung của nó một cách chính xác. Để xem file ***Dns.log*** trong ***Wordpad***, hãy tạo một bản sao của file này và sau đó mở xem bản sao này.

Theo mặc định, ***DNS debug log*** chỉ chứa các lỗi DNS. Tuy nhiên, bạn cũng có thể sử dụng nó để thu thập các gói tin DNS gửi hoặc nhận bởi máy chủ DNS nội bộ. Để kích hoạt tính năng ghi nhật ký các gói tin DNS, mở hộp thoại ***DNS Server Properties*** và sau đó nhấn vào thẻ ***Debug Logging.*** Theo mặc định, hộp chọn "***Log Packets For Debugging***" (Ghi nhật ký các gói tin để gỡ rối) là không được chọn và phần còn lại của các tùy chọn này là không thể chỉnh sửa.

Tuy nhiên, sau khi bạn lựa chọn hộp chọn ***Log Packets For Debugging***, như thể hiện trong Hình 4-12, bạn có thể cấu hình gói tin DNS nào mà bạn muốn thu thập và giữ lại trong nhật ký DNS.



Hình 4-12. Kích hoạt nhật ký gỡ rối

Trong ***Thẻ Debug Logging***, bạn có thể cấu hình các tùy chọn và các giá trị của chúng như mô tả trong Bảng 4-7.

Bảng 4-7. Các tùy chọn, giá trị và mô tả của nhật ký gỡ rối

Các tùy chọn	Các giá trị	Mô tả
Packet Direction	***Outgoing***	Các gói tin mà máy chủ DNS gửi đi được ghi lại trong file nhật ký của máy chủ DNS
	Incoming	Các gói tin mà máy chủ DNS gửi đi được ghi lại trong file nhật ký
Packet Contents	***Queries/Transfers***	Chỉ định rằng các gói tin chứa các truy vấn chuẩn được ghi lại trong nhật ký của máy chủ DNS
	Updates	Chỉ định rằng các gói tin chứa các cập nhật động được ghi lại trong nhật ký của máy chủ DNS
	Notifications	Chỉ định rằng các gói tin chứa các thông báo được ghi lại trong nhật ký máy chủ DNS
Transport Protocol	***UDP***	Chỉ định rằng các gói tin gửi và nhận bằng UDP sẽ được ghi lại trong nhật ký của máy chủ DNS

	TCP	Chỉ định rằng các gói tin gửi và nhận bằng TCP sẽ được ghi lại trong nhật ký của máy chủ DNS
Packet Type	***Request***	Chỉ định rằng các gói tin yêu cầu sẽ được ghi vào nhật ký của máy chủ DNS
	Response	Chỉ định rằng các gói tin phản hồi sẽ được ghi vào nhật ký của máy chủ DNS
Other Options	***Details***	Ghi lại rất cả các chi tiết của gói tin. Nếu không được lựa chọn, chỉ các thông tin tổng kết được ghi lại
	Filter Packets By IP Address	Cung cấp các bộ lọc bổ sung của các gói tin đã được ghi lại trong nhật ký máy chủ DNS. Tùy chọn này cho phép ghi lại các gói tin được gửi đi từ các địa chỉ IP cụ thể xác định đến máy chủ DNS hoặc từ một máy chủ DNS đến các địa chỉ cụ thể.
Log File	***File Name***	Chỉ định tên và nơi lưu của file nhật ký của máy chủ DNS
	Log File Maximum Size Limit	Thiết lập kích thước tối đa của file nhật ký trong máy chủ DNS

Các thông tin sau đây được lấy từ file ***Dns.log*** và đó là một ví dụ về các phản hồi cho truy vấn. Lưu ý rằng cờ phản hồi được thiết lập là 1 (***True***) và bản ghi tài nguyên PTR nằm trong phần ***Answer***:

17:19:33 8C8 PACKET UDP Snd 10.1.1.200 0001 R Q [8085 A DR NOERROR]
(3)200(1)1(1)1(2)10(7)in-addr(4)arpa(0)
UDP response info at 007AFE40
Socket = 372
Remote addr 10.1.1.200, port 4604
Time Query=157594, Queued=0, Expire=0
Buf length = 0x0200 (512)
Msg length = 0x004d (77)
Message:
XID 0x0001
Flags 0x8580

QR 1 (RESPONSE)
OPCODE 0 (QUERY)
AA 1
TC 0
RD 1
RA 1
Z 0
RCODE 0 (NOERROR)
QCOUNT 1
ACOUNT 1
NSCOUNT 0
ARCOUNT 0
QUESTION SECTION:
Offset = 0x000c, RR count = 0
Name "(3)200(1)1(1)1(2)10(7)in-addr(4)arpa(0)"
QTYPE PTR (12)
QCLASS 1
ANSWER SECTION:
Offset = 0x0029, RR count = 0
Name "[C00C](3)200(1)1(1)1(2)10(7)in-addr(4)arpa(0)"
TYPE PTR (12)
CLASS 1
TTL 1200
DLEN 24
DATA (8)acapulco(9)contoso01(3)com(0)
AUTHORITY SECTION:
empty
ADDITIONAL SECTION:
Empty

CẢNH BÁO. Kích hoạt DNS Debugging có thể ảnh hưởng đến hiệu năng. *Không nên để tính năng DNS debug logging được kích hoạt trong quá trình hoạt động bình thường bởi vì nó sử dụng các tài nguyên bộ vi xử lý và đĩa cứng. Kích hoạt nó chỉ khi bạn muốn chẩn đoán và giải quyết sự cố DNS.*

Giải quyết sự cố DNS bằng Replication Monitor

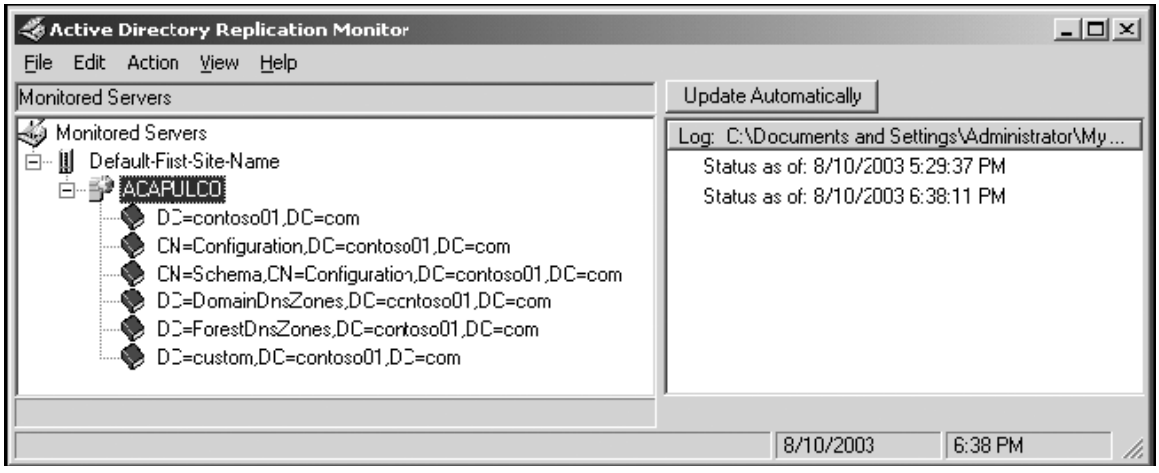
Replication Monitor (replmon.exe) là một công cụ đồ họa có trong ***Windows Support Tools*** cho phép bạn giám sát và giải quyết sự cố đồng bộ

Active Directory. Tính năng này là tính năng thiết yếu trong giám sát việc chuyển giao dữ liệu DNS trong các vùng tích hợp DNS

Bạn có thể sử dụng ***Replication Monitor*** để thực hiện các chức năng sau đây:

- Ép buộc đồng bộ dữ liệu DNS thông qua rất nhiều cách thức đồng bộ
- Phát hiện khi một đối tượng đồng bộ có vấn đề
- Hiển thị kiến trúc đồng bộ
- Thăm dò đối tượng đồng bộ và tạo ra các mục lịch sử riêng biệt của các sự kiện đồng bộ thành công hay thất bại.
- Hiển thị các thay đổi mà chưa được đồng bộ từ một đối tượng đồng bộ cụ thể nào đó.
- Giám sát trạng thái đồng bộ của các máy chủ quản trị miền từ nhiều rừng khác nhau

Sau khi bạn cài đặt ***Windows Support Tools***, chạy ứng dụng ***Replication Monitor*** bằng cách nhập vào ***replmon*** tại dấu nhắc dòng lệnh (hoặc trong hộp thoại Run) và sau đó nhấn ***Enter***. Sau khi mở ứng dụng ***Replication Monitor***, bạn phải thêm vào ít nhất một máy chủ để giám sát. Để thêm máy chủ để giám sát, nhấn vào ***Monitored Servers*** sau đó trong thực đơn ***Actions***, trỏ vào site, nhấn vào ***Add Monitored Server*** và sau đó thực hiện theo hướng dẫn của trình trợ giúp. Sau khi thêm vào máy chủ DNS, ***Replication Monitor*** trông sẽ như thể hiện trong Hình 4-13:



Hình 4-13. Bảng điều khiển Replication Monitor

Sau khi bạn đã thêm vào các máy chủ mà bạn muốn giám sát, bạn có thể lưu cấu hình bảng điều khiển này như một file ***.ini*** và có thể mở file này từ ***Replication Monitor*** để sử dụng sau đó.

Các vùng tích hợp Active Directory và phân vùng thư mục

Đối với mỗi máy chủ liệt kê trong bảng điều khiển, bạn có thể hiển thị các phân vùng thư mục Active Directory cài đặt trên máy chủ đó bằng cách mở rộng biểu tượng máy chủ tương ứng. Các máy chủ quản trị miền mà đồng thời là máy chủ DNS và chứa một vùng tích hợp Active Directory đơn sẽ bao gồm một bản sao của năm phân vùng theo mặc định.

Danh sách sau đây mô tả năm phân vùng này của một miền sử dụng Active Directory và vùng DNS tên là ***contoso.com***.

- **DC=contoso01,DC=com**. Phân vùng miền, nó chứa các đối tượng (ví dụ như các máy tính và người dùng) gắn với miền nội bộ. Mỗi máy chủ quản trị miền sẽ lưu một bản sao đầy đủ của phân vùng miền cho miền nội bộ của nó. Ngoài ra, trong phân vùng này, các dữ liệu DNS được lưu để tương thích với các máy chủ DNS của Microsoft Windows 2000. Để lưu các dữ liệu vùng DNS trong phân vùng miền, thiết lập phạm vi đồng bộ vùng trong bảng điều khiển DNS thành "***All Domain Controllers In The Domain domain_name***" (Tất cả các máy chủ quản trị miền trong miền ***domain_name*** *– trong đó* ***Domain_name*** *là tên miền của bạn*)

- **CN=Configuration,DC=contoso01,DC=com**. Phân vùng cấu hình, phân vùng này chứa cấu trúc đồng bộ và các thông tin cấu hình khác mà phải được đồng bộ trên toàn rừng. Mỗi máy chủ quản trị miền trong rừng có một bản sao của cùng một phân vùng cấu hình. Tuy nhiên, phân vùng này không thể chứa các dữ liệu vùng của DNS được.

- **CN=Schema,CD=Configuration,DC=contoso01,DC=com**. Phân vùng lược đồ, phân vùng này chứa các đối tượng ***classSchema*** và ***attributeSchema*** mà định nghĩa các kiểu đối tượng có thể tồn tại trong rừng Active Directory. Mọi máy chủ quản trị miền trong rừng có một bản sao của cùng một phân cùng lược đồ. Tuy nhiên, phân vùng này không thể chứa các dữ liệu vùng của DNS được.

- **DC=DomainDnsZones,DC=contoso01,DC=com**. Phân vùng thư mục xây dựng sẵn có tên là ***DomainDnsZones***, phân vùng này được đồng bộ với tất cả các máy chủ quản trị miền Windows Server 2003

mà đồng thời là máy chủ DNS trong một miền Active Directory thông thường. Để lưu dữ liệu vùng DNS trong phân vùng ***DomainDnsZones***, thiết lập phạm vi đồng bộ vùng trong bảng điều khiển DNS thành "***All DNS Servers In The Active Directory Domain Domain_Name***" (Tất cả các máy chủ DNS trong miền Active Directory domain_name)

- **DC=ForestDnsZones,DC=contoso01,DC=com**. Phân vùng thư mục xây dựng sẵn tên là ForestDnsZones, phân vùng này được đồng bộ với tất cả các máy chủ quản trị miền Windows Server 2003 mà đồng thời là máy chủ DNS trong một rừng Active Directory thông thường. Để lưu dữ liệu vùng DNS trong phân vùng ***DomainDnsZones***, thiết lập phạm vi đồng bộ vùng trong bảng điều khiển DNS thành "***All DNS Servers In The Active Directory Forest***" (Tất cả các máy chủ DNS trong rừng Active Directory)

Bạn còn có thể tạo ra các phân vùng thư mục ứng dụng tùy chọn và liệt kê các máy chủ quản trị miền mà bạn lựa chọn để lưu một bản sao của phân vùng đó. Trong Hình 4-13, ***Replication Monitor*** hiển thị một phân vùng thư mục ứng dụng tên là ***Custom***. Để lưu các dữ liệu vùng của DNS trong một phân vùng thư mục ứng dụng, thiết lập phạm vi đồng bộ của vùng trong bảng điều khiển DNS thành "***All Domain Controllers Specified In The Scope Of The Following Application Directory Partition***" (Tất cả các máy chủ quản trị miền chỉ định trong phạm vi của phân vùng thư mục ứng dụng sau đây). Sau đó lựa chọn phân vùng thư mục ứng dụng mà bạn muốn từ trong danh sách xổ xuống.

Để tìm ra phân vùng Active Directory nào được sử dụng để lưu dữ liệu của một vùng DNS cụ thể, bạn có thể hoặc kiểm tra trang thuộc tính của vùng DNS đó trong bảng điều khiển DNS hoặc sử dụng lệnh ***Dnscmd /zoneinfo ZoneName***, trong đó nhập vào tên của vùng vào vị trí của ***ZoneName***.

Để xác định phạm vi đồng bộ vùng của một miền tên là ***domain1.local***, nhập vào lệnh sau đây tại dấu nhắc dòng lệnh: **dnscmd /zoneinfo domain1.local.** Sau đó, hãy nhìn vào mục có tên là ***Directory Partition*** trong kết quả hiển thị ra. Để thay đổi phạm vi đồng bộ vùng, sử dụng khóa chuyển ***/zonechangedirectorypartition*** theo sau bởi bất kỳ một khóa chuyển tương ứng sau đây:

- ***/domain*** (cho tất cả mọi máy chủ DNS trong miền)
- ***/forest*** (cho tất cả mọi máy chủ DNS trong rừng)

- ***/legacy*** (cho mọi máy chủ quản trị miền trong miền)

Ví dụ, để thiết lập phạm vi đồng bộ của một vùng tên là ***domain1.local*** là tới tất cả các máy chủ DNS trong toàn miền, nhập vào dòng lệnh sau đây:

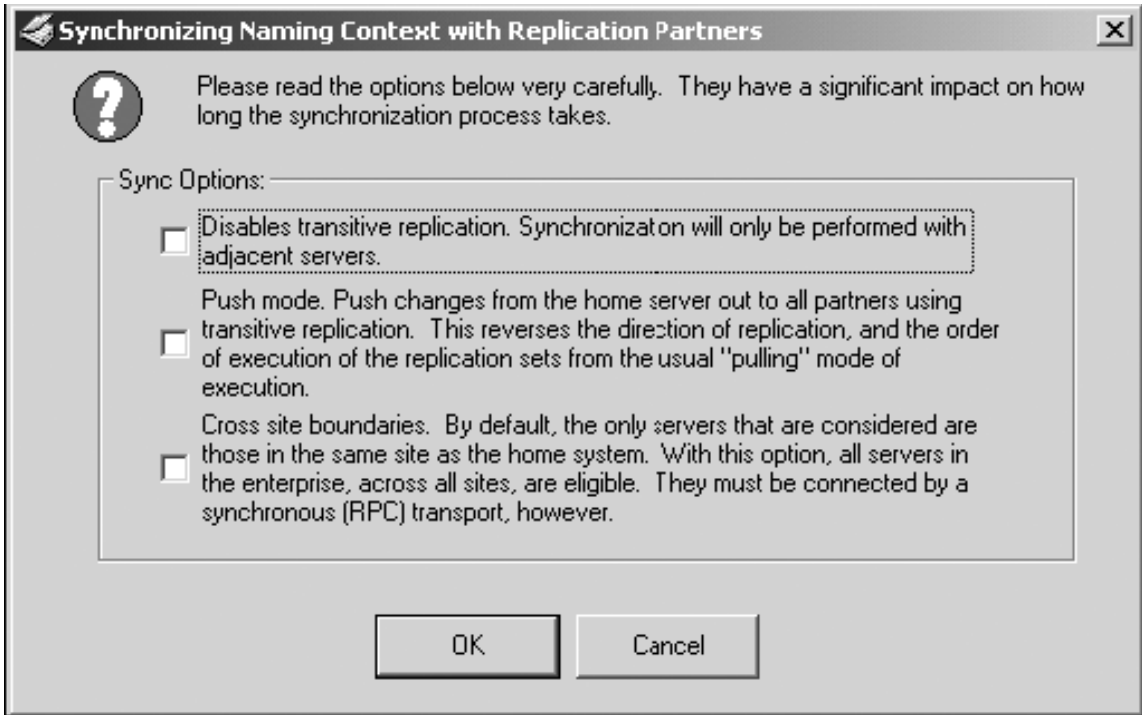
dnscmd /zonechangedirectorypartition domain1.local /domain

Nếu bạn đã có các thông tin ID và mật khẩu đúng, bạn thậm chí còn có thể sử dụng các dòng lệnh này từ xa. Trong trường hợp này, chỉ cần chỉ định tên máy chủ sau ***dnscmd***.

Ép buộc đồng bộ các vùng tích hợp Active Directory

Một khi bạn đã biết phân vùng thư mục trong đó các thông tin của vùng DNS được lưu ở đâu, bạn có thể ép buộc đồng bộ các vùng đó trong ***Replication Monitor***. Thủ tục này có thể hỗ trợ trong việc giải quyết sự cố của quá trình phân giải tên gây ra bởi việc các dữ liệu vùng là quá cũ.

Để ép buộc đồng bộ vùng tích hợp Active Directory, nhấn phải chuột vào phân vùng tương ứng trong bảng điều khiển Replication Monitor và lựa chọn "***This Directory Partition With All Servers***" (Phân vùng thư mục này với tất cả máy chủ). Hộp thoại "***Synchronizing Naming Context With Replication Partners***" (Đồng bộ ngữ cảnh tên với đối tác đồng bộ) xuất hiện như thể hiện trong Hình 4-14:

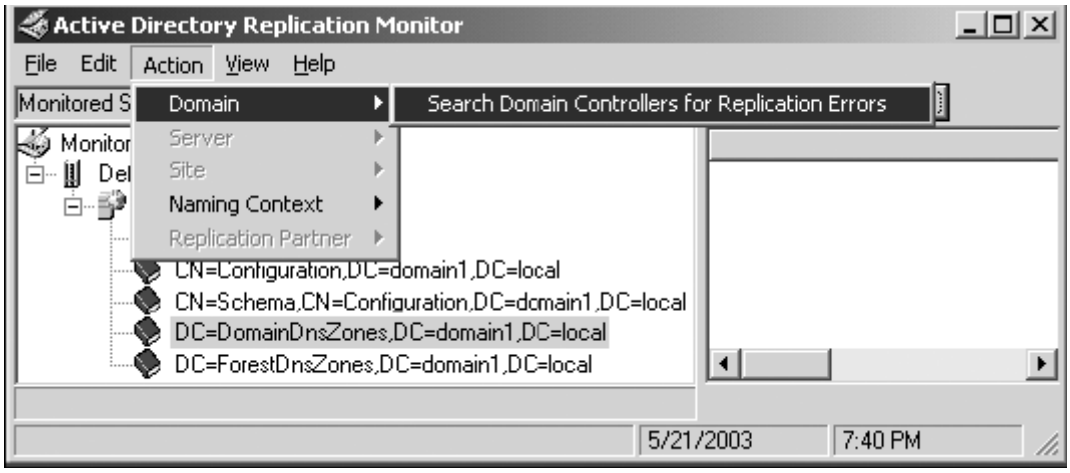


Hình 4-14. Ép buộc đồng bộ

Khi bạn thực hiện ép buộc đồng bộ, bạn có thể sử dụng hộp thoại này để chỉ đồng bộ tới các máy chủ bên cạnh, đồng bộ tới tất cả các máy chủ trong site nội bộ hoặc đồng bộ tới tất cả các máy chủ trên các site.

Tìm kiếm các lỗi đồng bộ

Các lỗi DNS trong các vùng tích hợp Active Directory có thể gây ra bởi các lỗi của việc đồng bộ vùng. Để làm điều này, trên thực đơn ***Action***, lựa chọn Domain, và sau đó lựa chọn "***Search Domain Controllers For Replication Errors***" (Tìm kiếm các máy chủ quản trị miền để biết các lỗi đồng bộ) như thể hiện trong Hình 4-15.



Hình 4-15. Tìm kiếm các lỗi đồng bộ

Một phương pháp thay thế khác, bạn có thể cấu hình ***Replication Monitor*** gửi thư điện tử đến một quản trị mạng sau một số lần đồng bộ lỗi cụ thể nào đó. Để thực hiện tác vụ này, trong thực đơn ***View***, lựa chọn ***Options***. Trong hộp thoại "***Active Directory Replication Monitor Options***" (Các tùy chọn giám sát đồng bộ Active Directory), lựa chọn "***Notify When Replication Fails After This Number Of Attempts***" (Thông báo khi số lần đồng bộ thất bại vượt quá:) và sau đó nhập vào số lần thất bại mà bạn muốn để kích hoạt một lần gửi thư điện tử. Cuối cùng, lựa chọn hộp chọn ***Send Email To*** và chỉ ra một địa chỉ email trong hộp văn bản tương ứng.

TỔNG KẾT

- Sử dụng các công cụ như ***Nslookup***, ***DNSLint*** và ***Dnscms*** để quản trị các máy chủ DNS

- Sử dụng ***Nslookup*** trong chế độ dòng lệnh hoặc chế độ tương tác để kiểm tra nội dung của các file của vùng DNS. Sử dụng ***DNSLint*** để xác nhận sự thống nhất, kiên định của một tập hợp xác định các bản ghi tài nguyên trên nhiều máy chủ DNS. Sử dụng ***Dnscmd*** để trợ giúp việc tự động quá trình quản trị và cập nhật các cấu hình của máy chủ DNS có sẵn.

- Tích hợp DNS và WINS là một quá trình trong đó DNS sử dụng WINS để phân giải các tên sang địa chỉ IP. DNS sử dụng để phân giải các tên máy và các dịch vụ sang các địa chỉ IP và WINS được sử dụng để phân giải các tên NETBIOS sang các địa chỉ IP.

- Sử dụng các thiết lập nâng cao trong máy chủ DNS để vô hiệu hóa sự đệ quy, tăng cường sự tương tác giữa các máy chủ, tăng cường tính toàn vẹn của dữ liệu và sắp xếp lại danh sách các tên liệt kê trong phản hồi bằng cách sử dụng ***round robin (****luân phiên)* và ***netmask ordering*** (*thứ tự mặt nạ mạng*). Bạn còn có thể sử dụng các thiết lập nâng cao để bảo mật bộ đệm khỏi bị làm sai hỏng, cấu hình kiểm tra các tên, chỉ định nơi mà dữ liệu vùng sẽ được nạp và kích hoạt tính năng tự động loại bỏ các bản ghi đã lỗi thời.

- Dịch vụ ***DNS Client*** duy trì một bộ đệm nội bộ, bạn có thể xem và xóa bằng lệng ***ipconfig.exe***

- Hiểu thêm rất nhiều các nguy cơ bảo mật trong DNS và chuẩn bị để đối phó bằng cách ấn định mức bảo mật cho doanh nghiệp của bạn. Dựa trên các thiết lập của bạn, tiến hành các thay đổi cấu hình tương ứng để hạn chế các cập nhật động, chuyển giao vùng, truy cập đến các vùng được gói trong file, các bản ghi tài nguyên và dịch vụ DNS Client.

- Bạn có thể sử dụng cả ***DNS Events Log*** và ***DNS debug log*** để giám sát và giải quyết sự cố DNS. Ví dụ, bạn có thể sử dụng nhật ký gỡ rối DNS để ghi lại tất cả các cập nhật động nhận được bởi máy chủ này.

BÀI TẬP

QUAN TRỌNG. Hoàn thành tất cả các bài tập. *Nếu bạn có kế hoạch làm bất kỳ bài tập nào trong sách lý thuyết của chương này, bạn phải thực hiện tất cả các bài tập khác trong chương để trả máy tính về trạng thái nguyên gốc của nó trước khi có thể làm các bài tập thực hnàh trong cuốn BÀI TẬP THỰC HÀNH.*

Bài tập 4-1. Hiển thị các thông tin vùng DNS bằng Dnscmd

1. Mở dấu nhắc dòng lệnh
2. Tại dấu nhắc dòng lệnh, nhập vào **dnscmd localhost /zoneinfo** *zone_name* (trong đó *zone_name* thể hiện một tên vùng phân giải xuôi hoặc ngược) và sau đó nhấn ***Enter***

Bài tập 4-2: Tích hợp DNS và WINS

1. Mở bảng điều khiển DNS
2. Trong bảng điều khiển, nhấn phải chuột vào vùng tương ứng và sau đó nhấn ***Properties***
3. Trong hộp thoại ***Properties***, nhấn vào Thẻ tương ứng:
   - Nhấn vào thẻ ***WINS*** nếu như vùng này là vùng phân giải xuôi
   - Nhấn vào thẻ ***WINS-R*** nếu như vùng này là vùng phân giải ngược
4. Trong thẻ ***WINS*** tương ứng, lựa chọn hộp chọn tương ứng để kích hoạt việc sử dụng phân giải tên bằng ***WINS***
   - Sử dụng WINS Forward Lookup nếu như vùng là vùng phân giải xuôi
   - Sử dụng WINS-R Lookup nếu như vùng là vùng phân giải ngược
5. Trong thẻ ***WINS***, nhập vào địa chỉ ***IP*** của một máy chủ ***WINS*** mà sẽ sử dụng để phân giải các tên không tìm thấy trong DNS. Đối với vùng phân giải ngược, trong thẻ ***WINS-R***, nhập vào tên trong trường ***Domain To Append To Returned Name***, nếu có thể.
6. Trong thẻ ***WINS***, nhấn vào ***Add*** để thêm vào địa chỉ ***IP*** của máy chủ. Đối với vùng phân giải ngược, trong Thẻ ***WINS-R***, nhấn vào ***Use WINS-R Lookup***
7. Nếu các địa chỉ của máy chủ ***WINS*** truyền thống được sử dụng cho vùng phân giải xuôi trong quá trình tham chiếu phân giải ***WINS***, lặp

lại các bước 5 và 6 nếu cần để thêm vào các địa chỉ máy chủ này trong danh sách.

8. Trong cả thẻ ***WINS*** và ***WINS-R***, lựa chọn ***Do Not Replicate This Record*** cho bản ghi WINS này nếu có thể.

   CẢNH BÁO. Không đồng bộ bản ghi WINS Locator. *Nếu bạn đang đồng bộ các dữ liệu vùng sang các vùng thứ cấp trên các máy chủ DNS của các hãng thứ ba mà các máy chủ này không nhận biết được các bản ghi WINS và WINS-R, lựa chọn hộp chọn "**Do Not Replicate This Record**" (Không đồng bộ bản ghi này). Điều này sẽ không cho các bản ghi **WINS localor** đồng bộ tới các máy chủ khác trong quá trình chuyển giao vùng. Bạn nên lựa chọn tùy chọn này khi thực hiện việc chuyển giao vùng đến các máy chủ **BIND**, bởi vì **BIND** không nhận biết được các bản ghi **WINS Locator***.

9. Tùy bạn chọn, trong thẻ ***WINS*** và ***WINS-R,*** nhấn vào ***Advanced*** để điều chỉnh cả giá trị ***Cache Time-Out*** và ***Lookup Time-Out.***

10. Tùy bạn chọn, trong thẻ ***WINS-R***, trong hộp thoại ***Advanced***, lựa chọn ***Submit DNS Domain As NetBIOS Scope***.

11. Trong hộp thoại ***Zone Properties***, nhấn OK

Bài tập 4-: Hiển thị và xóa bộ đệm phân giải.

1. Mở dấu nhắc dòng lệnh
2. Tại dấu nhắc dòng lệnh, nhập vào **ipconfig /displaydns** và nhấn ***Enter***
3. Tại dấu nhắc dòng lệnh, nhập vào **ping instructor01** và nhấn ***Enter***
4. Tại dấu nhắc dòng lệnh, nhập vào **ipconfig /displaydns** và nhấn ***Enter***
5. Cuộn xuống để tìm kiếm bản ghi London trong kết quả hiển thị.
6. Tại dấu nhắc dòng lệnh, nhập vào **ipconfig /flushdns** và nhấn ***Enter***

   Một thông báo hiện ra nói rằng bộ đệm phân giải DNS đã được xóa thành công.

7. Tại dấu nhắc dòng lệnh, nhập vào **ipconfig /displaydns** và nhấn ***Enter***

   Lưu ý rằng bản ghi London không còn tồn tại trong bộ đệm phân giải DNS

CÁC CÂU HỎI TỔNG KẾT

1. Chức năng của ***round robin*** trong DNS là gì ?
2. Tính năng nào sẽ có độ ưu tiên cao hơn – ***round robin*** hay ***netmask ordering***?
3. Đâu là lý do hợp lý để giám sát các thiết lập TTL trên các máy chủ DNS ? Chọn tất cả các câu trả lời có thể.
    a. Các lưu lượng truy vấn tăng khi các máy khách DNS yêu cầu các thông tin mà hết hạn từ bộ đệm của chúng
    b. Các máy khách DNS có thể lưu đệm các bản ghi lỗi thời
    c. Các máy khách DNS có thể không có khả năng phân giải các tên máy
    d. Các lưu lượng truy vấn giảm khi các máy khách DNS yêu cầu các thông tin mà hết hạn từ bộ đệm của chúng
4. Kiểu truy vấn kiểm tra nào có thể thực hiện trong thẻ Monitoring của trang thuộc tính máy chủ DNS?
    a. Truy vấn đệ quy
    b. Truy vấn đơn giản
    c. Truy vấn dài
    d. Truy vấn lặp
5. Phương thức nào sau đây cung cấp cảnh báo sớm nhất nếu như dịch vụ DNS bị sự cố ?
    a. Tạo ra một cảnh báo dựa trên các biến số đo hiệu năng chuẩn, và thiết lập giá trị mức ngưỡng để thông báo cho bạn nếu như biến số đo vượt quá 95% của mức ngưỡng đề xuất.
    b. Tạo ra một cảnh báo dựa trên các biến số đo mà bạn cho là đối tượng chỉ thị thích hợp của sự cố, và thiết lập một mức ngưỡng để thông báo bạn khi nó có giá trị 10% dưới mức ranh giới.
    c. Tạo ra một cảnh báo dựa trên các biến số đo chuẩn, và thiết lập các mức ngưỡng để thông báo cho bạn nếu giá trị của các biến số đo vượt quá 75% của giá trị mức ngưỡng khuyến cáo.
    d. Tạo ra một cảnh báo dựa trên các biến số đo mà bạn cho là đối tượng chỉ thị thích hợp của sự cố, và thiết lập một mức ngưỡng để thông báo bạn khi nó có giá trị 10% trên mức ranh giới.

6. Bạn là quản trị hệ thống của Contoso, Ltd. Contoso đang có kế hoạch đối với các vùng DNS của nó và bạn được hỏi xin ý kiến khuyên cách thức tốt nhất để cấu hình các vùng trên các máy chủ Windows Server 2003 của công ty. Bạn đề xuất sử dụng các vùng tích hợp Active Directory. Tại sao bạn để xuất cấu hình này ? Chọn tất cả các câu trả lời có thể

    a. Các dữ liệu DNS được đồng bộ với Active Directory

    b. Bạn có thể cấu hình các cập nhật động bảo mật

    c. Mức tải DNS sẽ được chia sẻ bởi các máy chủ quản trị miền khác sẽ trở thành các máy chủ DNS thứ cấp

    d. Bạn có thể cấu hình một phạm vi động bộ

7. Bạn là quản trị hệ thống của contoso Ltd và bạn đã cập nhật các địa chỉ IP cho một máy bằng cách sử dụng bảng điều khiển DNS. Giả định rằng nó tồn tại, kiểu bản ghi nào sau đây sẽ được gắn với bản ghi máy và cũng phải được cập nhật ?

    a. Bản ghi tài nguyên A

    b. Bản ghi tài nguyên MX

    c. Bản ghi tài nguyên NS

    d. Bản ghi tài nguyên PTR

    e. Bản ghi tài nguyên SOA

    f. Bản ghi tài nguyên SRV

8. Một máy khách trong mạng nội bộ của contoso Ltd không thể kết nối được đến máy chủ file. Bạn xác nhận rằng máy chủ file đang chạy và có khả năng kết nối được đến nó bằng cách sử dụng một máy tính khác trong cùng một mạng con. Bạn giả định rằng máy khách mà không thể kết nối đến đó có chứa thông tin đã lỗi thời trong bộ đệm nội bộ của nó. Thao tác nào sau đây sẽ giải quyết vấn đề này ?

    a. Tại máy khách, chạy lệnh ***Ipconfig /flushdns***

    b. Tại máy chủ file, chạy lệnh ***Ipconfig /flushdns***

    c. Tại máy chủ file, chạy lệnh ***Nslookup***.

    d. Tại máy chủ file, ngừng và khởi động lại dịch vụ ***DNS Client***

CÁC KỊCH BẢN TÌNH HUỐNG

Kịch bản tình huống 4-1: Kích hoạt người dùng mạng kết nối đến các tên máy trên Internet

Bạn là quản trị hệ thống của Contoso Ltd. Hệ thống mạng Contoso có chứa một miền đơn, contoso.com, nó được bảo vệ khỏi Internet bằng một tường lửa. Tường lửa chạy trên một máy tính tên là ***NS1*** được kết nối trực tiếp đến Internet. ***NS1*** đồng thời chạy dịch vụ ***DNS Server*** và tường lửa cho phép lưu lượng DNS được chuyển qua giữa Internet và dịch vụ ***DNS Server*** trên ***NS1*** nhưng không cho phép giữa Internet và mạng nội bộ. dịch vụ DNS trên NS1 được cấu hình sử dụng round robin. Phía trong tường lửa, hai máy tính chạy Windows Server 2003-***NS2*** và ***NS3*** có chứa một vùng DNS chính thức và thứ cấp tương ứng của contoso.com

Người dùng trong mạng công ty báo cáo rằng, mặc dù họ sử dụng các tên máy để kết nối đến các máy tính trong hệ thống mạng nội bộ, họ không thể sử dụng tên máy để kết nối đến các đích đến trên Internet, ví dụ như www.microsoft.com

Hành động nào sau đây yêu cầu ít thao tác quản trị nhất để cho phép các người dùng mạng kết nối đến các tên máy trên Internet ?

a) Vô hiệu hóa đệ quy trên ***NS2*** và ***NS3***

b) Kích hoạt ***Netmask Orderring*** trên NS1

c) Cấu hình ***NS2*** và ***NS3*** sử dụng ***NS1*** như là ***forwarder*** của chúng

d) Vô hiệu hóa ***round robin*** trên ***NS1***

Kịch bản tính huống 4-2: Triển khai cập nhật DNS

Bạn là quản trị hệ thống của công ty Contoso. Ltd. Công ty đang phát triển rất nhanh trong những năm qua và hiện tại đang sử dụng chỉ một vùng DNS đơn. Gần đây, phòng Marketing đã tạo ra một số yêu cầu thay đổi DNS vì chúng luôn bị trễ. Người dùng muốn có khả năng cập nhật bản ghi DNS của bản thân họ.

Bạn phải làm gì để giải quyết vấn đề này ?

a) Tạo một máy chủ thứ cấp trong phòng Marketing để người dùng có thể quản lý vùng riêng của bản thân họ.

b) Ủy quyền miền marketing cho một máy chủ DNS trong phòng Marketing

c) Đặt một máy chủ quản trị miền chạy DNS vào phòng Marketing để người dùng trong phòng này có thể tạo các thay đổi

d) Nâng cấp cơ sở hạ tầng hệ thống mạng để cải thiện hiệu năng của mạng.

CHƯƠNG 5: BẢO MẬT TRONG MẠNG

Sau khi kết thúc chương này, bạn có thể:

- Mô tả về các giao thức bảo mật trong mạng được dùng cho việc cấp phép.
- Gán các quyền cho người sử dụng ***(user right***) và hiểu được sự khác nhau giữa quyền cho người sử dụng và cấp phép (***permission***).
- Liệt kê và mô tả các công cụ cấu hình bảo mật đi kèm với Windows Server 2003, và cách sử dụng các công cụ cấu hình bảo mật để cấu hình các thiết lập bảo mật. Phân tích về bảo mật hệ thống trong mạng máy tính sử dụng Microsoft Windows 2000.
- Mô tả và thực hiện nguyên lý cấp quyền tối thiểu.
- Thực hiện cấu hình bảo mật cơ sở (***baseline***) và cấu hình kiểm soát (***audit***) bảo mật bằng cách sử dụng các mẫu (***template***) bảo mật có sẵn.
- Sử dụng hệ thống File mã hóa (EFS) để mã hóa và giải mã file bằng giao diện đồ họa và các tiện ích dòng lệnh (***command line***).
- Cài đặt và sử dụng công cụ ***Microsoft Baseline Security Analyzer*** (MBSA) để tăng mức độ bảo mật cho máy tính.

Quản lý và duy trì bảo mật là một công việc khá phức tạp vì vậy Windows Server 2003 cung cấp một số công cụ giúp bạn thực hiện được dễ dàng hơn. Để có thể trở thành một chuyên gia về mạng bạn cần phải hiểu được Windows Server 2003 thực hiện bảo mật như thế nào để có thể bảo vệ được mạng của bạn. Nghĩa là bạn phải hiểu được một số khái niệm bảo mật cơ bản như cấp phép (***permission***), quyền (***right***) và nguyên lý cấp quyền tối thiểu. Ngoài ra để hiểu hơn về nguyên tắc bảo mật của Windows Server 2003 bạn cũng cần phải biết và các công cụ và cách thực hiện của chúng để bảo mật mạng của bạn một cách hiệu quả. Các công cụ được đưa ra trong chương này là snap-in ***Security Configuration And Analysis***, snap-in ***Security Templates***, ***MBSA*** và snap-in ***Group Policy***. Các cách thực hiện như gán các quyền cho người sử dụng (***user right***), tạo ra sự bảo mật cơ sở,

mã hóa và giải mã file, sử dụng các mẫu bảo mật để áp dụng các chính sách bảo mật.

THỰC HIỆN CÁC GIAO THỨC BẢO MẬT TRONG MẠNG

Các giao thức bảo mật trong mạng được sử dụng để quản lý và bảo mật các quá trình xác thực (***authentication***), ủy quyền (***authorization***), riêng tư (***confidentiality***), toàn vẹn (***integrity***) và chấp nhận (***nonrepudiation***). Trong mạng máy tính sử dụng Windows Server 2003 các giao thức thường được sử dụng là **NTLM, Internet Protocol Security (IPSec)** và một số giao thức phụ khác. Một số giao thức truyền thông trong mạng, các cấu hình bảo mật và bảo vệ phải sử dụng các giao thức ở trên. Bảng 5-1 liệt kê các kiểu bảo mật và các giao thức hỗ trợ cho chúng.

Bảng 5-1 Các kiểu bảo mật và giao thức

Kiểu bảo mật	Mục đích	Các giao thức
Xác thực (***Authentication***)	Để xác thực bạn chính là người mà bạn khai báo	Kerberos và NTLM (mặc định NTLM không sử dụng nhưng cho phép cấu hình)
Ủy quyền (***Authorization***)	Để xác định bạn có thể làm gì trong mạng sau khi bạn đã được xác thực	Kerberos và NTLM
Riêng tư (***Confidentiality***)	Để lưu trữ các dữ liệu bí mật	Thành phần mã hóa (**Encryption**) của Kerberos, NTLM và IPSec(bảo mật việc trao đổi khác với việc xác thực)
Toàn vẹn (***integrity***)	Bảo đảm dữ liệu nhận được giống như dữ liệu gửi đi	Thành phần của Kerberos, NTLM và IPSec
Chấp nhận (***nonrepudiation***)	Xác định chính xác người gửi và người nhận các thông điệp	Kerberos và IPSec

Chương này sẽ tập trung vào các quá trình ủy quyền và riêng tư. Chương 6, "Bảo mật lưu thông trong mạng bằng cách sử dụng IPSec" sẽ cho chúng ta biết cụ thể về IPSec, đây là giao thức được sử dụng cho các quá trình riêng tư, toàn vẹn và chấp nhận.

QUẢN LÝ CÁC QUYỀN CỦA NGƯỜI SỬ DỤNG (USER RIGHT)

Một điều rất quan trọng đối với bạn là phải hiểu được vai trò về quyền của người sử dụng (***user right***) và cấp phép (***permission***) trong việc ủy quyền và phân biệt được sự khác nhau giữa hai khái niệm. *Quyền của người sử dụng*

xác định người sử dụng có thể và không thể làm gì trên hệ thống. *Cấp phép* xác định mức độ truy cập như thế nào (nếu có) của người sử dụng trên các đối tượng. Vì vậy các kiểu cho phép sẽ phụ thuộc vào các đối tượng. Cấp phép bạn cấp cho người sử dụng trên máy in sẽ khác với cấp phép bạn cấp cho người sử dụng khi truy cập vào file và thư mục. Quyền của người sử dụng được áp dụng cho cả hệ thống, trong khi cấp phép chỉ được áp dụng trên từng đối tượng cụ thể. Ví dụ, quyền của người sử dụng có thể bao gồm các quyền sau: sao lưu dữ liệu, đăng nhập vào máy tính và thay đổi thời gian trên máy chủ. Ví dụ về cấp phép là cấp phép đọc (***Read Permission***) được sử dụng để cấp cho người sử dụng khi truy cập vào thư mục, khi đó người sử dụng có thể xem thuộc tính của file và thư mục. Nếu chỉ có cấp phép đọc người sử dụng sẽ không thể thay đổi và xóa các thư mục.

Quyền (***Right***) được chia làm hai kiểu: quyền đặc biệt (***privilege***) và quyền đăng nhập (***logon right***). *Quyền đặc biệt* bao gồm các quyền như kiểm soát bảo mật hoặc quyền bắt buộc một hệ thống khác ngừng hoạt động. *Quyền đăng nhập* là quyền cho phép có thể kết nối với một máy tính. Quyền được tự động gán cho các nhóm dựng sẵn (***built-in group***) trong Windows Server 2003, mặc dù chúng ta cũng có thể gán cho từng người sử dụng cụ thể. Để việc quản lý quyền được dễ hơn gán chúng cho nhóm thay vì gán cho từng người sử dụng cụ thể. Nếu các thành viên của nhóm được nhận quyền từ nhóm đó thì khi một thành viên của nhóm không được cấp quyền bạn chỉ cần loại bỏ người sử dụng đó khỏi nhóm. Ví dụ, nhóm ***Backup Operator*** được quyền sao lưu cả hệ thống, do đó các thành viên của nhóm sẽ có quyền này. Nếu người sử dụng không bao giờ sao lưu hệ thống, thì nên loại bỏ người sử dụng này khỏi nhóm ***Backup Operator***. Bởi vì quyền được gán cho nhóm thay vì từng người sử dụng cụ thể, loại bỏ người sử dụng khỏi nhóm sẽ đảm bảo người sử dụng sẽ không được thừa kế quyền từ nhóm như sao lưu hệ thống, tắt máy và một số quyền khác. Người sử dụng sẽ nhận được các quyền từ nhóm mà người sử dụng là thành viên, vì vậy nếu sử dụng cách gán quyền trên hệ thống theo nhóm thì khi muốn xác định quyền của người sử dụng bạn chỉ cần xác định người sử dụng này thuộc những nhóm nào.

Người sử dụng thừa hưởng quyền từ các nhóm mà họ là thành viên, các quyền này được kết hợp lại với nhau. Ví dụ, nếu một người sử dụng là thành viên củ cả hai nhóm ***Backup Operators*** và ***Account Operators*** thì người sử dụng này sẽ được nhận tất cả các quyền gán cho hai nhóm này.

Một số quyền thường dùng của người sử dụng

Các quyền thường dùng của người sử dụng được liệt kê dưới đây:

- **Cho phép đăng nhập cục bộ (Allow Log On Locally)** Cho phép người sử dụng đăng nhập vào máy tính cục bộ (Local Computer) hoặc vào Miền trên máy tính là thành viên của Miền.
- **Thay đổi giờ hệ thống (Change The System Time)** Cho phép người sử dụng thay đổi thời gian trên máy tính.
- **Tắt máy tính (Shut Down The System)** Cho phép người sử dụng tắt máy tính cục bộ (local computer)
- **Truy nhập vào máy tính này qua mạng (Access This Computer From The Network)** Cho phép người sử dụng truy nhập vào máy tính sử dụng hệ điều hành Windows Server 2003 từ bất cứ máy tính nào trên mạng.
- **Cho phép đăng nhập qua dịch vụ đầu cuối (Allow Log On Through Terminal Services)** Cho phép người sử dụng đăng nhập vào máy chủ đầu cuối (Terminal Server) trên máy trạm.

Sự khác nhau giữa cấp phép (permission) và quyền của người sử dụng (user right)

Như đã nói ở trên, cấp phép xác định mức độ được phép truy cập của người sử dụng hoặc nhóm trên các đối tượng hoặc đặc tính của các đối tượng. Ví dụ, bạn cho phép nhóm Accounting đọc (***Read***) và ghi (***Write***) trên thư mục ***TimeSheets*** thì những người sử dụng có thể truy nhập vào thư mục này xem nội dung bên trong thư mục và thay đổi nội dung bên trong thư mục này.

Bạn có thể gán cấp phép trên các đối tượng cần bảo mật như file, máy in, các đối tượng trong **Active Directory** và các đối tượng trong registry. Bạn có thể gán cấp phép cho người sử dụng, nhóm bảo mật và máy tính. Tuy nhiên cũng giống như quyền của người sử dụng bạn nên gán cho nhóm người sử dụng thay vì gán cho từng người cụ thể.

Bạn có thể gán cấp phép trên các đối tượng cho:

- Các nhóm, các người sử dụng và các nhóm đồng nhất đặc biệt (***special identities***) trong miền.
- Các nhóm, các người sử dụng trên các Miền được tin cậy khác (***trusted domain***).
- Các nhóm và người sử dụng cục bộ trên máy tính chứa đối tượng đó.

Để gán cấp phép cho file hoặc thư mục, Windows Server 2003 yêu cầu sử dụng **file hệ thống NTFS.** Các loại file hệ thống **FAT và FAT32** không hỗ trợ bảo mật đến mức file và thư mục. Tuy nhiên tất cả các loại file hệ thống này đều hỗ trợ bảo mật trên thư mục chia sẻ (*Share Folder*) và máy in trên mạng (*Network Printer*).

Các quyền của người sử dụng được gán cho các nhóm dựng sẵn (Built-In Group)

Mặc định Windows Server 2003 gán một số quyền cho các nhóm dựng sẵn. Các nhóm dựng sẵn bao gồm các nhóm cục bộ (***Local Group***), các nhóm nằm trong đối tượng chứa ***Builtin*** và ***Users*** trên miền (domain).

Các quyền mặc định gán cho các nhóm cục bộ

Bảng 5-2 liệt kê danh sách các quyền được gán cho các nhóm cục bộ

Bảng 5-2 Các nhóm cục bộ và các quyền tương ứng

Nhóm	Quyền của người sử dụng
Administrators	• Access This Computer From The Network • Adjust Memory Quotas For A Process • Allow Log On Locally • Allow Log On Through Terminal Services • Back Up Files And Directories • Bypass Traverse Checking • Change The System Time • Create A Pagefile • Debug Programs • Enable Computer And User Accounts To Be Trusted For Delegation • Force Shutdown From A Remote System • Increase Scheduling Priority • Load And Unload Device Drivers • Manage Auditing And Security Log • Modify Firmware Environment Variables • Perform Volume Maintenance Tasks • Profile Single Process • Profile System Performance • Remove Computer From Docking Station • Restore Files And Directories • Shut Down The System • Take Ownership Of Files Or Other Objects
Backup Operators	• Access This Computer From The Network • Allow Log On Locally • Back Up Files And Directories

	• Bypass Traverse Checking • Restore Files And Directories • Shut Down The System
Power Users	• Access This Computer From The Network • Allow Log On Locally • Bypass Traverse Checking • Change The System Time • Profile Single Process • Remove Computer From Docking Station • Shut Down The System
Remote Desktop Users	• Allow Log On Through Terminal Services
Users	• Access This Computer From The Network • Allow Log On Locally • Bypass Traverse Checking

Các quyền mặc định gán cho các nhóm trong đối tượng chứa Builtin

Đối tượng chứa ***Builtin*** được tạo ra một cách mặc định và chứa các nhóm bảo mật cục bộ như ***Administrators***, ***Backup Operators*** và ***Guests***. Các quyền gán cho các nhóm này được liệt kê trong bảng 5-3.

Bảng 5-3 Các nhóm trong đối tượng chứa Builtin và các quyền tương ứng

Nhóm	**Quyền của người sử dụng**
Account Operators	• Allow Log On Locally • Shut Down The System
Administrators	• Access This Computer From The Network • Adjust Memory Quotas For A Process • Back Up Files And Directories • Bypass Traverse Checking • Change The System Time • Create A Pagefile • Debug Programs • Enable Computer And User Accounts To Be Trusted For Delegation • Force A Shutdown From A Remote System • Increase Scheduling Priority • Load And Unload Device Drivers • Allow Log On Locally • Manage Auditing And Security Log • Modify Firmware Environment Values • Profile Single Process • Profile System Performance • Remove Computer From Docking Station • Restore Files And Directories

	• Shut Down The System • Take Ownership Of Files Or Other Objects
Backup Operators	• Back Up Files And Directories • Allow Log On Locally • Restore files and directories • Shut Down The System
Pre–Windows 2000 Compatible Access	• Access This Computer From The Network • Bypass Traverse Checking
Print Operators	• Allow Log On Locally • Shut Down The System
Server Operators	• Back Up Files And Directories • Change The System Time • Force Shutdown From A Remote System • Allow Log On Locally • Restore Files And Directories • Shut Down The System

Các quyền mặc định gán cho các nhóm trong đối tượng chứa Users

Các quyền gán cho các nhóm trong đối tượng chứa ***Users*** được liệt kê trong bảng 5-4.

Bảng 5-4 Các nhóm trong đối tượng chứa Users và các quyền tương ứng

Nhóm	**Quyền của người sử dụng**
Domain Admins	• Access This Computer From The Network • Adjust Memory Quotas For A Process • Back Up Files And Directories • Bypass Traverse Checking • Change The System Time • Create A Pagefile • Debug Programs • Enable Computer And User Accounts To Be Trusted For Delegation • Force A Shutdown From A Remote System • Increase Scheduling Priority • Load And Unload Device Drivers • Allow Log On Locally • Manage Auditing And Security Log • Modify Firmware Environment Values • Profile Single Process • Profile System Performance • Remove Computer From Docking Station • Restore Files And Directories • Shut Down The System • Take Ownership Of files Or Other Objects

Enterprise Admins (nhóm này chỉ có trong miền gốc của rừng *forest root domain*)	• Access This Computer From The Network • Adjust Memory Quotas For A Process • Back Up Files And Directories • Bypass Traverse Checking • Change The System Time • Create A Pagefile • Debug Programs • Enable Computer And User Accounts To Be Trusted For Delegation • Force Shutdown From A Remote System • Increase Scheduling Priority • Load And Unload Device Drivers • Allow Log On Locally • Manage Auditing And Security Log • Modify Firmware Environment Values • Profile Single Process • Profile System Performance • Remove Computer From Docking Station • Restore Files And Directories • Shut Down The System • Take Ownership Of Files Or Other Objects

LƯU Ý: *Về* ***User Rights and Service Account Information*** *bạn có thể xem tại Microsoft Knowledge Base bài số 325349, "HOW TO: Grant User Rights to Manage Services in Windows Server 2003 ". Để tìm bài này bạn có thể vào trangWeb http://support.microsoft.com và nhập số ở trên trong hộp thoại Search The Knowledge Base.*

Cách gán quyền cho người sử dụng

Trong miền cách dễ nhất để gán quyền là sử dụng **Group Policy** tại mức Miền. Sử dụng ***Active Directory Users and Computers*** để soạn thảo các chính sách (***Group Policy***) trên Miền. Ví dụ, giả sử bạn muốn gán cho một số người sử dụng quyền thêm một máy trạm vào miền (***Add WorkStations to Domain***). Bạn có thể tạo ra nhóm ***Add WorkStations*** và thêm những người sử dụng trên vào nhóm này, sau đó gán quyền thêm một máy trạm vào miền cho nhóm ***Add WorkStations***. Như vậy mỗi người sử dụng trong nhóm ***Add WorkStations*** sẽ được nhận quyền thêm một máy trạm vào miền. Thông thường người quản trị thêm người sử dụng hoặc các nhóm người vào các nhóm dựng sẵn bởi vì các nhóm này đã được cấp các quyền từ trước. Trong một số trường hợp, các nhóm dựng sẵn có quá nhiều hoặc quá ít đối với một người sử dụng cụ thể, khi đó bạn phải tạo ra một nhóm mới hoặc gán quyền cho người sử dụng này một cách thủ công. Để gán quyền cho người sử dụng

hay nhóm, bạn thêm người sử dụng hoặc nhóm vào từng chính sách trong phần ***User Rights Assignment*** theo các bước dưới đây.

- **Gán quyền cho người sử dụng**

Để gán quyền cho người sử dụng bạn thực hiện theo các bước liệt kê sau đây:

1. Chọn ***Start*** sau đó chuyển đến ***Administrative Tools*** và nhấn chuột vào ***Domain Controller Security Policy***.
2. Trong cửa sổ vừa mở ra bạn mở ***Local Policies*** và nhấn chuột vào ***User Rights Assignment***.
3. Nhấn đúp chuột vào một chính sách ở bên phải
4. Sử dụng hộp thoại vừa mở tương ứng với quyền được chọn, thêm hoặc bớt các nhóm cần thiết đối với quyền này.

THỰC HÀNH QUẢN TRỊ BẢO MẬT

Trong các mạng lớn, duy trì bảo mật có thể là một tác vụ phức tạp nhất. Windows Server 2003 đưa ra một số lượng lớn các đặc điểm bảo mật và một số lượng lớn các chính sách bảo mật và các thuộc tính phải được cấu hình. Mặc dù với số lượng lớn các đặc điểm và định dạng sẽ cho phép bảo mật ở mức cao nhưng nó cũng gây ra khó khăn khi áp dụng các chính sách bảo mật phù hợp với từng tổ chức. Do đó để có thể thực hiện được quản trị bảo mật bạn nên tạo ra các ranh giới bảo mật (***baseline***) và áp dụng nguyên lý cấp quyền tối thiểu. Khi đó bạn có thể quản trị một cách dễ dàng hơn trong khi mạng của bạn vẫn được bảo vệ. Phần này sẽ hướng dẫn các bạn thực hiện điều này như thế nào.

Tạo ra ranh giới bảo mật để xác định các sự kiện có thể liên quan đến bảo mật

Một việc rất quan trọng là bạn phải xác định vai trò của mỗi máy tính trong tổ chức của bạn, sau đó từ những vai trò này bạn sẽ thiết kế các mẫu bảo mật (***security template***) để có thể bảo mật cho từng máy tính này. Ví dụ, bạn có thể tạo ra một ranh giới bảo mật cho tất cả các máy tính trong tổ chức của bạn không phụ thuộc vào vai trò của từng máy tính. Sau đó bạn áp dụng thêm các mẫu (***template***) cụ thể cho từng vai trò, như mẫu cho máy chủ cơ sở dữ liệu, máy chủ mail, máy chủ File và In ấn và các máy chủ khác. Các mẫu thêm vào (***incremental template***) chỉ bao gồm các cấu hình cần thiết để bảo mật cho từng vai trò tương ứng của máy chủ. Các mẫu thêm vào này kết hợp với ranh giới bảo mật tạo ra các mẫu bảo mật cụ thể cho từng vai trò của máy chủ. Các mẫu bảo mật sẽ được đưa ra cụ thể hơn trong phần "Sử dụng các mẫu bảo mật" trong chương này.

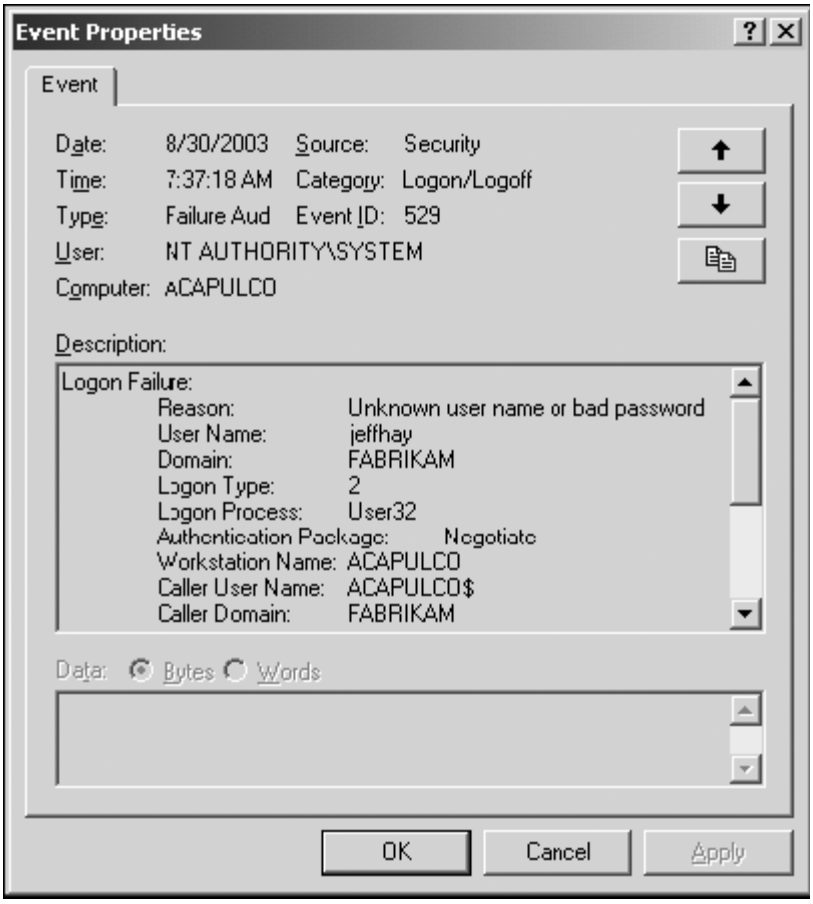
Đường bảo mật cơ sở sẽ giúp bạn áp dụng các cấu hình bảo mật hiệu quả và phù hợp với tổ chức của bạn. Để giúp cho việc xác định các cấu hình bảo

mật đã được áp dụng hay chưa bạn nên nhấn hoạt việc kiểm soát (***auditing***). *Kiểm soát* có nghĩa là bạn có thể nhận thấy các quá trình tấn công hoặc bạn có thể xác định các kiểu tấn công thường xảy ra. Ví dụ, bạn có thể đặt các chính sách kiểm soát để tạo ra các sự kiện (***Event***) ghi lại mỗi lần đăng nhập thất bại. Việc này sẽ cảnh báo bạn là có thể có Hacker đang cố truy nhập vào bằng quyền của người quản trị với các mật khẩu phỏng đoán. Để xác định chính xác các sự kiện này xảy ra khi nào bạn phải xem nhật ký kiểm soát bảo mật.

Hiển thị và duy trì nhật ký kiểm soát bảo mật

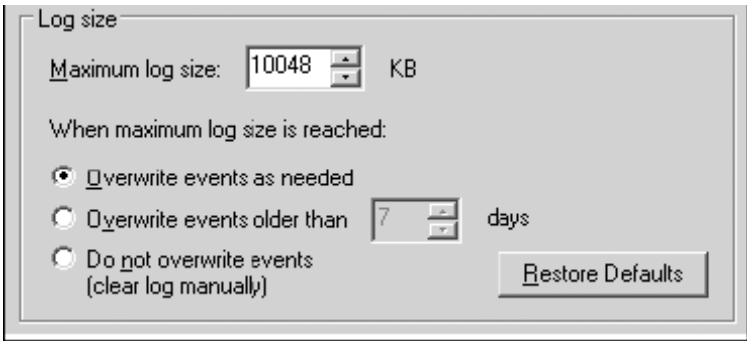
Nhật ký bảo mật sẽ cho biết các thông tin kiểm soát liên quan đến các sự kiện tuỳ theo các chính sách kiểm soát mà bạn đang áp dụng. Mỗi khi các sự kiện đã được kiểm soát xảy ra nó sẽ được thêm vào file nhật ký, khi đó bạn có thể lọc, sắp xếp, tìm kiếm hoặc chuyển (***export***) thành dạng khác. Nhật ký bảo mật tách biệt với các nhật ký ứng dụng và hệ thống, bạn có thể xem trong **Event Viewer** hoặc có thể tìm thấy trong công cụ quản trị ***Computer Management*** bằng cách mở ***System Tools***, ***Event Viewer***, và chọn ***Security***.

Mỗi sự kiện sẽ được lưu lại là một dòng trong nhật ký bao gồm các thông tin về các sự kiện được kiểm soát có thể bao gồm việc truy nhập thất bại hoặc thành công, ngày và giờ của sự kiện, mã số (ID) và phân loại sự kiện, người sử dụng và máy tính được kiểm soát. Thông tin chi tiết về từng sự kiện (Hình 5-1) có thể được hiển thị bằng cách nháy đúp vào từng dòng trong nhật ký



Hình 5-1 Thông tin chi tiết của một sự kiện bảo mật

Nhật ký bảo mật đã được cấu hình các thuộc tính xác định kích thước lớn nhất. Nếu bạn kiểm soát hệ thống với các sự kiện liên quan đến bảo mật, bạn phải đặt kích thước của file nhật ký đủ lớn để có thể ghi lại được tất cả các sự kiện này để tránh việc một số sự kiện sẽ không ghi vào được do kích thước của file nhật ký đã đến mức giới hạn. Một số thuộc tính bổ sung liên quan đến kích thước lớn nhất, mỗi file nhật ký có ba sự lựa chọn khi kích thước của file này đến mức giới hạn, xem hình 5-2 và danh sách dưới đây.



Hình 5-2 Các lựa chọn với File nhật ký

- **Overwrite Events As Needed** Nếu kích thước của file nhật ký quá nhỏ trong khi số lượng các sự kiện được ghi lại lớn, bạn sẽ không thể xem được các sự kiện xảy ra trong quá khứ.

- **Overwrite Events Older Than x Days** Lựa chọn này sẽ đảm bảo các sự kiện xảy ra trong x ngày từ ngày hiện tại sẽ không bị xóa. Mặc dù đảm bảo được các sự kiện xảy ra trong số ngày chỉ định không bị xóa nhưng nó cũng có thể gây ra đầy file nhật ký và không ghi lại được sự kiện mới xảy ra.

- **Do Not Overwrite Events (Clear Log Manually)** Lựa chọn này cung cấp tất cả các sự kiện xảy ra trong quá khứ nhưng cũng ngăn cản các sự kiện mới được ghi lại khi file nhật ký bị đầy**.**

Sau khi xem nhật ký bảo mật bạn có thể ghi lại bằng cách sử dụng ***Event Viewer***. Nháy chuột phải vào ***Security*** và chọn ***Save Log File As***. Chọn nơi lưu trữ và tên file sau đó chọn ***Save***.

Thực hành cấu hình các chính sách kiểm soát và hiển thị sự kiển bảo mật theo hướng dẫn của bài thực hành 5-2 "Hiển thị các sự kiện"

Áp dụng nguyên lý cấp quyền tối thiểu

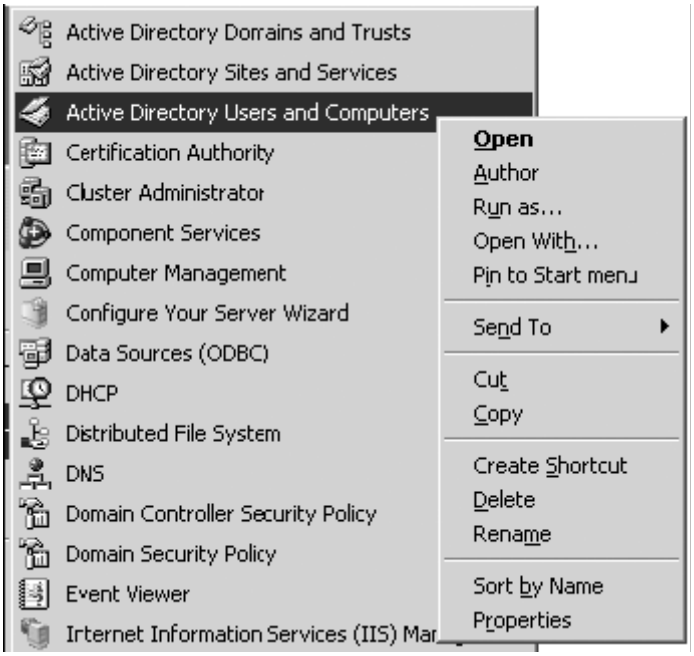
Bạn đã thiết kế các chính sách bảo mật cấp quyền cho người sử dụng và các cấp phép, nhưng bạn vẫn nên áp dụng nguyên lý cấp quyền tối thiểu. Nguyên lý này sẽ đảm bảo rằng không có bất cứ một người sử dụng hoặc đối tượng (như các dịch vụ) có được nhiều quyền hoặc truy cập thông tin và tài nguyên hơn mức cần thiết.

Áp dụng nguyên lý này có nghĩa là các người sử dụng được đưa vào các nhóm với quyền và cấp phép phù hợp với trách nhiệm và sự ủy quyền của từng người. Bạn cũng sẽ phải thường xuyên kiểm tra lại các quyền và cấp phép để bảo đảm mọi người sử dụng luôn nhận được các quyền và cấp phép thích hợp.

Nguyên lý cấp quyền tối thiểu cũng được áp dụng cho những người quản trị hệ thống. Mặc dù người quản trị hệ thống phải được quyền truy nhập toàn bộ hệ thống nhưng không cần mức quyền như thế này cho các công việc hàng ngày. Đăng nhập bằng tài khoản người sử dụng với quyền truy nhập không hạn chế vào hệ thống sẽ làm tăng sự rủi ro về bảo mật cho tổ chức của bạn. Người quản trị đăng nhập với các cấp phép không hạn chế sẽ vô tình chạy các chương trình phá hoại gây ra sự nguy hiểm tiềm tàng cho hệ thống hơn là các tài khoản đăng nhập vào với các quyền và cấp phép bị giới hạn. Vì vậy, người quản trị hệ thống nên áp dụng nguyên lý quyền tối thiểu bằng

cách sử dụng tài khoản người dùng với các cấp phép giới hạn và chỉ sử dụng quyền quản trị khi thực sự cần thiết.

Để thực hiện được điều này bạn có thể sử dụng đặc tính ***Run As***. Đặc tính ***Run As*** có thể sử dụng thông qua thực đơn ngữ cảnh (nháy chuột phải) khi bạn mở một chương trình (Hình 5-3), trực tiếp từ dòng lệnh, hoặc tạo ra shortcut.



Hình 5-3 Sử dụng đặc tính Run As

Dưới đây là bốn ví dụ về các shortcut của các công cụ quản trị thường dùng và cách tạo ra chúng.

