KS : TRƯƠNG HOÀNG VỸ - ĐỨC HÙNG

CĂN BẢN MẠNG KHÔNG DÂY (Wireless)



- Căn bản về xây dựng một mạng không dây (wireless)
- Cách giao tiếp của các máy tính
- Cách hoạt động của nối mạng không dây
- Tìm hiểu các chuẩn nối mạng không dây
- Chọn các thành phần mạng không dây
- Cài đặt trong môi trường Windows XP
- Chia sẻ một máy tính gia đình
- Cài đặt và cấu hình Router không dây
- Truy cập cấu hình Router
- Cài đặt và cấu hình các Adapter không dây
- Việc chia sẻ các tài nguyên mạng
- Ngăn chặn sự truy cập đến các Website
- Tận dụng các HotSpot không dây
- Bảo vệ hệ thống và dữ liệu
- Bảo vệ an toàn mạng không dây
- Bảo vệ mạng không dây

Căn bản mạng không dây (Wireless)

NHÀ XUẤT BẢN HẢI PHÒNG
5 - NGUYỄN KHUYẾN - NGÔ QUYỀN - HẢI PHÒNG
ĐT: 031 8 45970 - 855870 - 921410

CĂN BẢN MẠNG KHÔNG DÂY (WIRELESS)

Chịu trách nhiệm xuất bản:
NGUYỄN THẾ BỈNH
(Giám Đốc Tổng Biên Tập)

Biên tập: Thanh Xuân
Sửa bản in: Hoàng Nhân
Trình bày bìa: Xuân Duyên

Tổng phát hành : Công ty TNHH DỊCH VỤ VĂN HÓA KHANG VIỆT
Địa chỉ :
2bisA Đinh Tiên Hoàng - P.Đakao - Q.1 - TP.HCM
ĐT : 08 9102915 - Fax : 08 9111564

374 Xô Viết Nghệ Tĩnh P.25 – Q.BT – TP.HCM
ĐT: 5117907 – Fax: 8999898
Email: binhthanhbookstore@yahoo.com

In 5.000 bản, khổ 16×24cm, tại Công ty in VIỆT HƯNG. Số đăng ký kế hoạch : 831 – 2007/CXB/31 – 23/HP ngày 12/10/2007 . In xong và nộp lưu chiểu quý IV năm 2007.

KS: TRƯƠNG HOÀNG VỸ

CĂN BẢN
MẠNG KHÔNG DÂY
(WIRELESS)

- *Căn bản về xây dựng một mạng không dây (wireless)*
- *Cách giao tiếp của các máy tính*
- *Cách hoạt động của nối mạng không dây*
- *Tìm hiểu các chuẩn nối mạng không dây*
- *Chọn các thành phần mạng không dây*
- *Cài đặt trong môi trường Windows XP*
- *Chia sẻ một máy tính gia đình*
- *Cài đặt và cấu hình Router không dây*
- *Truy cập cấu hình Router*
- *Cài đặt và cấu hình các Adapter không dây*
- *Việc chia sẻ các tài nguyên mạng*
- *Ngăn chặn sự truy cập đến các Website*
- *Tận dụng các HotSpot không dây*
- *Bảo vệ hệ thống và dữ liệu*
- *Bảo vệ an toàn mạng không dây*
- *Bảo vệ mạng không dây*

NHÀ XUẤT BẢN HẢI PHÒNG

LỜI NÓI ĐẦU

Đối với các gia đình, văn phòng nhỏ, các quán cà phê và khách sạn có nhiều máy tính, sự nối mạng không dây là một phương pháp tuyệt vời để kết nối các máy tính lại với nhau nhằm dễ dàng giao tiếp, trao đổi thông tin, chia sẻ các file và máy in, và thậm chí chơi game trên mạng. Đồng thời đây cũng là một phương tiện thú vị để truy cập Internet và kết nối mọi người trên khắp thế giới lại với nhau.

Chính vì vậy, quyển sách "***Căn bản mạng không dây (wireless)***" được biên soạn nhằm mục đích hướng dẫn tất cả những điểm căn bản về nối mạng không dây, cách xây dựng các mạng không dây và làm thế nào để tận dụng các mạng này một cách hiệu quả. Cụ thể, sách đi vào trình bày cách chọn các thành phần mạng không dây, phân loại các nối kết Internet băng tần rộng, cài đặt trong môi trường Windows XP, tạo tài khoản người dùng, cấu hình các router và adapter không dây, cấu hình mạng gia đình Windows, sử dụng các hotspot không dây, chia sẻ thông tin và các tài nguyên mạng, và các phương pháp an ninh để bảo vệ an toàn mạng không dây.

Sách gồm 13 chương, được bố cục theo các bước tác vụ được đánh số rõ ràng nhằm giúp bạn nhanh chóng tập trung vào những tác vụ cụ thể mà bạn muốn thực hiện ngay. Hy vọng với cách bố cục này và sự trình bày ngắn gọn, quyển sách sẽ thật sự hữu ích cho bạn đọc trong lĩnh vực xây dựng mạng không dây an toàn, đặc biệt là các mạng gia đình và văn phòng nhỏ.

Chúng tôi thật sự rất vinh hạnh nếu nhận được sự góp ý chân tình từ quý bạn đọc. Xin chân thành cảm ơn.

Tác giả

Mục lục

Chương 1: Căn bản về xây dựng một mạng không dây (wireless) 11

Cách giao tiếp của các máy tính 11

Cách hoạt động của nối mạng không dây 13

Tìm hiểu các chuẩn nối mạng không dây 14

Chọn các thành phần mạng không dây 15

Router không dây 16

Các Adapter mạng WiFi 17

Cáp mạng 18

Tận dụng tối đa một mạng gia đình 18

Phân loại các nối kết Internet băng tần rộng 19

Chương 2: Cài đặt trong môi trường Windows XP 21

1. Bàn về môi trường Windows XP 21

2. Định hướng Windows Desktop và Menu Start 23

3. Duyệt tìm các File và Folder 25

4. Bàn về My Network Places 28

5. Sử dụng Control Panel 29

6. Xem Windows Security Center 31

7. Nhận sự trợ giúp trong Windows 33

8. Bàn về Windows Update 34

9. Sử dụng Windows Update 35

Chương 3 : Chia sẻ một máy tính gia đình 38

10. Bàn về việc chia sẻ một máy tính Windows XP 38
11. Tạo một tài khoản người dùng 41
12. Thay đổi ảnh tài khoản 43
13. Bảo vệ tài khoản người dùng bằng password một 45
14. Thay đổi loại tài khoản 47
15. Cấu hình một .NET Passport cho tài khoản người dùng .. 49
16. Đăng nhập Windows 51
17. Chuyển đổi các người dùng 53
18. Xóa một tài khoản người dùng 54

Chương 4: Cài đặt và cấu hình Router không dây 57

19. Bàn về việc cài đặt Router không dây 57
20. Lắp đặt Router 62
21. Bàn về việc cấu hình Router không dây 64
22. Truy cập cấu hình Router 66
23. Bàn về các xác lập Internet 68
24. Cấu hình các xác lập Internet 69
25. Bàn về các xác lập Wireless 71
26. Cấu hình các xác lập Wireless 72

Chương 5: Cài đặt và cấu hình các Adapter không dây 76

27. Bàn về các Adapter mạng không dây 76
28. Quyết định khả năng nâng cấp của các máy tính hiện tại 78
29. Cài đặt một Adapter không dây 82
30. Cài đặt tiện ích phần mềm Adapter 86

31. Kiểm tra việc cài đặt adapter WiFi 88

32. Bàn về việc cấu hình Adapter không dây 90

33. Cấu hình Adapter và kết nối với Router không dây 92

34. Cấu hình adapter để nối mạng từ máy tính này đến máy tính khác 96

35. Tao các Profile cấu hình 99

36. Bàn về việc cập nhật một Driver Adapter 100

Chương 6 : Cấu hình mạng gia đình Windows 103

37. Bàn về việc cấu hình các PC được nối mạng 103

Nối mạng Workgroup 104

Lập địa chỉ IP 105

38. Chạy Network Setup Wizard 108

39. Đặt tên cho máy tính và gia nhập Workgroup 112

40. Mở các thuộc tính nối kết và bật các client, giao thức và dịch vụ 114

41. Thêm một client hoặc dịch vụ mạng 118

42. Cấu hình các xác lập TCP/IP 122

43. Kiểm tra trạng thái Adapter WiFi 124

44. Xác nhận tư cách thành viên Workgroup và truy cập Network Neighborhood 126

Chương 7: Chia sẻ các tài nguyên mạng 128

45. Bàn về việc chia sẻ các tài nguyên mạng 128

46. Chia sẻ một máy in 131

47. Chia sẻ một Folder 133

48. Bàn về việc truy cập các tài nguyên mạng 137

49. Truy cập các Folder chia sẻ và mở các File chia sẻ 138

50. Ánh xạ một ổ đĩa mạng 141

51. Kết nối với một máy in chia sẻ 143
52. Tìm kiếm các máy tính mạng 146
53. Thêm một vị trí mạng 148

Chương 8: Lọc nội dung và mở các dịch vụ Game 151

54. Bàn về việc lọc nội dung và mở các cổng 151
Ngăn chặn nội dung 153
Ngăn chặn các dịch vụ 154
Các vấn đề về chơi Game và sự truy cập Workgroup 157
55. Ngăn chặn sự truy cập đến các Website 158
56. Ngăn chặn sự truy cập đến các dịch vụ Internet 161
57. Thiết lập một thời biểu lọc 165
58. Cấu hình Port Forwarding và Port Triggering 167

Chương 9: Tận dụng các HotSpot không dây 174

59. Bàn về các Hotspot không dây 174
Các tốc độ nối kết Hotspot 176
An ninh hotspot 176
60. Sử dụng Web để định vị các Hotspot 178
61. Phát hiện các hotspot WiFi và kết nối 180
62. Điều chỉnh các tham số nối kết Hotspot 182
63. Bàn về Wardriving 185

Chương 10: Bảo vệ hệ thống và dữ liệu 188

64. Bàn về việc sao lưu dự phòng và phục hồi dữ liệu 188
Phần mềm Backup 190
Phần cứng Backup 193
Các loại sao lưu 195
65. Sử dụng Windows Backup Wizard 197

66. Sử dụng các tính năng sao lưu cao cấp 202
67. Phục hồi dữ liệu được sao lưu 207
68. Tạo một điểm phục hồi hệ thống 210
69. Phục hồi hệ thống 213

Chương 11: Bảo vệ an toàn mạng không dây 218

70. Bàn về an ninh mạng 219
71. Bàn về các Firewall 221
72. Cấu hình các xác lập firewall của router 222
73. Thay đổi Password của Router 226
74. Sao lưu cấu hình Router 228
75. Tắt các Broadcast Server Set ID (SSID) 232
76. Bàn về các chiến lược an ninh 802.11 234
77. Cấu hình an ninh Wired Equivalent Privacy (WEP) 236
78. Cấu hình an ninh WiFi Protected Access (WPA) 241
79. Bàn về các địa chỉ MAC giao diện 244
80. Tạo một danh sách truy cập MAC mạng WiFi 245
81. Cấu hình Remote Management 248

Chương 12: Bảo vệ mạng không dây 252

82. Bàn về Malware 253
Virus 253
Worm và Trojan Horse 255
83. Cài đặt và sử dụng phần mềm chống virus 256
84. Cập nhật phần mềm chống Virus 259
85. Kích hoạt Windows XP Security Center 261
86. Bàn về Malware 265
87. Cài đặt Spyware 266

88. Sử dụng Antispyware 270

89. Bàn về Spam Email và Outlook Express 273

90. Cấu hình các quy tắc Outlook Express 274

Chương 13: Xử lý sự cố và giám sát mạng 279

91. Bàn về các sự cố nối kết mạng 279

Các sự cố phần cứng 280

Các sự cố phần mềm 283

92. Xác lập lại Adapter WiFi 285

93. Kiểm tra trạng thái Router 287

94. Xem các thiết bị được nối kết 291

95. Xem log Router 293

96. Bàn về các công cụ dòng lệnh 295

97. Sử dụng các công cụ dòng lệnh 296

98. Bàn về việc nâng cấp firmware Router và các driver Adapter 299

Chương 1

CĂN BẢN VỀ XÂY DỰNG MỘT MẠNG KHÔNG DÂY (WIRELESS)

Ngày nay, chẳng có gì là lạ khi trong một gia đình hay văn phòng nhỏ mà cũng có nhiều máy tính. Và hầu hết những người dùng gia đình và văn phòng nhỏ để giải quyết các vấn đề nối kết máy tính này sao cho họ có thể chia sẻ các file và những nguồn tài nguyên khác, chẳng hạn như các máy in và một nối kết Internet tốc độ cao.

Bằng chứng của những sự thâm nhập này vào khả năng kết nối máy tính thường rất rõ ràng, đó là các dây mạng bên dưới chân và trên đầu. Một giải pháp tốt hơn là xây dựng mạng không dây (wireless) hoặc WLAN (mạng cục bộ không dây). Với loại mạng này, như không chỉ loại bỏ mọi sự nối cáp mạng mà bạn còn đặt một thiết bị "thông minh", một router không dây để làm trung gian giữa mạng không dây của bạn và nối kết Internet băng tần rộng (broadband).

Chương này sẽ trình bày cách các máy tính giao tiếp với nhau như thế nào và sự nối mạng không dây được thực hiện ra sao. Chương cũng thảo luận các thành phần nối mạng không dây và cách bạn có thể tận dụng tối đa mạng không dây trong văn phòng nhỏ hoặc gia đình.

Cách giao tiếp của các máy tính

Trước khi xem xét sự nối mạng không dây thật sự diễn ra như thế nào, hãy xem xét sơ lược cách các máy tính giao tiếp với nhau trên một mạng. Để các máy tính giao tiếp trên một mạng, phải có một cấu trúc mạng xác định cách dữ liệu di chuyển từ một máy tính qua dây trên một LAN được nối cáp) hoặc tín hiệu không dây (trên một WLAN) như thế nào.

Cấu trúc mạng được sử dụng rộng rãi nhất là Ethernet. Các chuẩn Ethernet định nghĩa cách adapter mạng Ethernet, switch Ethernet, access point Ethernet và những thiết bị Ethernet khác truyền dữ liệu trên mạng. Tốc độ truyền dữ liệu được đo bằng các bit mỗi giây (bps). Một bit là một chữ số nhị phân, 1 hoặc 0 (nó là đơn vị dữ liệu nhỏ nhất, 8 bit tạo nên một byte). Ethernet cung

cấp các tốc độ truyền dữ liệu vượt quá một triệu bit mỗi giây (Mbps). Đối với việc nối mạng, băng thông được xem là số bit được gởi qua phương tiện mạng (chẳng hạn như mạng hữu tuyến hoặc không dây) vào một thời điểm. Do đó các thuật ngữ data transmission speed (tốc độ truyền dữ liệu) và bandwidth (băng thông) thường được sử dụng thay thế cho nhau.

Ethernet là một cấu trúc mạng thụ động, đợi và lắng nghe. Các máy tính phải tranh dành thời gian truyền trên phương tiện mạng. Để nhận dữ liệu, các máy tính chỉ việc ngồi đợi lắng nghe mạng. Khi chúng cảm nhận có một nội dung truyền cụ thể cho chúng, chúng nhận nội dung đó trên adapter mạng của chúng.

Ethernet xử lý việc di chuyển dữ liệu tại cấp phần cứng. Nhưng những người dùng như chúng ta thích làm việc với phần mềm. Phần mềm cung cấp phương pháp giao tiếp với phần cứng của máy tính. Để các ứng dụng phần mềm máy tính khác nhau giao tiếp trên mạng, phải có một số chuẩn phần mềm. Những chuẩn này là các giao thức giao tiếp. Một giao thức (protocol) thật sự là mã phần mềm cung cấp quy tắc cho cách các máy tính giao tiếp với nhau trên phần cứng Ethernet.

THUẬT NGỮ CHÍNH

Protocol (giao thức). Một tập hợp quy tắc phần mềm ấn định các máy tính và những thiết bị khác giao tiếp với nhau như thế nào qua một cấu trúc mạng chẳng hạn như Ethernet.

Giao thức mạng duy nhất cần được thảo luận trong chương này là ngăn xếp giao thức mạng TCP/IP (nó là một ngăn xếp bởi vì nó chứa một số giao thức có các tác vụ khác nhau). Một ngăn xếp giao thức (protocol stack) chẳng hạn như giao thức TCP/IP phải cung cấp một hệ thống địa chỉ và cũng xử lý việc chuyển đổi dữ liệu mà chúng ta tạo trong các ứng dụng phần mềm thành một dạng mà có thể được di chuyển bởi phần cứng Ethernet dưới dạng một luồng bit.

THUẬT NGỮ CHÍNH

TCP/IP (Transmission Control Protocol/Internet Protocol). Ngôn ngữ chung cho thế giới nối mạng. TCP/IP là bộ (hoặc ngăn xếp) giao thức vốn được sử dụng làm nền tảng cho mega-network được gọi là Internet. Hầu như tất cả hệ điều hành máy tính lựa chọn TCP/IP làm giao thức nối mạng mặc định của chúng.

Để làm cho một hành trình dài trở nên ngắn đi, TCP/IP xử lý tiến trình chuyển đổi dữ liệu và cũng cung cấp hệ thống lập địa chỉ cho các máy tính và những thiết bị khác trên mạng. Hệ thống lập địa chỉ gồm các địa chỉ IP. Một địa chỉ IP duy nhất được gán vào mỗi thiết bị trên mạng. Mỗi phần dữ liệu được gởi qua mạng được ghi nhãn bằng các địa chỉ IP của thiết bị gởi và thiết bị nhận, cho phép di chuyển dữ liệu từ điểm A đến điểm B.

Các máy tính và thiết bị trên một mạng TCP/IP có thể có các địa chỉ IP của chúng được cấu hình bằng thủ công hoặc động. Để cấu hình thủ công một máy tính với một địa chỉ IP tĩnh (nghĩa là một địa chỉ vốn không bao giờ thay đổi), bạn cấu hình máy tính với một địa chỉ IP duy nhất và một subnet mask đi kèm (subnet mask giúp những máy tính khác xác định phần nào của địa chỉ là thông tin mạng và phần nào là thông tin riêng của thiết bị).

Lựa chọn thay thế cho việc cấu hình bằng thủ công các thiết bị với một địa chỉ IP và subnet mask (mặt nạ mạng con) là sử dụng một server DHCP (Dynamic Host Configuration Protocol) trên mạng. Server DHCP cho các máy tính và những thiết bị khác trên mạng thuê các địa chỉ IP. Các router không dây (được thảo luận trong một số chương của sách này) có chức năng như các server DHCP, do đó bạn không cần phải gán các địa chỉ IP vào tất cả máy tính trên mạng không dây, router thực hiện điều đó một cách tự động và trong hậu cảnh.

Trong Windows XP (cả phiên bản Home và Professional), địa chỉ IP được cấu hình trong hộp thoại Internet Protocol (TCP/IP) Properties. Bạn có thể cấu hình máy tính Windows XP với một địa chỉ tĩnh (static) hoặc cấu hình nó để chấp nhận một địa chỉ IP từ một server DHCP trên mạng (chẳng hạn như router không dây).



Các máy tính chạy Windows XP có thể được cấu hình với một địa chỉ IP tĩnh hoặc được cấu hình để chấp nhận một địa chỉ IP từ một server DHCP.

TCP/IP xử lý việc giao tiếp mạng tại cấp phần mềm và Ethernet xử lý việc giao tiếp tại cấp phần cứng. Các chuẩn không dây được sử dụng cho các WLAN thật sự là các chuẩn Ethernet. Ethernet không dây sẽ được thảo luận trong mục sau "Tìm hiểu các chuẩn nối mạng không dây" của chương này.

Cách hoạt động của nối mạng không dây

Bây giờ bạn có thể cảm nhận được các máy tính và những thiết bị khác giao tiếp với nhau như thế nào trên một mạng, chúng ta sẽ xem nối mạng

không dây thật sự hoạt động như thế nào. Các nối kết mạng không dây xử lý các tín hiệu vô tuyến và ánh sáng hồng ngoại (những nối kết này có phạm vi hoạt động giới hạn). Các nối kết WiFi giữa các máy tính được bật WiFi và những thiết bị WiFi khác chẳng hạn như các router không dây có phạm vi hoạt động tối đa là khoảng 300 feet.

Đối với nối mạng gia đình và văn phòng nhỏ, phần cứng Ethernet WLAN có sẵn để xử lý nối kết vô tuyến. Thiết bị vận hành trong dãy tần số mà FCC đã dành riêng cho việc sử dụng không kiểm soát, bạn sẽ thấy các LAN không dây vận hành trong các dãy 2.4GHz trở lên.

Sự khác biệt duy nhất giữa một LAN Ethernet (hữu tuyến) và một WLAN Ethernet là WLAN gởi dữ liệu qua các sóng vô tuyến thay vì qua các cáp mạng. WLAN vẫn là một mạng Ethernet đơn giản. Tuy nhiên, Ethernet không dây có tập hợp chuẩn riêng của nó đã được phát triển bởi IEEE (viện kỹ sư điện và điện tử, một tổ chức tiêu chuẩn toàn cầu). Hãy xem xét các chuẩn Ethernet không dây.

Tìm hiểu các chuẩn nối mạng không dây

IEEE đã thiết lập một bộ tiêu chuẩn nối mạng theo các thông số kỹ thuật IEEE 802 (một loạt các thông số kỹ thuật thiết kế cho những thiết bị). Chuẩn trên Ethernet không dây được ấn định là 802.11. Ba loại chuẩn 802.11 hiện được sử dụng cho loại chuẩn nối mạng không dây là:

Ghi chú

Các chuẩn không dây 802.11 còn được gọi là WiFi. Bạn sẽ thường thấy phần cứng 802.11 được ghi nhãn là "các thiết bị WiFi". Nó không phải là một chuẩn không dây khác, chỉ là một bí danh.

- *802.11a. Thông số 802.11 này có thể cung cấp băng thông lên đến 54Mbps và vận hành trong dãy tần số 5GHz của phổ vô tuyến (công cộng) khả dụng. 802.11a chỉ mới bắt đầu thâm nhập vào thị trường nối mạng gia đình và các nhà cung cấp thiết bị không dây chẳng hạn như Linksys đã bắt đầu phân phối các sản phẩm sử dụng thông số kỹ thuật này. Thật là lạ, WiFi 802.11b và 802.11g đã là các chuẩn WiFi có sẵn trước khi 802.11a được thực thi.*
- *802.11b. Thông số kỹ thuật này cung cấp thông lượng lên đến 11Mbps và vận hành trong dãy tần số 2.4GHz. 802.11b là thông số Ethernet không dây có sẵn đầu tiên (năm 1999). Tốc độ một máy tính kết nối với một access point 802.11b giảm đi khi máy tính càng cách xa access point. Chuẩn 802.11b không cung cấp loại phạm vi hoạt động mà bạn có được từ 802.11g. Một khoảng cách 100 feet trở lên giữa access point và máy tính được vận hành WiFi thường không đem lại cường độ tín hiệu đủ mạnh đủ.*

- *802.11g. Thông số kỹ thuật này cung cấp băng thông giữa 20 và 54Mbps trong dây tần số 2.4GHz. Nó hiện là sự thực thi phát triển nhanh nhất của nối mạng không dây cho các mảng gia đình và LAN nhỏ. Thông số kỹ thuật này có thể cung cấp các kết nối tốt giữa các access point và máy tính được vận hành bằng WiFi ở cách nhau lên đến 300 feet.*

Về chi phí, các thiết bị 802.11a đắt nhất và chỉ một vài nhà cung cấp hiện có sẵn các sản phẩm 802.11a dành cho nối mạng gia đình và văn phòng nhỏ. Các sản phẩm 802.11g chắc chắn phổ biến nhất và cung cấp nhiều băng thông nhất tương ứng với chi phí. Bạn thật sự không đi sai đường khi xây dựng mạng của bạn với các thiết bị 802.11g.

Các sản phẩm 802.11b bắt đầu biến mất khỏi các cửa hàng và bạn sẽ thấy hầu hết phần cứng 802.11b được bán hạ giá. Nếu bạn có thể làm việc với tốc độ chậm hơn mà 802.11b cung cấp, bạn có thể lắp ráp một mạng gia đình không dây cho hầu như một bản nhạc. Tuy nhiên, chắc chắn bạn sẽ không có được hiệu suất hoặc phạm vi hoạt động mà bạn có được từ thiết bị 802.11g.

Chọn các thành phần mạng không dây

Nhiều nhà phân phối tung ra thị trường phần cứng WiFi bao gồm các router WiFi, access point và những adapter mạng không dây. Ba trong số các công ty nổi tiếng là Linksys, Netgear và D-Link.

THUẬT NGỮ CHÍNH

Router WiFi. Một thiết bị cung cấp một nối kết cho một mạng gia đình với nối kết Internet tốc độ cao (mà đến lượt nó lại được cung cấp bởi một thiết bị chẳng hạn như modem cáp). Router WiFi cũng cung cấp một access point mà qua đó các máy tính được bật WiFi có thể kết nối với mạng. Các máy tính có các adapter mạng hữu tuyến truyền thống cũng có thể được nối với router WiFi thông qua switch mạng được lắp sẵn vào hầu hết các router WiFi. Router WiFi là một thiết bị thông minh trong đó nó có những cấu hình để đưa ra quyết định về loại truy cập nào được nối kết với Internet tốc độ cao và loại lưu lượng dữ liệu nào có thể được cho phép đi qua router trên mạng cục bộ.

Adapter mạng (network adapter). Một thiết bị cho phép một máy tính gia nhập mạng. Adapter mạng lấy dữ liệu từ máy tính và chuẩn bị dữ liệu để truyền trên qua phương tiện mạng chẳng hạn như cáp mạng hoặc các tín hiệu vô tuyến WiFi.

Bởi vì các thiết bị không dây được sản xuất bởi những công ty này lựa chọn các chuẩn 802.11 nên về lý thuyết tất cả thiết bị sẽ tương thích nhau ngay cả các thiết bị trên mạng không dây của bạn đến từ những nhà cung cấp khác nhau.

Để phân loại các thiết bị WiFi tốt nhất cho mạng không dây của bạn, bạn cần nghiên cứu một chút. Từng nhà cung cấp WiFi có những bước đi riêng của nó trên các chuẩn 802.11.

Ví dụ Netgear đã phát triển MIMO, một chiến lược wireless tận dụng nhiều anten. Các thiết bị MIMO hoàn toàn tương thích với các chuẩn WiFi 802.11g và 802.11b nhưng được quảng cáo là cung cấp phạm vi phủ sóng, vùng hoạt động và tốc độ lớn hơn WiFi chuẩn (nghĩa là 802.11g). Chi phí cho một router MIMO nhiều hơn chi phí của một router không dây 802.11g chuẩn (từ 60 đến 80 đô la trở lên). Do đó, bạn phải quyết định xem sự chênh lệch chi phí có xứng đáng với việc gia tăng hiệu suất đã quảng cáo hay không. Hãy nhớ rằng MIMO là một sự thực thi của 802.11g; đó chính là nhiều anten (MIMO) cung cấp khả năng kết nối tốt hơn giữa các máy tính WiFi và router.

Tài nguyên Web

http://www.linksys.com

http://www.netgear.com

http://www.dlink.com

Bắt đầu tại những site này để tiến hành việc nghiên cứu riêng của bạn trước khi mua các sản phẩm WiFi. Cũng tìm kiếm các bài bình luận về sản phẩm WiFi và xem các chuyên gia WiFi nói gì về những sản phẩm khác nhau.

Điều cốt yếu là có nhiều sản phẩm WiFi khác nhau trên thị trường. Bạn sẽ phải đọc một chút, so sánh các sản phẩm và sau đó đưa ra một số quyết định để lắp ráp mạng WiFi của bạn. Hãy xem những thiết bị WiFi và những thành phần khác mà bạn sẽ cần để xây dựng WLAN gia đình hoặc văn phòng nhỏ của bạn.

Router không dây

Giả sử bạn xây dựng một WLAN chia sẻ một nối kết Internet tốc độ cao, có cả các máy tính không dây và hữu tuyến tham gia trên mạng. Bạn chỉ cần một thiết bị, một router không dây để nhận biết cả ba loại nối kết này.

Router không dây thường có những tính năng sau đây:

- ***Access point không dây***. *Access point là điểm kết nối với WLAN cho các máy tính không dây và những thiết bị khác. Bây giờ hầu hết các router không dây có sẵn hỗ trợ các client 802.11g và 802.11b.*
- ***Switch Ethernet***. *Switch cho phép bạn kết nối các máy tính mạng hữu tuyến với router không dây. Hầu hết các router không dây dành cho việc sử dụng gia đình và văn phòng nhỏ cung cấp bốn cổng LAN Ethernet. Trong hầu hết các trường hợp, bạn cũng có thể kết nối một switch chuyên dụng với router nếu bạn cần nhiều cổng LAN hơn.*

- ***Broadband connector (bộ nối băng tần rộng).*** *Router cũng có chức năng như nối kết của mạng với thiết bị băng tần rộng chẳng hạn như modem cáp hoặc router DSL. Điều này có nghĩa toàn bộ mạng có thể truy cập Internet. Hầu hết các router không dây cũng giúp bảo vệ mạng khỏi sự xâm nhập từ Internet bằng việc cung cấp một firewall (tường lửa).*

Như đã nói trước đó, một số nhà sản xuất bán các router không dây. Đọc các thông số cho những router có sẵn và cũng xem xét những tính năng bổ sung mà router cung cấp. Điều này sẽ giúp bạn chọn đúng router cho mạng gia đình của bạn (và chắc chắn có nhiều router, do đó hãy xem xét giá cả).



Linksys WRT54G Wireless-G Broadband Router là một ví dụ về router không dây.

Các Adapter mạng WiFi

Bạn cũng sẽ cần các adapter mạng WiFi cho các máy tính sử dụng một nối kết không dây với mạng. Hầu hết các máy tính notebook mới được trang bị một adapter WiFi (trong hầu hết tất cả trường hợp, một adapter 802.11g) vốn cũng cung cấp một cổng cho nối kết LAN hữu tuyến.

Nếu bạn cần nâng cấp các máy tính hiện có lên thành WiFi, bạn có hai lựa chọn: Bạn có thể cài đặt adapter WiFi trong một khe mở rộng (expansion slot) trên máy tính (các máy tính desktop và notebook đều có các khe mở rộng mặc dù chúng khác nhau đáng kể) hoặc bạn có thể mua một adapter WiFi và cắm nó vào một cổng USB trống trên máy tính (một máy tính desktop hoặc notebook).

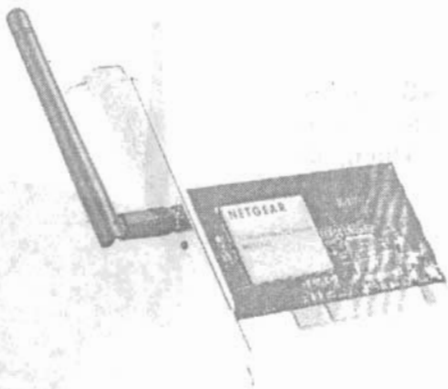
Nếu bạn mua một adapter WiFi để cài đặt vào một khe mở rộng trên máy tính desktop, hãy chắc chắn bạn có một khe PCI trống trong máy tính rồi mới mua một adapter PCI Wireless G.

Để nâng cấp một máy tính notebook cho WiFi, bạn cần một khe PC card loại II còn trống (bạn có thể thay một card LAN hữu tuyến hiện có nếu cần). Các adapter card PC rất dễ lắp đặt bởi vì thật sự chỉ là một vấn đề trượt chúng vào khe trống trên máy tính notebook.

Cáp mạng

Bạn cũng sẽ cần một số cáp mạng để gắn các thiết bị Internet băng tần rộng với router không dây và kết nối bất kỳ máy tính hữu tuyến với các cổng LAN của router không dây. Các cáp mạng Ethernet là các cáp UTP (Unshielded Twisted Pair) Category 5 (CAT 5) có bốn cặp dây xoắn bên trong lớp bọc cáp nhựa. Những cáp này được kết thúc bằng các phích cắm RJ 45. Bạn có thể nghe những loại cáp này được gọi là các cáp Ethernet hoặc các cáp CAT 5.

Mặc dù các cáp CAT 5 có vẻ trông giống như dây điện thoại bình thường, nhưng chắc chắn chúng không phải là cùng một thứ; chỉ việc so sánh phích cắm RJ-45 trên CAT 5 với phích cắm RJ-11 trên cáp điện thoại. RJ-45 thì lớn hơn.



Bạn có thể nâng cấp máy tính desktop cho WiFi bằng cách lắp đặt adapter PCI chẳng hạn như adapter PCI Netgear WG311 54 Mbps.

Bạn sẽ cần một cáp CAT 5 để kết nối router không dây với thiết bị băng tần rộng. Cáp này thường đi kèm với router không dây. Bạn cũng sẽ cần cáp CAT 5 để nối bất kỳ PC "hữu tuyến" với các cổng LAN của router.

Ghi chú

Một loại cáp Ethernet "mới hơn" được gọi là CAT 6 được sử dụng trên các mạng công ty tốc độ cao chẳng hạn như Gigabit Ethernet (vốn đòi hỏi các card mạng và thiết bị mạng đắt tiền chẳng hạn như các switch). Bạn không cần các cáp CAT 6 cho mạng WiFi. Chỉ cần các cáp CAT 5 là đủ.

Tận dụng tối đa một mạng gia đình

Sau khi bạn đã thiết lập mạng không dây (cũng được trình bày chi tiết trong sách này), bạn sẽ muốn chia sẻ các máy in, các file và những nguồn tài nguyên mạng khác, nhất là nối kết Internet tốc độ cao. **Mục 20** và **mục 22** cung cấp cho bạn các bước cần thiết để nối kết router không dây với nối kết Internet. **Mục 45** trình bày chi tiết về cách chia sẻ các máy in và file trên mạng.

Để tận dụng tối đa mạng WiFi gia đình, bạn sẽ muốn bảo đảm xây dựng một mạng an toàn, không xảy ra những xâm nhập an ninh từ bên ngoài mạng. Bởi vì WiFi sử dụng các tín hiệu vô tuyến để truyền dữ liệu, những người có ý

đồ xấu sẽ nghe lén mạng của bạn và thật sự xem dữ liệu. Chúng ta đã đọc về tất cả loại cuộc tấn công khác nhau có thể xảy ra khởi động trên Internet. **Mục 70** là mục mà bạn nên đọc. Bạn sẽ không tận dụng được tối đa phần cứng WiFi nếu bạn liên tục chứng kiến những cuộc xâm nhập trên mạng.

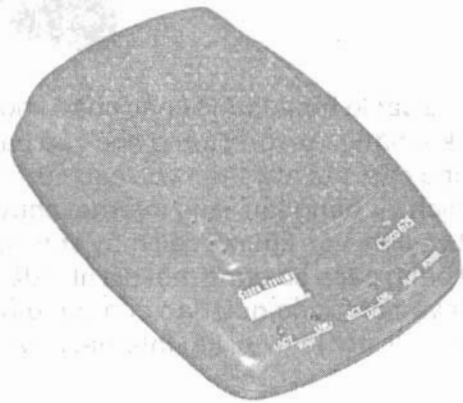
Trang bị cho gia đình hoặc doanh nghiệp nhỏ của bạn một mạng WiFi chắc chắn là một bước đi khôn ngoan. Nó không chỉ giúp những người dùng trên mạng cộng tác dễ dàng hơn mà mạng còn có thể được sử dụng để chơi các game dành cho nhiều người và những nhu cầu giải trí khác.