➢ Tạo ra các shortcut sử dụng lệnh Run As

Để tạo ra các shortcut sử dụng lệnh ***Run As,*** tiến hành theo các bước dưới đây:

1. Nháy chuột phải vào màn hình nền (***Desktop***), chuyển tới ***New*** và chọn ***Shortcut***.
2. Trong hộp thoại ***Type The Location Of The Item*** nhập **runas** và các tham biến bạn muốn sử dụng. Xem các ví dụ trong bảng 5-5

Bảng 5-5 Các ví dụ về Run As

Mục đích của Shortcut	**Câu lệnh**	**Mô tả**
Cửa sổ lệnh (Command Prompt) với quyền quản	***runas /user:computer-name\administrator cmd***	Thanh tiêu đề của cửa sổ lệnh sẽ cho biết cửa sổ lệnh này đang được sử dụng với tài khoản nào

trị		
Công cụ Computer Management với quyền quản trị	***runas /user:computer-name\administrator "mmc %windir%\system32\compmgmt.msc"***	Cửa sổ ***Computer Management*** không hiển thị là đang được sử dụng với tài khoản nào. Điều này có thể gây ra nhầm lẫn khi bạn sử dụng hai cửa sổ ***Computer Management*** với các mức bảo mật khác nhau.
Active Directory Users and Computers với quyền quản trị miền	***runas /user:domain-name\administrator "mmc %windir%\system32\dsa.msc"***	Cửa sổ ***Active Directory Users and Computers*** không hiển thị là đang được sử dụng với tài khoản nào. Điều này có thể gây ra nhầm lẫn khi bạn sử dụng hai cửa sổ ***Active Directory Users and Computers*** với các mức bảo mật khác nhau.
Active Directory Users and Computers trong một rừng (***forest***) khác	***runas /netonly/user: domainname\User Name "mmc dsa.msc"***	Cửa sổ ***Active Directory Users and Computers*** không hiển thị là đang được sử dụng với tài khoản nào. Điều này có thể gây ra nhầm lẫn khi bạn sử dụng hai cửa sổ ***Active Directory Users and Computers*** với các mức bảo mật khác nhau.

3. Nhấn ***Next***, nhập tên cho ***Shortcut***, sau đó nhấn ***Finish***.

LƯU Ý: Dịch vụ Secondary Logon và lện Run As *Để lệnh Run As có thể thực hiện được, dịch vụ Secondary Logon phải đang chạy (running) và điều kiện bạn cung cấp (tên và mật khẩu) phải được chấp nhận. Run As không thể làm việc được với Smart Card.*

Các hướng dẫn về quyền tối thiểu

Dưới đây là một số hướng dẫn bổ ích cho việc áp dụng nguyên lý cấp quyền tối thiểu:

- Nhóm người sử dụng theo các vai trò để từ đó có thể gán các quyền và cấp phép theo từng vai trò.
- Cấu hình các danh sách điều khiển truy nhập (ACL) cho các file và thư mục, khóa trong registry, đối tượng trong Active Directory và máy in chỉ cho phép truy nhập chính xác theo yêu cầu của người sử dụng.

- Bảo vệ máy chủ một cách vật lý (physical). Chỉ cho phép những người được ủy quyền được can thiệp và bảo mật việc ủy quyền này.
- Kiểm tra nhật ký kiểm soát và các nhật ký khác để phát hiện các truy nhập không được phép.
- Sử dụng Web Proxy để giới hạn người sử dụng truy nhập các tài nguyên bên ngoài.
- Sử dụng FireWall để giới hạn truy nhập vào mạng bên trong.

SỬ DỤNG CÁC MẪU BẢO MẬT (SECURITY TEMPLATE)

Để có thể quản lý được một số lượng lớn các lựa chọn bảo mật và các thiết lập cấu hình, Windows Server 2003 cung cấp các mẫu bảo mật. Nếu không có các mẫu bảo mật này thì gần như không thể quản lý được hàng nghìn thiết lập cấu hình cho từng máy tính, từng vai trò mà các máy tính này đang thực hiện và các thiết lập khi kết hợp các vai trò.

Các *mẫu bảo mật(security template)* là các file cấu hình bao gồm tất cả các thuộc tính bảo mật của hệ thống. Chỉ với một giao diện đơn giản, người quản trị có thể tạo ra một mẫu bảo mật hoặc tập các mẫu tương ứng với chính sách bảo mật của công ty cũng như với từng máy tính cụ thể hoặc một tập hợp máy tính và sau đó áp dụng cho máy tính cục bộ hoặc nạp (*import*) vào đối tượng chính sách nhóm (GPO) trong Active Directory. Khi bạn nhập mẫu bảo mật vào GPO, tất cả các máy tính ảnh hưởng bởi đối tượng này sẽ nhận các thiết lập từ mẫu bảo mật này.

Sử dụng Snap-In Security Templates

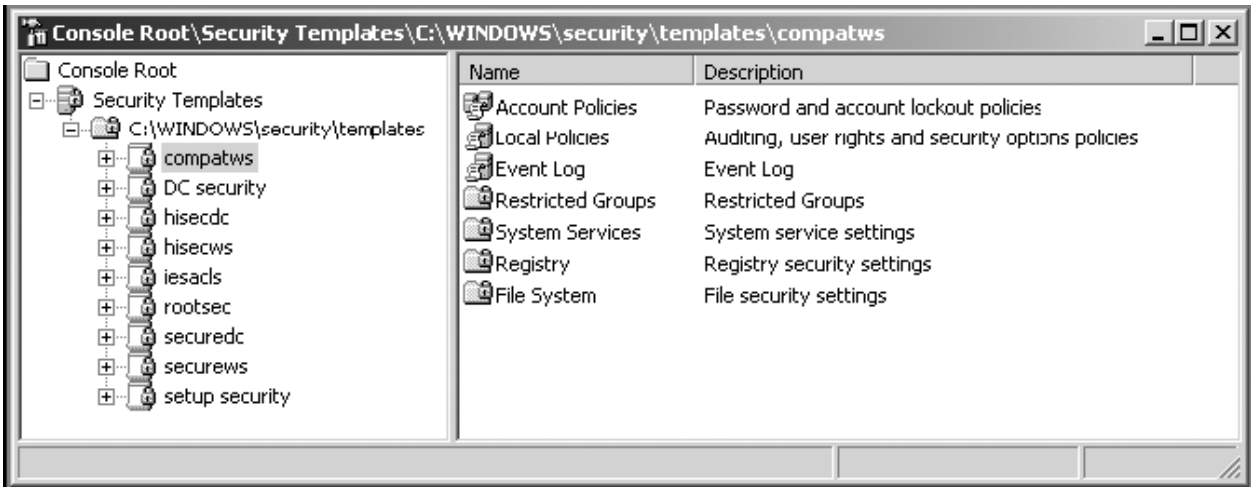
Các mẫu bảo mật có thể tạo ra và thay đổi bằng Snap-In ***Security Templates*** của ***Microsoft Management Console*** (MMC). Để thêm snap-in vào MMC tiến hành theo các bước dưới đây.

1. Nhấn ***Start***, nhấn ***Run*** trong hộp ***Open*** nhập **mmc** sau đó nhấn ***OK***.
2. Trên thực đơn File, nhấn ***Add/Remove Snap-In***.
3. Trong cửa sổ ***Add/Remove Snap-In***, nhấn ***Add***.
4. Trong cửa sổ Add Standalone Snap-In, nhấn Security Templates, nhấn Add và sau đó nhấn Close.

5. Trong cửa sổ ***Add/Remove Snap-In***, nhấn ***OK***.

6. Snap-In ***Security Templates*** đã được thêm vào tại gốc của cây bảng điều khiển.

7. Trong cây bảng điều khiển, mở ***Security Templates*** và thư mục ***%systemroot%\Security\Templates*** để hiển thị danh sách các mẫu đã có từ trước. Những mẫu này đã được cấu hình sẵn và có thể thay đổi tùy theo yêu cầu của từng tổ chức cụ thể. Khi một mẫu mới được tạo ra hoặc copy từ một mẫu đang có sẵn, nó sẽ được thêm vào trong danh sách. Chọn bất kỳ một trong các chính sách có sẵn, bạn sẽ thấy các chính sách được liệt kê ở phần bên phải để cho chúng ta có thể thiết lập cấu hình một cách dễ dàng (Hình 5-4).



Hình 5-4 Các mẫu bảo mật có sẵn

Mỗi mẫu bảo mật trong danh sách này sẽ được biểu thị bằng một file ***.inf.*** Snap-In ***Security Templates*** là giao diện để thay đổi các file mẫu bảo mật này. Các file này lưu trữ tại thư mục: ***%systemroot%\Security\Templates.*** Dưới đây là một phần nhỏ của mẫu ***Securews*** (***securews.inf***) cho chúng ta biết về ***Accounts Policies***:

```
[System Access]
;---------------------------------------------------------
;Account Policies - Password Policy
;---------------------------------------------------------
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
ClearTextPassword = 0
```

LSAAnonymousNameLookup = 0
EnableGuestAccount = 0

Khảo sát các mẫu chính sách

Mỗi mẫu bao gồm các thiết lập thuộc tính cho bảy phần cấu hình bảo mật trong Windows Server 2003. Nhấn đúp vào từng phần bảo mật trong ô bên phải của console hoặc mở rộng console tree ở ô bên trái để hiển thị từng phần cụ thể. Các phần này được liệt kê dưới đây:

- **Account Policies** bao gồm các chính sách gắn liền với tài khoản người sử dụng đó là ***Password Policy***, ***Account Lockout Policy*** và ***Kerberos Policy***.

- **Local Policies** bao gồm các chính sách gắn liền với ai sử dụng hoặc truy nhập vào máy tính này qua mạng và khi nào các sự kiện được kiểm soát đó là ***Audit Policy***, ***User Right Assignment*** và ***Security Options***.

- **Event Log** bao gồm các thuộc tính liên quan đến các nhật ký ứng dụng, bảo mật và hệ thống. Các thuộc tính nhật ký này bao gồm ***Maximum Size***, ***Access Restriction***. Nhật ký của các sự kiện được xem bằng ***Event Viewer***.

- **Restricted Groups** Thiết lập bảo mật ***Restricted Groups*** được sử dụng để thêm các thành viên vào các nhóm người sử dụng dựng sẵn (đã có sẵn các quyền) hoặc vào các nhóm tạo ra bởi người quản trị mà các nhóm này có thể được gán các đặc quyền nhất định..

- **System Services** bao gồm các thuộc tính bảo mật của tất cả các dịch vụ hệ thống trên máy tính cục bộ. Dịch vụ hệ thống này bao gồm các dịch vụ file, dịch vụ máy in, dịch vụ mạng và các dịch vụ cụ thể cho từng ứng dụng như ***Microsoft Exchange System Attendant***.

- **Registry** bao gồm các thuộc tính bảo mật cho các khóa có sẵn trong registry, kể cả các thông tin kiểm soát và cho phép truy cập.

- **File System** cho phép bạn cấu hình cấp phép truy cập và kiểm soát các file và thư mục trên hệ thống cục bộ.

Sử dụng các mẫu bảo mật có sẵn

Các mẫu bảo mật có sẵn được cung cấp bởi Windows Server 2003 có thể được sử dụng hoặc có thể thay đổi để phù hợp với các yêu cầu bảo mật nghiêm ngặt hơn. Các mẫu này cho chúng ta một dải các mức bảo mật khác nhau và tương ứng với các tình huống bảo mật điển hình của các máy tính có vai trò khác nhau trong hệ thống như: trạm làm việc (*workstation*), máy chủ (*server*) và Máy chủ Quản trị Miền (*domain controller*). Bảng 5-6 liệt kê một số các mẫu bảo mật định sẵn; được tổ hợp theo các mức bảo mật

Bảng 5-6 Một số mẫu bảo mật có sẵn

Mức bảo mật	Tên mẫu	Mô tả
Secure	***securews***	Mẫu bảo mật dành cho trạm làm việc hoặc máy chủ
	securedc	Mẫu bảo mật dành cho máy quản trị miền
Highly secure	***hisecws***	Mẫu bảo mật mức cao dành cho trạm làm việc hoặc máy chủ
	hisecdc	Mẫu bảo mật mức cao dành cho máy quản trị miền
Compatible	***compatws***	Mẫu bảo mật tương thích dành cho trạm làm việc hoặc máy chủ
Out of the box	***setup security***	Mẫu bảo mật thiết lập mặc định khác

Các mẫu bảo mật cơ sở đi kèm với Windows Server 2003 không liệt kê trong bảng trên. Các mẫu này được bỏ đi để đảm bảo rằng Windows Server 2003 được bảo mật cao hơn. Trong Windows Server 2003 bạn phải chọn các mẫu bảo mật ở mức bảo mật cao hơn.

Mẫu bảo mật Secure

Hai mẫu bảo mật cung cấp mức độ bảo mật cao hơn được đưa ra: một dành cho máy quản trị miền mẫu còn lại có thể áp dụng cho các trạm làm việc hoặc máy chủ. Các mẫu ***Securews*** và ***Securedc*** cung cấp mức độ bảo mật trung bình bằng cách bắt buộc mật khẩu và các chính sách khóa tài khoản chặt chẽ hơn đồng thời hạn chế truy cập của các tài khoản ***Guest***.

Các sự kiện đăng nhập thất bại và sử dụng quyền ưu tiên cũng như việc quản lý tài khoản thành công hay thất bại và thay đổi chính sách sẽ được kiểm soát. Ngoài ra mẫu bảo mật máy quản trị miền còn cung cấp thêm việc kiểm soát truy cập các đối tượng trong Active Directory. Các chính sách về tài khoản (***account***) và cục bộ (***local***) cũng được liệt kê trong mẫu bảo mật máy quản trị miền. Bởi vì các cấp phép của file, thư mục và các khoá trong

registry đã được cấu hình bảo mật theo mặc định nên các phần này không liệt kê trong các mẫu bảo mật này.

Mẫu bảo mật Highly Secure

Mẫu bảo mật ***Highly Secure*** không được dùng nhiều trong thực tế và chỉ tập trung vào bảo mật trao đổi thông tin trong môi trường ***native-mo`de*** (Windows Server 2003). Trong mẫu bảo mật này các thuộc tính bảo mật được đặt cho việc tạo chữ ký số trong việc trao đổi giữa các máy trạm và máy chủ và cho việc tạo chữ ký, mã hóa bảo mật các kênh dữ liệu. Bởi vì đã đặt rất nhiều các giao thức bảo mật nên khi các hệ thống áp dụng các mẫu bảo mật này sẽ không thể giao tiếp được với các máy tính sử dụng Windows 95, Windows 98 hoặc Windows NT. Ngoài ra trong mẫu bảo mật ***Hisecws*** sẽ không có ***Acuthenticated Users*** trong nhóm hạn chế (***restricted***) ***Power Users*** còn các mẫu bảo mật ***Hisecdc*** và ***Hisecws*** về bản chất là gần giống nhau.

Mẫu bảo mật Compatible

Mục đích của mẫu bảo mật ***Compatible*** là cho phép hầu hết các ứng dụng có thể sử dụng được mà không cần đến mức bảo mật của ***Power Users***. Mẫu bảo mật ***Compatible*** thiết lập cho phép các thành viên của nhóm cục bộ ***Users*** chỉ có thể chạy các ứng dụng xác thực bởi Windows, ngược lại chỉ có các thành viên của nhóm ***Power Users*** hoặc cao hơn mới có thể chạy các ứng dụng không được xác thực. Vì vậy nếu người sử dụng cần chạy các ứng dụng không xác thực bạn phải thêm các người sử dụng này tối thiểu vào nhóm ***Power Users***.

Áp dụng các mẫu bảo mật

Các mẫu bảo mật có thể được áp dụng bằng cách nhập (***import***) vào GPO. Để có thể thực hiện được điều này tiến hành theo các bước dưới đây:

1. Chọn GPO muốn nhập vào (ví dụ, sử dụng công cụ ***Active Directory Users and Computers*** để liên kết GPO này với **organization unit[OU]** và sau đó sửa GPO này).

2. Mở rộng đối tượng này, mở ***Computer Configuration*** và sau đó mở ***Windows Settings.***

3. Nháy chuột phải vào ***Security Settings*** và nhấn ***Import Policy***.

4. Từ danh sách của các file ***.inf*** chọn mẫu bảo mật đã được xác định sau đó nhấn ***Open***.

Dưới đây là một số hướng dẫn bổ ích khi các bạn áp dụng nguyên lý cấp quyền tối thiểu với các mẫu bảo mật:

- Gán quyền tối thiểu cho người sử dụng. Giảm số quyền bạn gán cho người sử dụng đến mức tối đa có thể, nhất là các quyền truy cập và đăng nhập.
- Bắt buộc sử dụng các chính sách mật khẩu chặt chẽ để ngăn cản các truy cập bất hợp pháp.
- Sử dụng các lựa chọn bảo mật để ngăn chặn truy nhập và hạn chế phạm vi hoạt động.
- Sử dụng danh sách điều khiển truy cập(ACL) trên file và registry.
- Sử dụng ***Restricted Group*** để bắt buộc và hạn chế số lượng thành viên trong các nhóm quan trọng.
- Sử dụng ***System Services*** để hạn chế các dịch vụ cũng như hạn chế các tài khoản có thể quản lý chúng.
- Đưa ra các ranh giới bảo mật cho từng vai trò của máy tính, và thực hiện các mẫu bảo mật sẽ được sử dụng để nhập vào các GPO tương ứng với từng OU.
- Áp dụng các kế hoạch kiểm soát một cách toàn diện.

QUẢN LÝ HỆ THỐNG FILE MÃ HÓA (EFS)

EFS cung cấp kỹ thuật mã hóa file cốt lõi cho việc lưu trữ file trên các phân vùng NTFS. Kỹ thuật mã hóa EFS sử dụng cơ sở khóa công khai (***public key***) và chạy như là các dịch vụ tích hợp hệ thống từ đó sẽ giúp cho chúng ta quản lý dễ dàng hơn, khó bị tấn công hơn và là trong suốt với người sở hữu file.

Mặc định, dữ liệu mã hóa sẽ không được mã hóa khi truyền trên mạng mà chỉ được mã hóa khi lưu trữ trên ổ đĩa, trừ khi hệ thống của bạn sử dụng IPSec hoặc ***Web Distributed Authoring and Versioning*** (WebDAV). IPSec mã hóa dữ liệu khi nó được truyền đi trên mạng **Transmission Control Protocol/ Internet Protocol (TCP/IP)**. Nếu file được mã hóa trước khi sao chép hoặc di chuyển tới thư mục WebDAV trên máy chủ, nó vẫn được mã hóa trong khi truyền và khi lưu trữ trên máy chủ.

Người sử dụng là sở hữu của file hoặc thư mục có thể mã hóa hoặc giải mã file hoặc thư mục này. Nếu người sử dụng truy nhập vào các file được mã hóa và có khóa riêng cho file này, người sử dụng có thể mở file và làm việc một cách trong suốt trên file này giống như các tài liệu thông thường. Người sử dụng không có khóa riêng sẽ bị từ chối truy cập. Mã hóa và giải mã với nhiều chức năng hơn có thể thực hiện bằng tiện ích dòng lệnh ***Cipher***. (Cipher sẽ được giới thiệu trong phần "Sử dụng tiện ích cipher" dưới đây)

Các tổ chức có thể đặt các chính sách khôi phục dữ liệu mã hóa EFS khi cần thiết. Chính sách khôi phục này được tích hợp với hầu hết các chính sách bảo mật của Windows Server 2003. Việc quản lý chính sách có thể được ủy quyền cho một số người cụ thể có thẩm quyền khôi phục, và các chính sách khôi phục có thể được cấu hình cho từng bộ phận trong tổ chức. Khi khôi phục file dữ liệu đã mã hóa, bạn không thể khôi phục được các khóa đã sử dụng để mã hóa file này. Một vài biện pháp bảo vệ đã được đưa ra để đảm bảo rằng dữ liệu luôn luôn có thể khôi phục được và không xảy ra mất mát dữ liệu kể cả trong trường hợp toàn bộ hệ thống bị hỏng.

EFS cho phép người sử dụng mã hóa các file NTFS bằng cách sử dụng hệ thống mật mã trên cơ sở khóa công khai mạnh từ đó mã hóa tất cả các file trong thư mục. Người sử dụng với Khái lược Di trú (***roaming profile)*** có thể dùng cùng một khóa riêng (***private key***) với các hệ thống được tin cậy khác. Để bắt đầu sử dụng EFS, bạn sẽ không cần bất cứ quyền quản trị gì và tất cả các quá trình đều diễn ra trong suốt. Các file sao lưu và sao chép của các file mã hóa cũng được mã hóa nếu chúng ở trên các phân vùng NTFS. Các file vẫn giữ nguyên trạng thái mã hóa khi bạn dịch chuyển (*move*) hoặc khi đổi tên của chúng.

Bạn có thể sử dụng EFS để mã hóa và giải mã các file trên máy chủ File, nhưng không thể mã hóa dữ liệu truyền đi trên mạng. Windows Server 2003 cung cấp các giao thức mạng như **Secure Socket Layer(SSL)** và IPSec để mã hóa dữ liệu khi truyền đi trên mạng. SSL là một chuẩn mở được đưa ra để thiết lập một kênh truyền dẫn bảo mật nhằm ngăn chặn việc lấy trộm các thông tin quan trọng như là số của ***Credit Card***.

Đặc điểm của EFS

Các đặc điểm của EFS được liệt kê dưới đây:

- **Mã hóa trong suốt** Với EFS, các file được mã hóa sẽ không yêu cầu người sở hữu file phải mã hóa và giải mã file trong mỗi lần sử dụng. Mã hóa và giải mã được thực hiện một cách trong suốt khi người sử dụng đọc hoặc ghi file.

- **Bảo vệ tốt các khóa mã hóa** Các khóa mã hóa có thể chống lại gần như tất cả các phương thức tấn công tinh vi nhất. Bởi vì trong EFS sử dụng khóa công khai (***public key***) từ giấy xác nhận người dùng X.509 v3 để mã hóa các khóa mã hóa, mà được sử dụng để mã hóa file. Danh sách các khóa mã hóa của file được lưu trữ cùng với file mã hóa và duy nhất đối với file. Để giải mã các khóa mã hóa của file, người sở hữu file cung cấp khóa riêng mà chỉ có người sở hữu file có.

- **Tích hợp khôi phục dữ liệu trên hệ thống** `Danh sách của các file khóa mã hóa được mã hóa lần nữa bằng cách sử dụng khóa công khai của tác nhân phục hồi, và danh sách này cũng được lưu trữ cùng với file mã hóa. Có thể có nhiều hơn một tác nhân phục hồi và sẽ có các khóa công khai tương ứng khác nhau. Phải có ít nhất một khóa công khai phục hồi trong hệ thống để mã hóa file.

- **Bảo mật các file tạm thời và file hoán chuyển (paging)** Rất nhiều ứng dụng tạo ra các file tạm thời trong khi bạn sửa các tài liệu, và những file tạm thời này sẽ không được mã hóa ở trên ổ cứng. Nhưng vì EFS thực hiện tại mức thư mục nên các file tạm thời này cũng sẽ được mã hóa.

Trong Windows Server 2003, các file khóa mã hóa được tập trung trong **Windows Operating System Kernel** và được lưu trữ trong ***Nonpaged Pool*** (*Vùng bộ nhớ không hoán chuyển*), để đảm bảo chúng sẽ không bao giờ được chép vào file hoán chuyển. Điều đó đảm bảo rằng file hoán chuyển không thể sử dụng để truy nhập các tài liệu đã được mã hóa với một khóa đơn.

Mã hóa File hoặc Thư mục

Để mã hóa các **file** hoặc thư mục bạn phải tạo ra thư mục NTFS sau đó bạn mã hóa bằng cách sử dụng hộp thoại ***Properties*** của thư mục này. Trong thẻ ***General*** nhấn ***Advanced*** sau đó nhấn ***Encrypt Content To Secure Data***.

> ***LƯU Ý: Mã hóa và nén*** *Mã hóa và nén không thể lựa chọn đồng thời. Bạn không thể mã hóa file trên phân vùng được nén.*

Sau khi bạn mã hóa thư mục, khi bạn ghi file vào thư mục này, file sẽ được mã hóa bằng cách sử dụng các khóa mã hóa file, đó là các khóa đối xứng nhanh được thiết kế cho việc mã hóa số lượng lớn. File được mã hóa theo các khối, với các khóa mã hóa file khác nhau cho từng khối. Tất cả các khóa mã hóa file cũng được mã hóa và lưu trữ trong ***Data Decryption Field***

(DDF) và ***Data Recovery Field*** (DRF). DDF và DRF được đặt tại phần đầu (***header)*** của file.

Tất cả các file và thư mục con bạn tạo ra trong thư mục đã được mã hóa sẽ tự động mã hóa, cũng như bất kỳ file nào bạn dịch chuyển hoặc chép vào thư mục mã hóa này. Nếu bạn dịch chuyển hoặc chép file từ thư mục mã hóa sang thư mục không được mã hóa, file này cũng vẫn bị mã hóa. Mỗi file có một khóa mã hóa duy nhất, từ đó nó sẽ bảo đảm an toàn ngay cả khi bạn đổi tên file.

Thực hành mã hóa file theo hướng dẫn của bài thực hành 5-3 "Mã hóa file"

Giải mã File hoặc Thư mục

Khi bạn mở file đã được mã hóa, EFS tự động phát hiện file mã hóa, tìm giấy xác thực người dùng và khóa riêng kết hợp với file trong phần đầu (***header***) của file. Khóa riêng này áp dụng cho DDF để mở khóa cho danh sách các khóa mã hóa file. Điều này cho phép nội dung file được hiển thị dưới dạng đọc được.

Truy nhập vào các file mã hóa bị từ chối với bất cứ người khác ngoại trừ người sở hữu khóa riêng, và bạn không thể chia sẻ file mã hóa. Chỉ có người sở hữu của file và tác nhân phục hồi mới có thể giải mã file. Kể cả khi người quản trị thay đổi cấp phép hoặc thuộc tính của file, lấy quyền sở hữu của file thì họ vẫn không thể đọc được nội dung file trừ khi họ có khóa riêng hoặc là tác nhân phục hồi.

Sử dụng tiện ích Cipher

Windows Server 2003 cũng có tiện ích dòng lệnh để cung cấp nhiều hơn các chức năng cho một số các quá trình quản trị. Tiện ích ***Cipher*** có thể mã hóa và giải mã một số lượng lớn các file và folder từ dấu nhắc lệnh bằng cách sử dụng kí tự đại diện *****. ***Cipher*** cũng có thể sử dụng để ghi đè lên các dữ liệu đã bị xóa.

Cấu trúc của câu lệnh ***Cipher*** được liệt kê dưới đây:

cipher [/e|/d] [/s:folder_name] [/a] [/i] [/f] [/q] [/h] [/k] [path_name [...]]

Bảng 5-7 mô tả các lựa chọn khi bạn sử dụng câu lệnh ***Cipher***

Bảng 5-7 Các lựa chọn của lệnh Cipher

Các lựa chọn	Mô tả
/e	Mã hóa thư mục chỉ định. Sau khi mã hóa thư mục các file

	thêm vào thư mục này sẽ được mã hóa.
/d	Giải mã thư mục chỉ định. Sau khi giải mã thư mục các file thêm vào thư mục này sẽ không được mã hóa.
/s	Thực hiện câu lệnh chỉ định trên thư mục và cả các thư mục con bên trong nó.
/a	Bao gồm cả file và thư mục khi thực hiện câu lệnh.
/i	Tiếp tục thực hiện câu lệnh ngay cả khi có lỗi xảy ra. Theo mặc định Cipher sẽ không thực hiện tiếp khi có lỗi xảy ra.
/f	Bắt buộc quá trình mã hóa trên tất cả các file chỉ định, kể cả các file đã được mã hóa. Theo mặc định các file đã mã hóa sẽ được bỏ qua khi chúng ta thực hiện mã hóa nhiều file
/q	Chỉ ghi lại các thông tin cần thiết nhất.
/h	Bao gồm cả các file ẩn và file hệ thống.
/k	Tạo ra file khóa mã hóa mới cho người sử dụng chạy tiện ích cipher. Nếu sử dụng lựa chọn này, Cipher sẽ loại bỏ các lựa chọn khác.
path_name	chỉ ra đường dẫn tới file và thư mục

Nếu bạn sử dụng lệnh ***Cipher*** mà không có các lựa chọn thêm, nó sẽ hiển thị tình trạng mã hóa của thư mục hiện thời và bất cứ file nào bên trong thư mục này. Bạn có thể chỉ định nhiều file một lúc bằng cách sử dụng kí tự đại diện *. Khi sử dụng các lựa chọn của lệnh ***Cipher*** bạn phải đặt các khoảng trống giữa các lựa chọn.

Để mã hóa thư mục ***C:\Test_files*** bạn sử dụng lệnh như sau:

cipher /e Test_files

Để mã hóa các file có cụm từ "***cnfdl***" trong tên file bạn sử dụng lênh sau:

Cipher /e /s *cnfdl*

Khôi phục lại các file mã hóa

Nếu người sở hữu khóa riêng không còn tồn tại, tác nhân phục hồi có thể mở các file bằng khóa riêng của họ, khóa riêng này áp dụng cho DRF để mở khóa danh sách các file khóa mã hóa. Khi khôi phục các file mã hóa, nên gửi file này tới máy tính của tác nhân phục hồi hơn là sử dụng khóa của tác nhân phục hồi tại nơi lưu trữ ban đầu của file. Khi chép các khóa riêng tới các máy tính khác sẽ không đáp ứng tốt cho việc bảo mật trong thực tiễn.

Theo mặc định, các quản trị miền là các tác nhân phục hồi. Tài khoản quản trị cục bộ là tác nhân phục hồi mặc định trên các máy tính đơn (***stand-alone***). Nếu cần thêm tác nhân phục hồi, bạn phải tạo ra và áp dụng các giấy xác thực, gán cho người sử dụng các giấy xác thực này và sử dụng ***Group Policy*** để chỉ định tác nhân phục hồi cho các giấy xác thực kể trên.

> ***THÔNG TIN THÊM Về Group Policy*** *xem chương 7 "Tổng quan về Group Policy" của quyển sách Lập kế hoạch, Thực hiện và Duy trì Cơ sở Hạ tầng Microsoft Windows Server 2003 Active Directory (Microsoft Press 2004).*

Thay đổi các tác nhân phục hồi là việc làm rất tốt trong thực tiễn bảo mật. Tuy nhiên nếu tác nhân phục hồi đã chỉ định bị thay đổi, truy nhập vào file sẽ bị từ chối. Vì vậy bạn cần giữ lại tất cả các giấy chứng nhận và khóa riêng cho đến khi tất cả các file mã hoá sử dụng kết hợp với chúng hoàn thành việc cập nhật.

Để khôi phục các file và thư mục đã mã hóa, tác nhân phục hồi đã chỉ định cần tiến hành các bước sau:

1. Sử dụng NTBackup hoặc các công cụ sao lưu khác để khôi phục từ phiên bản sao lưu các file và thư mục của người sử dụng đã mã hóa vào máy tính lưu trữ giấy chứng nhận khôi phục file của người sử dụng.

2. Trong Windows Explorer mở hộp thoại ***Properties*** của file và thư mục sau đó nhấn ***Advanced*** trong thẻ ***General***.

3. Xóa lựa chọn Encrypt Content to Secure Data.

4. Tạo ra phiên bản sao lưu của file và thư mục đã giải mã và trả lại phiên bản sao lưu cho người sử dụng.

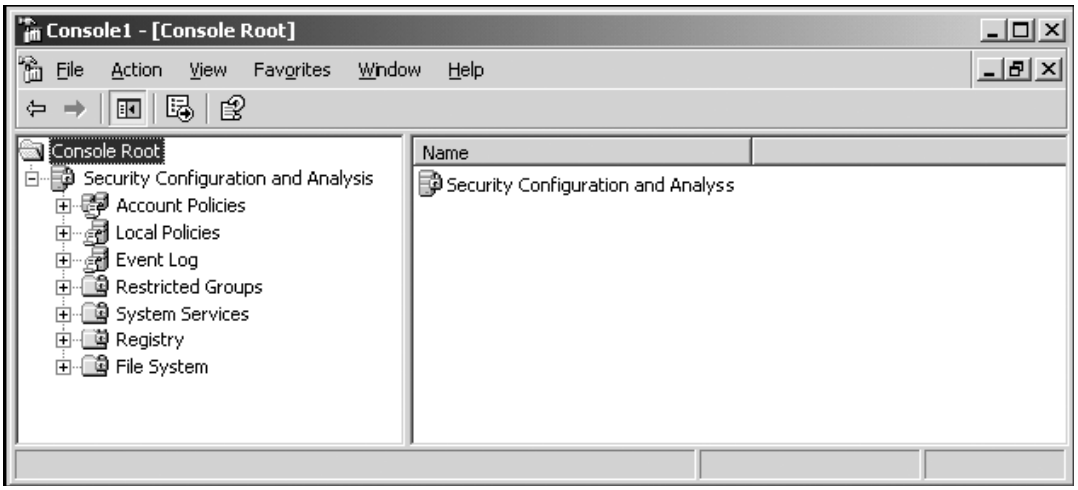
SỬ DỤNG CÁC CÔNG CỤ CẤU HÌNH BẢO MẬT

Windows Server 2003 cung cấp một tập hợp các công cụ cấu hình bảo mật nhằm làm đơn giản hơn các quá trình bảo mật trên mạng và các công việc phân tích và kiểm soát bảo mật trên mạng. Các công cụ này là các snap-in MMC và các tiện ích dòng lệnh. Các công cụ này giúp cho bạn có thể thực hiện các mức độ bảo mật thích hợp cho tổ chức của bạn và giúp bạn luôn duy trì mức bảo mật này. Các thiết lập bảo mật bao gồm các chính sách bảo mật (chính sách tài khoản và chính sách cục bộ), điều khiển truy cập (dịch

vụ, file và registry), nhật ký sự kiện, quan hệ thành viên nhóm (***restricted group***), chính sách IPSec và chính sách khóa công khai. Các công cụ cấu hình bảo mật gồm ba snap-in và một tiện ích dòng lệnh: snap-in ***Security Configuration And Analysis***, snap-in ***Security Templates***, snap-in ***Group Policy*** và tiện ích dòng lệnh ***Secedit***.

Snap-In Security Configuration And Analysis

Security Configuration And Analysis là một snap-in MMC cho phép người quản trị có thể kiểm tra và cấu hình các thiết lập trên máy tính hiện thời với một hoặc nhiều các mẫu bảo mật lưu trữ trong cơ sở dữ liệu (Hình 5-5)



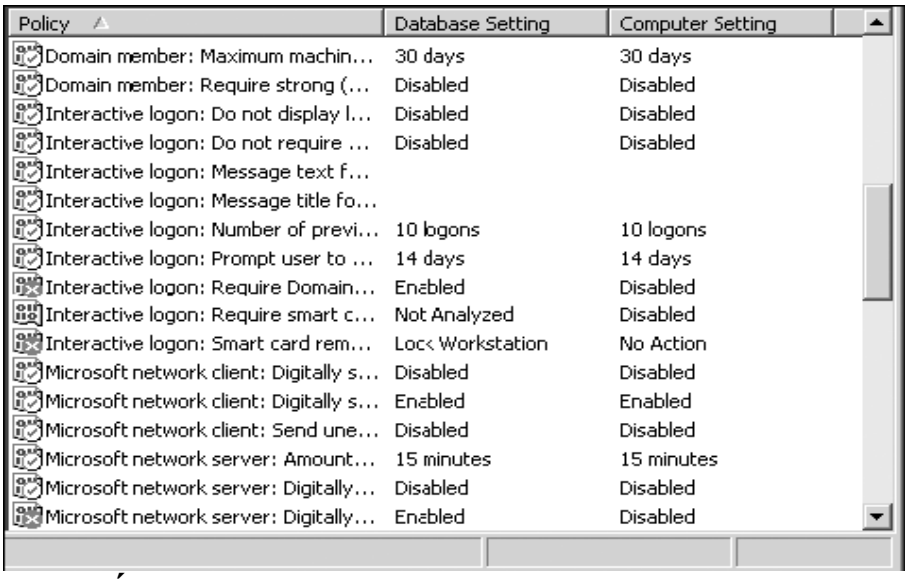
Hình 5-5 Snap-In Security Configuration And Analysis

Các mẫu bao gồm các thiết lập cho từng thuộc tính bảo mật của hệ thống. Khi chúng được nhập vào cơ sở dữ liệu của ***Security Configuration And Analysis,*** các thiết lập hiện thời có thể phân tích và cấu hình cho phù hợp với toàn bộ mẫu nhập vào hoặc chúng có thể cấu hình từng phần. Khi tất cả các thiết lập đã được xác định, chúng có thể xuất ra và áp dụng cho các máy tính khác, từ đó sẽ làm đơn giản hơn các quá trình áp dụng các chính sách bảo mật cho tổ chức.

Security Configuration And Analysis hiển thị các khuyến nghị ngay bên cạnh các thiết lập hiện thời của hệ thống và sử dụng các biểu tượng (xem Bảng 5-8) hoặc đánh dấu các vùng trong thiết lập hiện thời không phù hợp với mức bảo mật đề xuất. ***Security Configuration And Analysis*** cũng giúp cho chúng ta cách giải quyết bất kỳ sự không thống nhất nào mà quá trình phân tích phát hiện ra.

Bảng 5-8 Các biểu tượng của Security Configuration And Analysis

Biểu tượng	Ý nghĩa
Chữ X đỏ	Chính sách này được định nghĩa trong cơ sở dữ liệu phân tích và hệ thống nhưng giá trị không giống nhau
Đánh dấu xanh	Chính sách này được định nghĩa trong cơ sở dữ liệu phân tích và hệ thống và có giá trị giống nhau
Dấu chấm hỏi	Chính sách này không được định nghĩa trong cơ sở dữ liệu phân tích và vì vậy không được phân tích. Nếu chính sách này không được phân tích, nó có thể không được định nghĩa trong cơ sở dữ liệu phân tích hoặc người sử dụng đang tiến hành phân tích không có đủ quyền trên đối tượng hoặc vùng chỉ định này.
Dấu chấm than	Chính sách này được định nghĩa trong cơ sở dữ liệu phân tích nhưng không tồn tại trên hệ thống. Ví dụ, restricted group có thể được định nghĩa trên cơ sở dữ liệu phân tích nhưng không tồn tại trên hệ thống được phân tích
Không tô sáng	Chính sách không được định nghĩa trong cơ sở dữ liệu phân tích hoặc trên hệ thống



Hình 5-6 Kết quả sau khi sử dụng Security Configuration And Analysis

Cấu hình bảo mật

Snap-in ***Security Configuration And Analysis*** có thể sử dụng để cấu hình bảo mật hệ thống cục bộ bằng cách thay đổi trực tiếp các thiết lập hoặc nhập vào và áp dụng các mẫu bảo mật (tạo ra từ ***Security Templates***) cho GPO của máy tính cục bộ. Trong một số trường hợp khác, các thiết lập bảo mật hệ thống được cấu hình với các mức chỉ định trong snap-in hoặc sử dụng mẫu.

Phân tích bảo mật

Theo định nghĩa tăng mức bảo mật nghĩa là tăng độ phức tạp và như vậy sẽ tăng các vấn đề khi truy nhập tài nguyên trên hệ thống. Khi người sử dụng không thể truy nhập vào tài nguyên hệ thống bởi vì các vấn đề bảo mật, giải pháp thường sử dụng đó là nới lỏng bảo mật. Mặc dù nới lỏng bảo mật có thể giải quyết nhanh vấn đề này nhưng nó cũng có thể làm cho tổ chức của bạn gặp rủi ro về bảo mật. Việc đi ngược lại các chính sách bảo mật thường xuyên sẽ làm cho chúng ta quên và không quan sát được cho đến khi bị tấn công. Để tránh điều này và một số trường hợp khác gây ra các lỗ hổng bảo mật, sử dụng công cụ ***Security Configuration And Analysis*** để phân tích các thiết lập bảo mật trên máy tính dựa vào các mẫu bảo mật đã được thiết kế cho các thiết lập bảo mật phù hợp.

Sử dụng Snap-In Security Configuration And Analysis

Người quản trị có thể sử dụng snap-in để có thể thay đổi các chính sách bảo mật và phát hiện các thiếu sót bảo mật đang tồn tại trong hệ thống. Snap-In ***Security Configuration And Analysis*** cho phép bạn có thể thực hiện các tác vụ sau:

- Phân tích bảo mật hệ thống bằng cách so sánh các thiết lập bảo mật hiện thời với các thiết lập được đưa ra trong một hoặc nhiều mẫu bảo mật.
- Xem lại kết quả phân tích bảo mật.
- Cấu hình bảo mật hệ thống bằng cách áp dụng một hoặc nhiều mẫu bảo mật.
- Sửa đổi cấu hình bảo mật cơ sở
- Nhập và xuất các mẫu bảo mật

Lưu ý *Thực hành sử dụng Snap-In Security Configuration And Analysis theo hướng dẫn của bài thực hành 5-5 "Sử dụng Snap-In Security Configuration And Analysis"*

Tiện ích Secedit

Secedit là phiên bản dòng lệnh của Snap-In ***Security Configuration And Analysis***; cũng tương tự như Snap-In, ***Secedit*** cấu hình và phân tích bảo mật hệ thống bằng cách so sánh cấu hình hiện thời với ít nhất một mẫu bảo mật. ***Secedit*** rất tiện dụng khi bạn cần phân tích hoặc cấu hình bảo mật trên nhiều máy tính và khi bạn cần tiến hành tác vụ ***Secedit*** trong thời gian nghỉ. Dưới đây là cú pháp của ***Secedit*** (6 phần) và Bảng 5-9 chỉ ra từng thiết lập tương ứng.

secedit /configure /db *FileName* [/cfg *FileName*] [/overwrite][/areas *Area1 Area2* ...] [/log *FileName*] [/quiet]

secedit /analyze /db *FileName*.sdb [/cfg *FileName*] [/overwrite] [/log *FileName*] [/quiet]

secedit /import /db *FileName*.sdb /cfg *FileName*.inf [/overwrite] [/areas *Area1 Area2* ...] [/log *FileName*] [/quiet]

secedit /export [/DB FileName] [/mergedpolicy] [/CFG FileName] [/areas Area1 Area2 ...] [/log FileName] [/quiet]

secedit /validate *FileName*

secedit /GenerateRollback /CFG *FileName*.inf /RBK S*ecurity Template filename*.inf [/log *RollbackFileName*.inf] [/quiet]

Bảng 5-9 Cú pháp Secedit

Thiết lập	Mô tả	Chú thích
configure	Áp dụng các thiết lập bảo mật từ mẫu	Không bao giờ sử dụng thiết lập này trước khi tạo ra bản sao lưu các thiết lập bảo mật có sẵn. Nếu bạn phát hiện thấy các mẫu bảo mật bị lỗi hoặc phát sinh vấn đề, bản sao lưu sẽ được sử dụng để giúp bạn quay lại các cấu hình bảo mật trước đó.
analyze	So sánh các thiết lập bảo mật có sẵn trong cơ sở dữ liệu của mẫu bảo mật với các thiết lập hiện thời trên máy tính.	Sử dụng thiết lập này để kiểm soát các thiết lập bảo mật hiện thời.

import	Nhập mẫu vào cơ sở dữ liệu	Khi bạn sử dụng thiết lập này để nhập các mẫu bảo mật vào cơ sở dữ liệu thì những thiết lập chỉ định trên mẫu sẽ được áp dụng cho hệ thống.
export	Xuất ra mẫu từ cơ sở dữ liệu	Sử dụng thiết lập này để tạo ra mẫu mới kết hợp từ một hoặc nhiều mẫu. Việc này có thể thực hiện đơn giản bằng cách thêm mỗi mẫu vào cơ sở dữ liệu theo thứ tự bạn lựa chọn và sử dụng lệnh Export để tạo ra file mẫu .inf
validate	Xác nhận cú pháp của mẫu.	Sử dụng thiết lập này nếu bạn thêm các thiết lập trực tiếp vào file .inf
Generate -rollback	Tạo ra mẫu ngược lại, mẫu này sẽ loại bỏ hầu hết các thiết lập khi bạn áp dụng	Luôn luôn sử dụng thiết lập này trước khi bạn áp dụng các mẫu mới. Lưu ý không thay đổi ACL trên file và trong registry đã được đặt với mẫu này.
db	Chỉ ra tên của cơ sở dữ liệu được tạo ra hoặc sử dụng	Bạn có thể phải nhập vào đầy đủ đường dẫn đến file.
cfg	Chỉ định tên của mẫu sẽ được sử dụng	Bạn có thể phải nhập vào đầy đủ đường dẫn đến file.
overwrite	Ghi đè bất cứ mẫu đang có trong file bằng mẫu khác.	Sử dụng thiết lập này nếu bạn không muốn kết hợp nhiều mẫu. Nếu các mẫu cũ trong file đã áp dụng các thiết lập bảo mật, sử dụng thiết lập này sẽ không thay đổi các thiết lập bảo mật mà mẫu mới không áp dụng.
log	Chỉ định file nhật ký nhằm ghi lại các lỗi xảy ra.	Thiết lập này luôn ghi lại các lỗi xảy ra. Theo mặc định nếu không chỉ định file nhật ký, hệ thống sẽ sử dụng WINDOWS\Security\Logs\Scesrv.log.
quiet	Chỉ định sẽ không có dữ liệu được hiển thị trên màn hình và không có chú thích về tiên trình cung cấp cho người sử	Khi bạn sử dụng thiết lập này bên trong kịch bản (script), người dùng đã đăng nhập sẽ không biết khi chương trình đang chạy.

	dụng	
areas	Chỉ áp dụng các thiết lập của mẫu cho các vùng chỉ định, các thiết lập khác sẽ bỏ qua.	Các vùng bao gồm, SECURITY POLICY, GROUP_MGMT (các nhóm restricted), USER_RIGHTS, REGKEYS, FILESTORE và SERVICES.
mergedpolicy	Kết hợp và xuất ra các chính sách miền và cục bộ	Thiết lập này ghi lại tất cả các thiết lập bảo mật.
rbk	Chỉ định tên của mẫu bảo mật sẽ được tạo ra.	Thiết lập này chỉ có khi sử dụng thiết lập /generaterollback.

Dưới đây là một số ví dụ của lệnh Secedit:

- Cấu hình máy tính sử dụng mẫu ***foo***:

  secedit /configure /db foo.sdb /cfg foo.inf /log foo.log

- Cấu hình mẫu ***rollback*** cho mẫu ***foo***:

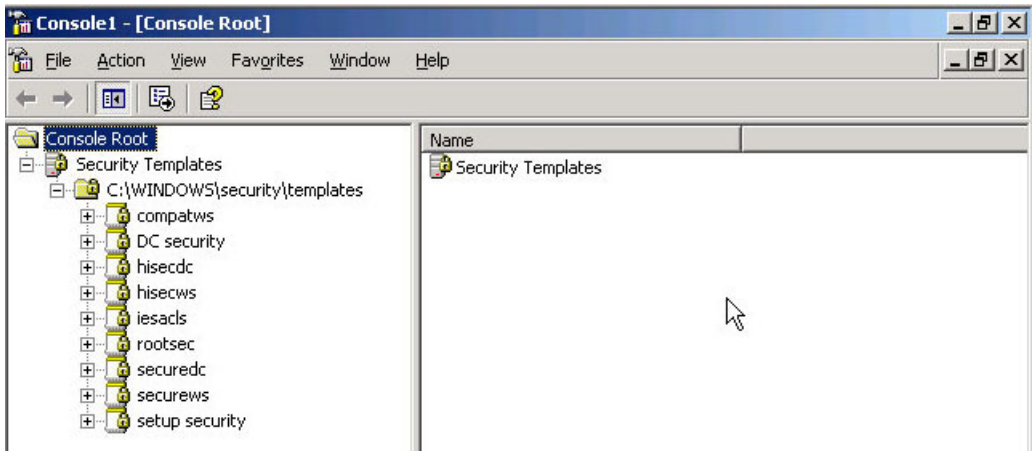
  secedit /generaterollback /cfg foo.inf /rbk foorollback.inf /log foorollback.log

LƯU Ý Sử dụng Gpupdate thay cho secedit /refreshpolicy *Lệnh Secedit /refreshpolicy đã được thay thể bằng lệnh Gpupdate.*

Snap-In Security Templates

Snap-In ***Security Templates*** (Hình 5-7) là công cụ để tạo ra và gán các mẫu bảo mật cho một hoặc nhiều máy tính. Như đã nói từ trước *mẫu bảo mật* là các file vật lý biểu diễn các cấu hình bảo mật.

Khi bạn nhập mẫu bảo mật vào GPO, Group Policy sẽ áp dụng mẫu bảo mật này cho các thành viên bên trong, có thể bao gồm người sử dụng hoặc máy tính.



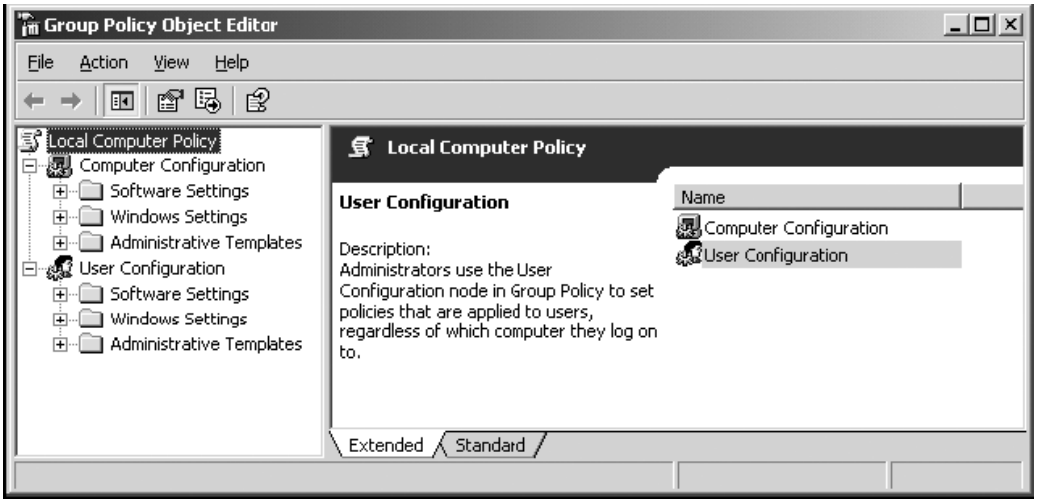
Hình 5-7 Snap-In Security Templates

Snap-In ***Securrity Templates*** cho phép bạn có thể thực hiện được một số tác vụ sau:

- Thay đổi các mẫu bảo mật đã có từ trước
- Tạo ra mẫu bảo mật mới
- Xóa mẫu bảo mật
- Làm mới lại danh sách các mẫu bảo mật
- Đặt các mô tả về mẫu bảo mật

Snap-In Group Policy

Sử dụng Group Policy để định nghĩa và điều khiển các chương trình, tài nguyên mạng và hệ điều hành tương ứng với các người sử dụng và máy tính trong tổ chức. Snap-In **Group Policy Object Editor** (Hình 5-8) sử dụng Active Directory để cấu hình bảo mật tập trung. Người quản trị sử dụng phần ***Security Settings*** của ***Computer Configuration*** và ***User Configuration*** để đặt các chính sách có thể giới hạn người sử dụng truy cập vào file và thư mục, số lần người sử dụng có thể nhập sai mật khẩu trước khi bị khóa, cấp quyền cho người sử dụng chẳng hạn như người sử dụng có thể đăng nhập vào máy quản trị miền.



Hình 5-8 Snap-In Group Policy Object Editor

Gpupdate

Gpupdate làm mới các chính sách thiết lập trên máy cục bộ và các thiết lập chính sách lưu trữ trong Active Directory, bao gồm cả các thiết lập bảo mật. Sau khi bạn thay đổi các chính sách, bạn muốn chúng được áp dụng ngay lập tức thay vì đợi đến thời gian cập nhật theo mặc định (90 phút trên các máy thành viên của Miền, 5 phút trên máy quản trị miền) hoặc khởi động lại máy tính. Để thực hiện được điều này bạn chạy tiện ích ***Gpupdate*** tại dấu nhắc lệnh. Câu lệnh này thay thế lựa chọn ***/refreshpolicy*** của lệnh ***Secedit***. Cú pháp dưới đây và Bảng 5-10 mô tả các tham biến của lệnh ***Gpupdate.***

gpupdate [/target: {computer | user }] [/force] [/wait: Value] [/logoff] [/boot]

Bảng 5-10 Các tham biến của Gpupdate

Tham biến	Mô tả
/target: {*computer* | *user*}	Chỉ tiến hành cập nhật các thiết lập về máy tính hoặc các thiết lập về người sử dụng hiện thời. Theo mặc định sẽ cập nhật đồng thời các thiết lập về máy tính và các thiết lập người sử dụng.
/force	Áp dụng lại tất cả các thiết lập chính sách. Theo mặc định chỉ áp dụng các chính sách đã được thay đổi.
/wait:*value*	Số giây mà việc cập nhật chính sách chờ đợi để hoàn thiện. Mặc định là 600 giây; bằng 0 là không chờ, và bằng –1 là chờ không giới hạn.
/logoff	Đăng xuất sau khi hoàn thành việc làm mới. Lựa chọn này yêu cầu khi thực hiện một số chính sách dành cho máy trạm không được cập nhật ở mức nền tảng (background) mà chỉ được cập nhật khi người sử dụng đăng nhập như là Group Policy Software Installation và Folder Redirection của người

	sử dụng. Lựa chọn này sẽ không có tác dụng nếu không một chính sách thiết lập nào yêu cầu người sử dụng đăng xuất.
/boot	Khởi động lại máy tính sau khi hoàn thành quá trình làm mới. Lựa chọn này yêu cầu khi thực hiện một số chính sách dành cho máy trạm không được cập nhật ở mức nền tảng (background) mà chỉ được cập nhật khi máy tính khởi động lên như là Group Policy Software Installation của máy tính. Lựa chọn này sẽ không có tác dụng nếu không một chính sách thiết lập nào yêu cầu máy tính khởi động lại..
/?	Hiển thị phần trợ giúp tại dấu nhắc lệnh.
/synch	Yêu cầu chính sách ứng dụng kế tiếp sẽ xảy ra một cách đồng thời. Bạn có thể chỉ định cho người sử dụng, máy tính hoặc cả hai bằng cách sử dụng tam biến /target. Tham biến /wait và /force sẽ bị loại bỏ khi sử dụng tham biến /synch.

Sử dụng Microsoft Baseline Securrity Analyzer (MBSA)

MBSA là một công cụ rất mạnh để kiểm tra các thiết lập bảo mật của nhiếu máy tính. Thông thường đây là công cụ đầu tiên bạn nên sử dụng để kiểm tra lại tình trạng bảo mật của các máy tính trên mạng của bạn.

- **Sử dụng MBSA**

1. Để sử dụng MBSA, tiến hành theo các bước sau
2. Tải và cài đặt chương trình từ web site bảo mật của Microsoft theo liên kết *http://www.microsoft.com/technet/security/tools/mbsahome.mspx*
3. Khởi động chương trình từ thực đơn ***Start*** hoặc từ màn hình nền
4. Nhấn vào liên kết ***Scan a Computer*** để quét một máy tính, hoặc nhấn vảo liên kết ***Scan More Than One Computer*** để quét nhiều máy tính.
5. Chỉ định địa chỉ IP hoặc dải địa chỉ của một hoặc nhiều máy tính mà bạn muốn quét và sau đó nhấn ***Start Scan.***
6. Kiểm tra lại kết quả, xem hình 5-9 và sau đó nhấn vào các liên kết để xem từng kết quả cụ thể hơn.

Hình 5-9 Kết quả của MBSA

TỔNG KẾT

- Windows Server 2003 cung cấp một tập các công cụ cấu hình bảo mật cho phép bạn cấu hình các thiết lập bảo mật và tiến hành phân tích hệ thống một cách thường xuyên để đảm bảo rằng các cấu hình vẫn giữ nguyên hoặc thay đổi nếu cần thiết.
- Nguyên lý của cấp quyền tối thiểu là bạn không nên cấp quyền cho người sử dụng hoặc đối tượng truy nhập thông tin và tài nguyên nhiều hơn mức cần thiết.
- Snap-In ***Security Configuration And Analysis*** cho phép bạn cấu hình và phân tích bảo mật hệ thống cục bộ. Nó cho phép xem lại và phân tích các thiết lập bảo mật hiện thời và các khuyến nghị thay đổi thiết lập hiện thời của hệ thống.
- Snap-In ***Security Templates*** cho phép bạn tạo ra và gán các mẫu bảo mật cho một hoặc nhiều máy tính.
- Snap-In ***Group Policy Object Editor*** cho phép bạn cấu hình bảo mật tập trung lưu trữ trong Active Directory.

BÀI TẬP

LƯU Ý Hoàn thành tất cả các bài tập *Nếu bạn định làm bất cứ bài tập nào trong chương này, bạn phải làm tất cả các bài tập trong chương để máy tính của bạn có thể quay lại tình trạng ban đầu cho phép bạn có thể thực hành theo hướng dẫn của sách Bài Tập Thực Hành.*

Bài tập 5-1: Cấp quyền cho người sử dụng

Trong bài tập này bạn sẽ cấp quyền ***Add WorkStations To The Domain*** cho nhóm ***Authenticated Users***.

1. Nhấn ***Start***, chỉ vào ***Administrative Tools*** và nhấn ***Domain Security Policy.***
2. Mở Security Settings, mở Local Policies, nhấn User Rights Assignment.

3. Bên khung chi tiết bên phải, nhấn đúp vào ***Add WorkStation To Domain***.

4. Trong hộp thoại Add WorkStation To Domain Properties, nhấn Define These Policy Settings.

5. Nhấn Add User Or Group.

6. Trong hộp thoại Add User Or Group, trong hộp User And Group Names, nhập authenticated users và sau đó nhấn OK.

Bài tập 5-2: Xem các sự kiện

Trong bài tập này, bạn sẽ cấu hình các thiết lập kiểm soát để lưu lại các sự kiện trong nhật ký kiểm soát và sau đó bạn sẽ xem nó.

Để cấu hình kiểm soát, tiến hành theo các bước sau:

1. Nhấn Start, chỉ vào ***Administrative Tools***, và sau đó nhấn ***Domain Controller Security Policy.***

2. Trong MMC ***Domain Controller Security Settings Policy***, mở ***Security Settings***, mở ***Local Policies*** và sau đó nhấn ***Audit Policy.***

3. Trong khung chi tiết, nhấn đúp vào ***Audit Logon Events***.

4. Trên cửa sổ ***Audit Logon Events Properties***, nhấn ***Define These Policy Settings,*** nhấn ***Success, Failure*** và sau đó nhấn ***OK***.

5. Đóng MMC ***Domain Controller Security Settings Policy***.

6. Nhấn ***Start*** và sau đó nhấn ***Command Prompt***.

7. Để bắt buộc các thiết lập chính sách có kết quả ngay tức khắc, tại dấu nhắc lệnh nhập **gpupdate /force** và sau đó nhấn ***Enter***.

8. Thông báo quá trình làm mới đã hoàn thành sẽ xuất hiện. Đóng cửa sổ lệnh.

9. Đăng xuất.

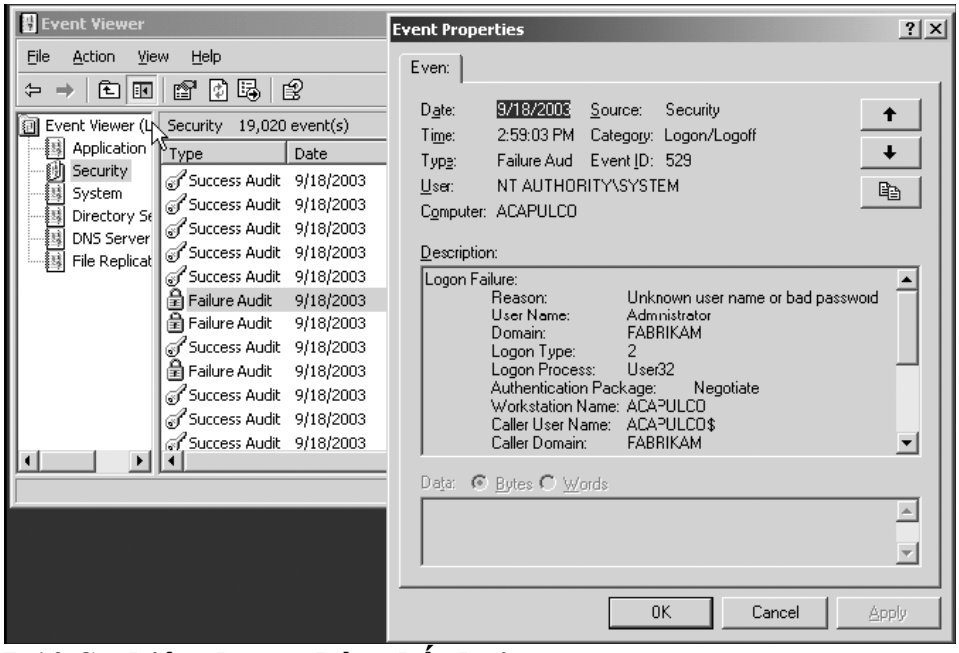
10. Thử đăng nhập vào máy chủ bằng tài khoản ***Administrator*** và nhập sai mật khẩu.

11. Đăng nhập vào bằng tài khoản ***Administrator*** và nhập đúng mật khẩu.

12. Nhấn ***Start***, chỉ vào ***Administrative Tools,*** và sau đó nhấn Eve***n***t ***Viewer***.

13. Trong MMC ***Event Viewer*** nhấn ***Security***.

14. Trong khung chi tiết, tìm sự kiện kiểm soát thất bại (***failed***) do sự đăng nhập không thành công của tài khoản ***Administrator***. Sự kiện kiểm soát thất bại này và chi tiết của nó được hiển thị trong Hình 5-10.



Hình 5-10 Sự kiện đăng nhập thất bại

Bài tập 5-3: Mã hóa File

Trong bài tập này bạn sẽ sử dụng Windows Explorer để mã hóa file.

1. Mở Windows Explorer.
2. Trong cây thư mục, nhấn ***Desktop***.
3. Trên thực đơn ***File***, chỉ vào ***New*** và sau đó nhấn ***Folder***.
4. Đặt tên thư mục này là ***My Encrypted Files.***
5. Tại ***desktop***, trên thực đơn ***File***, chỉ vào ***New*** và sau đó nhấn ***Text Document***.

6. Đặt tên file này là ***PasswordFile.txt.***
7. Mở file này sau đó cập nhật dữ liệu vào file.
8. Ghi sau đó đóng file này lại.
9. Sử dụng Windows Explorer, nhấn chuột phải vào thư mục ***My Encrypted Files*** sau đó nhấn ***Properties***.
10. Trong thẻ ***General***, nhấn ***Advanced***.
11. Trên cửa sổ Advanced Attributes, chọn Encrypt Contents To Secure Data, và sau đó nhấn OK.
12. Đóng cửa sổ My Encrypted Files Properties bằng cách nhấn OK.
13. Thư mục ***My Encrypted Files*** sẽ có màu khác, biểu diễn nó đã được mã hóa.
14. Kéo PasswordFile.txt vào thư mục My Encrypted Files.
15. Mở thư mục My Encrypted Files.
16. Lưu ý màu của ***PasswordFile.txt*** sẽ được thay đổi và đó là do nó đã được mã hóa.

Bài tập 5-4: Giải mã File

Trong bài tập này bạn sẽ sử dụng Windows Explorer để giải mã file.

1. Mở Windows Explorer.
2. Nhấn chuột phải vào thư mục ***My Encrypted Files***, và sau đó nhấn ***Properties***.
3. Trong thẻ ***General*** nhấn ***Advanced***.
4. Trong cửa sổ ***Advanced Attribute***, xóa dấu chọn tại hộp kiểm tra ***Encrypt Contents To Secure Data***, và sau đó nhấn ***OK***.
5. Đóng cửa sổ ***My Encrypted Files Properties*** bằng cách nhấn OK.
6. Trong hộp thoại Custom Attribute Changes, đảm bảo rằng Apply Changes To This Folder, Subfolders, And Files đã được chọn và sau đó nhấn OK.

My Encrypted Files và ***PasswordFile.txt*** sẽ không có màu khác nữa, chứng tỏ nó đã không còn được mã hóa.

Bài tập 5-5: Sử dụng Snap-In Security Configuration And Analysis

Trong bài tập này, bạn sẽ sử dụng công cụ Security Configuration And Analysis, để nhập các mẫu bảo mật và thực hiện phân tích các thiết lập hiện thời trên máy tính so với mẫu bảo mật này.

1. Nhấn ***Start***, nhấn ***Run***, nhập **mmc** và sau đó nhấn ***OK***.
2. Trên thực đơn file, nhấn ***Add/Remove Snap-in.***
3. Trong cửa sổ ***Add/Remove Snap-in***, nhấn ***Add***.
4. Trong hộp thoại Add Standalone Snap-in, nhấn Security Configuration And Analysis, nhấn Add, và sau đó nhấn Close.
5. Trong cửa sổ ***Add/Remove Snap-in***, nhấn ***OK***.
6. Trên thực đơn File, nhấn ***Save***.
7. Trong hộp thoại ***Save As,*** phần ***File Name*** nhập **sca** sau đó nhấn ***Save***.

Phân tích bảo mật của hệ thống

Để phân tích bảo mật của hệ thống tiến hành theo các bước sau:

1. Sử dụng MMC ***Security Configuration And Analysis***, nhấn chuột phải vào ***Security Configuration And Analysis,*** sau đó nhấn ***Open Database.***
2. Trong cửa sổ ***Open Database***, phần ***File Name*** nhập ***scadb***, và sau đó nhấn ***Open***.
3. Trong cửa sổ ***Import Template,*** nhấn ***securedc.inf*** và sau đó nhấn ***Open***
4. Trên cửa sổ cây công cụ, nhấn chuột phải vào ***Security Configuration And Analysis*** sau đó nhấn ***Analyze Computer Now***.
5. Trong hộp thoại ***Perform Analysis***, nhấn ***OK*** để đồng ý với đường dẫn mặc định để lưu trữ file nhật ký khi bị lỗi.

6. Mở Security Configuration And Analysis, mở Local Policies và sau đó nhấn Security Options.

7. Trong khung chi tiết, xem lại các chính sách đã được phân tích. Phần này sẽ cho chúng ta kết quả của việc so sánh giữa các thiết lập hiện thời và các thiết lập trong cơ sở dữ liệu.

CÂU HỎI *Liệt kê một số thiết lập cấu hình giống nhau giữa cơ sở dữ liệu và trên máy tính.*

CÂU HỎI *Liệt kê một số thiết lập cấu hình khác nhau giữa cơ sở dữ liệu và trên máy tính.*

CÁC CÂU HỎI KIỂM TRA

1. Bạn hay cho biết trong các lựa chọn dưới đây, lựa chọn nào là quyền của người sử dụng (***user rights***)?
   a. Allow log on locally
   b. Access a share with full control
   c. Open a database file
   d. Back up files and directories
2. Người quản trị tạm thời cấp quyền cho người sử dụng đănh nhập vào máy chủ quản trị miền bằng cách áp dụng chính sách(GPO) trên miền. Người quản trị không thêm người sử dụng vào bất cứ nhóm nào khác. Khi người sử dụng đăng nhập, Windows Server 2003 hiển thị lỗi sau: "***User does not have the right to log on interactively***." Hãy cho biết nguyên nhân chủ yếu nhất gây ra vấn đề này?
3. Bạn là quản trị hệ thống và có nhiệm vụ tạo ra, cấu hình và quản lý GPO cho tổ chức của bạn. Các kỹ sư hệ thống đưa cho bạn kế hoạch, và bạn phải xác định bạn có thể sử dụng các mẫu mặc định được hay không. Bạn hãy cho biết trong các mẫu Group Policy mặc định dưới đây, mẫu nào cung cấp các thiết lập bảo mật cao nhất cho máy trạm?
   a. Rootsec
   b. Hisecws
   c. Securews
   d. Compatws
4. Bạn là quản trị hệ thống và có nhiệm vụ tạo ra, cấu hình và quản lý GPO cho tổ chức của bạn. Bạn phải xác định các thiết lập nào trên máy quản trị miền không đúng với các chính sách bảo mật đã được áp dụng bằng cách sử dụng mẫu chỉ định. Công cụ nào dưới đây bạn có thể sử dụng để thực hiện điều này?
   a. Domain Security Policy
   b. Security Configuration And Analysis snap-in
   c. Group Policy Management
   d. Active Directory Users And Computers
5. Bạn là quản trị hệ thống và có nhiệm vụ tạo ra, cấu hình và quản lý GPO cho tổ chức của bạn. Trước khi bạn có thể xác định các thiết lập của Group Policy bạn phải áp dụng từng GPO, bạn phải xác định các kiểu thiết lập của Group Policy mà bạn có thể cấu hình. Những kiểu thiết lập nào của Group Policy dưới đây bạn có thể cấu hình trong môi trường Active Directory? Có thể chọn tất cả nếu bạn thấy đúng.
   a. Desktop settings
   b. Network connections
   c. Location of computers
   d. Inventory-installed software
   e. Who can log on to a computer and when

CÁC BÀI TẬP TÌNH HUỐNG

Tình huống 5-1: Chuyển hướng thư mục (Folder Redirection)

Bạn là quản trị hệ thống của Contoso, Ltd., và bạn muốn lưu trữ tập trung dữ liệu của người sử dụng bằng cách sử dụng ***Folder Redirection***. Cụ thể, bạn muốn cấu hình chuyển hướng thư mục cho thư mục My Documents vào thư mục cá nhân(Home Directory) của từng người sử dụng. Người sử dụng nên được dành riêng quyền truy nhập dữ liệu của thư mục My Document của họ. Bạn sẽ làm thế nào để hoàn thành mục đích này? Chọn hai phương án

a. Cấu hình ***GPO*** đặt chính sách ***Folder Redirection*** để chuyển hướng vào thư mục cá nhân của người sử dụng, và liên kết với ***OU*** thích hợp.
b. Cấu hình ***GPO*** đặt chính sách ***Grant The User Exclusive Rights To My Document***s là ***Disabled***, và liên kết với ***OU*** thích hợp.
c. Cấu hình GPO đặt chính sách ***Folder Redirection*** để chuyển hướng vào ***OU*** riêng biệt.
d. Cấu hình GPO đặt chính sách ***Grant The User Exclusive Rights To My Documents*** là ***Enabled***, và liên kết với ***OU*** thích hợp.