Phân loại các nối kết Internet băng tần rộng

Nếu bạn chưa sẵn sàng đăng ký một nối kết Internet băng tần rộng (broadband), phần này trình bày một số thông tin cơ bản về băng tần rộng và các ISP (nhà cung cấp dịch vụ Internet). Phụ thuộc vào địa điểm của bạn, bạn có thể có nhiều lựa chọn cho một nối kết Internet băng tần rộng.

Hai loại nối kết băng tần rộng phổ biến nhất được sử dụng trong gia đình và văn phòng nhỏ là DSL (Digital Subscriber Line) và cáp băng tần rộng (cable broadband). DSL cho phép truyền tiếng nói và dữ liệu đồng thời qua các đường dây điện thoại thông thường. Với DSL, bạn có thể nói chuyện trên điện thoại và truy cập Internet cùng thời điểm từ một đường dây điện thoại.

Để đăng ký DSL, hãy liên lạc với nhà cung cấp điện thoại tại địa phương của bạn. Trong nhiều trường hợp, công ty điện thoại cung cấp router DSL để kết nối đường dây điện thoại vào nhà của bạn. Sau đó bạn kết nối router WiFi với router DSL bằng cách sử dụng một cáp mạng truyền thống để thiết lập kết nối với Internet.



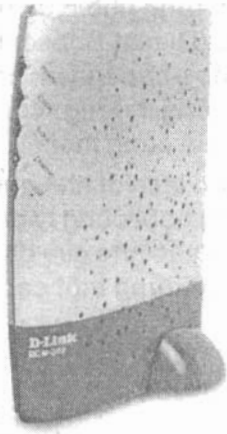
Một router DSL chẳng hạn như router Cisco 675 ADSL được sử dụng làm thiết bị kết nối Internet cho một nối kết DSL tại gia đình.

Các tốc độ nối kết DSL và chi phí dịch vụ thay đổi giữa các nhà cung cấp khác nhau. Các tốc độ xuôi dòng (tốc độ dữ liệu được lấy từ Internet bởi các máy tính trên mạng) trung bình khoảng 1.54 Mbps và các tốc độ ngược dòng (tốc độ dữ liệu được đẩy từ mạng của bạn lên Internet) là từ 256Kbps đến 512Kbps. Để tận dụng DSL, công ty điện thoại tại địa phương phải cung cấp dịch vụ.

Một dịch vụ Internet tốc độ cao thông thường khác là cáp băng tần rộng (cable broadband). Cáp băng tần rộng cáp được cung cấp bởi công ty truyền hình cáp. Dữ liệu được di chuyển trên cùng một cáp với tín hiệu truyền hình. Bởi vì cáp băng tần rộng có các kênh khác nhau, một kênh được sử dụng để truyền dữ liệu ngược dòng và một kênh riêng biệt được sử dụng để truyền dữ liệu xuôi dòng. Như với DSL, các tốc độ nối kết và chi phí khác nhau giữa các công ty cáp. Tốc độ cho những thực thi cáp băng tần rộng gia đình có thể bắt đầu từ 500-700 Kbps xuôi dòng và 128-256 Kbps ngược dòng (có thể đạt được các tốc độ dữ liệu mạnh hơn, nhưng trong hầu hết các trường hợp, bạn có thể phải trả tiền nhiều hơn cho tốc độ dữ liệu nhanh hơn).

Khi bạn đăng ký cáp băng tần rộng, nhà cung cấp dịch vụ sẽ thường cung cấp cho bạn một modem cáp (miễn phí). Thiết bị này không thật sự là một modem nhưng được thiết kế để kết nối với Internet (thông qua cáp truyền hình). Bạn gắn router không dây với modem cáp để chia sẻ Internet với mạng WiFi.

Một modem cáp được sử dụng để kết nối một mạng gia đình với Internet.



DSL và cable broadband chắc chắn không phải là khả năng duy nhất cho một nối kết băng tần rộng trong nhà của bạn. Các dịch vụ truyền hình vệ tinh cũng cung cấp các tùy chọn cho các nối kết Internet băng tần rộng và cũng có các dịch vụ băng tần rộng Internet chuyên dụng chẳng hạn như truy cập Internet vệ tinh, vốn kết nối các máy tính gia đình hoặc doanh nghiệp nhỏ với Internet bằng cách sử dụng một đĩa nhỏ để tiếp vận các tín hiệu dữ liệu thông qua một vệ tinh trong quỹ đạo của trái đất. Có thể đạt được tốc độ lên đến 500 Kbps với một loại nối kết Internet này.

Chương 2

CÀI ĐẶT TRONG MÔI TRƯỜNG WINDOWS XP

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *1. Bàn về môi trường Windows XP*
- *2. Định hướng Windows Desktop và Start Menu*
- *3. Duyệt tìm các file và folder*
- *4. Bàn về My Network Places*
- *5. Sử dụng Control Panel*
- *6. Xem Windows Security Center.*
- *7. Nhận sự trợ giúp trong Windows*
- *8. Bàn về Windows Update*
- *9. Sử dụng Windows Update*

Nối mạng không dây cho bạn truy cập các tài nguyên mạng và các dịch vụ Internet chẳng hạn như World Wide Web một cách nhanh chóng và dễ dàng. Để tận dụng tất cả tính năng mà nối mạng không dây mang lại, bạn cần có một kiến thức vững chắc về cách định hướng giao diện người dùng đồ họa của hệ điều hành Windows XP. Chương này trình bày một cái nhìn tổng quan về định hướng môi trường Windows, định vị các file trên máy tính (và mạng) và truy cập Windows Control Panel.

1. Bàn về môi trường Windows XP

Trước khi bạn bắt đầu	Xem thêm
Nhảy ngay vào!	Mục 45
	Mục 46
	Mục 47

Windows XP chấp nhận một phương pháp tối thiểu trong môi trường làm việc mà nó cung cấp cho những người sử dụng nó. Desktop Windows (được Microsoft gọi là "desktop") trải nghiệm người dùng" về cơ bản ngăn nắp với những biểu tượng, ban đầu cung cấp chỉ một biểu tượng Recycle Bin. Sự truy cập đến các chương trình được cài đặt và các công cụ Windows (chẳng hạn như My Computer, My Network Places và My Documents) được cung cấp bởi menu Start.

Ghi chú

Các biểu tượng desktop thì tùy chọn, bạn có thể thêm các biểu tượng vào desktop nếu bạn muốn trên cơ sở khi cần thiết. Bất kỳ biểu tượng (icon) hiện diện trên menu Start có thể được sao chép và được dán lên trên desktop.

Menu Start xuất hiện theo một dạng hai cột, các ứng dụng được sử dụng gần đây liệt kê trong cột trái (hai biểu tượng được ghim thường trực vào cột trái theo mặc định) và các biểu tượng để truy cập nhanh các file và những công cụ khác chẳng hạn như hệ thống Help được đặt trong cột phải. Truy cập các biểu tượng của ứng dụng mà bạn đã cài đặt trên máy tính chỉ là một thao tác chọn All Programs để mở danh sách All Programs. Sau khi các chương trình mở trên desktop, bạn có thể chuyển đổi giữa nhiều cửa sổ ứng dụng bằng cách nhấp nút ứng dụng của nó trên taskbar (thanh tác vụ).

Bạn có thể pin (ghim) các ứng dụng lên menu khi cần thiết. Nhấp phải bất kỳ biểu tượng ứng dụng được hiển thị trên danh sách All Programs và chọn Pin to Start Menu từ menu ngữ cảnh.



Menu Start cho phép truy cập tất cả ứng dụng và công cụ Windows.

THỦ THUẬT: Để thêm một biểu tượng cho My Documents hoặc My Computer vào desktop, nhấp phải biểu tượng My Documents hoặc My Computer trên menu Start và chọn Show on Desktop từ menu ngữ cảnh.

Mặc dù các biểu tượng có thể được thêm dễ dàng vào desktop, nhưng desktop thật sự được sử dụng làm không gian làm việc (workspace) cho các ứng dụng đang chạy và những công cụ phần mềm khác. Do đó, thay vì thêm

các biểu tượng vào desktop, bạn có thể muốn thêm thanh công cụ Quick Launch vào taskbar. Thanh công cụ Quick Launch có thể là nơi dành cho những biểu tượng thường nằm trên desktop và bạn có thể thêm những biểu tượng khác vào thanh công cụ Quick Launch khi cần thiết. Nhấp phải vào một vùng trống trên taskbar, trỏ vào Toolbars trên menu ngữ cảnh và sau đó chọn Quick Launch để đặt thanh công cụ Quick Launch trên taskbar. Bạn có thể rê bất kỳ biểu tượng từ desktop lên trên thanh công cụ Quick Launch để thêm một bản sao của biểu tượng.

THỦ THUẬT: Nếu taskbar bị khóa, thanh công cụ Quick Launch chỉ hiển thị các biểu tượng đã được đặt trên đó trước khi thanh công cụ bị khóa (bởi vì nó đã được định kích cỡ để chứa biểu tượng gốc đó). Nhấp phải taskbar và chọn Taskbar để xóa dấu kiểm và mở khóa taskbar. Bây giờ bạn có thể rê núm thanh công cụ Quick Launch để tăng kích cỡ của nó và hiển thị tất cả biểu tượng được thêm vào. Sau đó, bạn có thể khóa lại taskbar nếu bạn chọn.

Một vùng khác của desktop nên được đề cập là vùng thông báo (notification). Phần này của taskbar nằm ở phía bên phải và cung cấp thông tin về chương trình đang chạy và những báo động (alert) quan trọng. Ví dụ, khi các bản cập nhật đã được download cho bản cài đặt Windows XP, một hộp thông báo mở ra trong vùng thông báo để cho bạn biết một bản cập nhật sẵn sàng được cài đặt. Vùng thông báo cũng gây sự chú ý đến bạn bởi vì bạn có thể chọn hiển thị các biểu tượng nối kết LAN và WiFi trong vùng thông báo. Những biểu tượng này cho bạn kiểm tra nhanh tốc độ của một nối kết và việc nối kết có hoạt động hay không (đặc biệt hữu dụng trong trường hợp của các nối kết WiFi).

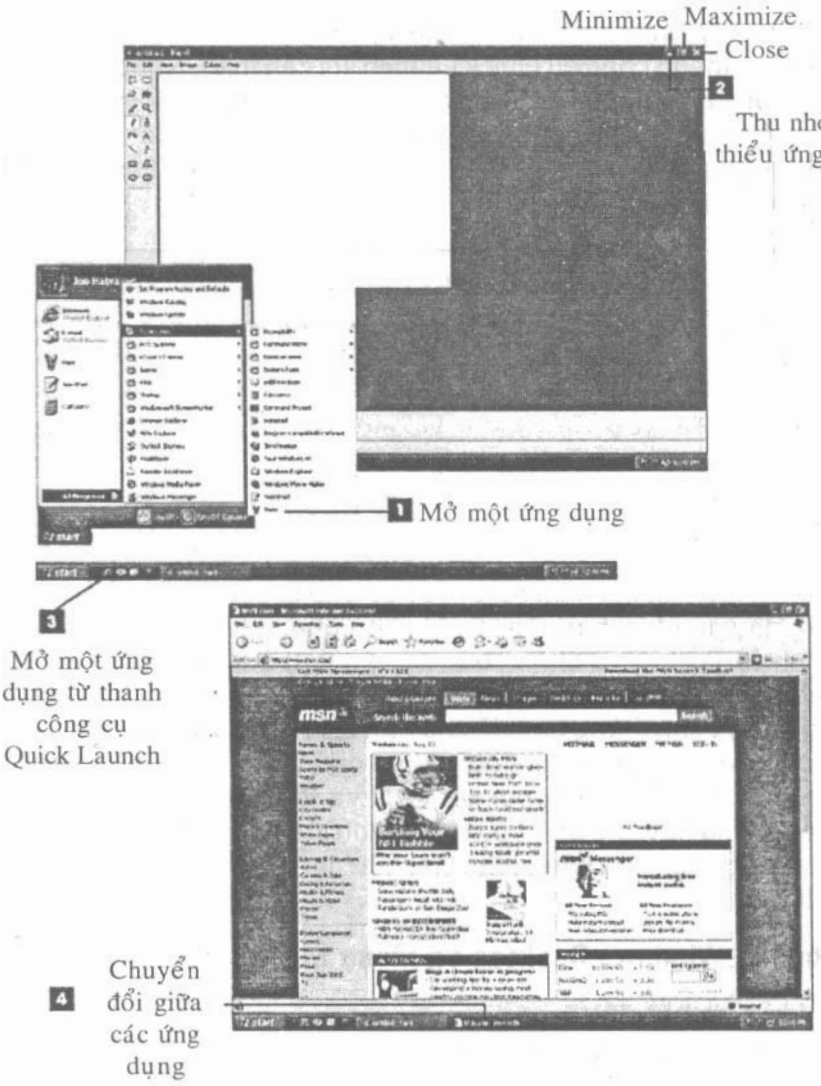
2. Định hướng Windows Desktop và Menu Start

Trước khi bạn bắt đầu

1. Bàn về môi trường Windows XP

Định hướng desktop Windows XP và menu Start thật sự chỉ là việc làm quen với môi trường người dùng Windows. Truy cập dễ dàng các ứng dụng, công cụ và xác lập thường chỉ đòi hỏi hai cú nhấp chuột từ desktop.

2. Định hướng Windows Desktop và Menu Start



1. Mở một ứng dụng

   Chọn menu Start, trỏ vào All Programs, trỏ vào Accessories và sau đó chọn một biểu tượng chương trình từ danh sách các chương trình được cài đặt trên máy tính. Ứng dụng mở trên desktop Windows.

2. Thu nhỏ tối thiểu (minimize) ứng dụng

   Bạn có thể phóng to tối đa (maximize), thu nhỏ tối thiểu (minimize), đóng các cửa sổ ứng dụng và đóng các nút thích hợp ở bên phải phía trên của cửa sổ ứng dụng. Để thu nhỏ tối thiểu ứng dụng và hiển thị desktop, hãy chọn nút Minimize.

THỦ THUẬT: Để nhanh chóng thu nhỏ tối thiểu tất cả ứng dụng đang chạy trên desktop (sao cho bạn có thể thấy desktop), nhấp biểu tượng Show Desktop trên thanh công cụ Quick Launch.

3. Mở một ứng dụng từ thanh công cụ Quick Launch

   Các ứng dụng cũng có thể được khởi động từ thanh công cụ Quick Launch. Để làm điều này, nhấp một biểu tượng ứng dụng trong thanh công cụ Quick Launch chẳng hạn như Internet Explorer để khởi động trình duyệt Web trên desktop.

4. Chuyển đổi giữa các ứng dụng.

   Nếu có nhiều ứng dụng chạy trên desktop, bạn có thể muốn chuyển đổi giữa các cửa sổ ứng dụng. Trong taskbar, nhấp nút trong ứng dụng mà bạn muốn đặt "lên trên cùng". Chuyển đổi giữa các ứng dụng khi cần thiết, sử dụng các nút taskbar cho các ứng dụng.

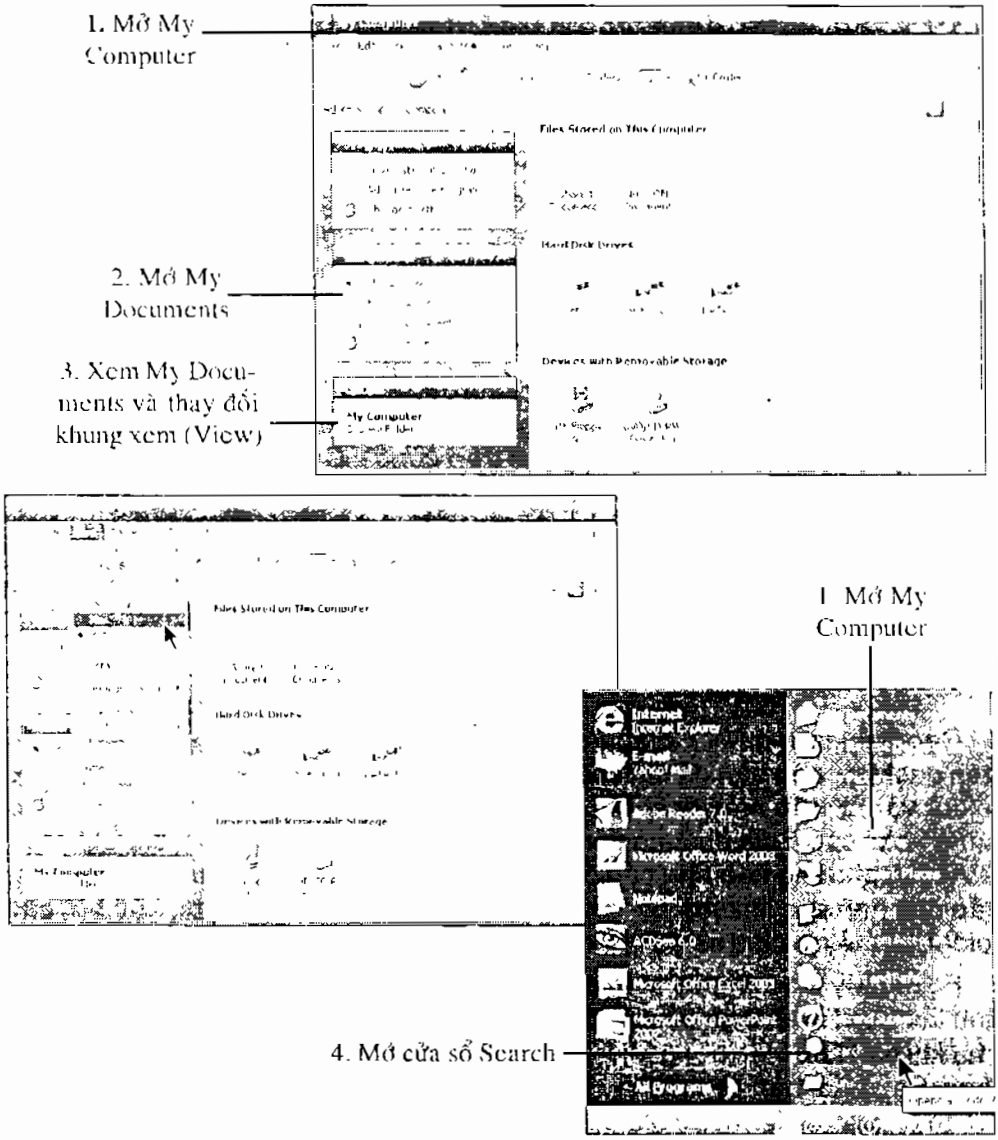
3. Duyệt tìm các File và Folder

Trước khi bạn bắt đầu	Xem thêm
1. Bàn về môi trường Windows XP	**Mục 48**
	Mục 49

Các biểu tượng My Computer và My Documents trên menu Start (hoặc trên desktop, nếu bạn đã đặt chúng ở đó) cho phép truy cập dễ dàng đến các folder và file trên máy tính. My Computer cho phép bạn duyệt nhanh ổ đĩa cứng hoặc các ổ đĩa phương tiện rời khác, chẳng hạn như các ổ đĩa CD hoặc DVD (và phương tiện như các ổ đĩa USB). Cửa sổ My Computer cũng cung cấp cho bạn các link mà bạn có thể sử dụng để truy cập mạng cục bộ, các folder và máy in chia sẻ do những máy tính khác trên mạng cung cấp.

Folder My Documents là folder được sử dụng bởi các ứng dụng trên máy tính làm vị trí mặc định để lưu các file. Do đó khi bạn lưu một file, chẳng hạn như khi bạn làm việc trong Microsoft Word và không thay đổi folder trong hộp thoại Save As, bạn sẽ tìm thấy nó trong My Documents. Nếu bạn không thể tìm thấy một folder hoặc file cụ thể bằng cách duyệt máy tính sử dụng My Computer hoặc My Documents, bạn có thể sử dụng công cụ Windows Search để tìm kiếm một hoặc nhiều file.

3. Duyệt tìm các File và Folder



1. Mở My Computer

Mở cửa sổ My Computer từ menu Start (chọn Start, sau đó chọn My Computer) hoặc bằng cách nhấp đôi biểu tượng My Computer trên desktop. Cửa sổ My Computer hiển thị ổ đĩa cứng của máy tính và bất kỳ ổ đĩa tháo rời được. Để mở ổ đĩa cứng và xem các folder được lưu trữ trên ổ đĩa cứng, hoặc để mở một CD hoặc DVD trong một ổ đĩa tháo rời được, hãy nhấp đôi biểu tượng ổ đĩa thích hợp.

THỦ THUẬT: Nếu bạn đã đặt biểu tượng My Computer trên desktop (nhấp phải My Computer trên menu Start và chọn Show on Desktop để đặt nó ở đó), nhấp đôi biểu tượng desktop để mở cửa sổ My Computer.

2. Mở My Documents

Cửa sổ My Computer cũng cung cấp một loạt các link dọc theo phía bên trái cửa sổ. Để mở folder My Documents, chọn link My Documents trong khung Other Places.

3. Xem My Documents và thay đổi khung xem

Trong cửa sổ My Documents, bạn có thể xem các file mà bạn đã lưu sang folder. Bất kỳ folder mà bạn đã tạo hoặc sao chép sang folder My Documents cũng được liệt kê.

THỦ THUẬT: Bạn có thể tạo nhanh một folder con mới bên trong folder hiện đang mở chẳng hạn như folder My Documents (hay bất kỳ folder khác): chọn File , New, Folder. Trong hộp thoại New Folder vừa mở ra, gõ nhập một tên mới cho folder và nhấp OK.

Khung xem mặc định cho My Documents là Tiles. Khung xem này hiển thị nội dung của folder dưới dạng các biểu tượng lớn (được sắp xếp theo chiều ngang trong cửa sổ). Bạn có thể thay đổi nhanh khung xem nội dung của folder My Documents hay bất kỳ folder hoặc ổ đĩa), chọn View và sau đó chọn một khung xem mới chẳng hạn như Icons. List hoặc Details.

THỦ THUẬT: Bạn cũng có thể sắp xếp các file trong một folder bằng cách sử dụng menu View. Chọn Arrange Icons by và sau đó chọn Name, Size hoặc Modified.

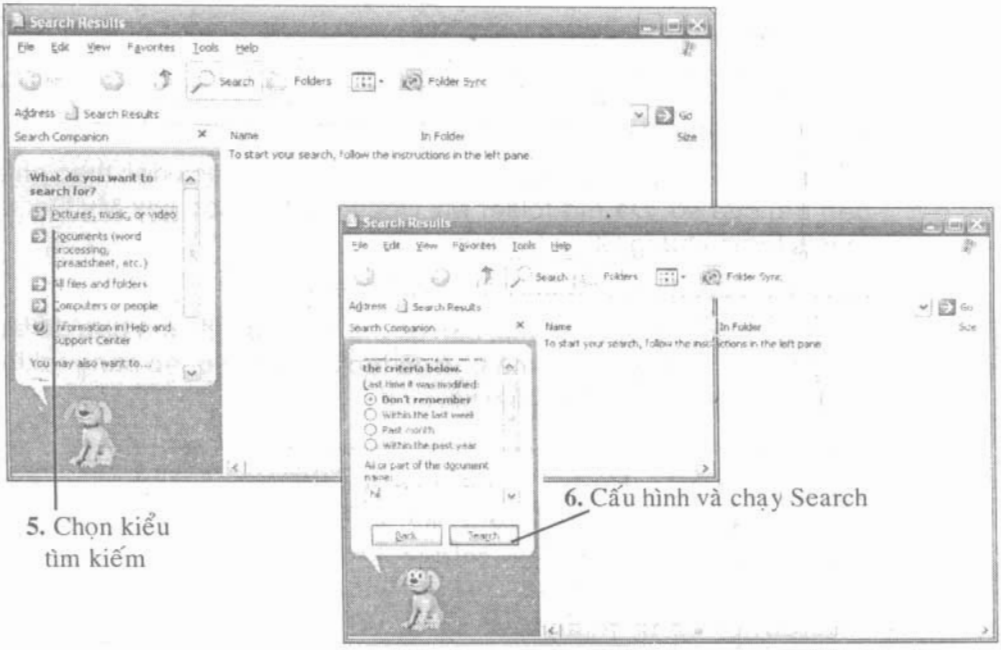
4. Mở cửa sổ Search.

Khi việc duyệt tìm một file cụ thể tỏ ra vô vọng, bạn có thể mở cửa sổ Search và xác lập tiêu chuẩn nhằm giúp định vị file. Để mở cửa sổ Search, chọn Size và sau đó chọn Search.

5. Chọn kiểu tìm kiếm.

Trong cửa sổ Search, chọn kiểu tìm kiếm mà bạn muốn tiến hành trong khung trái của cửa sổ. Nếu bạn tìm các hình ảnh hoặc các file media khác, chọn Pictures, music or video. Nếu bạn tìm các tài liệu ứng dụng chẳng hạn như các tài liệu mà bạn đã tạo với Microsoft Office, chọn Documents (word processing, spreadsheet,...). Để tiến

hành tìm kiếm các file và folder một cách khái quát hơn, chọn liên kết All files and folders.



6. Cấu hình và chạy Search

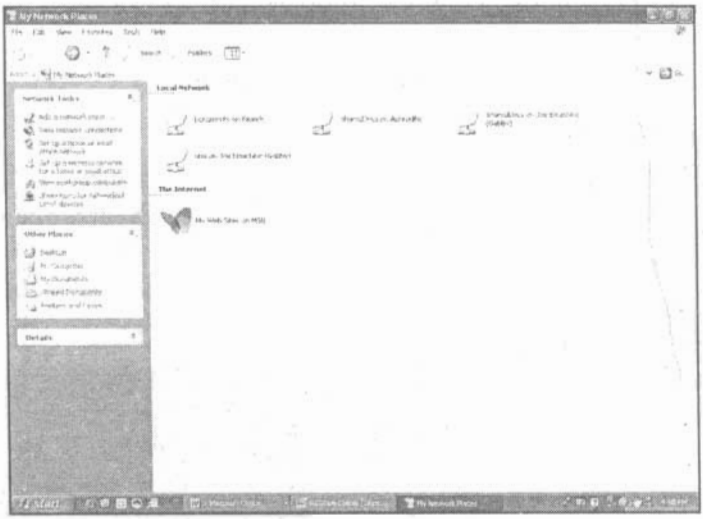
Sau khi chọn kiểu tìm kiếm bạn muốn chạy, nhập tiêu chuẩn tìm kiếm. Ví dụ, khi tìm kiếm tất cả file và folder, bạn có thể nhập một phần của tên file hoặc nhập các từ khóa chứa trong file. Bạn cũng có thể xác định vị trí mà bạn muốn tìm kiếm trong đó. Khi bạn đã nhập xong tiêu chuẩn tìm kiếm, nhấp nút Search. Các kết quả tìm kiếm xuất hiện trong khung phải của cửa sổ Search.

4. Bàn về My Network Places

Trước khi bạn bắt đầu	Xem thêm
2. Định hướng Desktop Windows và menu Start.	Mục 48
	Mục 49

My Network Places là một công cụ duyệt mạng cho phép xem các máy tính được nối kết và truy cập các folder và máy in chia sẻ của chúng. Sử dụng My Network Places nếu bạn kết nối với một mạng cần nguồn tài nguyên (chẳng hạn như một file hoặc máy in) trên một máy tính khác vốn là thành phần của mạng. Bởi vì sách này đề cập đến việc thiết lập và cấu hình một mạng gia đình không dây, bạn sẽ thấy việc quen thuộc với cửa sổ My Network Places sẽ giúp bạn dễ dàng chia sẻ các tài nguyên với những máy tính khác và truy cập các tài nguyên chia sẻ của chúng.

Bạn có thể mở cửa sổ My Network Places (thật sự không phải là một nơi giống như danh sách các máy tính được nối kết và các tài nguyên chia sẻ của chúng) từ menu Start: Chọn Start và sau đó chọn My Network Places. Các máy tính trên mạng chia sẻ các tài nguyên chẳng hạn như các folder được liệt kê trong cửa sổ My Network Places (chúng thường không được liệt kê trừ khi bạn đã truy cập chúng tối thiểu một lần).



My Network Places cung cấp cho bạn một công cụ mạnh mẽ để duyệt mạng cục bộ.

Cửa sổ My Network Places cung cấp các link nhằm cho phép bạn thêm một vị trí mạng (kết nối với một máy tính và nguồn tài nguyên chia sẻ), xem các nối kết mạng, và xem các máy tính workgroup (các máy tính vốn là một phần của mạng gia đình hoặc mạng văn phòng nhỏ). Quan trọng hơn, My Network Places làm cho bạn dễ dàng xây dựng một mạng workgroup sau khi các máy tính khác nhau đã được kết nối với mạng không dây.

5. Sử dụng Control Panel

Trước khi bạn bắt đầu	Xem thêm
1. Bàn về môi trường Windows XP	**Mục 37**

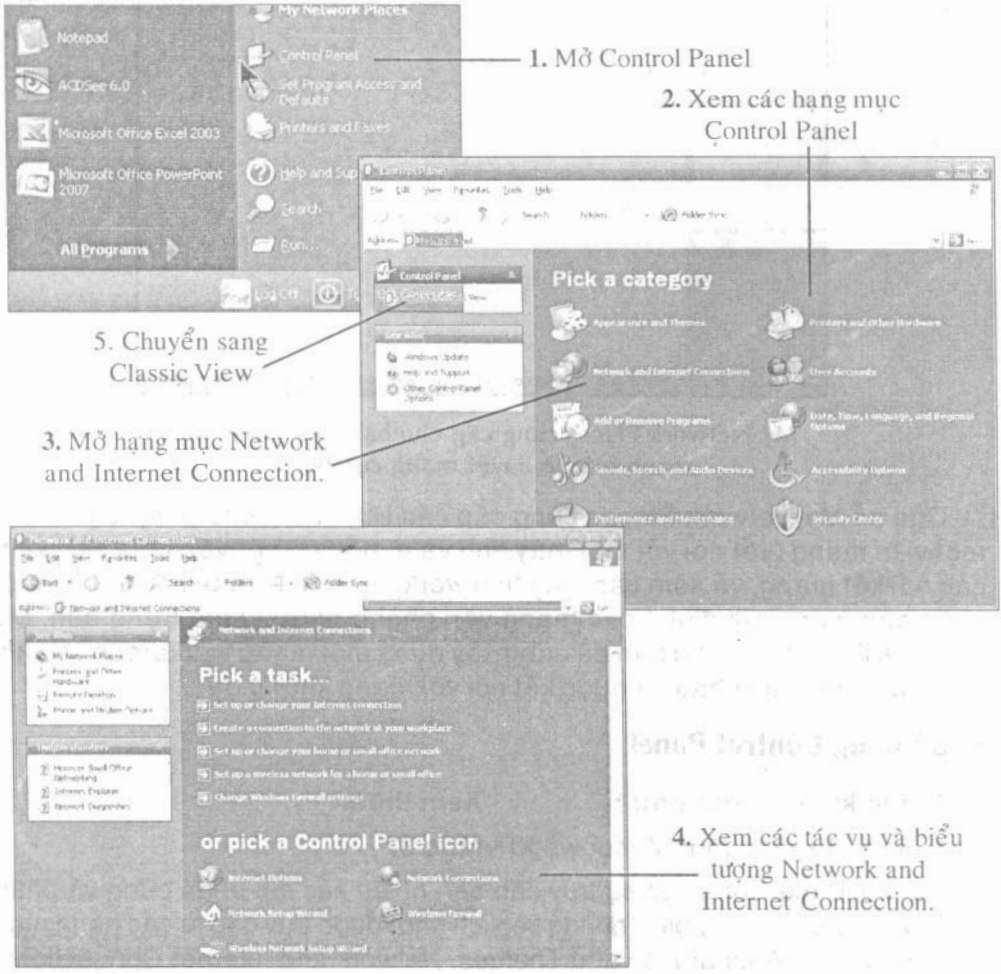
Control Panel cung cấp sự truy cập đến nhiều xác lập phần cứng và phần mềm Windows. Các applet (những tiện ích nhỏ) được truy cập từ các hạng mục chẳng hạn như Appearance and Themes, Network and Internet Connections. Add or Remove Programs, Printers and Other Hardware và User Accounts.

Thuật ngữ chính

Applet. Một tiện ích phần mềm thường được sử dụng để điều khiển các xác lập phần mềm hoặc phần cứng. Hầu hết các applet Windows được truy cập từ Windows Control Panel.

Số applet có sẵn trong một hạng mục (category) phụ thuộc vào hạng mục cụ thể mà bạn chọn. Ví dụ, hạng mục Add or Remove Programs cung cấp một applet, applet Add or Remove Programs cho phép bạn thêm hoặc loại bỏ phần mềm ra khỏi máy tính và thêm hoặc gỡ bỏ các thành phần Windows. Mặt khác hạng mục Network and Internet Connections (quan trọng đối với việc nối mạng một máy tính Windows) cho phép truy cập một số applet chẳng hạn như Internet Options, Network Setup Wizard và Wireless Network Setup Wizard.

5. Sử dụng Control Panel.



1. Mở Control Panel

   Chọn menu Start và sau đó chọn Control Panel.

2. Xem các hạng mục Control Panel

   Khung xem (view) mặc định cho Categories là khung xem Categories. Categories (Các hạng mục) được liệt kê trong khung phải của

cửa sổ Control Panel. Các link bước tắt được cung cấp trong khung trái. Các link bước tắt nào được liệt kê phụ thuộc vào hạng mục mà bạn đã mở trong khung phải của cửa sổ Control Panel.

3. Mở hạng mục Newtwork and Internet Connection

   Hạng mục cung cấp sự truy cập đến các applet để cấu hình nối kết Internet và các xác lập mạng gia đình là hạng mục Network and Internet Connection. Nhấp link Network and Internet Connection trong khung phải của Control Panel.

4. Xem các tác vụ và biểu tượng Network and Internet Connection

   Hầu hết các hạng mục Control Panel cung cấp cho bạn hai cách để làm việc với một xác lập hoặc vấn đề cụ thể. Bạn có thể chọn từ một danh sách các tác vụ (task) hoặc chọn một biểu tượng vốn khởi động một applet cụ thể. Ví dụ, trong hạng mục Network and Internet Connection, bạn có thể chọn một tác vụ chẳng hạn như Set up hay thay đổi nối kết Internet hoặc bạn có thể khởi động applet chẳng hạn như Network Setup Wizard bằng cách nhấp biểu tượng của nó.

   Khi bạn xem xong cửa sổ Network and Internet Connection, quay trở về Control Panel bằng cách nhấp nút Back trên thanh công cụ.

5. Chuyển sang Classic View

   Nếu bạn không thích truy cập các applet Control Panel khác nhau theo các hạng mục, bạn có thể chuyển sang khung xem Classic View. Khung xem này xem xét tất cả các biểu tượng cho applet Control Panel quan trọng. Trong khung trái của Control Panel, nhấp link Switch to Classic View.

THỦ THUẬT: Nếu bạn không thích Classic View, bạn có thể quay trở về khung xem Category. Trong Control Panel, nhấp link Switch to Category View trong khung trái.