Tình huống 5-2: Thực hiện kiểm soát (Auditing)

Một số người thông báo với bạn rất khó truy nhập vào tài nguyên chia sẻ của hai máy File Server trong tổ chức của bạn. Bạn quyết định kiểm tra lại nhật ký kiểm soát của hai máy chủ này để xác định nguyên nhân gây ra hiện tượng này. Khi bạn xem nhật ký sự kiện, bạn nhận thấy trong nhật ký chỉ có các sự kiện trước đó 12 giờ. Điều gì dưới đây có thể gây ra sự thiếu dữ liệu này? Chọn tất cả nếu bạn thấy đúng.

a. Kích thước cực đại của nhật ký sự kiện quá nhỏ.
b. Bạn kiểm soát quá nhiều sự kiện.
c. Thiết lập ***Overwrite Events Older Than [x] Days*** được đặt là ***1*** ngày
d. Người quản trị khác đã xóa nhật ký sự kiện.
e. Các sự kiện liên quan sẽ được lưu lại trên máy chủ quản trị miền, không lưu trên máy chủ thành viên.

CHƯƠNG 6: BẢO MẬT LƯU THÔNG MẠNG VỚI IPSEC

Sau khi hoàn thành chương này, bạn sẽ có khả năng:

- Nhận dạng và giải thích các cấu thành và khái niệm chủ yếu của ***Internet Protocol Security (*IPSec –** *Giao thức bảo mật lớp Internet)* bao gồm các liên kết bảo mật, các giao thức phần ***header***, ***Internet Key Exchange (*IKE –** *Trao đổi khóa internet)*,* vai trò của ***IPSec Policy Agent (****đại lý chính sách bảo mật IP)* và ***IPSec Driver (****Trình điều khiển IPSec)*,* và quá trình dàn xếp bảo mật.

- Hiểu rõ vai trò của các Giao thức ***Authentication Header*** (AH) và ***Encapsulating Security Payload*** (ESP) thực hiện trong việc cung cấp tính riêng tư (***confidentiality***) và xác thực (***authentication***).

- Sử dụng bảng điều khiển **IP Security Policy Management** để thêm hay thay đổi các chính sách bảo mật **IPSec.**

- Xác định khi nào sẽ sử dụng dịch vụ thư mục **Active Directory** hay các Chính sách Cục bộ khi triển khai **IPSec.**

- Sử dụng các công cụ để quản lý, theo dõi, và khắc phục các sự cố **IPSec.** Các công cụ này bao gồm **IP Security Monitor** *(Trình Theo dõi Bảo mật IP***),** bảng điều khiển **IP Security Policy Management (***Quản lý Chính sách bảo mật IP***), Resultant Set of Policy (RSoP –** *Tập Kết quả của Chính sách***), Event Viewer (***Trình Xem các Sự kiện***), Netsh,** và nhật ký **Oakley.**

- Hiểu rõ tại sao bạn nên sử dụng Giấy chứng nhân (C***ertificates***) với **IPSec** để bảo mật các lưu thông mạng**.**

- Mô tả được quá trình cấp Giấy chứng nhận.

- Cấu hình **IPSec** để sử dụng Giấy chứng nhận.

- Giải thích các vấn đề liên quan đến **Network Address Translation (NAT** – *Chuyển đổi Địa chỉ Mạng***)** khi sử dụng **IPSec** và nhận dạng các phương pháp **Microsoft Windows Server 2003** sử dụng để giải quyết các vấn đề trên**.**

- Sử dụng lênh "**Netsh"** để quản lý và theo dõi **IPSec.**

Cho dù bạn dang làm việc trên mạng Internet công cộng hay đang duy trì một mạng riêng, việc bảo mật các dữ liệu của bạn vẫn là các yêu cầu cốt lõi. Chúng ta thường để ý quá nhiều đến việc bảo mật trên đường biên và chống lại những cuộc tấn công từ bên ngoài vào nhưng thường để ý quá ít đến các cuộc tấn công nội mạng, là nơi mà dường như các cuộc tấn công thường xẩy ra hơn.

Một chiến lược bảo mật chắc chắn phải bao gồm nhiều lớp bảo mật được kết hợp với nhau. Các tổ chức cũng thường triển khai các giới hạn để bảo mật đường biên mạng và bảo mật các truy nhập đến các tài nguyên bằng cách thiết lập các kiểm soát truy nhập và xác thực. Mặc dù vậy, việc bảo mật các gói IP thực sự và nội dung của nó vẫn thường bị bỏ qua.

Chương này sẽ đề cập tới việc bảo mật các lưu thông IP bằng cách sử dụng IPSec. chúng ta sẽ bàn luận về mục đích và các tính năng của IPSec, cách xác định và triển khai các chính sách IPSec, và cách làm thể nào để thực thi IPSec bằng cách sử dụng Giấy chứng nhận. Sau khi chúng ta đã giải thích được mục đích của IPSec và cách triển khai chúng như thế nào, chũng ta sẽ học cách quản lý và theo dõi IPSec bằng các công cụ như Trình Theo dõi Bảo mật IP (***IP Security Monitor***), **RSoP**, **Event Viewer**, nhật ký **Oakley**, **Netsh**, và **Netdiag**.

MỤC ĐÍCH CỦA IPSEC

Các ***Header*** (*tiêu đề*) của IP, **Transmission Control Protocol (TCP –***Giao thức Kiểm soát Truyền dẫn***)**, và **User Datagram Protocol (UDP –** *Giao thức gói Dữ liệu Người dùng***)** đều chứa một Số Kiểm soát (***Checksum***) được sử dụng để kiểm soát tính toàn vẹn (***Integrity***) dữ liệu của một gói IP. Nếu dữ liệu bị hỏng, Số Kiểm soát sẽ thông báo cho người nhận biết. Tuy nhiên, do thuật toán Số Kiểm soát này được phổ biến rộng rãi nên kể cả người dùng không có chức năng sẽ dễ dàng truy nhập vào gói tin, thay đổi nội dung của chúng và tính lại Số Kiểm soát, sau đó lại chuyển tiếp gói tin đến tay người nhận mà không một ai, kể cả người gửi lẫn người nhận, biết đến sự can thiệp này. Do các hạn chế về chức năng của Số Kiểm soát như vậy, tại nơi nhận, người dùng không hề biết và cũng không thể phát hiện ra việc gói tin đã bị thay đổi.

Trong quá khứ, các ứng dụng cần bảo mật sẽ tự cung cấp cơ chế bảo mật cho riêng chúng, dẫn tới việc có quá nhiều các chuẩn bảo mật riêng và không tương thích. **IPSec là một bộ các Giao thức và Thuật toán Mã hóa cung cấp khả năng bảo mật tại lớp Internet (*Internet Layer*), mà không**

cần quan tâm đến các ứng dụng gửi hay nhận dữ liệu. Sử dụng IPSec, chỉ một chuẩn bảo mật được áp dụng và việc thay đổi ứng dụng không cần thiết.

IPSec có hai mục đích:

- Bảo vệ nội dung của các gói IP.
- Cung cấp việc bảo vệ chống lại các cuộc tấn công mạng thông qua việc lọc gói tin và việc bắt buộc sử dụng các kết nối tin cậy.

Cả hai mục tiêu trên đều có thể đạt được thông qua việc sử dụng các dịch vụ phòng chống dựa trên cơ sở mã hóa, các giao thức bảo mật và việc quản lý các khóa động. Với các nền tảng như vậy, IPSec cung cấp cả hai tính năng Mạnh và Uyển chuyển trong việc bảo vệ các cuộc liên lạc giữa các máy tính trong mạng riêng, Miền, Site (bao gồm cả các Site truy cập từ xa), các mạng Intranet, các máy khách truy cập qua đường điện thoại. Thạm chí nó còn được sử dụng dể khóa việc nhận hay gửi của một loại lưu thông chuyên biệt nào đó.

Chống lại các cuộc tấn công bảo mật

IPSec bảo vệ dữ liệu, làm cho chúng trở thành quá khó, nếu không nói là không thể, đối với các kẻ xâm nhập để có thể dịch được các dữ liệu mà họ thu giữ được. IPSec có một số các tính năng mà có thể làm giảm đáng kể hay ngăn ngừa được các loại tấn công sau:

- **Do thám gói dữ liệu (Packet sniffing):** ***Packet Sniffer*** là một ứng dụng hay một thiết bị có thể theo dõi và đọc các gói dữ liệu. Nếu gói dữ liệu không được mã hóa, các ***Packet Sniffer*** có thể trình bầy đầy đủ các nội dung bên trong các gói dữ liệu. Chương trình ***Network Monitor*** là một ví dụ của ***Packet Sniffer***. Giao thức ESP trong IPSec cung cấp tính riêng tư cho dữ liệu bằng cách mã hóa phần dữ liệu truyền tải của gói IP.
- **Thay đổi dữ liệu:** Kẻ tấn công có thể thay đổi các thông điệp đang được vận chuyển và gửi đi các dữ liệu giả mạo, nó có thể ngăn cản người nhận nhận được các dữ liệu chính xác, hay có thể cho phép kẻ tấn công lấy được thêm các thông tin bảo mật. IPSec sử dụng các khóa mã hóa, chỉ được chia sẽ giữa người gửi và người nhận, để tạo ra các Số Kiểm soát được mã hóa cho mỗi gói IP. Mọi thay đổi đối với gói dữ liệu đều dẫn đến việc thay đổi Số Kiểm soát và sẽ chỉ ra cho người nhận biết rằng gói dữ liệu đã bị thay đổi trên đường truyền.

- **Nhận dạng giả mạo:** kẻ tấn công có thể làm giả các mã nhận dạng (***Identity Spoofing***) bằng cách sử dụng một chương trình đặc biệt để xây dựng các gói IP mà xuất hiện như các gói dữ liệu gốc từ các địa chỉ hợp lệ bên trong mạng được tin cậy. IPSec cho phép trao đổi và xác nhận lại các mã nhận dạng mà không phơi chúng ra cho các kẻ tấn công dịch. Sự xác nhận lẫn nhau (xác thực) được sử dụng để thiết lập sự tin cậy giữa các hệ thống cũng tham gia liên lạc, và chỉ các hệ thống được tin cậy mới có thể liên lạc với các hệ thống khác. Sau khi các mã nhận dạng được thiết lập, IPSec sử dụng các khóa mã hóa, được chia sẻ chỉ giữa người gửi và người nhận, để tạo các Số Kiểm soát được mã hóa cho mỗi gói IP. Các số kiểm soát được mã hóa đảm bảo rằng chỉ các máy tính đã biết rõ về các khóa là có thể gửi được từng gói dữ liệu.

- **Tấn công ngang đường (man-in-the- middle attack)** trong dạng tấn công này, một người nào đó, đứng giữa hai máy tính đang liên lạc với nhau, sẽ tiến hành theo dõi, thu thập và điều khiển các dữ liệu một cách trong suốt (Ví dụ, kẻ tấn công có thể định tuyến lại các dữ liệu đang trao đổi). IPSec kết hợp việc xác thực lẫn nhau và các khóa được mã hóa để chống lại dạng tấn công này.

- **Tấn công từ chối dịch vụ (DoS):** Kiểu tấn công này ngăn cản việc vận hành bình thường của các tài nguyên mạng và máy tính. Làm lụt các tài khoản E-mail bằng các thôgn điệp không mong muốn là một ví dụ của dạng tấn công này. IPSec sử dụng phương pháp lọc các gói IP (***IP packet Filtering***) làm cơ sở cho việc xác định mối liên lạc nào là được phép, bảo mật hay phải khóa lại. Việc xác định trên dựa vào dẫy địa chỉ IP, Giao thức IP hay thậm chí một số cổng TCP hay UDP xác định nào đó.

TÌM HIỂU IPSEC

Trước khi chúng ta có thể bàn luận về việc IPSec hoạt động như thế nào, và điểm qua các bước cấu hình IPSec, bạn cần phải hiểu rõ về các tính năng, các khái niệm và các cấu thành của khung IPSec.

IPSec là một khung kiến trúc cung cấp các dịch vụ bảo mật mật mã dành cho các gói IP. IPSec là một kỹ thuật bảo mật điểm tới điểm (***end-to-end).*** Điều đó có nghĩa là chỉ có những trạm biết rõ về sự hiện diện của IPSec, chính là hai máy tính sử dụng IPSec đang liên lạc với nhau, là biết rõ về cơ chế bảo mật. Các bộ định tuyến giữa đường không thể biết được quan hệ bảo mật của hai trạm trên và chúng chỉ chuyển tiếp các gói IP như là chúng đã làm với

tất cả các gói IP khác. Mỗi máy tính sẽ điều khiển chức năng bảo mật tại đầu của nó với giả thiết rằng tất cả các trạm ngang đường đều là không bảo mật. Các máy tính chỉ làm nhiệm vụ định tuyến các gói tin từ nguồn đến đích không cần thiết phải hỗ trợ IPSec. Chỉ có một loại trừ là các bộ lọc gói tin dạng ***Firewall*** hay NAT đứng giữa hai máy tính. Với mô hình này, IPSec sẽ được triển khai thành công theo các kịch bản sau:

- **Mạng cục bộ (LAN):** mạng cục bộ dạng Chủ - Khách hay mạng ngang hàng.
- **Mạng diện rộng (WAN):** Mạng WAN giữa các bộ định tuyến (***Router-to-Router***) hay giữa các cổng (***Gateway-to-Gateway***)
- **Truy cập từ xa:** Các máy khách quay số hay truy cập Internet từ các mạng riêng**.**

Thông thường, cả hai đầu đều yêu cầu cấu hình IPSec, hay còn được gọi là Chính sách IPSec, để đặt các tùy chọn và các thiết lập bảo mật cho phép hai hệ thống thỏa thuận việc sẽ bảo mật các lưu thông giữa chúng như thế nào. Các hệ điều hành Windows Server 2000, Windows XP, và Windows Server 2003 thực thi IPSec dựa trên các chuẩn công nghiệp do nhóm IPSec, của IETF (***Internet Engineering Task Force***) phát triển.

Các tính năng bảo mật của IPSec

IPSec có rất nhiều tính năng bảo mật được thiết kế để thỏa mãn mục tiêu bảo vệ các gói IP và chống lại các cuộc tấn công nhờ vào các bộ lọc và cơ chế kết nối tin cậy. Một vài trong các tính năng bảo mật của IPSec được liệt kê sau:

- **Sự kết hợp bảo mật tự động:** IPSec sử dụng **Internet Security Association (***Kết hợp Bảo mật Internet***)** và **Key Management Protocol (ISAKMP –** *Giao thức Quản lý Khóa***)** để thỏa thuận một cách tích cực về một tập của các yêu cầu bảo mật cho cả hai phía giữa các máy tính với nhau. Các máy tình không đòi hỏi phải có các chính sách giống hệt nhau, chúng chỉ cần các chính sách đã được cấu hình các tùy chọn đã được thỏa thuận đủ để thiết lập một tập chung các yêu cầu bảo mật với máy tính kia.
- **Lọc gói IP:** Quá trình lọc này cho phép hay cấm các liên lạc cần thiết bằng cách chỉ định các khoảng địa chỉ IP, các Giao thức, hay thậm chí cả những cổng của giao thức.

- **Bảo mật lớp mạng:** IPSec nằm tại lớp mạng, cung cấp cơ chế bảo mật một cách tự động, trong suốt cho các ứng dụng.

- **Xác thực ngang hàng:** IPSec xác nhận lại mã nhận dạng của máy tính đối tác trước khi có bất cứ một gói dữ liệu nào được chuyển. Việc xác thực đối tác IPSec trong Windows Server 2003 được dựa trên các khóa đã chia sẻ, các khóa công khai (ví dụ như các Giấy chứng nhận ***X509***) hoặc ***Kerberos*** và ***Active Directory.*** Các máy khách bắt buộc phải là thành viên của Miền ***Active Directory*** để được xác thực bằng ***Kerberos***.

- **Xác thực dữ liệu gốc:** Việc xác thực nguồn gốc dữ liệu ngăn cản các người dùng không đúng chức năng khỏi việc can thiệp vào gói tin và khai báo họ là người gửi dữ liệu. Mỗi gói dữ liệu được bảo vệ bằng IPSec bao gồm một Số Kiểm soát bằng mật mã trong định dạng của một giá trị băm có khóa (***Keyed hash***). Số Kiểm soát bằng mật mã cũng còn được biết dưới cái tên ***Integrity Check Value*** (ICV *–Giá trị Kiểm soát tính Nguyên vẹn*) hay ***Hash-based Message Authentication Code*** (HMAC *–Mã xác thực thông điệp được băm nhỏ*). ***Hash*** (*hàm băm*) là loại thuật toán mã hóa một chiều có các thông điệp đầu vào có chiều dài tùy ý và cho ra các đoạn văn bản có chiều dài cố định. ***Keyed Hash*** bao gồm cả khóa bảo mật trong tính toán của nó. Số Kiểm soát bằng mật mã bảo đảm rằng chỉ các máy tính biết rõ về khóa bảo mật là có thể gửi gói dữ liệu. Người sử dụng có ác tâm giả danh như là người gửi gói tin sẽ không thể tính được chính xác Số Kiểm soát bằng mật mã. Nếu Số Kiểm soát bằng mật mã không đúng, người nhận sẽ hủy bỏ gói tin.

- **Tính nguyên vẹn (*Integrrity*) của dữ liệu:** Với việc sử dụng Số Kiểm soát bằng mật mã, IPSec bảo vệ dữ liệu đang vận chuyển không bị sửa đổi bởi các người dùng không được xác thực, hay không phát hiện được trong quá trình vận chuyển, đảm bảo chắc chắn rằng các dữ liệu mà người nhận có được là chính xác các thông tin mà người gửi đã gửi cho mình. Các người sử dụng có ác tâm muốn thay đổi nội dung của gói tin phải cập nhật lại một cách chính xác Số Kiểm soát bằng mật mã, một điều gần như là không thể thực hiện được nếu không biết được các khóa chia sẻ.

- **Tính riêng tư (*Confidentialy*) của dữ liệu**: Các gói dữ liệu khi được gửi là được mã hóa bằng các ký thuật mã hóa khóa bí mật qui ước. Điều này làm cho dữ liệu trở nên riêng tư. Thậm chí ngay cả

khi dữ liệu bị truy nhập và quan sát, kẻ truy nhập cũng chỉ nhìn thấy các dữ liệu đã được mã hóa. Nếu không biết được về các khóa bí mật đã sử dụng để mã hóa dữ liệu thì các dữ liệu gốc vẫn là ẩn. Do khóa bí mật chỉ được chia sẻ giữa người gửi và người nhận, tính riêng tư của dữ liệu đảm bảo rằng chỉ người nhận đã định trước của gói tin là có thể giải mã và trình bầy được gói tin.

- **Tính không lặp**: Bằng cách sử dụng số thứ tự trên mỗi gói tin đã được bảo vệ được gửi giữa các đối tác có sử dụng IPSec. dữ liệu được trao đổi giữa các đối tác không thể bị lập lại để thiết lập các quan hệ bảo mật khác hay nhận được sự truy cập không xác thực đến các thông tin hay tài nguyên.

- **Quản lý khóa**: Việc xác thực nguồn gốc dữ liệu, tính nguyên vẹn, tính riêng tư hoàn toàn phụ thuộc vào các thông tin được chia sẽ của khóa bí mật. Nếu khóa bị tổn thương, liên lạc sẽ không còn là bảo mật nữa. Để giữ các khóa không bị các người sử dụng có ác tâm phát hiện (trừ các phương pháp phát hiện thô bạo như thử tất cả các khả năng kết hợp của khóa cho đến khi xác định được chúng), IPSec cung cấp một phương thức an toàn cho việc trao đổi thông tin khóa để nhận được khóa bảo mật chia sẻ và thay đổi khóa một cách dịnh kỳ cho các liên lạc cần bảo mật.

Các tính năng mới của IPSec trong Windows Server 2003

IPSec được tích hợp vào và có thể sử dụng để bảo vệ các cuộc liên lạc mạng trong Windows 2000, Windows XP Professional, và Windows Server 2003. IPSec hợp lệ dành cho các máy khách cũng có cho các hệ điều hành Microsoft Windows NT 4.0 Microsoft Windows 98, Microsoft Windows Millennium Edition (Me) (Bạn có thể tải phần mềm IPSec máy khách từ địa chỉ
http://www.microsoft.com/windows2000/server/evaluation/news/bulletins
/l2tpclient.asp.). Các tính năng mới của IPSec trong Windows Server 2003 bao gồm:

- Snap-in ***IP Security Monitor*** (*Trình Theo dõi Bảo mật IP*) được cải tiến từ công cụ ***IPSecMon*** có trong Windows 2000 (Snap-in này là mới trong Windows XP Professional và Windows Server 2003).

- Khóa chủ mã hóa mạnh hơn, việc trao đổi khóa Diffie-Hellman 2048-bit được sử dụng.

- Công cụ quản lý dạng dòng lệnh ***Netsh*** cung cấp tính tiện ích, có thêm nhiều khả năng cấu hình không có tại Snap-in ***IP Security Policy Management*** trong phiên bản Windows 2000.

- Việc khởi động máy tính được bảo mật. Nếu máy tính được cấu hình sử dụng các chế độ kết nối trạng thái (***Stateful***), các thông tin đi vào mà được gửi để đáp lại các thông tin máy tính gửi ra sẽ được chấp nhận, như các lưu thông chiều vào đáp ứng được các tiêu chí lọc bạn đã cấu hình, cũng giống như các lưu thông DHCP. Tất cả các thông tin chiều vào khác (bao gồm các gói gủi có địa chỉ (***Unicast***), quảng bá (***Broadcast***), quảng báo có địa chỉ (***Multicast***)) đều bị loại bỏ. Các thông tin chiều vào ở chế độ kết nối trạng thái cho phép các bộ lọc được hủy bỏ sau khi dịch vụ IPSec khởi động và thiết lập chính sách IPSec cố định.

- Chính sách IPSec cố định sẽ được áp dụng trong trường hợp chính sách cục bộ hay chính sách ***Active Directory*** không được áp dụng.

- Chỉ các thông tin IKE là được miễn trừ khỏi các thiết lập của bộ lọc. Sự miễn trừ này là cần thiết trong việc thiết lập mối liên lạc bảo mật.

- Có những hạn chế nhất định sẽ được xác định với những máy tính đươc phép kết nối dựa trên Miền, trên nguồn gốc Giấy chứng nhận, hay trên nhóm máy tính.

- Tên của **Certificate Authority (CA)**, sẽ có thể không bao gồm trong các yêu cầu giấy chúng nhận để tránh việc phát hiện các thông tin trong quan hệ tin cậy của máy tính như Miền, CA và công ty.

- Các cách cung cấp địa chỉ IP một cách Logic sẽ được áp dụng cho việc cấu hình IP cục bộ - như Máy chủ DHCP, ***Domain Name System*** **(DNS)**, và ***Windows Internet Naming Service*** **(WINS).**

- IPSec hoạt động trên NAT cho phép các gói ESP đi qua NAT (với các trạm NAT cho phép các lưu thông UDP đi qua).

- Tính năng tích hợp với ***Network Load Balancing*** – NBL (*Cân bằng tải mạng*) được cải thiện, đem lại các lợi ích cho việc cân bằng tải của dịch vụ VPN dựa trên IPSec.

- Sự hỗ trợ được cung cấp cho Snap-in RSoP giúp ta có thể xem được các thiết lập trong chính sách IPSec.

Các giao thức IPSec cung cấp sự bảo mật dựa trên việc sử dụng kết hợp các giao thức, trong đó có giao thức AH và giao thức ESP. Các giao thức này được sử dụng độc lập hay cái trước cái sau, phụ thuộc vào các yêu cầu của việc giữ tính riêng tư và xác thực.

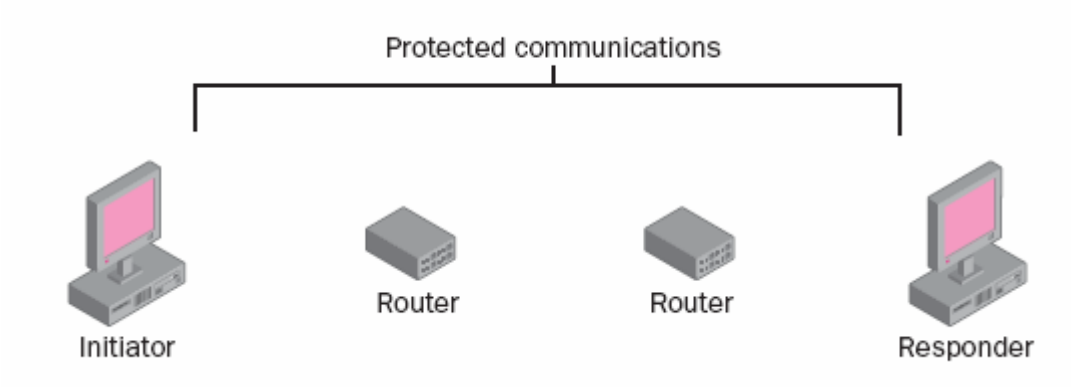
1. Giao thức AH cung cấp tính xác thực, nguyên vẹn và không lặp cho toàn bộ gói tin (gồm cả phần tiêu đề của IP (***IP header***) và các dữ liệu được chuyển trong gói tin). Nó không cung cấp tính riêng tư, có nghĩa là nó không mã hóa dữ liệu. Dữ liệu vẫn có thể đọc được, nhưng chúng được bảo vệ chống lại việc thay đổi. Giao thức AH sử dụng các thuật toán ***Keyed hash*** để đánh dấu gói dữ liệu nhằm đảm bảo tính toàn vẹn của nó.

2. Giao thức ESP cung cấp tính riêng tư (thêm vào cho tính xác thực, toàn vẹn và không lặp) cho dữ liệu (***IP Payload***). ESP trong trang thái vận chuyển sẽ không đánh dấu toàn bộ gói tin. Chỉ các thân gói tin IP (***IP Payload***) – không phải là ***IP Header*** – là được bảo vệ. ESP có thể được sử dụng độc lập hay kết hợp với AH. Ví dụ, khi sử dụng kết hợp với AH, các gói ***IP Payload*** được gửi từ máy tính A đến máy tính B được mã hóa và đánh dấu để đảm bảo tính nguyên vẹn. Khi nhận được, phần dữ liệu được truyền sẽ được giải mã sau khi quá trình xác nhận tính toàn vẹn được thực hiện thành công. Và người nhận có thể biết chắc chắn rằng ai đã gửi gói dữ liệu, dữ liệu không bị thay đổi và không ai khác có thể đọc được chúng.

Các phương thức IPSec

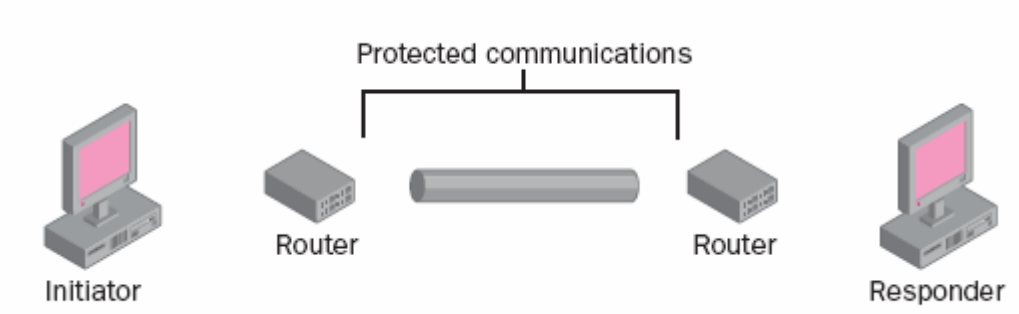
Bạn có thể cấu hình IPSec sử dụng mọt trong hai phương thức sau:

1. **Phương thức Vận chuyển (*Transport Mode):*** Bạn sẽ sử dụng ***Transport Mode*** khi bạn có yêu cầu lọc gói tin và bạn yêu cầu sự bảo mật điểm-tới-điểm. Cả hai trạm cần hỗ trợ IPSec sử dụng cùng giao thức xác thực, bắt buộc phải sử dụng các bộ lọc IP tương thích và không đi qua một giao tiếp NAT nào. Liên lạc đi qua giao tiếp NAT sẽ đổi địa chỉ IP trên phần tiêu đề và làm mất hiệu lực của ICV (*Giá trị Kiểm soát tính Nguyên vẹn*). Hình 6-1 chỉ ra một ví dụ của ***Transport Mode.***



Hình 6-1: Bảo vệ Điểm-tới-Điểm trong *Transport mode.*

2. **Tunel Mode (*Phương thức Đường hầm*):** Bạn sử dụng ***Tunel Mode*** trong trường hợp bạn cần kết nối Site-to-Site thông qua Internet (hay các mạng công cộng khác). ***Tunel Mode*** cung cấp sự bảo vệ Gateway-to-Gateway (*cửa-đến-của*). hình 6-2 mô tả một ví dụ của phương thức này.



Hình 6-2: Bảo vệ Gateway-to-Gateway trong tunel mode.

Security Associations (*Sự Liên kết Bảo mật*)

Sự Liên kết Bảo mật (SA) là một tập hợp của các dịch vụ bảo mật, các cơ chế bảo vệ, và các khóa mã hóa được các cặp đối tượng đang thực hiện liên lạc với nhau cùng thỏa thuận. SA bao gồm các thông tin cần thiết để xác định các lưu thông sẽ dược bảo mật như thế nào (các dịch vụ bảo mật và cơ chế bảo vệ) và với khóa bảo mật nào (Khóa mã hóa). Có hai loại SA sẽ được tạo ra khi khi các cặp máy tính sử dụng IPSec trao đổi với nhau trong trạng thái bảo mật: SA ISAKMP và SA IPSec.

SA ISAKMP

SA ISAKMP, còn được gọi là ***SA Phương thức Chính*** (***Main Mode SA***) được sử dụng để bảo vệ các thỏa thuận bảo mật IPSec. SA ISAKMP được tạo ra bằng việc thỏa thuận một bộ mật mã (một tập hợp các thuật toán mã

hóa được sử dụng để mã hóa dữ liệu), mà sẽ được sử dụng để bảo vệ các lưu thông ISAKMP trong tương lai, trao đổi các chất liệu tạo khóa, sau đó sẽ xác nhận và xác thực từng đối tượng IPSec. SA được lưu trong CSDL Liên kết Bảo mật (***Security Association Database - SADB***). Khi quá trình tạo SA ISAKMP kết thúc, tất cả các thỏa thuận SA trong tương lai cho cả hai loại SA đều được bảo vệ. Dó chính là một khía cạnh của việc liên lạc bảo mật được biết đến với tên *Thỏa thuận bộ Mã hóa được Bảo vệ (**Protected Ciphersuite negotiation**)*. Với cơ chế này, không chỉ các dữ liệu được bảo vệ, mà cả việc xác định các thuật toán bảo mật đã được thỏa thuận giữa các đối tác IPSec cũng được bảo vệ. Để phá vỡ việc bảo vệ IPSec, các người dùng ác ý trước hết phải xác định được bộ mật mã bảo vệ dữ liệu, mà bộ mật mã này lại đưa ra một rào cản khác. Đối với IPSec, chỉ có một ngoại lệ để hoàn thành việc thỏa thuận bộ mật mã được bảo vệ là tiến hành thỏa thuận về bộ mật mã với SA ISAKMP ban đầu, được gửi dưới dạng văn bản tường minh .

SA IPSec

SA IPSec, còn được gọi là ***SA Phương thức Nhanh (Quick Mode SA),*** được sử dụng để bảo vệ các dữ liêu được gửi giữa các đối tác IPSec. Việc thỏa thuận bộ mật mã SA IPSec được SA ISAKMP bảo vệ. Không một thông tin nào về kiểu lưu thông hay cơ chế bảo vệ được gửi dưới dạng văn bản tường minh. Với mỗi cặp đối tác IPSec, hai kiểu SA IPSec luôn tồn tại cho mỗi giao thức được sử dụng: một được thỏa thuận cho các lưu thông chiều vào (***inbound***), một cho các lưu thông chiều ra (***Outbound***). SA chiều vào của một đối tác IPSec này sẽ là SA chiều ra của đối tác IPSec kia.

Chỉ mục các Thông số Bảo mật (*Sercurity Parameters Inđex - SPI*)

Với mỗi phiên IPSec, các đối tác IPSec bắt buộc phải lần theo dấu vết việc sử dụng của ba SA khác nhau: SA ISAKMP, SA IPSec chiều vào và SA IPSec chiều ra. Để nhận dạng một SA nhất định, người ta sử dụng một số ngẫu nhiên giả 32 bit, được gọi là *Chỉ mục các Thông số Bảo mật* (***Sercurity Parameters Inđex - SPI***). SPI, là một trường trong tiêu đề của IPSec, chỉ ra SA mà đối tác đích sẽ dùng và được gửi cùng với từng gói dữ liệu. Đối tác nhận có trách nhiệm cung cấp một SPI duy nhất cho từng giao thức.

Đối tác khởi tạo một phiên IPSec được gọi là *Người Khởi tạo (**Initiator**)*. Đối tác có trách nhiệm yêu cầu thực hiện việc bảo vệ IPSec được gọi là *Người đáp* (***responder***). *Người Khởi tạo* sẽ chọn SPI của SA ISAKMP, và

mỗi đối tác IPSec sẽ chọn SPI của SA IPSec dành cho các lưu thông chiều ra của nó.

Trao đổi Khóa Internet (*Internet Key Exchange - IKE*)

IKE là tiêu chuẩn xác định cơ chế thiết lập SA. IKE kết hợp ISAKMP và giao thức ***Oakley Key Determination*** để tạo ra các chất liệu khóa bảo mật. ***Oakley*** được xây dựng dựa trên thuật toán *Trao đổi khóa Diffie-Hellman* ***(Diffie-Hellman Key Exchange)***, cho phép hai đối tác IPSec xác định khóa bảo mật bằng cách trao đổi các các giá trị không được mã hóa thông qua mạng công cộng.

Kết quả của quá trình trao đổi khóa ***Diffie-Hellman*** bằng cách trao đổi hai số qua mạng công cộng sẽ tạo ra khóa bảo mật mà chỉ riêng hai đối tác tham gia vào quá trình trao đổi được biết. Người dùng ác ý khi truy cập vào các gói tin trao đổi khóa cũng có thể xem các số này, nhưng họ sẽ không thực hiện được cùng một phép tính như các đối tác tham gia thỏa thuận đã thực hiện để nhận được khóa bảo mật chia sẻ.

Quá trình trao đổi khóa ***Diffie-Hellman*** không ngăn cản các vụ tấn công ngang đường, trong đó người sử dụng ác ý đứng giữa hai đối tác IPSec sẽ thực hiện hai quá trình trao đổi khóa ***Diffie-Hellman,*** mỗi quá trình với một đối tác IPSec. Sau khi đã hoàn thành cả hai quá trình trao đổi khóa nói trên, người dùng ác ý sẽ có các khóa bảo mật để liên lạc với cả hai đối tác. Để tránh các cuộc tấn công như vậy, IPSec trong Windows Server 2003 thực hiện việc xác thực ngay sau khi quá trình trao đổi khóa kết thúc. Trong trường hợp đối tác IPSec không thể thực hiện việc xác thực mọt cách chính xác, thỏa thuận bảo mật sẽ bị loại bỏ trước khi có bất cứ một dữ liệu nào được gửi đi.

IPSec trong Windows Server 2003 cũng hỗ trợ cơ chế tạo lại khóa động (***Dynamic Rekeying***), sẽ xác định các chất liệu tạo khóa mới thông qua một trao đổi ***Diffie-Hellman*** mới. Cơ chế tạo lại khóa động dựa trên thời gian đã trôi qua (mặc định là 480 phút hay 8 giờ) hoặc dựa trên số các phiên trao đổ dữ liệu với cùng một tập các chất liệu tạo khóa (Mặc định, số này là không giới hạn).

> ***THÔNG TIN THÊM Quá trình thỏa thuận IKE*** *Để có thêm thông tin về quá trình thỏa thuận IKE, xem RFC 2409 "The Internet Key Exchange (IKE)" tại địa chỉ* ***http://www.ietf.org/rfc/rfc2409.txt***

Dịch vụ IPSec Policy Agent

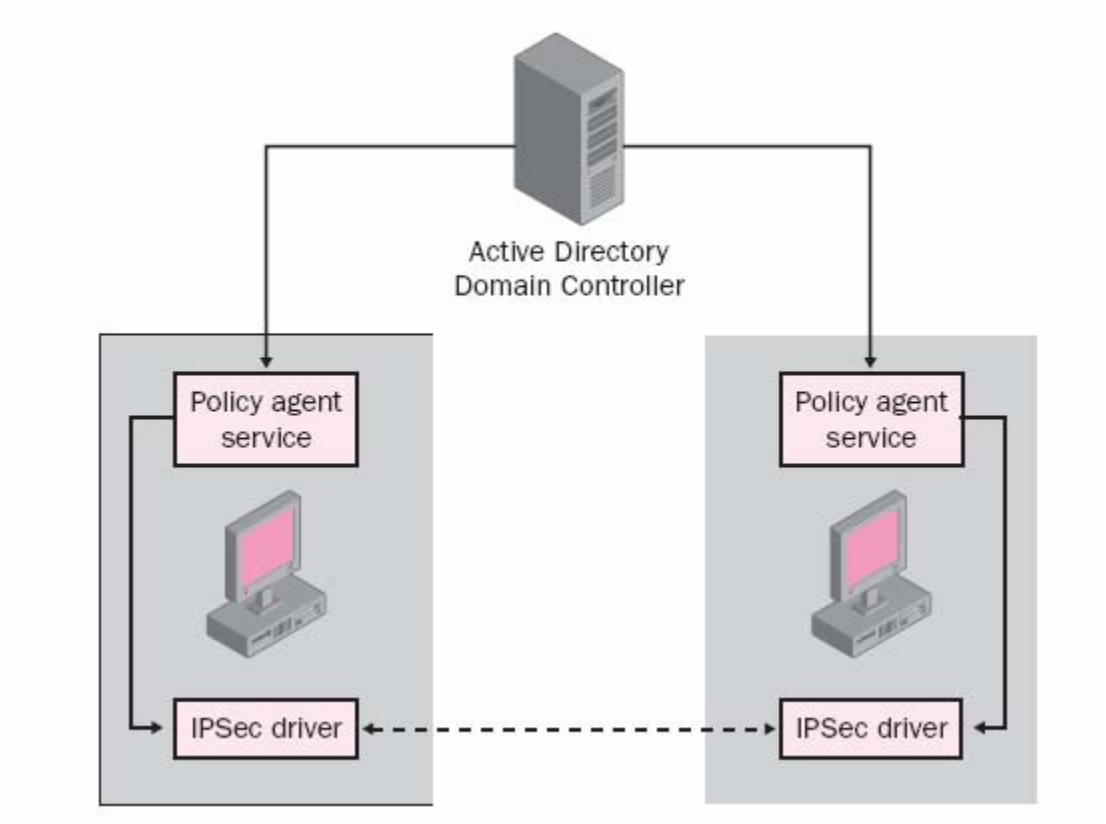
Mục dích của ***IPSec Policy Agent*** (*Đại lý Chính sách IPSec*) là dùng để phục hồi lại các thông tin chính sách và chuyển chúng cho các cấu thành IPSec khác có yêu cầu các thông tin này để thực hiện các dịch vụ bảo mật.

IPSec Policy Agent là một dịch vụ tồn tại trong mỗi máy tính chạy hệ điều hành Windows Server 2003, xuất hiện như là các dịch vụ IPSec trong danh sách các dịch vụ hệ thống tại bảng điều khiển ***Services. IPSec Policy Agent*** sẽ thực hiện một số chức năng trong hệ điều hành bao gồm:

1. Phục hồi các chính sách IPSec thích hợp (nếu chúng đã được gán) từ Active Directory (như chỉ ra trong hình 6-3) nếu máy tính là thành viên của Miền, hoặc từ Sổ đăng ký (***registry***) nếu máy tính không phải là thành viên của Miền.

2. Thu thập các thay đổi trong việc cấu hình chính sách.Gửi các thông tin chính sách IPSec đến trình điều khiển IPSec.

3. Nếu máy tính là thành viên của miền, quá trình phục hồi chính sách sẽ bắt đầu khi hệ thống khởi động, với khoảng thời gian đã được xác định trong chinh sách IPSec, và tại khoảng thời gian thu thập đăng nhập Windows mặc định. Bạn cũng có thể thu thập các thông tin thay đổi cấu hình chính sách IPSec trong Active Directory một cách thủ công nhờ việc thực hiện lệnh ***GPUpdate /target:tênmáytính***.



Hình 6-3: *IPSec Policy Agent* liên lạc với trình điều khiển IPSec

Sau đây là các khía cạnh khác của hành vi chính sách IPSec dành cho các máy tính là thành viên Miền:

1. Nếu các thông tin chính sách IPSec cho các máy tính là thành viên Miền là được cấu hình tập trung, các thông tin chính sách được lưu trong Active Directory và lưu tạm trong ***Registry*** cục bộ của máy tính sẽ được áp dụng chính sách.

2. Nếu máy tính tạm thời không kết nối tới Miền và chính sách đã được lưu tạm, các thông tin chính sách mới dành cho máy tính đó sẽ thay thế cho các thông tin chính sách cũ đang được lưu tạm khi máy tính được kết nối lại tới Miền.

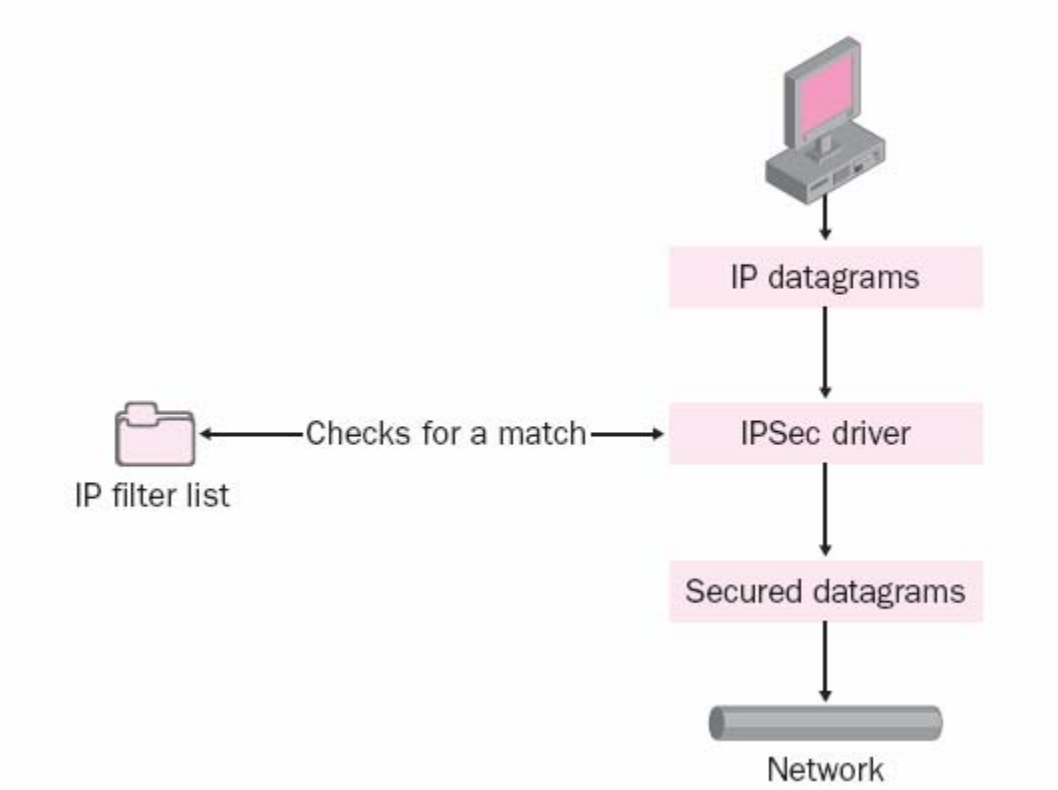
3. Nếu máy tính là máy tính độc lập hay là thành viên của Miền không sử dụng Active Directory để lưu trữ chính sách, Chính sách IPSec được lưu trong ***Registry*** cục bộ.

4. Nếu không có các chính sách IPSec trong Active Directory hay trong ***Registry*** khi ***IPSec Policy Agent*** khởi động một cách tự động tại thời điển hệ thống khởi động, hay ***IPSec Policy Agent*** không

thể kết bối tới Active Directory, ***IPSec Policy Agent*** sẽ đợi cho đến khi chính sách được gán hay kích hoạt.

Trình điều khiển IPSec

Trình điều khiển IPSec nhận danh sách bộ lọc IP tích cực từ ***IPSec Policy Agent,*** như chỉ ra trong hình 6-4. Đại lý Chính sách sau đó sẽ kiểm tra sự phù hợp của mỗi gói thông tin chiều ra cũng như chiều vào so với danh sách trong bộ lọc. Bộ lọc IP cho phép quản trị mạng xác định một cách chính xác các lưu thông IP nào là bảo mật. Mỗi danh sách bộ lọc IP bao gồm một hay nhiều bộ lọc, xác định địa chỉ IP và kiểu lưu thông. Một danh sách bộ lọc IP có thể được sử dụng trong nhiều kịch bản liên lạc. Bạn có thể truy cập các bộ lọc IP bằng cách sử dụng Snap-in ***IP Security Policy management*** Để truy cập các danh sách bộ lọc IP, trong Snap-in ***IP Security Policy management***, nhấn chuột phải vào điểm ***IP security Policy,*** sau đó nhấn ***Manage IP Filter Lists And Filter Actions.***



Hình 6-4: Trình điều khiển IPSec kiểm tra sự phù hợp của gói tin với bộ lọc IP.

Khi gói tin phù hợp với bộ lọc, nó sẽ áp dụng các hành vi bộ lọc tương ứng. Khi gói tin không phù hợp bất cứ bộ lọc nào, nó sẽ được chuyển ngược lại

cho trình điều khiển TCP/IP để được nhận hay truyền mà không có sự thay đổi nào.

Nếu hành động của bộ lọc cho phép truyền, gói tin sẽ được nhận hay truyền mà không bị thay đổi. Nếu hành động của bộ lọc là khóa truyền dẫn, gói tin sẽ bị vô hiệu hóa. Nếu hành động của bộ lọc yêu cầu thỏa thuận về bảo mật, SA phương thức chính và phương thức nhanh sẽ được thỏa thuận (sẽ được mô tả trong phần "Quá trình Thỏa thuận bảo mật", tại phần sau của chương này).

Các khóa và SA phương thức nhanh đã được thỏa thuận được sử dụng vơi cả các lưu thông chiều ra và chiều vào. Trình điều khiển IPSec lưu toàn bộ các SA phương thức nhanh trong CSDL. Trình điều khiển IPSec sử dụng trường SPI để kiểm tra sự phù hợp của SA với gói tin.

Khi một gói tin chiều ra thỏa mãn các điều kiện của danh sách bộ lọc IP với hành động thỏa thuận bảo mật, Trình điều khiển IPSec sẽ xếp gói tin vào hàng đợi, và quá trình IKE bắt đầu tiến hành thỏa thuận bảo mật với địa chỉ IP đích của gói tin.

Sau khi việc thỏa thuận bảo mật hoàn tất, trình điều khiển IPSec trên máy tính gửi sẽ thực hiện các hành động sau:

1. Trình điều khiển IPSec nhận SA có chứa khóa phiên từ quá trình IKE.
2. Trình điều khiển IPSec định vị SA chiều ra trong CSDL của nó và chèn SPI lấy từ SA vào tiêu đề (***header***).
3. Trình điều khiển IPSec ký vào gói tin và mã hóa chúng nếu tính riêng tư được yêu cầu.
4. Trình điều khiển IPSec gửi gói tin đến lớp IP để truyền chúng đến máy tính đích.

Trong trường hợp việc thỏa thuận thất bại, trình điều khiển IPSec sẽ triệt tiêu gói tin.

Khi một gói tin được bảo mật IPSec chiều vào thỏa mãn các điều kiện của bộ lọc trong danh sách các bộ lọc IP, trình điều khiển IPSec sẽ thực hiện các hành động sau:

1. Trình điều khiển IPSec nhận khóa phiên, SA, SPI từ quá trình IKE.

2. Trình điều khiển IPSec định vị SA chiều vào trong CSDL bằng cách sử dụng địa chỉ đích và SPI.

3. Trình điều khiển IPSec kiểm tra chữ ký và, nếu cần thiết, giải mã gói tin.

4. Trình điều khiển IPSec tìm các gói IP thỏa mãn bộ lọc trong danh sách bộ lọc để chắc chắn rằng không nhận thừa một lưu thông nào ngoài những lưu thông đã được chấp nhận trong quá trình thỏa thuận.

5. Trình điều khiển IPSec gửi gói tin đến trình điều khiển TCP/IP để chuyển cho ứng dụng nhận.

Khi nhận được một gói tin không được bảo mật, Trình điều khiển IPSec tìm kiếm điều kiện lọc thỏa mãn trong danh sách bộ lọc. Nếu việc tìm kiếm là thành công và hành động lọc của bộ lọc đó là yêu cầu bảo mật IP hay khóa gói tin, gói tin sẽ bị triệt tiêu.

> ***LƯU Ý*** ***Thỏa mãn các bộ lọc đường hầm trước*** *Trình điều khiển IPSec thỏa mãn tất cả các gói tin chiều vào không bảo mật với danh sách của các bộ lọc xác định đường hầm IPSec trước tiên, sau đó phải thỏa mãn các gói tin với tất cả các bộ lọc xác định điểm-tới –điểm.*

Quá trình Thỏa thuận Bảo mật

Quá trình xử lý IPSec có thể được chia thành hai loại thỏa thuận: thỏa thuận phương thức chính và thỏa thuận phương thức nhanh. Hình 6-5 trình bầy một cái nhìn khái quát ở mức cao của quá trình xử lý sử dụng hai trạm: trạm ***A*** và trạm ***B***:

1. Trạm ***A*** yêu cầu liên lạc bảo mật.

2. Việc thỏa thuận theo phương thức chính được bắt đầu và hoàn tất (Khóa chủ - ***Master Key*** **–** và SA IKE được thiết lập – *xem phần "Thỏa thuận Phương thức Chính"*).

3. Việc thỏa thuận phương thức nhanh của cặp SA (chiều vào và chiều ra) cho việc truyền gói tin ứng dụng hoàn tất.

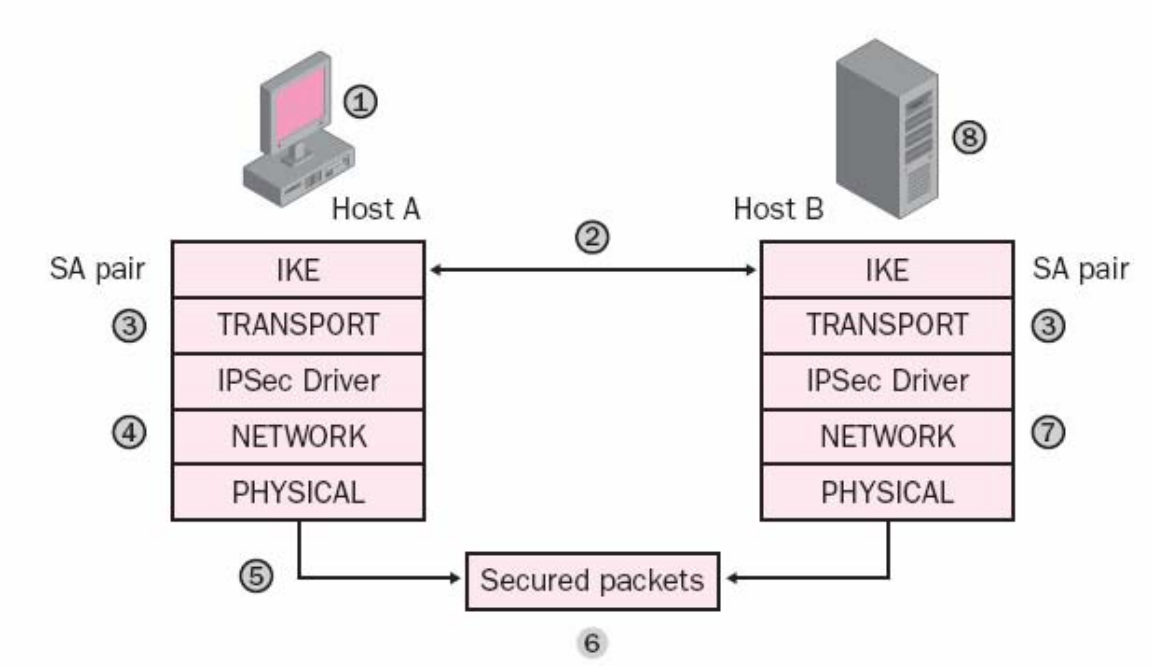
4. Các gói tin ứng dụng từ trạm ***A*** được trình điều khiển TCP/IP chuyển cho Trình điều khiển IPSec.

5. Trình điều khiển IPSec định dạng và mã hóa gói tin, sau đó sử dụng SA chiều ra để gửi nó cho trạm ***B***.

6. Các gói tin bảo mật được truyền trên mạng.

7. Trình điều khiển IPSec trên trạm ***B*** xử lý mật mã các gói tin đến trên SA chiều vào, định dạng chúng như các gói IP thông dụng, sau đó chuyển chúng cho trình điều khiển TCP/IP.

8. Trình điều khiển TCP/IP chuyển các gói tin cho ứng dụng trên trạm ***B.***



Hình 6-5: Quá trình xử lý IPSec

Thỏa thuận Phương thức Chính

Việc thỏa thuận phương thức chính Oakley được sử dụng để xác định chất liệu khóa mã hóa và phòng chống bảo mật để sử dụng trong các quá trình bảo vệ các liên lạc phương thức chính hay phương thức nhanh. Việc thỏa thuận phương thức chính sẽ được trình bầy chi tiết hơn trong các bước sau:

1. Gói tin liên lạc được gửi từ trạm **A** đến trạm ***B***.

2. Trình điều khiển IPSec trên trạm ***A*** kiểm tra các danh sách bộ lọc IP chiều ra của nó và kết kuận rằng các gói tin thỏa mãn bộ lọc và hành động của bộ lọc là ***Negotiate Security*** (*Thỏa thuận Bảo mật*) – các gói tin bắt buộc phải được bảo mật.

3. Trình điều khiển IPSec bắt đầu quá trình thỏa thuận IKE

4. Trạm ***A*** kiểm tra các thiết lập phuương thức chính (việc xác thực, nhóm Diffie-Hellman, việc mã hóa và tính toàn vẹn) trong các chính sách của nó để đề xuất với trạm ***B***.

5. Trạm ***A*** gửi thông điệp IKE đầu tiên sử dụng UDP có địa chỉ cổng nguồn 500 và địa chỉ cổng đích 500.

6. Trạm ***B*** nhân thông điệp nói trên, có yêu cầu thỏa thuận bảo mật, sau đó sử dụng các địa chỉ IP nguồn và đích của gói tin để tìm kiếm trong bộ lọc IKE của riêng nó. Bộ lọc IKE cung cấp các yêu cầu bảo mật dành cho các liên lạc từ trạm ***A***.

7. Nếu các thiết lập bảo mật do trạm ***A*** đề xuất được trạm ***B*** chấp nhận việc thỏa thuận phương thức chính hay SA IKE bắt đầu.

8. Hai máy tính sẽ thỏa thuận các tùy chọn, trao đổi các mã nhận dạng và xác thực chúng, và sinh ra Khóa chính (***Master Key***). SA IKE được thiết lập.

Tóm lại, việc thỏa thuận phương thức chính tạo ra SA ISAKMP. *Người Khởi tạo* và *Người đáp* trao đổi hàng loạt các thông điệp ISAKMP để thỏa thuận về bộ mật mã dành cho SA ISAKMP (dưới dạng văn bản tường minh), trao đổi các vật liệu xác định khóa (dưới dạng văn bản tường minh) và nhận dạng và xác thực lẫn nhau (dưới dạng văn bản mã hóa).

Thỏa thuận Phương thức nhanh

Khi việc thỏa thuận theo phương thức chính hoàn tất, mối đối tác trong cặp IPSec đã hoàn thành việc lựa chọn một tập nhất định các thuật toán mã hóa được dùng cho các thông điệp bảo mật phương thức chính và phương thức nhanh, đã trao đổi các thông tin khóa để nhận được khóa bảo mật chia sẻ, và đã thực hiện xong việc xác thực. Trước khi các dữ liệu bảo mật được gửi đi, việc thỏa thuận theo phương thức nhanh nhất thiết phải được thực hiện nhằm xác định kiểu lưu thông sẽ được bảo mật và chúng sẽ được bảo mật như thế nào. Việc thỏa thuận phương thức nhanh cũng được thực hiện khi SA phương thức nhanh hết hạn.

Các thông điệp Phương thức Nhanh là các thông điệp ISAKMP đã được mã hóa bằng việc sử dụng SA ISAKMP. Như đã trình bầy ở trên, kết quả của việc thỏa thuận phương thức nhanh là hai SA IPSec: Một dành cho các

thông tin chiều đi và một dành cho các thông tin chiều đến. Quá trình thỏa thuận được tiến hành như sau:

1. Trạm A thực hiện việc tìm kiếm chính sách của phương thức IKE nhằm xác định toàn bộ các chính sách đã có.

2. Trạm A đưa ra các các đề nghị về các lựa chọn của nó (mật mã, cũng như tần xuất của việc thay đổi khóa, vv…) và về các bộ lọc cho trạm B.

3. Trạm B thực hiện việc tìm kiếm chính sách của phương thức IKE của chính nó, nếu kết quả tìm được là thỏa mãn các đề xuất của trạm A, nó hoàn tất việc thỏa thuận phương thức nhanh để tạo ra cặp SA IPSec.

4. Một SA sẽ được dành cho chiều đi và một SA sẽ được dành cho chiều đến. Mối SA sẽ được nhận dạng nhờ SPI, và SPI là một phần trong phần đầu (*tiêu đề*) của mỗi gói tin được gửi đi.

5. Trình điều khiển IPSec chuyển các gói tin cho trình điều khiển của cạc mạng.

6. Trình điều khiển cạc mạng đưa các khung dữ liệu lên mạng.

7. Cạc mạng tại trạm B nhận các gói tin đã mã hóa (từ mạng).

8. Trạm B sử dụng SPI để tìm ra SA tương ứng. (SA này có chứa khóa mã hóa tương ứng cần thiết để giải mã và xử lý gói dữ liệu.)

9. Nếu Cạc mạng được thiết kế đặc biệt để mã hóa – và do đó có thể giải mã các gói tin, nó sẽ thực hiện công việc này. Sau đó, nó chuyển các gói tin cho Trình điều khiển IPSec.

10. Trình điều khiển IPSec tại trạm B sử dụng SA chiều đến để phục hồi lại các khóa và xử lý các gói tin nếu cần.

11. Trình điều khiển IPSec chuyển đổi các gói tin quay trở lại định dạng của các gói tin IP thông thường và chuyển chúng cho trình điều khiển TCP/IP, và đến lượt chúng sẽ chuyển tiếp cho ứng dụng nhận.

12. SA IPSec liên tục xử lý các gói tin, SA được làm mới bằng việc thỏa thuận phương thức nhanh IKE trong suốt thời gian ứng dụng gửi và nhận dữ liệu. Khi SA không làm việc, chúng sẽ được xóa.

IKE phương thức chính không bị xóa khi không làm việc. Tuổi thọ của nó là 8 giờ, nhưng con số này là có thể thay đổi được (từ 5 phút tới tối đa là 48 giờ). Trong phạm vi thời gian đã định này, các lưu thông mới sẽ chỉ kích hoạt việc thỏa thuận phương thức nhanh. Khi IKE phương thức chính hết hạn, một phương thức IKE mới sẽ được thỏa thuận khi cần.

TÌM HIỂU CÁC CHÍNH SÁCH BẢO MẬT IPSEC.

Chính sách là các luật xác định mức độ bảo mật. thuật toán băm, thuật toán mã hóa , và độ dài của khóa được yêu cầu. Các luật này cũng xác định các địa chỉ, giao thức, tên DNS, mạng con và kiểu kết nối mà các thiết lập bảo mật áp dụng.

Các chính sách IPSec có thể được cấu hình để đáp ứng được các yêu cầu về bảo mật của người dùng, nhóm, ứng dụng, miền, site, hay toàn bộ doanh nghiệp. Windows Server 2003 cung cấp Snap-in ***IP Security Policy Management*** (*Quản trị Chính sách Bảo mật IP*) được dùng để tạo và quản trị các chính sách IPSec một cách cục bộ hay thông qua Chính sách Nhóm (GP – ***Group Policy***).

Các chính sách đã xác định trước được cung cấp cho cả hai loại cấu hình bảo mật cục bộ và nhóm. Chúng cũng có thể được thay đổi để thỏa mãn các yêu cầu đặc biệt. hay bạn cũng có thể tạo mới hoàn toàn các chính sách. Một khi chính sách đã được xác định, để cho chúng có thể thực sự có tác dụng, bạn phải gán nó cho một đối tượng nào đó. Mặc định không có chính sách nào được gán sẵn.

Gán các chính sách IPSec

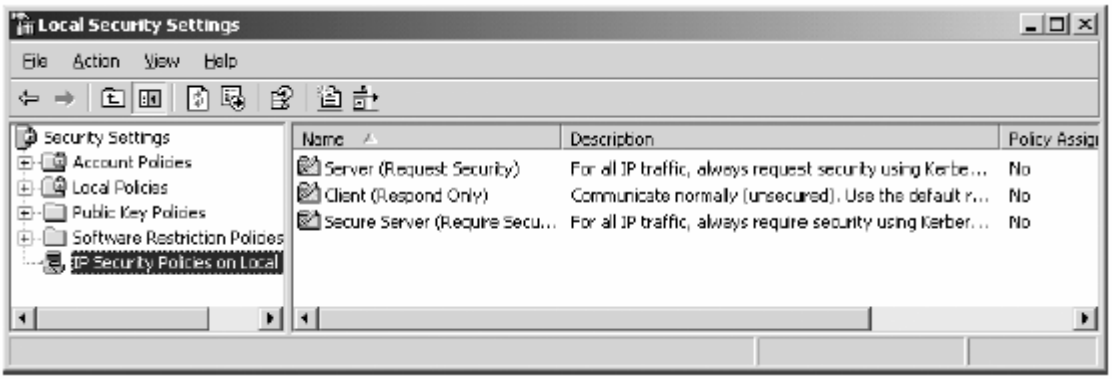
Như đã thảo luận ở trên, chính sách IPSec được chuyển từ ***Policy Agent*** (*Đại lý Chính sách*) sang cho trình điều khiển IPSec và xác định các thủ tục hoàn hảo cho tất cả các khía cạnh của giao thức – từ đâu, khi nào, và làm thế nào để bảo mật dữ liệu với các phương pháp bảo mật được sử dụng. Có thể có một vài chính sách được xác định, nhưng trong một thời điểm, chỉ có một chính sách được gán cho máy tính mà thôi. Để gán chính sách, bạn có thể nhấn chuột phải vào ***IPSec Policy*** trong ***Local Security Policy*** hay trong bảng điều khiển ***Group Policy*** thích hợp, sau đó nhấn ***Assign***.

Để có thể hiểu rõ hơn về các khả năng của chính sách, bạn bắt buộc phải biết về các cấu thành của chính sách. Các cấu thành này bao gồm:

- **Thiết lập đường hầm (*Tunnel*):** Địa chỉ IP kết thúc đường hầm (nếu sử dụng kỹ thuật đường hầm IPSec để bảo vệ các gói tin đến.)
- **Kiểu mạng:** Kiểu kết nối bị chính sách IPSec tác dụng: tất cả các kết nối, LAN, hay truy cập từ xa.
- **Bộ lọc IP:** tập con của lưu thông mạng dựa trên địa chỉ IP, cổng, và giao thức vận chuyển. Nó thông báo cho trình điều khiển IPSec các lưu thông chiều ra hay chiều vào nào là được bảo mật.
- **Danh sách bộ lọc IP:** Tập hợp của một hay nhiều bộ lọc IP, xác định dẫy của các lưu thông mạng.
- **Hành động của bộ lọc:** Trình điều khiển IPSec sẽ bảo mật lưu thông mạng như thế nào. Các hành động của bộ lọc được xác định trước bao gồm: ***Permit (****Cho phép****), Request Security (Optional) (****Đề nghị bảo mật – tùy chọn****),*** và ***Require Security (****Yêu cầu bảo mật.****)***
- **Phương thức xác thực:** Một trong các thuật toán bảo mật và kiểu được sử dụng cho việc xác thực và trao đổi khóa
  - ***Kerberos***
  - ***Certificates (****Giấy chứng nhận****)***
  - ***Preshared key (****Khóa chia sẻ trước****)***

Các chính sách bảo mật IPSec mặc định

Bạn tạo và cấu hình các chính sách IPSec cục bộ bằng cách sử dụng tính năng ***IP Security Policies On Local Computer*** (*các Chính sách Bảo mật IP trên Máy tính Cục bộ*), như được chỉ ra trên hình 6-6. (Để truy nhhập Snap-in này, tham khảo bài tập 6-2, "Cấu hình IPSec để sử dụng Giấy chứng nhận", từ bước 1 đến bước 7.)



Hình 6-6: IP Security Policies On Local Computer

Sử dụng chính sách ***Client (Respond Only)*** *(Máy tram – Chỉ Đáp)* trên các máy tính thông thường không gửi các dữ liệu được bảo mật. Chính sách này không khởi tạo các liên lạc bảo mật. Nếu máy chủ yêu cầu bảo mật, máy trạm sẽ đáp ứng và bảo mật chỉ các lưu thông với cổng và giao thức được yêu cầu với máy chủ đó.