---

6. Xem Windows Security Center

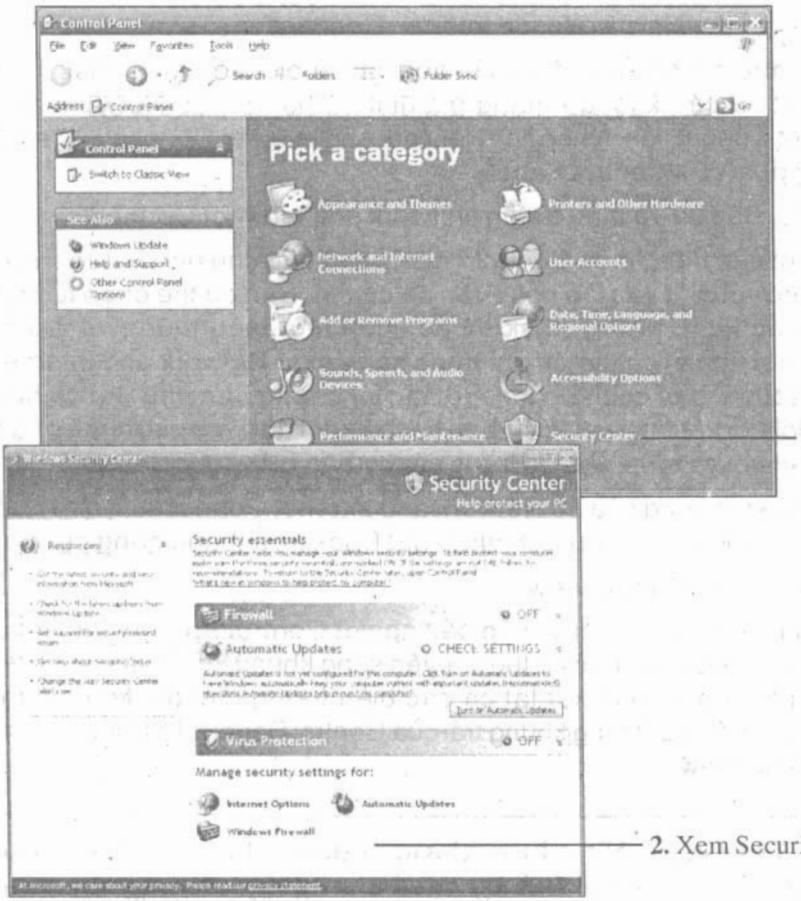
Trước khi bạn bắt đầu	Xem thêm
6. Sử dụng Control Panel	**Mục 71**
	Mục 83

Với những tiến bộ không thể tin được trong sự kết nối và khả năng kết nối máy tính (chẳng hạn như khả năng kết nối Internet và nối mạng không dây) cũng một số rủi ro và sự cố về an ninh). Các virus máy tính mới dường như xuất hiện mỗi ngày và các cracker (những hacker xấu) tìm cách mới để khai thác máy tính nhanh hơn các công ty phần mềm chẳng hạn như Microsoft ngăn chặn các cuộc tấn công.

Bản cập nhật Microsoft Service Pack 2 (SP2) cho Windows XP đã bổ sung Windows Security Center vào hệ điều hành, cung cấp một cách dễ dàng để

bạn giám sát những vấn đề thiết yếu về an ninh chẳng hạn như các bản cập nhật Windows, phần mềm chống virus và Windows Firewall.

6. Xem Windows Security Center



1. Mở Security Center.

   Từ Control Panel, chọn link Security Center (hoặc trong Classic view, nhấp đôi biểu tượng Security Center).

2. Xem Security Center.

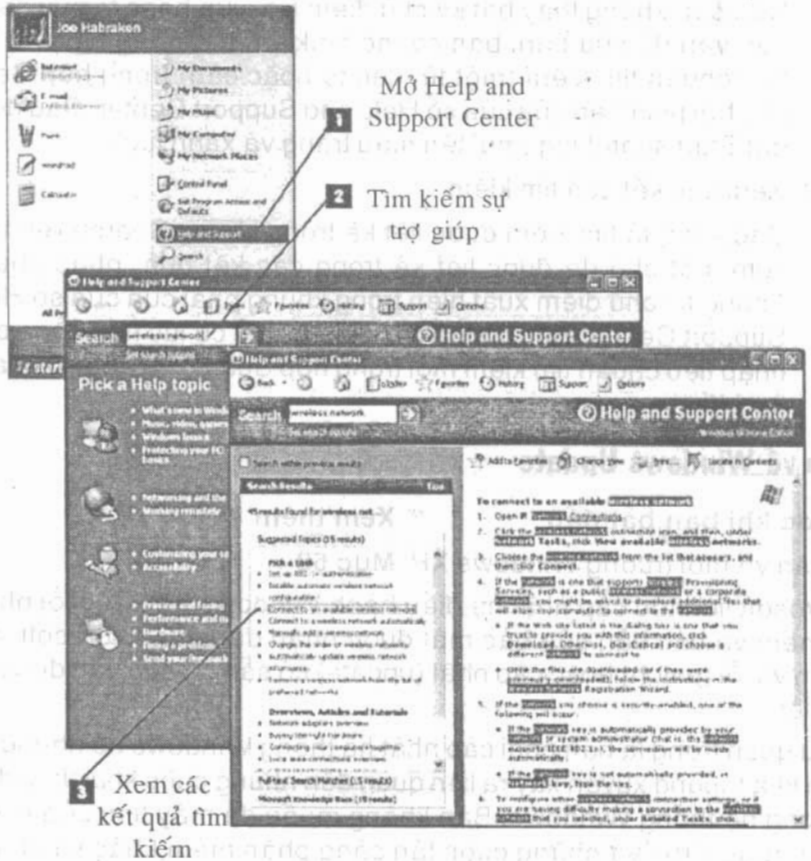
   Security Center cung cấp trạng thái hiện hành của firewall, các bản cập nhật tự động (automatic updates) và việc chống virus. Bạn có thể xem thêm thông tin về tình trạng của một mục bằng cách nhấp nút chuyển đổi ở phía bên phải mục đó.

   Security Center cũng cung cấp các link trong khung trái dẫn đến các tin tức an ninh và virus từ Microsoft và dẫn đến các bản cập nhật tự động Windows Help and Support. Các biểu tượng nằm ở cuối cửa sổ Security Center cho phép truy cập các applet chẳng hạn như Internet Options và Windows Firewall. Khi bạn đã xem xong Security Center, đóng cửa sổ.

7. Nhận sự trợ giúp trong Windows

Cho dù bạn làm việc thành thạo trong môi trường Windows như thế nào, một điều gì đó luôn xuất hiện gây ra những vấn đề hóc búa và đòi hỏi một sự trợ giúp nào đó. Sử dụng cửa sổ Windows Help and Support để chọn lựa từ các chủ điểm trợ giúp và tác vụ khác nhau và để tìm ra thông tin về bất kỳ chủ điểm trong hệ thống Help.

7. Nhận sự trợ giúp trong Windows.



1. Mở Help and Support Center

Chọn menu Start và sau đó chọn Help and Support. Cửa sổ Help and Support Center mở ra, bạn có thể chọn bất kỳ chủ điểm (topic) hoặc tác vụ (task) được liệt kê trong Help and Support Center để đọc sự trợ giúp về vùng chủ đề cụ thể đó.

THỦ THUẬT: Cửa sổ Help and Support Center làm việc rất giống như một cửa sổ trình duyệt Web. Bạn có thể sử dụng các nút mũi tên trong thanh công cụ để di chuyển tới lui. Bạn có thể xem các chủ điểm Help đã được thêm

vào danh sách Favorites bằng cách nhấp nút Favorites trên thanh công cụ. (Để thêm một chủ điểm vào danh sách, nhấp nút Add to Favorites khi bạn xem chủ điểm cụ thể đó). Nếu bạn muốn xem lịch sử của các chủ điểm trợ giúp mà bạn đã xem, nhấp nút History trên thanh công cụ.

2. Tìm kiếm sự trợ giúp

   Nếu bạn không thấy bất kỳ chủ điểm trợ giúp hoặc tác vụ liên quan đến vấn đề của bạn, bạn có thể tìmkiếm hệ thống Help. Gõ nhập tiêu chuẩn tìm kiếm (một từ, các từ hoặc câu) trong hộp Search ở góc trái phía trên của cửa sổ Help and Support Center. Sau đó, nhấp nút Start searching (mũi tên màu trắng và xanh lục).

3. Xem các kết quả tìm kiếm

   Các kết quả tìm kiếm được liệt kê trong khung Search Results. Để xem một chủ đề được liệt kê trong các kết quả, nhấp chủ điểm. Thông tin chủ điểm xuất hiện trong khung phải của cửa sổ Help and Support Center. Bạn có thể tìm kiếm lại bất cứ lúc nào bằng cách gõ nhập tiêu chuẩn tìm kiếm mới trong hộp Search và sau đó chạy cuộc tìm kiếm.

8. Bàn về Windows Update

Trước khi bạn bắt đầu **Xem thêm**

1. Bàn về môi trường Windows XP **Mục 68**

Microsoft liên tục cập nhật hệ điều hành Windows XP. Các lỗi nhỏ trong phần mềm và các bản sửa bảo mật được nhận dạng và Microsoft làm cho một bản vá lỗi (patch) hoặc cập nhật (update) có sẵn để sửa vấn đề vừa được nhận biết.

Điều quan trọng là bạn phải cập nhật hệ thống Windows do những vấn đề an ninh khá thường xuyên xảy ra liên quan đến những cuộc khai thác được tìm thấy trong hệ thống Windows. Bạn không muốn để máy tính của mình phơi mình ra trước virus và những cuộc tấn công phần mềm khác và chắc chắn bạn không muốn làm cho ai đó dễ dàng kết nối bí mật với máy tính của bạn và đánh cắp thông tin, hoặc sử dụng máy tính của bạn tấn công một máy tính khác chẳng hạn như một Web server trên Internet.

Automatic updates chạy trên PC của bạn như thế nào thật sự tùy thuộc vào bạn. Nếu bạn truy cập Windows Security Center từ Control Panel, bạn có thể nhấp biểu tượng Automatic Updates để xem các xác lập hiện hành trong hộp thoại Automatic Updates.



Hộp thoại Automatic Updates cho phép bạn điều khiển khi nào và cách cài đặt các bản cập nhật tự động (automatic updates) trên máy tính.

Trong hộp thoại Automatic Updates, bạn có thể chọn thời gian (và ngày trong tuần) khi các bản cập nhật được download và được cài đặt trên máy tính. Bạn cũng có thể chọn các bản cập nhật được download và được cài đặt bởi bạn (khi bạn muốn cài đặt chúng). Việc tắt automatic updates là một tùy chọn, nhưng làm như vậy có thể để hệ thống của bạn mở ngõ trước cuộc tấn công. Windows thường chạy tốt hơn sau khi bạn cài đặt các bản cập nhật.

Bạn sử dụng automatic updates hay không đều tùy thuộc vào bạn, nhưng có lẽ việc chọ phép các bản cập nhật tự động xảy ra là một thói quen tốt. Khi một bản cập nhật mới được download, bạn sẽ thấy một biểu tượng update trong vùng thông báo Windows (ở góc phải của taskbar). Việc nhấp biểu tượng Update sẽ cho phép bản cập nhật được cài đặt sang máy tính.

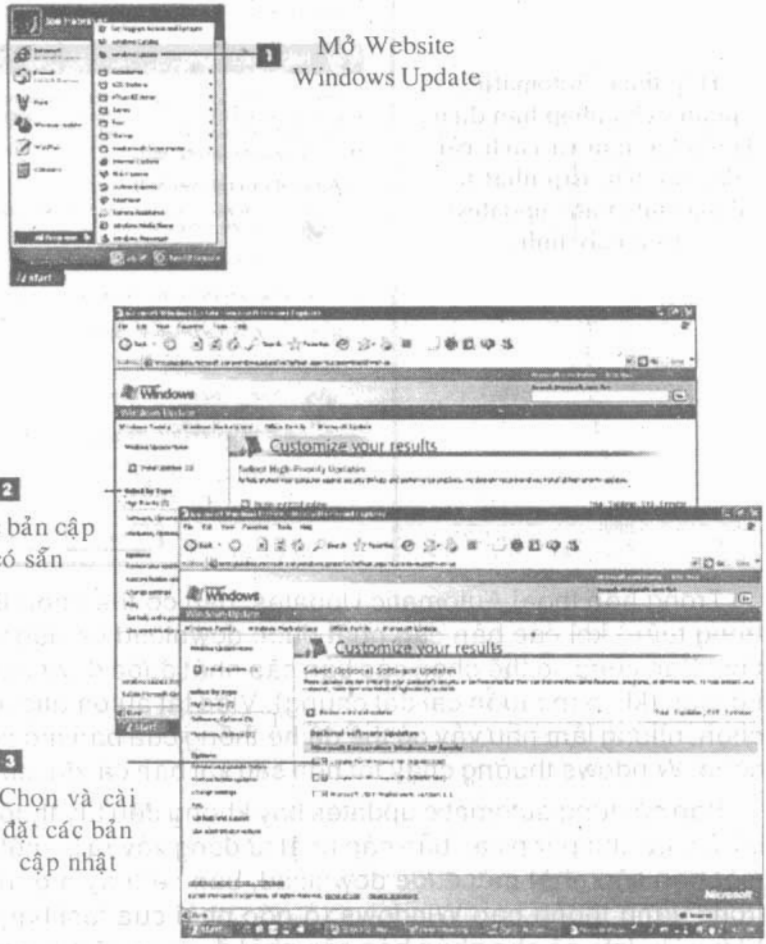
9. Sử dụng Windows Update

Trước khi bạn bắt đầu

8. Bàn về Windows Update

Nếu bạn cấu hình các bản cập nhật để chúng tự động xảy ra, bạn đã chuẩn bị mọi thứ. Tuy nhiên, thỉnh thoảng ghé thăm Website Windows Update và quét hệ thống để tìm các bản cập nhật thì không phải là một ý tồi. Điều này có thể hữu dụng đối với các bản cập nhật không quan trọng chẳng hạn như các driver mới cho các thành phần phần cứng khác nhau hoặc các bản cập nhật của phần mềm Windows, chẳng hạn như Windows Media Player.

9. Sử dụng Windows Update



1. Mở Website Windows Update

Chọn menu Start, trỏ vào All Programs và sau đó chọn Windows Update. Cửa sổ trình duyệt web (thường là Internet Explorer) mở và tải Windows Update. Nếu bạn muốn hiển thị chỉ các bản cập nhật có quyền ưu tiên cao, nhấp nút Express. Nếu bạn muốn xem tất cả bản cập nhật (kể cả các bản cập nhật có quyền ưu tiên thấp liên quan đến các driver và phần mềm), chọn nút Custom.

THỦ THUẬT: Nếu hệ thống của bạn cần được cập nhật phần mềm Windows Update, một cửa sổ xuất hiện, yêu cầu quét máy tính. Một trang mới xuất hiện cho bạn biết rằng các bản cập nhật có sẵn cho phần mềm Update, nhấp nút Download and Install Now. Sau khi phần mềm được cài đặt, nhấp Close (để đóng cửa sổ cài đặt) và sau

đó nhấp Continue. Hệ thống sẽ được quét để tìm các bản cập nhật Windows. Sau khi các bản cập nhật được cài đặt, bạn thường phải khởi động lại hệ thống.

Hệ thống được quét để tìm các bản cập nhật có sẵn, những bản cập nhật đó được liệt kê để bạn lựa chọn (các bản cập nhật nào được liệt kê phụ thuộc vào việc bạn chọn Express hay Custom ở bước 1).

2. Xem các bản cập nhật có sẵn

   Nếu bạn đã chọn Custom ở bước 1, tất cả bản cập nhật có quyền ưu tiên cao (nếu có sẵn) và các bản cập nhật có quyền ưu tiên thấp hơn (phần mềm và phần cứng) được liệt kê theo loại trong khung trái của cửa sổ trình duyệt. Để xem các bản cập nhật trong một hạng mục cụ thể, chọn hạng mục đó.

3. Chọn và cài đặt các bản cập nhật

   Các bản cập nhật trong một hạng mục cụ thể được liệt kê. Để cài đặt một hoặc nhiều bản cập nhật, chọn hộp kiểm của bản cập nhật mà bạn muốn. Sau đó nhấp Review và cài đặt các bản cập nhật. Các bản cập nhật mà bạn đã chọn được liệt kê để cài đặt. Nhấp Install Updates.

   Một hộp thoại Install Updates xuất hiện thể cho thấy độ cài đặt. Khi các bản cập nhật đã được hoàn tất, bạn có tùy chọn để khởi động lại hệ thống hoặc đóng hộp thoại cài đặt và khởi động lại hệ thống vào thời điểm sau đó. Để sự cập nhật thật sự có hiệu lực, bạn cần khởi động lại hệ thống vào thời điểm nào đó.

Chương 3

CHIA SẺ MỘT MÁY TÍNH GIA ĐÌNH

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *10. Bàn về việc chia sẻ một máy tính Windows XP*
- *11. Tạo một tài khoản người dùng*
- *12. Thay đổi ảnh tài khoản*
- *13. Bảo vệ tài khoản người dùng bằng password*
- *14. Thay đổi loại tài khoản*
- *15. Cấu hình một .NET Passport cho tài khoản người dùng*
- *16. Đăng nhập Windows*
- *17. Chuyển đổi các người dùng*
- *18. Xóa một tài khoản người dùng*

Ngay cả trong nhiều hộ gia đình và văn phòng nhỏ có nhiều máy tính (lý do bạn thiết lập mạng không dây), việc chia sẻ một máy tính với những người dùng khác thì không có gì là lạ. Chương này xem xét việc chia sẻ một máy tính với người khác và tập trung vào việc tạo và quản lý các tài khoản người dùng Windows. Chương cũng xem xét tiến trình đăng nhập (logon) và đăng xuất (logoff) hệ thống Windows và chuyển đổi các người dùng.

10. Bàn về việc chia sẻ một máy tính Windows XP

Trước khi bạn bắt đầu

5. Sử dụng Control Panel

Khi bạn cài đặt Windows XP trên một máy tính (hoặc khởi động một máy tính mới lần đầu tiên với Windows XP được cài đặt sẵn), bạn được dẫn dắt qua tiến trình tạo tài khoản người dùng (user account). Tài khoản người dùng

đầu tiên này là tài khoản Computer Administrator cho máy tính. Tài khoản ban đầu có các khả năng quản lý, chẳng hạn như khả năng tạo những user mới (xóa các user) và bảo trì hệ điều hành Windows bao gồm thực hiện các thay đổi đối với những xác lập hệ thống và gỡ bỏ phần mềm và phần cứng.

Ghi chú

Bởi vì chủ đề của sách này là xây dựng một mạng không dây gia đình, các bước và hình ảnh được minh họa cho những người dùng ấn bản Windows XP Home. Tuy nhiên, trong hầu như tất cả trường hợp, nội dung cũng thích hợp cho những người dùng ấn bản Windows XP Professional.

Khi chỉ có một tài khoản trên một máy tính Windows XP (tài khoản ban đầu được tạo ngay sau khi cài đặt hệ điều hành Windows). Bạn được đưa trực tiếp đến desktop Windows sau tiến trình khởi động. Hành vi này cũng được quy cho là tài khoản ban đầu được tạo không có password. Do đó hệ thống của bạn thật sự an toàn bởi vì nó tự động khởi động sang một và chỉ một tài khoản người dùng mà ngẫu nhiên có những khả năng quản lý. Bạn xác định tên cho tài khoản lần đầu tiên bạn sử dụng Windows và bước qua tiến trình tạo tối thiểu một tài khoản người dùng và kích hoạt Windows trên Internet. Điều này có nghĩa rằng tài khoản quản lý (tài khoản mà bạn đã đặt tên) không được bảo vệ bằng password. Bạn nên tạo một password cho tài khoản người dùng quản lý để cung cấp một sự an ninh cơ bản cho máy tính đối với những ai có thể đăng nhập vào hệ thống của bạn. Nếu những người dùng khác cần truy cập, bạn nên tạo các tài khoản người dùng cho họ.

THỦ THUẬT: Nếu bạn phải mắc công tạo một password cho tài khoản quản trị (administrator) của máy tính, đừng đưa password của bạn cho những người dùng máy tính khác. Tạo một tài khoản cho mỗi người dùng (bạn nên tạo một tài khoản limited nhằm "giới hạn" người dùng về việc cài đặt phần mềm và thay đổi các xác lập cho những người dùng khác. Sau đó mỗi người dùng tự quyết định xem mình có muốn bảo vệ bằng password tài khoản riêng của mình hay không. Thậm chí các tài khoản limited có thể tạo và thay đổi các password riêng của mình.

Bởi vì tài khoản người dùng ban đầu trên hệ thống Windows được tạo với các khả năng quản lý, người dùng này (bạn) nên tạo thêm bất kỳ tài khoản người dùng. Nếu nhiều người sử dụng một máy tính, mỗi người dùng nên có tài khoản riêng của mình. Có những lợi ích cho mỗi người dùng có tài khoản riêng của mình, thậm chí không xem xét đến vấn đề an ninh. Ví dụ, mỗi người dùng có thể cá nhân hóa desktop Windows bao gồm các font, nền desktop và các biểu tượng desktop.

Ghi chú

Một tài khoản Guest cũng được tạo khi bạn cài đặt Windows XP trên máy tính. Theo mặc định, tài khoản Guest được tắt. Nó được thiết kế để cho người dùng tạm thời truy cập một máy tính dưới dạng "Guest" (khách). Tài khoản Guest có thể được mở và tắt bởi một người dùng tài khoản Computer Administrator. Khi tài khoản Guest được mở, biểu tượng Guest xuất hiện trên màn hình Windows Welcome và khách (Guest) có thể đăng nhập mà không cần password.

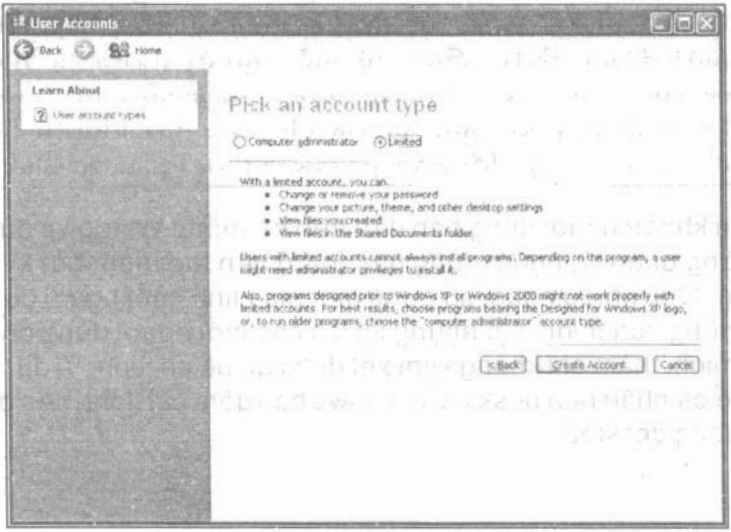
Có hai loại tài khoản người dùng mà bạn có thể tạo. Bạn có thể tạo các tài khoản người dùng vốn là nhà quản trị máy tính được chỉ định (như tài khoản ban đầu của bạn) hoặc bạn có thể tạo các tài khoản giới hạn (limited). Loại limited không thể thêm, xóa hoặc biên tập các tài khoản người dùng. Một người dùng limited cũng không thể thay đổi các xác lập toàn hệ thống hoặc cài đặt phần mềm và phần cứng. Bạn quyết định loại tài khoản người dùng khi bạn tạo tài khoản và bạn có khả năng thay đổi một tài khoản hiện có từ nhà quản trị máy tính (computer administrator) thành Limited nếu được yêu cầu.

THUẬT NGỮ CHÍNH

Computer administrator. Một tài khoản người dùng Windows vốn có thể thay đổi các xác lập hệ thống, thêm và gỡ bỏ phần cứng và phần mềm, tạo và biên tập các tài khoản người dùng khác.

Limited user. Một tài khoản người dùng không có các khả năng quản lý. Người dùng này có thể thay đổi các xác lập deskop và thay đổi password và ảnh tài khoản người dùng của mình.

Các tài khoản người dùng có thể được ấn định là computer administrator hoặc limited.



Nếu bạn sử dụng tài khoản quản trị và tạo các tài khoản người dùng mới, bạn phải cung cấp tên cho những tài khoản đó (**xem mục 11**).

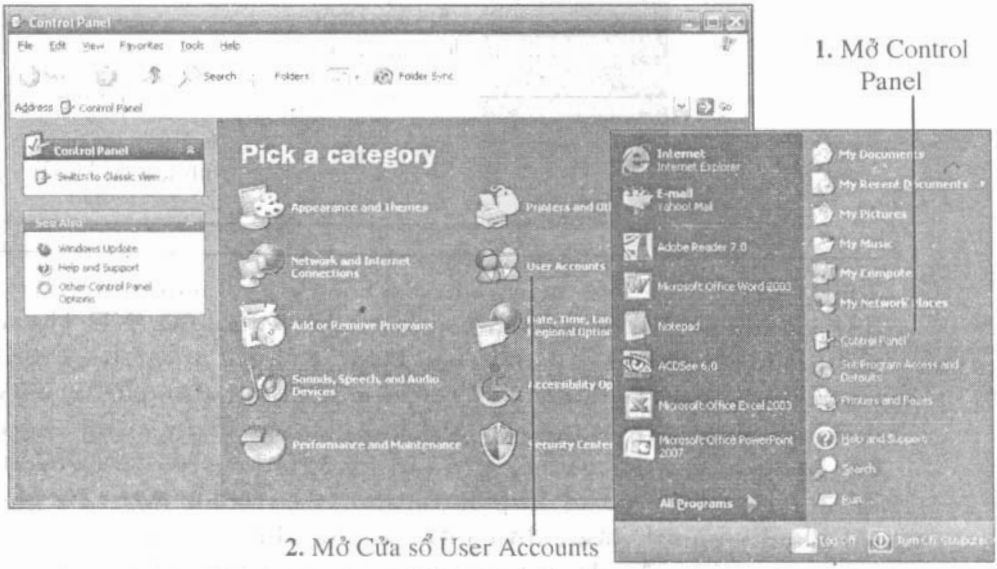
11. Tạo một tài khoản người dùng

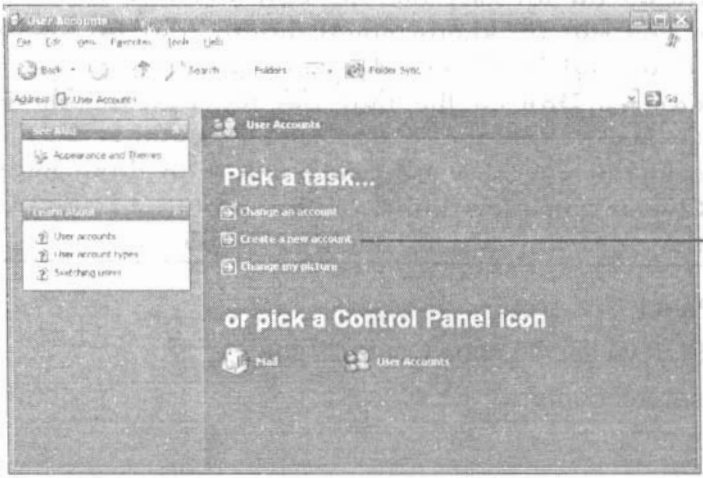
Trước khi bạn bắt đầu

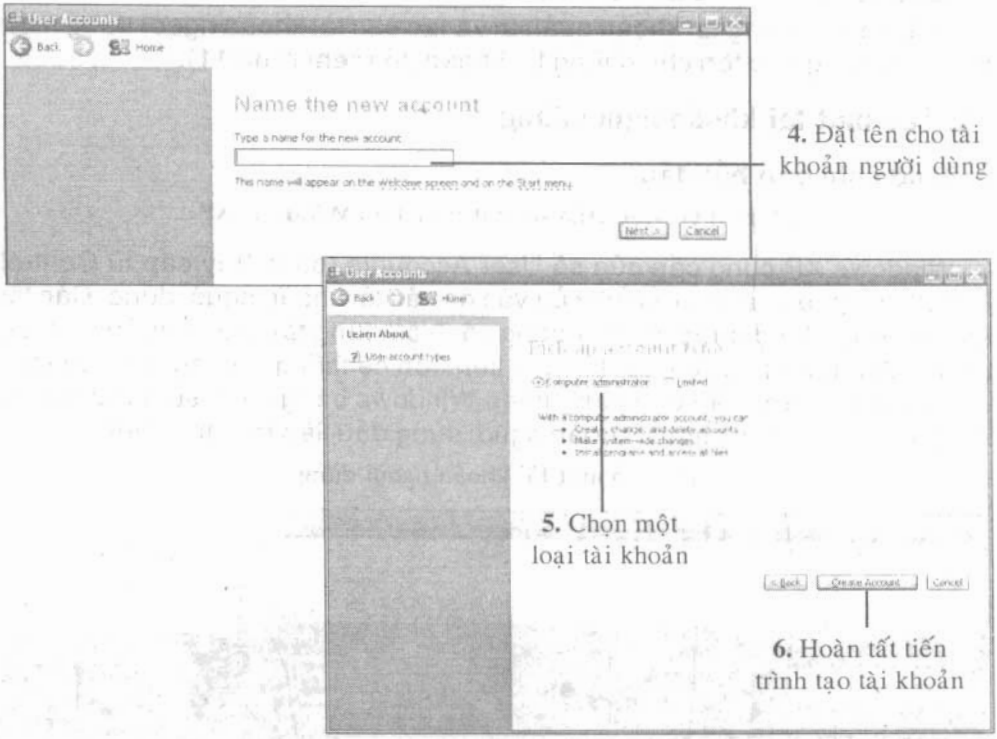
10. Bàn về việc chia sẻ một máy tính Windows XP

Windows XP cung cấp cửa sổ User Accounts (được truy cập từ Control Panel) cho phép bạn tạo, chỉnh sửa và xóa các tài khoản người dùng. Các tài khoản người dùng được quản lý bằng cách sử dụng tài khoản quản trị được tạo khi Windows được cài đặt lần đầu tiên trên hệ thống. Để làm việc qua tác vụ này, hãy chắc chắn bạn đăng nhập Windows bằng cách sử dụng tên tài khoản được ấn định cho tài khoản người dùng đầu tiên trên máy tính.

11. Tạo một tài khoản người dùng







THỦ THUẬT: Khi bạn mua một máy tính mới được cài đặt Windows XP hoặc khi bạn cài đặt Windows XP Home Edition trên một máy tính mà bạn sở hữu, bạn được bắt buộc thiết lập tối thiểu một tài khoản người dùng trên máy tính lần đầu tiên Windows XP khởi động. Bạn cũng được bắt buộc kích hoạt và tùy ý đăng ký Windows với Microsoft. Trong một số trường hợp hiếm hoi, tiến trình đặt tên cho tài khoản người dùng đầu tiên có thể được bỏ qua (ví dụ, nếu người nào đó đã tắt máy tính khi bạn làm việc qua các bước đặt tên cho một tài khoản người dùng). Một tài khoản người dùng được gọi là Owner được tạo tự động. Đây là tài khoản quản trị. Bạn có thể thay đổi tên của tài khoản này (nếu bạn muốn) trong cửa sổ User Accounts. Bởi vì Owner là tài khoản duy nhất trên máy tính, bạn đăng nhập với quyền Owner cho đến khi bạn tạo những tài khoản khác hoặc thay đổi tên của tài khoản Owner.

1. Mở Control Panel

   Nhấp menu Start và sau đó chọn Control Panel.

2. Mở cửa sổ User Accounts

Trong Control Panel, nhấp biểu tượng User Account. Cửa sổ User Accounts mở ra; nó cung cấp cho bạn các công cụ để tạo, chỉnh sửa và xóa các tài khoản người dùng. Bạn có thể chọn một tác vụ (task) để truy cập một công cụ cụ thể hoặc chỉnh sửa một tác vụ hiện có bằng cách nhấp biểu tượng cho tài khoản đó.

3. Tạo một tài khoản mới.

   Trong cửa sổ User Accounts, chọn một tác vụ Create a new account task. Một loạt các màn hình như một user sẽ dẫn dắt bạn qua tiến trình tạo những tài khoản mới.

4. Đặt tên cho tài khoản người dùng.

   Trong màn hình đầu tiên, gõ nhập một tên cho tài khoản người dùng. Tên tài khoản người dùng có thể gồm 20 ký tự (chữ hoa, chữ thường hoặc kết hợp cả hai, kể cả các khoảng trống). Bạn không thể sử dụng ký tự đặc biệt sau đây:

   " / \ [ ] : ; | = , + * ? < >

   Sau khi gõ nhập tên tài khoản, nhấp Next.

5. Chọn một loại tài khoản.

   Trên màn hình kế tiếp, chọn một loại tài khoản: Computer administrator hoặc Limited. Các tài khoản Computer administrator có toàn bộ quyền điều khiển các xác lập của máy tính. Các tài khoản limited có những khả năng giới hạn trong việc thay đổi các xác lập và chọn loại phần mềm. Chọn loại tài khoản nào tùy thuộc vào mức độ cấu trúc mà bạn cần.

THỦ THUẬT: Nếu mọi tài khoản mà bạn tạo cho Windows XP là Computer administrator, bạn đang thiết lập một môi trường điện toán cực kỳ rối loạn và hỗn độn. Hãy xem xét có chỉ một tài khoản Computer administrator (tài khoản riêng của bạn) và sau đó tạo tất cả tài khoản khác dưới dạng limited.

---

6. Hoàn tất tiến trình tạo tài khoản

   Để hoàn tất tiến trình tạo tài khoản, nhấp Create Account. Bạn quay trở về cửa sổ User Account. Một biểu tượng mới xuất hiện trên màn hình tượng trưng cho tài khoản mới được tạo.

12. Thay đổi ảnh tài khoản

Trước khi bạn bắt đầu

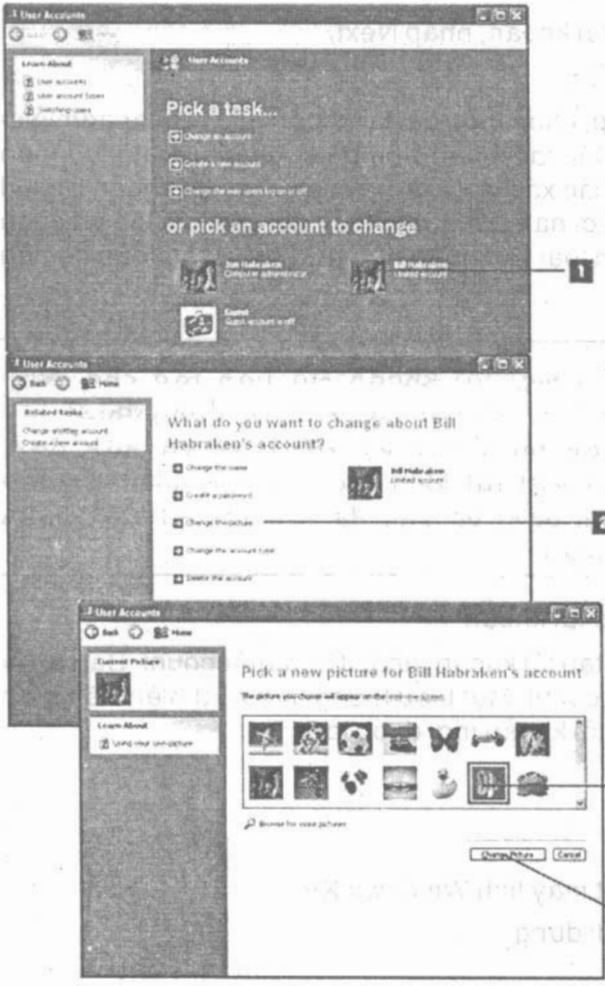
10. Bàn về việc chia sẻ một máy tính Windows XP.
11. Tạo một tài khoản người dùng

Sau khi một tài khoản người dùng đã được tạo, bạn có thể chỉnh sửa các thuộc tính khác nhau của nó chẳng hạn như loại tài khoản và ảnh tài khoản. Ảnh tài khoản là ảnh được sử dụng để tượng trưng cho tài khoản trên màn hình Windows Welcome. Ảnh của người dùng hiện được đăng nhập cũng xuất hiện trên menu Start và trong cửa sổ User Accounts.