Chính sách ***Server (Request Security)*** *(Máy chủ - Đề xuất bảo mật)* có thể được sử dụng trên bất cứ máy tính nào – máy trạm hay máy chủ - cần thiết khởi tạo các liên lạc bảo mật. Không giống như chính sách máy trạm, chính sách máy chủ này sẽ bảo vệ tất cả các truyền thông chiều ra. Các truyền thông chiều vào, không bảo mật cũng được chấp nhận. Mặc dù vậy chúng sẽ không được xử lý cho đến khi nhận được các đề xuất bảo mật IPSec từ máy gửi cho tất cả các gói tin đã truyền. Chính sách này yêu cầu sử dụng giao thức bảo mật Kerberos

Chính sách chặt chẽ nhất trong các chính sách bảo mật xác định trước, chính sách ***Secure Server (Require Security)*** (*Máy chủ Bảo mật – yêu cầu bảo mật*) không gửi hay chấp nhận các truyền thông không bảo mật. Các máy trạm muốn liên lạc với máy chủ bảo mật bắt buộc phải sử dụng ít nhất Chính sách Máy chủ xác định trước hay tương đương, Giống như Chính sách Máy chủ, Chính sách Máy chủ Bảo mật sử dụng xác thực Kerberos

Luật Đáp Mặc định

Luật Đáp Mặc định, được kích hoạt một cách mặc định cho tất cả các chính sách, được sử dụng để đảm bảo rằng máy tính sẽ đáp ứng các yêu cầu của các liên lạc bảo mật. Nếu chính sách hiện hành không có luật xác định cho máy tính đề xuất liên lạc bảo mật, luật Đáp mặc định sẽ được áp dụng và bảo mật sẽ được thỏa thuận. Ví dụ, khi máy tính A liên lạc một cách bảo mật với máy tính B và máy tính B không có bộ lọc thông tin chiều vào dành cho máy tính A, luật Đáp mặc định sẽ được áp dụng.

Các phương thức bao mật và phương thức xác thực có thể được cấu hình cho Luật Đáp mặc định. Sử dụng Snap-in ***IP Security Policy Management*** để thay đổi luật đáp mặc định. (Để tạo bảng điều khiển có chứa Snap-in ***IP Security Policy Management,*** tham khảo bài tập 6-2, "Cấu hình IPSec để sử dụng Giấy chứng nhận", từ bước 1 đến bước 7.)

- **Truy nhập và Thay đổi Phương thức Bảo mật của Hành động Bộ lọc**

1. Mở hay tạo bảng điều khiển có chứa Snap-in ***IP Security Policy Management***
2. Trên cấu trúc hình cây của bảng điều khiển. nhấn chuột vào vị trí có chứa chính sách bạn muốn thay đổi.
3. Trong khung Chi tiết, nhấn đúp chuột vào chính sách bạn muốn thay đổi.
4. Trong thẻ ***Rules,*** tại hộp ***IP Sercurity Rules*** chọn luật bạn muôn thay đổi, và nhấn ***Edit***.
5. Trong thẻ ***Filter Action***, chọn Hành động Bộ lọc bạn muốn thay đổi, và nhấn ***Edit***.
6. Trong thẻ ***Security Methods***, thêm, thay đổi, ghi lại, hay loại bỏ phương thức bảo mật

Luật Đáp mặc định có các đặc tính sau:

- **IP Filter List of <Dynamic>:** Chỉ ra rằng danh sách bộ lọc là chưa được cấu hình, nhưng các bộ lọc đã được tạo một cách tự động trên cơ sở nhận được các gói thỏa thuận IKE.
- **Filter Action of Default Response (***Hành động Bộ lọc của Luật Đáp Mặc định***):** Bạn có thể xem và thay đổi Hành động Bộ lọc của một chính sách bằng cách mở trang thuộc tính (***Property***) của chính sách tương ứng trong Snap-in ***IP Security Policy Management***. Hành động Bộ lọc của Luật Đáp Mặc định chỉ ra các hành động của bộ lọc (***Permit*** – *Cho phép*, ***Block*** - *Khóa*, hay ***Negotiate Security*** – *Thỏa thuận Bảo mật*) là không thể cấu hình được. ***Negotiate Security*** sẽ được sử dụng**.**

Mặc dù vậy, bạn vẫn có thể cấu hình các tham số sau:

- Các phương thức bảo mật và thứ tự áp dụng của chúng trong thẻ ***Security methods.***

- Các phương thức xác thực và thứ tự áp dụng của chúng trong thẻ ***Authentication Methods.***

LƯU Ý: Không thể xóa Luật Đáp mặc định *Bạn không thể xóa được luật đáp mặc định, nhưng nó có thể bị vô hiệu hóa (**Deactivate**)*

➢ **Thêm thiết lập chính sách**

Khi bạn chọn Snap-in ***IP Security Policy Management*** để thêm vào bảng điều khiển, bạn sẽ có bốn lựa chọn để quản trị các chính sách bảo mật:

- **Local Computer (***máy tính cục bộ***):** sử dụng tùy chọn này để quản trị các Chính sách Bảo mật IP trên máy tính có chạy bảng điều khiển.

- **The Active Directory Domain Of Which This Computer Is A Member (***Miền Active Directory mà máy tính này là thành viên***)** Sử dụng tùy chọn này khi bạn muốn quản trị các chính sách áp dụng cho toàn bộ miền cục bộ.

- **Another Active Directory Domain (Use The Full DNS Name Of IP Address) (***Miền Active Directory khác – Sử dụng tên DNS đầy đủ hay địa chỉ IP***):** Sử dụng tùy chọn này khi bạn muốn quản trị các chính sách sẽ áp dụng trên toàn bộ một miền ở xa.

- **Another Computer (Máy tính khác):** Sử dụng tùy chọn này để quản trị các chính sách được lưu trữ cục bộ trên máy tính khác.

Để có thể quản trị các chính sách IPSec dựa trên Active Directory, bạn bắt buộc phải là thành viên của nhóm ***Domain Admin*** trong Active Directory, hoặc bạn cần có sự ủy quyền thích hợp.

1. Tạo hay mở bảng điều khiển có chứa Snap-in ***IP Security Policy Management***

2. Trên cấu trúc hình cây của bảng điều khiển, nhấn ***IP Security Policies*** tại vị trí bạn muốn quản trị (máy tính cục bộ, máy tính ở xa, miền Active Directory cục bộ, hay miền Active Directory ở xa).

3. Trên thực đơn Action, nhấn Create IP Security Policy.

4. Trên trang Welcome To The IP Security Policy Wizard, nhấn Next.

5. Trên trang ***IP Security Policy Name***, trong hộp ***Name***, nhập tên cho Chính sách Bảo mật IP mới. Mếu cần, bạn có thể cung cấp các mô tả sau đó nhấn ***Next***.

6. Để sử dụng Luật Đáp Mặc định, trên trang ***Requests For Secure Communication***, Kiểm tra xem ***Activate The Default Response Rule*** đã được lựa chọn và nhấn ***Next***.

7. Trên trang ***Default Response Rule Authentication Method***, chọn phương thức xác thực ban đầu cho luật bảo mật, cung cấp các thông tin thêm cho phương thức đã chọn, sau đó nhấn ***Next***.

8. Trên trang Completing The IP Security Policy Wizard, bỏ lựa chọn hộp Edit Properties, sau đó nhấn Finish.

- **Thay đổi Thiết lập Chính sách**

Để thay đổi một chính sách đang tồn tại, nhấn đúp chuột vào chính sách bạn muốn thay đổi, chọn luật bạn muốn thay đổi và nhấn ***Edit***.

- **Dỡ bỏ Thiết lập Chính sách**

Để dỡ bỏ một chính sách, nhấn chuột vào chính sách bạn muốn dỡ bỏ, và trên thực đơn ***Action***, nhấn ***Delete***.

TRIỂN KHAI CHÍNH SÁCH IPSEC

Chính sách IPSec có thể được triển khai bằng cách sử dụng các chính sách cục bộ, Active Directory, hoặc cả hai. Mỗi phương pháp đều có các điểm mạnh và yếu của riêng nó.

Triển khai IPSec sử dụng các Chính sách Cục bộ

Chỉ có một Đối tượng Chính sách Nhóm (GPO) cục bộ, thường được biết với tên ***Local Computer Policy (****Chính sách Máy tính Cục bộ****),*** được lưu trên máy tính cục bộ. Khi sử dụng GPO cục bộ, bạn có thể lưu các thiết lập Chính sách Nhóm trên từng máy tính riêng mà không cần quan tâm đến việc chúng có phải là thành viên của miền Active Directory hay không.

Trên một mạng không có miền Active Directory (mạng không có Máy chủ Điều khiển Miền Windows 2000 hay Windows Server 2003), các thiết lập GPO cục bộ xác định các hành vi IPSec do chúng không bị các GPO khác ghi đè. GPO cục bộ có thể bị các GPO đã được gán cho Site, Miền, hay OU ghi đè trong môi trường Active Directory.

Các thiết lập Chính sách IPSec cục bộ sẽ được thêm vào các chính sách cố định nếu chính sách cố định đã được cấu hình. Trong trường hợp chính sách IPSec dựa trên Active Directory đã được gán và máy tính kết nối tới miền Active Directory, các thiết lập của chính sách dựa trên Active Directory sẽ được áp dụng thay cho các chính sách IPSec cục bộ.

Bạn nên sử dụng Chính sách Cục bộ trong hai kịch bản sau:

- Bạn không có sẵn nền tảng Active Directory, hoặc bạn chỉ có một số rất ít các máy tính cần sử dụng IPSec.
- Bạn không muốn tập trung hóa chiến lược IPSec trong cơ quan.

Các Chính sách Cố định (Persistent Policy)

Bạn có thể cấu hình các chính sách cố định để mở rộng các chính sách IPSec Cục bộ hay IPSec dựa trên Active Directory đã có, ghi đè lên các chính sách này, và tăng cường khả năng bảo mật trong quá trình máy tính khởi động. Các Chính sách Cố định tăng cường khả năng bảo mật bằng cách cung cấp khả năng bảo mật trong thời gian quá độ từ khi máy tính khởi động cho đến khi các chính sách IPSec dựa trên Active Directory thực sự có tác dụng. Các Chính sách Cố định, nếu được cấu hình, sẽ được lưu trong Sổ đăng ký (***Registry***) cục bộ. Bnạ có thể cập nhật Chính sách Cố định bất cứ lúc nào, một khi dịch vụ IPSec vẫn chạy. mặc dù vậy, các thay đổi trong Chính sách Cố định không được kích hoạt tức thời. Bạn cần khởi động lại dịch vụ IPSec để tải các thiết lập mới của Chính sách Cố định.

Nếu bạn đã cấu hình các chính sách dựa trên Active Directory, bạn có thể sử dụng Chính sách Cố định như là một công cụ để yêu cầu các lưu thông tới Active Directory luôn được bảo mật bằng IPSec, bao gồm cả việc phục hồi các chính sách IPSec dựa trên Active Directory. Khi các chính sách cục bộ hay dựa trên Active Directory được áp dụng, các thiết lập chính sách này sẽ được thêm vào các thiết lập chính sách cố định.

Triển khai IPSec sử dụng Active Directory

Để triển khai các chính sách IPSec sử dụng Active Directory, cần gán các chính sách IPSec cho GPO đích của Site, miền, hay OU. Việc gán các chính

sách này cho GPO sẽ có hiệu quả đối với tất cả các tài khoản máy tính nằm trong phạm vi ảnh hưởng của GPO đó.

Sử dụng bảng điều khiển ***IP Security Policy Management*** hay lệnh ***Netsh*** để quản trị chính sách dựa trên Active Directory. Bảng điều khiển ***IP Security Policy Management*** đã được thảo luận trong quá trình "Thêm Thiết lập Chính sách". Để biết thêm thông tin về lệnh ***Netsh,*** bạn có thể xem thêm phần "Quản trị và Theo dõi IPSec" trong phần sau của chương này.

Chính sách dựa trên Active Directory luôn ghi đè lên bất cứ chính sách IPSec cục bộ nào được gán và thêm vào chính sách IPSec cố định đang được ***IPSec Policy Agent*** (*Đại lý Chính sách IPSec*) áp dụng. nếu chính sách cố đinh đã được cấu hình. Nếu có xung đột giữa chính sách IPSec cố định với hoặc chính sách miền hoặc chính sách cục bộ, các thiết lập chính sách cố định sẽ chiếm ưu thế.

Khi gán chính sách IPsec trong Active Directory, cần cân nhắc các điểm sau:

- Bạn có thể gán danh sách của tất cả các chính sách IPSec tại bất cứ cấp nào trong cấu trúc Active Directory. Mặc dù vậy, chỉ một chính sách IPSec được gán tại một cấp nhất định của Active Directory.
- OU sẽ kế thừa chính sách của OU cha trừ trường hợp tính kế thừa bị khóa hay chính sách được gán một cách trực tiếp.
- Không thể gộp các chính sách IPSec từ các OU khác nhau.
- Chính sách IPSec được gán cho OU trong Active Directory có quyền ưu tiên cao hơn so với chính sách ở mức miền đối với các thành viên của OU đó.
- Chính sách IPSec được gán cho OU mức thấp nhất trong cấu trúc Active Directory sẽ ghi đè lên chính sách IPSec được gán cho OU mức cao hơn đối với các thành viên của OU đó.
- Bạn nên sử dụng việc gán chính sách cho cấp cao nhất có thể trong cấu trúc của Active Directory để giảm thiểu việc cấu hình và công tác quản trị cần thiết.

Bạn nên sử dụng Active Directory để triển khai các chính sách nếu cơ quan của bạn đáp ứng các tiêu chí sau:

- Có hạ tầng Active Directory.

- Bạn sử dụng một số lượng đáng kể các máy tính cần nhóm lại để gán IPSec.
- Bạn muốn tập trung hóa chiến lược IPSec của cơ quan

Triển khai trong môi trường hỗn hợp

Bạn có thể triển khai IPSec trong môi trường có các máy tính là thành viên của miền và sẽ nhận được chính sách IPSec thông qua chính sách nhóm Active Directory, và cả các máy tính không phải là thành viên của miền và sẽ nhận được chính sách IPSec thông qua Chính sách Nhóm Cục bộ. Không phụ thuộc vào việc các máy tính nhận được chính sách IPSec như thế nào, hai máy tính cần liên lạc với nhau vẫn có thể thỏa thuận vè các luật xác định trong các chính sách IPSec của chúng.

THỰC THI IPSEC SỬ DỤNG GIẤY CHỨNG NHẬN

IPSec dựa vào sự xác thực lẫn nhau để cung cấp các liên lạc bảo mật. Do IPSec là một chuẩn công nghiệp, việc xác thực này có thể xẩy ra với các hệ thống không chia sẻ kết cấu hạ tầng xác thực thông qua giao thức Kerberos tập trung. Các giấy chứng nhận X.509 cung cấp một khả năng xác thực khác dành cho IPSec đã được chuẩn hóa và có thể sử dụng trong trường hợp có ***Public Key Infrastructure*** (PKI- *Hạ tầng Khóa Công khai*) tin cậy. Phần này mô tả cách bạn có thể sử dụng giấy chúng nhận khóa công khai để xác thực nhằm cung cấp các liên lạc bảo mật và tin cậy trên mạng.

Giấy chứng nhận X.509

Giấy chứng nhận X.509, còn được gọi là *chứng nhận số,* là một dạng giấy ủy nhiệm điện tử được dùng rộng rãi trong việc xác thực và trao đổi các thông tin bảo mật trên các mạng mở, như Internet, mạng liên ngành (***Extranet***) hay mạng nội bộ (***Intranet***).

Giấy chứng nhận kết buộc một cách tin cậy khóa công khai với thực thể nắm giữ khóa riêng tương ứng. Ví dụ, bạn có thể mã hóa dữ liệu dành cho người nhận bằng khóa công khai của người nhận, và hoàn toàn tin chắc rằng chỉ có người nhận có khóa riêng cần thiết mới giải mã được dữ liệu.

Người xuất bản giấy chứng nhận (***Certificate issuer***), được gọi là *Người Chúng nhân (**Certificate Authority - CA**)*, sẽ đặt một dấu hiệu số lên giấy chứng nhận. Giấy chứng nhận có thể được cấp cho người dùng, máy tính, hay dịch vụ, ví dụ như IPSec.

Giấy chứng nhận bao gồm các thông tin sau:

- Khóa mã hóa công khai từ cặp khóa riêng và công khai của chủ thể giấy chứng nhận.
- Thông tin về chủ thể yêu cầu giấy chứng nhận.
- Tên phân biệt X.500 của người dùng hay máy tính.
- Địa chỉ E-Mail của người sở hữu giấy chứng nhận.
- Chi tiết về CA.
- Ngày hết hạn.
- Giá trị băm của nội dung giấy chứng nhận nhằm đảm bảo tính xác thực (chữ ký số)

Vai trò của CA

Nếu bạn lựa chọn sư dụng giấy chứng nhận để xác thực, bạn cần chọn CA, thường là CA gốc với máy tính chứng nhận đã cài đặt của bạn. Bạn không thể để trường ***Use A Certificate From This Certification Authority (CA)*** trống.

- **Cấu hình IPSec Sử dụng giấy Chứng nhận.**

Để cấu hình IPSec sử dụng Giấy Chứng nhận, làm theo các bước sau:

1. Tạo snap-in ***IP Security Management*** có chứa các chính sách bảo mật IP, hay mở file bảng điều khiển đã lưu có chứa các chính sách bảo mật IP.
2. Nhấn đúp chuột vào chính sách bạn muốn thay đổi.
3. Trong hộp thoại ***Policy Properties*** (ở đây *Policy* là tên của chính sách bảo mật IP), nhấn đúp chuột lên luật bảo mật IPSec bạn muốn thay đổi.
4. Trong hộp thoại ***Edit Rule Properties***, trong thẻ ***Authentication Methods***, nhấn ***Add***, hoặc, nếu bạn muốn cấu hình lại một phương thức đã có, chọn phương thức xác thực và nhấn ***Edit***.
5. Chọn Use A Certificate From This Certificate Authority (CA), và nhấn Browse.

6. Trong hộp thoại ***Select Certificate***, chọn CA thích hợp và nhấn ***OK***.

7. Trong thẻ Authentication Method, nhấn OK.

8. Trong hộp thoại ***Edit Rule Properties***, nhấn ***OK***.

9. Trong hộp thoại ***Policy Properties***, nhấn ***OK.***

SỬ DỤNG NAT VỚI IPSEC

NAT là một quá trình dịch được sử dụng rộng rãi cho phép một mạng với các địa chỉ IP riêng có thể truy nhập thông tin trên Internet. Một kịch bản thường gặp là công ty chỉ có một vài địa chỉ IP công cộng, có thể định tuyến được và phân phối các địa chỉ IP riêng cho các tài nguyên nội bộ của họ.

Việc chuyển đổi các địa chỉ, cổng TCP, hay cổng UDP trong NAT để kết nối người dùng với Internet làm mất hiệu lực của đic vụ bảo mật IPSec. Đặc biệt, địa chỉ và cổng được dịch sẽ gây ra các vấn đề sau cho các lưu thông IPSEc dựa trên ESP.

- Với các gói tin được bảo vệ ESP, các cổng TCP và UDP là được mã hóa và do đó chúng không thể được dịch.

- Các thông điệp ISAKMP tính toán giá trị băm và các chữ ký dựa trên các thông tin SA, có chứa địa chỉ IP. Dịch địa chỉ IP sẽ làm mất hiệu lực của các giá trị băm hay chữ ký.

  ***LƯU Ý**: **IKE qua NAT** Để cho phép việc thỏa thuận IKE và các gói yin ESP đã được bọc gói làm việc qua NAT, IPSec trong Windows Server 2003 hỗ trợ **IPSec NAT Traversal (NAT-T). NAT-T** được sử dụng đặc biệt hiệu quả khi thiết lập các kết nối **Layer Two Tunneling Protocol (L2TP)/IPSec** với các máy trạm VPN đứng phía sau NAT.*

QUẢN TRỊ VÀ THEO DÕI IPSEC

Windows Server 2003 cung cấp một vài công cụ bạn có thể sử dụng để quản trị và theo dõi IPSec, Bao gồm ***IP Security Monitor, RSoP, Event Viewer,*** nhật ký ***Oakley, Netsh,*** và ***Netdiag.***

Sử dụng IP Security Monitor (*Trình Theo dõi Bảo mật IP*)

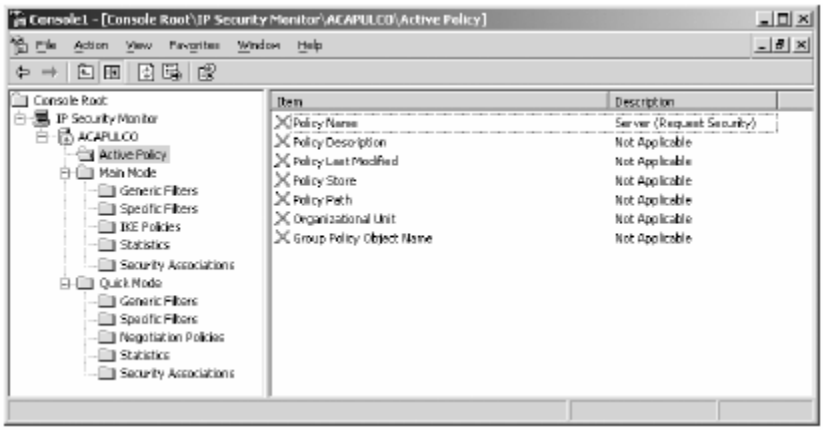
Trong Windows 2000, ***IP Security Monitor*** được thực thi dưới dạng chương trình chạy (***IPSecmon***). Trong Windows Server 2003 và Windows XP, ***IP Security Monitor*** được thực thi dưới dạng một bảng điều khiển MMC, và bao gồm các tính năng nâng cao cho phép bạn thực hiện các công việc sau:

- Theo dõi các thông tin IPSec tại máy tính cục bộ cũng như các máy tính từ xa.
- Xem chi tiết về các chính sách IPSec đang hoạt động, bao gồm tên, mô tả, ngày thay đổi cuối, lưu trữ, đường dẫn, OU, và tên GPO.
- Xem các bộ lọc chung và riêng của phương thức chính và phương thức nhanh.
- Xem các thống kê phương thức chính và phương thức nhanh. (Để nắm thông tin về các thông số thống kê được biểu diễn trên ***IP Security Monitor***, xem "Các Thống kê Phương thức Chính và Phương thức Nhanh trong ***IP Security Monitor***").
- Xem các SA Phương thức Chính và Phương thức Nhanh.
- Xem các chính sách IKE Phương thức Chính.
- Xem các chính sách thỏa thuận Phương thức Nhanh.
- Tùy chỉnh tần suất làm mới, và sử dụng sự phân giải tên DNS cho bộ lọc và SA chiều ra.
- Tìm kiếm các bộ lọc Phương thức Chính và Phương thức Nhanh nhất định thỏa mãn bất ký địa chỉ IP đi hay đến nào, địa chỉ IP đi hay đến trên máy tính cục bộ, hay địa chỉ IP đi hay đến nhất định nào đó.

Sử dụng IP Security Monitor để theo dõi lưu thông IPSec

Nếu chính sách IPSec đã được kích hoạt, bạn có thế sử dụng ***IP Security Monitor*** (như chỉ ra trong hình 6-7) để kiểm tra chính sách và các hoạt động của nó. Bạn chỉ có thể theo dõi IPSec chỉ trên các máy tính chạy hệ điều hành Windows XP hay Windows Server 2003. Để theo dõi IPSec trên máy tính chạy Windows 2000, sử dụng lệnh ***IPSecmon*** tại dấu nhắc lệnh. Các thông tin bạn có thể nhận được bao gồm:

- Tên của chính sách IPSec hiện đang kích hoạt.
- Các chí tiết của chính sách đang kích hoạt.
- Các thông số thống kê Chế độ Nhanh.
- Các thông số thống kê Chế độ Chính.
- Các thông tin về các SA hiện hành.



Hình 6-7: IP Security Monitor

Tìm hiểu các thông số thống kê Chế độ Chính và Chế độ Nhanh trong IP Security Monitor.

Việc xem các thông số thống kê có thể thực hiện rất đơn giản bằng cách mở rộng nút ***Server***, tiếp tục mở rộng nút ***Main mode*** hay ***Quick mode*** sau đó chọn nút ***Statistics***. Xong việc hiểu rõ ý nghĩa của từng thông số thì lại khó hơn nhiều. Bảng 6-1 mô tả các thông số thông dụng nhất của các thông số thống kê của Chế độ chính. (bảng 6-2 mô tả các thông số thống kê thông dụng nhất của Chế độ Nhanh). Trong bảng 6-1, có một vài thông sô thống kê có liên quan đến Chế độ Nhanh. Mặc dù chúng có liên quan nhưng do chúng được khởi tạo trong quá trình thỏa thuận IKE Chế độ Chính, do vậy, chúng được kể vào như là một phần của bảng các thông số thống kê Chế độ Chính.

Bảng 6-1: Các thông số thống kê IPSec Chế độ Chính

Thông số	**Mô tả**
Active Acquire	Số lượng các yêu cầu đang chờ thỏa thuận IKE cho các SA giữa các cặp IPSec
Active Receive	Số lượng các thông điệp IKE trong hàng đợi xử lý
Acquire Failures	Số lượng các yêu cầu chiều ra để thiết lập SA bị lỗi kể từ khi dịch vụ IPSec khởi động
Receive Failures	Số lượng các lỗi được tìm thấy trong các thông điệp

	IKE đã nhận kể từ khi địch vụ IPSec khởi động lần cuối.
Send Failures	Số lượng các lỗi xẩy ra khi gửi IKE kể từ khi dịch vụ IPSec khởi động lần cuối.
Acquire Heap Size	Số lượng các yêu cầu chiều ra để thiết lập SA thành công.
Receive Heap Size	Số lượng các thông điệp có trong bộ đệm nhận IKE.
Authentication Failures	Số các lỗi xác thực xẩy ra kể từ khi dịch vụ IPSec khởi động lần cuối. Trong trường hợp bạn không thể thiết lập kết nối IPSec, cần kiểm tra xem các lỗi xác thực có tăng lên trong quá trình kết nối hay không. Nếu chúng tăng, lối xác thực chính là nguyên nhân của việc không thiết lập được kết nối IPSec. Kiểm tra các thông số bảo mật được chia sẻ là phù hợp, các thành viên trong cặp IPSec là cùng một miền, và các giấy chứng nhận là đúng.
Negotiation Failures	Số các thỏa thuận Chế độ Chính bị lỗi kể từ khi địch vụ IPSec khởi động lần cuối. Thực hiện kết nối và quan sát xem số lỗi thỏa thuận có tăng lên không. Nếu chúng tăng, kiểm tra các thông số thiết lập phương thức bảo mật và xác thực để phát hiện các cấu hình sai hay không phù hợp.
Invalid Cookies Received	Tổng số các ***Cookies*** không phù hợp với SA Chế độ Chính hiện tại kể từ khi dịch vụ IPSec khởi động lần cuối. ***Cookies*** là giá trị có chứa trong thông điệp IKE nhận được được sử dụng để xác định SA Chế độ Chính phù hợp.
Total Acquire	Tổng số các yêu cầu đã được chuyển tới cho IKE kể từ khi dịch vụ IPSec khởi động lần cuối nhằm thiết lập SA. Số này bao gồm cả các kết quả nhận được trong SA mềm.
Total Get SPI	Tổng số các yêu cầu được do IKE gửi cho trình điều khiển IKE nhằm nhận được SPI duy nhất kể từ khi dịch vụ IPSec được khởi động lần cuối. SPI phải phù hợp với các gói tin chiều đến có chứa SA.
Key Additions	Tổng số các SA Phương thức Nhanh chiều ra được IKE thêm vào trình điều khiển IPSec kể từ khi dịch vụ IPSec được khởi động lần cuối.
Key Updates	Tổng số các SA Phương thức Nhanh chiều vào được

	IKE thêm vào trình điều khiển IPSec kể từ khi dịch vụ IPSec được khởi động lần cuối.
Get SPI Failures	Tổng số các yêu cầu đã được IKE chuyển tới trình điều khiển IPSec để nhận đươc SPI duy nhất bị lỗi kể từ khi dịch vụ IPSec được khởi động lần cuối.
Key Addition Failures	Tổng số các yêu cầu phụ SA Phương thức Nhanh chiều ra do IKE chuyển tới trình điều khiển IPSec bị lỗi kể từ khi dịch vụ IPSec khởi động lần cuối.
Key Update Failures	Tổng số các yêu cầu phụ SA Phương thức Nhanh chiều vào do IKE chuyển tới trình điều khiển IPSec bị lỗi kể từ khi dịch vụ IPSec khởi động lần cuối.
ISADB List Size	Số lượng các mục vào trạng thái Phương thức Chính. Số này bao gồm các SA Phương thức Chính đã được thỏa thuận thành công, các SA Phương thức Chính đang trong quá trình thỏa thuận, và các SA Phương thức Chính có thỏa thuận bị lỗi hay dã hết hạn nhưng chưa bị xóa.
Connection List Size	Số các thỏa thuận Phương thức Nhanh đang trong quá trình thực hiện.
IKE Main Mode	Tổng số các SA thành công đã được tạo ra trong quá trình thỏa thuận Phương thức Chính kể từ khi dịch vụ IPSec được khởi động lần cuối.
IKE Quick Mode	Tổng số các SA thành công đã được tạo ra trong quá trình thỏa thuận Phương thức Nhanh kể từ khi dịch vụ IPSec được khởi động lần cuối.
Soft Associations	Tổng số các SA được thiết lập với các máy tính không đáp ứng được các dự định thỏa thuận SA Phương thức Chính kể từ khi dịch vụ IPSec được khởi động lần cuối. Mặc dù các máy tính nói trên không đáp ứng được các dự định thỏa thuận Phương thức Chính nhưng chính sách IPSec vẫn cho phép liên lạc với các máy tính này. SA mềm là không được bảo mật như IPSec.
Invalid Packets Received	Tổng số các thông điệp IKE không hợp lệ đã nhận được kể từ khi dịch vụ IPSec được khởi động lần cuối. Số này bao gồm các thông điệp IKE có trường ***Header*** không hợp lệ, có độ dài thân gói tin (***Payload***) không đúng, các giá trị Cookie đáp sai. Các thông điệp IKE không hợp lệ phần lớn do việc truyền lại các thông

	điệp IKE, hay do các khóa chia sẻ trước không phù hợp giữa các thành viên trong cặp IPSec.

Bảng 6-2: Các thông số thống kê IPSec Chế độ Nhanh

Thông số	Mô tả
Active Security Association	Số lượng các SA Phương thức Nhanh
Offloaded Security Associations	Số lượng các SA Phương thức Nhanh sử dụng việc mã hóa phần cứng (***Hardware Offload***). Một số cạc mạng có thể tự xử lý các dữ liệu mã hóa nhằm tăng cường hiệu năng chung.
Pending Key Operations	Số lượng các hoạt động trao đổi khóa đang được thực hiện.
Key Additions	Số lượng các khóa dành cho SA Phương thức Nhanh đã được thêm thành công kể từ khi máy tính khởi động.
Key Deletions	Số lượng các khóa dành cho SA Phương thức Nhanh đã xóa thành công kể từ khi máy tính khởi động.
Rekeys	Số lượng các hoạt động làm mới khóa dành cho SA Phương thức Nhanh.
Active Tunnels	Số lượng các đường hầm đang hoạt động.
Bad SPI Packets	Số lượng các gói tin có SPI không đúng tính kể từ khi máy tính khởi động lần cuối. SPI có thể hết hạn hay các gói tin vừa đến đã quá cũ. Số này sẽ tăng lên nếu việc làm mới khóa là thường xuyên và có rất nhiều các SA. Nó cũng có thể là biểu hiện của các cuộc tấn công lừa đảo.
Packets Not Decrypted	Số lượng các gói tin không thể giải mã kể từ khi máy tính khởi động lần cuối. Gói tin có thể không được giải mã nếu việc kiểm tra đánh giá nó không thành công.
Packets Not Authenticated	Số lượng các gói tin mà các dữ liệu của nó không được kiểm chứng (việc kiểm chứng tính toàn vẹn của gói tin không thành công) kể từ khi máy tính được khởi động lần cuối. Chỉ số này tăng có thể là biểu hiện của việc tấn công lừa đảo hay thay dổi gói tin, nó cũng có thể là biểu hiện của các gói tin bị hỏng do các thiết bị mạng gây ra.
Packets With Replay Detection	Số lượng các gói tin có chứa số thứ tự sai kể từ khi máy tính khởi động lần cuối. Chỉ số này tăng có thể là

	biểu hiện của các cuộc tấn công lặp lại hay các trục trặc về mạng.
Confidential Bytes Sent	Số lượng các Byte đã được gửi sử dụng giao thức ESP kể từ khi máy tính được khởi động lần cuối.
Confidential Bytes Received	Số lượng các Byte đã nhận được sử dụng giao thức ESP (không tính các Byte ESP không mã hóa) kể từ khi máy tính được khởi động lần cuối.
Authenticated Bytes Sent	Số lượng các Byte đã được xác thực được gửi sử dụng giao thức ESP hoặc giao thức AH kể từ khi máy tính được khởi động lần cuối.
Authenticated Bytes Received	Số lượng các Byte đã được xác thực nhận được sử dụng giao thức ESP hoặc giao thức AH kể từ khi máy tính được khởi động lần cuối.
Transport Bytes Sent	Số lượng các Byte được gửi sử dụng phương thức vận chuyển IPSec kể từ khi máy tính được khởi động lần cuối.
Transport Bytes Received	Số lượng các Byte nhận được sử dụng phương thức vận chuyển IPSec kể từ khi máy tính được khởi động lần cuối.
Bytes Sent In Tunnels	Số lượng các Byte được gửi sử dụng phương thức đường hầm IPSec kể từ khi máy tính được khởi động lần cuối.
Bytes Received In Tunnels	Số lượng các Byte nhận được sử dụng phương thức đường hầm IPSec kể từ khi máy tính được khởi động lần cuối.
Offloaded Bytes Sent	Số lượng các Byte được gửi sử dụng phương thức mã hóa phần cứng kể từ khi máy tính khởi động lần cuối.
Offloaded Bytes Received	Số lượng các Byte nhận được sử dụng phương thức mã hóa phần cứng kể từ khi máy tính khởi động lần cuối.

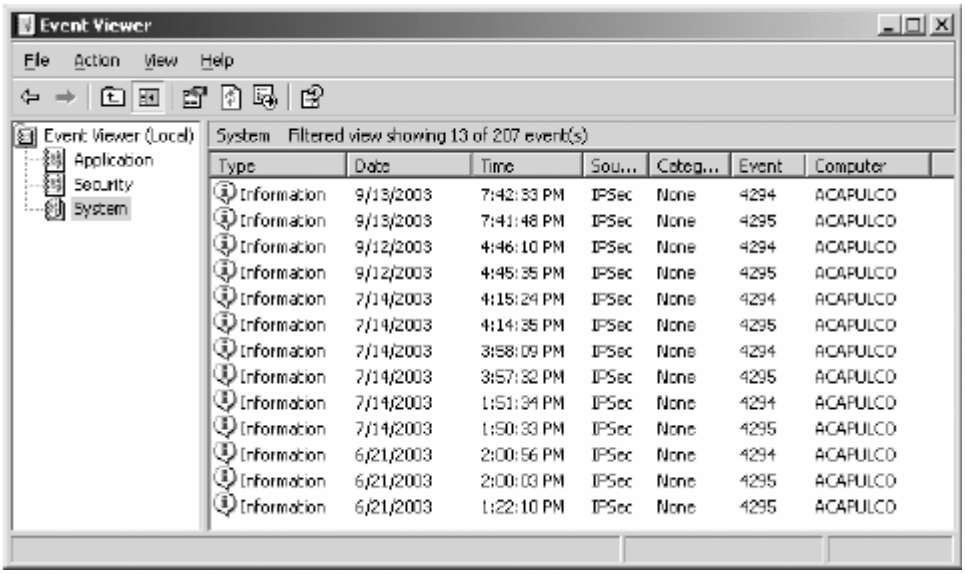
Sử dụng RSoP

Bên cạnh việc xem các chính sách bằng ***IP Security Monitor (****Trình Theo dõi Bảo mật IP****),*** bạn có thể sử dụng RSoP để xác định các chính sách IPSec đã được gán, nhưng chúng không được ứng dụng cho các náy khách IPSec. Snap-in RSoP chỉ hiển thị các thiết lập IPSec chi tiết. Nó hiển thị các luật bộ lọc, các hành động bộ lọc, phương thức xác thực, các đầu đường hầm, và kiểu kết nối của chính sách đang được áp dụng.

Sử dụng Event Viewer

Bạn có thể sử dụng ***Event Viewer*** để xem các sự kiện liên quan đến IPSec (Hình 6-8):

- Các sự kiện ***IPSec Policy Agent*** trong Nhật ký Kiểm toán
- Các sự kiện trình điều khiển IPSec trong Nhật ký Hệ thống
- Các sự kiện IKE trong Nhật ký Kiểm định
- Các sự kiện thay đổi chính sách IPSec trong Nhật ký Kiểm định



Hình 6-8: Event Viewer đã được lọc để xem các sự kiện IPSec

> ***LƯU Ý: Tăng kích thước của nhật ký sự kiện*** *Nếu bạn kích hoạt việc ghi nhật ký kiểm định, bạn có thể làm cho nhật ký sự kiện nhanh chóng được điền đầy với các sự kiện. Trong trường hợp bạn định kiểm định với một số lượng lớn các sự kiện, cần chắc chắn rằng bạn đã tăng kích thước của file nhật ký sự kiện đủ lớn để có thể chứa được toàn bộ các sự kiện cần ghi lại.*

Sử dụng nhật ký Oakley

Bạn có thể sử dụng nhật ký Oakley để xem chi tiết của quá trình thiết lập SA. Nhật ký Oakley có thể được kích hoạt thông qua ***Registry*****, (**mặc định chúng không được kích hoạt). Để kích hoạt nhật ký Oakley, bạn đặt giá trị của khóa ***HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services \PolicyAgent\Oakley\EnableLogging*** trong ***Registry*** bằng 1.

Nhật ký Oakley ghi lại toàn bộ các sự kiện thỏa thuận ISAKMP Phương thức Chính và Phương thức Nhanh. Một File nhật ký Oakley mới sẽ được tạo ra mỗi khi ***IPSec Policy Agent*** khởi động, và phiên bản trước của file nhật ký này sẽ được lưu dưới dạng ***Oakley.log.sav.***

Sử dụng Netsh

Netsh là công cụ dạng dòng lệnh của Windows Server 2003 mà bạn có thể sử dụng để hiển thị hay thay đổi cấu hình mạng của các máy tính chạy Windows Server 2003 cục bộ hay từ xa. Bạn có thể chạy ***Netsh*** từ một file bó (***batch file***) hay tại dấu nhắc lệnh. Bạn có thể sử dụng các lệnh ***Netsh*** dành cho IPSec để cấu hình các chính sách IPSec chỉ trên các máy tính chạy các phiên bản của họ hệ điều hành Windows Server 2003.

> ***THÔNG TIN THÊM: Các lệnh Netsh dành cho IPSec*** *Để có danh sách đầy đủ của các lệnh* ***Netsh*** *dành cho IPSec, trong* ***Help And Support Center*** *của Windows Server 2003, nhấn* ***Tools,*** *nhấn* ***Command Line Reference,*** *sau đó duyệt và nhấn* ***Netsh Commands For Internet Protocol Security (IPSec).***

Để thiết lập ngữ cảnh IPSec của lệnh ***Netsh***, nhập từ ***Static*** hay ***Dynamic*** tại dấu nhắc ***Netsh IPSec***. *Ngữ cảnh* ***(context)*** là một tập xác định của các lệnh được bố trí trong phạm vi của cấu trúc hình cây. Ví dụ, để truy cập các lệnh có thể có trong ngữ cảnh IPSec, gõ ***IPSec*** tại dấu nhắc ***Netsh (Netsh>)***. Sau khi bạn lựa chọn ngữ cảnh, bạn có thể sử dụng các lệnh ***Netsh*** để tạo chính sách hay theo dõi các hoạt động IPSec. Lệnh ***Netsh*** trong ngữ cảnh IPSec có hai chế độ: Chế độ tĩnh (***Static mode***) cho phép bạn tạo, thay đổi hay gán các chính sách mà không hề làm ảnh hưởng đến chính sách IPSec đang hoạt động. Chế độ động (***Dynamic mode***) cho phép bạn hiển thị trạng thái hiện thời và thực hiện các thay đổi ngay lập tức đối với chính sách IPSec đang hoạt động. Các lệnh ***Netsh*** chế độ động chỉ ảnh hưởng đến dịch vụ IPSec khi nó đang chạy. Trong trường hợp dịch vụ này đang dừng, các thiết lập chính sách chế độ động sẽ bị hủy bỏ.

> ***LƯU Ý: làm cho các thay đổi chế độ động có hiệu lực tức thời***
> *Nếu bạn bắt buộc phải khởi tạo các thay đổi cho quá trình xử lý IPSec một cách tức thời, sử dụng Chế độ động là rất hiệu quả do các lệnh đưa ra tại chế độ này sẽ được thức hiện một cách tức thời (ngoại trừ khi dịch vụ bắt buộc phải dừng và khởi động lại). Mặc dù vậy, Chế độ động cũng ẩn chứa các rủi ro, trong trường hợp bạn phạm phải sai lầm trong khi thực hiện lênh* ***Netsh*** *ở chế độ động, bạn sẽ không có cơ hội tìm hiểu nó trước khi thực hiện các thay đổi,*

do vậy, bạn có thể vô tình tạo ra các cấu hình sai mà không có bất cứ một cảnh báo nào.

Sử dụng Netsh để theo dõi IPSec

Bạn có thể sử dụng ***Netsh*** để theo dõi phiên làm việc IPSec hiện tại. Việc theo dõi bao gồm việc hiển thị các thông tin chính sách, thực hiện các chuẩn doán và ghi nhật ký các thông tin IPSec. Bất cứ thông tin nào bạn có thể tìm thấy với Snap-in ***IP Security Monitor***, bạn cũng có thể tìm thấy với lệnh ***Netsh***. Để nhận được các thông tin về cú pháp của lệnh ***Netsh***, tại dấu nhắc lệnh, bạn gõ ***Netsh /?***, sau đó nhấn ***ENTER***.

Hiển thị các thông tin IPSec

Để tìm ra chính sách IPSec hiện tại là gì, ta sử dụng lệnh ***Show***. Nếu bạn chọn sử dụng lệnh ***Show all***, ta sẽ nhận được rất nhiều thông tin, như hiển thị trong hình 6-9 (lưu ý rằng chỉ một phần của các thông tin là được hiển thị trong hình này).

Hình 6-9: Các thông tin được xuất ra từ lệnh *Show All*

Do có một số lượng lớn các thông tin về cấu hình IPSec, nên sẽ là hiệu quả hơn nếu chúng ta chỉ xem một phần của chúng. Một vài lệnh con của lệnh ***Show*** có thể giúp chúng ta thực hiện điều này. Bảng 6-3 trình bầy một vài lệnh con trong số đó. Bạn có thể nhập tất cả các lệnh từ ngữ cảnh IPSec của lệnh ***Netsh*** trong chế độ tĩnh hay chế độ động, hoặc, với sự thay đổi, từ dấu nhắc lệnh

Bảng 6-3: Lệnh *Netsh IPSec Show Static*

Hoạt động	**Lệnh**
Để hiển thị danh sách các bộ lọc nhất định, sử dụng…	**show filterlist name =*filterlistname***

Để hiển thị chính sách đã gán cho GPO, sử dụng…	**show gpoassignedpolicy name =*name***
Để hiển thị một chính sách nhất định, sử dụng…	**show policy name =*policyname***
Để hiển thị một luật nhất định, sử dụng …	**show rule name =*rulename***

Thu nhận các thông tin chuẩn đoán IPSec

Một trong các bước trong quá trình chuẩn đoán các sự cố IPSec – hay thiết lập chính sách sẽ làm việc theo đúng những gì bạn dự định – là thu thập các thông tin về chính sách hiện hành. Các lệnh ***Show*** được mô tả trong bảng 6-3 cung cấp cho chúng ta các thông tin như vây. Thông tin mà mỗi lệnh hiển thị sẽ xác định các thiết lập trong chính sách. Ví dụ, lệnh ***Show Filterlist*** sẽ liệt kê các thông tin trong danh sách bộ lọc của các chính sách. Một số ví dụ về cú pháp của lệnh ***Show*** được trình bầy trong bảng 6-4. Tại bảng 6-5, trong các lệnh, dấu bằng (=) là một phần của lệnh và bạn cần thay từ ***value*** (*in nghiêng*) bằng các giá trị xác định.

Bảng 6-4: Mô tả cú pháp của lệnh *Show*

Command	Description
show config	Hiển thị cấu hình IPSec và các hành vi trong thời gian khởi động.
show mmsas	Hiển thị các thông tin về IPSec SA Phương thức Chính . bạn có thể thấy các địa chỉ nguồn và đích. Khi sử dụng cùng khóa ***Resolvedns=yes***, tên của máy tính sẽ được hiển thị.
show qmsas	Hiển thị các thông tin về IPSec SA Phương thức Nhanh.
show stats	Hiển thị các thông số thống kê IKE, IPSec Phương thức Nhanh, hoặc cả hai. Các thông số thống kê cũng giống như đã mô tả trong bảng 6-2.

Bên cạnh các lệnh ***Show***, bạn có thể sử dụng các lệnh chuẩn doán ***Netsh IPSec*** chế độ động để thu các thông tin chuẩn đoán, như liệt kê trong bảng 6-5 dưới đây.

Bảng 6-5: Các lệnh chuẩn đoán *Netsh IPSec Chế độ Động*

Lệnh	Mô tả
set config property= ipsecdiagnostics value=*value*	Có thể đặt với giá trị ***Value*** từ 0 tới 7, xác định mức độ chi tiết của nhật ký chuẩn đoán IPSec. Giá trị mặc định là 0, điều đó có nghĩa là việc ghi nhật ký không được thực hiện. Cấp độ 7 sẽ làm cho hệ thống ghi lại toàn bộ các thông tin chuẩn đoán. Máy tính nhất định phải được khởi động lại để việc ghi nhật ký được thực hiện.
set config property= ipseclogginterval value=*value*	Chỉ định tần xuất (tính theo giây) các sự kiện IPSec được gửi tới cho nhật ký sự kiện hệ thống. Thông số ***Value*** có giá trị nằm trong khoảng từ 60 đến 86.400, mặc định là 3600.
set config property= ikelogging value=*value*	Có thể đặt giá trị ***Value*** là 0 hay 1, xác định việc ghi nhật ký IKE (Oakley) có xẩy ra hay không. Lệnh này sẽ sinh ra một file nhật ký với số lượng lớn các thông tin. Bạn phải hiểu rõ các RFC (*Requests for Comments*) như một chuyên gia để có thể hiểu được các nhật ký Oakley.
set config property= strongcrlcheck value=*value*	Xác định việc kiểm tra Danh sách Thu hồi Giấy chứng nhận (***Certificate Revocation List* - CRL)** có được tiến hành hay không. Nếu ***Value*** là 0, chế độ kiểm tra được tắt. nếu ***Value*** là 1, việc kiểm chứng giấy chứng nhận sẽ bị lỗi chỉ khi giấy chứng nhận đã bị thu hồi. Khi ***Value*** là 2, việc kiểm chứng sẽ lỗi khi có bất cứ một lỗi nào trong việc kiểm tra CRL. Việc kiểm tra CRL sẽ là lỗi nếu CRL không thể định vị trên mạng. Bạn có thể thực hiện các chuẩn đoán khác bằng cách thay đổi chính sách hiện tại nhằm giảm mức độ bảo mật. Ví dụ, khi bạn đổi việc xác thực sang ***Shared Secret*** trên cả hai máy tính thay vì sử dụng ***Kerberos*** hay ***Certificate***, bạn sẽ loại trừ được khả năng các trục trặc liên quan đến việc xác thực gây ra.

Sử dụng *Netdiag*

Netdiag là công cụ dạng dòng lệnh bạn có thể sử dụng để hiển thị các thông tin IPSec, thử và xem các cấu hình mạng. ***Netdiag*** hiện có trong Windows Server 2003, Windows 2000, và Windows XP. Mặc dù vậy, chúng được cài đặt theo các phương thức khác nhau đối với mỗi hệ điều hành. Đối với Windows Server 2003, ***Netdiag*** được cài đặt cùng với ***Windows Server 2003 Support Tools***, Đối với Windows 2000, ***Netdiag*** có sẵn trong các công cụ của ***Windows 2000 Resource Kit*** mà bạn có thể tải về từ Internet. ***Netdiag*** cũng có sẵn trong đĩa cài đặt của Windows XP và sẽ được cài đặt nếu bạn chạy ***Setup*** trong thư mục ***Support Tools*** của đĩa CD cài đặt.

Bạn có thể nhận được các thông tin chuẩn đoán tổng quát về mạng (nhưng không có các thông tin IPSec) bằng cách sử dụng lệnh ***Netdiag***. Ví dụ, lệnh ***netdiag /v /l*** sẽ cung cấp các cấu hình IP và cấu hình định tuyến của máy tính, thử việc phân giải tên DNS và WINS, thông báo số phiên bản của hệ điều hành và các bản sửa lỗi nóng đã được cài đặt, và kiểm tra các mỗi quan hệ tin cậy. Toàn bộ các thông tin này là rất hữu dụng khi bạn cần loại trừ các vấn dề mạng thông thường trước khi bạn tiến hành các việc chuẩn đoán IPSec.

> ***LƯU Ý: Sử dụng Netsh thay cho Netdiag*** *Mặc dù lệnh* ***netdiag*** *là có sẵn trong Windows Server 2003, nhưng lựa chọn* ***Netdiag /test:IPSec*** *đã được dỡ bỏ. Sử dụng lệnh* ***netsh*** *để thay thế. Sử dụng* ***Netdiag*** *cho các phiên bản trước của hệ điều hành Windows. Để có thể khảo sát từ xa chính sách IPSec trên các máy tính chạy Windows XP hay Windows 2000, cân nhắc việc sử dụng các phiên làm việc toàn màn hình từ xa (****Remote Destop****)và công cụ* ***Netdiag****.*

TỔNG KẾT

- IPSec là một phương thức chuẩn để cung cấp các dịch vụ bảo mật cho các gói IP.
- Giao thức ESP cung cấp tính riêng tư (bên cạnh các tính xác thực, toàn vẹn, và duy nhất) cho thân gói tin IP, trong khi đó giao thức AH cung cấp tính xác thực, toàn vẹn và duy nhất cho toàn bộ gói tin.
- Có hai loại SA được tạo ra khi các đối tác trong cặp IPSec thực hiện liên lạc bảo mật: SA ISAKMP và SA IPSec.
- Để thỏa thuận SA dành cho việc gửi các thông tin bảo mật, IPSec sử dụng IKE, một tổ hợp của ISAKMP và giao thức ***Oakley Key Determination*** (*Giao thức Xác định Khóa Oakley*). Thông điệp ISAKMP có thể chứa rất nhiều loại khác nhau của thân thông điệp (***Payload***) để trao đổi thông tin trong quá trình thỏa thuận SA.
- Thỏa thuận Phương thức Chính được sử dụng để thiết lập SA ISAKMP, mà nó được dùng để bảo vệ cho các thỏa thuận Phương thức Chính sau này và toàn bộ các thỏa thuận Phương thức Nhanh.
- Thỏa thuận Phương thức Nhanh được sử dụng để thiết lập SA IPSec dùng để bảo vệ dữ liệu.
- Các giấy chúng nhận giúp thực hiện việc xác thực giữa các hệ thống không chia sẻ cùng kết cấu hạ tầng xác thực trung tâm dựa trên giao thức Kerberos.
- Bạn có thể sử dụng lệnh ***Netsh IPSec*** tại chế độ tĩnh để tạo và gán các chính sách IPSec, thêm các chính sách cố định, và thay đổi các tính năng cấu hình khác.

BÀI TẬP

QUAN TRỌNG: Hoàn thành tất cả các bài tập *Nếu bạn có ý định làm bất kể bài tập nào trong sách này, bạn bắt buộc phải hoàn thiện tất cả các bài tập nhằm đưa máy tính trở về trang thái ban đầu để chuẩn bị cho các bài tập trong sách BÀI TẬP THỰC HÀNH.*

Bài tập 6-1: Thêm chính sách bảo mật IPSec

1. Nhấn ***Start***, trỏ đến ***Administrative Tools,*** và nhấn ***Domain Controller Security Policy.***
2. Tại khung phạm vi của bảng điều khiển, mở rộng ***Security Settings***, và nhấn ***IP Security Policies On Active Directory***.
3. Trên thực đơn ***Action***, nhấn ***Create IP Security Policy***.
4. Trên trang ***Welcome To The IP Security Policy Wizard***, nhấn ***Next***.
5. Trên trang ***IP Security Policy Name,*** trong hộp ***Name***, gõ "***security policy example"***, và sau đó nhấn ***Next***.
6. Trên trang ***Requests For Secure Communication***, kiểm tra để chắc chắn rằng hộp lựa chọn ***Activate The Default Response Rule*** đã được đanh dấu, và nhấn ***Next***.
7. Trên trang ***Default Response Rule Authentication Method,*** Kiểm tra hộp lựa chọn ***Active Directory Default (Kerberos V5 Protocol)*** đã được đánh dấu, và nhấn ***Next***.
8. Trên trang ***Completing The IP Security Policy Wizard***, nhấn ***Finish***.

Bài tập 6-2: Cấu hình IPSec để sử dụng Giấy chứng nhận (Certificate).

Để cấu hình IPSec để sử dụng Giấy chứng nhận, làm theo các bước sau đây:

1. Nhấn ***Start***, nhấn ***Run***, nhập "***mmc"*** vào hộp ***Open***, và nhấn ***OK***.
2. Trong cửa sổ ***Console1***, trên thực đơn ***File***, nhấn ***Add/Remove Snap-In***.

3. Trong của sổ ***Add/Remove Snap-In***, nhấn ***Add***.
4. Trong cửa sổ Add Standalone Snap-In, nhấn IP Security Policy Management, và nhấn Add.
5. Trong cửa sổ ***Select Computer Or Domain***, kiểm tra để chắc chắn tùy chọn ***Local Computer***, và nhấn ***Finish***.
6. Trong của sổ Add Standalone Snap-In, nhấn Close.
7. Trong của sổ ***Add/Remove Snap-In***, nhấn ***OK***.
8. Trong khung phạm vi, nhấn IP Security Policies On Local Computer.
9. Trong khung chi tiết, nhấn đúp chuột trên ***Security Policy Example*** (mà bạn đã tạo ra trong bài tập 6-1).
10. Trong cửa sổ ***Security Policy Example Properties,*** nhấn đúp chuột trên ***default response rule*** (luật đáp mặc định).
11. Trong hộp thoại ***Edit Rule Properties,*** tại thẻ ***Authentication Methods,*** nhấn ***Add.***
12. Chọn ***Use A Certificate From This Certification Authority (CA),*** và nhấn ***Browse***.
13. Trong hộp thoại ***Select Certificate***, nhấn ***Microsoft Root Certificate Authority,*** và nhấn ***OK***.
14. Trong cửa sổ ***New Authentication Method Properties***, nhấn ***OK***.
15. Trong cửa sổ ***Edit Rule Properties***, nhấn ***OK***.
16. Trong cửa sổ ***Security Policy Example Properties***, nhấn ***OK***.

Bài tập 6-3: Sử dụng Netsh để hiển thị các thông tin IPSec

1. Mở cửa sổ dấu nhắc lệnh.
2. Tại dấu nhắc lệnh, gõ "***netsh"***, và nhấn ***ENTER***. Dấu nhắc lệnh được đổi thành ***netsh>***.

3. Tại dấu nhắc lệnh, để chuyển sang ngữ cảnh IPSec tĩnh, gõ "***ipsec static"***, và nhấn ***ENTER***.

4. Tại dấu nhác lệnh, để xem các thông tin về chính sách IPSec ***Security Policy Example***, nhập "***show policy "security policy example""***, và nhấn ***ENTER***.

5. Để hiển thị luật tương ứng với chính sách IPSec ***Security Policy Example***, tại dấu nhắc lệnh, nhập "***show rule all "security policy example""***, và nhấn ***ENTER***.

Lưu ý danh sách của Giấy chứng nhận bạn đã thêm trong bài tập 6-2.

CÂU HỎI ÔN TẬP

1. Mệnh đề nào sau đây mô tả chính xác nhất chức năng của luật chính sách mặc định ***Clent (Respond Only).***

    a. Máy khách chỉ đáp lại các yêu cầu được bảo mật bởi IPSec

    b. Máy khách sẽ đáp lại các yêu cầu không được bảo mật, nhưng chỉ đáp lại bằng cách sử dụng IPSec.

    c. Máy khách sẽ đáp lại các yêu cầu không được bảo mật bằng các các lời đáp không bảo mật, nhưng sẽ đáp lại các yêu cầu bảo mật với các lời đáp bảo mật.

    d. Máy khách sẽ chỉ đáp lại máy chủ nếu chúng có thể thực hiện được việc truy vấn ngược (***Reverse lookup***) địa chỉ IP của máy chủ

2. Công ty Fabrikam Inc. thực hiện việc đưa hai máy chủ gia nhập miền của công ty. Sau khi việc gia nhập của các máy chủ hoàn tất, công ty không thể thực hiện các trao đổi thông tin trên mạng. bạn chuẩn đoán rằng việc áp dụng các chính sách IPSec đã gây ra vấn đề này. Công cụ nào bạn sẽ sử dụng để xác định chuẩn đoán của bạn là đúng?

    a. Network Monitor

    b. Nhật ký Bảo mật trong ***Event Viewer***

    c. Resultant Set of Policies (RSoP – Tập hậu quả của các chính sách)

    d. IP Security Monitor

3. Bạn muốn xác định liệu SA Phương thức Nhanh có hiện hữu tại thời diểm hiện tại không. Bạn có thể sử dụng công cụ nào sau đây để thực hiện việc này?

    a. RSoP

    b. Event Viewer

    c. File nhật ký ***Oakley***

d. IP Security Monitor

4. IPSec có thể dược sử dụng để bảo mật các liên lạc giữa hai máy tính. Nguyên nhân nào sau đây là thỏa đáng để sử dụng IPSec? Chọn tất cả các phương án đúng.

a. Kiểm tra các thẻ Kerberos.

b. Cấm vận chuyển các gói tin sử dụng một giao thức nhất định nào đó.

c. Cho phép vận chuyển các gói tin có cổng TCP đích là 23 từ bất cứ máy tính nào đến máy chủ.

d. Cho phép một người dùng sử dụng ***Telnet*** để truy cập máy tính, trong khi cấm tất cả các người dùng khác.

5. Nguyên nhân nào là thỏa dáng để gán chính sách IPSec bằng cách sử dụng ***Netsh*** thay cho sử dụng Chính sách Nhóm?

a. Sử dụng ***Netsh*** là cách duy nhất để áp dụng chính sách mà có thể được dùng để cho phép máy tính của một người dùng sử dụng phiên làm việc ***Telnet*** với máy tính khác, trong khi vẫn cấm tất cả các liên lạc ***Telnet*** khác.

b. Sử dụng ***Netsh*** là dễ dàng thực hiện hơn so với Chính sách Nhóm khi phải cấu hình nhiều máy tính.

c. Bạn có thể sử dụng ***Netsh*** thậm chí cả với các máy tính không gia nhập miền, trong khi đó Chính sách nhóm chỉ có thể áp dụng với các máy tính thuộc miền.

d. Bạn có thể sử dụng ***Netsh*** để tạo ra các chính sách cố định trong trường hợp không thể sử dụng Chính sách Nhóm.

6. ***Netsh*** được sử dụng để tạo và gán chính sách IPSec cho máy chủ độc lập chạy Windows Server 2003. Một trog các lệnh được sử dụng trong ngữ cảnh ***Netsh IPSec static*** như sau:

Add rule name="SMTPBlock" policy="smtp" filterlist="smtp computerlist" filteraction="negotiate smtp" description="this rule negotiates smtp"

Tại sao chính sách trên không hoạt động?

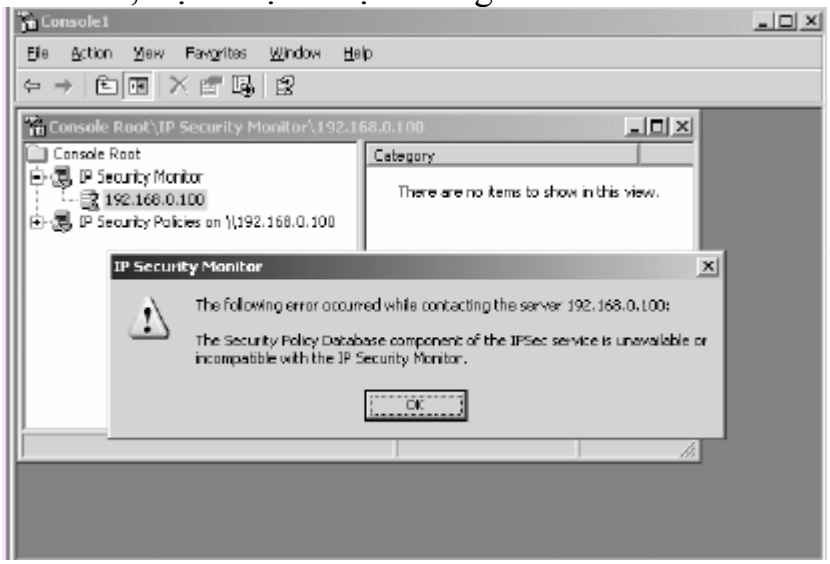
a. Chính sách đã được thiết lập với địa chỉ IP sai.

b. Mỗi chính sách chỉ định một thuật toán mã hóa khác nhau.

c. Máy chủ độc lập không có dịch vụ SMTP, do vậy chính sách là không được gán.

d. Chính sách sử dụng Kerberos để xác thực, và máy tính không phải là thành viên của miền.

7. Bạn muốn cài đặt một công cụ để duy trì và theo dõi các chính sách IPSec trên các máy tính ở xa trong miền của bạn. Bạn thêm các Snap-in ***IP Security Monitor*** and ***IP Security Policy Management*** vào trong bảng điều khiển của mình. Mặc dù vậy, khi bạn thử thêm máy tính 192.168.0.100 vào ***IP Security Monitor***, bạn nhận được thông báo lỗi như hình 6-10 sau đây:



Hình 6-10: Thông báo lỗi của bảng điều khiển IPSec

Bạn làm thế nào để quản trị và theo dõi IPSec trên máy tính 192.168.0.100:

a. Bạn không thể thực hiện được việc này. Máy tính 192.168.0.100 không hỗ trợ IPSec.

b. Máy tính 192.168.0.100 không phải là thành viên của miền. Bạn nhất thiết phải đưa máy tính trên gia nhập miền của bạn nếu bạn muốn sử dụng ***IP Security Monitor***.

c. Chỉ các chính sách IPSec sử dụng phương thức xác thực của bạn mới có thể được quản lý và theo dõi bằng ***IP Security Monitor***. Bạn nhất thiết phải gán chính sách đó cho máy tính 192.168.0.100

d. Bạn cần sử dụng ***IPSecmon***.

e. Bạn không thể thêm máy tính bằng địa chỉ IP. Bạn băt buộc phải sử dụng tên DNS của máy tính.

8. Trong quá trình thử nghiệm các chính sách IPSec, máy trạm bạn sử dụng như là một máy tính thử nghiệm làm việc tốt và các lưu thông là được mã hóa. Mặc dù vậy khi bạn khôi phục lại việc thử nghiệm sau khi tiến hành một vài thay đổi trên các máy chủ, máy trạm này không thể liên lạc được với các máy chủ đó. Chính sách bạn đặt trên máy chủ yêu cầu sử dụng Kerberos như là một giao thức xác thực. Nguyên nhân nào là dễ gây ra việc mất liên lạc nói trên nhất?

   a. Máy trạm của bạn mất kết nối tới Máy chủ Quản trị Miền (***Domain Controller***).

   b. Máy trạm của bạn mất kết nối tới CA

   c. IPSec Policy Agent mất liên lạc với Máy chủ Quản trị Miền và bắt buộc phải khởi động lại.

   d. Bạn phải áp dụng lại chính sách IPSec trên máy chủ.

KỊCH BẢN TÌNH HUỐNG

Kịch bản tình huống 6-1: Bảo mật các Liên lạc

Bạn đang quản trị miền Active Directory Windows Server 2003. Tất cả các máy tính khách trong miền đều thuộc về OU cấp cao nhất có tên là ***Clients***, và toàn bộ các các máy chủ (trừ các Máy chủ Quản trị Miền) đều thuộc về OU cấp cao nhất ***Servers***. Các Máy chủ Quản trị Miền thuộc về OU mặc định của nó. Chính sách IPSec mặc định ***Secure Server (Require Security)*** được gán cho tất cả các máy chủ, bao gồm cả các Máy chủ Quản trị Miền. Chính sách IPSec ***Client (Respond Only)*** được gán cho tất cả các máy trạm. Tất cả các máy trạm đều chạy hệ điều hành Windows 2000 Professional.

Một vấn đề quản lý xẩy ra là các máy trạm của phòng ***Research*** không thể tiến hành liên lạc một cách bảo mật với nhau và với các máy trạm khác. Chỉ có bốn máy tính như vậy tồn tại. Trên một máy trong số đó, bạn tạo một chính sách tùy biến yêu cầu bảo mật các liên lạc. Bạn xuất chính sách đã tạo nói trên ra file và nhập nó vào cho ba máy tính còn lại. Bạn gán chính sách này cho cả bốn máy tính của phòng.

Tiếp theo, bạn sử dụng ***IP Security Monitor*** nằm trên một trong bốn máy tính và thấy rằng không có một SA nào được cài đặt giữa các máy trạm của phòng ***Research*** hay với các máy trạm còn lại của các phòng khác. Bạn sử dụng ***Network Monitor*** để chụp các lưu thông mạng và phát hiện ra rằng các lưu thông không mã hóa đang được chuyển qua lại giữa các máy tính của phòng ***Researrch***. Bước nào sau đây bạn sẽ cần thực hiện đầu tiên để giải quyết vấn đề trên.

a. Thay đổi phương thức xác thực trên chính sách tùy biến sang việc sử dụng khóa chia sẻ trước (***Preshared key***).

b. Thay đổi thuật toán mã hóa từ 3DES sang DES

c. Tạo một OU riêng

d. Chuyển các tài khoản của máy trạm trong phòng ***Research*** vào OU ***Servers***

Kịch bản tình huống 6-2: Khắc phục sự cố IPSec

Công ty của bạn không sử dụng mô hình Miền, thay vào đó, họ sử dụng mô hình Nhóm Làm việc. Nhóm làm việc ***Research*** có sáu máy trạm chạy Windows XP professional, bốn máy trạm chạy Windows 2000 professional, và hai máy chủ độc lập chạy Windows Server 2003. Liên lạc giữa các máy tính nói trên trong nhóm bắt buộc phải được bảo mật. Một thành viên của đội ngũ hỗ trợ kỹ thuật cấu hình và gán chính sách bảo mật IP cho tất cả các máy tính trong nhóm. Tất cả các máy đều có thể ***Ping*** các máy khác bằng cách sử dụng địa chỉ IP. Nhưng nhân viên của phòng ***Research*** không thể truy cập các file trên các máy chủ từ máy trạm của họ.

Bạn đăng nhập vào một trong các máy chủ sử dụng tài khoản ***Administrator*** cục bộ, truy cập đến ***Security Setting*** trong ***Local Computer Policy***, và bạn kích hoạt chính sách kiểm định các sự kiện đăng nhập thành công hay thất bại. Bạn mở ***Event Viewer*** và thấy sự kiện kiểm định thất bại số 547 trong nhật ký bảo mật. Nguyên nhân của thất bại này được mô tả ***"Failed to obtain Kerberos server credentials for the ISAKMP/ERROR_IPSEC_IKE***

service." - *(Quá trình nhận các thông số đăng nhập Kerberos của máy chủ dành cho dịch vụ **ISAKMP/ERROR_IPSEC_IKE** thất bại).* Nguyên nhân nào sau đây đã gây ra trục trặc trên:

a. Luật đáp mặc định không được kích hoạt.

b. Kerberos được chỉ định là phương thức xác thực ban đầu.

c. Thuật toán mã hóa 3DES được chỉ định, nhưng chúng không thể được sử dụng trên các máy tính chạy Windows 2000

d. Gán sai chính sách.

CHƯƠNG 7: SỬ DỤNG RRAS ĐỂ CẤU HÌNH ĐỊNH TUYẾN

Hoàn thành chương này bạn có khả năng:

■ Cấu hình Microsoft Windows Server 2003 hoạt động như một bộ định tuyến (router) trên mạng **LAN**.

■ Cấu hình và sửa lỗi truy cập quay số (dial-up) và truy cập từ xa qua mạng riêng ảo **VPN**.

■ Tìm hiểu cách thức làm việc của cơ chế chuyển đổi địa chỉ mạng (***Network Address Translation* - NAT**) và phương pháp cấu hình nó.

■ Quản trị các **giao thức định tuyến**, các **bảng định tuyến** và các **cổng định tuyến.**

■ Tìm hiểu xem một bảng định tuyến sẽ định hướng các gói tin như thế nào và sử dụng chế độ dòng lệnh và màn hình quản trị ***Routing And Remote Access (RRAS)*** để hiển thị bảng định tuyến.

■ Cấu hình và quản trị **các bộ lọc gói**.

■ Cấu hình định tuyến quay số theo yêu cầu và mô tả khi nào bạn nên sử dụng cơ chế này.

■ Cấu hình các chính sách RRAS nhằm cho phép hoặc ngăn cấm quá trình truy cập.

■ Tập trung hóa việc xác thực truy cập mạng và các chính sách bằng cách sử dụng RADIUS (***Remote Authentication Dial-In User Service*** - *dịch vụ xác thực người sử dụng truy cập từ xa tới hệ thống*) và IAS (***Internet Authentication Service*** – *dịch vụ xác thực Internet*).

■ Phân biệt các phương pháp xác thực truy cập từ xa và lựa chọn mô hình phù hợp nhất.

Định tuyến là một tiến trình truyền dữ liệu từ mạng LAN này sang mạng LAN khác trên một liên mạng. Nó được coi là nền tảng cung cấp cho quá trình truyền thông trên Internet và cho hầu hết tất cả các mạng. Nó đóng một vai trò chính trong các tổ chức có kết nối với thế giới Internet hoặc tổ chức

đó được chia thành nhiều phân đoạn mạng khác nhau. Định tuyến là một vấn đề rất phức tạp nhưng nếu bạn hiểu được một số khái niệm chính như: xác thực, nhận thực, định tuyến tĩnh và các chính sách thì bạn hoàn toàn có thể cấu hình, giám sát và sửa lỗi những vấn đề liên qua tới chúng. Dịch vụ ***Routing and Remote Access*** (hay còn được gọi là RRAS – dịch vụ định tuyến và truy cập từ xa) của Windows Server 2003 cung cấp các tính năng sau:

■ Kết nối các phân đoạn mạng LAN (hay còn gọi là các mạng LAN con) trong phạm vi một tổ chức doanh nghiệp.

■ Kết nối văn phòng của các chi nhánh với mạng Intranet của toàn công ty và chia sẻ các tài nguyên như thể chúng được kết nối với nhau bằng mạng LAN.

■ Cho phép các máy tính ở xa truy cập đến các tài nguyên trên mạng của công ty.

■ Cung cấp cơ chế định tuyến ***unicast*** đa giao thức đối với giao thức ***IP*** và ***AppleTalk***.

■ Sử dụng các giao thức định tuyến ***IP unicast*** tuân theo chuẩn:

- ***Open Shortest Path First*** (OSPF – một giao thức định tuyến sử dụng thuật toán SPF để lựa chọn đường đi tốt nhất đến đích)
- ***Routing Information Protocol*** phiên bản 1 và 2 (RIP – cũng là một giao thức định tuyến sử dụng cơ chế trao đổi thông tin với các ***router*** liền kề để xây dựng nên bảng định tuyến)
- Cung cấp các dịch vụ ***IP multicast*** (chế độ ***router IGMP*** và chế độ ***proxy IGMP***) cho phép lưu chuyển lưu lượng ***IP multicast***.

■ Sử dụng các dịch vụ ánh xạ địa chỉ IP (NAT) nhằm ẩn địa chỉ các mạng của văn phòng hoặc văn phòng tại gia đình đối với thế giới Internet.

■ Cho phép triển khai một dịch vụ lọc gói đơn giản (firewall đơn giản) trên bất kỳ một giao diện nào kết nối với thế giới bên ngoài thậm chí giao diện đó đã được cấu hình với NAT.

■ Sử dụng định tuyến quay số theo yêu cầu thông qua các đường truyền WAN quay số.

■ Hỗ trợ VPN bằng giao thức PPTP (***Point-to-Point Tunneling Protocol***) và L2TP (***Layer Two Tunneling Protocol***) trên nền giao thức IPSec (***Internet Protocol***) hay còn được gọi tắt là ***L2TP/IPSec***.

■ Hỗ trợ cơ chế hoạt động ***DHCP Relay Agent*** cho IP (Đây là một dịch vụ cho phép các máy trạm tại một văn phòng ở xa nhận địa chỉ IP động thông qua một máy chủ DHCP đặt tại trung tâm).

TỔNG QUAN VỀ DỊCH VỤ RRAS TRÊN WINDOWS SERVER 2003

Hầu hết mạng của các doanh nghiệp đều triển khai một vài thiết bị mạng thông dụng như: ***hub***, ***switch*** và ***router***. Chương này sẽ tập trung khả năng định tuyến của Windows Server 2003. Trước khi kiểm tra phân này, chúng ta sẽ cùng nhau điểm lại ba thiết bị mạng này và xác định một cách rõ ràng vai trò của ***router***.

Hub (đôi khi cũng được gọi là ***repeater***) hoạt động tại lớp 1 trong mô hình tham chiếu 7 lớp OSI. Do ***hub*** hoạt động tại lớp 1 (lớp vật lý) nên nó không xử lý bất kỳ dữ liệu nào mà nó nhận được. Thay vào đó nó đơn giản chỉ nhận tín hiệu đến và tái tạo lại chúng rồi chuyển đến tất cả các cổng của nó. ***Hub*** cho phép mở rộng kích thước mạng bằng cách gom nhiều phân đoạn lại thành một phân đoạn lớn hơn. Đối với tất cả các ***node*** được triển khai trên một mạng LAN, ***hub*** trong suốt đối với chúng.

> **Thông tin thêm:** ***Các lớp mô hình OSI*** *Để biết thêm thông tin về các lớp của mô hình OSI, tham khảo tài liệu Network+ Certification Training Kit, Second Edition (Microsoft Press, 2003).*

Không giống như ***hub***, ***switch*** (bộ chuyển mạch) kiểm tra địa chỉ nguồn và đích của khung dữ liệu đến và chuyển chúng đến cổng thích hợp dựa trên địa chỉ đích. Hầu hết các ***switch*** hoạt động tại lớp 2 của mô hình OSI (lớp liên kết dữ liệu - ***data-link layer***).

Các ***switch*** có nhiều đường dữ liệu song song. Chúng sử dụng các kết nối tạm thời hay kết nối ảo để liên kết các cổng nguồn và đích tại thời điểm chuyển khung dữ liệu đi (hay còn gọi là một phân đoạn của gói dữ liệu trên mạng LAN). Sau khi khung dữ liệu được chuyển từ nguồn tới đích, kết nối ảo sẽ bị dừng. Các ***switch*** hoạt động với tốc độ cao và không quá đắt nên chúng thường được sử dụng để phân đoạn một mạng LAN thành các phân đoạn nhỏ hơn. Qua đó nó sẽ giúp gia tăng tốc độ truyền dữ liệu trên mạng hiện thời.

Đúng như cái tên cuả mình, ***router*** (bô định tuyến) làm nhiệm vụ xác định các tuyến đường đi để gửi các gói dữ liệu trên mạng dựa trên địa chỉ của gói tin. Các ***router*** hoạt động tại lớp 3 của mô hình tham chiếu OSI (lớp mạng _ ***network layer***), do đó nó làm việc với các gói dữ liệu chứ không phải khung dữ liệu như ***switch***. Chính vì vậy mà ***router*** được xem như các thiết bị lớp 3. Phần mềm lớp 3 như IP hoặc IPX có nhiệm vụ tạo các gói dữ liệu này.

Các ***router*** được sử dụng trong các trường hợp sau:

■ Kết nối các mạng trên một mạng WAN ở xa nhau. Lưu lượng WAN thường được di chuyển trên nhiều đường đi và ***router*** có nhiệm vụ lựa chọn một đường đi nhanh nhất hoặc rẻ nhất.

■ Kết nối các mạng LAN khác nhau như mạng LAN sử dụng công chuẩn ***Ethernet*** tới đường trục FDDI (***Fiber Distributed Data Interface***).

Chú ý: ***Gateway và router*** *Các thuật ngữ* ***gateway*** *và* ***router*** *thường được sử dụng thay thế lẫn nhau mà không làm ảnh hưởng đến phương cách hoạt động của chúng. Về mặt kỹ thuật,* ***gateway*** *là một thiết bị dùng để chuyển đổi giữa các mạng của kiến trúc khác nhau như* ***NetWare*** *và* ***Microsoft Windows*** *chẳng hạn.* ***Router*** *là một thiết bị gửi các gói dữ liệu giữa hai hoặc nhiều phân đoạn mạng thông qua các địa chỉ IP.*

Một trong số những vai trò mà Windows Server 2003 có thể đóng là định tuyến mạng. Sử dụng Windows Server 2003 thay cho một ***router*** cứng, cho phép bạn nhận được tính năng ưu việt như: chi phí, quản trị và các tính năng tiên tiến khác so với thiết bị vật lý. Đó là do Windows Server 2003 đã tích hợp khả năng định tuyến của nó với các tính năng của hệ điều hành như: chính sách nhóm, tính năng bảo mật và các công cụ quản trị như MMC chẳng hạn.

Các ví dụ về định tuyến

Bạn có thể sử dụng các ***router*** trong nhiều cấu trúc và các cấu hình mạng khác nhau. Khi cấu hình một máy chủ cài đặt dịch vụ RRAS như một ***router***, bạn có thể xác định những lựa chọn sau:

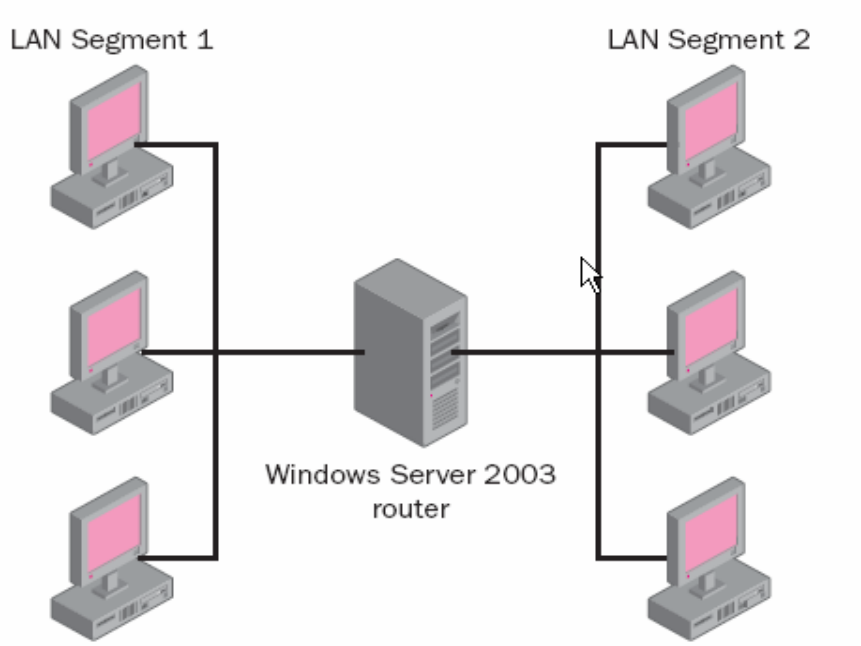
■ Các giao thức được định tuyến (***IP*** hay ***Apple Talk***) bởi các bọ định tuyến

■ Các giao thức định tuyến (***RIP***, ***OSPF***, ***IGMP*** và ***DHCP Relay***) cho mỗi giao thức được định tuyến

■ Các thiết bị trong môi trường mạng LAN hoặc WAN (các giao tiếp mạng, modem và thiết bị quay số khác)

Mô hình định tuyến đơn giản

Hình 7-1 mô phỏng một cấu hình mạng đơn giản với một máy chủ cài đặt dịch vụ RRAS kết nối hai phân đoạn mạng với nhau (***LAN Segment 1*** và ***LAN Segment 2***). Trong cấu hình này, ***router*** có nhiệm vụ kết hợp hai phân đoạn mạng này với nhau. Trong mô hình này, không cần sử dụng các giao thức định tuyến (***routing protocol***) do chỉ có một ***router***. Lý do bởi vì ***router*** được kết nối với cả hai mạng mà nó có nhiệm vụ định tuyến các gói tin nên bạn cũng không cần tạo ra các đường định tuyến tĩnh.



Hình 7-1: Hai phân đoạn mạng được kết nối nhau qua một router

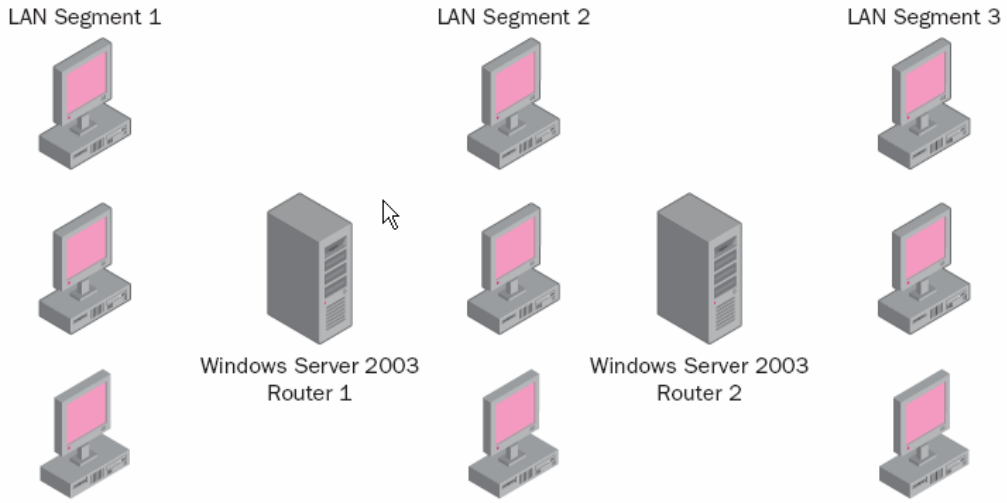
Mô hình định tuyến với nhiều routers

Hình 7-2 biểu diễn một mô hình định tuyến phức tạp hơn. Ở đây có tất cả 03 mạng (***LAN Segment*** (*phân đoạn mạng*) 1,2 và 3) được kết nối với nhau bởi 02 ***router*** (***router*** 1 và 2).

Router 1 được kết nối trực tiếp với phân đoạn 1 và 2 còn ***Router*** 2 thì kết nối trực tiếp với phân đoạn 2 và 3. ***Router*** 1 phải thông báo cho ***Router*** 2 rằng muốn kết nối đến phân đoạn 1 thì phải thông qua nó và ngược lại ***Router*** 2 cũng thông báo cho ***Router*** 1 về phân đoạn 3. Quá trình thông báo này sẽ được diễn ra một cách tự động nếu các ***router*** sử dụng các giao thức định tuyến như RIP và OSPF chẳng hạn. Nếu không có chúng, người quản

trị phải cấu hình một cách thủ công các bảng định tuyến thông tin về các phân đoạn mà chúng không quản lý thông qua các đường định tuyến tĩnh. Sử dụng các đường định tuyến tĩnh chỉ phù hợp với các mạng nhỏ, đơn giản. Tuy nhiên với các mạng lớn hơn chúng không đáp ứng được do các đường định tuyến tĩnh không tự động đáp ứng được những sự thay đổi trong cấu trúc của toàn hệ thống.

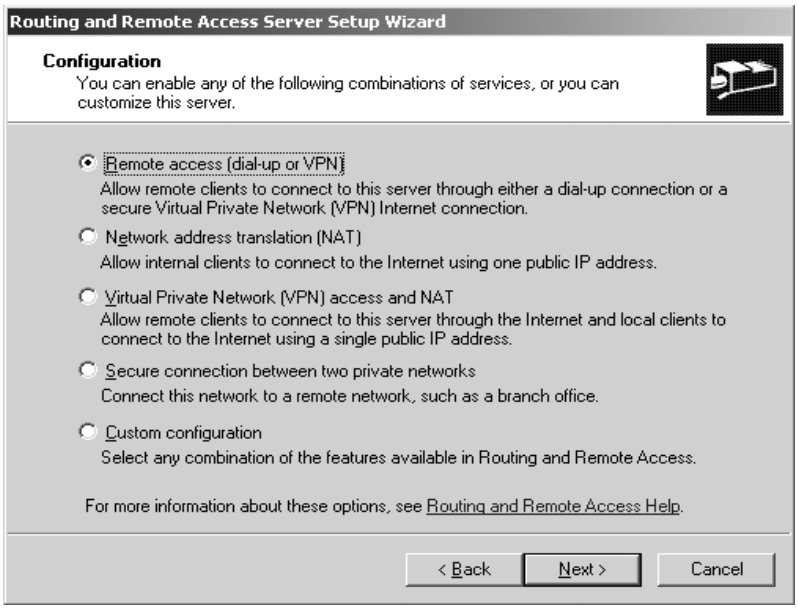
Khi quá trình định tuyến được cấu hình đúng thì một người sử dụng trên phân đoạn 1 muốn liên lạc với một người sử dụng khác trên phân đoạn 3, máy tính trên mạng ***LAN 1*** sẽ hướng các gói tin tới ***router 1***. Tiếp theo ***router 1*** sẽ hướng các gói tin đó tới ***router 2***, kế đó ***router 2*** sẽ hướng các gói tin tới máy tính trên mạng ***LAN 3***.



Hình 7-2: Ba phân đoạn mạng được kết nối với nhau qua hai router

CÁC LỰA CHỌN TRONG VIỆC CẤU HÌNH CHO CÁC MÁY CHỦ TRUY CẬP TỪ XA

Như Hình 7-3, tiến trình ***Routing And Remote Access Server Setup Wizard*** cung cấp cho bạn một trang cấu hình mà ở đó bạn có thể lựa chọn các dịch vụ. Lựa chọn cuối cùng trong danh sách này là ***Custom Configuration*** (cấu hình tùy biến). Bạn sẽ sử dụng lựa chọn này nếu bạn có khả năng cấu hình máy chủ một cách thủ công và nếu như không có dịch vụ nào ở trên phù hợp một cách chính xác với nhu cầu truy cập định tuyến và truy cập từ xa của bạn.



Hình 7-3: Các lựa chọn cho dịch vụ định tuyến và truy cập từ xa

Có một vài lựa chọn dành cho bạn khi cấu hình dịch vụ truy cập từ xa:

■ **Remote Access (Dial-up Or VPN)** Lựa chọn này cho phép các máy trạm từ xa kết nối tới các máy chủ thông qua kết nối quay số hoặc một mạng riêng ảo bảo mật.

■ **Network Address Translation (NAT)** Lựa chọn này cho phép các máy trạm cục bộ kết nối tới mạng Internet bằng cách sử dụng một địa chỉ IP bên ngoài.

■ **Virtual Private Network (VPN) Access And NAT** Lựa chọn này cho phép bạn cấu hình NAT cho mạng cục bộ và các kết nối mạng riêng ảo VPN.

■ **Secure Connection Between Two Private Networks** Lựa chọn này phù hợp khi bạn muốn thiết lập một kết nối mạng riêng ảo VPN kiểu router-đến-router.

■ **Custom Configuration** Như đã đề cập ở trên, bạn sẽ sử dụng lựa chọn cuối cùng này khi các lựa chọn nói trên không đáp ứng được nhu cầu cho dịch vụ của bạn.

Cấu hình truy cập từ xa thông qua kết nối quay số

Truy cập từ xa thông qua kết nối quay số hay còn gọi là mạng quay số cho phép các máy tính từ xa sử dụng một modem kết nối tới mạng của một tổ

chức như thể máy tính đó được kết nối cục bộ mặc dù tốc độ truyền dữ liệu là thấp hơn nhiều. Các máy chủ cho phép truy cập từ xa sử dụng hệ điều hành Windows Server 2003 cho phép các máy trạm cài đặt hệ điều hành Windows Server 2003, Microsoft Windows XP Professional, Microsoft Windows NT, Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows for Workgroups, MS-DOS hoặc Apple Macintosh kết nối tới. Thông thường, máy trạm kết nối tới máy chủ thông qua một đường thoại chuẩn – đó có thể là một đường thoại thông thường hoặc mạng ISDN hoặc đường cáp thuê báo số (DSL) hoặc mạng truyền dẫn X25 hoặc một đường truyền dẫn ATM.

Để cho phép nhiều người sử dụng quay số kết nối đồng thời tới mạng của bạn, bạn phải có một dãy các modem, các kết nối tương ứng tới nhà cung cấo dịch vụ viễn thông và một thiết bị kết nối dãy modem (đó có thể là một giao diện mạng được gắn trên máy tính cài đặt hệ điều hành Windows Server 2003). Sau khi đã hoàn thành công việc cài đặt phần cứng, bạn sẽ thực hiện các công việc dưới đây:

1. Nhấp Start, trỏ tới Administrative Tools rồi nhấp Routing And Remote Access.

2. Trong màn hình quản trị, kích chuột phải vào máy chủ rồi nhấp ***Configure And Enable Routing And Remote Access***.

3. Trong trang ***Welcome To Routing And Remote Access Setup Wizard*** nhấp ***Next***.

4. Trong trang ***Configuration*** nhấp ***Remote Access (Dial-up Or VPN)*** rối nhấp ***Next***.

5. `Trong trang ***Remote Access***, lựa chọn hộp kiểm tra ***Dial-up*** rồi nhấp ***Next***.

6. Nếu máy chủ của bạn có nhiều giao diện mạng thì trên trang Network ***Selection*** nhấp vào giao diện mà bạn muốn gán cho các máy trạm truy cập từ xa đến rồi nhấp ***Next***.

7. Trong trang ***IP Address Assignment***, lựa chọn hoặc ***Automatically*** (*tự động - sử dụng máy chủ DHCP để gán địa chỉ IP*) hoặc ***From A Specified Range Of Addresses*** (*Sử dụng giải địa chỉ IP đã chỉ định - tại máy chủ cài đặt dịch vụ định tuyến và truy cập từ xa*) rồi nhấp ***Next***.

8. Trong hộp thoại ***Managing Multiple Remote Access Servers***, không sử dụng lựa chọn ***RADIUS Server***.

9. Nhấp ***Next*** rồi nhấp ***Finish***. Dịch vụ ***Routing And Remote Access*** bắt đầu hoạt động và tự động khởi tạo.

Sửa lỗi các vấn đề liên quan đến các kết nối truy cập từ xa thông qua cơ chế quay số

Sau khi đã hoàn thành quá trình cài đặt dãy modem và cấu hình dịch vụ ***Routing And Remote Access***, nếu có lỗi xảy ra bạn hãy sử dụng danh sách kiểm tra dưới đây cho công việc tìm và sửa lỗi:

■ Đảm bảo rằng lựa chọn ***Remote Access Server*** đã được lựa chọn trong thẻ ***General*** trong màn hình quản trị ***Routing And Remote Access***.

■ Nếu bạn sử dụng một dải địa chỉ IP tĩnh, bạn cần phải đảm bảo dải này đủ lớn để cấp địa chỉ IP cho các máy trạm khi chúng kết nối tới máy chủ.

■ Nếu bạn sử dụng cơ chế gán địa chỉ IP cho các máy trạm thông qua máy chủ DHCP, bạn cần đảm bảo rằng dải địa chỉ IP được định nghĩa trên máy chủ DHCP phải đủ lớn tương đương với dải địa chỉ được xác định qua khóa registry ***InitialAddressPoolSize*** có đường dẫn như sau: ***HKEY_LOCAL_MACHINE\CurrentControlSet\ Services\RemoteAccess\Parameters\IP***.

■ Bạn cần đảm bảo đủ các thiết bị modem được cấu hình trong phần ***Ports*** (để truy cập vào phần này bạn mở rộng phần máy chủ rồi kích vào Ports) nhằm đáp ứng số lượng lớn nhất các kết nối từ phía máy trạm tới máy chủ.

■ Đảm bảo rằng bạn đã cấu hình máy trạm, máy chủ và các chính sách truy cập từ xa sử dụng ít nhất một giao thức xác thực chung.

■ Đảm bảo rằng bạn đã cấu hình máy trạm, máy chủ và các chính sách truy cập từ xa sử dụng ít nhất một phương pháp mã hóa chung.

■ Đảm bảo rằng kết nối truy cập từ xa thông qua cơ chế quay số có các quyền tương ứng thông qua các đặc tính quay số của tài khoản người sử dụng và các chính sách truy cập từ xa.

■ Đảm bảo rằng máy chủ cho phép truy cập từ xa (hay còn gọi là máy chủ RADIUS) là một thành viên của nhóm bảo mật ***RAS and IAS Servers*** trên miền.

■ Đảm bảo rằng các thiết lập trong chính sách truy cập từ xa không xung đột với các đặc tính của máy chủ.

■ Nếu bạn sử dụng giao thức xác thực là MS-CHAP v1, cần đảm bảo rằng mật khẩu của người sử dụng không được vượt quá 14 ký tự.

Cấu hình VPN

Một phương pháp khác cho phép người sử dụng truy cập từ xa đến hệ thống đó là mạng riêng ảo VPN. Đây là một kỹ thuật cho phép mở rộng một mạng mang tính chất riêng tư dựa trên nền tảng một mạng công cộng như mạng Internet chẳng hạn. Tương tự như truy cập từ xa qua cơ chế quay số, sau khi người sử dụng kết nối tới mạng của công ty có thể coi như anh ta đang kết nối một cách trực tiếp về mặt vật lý tới hệ thống mạng (tất nhiên tốc độ truyền dữ liệu có chậm hơn).

Do một mạng VPN có thể được thiết lập thông qua Internet nên mạng của công ty bạn có khả năng truy cập trên diện rộng. Khả năng truy cập này là nhanh chóng, chi phí thấp và an toàn trên toàn thế giới. Với công nghệ VPN, bạn sẽ không cần sử dụng các đường kết nối chuyên dụng trên mạng của bạn và cho phép triển khai tính bảo mật ở mức cao nhất.

Khi nào không nên sử dụng VPN

Mặc dù VPN rất mềm dẻo và cung cấp một giải pháp cho nhiều loại hình kết nối khác nhau như các chi nhánh, các nhà cung cấp dịch vụ viễn thông, các nhân viên hay đi công tác xa. Tuy nhiên bạn không nên sử dụng VPN trong các trường hợp sau:

■ Khi bạn đặt hiệu năng là mối quan tâm hàng đầu mà không cần quan tâm đến giá cả.

■ Khi hầu hết lưu lượng trên đường truyền cần đồng bộ như truyền dẫn thoại và video.

■ Khi có một ứng dụng sử dụng các giao thức không tương thích với tập giao thức TCP/IP.

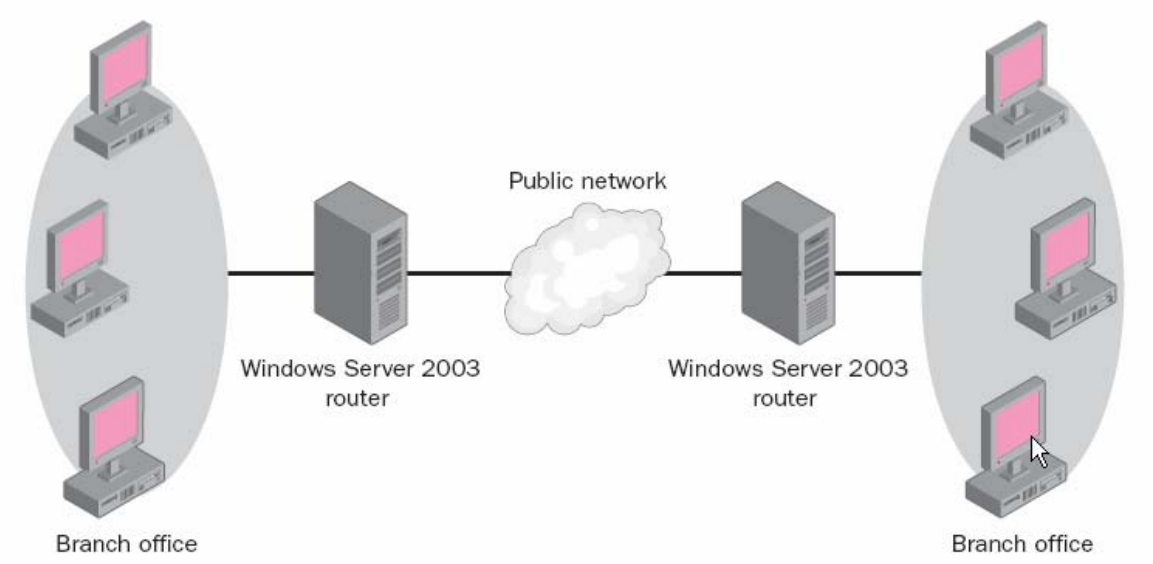
Trong các trường hợp này bạn sẽ phải cân nhắc việc sử dụng một đường kết nối chuyên dụng cho mạng của công ty.

VPN làm việc như thế nào?

Trong một kết nối VPN, cả hai phía của kết nối đều tạo một đường kết nối tới mạng công cộng như mạng Internet chẳng hạn. Các đường kết nối đó có thể là: một đường điện thoại thông thường, một đường ISDN hoặc một đường kết nối chuyên dụng. Khác với các node thông thường khi gửi một gói tin đi VPN sẽ sử dụng một giao thức "đường hầm" (***tunneling protocol***) để đóng gói dữ liệu bằng cách gắn thêm một phần tiêu đề (***header***) vào gói dữ liệu. Phần tiêu đề sẽ cung cấp thông tin định tuyến nhằm đảm bảo gói dữ liệu đã được đóng gói có thể di chuyển trên mạng trung gian công cộng. Dữ liệu sẽ được mã hóa nhằm đảm bảo tính bảo mật. Nếu gói dữ liệu bị đánh cắp, người sử dụng cũng không thể đọc được nội dung của dữ liệu nếu họ không có các khóa mã hóa.

Ví dụ, VPN cho phép một người sử dụng từ xa ở TP Hồ Chí Minh thiết lập một kết nối quay số tới bất kỳ một nhà cung cấp dịch vụ Internet (các ISP như VDC, FPT,…) và thông qua kết nối đó tạo một kết nối trực tiếp tới một máy chủ trên hệ thống mạng của công ty đặt tại Hà Nội. Phương pháp này nhanh chóng, chi phí thấp và dễ dàng thiết lập. VPN cho phép các nhân viên đi công tác, các nhân viên làm việc từ xa.trong các văn phòng tại gia đình và các nhân viên trong các văn phòng chi nhánh kết nối tới mạng của công ty. Mỗi thành phần kết nối tới các ISP thông qua các kênh truyền thông khác nhau nhưng chúng lại là một phần của một mạng VPN.

Cũng tương tự như những người sử dụng ở xa có thể kết nối tới mạng công ty bằng cách sử dụng hệ thống liên mạng trung gian, hai router cũng có thể thiết lập một kết nối VPN. Hình 7-4 biểu diễn một ví dụ về một mạng VPN được thiết lập giữa hai ***router*** với nhau.



Hình 7-4: Mạng VPN kiểu Router-đến-Router

Các thành phần của VPN

Một kết nối VPN trong Windows Server 2003 gồm có các thành phần sau:

- Máy chủ VPN
- Máy trạm VPN
- Kết nối VPN (phần kết nối dữ liệu được mã hóa)
- "Đường hầm" VPN (phần kết nối dữ liệu được bọc gói). Hai giao thức đường hầm dưới đây được cung cấp và cài đặt cùng với dịch vụ RRAS.

a. **Point-To-Point Tunneling Protocol (PPTP– giao thức đường hầm điểm-điểm)** Đây là một giao thức được phát triển từ giao thức PPP (giao thức điểm nối điểm). Lần đầu tiên nó được sử dụng trong hệ điều hành Windows NT4.

b. **Layer Two Tunneling Protocol (L2TP-giao thức đường hầm lớp hai)** Một giao thức đường hầm dựa trên chuẩn của IETF được sử dụng với mục đích đóng gói các khung dữ liệu PPP có khả năng truyền dẫn trên các mạng TCP/IP, X.25, FrameRelay, ATM. L2TP kết hợp các tính năng tiêu biểu của giao thức PPTP (do hãng Microsoft phát triển) và giao thức L2F (do hãng Cisco phát triển). Bạn có thể triển khai L2TP kết hợp cùng với IPSec nhằm cung cấp một giải pháp VPN có độ an toàn và bảo mật rất cao.

Thông tin thêm ***Thông tin về giao thức VPN*** *Để biết thông tin về các giao thức VPN, hãy tham khảo RFC 2637 "Point-To-Point Tunneling Protocol" và RFC 2661 "Layer Two Tunneling Protocol". Bạn có thể tìm thấy cả hai RFC này tại trang Web: http://www.rfc-editor.org/rfcsearch.html.*

Cấu hình cơ chế chuyển đổi địa chỉ NAT

Dịch vụ RRAS của hệ điều hành Windows Server 2003 cung cấp một giao thức có tên NAT cho phép các mạng riêng có khả năng kết nối với thế giới Internet. Giao thức NAT chuyển đổi các địa chỉ IP bên trong thành các địa chỉ công cộng và ngược lại. Tính năng này sẽ làm giảm số lượng địa chỉ IP mà một tổ chức cần phải có và qua đó cũng làm giảm chi phí thuê bao địa chỉ IP. Đó là vì các địa chỉ IP bên trong chỉ được sử dụng trong phạm vi một tổ chức cụ thể, chúng sẽ được chuyển đổi thành các địa chỉ IP công cộng khi

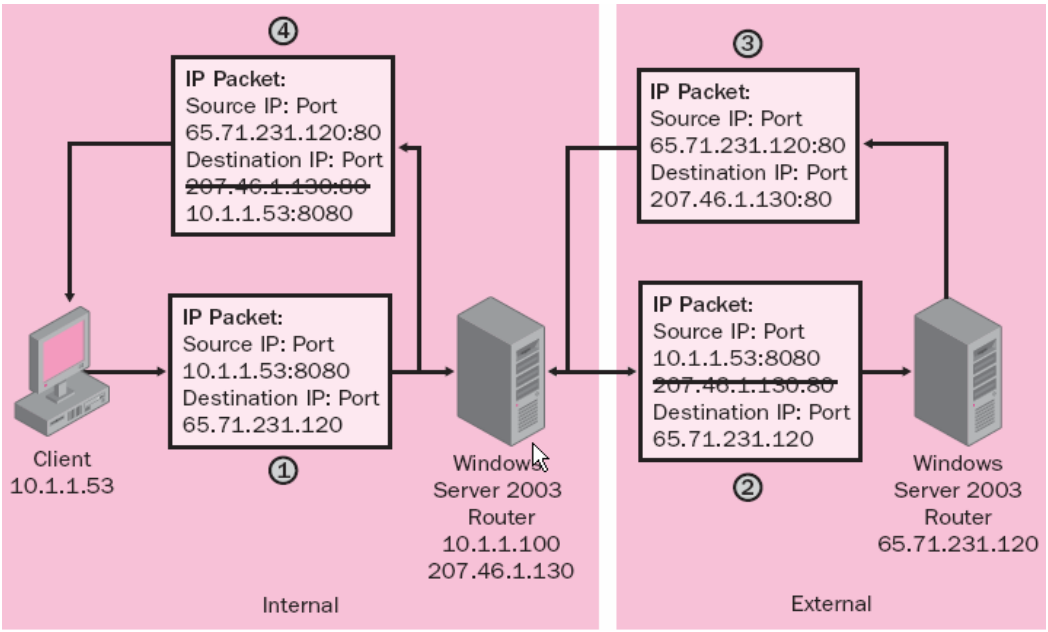
có nhu cầu kết nối với thế giới Internet. NAT còn có một tính năng khác đó là bảo vệ các mạng LAN trước các cuộc truy cập bất hợp pháp bằng cách ẩn địa chỉ IP bên trong đối với thế giới Internet. Chỉ có duy nhất địa chỉ IP của máy tính cài đặt dịch vụ NAT là được công bố ra thế giới Internet.

> **Thông tin thêm** ***Thông tin về dịch vụ NAT*** *Để biết thông tin về NAT, hãy tham khảo RFC 3022 "Traditional IP Network Address Translator (Traditional NAT)" và RFC 1631 "The IP Network Address Translator (NAT)". Bạn có thể tìm thấy cả hai RFC này tại trang Web: http://www.ietf.org/rfc.html.*

NAT làm việc như thế nào?

Khi NAT được sử dụng để kết nối một người sử dụng trong một mạng riêng tới một mạng công cộng, tiến trình dưới đây sẽ xảy ra (xem Hình 7-5):

1. Giao thức IP trên máy tính của người sử dụng sẽ tạo ra một gói tin IP với các giá trị xác định trong phần tiêu đề của gói tin IP và TCP hoặc UDP. Kế đó máy tính của người sử dụng sẽ hướng gói tin IP tới máy tính cài đặt dịch vụ NAT.
2. Máy tính cài đặt dịch vụ NAT sẽ thay đổi phần tiêu đề của gói tin trước khi gửi nó ra thế giới bên ngoài với ngụ ý rằng nó được gửi đi từ địa chỉ bên ngoài của máy tính chạy NAT nhưng máy tính này sẽ không thay đổi địa chỉ đích. Gói tin sau khi đã được máy chủ NAT ánh xạ lại sẽ được gửi ra thế giới Internet tới máy chủ Web.
3. Máy chủ Web trên mạng Internet nhận được gói tin này và gửi trả phản hồi tới máy chủ NAT.
4. Máy chủ NAT nhận được gói tin phản hồi và kiểm tra thông tin đã được ghi lại trong bảng ánh xạ của nó nhằm xác định địa chỉ của máy trạm. Máy chủ NAT sẽ thay đổi phần tiêu đề của gói tin trỏ tới địa chỉ của máy trạm rồi gửi nó tới máy tính của người sử dụng.



Hình 7-5: Tiến trình làm việc của dịch vụ NAT

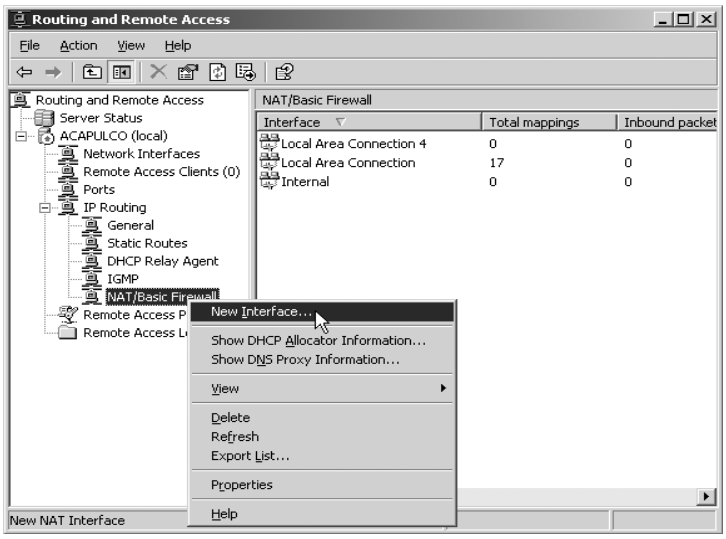
- **Cấu hình một máy chủ cài đặt dịch vụ NAT**

Các bước dưới đây sẽ giúp bạn cấu hình một máy chủ NAT:

1. Mở màn hình quản trị Routing And Remote Access
2. Trong màn hình này, kích chuột phải vào máy chủ rồi nhấp vào ***Configure An Enable Routing And Remote Access***.
3. Trong trang Routing And Remote Access Server Setup Wizard nhấp Next.
4. Trong trang Configuration, nhấp vào Custom Configuration rồi nhấp Next.
5. Trong trang Custom Configuration nhấp vào NAT And Basic Firewall rồi nhấp Next.
6. Trong trang Completing The Routing And Remote Access Server Setup Wizard nhấp Finish.
7. Khi bạn nhận được thông báo nhắc nhở khởi động dịch vụ ***Routing And Remote Access*** nhấp ***Yes***.

8. Trong màn hình quản trị, mở rộng phần chứa máy chủ, mở rộng ***IP Routing***, kích chuột phải vào ***NAT/Basic Firewall*** rồi nhấp vào ***New Interface*** (xem Hình 7-6).

9. Trong hộp thoại ***New Interface For Network Address Translation (NAT)*** nhấp vào giao diện mà bạn muốn sử dụng để chuyển đổi địa chỉ rồi nhấp ***OK***.



Hình 7-6: Xây dựng một giao diện mới cho NAT

10. Trong trang ***Network Address Translation Properties*** được áp dụng cho giao diện bạn chọn ở trên, cấu hinh các đặc tính dưới đây rồi nhấp ***OK***:

    - ❖ Lựa chọn ***Public Interface Connected To The Internet***.
    - ❖ Lựa chọn hộp kiểm tra ***Enable NAT On This Interface.***
    - ❖ Nếu mạng của bạn chưa có một ***firewall***, hãy lựa chọn hộp kiểm tra ***Enable A Basic Firewall On This Interface***.
    - ❖ Nếu muốn bạn có thể hạn chế lưu lượng dựa trên các đặc tính của gói tin bằng cách cấu hình I***nbound Filters*** và O***utbound Filters*** (các bộ lọc luồng lưu lượng đi ra và đi vào một giao diện).
    - ❖ Trong phần ***Address Pool,*** thêm dải địa chỉ bạn nhận được từ phía nhà cung cấp dịch vụ (***ISP***) và giới hạn một hoặc nhiều máy tính cụ thể.

- Trong phần ***Services And Ports,*** lựa chọn các dịch vụ mà người sử dụng sẽ truy cập. Khi bạn lựa chọn một dịch vụ nào đó, một hộp thoại các đặc tính sẽ được mở ra và yêu cầu địa chỉ ***IP*** mạng ***LAN*** nào có gói tin sử dụng dịch vụ này sẽ được gửi đi.

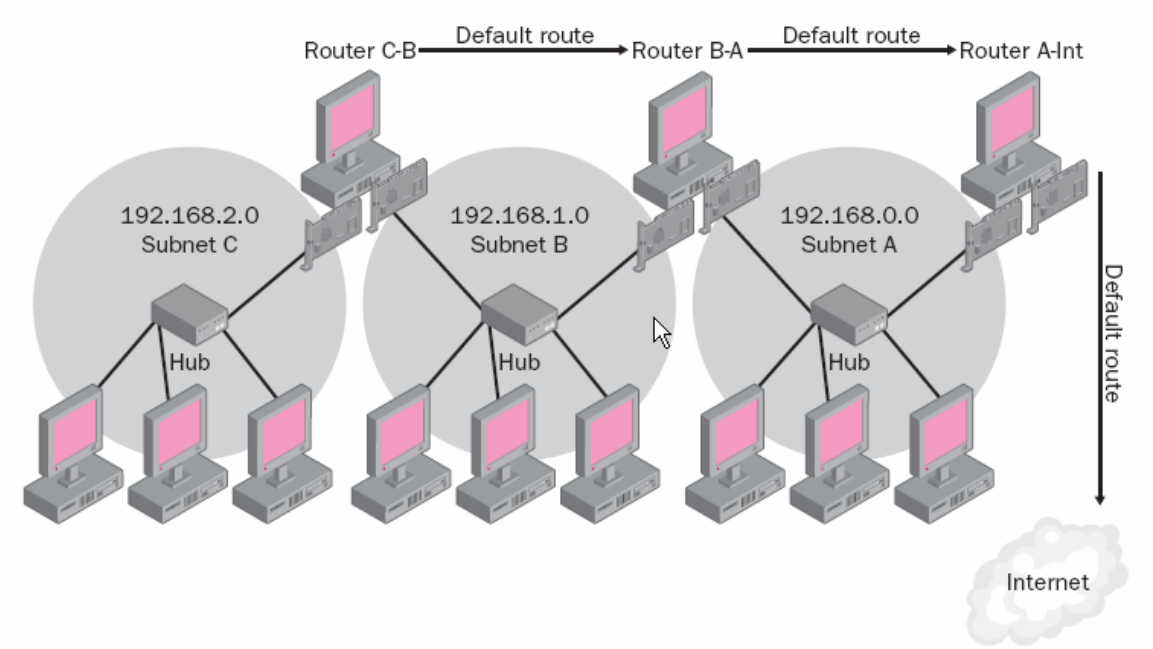
- Trong phần ***ICMP***, các yêu cầu đã được thiết kế cho loại thông tin mà máy chủ sẽ phản hồi.

LỰA CHỌN GIAO THỨC ĐỊNH TUYẾN

Để có thể chuyển các gói tin đến các mạng đích không kết nối trực tiếp, một router phải có một bảng định tuyến chứa thông tin về các mạng này. Trong một hệ thống mạng nhỏ mà những thay đổi của các đường định tuyến là không thường xuyên thì chỉ cần cấu hình bằng tay các đường định tuyến tĩnh trong bảng định tuyến là đủ. Tuy nhiên bạn cũng nên cân nhắc sử dụng giao thức định tuyến RIP đối với các mạng nhỏ nhưng có sự thay đổi thường xuyên đối với các đường định tuyến hoặc các mạng có kích thước trung bình. Đối với mạng có kích thước lớn hơn, hãy cân nhắc việc sử dụng giao thức định tuyến OSPF.

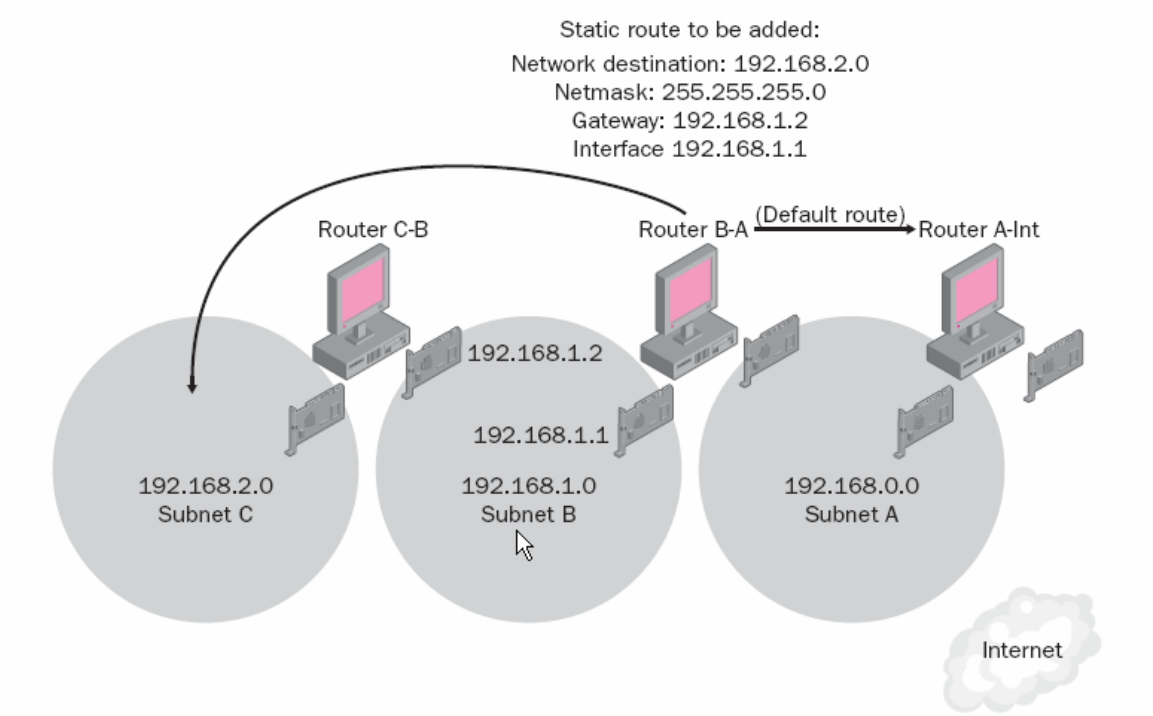
Sử dụng các đường định tuyến tĩnh

Một môi trường IP với các đường định tuyến tĩnh rất phù hợp với các mạng nhỏ có đường kết nối đơn và địa chỉ IP tĩnh. Theo định nghĩa, các mạng với các đường định tuyến tĩnh sẽ không sử dụng bất kỳ một giao thức định tuyến nào như RIP hoặc OSPF để trao đổi thông tin định tuyến giữa các router với nhau. Nhằm thu được kết quả tốt nhất, hệ thống mạng cần có ít hơn 10 mạng con với một lưu lượng mạng có thể dự đoán một cách dễ dàng (ví dụ như hệ thống bao gồm các mạng con được sắp xếp trên một đường thẳng, xem Hình 7-7). Và tất nhiên môi trường định tuyến tĩnh chỉ phù hợp khi mà các đường định tuyến vẫn được giữ nguyên.



Hình 7-7: Một môi trường mạng định tuyến tĩnh với lưu lượng mạng có thể dự đoán

Trong Hình 7-7, Router C-B có thể biết được tất cả các máy tính nằm trong mạng con C và B. Khi router này nhận được một gói tin với đích là một địa chỉ nằm ngoài mạng con C hoặc B, nó sẽ hướng gói tin này đến router B-A dựa trên đường định tuyến mặc định. Do tất cả các máy tính bên ngoài mạng con B và C đều nằm trên hướng của đường định tuyến tĩnh nên bạn sẽ không cần phải thêm các đường định tuyến tĩnh vào trong bảng định tuyến của router C-B. Tuy nhiên đối với router B-A, các máy tính trên mạng con C sẽ không nằm trên hướng của đường định tuyến mặc định. Nếu router B-A nhận được một gói tin với đích là mạng con C, nó sẽ hướng sai gói tin đến router A-Int trừ phi nó được hướng dẫn đi theo một con đường khác. Chính vì vậy việc thêm một đường định tuyến tĩnh vào trong bảng định tuyến của router B-A (xem Hình 7-8) sẽ cho phép router này hướng lưu lượng mạng có đích là mạng con C tới router C-B.



Hình 7-8: Thêm một đường định tuyến tĩnh

Sử dụng các đường định tuyến động

Windows Server 2003 cung cấp 04 giao thức định tuyến dưới đây, cho phép bạn đưa vào dịch vụ RRAS:

■ **RIP** Được thiết kế cho việc trao đổi thông tin định tuyến trong phạm vi một mạng có kích thước từ nhỏ đến trung bình. Cho phép các router xác định đường đi phù hợp nhất trước khi gửi lưu lượng mạng đi.

■ **OSPF** Được thiết kế cho việc trao đổi thông tin định tuyến trong phạm vi một mạng có kích thước lớn hoặc rất lớn. Cho phép các router xác định đường đi phù hợp nhất trước khi gửi lưu lượng mạng đi.

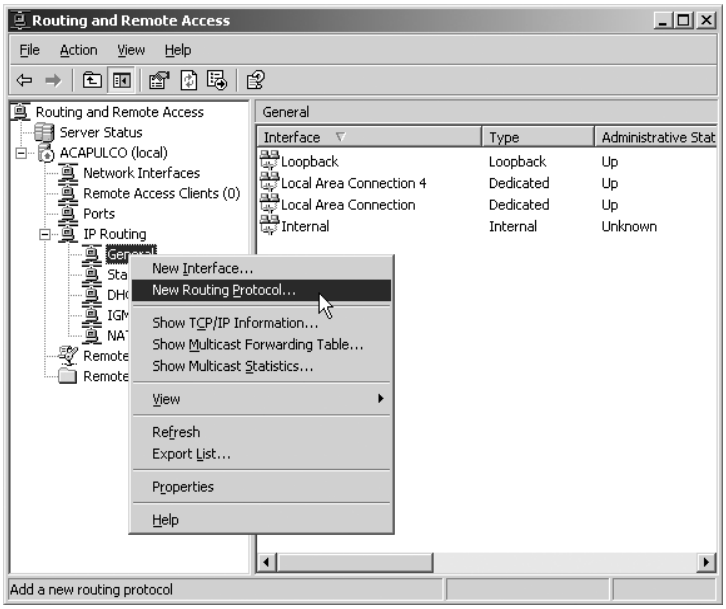
■ **IGMP Router And Proxy** Sử dụng để hướng lưu lượng mạng dạng multicast.

■ **DHCP Relay Agent** Cũng được coi như một giao thức định tuyến trong dịch vụ RRAS. Dịch vụ này cho phép chuyển tiếp thông tin về dịch vụ DHCP giữa các máy chủ DHCP nhằm mục đích cung cấp một cấu hình về địa chỉ IP cho các máy tính thuộc các mạng con khác.

➢ **Thêm giao thức định tuyến**

Để thêm giao thức định tuyến, thực hiện các bước dưới đây:

1. Trong màn hình quản trị ***Routing And Remote Access,*** mở rộng phần máy chủ, mở rộng ***IP Routing*** kích chuột phải vào ***General*** rồi nhấp vào ***New Routing Protocol*** (xem Hình 7-9)



Hình 7-9: Hộp thoại New Routing Protocol

2. Trong hộp thoại ***New Routing Protocol***, lựa chọn giao thức định tuyến phù hợp rồi nhấp ***OK***.

QUẢN TRỊ CÁC BẢNG ĐỊNH TUYẾN

Bảng định tuyến (xem Hình 7-10) chứa các bản ghi được gọi là các đường định tuyến nhằm cung cấp hướng và đường đi tới các mạng hoặc các máy đích. Bảng định tuyến giúp cho giao thức IP quyết định xem nó sẽ gửi lưu lượng đi ra giao diện nào hoặc cổng ra nào. Bảng định tuyến bao hàm nhiều đường định tuyến riêng lẻ; mỗi đường định tuyến gồm có: địa chỉ đích, mặt nạ mạng, giao diện đầu ra, địa chỉ cổng ra (***gateway***) và trọng số đường định tuyến (***metric***). Bảng định tuyến được sắp xếp theo thứ tự từ cái cụ thể nhất đến cái chung nhất nên gói tin sẽ được gửi tới địa chỉ cổng ra đầu tiên trong bản ghi có địa chỉ đích phù hợp với thông tin trong bản ghi đó. Nếu có hai đường định tuyến tương tự nhau thì đường nào có giá trị đường đi thấp hơn sẽ được lựa chọn. Trong trường hợp hai đường này lại có giá trị ***metric*** bằng nhau thì router sẽ lựa chọn một cách ngẫu nhiên một trong hai đường. Có tất cả 04 kiểu đường định tuyến:

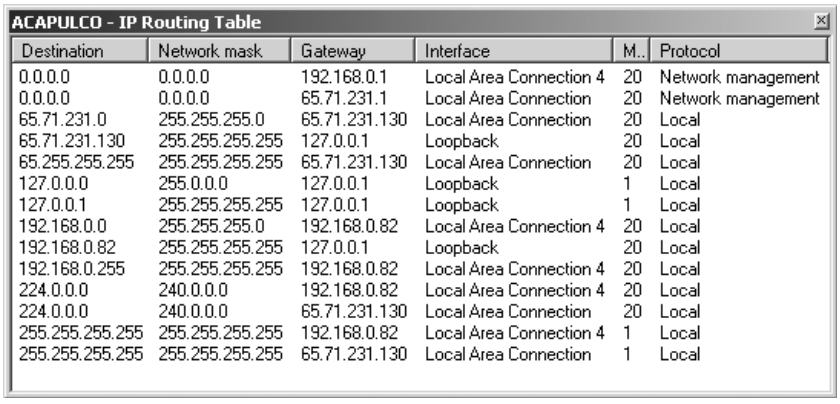
■ **Các đường định tuyến tới mạng được kết nối trực tiếp** Đây là các đường định tuyến tới các mạng con được gắn trực tiếp với router. Đối với các mạng này, cột Gateway hoặc là để trống hoặc là địa chỉ IP của giao

diện kết nối với mạng con đó. Nếu địa chỉ đích là cục bộ thì router không cần mất nhiều thời gian để xử lý gói tin. Giao thức phân giải địa chỉ ARP sẽ có nhiệm vụ chuyển đổi địa chỉ IP thành địa chỉ phần cứng (*thông thường địa chỉ này gọi là địa chỉ MAC, là một địa chỉ duy nhất trên toàn thế giới ứng với mỗi giao diện mạng*) của giao diện mạng máy đích.

■ **Các đường định tuyến tới các mạng ở xa** Đây là các đường định tuyến tới các mạng con đi qua nhiều router và không được kết nối trực tiếp với nó. Với các đường định tuyến này, điều quan trọng nhất đó là xác định địa chỉ IP của ***gateway*** và giao diện đầu ra. Địa chỉ IP của ***gateway*** là địa chỉ của ***router*** ở xa mà ***router*** này kết nối trực tiếp với nó thông qua các đường kết nối. Trong một mạng chỉ có một ***router*** hoạt động đóng vai kết nối với thế giới bên ngoài thì việc xác định này là không cần thiết. Nhưng nếu một hệ thống có từ hai ***router*** trở lên thì việc xác định chính xác ***gateway*** sẽ giúp cho việc định tuyến gói tin giữa các mạng chính xác.

■ **Các đường định tuyến tới các trạm** Đây là một đường định tuyến tới một địa chỉ IP xác định. Các đường định tuyến này cho phép định tuyến tới từng địa chỉ IP cụ thể và mặt nạ mạng được sử dụng trong trường hợp này là 255.255.255.255.

■ **Đường định tuyến mặc định** Đường định tuyến này sẽ được sử dụng trong trường hợp khi các đường định tuyến tới các mạng và các trạm không phù hợp. Địa chỉ đích của đường định tuyến này là 0.0.0.0 còn mặt nạ mạng là 0.0.0.0. Địa chỉ bước nhảy kế tiếp (*next-hop*) của đường định tuyến mặc định thông thường là địa chỉ gateway mặc định của máy chủ.


ACAPULCO - IP Routing Table

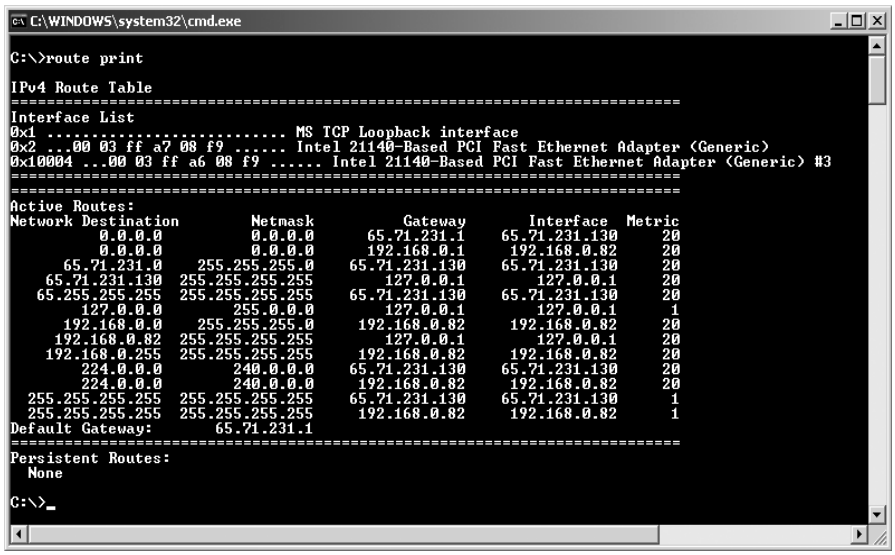
Destination	Network mask	Gateway	Interface	M..	Protocol
0.0.0.0	0.0.0.0	192.168.0.1	Local Area Connection 4	20	Network management
0.0.0.0	0.0.0.0	65.71.231.1	Local Area Connection	20	Network management
65.71.231.0	255.255.255.0	65.71.231.130	Local Area Connection	20	Local
65.71.231.130	255.255.255.255	127.0.0.1	Loopback	20	Local
65.255.255.255	255.255.255.255	65.71.231.130	Local Area Connection	20	Local
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.0.0	255.255.255.0	192.168.0.82	Local Area Connection 4	20	Local
192.168.0.82	255.255.255.255	127.0.0.1	Loopback	20	Local
192.168.0.255	255.255.255.255	192.168.0.82	Local Area Connection 4	20	Local
224.0.0.0	240.0.0.0	192.168.0.82	Local Area Connection 4	20	Local
224.0.0.0	240.0.0.0	65.71.231.130	Local Area Connection	20	Local
255.255.255.255	255.255.255.255	192.168.0.82	Local Area Connection 4	1	Local
255.255.255.255	255.255.255.255	65.71.231.130	Local Area Connection	1	Local

Hình 7-10: Bảng định tuyến IP ở chế độ giao diện đồ họa

Hiển thị bảng định tuyến IP

Bạn có thể hiển thị bảng định tuyến IP bằng cách sử dụng màn hình quản trị ***Routing And Remote Access*** hoặc chế độ dòng lệnh. Trong màn hình quản trị ***Routing And Remote Access***, mở rộng phần ***IP Routing***, kích chuột phải vào phần ***Static Routes*** rồi nhấp vào ***Show IP Routing Table*** (xem Hình 7-10)

Để hiển thị bảng định tuyến từ chế độ dòng lệnh, tại dấu nhắc dòng lệnh gõ **route print** rồi nhấn ***Enter*** (xem Hình 7-11)



Hình 7-11: Hiển thị bảng định tuyến từ chế độ dòng lệnh

Đọc bảng định tuyến IP

Các router sử dụng các bảng định tuyến để xác định xem nó gửi gói các gói tin đi đâu. Khi các gói tin IP được gửi tới một router, router sẽ đọc địa chỉ đích của gói tin và so sánh địa chỉ này với các bản ghi trong bảng định tuyến.

Một trong số các bản ghi được sử dụng để xác định xem gói tin được gửi tới giao diện nào và địa chỉ của gateway mà gói tin sẽ được gửi tới trong lần kế tiếp. Như Hình 7-11 ở trên, mỗi bản ghi trong bảng định tuyến gồm có 05 cột được miêu tả ở đây:

- **Địa chỉ mạng đích** Router so sánh địa chỉ đích của tất cả các gói tin IP mà nó nhận được với các bản ghi trong bảng định tuyến. Các bản ghi dưới đây đều có mặt trong hầu hết các bảng định tuyến:

- **0.0.0.0** biểu diễn đường định tuyến mặc định, đường này sẽ được sử dụng khi không có một bản ghi nào trong bảng định tuyến phù hợp.
- **127.0.0.0** trỏ tới địa chỉ loopback 127.0.0.1 (đây là địa chỉ lặp được sử dụng với mục đích kiểm tra) tương ứng với máy tính cục bộ.
- **224.0.0.0** Các bản ghi này đề cập tới một đường định tuyến multicast phân biệt.
- **w.x.y.255** biểu diễn một địa chỉ quảng bá. Địa chỉ quảng bá gồm có các địa chỉ quảng bá cho các mạng con cụ thể như 192.168.0.255.
- **255.255.255.255** là địa chỉ quảng bá hạn chế, thông thường được áp dung cho tất cả các mạng và các router.

■ **Mặt nạ mạng** Mặt nạ mạng được áp dụng cho địa chỉ IP đích khi kiểm tra xem nó có đáp ứng giá trị trong trường ***Destination*** hay không. Thông tin này rất quan trọng bởi vì việc đáp ứng lớn hơn sẽ xác định xem đường định tuyến nào hay bản ghi nào trong bảng định tuyến được áp dụng cho gói tin. Ví dụ, xem xét bảng định tuyến của một router được biểu diễn trên hình 8-11. Giả thiết, router này nhận được hai gói tin một cái có địa chỉ đích 192.168.0.82, cái còn lại có địa chỉ đích 192.168.0.87. Cả hai đều đáp ứng bản ghi thứ 7 trong bảng định tuyến (192.168.0.0) bởi vì giá trị mặt nạ mạng 255.255.255.0 muốn nói rằng 03 octet đầu tiên (cộng với con số 0 cho octet thứ tư) phù hợp với giá mạng đích 192.168.0.0 trong bảng định tuyến. Bản ghi thứ tám (192.168.0.82) có mặt nạ mạng 255.255.255.255 có nghĩa cả 04 octet đều phải giống hệt với địa chỉ mạng đích 192.168.0.82 trong bảng định tuyến. Octet thứ tư của gói tin thứ hai có giá trị là 87 nên sẽ không phù hợp với giá trị octet thứ tư 82 của bản ghi thứ tám. Vì vậy chỉ có duy nhất gói tin thứ nhất là phù hợp với bản ghi thứ tám này. Do vậy bản ghi thứ bảy (192.168.0.0) sẽ được áp dụng cho gói tin thứ nhất vì bản ghi này đáp ứng lớn hơn trong bảng định tuyến. Đồng thời, bản ghi thứ bảy này cũng được áp dụng cho gói tin thứ hai bởi vì ngoài đường định tuyến mặc định thì đây là bản ghi duy nhất mà gói tin thứ hai phù hợp trong bảng định tuyến.

■ **Gateway** Khi một đường định tuyến nào đó được áp dụng cho một gói tin thì kế đó giá trị gateway sẽ xác định địa chỉ IP hoặc bước nhảy kế tiếp mà gói tin sẽ được chuyển tới đó. Ví dụ, xem xét bảng định tuyến trên Hình 7-11, một gói tin có địa chỉ đích 206.73.118.5 (địa chỉ này chỉ

phù hợp với đường định tuyến mặc định 0.0.0.0) tiếp theo sẽ được hướng tới địa chỉ gateway 65.71.231.130. Trong Hình 7-11, hai đường định tuyến mặc định đều được hiển thị do máy tính này có hai giao diện mạng. Chú ý rằng giá trị gateway của đường định tuyến mặc định trùng với địa chỉ gateway mặc định được cấu hình trong đặc tính TCP/IP.

■ **Giao diện (Interface)** Khi một gói tin chịu sự tác động của một đường định tuyến nào đó, giá trị này xác định giao diện cục bộ nào trên router sẽ được sử dụng để chuyển gói tin tới bước nhảy kế tiếp. Ví dụ, xem xét bảng định tuyến trên Hình 7-11, một gói tin có địa chỉ đích 131.107.23.101 sẽ chỉ đáp ứng duy nhất đường định tuyến mặc định. Dựa trên bảng định tuyến, gói tin này sẽ được gửi thông qua giao diện 65.71.231.130 để chuyển tiếp tới địa chỉ gateway mặc định.

■ **Trọng số đường đi (Metric)** Cột này xác định chi phí khi sử dụng một đường định tuyến. Nếu có nhiều đường định tuyến phù hợp với địa chỉ đích của gói tin thì giá trị metric sẽ được sử dụng để xác định xem đường định tuyến nào được áp dụng cho gói tin. Các đường định tuyến có giá trị metric thấp hơn sẽ có độ ưu tiên cao hơn. Với giao thức định tuyến RIP, metric được xác định thông qua thông qua số lượng các bước nhảy mà một gói tin phải đi qua trước khi tới đích. Tuy nhiên bạn có thể sử dung bất kỳ một thuật toán nào đó để xác định giá trị metric nếu bạn cấu hình đường định tuyến một cách thủ công.

Cấu hình bảng định tuyến IP

Bạn có thể hiển thị bảng định tuyến IP từ chế độ dòng lệnh hoặc có thể sử dụng màn hình quản trị Routing And Remote Access. Để cấu hình bảng định tuyến, sử dụng công cụ Route ở chế độ dòng lệnh. Cú pháp của dòng lệnh Route như sau:

route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric Metric]] [if Interface]

Bảng 7-1 liệt kê tất cả các câu lệnh sẵn có, chức năng của chúng và một ví dụ mô tả cách thức sử dụng câu lệnh đó như thế nào. Gõ **route /?** Tại dấu nhắc dòng lệnh để biết thêm thông tin sử dụng công cụ này.