Một ảnh mặc định (các con cờ tướng) được chọn tự động khi bạn tạo một tài khoản mới. Bạn có thể thay đổi ảnh tài khoản thành bất kỳ ảnh nào được cung cấp bởi Windows XP. Bạn cũng có thể sử dụng những bức ảnh kỹ thuật số riêng của mình (từ một camera kỹ thuật số hoặc máy scan) hay bất kỳ bức ảnh mà bạn sao chép hoặc download từ Web.

Một người dùng có thể thay đổi ảnh tài khoản người dùng của mình cho dù tài khoản là một tài khoản quản trị (administrator) hoặc giới hạn (limited). Những người dùng có các tài khoản quản trị cũng có thể thay đổi ảnh cho những tài khoản người dùng khác (một lý do tốt khác để có chỉ một tài khoản administrator).

12. Thay đổi ảnh tài khoản.



1. Chọn một tài khoản người dùng

Giả sử bạn sử dụng tài khoản Computer administrator. Trong cửa sổ User Accounts (chọn User Accounts trong Control Panel để truy cập cửa sổ này), nhấp tài khoản người dùng mà bạn muốn thay đổi ảnh. Danh sách tác vụ cho tài khoản được chọn mở ra.

Ghi chú

Những người dùng có các tài khoản Limited không thấy những tài khoản người dùng khác được cài đặt trên máy tính khi họ nhấp User Accounts trong Control Panel. Những người dùng có các tài khoản Limited được đưa trực tiếp đến màn hình tác vụ riêng để cung cấp cho người dùng khả năng tạo một password hoặc thay đổi password (hoặc thay đổi ảnh tài khoản).

2. Chọn Change the Picture

Chọn tác vụ Change the Picture. Một hộp Picture mở ra, hiển thị các ảnh có sẵn.

3. Chọn một ảnh mới

Cuộn qua các ảnh trong hộp danh sách. Nhấp ảnh mà bạn muốn sử dụng cho tài khoản hiện được chọn.

THỦ THUẬT: Để sử dụng một ảnh kỹ thuật số mà bạn đã tạo bằng một camera kỹ thuật số hay máy scan hoặc đã sao chép từ Web, nhấp tùy chọn Browse for more pictures bên dưới hộp picture. Hộp thoại Open mở ra. Duyệt để tìm file ảnh trên đĩa cứng của máy tính. Khi bạn đã tìm thấy ảnh, chọn nó và nhấp nút Open. Bạn được đưa trở về danh sách tác vụ của tài khoản và ảnh mới được hiển thị dưới dạng ảnh của tài khoản.

4. Thay đổi ảnh

Sau khi chọn ảnh mà bạn muốn sử dụng, nhấp nút Change Picture, bạn được đưa trở về danh sách tác vụ của tài khoản và ảnh tài khoản được thay đổi thành ảnh mà bạn chọn.

13. Bảo vệ tài khoản người dùng bằng password một

Trước khi bạn bắt đầu

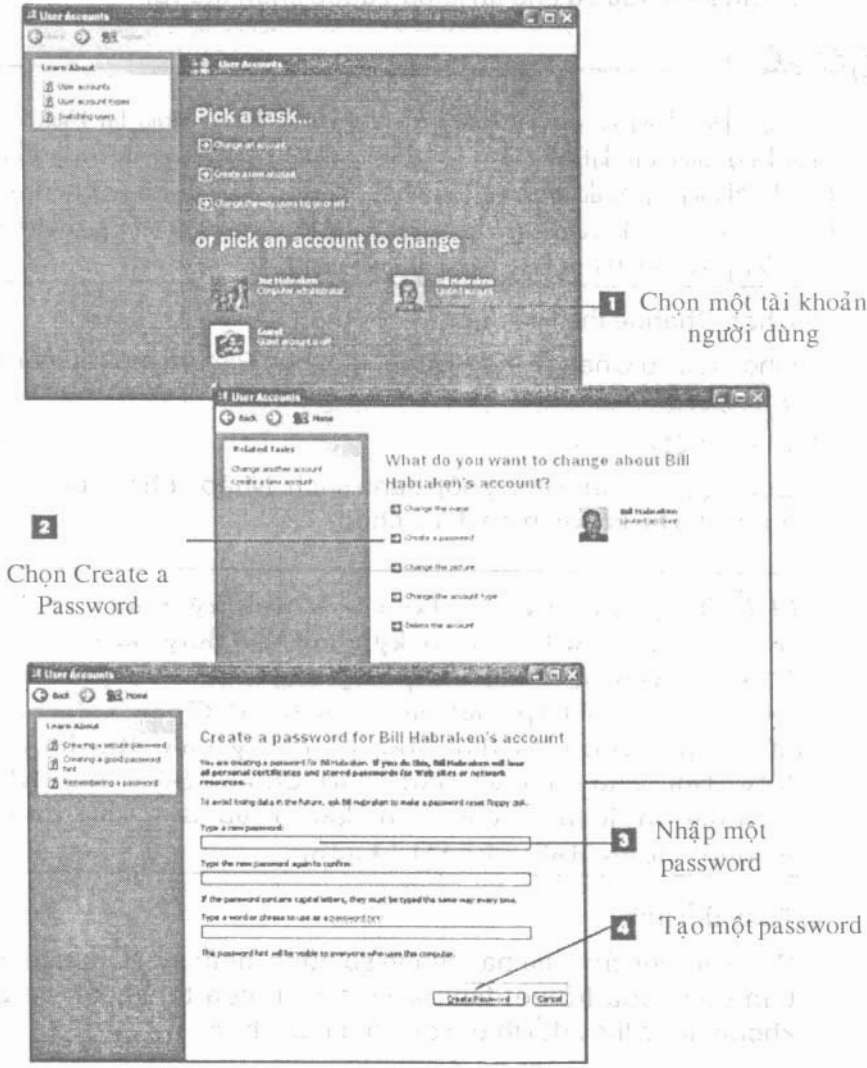
11. Tạo một tài khoản người dùng

12. Thay đổi ảnh tài khoản

Các tài khoản người dùng Windows XP có thể được gán một password. Điều này có nghĩa rằng để một người dùng đăng nhập với tài khoản có sẵn, người đó phải biết password. Người có tài khoản quản trị thì có thể gán các

password vào những tài khoản người dùng khác. Mỗi người dùng (cho dù người dùng này có các đặc quyền administrator) cũng có thể tạo và thay đổi password tài khoản của mình khi cần thiết.

13. Bảo vệ tài khoản người dùng bằng password



1. Chọn một tài khoản người dùng

   Trong cửa sổ User Accounts (chọn User Accounts trong Control Panel để mở cửa sổ này), chọn tài khoản người dùng mà bạn muốn tạo một password tài khoản riêng của bạn hoặc bất kỳ tài khoản nếu bạn là một nhà quản trị máy tính).

2. Chọn Create a Password

   Chọn tác vụ Create a Password để tạo một password cho người dùng được chọn. Cửa sổ Create a password mở ra. Nếu bạn thay

đổi một password hiện có (một password mà bạn xác lập trước đó), link xuất hiện dưới dạng Change the Password thay vì Create a password.

3. Nhập một password

Trong hộp text thứ nhất, gõ nhập một password cho tài khoản. Sau đó gõ nhập lại password như được yêu cầu trong hộp text thứ hai. Bạn cũng có thể nhập một gợi ý (hint) tùy chọn cho password. Gợi ý được hiển thị trên màn hình Windows Welcome và được thiết kế để giúp bạn nhớ password.

THỦ THUẬT: Nếu bạn sử dụng một gợi ý password, hãy nhớ rằng tất cả người dùng máy tính có thể thấy password tại màn hình Welcome. Gợi ý này không nên là một sự phân phát hoàn toàn trong việc cho phép những người dùng khác đoán password của bạn.

---

4. Tạo Password

Sau khi bạn đã nhập và sau đó nhập lại password (và gợi ý tùy chọn), nhấp nút Create Password. Bây giờ tài khoản được bảo vệ bằng password. Password phải được cung cấp khi bạn (hoặc người sở hữu tài khoản nếu bạn xác lập password cho một người dùng khác) đăng nhập vào hệ thống.

14. Thay đổi loại tài khoản

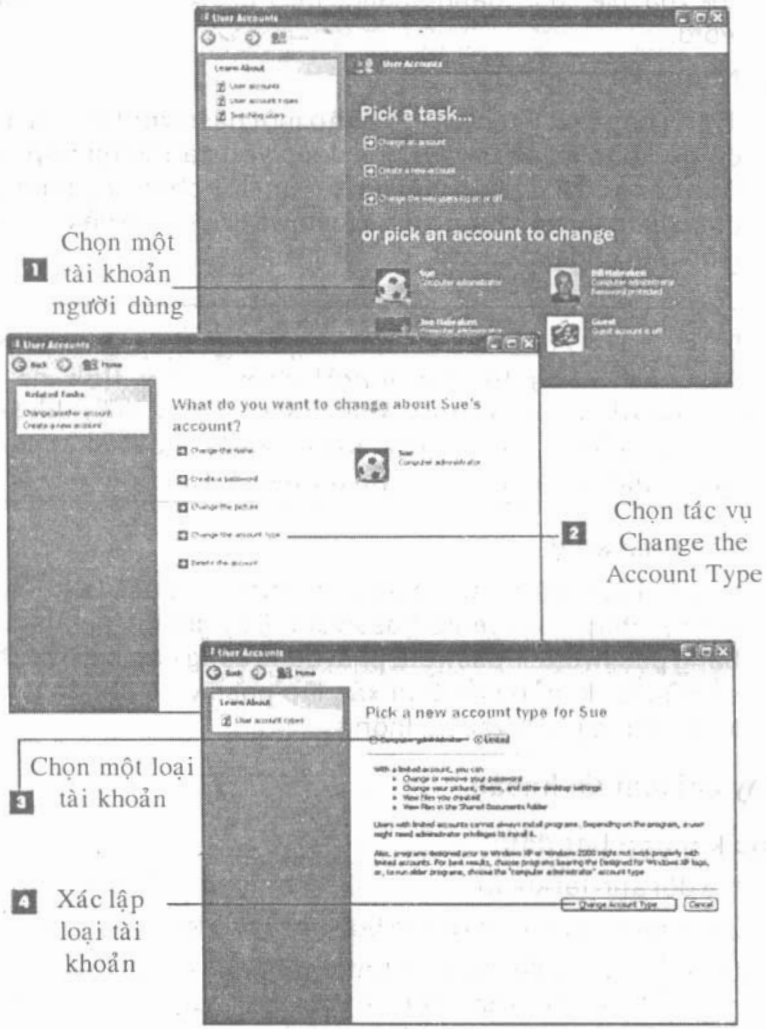
Trước khi bạn bắt đầu

12. Thay đổi ảnh tài khoản

13. Bảo vệ tài khoản người dùng bằng password

Một tài khoản computer administrator có thể thay đổi loại tài khoản được gán vào những tài khoản khác trên hệ thống. Ví dụ, một tài khoản computer administrator có thể được thay đổi thành tài khoản limited hoặc ngược lại. Bởi vì bất kỳ tài khoản computer administrator có thể thay đổi loại tài khoản cho tất cả tài khoản khác, các tài khoản computer administrator không thể được bảo vệ nghĩa là một nhà quản trị (administrator) có thể giảm cấp một nhà quản trị khác xuống thành một tài khoản limited.

14. Thay đổi loại tài khoản



1. Chọn một tài khoản người dùng

   Trong cửa sổ User Accounts (chọn User Accounts trong Control Panel để hiển thị cửa sổ này), chọn tài khoản người dùng mà bạn muốn chỉnh sửa loại tài khoản.

Ghi chú

Khi bạn thay đổi các xác lập cho tài khoản người dùng riêng của bạn, tác vụ kết hợp với tài khoản được ghi nhãn là Change my name, Change my picture,..Khi bạn thay đổi các xác lập cho một tài khoản khác (mà chỉ một nhà quản trị máy tính có thể thực hiện), các tác vụ được liệt kê là Change the name, Change the picture,...

2. Chọn Change the Account Type

   Trong cửa sổ tác vụ của tài khoản, chọn tác vụ Change the Account Type. Màn hình account type mở ra.

3. Chọn một loại tài khoản.

   Chọn loại tài khoản mới cho tài khoản (nếu tài khoản hiện có là Computer administrator, tùy chọn duy nhất là Limited và ngược lại).

4. Xác lập loại tài khoản

   Sau khi chọn loại tài khoản, nhấp nút Change Account Type để xác nhận việc thay đổi loại tài khoản.

15. Cấu hình một .NET Passport cho tài khoản người dùng

Trước khi bạn bắt đầu

11. Tạo một tài khoản người dùng

Mỗi tài khoản người dùng trên một máy tính chạy Windows XP có thể được kết hợp với một Microsoft .NET Passport. Mục đích của passport là nhận dạng người dùng khi họ truy cập nội dung Microsoft nhất định trên Web bao gồm các trang Web được cá nhân hóa và những công cụ khác chẳng hạn như dịch vụ Instant Messaging của Microsoft. Các xác lập .NET Passport phải được cấu hình bởi mỗi người dùng riêng lẻ. (Thậm chí một nhà quản trị không thể cấu hình một passport cho người dùng khác). Các tài khoản Computer administrator và Limited có thể được kết hợp với một .NET Passport.

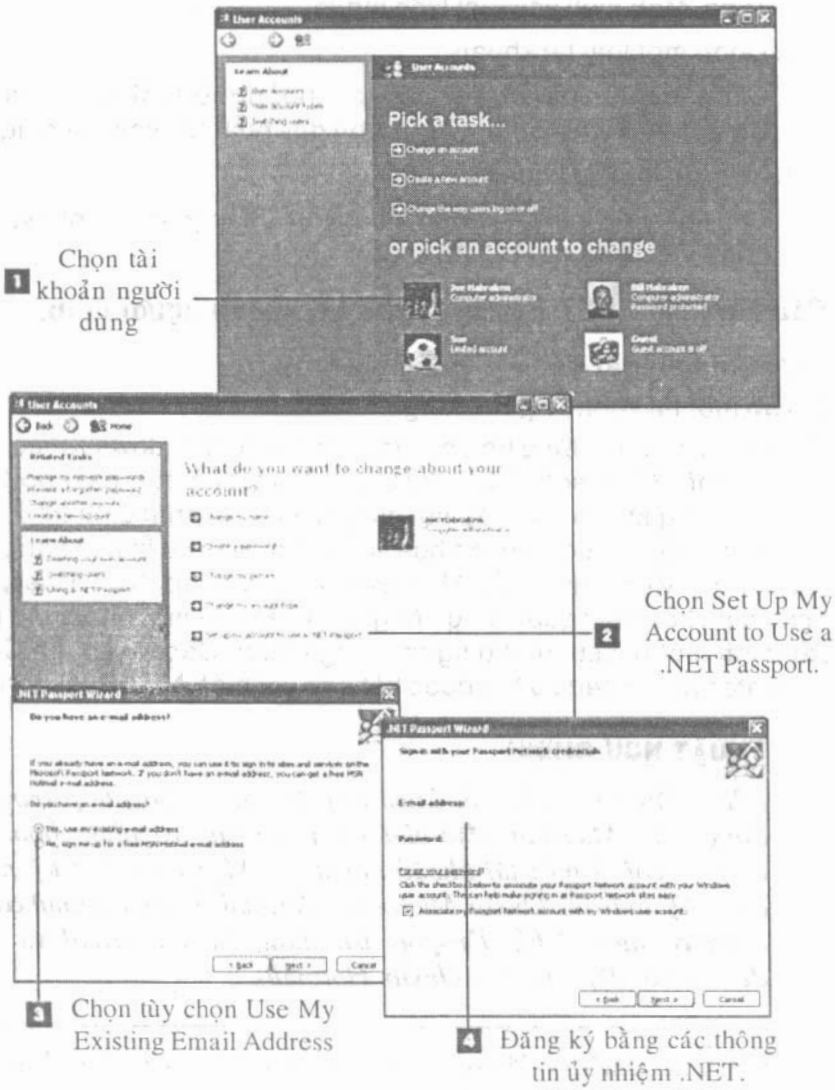
THUẬT NGỮ CHÍNH

.NET Passport. Một tài khoản người dùng cho phép truy cập nội dung Web Microsoft đặc biệt và mang tính cá nhân hóa. Passport thật sự chỉ là một tài khoản email với Microsoft; bất kỳ người nào đăng ký một tài khoản Microsoft Hotmail (www.hotmail.com) sẽ tự động có một .NET Passport (sử dụng địa chỉ email và password được thiết lập cho tài khoản Hotmail).

THỦ THUẬT: Bạn có thể đăng ký một .NET Passport bằng cách đăng ký một tài khoản email Microsoft Hotmail. Mặc dù bạn có thể đăng ký tài khoản trong tiến trình kết hợp password với tài khoản người dùng Windows của bạn, nhưng bạn có thể muốn đăng ký tài khoản hotmail trước khi bạn bắt đầu tiến trình tạo một .NET Passport (điều này làm cho mọi thứ trở nên dễ dàng hơn). Đi đến http://www.hotmail.com để đăng ký. Bạn sẽ thiết lập một tên tài khoản email và passport tài khoản trong tiến trình đăng ký.

---

15. Cấu hình một .NET Passport cho tài khoản người dùng



1. Chọn tài khoản người dùng

   Trong cửa sổ User Accounts (chọn User Accounts trong Control Panel để mở cửa sổ này), chọn tài khoản người dùng. Bạn phải chọn tài khoản riêng của bạn; bạn không thể cấu hình.NET Passport cho một tài khoản không phải tài khoản riêng của bạn.

Ghi chú

Khi một người dùng Limited truy cập cửa sổ User Accounts, các lựa chọn duy nhất có sẵn áp dụng cho người dùng đó. Để người dùng kết hợp một .NET Passport với tài khoản người dùng của mình, người dùng chọn tác vụ Set up my

account to use a .NET Passport sau khi mở cửa sổ User Accounts.

2. Chọn Set Up My Account To Use A .Net Passport

   Trong danh sách tác vụ cho người dùng đã chọn (tài khoản riêng của bạn), chọn tác vụ Set up my account to use a .NET Passport. .NET Passport Wizard mở ra. Nhấp Next để bỏ qua màn hình wizard ban đầu.

3. Chọn tùy chọn Use My Existing Email Account

   Giả sử bạn đã đăng ký một tài khoản email Hotmail như được đề nghị trước đó, trên màn hình wizard kế tiếp, hãy chắc chắn tùy chọn Yes, use my existing email address được chọn. Sau đó nhấp Next. Màn hình kế tiếp xác nhận rằng bạn đã đăng ký bằng các thông tin ủy nhiệm .NET của bạn. Nhấp Next để tiếp tục.

4. Đăng ký bằng những thông tin ủy nhiệm .NET

   Nhập địa chỉ tài khoản email Hotmail và sau đó nhập password tài khoản Hotmail. Nhấp Next để tiếp tục. Màn hình wizard cuối cùng xuất hiện. Nhấp Next. Bây giờ khi bạn đăng nhập vào hệ thống, .NET Passport của bạn sẽ được tự động kích hoạt. Như đã đề cập, một .NET Passport cho phép bạn truy cập nội dung Web Microsoft đặc biệt (chẳng hạn như My MSN (www.msn.com). .NET Passport cũng có thể được kết hợp với những nội dung đăng ký mà bạn đã mua từ Microsoft chẳng hạn như nội dung đăng ký có trả phí cho Microsoft Developers Network (MSDN). Để sử dụng nội dung đăng ký MSDN và đăng nhập vào site MSDN, bạn phải có một .NET Passport để kết hợp với nội dung đăng ký.

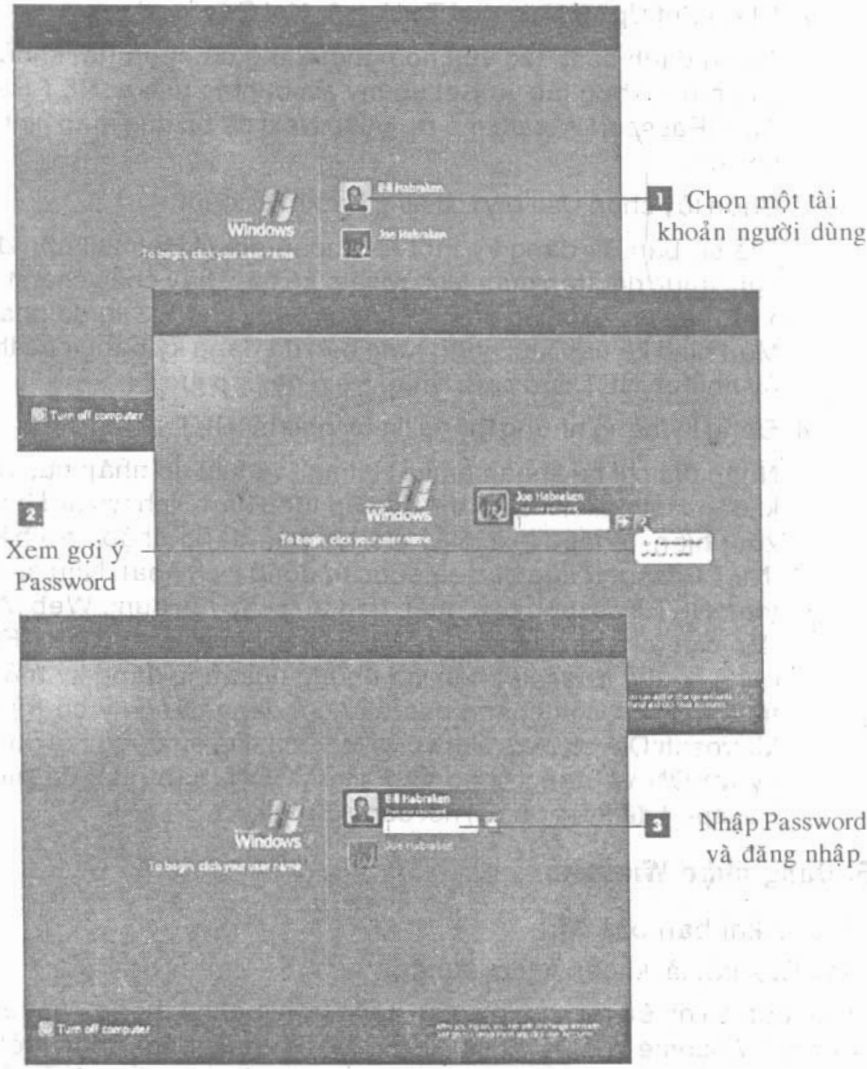
16. Đăng nhập Windows

Trước khi bạn bắt đầu

11. Tạo một tài khoản người dùng

Nếu bạn có nhiều tài khoản người dùng trên một hệ thống Windows, một màn hình Welcome xuất hiện sau khi hệ thống khởi động. Chọn một ảnh tài khoản người dùng để đăng nhập người dùng đó vào hệ thống. Nếu tài khoản được bảo vệ bằng password, người dùng phải nhập password cho tài khoản đó để hoàn tất tiến trình đăng nhập.

16. Đăng nhập vào Windows



1. Chọn một tài khoản người dùng

Khởi động hệ thống. Tại màn hình Welcome, nhấp ảnh của tài khoản bạn muốn đăng nhập vào.

Ghi chú

Khi một người dùng đăng xuất (logoff) hệ thống bằng cách chọn logoff trên menu Start, màn hình Welcome xuất hiện. Sau đó, một người dùng mới có thể đăng nhập mà không khởi động lại hệ thống.

2. Xem gợi ý Password

Nếu tài khoản được chọn có password đi kèm và bạn muốn xem gợi ý cho password đó, nhấp ảnh tài khoản người dùng. Sau đó nhấp

biểu tượng dấu hỏi nằm bên phải hộp text password. Gợi ý cho password xuất hiện.

3. Nhập Password và đăng nhập

Gõ nhập password cho tài khoản người dùng trong hộp text password và nhấn Enter. Windows xác nhận password và sau đó cho bạn đăng nhập vào hệ thống.

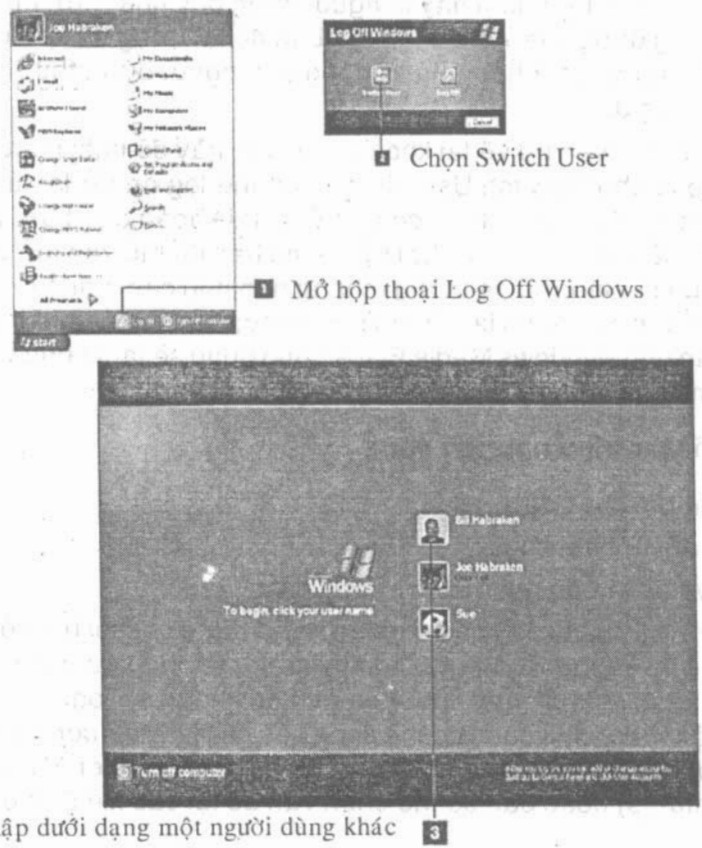
17. Chuyển đổi các người dùng

Trước khi bạn bắt đầu

16. Đăng nhập vào Windows

Đăng xuất (logoff) hệ thống (sử dụng menu Start) làm cho hệ thống sẵn sàng cho người dùng kế tiếp đăng nhập. Tuy nhiên, bạn không cần phải logoff để một người dùng khác đăng nhập. Thực tế, bạn có thể để các ứng dụng chạy (thực tế "bạn để lại tài khoản của bạn") và sử dụng tính năng Switch User để cho phép người dùng khác đăng nhập và sử dụng hệ thống. Khả năng chuyển đổi những người dùng này cho phép nhiều người dùng đăng nhập vào hệ thống mà không cần phải khởi động lại, hoặc tắt các ứng dụng đang chạy bằng việc đăng xuất và chuyển đổi các người dùng

17. Chuyển đổi các người dùng



1. Mở hộp thoại Log Off Windows

   Nhấp nút Start và chọn Log Off từ menu Start.

2. Chọn Switch User

   Trong hộp thoại Log Off Windows vừa mở ra, nhấp Switch User. Màn hình Logon xuất hiện.

THỦ THUẬT: Mặc dù chuyển đổi các người dùng là một cách nhanh cho người nào đó truy cập máy tính mà không cần buộc bạn tắt các ứng dụng, nhưng việc nhiều người dùng đăng nhập với các ứng dụng đang chạy đòi hỏi các tài nguyên hệ thống, nghĩa là hệ thống sẽ chạy chậm hơn. Nếu bạn làm việc xong trên máy tính và một người khác muốn sử dụng nó, hãy log off thay vì chỉ chuyển đổi các người dùng.

---

3. Đăng nhập dưới dạng một người dùng khác

   Người dùng mà bạn chuyển sang bây giờ có thể đăng nhập từ màn hình Logon. Người này có thể chọn một tài khoản, nhập password thích hợp nếu cần và bắt đầu một user session (phiên làm việc người dùng) như thể người này là người dùng duy nhất trên máy tính. Tất cả ứng dụng, file và xác lập mà bạn để lại trong tài khoản không bị ảnh hưởng bởi những hành động của người dùng thứ hai trong tài khoản mới.

Khi bạn cần chuyển trở về tài khoản của bạn, hãy đề nghị người dùng thứ hai log off hoặc chọn Switch User để bạn có thể log on trở lại tài khoản và desktop của bạn. Chú ý khi bạn log on trở lại tài khoản của bạn, bất kỳ ứng dụng mà bạn để chạy vẫn chạy, bất kỳ file mà bạn để mở vẫn mở và mọi khía cạnh khác của desktop và hệ thống (chẳng hạn như các mục trên clipboard) vẫn y như lúc bạn để chúng lại. Trong trường hợp của các ứng dụng multimedia chẳng hạn như Windows Media Player, ứng dụng sẽ tạm dừng bởi vì quyền điều khiển máy tính được chuyển sang người dùng mới.

18. Xóa một tài khoản người dùng

Trước khi bạn bắt đầu

12. Thay đổi ảnh tài khoản

13. Bảo vệ tài khoản người dùng bằng password

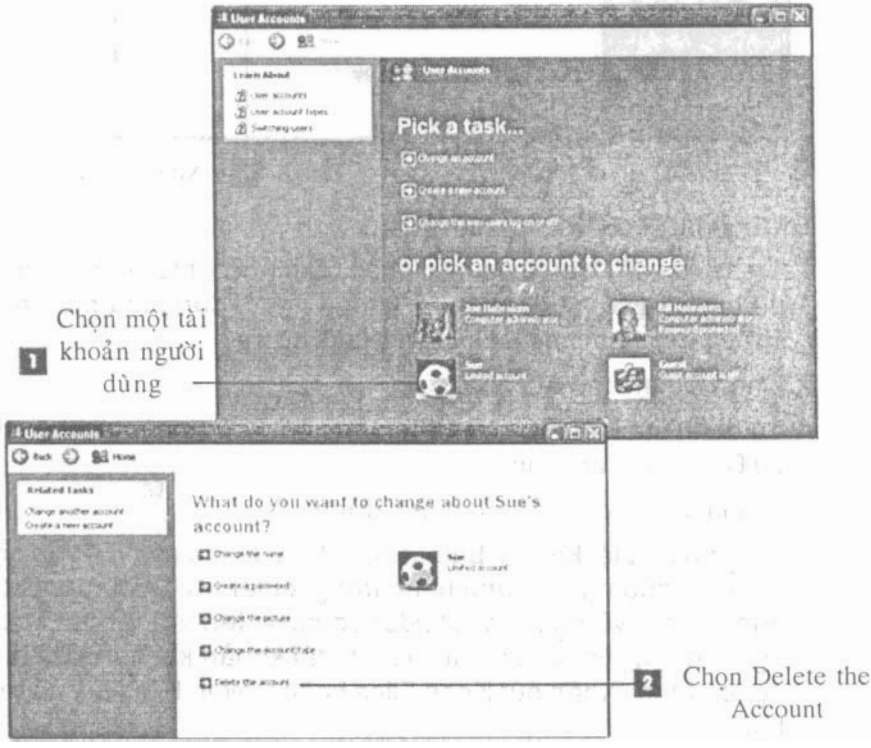
Bạn có thể thấy cần xóa các tài khoản người dùng ra khỏi hệ thống. Những người có các tài khoản Computer administrator có thể xóa bất kỳ tài khoản người dùng khác ra khỏi máy tính. Xóa một tài khoản sẽ loại bỏ người dùng đó ra khỏi hệ thống. Bạn cũng có thể chọn xóa các file đã được kết hợp với tài khoản người dùng đó (chẳng hạn như các file trong folder My Documents hoặc My Pictures) hoặc bạn có thể chọn vẫn để lại các file đó trên máy tính

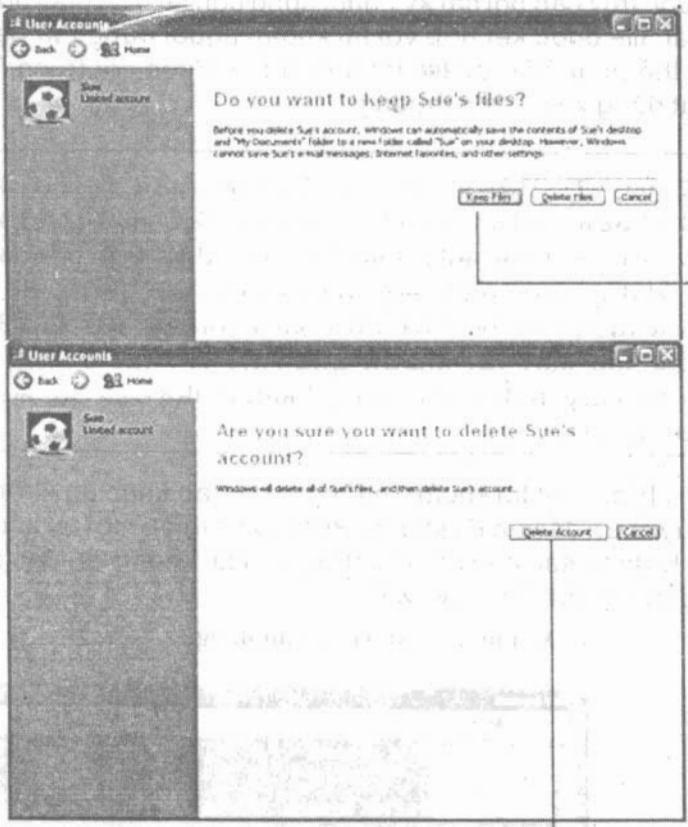
(chúng có thể được truy cập bởi bất kỳ người dùng còn lại trên máy tính). Nếu bạn chọn xóa các file được kết hợp với tài khoản người dùng mà bạn đang xóa, bạn không thể phục hồi các file (chúng không được đặt trong Recycle Bin như một hoạt động xóa thông thường).

THỦ THUẬT: Bởi vì các tài khoản quản trị có thể xóa các tài khoản quản trị khác, bạn có thể muốn chỉ một tài khoản quản trị trên máy tính lúc ban đầu bởi vì cuối cùng bạn sẽ không gặp phải một tình huống mà trong đó những người dùng quản trị bắt đầu xóa những tài khoản của nhau. Có chỉ một tài khoản quản trị với tất cả tài khoản khác trên máy tính dưới dạng limited thật sự là một "thói quen tốt nhất".

Nếu máy tính chỉ có một tài khoản (những tài khoản khác đã không được tạo), không có tùy chọn để xóa tài khoản. Phải có tối thiểu một tài khoản trên máy tính (đây là lý do tại sao bạn phải thiết lập một tài khoản lần đầu tiên bạn khởi động một bản cài đặt Windows XP).

18. Xóa một tài khoản người dùng





1. Chọn tài khoản người dùng

   Trong cửa sổ User Accounts (chọn User Accounts trong Control Panel để mở cửa sổ này), chọn tài khoản người dùng mà bạn muốn xóa khỏi danh sách các tài khoản ở cuối cửa sổ.