Bảng 7-1: Các lựa chọn dành cho câu lệnh Route

Câu lệnh	Chức năng	Ví dụ
Print	Hiển thị bảng định tuyến	***route print***
Add	Thêm một đường định tuyến vào bảng	***route add –p 10.0.0.1 mask***

	định tuyến. Mặc định, các đường định tuyến sẽ không lưu giữ khi hệ thống khởi động lại. Sử dụng lựa chọn –p để tạo nên một đường định tuyến vẫn được lưu giữ kể cả khi hệ thống khởi động lại. Các đường định tuyến này được lưu trong HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes	***255.0.0.0 192.168.0.1***
Change	Sử dụng câu lệnh Change để thay đổi một đường định tuyến sẵn có	***route change 10.0.0.1 mask 255.0.0.0 10.27.0.25***
Delete	Xóa một đường định tuyến sẵn có. Để xóa một đường định tuyến, bạn chỉ cần cung cấp địa chỉ IP của đường định tuyến	***route delete 10.0.0.1***

- **Thêm một đường định tuyến vào bảng định tuyến**

Để thêm một đường định tuyến vào bảng định tuyến, sử dụng câu lệnh Route:

1. Kích hoạt cửa sổ chế độ dòng lệnh
2. Tại dấu nhắc lệnh, gõ **route add *IP_address* mask *subnet_mask_address next_hop_destination_address***

LỌC GÓI TIN

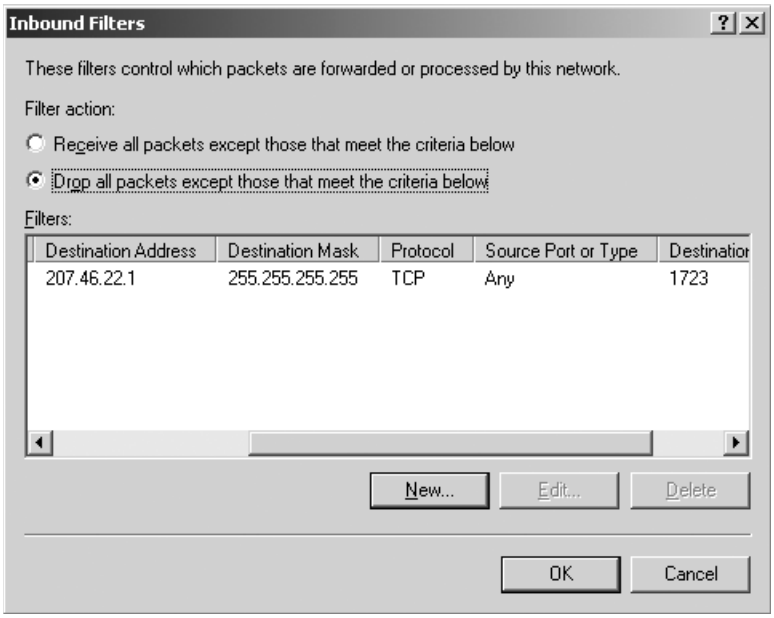
Lọc gói tin là cơ chế cho phép bạn ngăn không cho gửi hoặc nhận các kiểu gói tin xác định trên một router. Một bộ lọc gói tin là một thiết lập trong cấu hình TCP/IP được thiết kế để cho phép hoặc ngăn chặn các gói tin IP theo chiều đi ra hoặc đi vào một giao diện xác định. Các bộ lọc gói tin có thể hạn chế lưu lượng trên một giao diện xác định dựa trên địa chỉ nguồn, địa chỉ đích, hướng hoặc kiểu giao thức.

Đặc tính lọc gói trong dịch vụ RRAS được dựa trên tính loại trừ. Bạn có thể đặt các bộ lọc gói cho từng giao diện và cấu hình chúng thực hiện một trong các hành động sau:

■ Cho tất cả lưu lượng đi qua ngoại trừ các gói tin phù hợp với các bộ lọc.

■ Loại bỏ tất cả lưu lượng ngoại trừ các gói tin được cho phép bởi các bộ lọc.

Trong Windows Server 2003, các bộ lọc gói có hai kiểu: các bộ lọc gói theo chiều vào và các bộ lọc gói theo chiều ra. Các bộ lọc gói theo chiều vào sẽ hạn chế lưu lượng đi vào một giao diện từ mạng kết nối trung gian. Các bộ lọc gói theo chiều ra sẽ hạn chế lưu lượng được gửi từ một giao diện đi tới các mạng kết nối trung gian. Hình 7-12 minh họa một bộ lọc chiều vào ngăn chặn tất cả các gói tin ngoại trừ những gói tin có địa chỉ cổng đích TCP 1723 và địa chỉ IP đích 207.46.22.1.



Hình 7-12: Ví dụ về bộ lọc gói

Tạo các bộ lọc gói tin

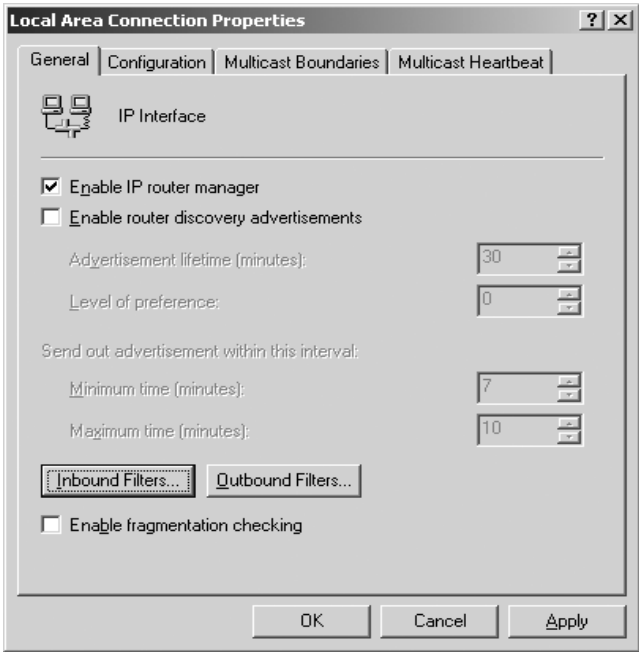
Để tạo các bộ lọc gói bạn có thể sử dụng màn hình quản trị ***Routing And Remote Access*** thông qua phần ***IP Routing***. Trong phần ***IP Routing*** bạn có thể lựa chọn hoặc phần ***General*** hoặc phần ***NAT/Basic Firewall.*** Tiếp đó các bộ lọc gói được cấu hình thông qua các trang đặc tính của giao diện tương ứng. Bạn cần chú ý phần ***NAT/Basic Firewall*** chỉ cho phép bạn tạo các bộ lọc gói cho các giao diện phía ngoài trong khi phần ***General*** cho phép bạn tạo các bộ lọc gói cho bất kỳ giao diện nào.

➢ Tạo một bộ lọc gói

Để tạo một bộ lọc gói, bạn hãy thực hiện theo các bước dưới đây:

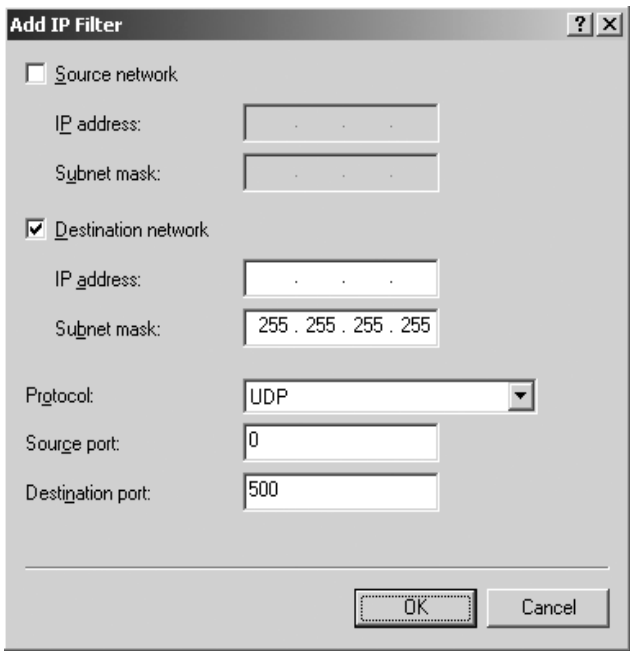
1. Mở màn hình quản trị ***Routing And Remote Access***.

2. Trong màn hình này, mở rộng phần ***IP Routing*** rồi nhấp vào phần ***General***.
3. Trong trang liệt kê chi tiết các đặc tính, kích chuột phải vào giao diện mà bạn muốn thêm một bộ lọc rồi nhấp vào ***Properties***. Hộp thoại ***Properties*** của giao diện xuất hiện như Hình 7-13.



Hình 7-13: Cấu hình các bộ lọc gói

4. Trong thẻ ***General***, nhấp vào ***Inbound Filters*** hoặc ***Outbound Filters***.
5. Trong hộp thoại ***Inbound Filters*** hoặc ***Outbound Filters*** nhấp ***New***.
6. Trong hộp thoại ***Add IP Filter*** nhập các tham số thiết lập cho bộ lọc rồi nhấp ***OK*** (xem Hình 7-14 để tham khảo một ví dụ)



Hình 7-14: Thêm một bộ lọc IP

7. Trong ***Filter Action***, lựa chọn hành động lọc gói tương ứng rồi nhấp ***OK***.
8. Nhấp ***OK*** để đóng hộp thoại ***Filters Properties***.

   CHÚ Ý Định nghĩa các bộ lọc gói *Bạn cũng có thể định nghĩa các bộ lọc gói trong một chính sách truy cập từ xa. Các chính sách truy cập từ xa (phần này sẽ được đề cập trong phần sau "Áp dụng các chính sách truy cập từ xa" của chương này) cho phép bạn áp dụng các luật và các giới hạn cho các kết nối truy cập từ xa cụ thể. Bằng cách định nghĩa các bộ lọc gói tại mức chính sách truy cập từ xa, bạn có thể áp dụng các mức hạn chế truy cập khác nhau cho người sử dụng khác nhau.*

CẤU HÌNH ĐỊNH TUYẾN QUAY SỐ THEO YÊU CẦU

Routing And Remote Access cũng hỗ trợ tính năng định tuyến quay số theo yêu cầu (***Demand-dial Routing***). Khi ***router*** nhận được một gói tin, ***router*** có thể sử dụng tính năng định tuyến quay số theo yêu cầu để khởi tạo một kết nối tới site ở xa. Kết nối này chỉ kích hoạt khi dữ liệu được gửi tới site đầu xa. Đường truyền sẽ bị ngắt khi không có dữ liệu trên đường truyền trong một khoảng thời gian xác định. Do các kết nối quay số theo yêu cầu thường dành cho các trường hợp lưu lượng thấp nên bạn có thể sử dụng các

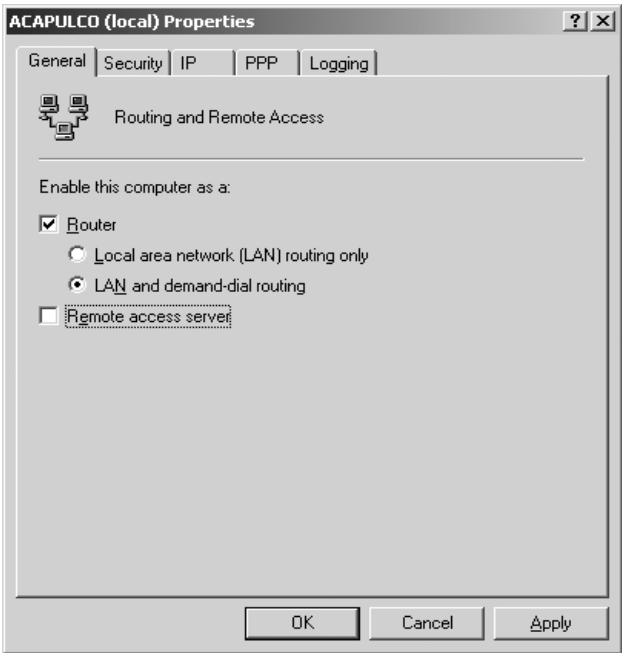
đường điện thoại quay số sẵn có thay cho các đường leased-line, qua đó nó làm giảm chi phí kết nối.

Bạn có thể sử dụng các bộ lọc quay số theo yêu cầu để xác định xem loại lưu lượng nào được phép tạo kết nối. Các bộ lọc quay số theo yêu cầu hoàn toàn tách biệt với các bộ lọc gói IP, qua đó bạn có thể cấu hình để xác định loại lưu lượng nào được phép đi vào hoặc đi ra một giao diện sau khi kết nối đã được thực hiện.

Bước đầu tiên trong quá trình triển khai định tuyến quay số theo yêu cầu đó là cấu hình một giao diện trên máy tính mà bạn muốn nó hoạt động như một router quay số theo yêu cầu. Bạn có thể cấu hình các giao diện này bằng cách sử dụng ***Demand-Dial Interface Wizard*** khi khởi tạo cài đặt dịch vụ ***Routing And Remote Access*** hoặc coi đó là một lựa chọn sau khi dịch vụ ***Routing And Remote Access*** đã được cấu hình và kích hoạt.

Nếu trước đó bạn đã cấu hình và kích hoạt dịch vụ ***Routing And Remote Access*** mà không có chức năng quay số theo yêu cầu thì bạn phải kích hoạt tính năng này trước khi tạo bất kỳ giao diện quay số theo yêu cầu.

Để kích hoạt tính năng quay số theo yêu cầu, lựa chọn ***LAN And Demand-Dial Routing*** trong phần ***General*** của hộp thoại ***Routing And Remote Access Server Properties*** như Hình 7-15.



Hình 7-15: Kích hoạt định tuyến quay số theo yêu cầu

Kiểm tra các kết nối quay số theo yêu cầu

Sau khi kích hoạt tính năng ***LAN and demand-dial routing*** (định tuyến quay số theo yêu cầu và định tuyến giữa các mạng LAN) và sau khi cấu hình các giao diện quay số theo yêu cầu, bạn có thể kiểm tra xem kết nối này có làm việc chính xác hay không bằng cách sử dụng phương pháp kiểm tra thủ công hoặc tự động.

Kiểm tra thủ công

Bằng cách kiểm tra một cách thủ công một kết nối quay số theo yêu cầu, bạn đang kiểm tra xem đường truyền PPP đã được thiết lập hay chưa. Phương pháp này xác nhận rằng cấu hình của các phương pháp xác thực, mã hóa, tài khoản của người sử dụng và địa chỉ dành cho giao diện quay số theo yêu cầu đã hợp lệ hay chưa.

➢ Kiểm tra thủ công giao diện quay số theo yêu cầu

Để kết nối thủ công giao diện quay số theo yêu cầu, bạn hãy thực hiện theo các bước dưới đây:

1. Trong màn hình quản trị ***Routing And Remote Access*** mở rộng máy chủ tương ứng rồi nhấp vào ***Routing Interfaces***.
2. Trong trang liệt kê chi tiết, kích chuột phải vào giao diện quay số theo yêu cầu tương ứng.
3. Nhấp ***Connect.***
4. Sau khi kết nối quay số theo yêu cầu được thực hiện, cột ***Connection Status*** (trạng thái kết nối) của giao diện quay số theo yêu cầu sẽ chuyển đổi trạng thái từ ***Disconnected*** (chưa kết nối) thành ***Connected*** (đã kết nối).

Kiểm tra tự động

Bằng cách kiểm tra tự động một kết nối quay số theo yêu cầu, bạn đang kiểm tra xem kết nối quay số theo yêu cầu có được khởi tạo tự động hay không khi lưu lượng phù hợp với một đường định tuyến đã được cấu hình được gửi tới ***router***.

Để kiểm tra một kết nối tự động, xác nhận rằng giao diện quay số theo yêu cầu chuẩn bị được kiểm tra đang ở trạng thái chưa kết nối. Kế đó, tạo một lưu lượng chuyển tới một vị trí sẵn có dọc theo kết nối quay số theo yêu cầu. Một cách dễ dàng để tạo lưu lượng IP đó là sử dụng câu lệnh ***Ping*** hoặc ***Tracert***.

Khi sử dụng các câu lệnh ***Ping*** hoặc ***Tracert***, lần đầu có thể bạn nhìn thấy trạng thái không thành công do độ trễ của quá trình thiết lập kết nối. Tuy nhiên, gói tin đầu tiên được gửi tới giao diện sẽ làm cho giao diện này thiết lập kết nối và các gói tin kế tiếp sẽ thành công khi kết nối đã được thiết lập. Một phương pháp cho phép bạn xem tiến trình kết nối đó là sử dụng câu lệnh ***Ping*** cùng với tham số ***-t*** để tiếp tục gửi các bản tin ***ICMP Echo*** cho tới khi ngắt thì thôi. Bạn sẽ thấy các thông điệp "***Request timed out***" cho tới khi kết nối quay số theo yêu cầu được thiết lập, sau đó bạn sẽ thấy các phản hồi từ phía máy đích.

Sửa lỗi các vấn đề liên quan tới định tuyến quay số theo yêu cầu

Các phần dưới đây cung cấp cho bạn những mẹo trong việc sửa lỗi, qua đó giúp bạn xác định được nguyên nhân gây ra những lỗi về định tuyến theo yêu cầu bằng việc cách ly những lỗi về cấu hình hoặc lỗi về kiến trúc hạ tầng tạo ra:

- Kết nối theo yêu cầu không xảy ra tự động.
- Không thể tạo được một kết nối quay số theo yêu cầu.

Kết nối theo yêu cầu không xảy ra tự động

Nếu một kết nối theo yêu cầu không xảy ra tự động, xác nhận những vấn đề dưới đây:

- Có các đường định tuyến tĩnh chính xác và được cấu hình với giao diện quay số theo yêu cầu tương ứng.
- Đối với các đường định tuyến tĩnh sử dụng một giao diện quay số theo yêu cầu, hộp kiểm tra ***Use This Route To Initiate Demand-Dial Connections*** đã được lựa chọn.
- Giao diện quay số theo yêu cầu không ở trong trạng thái chưa kích hoạt. Để kích hoạt giao diện, kích chuột phải vào giao diện quay số theo yêu cầu rồi lựa chọn ***Enable***.
- Những giờ không cho phép quay số được áp dụng cho giao diện trên ***router*** sẽ ngăn không cho thiết lập kết nối.
- Các bộ lọc quay số theo yêu cầu được áp dụng cho giao diện trên ***router*** sẽ ngăn không cho thiết lập kết nối.

Không thể tạo một kết nối quay số theo yêu cầu

Nếu hệ thống của bạn không thể tạo được kết nối quay số theo yêu cầu, xác nhận các vấn đề dưới đây cho cả hai router gọi và nhận như sau:

- Dịch vụ ***Routing And Remote Access*** đều đang chạy trên cả hai ***router***.
- Định tuyến đã được kích hoạt ở chế độ ***LAN and demand-dial routing*** trên cả hai ***router***.
- Các cổng quay số sẽ được sử dụng trên cả hai router đều được cấu hình để cho phép các kết nối định tuyến quay số theo yêu cầu (chiều vào và chiều ra).
- Có ít nhất một trong các cổng quay số trên cả hai ***router*** duy trì trạng thái chưa kết nối.
- Cả hai ***router***, kết hợp với một chính sách truy cập từ xa được kích hoạt để sử dụng ít nhất một phương pháp xác thực chung.

ỦY QUYỀN CHO CÁC KẾT NỐI TRUY CẬP TỪ XA

Sau khi các chứng thực của người sử dụng được xác thực thông qua kết nối truy cập từ xa thì kết nối phải được ủy quyền truy cập. Quá trình ủy quyền truy cập từ xa gồm có hai bước:

1. Các đặc tính quay số của tài khoản người sử dụng được xác nhận.
2. Chính sách truy cập từ xa đầu tiên đáp ứng được liệt kê trong màn hình quản trị ***Routing And Remote Access*** sẽ được áp dụng.

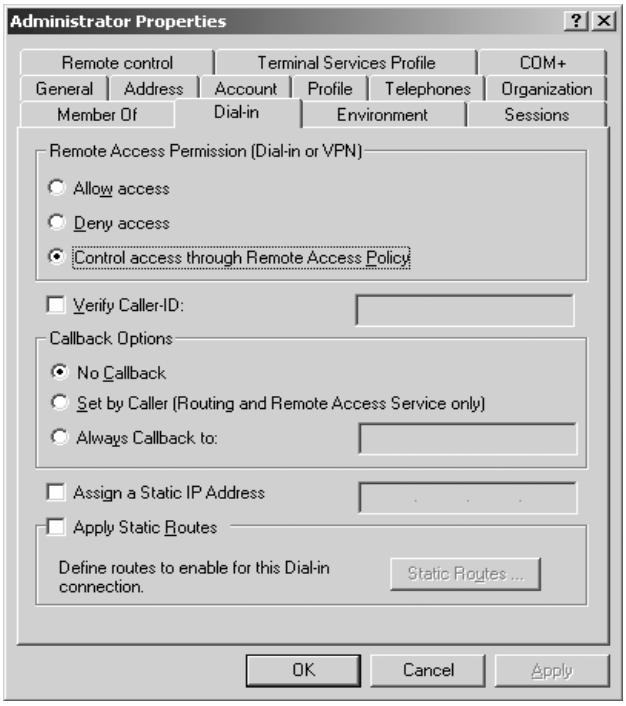
Cấu hình các đặc tính quay số của tài khoản người sử dụng

Các đặc tính quay số được cung cấp cho cả kết nối quay số và kết nối VPN sẽ được cấu hình trong phần Dial-In của hộp thoại ***User Account Properties***. Nếu một người sử dụng đang quay số tới một miền thì một tài khoản tương ứng với tên được gửi thông qua kết nối quay số phải tồn tại trên miền. Do đó, các đặc tính quay số của tài khoản này phải được cấu hình trong màn hình quản trị ***Active Directory Users And Computers.***

Nếu người sử dụng đó quay số tới một máy chủ độc lập (không thuộc bất kỳ miền nào) thì tài khoản của anh ta phải tồn tại trên cơ sở dữ liệu SAM của máy chủ đó. SAM là một dịch vụ trên hệ điều hành Windows được sử dụng

trong suốt tiến trình đăng nhập. SAM duy trì thông tin về tài khoản của người sử dụng bao gồm cả thông tin người sử dụng thuộc về nhóm nào. Các đặc tính quay số của tài khoản này có thể được cấu hình trong phần ***Local Users And Groups*** của màn hình quản trị ***Computer Management.***

Hình 7-16 hiển thị màn hình của thẻ Dial-In trong các đặc tính tài khoản người sử dụng và phần này sẽ được miêu tả trong phần kế tiếp.



Hình 7-16: Cấu hình các đặc tính quay số cho một người sử dụng

Trong tất cả các môi trường hoạt động của máy chủ ngoại trừ các miền AD có chức năng hoạt động là hỗn hợp Windows 2000 thì lựa chọn ***Control Access Through Remote Access Policy*** (*điều khiển truy cập thông qua chính sách truy cập từ xa*) mặc định sẽ được kích hoạt. Bạn có thể thiết lập quyền truy cập từ xa cho các tài khoản ở một trong ba mức sau:

■ **Control Access Through Remote Access Policy** (Điều khiển truy cập thông qua chính sách truy cập từ xa) Lựa chọn này hoặc cho phép hoặc cấm cho phép truy cập quay số đối với người sử dụng. Thay vào đó, quyền của người sử dụng sẽ được xác định thông qua chính sách truy cập đầu tiên phù hợp được áp dụng cho kết nối. (Mặc định, các chính sách truy cập từ xa sẽ cấm tất cả các kết nối truy cập từ xa)

■ **Deny Access** (cấm truy cập) Khi bạn chọn lựa chọn này, người sử dụng sẽ không thể thực hiện truy cập qua cơ chế quay số tới hệ thống được bất kể anh ta nhận được các thiết lập hoặc các chính sách khác.

■ **Allow Access** (cho phép truy cập) Khi bạn chọn lựa chọn này, người sử dụng sẽ được phép truy cập qua cơ chế quay số tới hệ thống. lựa chọn này sẽ ghi dè lên các thiết lập về cấp phép truy cập từ xa trong các chính sách. Bạn cần chú ý lựa chọn ***Allow Access*** không phải lúc nào cũng ngăn không cho các chính sách truy cập từ xa khóa các cấp phép truy cập. Một chính sách truy cập từ xa vẫn có thể ngăn không cho phép một tài khoản truy cập thông qua *khái lược chính sách truy cập từ xa*. Ví dụ, một *khái lược* yêu cầu người sử dụng chỉ có thể truy cập trong khoảng thời gian làm việc trong ngày vì vậy anh ta không thể truy cập tới hệ thống vào buổi tối thậm chí khi lựa chọn ***Allow Access*** đã được thiết lập trong đặc tính quay số trong tài khoản người sử dụng. Tuy nhiên, lựa chọn này lại phủ nhận thiết lập ***Deny Remote Access Permission*** (cấm quyền truy cập từ xa) trong các chính sách truy cập từ xa.

> **QUAN TRỌNG** ***Các quyền truy cập từ xa trên miền Active Directory hoạt động ở chế độ hỗn hợp*** *Mặc định, các miền Active Directory trong Windows Server 2003 lần đầu tiên cài đặt sẽ hoạt động ở chế độ hỗn hợp Windows 2000. Trong môi trường này, bạn chỉ có thể gán lựa chọn Allow Access và Deny Access cho tài khoản của người sử dụng. Mặc định lựa chọn Allow Access được chọn và nó tương đương với thiết lập Control Access Through Remote Access Policy trong tất cả các môi trường máy chủ khác. Với môi trường hoạt động này, không có thiết lập cho phép bạn phủ nhận các quyền truy cập từ xa mức người sủ dụng trong các chính sách.*

Kiểm chứng mã số ID của người khởi tạo kết nối quay số

Nếu hộp kiểm tra ***Verify Caller ID*** được chọn, máy chủ sẽ kiểm chứng số điện thoại của người khởi tạo kết nối. Nếu số điện thoại không đáp ứng với số đã được cấu hình thì kết nối sẽ bị cấm. Thiết bị khởi tạo kết nối, hệ thống điện thoại giữa phía khởi tạo và máy chủ, máy chủ truy cập từ xa phải hỗ trợ tính năng ***Caller ID*** (mã số phía khởi tạo). Trên một máy tính cài đặt dịch vụ ***Routing And Remote Access***, hỗ trợ tính năng này gồm có thiết bị trả lời cuộc gọi có nhiệm vụ cung cấp thông tin mã số phía khởi tạo và trình điều khiển Windows tương ứng để chuyển thông tin tới dịch vụ RRAS. Nếu bạn cấu hình một số điện thoại cho một người sử dụng và bạn không hỗ trợ tính năng chuyển thông tin ***caller ID*** từ phía khởi tạo tới dịch vụ ***Routing And Remote Access*** thì kết nối sẽ bị cấm.

Tìm hiểu lựa chọn callback

Mặc định thiết lập này được cấu hình là ***No Callback***. Nếu lựa chọn ***Set By Caller*** được chọn, máy chủ sẽ khởi tạo ngược lại một kết nối đến phía khởi

tạo theo số điện thoại được cung cấp. Nếu lựa chọn ***Always Call Back To*** được chọn, người quản trị phải xác định một số điện thoại để máy chủ luôn sử dụng nó trong suốt quá trình khởi tạo ngược lại. Tính năng khởi tạo ngược lại yêu cầu phần mở rộng **LCP** (***Link Control Protocol*** – Giao thức điều khiển đường truyền) được kích hoạt trong ***Routing And Remote Access*** (mặc định, chúng được kích hoạt).

Gán địa chỉ IP tĩnh

Bạn có thể cấu hình thiết lập ***Assign A Static IP Address*** nhằm gán một địa chỉ IP cụ thể cho một người sử dụng khi kết nối được thực hiện.

Áp dụng các đường định tuyến tĩnh

Bạn có thể sử dụng thiết lập ***Apply Static Routes*** để định nghĩa một loạt các đường định tuyến tĩnh, sau đó đưa vào bảng định tuyến của máy chủ cài đặt dịch vụ ***Routing And Remote Access*** khi kết nối được thực hiện.

ÁP DỤNG CÁC CHÍNH SÁCH TRUY CẬP TỪ XA

Chính sách truy cập từ xa là một tập hợp các quyền hoặc những giới hạn được một máy chủ xác thực đọc và áp dụng cho các kết nối truy cập từ xa. Trong Windows NT4 và 3.51, các quyền truy cập từ xa khá đơn giản. Các quyền truy cập từ xa được gán trực tiếp cho các tài khoản bằng cách sử dụng công cụ ***User Manager*** hoặc ***Remote Access Administration***. Mặc dù các quyền này đơn giản và dễ hiểu nhưng chúng chỉ làm việc tốt khi số lượng người sử dụng yêu cầu quyền truy cập từ xa là ít.

Trong Windows Server 2003 và Windows 2000, quá trình xác thực truy cập từ xa phức tạp hơn và bạn cần chú ý nhiều hơn để hiểu về vấn đề này. Tuy nhiên nó cũng cung cấp cho bạn nhiều tính năng mạnh hơn và bạn có thể cấu hình một cách chính xác nhằm đáp ứng những yêu cầu về bảo mật và truy cập cho cả môi trường mạng nhỏ và lớn.

Như đã đề cập ở trên, quá trình xác thực sẽ kết hợp cả đặc tính quay số của tài khoản người sử dụng và các chính sách truy cập từ xa. Với các chính sách, các kết nối có thể được xác thực hoặc ngăn cấm dựa trên các đặc tính của người sử dụng, thành viên nhóm, thời điểm trong ngày, loại kết nối yêu cầu và nhiều tham số khác.

> ***CHÚ Ý Phân biệt giữa xác thực (authentication) với ủy quyền (authorization)*** *Các khái niệm này thông thường rất dễ bị nhầm lẫn. Xác thực là quá trình xác nhận một thực thể hoặc một đối tượng xem*

đó có đúng như đã khai báo hay không. Ví dụ, để xác nhận về nguồn gốc và tính toàn vẹn của dữ liệu, người ta có thể kiểm chứng thông qua một chữ ký điện tử hoặc mã nhận diện của một người sử dụng hoặc một máy tính. Trong khi đó ủy quyền là quá trình xác định xem một người sử dụng được phép làm gì trên một máy tính hoặc mạng. Về bản chất thì việc ủy quyền sẽ chỉ xảy ra sau khi quá trình xác thực thành công.

CẤU HÌNH MỘT CHÍNH SÁCH TRUY CẬP TỪ XA

Một chính sách truy cập từ xa là một luật dùng để áp dụng cho các kết nối từ xa gồm có ba thành phần: các điều kiện, các quyền truy cập từ xa và *khái lược (profile)*:

■ **Các điều kiện** Các điều kiện trong chính sách truy cập từ xa bao gồm một hoặc nhiều các đặc tính và chúng sẽ được sử dụng để so sánh với các tham số do kết nối tạo ra. Nếu có nhiều điều kiện đưa ra thì tất cả các điều kiện đó phải được đáp ứng thì kết nối đó mới được coi là đáp ứng chính sách.

■ **Các quyền truy cập từ xa** Nếu tất cả các điều kiện của một chính sách được đáp ứng thì thiết lập ***If A Connection Request Matches The Specified Conditions*** (*nếu một kết nối đáp ứng các điều kiện đặt ra*) được áp dụng và kết nối đó sẽ được áp gán quyền truy cập hoặc ngăn cấm. Cần chú ý quyền truy cập từ xa cũng được gán hoặc cấm đối với từng tài khoản. Các quyền này sẽ có độ ưu tiên cao hơn so với các quyền trong chính sách. Khi quyền truy cập từ xa của một tài khoản được đặt là ***Control Access Through Remote Access Policy*** (*điều khiển truy cập thông qua chính sách*) thì chính sách sẽ xác định xem người sử dụng đó có được phép truy cập hay không. Gán quyền truy cập thông qua quyền của tài khoản hoặc thông qua chính sách là bước đầu tiên trong việc chấp nhận một kết nối. Một kết nối khi được khởi tạo sẽ bao gồm các tham số và chúng sẽ là mục tiêu để so sánh với cả các đặc tính quay số của người sử dụng lẫn các đặc tính trong *khái lược (profile)* của chính sách. Nếu một kết nối không đáp ứng được các thiết lập trong tài khoản người sử dụng hoặc trong *khái lược(profile)* của chính sách thì kết nối đó sẽ bị loại bỏ.

■ ***Khái lược (profile)*** Sau khi kết nối đã được ủy quyền thì một tập hợp các đặc tính chứa trong *khái lược (profile)* của chính sách truy cập từ xa

sẽ được áp dụng. Tập hợp các đặc tính (sẽ được giải thích trong phần này) gồm có (xem Hình 7-17):

c. Dial-In Constraints

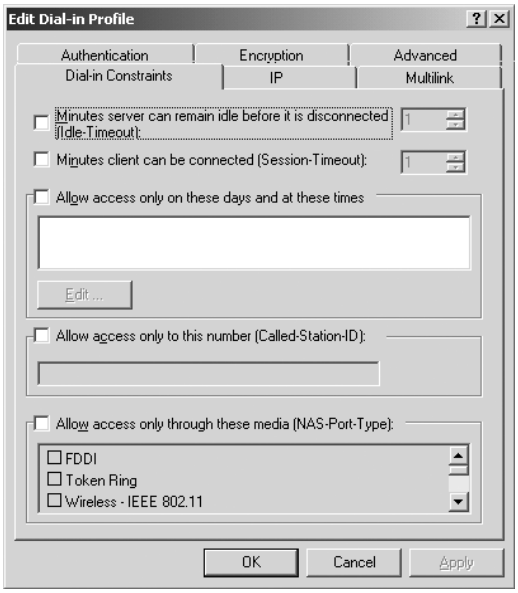
d. IP

e. Multilink

f. Authentication

g. Encryption

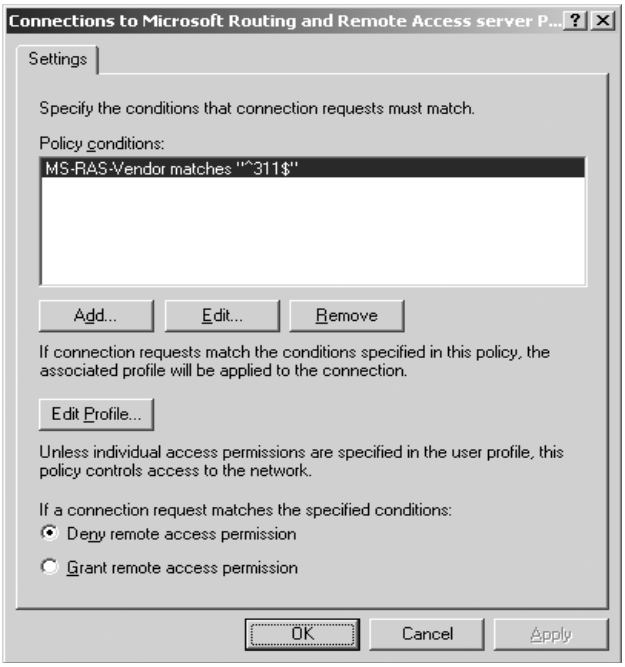
h. Advanced



Hình 7-17: Các thiết lập trong *Khái lược* Dial-In

Mặc định, dịch vụ ***Routing And Remote Access*** được cấu hình với hai chính sách dưới đây:

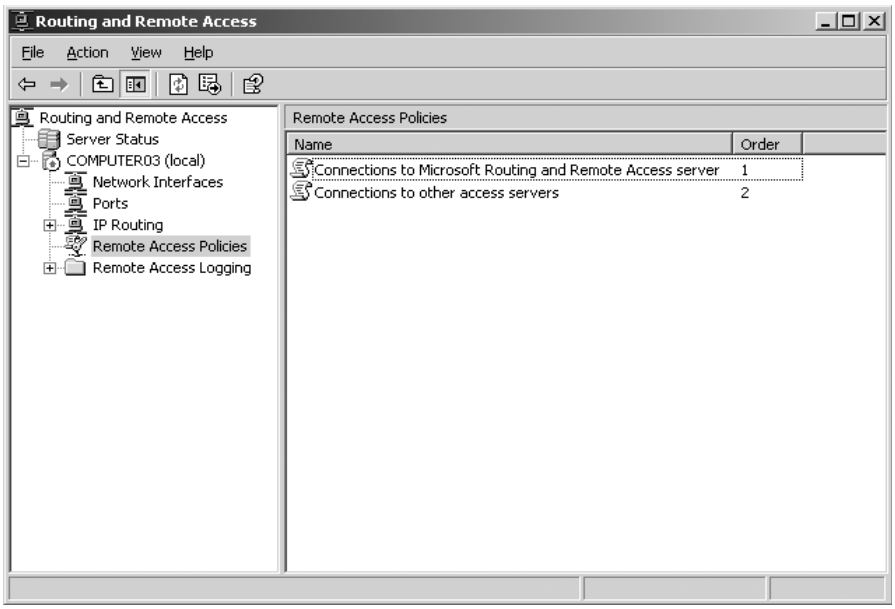
■ **Connections To Microsoft Routing And Remote Access** Chính sách này chỉ chứa duy nhất một điều kiện: ***MS-RAS-Vendor Matches "^311$"*** (xem Hình 7-18). Điều này có nghĩa rằng chính sách chỉ áp dụng khi phiên bản của ***RADIUS*** phía máy trạm là ***^311$.*** Bất kỳ máy trạm nào có phiên bản ***RADIUS*** không đáp ứng điều kiện nói trên sẽ được kiểm tra xem có đáp ứng chính sách thứ hai hay không.



Hình 7-18: Trang Properties của chính truy cập từ xa mặc định

■ **Connections To Other Access Servers** Chính sách này được cấu hình nhằm kiểm tra tính đáp ứng của mỗi kết nối đến bất kể kiểu máy chủ truy cập. Tuy nhiên do chính sách đầu tiên đáp ứng tất cả các kết nối tới ***Routing And Remote Access*** nên chỉ các kết nối tới các máy chủ truy cập khác mới được kiểm tra tính đáp ứng với điều kiện thứ tự của chính sách mặc định không bị thay đổi. Trừ phi chính sách đầu tiên bị xóa hoặc thứ tự chính sách mặc định thay đổi thì chính sách thứ hai này mới được máy chủ RADIUS đọc.

Như Hình 7-19, bạn có thể hiển thị các chính sách truy cập từ xa được cấu hình trong màn hình quản trị ***Routing And Remote Access*** bằng cách lựa chọn phần ***Remote Access Policies***.



Hình 7-19: Màn hình quản trị Routing And Remote Access

Các chính sách truy cập từ xa là duy nhất trên mỗi máy tính nhưng không duy nhất đối với ***Routing And Remote Access.*** Sau khi bạn tạo ra chúng, chúng có thể được ***Routing And Remote Access*** hoặc máy chủ ***RADIUS*** được cấu hình trên máy tính cục bộ đọc. Tương tự, bạn cũng không thể loại bỏ các chính sách truy cập từ xa đơn giản bằng cách cấm dịch vụ ***Routing And Remote Access***. Ngoài ra, các chính sách truy cập từ xa được lưu lên ổ đĩa cứng và được lưu trữ cho tới khi chúng bị xóa thông qua màn hình quản trị ***Routing And Remote Access*** hoặc ***Internet Authentication Service*** (đây là công cụ quản trị máy chủ RADIUS).

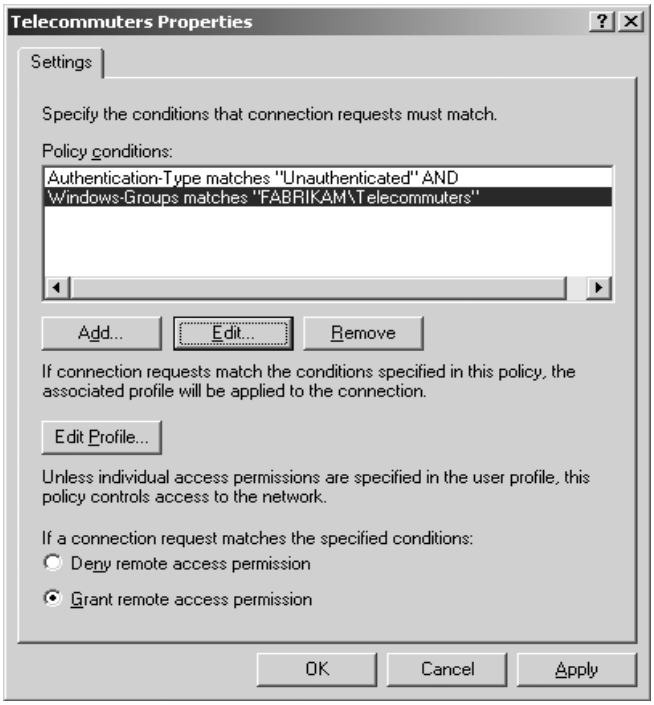
Mặc định, trên Windows Server 2003 có hai chính sách được cấu hình trước. Chính sách đầu tiên ***Connections To Microsoft Routing And Remote Access*** được cấu hình nhằm đáp ứng mỗi kết nối truy cập từ xa tới dịch vụ ***Routing And Remote Access***. Khi ***Routing And Remote Access*** đọc chính sách này, về bản chất nó sẽ đáp ứng mỗi kết nối đến. Tuy nhiên khi một máy chủ RADIUS đọc chính sách này, truy cập mạng có thể được cung cấp bởi một nhà sản xuất không phải là Microsoft nên chính sách này sẽ không đáp ứng các kiểu kết nối này.

Chính sách mặc định thứ hai là ***Connections To Other Access Servers.*** Chính sách này được cấu hình nhằm đáp ứng tất cả các kết nối đến bất kể chủng loại máy chủ truy cập tức là không quan tâm đến nhà sản xuất. Tuy nhiên do chính sách đầu tiên đáp ứng tất cả các kết nối tới ***Routing And Remote Access*** nên chỉ có các kết nối tới các máy chủ truy cập khác mới được kiểm tra tính đáp ứng với điều kiện thứ tự của chính sách mặc định

không bị thay đổi. Trừ phi chính sách đầu tiên bị xóa hoặc thứ tự chính sách mặc định thay đổi thì chính sách thứ hai này mới được máy chủ RADIUS đọc.

Các điều kiện trong chính sách truy cập từ xa

Mỗi chính sách truy cập từ xa được dựa trên các điều kiện của chính sách đó nhằm xác định xem khi nào thì chính sách được áp dụng. Ví dụ, một chính sách có thể có một điều kiện đặc tính Windows-Groups đáp ứng ***FABRIKAM\Telecommuters*** có nghĩa là chính sách này chỉ đáp ứng kết nối mà người sử dụng là thành viên của nhóm bảo mật toàn cục ***Telecommuters***. Hình 7-20 hiển thị chính sách đã mô tả trên.

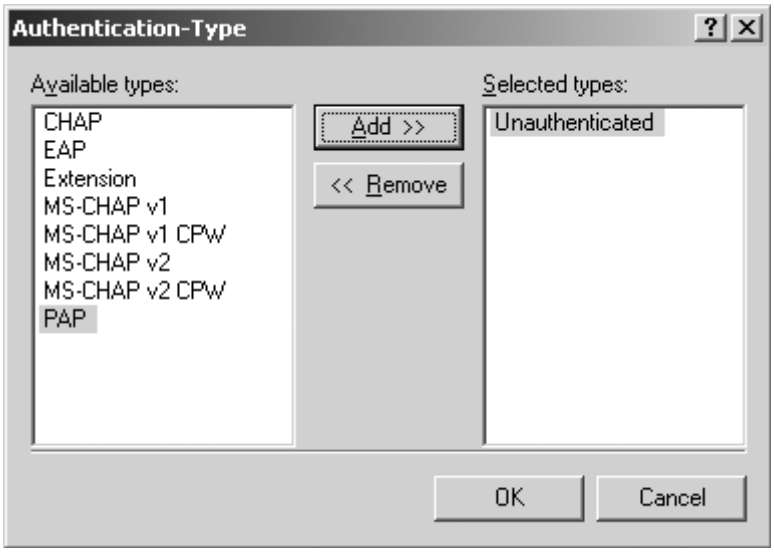


Hình 7-20: Các điều kiện về quay số của Telecommuters

Nhấp vào nút ***Add*** để mở hộp thoại ***Select Attribute*** cho phép bạn thêm một điều kiện mới vào chính sách truy cập từ xa. Ví dụ, đặc tính NAS-IP-Address cho phép một máy chủ RADIUS phân biệt các máy trạm truy cập từ xa kết nối qua một máy chủ cụ thể (được phân biệt bởi địa chỉ IP). Hình 7-21 hiển thị hộp thoại ***Select Attribute*** và tập hợp các đặc tính có khả năng cấu hình của nó.

Hình 7-21: Các đặc tính có thể đưa vào trong một chính sách

Bằng cách nhấp vào nút ***Add*** trong hộp thoại ***Select Attribute***, bạn có thể mở một hộp thoại cho phép bạn cấu hình điều kiện cho một đặc tính cụ thể. Ví dụ, như Hình 7-22, hộp thoại ***Authentication-Type*** xuất hiện nếu bạn nhấp vào nút ***Add*** khi đặc tính ***Authentication-Type*** được lựa chọn. Hộp thoại này cho phép bạn lựa chọn các kết nối truy cập từ xa nào đáp ứng chính sách thông qua giao thức *xác thực*. Trong ví dụ này, chính sách này được cấu hình để đáp ứng các kết nối không *xác thực*. Tương tự, bạn có thể xác định các thành phần cụ thể cho bất kỳ đặc tính nào bạn chọn để phục vụ như các điều kiện của một chính sách.



Hình 7-22: Ví dụ về các thành phần của một điều kiện

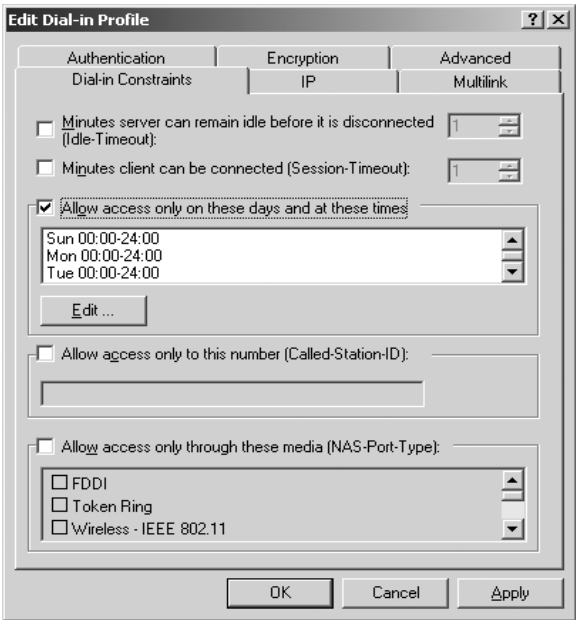
CHÚ Ý ***Điều kiện trong chính sách và các nhóm bảo mật global*** *Chỉ có các thành viên của các nhóm bảo mật toàn cục mới có thể đưa vào làm điều kiện trong các chính sách. Bạn không thể đưa thành viên của các nhóm bảo mật tổng hợp hoặc miền cục bộ vào làm điều kiện trong các chính sách.*

Cấp phép truy cập từ xa

Mỗi chính sách truy cập từ xa xác định xem một kết nối nếu đáp ứng các điều kiện trong chính sách đó sẽ được phép hay bị cấm. Các thiết lập Cấp phép này tương ứng với lựa chọn ***Grant Remote Access Permission*** hoặc ***Deny Remote Access Permission*** như được mô tả trong Hình 7-20 ở trên. Cần nhớ rằng lựa chọn ***Allow Access*** (không tính môi trường miền hoạt động ở chế độ hỗn hợp Windows 2000) và ***Deny Access*** (trong phần đặc tính quay số của một tài khoản riêng lẻ) thường sẽ có độ ưu tiên cao hơn thiết lập này.

Profile của chính sách

Một ***profile*** chính sách truy cập từ xa bao gồm một tập hợp các ràng buộc và các đặc tính được áp dụng cho một kết nối. Bạn có thể cấu hình một ***profile*** bằng cách nhấp vào nút ***Edit Profile*** trong trang ***Properties*** của chính sách như Hình 7-20. Nhấp vào nút này sẽ mở hộp thoại ***Edit Dial-In Profile*** như trên Hình 7-23. Mặc định, ***profile*** của một chính sách chưa được cấu hình nên sẽ không có bất kỳ ràng buộc nào hoặc đặc tính nào được áp dụng cho các kết nối.



Hình 7-23: Profile của chính sách truy cập từ xa đã được cấu hình

Các phần dưới đây miêu tả 06 thẻ xuất hiện trong profile của một chính sách

■ **Dial-In Constraints** (*các ràng buộc về quay số*) Thẻ này cho phép bạn đặt các ràng buộc sau:

- **Minutes Server Can Remain Idle Before It Is Disconnected**: kết nối sẽ bị ngắt sau khoảng thời gian xác định nếu không có dữ liệu trên đường truyền.
- **Minutes Client Can Be Connected:** khoảng thời gian cho phép các máy trạm kết nối tới.
- **Allow Access Only On These Days And At These Times**: chỉ cho phép quay số tới máy chủ tại những ngày xác định và vào những thời điểm xác định.
- **Allow Access Only To This Number:** chỉ cho phép truy cập bằng số điện thoại này.
- **Allow Access Only Through These Media:** chỉ cho phép truy cập thông qua những thiết bị được xác định bên dưới.

■ **IP** Bạn có thể đặt các đặc tính IP nhằm xác định quá trình gán địa chỉ IP. Bạn có những lựa chọn dưới đây:

- **Server Must Supply An IP Address**: máy chủ phải cấp phát một địa chỉ IP cho máy trạm.
- **Client May Request An IP Address**: máy trạm có thể yêu cầu một địa chỉ IP.
- **Server Settings Determine IP Address Assignment** (thiết lập mặc định): các thiết lập trên máy chủ sẽ xác định quá trình gán địa chỉ IP.
- **Assign A Static IP Address**. gán một địa chỉ IP tĩnh. Địa chỉ IP được gán thông thường được sử dụng nhằm đáp ứng các đặc tính tuân theo nhà sản xuất cho các địa chỉ IP.

Bạn cũng có thể sử dụng thẻ IP để định nghĩa các bộ lọc gói IP nhằm áp dụng cho lưu lượng của kết nối truy cập từ xa.

■ **Multilink** Bạn có thể thiết lập đặc tính **multilink** (đa đường) nhằm cho phép thực hiện một kết nối trên nhiều đường khác nhau và xác định số lượng lớn nhất các cổng (hay số lượng các modem) mà một kết nối đa đường có thể sử dụng.

Thêm vào đó, bạn có thể thiết lập chính sách BAP (***Bandwidth Allocation Protocol*** - *Giao thức Xác định Giải thông Sử dụng*) nhằm xác định mức độ sử dụng dải thông và xác định xem các đường truyền nào vượt quá mức BAP cho phép sẽ bị loại bỏ. Các đặc tính multilink và BAP có thể sử dụng được trong ***Routing And Remote Access***. Mặc định chúng không được kích hoạt.

Dịch vụ ***Routing And Remote Access*** phải kích hoạt tính năng ***multilink*** và ***BAP*** thì đặc tính ***multilink*** trong ***profile*** mới được thực thi.

■ **Authentication** Bạn có thể thiết lập các đặc tính *xác thực* nhằm cho phép: các kiểu *xác thực* được áp dụng cho một kết nối; kiểu EAP (giao thức *xác thực* mở rộng) phải được sử dụng. Ngoài ra, bạn có thể cấu hình kiểu EAP. Mặc định, MS-CHAP và MS-CHAP v2 được kích hoạt. Trong Windows Server 2003, bạn có thể xác định xem người sử dụng có thể thay đổi được mật khẩu đã hết hạn sử dụng bằng cách sử dụng MS-CHAP và MS-CHAP v2 (đây là các giao thức được kích hoạt theo mặc định).

Dịch vụ ***Routing And Remote Access*** phải kích hoạt các kiểu *xác thực* tương ứng thì các đặc tính *xác thực* trong profile mới được thực thi.

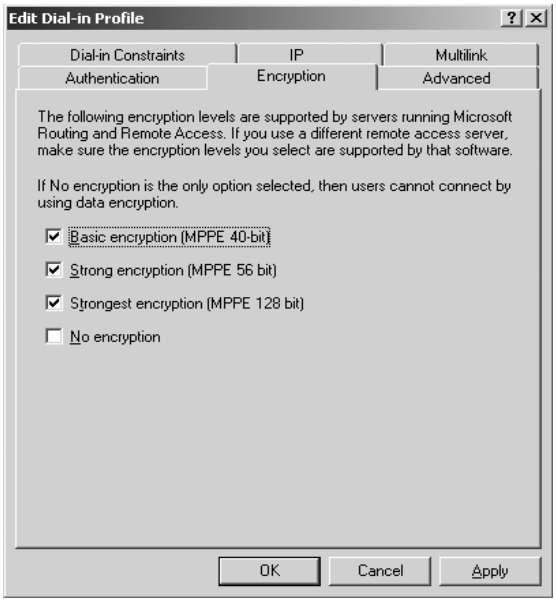
■ **Encryption** Windows Server 2003 hỗ trợ hai phương pháp mã hóa thông dụng cho dữ liệu của kết nối truy cập từ xa là: ***Rivest-Shamir-Adleman*** (RSA) RC4 và ***Data Encryption Standard*** (DES). RSA RC4 là thuật toán khá quen thuộc được sử dụng trong **MPPE** (***Microsoft Point-to-Point Encryption*** *– mã hóa kết nối điểm-điểm của Microsoft*). Kiểu mã hóa này được sử dụng với các giao thức *xác thực* MS-CHAP hoặc EAP-TLS (***Extensible Authentication Protocol-Transport Layer Security***) cho cả kết nối quay số lẫn kết nối VPN dựa trên PPTP. DES là cơ chế mã hóa thường được sử dụng với IPSec – một chuẩn bảo mật được sử dụng với giao thức *xác thực* L2TP trong các mạng riêng ảo VPN. (VPN, PPTP và L2TP/IPSec được đề cập trong phần "Các thành phần của một mạng riêng ảo" trong chương này).

Bảng 7-2 dưới đây sẽ mô tả các mức mã hóa mà MPPE và IPSec hỗ trợ.

Bảng 7-2: Các loại mã hóa

Kiểu mã hóa	Mức mã hóa hỗ trợ
MPPE chuẩn	40 bit, 56 bit
MPPE tăng cường	128 bit
IPSec DES	56 bit
IPSec Triple DES	168 bit

Các thiết lập trong thẻ ***Encryption*** trong một khái lược của chính sách truy cập từ xa (xem Hình 7-24) cho phép bạn xác định các mức mã hóa cho phép hoàn toàn độc lập với các kiểu mã hóa. Tuy nhiên, bản chất của mỗi mức mã hóa lại biến đổi theo cơ chế mã hóa được sử dụng.



Hình 7-24: Thẻ Encryption trong profile của một chính sách

Có tất cả bốn lựa chọn về mã hóa cho phép trong thẻ Encryption:

- **Basic Encryption (MPPE 40-Bit)** Đối với các kết nối quay số và VPN dựa trên PPTP thì MPPE được sử dụng với khóa có chiều dài 40 bit. Đối với các kết nối VPN L2TP/IPSec, cơ chế mã hóa DES 56 bit được sử dụng.

- **Strong Encryption (MPPE 56-Bit)** Đối với các kết nối quay số và VPN dựa trên PPTP thì MPPE được sử dụng với khóa có chiều dài 56 bit. Đối với các kết nối VPN L2TP/IPSec, cơ chế mã hóa DES 56 bit được sử dụng.

■ **Strongest Encryption (MPPE 128-Bit)** Đối với các kết nối quay số và VPN dựa trên PPTP thì MPPE được sử dụng với khóa có chiều dài 128 bit. Đối với các kết nối VPN L2TP/IPSec, cơ chế mã hóa Triple DES (một cơ chế mã hóa tương tự như DES nhưng sử dụng chiều dài khóa gấp ba lần) 168 bit được sử dụng.

■ **No Encryption** Lựa chọn này cho phép các kết nối không mã hóa và đáp ứng các điều kiện trong chính sách truy cập đưa ra. Xóa bỏ lựa chọn này tức là nó yêu cầu mã hóa.

■ **Advanced** Bạn có thể đặt các tham số mạnh hơn để xác định một loạt các đặc tính RADIUS mà máy chủ IAS sẽ quay trở lại kiểm tra máy chủ truy cập mạng (NAS) và máy trạm RADIUS. Chỉ có duy nhất máy chủ RADIUS sử dụng các thiết lập này còn Routing And Remote Access không sử dụng chúng.

QUẢN TRỊ XÁC THỰC TRUY CẬP MẠNG VÀ CÁC CHÍNH SÁCH

Sau khi máy trạm quay số tới máy chủ truy cập từ xa và các địa chỉ IP cần thiết được gán, các chứng thực được cung cấp cùng với kết nối phải được xác thực. Xác thực là tiến trình kiểm tra tính hợp lệ - thông qua việc xác nhận mật khẩu hoặc các chứng thực thay thế như chứng chỉ hoặc thẻ thông minh chẳng hạn – để xác nhận trên thực tế người dùng chính là người mà họ đã khai báo. Việc xác thực truy cập từ xa xảy ra trước tiến trình xác thực đăng nhập miền. Nếu một người sử dụng quay số cố gắng kết nối để đăng nhập vào miền từ xa thì kết nối đó phải được xác thực, ủy quyền và thiết lập kết nối trước khi quá trình đăng nhập miền thông thường xảy ra.

Để đăng nhập vào một miền thông qua kết nối quay số, lựa chọn hộp kiểm tra ***Log On Using Dial-Up Connection*** trong hộp thoại ***Log On To Windows***. Sau khi bạn nhập tên và mật khẩu rồi nhấp ***OK*** thì hộp thoại ***Network Connection*** xuất hiện. Từ danh sách thả xuống ***Choose A Network Connection*** lựa chọn kết nối mà bạn đã cấu hình cho việc truy cập từ xa qua cơ chế quay số rồi nhấp ***Connect***.

Kết nối quay số bắt đầu và tiếp đó là quá trình xác thực và ủy quyền. Thông thường, tên người sử dụng, miền và mật khẩu được cấu hình cho kết nối cũng giống với những gì bạn cần xác nhận với quá trình đăng nhập miền. Tuy nhiên hai tập các chứng thực này được cấu hình và xác thực hoàn toàn độc lập.

Một kết nối truy cập từ xa được thiết lập nếu các chứng thực cho kết nối đó được xác thực thành công và kết nối đó được ủy quyền. Quá trình đăng nhập miền thông thường xảy ra như sau: các chứng thực mà bạn nhập vào trong hộp thoại ***Log On To Windows*** sẽ được xác nhận với một máy chủ điều khiển miền phục vụ cho quá trình xác thực.

> **CHÚ Ý** ***Xác thực cục bộ và từ xa*** *Nếu người sử dụng quay số tới một máy chủ độc lập tức là máy chủ này không phải là thành viên của bất kỳ miền nào thì trước hết họ phải đăng nhập tới các tính cục bộ hoặc các miền cục bộ của họ trước khi kết nối tới máy chủ từ xa. Trong trường hợp này, quá trình xác nhận các chứng thực của máy tính từ xa được gửi trên kết nối quay số chỉ yêu cầu xác thực trước khi kết nối được ủy quyền và thiết lập. Các chứng thực này phải được lưu trên cơ sở dữ liệu SAM cục bộ của máy chủ đón kết nối trước khi người sử dụng kết nối.*

Thực hiện xác thực thông qua RADIUS

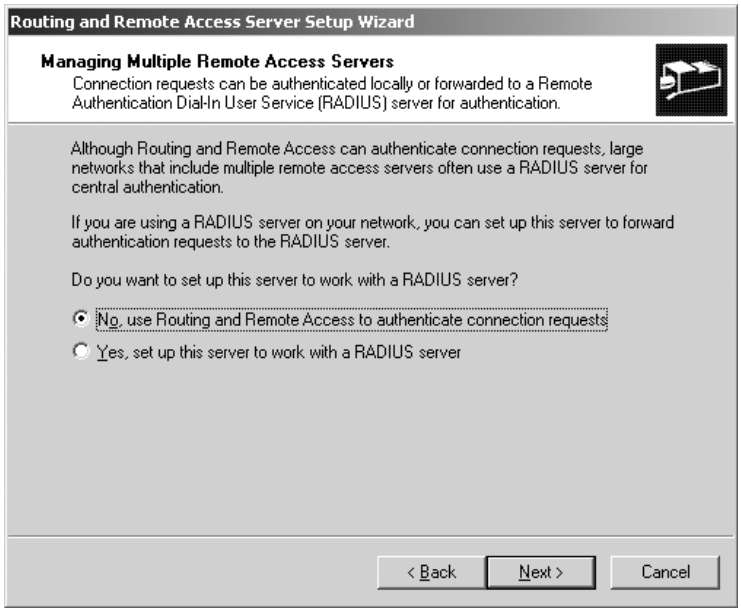
Bạn có thể cấu hình tiến trình *xác thực* truy cập từ xa được thực thi thông qua *xác thực* Windows hoặc một máy chủ RADIUS. Trong *xác thực* Windows, khi người sử dụng cố gắng quay số tới một máy tính thuộc một nhóm thì máy chủ sẽ xác thực kết nối bằng cách kiểm tra tính hợp lệ của tên và mật khẩu trong cơ sở dữ liệu bảo mật cục bộ nằm ngay trên máy chủ đó. Khi người sử dụng quay số kết nối tới một miền, máy chủ sẽ hướng các yêu cầu xác thực tới một máy chủ điều khiển miền. Tuy nhiên, khi bạn cấu hình một máy chủ RADIUS để xác thực các kết nối truy cập từ xa thì máy chủ sẽ chuyển cả hai trách nhiệm *xác thực* và ủy quyền đến một máy chủ trung tâm cài đặt dịch vụ IAS.

Bạn lựa chọn phương pháp xác thực này ở một trong hai nơi sau: trên trang ***Managing Multiple Remote Access Servers*** của ***Routing And Remote Access Server Setup Wizard*** (xem Hình 7-25) hoặc trong thẻ ***Security*** của hộp thoại ***Server Properties*** trong màn hình quản trị ***Routing And Remote Access*** (xem Hình 7-26). Chú ý rằng, nếu bạn muốn sử dụng *xác thực* Windows thay cho một máy chủ RADIUS trong *trình hướng dẫn*, bạn có thể chọn lựa chọn ***No, Use Routing And Remote Access To Authenticate Connection Requests*** (*Không, tôi muốn sử dụng RRAS để xác thực các yêu cầu kết nối*).

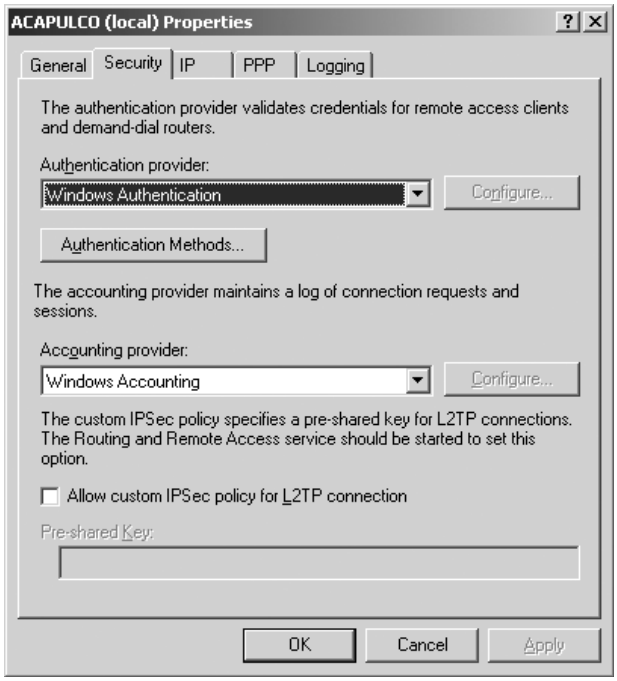
Lựa chọn các giao thức xác thực

Để *xác thực* các chứng thực được xác nhận qua kết nối quay số, trước hết máy chủ phải thỏa hiệp với phía máy trạm một giao thức xác thực chung.

Hầu hết các giao thức xác thực đều cung cấp một số phương pháp đo mức bảo mật do đó các chứng thực của người sử dụng không thể bị can thiệp. Các giao thức xác thực trên các máy trạm và máy chủ Windows được gán một độ ưu tiên dựa trên mức bảo mật này.



Hình 7-25: Lựa chọn phương pháp xác thực bằng cách sử dụng Routing And Remote Access Server Setup Wizard



Hình 7-26: Lựa chọn phương pháp xác thực bằng cách sử dụng thẻ Security

Giao thức xác thực được lựa chọn cho một kết nối truy cập từ xa luôn là bảo mật nhất trong số những giao thức được cho phép trên các đặc tính kết nối phía máy trạm, các đặc tính máy chủ kết nối từ xa và các chính sách được áp dụng cho kết nối. Mặc định, giao thức được chọn là MS-CHAP v2 được áp dụng cho tất cả các máy trạm và máy chủ cài đặt hệ điều hành Windows 2000, Windows XP, hoặc Windows Server 2003.

Dưới đây là một danh sách đầy đủ về các giao thức xác thực được Routing And Remote Access hỗ trợ trên hệ điều hành Windows Server 2003 (danh sách này liệt kê theo thứ tự từ bảo mật nhất đến bảo mật kém hơn):

■ **EAP-TLS** Một giao thức xác thực dựa trên chứng chỉ được thực hiện trên nền EAP (đây là một khuôn dạng có khả năng mở rộng nhằm hỗ trợ các phương pháp xác thực mới).

EAP-TLS thường được sử dụng kết hợp với các thẻ thông minh. Nó hỗ trợ mã hóa cả dữ liệu xác thực lẫn dữ liệu của kết nối. Chú ý rằng các máy chủ độc lập không hỗ trợ EAP-TLS nên để có thể sử dụng giao thức này máy chủ truy cập từ xa cài đặt Windows Server 2003 phải là thành viên của một miền.

■ **MS-CHAP v2** Một phương pháp xác thực hai chiều cung cấp khả năng mã hóa cả dữ liệu xác thực lẫn dữ liệu của kết nối. Một khóa mật mã mới được sử dụng cho mỗi kết nối và mỗi hướng truyền dẫn. MS-CHAP v2 được kích hoạt mặc định trên Windows 2000, Windows XP và Windows Server 2003.

■ **MS-CHAP v1** Một phương pháp xác thực một chiều cung cấp khả năng mã hóa cả dữ liệu xác thực lẫn dữ liệu của kết nối. Khóa mật mã được sử dụng cho tất cả các kết nối. MS-CHAP v1 hỗ trợ các máy trạm cài đặt hệ điều hành Windows cũ như Windows 95 và Windows 98.

■ **Extensible Authentication Protocol-Message Digest 5 Challenge Handshake Authentication Protocol (EAP-MD5 CHAP)** Một phiên bản của CHAP hỗ trợ mã hóa dữ liệu xác thực thông qua thuật toán "băm" MD5 và cung cấp khả năng tương thích với các máy trạm không cài đặt Windows như MAC OS X. Nó không hỗ trợ tính năng mã hóa dữ liệu kết nối.

■ **Challenge Handshake Authentication Protocol (CHAP)** Một phương pháp xác thực thông dụng cho phép mã hóa dữ liệu xác thực dựa trên thuật toán "băm" MD5. CHAP cung cấp khả năng tương thích với

các máy trạm không cài đặt Windows. Chính sách nhóm được áp dụng cho các tài khoản sử dụng phương pháp xác thực này phải được cấu hình để lưu trữ các mật khẩu sử dụng cơ chế mã hóa ngược (các mật khẩu phải được thiết lập lại sau khi chính sách mới này được áp dụng). Nó không hỗ trợ tính năng mã hóa dữ liệu kết nối.

■ **Shiva Password Authentication Protocol (SPAP)** Một giao thức xác thực được mã hóa yếu cung cấp khả năng tương thích với các sản phẩm từ xa Shiva. SPAP không hỗ trợ tính năng mã hóa dữ liệu kết nối.

■ **Password Authentication Protocol (PAP)** Một giao thức xác thực chung không hỗ trợ mã hóa dữ liệu xác thực. Các chứng thực của người sử dụng được gửi trên mạng theo dạng tường minh (*clear-text*). PAP không hỗ trợ tính năng mã hóa dữ liệu kết nối.

■ **Unauthenticated Access** Không có bất kỳ giao thức xác thực nào cả. Đây là một lựa chọn mà khi được thiết lập trên máy chủ truy cập từ xa và chính sách truy cập được áp dụng cho kết nối sẽ cho phép các kết nối từ xa kết nối tới máy chủ mà không cần cung cấp bất kỳ một chứng thực nào. Phương pháp này có thể được sử dụng để sửa lỗi hoặc kiểm tra kết nối truy cập từ xa. Rõ ràng truy cập này không hỗ trợ việc mã hóa dữ liệu kết nối.