2. Chọn Delete the Account

   Từ danh sách tác vụ cho tài khoản người dùng được chọn, chọn tác vụ Delete the account.

3. Giữ lại hoặc xóa các file người dùng

   Khi bạn xóa tài khoản, bạn có tùy chọn để lưu các file vốn nằm trên desktop của người dùng hoặc trong folder My Documents (các file được di chuyển đến một folder có cùng tên với tên tài khoản của người dùng) hoặc xóa các file của tài khoản khi bạn xóa tài khoản người dùng. Nhấp nút Keep Files hoặc Delete Files tùy sở thích của bạn.

4. Xóa tài khoản

   Trên màn hình kế tiếp, nhấp Delete Account. Tài khoản người dùng đã chọn bị xóa.

Chương 4

CÀI ĐẶT VÀ CẤU HÌNH ROUTER KHÔNG DÂY

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *19. Bàn về việc cài đặt router không dây*
- *20. Cài đặt Router*
- *21. Bàn về việc cấu hình router không dây*
- *22. Truy cập cấu hình Router*
- *23. Bàn về các xác lập Internet*
- *24. Cấu hình các xác lập Internet*
- *25. Bàn về các xác lập không dây*
- *26. Cấu hình các xác lập Wireless của Router*

Bước chính đầu tiên trong việc thiết lập một mạng gia đình không dây vốn chia sẻ một nối kết Internet băng tần rộng là cài đặt và cấu hình router không dây. Chương này sẽ trình bày cách thiết lập các nối kết vật lý khác nhau giữa router và thiết bị băng tần rộng (chẳng hạn như một modem cáp). Chương cũng sẽ trình bày những điểm cơ bản về việc cấu hình các xác lập Wireless và Internet của router.

19. Bàn về việc cài đặt Router không dây

Để xây dựng một mạng gia đình không dây có nối kết với một nối kết Internet băng tần rộng, bạn cần một router không dây. Router là đối tượng trung gian hoặc cổng nối (gateway) giữa thiết bị cung cấp nối kết Internet băng tần rộng (chẳng hạn như một router DSL hoặc một modem cáp) và mạng gia đình, gồm những máy tính muốn sử dụng Internet. Router không dây cũng được sử dụng làm access point WiFi cho những máy tính trên mạng

được trang bị các adapter mạng không dây. Các máy tính có các card mạng "hữu tuyến" cũng có thể được gắn với các cổng switch trên router không dây, cho phép những máy tính hữu tuyến này gia nhập cùng một mạng và truy cập nối kết Internet tốc độ cao.

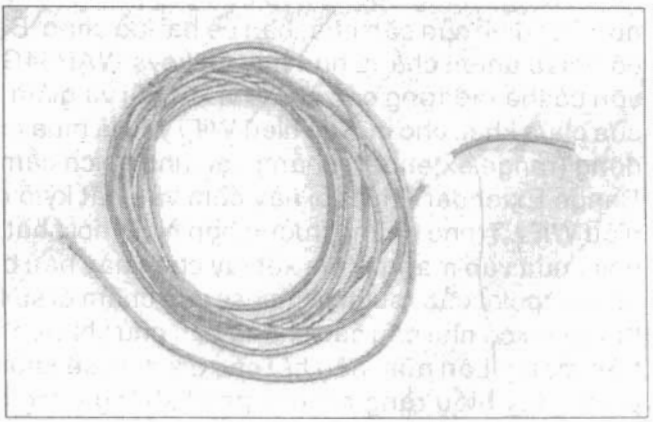
Thuật ngữ chính

Hub. Một thiết bị kết nối cung cấp nhiều cổng LAN. Các máy tính có thể được kết nối với những cổng LAN này bằng cách sử dụng cáp mạng. Một hub thường được xem là thiết bị nối kết "câm" và không thể cảm nhận loại kết nối và các tốc độ kết nối switch (ví dụ giữa 10MB và 100MB nếu điều đó được hỗ trợ bởi các adapter mạng trên các máy tính).

Thiết bị nối kết switch A thông minh hơn một hub vốn cho phép các máy tính kết nối với mạng bằng cách sử dụng các cáp. Các cổng trên switch tự động cảm biến các tốc độ kết nối. Các switch cao cấp hơn cũng thường cung cấp những khả năng để điều chỉnh thông lượng thật sự (lượng băng thông có sẵn) trên một cổng LAN cụ thể, cung cấp cho những máy tính nhất định hoặc các thiết bị khác băng thông mạng cao hơn.

Switch được lắp sẵn và hầu hết các router WiFi có sẵn ngày nay là một thiết bị kết nối tốc độ cao cung cấp một dãy kết nối tốc độ cho những máy tính được nối trực tiếp với switch bằng các cáp mạng. Hầu hết các switch router WiFi cung cấp các nối kết Ethernet thông thường và nhanh (10 Mbps và 100Mbps). Switch tự động cảm biến (autosensing), do đó nó nhận biết khi nào một máy tính có một card mạng Ethernet nhanh (100Mbps) gắn vào switch và có tốc độ kết nối thích hợp. Bởi vì nhiều router WiFi có sẵn cho việc nối mạng gia đình cung cấp chỉ bốn cổng LAN trên switch, bạn phải mua thêm một switch nếu bạn sẽ gắn hơn bốn máy tính vào router WiFi bằng cách sử dụng các cáp mạng. Hãy chắc chắn rằng switch mà bạn mua có khả năng tự động cảm biến và rằng nó hỗ trợ các nối kết Ethernet thông thường và nhanh. Một switch như vậy có thể đáp ứng tất cả máy tính trên mạng bất kể tuổi thọ của máy tính, tốc độ của các card mạng.

Đối với việc quyết định vị trí thật sự của router WiFi, hãy ghi nhớ một số vấn đề chẳng hạn như việc router WiFi cần kết nối với thiết bị băng tần rộng Ethernet bằng cách sử dụng một cáp mạng. Bạn phải lắp đặt router ở vùng đủ gần với modem cáp băng tần rộng hoặc router DSL để chúng có thể được nối cáp cùng với nhau bằng cách sử dụng một cáp nối mạng CAT 5. Cách này thường được đính kèm với router không dây. Tuy nhiên, cáp được cung cấp thường dài không quá 5 feet, do đó nếu router không dây được đặt xa hơn router từ thiết bị băng tần rộng, bạn sẽ mua một cáp CAT 5 dài hơn. Mặc dù chúng ta gọi router WiFi là một "thiết bị không dây", nhưng nó vẫn được gắn vào thiết bị nối kết Internet băng tần rộng và bất kỳ máy tính vốn được nối dây (được nối kết vật lý) với switch trên router WiFi.



Cáp nối mạng CAT 5 được sử dụng để nối kết router không dây và thiết bị băng tần rộng.

Nơi bạn đặt router không dây trong nhà cũng rất quan trọng bởi vì các phạm vi hoạt động trong nhà cho các cuộc truyền vô tuyến giữa router và các máy tính được vận hành bằng wireless chỉ 150 đến 300 feet. Phạm vi hoạt động này cũng bị ảnh hưởng bởi chất liệu được sử dụng trong cấu trúc của ngôi nhà. Một nhà khung gỗ điển hình cung cấp các phạm vi hoạt động không dây khá tốt trong mọi ngóc ngách của căn nhà và thường trên các hành lang và ván sàn. Tuy nhiên, một căn nhà có các nền nhà được đổ bê tông và các chất liệu xây dựng "có sức bền cao" có thể giảm đáng kể phạm vi hoạt động và thậm chí có thể quyết định việc các máy tính có thể truy cập những dịch vụ wireless hay không. Do đó các phạm vi hoạt động mà bạn thấy sẽ phụ thuộc vào các chất liệu xây dựng và cách bố trí của căn nhà.

Trong phân tích cuối cùng, vị trí của thiết bị nối kết Internet băng tần rộng (chẳng hạn như một modem cáp), vị trí của các máy tính được nối cáp trực tiếp với router wireless và toàn bộ kích cỡ và sơ đồ của căn nhà sẽ ảnh hưởng đến nơi bạn đặt router. Router wireless thật sự là một cầu nối tuyệt vời giữa các máy tính hữu tuyến, các máy tính được vận hành bằng WiFi và nối kết Internet.

Một điểm khác mà chúng ta nên thảo luận là nhu cầu cần tối thiểu một máy tính được nối kết vật lý với router bằng cáp mạng. Máy tính hữu tuyến này được sử dụng để cấu hình và giám sát router không dây (mặc dù bạn có thể cho phép truy cập router trên Web cho những mục đích cấu hình và giám sát router). Để lặp lại, bạn phải có tối thiểu một máy tính có một card mạng truyền thống được nối với router WiFi. Nối kết vật lý này với router thật sự nâng cao an ninh về ai có thể truy cập và cấu hình router (một máy tính có nối kết vật lý). Điều hợp lý nhất là nên đặt máy tính này trên cùng một căn phòng với router WiFi (và thiết bị nối kết Internet, chẳng hạn như một router DSL) để bạn không đối mặt với những cáp chạy ngoằn ngoèo khắp nơi, đây rất có khả năng là một trong những lý do bạn muốn kết nối wireless lúc ban đầu.

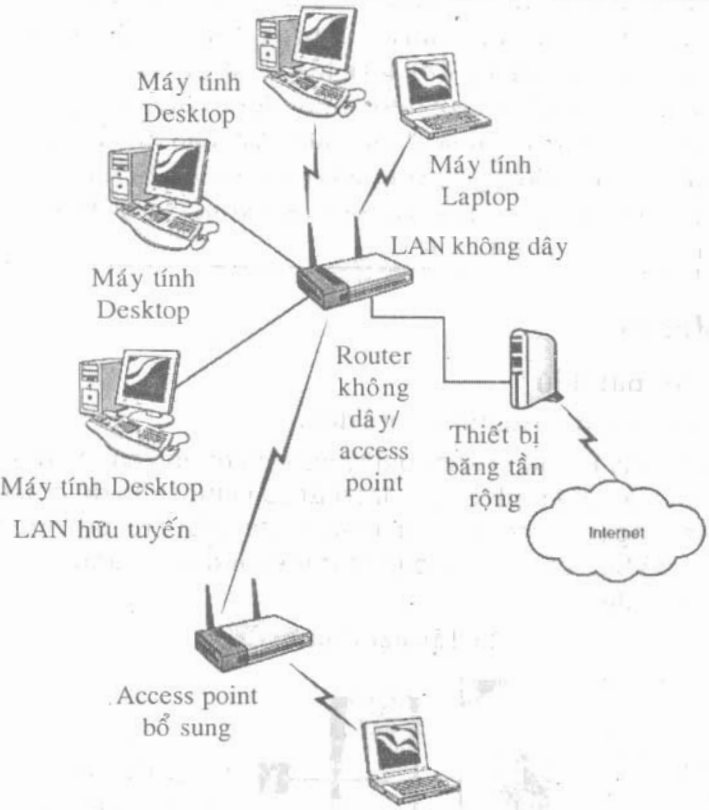
Trong hầu hết các trường hợp, một router Wireless có thể đáp ứng tất cả máy tính không dây và hữu tuyến trên mạng gia đình của bạn: 10 máy tính hoặc ít hơn. bởi vì nối mạng workgroup Windows được thiết kế dành cho 10 máy tính trở xuống, 10 chắc chắn là mức tối đa cho loại nối mạng ngang hàng

này. Trong những trường hợp bạn gặp phải các "vùng chết" WiFi trong những nơi nhất định của căn nhà, bạn có hai lựa chọn. Bạn mua một router WiFi mới có nhiều anten chẳng hạn như Linksys WAP54GX Wireless-G access point vốn có thể mở rộng các phạm vi kết nối và giảm đi các vùng chết. Một cách sửa chữa khác cho một tín hiệu WiFi yếu là mua một bộ mở rộng phạm vi hoạt động (range extender) chẳng hạn như phích cắm tường Netgear Wireless G Range Extender. Thiết bị này cắm vào bất kỳ ổ cắm điện và tăng cường tín hiệu WiFi. Trong những trường hợp hiếm hoi nhất, bạn phải thêm một access point nữa vào mạng. Xem xét tùy chọn này nếu bạn thấy rằng lưu lượng trên access point của router Wireless làm chậm đi sự truy cập mạng nhất là trong thời điểm có nhu cầu cao chẳng hạn như khi việc chơi game trực tuyến xảy ra trên mạng. Lần nữa, hầu hết các gia đình sẽ không đòi hỏi thêm một access point. Hãy hiểu rằng access point không cung cấp cổng nối (gateway) và những tính năng router của router WiFi, nhưng nó cung cấp một cách khác để mở rộng phạm vi hoạt động của mạng. Bạn sẽ cần một access point thứ hai chỉ trong những tình huống hiếm hoi nhất. Các access point thứ cấp kết nối không dây với router không dây chính để các máy tính trong tầm hoạt động xa của gia đình hoặc mạng có thể "bật trở lại" sang router chính. Bạn cấu hình access point phụ giống như bạn cấu hình access point trên router nghĩa là sử dụng cùng một SSID và những xác lập khác.

Khi bạn đã quyết định nơi bạn sẽ đặt router không dây, bạn có thể lắp đặt nó. Sau khi router được lắp đặt (nghĩa là được đặt và được nối kết bằng phương diện vật lý), bạn có thể cấu hình các xác lập cơ bản trong router. Lắp đặt router đòi hỏi bạn tắt modem băng tần rộng (nối kết Internet sẽ không có sẵn). Bạn cũng nên tắt nguồn tất cả máy tính hiện ở trên mạng chẳng hạn như các máy tính được kết nối với một switch hoặc một hub vốn nối với thiết bị băng tần rộng. Tóm lại, hãy tắt mọi thứ để bắt đầu tiến trình lắp đặt.

Bạn cần tối thiểu hai cáp mạng Ethernet CAT 5 để tạo các nối kết cần thiết cho mạng không dây: bạn sẽ nối router không dây với modem cáp hoặc router DSL. Bạn cũng sẽ nối một máy tính với router không dây (cho phép bạn truy cập và cấu hình router). Một cáp mạng thường đi cùng với router không dây. Và bởi vì bạn đã có một nối kết băng tần rộng với tối thiểu một máy tính, sẽ có tối thiểu một cáp chạy từ thiết bị băng tần rộng đến máy tính mà bạn có thể sử dụng.

Một router không dây cho phép tạo một mạng gia đình gồm các máy tính hữu tuyến và không dây.



THỦ THUẬT: Nếu bạn sẽ nối kết thêm các máy tính hoặc một thiết bị khác chẳng hạn như hub hoặc switch với router không dây, bạn sẽ cần thêm các cáp nối mạng. Các cổng Ethernet trên hầu hết các router tự động cảm biến, nghĩa là cổng được cấu hình chính xác cho đến khi thiết bị được nối với cổng. Bạn có thể sử dụng cáp Ethernet CAT 5 thông thường cho dù bạn nối kết một máy tính hoặc một switch khác với router không dây. Bạn không cần mua các cáp chéo (crossover cable) để nối router với các switch và hub (hầu hết các hub có một cổng uplink). Tuy nhiên một số cổng cũ hơn có thể nối các cáp chéo với một cổng LAN trên hub với switch của router WiFi. Một cáp chéo trông như cáp CAT 5 bình thường (mặc dù một số công ty làm cho các cáp chéo của họ có màu vàng để bạn biết nó là một cáp chéo, cáp cũng sẽ được đóng dấu bằng tên "patch cord"). Một cáp chéo khác với một cáp LAN thường ở điểm 4 cặp dây trong các bộ nối RJ 45 ở các đầu của cáp được "bắt chéo" tái sắp xếp trên cáp chéo, các dây chạy "thẳng qua" trong một cáp

LAN CAT 5 thông thường. Hãy chắc chắn bạn đọc tài liệu của các thiết bị nối kết hiện có (chẳng hạn như các switch hoặc hub) trước khi mua thêm bất kỳ cáp. Bởi vì hầu hết các hub cũ hơn được thiết kế cho Ethernet 10Mbps, bạn nên thay chúng bằng các switch mới cung cấp các cổng tự động cảm biến và thông lượng 10 Mbps và không đòi hỏi các cáp đặc biệt.

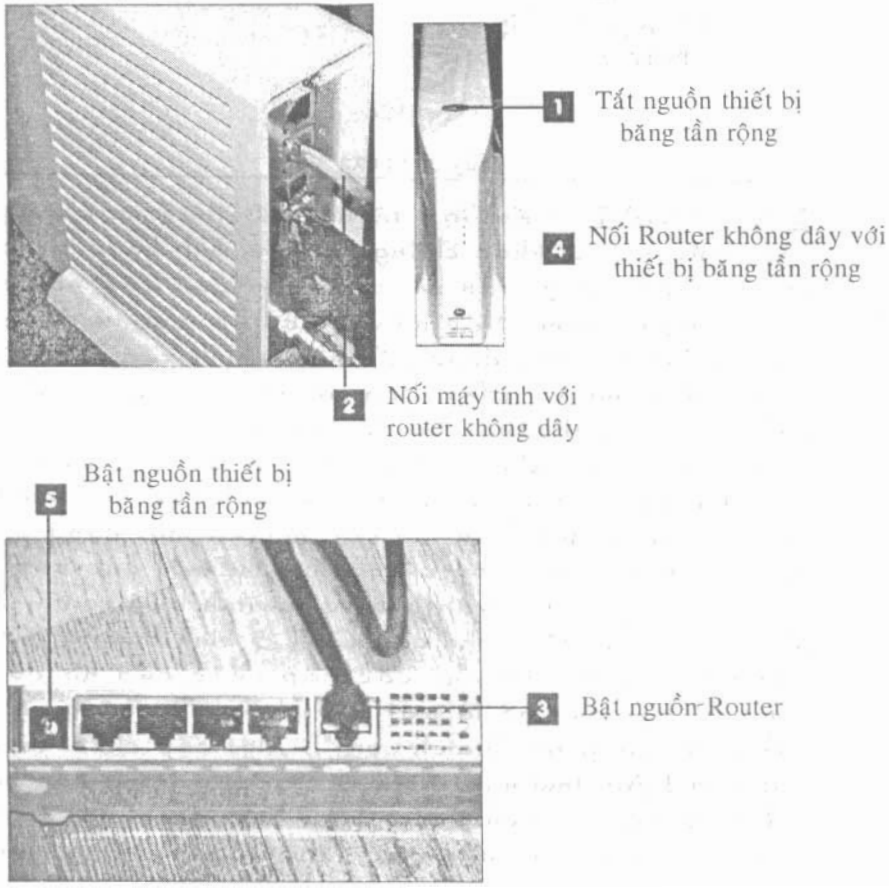
20. Lắp đặt Router

Trước khi bạn bắt đầu

19. Bàn về việc lắp đặt Router không dây

Sau khi bạn đã lấy ra router không dây và xem nhanh các hướng dẫn lắp đặt, bạn sẵn sàng lắp đặt router. Lắp đặt thật sự là một vấn đề nối router với thiết bị băng tần rộng (một modem cáp hoặc router DSL) rồi bật nguồn router không dây. Sau đó bạn có thể truy cập router không dây bằng cách nối trực tiếp máy tính với router.

20. Lắp đặt Router



1. Tắt nguồn thiết bị băng tần rộng

   Tắt modem cáp hoặc router DSL. Điều này có thể đòi hỏi rút phích cắm thiết bị băng tần rộng (nhiều thiết bị này có các công tắc on/off).

Ghi chú

Việc rút phích cắm thiết bị băng tần rộng thực tế sẽ xác lập lại thiết bị. Bởi vì thiết bị băng tần rộng theo dõi thông tin chẳng hạn như các "thuê bao" địa chỉ IP (các địa chỉ đã được tạm thời gán cho các máy tính, điều quan trọng là phải xóa thông tin này trước khi thiết lập router không dây, điều này thật sự sẽ đảm nhiệm công việc gán các địa chỉ IP vào các mạng không dây và hữu tuyến trên mạng.

2. Nối Router không dây với thiết bị băng tần rộng

   Nối router không dây với thiết bị băng tần rộng bằng cách sử dụng một cáp UTP CAT 5 (trong hầu hết các trường hợp với router). Cắm cáp vào router không dây trong cổng Ethernet được ấn định cho "Internet".

Ghi chú

Cho dù bạn sử dụng nhãn hiệu router không dây nào, một cổng trên router sẽ được ấn định cho nối kết Internet vốn là nối kết giữa thiết bị băng tần rộng và router không dây. Những cổng khác trên router không dây thường được ghi nhãn là các cổng "LAN" và được sử dụng để nối trực tiếp các máy tính hoặc những thiết bị mạng khác với router.

3. Nối máy tính với Router không dây

   Nối một máy tính (một máy tính laptop hoặc desktop) bằng cách chạy một cáp từ adapter mạng trong của máy tính đến router không dây bằng cách sử dụng một trong các cổng LAN của router. Máy tính này bây giờ được "nối dây cứng" với router WiFi sẽ có chức năng như console quản lý để cấu hình và giám sát router WiFi. Nó cũng là máy tính mà bạn sẽ sử dụng để giao tiếp ban đầu với router và tạo cấu hình của router bằng cách sử dụng CD hoặc DVD cài đặt đính kèm với router WiFi.

Ghi chú

Bạn thật sự nên bố trí một máy tính trên mạng có một adapter LAN "hữu tuyến" để bạn có thể cấu hình access point của router WiFi vào lúc ban đầu. Nếu bạn không có một máy tính hữu tuyến trên mạng, hãy mượn một laptop có một adapter LAN hữu tuyến; thiết lập router WiFi bằng cách sử dụng CD cài đặt. Sau đó, bạn có thể cấu hình router để nó được truy cập theo bất kỳ máy tính trên mạng bằng cách sử dụng một trình duyệt Web. Tuy nhiên, phương

pháp này không an toàn như việc có một nối kết cáp "cứng" với router. Nếu bạn đã có một modem băng tần rộng trong nhà của bạn (trước khi bạn quyết định WiFi), nó được nối với tối thiểu một máy tính bằng một nối kết LAN "hữu tuyến". Sử dụng máy tính này để cấu hình router. Đối với một máy tính không được nối trực tiếp với router bằng một nối kết hữu tuyến để cấu hình router, bạn nên mở chức năng truy cập Web đưa router ra trước khả năng tấn công từ bên ngoài mạng.

4. Bật nguồn thiết bị băng tần rộng

   Nối lại thiết bị băng tần rộng với nguồn điện. Đợi 2 đến 3 phút để cho thiết bị bắt đầu chọn với giao thức ISP và nối kết với Internet. Hãy chắc chắn tất cả đèn đều sáng trên thiết bị băng tần rộng (đặc biệt đèn nối kết Internet thường được ghi nhãn là "Online").

5. Bật nguồn Router

   Cắm router không dây vào một nguồn điện. Theo dõi các đèn chỉ báo ở phía trước router. Khi bạn thấy hoạt động trên bộ chỉ báo Internet và cổng LAN được nối với PC, bạn đã hoàn tất việc lắp đặt router không dây và sẵn sàng cấu hình các xác lập cơ bản cho router.

Nếu bạn không thấy một đèn hoạt động cho bộ chỉ báo Internet trên router WiFi, hãy kiểm tra nối kết cáp giữa router và thiết bị băng tần rộng (chẳng hạn như một modem cáp). Nếu nối kết tốt, hãy đảo ngược cáp bởi vì đôi khi hoạt động này buộc bạn nối kết các bộ nối cáp vào các cổng thích hợp trên các thiết bị. Modem cáp (hoặc thiết bị nối kết khác) cũng sẽ cho thấy một đèn nối kết Internet. Nếu nó không được mở, hãy tắt thiết bị băng tần rộng WiFi và lặp lại các bước trong tác vụ này cũng kiểm tra nối kết điện cho router WiFi. Nếu bạn gặp các sự cố nối kết LAN, hãy kiểm tra cáp LAN giữa máy tính và switch của router WiFi. Đối với các sự cố ngoại trừ những sự cố rõ ràng, hãy **xem mục 91** và **mục 93**.

21. Bàn về việc cấu hình Router không dây

Trước khi bạn bắt đầu	Xem thêm
20. Lắp đặt Router	**Mục 40**
	Mục 42

Khi bạn đã bật nguồn router không dây và xác nhận rằng "nó đang giao tiếp với thiết bị băng tần rộng (nghĩa là tất cả đều sáng), bạn sẵn sàng cấu hình các xác lập cơ bản của router. Hầu hết các router không dây được cấu hình từ xưởng với khả năng kết nối không dây được tắt. Điều đó có nghĩa rằng bạn phải mở khả năng kết nối không dây của router trong quá trình cấu hình ban đầu. Trong suốt quá trình cấu hình ban đầu, bạn cũng phải thay đổi (và nên thay đổi) tên mạng không dây hoặc SSID (service set identifier), vốn nhận dạng mạng không dây của bạn.

Thuật ngữ chính

SSID (service set identifier). Một định danh duy nhất (tối đa 32 ký tự) được sử dụng để phân biệt một WLAN này với một WLAN khác. Các thiết bị cố kết nối với một WLAN cụ thể, sử dụng SSID được cấu hình cho WLAN đó.

Ghi chú

SSID mặc định cho hầu hết các router không dây là tên của công ty sản xuất router. Ví dụ, trên một router Linksys, SSID mặc định là LINKSYS. Router không dây NETGEAR được sử dụng để giải thích cấu hình cơ bản và thiết lập của một router trong mục 20, SSID mặc định là NETGEAR.

Hai tập hợp tùy chọn cấu hình cơ bản mà bạn sẽ làm việc liên quan đến nối kết Internet (chẳng hạn như địa chỉ IP được sử dụng bởi router không dây) và mạng không dây (các tùy chọn chẳng hạn như tên SSID và chế độ mạng). Những xác lập ban đầu này thường có thể được cấu hình bằng cách sử dụng setup wizard nằm trên một CD hoặc DVD đính kèm với router không dây. Trong hầu hết trường hợp, bạn có thể tùy chọn cấu hình router không dây mà không cần đến wizard bằng cách nối kết với router sử dụng trình duyệt web.



Hầu như tất cả router không cây cài đặt sẽ giúp bạn nối kết với router.

THỦ THUẬT: Hãy chắc chắn máy tính nối với router không dây được cấu hình để nhận địa chỉ IP của nó và những xác lập TCP khác từ router không dây thông qua DHCP. Trong hộp thoại TCP/IP Properties cho adapter

mạng của máy tính, tùy chọn Obtain an IP address automatically và tùy chọn Obtain DNS server address nên được chọn.

Một URL được cung cấp trong tài liệu của router không dây cho phép bạn truy cập router từ máy tính được nối kết (qua cáp LAN) với router. Ví dụ, URL cho router Netgear là http://www.routerlogin.net/basicsetting.htm. Tài liệu cho router này cũng cung cấp một tên đăng nhập là admin và một password là password. Khi bạn đăng nhập vào router (sử dụng một wizard được cung cấp bởi CD cài đặt của router hoặc bằng cách sử dụng URL), bạn có thể truy cập các xác lập khác nhau bằng cách sử dụng các link được cung cấp trên các trang web kết hợp với cấu hình của router.

22. Truy cập cấu hình Router

Trước khi bạn bắt đầu

21. Bàn về việc cấu hình Router không dây

Để cấu hình router không dây, bạn phải truy cập router. Bạn thực hiện điều này từ một máy tính nối trực tiếp với router không dây bằng một cáp mạng. Sau cấu hình ban đầu, bạn có thể truy cập router bằng cách sử dụng trình duyệt web của máy tính chẳng hạn như Internet Explorer.

Sau khi truy cập router, bạn nên mở chức năng WiFi để các máy tính trên mạng có thể kết nối với các access point của router WiFi. Bạn cũng nên cho phép các thông báo truyền đại chúng SSID (tên mạng WiFi được truyền phát đại chúng bởi router), điều này làm cho bạn dễ truy cập các máy tính được vận hành bởi WiFi vốn sẽ kết nối với access point của router hơn.

22. Truy cập cấu hình Router





Bật chức năng truy cập không dây (Wireless Access) và truyền phát đại chúng SSID (SSID Broadcast).

1. Nhập URL cho router không dây

   Trong trình duyệt web (chẳng hạn như Internet Explorer), gõ nhập URL được cung cấp bởi nhà sản xuất router không dây trong hộp text Address và nhấp Go. Một hộp thoại an ninh mở ra.

2. Nhập Username và Passowrd.

   Nhập username và password được cung cấp trong tài liệu router. Nhấp OK. Cửa sổ quản lý router mở ra trong cửa sổ trình duyệt.

THỦ THUẬT: Nếu bạn muốn làm cho sự nối kết các router dễ dàng hơn trong tương lai, chọn hộp kiểm Remember my password trong hộp thoại an ninh.

---

3. Bật chức năng Wireless access và SSID Broadcast.

   Chọn tùy chọn Wireless Settings trên trang cấu hình của router WiFi. Ví dụ đối với WiFi Netgrear WiFi, nhấp Wireless Settings bên dưới tiêu đề Advanced ở bên trái cửa sổ trình duyệt. Sau đó nhấp Enable Wireless Router Radio và Enable SSID Broadcast để mở các chức năng nối mạng WiFi và cho phép router WiFi truyền phát đại chúng SSID mạng. Tên của những tùy chọn mà bạn chọn có thể thay đổi phụ thuộc vào phần mềm cấu hình và router WiFi mà bạn sử dụng, nhưng bạn nên mở hai xác lập này.

Ghi chú

Bạn sẽ thấy rằng các trang web được sử dụng để truy cập cấu hình của router không dây khá tương tự bất kể nhãn hiệu router nào mà bạn đang sử dụng. Các giao diện thường đơn giản và dễ làm việc khi bạn cấu hình và giám sát router.

23. Bàn về các xác lập Internet

Trước khi bạn bắt đầu

21. Bàn về cấu hình router không dây

22. Truy cập cấu hình router

Các xác lập Internet router không dây thì thiết yếu; chúng phải được nhập chính xác để router không dây có thể kết nối với thiết bị băng tần rộng và cuối cùng với ISP vốn cung cấp nối kết Internet. Bạn nên có thông tin sau đây (do ISP cung cấp khi bạn đăng ký dịch vụ) để xác lập các cấu hình Internet của router:

- *Tên và Password đăng nhập. Nếu nhà cung cấp dịch vụ của bạn đòi hỏi bạn đăng nhập truy cập Internet, ISP của bạn sẽ cung cấp cho bạn một login và password. Những xác lập này phải được nhập vào cấu hình router để truy cập Internet. Tên và password đăng nhập không giống với tên và password đăng nhập mà bạn sử dụng để truy cập router WiFi thông qua trình duyệt web. Bạn phải nhận tên và password đăng nhập này từ nhà cung cấp dịch vụ Internet.*

Ghi chú

Một số ISP cũng cung cấp cho bạn một tên dịch vụ để truy cập Internet. Bạn cũng sẽ cần thông tin này để cấu hình router không dây. Hãy gọi đến bộ phận trợ giúp của ISP trước khi cấu hình router WiFi để bạn có thể thu thập thông tin cần thiết nhằm cấu hình router chính xác.

- *IP Address và Subnet Mask. Nếu ISP đã cung cấp cho bạn một địa chỉ IP tĩnh, bạn sẽ cần địa chỉ mà bạn đã được cung cấp. Nếu không, bạn sẽ được cấu hình router không dây để nó nhận địa chỉ IP của nó và những xác lập TCP/IP khác một cách động.*
- *Các tên server DNS. Một số ISP đòi hỏi bạn cấu hình router sao cho nó biết các địa chỉ IP của các name server DSN chính và phụ. Nếu không, thông tin này được cấu hình động.*

Hãy chắc chắn bạn ghi chép tất cả thông tin này lên một mảnh giấy để bạn có thể cấu hình router khi bạn truy cập tiện ích cấu hình. Trong những tình huống bạn không cần một tên đăng nhập (và password) và nhận địa chỉ IP và các xác lập TCP/IP khác một cách động thông qua server DHCP của ISP, bạn sẽ không cần bất kỳ thông tin này, điều này làm cho cấu hình router trở nên cực kỳ đơn giản.

Như với bất kỳ xác lập router và adapter mạng không dây được thảo luận, các xác lập thật sự thay đổi từ thiết bị này đến thiết bị khác. Tuy nhiên, bạn sẽ thấy rằng các tiện ích cấu hình router cho các router không dây của các nhà cung cấp khác nhau rất tương tự về cách các xác lập được nhóm lại trên những màn hình cấu hình.

24. Cấu hình các xác lập Internet

Trước khi bạn bắt đầu

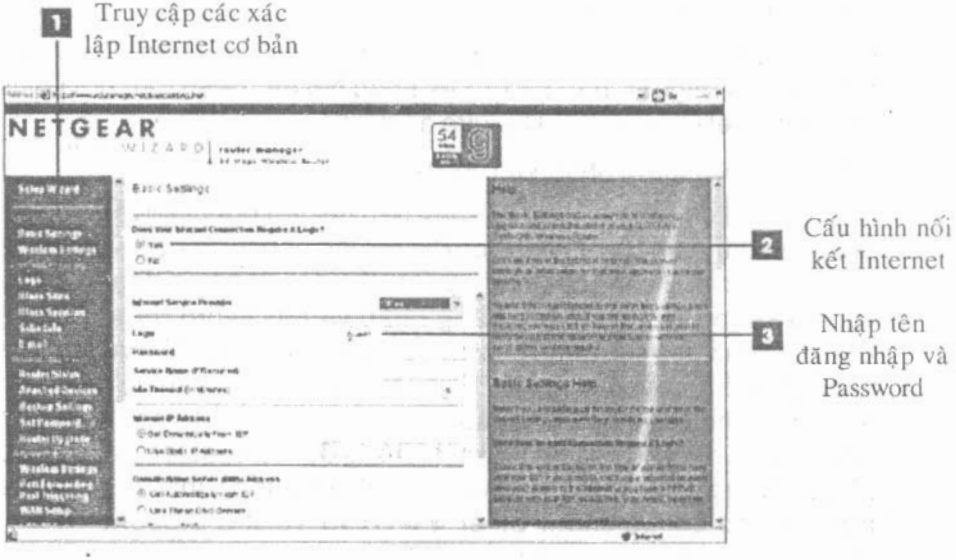
22. Truy cập cấu hình Router

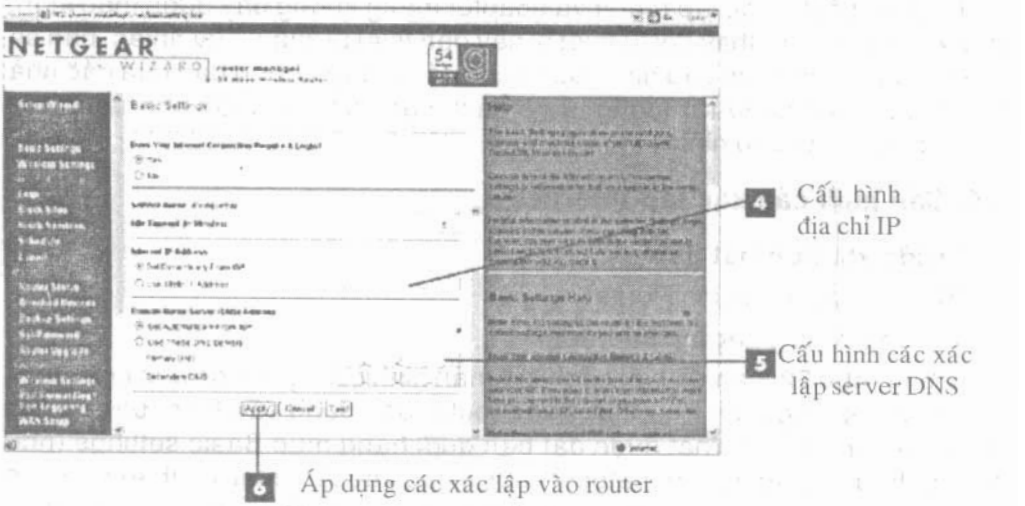
23. Bàn về các xác lập Internet

Trong **mục 22**, bạn đã biết cách mở màn hình configuration settings chính cho router không dây. Phụ thuộc vào router bạn đang cấu hình, bạn có thể thấy các xác lập Internet được đặt bên dưới hạng mục Basic settings (như trường hợp với các router Netgear) bởi vì các xác lập Internet thiết yếu cho router cung cấp cho mạng một nối kết Internet. Tuy nhiên, bạn có thể tìm thấy các xác lập Internet được đặt trong hạng mục riêng của chúng. Ví dụ, bạn có thể truy cập chúng bằng cách sử dụng một link có tên là Internet settings).