Bảng 7-3 cung cấp thông tin giúp bạn đối chiếu những yêu cầu với các giao thức xác thực tương ứng.

Bảng 7-3: Lựa chọn giao thức xác thực

Yêu cầu	Lựa chọn
Xác thực mã hóa hỗ trợ các máy trạm cài đặt hệ điều hành Windows 95, Windows 98, Microsoft Windows Me hoặc Windows NT4 (hỗ trợ thuần túy)	MS-CHAP v1
Xác thực mã hóa hỗ trợ các máy trạm cài đặt hệ điều hành Windows 95, Windows 98, Microsoft Windows Me hoặc Windows NT4 (với việc cập nhật Dial-Up Networking mới nhất)	MS-CHAP v2 (chỉ duy nhất kết nối VPN với Windows 95)
Xác thực mã hóa hỗ trợ PKI dựa trên chứng chỉ, ví dụ việc sử dụng các thẻ thông minh (khi máy chủ truy cập từ xa là thành viên của miền Windows 2000 Server hoặc Windows Server	EAP-TLS

2003)

Xác thực mã hóa hỗ trợ các máy trạm truy cập từ xa Windows 2000, Windows XP và Windows Server 2003	MS-CHAP v2
Xác thực hai chiều (máy trạm và máy chủ luôn luôn xác thực lẫn nhau)	EAP-TLS và MS-CHAP v2
Hỗ trợ mã hóa dữ liệu kết nối	MS-CHAP v1, MS-CHAP v2 và EAP-TLS
Xác thực mã hóa hỗ trợ các máy trạm sử dụng hệ điều hành khác	CHAP và EAP-MD5 CHAP
Xác thực mã hóa hỗ trợ các máy trạm cài đặt phần mềm Shiva LAN Rover	SPAP
Xác thực không mã hóa khi các máy trạm không hỗ trợ bất kỳ giao thức nào	PAP
Máy trạm không cung cấp bất kỳ một chứng thực nào	Unauthenticated access

TỔNG KẾT

■ Bằng việc sử dụng dịch vụ Routing And Remote Access, Windows Server 2003 có thể được cấu hình như một router và một máy chủ kết nối từ xa. Một ưu điểm đáng kể khi sử dụng Windows Server 2003 đó là cách nó tích hợp với các đặc tính của Windows như chính sách nhóm và dịch vụ thư mục Active Directory. Màn hình quản trị ***Routing And Remote Access*** là công cụ duy nhất được sử dụng để cấu hình và quản trị dịch vụ này.

■ ***Routing And Remote Access*** có thể được cấu hình một cách tự động theo một vài lựa chọn: Truy cập từ xa (quay số hoặc VPN), Chuyển đổi địa chỉ mạng (NAT), truy cập mạng riêng ảo (VPN) và NAT, bảo mật kết nối giữa hai mạng cục bộ. Nếu như các lựa chọn chuẩn được nêu ở trên không phù hợp với yêu cầu của bạn, bạn có thể cấu hình Routing And Remote Access bằng tay.

■ Nếu không sử dụng các giao thức định tuyến như OSPF và RIP, người quản trị mạng phải thêm các đường định tuyến tĩnh để kết nối với các mạng con không kết nối trực tiếp với router khi mà các mạng con này không cùng hướng với các đường định tuyến mặc định.

■ Các ***router*** đọc thông tin địa chỉ đích trong các gói tin nhận được và định tuyến chúng tùy theo hướng được cung cấp trong bảng định tuyến. Trong Windows Server 2003, bạn có thể hiển thị bảng định tuyến IP thông qua màn hình quản trị ***Routing And Remote Access*** hoặc qua câu lệnh ***Route Print*** ở chế độ dòng lệnh.

■ Windows Server 2003 cung cấp khả năng hỗ trợ mở rộng cho định tuyến quay số theo yêu cầu. Đó là định tuyến các gói tin trên các đường truyền điểm nối điểm vật lý như các đường điện thoại analog và ISDN, các đường truyền điểm nối điểm ảo như PPTP và L2TP. Định tuyến quay số theo yêu cầu cho phép bạn kết nối với Internet, với các chi nhánh hoặc thực thi kết nối VPN giữa hai router.

■ Kết nối truy cập từ xa phải được ủy quyền sau khi nó được *xác thực*. ủy quyền truy cập từ xa bắt đầu với các đặc tính quay số của tài khoản người sử dụng; trước hết đáp ứng chính sách truy cập rồi mới được áp dụng cho kết nối.

■ Microsoft triển khai một máy chủ RADIUS là IAS. Sử dụng máy chủ RADIUS cho phép bạn tập trung hóa việc *xác thực*, ủy quyền và đăng nhập cho các kết nối từ xa. Khi bạn triển khai RADIUS, nhiều máy tính cài đặt dịch vụ ***Routing And Remote Access*** sẽ hướng các yêu cầu truy cập đến máy chủ này. Kế đó, máy chủ RADIUS sẽ truy vấn máy chủ điều khiển vùng cho tiến trình xác thực và áp dụng các chính sách cho các yêu cầu kết nối.

BÀI TẬP THỰ C HÀNH

CHÚ Ý QUAN TRỌNG *Hoàn thành tất cả các bài tập thực hành*
Nếu bạn lập kế hoạch thực hiện các bài thực hành của quyển sách này thì bạn phải làm tất cả các bài thực hành trong chương này rồi đưa máy tính quay trở về trạng thái ban đầu để kết hợp với các bài thực hnành trong cuốn BÀI TẬP THỰC HÀNH

Bài tập thực hành 7-1: Hiển thị bảng định tuyến IP

Trong bài thực hành này, bạn sẽ hiển thị bảng định tuyến IP tại chế độ dòng lệnh.

1. Mở cửa sổ chế độ dòng lệnh.
2. Tại chế độ dòng lệnh, gõ **route print** rồi nhấp phím **ENTER**.

   CÂU HỎI *Mặt nạ mạng của mạng đích 10.1.0.0 là gì?*

CÂU HỎI ÔN TẬP

1. Bạn là nhà quản trị mạng của công ty ABC. Mạng của công ty này có một vài mạng con. Hiện tại, người sử dụng mạng chỉ yêu cầu truy cập đến mạng Intranet của công ty và các tài nguyên cục bộ khác như các tài nguyên chia sẻ file và các máy in. Gần đây, công ty có thuê một đội phát triển. Họ sẽ gia nhập vào mạng của bạn và yêu cầu bạn phải hỗ trợ. Những lựa chọn nào dưới đây yêu cầu bạn triển khai một giải pháp định tuyến cho đội phát triển này? Chọn tất cả các lựa chọn đáp ứng.
   a. Đội phát triển cần kết nối tới mạng của công ty nhưng các ứng dụng kiểm tra của họ phải được tách riêng ra khỏi mạng.
   b. Đội phát triển sử dụng mạng Internet để truy cập tới mạng công ty.
   c. Đội phát triển không yêu cầu truy cập Internet và các ứng dụng kiểm tra của họ không cần kết nối tới mạng công ty.

d. Mã nguồn phải được mã hóa khi lưu trữ và truy cập qua mạng.

2. Bạn là nhà quản trị mạng của công ty ABC. Mạng của công ty này có một vài mạng con. Hiện tại, người sử dụng mạng chỉ yêu cầu truy cập đến mạng Intranet của công ty và các tài nguyên cục bộ khác như các tài nguyên chia sẻ file và các máy in. Gần đây, công ty có thuê một đội phát triển. Họ sẽ gia nhập vào mạng của bạn và yêu cầu bạn phải hỗ trợ. Những lựa chọn nào dưới đây yêu cầu bạn xác định một giải pháp lọc gói cho đội phát triển này? Chọn tất cả các lựa chọn đáp ứng.

   a. Đội phát triển cần kết nối đầy đủ tới mạng của công ty nhưng các ứng dụng kiểm tra của họ phải được tách riêng chỉ với các máy tính kiểm tra.

   b. Đội phát triển cần kết nối tới mạng công ty nhưng các ứng dụng kiểm tra của họ phải được cách ly hoàn toàn với người sử dụng trên mạng.

   c. Đội phát triển không yêu cầu truy cập Internet và các ứng dụng kiểm tra của họ cũng không cần kết nối tới mạng công ty.

   d. Đội phát triển sử dụng một giao thức duy nhất được xác định trước để kiểm tra các ứng dụng.

3. Qua một vài tuần bạn nhận được những lời phần nàn từ phía người sử dụng rằng họ không thể kết nối một cách liên tục tới máy chủ VPN. Bạn kiểm tra lại các file nhật ký và nhận ra rằng những phàn nàn đó xảy ra khi mức độ sử dụng mạng là cao. Bạn loại trừ tình huống địa chỉ là nguyên nhân của vấn đề. Vậy đâu là lý do của những vấn đề truy cập không liên tục?

4. Bạn cấu hình máy chủ truy cập từ xa nhằm phân phối địa chỉ cho các máy trạm thông qua một máy chủ DHCP. Tuy nhiên, bạn nhận ra rằng các máy trạm được gán địa chỉ APIPA của chính nó. Hãy đưa ra hai nguyên nhân có thể gây ra lỗi này.

5. Công ty ABC gần đây có triển khai các thẻ thông minh cho các nhân viên có nhu cầu truy cập từ xa tới mạng của công ty. Bạn sẽ sử dụng giao thức xác thực nào để hỗ trợ việc sử dụng các thẻ thông minh này?

6. Người quản trị công ty ABC muốn đảm bảo dữ liệu phải được mã hóa trong suốt quá trình truy cập từ xa xảy ra. Các giao thức xác thực nào cung cấp quá trình mã hóa dữ liệu?

7. Gần đây bạn tạo một miền mới trên mạng Windows Server 2003 và môi trường hoạt động của miền là hỗn hợp Windows 2000. Thiết lập

Allow Access trong các đặc tính quay số của một tài khoản người sử dụng trong môi trường này khác với các môi trường máy chủ khác như thế nào?

8. Bạn đang sửa lỗi một kết nối truy cập từ xa bị lỗi. Bạn xác nhận rằng các đặc tính quay số của tài khoản người sử dụng được thiết lập là ***Allow Access*** và chính sách truy cập đáp ứng đầu tiên được đặt là ***Grant Remote Access Permission***. Nhưng máy trạm vẫn không kết nối được. Bạn sẽ kiểm tra gì kế tiếp?

CÁC KỊCH BẢN TÌNH HUỐNG

==========

Kịch bản 7-1: Xác thực số điện thoại

Công ty ABC có 10 nhà sản xuất phải truy cập vào hệ thống mạng của công ty. Nhằm đảm bảo tính bảo mật, ABC muốn ABC muốn 10 nhà sản xuất này chỉ được xác thực duy nhất thông qua số điện thoại mà họ sử dụng để kết nối tới mạng công ty. Do đó họ phải được xác thực bởi các số điện thoại và ABC cũng không muốn yêu cầu họ nhập tên cũng như mật khẩu cho quá trình xác thực. Bạn có thể triển khai cấu hình này như thế nào?

==========

Kịch bản 7-2: Bản ghi chứng thực duy nhất

Bạn là nhà tư vấn mạng cho công ty ABC. Công ty này đã cấu hình một VPN kiểu PPTP. Mặc dù người sử dụng không có lỗi gì trong vấn đề kết nối nhưng họ vẫn phải nhập tên và mật khẩu hai lần. Bạn nhận được yêu cầu cấu hình hệ thống sao cho người sử dụng chỉ cần nhập mật khẩu của họ một lần duy nhất để kết nối tới miền của công ty. Bạn có thể cho phép người sử dụng tránh việc nhập các chứng thực của họ trong cả màn hình ***Log On To Windows*** và hộp thoại kết nối VPN như thế nào? Các giao thức xác thực nào có thể được sử dụng qua kết nối VPN?

CHƯƠNG 8: DUY TRÌ KIẾN TRÚC HẠ TẦNG MẠNG

Hoàn thành chương này bạn có khả năng:

- Sử dụng thẻ ***Networking*** trong Trình Quản trị Tác vụ (***Task Manager***) để hiển thị các hoạt động liên quan đến mạng.
- Giám sát lưu thông mạng.
- Tìm kiếm và thiết lập các cảnh báo sử dụng bảng điều khiển Hiệu năng (***Performance Console*****).**
- Thu thập dữ liệu xác định bằng cách sử dụng phiên bản giám sát mạng ***Network Monitor*** đi kèm trong hệ điều hành Windows Server 2003.
- Sửa lỗi kết nối với Internet.
- Sửa lỗi các dịch vụ trên máy chủ bằng cách sử dụng công cụ ***Service*** và ***Event Viewer***.
- Sử dụng các lựa chọn phục hồi dịch vụ để chẩn đoán và giải quyết các vấn đề liên quan tới dịch vụ.
- Chẩn đoán và giải quyết các vấn đề liên quan tới các dịch vụ phụ thuộc (***Service Dependency***).

Có hai phương pháp để duy trì mạng của bạn: phương pháp chủ động và phương pháp thụ động. Sau khi quá trình triển khai thiết kế mạng của bạn được hoàn thành và bạn xác nhận rằng mạng làm việc tốt thì mô hình thụ động có nghĩa là bạn sẽ "đợi và xem" có những lỗi gì xảy ra không. Còn mô hình chủ động thì lại ngược lại không đợi cho tới khi có lỗi xảy ra. Mô hình này có khả năng phòng ngừa và sử dụng các công cụ hỗ trợ như ***Task Manager***, màn hình quản trị ***Performance***, ***Network Monitor***, tính năng sửa lỗi kết nối mạng (***Repair***) và ***Netdiag***. Các công cụ này sẽ hỗ trợ các nhà quản trị một hệ thống theo phương pháp chủ động trong việc phát hiện các nguy cơ tiềm ẩn cũng như các vấn đề liên quan đến mạng đang hoạt động mà không cần mất thời gian suy đoán xem lỗi đó là gì do không có dữ liệu về tình trạng hoạt động trước đó của hệ thống. Chúng thực hiện công việc này bằng cách giám sát, ghi nhật ký qua file nhật ký và phân tích dữ liệu mạng một cách hệ thống.

Trong chương này sẽ đề cập về ba công cụ giúp bạn chẩn đoán và sửa lỗi các rắc rối về mạng một cách chủ động. Trước hết, bạn sẽ làm quen với các công cụ mạng đơn giản và thông dụng trong ***Task Manager***. Công cụ thứ hai bạn kiểm tra đó là màn hình quản trị ***Performance*** (thường được gọi là ***Performance Monitor***) cung cấp cho bạn một cách nhìn sâu sắc hơn về việc đo đạc hiệu năng của hệ thống. Cuối cùng, bạn sẽ khám phá một số tính năng thu thập dữ liệu tiên tiến trong ***Network Monitor***.

SỬ DỤNG THẺ NETWORKING TRONG CÔNG CỤ TASK MANAGER

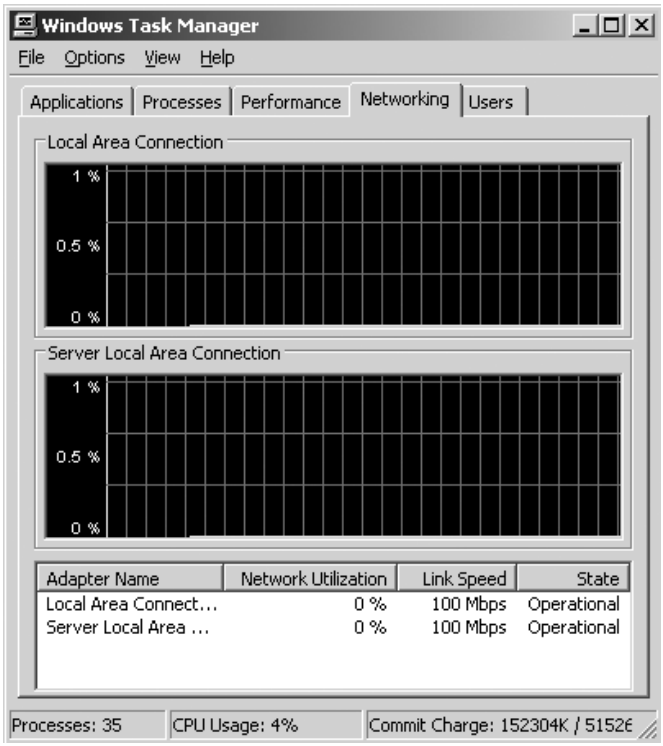
Công cụ quản trị tác vụ hệ thống ***Task Manager*** cung cấp một bức tranh hiện thời về những thông tin chính trên máy tính cục bộ. Nó kết hợp tất cả thông tin mạng, thông tin về ứng dụng, các tiến trình đang chạy, các biến đếm quan trọng về hiệu năng của hệ thống và những người sử dụng đã kết nối vào trong một màn hình hiển thị. Khi được kích hoạt, ***Task Manager*** cũng thiết lập một biểu đồ nhỏ trong khu vực thông báo về mức độ sử dụng của bộ vi xử lý theo thời gian thực.

Task Manager là công cụ thông dụng nhất để có thể phản hồi ngay lập tức về các tình trạng của máy tính cục bộ. Ví dụ, hiệu năng của một máy tính giảm đáng kể và bạn muôn biết ứng dụng nào đang chiếm dụng tài nguyên của CPU nhiều nhất. Để thực hiện điều này, bạn có thể kích hoạt ***Task Manager***, nhấp vào ***Processes*** rồi sắp xếp thứ tự theo cột CPU. Khi đó màn hình sẽ hiển thị theo thứ tự giảm dần các tiến trình chiếm dụng bộ vi xử lý thông qua phần trăm thời gian. Tức là, ứng dụng chiếm dụng thời gian xử lý nhiều nhất được hiển thị đầu tiên. ***Task Manager*** cũng hiển thị lượng bộ nhớ trong mà mỗi tiến trình sử dụng. Để kích hoạt ***Task Manager*** (***Taskmanager.exe***) sử dụng tổ hợp phím **CTL+ALT+DEL** rồi nhấn vào ***Task Manager***.

Task Manager cũng có khả năng thông báo nhanh dải thông mà mỗi kết nối mạng sử dụng trên máy tính cục bộ. Hình 8-1 hiển thị thẻ ***Networking*** và phần trăm mức độ sử dụng dải thông tổng cộng. Thẻ ***Networking*** cũng cung cấp một cách tổng quan mức độ sử dụng của mỗi kết nối mạng. Bạn cũng có thể xác định dữ liệu khác như đường truyền có hoạt động hay không không được kết nối hay không bằng cách nhìn vào cột ***State***. Cuối cùng trong cột ***Link Speed*** bạn cũng có thể nhìn thấy tốc độ đường truyền là bao nhiêu.

Tỷ lệ bên trái được tính theo phần trăm và nó tự động thay đổi tỷ lệ phụ thuộc vào mức độ sử dụng đường truyền là bao nhiêu. Bạn cần chú ý kỹ tỷ lệ trong hình 8-1, nó thay đổi từ 0% đến 1%. Sử dụng tỷ lệ này, nếu đường

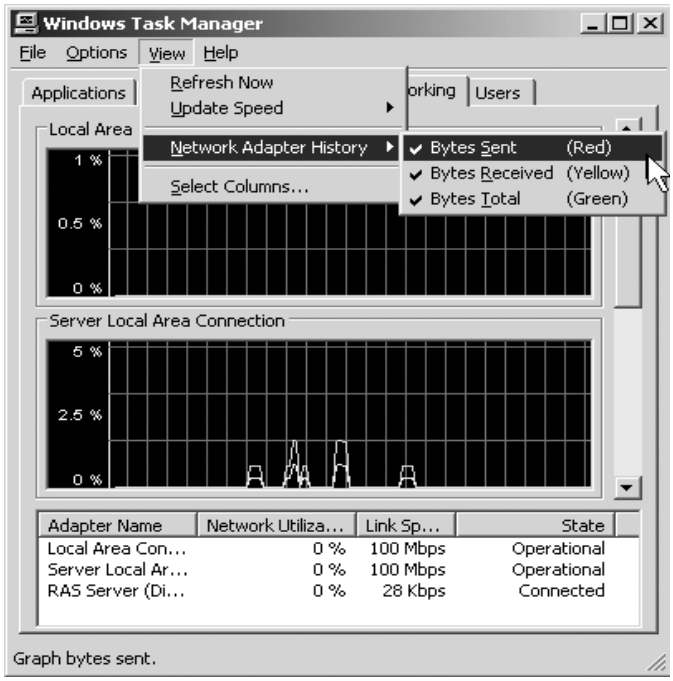
xung nhọn về mức độ sử dụng mạng lên tới đỉnh của biểu đồ thì chỉ có duy nhất 1% của dải thông tổng cộng được sử dụng.



Hình 8-1: Thẻ Networking trong Task Manager

Lọc lưu lượng mạng

Nếu bạn nhận được các thông báo rằng máy chủ không phản hồi đủ nhanh đối với các công việc đọc và ghi, bạn muốn hiển thị lưu thông mạng một cách độc lập. Thực vậy, bạn có thể lựa chọn để hiển thị và tô sáng lưu thông tổng (mặc định) hoặc bạn có thể lựa chọn để hiển thị và tô sáng các byte gửi hoặc nhân như hình 8-2.



Hình 8-2: Lọc theo hướng của luồng dữ liệu mạng

Việc *Lọc* cho phép bạn lựa chọn các hướng lưu thông mạng bạn muốn giám sát. Ví dụ, nếu bạn đang chẩn đoán và sửa lỗi một máy chủ không phản hồi nhanh các công việc ghi, bạn có thể bỏ qua một cách tạm thời các byte được gửi đi. Ngược lại, nếu bạn đang chẩn đoán và sửa lỗi một máy chủ không phản hồi nhanh các công việc đọc, bạn có thể bỏ qua một cách tạm thời các byte nhận được.

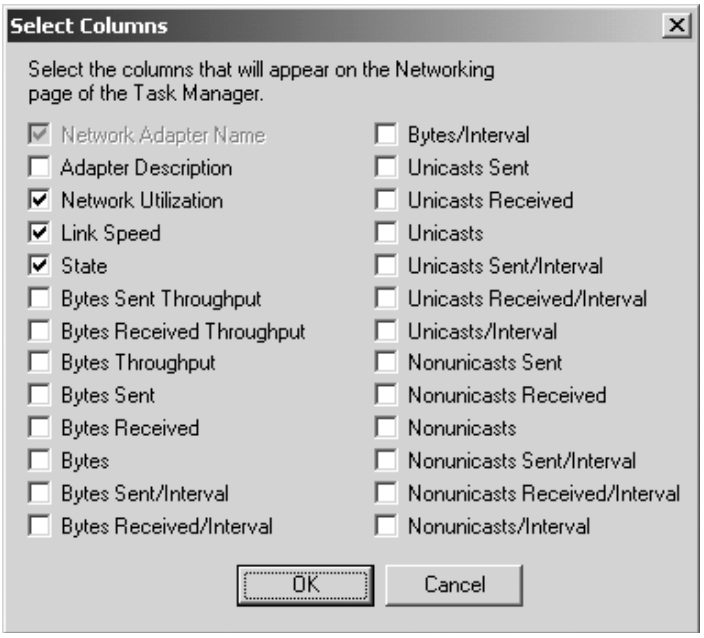
Lựa chọn các cột

Như những gì bạn đã thấy trong hình 8-1, bạn có thể nhận được một hình ảnh tổng quan của một số dữ liệu trạng thái quan trọng như tốc độ đường truyền chẳng hạn. Tuy nhiên, thẻ ***Networking*** cũng là một công cụ thông dụng để xác định loại lưu thông nào đang đi qua một giao diện. Bạn cũng có thể gia tăng đáng kể hình ảnh những gì đang diễn ra thông qua các phương tiện của một biến đếm mạng. Đó là một mẩu thông tin đôi khi được gọi là điểm dữ liệu mà bạn có thể truy cập để xem các trạng thái hiện thời. Nếu bạn xác định giá trị của một điểm dữ liệu trong một khoảng thời gian, có nghĩa là bạn đang lấy mẫu dữ liệu.

Bạn có thể lựa chọn để thêm các biến đếm khác vào biểu đồ bằng cách nhấp vào thực đơn ***View*** rồi chọn ***Select Columns*** và lựa chọn thông tin thêm mà bạn muốn hiển thị từ hộp thoại ***Select Columns*** (xem hình 8-3).

Mặc dù có công cụ này cung cấp nhiều biến đếm khác nhau nhưng chỉ có một số ít trong chúng là cần thiết cho công việc chẩn đoán và sửa lỗi. Bảng

8-1 biểu diễn một số biến đếm thông dụng nhất được dùng cho công việc chẩn đoán và sửa lỗi hiệu năng mạng.



Hình 8-3: Các cột mà công cụ Task Manager cung cấp cho thẻ Networking

Bảng 8-1: Chẩn đoán và sửa lỗi bằng các bộ đếm hiệu năng

Đặc tính	Mô tả
Network Adapter Name	Tên của Giao tiếp mạng. Hộp kiểm tra này luôn luôn được lựa chọn. Nếu bạn có nhiều Giao tiếp mạng, bạn sẽ nhìn thấy nhiều danh sách.
Link Speed	Tốc độ của giao diện mạng. Nếu bạn suy đoán có nghẽn cổ chai, kiểm tra rằng số này chính là tốc độ lớn nhất của mạng. Thỉnh thoảng, Giao tiếp mạng nhận được một tín hiệu từ router để giảm xuống một tốc độ thấp hơn (thông thường 100 Mbps xuống còn 10 Mbps)
Bytes/Interval	Tốc độ tại đó các byte được gửi và nhận trên Giao tiếp mạng trong suốt quãng thời gian trao đổi (mặc định 2s một lần). Như nhiều biến đếm khác, mức hiệu năng cơ sở (***Baseline -*** *mức hiệu năng được thu thập khi hệ thống làm việc tại chế độ bình ổn, sử dụng để tham chiếu*) là rất hữu ích trong quá trình phân tích biến đếm này.
Unicasts/Interval	Số lượng các gói dữ liệu ***unicast*** nhận được trong suốt quãng thời gian trao đổi (mặc định 2s một lần). Dữ liệu

	được xác định bởi biến đếm này là lưu thông trực tiếp chứ không phải lưu thông quảng bá.
Nonunicasts/Interval	Số lượng các gói dữ liệu quảng bá và ***multicast*** nhận được trong suốt quãng thời gian trao đổi (mặc định 2s một lần). Nếu biến đếm này có dữ liệu, giao diện của bạn phải đối đầu với lưu thông quảng bá hay các lưu thông nền. Giá trị của biến đếm này càng cao có thể là biểu hiện của các lỗi trên mạng của bạn không liên quan đến máy chủ nhận lưu thông

SỬ DỤNG MÀN HÌNH QUẢN TRỊ PERFORMANCE

Task Manager là một công cụ hiệu quả nhằm mang lại một hình ảnh nhanh về hiệu năng sử dụng mạng của một máy tính cục bộ. Tuy nhiên màn hình quản trị ***Performance*** lại cung cấp cho bạn thông tin cần thiết phục vụ cho việc phân tích chiều sâu, khả năng ghi lại nhật ký và các cảnh báo. Những tính năng này rất phù hợp cho các cảnh báo về những vấn đề hệ thống trước khi nó có thể xảy ra. Sử dụng màn hình quản trị ***Performance*** thay cho ***Task Manager*** khi bạn cần:

- Sử dụng nhiều biến đếm hiệu năng.
- Khả năng gửi các cảnh báo ngay lập tức dựa vào tính huống cụ thể.

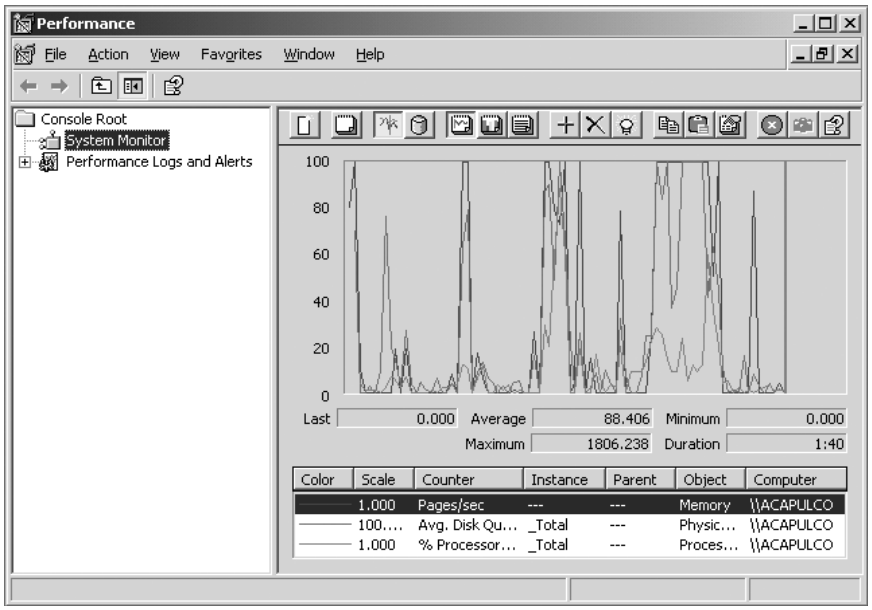
➢ **Khởi tạo màn hình quản trị *Performance***

Bạn có thể khởi tạo màn hình quản trị ***Performance*** theo nhiều cách khác nhau. Một trong những phương pháp đơn giản nhất đó là mở thực đơn ***Start***, chọn ***Run*** gõ **perfmon.exe** rồi nhấp ***OK***. ***Performance Monitor*** tự động khởi tạo với 03 biến đếm được sử dụng nhiều nhất như hình 8-4.

1. **Pages/Sec** Hiển thị sau bao lâu thì các trang bộ nhớ được tráo đổi theo chiều vào và chiều ra của RAM tới đĩa. Các giá trị được duy trì ở mức cao muốn thông báo rằng lượng RAM trên máy tính là không đủ.
2. **Avg. Disk Queue Length** Giám sát biến đếm này để xem có bao nhiêu yêu cầu hệ thống phải đợi để truy cập đĩa. Số lượng các yêu cầu vào/ra đợi có thể được duy trì tại một mức không

nhiều hơn 1,5 đến 2 lần số lượng các trục quay tạo ra đĩa cứng vật lý.

3. **% Processor Time** Hiển thị bao nhiêu phần trăm CPU đang được sử dụng. Các giá trị duy trì liên tục ở mức cao thông báo rằng bộ vi xử lý không đủ nhanh hoặc có thể không đủ RAM.

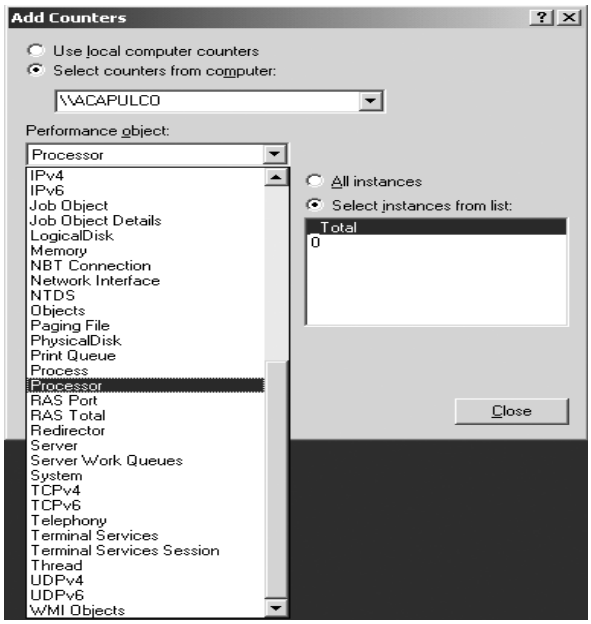


Hình 8-4: Màn hình quản trị Performance với các bộ đếm mặc định được tải

Thêm các biến đếm mạng

Màn hình quản trị ***Performance*** có khả năng lấy mẫu một dải lớn các biến đếm hiệu năng, nhiều hơn rất nhiều so với ***Task Manager***. Các thành phần mạng và không liên quan đến mạng này được phân thành một vài nhóm, như hình 8-5.

> **CHÚ Ý** ***Các nhóm sẵn có*** *Các nhóm mà* ***Performance*** *có thể cung cấp cho bạn có thể thay đổi dựa trên phần mềm máy chủ được cài đặt.*



Hình 8-5: Các nhóm biến đếm được dành cho giám sát hiệu năng

Nhiệm vụ chính của chúng ta là giám sát các vấn đề về mạng. Danh sách dưới đây miêu tả các đối tượng chính liên quan đến hiệu năng mạng:

- **Network Interface (giao diện mạng)** Đối tượng này chứa một số các biến đếm giống như biến đếm ***Task Manager***. Tuy nhiên nó cũng chứa các biến đếm dùng để giám sát các chi tiết cụ thể về các gói trên mạng.

- **TCPv4** Đối tượng này chứa các biến đếm liên quan đến các kết nối dựa trên giao thức truyền dẫn TCP phiên bản 4.

- **TCPv6** Đối tượng này chứa các biến đếm liên quan đến các kết nối dựa trên giao thức truyền dẫn TCP phiên bản 6.

- **NBT Connection** Đối tượng này chứa các biến đếm nhằm đo các tốc độ các byte được gửi và nhận qua giao thức NetBIOS trên nền TCP/IP (NetBT hoặc NBT). Đây là giao thức hỗ trợ NetBIOS cho bộ giao thức TCP/IP.

- **RAS Port** Nhóm này phù hợp nếu bạn có mạng riêng ảo VPN hoặc các kết nối truy cập từ xa. Với những kết nối này, bạn có thể lựa chọn để chẩn đoán và sửa lỗi những vấn đề về kết nối dựa trên các cổng xác định. Bạn có thể kiểm tra các lỗi trên một cổng hoặc trên các biến đếm khác như ***Percent Compression Out*** chẳng hạn.

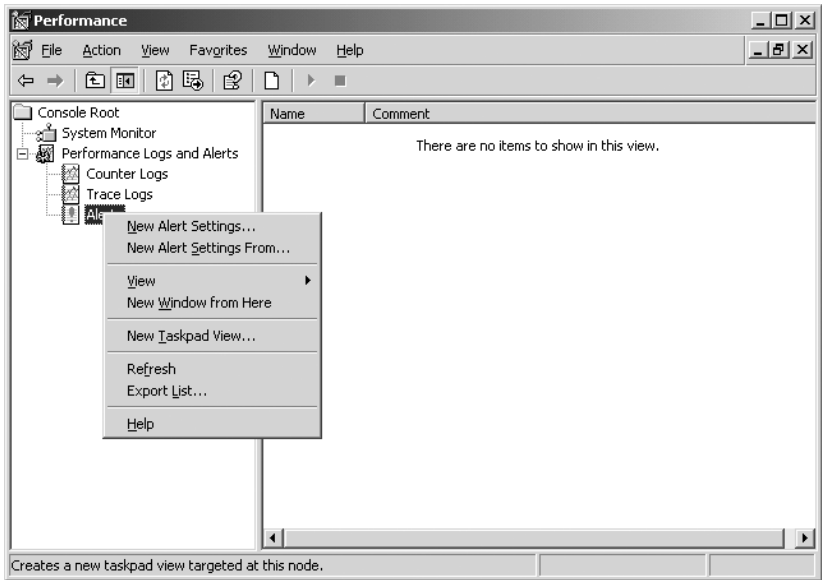
- **RAS Total** Đối tượng này chứa các biến đếm hiển thị hiệu năng RAS được kết hợp tổng thể. Nó khác với đối tượng ***RAS Port*** chỉ hiển thị hiệu năng trên một cổng cụ thể.

Sử dụng màn hình quản trị Performance để tạo các cảnh báo

Như bạn đã thấy, sử dụng các biến đếm để giám sát hiệu năng hệ thống của bạn theo thời gian thực là đặc tính mạnh nhất của màn hình quản trị ***Performance***. Một tính năng khác của nó rất thông dụng đối với người quản trị hệ thống đó là tạo các cảnh báo.

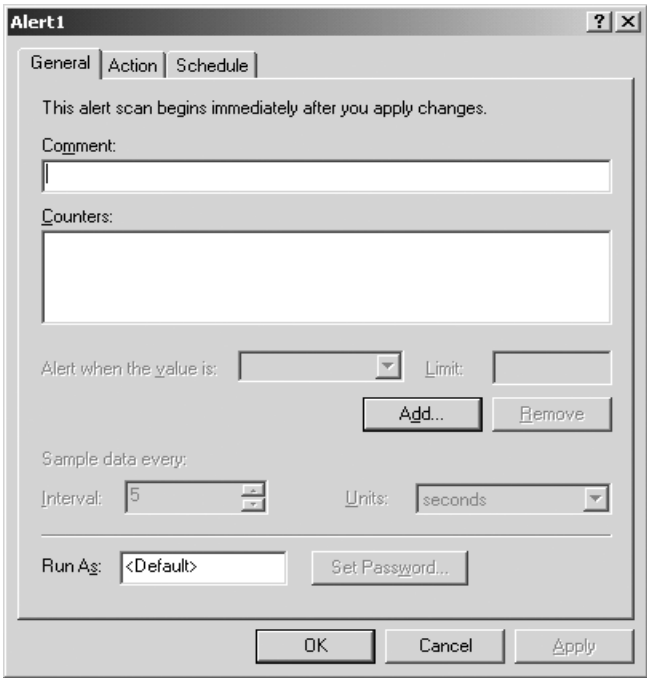
Các cảnh báo được thiết lập để thông báo cho bạn khi hệ thống vượt quá một ngưỡng xác định. Ví dụ, bạn có thể thiết lập một cảnh báo để thông báo khi nào thì hệ thống của bạn không gian đĩa trống thấp hơn 20% so với không gian đĩa tổng cộng.

Bạn có thể tạo các cảnh báo trong phần ***Performance Logs And Alerts*** trong màn hình quản trị ***Performance***. Nhấp chuột phải vào ***Alerts*** rồi chọn ***New Alert Settings*** như hình 8-6.



Hình 8-6: Thiết lập các cảnh báo mới

Tên của các cảnh bảo được dựa trên loại biến đếm mà bạn muốn giám sát và kế đó lựa chọn các biến đếm. Khi bạn nhấp vào nút ***Add*** (xem hình 8-7) bạn có thể lựa chọn các đối tượng hiệu năng khác nhau (***PhysicalDisk*** chẳng hạn), kế đó chọn một biến đếm cụ thể (như ***%DiskTime*** chẳng hạn). Đôi khi bạn có thể muốn lựa chọn nhiều hơn một biến đếm để gửi ngay một cảnh báo khi có lỗi. Ví dụ, bạn có thể lựa chọn để nhận một thông báo nếu cả dải thông mạng dải thông mạng lẫn số lượng các lỗi được tạo ra là cao.



Hình 8-7: Thêm một cảnh báo

Trước khi bạn lựa chọn xem bạn muốn cảnh báo được thông báo như thế nào, bạn phải đặt một vài lựa chọn trong thẻ ***General*** để xác định xem bạn muốn lấy mẫu các biến đếm như thế nào.

Danh sách dưới đây miêu tả một số tham số mà bạn có thể cấu hình trong thẻ ***General***:

■ **Comment** Mặc dù các cảnh báo đều có một tên nhưng bạn vẫn có thể cho nó một lời chú giải, nhờ đó bạn hoặc người khác có thể biết được mục đích của cảnh báo này là gì và cảnh báo được gửi cho ai.

■ **Alert When The Value Is** Cho phép bạn xác định xem bạn muốn khởi tạo một cảnh báo khi giá trị của nó nhỏ hơn hay lớn hơn giá trị tới hạn.

■ **Interval** Bạn có thể thiết lập sau bao lâu thì màn hình quản trị *Performance* sẽ truy vấn hệ thống một lần đối với những gì bạn muốn giám sát. Hệ thống không giám sát liên tục các biến đếm mà bạn muốn quản trị. Thay vào đó, dữ liệu mẫu được thu thập tại những khoảng thời gian lặp trong suốt một khoảng thời gian cụ thể. Ví dụ, bạn có thể thiết lập một khoảng thời gian lặp 5 giây và thu thập dữ liệu trong vòng 10 phút. Điều đó có nghĩa rằng một bản chụp của các biến đếm mà bạn đã lựa chọn sẽ được thực hiện mỗi lần 5 giây trong khoảng thời gian 10 phút. Khoảng thời gian lặp càng dài thì độ chính xác của mẫu càng ít bởi vì nó được lấy mẫu ít hơn.

Khoảng thời gian lặp càng lớn thì mẫu càng chính xác nhưng bộ vi xử lý phải làm việc nhiều hơn để lấy mẫu.

■ **Units** Bạn có thể xác định các đơn vị thời gian để thu thập các mẫu. Chẳng hạn như có thể bạn không muốn lấy mẫu 5 giây mỗi lần mà thay vào đó bạn muốn lẫy mẫu 1 phút mỗi lần. Có nghĩa là, nếu bạn giảm tần suất lấy mẫu hoặc giảm tốc độ lấy mẫu bạn sẽ sử dụng các chu kì bộ vi xử lý ít hơn nhưng các mẫu của bạn sẽ cung cấp thông tin ít hơn do có ít mẫu hơn.

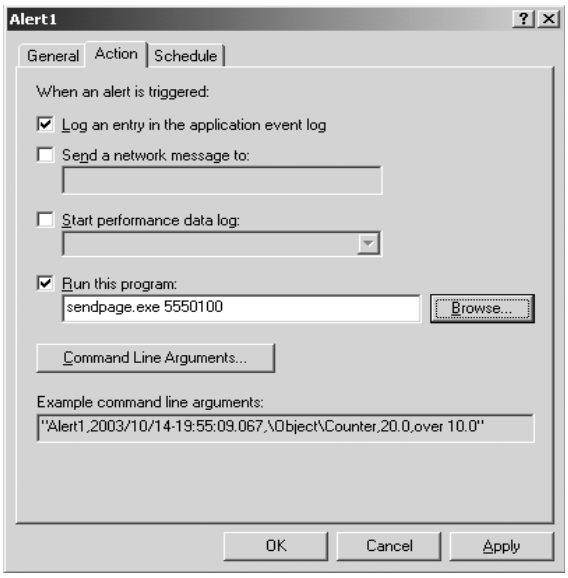
■ **Run As** Bạn có thể lấy mẫu các biến đếm bằng cách lựa chọn hoặc tài khoản *System* hoặc tài khoản khác do bạn lựa chọn. Tuy nhiên, để giám sát các biến đếm liên quan đến mạng thì tài khoản *System* truy cập được tới những gì nó cần để thực hiện công việc.

> **CHÚ Ý *Sử dụng chú giải và Run As cho tất cả các bộ đếm*** *Nếu bạn muốn giám sát từ hai bộ đếm trở lên, bạn phải lựa chọn bộ đếm và thiết lập các trường* ***Alert When The Value Is, Limit, Interval*** *và* ***Units*** *cho mỗi bộ đếm riêng biệt. Trường* ***Comment*** *và* ***Run As*** *được sử dụng cho tất cả các bộ đếm trong một cảnh báo.*

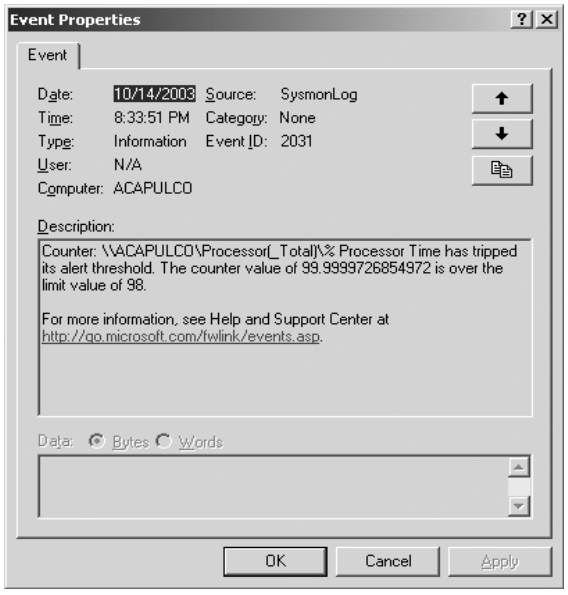
Sau khi bạn thiết lập các tham số này, lựa chọn thẻ ***Action*** như hình 8-8.

Thẻ ***Action*** xác định những gì diễn ra sau khi một cảnh báo được tạo ra. Có nhiều lựa chọn cho phép bạn biết rằng tiêu chuẩn của biến đếm có đáp ứng không. Những lựa chọn này gồm có:

■ **Log An Entry In The Application Event Log** Chọn lựa chọn này sẽ đưa một sự kiện vào trong nhật ký sự kiện hệ thống mà bạn có thể sử dụng công cụ ***Event Viewer*** để xem. Một thông báo của biến đếm, giá trị và giới hạn là một phần của bản ghi nhật ký như hình 8-9.



Hình 8-8: Xác định xem bạn muốn điều khiển thông báo như thế nào bằng thẻ Action



Hình 8-9: Ví dụ về một sự kiện

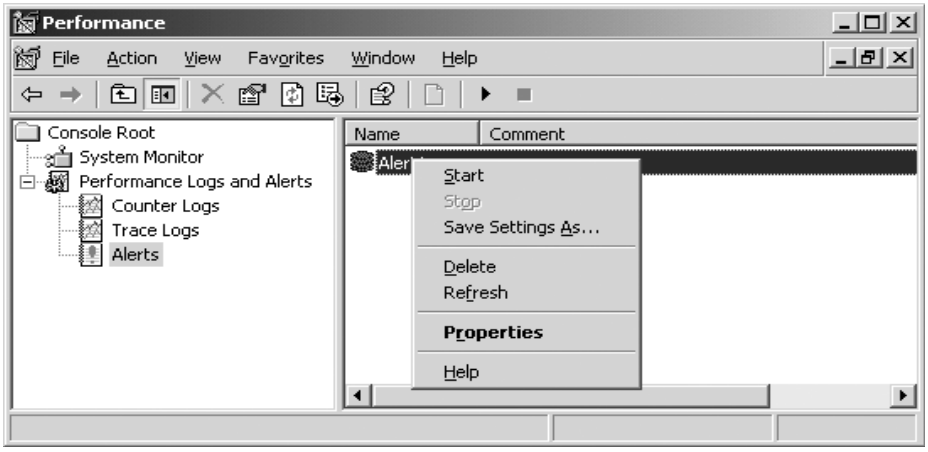
- **Send A Network Message To** Chọn lựa chọn này sẽ gửi các bản thông báo tới một máy tính khác được khai báo trong trường tương ứng. Quá trình này tương tự như sử dụng câu lệnh ***Net Send*** được dùng để gửi các bản tin tới những người sử dụng khác hoặc máy tính khác trên mạng. Với các bản tin được gửi, dịch vụ ***Alerter*** phải được khởi tạo trên máy tính mà bạn đang giám sát. Với các bản tin nhận được, dịch vụ ***Messenger*** phải được khởi tạo trên máy tính nhận tin.

CHÚ Ý *Kích hoạt các dịch vụ một cách thủ công* *Dịch vụ **Alerter** và **Messenger** không chạy trên máy tính mới được cài đặt hệ điều hành Windows Server 2003. Bạn phải thay đổi thủ công trạng thái từ **Disable** thành **Automatic** và đảm bảo rằng các dịch vụ này đang chạy.*

- **Start Performance Data Log** Bạn có thể cấu hình hệ thống cảnh báo khởi tạo bằng cách đưa thêm các biến đếm vào một file nhật ký. Các biến đếm này có thể được xem lại sau đó. Bạn phải thiết lập trước file nhật ký bằng cách sử dụng phần ***Counter Logs*** trong ***Performance Logs And Alerts.*** Lựa chọn này phù hợp khi bạn muốn khởi tạo một file nhật ký chỉ khi nào hệ thống đang được giám sát có những đặc tính cụ thể như giám sát ***paging file*** khi không gian đĩa cứng còn trống thấp hơn 15%.

  Sử dụng thiết lập này để thực hiện một chương trình sau khi một hoặc nhiều biến đếm mà bạn thiết lập vượt quá ngưỡng của nó. Sử dụng lựa chọn này để xác định một ứng dụng phân trang, một file ***.bat*** hoặc nếu cần thiết có thể tắt hệ thống bằng việc sử dụng lệnh ***Shutdown***.

Sử dụng thẻ ***Schedule*** để tự động khởi tạo và dừng cảnh báo. Ví dụ, bạn muốn thiết lập cảnh báo về hoạt động trong suốt thời gian mà mức độ sử dụng mạng là cao điểm như thời điểm mà một loạt người sử dụng đăng nhập vào mạng. Bạn cũng có thể đặt cảnh báo về hoạt động trong suốt thời gian ngoài giờ cao điểm như những giờ sáng sớm. Nếu bạn không xác định một lịch trình hoặc nếu bạn xác định một phương pháp khởi tạo bằng tay cảnh báo thì bạn có thể khởi tạo nó bằng cách nhấp chuột phải vào nó rồi chọn ***Start*** như hình 8-10.

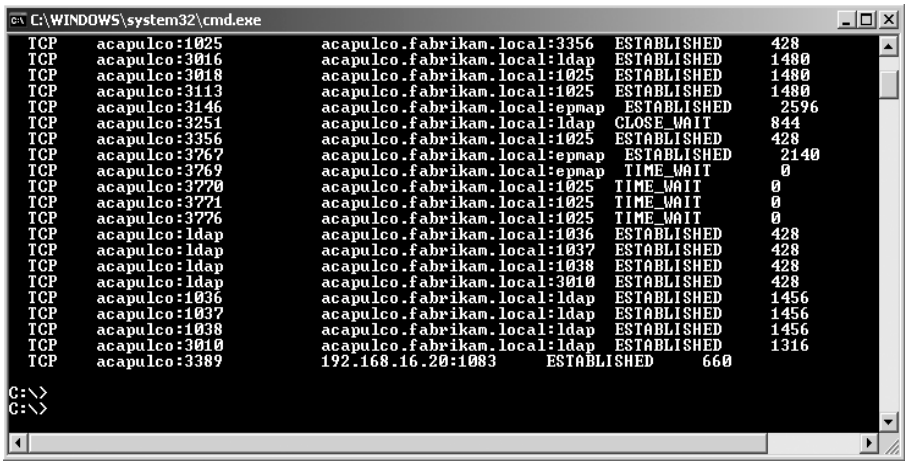


Hình 8-10: Khởi tạo các cảnh báo bằng tay

GIÁM SÁT LƯU LƯỢNG MẠNG BẰNG CÔNG CỤ NETSTAT

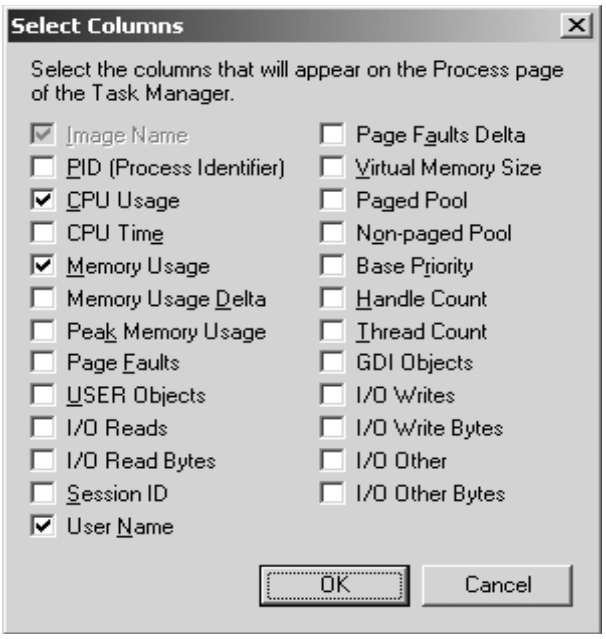
Một công cụ khác ở chế độ dòng lệnh sẽ giúp bạn giám sát lưu thông đó là ***Netstat.*** ***Netstat*** cung cấp thông tin về các kết nối mạng hiện thời của một máy tính cài đặt TCP/IP và các thông kê về hoạt động mạng. Ví dụ, nếu bạn muốn xác định xem cổng nào trên một hệ thống đang lắng nghe các kết nối bạn có thể chạy câu lệnh ***Netstat –a***. Chạy câu lệnh này, kết quả sẽ hiển thị các kết nối hiện tại và các cổng đang lắng nghe.

Sau khi bạn đã xác định cổng nào đang lắng nghe, bạn muốn đóng một cổng xác định nhưng trước khi đóng nó bạn muốn xác định xem những ứng dụng nào đang sử dụng nó. Để làm được điều này, mở một cửa sổ chế độ dòng lệnh và gõ **netstat –o** rồi nhấn ***ENTER***. Câu lệnh này sẽ hiển thị giao thức, cổng theo chiều vào đang mở, kết nối tới/từ máy tính khác và cổng sử dụng như hình 8-11 miêu tả.



Hình 8-11: Sử dụng Netstat –o để hiển thị các tiến trình và các cổng đang sử dụng trên một máy chủ

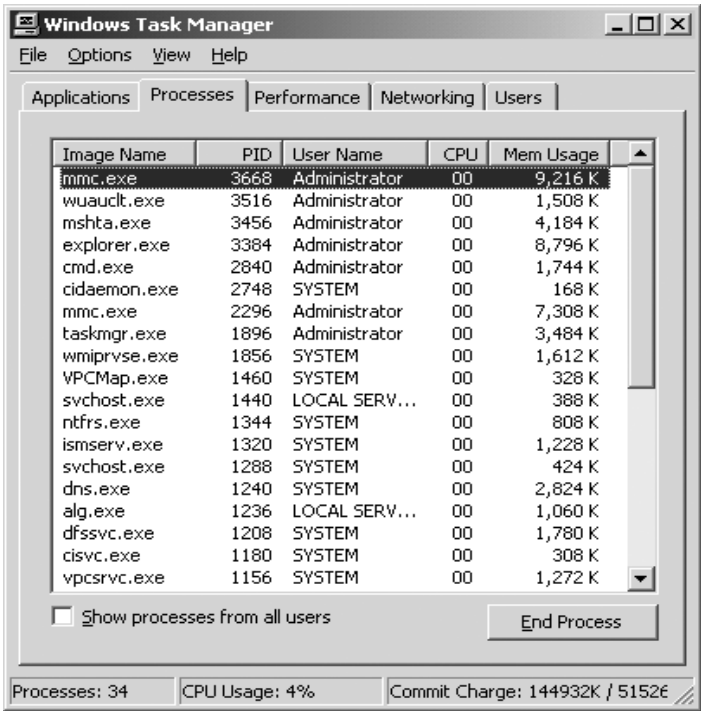
Trong ví dụ này, chú ý rằng bản ghi cuối cùng hiển thị ***Acapulco*** và máy tính có địa chỉ 192.168.16.20 đang truyền thông qua cổng 3389. Trong trường hợp này, bạn có thể thấy rằng PID (mã nhận diện tiến trình) là 660. Sử dụng thẻ ***Process*** trong Windows ***Task Manager*** để xác định xem tiến trình nào được gán ID là 660. Mặc định, thẻ ***Process*** không hiển thị các PID của các tiến trình. Bạn hiển thị PID bằng cách mở thực đơn ***View***, lựa chọn ***Select Columns*** rồi lựa chọn PID (xem hình 8-12).



Hình 8-12: Cấu hình Task Manager để hiển thị PID

Nếu bạn lựa chọn cột PID, bạn sẽ nhìn thấy một màn hình tương tự với hình 8-13.

So sánh PID và tiến trình để xác định xem tiến trình nào hoặc ứng dụng nào có cổng đang mở. Nếu PID phụ thuộc vào tiến trình ***Svchost***, bạn phải làm thêm một bước nữa để xác định xem dịch vụ nào được kết hợp lại trong tiến trình ***Svchost***. Để hiển thị danh sách các dịch vụ tổng hợp, mở một cửa sổ dòng lệnh và gõ **tasklist /svc**. Trong ví dụ hiện thời, tiến trình ***Svchost*** với PID là 660 cung cấp các dịch vụ cho ***TermService*** (dịch vụ đầu cuối cho phép đăng nhập vào một máy tính ở xa). Dịch vụ **Terminal Services** sử dụng cổng ***3389*** để liên kết. Sử dụng phương pháp này, bạn có thể tìm ra các ứng dụng và các dịch vụ được kết hợp với các cổng đang mở trước khi đóng cổng này lại.



Hình 8-13: Sử dụng Task Manager để xem PID của mỗi tiến trình

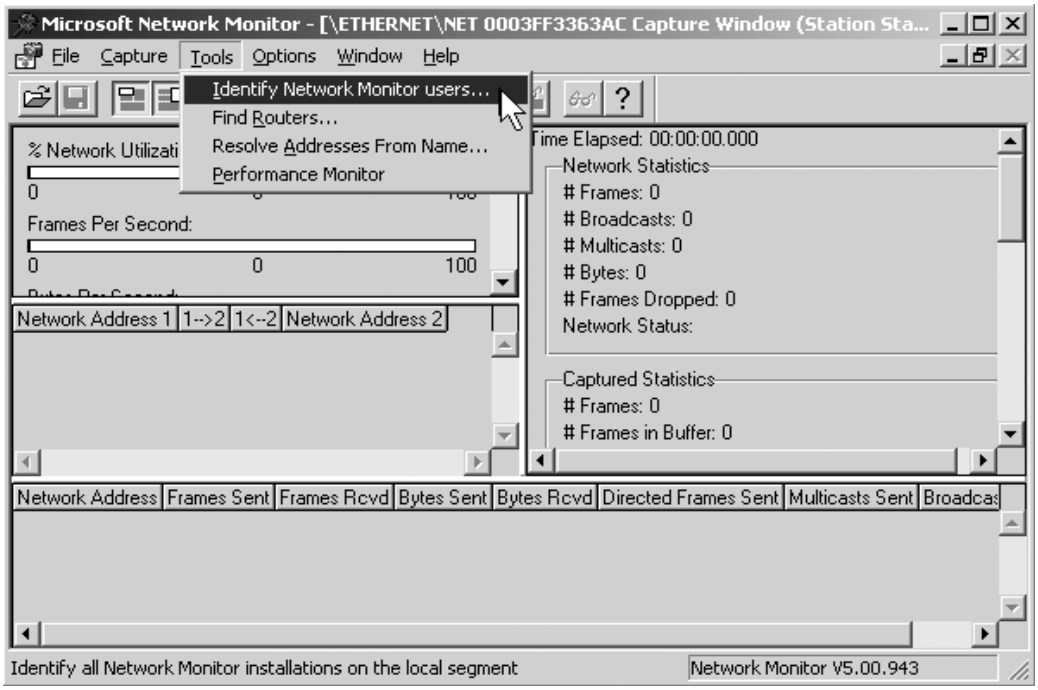
SỬ DỤNG CÔNG CỤ GIÁM SÁT MẠNG NETWORK MONITOR

Hệ điều hành Windows Server 2003 cung cấp công cụ giám sát mạng thu gọn ***Network Monitor*** (sử dụng ***Windows Component Wizard*** để cài đặt công cụ này). Đây là một công cụ mạnh tuy nhiên một phiên bản cao cấp hơn của công cụ này được cung cấp trong ***Microsoft Systems Management Server***. Để xác định xem bạn đang sử dụng phiên bản thu gọn nào của ***Network Monitor*** (một phần của ***Network Monitor***), trên thực đơn ***Help*** nhấp vào ***About***. Thông tin trong hộp thoại ***Network Monitor*** sẽ đưa ra thông tin bạn đang sử dụng phiên bản nào. Có hai sự khác biệt chính giữa phiên bản chuẩn và phiên bản thu gọn của ***Network Monitor*** đó là:

- Phiên bản thu gọn của ***Network Monitor*** chỉ có thể thu thập được lưu thông gửi tới hoặc từ giao diện mạng của chính nó. Trong khi đó phiên bản chuẩn của ***Network Monitor*** có thể hoạt động trong chế độ hỗn hợp. Điều đó có nghĩa rằng nó có thể thu thập 100% lưu thông mạng trên giao diện mạng.

- Phiên bản chuẩn của ***Network Monitor*** cho phép bạn xem có phiên bản nào của ***Network Monitor*** đang chạy trên mạng không. Thông tin này phù hợp khi bạn thiết lập nhiều trạm giám sát dọc theo mạng và

kế đó sử dụng một điểm giám sát trung tâm để thu thập dữ liệu. Do dữ liệu nhạy cảm có thể được thu thập và kiểm tra khi sử dụng công cụ này nên bạn cần biết ai sử dụng phiên bản của công cụ này ở chế độ hỗn hợp từ đó giúp bạn duy trì một môi trường mạng an toàn. Để xác định ai đang chạy ***Network Monitor***, lựa chọn ***Identify Network Monitor Users*** trên thực đơn ***Tools*** như hình 8-14.



Hình 8-14: Theo dõi các trường hợp Network Monitor khác

- **Cài đặt công cụ Network Monitor thu gọn**

Để cài đặt ***Network Monitor*** thu gọn, thực hiện theo các bước sau:

1. Mở ***Control Panel***

2. Nhấp đúp vào ***Add Or Remove Programs***

3. Trong cửa sổ ***Add Or Remove Programs,*** nhấp vào ***Add/Remove Windows Components.***

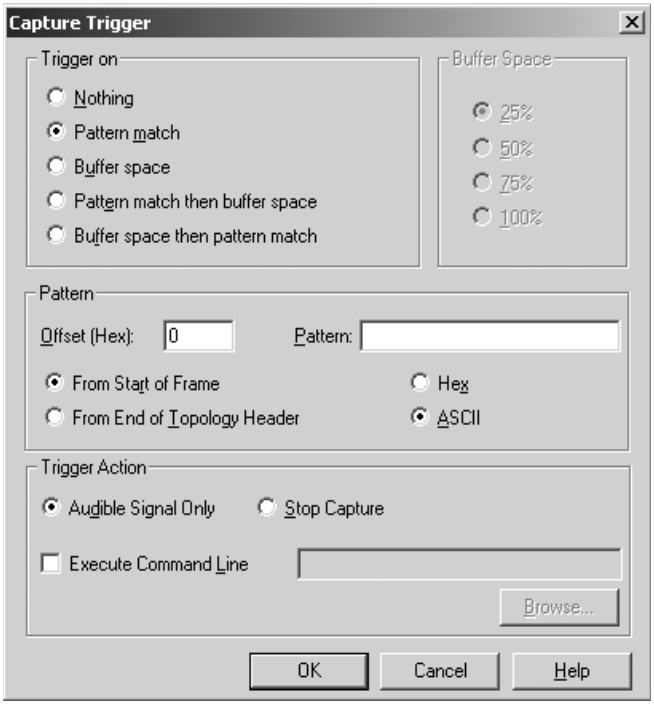
4. Trong ***Windows Components Wizard*** nhấp vào ***Management And Monitoring Tools*** rồi nhấp ***Details***.
5. Lựa chọn hộp kiểm tra ***Network Monitor Tools*** rồi nhấp ***OK***.
6. Trong cửa sổ ***Windows Components*** nhấp ***Next***.
7. Trên màn hình ***Windows Setup*** nhấp ***Finish***.

Sử dụng các bộ khởi tạo (Trigger) trên công cụ Network Monitor

Chức năng chính của ***Network Monitor*** đó là thu thập các gói tin khi chúng di chuyển trên mạng. Tuy nhiên khi xem ***Network Monitor*** theo thời gian thực và đợi cho lỗi xuất hiện là một điều không thực tế. Như đã đề cập ở trên, bạn có thể thiết lập các bộ khởi tạo để thông báo khi những điều kiện cụ thể được đáp ứng. Để cấu hình một bộ khởi tạo, hãy bắt đầu từ ***Network Monitor*** và từ thực đơn ***Capture*** lựa chọn ***Trigger***. Hộp thoại ***Capture Trigger*** xuất hiện như hình 8-15.

Mặc định, không có bộ khởi tạo nào được kích hoạt. Bạn có thể thiết lập một bộ khởi tạo để thông báo cho bạn dựa trên kích thước của bộ đệm hoặc các mẫu được tìm thấy trong quá trình thu thập dữ liệu hoặc cả hai. Ví dụ, bạn có thể cấu hình bộ khởi tạo thông báo khi không gian bộ đệm là 25%, 50%, 75% hoặc 100%.

> **CHÚ Ý** ***Bộ đệm dành cho giám sát mạng*** *Trong suốt tiến trình thu thập,* ***Network Monitor*** *sẽ chép các khung dữ liệu phù hợp với bộ lọc của bạn vào một file tạm được gọi là file bộ đệm. Bạn có thể xác định cả kích thước lẫn vị trí của file này. Khi bộ đệm đạt tới kích thước tới hạn của nó, các khung dữ liệu mới sẽ ghi đè lên các khung dữ liệu cũ nhất.*



Hình 8-15: Cấu hình một bộ khởi tạo (Trigger) để thông báo bạn về các trạng thái cụ thể nào đó

Do các khung dữ liệu cũ sẽ bị ghi đè lên khi kích thước của bộ đệm bị đầy nên bạn muốn nhận được thông báo khi kích thước bộ đệm bằng 75% kích thước tổng để bạn có thể lưu bộ đệm lên một file khác. Bạn cũng muốn sử dụng tính năng ***Pattern Match*** (được lựa chọn trong hình 8-15), qua đó bạn có thể nhập thông tin tìm kiếm ở hệ đếm cơ số 16 (hexa) hoặc bảng mã ACSII. Ví dụ, bạn có thể tìm kiếm bất kỳ một chuỗi ký tự nào đó và kế đó bằng cách sử dụng lựa chọn ***Execute Command Line*** sẽ có một thông báo gửi tới bạn nói rằng chuỗi văn bản đã được tìm thấy.

XỬ LÝ SỰ CỐ KẾT NỐI INTERNET

Một trong những vấn đề liên quan đến việc xử lý sự cố mạng thường gặp đó là không kết nối được với Internet. Có một vài đường truyền trong chuỗi kết nối từ máy trạm tới Internet. Nếu một trong những đường truyền này bị đứt thì người sử dụng không thể kết nối với Internet được. Là một nhà quản trị hệ thống, bạn phải lựa chọn phương án làm thế nào để xử lý sự cố không kết nối được với Internet trong mỗi trường hợp.

Có hai phương án cơ bản để xử lý sự cố không kết nối được với Internet đó là: từ trong ra ngoài và từ ngoài vào trong. Phương án từ trong ra ngoài bắt đầu tại điểm bên trong, từ phía máy trạm và kết nối tới mạng công cộng bên ngoài. Phương án từ ngoài vào trong thì ngược lại: nó bắt đầu từ phía ngoài của firewall hoặc router của công ty và kết nối tới máy trạm ở bên trong. Cả hai phương pháp này đều rất tốt và sẽ được sử dụng trong từng trường hợp cụ thể.

Khi một người sử dụng phàn nàn rằng "Internet bị lỗi" thì phương pháp hiệu quả hơn là từ trong ra ngoài. Mặc dù không có dấu hiệu nào chỉ ra lỗi gây ra không kết nối được với Internet nhưng thực sự biết rằng chỉ có duy nhất một người sử dụng trên mạng có vấn đề. Vì vậy, bạn sẽ sử dụng mô hình từ trong ra ngoài và bắt đầu thu thập thêm thông tin về người sử dụng này. Bạn cũng sẽ xác định xem có ai trên cùng mạng với người sử dụng này vẫn có thể truy cập được Internet hay không. Nếu những người sử dụng khác vẫn có thể truy cập được Internet thì vấn đề gây ra lỗi này là do cấu hình sai trên máy tính của người sử dụng hoặc một số vấn đề khác liên quan trực tiếp đến máy trạm đó. Nếu một mạng con nào đó hoặc nhiều mạng con không thể kết nối được với Internet thì phương pháp từ ngoài vào trong sẽ hiệu quả hơn.