Khi bạn không thể tự mình cấu hình thành thạo những xác lập này, hãy sử dụng CD này cài đặt với router WiFi. Nó dẫn dắt bạn qua việc cài đặt cơ bản router. CD nên được đặt trong máy tính được nối trực tiếp với router WiFi bởi một cáp LAN.

24. Cấu hình các xác lập Internet





1. Truy cập các xác lập Internet cơ bản

   Nối kết với router không dây bằng cách sử dụng trình duyệt web của máy tính (nhập URL cho router và cung cấp tên đăng nhập và password mà bạn đã cung cấp trong tài liệu khởi động nhanh của router). Trong cửa sổ trình duyệt, chọn hạng mục setting cho phép cấu hình các xác lập Internet cho router (chẳng hạn như Basic Settings trên một router Netgear).

2. Cấu hình nối kết Internet

   Nhấp nút tùy chọn mô tả tốt nhất nối kết Internet của bạn. Ví dụ trên một router Netgear, bạn nhấp Yes hoặc No để trả lời câu hỏi Does Your Internet Connection Require a Login?

3. Nhập một tên đăng nhập và Password

   Nếu bạn đã chọn No ở bước 2, hãy tiếp tục với bước 4. Nếu không, nhập tên đăng nhập và password trong các hộp thích hợp. Thông tin này đã được ISP cung cấp cho bạn khi lần đầu tiên bạn đăng ký dịch vụ. Nó không giống với tên đăng nhập và password router. Tham khảo tài liệu được cung cấp cho bạn bởi nhà cung cấp dịch vụ Internet hoặc gọi bộ phận hỗ trợ của ISP để bảo đảm rằng bạn có thông tin này. Hãy nhớ các nhà cung cấp băng tần rộng chẳng hạn như dịch vụ Road Runner của Time Warner không đòi hỏi một tên đăng nhập và password Internet. Trong danh sách xổ xuống Internet service provider, có ba lựa chọn: Other, PPTP và Telstra Bigpond. Ở Mỹ, hãy chắc chắn Other được chọn, đây là loại nối kết ISP phổ biến nhất mà bạn sử dụng (thật ra nó là PPoE) vốn là giao thức point-to-point được sử dụng với nhà cung cấp dịch vụ Internet). Nếu bạn ở Áo, có thể bạn phải chọn PPTP (một giao thức phần mềm khác để kết nối với Internet). Nếu bạn ở Úc, có thể bạn phải chọn Telstra Bigpond. Lần nữa, hãy trao đổi với nhà cung cấp dịch vụ Internet của

bạn trước khi cấu hình router WiFi để chắc chắn rằng bạn đã có thông tin thích hợp.

4. Cấu hình địa chỉ IP

   Việc bạn nhận được địa chỉ IP một cách tự động (nó sẽ là địa chỉ IP cho router WiFi), từ nhà cung cấp dịch vụ Internet bằng cách sử dụng DHCP hay được gán một địa chỉ IP tĩnh là tùy thuộc vào ISP. Nếu bạn sử dụng một địa chỉ IP tĩnh để kết nối với Internet (vốn đã được cung cấp cho bạn khi bạn đăng ký dịch vụ Internet của ISP), hãy nhập địa chỉ IP trong các hộp thích hợp. Nếu không, chọn tùy chọn Get Dynamically from ISP.

5. Cấu hình các xác lập server DNS

   Nếu bạn nhận được địa chỉ IP một cách tự động thông qua DHCP, router WiFi cũng tự động nhận được các địa chỉ server DNS chính và phụ. Tuy nhiên, nếu bạn sử dụng một địa chỉ IP tĩnh mà ISP gán cho bạn, bạn cũng phải nhập các địa chỉ IP của các server DNS chính và phụ (các server DNS của ISP) trong các hộp thích hợp. Nếu không, chọn tùy chọn Get Automatically from ISP.

   Trước khi bạn cố cấu hình router WiFi, hãy xem qua tài liệu mà bạn đã nhận khi đăng ký với dịch vụ Internet ISP của bạn. Nếu bạn không có tất cả thông tin bạn cần, hãy gọi cho bộ phận trợ giúp của ISP. Có lẽ họ sẽ cho bạn biết rằng họ có thể thiết lập mạng WiFi của bạn với một chi phí nào đó. Hãy lễ phép từ chối yêu cầu này. Hỏi họ về những thông tin sau đây:

   - *Tôi có cần một tên đăng nhập và password để kết nối với Internet hay không? Có hoặc không? Nếu có, tên đăng nhập và password của tôi là gì? Tôi có nhận được địa chỉ IP một cách động hay không? Có hay không? Nếu không, địa chỉ IP của tôi là gì và các địa chỉ IP của các server DNS chính và phụ được bảo trì bởi ISP là gì?*

6. Áp dụng các xác lập cho router

   Sau khi nhập thông tin được yêu cầu, nhấp nút Apply (hoặc nút vốn lưu xác nhận router cho router cụ thể của bạn). Bây giờ router không dây được thiết lập để truy cập Internet bằng cách sử dụng ISP và thiết bị nối kết băng tần rộng mà router được nối với.

25. Bàn về các xác lập Wireless

Trước khi bạn bắt đầu	Xem thêm
21. Bàn về việc cấu hình Router không dây	**Mục 76**
22. Truy cập cấu hình Router	**Mục 77**
	Mục 78
	Mục 40

Trong mục 24, bạn được cung cấp thông tin để router không dây truy cập Internet bằng cách sử dụng một thiết bị nối kết băng tần rộng (modem cáp hoặc modem DSL). Những tùy chọn cấu hình cơ bản khác mà bạn nên xác lập trước khi đăng nhập vào router lần đầu tiên là các xác lập wireless của router. Những xác lập này bao gồm tên mạng SSID của nó), khu vực mà mạng được định vị (chẳng hạn như United States), kênh của router (tần số mà router sẽ vận hành) và loại chế độ WLAN (802.11g và 802.11b) mà router hỗ trợ.

Ghi chú

Nếu mạng của bạn bao gồm những máy tính sử dụng các adapter mạng 802.11b, chúng có thể giao tiếp với router không dây miễn là bạn cấu hình router để hỗ trợ chế độ wireless ban đầu này.

Phụ thuộc vào router cụ thể, màn hình cấu hình wireless có thể bao gồm những xác lập cho những xác lập an ninh wireless của router. Mục 70 giới thiệu an ninh wireless của router không dây, xác lập an ninh mà bạn cấu hình trên router cũng phải được cấu hình trên một máy tính vốn nối kết với mạng bằng một adapter không dây (nếu không, máy tính không thể kết nối với mạng). Một biện pháp an ninh đơn giản chẳng hạn như tắt các thông báo truyền đại chúng SSID thật sự "che giấu" mạng WiFi của bạn khỏi những người đang quét tìm các nối kết WiFi có sẵn. Những biện pháp an ninh phức tạp hơn như Wired Equivalent Privacy (WEP) hoặc WiFi Protected Access (WPA) sử dụng sự mã hóa và những chiến lược khác để bảo vệ an toàn mạng WiFi.

26. Cấu hình các xác lập Wireless

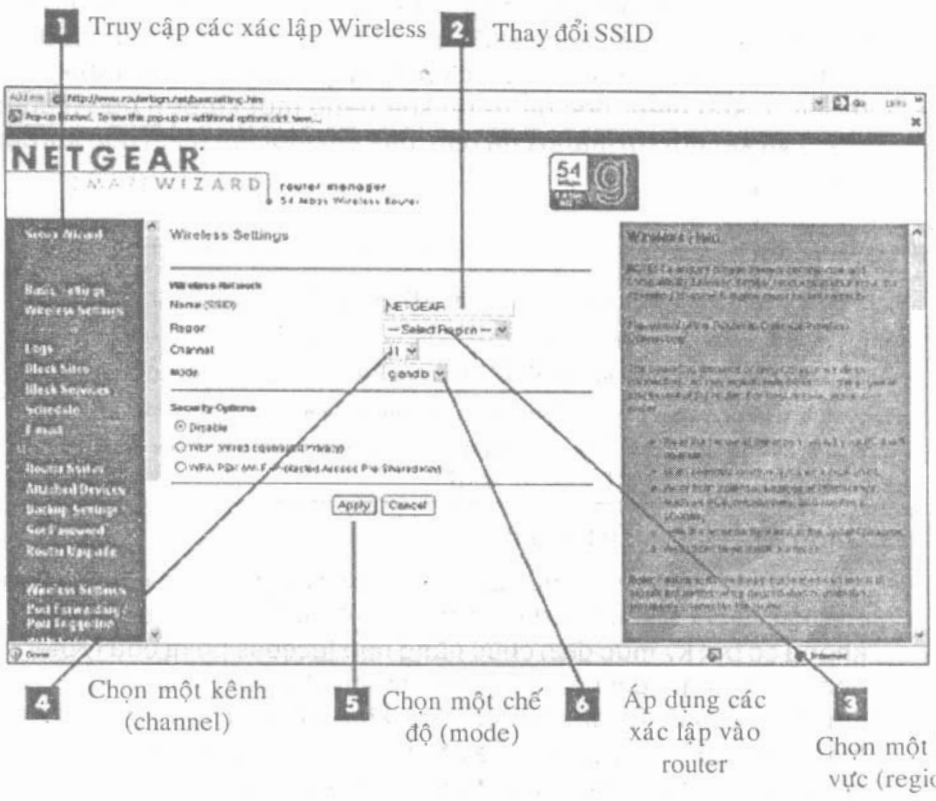
Trước khi bạn bắt đầu

22. Truy cập cấu hình Router

25. Bàn về các xác lập Wireless

Trong **mục 22**, bạn đã học cách mở màn hình Configuration Settings của router không dây. Trong **mục 24**, bạn đã cung cấp thông tin để router không dây có thể truy cập Internet bằng cách sử dụng thiết bị kết nối băng tần rộng (cáp hoặc modem DSL). Ngoài các xác lập Internet, bạn nên thiết lập các xác lập wireless cho router lần đầu tiên bạn truy cập các xác lập cấu hình. Bạn có thể thay đổi những xác lập này khi cần thiết trong tương lai. Trong một số trường hợp, có thể bạn phải thử các xác lập kênh (channel) khác nhau cho router bởi vì router không dây có thể nhiễu sóng với bất kỳ điện thoại kỹ thuật số mà bạn sử dụng trong nhà hoặc văn phòng vốn có thể chạy trong cùng một tần số.

26. Cấu hình các xác lập Wireless của Router



1. Truy cập các xác lập Wireless

Nối kết với router không dây bằng cách sử dụng trình duyệt web của máy tính (nhập URL cho router và cung cấp ID đăng nhập và password cho tài khoản quản trị của router). Trong cửa sổ trình duyệt, chọn hạng mục settings cho phép cấu hình các xác lập wireless cho router (chẳng hạn như Wireless Settings trên một router Netgear).

Ghi chú

Một số router không dây chẳng hạn như các router được sản xuất bởi Netgear cung cấp một nút Test trên các màn hình cấu hình khác nhau. Nhấp nút Test để kiểm tra các xác lập mà bạn đã nhập để xem chúng có hoạt động hay không trước khi bạn áp dụng và lưu chúng sang router.

2. Thay đổi SSID

Nhập tên mới cho mạng không dây trong hộp SSID. Tên có thể dài đến 32 ký tự. Các tên mạng nhạy kiểu chữ, do đó hãy ghi nhớ điều này khi tạo tên mới. Để dễ dàng nhận dạng mạng cho những người

dùng của bạn (và không bị nhầm lẫn bởi một người hàng xóm nào đó ngẫu nhiên phát hiện mạng WiFi của bạn), chọn một tên có tính mô tả. Ví dụ đối với mạng WiFi gia đình, bạn có thể muốn sử dụng SSID habrakenwifi hoặc habraken-family. Nếu bạn cảm thấy cần một tên "khó hiểu" hơn để tránh khả năng một kẻ bên ngoài đoán SSID và kết nối với mạng của bạn, hãy tạo một tên thích hợp khi cần thiết.

Ghi chú

Các thông báo truyền đại chúng (broadcast) SSID từ access point của router WiFi có thể được tắt. Broadcast SSID chỉ là router thông báo trên kênh vô tuyến được cấu hình rằng mạng WiFi của bạn hiện hữu. Việc tắt các broadcast sẽ từ chối những người khác chẳng hạn như những người hàng xóm lân cận hoặc người nào đó đậu xe trên đường không quét tìm mạng của bạn. Xem mục 78 để biết thông tin về cách tắt broadcast SSID.

3. Chọn một khu vực (Region)

   Bạn phải xác định một khu vực cho router. Nhấp danh sách xổ xuống Region và chọn khu vực thích hợp. Việc chọn một khu vực sẽ thật sự không có bất kỳ mục đích chức năng nào (access point của router sẽ hoạt động thậm chí nếu bạn chọn nhầm khu vực). Tuy nhiên ở Mỹ luật pháp quy định bạn phải xác định khu vực là United States. Ở Mỹ, thậm chí phổ "công cộng" của các tín hiệu vô tuyến được kiểm soát và được quy định bởi ủy ban truyền thông liên bang (FCC) và luật. Bên ngoài nước Mỹ, các luật thay đổi, do đó việc chọn khu vực thích hợp chẳng hạn như Mexico hoặc South America thật sự chỉ là sự xác nhận của bạn mà bạn hiểu rằng phổ vô tuyến công cộng có thể hoặc không thể được quản lý bởi một cơ quan chính phủ trong khu vực của bạn.

4. Chọn một kênh (Channel)

   Kênh là dãy tần số mà router không dây được sử dụng để giao tiếp với các máy tính được vận hành bằng wireless. Một giá trị mặc định thường được cung cấp bởi nhà sản xuất router. Thay đổi giá trị khi cần thiết bằng cách sử dụng danh sách xổ xuống Channel, đặc biệt nếu bạn gặp phải sự nhiễu với các điện thoại gia đình hoặc những thiết bị kỹ thuật số không dây khác. Trong hầu hết các trường hợp, bạn có thể đi cùng với giá trị mặc định. Hãy nhớ rằng tất cả máy tính được vận hành bằng WiFi phải được cấu hình để sử dụng cùng một kênh tín hiệu vô tuyến mà bạn xác lập trên router. **Xem mục 33** để biết thêm thông tin.

Ghi chú

Khi bạn quét tìm các mạng WiFi có sẵn bằng cách sử dụng một máy tính được bật WiFi, máy tính duyệt qua tất cả kênh vô tuyến có sẵn nhằm tìm kiếm các SSID hoặc các tên mạng WiFi. Khi bạn kết nối SSID bằng cách sử dụng mạng WiFi (hoặc tên), kênh được xác lập tự động trên adapter mạng WiFi trên máy tính. Khi bạn tắt các broadcast SSID, bạn không thể kết nối với access point WiFi bằng cách tìm SSID. Trong trường hợp đó các adapter mạng WiFi trên máy tính mạng phải được cấu hình với cùng một SSID và kênh vô tuyến đã được cấu hình trên router WiFi.

5. Chọn một chế độ (Mode)

   Nhấp danh sách xổ xuống Mode (hoặc một tên tùy chọn tương tự trên màn hình cấu hình của router) để xác lập chế độ mà router sẽ hỗ trợ. Trong hầu hết các trường hợp, xác lập g và b là xác lập mặc định và hỗ trợ các thiết bị 802.11g và 802.11b.

6. Áp dụng các xác lập cho Router

   Sau khi cấu hình các xác lập wireless cho router, nhấp nút Apply để lưu cấu hình của router.

THỦ THUẬT: Khi bạn đã hoàn tất việc cấu hình router, bạn nên đăng xuất (log off) router. Chọn link Logoff trên màn hình cấu hình của router (tên của link này thay đổi từ router này đến router khác). Ví dụ trên màn hình cấu hình router WiFi của Netgear, bạn phải cuộn hết đến cuối cửa sổ trình duyệt và sau đó chọn log on nằm ở phía bên trái màn hình. Log off thì tốt hơn là chỉ đóng cửa sổ trình duyệt.

Chương 5

CÀI ĐẶT VÀ CẤU HÌNH CÁC ADAPTER KHÔNG DÂY

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *27. Bàn về các adapter mạng không dây*
- *28. Quyết định khả năng nâng cấp của các máy tính hiện tại*
- *29. Cài đặt một adapter không dây*
- *30. Cài đặt tiện ích phần mềm adapter*
- *31. Kiểm tra việc cài đặt adapter*
- *32. Bàn về việc cấu hình adapter không dây*
- *33. Cấu hình adapter và kết nối với router không dây*
- *34. Cấu hình adapter để nối mạng giữa các máy tính*
- *35. Tạo các profile cấu hình*
- *36. Bàn về việc cập nhật một Driver Adapter*

Một adapter mạng WiFi cho phép một máy tính gia nhập vào mạng không dây. Chương này sẽ xem xét các adapter mạng không dây và cách cài đặt và cấu hình một adapter để nó có thể giao tiếp với router.

27. Bàn về các Adapter mạng không dây

Để một máy tính giao tiếp trên một mạng hữu tuyến hoặc không dây, máy tính phải được trang bị một adapter (bộ điều hợp) mạng. Adapter mạng cung cấp nối kết giữa máy tính và phương tiện truyền dữ liệu của mạng. Trên một mạng hữu tuyến, phương tiện này thường là một dây CAT 5 đồng. Trên một mạng vô tuyến, phương tiện là một tín hiệu vô tuyến.

Adapter mạng, dù là hữu tuyến hay không cây có trách nhiệm lấy dữ liệu từ máy tính và chuyển đổi nó thành một dạng (một luồng dữ liệu) mà có thể di chuyển qua phương tiện mạng. Các adapter mạng thường chứa một bộ thu phát (bộ phát/bộ thu) nhằm cho phép chuyển đổi dữ liệu (dữ liệu được chuyển đổi khi nó được nhận để máy tính xử lý).

Các adapter mạng không dây có thể được thêm vào một máy tính notebook hoặc desktop (nếu có sẵn một khe mở rộng còn trống). Hầu hết các máy tính notebook mới đã được lắp đặt một adapter WiFi và hầu hết các nhà sản xuất máy tính cung cấp một tùy chọn adapter WiFi cho những máy tính desktop mà họ bán. Xem **mục 28** để biết thêm thông tin về việc máy tính hiện đại của bạn có thể hỗ trợ một adapter mạng không dây hay không.

Ghi chú

Các nhà sản xuất bộ xử lý PC chẳng hạn như Intel và AMD đã phát triển các bộ xử lý máy tính (đầu não của máy tính) cho những máy tính notebook vốn được tích hợp chặt chẽ với những tính năng công nghệ di động chẳng hạn như các adapter mạng WiFi. Ví dụ, Intel cung cấp công nghệ Centrino Mobile và ADM cung cấp công nghệ AMD Turion 64 Mobile. Bất kỳ máy tính notebook mà bạn mua có logo của một trong hai công nghệ di động (mobile) này thì được thiết kế đặc biệt cho nối mạng WiFi.

Trong các lựa chọn liên quan đến việc thêm một adapter WiFi và máy tính hiện tại, bạn có thể thêm một adapter WiFi và một khe mở rộng (expansion slot) hoặc bạn có thể sử dụng một adapter WiFi ngoài vốn nối với một cổng USB trên máy tính. Lựa chọn tốt nhất và dễ nhất là thêm một adapter WiFi ngoài USB vào máy tính. Thậm chí các máy tính đời cũ hơn (bao gồm nhiều máy tính có cách đây lên đến 6 hoặc 8 năm) thường có tối thiểu một cổng USB.

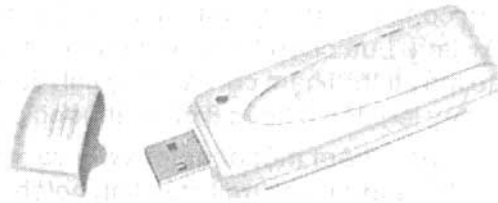
Đối với việc thêm một adapter WiFi vào một khe mở rộng trên máy tính, adapter WiFi add-on cho một máy tính notebook rất khác với adapter WiFi mà bạn thường thêm vào một máy tính desktop. Các máy tính notebook thường cung cấp tối thiểu một khe mở rộng PCMCIA (Personal Computer Memory Card International Association) vốn được sử dụng để thêm các thành phần chẳng hạn như các adapter mạng (chẳng hạn như một card WiFi). Nâng cấp một máy notebook là chỉ là việc trượt một card mở rộng (PCMCIA) nhỏ vào khe mở rộng.

THỦ THUẬT: Các máy tính notebook có một trong ba loại PCMCIA: Type 1, Type 2 hoặc Type 3. Từng loại khe (slot) này dành riêng cho một loại card. Tham khảo tài liệu hướng dẫn để xác định loại khe trên máy tính. Hầu hết các adapter WiFi là các card Type 2 và hầu hết máy tính notebook cung cấp một khe Type 2 hoặc một khe PCMCIA có thể chứa nhiều loại card chẳng hạn như Type 1 và Type 2. Thế hệ mới nhất của các loại card

adapter PCMCIA dành cho các máy notebook còn được gọi là các card CardBus.

Các máy tính desktop (kể cả các máy dạng tower) thường cung cấp một hoặc nhiều khe mở rộng PCMCIA. Khe Peripheral Component Interconnect (PCI) là một khe mở rộng trên motherboard của máy tính desktop/tower và là loại khe mở rộng chuẩn cho các motherboard tương thích Intel (board mạch chính cho máy tính). Nâng cấp một máy tính desktop đòi hỏi bạn mở case (thùng máy) và lắp đặt adapter mạng trong một khe PCI trống. Như đã được đề cập, hầu hết các máy tính desktop tower cung cấp tối thiểu một hoặc hai khe PCI. Nếu bạn đã không thêm bất kỳ thiết bị ngoại vi chẳng hạn như một card âm thanh hoặc video adapter mới vào máy tính, có lẽ đã có một khe dành cho card adapter. Tuy nhiên, bạn có thể chỉ chắc chắn bằng việc mở case và kiểm tra motherboard để xem có sẵn các khe hay không.

Bởi vì các máy tính notebook và máy tính desktop/tower có các cổng USB, một trong hai loại máy tính có thể được nâng cấp lên WiFi bằng cách sử dụng một adapter WiFi USB ngoài. Các máy tính mới hơn thường có nhiều cổng USB; các máy notebook mới thường có tối thiểu 2 cổng USB và nhiều máy tính desktop có các cổng USB ở phía sau và phía trước case máy tính. Nếu bạn muốn sử dụng một adapter WiFi USB ngoài nhưng hết cổng USB, bạn có thể mua một hub USB vốn mở rộng số cổng USB có sẵn trên máy tính. Hub USB thường là một thiết bị khá nhỏ nối với một trong các cổng USB hiện có trên máy tính. Các thiết bị USB bổ sung (chẳng hạn như adapter WiFi) sau đó có thể được nối với Hub.



Một adapter nối mạng không dây USB có thể cho máy tính có sẵn cổng USB khả năng giao tiếp trên một mạng không dây.

Đối với việc chọn thật sự một adapter WiFi cho máy tính notebook hoặc desktop, hãy chắc chắn bạn chọn một adapter tận dụng tốc độ nối kết mà router không dây cung cấp. Nếu bạn sử dụng một router G không dây, nghĩa là một router được sản xuất theo những thông số kỹ thuật của các chuẩn 802.11g, bạn nên chọn một adapter mạng G không dây. Mặc dù một adapter WiFi không dây 802.11b (wireless B) có thể nối kết với một router/access point G không dây, nhưng wireless B (với tốc độ nối kết 11 Mbps) sẽ không cho bạn nối kết tốc độ cao hơn tốc độ mà các adapter wireless G cung cấp (lên đến 54 Mbps).

28. Quyết định khả năng nâng cấp của các máy tính hiện tại

Trước khi bạn bắt đầu

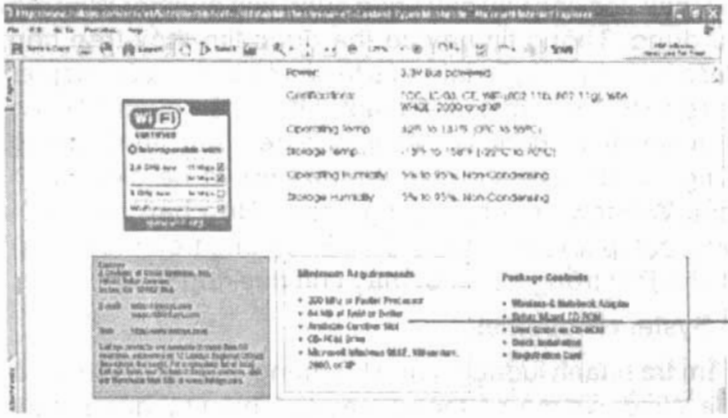
27. Bàn về các Adapter mạng không dây

Việc bạn nâng cấp máy tính hiện tại với một adapter mạng WiFi hay không là tùy thuộc vào cấu hình phần cứng của hệ thống và hệ điều hành) thường là phiên bản của Windows) mà bạn đang chạy trên máy tính.

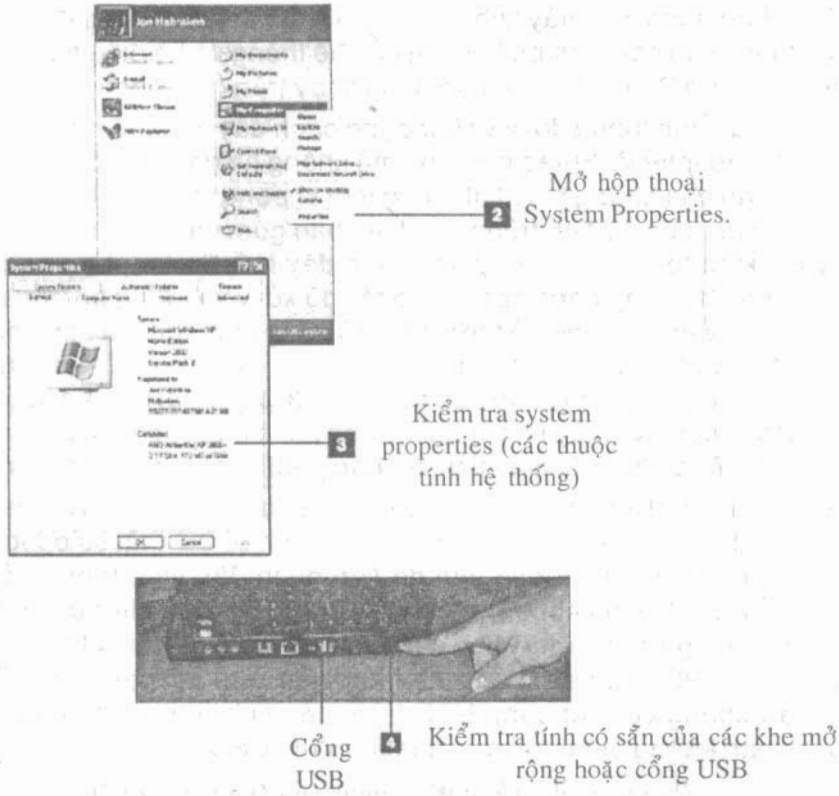
Nếu máy tính tương đối mới (sử dụng cách đây 1 đến 5 năm), bạn có thể thêm một adapter WiFi vào máy tính mà không hề gặp rắc rối (các cổng USB đã là chuẩn cho những máy tính trong một khoảng thời gian). Điều này tương tự đối với tất cả máy tính trong gia đình, bao gồm các máy notebook và các máy desktop/tower. Nếu máy tính cách đây hơn 6 năm, bạn có thể ở trên "đỉnh" của khả năng nâng cấp xét về tốc độ xử lý và lượng bộ nhớ mà nó có. Quyết định xem có đáng bỏ thêm tiền để nâng cấp một máy tính cũ hơn sao cho một adapter WiFi có thể được thêm vào hay không. Nếu bạn thật sự muốn nâng cấp một máy tính gần như lỗi thời, bạn phải nghiên cứu thêm. Về chi phí thấp của các máy tính, mua một máy tính mới vào thời điểm này có thể rẻ như cố nâng cấp một máy tính cũ, bạn phải tự quyết định điều này.

Đừng mua bất kỳ thiết bị nâng cấp WiFi cho máy tính (máy tính notebook hoặc desktop) trước khi bạn quyết định máy tính có thể thật sự được nâng cấp hay không. Cũng có một số vấn đề liên quan đến việc thêm một adapter WiFi. Nếu máy tính notebook không có một khe CardBus trống bạn không thể thêm một adapter. Nếu máy tính desktop (bao gồm các máy tower) không có sẵn một khe PCI, bạn sẽ không thể thêm một card adapter trong. Sau cùng, nếu bạn không có một cổng USB trên máy tính (notebook hoặc desktop/tower), bạn không thể thêm một adapter WiFi USB.

28. Quyết định khả năng nâng cấp của các máy tính hiện tại.



Kiểm tra các yêu cầu phần cứng cho adapter WiFi



1. Kiểm tra các yêu cầu phần cứng cho adapter WiFi

   Trước khi mua, hãy đọc các yêu cầu phần cứng cho adapter WiFi mà bạn muốn sử dụng. Thông tin này có thể được tìm thấy trên hộp adapter wireless hoặc trực tuyến tại website của nhà sản xuất adapter WiFi. Các yêu cầu tối thiểu cho một adapter WiFi liên quan đến tốc độ bộ xử lý của máy tính, lượng RAM (bộ nhớ trên máy tính), không gian ổ đĩa cứng có sẵn của nó (cho phần mềm) và hệ điều hành (phiên bản của Windows mà bạn đang chạy). Nếu bạn mua một card WiFi trong, bạn phải có một khe CardBus trống trên một desktop hoặc một khe PCI trống trên một máy tính desktop/tower.

2. Mở hộp thoại System Properties

   Bạn có thể kiểm tra nhanh lượng bộ nhớ hệ thống, tốc độ bộ xử lý và phiên bản của Windows mà hệ thống máy tính hiện tại đang chạy bằng cách sử dụng hộp thoại System Properties. Để mở hộp thoại, nhấp Start, sau đó nhấp phải biểu tượng My Computer trên menu Start. Từ menu ngữ cảnh vừa mở ra, chọn Properties. Hộp thoại System Properties xuất hiện.

3. Kiểm tra System Properties

   Hãy chắc chắn tab General được chọn trong hộp thoại System Properties và ghi chú thông tin được cung cấp. Tab này cung cấp phiên

bản hệ điều hành mà bạn đang chạy (kể các các service pack được cài đặt), lượng bộ nhớ hệ thống và tốc độ bộ xử lý cho hệ thống. Hãy chắc chắn thông tin bạn tích lũy về các yêu cầu adapter ở bước 1 khớp hoặc vượt quá bởi các thuộc tính hệ thống của máy tính. Chúng không cần phải khớp chính xác miễn là máy tính có những thông số kỹ thuật tối thiểu mà adapter WiFi cần.

THỦ THUẬT: Cho dù bạn lập kế hoạch tốt như thế nào đi nữa, luôn có khả năng xảy ra các sự cố khi bạn thêm phần cứng mới vào một máy tính. Hãy chắc chắn bạn đã cập nhật bản cài đặt Windows XP với các service pack mới nhất. Kiểm tra website của adapter WiFi mà bạn dự định mua và xem có bất kỳ vấn đề với khả năng tương thích và service pack Windows XP hay không. Nếu website của nhà sản xuất cung cấp phần mềm cài đặt mới hơn những gì có sẵn trên CD đính kèm với adapter, bạn nên download nó và sử dụng nó khi bạn cài đặt phần mềm cho adapter. Một chút hoạch định trước và nghiên cứu sẽ giúp bạn tránh khỏi nhiều phiền toái trong việc lắp đặt adapter WiFi mới.

---

4. Kiểm tra tính có sẵn của các khe mở rộng hoặc cổng USB

Kiểm tra máy tính notebook hoặc desktop để nhận biết tính có sẵn của các khe mở rộng hoặc các cổng USB. Ví dụ, trên một máy tính notebook, bạn tìm một khe card có sẵn thường được đặt ở một phía máy tính. Trên một máy tính desktop/tower, nhìn vào phía sau của máy tính và xem các nách khe kim loại vẫn còn trên bất kỳ khe mở rộng hay không; điều này thường có nghĩa là một khe đã không được sử dụng. Mở khe để bảo đảm rằng PCI có sẵn. Nếu bạn tìm các cổng USB mà bạn có thể nối một USB adapter ngoài vào, hãy nhìn ở phía trước hoặc cạnh bên của máy tính.

THỦ THUẬT: Nếu bạn muốn cần thêm thông tin về hệ thống hơn khả năng bạn thu thập sử dụng các bước được cung cấp, sử dụng tiện ích Windows System Information để xem xét phần cứng và phần mềm máy tính một cách chuyên sâu hơn. (Chú ý rằng tiện ích này có thể gây nhầm lẫn bởi vì nó cung cấp nhiều thông tin hơn bạn cần. Nhấp Start và trỏ vào All Programs, sau đó chọn Accessories, System Tools, System Information. Nhấp một hạng mục phần cứng cụ thể (chẳng hạn như Memory hoặc USB để xem các thông số kỹ thuật cho thành phần phần cứng máy tính cụ thể đó). Nếu có đủ tốc độ bộ xử lý, bộ nhớ

và không gian ổ đĩa cứng cho adapter mà bạn đang xem xét mua, việc kiểm tra PC đủ để quyết định khả năng nâng cấp nó. Ví dụ, nếu có một cổng USB trống (tốc độ của cổng không quan trọng, các adapter WiFi có thể được sử dụng trên các adapter WiFi 1.1 và 2.0), bạn có thể thêm một adapter USB. Nếu bạn có một máy tính note book có nhiều khe mở rộng còn trống, tham khảo tài liệu notebook để quyết định loại khe có sẵn (hoặc sử dụng tiện ích Windows System Information như được đề cập) và sau đó thêm loại card adapter WiFi thích hợp. Điều cốt yếu là việc có sẵn của các khe và cổng thật sự là những gì quyết định loại adapter WiFi add-on mà bạn sẽ mua đặc biệt nếu PC của bạn tương đối mới. Bạn nên sử dụng một adapter WiFi USB trong hầu hết các trường hợp đặc biệt trên một máy tính desktop/tower (thêm một adapter WiFi vào một khe PCJ không dễ dàng như thế). Nếu máy tính notebook/laptop có một khe trống, bạn nên lấp đầy khe đó vì các card PCMCJA nhỏ dễ gắn vừa vào khe. Việc biết hệ thống của bạn sẽ giúp bạn sẽ tham khảo các website của các nhà sản xuất adapter WiFi (chẳng hạn như www.netgear.com và www.linksys.com) và chọn sự nâng cấp adapter WiFi thích hợp trước khi bạn đi đến cửa hàng hoặc mua adapter trực tuyến.

29. Cài đặt một Adapter không dây

Trước khi bạn bắt đầu

28. Quyết định khả năng nâng cấp của các máy tính hiện tại

Sau khi bạn đã kiểm tra hệ thống xét về khả năng tương thích của hệ thống với những adapter WiFi có sẵn, bạn có thể mua adapter mạng thích hợp cho máy tính. Nếu bạn thêm các adapter WiFi vào nhiều máy tính và các thông số kỹ thuật máy tính hỗ trợ nó, hãy mua cùng một adapter cho tất cả máy tính. Bởi vì một card PCMCIA laptop sẽ không hoạt động trong một máy tính desktop hoặc tower, bạn nên mua các loại adapter khác nhau mà bạn cần từ cùng một nhà sản xuất để có thể tận dụng các tiện ích phần mềm giống nhau hoặc tương tự vào việc cấu hình và quản lý các adapter mạng.

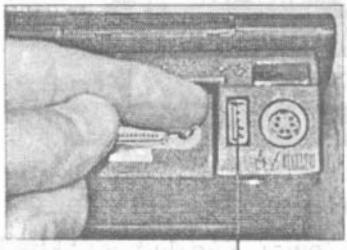
THỦ THUẬT: Nếu bạn đã mua một WiFi router wireless G (802.11g), bạn nên mua các adapter mạng wireless G. Sau đó bạn tận dụng tối đa router và các adapter WiFi xét về tốc độ kết nối tối đa. Bạn cũng nên mua các adapter WiFi và router WiFi cùng nhãn hiệu để ngăn ngừa bất kỳ

vấn đề tương thích có thể có giữa phần cứng và các nhà sản xuất khác nhau.

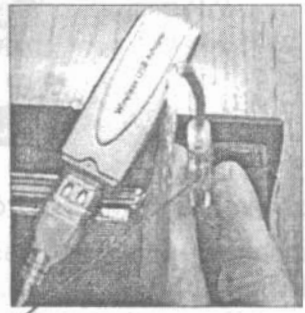
Bước kế tiếp là lắp đặt adapter. Đối với các máy tính notebook, đây là một vấn đề trượt card WiFi vào khe mở rộng. Nếu bạn nâng cấp một hệ thống desktop và muốn lắp đặt một adapter WiFi trong, bạn cần một chìa vặn vít để mở case và gắn card cho một khe trên motherboard. Như được đề cập trước đó, cách dễ nhất để nâng cấp một trong hai loại hệ thống (notebook hoặc desktop) là sử dụng một adapter WiFi USB, không cần các công cụ để lắp đặt. Các bước sau đây trình bày cho bạn thông tin về việc lắp đặt một adapter WiFi USB, PCI hoặc PCMCIA.

THỦ THUẬT: Điều quan trọng là bạn nên đọc hướng dẫn lắp đặt đính kèm adapter WiFi mà bạn mua. Trong nhiều trường hợp, một trang "khởi động nhanh" liệt kê các bước quan trọng nhất trong tiến trình lắp đặt. Phần cứng mới không hoạt động trên máy tính cho đến khi bạn cài đặt phần mềm và các driver (phần mềm cho phép thiết bị giao tiếp với hệ điều hành) được cung cấp với thiết bị phần cứng. Những phần mềm này thường được đặt trên một CD. Trong một số trường hợp, bạn sẽ được khuyên cài đặt phần mềm trước khi lắp đặt phần cứng. Phụ thuộc vào các bước cài đặt được cung cấp cho adapter WiFi, bạn có thể được yêu cầu hoàn thành mục 30 trước khi hoàn tất tác vụ hiện tại này.

29. Lắp đặt một adapter không dây



Xác định cổng USB



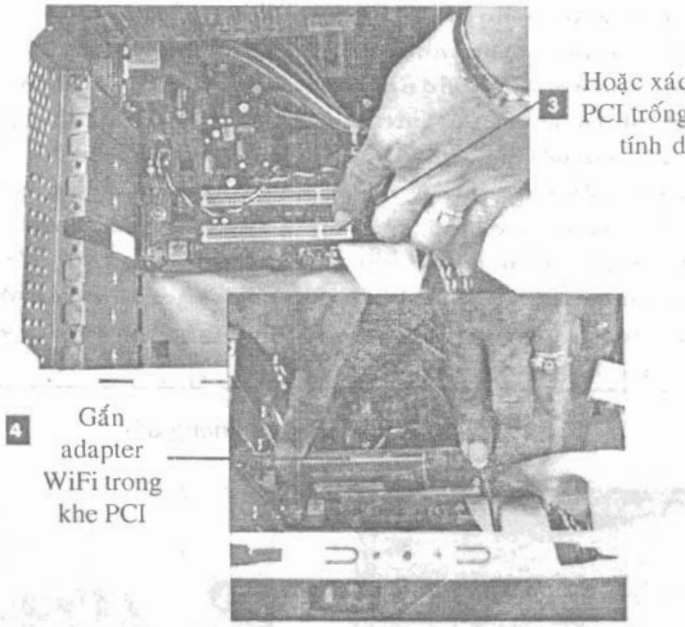
Lắp đặt adapter wireless USB

1. Xác định cổng USB

   Xác định một cổng USB trống trên máy tính mà bạn dự định sử dụng để gắn adapter WiFi mới.

2. Lắp đặt adapter WiFi USB

   Gắn adapter WiFi USB trực tiếp vào cổng USB hoặc gắn cáp USB tùy chọn từ adapter WiFi vào một cổng USB trên máy tính. Bởi vì Windows XP cung cấp công nghệ Plug and Play (nghĩa là nó nhận biết việc bổ sung phần cứng vào hệ thống máy tính), Windows nhận biết adapter WiFi USB mới và Found New Hardware Wizard mở ra. Chèn CD đính kèm với adapter USB và nhấp Next để cài đặt driver cho adapter WiFi USB mới. Nhấp Finish khi tiến trình cài đặt driver phần mềm hoàn tất. Bạn không cần phải khởi động lại sau khi cài đặt driver thiết bị. Bây giờ bạn có thể đi đến **mục 30**.



3. Hoặc xác định khe PCI trống trên máy tính Desktop

   Mở case trên máy tính desktop/tower. Xác định một khe PCI có sẵn trên motherboard. Nếu cần, tháo nắp khe kim loại bằng cách tháo vít đang giữ cố định nắp khe.

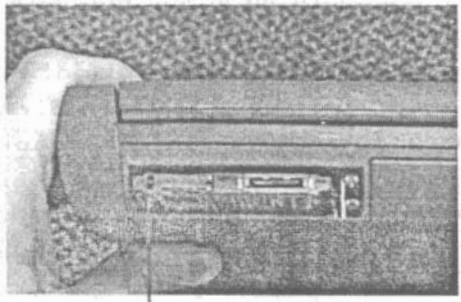
THỦ THUẬT: Nếu bạn sẽ lắp đặt một adapter WiFi trong PCI trên một PCI desktop, đừng sử dụng chìa vặn vít từ tính và chắc chắn bạn mở khe của máy tính trong một môi trường mà tĩnh điện không được sản sinh, nghĩa là bạn nên làm việc trong một căn phòng không có thảm. Bạn có thể

mua một dải đeo tay chống tĩnh điện nối với case máy tính và có chức năng tiếp đất bạn trong khi bạn làm việc trên hệ thống. Một điện tích tĩnh có thể dễ dàng làm hư hại hệ thống, do đó bạn nên cẩn thận khi mở case máy tính và làm việc xung quanh motherboard. Để lắp đặt bất kỳ adapter WiFi trong, hãy cẩn thận đọc các hướng dẫn lắp đặt đi kèm adapter.

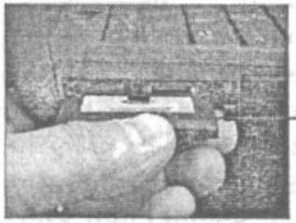
4. Gắn adapter WiFi vào khe PCI

Card adapter PCI có một ngấn nhỏ ở đáy card (hướng đến mặt trước của adapter). Đặt phần ngắn của adapter (phần ở phía trước ngấn) phía trước khe PCI. Lắc adapter PCI hướng ra phía sau máy tính để gắn adapter vào. Ấn chặt để chắn chắn adapter được lắp trong khe. Sau đó gắn vít mặt sau của adapter (phần gắn nắp khe kim loại vào) vào mặt sau của case máy tính. Gắn case của máy tính vào. Nếu card adapter có một anten tháo được, bạn có thể gắn vít anten vào card nơi nó được làm lộ ra ở phía sau case của máy tính.

Khi bạn mở hệ thống và Windows khởi động, Found New Hardware Wizard xuất hiện. Chèn CD đính kèm adapter PCI WiFi và nhấp Next để cài đặt driver cho adapter WiFi mới. Nhấp Finish khi tiến trình cài đặt driver phần mềm hoàn tất. Đi đến **mục 30**.



5 Hoặc xác định khe PCMCIA trống trên máy tính notebook



6 Gắn adapter WiFi PCMCIA vào máy tính Notebook

5. Hoặc định vị khe PCMCIA trống trên máy tính notebook.

Tắt nguồn máy tính laptop. Kiểm tra phía trái và phía phải của máy tính notebook để định vị một khe PCMCIA trống. Một số khe được che phủ bởi các cửa nắp nhựa nhỏ đẩy hướng vào trong để làm lộ ra khe.

6. Gắn adapter WiFi PCMCIA vào máy tính Notebook

Trượt adapter PCMCIA vào khe. Trượt card hết vào bên trong cho đến khi nó ăn khớp. Bật nguồn máy tính notebook; sau khi Windows khởi động, Found New Hardware Wizard xuất hiện. Chèn CD đính kèm với adapter PCI WiFi vào và nhấp Next để cài đặt driver cho adapter WiFi mới. Nhấp Finish khi tiến trình cài đặt driver phần mềm hoàn tất. Đi đến **mục 30**.

30. Cài đặt tiện ích phần mềm Adapter

Trước khi bạn bắt đầu

29. Lắp đặt một adapter không dây

Các adapter mạng WiFi add-on có phần mềm cho phép bạn cấu hình và giám sát adapter. Phần mềm được đính kèm với hầu như tất cả adapter và thường được cung cấp trên một CD. Hầu hết các nhà sản xuất các adapter WiFi cũng cho bạn khả năng download phần mềm, các driver và các bản cập nhật phần mềm kết hợp với adapter wireless cụ thể của bạn. CD không chỉ cung cấp các tiện ích cấu hình, CD còn chứa driver phần mềm mà bạn cần khi cài đặt một adapter WiFi trên PC (**xem mục 29**).

THỦ THUẬT: Trong hầu hết các trường hợp, bạn nên cài đặt tiện ích phần mềm mà nhà sản xuất adapter đã cung cấp cho adapter WiFi add-on (trừ khi được ghi chú theo cách khác bởi hướng dẫn cài đặt của nhà sản xuất). Phần mềm được thiết kế đặc biệt để cho phép bạn thay đổi cấu hình adapter WiFi sao cho adapter có thể nối kết với access point của adapter WiFi và cũng giám sát nối kết của adapter. Một số nhà sản xuất đề nghị bạn không nên cài đặt tiện ích phần mềm "đặc quyền" nếu bạn chạy Windows XP (điều này thay đổi giữa các nhà sản xuất khác nhau) bởi vì Windows XP cung cấp tiện ích Wireless Connection riêng của nó. (Các phiên bản Windows trước đây, chẳng hạn như Windows 98 không cung cấp tiện ích này. Bạn có thể sử dụng tiện ích Windows XP Wireless Connection để cấu hình và giám sát adapter WiFi. Tuy nhiên, tiện ích được cung cấp trên CD đính kèm adapter WiFi thường dễ sử dụng hơn và có những tính năng mà tiện ích Windows Wireless Connection không có.

THUẬT NGỮ CHÍNH

Driver. Phần mềm cho một thiết bị adapter chẳng hạn như mạng WiFi cho phép hệ điều hành và thiết bị giao tiếp một cách chính xác.

Mỗi adapter mạng WiFi cung cấp một tiện ích phần mềm khác để cài đặt phần mềm của adapter. Tác vụ này xem xét việc cài đặt phần mềm cho một adapter USB Netgear. Tiến trình cài đặt phần mềm của mỗi adapter sẽ khác nhau. Một số adapter WiFi đòi hỏi bạn cài đặt phần mềm (và driver) trước khi gắn adapter WiFi vào PC. Những adapter khác thường được lắp đặt trên PC trước tiên và sau đó phần mềm được tải. Trước khi cài đặt phần cứng hoặc phần mềm adapter WiFi, đọc thông tin cài đặt do nhà sản xuất cung cấp để phần cứng và phần mềm adapter WiFi được cài đặt một cách chính xác.

30. Cài đặt tiện ích phần mềm adapter



1. Bắt đầu cài đặt phần mềm

   Chèn CD đi kèm adapter vào ổ đĩa CD ROM hoặc DVD. Phần mềm trên DVD sẽ tự động mở. Chọn tùy chọn để tự động cài đặt phần mềm tiện ích của adapter (trong một số trường hợp, tùy chọn này cũng tự động cài đặt phần mềm cho adapter).

2. Chấp nhận Licensing Agreement

   Trong hầu hết các trường hợp, bạn phải xem lại và chấp nhận licensing agrement (hợp đồng đăng ký bản quyền) cho phần mềm sẽ được cài đặt trên hệ thống. Nhấp Yes và sau đó tiếp tục tiến trình cài đặt.

3. Xác định một vị trí để cài đặt.

   Bạn sẽ được cung cấp một vị trí mặc định để cài đặt phần mềm. Để thay đổi vị trí, sử dụng nút Browse và định hướng sang vị trí trên đĩa cứng nơi bạn muốn cài đặt phần mềm. Khi bạn đã nhận dạng vị trí đĩa cứng, đi đến bước kế tiếp trong wizard hoặc các hướng dẫn cài đặt.

4. Xác định một Folder chương trình

   Một folder chương trình mặc định được xác định cho bản cài đặt này. Folder này sẽ xuất hiện trên menu Start và cho phép truy cập các biểu tượng vốn khởi động tiện ích kết hợp với adapter. Phần mềm tiện ích mà bạn cài đặt được sử dụng để cấu hình và giám sát WiFi cho adapter (nối kết với router WiFi). Trong hầu hết các trường hợp, bạn sẽ muốn đi cùng với lựa chọn mặc định. Tuy nhiên để chọn một lựa chọn khác, chọn một tùy chọn folder từ danh sách được cung cấp. Sau đó nhấp Next để hoàn tất tiến trình cài đặt. Khi tiến trình cài đặt hoàn thành, bạn có thể lấy CD ra khỏi ổ đĩa của máy tính.

31. Kiểm tra việc cài đặt adapter WiFi

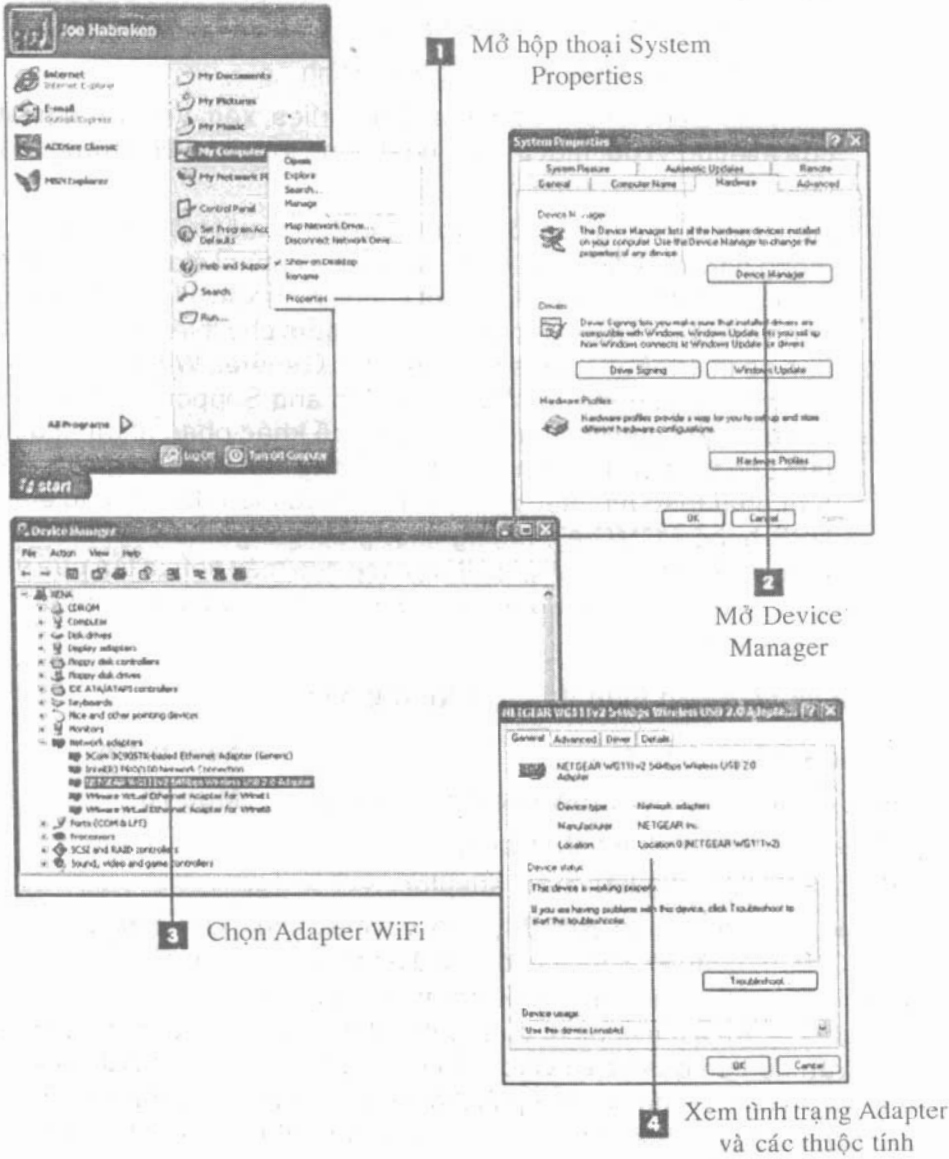
Trước khi bạn bắt đầu

29. Lắp đặt một Adapter không dây

30. Cài đặt tiện ích phần mềm Adapter

Windows XP cho bạn một cách nhanh để kiểm tra việc cài đặt phần cứng mới, bao gồm driver phần mềm của adapter mạng WiFi. Device Manager không chỉ cho phép bạn kiểm tra tình trạng của một thiết bị phần cứng cụ thể, mà nó còn cho phép bạn cập nhật hoặc phục vụ driver phần mềm cho thiết bị. Device Manager cũng cho phép dễ dàng truy cập một "troubleshooter" phần cứng nhằm giúp bạn chẩn đoán những sự cố liên quan đến một phần cứng cụ thể.

31. Kiểm tra việc cài đặt adapter WiFi



1. Mở hộp thoại System Properties

   Nhấp Start và sau đó nhấp phải biểu tượng My Computer trên menu Start. Chọn Properties từ menu ngữ cảnh vừa xuất hiện. Hộp thoại System Properties mở ra.

2. Mở Device Manager

   Trên tab Hardware của hộp thoại System Properties, nhấp nút Device Manager. Cửa sổ Device Manager xuất hiện.

3. Chọn Adapter WiFi

Trong cửa sổ Device Manager, mở rộng hạng mục Network Adapters và sau đó nhấp đôi danh sách cho adapter WiFi của bạn. Hộp thoại Properties cho adapter mở ra.

4. Xem tình trạng Adapter và các thuộc tính

Trên tab General của hộp thoại Properties, xem tình trạng (status) của thiết bị. Ví dụ, một thiết bị hoạt động tốt sẽ có tình trạng là This device is working properly.

Nếu thiết bị không hoạt động tốt, tình trạng xuất hiện dưới dạng một thông báo lỗi chẳng hạn như This device cannot start. Giả sử thiết bị được cài đặt trong máy tính một cách chính xác. Hầu hết các sự cố phần cứng liên quan đến driver phần mềm cho thiết bị. Vào lúc này, bạn có thể nhấp Troubleshoot trên tab General, Windows Help and Support Center mở ra. Windows Help and Support Center sẽ dẫn dắt bạn qua các tình huống xử lý sự cố khác nhau nhằm giúp bạn làm cho thiết bị khởi động và chạy. Trong một số trường hợp, có thể bạn phải tháo adapter WiFi (khá dễ thực hiện đối với các adapter USB hoặc PCMCIA), nhưng không dễ dàng như vậy đối với các adapter PCI bởi vì bạn phải tháo case của máy tính ra lần nữa và lặp lại thiết bị lắp đặt. Cài đặt lại driver phần mềm và tiện ích phần mềm cho thiết bị.

32. Bàn về việc cấu hình Adapter không dây

Trước khi bạn bắt đầu	Xem thêm
26. Cấu hình các xác lập Wireless của Router	**Mục 76**
29. Cài đặt một adapter không dây	
30. Cài đặt tiện ích phần mềm adapter	

Sau khi adapter mạng WiFi được nối với máy tính (dưới dạng một thiết bị USB, PCMCIA hoặc PCI) và bạn đã cài đặt driver và phần mềm cấu hình cho adapter WiFi mới, bạn có thể nối kết máy tính được bật WiFi với mạng không dây (nghĩa là với access point của router WiFi). Nhưng trước khi thảo luận những vấn đề liên quan đến việc kết nối máy tính được bật WiFi với router WiFi, chúng ta nên xem xét ý nghĩa thật sự của "cấu hình adapter WiFi". Có hai điều mà bạn phải cấu hình trên một adapter WiFi các xác lập mode (chế độ) và an ninh (security).

Chế độ liên quan đến hai cách khác nhau mà các máy tính có thể giao tiếp không dây: chế độ infrastructure hoặc chế độ Ad Hốc. Chế độ Infrastructure chỉ là các mà một chuyên gia máy tính nói rằng các máy tính trên mạng giao tiếp bằng cách kết nối với access point của router WiFi. Router WiFi có chức năng như "ngân hàng hối đoái" trung tâm cho dữ liệu của mạng khi nó di chuyển từ máy tính này đến máy tính khác. Chiến lược kết nối thay thế cho một mạng WiFi gia đình là chế độ Ad Hoc vốn cho phép các máy tính được bật WiFi kết nối trực tiếp máy tính này với máy tính khác mà không cần đến một access point. Mặc dù chế độ Ad Hoc có thể nghe có vẻ tiện lợi, nhưng nó

có các sự cố kèm theo. Trên hết, tất cả lý do chính để xây dựng một mạng WiFi gia đình là chia sẻ một nối kết Internet tốc độ cao. Điều này được thực hiện tốt nhất bằng cách sử dụng một router WiFi. Thứ hai là một lý do thật sự hợp lý không sử dụng chế độ Ad Hoc (trừ khi bạn ngồi trong một tiệm cà phê và muốn chia sẻ nhanh một file với một đồng nghiệp bằng cách kết nối trong chế độ Ad Hoc, (các thông số chế độ Ad-Hoc được tuân theo mà các nhà sản xuất adapter WiFi tuân theo thì không đòi hỏi các adapter vận hành với tốc độ truyền dữ liệu cao nhất vốn có thể lên đến 54Mbps cho một adapter mạng wireless G. Thực tế, các adapter wireless G vận hành với tốc độ chỉ 11Mbps ở chế độ Ad-Hoc, và không có cách nào để tăng tốc độ thông lượng dữ liệu.

Thuật ngữ chính

Ad Hoc mode. Một chế độ nối kết không dây từ máy tính với máy tính cho phép các máy tính được bật WiFi kết nối trực tiếp mà không giao tiếp qua một thiết bị trung gian chẳng hạn như một access point WiFi.

Để cấu hình các adapter WiFi cho chế độ Infrastructure cho chế độ bằng cấu hình adapter với đúng SSID cho mạng WiFi (như được cấu hình trên router WiFi) và bất kỳ xác lập an ninh được yêu cầu bởi những tính năng an ninh mà bạn đã bật lên router WiFi, chẳng hạn như WEP (WiFi Equivalent Privacy) và WPA (WiFi Protected Access). Để biết thêm thông tin về WEP và WPA, **xem mục 77 và 78.**



Adapter mạng WiFi được cấu hình để kết nối với mạng WiFi sử dụng SSID và các xác lập an ninh mạng tùy chọn.

Ghi chú

Các xác lập mà bạn cấu hình cho adapter WiFi để nối kết với router WiFi và access point phụ thuộc vào việc bạn đã cấu hình router như thế nào. SSID và

bất kỳ xác lập cấu hình an ninh được quyết định khi bạn cấu hình router. Sau đó bạn nhập bằng tay SSID và những xác lập cấu hình khác bằng cách sử dụng tiện ích cấu hình adapter WiFi.

Bởi vì luôn có khả năng bạn sẽ muốn cấu hình máy tính được bật WiFi để nối kết với nhiều mạng WiFi (phụ thuộc vào vị trí của bạn), bạn sẽ thấy hầu hết các tiện ích phần mềm adapter WiFi cho bạn khả năng tạo các profile cấu hình. Một profile chứa thông tin chẳng hạn như SSID và khóa an ninh (cho an ninh WEP hoặc WPA) cần để kết nối với một access point và mạng WiFi cụ thể. Rõ ràng khả năng tạo nhiều profile cấu hình đặc biệt hữu dụng khi bạn có một máy tính notebook mà bạn sử dụng tại nhiều vị trí chẳng hạn như gia đình và cơ quan. Một profile cấu hình cụ thể có thể được tạo cho từng mạng này (gia đình và cơ quan) để bạn có thể truy cập nhanh một mạng WiFi nào đó. Các profile cấu hình được giải thích trong **mục 35**.

Bạn không cần phải cấu hình adapter WiFi qua mọi mạng WiFi mà bạn truy cập, đặc biệt các hotspot không dây mà bạn kết nối tại các tiệm cà phê và khách sạn hoặc những cơ sở khác vốn cung cấp sự truy cập dễ dàng đến một access point WiFi công cộng, không an toàn. Bạn có thể dễ dàng duyệt tìm những nối kết này vì chúng đến và đi, và các SSID thường thay đổi như được giải thích trong **mục 60**.



Bạn có thể duyệt tìm các hotspot công cộng, thường không đòi hỏi adapter được cấu hình sẵn để truy cập mạng WiFi đó.

33. Cấu hình Adapter và kết nối với Router không dây

Trước khi bạn bắt đầu	Xem thêm
32. Bàn về việc cấu hình Adapter không dây	**Mục 35**

Để truy cập mạng WiFi cục bộ và các dịch vụ chẳng hạn như một nối kết Internet băng tần rộng, bạn cần nối kết máy tính với router WiFi. Windows

cung cấp một biểu tượng nối kết mạng không dây trong vùng thông báo (còn được gọi là system tray) nằm ở đầu bên phải taskbar. Khi bạn mở biểu tượng mạng không dây, bạn có thể xem trạng thái của adapter (mạng WiFi), quét tìm một mạng WiFi có sẵn và kết nối với nó. Nếu bạn đã mua một máy tính notebook hoặc một máy tính desktop vốn có sẵn WiFi (đặc biệt các notebook sử dụng công nghệ Centrino của Intel), bạn có thể sử dụng tiện ích Windows Wireless Connection để giám sát nối kết WiFi và kết nối với các mạng WiFi có sẵn. Để sử dụng nó, nhấp phải biểu tượng vùng thông báo (một máy tính có các tín hiệu vô tuyến).

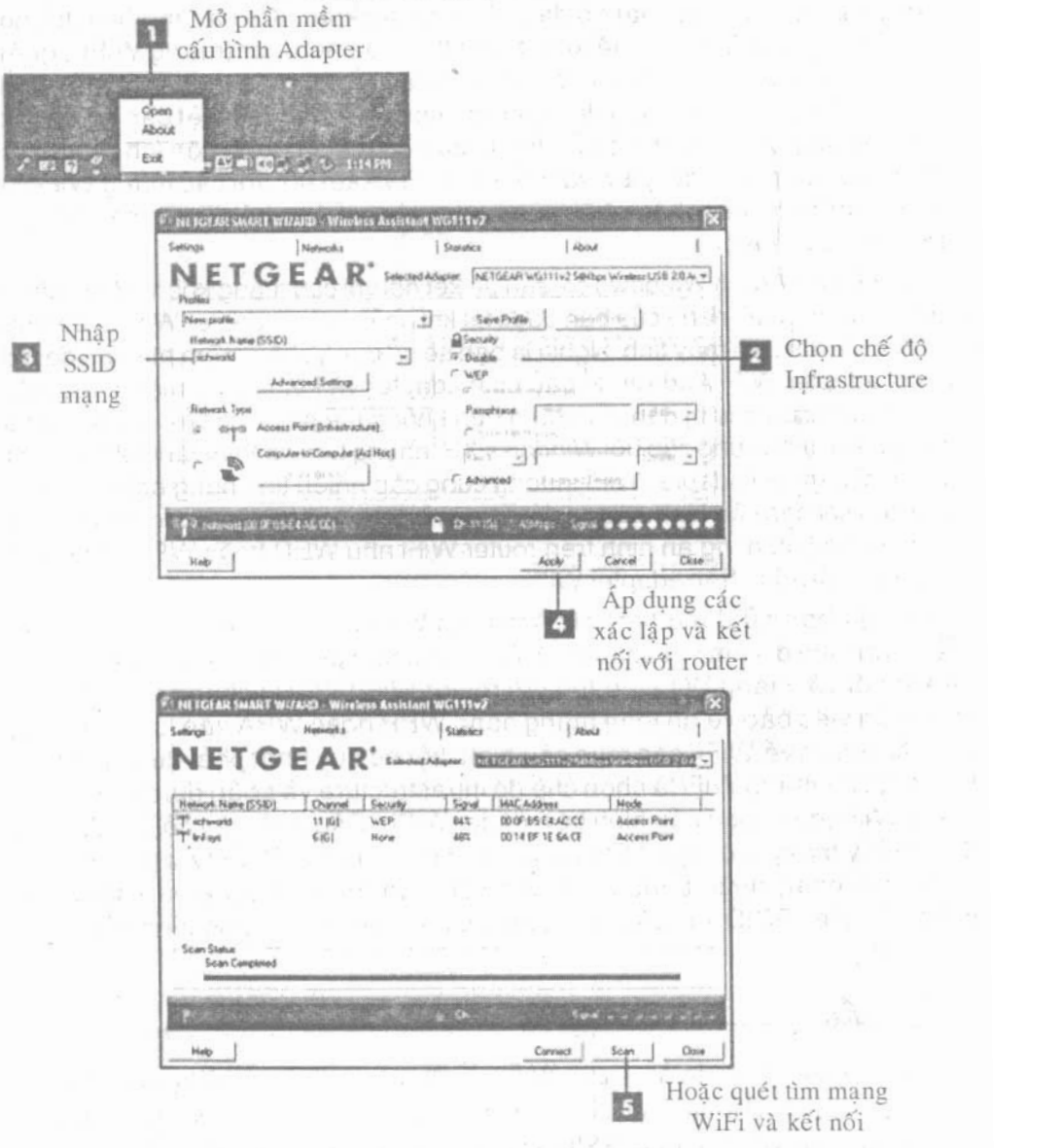
Tuy nhiên, tiện ích Windows cài sẵn để kết nối với các mạng không dây chẳng hạn như mạng WiFi riêng của bạn được tắt khi phần mềm adapter WiFi nhóm thứ ba được cài đặt trên máy tính. Nghĩa là bạn sẽ sử dụng phần mềm mà bạn đã cài đặt với adapter WiFi Add-on để cấu hình adapter và kết nối với mạng. Mặc dù bạn có cảm giác như bị đánh lừa rằng bạn không thể sử dụng tiện ích Wireless Connection được cung cấp bởi Windows XP, nhưng bạn sẽ thấy rằng phần mềm tiện ích đi kèm với adapter WiFi thường cung cấp nhiều tính năng hơn và dễ sử dụng hơn khi bạn cấu hình adapter WiFi, đặc biệt trong những trường hợp bạn sử dụng những tính năng an ninh trên router WiFi như WEP hoặc WPA vốn cũng phải được cấu hình trên adapter WiFi.

Cho dù bạn sử dụng tiện ích Windows Wireless Connection hoặc phần mềm cấu hình đi kèm với adapter WiFi, nhưng bạn phải cấu hình adapter WiFi để kết nối với mạng WiFi (cụ thể với router WiFi). Bởi vì chúng ta đã không thảo luận việc bảo vệ an toàn mạng bằng WEP hoặc WPA vào lúc này trong việc thảo luận về WiFi, các mục cấu hình thật sự duy nhất phải được thiết lập trên adapter mạng WiFi là chọn chế độ infrastructure và nhập đúng SSID cho mạng WiFi (như được cấu hình trên router WiFi). Cấu hình này có thể được tự động xử lý bằng cách quét tìm và sau đó nối với router WiFi (vì an ninh chưa được kích hoạt) hoặc bằng cách chọn chế độ Infrastructure và sau đó gõ nhập bằng tay SSID vào cấu hình của adapter WiFi (như được trình bày trong tác vụ này).

Ghi chú

Các bước để cấu hình adapter WiFi phụ thuộc vào tiện ích phần mềm được cung cấp bởi nhà sản xuất adapter. Điều cốt yếu: bạn phải quét tìm hoặc nhận dạng mạng của bạn bằng SSID của nó, bạn cũng phải cung cấp bất kỳ pass phrase an ninh hoặc khóa mã hóa mà bạn đã cấu hình trên adapter nếu router nối kết thành công với router WiFi.

33. Cấu hình Adapter và nối kết với Router không dây



1. Mở phần mềm cấu hình Adapter

   Nhận dạng biểu tượng cho tiện ích phần mềm adapter WiFi trong vùng thông báo của taskbar. Nhấp phải biểu tượng và chọn Open từ menu ngữ cảnh. Tiện ích cấu hình cho adapter WiFi mở ra.

2. Chọn chế độ Infrastructure

   Nhấp nút tùy chọn hoặc hộp kiểm thích hợp (phụ thuộc vào phần mềm cấu hình) để chọn chế độ Infrastructure. Ví dụ, đối với tiện ích cấu hình adapter WiFi Netgear, chọn tùy chọn Access Point (Infrastruture) bên dưới hạng mục Network Type.

3. Nhập Network SSID

Gõ nhập SSID cho mạng (SSID mà bạn đã xác định khi cấu hình router WiFi được giải thích trong mục 26) trong hộp text thích hợp trong cửa sổ tiện ích cấu hình.

THỦ THUẬT: Nếu bạn không nhớ SSJD, hãy sử dụng tính năng scan của tiện ích phần mềm để quét tìm các mạng WiFi trong tầm hoạt động. Sau đó bạn có thể chọn mạng từ danh sách được cung cấp. Nếu bạn đã cấu hình bất kỳ xác lập an ninh trên router, bạn phải cung cấp pass phrase hoặc các khóa mã hóa để thật sự kết nối với router. Để bắt đầu với chế độ an ninh trên router WiFi, hãy xem mục 70.

---

4. Áp dụng các xác lập và kết nối với router

Nhấp nút Apply để áp dụng các xác lập vào adapter WiFi và để kết nối với mạng WiFi bằng cách sử dụng router/access point. Nếu bạn không thể kết nối với mạng, đi đến bước 5.