Xác định vấn đề mạng cụ thể

Tại máy trạm, bạn có thể thực hiện một số bước đơn giản nhằm thu hẹp phạm vi tìm kiếm lỗi. Trước hết, bạn có thể xác định cấu hình IP của máy

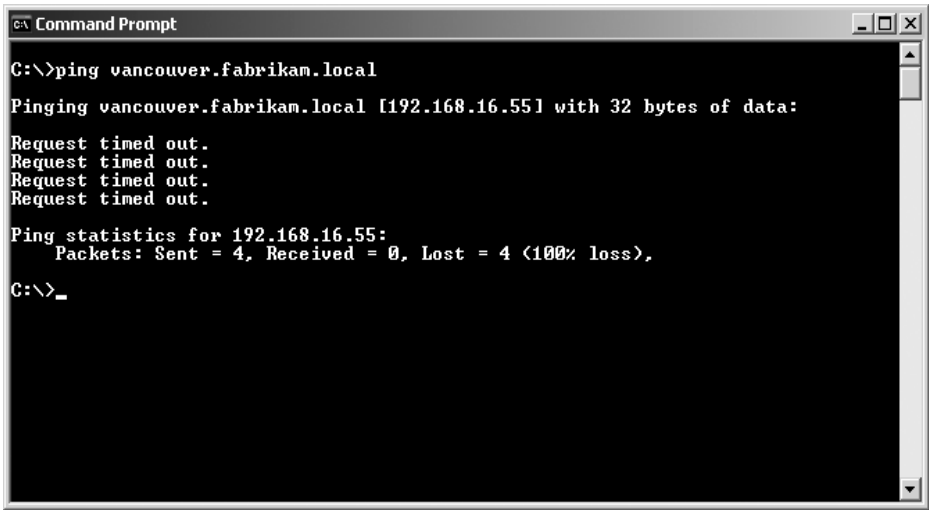
tinh bằng cách mở cửa sổ dòng lệnh và gõ **ipconfig /all**. Xem xét lại kết quả do câu lệnh này đưa ra và kiểm tra các thông số dưới đây:

- Máy tính có địa chỉ IP và mặt nạ mạng hợp lệ.
- Địa chỉ gateway mặc định là chính xác.
- Có ít nhất một máy chủ DNS được liệt kê.
- Nếu máy tính được cấu hình nhận địa chỉ IP động từ máy chủ DHCP, xác nhận rằng đặc tính ***DHCP Enabled*** hiển thị là ***Yes***.
- Máy tính không có địa chỉ IP trong dải từ 169.254.0.0 đến 169.254.255.255 trừ phi bạn có ý định sử dụng APIPA.

Sau khi đã kiểm tra cấu hình IP, bạn cũng có thể xác định xem vấn đề có liên quan tới quá trình phân giải tên hay không.

Xác định các vấn đề kết nối

Để kiểm tra xem vấn đề có liên quan tới việc phân giải tên hay không, thực hiện ***ping*** một máy trạm trên mạng khác như hình 8-16.



Hình 8-16: Các kết quả của việc ping địa chỉ DNS nhưng các gói tin khôg tìm thấy địa chỉ đích

Phản hồi từ câu lệnh ***Ping*** là rất hữu dụng. Mặc dù phản hồi đối với việc ***ping vancouver.fabrikam.local*** là "***Request Time Out***" nhưng bạn biết rằng việc phân giải tên không phải là nguyên nhân gây ra lỗi do địa chỉ IP đúng của ***vancouver.fabrikam.local*** được đặt trong phần móc vuông. Điều đó có nghĩa rằng tên trạm đã được phân giải chính xác thành một địa chỉ IP. Với

tình huống này, bạn sẽ tập trung vào các vấn đề kết nối chứ không liên quan tới phân giải tên.

Công cụ logic kế tiếp đó là ***PathPing***. Công cụ này hiển thị mỗi đường định tuyến giữa máy trạm và đích và giúp bạn xác định đường truyền nào không chuyển gói tin tới đích kế tiếp. Dưới đây là một ví dụ mô tả bạn sử dụng ***PathPing*** để tìm đường đi tới ***Mail01*** như thế nào. Để tiết kiệm thời gian, sử dụng lựa chọn ***–n*** để ngăn không cho ***PathPing*** cố gắng phân giải các địa chỉ IP của các router trung gian thành tên của chúng.

```
D:\> pathping -n mail01

Tracing route to mail01 [10.54.1.196]
over a maximum of 30 hops:
  0  172.16.87.35
  1  172.16.87.218
  2  192.168.52.1
  3  192.168.80.1
  4  10.54.247.14
  5  10.54.1.196

Computing statistics for 125 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           172.16.87.35
                                     0/ 100 =  0%   |
  1   41ms     0/ 100 =  0%     0/ 100 =  0%  172.16.87.218
                                    13/ 100 = 13%   |
  2   22ms    16/ 100 = 16%     3/ 100 =  3%  192.168.52.1
                                     0/ 100 =  0%   |
  3   24ms    13/ 100 = 13%     0/ 100 =  0%  192.168.80.1
                                     0/ 100 =  0%   |
  4   21ms    14/ 100 = 14%     1/ 100 =  1%  10.54.247.14
                                     0/ 100 =  0%   |
  5   24ms    13/ 100 = 13%     0/ 100 =  0%  10.54.1.196
Trace complete.
```

Xác định các vấn đê liên quan đến phân giải tên

Nếu bạn nhận được phản hồi như hình 8-17, bạn sẽ nhận ra rằng các lỗi của máy trạm là nó không có khả năng phân giải các tên trạm thành các địa chỉ IP.

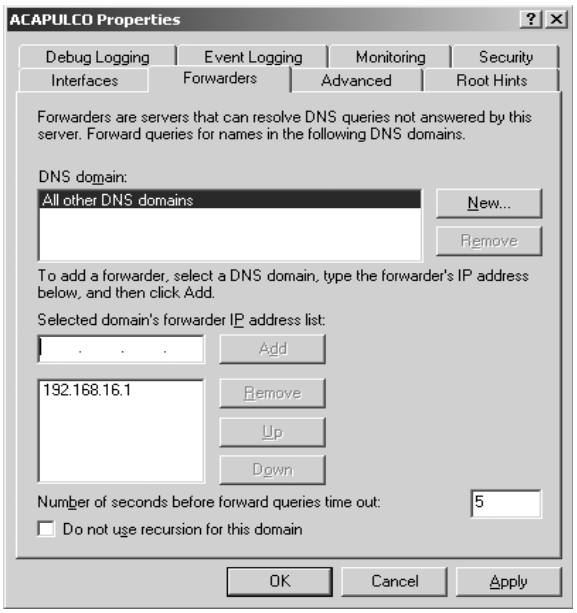
Hình 8-17: Các kết quả yêu cầu ping chỉ rằng DNS không thể phân giải tên trạm được yêu cầu

Trong hình 8-17, không có dấu hiệu nào cho thấy máy trạm có thể phân giải tên ***stlouis.fabrikam.local*** thành một địa chỉ IP. Nếu bạn suy đoán rằng vấn đề là do phân giải tên và bạn biết địa chỉ IP của ***stlouis.fabrikam.local*** thì hãy gõ **ping *ip_address*** (trong đó *ip_address là địa chỉ IP của* ***stlouis.fabrikam.local***). Nếu bạn nhận được phản hồi báo ***ping*** thành công thì có nghĩa rằng lỗi là do phân giải tên gây ra. Để giải quyết vấn đề này, kiểm tra cấu hình máy chủ DNS, các máy chủ WINS và nếu có thể kiểm tra file ***local host*** và file ***Lmhost***.

Để xác định xem máy chủ DNS có chứa địa chỉ đúng của máy trạm hay không ta sử dụng câu lệnh ***Nslookup***. Ví dụ, tại dấu nhắc lệnh, gõ **nslookup stlouis.fabrikam.local** rồi nhấp phím ***ENTER***. Câu lệnh này sẽ hiển thị địa chỉ IP do máy chủ DNS mặc định cung cấp cho máy trạm.

> **CHÚ Ý *Hướng dẫn Nslookup*** *Một hướng dẫn tuyệt vời về Nslookup đó là Microsoft Knowledge Base article 200525, "Sử dụng Nslookup.exe". Để tìm bài này, truy cập vào trang Web http://support.microsoft.com và nhập số hiệu bài này vào hộp văn bản Search The Knowledge Base.*

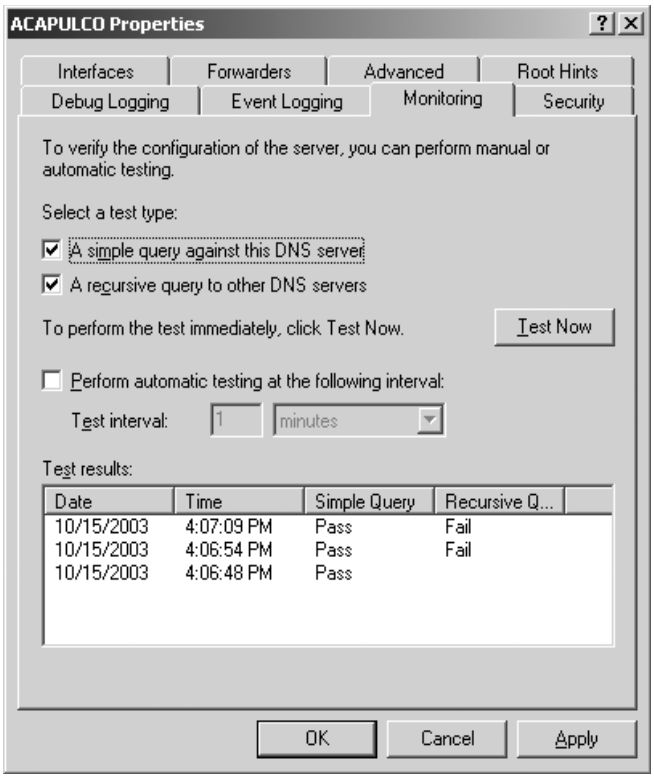
Nếu bạn suy đoán những vấn đề liên quan đến phân giải tên DNS do một máy chủ nào đó hoặc do phía bên ngoài tổ chức của bạn gây ra thì tiếp theo bạn sẽ kiểm tra máy chủ DNS. Trước hết, đảm bảo rằng máy chủ DNS đã được cấu hình để hướng những yêu cầu DNS không thuộc phạm vi quản lý của nó tới một vị trí logic kế tiếp. Bạn có thể thực hiện công việc này bằng cách xác nhận cấu hình của thẻ ***Forwarders*** như hình 8-18.



Hình 8-18: Đảm bảo rằng các máy chủ DNS cấp trên được cấu hình chính xác

Thông thường, máy chủ DNS hướng các yêu cầu tới một máy chủ nắm giữ nhiều thông tin hơn hoặc hướng trực tiếp tới nhà cung cấp dịch vụ Internet (ISP). Nếu không có tham số này bạn cần điều chỉnh các tham số này trong thẻ ***Forwarders***.

Ngoài ra, bạn cũng cần xác nhận rằng bản thân máy chủ đang phản hồi các yêu cầu và nó cũng phản hồi với các phép thử trên các máy chủ mà nó hướng thông tin tới đó. Trong ví dụ trên hình 8-19, máy chủ phản hồi với các yêu cầu phân giải tuy nhiên nó không thể nhận được bất kỳ đáp trả nào từ các máy chủ mà nó hướng yêu cầu tới đó.

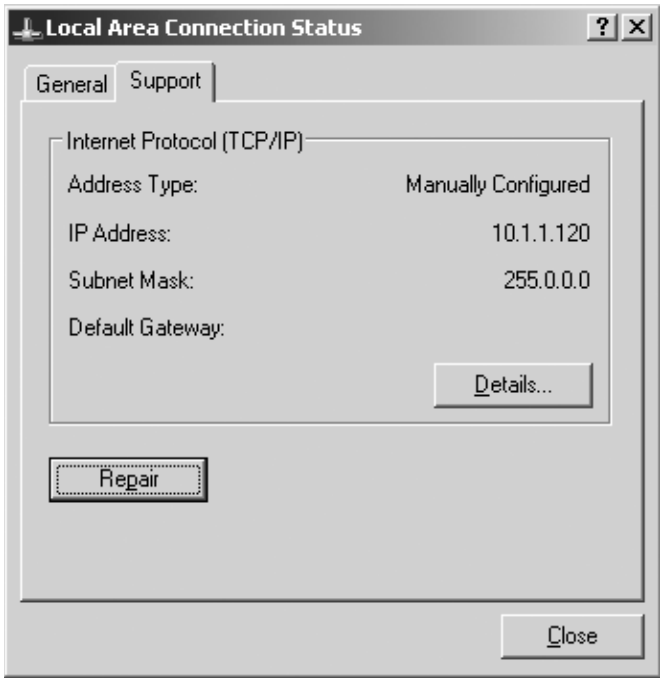


Hình 8-19: Lỗi của truy vấn đệ quy, thông thường chỉ một lỗi hướng yêu cầu

Lỗi này thường chỉ ra rằng vấn đề phân giải tên không xảy ra trên máy chủ của bạn mà trên các máy chủ cấp trên.

Sử dụng tính năng sửa lỗi

Tính năng sửa lỗi trong Windows Server 2003 cho phép bạn thực hiện nhiều công việc chỉ trong một động tác. Bạn có thể tìm thấy tính năng này trong thẻ ***Support*** trong quá trìn kiểm tra trạng thái của một Giao tiếp mạng như hình 8-20.



Hình 8-20: Sử dụng nút Repair để thực hiện động tác thiết lập lại nhiều tham số của cấu hình

Nhấp vào nút ***Repair*** sẽ khởi tạo nhiều hoạt động như thể bạn đang gõ các câu lệnh trong chế độ cửa sổ lệnh. Các câu lệnh được thực hiện theo thứ tự sau trong bảng 8-2.

Bảng 8-2: Các hoạt động trong tiến trình sửa lỗi

Hoạt động trên nút Reapir	Mô tả
Ipconfig /renew	Thay đổi thời hạn thuê bao địa chỉ IP
Arp –d *	Xóa bỏ bộ đệm dùng để lưu trữ bảng ánh xạ địa chỉ ARP (một giao thức được sử dụng để chuyển đổi địa chỉ IP thành địa chỉ MAC)
Nbtstat –R	Tải lại bộ đệm NetBIOS
Nbtstat –RR	Gửi tên NetBIOS của máy tính tới WINS cho tiến trình cập nhật
Ipconfig /flushdns	Xóa bỏ bộ đệm DNS
Ipconfig /registerdns	Đăng ký tên với máy chủ DNS

THÔNG TIN THÊM ***Thông tin thêm về nút sửa lỗi*** *Bạn có thể biết thêm về nút* ***Repair*** *trong Microsoft Knowledge Base article 289256 "****A Description of the Repair Option on a Local Area Network or***

***High-Speed Internet Connection**". Để tìm thấy bài viết này, bạn hãy truy cập vào trang Web http://support.microsoft.com và nhập số hiệu bài này vào hộp văn bản Search The Knowledge Base.*

Kiểm tra máy chủ DHCP

Nếu máy trạm không nhận được địa chỉ IP, địa chỉ gateway mặc định và ít nhất một địa chỉ máy chủ DNS thì máy trạm không thể truy cập được Internet. Dưới đây là một số lý do mà thông tin DHCP không thể chuyển tới máy trạm được:

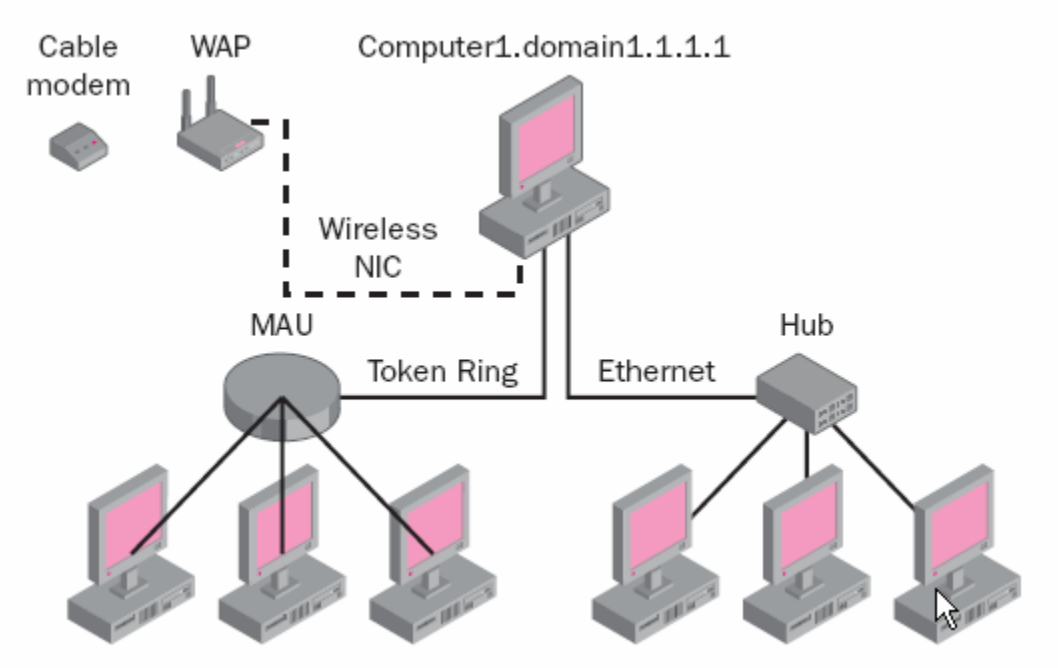
- Router khóa giao thức BOOTP (***Bootstrap Protocol***).
- ***DHCP relay agent*** không tồn tại trên các phân đoạn mạng không có ***BOOTP relay***.
- Dải địa chỉ cung cấp cho máy trạm (***DHCP scope***) không chứa địa chỉ nào.
- Máy chủ DHCP có thể không hoạt động.

Trong khi kiểm tra máy chủ DHCP bạn cũng nên kiểm tra lại tính hợp lệ về địa chỉ IP, gateway mặc định và các máy chủ DNS được cấp phát cho máy trạm.

Nếu có một số máy trạm vẫn kết nối được với Internet trong khi một số khác lại không thực hiện được và bạn xác nhận rằng các máy tính được cấu hình để nhận thông tin cấu hình DHCP từ các dải khác nhau thì có nghĩa là tồn tại một máy chủ DHCP giả mạo ở trên mạng. Một máy chủ DHCP giả mạo là một máy chủ không được ủy quyền hoạt động ở trên mạng. Thông thường, các máy chủ DHCP giả mạo này được thiết lập với mục đích kiểm tra, tuy nhiên chúng có thể cấp phát thông tin cấu hình và địa chỉ không đúng cho các máy trạm dẫn đến tình trạng chúng không thể truy cập được Internet.

Nếu các máy chủ DHCP không được ủy quyền hoạt động, chúng sẽ tự động tắt. Sử dụng công cụ **Dhcploc** được cung cấp trong công cụ hỗ trợ ***Windows Server 2003 Support Tools,*** để tìm kiếm các máy chủ DHCP chưa được ủy quyền hoặc các máy chủ DHCP khác không cần được ủy quyền như các máy chủ DHCP sử dụng trên các hệ điều hành Microsoft cũ hoặc các máy chủ DHCP được cài đặt trên hệ điều hành không phải của Microsoft. Bạn có thể cấu hình ***Dhcploc*** gửi các cảnh báo khi các máy chủ DHCP giả mạo được xác định.

Đôi khi, bạn cũng nhận được yêu cầu giải quyết sự cố liên quan đến các kết nối tới Internet từ các máy trạm không dây. Trong một số trường hợp, bạn muốn thực hiện cầu nối từ một WAP (điểm truy cập không dây) với nhiều cấu trúc mạng khác nhau như hình 8-21.

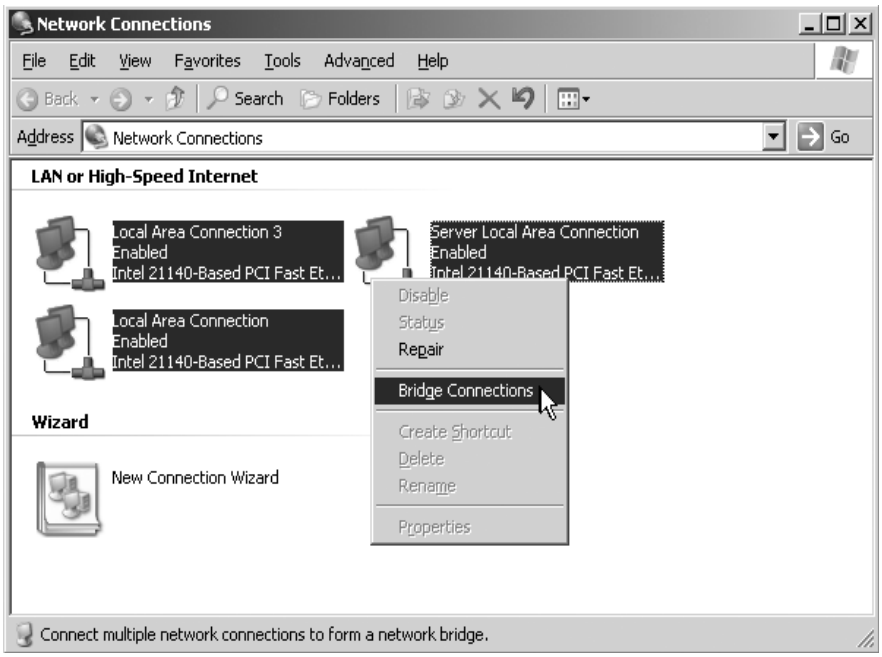


Hình 8-21: Ví dụ minh họa về mạng bắc cầu

Kết nối nhiều mạng với nhau

Trong hình 8-21, một kết nối Internet được đặt trên WAP. Kế đó, WAP liên kết với Giao tiếp mạng không dây trên máy chủ. Ngoài ra, máy chủ còn có một kết nối ***Ethernet*** và một kết nối ***Token Ring*** được kết nối với các Giao tiếp mạng khác.

Khi bạn cho phép tính năng bắc cầu trên kết nối này, tất cả các điểm truy cập vào máy chủ (không dây, ***Token Ring***, ***Ethernet***) dường như nằm trên cùng một mạng. Do đó, bạn có thể chia sẻ kết nối không dây để tất cả đều có thể đi ra ngoài Internet. Để tạo một mạng bắc cầu, giữ phím CTRL khi bạn nhấp vào nhiều kết nối trên máy chủ. Tiếp đó nhấp chuột phải và lựa chọn ***Bridge Network*** như hình 8-22.



Hình 8-22: Lựa chọn nhiều mạng rồi nhấp chuột phải để kết nối chúng với nhau

Khi bạn cấu hình tính năng bắc cầu mạng, bạn cho phép lưu thông từ Giao tiếp mạng không dây, ***Ethernet*** và ***Token Ring*** chia sẻ cùng một không gian mạng. Do đó, một Giao tiếp mạng không dây duy nhất sẽ trở thành cổng ra để phân tách các mạng.

Để chẩn đoán và xử lý kết nối được bắc cầu tới Internet, thực hiện các bước sau:

- Trong các đặc tính trên thẻ ***General*** của kết nối được bắc cầu, xác nhận rằng tất cả các mạng đã được bắc cầu.
- Cầu nối sẽ có một địa chỉ IP riêng biệt. Kiểm chứng điều này bằng cách gõ **ipconfig/all** trong cửa sổ chế độ dòng lệnh. Nếu cầu nối không có một địa chỉ IP riêng biệt, bạn hãy loại bỏ và tạo lại nó.
- Kiểm tra kết nối vật lý giữa các phân đoạn trên cầu nối.

Sử dụng công cụ Netdiag

Netdiag là một công cụ ở chế độ dòng lệnh được sử dụng để thực hiện một loạt các bước kiểm tra nhằm giúp cho người quản trị mạng cách ly các vấn đề mạng và vấn đề kết nối.

Để giúp bạn hiểu xem ***Netdiag*** làm việc như thế nào hãy xem xét tình huống sau đây. Bạn là nhà quản trị mạng của công ty ABC và một người sử dụng

phàn nàn với bạn rằng cô ta không thể kết nối tới các tài nguyên mạng. Bạn chỉ nhận được thông báo "***Network path not found***" và không còn thông tin nào khác. Mặc dù bạn dự đoán rằng có thể máy chủ DNS có vấn đề nhưng bạn vẫn quyết định sử dụng công cụ ***Netdiag*** để nhận được phản hồi nhanh qua một loạt các bước kiểm tra. Tại dấu nhắc lệnh, gõ **netdiag** rồi nhấp phím ***ENTER***.

Khi đó ***Netdiag*** thực hiện các bước kiểm tra mang tính tổng thể trên mỗi Giao tiếp mạng. Các bước kiểm tra trên các Giao tiếp mạng được thực hiện theo thứ tự sau:

1. Kiểm tra các truy vấn ***Netcard***
2. Kiểm tra ***Ipconfig***
3. Kiểm tra cấu hình tự động (APIPA)
4. Kiểm tra gateway mặc định
5. Kiểm tra tên NetBT
6. Kiểm tra dịch vụ WINS.

Nediag thực hiện các bước kiểm tra mang tính tổng thể theo thứ tự sau:

1. Kiểm tra thành viên của miền
2. Kiểm tra tiến trình vận chuyển NetBT
3. Kiểm tra địa chỉ tự động cấu hình (APIPA)
4. Kiểm tra ***ping*** địa chỉ ***IP Loopback***
5. Kiểm tra ***gateway*** mặc định
6. Kiểm tra tên ***NetBT***
7. Kiểm tra ***Winsock***
8. Kiểm tra ***DNS***
9. Kiểm tra ***Redir*** và ***Browser***
10. Kiểm tra quá trình phát hiện máy chủ DC
11. Kiểm tra danh sách máy chủ DC
12. Kiểm tra mối quan hệ tin cậy
13. Kiểm tra giao thức xác thực Kerberos
14. Kiểm tra giao thức truy vấn cơ sở dữ liệu LDAP
15. Kiểm tra tính liên kết

16.Kiểm tra cấu hình WAN

17.Kiểm tra cấu hình modem

18.Kiểm tra tính bảo mật IP

Dưới đây là kết quả của câu lệnh ***Netdiag***. Kết quả của các bước kiểm tra này sẽ hiển thị giao thức nào được sử dụng trên Giao tiếp mạng, các mối liên kết và các quá trình kiểm tra địa chỉ IP thành công. Tiến trình kiểm tra DNS thông qua câu lệnh ping bị lỗi và xác nhận rằng máy chủ DNS không thể liên lạc được.

Computer Name: RKSRVR-2
DNS Host Name: rksrvr-2.reskita.microsoft.com
System info : Windows 2000 Server (Build 2467)
Processor : x86 Family 6 Model 6 Stepping 0, GenuineIntel
List of installed hotfixes : Q147222

Netcard queries test . . . . . : Passed
[WARNING] The net card 'Intel(R) PRO/100+ Management Adapter' may not be working.
Per interface results:
Adapter : Local Area Connection
Netcard queries test . . . : Passed
Host Name. . . . . : rksrvr-2
IP Address . . . . . : 10.10.1.51
Subnet Mask. . . . . : 255.255.255.0
Default Gateway. . . . . :
Dns Servers. . . . . : 10.10.1.77
AutoConfiguration results. . . . . : Passed
Default gateway test . . . : Skipped
[WARNING] No gateways defined for this adapter.
NetBT name test. . . . . : Passed
WINS service test. . . . . : Skipped
There are no WINS servers configured for this interface.
Adapter : Local Area Connection 2
Netcard queries test . . . : Failed
NetCard Status: DISCONNECTED
Some tests will be skipped on this interface.
Host Name. . . . . : rksrvr-2
Autoconfiguration IP Address : 169.254.74.217
Subnet Mask. . . . . : 255.255.0.0

Default Gateway. . . . . :
Dns Servers. . . . . :

Global results:
Domain membership test . . . . . : Passed
NetBT transports test. . . . . : Passed
List of NetBt transports currently configured:
NetBT_Tcpip_{A2D04C22-3BB8-4FA0-B7DA-414DC1DD08A7}
NetBT_Tcpip_{56079E37-8246-4712-8B36-F503FF6F9873}
2 NetBt transports currently configured.
Autonet address test . . . . . : Passed
IP loopback ping test. . . . . : Passed
Default gateway test . . . . . : Failed
[FATAL] NO GATEWAYS ARE REACHABLE.
You have no connectivity to other network segments.
If you configured the IP protocol manually then
you need to add at least one valid gateway.
NetBT name test. . . . . : Passed
Winsock test . . . . . : Passed
DNS test . . . . . : Failed
[WARNING] Cannot find a primary authoritative DNS server for the name 'bdover.reskita.microsoft.com.'. [ERROR_TIMEOUT] The name 'bdover.reskita.microsoft.com.' may not be registered in DNS
[WARNING] The DNS entries for this DC cannot be verified right now on DNS server 10.10.1.77, ERROR_TIMEOUT.
[FATAL] No DNS servers have the DNS records for this DC registered.
Redir and Browser test . . . . . : Passed
List of NetBt transports currently bound to the Redir
NetBT_Tcpip_{A2D04C22-3BB8-4FA0-B7DA-414DC1DD08A7}
NetBT_Tcpip_{56079E37-8246-4712-8B36-F503FF6F9873}
The redir is bound to 2 NetBt transports.
List of NetBt transports currently bound to the browser
NetBT_Tcpip_{A2D04C22-3BB8-4FA0-B7DA-414DC1DD08A7}
NetBT_Tcpip_{56079E37-8246-4712-8B36-F503FF6F9873}
The browser is bound to 2 NetBt transports.
DC discovery test. . . . . : Passed
DC list test . . . . . : Passed
Trust relationship test. . . . . : Failed
Secure channel for domain 'RESKITA' is to '\\a-dcp.reskita.microsoft.com'.

[FATAL] Cannot set secure channel for domain 'RESKITA' to PDC emulator. [ERR OR_NO_LOGON_SERVERS]
Kerberos test. . . . . : Passed
LDAP test. . . . . : Passed
[WARNING] Failed to query SPN registration on DC 'adcp.reskita.microsoft.com'.
[WARNING] Failed to query SPN registration on DC 'adc1.reskita.microsoft.com'.
[WARNING] Failed to query SPN registration on DC 'adc3.reskita.microsoft.com'.
Bindings test. . . . . : Passed
WAN configuration test . . . . . : Skipped
No active remote access connections.
Modem diagnostics test . . . . . : Passed
IP Security test . . . . . : Passed
Service status is: Started
Service startup is: Automatic
IPSec service is available, but no policy is assigned or active
Note: Run "ipseccmd /?" for more detailed information

The command completed successfully

Với thông tin này, người quản trị hệ thống biết rằng hoặc địa chỉ máy chủ DNS không chính xác hoặc máy chủ DNS không phản hồi. Do địa chỉ máy chủ DNS cũng được hiển thị qua kết quả nên bạn dễ dàng xác định xem địa chỉ đó có đúng hay không.

Sau khi đã cách ly được lỗi, người quản trị có thể thực hiện thêm các bước chẩn đoán để xác định xem tại sao máy chủ DNS không hoạt động

XỬ LÝ SỰ CỐ CÁC DỊCH VỤ TRÊN MÁY CHỦ

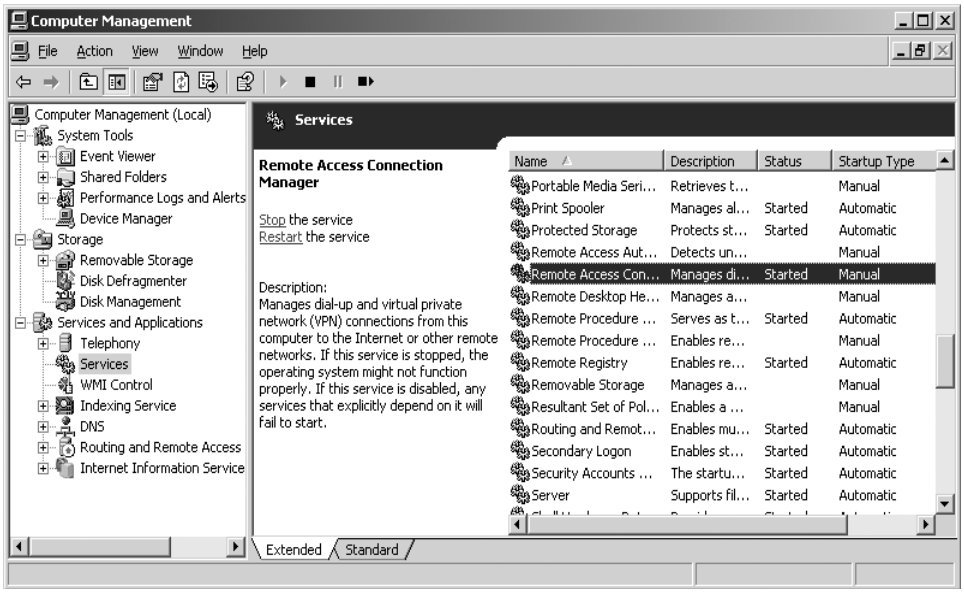
Khi một máy chủ hoạt động bạn có thể nghĩ rằng mọi việc là ổn nhưng trong thực tế bạn phải rất cẩn trọng. Phần này sẽ giúp bạn chẩn đoán và giải quyết các dịch vụ như thế nào nhằm đảm bảo cho máy chủ hoạt động trơn tru.

Kiểm tra sự phụ thuộc của dịch vụ

Cũng giống như các máy chủ khác của Microsoft, Windows Server 2003 được tạo nên bởi một tập hợp các tiến trình, mỗi cái thực hiện một tác vụ cụ thể. Đôi khi các tác vụ này chạy như các dịch vụ. Một dịch vụ có thể chạy hoặc ở chế độ bề mặt (yêu cầu tương tác với người sử dụng) hoặc ở chế độ

ngầm (không cần tương tác với người sử dụng). Thông thường, các dịch vụ chạy ở chế độ ngầm và ít khi yêu cầu tương tác với người sử dụng để thực hiện công việc cụ thể. Một ví dụ về một dịch vụ chạy ở chế độ ngầm đó là dịch vụ ***Net Logon***, chịu trách nhiệm trong việc xác thực quyền cho người sử dụng và các dịch vụ.

Để xác định xem dịch vụ nào được cài đặt và đang chạy, trên thực đơn ***Start*** kích chuột phải vào ***My Computer*** chọn ***Manage*** rồi mở rộng phần ***Services And Applications***. Tiếp đó nhấp vào ***Services***. Hình vẽ 9-23 dưới đây minh họa ví dụ về một danh sách các dịch vụ.

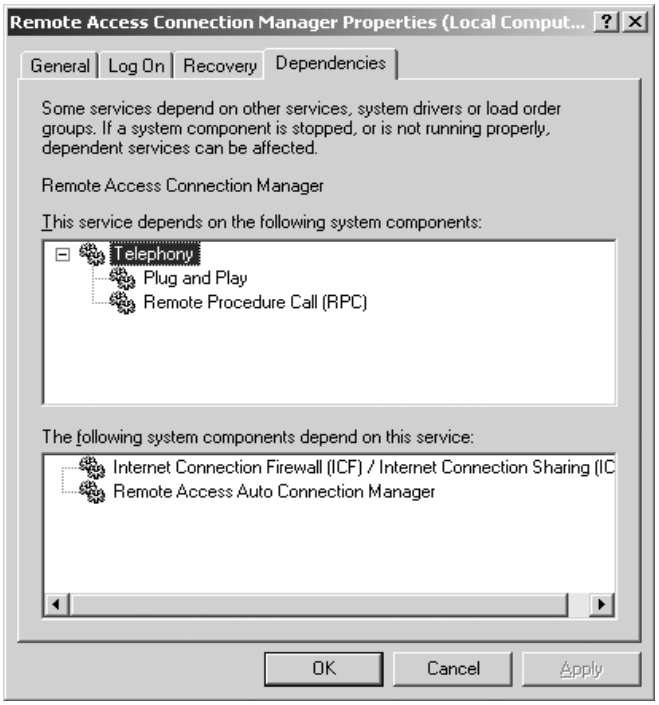


Hình 8-23: Phần Services hiển thị trạng thái của tất cả các dịch vụ

Các dịch vụ có thể nằm ở một trong ba trạng thái sau: đã khởi động (***started***), dừng (***stopped***) hoặc tạm dừng (***paused***). Có ba phương pháp để cấu hình quá trình khởi tạo một dịch vụ:

- **Automatic (tự động)** Dịch vụ sẽ tự động khởi tạo khi hệ thống khởi động lại.
- **Manual (thiết lập thủ công)** Dịch vụ không tự động khởi tạo khi hệ thống khởi động lại nhưng nó sẽ khởi tạo nếu nó được khởi tạo bằng tay hoặc có một tiến trình khác yêu cầu dịch vụ này.
- **Disable (tắt)** Dịch vụ không tự động khởi tạo khi hệ thống khởi động lại. Dịch vụ cũng sẽ không khởi tạo ngay cả trong trường hợp nó được khởi tạo bằng tay hoặc có một tiến trình khác yêu cầu dịch vụ này.

Một số dịch vụ phụ thuộc vào các dịch vụ khác để khởi tạo. Khái niệm này được gọi là sự phụ thuộc của dịch vụ. Vì vậy, nếu như có một dịch vụ có trục trặc thì nó sẽ gây ra ảnh hưởng xếp chồng trên máy chủ. Sử dụng màn hình ***Services***, nếu bạn quen với dịch vụ ***Remote Access Connection*** Manager (kích đúp vào dịch vụ rồi lựa chọn thẻ ***Dependencies***), bạn có thể ***nhìn*** thấy các dịch vụ mà nó phụ thuộc cho tiến trình khởi tạo cũng như các dịch vụ phụ thuộc vào nó trong quá trình khởi tạo. Hình 8-24 sẽ minh họa điều này.



Hình 8-24: Thẻ Dependencies hiển thị sự phụ thuộc của một dịch vụ

Trong trường hợp này, bạn có thể nhìn thấy dịch vụ ***Remote Access Connection Manager*** phụ thuộc vào dịch vụ ***Telephony*** trong khi dịch vụ này lại phụ thuộc vào hai dịch vụ khác là: ***Plug And Play*** và ***Remote Procedure Call (RPC)***. Nếu dịch vụ ***Remote Access Connection Manager*** không hoạt động thì cả hai dịch vụ phụ thuộc vào nó: ***Internet Connection Firewall***/***Internet Connection Sharing*** (ICF/ICS) và ***Remote Access Auto Connection Manager*** đều không khởi tạo được.

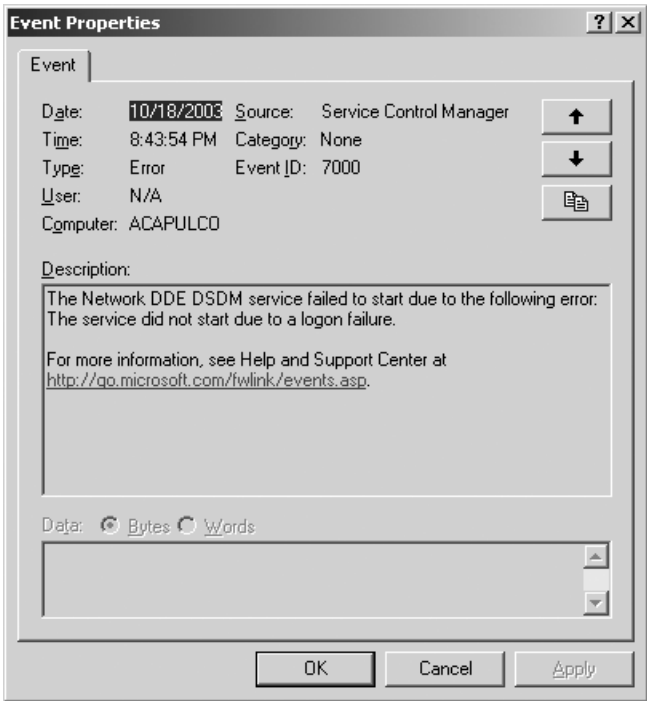
Sử dụng các lựa chọn phục hồi trạng thái dịch vụ

Hầu hết các dịch vụ được cài đặt trên Windows Server 2003 đều chạy trong ngữ cảnh ***Local System***. Đây là một tài khoản hệ thống đặc biệt có tính cục bộ để điều khiển khi nào thì dịch vụ được khởi tạo và dừng. Tuy nhiên, các dịch vụ được tải thêm (thông thường chúng được tải bởi Microsoft hoặc các

ứng dụng của hãng thứ ba) chạy trong các ngữ cảnh khác. Thông thường khi dịch vụ được tải, hệ thống yêu cầu người quản trị cung cấp các chứng thực trên hệ thống mà dịch vụ đang chạy. Thay vì cung cấp dịch vụ truy cập thông suốt tới hệ thống qua tài khoản đặc biệt ***System*** thì dịch vụ bị hạn chế tính năng qua tài khoản người sử dụng do người quản trị xác định. Tài khoản này là một người sử dụng cục bộ trên máy tính (hay tài khoản quản trị cục bộ). Nói cách khác tài khoản có ít quyền hơn. Mức độ truy cập được yêu cầu phụ thuộc vào những yêu cầu của ứng dụng và các dịch vụ cài đặt.

Tuy nhiên mô hình tốt nhất là chỉ cung cấp cho tài khoản mức độ truy cập tối thiểu. Ví dụ, nếu tài khoản dịch vụ bắt đầu với một tài khoản người sử dụng cục bộ thì bạn không cần thiết phải tạo tài khoản đó bởi vì tài khoản quản trị cục bộ sẽ được sử dụng để điều khiển dịch vụ. Với mỗi ứng dụng bạn có kế hoạch cài đặt, hãy tham khảo tài liệu cài đặt để biết được các quyền cần thiết cho tiến trình cài đặt.

Thỉnh thoảng, sau khi cài đặt một ứng dụng mới tương ứng với việc cài đặt dịch vụ mới thì dịch vụ của ứng dụng này không khởi tạo được. Bạn có thể nhìn thấy xem dịch vụ đã được khởi tạo hay chưa và các lỗi đi kèm theo dịch vụ chỉ ra lý do tại sao nó không thể hoạt động được thông qua ***Computer Management*** hoặc xem các file nhật ký trong phần ***System*** như hình 8-25.

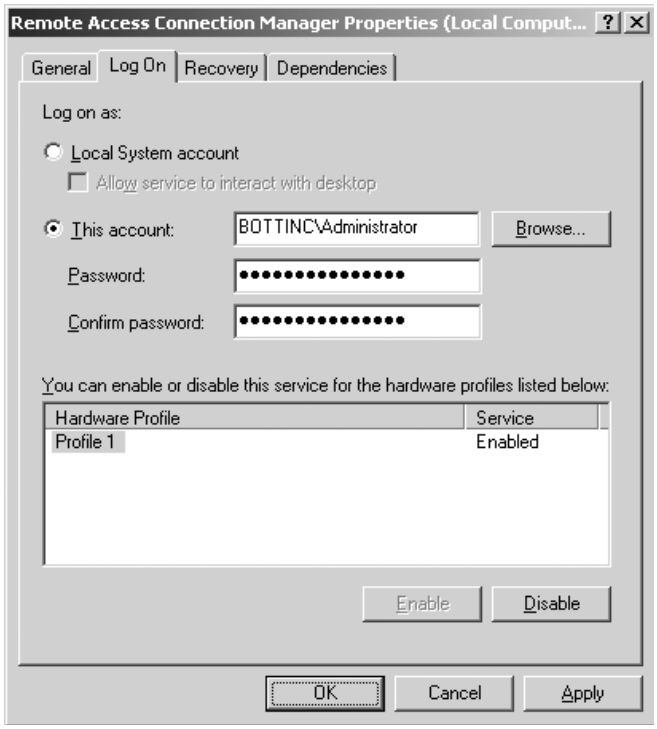


Hình 8-25: Dịch vụ Network DDE DSDM lỗi trong quá trình khởi tạo

Nếu bạn xác định lỗi là do quá trình đăng nhập thì bạn cần phải xem xét lý do gây ra lỗi. Có nhiều lý do có thể gây nên lỗi này:

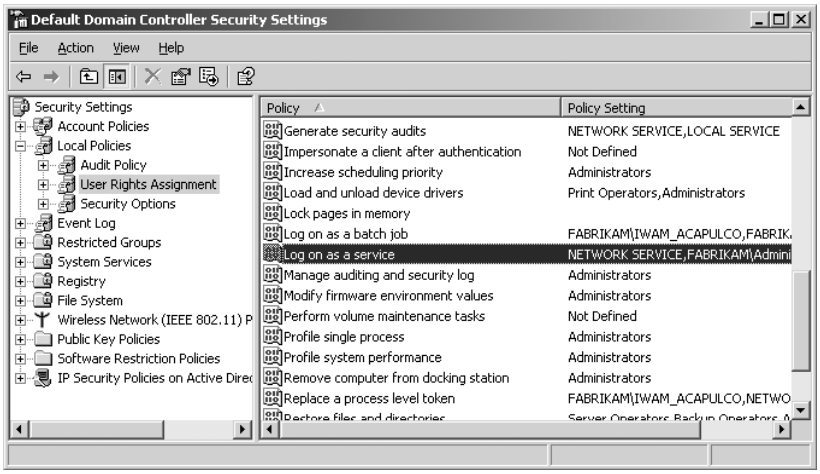
- Tên người sử dụng của tài khoản này đã bị thay đổi, bị xóa, bị cấm hoạt động.
- Mật khẩu của tài khoản này bị hết hạn và cần được thiết lập lại.
- Tài khoản dùng để chạy dịch vụ này không được gán quyền ***Log On As A Service.***

Để xác định được những lỗi này, trước hết ngay trên bản thân dịch vụ bạn hãy kiểm tra thẻ ***Log On*** (xem hình 8-26) để đảm bảo rằng thông tin tài khoản được cung cấp là chính xác dựa trên những đặc tả của ứng dụng.



Hình 8-26: Sử dụng thẻ Log On để đảm bảo rằng thông tin tài khoản dành cho dịch vụ là chính xác

Sau khi kiểm tra tên và mật khẩu, bạn cần đảm bảo rằng tài khoản được gán quyền ***Log On As A Service***. Nếu bạn sử dụng một tài khoản trên miền để chạy một dịch vụ, bạn cần kiểm tra chính sách ***Default Domain Controller***. Để thực hiện tác vụ này, trên thực đơn ***Start*** trỏ tới Administrative Tools rồi nhấp vào ***Domain Controller Security Policy***. Trên màn hình quản trị bên trái, trong phần ***Local Policies*** kích đúp vào ***User Right Assignment*** và ở phía bên phải của màn hình hãy chọn ***Log On As A Service*** như hình 8-27.



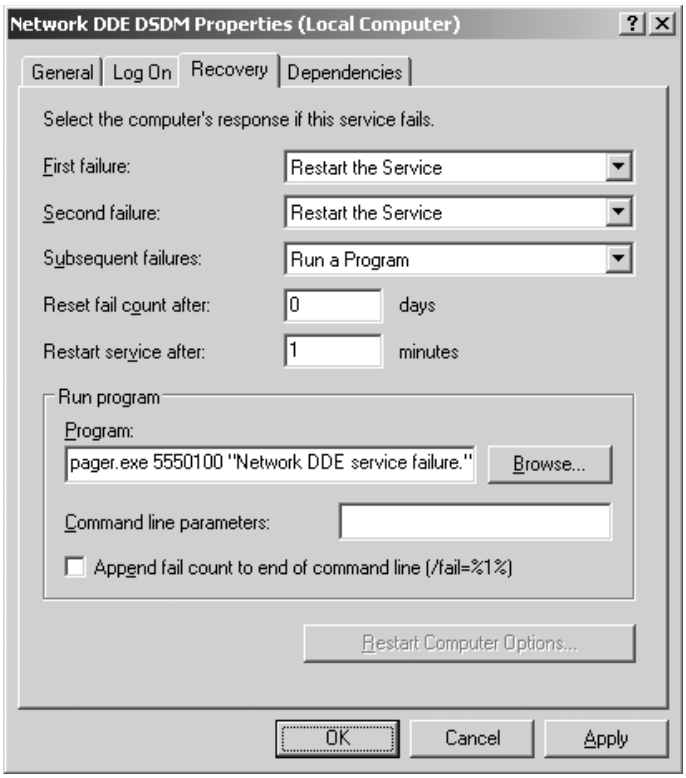
Hình 8-27: Đảm bảo rằng dịch vụ được gán quyền Log On As A Service

Sau khi xác nhận tài khoản miền đã được khai báo trong ***Policy Setting***, bạn hãy khởi động lại dịch vụ.

Nếu tài khoản bạn muốn sử dụng nằm trên một máy tính độc lập cài đặt hệ điều hành Windows Server 2003, hãy chạy công cụ ***Gpedit***. Kế đó, mở rộng ***Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies*** và cuối cùng lựa chọn ***User Right Assignment***. Xác định quyền ***Log On As A Service*** và đảm bảo rằng tài khoản mà bạn muốn sử dụng đã được liệt kê.

Windows Server 2003 có nhiều tùy chọn trong trường hợp khởi tạo dịch vụ bị lỗi do những lý do đã nêu ra ở trên. Nếu dịch vụ bị lỗi, các sự kiện sẽ được ghi lại trên máy chủ đã khởi tạo dịch vụ đó. Tuy nhiên, bạn có thể lựa chọn để có được một mô hình chủ động hơn trong quá trình quản trị dịch vụ.

Nếu bạn lựa chọn thẻ ***Recovery*** của dịch vụ, một vài lựa chọn cho phép bạn chỉ định hành vi của hệ thống sau khi dịch vụ bị lỗi như hình 8-28.



Hình 8-28: Thiết lập cách thức hành động trong thẻ Recovery

Nếu một dịch vụ bị lỗi, bạn có bốn lựa chọn sau:

- ***Take No Action*** (không thực hiện bất kỳ hành động nào)
- ***Restart The Service*** (khởi động lại dịch vụ)
- ***Run A Program*** (chạy một chương trình nào đó)
- ***Restart The Computer*** (khởi động lại máy tính)

Lỗi một dịch vụ đơn có thể là một hiện tượng không bình thường. Dịch vụ này không khởi tạo được có thể là do dịch vụ mà nó phụ thuộc chưa được khởi tạo. Tình trạng này có thể xảy ra do một số nguyên nhân như truy cập đĩa chậm một cách tạm thời hoặc dịch vụ khác phải kết thúc tiến trình ghi vào file nhật ký trước khi quá trình khởi tạo hoàn tất. Do đó, khi các dịch vụ khác chưa được khởi tạo hoàn toàn thì dịch vụ này vẫn nằm trong tiến trình yêu cầu cho quá trình khởi tạo. Vì vậy, trong lần lỗi đầu tiên bạn nên khởi động lại dịch vụ.

Tuy nhiên, nếu dịch vụ bị lỗi nhiều lần, bạn nên cố gắng khởi động lại một lần nữa hoặc chạy một chương trình cho phép bạn biết được dịch vụ có khởi

tạo được hay không. Nếu không bạn sẽ khởi động lại máy tính để xem sự phụ thuộc thời gian có biến mất hay không.

TỔNG KẾT

- Sau khi hoàn thành quá trình triển khai mạng, một vấn đề rất quan trọng đối với bạn đó là duy trì một cách chủ động các hoạt động trên mạng Windows Server 2003 của bạn.

- Thẻ ***Task Manager Networking*** là một cách nhanh nhất để hiển thị các hoạt động mạng. Bạn có thể thêm các cột vào trang này để hiển thị thêm thông tin.

- Sử dụng bảng điều khiển ***Performance*** để giám sát các hoạt động theo thời gian thực, cấu hình các cảnh báo và tạo các file nhật ký về hiệu năng hoạt động của hệ thống. Màn hình này còn cung cấp các phân tích chi tiết về các mức độ sử dụng tài nguyên hệ thống thông qua việc sử dụng các biến đếm để xác định các nút cổ chai. Màn hình quản trị ***Performance*** cho phép bạn cấu hình để gửi một thông báo sau khi bộ khởi tạo đã được thiết lập.

- Công cụ ***Netstat*** sẽ giúp bạn giám sát lưu thông mạng và câu lệnh ***Netstat –o*** cho phép bạn xác định ***PID*** của tiến trình đang mở một cổng. Sử dụng ***Task Manager*** để hiển thị các tiến trình có PID tương ứng.

- Có hai phiên bản của công cụ giám sát mạng ***Network Monitor***: phiên bản thu gọn và phiên bản chuẩn. Phiên bản thu gọn của ***Network Monitor*** chỉ có thể thu thập được lưu thông gửi tới hoặc từ chính giao diện mạng của nó. Trong khi đó phiên bản chuẩn của ***Network Monitor*** có thể chạy ở chế độ hỗn hợp có nghĩa là nó có thể thu thập 100% lưu thông mạng trên giao diện mạng. Phiên bản chuẩn của ***Network Monitor*** được tìm thấy trên phần mềm ***System Management Server*** (SMS) và có thể thu thập lưu thông giữa các máy tính trên phân đoạn mạng. ***Network Monitor*** cho phép bạn thu thập các gói tin cụ thể từ mạng của bạn để phân tích tình hình hoạt động trên mạng. Bạn có thể cấu hình ***Network Monitor*** để khởi tạo một cảnh báo khi các mẫu cụ thể được đáp ứng hoặc một không gian bộ nhớ đệm xác định được sử dụng.

- Khi chẩn đoán sự cố về kết nối Internet kiểm tra các thiết lập về địa chỉ IP, DNS của máy trạm và các thiết lập về chuyển truy vấn lên máy chủ DNS cấp trên.

- Nếu có lỗi liên quan tới DNS, bạn phải đảm bảo rằng máy trạm đã có thông tin chính xác về máy chủ DNS. Trước hết sử dụng câu lệnh Nslookup để xác nhận rằng máy chủ phản hồi chính xác những gì bạn truy vấn. Kế đó xác nhận tính năng chuyển tiếp các truy vấn lên máy chủ DNS cấp trên (***forwarder***).

- Nút ***Repair*** của một Giao tiếp mạng thực hiện một loạt các bước kiểm tra và các chức năng có thể giải quyết được những lỗi về kết nối.

- Tính năng cấu nối mạng cho phép truy cập từ nhiều mạng giống như thể truy cập từ một mạng duy nhất.

- Một số dịch vụ phụ thuộc lẫn nhau trong quá trình khởi tạo. Bạn có thể kiểm tra tính phụ thuộc trong thẻ ***Dependencies*** của dịch vụ. Các lựa chọn phục hồi dịch vụ cho phép bạn khởi động lại dịch vụ, chạy một chương trình hoặc khởi động lại máy tính sau khi có một hoặc nhiều dịch vụ bị lỗi. Khi chẩn đoán sự cố lỗi dịch vụ, bạn có thể kiểm tra tên người sử dụng, mật khẩu và quyền ***Log On As A Service***. Bạn có thể cấu hình các lựa chọn phục hồi để thông báo cho bạn biết khi một dịch vụ bị lỗi khởi tạo.

BÀI TẬP THỰC HÀNH

CHÚ Ý QUAN TRỌNG *Hoàn thành tất cả các bài tập thực hành*
Nếu bạn lập kế hoạch thực hiện các bài thực hành của quyển sách này thì bạn phải làm tất cả các bài thực hành trong chương này rồi đưa máy tính quay trở về trạng thái ban đầu để kết hợp với các bài lab trong cuốn BÀI TẬP THỰC HÀNH. Bạn cần một máy chủ DNS đã cài đặt để làm bài thực hành 9-2, "Kiểm tra cấu hình hoặc tính năng chuyển tiếp DNS". Nếu DNS chưa được cài đặt, tham khảo bài thực hành 3-1 trong cuốn sách này, "Thêm vai trò DNS cho máy chủ", để cài đặt DNS.

==========

Bài tập thực hành 8-1: Hiển thị Task Manager

Trong bài thực hành này, bạn sẽ sử dụng ***Task Manager*** để hiển thị danh sách các tiến trình đang hoạt động và hiển thị các hoạt động mạng.

1. Đăng nhập với tài khoản ***Administrator***, sử dụng tổ hợp phím ***CTL+ALT+DEL*** rồi nhấp vào ***Task Manager***.
2. Nhấp vào thẻ ***Networking***.
3. Trên thực đơn ***View*** nhấp vào ***Select Columns***.
4. Lựa chọn các biến đếm sau rồi nhấp ***OK***:
    a. ***Network Utilization***
    b. ***Link Speed***
    c. ***State***
    d. ***Unicasts/Interval***
    e. ***Nonunicasts/Interval***
5. Để mở cửa số chế độ dòng lệnh, nhấp ***Start*** -> ***Run*** rồi gõ **cmd** và nhấp ***Ok***.
6. Tại dấu nhắc lệnh, gõ **ping *maytinhgiaovien*** (trong đó ***maytinhgiaovien*** *là địa chỉ IP của máy giáo viên*).
7. Chọn thẻ ***Networking***. Bạn sẽ nhìn thấy hoạt động trên kết nối thông qua các gói tin của câu lệnh ping được gửi đi.

==========

Bài tập thực hành 8-2: Kiểm tra cấu hình của DNS Forwarding

Trong bài thực hành này, bạn sẽ sử dụng thẻ Monitoring để kiểm tra quá trình chuyển các truy vấn lên máy chủ DNS cấp trên.

> **CHÚ Ý *Cài đặt DNS*** *Nếu DNS chưa được cài đặt, tham khảo bài thực hành 3-1 trong cuốn sách này, "Thêm vai trò DNS cho máy chủ", để cài đặt DNS trước khi bắt đầu bài thực hành này..*

1. Đăng nhập với tài khoản ***Administrator***.
2. Nhấp ***Start*** -> ***Administrative Tools*** rồi chọn ***DNS***.
3. Lựa chọn và nhấp chuột phải vào tên máy tính của bạn rồi chọn ***Properties***.
4. Trên trang đặc tính tương ứng, trong thẻ ***Monitoring*** nhấp ***Select A Recursive Query To Other DNS Server.***
5. Nhấp ***Test Now***. Một phản hồi sẽ hiển thị trong hộp ***Test Results***.

==========

Bài tập thực hành 8-3: Cấu hình các dịch vụ

Trong bài thực hành này, bạn sẽ cấu hình tính phụ thuộc của dịch vụ và các lựa chọn phục hồi.

1. Nhấp ***Start***, kích chuột phải vào ***My Computer*** rồi kế đó chọn ***Manage***.
2. Mở rộng ***Service And Applications*** rồi nhấp vào phần ***Services***.
3. Kích đúp vào dịch vụ ***ClipBook***.
4. Trên trang ***ClipB***ook ***Properties*** thay đổi ***Startup Type*** từ ***Disable*** thành ***Automatic*** rồi nhấp ***Apply***.
5. Nhấp ***Start*** để khởi tạo dịch vụ. Một lỗi xuất hiện với dòng thông báo "***Could not Start the ClipBook service on Local Computer. Error 1068: The dependency service or group failed to Start***". Nhấp ***OK***.
6. Trên thẻ ***Dependencies***, hiển thị các dịch vụ mà ***ClipBool*** phụ thuộc. Chú ý rằng các dịch vụ ***Network DDE*** và ***Network DDE DSDM*** phải được khởi tạo do dịch vụ ***ClipBook*** phụ thuộc vào chúng. Nhấp ***Ok*** để đóng trang ***ClipBook Properties*** lại.
7. Xác định dịch vụ ***Network DDE DSDM*** và kích đúp vào nó để hiển thị các đặc tính của nó.

8. Thay đổi ***Startup Type*** từ ***Disable*** thành ***Automatic*** rồi nhấp ***Apply***.
9. Nhấp ***Start*** để khởi tạo dịch vụ. Nhấp ***OK*** để đóng trang ***Network DDE DSDM Properties.***
10. Bây giờ xác định dịch vụ ***Network DDE*** và kích đúp vào nó để hiển thị các đặc tính. Thay đổi ***Startup Type*** từ ***Disable*** thành ***Automatic*** rồi nhấp ***Apply***.
11. Nhấp ***Start*** để khởi tạo dịch vụ. Nhấp ***OK*** để đóng trang ***Network DDE Properties***.
12. Nhấp chuột phải vào dịch vụ ***ClipBook*** và nhấp ***Start*** để khởi tạo dịch vụ ***ClipBook***. Dịch vụ này được khởi tạo.
13. Dừng và vô hiệu hóa các dịch vụ ***Network DDE***, ***Network DDE DSDM*** và ***ClipBook***.

CÂU HỎI ÔN TẬP

1. Bạn nhận được một báo cáo rằng máy tính của một người sử dụng phản ứng chậm với những yêu cầu mạng của người sử dụng. Bạn muốn xem nhanh nhất các loại lưu thông mạng mà máy chủ đang nhận. Bạn sử dụng ***Network Monitor***. Bạn muốn xem có bất kỳ lưu thông quảng bá nào được gửi ra mạng hay không. Bạn sẽ sử dụng biến đếm nào?
   a. ***Nonunicasts/Interval***
   b. ***Unicasts/Interval***
   c. ***Bytes Sent/Interval***
   d. ***Bytes Received/Interval***
2. Bạn thiết lập ***Performance And Alerts*** để gửi một bản tin tới máy tính B để thông báo cho nhân viên điều hành khi mức độ sử dụng dải thông mạng trên máy tính A đạt đến một mức nhất định. Tuy nhiên, máy tính B không hề nhận được bản tin nào từ máy tính A. Bạn phải làm gì để cho phép các bản tin được gửi từ máy tính A tới máy tính B? Chọn tất cả các lựa chọn đáp ứng.
   a. Trên máy tính A, khởi tạo dịch vụ ***Messenger***.
   b. Trên máy tính A, khởi tạo dịch vụ ***Alerter***.
   c. Trên máy tính B, khởi tạo dịch vụ ***Messenger***.
   d. Trên máy tính B, khởi tạo dịch vụ ***Alerter***.

3. Bạn suy đoán máy tính của bạn cài đặt hệ điều hành Windows Server 2003 đã bị nhiễm một con virus. Bạn xác định chắc chắn virus này sẽ truyền dữ liệu từ máy chủ của bạn qua mạng thông qua một cổng nào đó. Bạn muốn xác định xem tiến trình nào đang sử dụng cổng đó. Bạn sẽ sử dụng câu lệnh nào?

   a. ***Nbtstat –RR***

   b. Nbtstat –r

   c. Nbtstat –a

   d. Nbtstat -o

4. Một người sử dụng tại một chi nhánh thông báo rằng anh ta không thể sử Microsoft Internet Explorer để mở một Web site thông dụng trên mạng Internet. Tại máy trạm của bạn ở văn phòng trung tâm, bạn vẫn có thể ***ping*** địa chỉ đích. Bạn sẽ làm gì để khắc phục sự cố này? Chọn tất cả các lựa chọn đáp ứng.

   a. Từ máy tính của người sử dụng, ***ping*** địa chỉ đích

   b. Từ máy tính của người sử dụng, sử dụng tính năng ***Network Repair***

   c. Từ máy chủ ***DNS***, thực hiện một bước kiểm tra truy vấn đơn giản

   d. Từ máy chủ ***DNS***, thực hiện một bước kiểm tra truy vấn đệ quy

5. Một người sử dụng tại một chi nhánh thông báo rằng anh ta không thể sử Microsoft Internet Explorer để mở một Web site thông dụng trên mạng Internet. Tại máy trạm của bạn ở văn phòng trung tâm, bạn chạy ***Nslookup*** để kiểm tra địa chỉ đích và nhận được địa chỉ đúng. Tại máy tính của người sử dụng, bạn cũng chạy ***Nslookup*** nhưng địa chỉ phản hồi không đúng. Bạn sẽ làm gì để khắc phục sự cố này? Chọn tất cả các lựa chọn đáp ứng.

   a. Xác nhận rằng máy trạm khai báo địa chỉ IP của các máy chủ DNS chính xác.

   b. Chạy ***Ipconfig /flushdns***

   c. Chạy ***Ipconfig /registerdns***

   d. Chạy ***Ipconfig /renew***

6. Bạn cài đặt một ứng dung mới và nhận được thông báo nó đang cài đặt một dịch vụ trên máy tính. Tuy nhiên khi bạn cố gắng chạy ứng dụng lần đầu tiên thì nó không thể khởi tạo. Bạn kiểm tra các file nhật

ký để xác định nguyên nhân của lỗi này. Bạn nhận được một lỗi thông báo, "***The service did not Start due to a logon failure***". Bạn cần thực hiện những bước nào để xử lý sự cố này?

a. Xác nhận rằng dịch vụ đã được cấu hình để khởi tạo tự động

b. Thay đổi mật khẩu cùng tên với tài khoản

c. Xác nhận mật khẩu chính xác đã được cung cấp trên trang các đặc tính của dịch vụ

d. Xác nhận rằng tài khoản đã được gán các quyền quản trị

7. Bạn cài đặt một ứng dụng mới trên một máy chủ thành viên. Ứng dụng thông báo rằng nó đang cài đặt một dịch vụ trên máy tính. Quá trình cài đặt dịch vụ yêu cầu một tên và mật khẩu để chạy dịch vụ. Bạn cung cấp tên ***DOMAIN1\Service1***. Tuy nhiên khi bạn cố gắng chạy ứng dụng lần đầu tiên, nó không thể khởi tạo được. Bạn suy đoán rằng tài khoản này chưa được gán các quyền tương ứng để khởi tạo dịch vụ. Bạn sẽ làm gì?

a. Trên máy chủ thành viên, gán cho tài khoản ***Service1*** quyền ***Log On As A Service.***

b. Trên miền, gán cho tài khoản ***Service1*** quyền ***Log On As A Service.***

c. Trên máy chủ thành viên, gán cho tài khoản ***Service1*** quyền ***Log On As A Batch Job.***

d. Trên miền, gán cho tài khoản ***Service1*** quyền ***Log On As A Batch Job.***

8. Một người sử dụng phàn nàn rằng sau khi cô ta khởi động lại máy tính, cô tả không thể truy cập được Internet. Bạn kiểm tra các thiết lập mạng của cô ta và thấy rằng cô ta có một địa chỉ IP nằm trên mạng con sai và địa chỉ gateway mặc định nằm trên mạng dùng cho mục đích kiểm tra. Bạn suy đoán có một máy chủ DHCP giả mạo. Công cụ nào cho phép bạn sử dụng để xác định máy chủ DHCP này?

a. ***Ipconfig***

b. ***Dhcploc***

c. ***Netdiag***

d. ***Netstat***

CÁC KỊCH BẢN TÌNH HUỐNG

==========

Kịch bản 8-1: Sử dụng các công cụ chẩn đoán

Bạn là nhà quản trị mạng cho công ty ABC. Người sử dụng và các nhà quản trị khác thông báo có các vấn đề trục trặc trên mạng. Bạn phải quyết định công cụ chẩn đoán nào sẽ giải quyết một cách tương ứng hầu hết vấn đề này.

Năm vấn đề hỗ trợ khác nhau sẽ được miêu tả. Với mỗi vấn đề, xác định công cụ tương ứng. Lựa chọn từ các công cụ sau. Cung cấp một lý do để minh chứng cho sự lựa chọn của mình. Có thể bạn không cần sử dụng tất cả các lựa chọn trả lời có thể.

Các công cụ xử lý sự cố gồm có:

- Phiên bản chuẩn của ***Network Monitor***
- Phiên bản thu gọn của ***Network Monitor***
- ***Netstat***
- ***Ping***
- Tính năng kiểm tra trong thẻ ***DNS Monitoring***
- Nút ***Network Repair***
- Cầu nối mạng
- Các cấu hình dịch vụ

1. Một người sử dụng ở Hà Nội phản ánh rằng anh ta không thể duyệt Internet được. Bạn yêu cầu anh ta ***ping*** địa chỉ ***gateway*** cục bộ và sau khi thực hiện điều này, anh ta không nhận được một phản hồi thành công từ ***gateway*** cục bộ. Những người sử dung khác trên mạng không gặp phải lỗi này.
2. Tất cả người sử dụng trên mạng của công ty phản ánh rằng họ không thể duyệt Internet mặc dù người sử dụng vẫn nhận được các phản hồi khi họ ping các tài nguyên bên ngoài bằng địa chỉ IP. Truy cập đến các tài nguyên của công ty không hề bị ảnh hưởng.

3. Một nhà quản trị ở Da Nang muốn biết cách tốt nhất để thực thi một phân đoạn mới trên mạng với cấu trúc vật lý khác hẳn. Cô ta không muốn mua một router cứng.
4. Một nhà quản trị ở Da Nang thông báo rằng một dịch vụ của hãng thứ ba trên máy chủ không khởi tạo. Anh ta đã cố gắng để khởi tạo dịch vụ một vài lần nhưng nó vẫn không chạy.
5. Một nhà quản trị tại chi nhánh ở xa nghĩ rằng máy chủ của cô ta bị ảnh hưởng bởi một virus hoặc chương trình "con ngựa thành Trojan". Một cổng xác định xuất hiện trong trạng thái mở. Nhà quản trị phải làm như thế nào để xác định tiến trình nào sử dụng cổng nói trên?