5. Hoặc quét tìm mạng WiFi và kết nối

Nếu bạn không muốn cấu hình bằng tay adapter WiFi, bạn có thể quét tìm mạng WiFi và kết nối tự động sau khi bạn bật các tính năng trên router (chẳng hạn như WEP hoặc WPA), bất kỳ nỗ lực nhằm tự động kết nối đòi hỏi bạn nhập passkey cho tùy chọn an ninh được bật trên router. Sau khi bạn đã bật các tính năng an ninh trên router WiFi, việc cấu hình bằng tay adapter WiFi và lưu cấu hình dưới dạng một adapter WiFi là điều bạn nên làm.

Chọn tùy chọn Scan cho phần mềm bạn cấu hình adapter WiFi; ví dụ, phần mềm tiện ích Netgear đòi hỏi bạn nhấp tab Networks trên cửa sổ phần mềm và sau đó chọn Scan. Một danh sách các mạng WiFi có sẵn; chọn mạng WiFi của bạn (nếu bạn thấy nhiều mảng được liệt kê, điều đó có nghĩa rằng các mạng WiFi khác đang hoạt động gần đó) và sau đó nhấp Connect. Bạn sẽ được kết nối với mạng WiFi.

THỦ THUẬT: Nếu bạn không thấy mạng WiFi của bạn khi sử dụng tính năng Scan, có thể router WiFi đã không được cấu hình một cách chính xác. Kiểm tra cấu hình router để bảo đảm các SSJD broadcast đã được bật và router được bật để nối mạng WiFi. Nếu bạn vẫn gặp các sự cố nối kết, hãy kiểm tra mục 91.

---

34. Cấu hình adapter để nối mạng từ máy tính này đến máy tính khác

Trước khi bạn bắt đầu	Xem thêm
33. Cấu hình Adapter và nối kết với Router không dây	Mục 42
	Mục 38
	Mục 45

Bạn có thể cấu hình Adapter mạng WiFi cho chế độ Ad-Hoc (còn được gọi là nối mạng peer-to-peer). Điều này có nghĩa rằng bạn sử dụng mạng adapter WiFi để kết nối trực tiếp với những máy tính khác vốn cũng có các adapter WiFi và đã được cấu hình để nối mạng peer-to-peer hoặc Ad Hoc. Sự giao tiếp theo cách này sẽ cho phép các máy tính chia sẻ các file và những thiết bị khác chẳng hạn như các máy in.

Ghi chú

Kết nối hai máy tính trong chế độ Ad Hoc tương tự như nối hai máy tính bằng một cáp chéo. Hai máy tính có thể giao tiếp bởi vì một phương tiện mạng nối kết chúng. Nối mạng WiFi sử dụng các tín hiệu vô tuyến mà thực tế giống như một cáp LAN. Do đó chế độ Ad Hoc có sẵn bởi vì hai hay nhiều thuộc tính có thể được nối bằng cách cấu hình chúng cho cùng một kênh WiFi.

Để cấu hình một máy tính được bật WiFi để nối mạng peer-to-peer, bạn cấu hình adapter WiFi của máy tính cho chế độ Ad Hoc. Chế độ Ad Hoc không đòi hỏi một router WiFi access point kết nối với một máy tính khác cũng đã được cấu hình cho chế độ Ad-Hoc. Cả hai máy tính sử dụng chế độ Ad Hoc cũng phải được cấu hình để sử dụng một tên mạng hoặc SSID cụ thể (mặc dù không có một access point tham gia) và chúng đã được cấu hình cho một giao thức WiFi cụ thể (802.11b hoặc 802.11g) một kênh riêng biệt.

Mặc dù nối mạng WiFi Ad Hoc dường như là một cách tốt để tránh chi phí của một router WiFi nhưng hãy nhớ rằng chế độ Ad Hoc không cho phép bạn đạt được thông lượng tối đa có sẵn cho adapter của mạng máy tính. Các adapter Wireless G có thể kết nối với tốc độ lên đến 54Mbps, nhưng chế độ Ad-Hoc thường cung cấp chỉ 11Mbps. Bạn nên sử dụng chế độ Ad-Hoc chỉ trong những tình huống mà bạn muốn nối kết nhanh với một máy tính được bật WiFi khác để bạn có thể hoán đổi các file hoặc chia sẻ một máy in. Trong xác lập mạng gia đình, router WiFi cung cấp hạ tầng mạng và kết nối với nối kết Internet tốc độ cao.

Để hai máy tính chia sẻ các tài nguyên khi khi giao tiếp với nhau trong chế độ Ad Hoc, cả hai máy tính phải được cấu hình để chia sẻ file và máy in Windows và cũng là các thành viên của cùng một workgroup Windows. Các xác lập chia sẻ file và máy in được tìm thấy trong hộp thoại Properties cho nối kết WiFi LAN. Để đặt các máy tính được nối mạng Ad-Hoc trong cùng một workgroup, chạy Network Setup Wizard từ Windows Control Panel (**xem mục 37**).

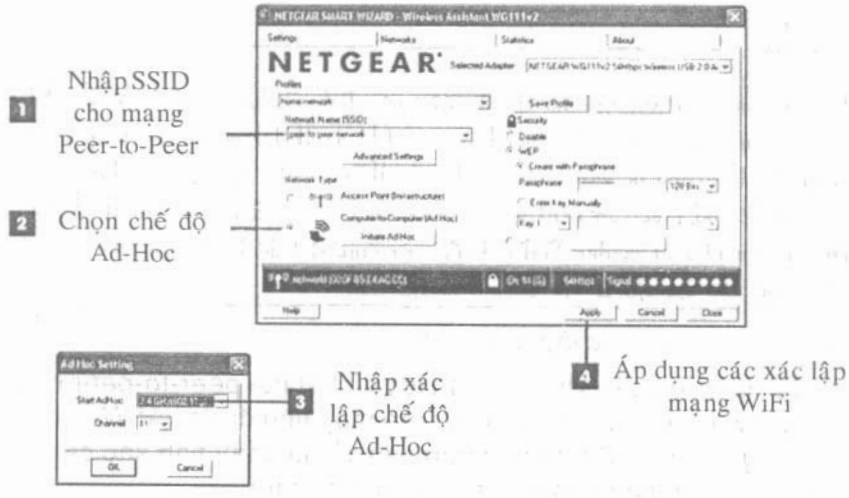
THỦ THUẬT: Một dãy địa chỉ IP đã được sử dụng để xác định trên các mạng riêng. Có ba dãy địa chỉ khác nhau mà bạn có thể sử dụng để nối mạng riêng chẳng hạn như cấu hình các máy tính cho chế độ WiFi Ad-Hoc. Những dãy này là 10.0.0.0 đến 10.255.255.255 (subnet mask 255.0.0), 172.16.0.0 đến 172.31.255.255 (subnet mask 255.255.0), và 192.168.0.0 đến 192.168.255.255 (subnet mask 255.255.255.0). Làm việc với các địa chỉ IP và subnet masks hiểu một số đi cùng với các lớp địa chỉ IP có thể gây bối rối. Để biết thêm thông tin về việc lập địa chỉ IP, xem mục 37.

Một xác lập quan trọng khác được yêu cầu để adapter WiFi hoạt động trong chế độ Ad-Hoc là địa chỉ IP tĩnh. Điều này có nghĩa rằng một địa chỉ IP phải được gán vào máy tính thay vì cho phép máy tính nhận địa chỉ IP của nó từ router WiFi vốn cũng có chức năng như một server DHCP (server cung cấp động các địa chỉ IP cho các máy tính trên mạng). Bạn xác định địa chỉ IP (và subnet mask) cho một nối kết chẳng hạn như một adapter WiFi trong hộp thoại TCP/IP Properties dành cho adapter mạng đó).

Ghi chú

Các bước thật sự để cấu hình Ad Hoc trên một máy tính có thể khác phụ thuộc vào tiện ích phần mềm nào được đính kèm với adapter WiFi.

34. Cấu hình Adapter để nối mạng từ máy tính này đến máy tính khác



1. Nhập SSID cho mạng Peer-to-Peer

   Trên màn hình cấu hình của tiện ích phần mềm của adapter WiFi (khởi động tiện ích từ vùng thông báo ở đầu phải của taskbar), gõ nhập một tên mạng còn được gọi là SSID của nó cho mạng peer-to-peer/Ad-Hoc. Bạn có thể sử dụng bất kỳ tên mà bạn muốn cho SSID của mạng Ad-Hoc. Bạn có sẵn 32 ký tự chữ - số (không sử dụng các khoảng trống). Ví dụ, bạn có thể đặt tên cho SSID Ad-Hoc là Joe Kim's để cho bạn biết rằng đây là nối kết mà bạn sử dụng để kết nối giữa các máy tính được bật WiFi của Joe và Kim. Nếu bạn thường sử dụng nối kết này (ví dụ bất cứ khi nào bạn cách xa mạng WiFi gia đình), lưu các xác lập Ad-Hoc dưới dạng một profile cấu hình. Bởi vì các mạng infrastructure và Ad-Hoc là những mạng thực thể đặc biệt, bạn không thật sự dành riêng các địa chỉ IP và những xác lập khác cho mạng WiFi Ad-Hoc khi bạn cấu hình. Bạn có thể sử dụng các địa chỉ IP y như vậy và những xác lập khác cho bao nhiêu mạng Ad-Hoc tùy thuộc bạn muốn cấu hình. Hãy nhớ rằng hai máy tính trên mang Ad-Hoc không thể có cùng một địa chỉ IP.

2. Chọn chế độ Ad-Hoc

   Chọn chế độ Ad-Hoc trong cửa sổ cấu hình. Ví dụ, trong tiện ích cấu hình Netgear, nhấp nút tùy chọn Computer to Computer (Ad Hoc).

3. Nhập các xác lập chế độ Ad-Hoc

   Các xác lập chế độ Ad-Hoc bao gồm giao thức WiFi cần sử dụng (802.11b hoặc 802.11g) và kênh cần sử dụng để truyền. Để sử dụng những xác lập này khi sử dụng một adapter Netgear, nhấp nút Initiate Ad Hoc và sử dụng các hộp xổ xuống trên hộp thoại Ad Hoc Setting để xác định giao thức WiFi và kênh, sau đó nhấp OK.

Ghi chú

Để cấu hình các xác lập địa chỉ IP của máy tính sử dụng chế độ WiFi Ad-Hoc, bạn sử dụng hộp thoại Internet Protocol (TCP/IP) Properties. Hộp thoại này cung cấp tùy chọn để cấu hình các địa chỉ IP cố định (chẳng hạn như các địa chỉ mà chế độ Ad-Hoc cần đến) và tùy chọn để nhận tự động địa chỉ IP từ thiết bị, chẳng hạn như từ router WiFi. Kiểm tra mục 42 để biết thêm chi tiết về việc cấu hình các địa chỉ IP và subnet mask.

4. Áp dụng các xác lập mạng WiFi

   Để áp dụng các xác lập Ad-Hoc và kết nối peer-to-peer mới, nhấp Apply. Lặp lại các bước này trên máy tính được bật WiFi thứ hai sử dụng các xác lập giống nhau cho cả hai máy tính sao cho hai máy tính có thể giao tiếp trên mạng Ad Hoc mới.

   Để tận dụng mạng Ad Hoc, mở Network neighborhood từ menu Start và sau đó duyệt tìm các máy tính hiện có sẵn trong workgroup. Nhấp đôi để mở máy tính vốn cung cấp một tài nguyên chia sẻ chẳng hạn

như máy in hoặc folder mà bạn muốn truy cập. Máy in hoặc folder sẽ xuất hiện dưới dạng một tài nguyên chia sẻ.

35. Tạo các Profile cấu hình

Trước khi bạn bắt đầu

32. Bàn về việc cấu hình Adapter không dây

Rất có thể bạn sẽ có nhiều cấu hình cho adapter mạng WiFi, một cấu hình cho mạng gia đình, một cấu hình cho mạng WiFi tại cơ quan và một cấu hình Ad Hoc để nối mạng peer-to-peer. Bạn có thể lưu các cấu hình khác nhau cho adapter WiFi dưới dạng các profile nhằm cho phép bạn tải nhanh một tập hợp xác lập cấu hình cụ thể khi bạn muốn kết nối với mạng WiFi đó.

THUẬT NGỮ CHÍNH

Configuration Profile. Một tập hợp tùy chọn cấu hình cho adapter mạng WiFi vốn đã được lưu với một tên profile. Lưu profile cho phép bạn gọi lại nhanh những xác lập này bất cứ lúc nào từ phần mềm cấu hình của adapter WiFi.

Ghi chú

Các tiện ích cấu hình phần mềm cho hầu hết các adapter WiFi cung cấp một tiện ích để lưu cấu hình dưới một tên hoặc ở dạng một profile. Tham khảo tài liệu của adapter WiFi để xem các bước thật sự để lưu một cấu hình hoặc tạo một profile. Các bước trong tác vụ này sử dụng một adapter Netgear để giải thích tiến trình tạo và gọi lại một profile.

35. Tạo các Profile cấu hình



1. Cấu hình các xác lập mạng WiFi và đặt tên cho Profile

   Trong cửa sổ tiện ích cấu hình của adapter WiFi, khởi động tiện ích cấu hình của vùng Notification ở đầu phải của taskbar hoặc từ menu Start, xác lập các tham số cấu hình (SSID, access point hoặc chế độ Ad Hoc,...) cho nối kết mạng WiFi. Gõ nhập một tên cho profile mới ở nơi được chỉ định (trong ví dụ này sử dụng tiện ích Netgear, gõ nhập tên của profile trong hộp text profile). Đối với các quy ước đặt tên, profile được lưu trữ cục bộ, do đó bạn không cần phải bận tâm về các profile được đặt tên trên các máy tính được bật WiFi khác trên mạng. Profile có thể mô tả tùy mức độ cần thiết và có thể chứa các khoảng trống trong tên.

2 Lưu Profile

   Nhấp Save Profile (hoặc một nút có tên tương tự khác) để lưu profile khác. Tất cả xác lập mà bạn đã cấu hình cho adapter mạng WiFi để truy cập mạng hiện hành được lưu trong profile này với tên chỉ định. Các xác lập Windows khác chẳng hạn như workgroup hiện hành và các xác lập TCP/IP không được lưu dưới dạng một phần của profile này. Chuyển đổi một mạng WiFi sang một mạng WiFi khác (chẳng hạn như từ một mạng infrastructure sang một mạng Ad Hoc) đòi hỏi những xác lập khác được thay đổi trên máy tính trước khi bạn có thể nối kết với mạng WiFi đã xác định.

3. Chọn Profile

   Lần kế tiếp bạn muốn truy cập một mạng cụ thể, bạn có thể đơn giản chọn profile cho mạng đó thay vì cấu hình lại bằng tay tất cả xác lập thích hợp. Để chọn một profile (vốn nối kết máy tính với mạng WiFi được xác lập trong profile), mở tiện ích phần mềm của adapter (như được mô tả ở bước 1), mở danh sách xổ xuống profile và chọn profile cho mạng mà bạn muốn kết nối. Sau đó áp dụng profile cấu hình. Trong trường hợp của phần mềm cấu hình Netgear, nhấp nút Apply. Khi bạn kết nối với mạng, một khung thoại xuất hiện kế bên biểu tượng vùng thông báo cho adapter mạng.

36. Bàn về việc cập nhật một Driver Adapter

Trước khi bạn bắt đầu

30. Cài đặt tiện ích phần mềm Adapter

31. Kiểm tra cài đặt Adapter WiFi

Để adapter mạng WiFi vận hành tốt, driver phần mềm thích hợp phải được cài đặt. Hầu hết các vấn đề liên quan đến các thiết bị phần cứng thường liên quan đến driver phần mềm.

Ghi chú

Việc nhà sản xuất một adapter cập nhật phần mềm vốn có sẵn cho một adapter WiFi nào đó thì hoàn toàn không có gì là lạ. Thỉnh thoảng hãy kiểm tra website của nhà sản xuất để xem có sẵn các bản cập nhật cho adapter mạng của bạn hay không. Các tiện ích phần mềm cập nhật cho một thiết bị thường cung cấp những tính năng mới hoặc cải tiến phần mềm để làm cho thiết bị dễ cấu hình và quản lý hơn.

Adapter WiFi đính kèm một CD (hoặc media khác) cung cấp một driver và các tiện ích phần mềm cho thiết bị. Đôi khi driver đi kèm một thiết bị không cung cấp chức năng thích hợp cho thiết bị. Nếu bạn gặp phải các sự cố với adapter WiFi, bạn nên kiểm tra website của nhà sản xuất để xem có sẵn một driver mới (sửa đổi) cho adapter của bạn hay không.

Các tác vụ trong chương này sử dụng adapter Wireless 2.0 Netgear WG111v2 để trình bày cách cài đặt và cấu hình một adapter WiFi. Nếu bạn đi đến trang hỗ trợ Netgear cho thiết bị, bạn có thể thấy phần mềm và/hoặc các driver cập nhật có sẵn hay không. Hầu hết các trang hỗ trợ của nhà sản xuất cũng có những thủ thuật về xử lý sự cố và những hướng dẫn để nâng cao hiệu suất của adapter.

Trang web hỗ trợ của nhà sản xuất cho adapter WiFi có thể cung cấp các link dẫn đến các driver và phần mềm mới và cung cấp thủ thuật xử lý sự cố.

Nếu có sẵn phần mềm mới thì cũng có một driver mới. Do đó download phần mềm bằng cách sử dụng trình duyệt web và sau đó chạy phần mềm trên máy tính để cập nhật thiết bị. Nếu bạn download một driver cập nhật mà không có một tiện ích để cài đặt driver, bạn có thể cài đặt driver từ tab driver của hộp thoại Properties từ thiết bị. Mở hộp thoại này bằng cách nhấp đôi vào danh sách các thiết bị trong Windows Device Manager, được truy cập qua tab Device của hộp thoại Properties của hệ thống.

Từ tab Driver, bạn cũng có thể phục hồi trở lại một driver nếu bạn gặp phải các sự cố với một driver mới. Bạn nên cập nhật driver của thiết bị chỉ khi bạn gặp phải các sự cố với thiết bị. Trước khi bạn download các bản cập nhật cho tiện ích đi kèm với thiết bị, hãy đọc xem bản cập nhật nói về những tính năng và chức năng nào rồi quyết định có nên download và cài đặt phần mềm hay không.



Nhấp nút Update Driver trên tab Driver trong hộp thoại Properties của thiết bị để tìm và cài đặt driver được download nếu driver không cung cấp tiện ích cài đặt riêng của nó.

THỦ THUẬT: Bạn cũng có thể kết nối với Website cập nhật Windows bằng cách nhấp nút Windows Update trên tab Hardware của hộp thoại System Properties. Website Windows Update thường cung cấp các driver cập nhật cho những thiết bị chẳng hạn như các adapter WiFi. Sử dụng tính năng Windows Update để cập nhật các driver là cách dễ nhất để cập nhật các driver thiết bị bởi vì tiến trình cài đặt driver được xử lý tự động.

Chương 6

CẤU HÌNH MẠNG GIA ĐÌNH WINDOWS

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *37. Bàn về việc cấu hình các PC để nối mạng*
- *38. Chạy Network Setup Wizard*
- *39. Đặt tên cho máy tính và gia nhập một workgroup*
- *40. Mở các thuộc tính nối kết và bật các client, giao thức và dịch vụ.*
- *41. Thêm một client hoặc dịch vụ mạng*
- *42. Cấu hình các xác lập TCP/IP*
- *43. Kiểm tra trạng thái adapter WiFi*
- *44. Xác nhận tư cách thành viên workgroup và truy cập Network Neighborhood*

Mục đích của các máy tính nối mạng là chia sẻ các nguồn tài nguyên chẳng hạn như file, máy in và một nối kết Internet tốc độ cao. Các máy tính nối mạng cũng cho bạn khả năng chơi game trên mạng. Cho dù các máy tính được nối cứng để nối mạng hoặc tham gia một mạng WiFi hay không, chúng sẽ được cấu hình thích hợp để gia nhập mạng. Trong các tác vụ của chương này, chúng ta sẽ xem việc xác lập các thuộc tính LAN và cấu hình các máy tính để gia nhập vào mạng WiFi.

37. Bàn về việc cấu hình các PC được nối mạng

Trước khi bắt đầu	Xem thêm
4. Duyệt và tìm kiếm các file và folder	**Mục 32**
5. Bàn về My Network Places	**Mục 35**
5. Sử dụng Control Panel	**Mục 34**

Để các PC vận hành chính xác trên mạng WiFi gia đình hoặc văn phòng nhỏ, bạn phải cấu hình một số xác lập. Bởi vì nối mạng Windows sử dụng các quy ước nhất định để nhận dạng các máy tính trên mạng và bởi vì các mạng IP chẳng hạn như Internet đòi hỏi các máy tính tham gia sử dụng một quy ước địa chỉ cụ thể để truy cập Internet, bạn phải kiểm tra và cấu hình một số xác lập trước khi một máy tính sẽ khởi động và chạy trên mạng.

Nối mạng Workgroup

Nối mạng Microsoft cho các mạng gia đình và văn phòng nhỏ (và các mạng lớn hơn vốn sử dụng một server mạng) được gọi là nối mạng peer-to-peer (ngang hàng) bởi vì một máy tính trên mạng vận hành dưới dạng một peer, nghĩa là nó có thể vừa cung cấp các dịch vụ (chẳng hạn như một file hoặc máy in) vừa truy cập các dịch vụ từ những máy tính khác trên mạng. Bản thân mạng được gọi là một workgroup.

THUẬT NGỮ CHÍNH

Workgroup. Một mạng peer-to-peer Microsoft Windows. Mỗi máy tính trong một workgroup có thể cung cấp và truy cập các nguồn tài nguyên.

Ghi chú

Từ peer-to-peer networking (nối mạng ngang hàng) có thể gây một số nhầm lẫn. Đối với nối mạng gia đình hoặc văn phòng nhỏ Microsoft Windows, mạng peer-to-peer là một workgroup. Workgroup gồm nhiều máy tính chia sẻ các nguồn tài nguyên ngang bằng nhau. Chúng là các peer. Từ peer-to-peer networking được sử dụng để mô tả nối mạng WiFi Ad Hoc, trong đó hai máy tính được cấu hình để giao tiếp trực tiếp bằng cách sử dụng WiFi.

Để một máy tính gia nhập mạng, nó phải là một thành viên (member) của workgroup. Các workgroup được giới hạn chỉ trong 10 máy tính bởi vì một máy tính peer chạy một hệ điều hành chẳng hạn như Windows XP có thể đáp ứng chỉ 10 nối kết với một nguồn tài nguyên chia sẻ cụ thể chẳng hạn như một folder hoặc máy in. Bạn có thể thấy nếu một số máy tính in sang một máy in vốn được chia sẻ với một máy tính cụ thể trong workgroup, máy tính chia sẻ máy in trở nên ì ạch và chạy chậm hơn bởi vì khả năng xử lý và bộ nhớ bị đè nặng do "phục vụ" nguồn tài nguyên cho những máy tính khác trong workgroup. Bạn nên giới hạn workgroup chỉ trong 5 hoặc 6 máy tính đặc biệt nếu mọi người in sang một máy in vốn được cung cấp dưới dạng một tài nguyên chia sẻ bởi một trong các máy tính workgroup

Ghi chú

Mặc dù hệ điều hành Windows XP cung cấp các khả năng chia sẻ các tài nguyên trên một mạng, nhưng chắc chắn nó không được thiết kế để giải quyết

lưu lượng mạng cao hoặc phục vụ nhiều nguồn tài nguyên cho một số lớn các máy tính. Các mạng công ty sử dụng các server mạnh với phần mềm server mạng để cung cấp các tài nguyên in và file. Những loại mạng này có thể đáp ứng một số lớn người dùng (hàng trăm và thậm chí hàng ngàn) do các server chuyên "phục vụ" các tài nguyên mạng. Windows XP được thiết kế như là một môi trường desktop người dùng cuối để chạy các ứng dụng cục bộ chẳng hạn như email client, bộ xử lý văn bản và trình duyệt web. Mặc dù Windows XP có thể "phục vụ" các tài nguyên, nhưng nó cực kỳ giới hạn về số máy tính khác (giới hạn là 10 nối kết) mà nó có thể phục vụ một tài nguyên bất cứ lúc nào.

Mỗi máy tính trong workgroup nên được nhận biết bằng một tên duy nhất. Tên này còn được gọi là tên NetBIOS và nó có thể dài đến 15 ký tự. Từ NetBIOS là thứ còn sót lại từ một chiến lược nối mạng Microsoft ban đầu, nhưng các tên duy nhất vẫn được yêu cầu để nhận dạng các máy tính trong workgroup.

Các máy tính tham gia workgroup phải được cấu hình để chia sẻ file và in và cũng phải được cấu hình dưới dạng các client mạng Microsoft. Cả hai xác lập này được cấu hình trong hộp thoại Properties cho adapter mạng của máy tính mà trong trường hợp này sẽ là adapter mạng WiFi. Cấu hình adapter WiFi để chia sẻ file và in được mô tả trong **mục 41**. Tạo workgroup rất đơn giản bởi vì Microsoft cung cấp một Network Setup Wizard vốn dẫn dắt bạn qua các bước tạo workgroup mới. Network Setup Wizard được thảo luận trong **mục 38.**

Sau khi phương tiện mạng (WiFi) được bật trên các máy tính và router WiFi, các máy tính phải được cấu hình với các xác lập mạng thích hợp để cho phép chúng chia sẻ các tài nguyên và cũng trở thành một thành viên của một workgroup Windows. Sau cùng, các máy tính trên mạng WiFi (điều này tương tự đối với các máy tính trên một LAN hữu tuyến) phải được cấu hình bằng một hệ thống lập địa chỉ mạng vốn nhận dạng duy nhất mỗi máy tính. Đây là nơi lập địa chỉ IP được thực thi.

Lập địa chỉ IP

Giao thức TCP/IP là một tập hợp quy tắc ấn định các máy tính sử dụng các địa chỉ IP như thế nào để giao tiếp trên một mạng TCP/IP. Ngày nay, địa chỉ IP được sử dụng trên các mạng (workgroup) lớn và nhỏ bởi vì các máy tính cần truy cập Internet mà bản thân là một mạng TCP/IP khổng lồ.

Ghi chú

Giao thức TCP/IP được thiết lập theo mặc định trên một máy tính chạy hệ điều hành Windows XP Home hoặc Professional.

Mọi thiết bị (các máy tính và router WiFi) trên mạng phải được gán một địa chỉ IP. Router WiFi thường được gán tự động địa chỉ IP của nó bởi nhà cung

cấp dịch vụ Internet khi bạn kết nối router WiFi với thiết bị nối kết băng tần rộng (chẳng hạn như router DSL hoặc modem băng tần rộng).

Các địa chỉ IP là các địa chỉ số thập phân chấm chấm được viết dưới dạng bốn tập hợp số thập phân được tách nhau bằng các dấu chấm. Ví dụ, 13.0.1.1 là đúng dạng cho một địa chỉ IP. Các địa chỉ IP cũng được đính kèm bởi một subnet mask (mặt nạ mạng con). Subnet mask giúp các máy tính quyết định phần nào của địa chỉ IP tham chiếu mạng và phần nào của địa chỉ tham chiếu máy tính đã được gán địa chỉ. Các subnet mask cũng được viết theo dạng số thập phân. Ví dụ, 255.255.0.0 là một subnet mask có thể đính kèm địa chỉ IP 130.0.1.1.

THUẬT NGỮ CHÍNH

Địa chỉ IP. Một sự thể hiện số thập phân chấm chấm của một địa chỉ nhị phân được gán duy nhất cho mỗi máy tính và thiết bị chạy trên một mạng IP.

Subnet mask. Một sự thể hiện số thập phân chấm chấm của một mặt nạ nhị phân được sử dụng bởi các máy tính để quyết định phần của một địa chỉ IP cung cấp thông tin mạng và phần của địa chỉ IP cung cấp thông tin địa chỉ máy tính.

Các mạng IP (Internet Protocol) đòi hỏi mỗi máy tính có một địa chỉ IP duy nhất. Địa chỉ này được sử dụng để nhận dạng máy tính gởi và nhận dữ liệu trên mạng IP. Bởi vì router WiFi tự động cung cấp địa chỉ IP cho các máy tính trên mạng WiFi, bạn không cần phải bận tâm về việc cấu hình các máy tính với địa chỉ IP và subnet mask bắt buộc. Router thực hiện điều này cho bạn bằng cách sử dụng Dynamic Host Configuration Protocol. Khi một máy tính online, nó hỏi router một địa chỉ IP và subnet mask. Router trả lời bằng cách cung cấp thông tin này cho máy tính.

Lần duy nhất bạn sẽ phải gán các địa chỉ IP tĩnh cho các máy tính bật WiFi là khi bạn muốn các máy tính giao tiếp trên một mạng Ad Hoc vốn không sử dụng các router WiFi (xem mục 34). Mặc dù cho router WiFi phân phối các địa chỉ IP và subnet mask thích hợp cho các máy tính workgroup làm cho bạn không biết một cách dễ chịu về việc làm việc thật sự với các lớp địa chỉ IP khác nhau và việc lập địa chỉ tĩnh, nhưng chắc chắn có sự hiểu biết cơ bản về việc lập địa chỉ IP và các subner mask thì không có hại gì cả.

Phương pháp lập địa chỉ IP đã thật sự phát triển trong những năm 1970 khi Internet được sáng tạo lần đầu tiên. Ngày nay, ở Mỹ (và cả Bắc và Nam Mỹ, các địa chỉ IP đã được "cho thuê" bởi các công ty từ American Registry for Internet Numbers (ARIN). Công ty trả tiền cho một dãy địa chỉ và sau đó sử dụng chúng làm các địa chỉ IP công cộng để công ty có thể tham gia Internet. Nhà cung cấp dịch vụ Internet của bạn thuê các địa chỉ IP của no từ ARIN và sau đó gán cho bạn một địa chỉ IP cho nối kết Internet tốc độ cao của ban bằng cách sử dụng DHCP.

Sơ đồ lập địa chỉ IP thật sự được chia thành ba lớp khác nhau: lớp A, B và C. Những lớp (class) này đã được tạo để các công ty có thể được gán các dãy địa chỉ IP dựa vào quy mô và nhu cầu của họ (xét về số địa chỉ được yêu cầu).

Tài nguyên Web

http://webopedia.internet.com/TERM/I/IP address.html.

Từng lớp địa chỉ IP đã được thiết kế cho một kích cỡ mạng cụ thể. Để biết thông tin cơ bản về các lớp địa chỉ IP, tham khảo site Webopedia.

Mỗi địa chỉ IP cũng có một subnet mask mặc định. Mask được sử dụng bởi các máy tính và những thiết bị khác trên mạng để quyết định phần nào của một địa chỉ IP cung cấp thông tin mạng và phần nào của địa chỉ cung cấp thông tin địa chỉ liên quan đến một máy tính cụ thể.

Các class subnet như sau:

- *Class A: 255.0.0.0*
- *Class B: 255.255.0.0*
- *Class C: 255.255.255.0*

Ghi chú

Nếu bạn nhìn vào các subnet mask cho mỗi class, sẽ thấy rằng đối với một mạng Class A-,octet (byte 8 bit) đầu tiên của địa chỉ IP được che bởi subnet mask (255) và do đó thông tin mạng được tìm thấy trong địa chỉ IP thật sự gồm octect đầu tiên. Trong một mạng Class B, hai octet đầu tiên là thông tin mạng; trong một mạng Class C, ba octet đầu tiên là thông tin mạng. Với ít octet hơn dành cho các địa chỉ IP thật sự khi bạn di chuyển từ Class A đến Class B, bạn có thể thấy tại sao các mạng Class C cung cấp ít địa chỉ IP cá nhân hơn.

Các địa chỉ IP công cộng cho phép các máy tính và các thiết bị khác nối kết trực tiếp với Internet. Bạn không cần phải bận tâm đến các địa chỉ IP công cộng và nối kết của mạng Internet. Tất cả điều này được xử lý bởi nhà cung cấp dịch vụ Internet. Router WIFI được gán động một địa chỉ IP để giao tiếp với nhà cung cấp dịch vụ Internet và Internet. Bởi vì router WiFi đứng tại một gateway (cổng nối) giữa mạng WiFi và Internet (nối kết Internet được cung cấp bởi ISP), các địa chỉ IP được sử dụng trên mạng cục bộ (bao gồm WiFi và các máy tính được nối cáp trên mạng) không cần phải là các địa chỉ IP công cộng thật sự. Điều này đúng bởi vì LAN "ẩn giấu đằng sau" router WiFi.

Các địa chỉ IP được cung cấp động bởi router WiFi là các địa chỉ IP riêng. Khi hệ thống lập địa chỉ IP đã được thiết kế ban đầu trên Internet, nhóm địa chỉ từ các dãy Class A, Class B, Class C được dành cho nối mạng riêng Những địa chỉ này được sử dụng với các thiết bi khác trên mạng để giao tiếp cục bộ. Bất kỳ sự giao tiếp được yêu cầu với Internet chẳng hạn như duyệt Web hoặc gởi email được chuyển tiếp từ mạng cục bộ đến Internet (bởi ISP) qua router WiFi.

Sau đây là dãy địa chỉ dành riêng để sử dụng riêng:

- *Class A: 10.0.0.0 đến 255.255.255 (subnet mask 255.0.0).*

- *Class B: 172.16.0.0 sang 172.31.255.255 (subnet mask 255.255.0)*
- *Class C: 192.168.0.0 sang 192.168.255.255 (subnet mask 255.255.255.0).*

Bạn sẽ thấy router WiFi gán các địa chỉ IP vào các máy tính trên mạng bằng cách sử dụng một trong dãy địa chỉ riêng (ví dụ, router Netgear cùng dãy địa chỉ từ 192.168.1.2 đến 192.168.1.5 (Class C) làm pool (bộ chứa) mặc định để gán động các địa chỉ IP vào các máy tính trên mạng cục bộ WiFi. Hầu hết các router WiFi cho phép bạn mở rộng hoặc thay đổi dãy nếu cần. Để xem dãy địa chỉ, truy cập cấu hình của router và sau đó truy cập màn hình vốn cung cấp các xác lập LAN IP. Ví dụ trên router Netgear, truy cập màn hình thiết lập IP LAN bằng cách sử dụng các xác lập nâng cao (advanced) của router.

Bởi vì router WiFi xử lý việc lập địa chỉ IP cho máy tính nên bạn không cần phải bận tâm về việc cấu hình các máy tính với các địa chỉ tĩnh trừ khi những máy tính đó sẽ được thiết lập trong chế độ Ad-Hoc. Bạn có thể sử dụng bất kỳ địa chỉ IP từ bất kỳ các dãy mang riêng. Hãy bảo đảm rằng bạn nhất quán. Nếu hai máy tính sẽ giao tiếp trong chế độ Ad-Hoc, cấu hình mỗi máy tính với một địa chỉ IP từ cùng một class chẳng hạn như các địa chỉ IP class A 10.0.01 và 10.0.0.2.

Cấu hình thành công một máy tính để gia nhập mạng WiFi gia đình hoặc văn phòng nhỏ đòi hỏi bạn cấu hình máy tính để gia nhập workgroup (nghĩa là bạn phải cung cấp cho máy tính một tên và các xác lập workgroup thích hợp của nó). Bạn cũng phải cấu hình máy tính sao cho nó nhận một địa chỉ IP và subnet mask hợp lệ từ router WiFi hoặc bạn phải cấu hình máy tính hoặc các máy tính với các địa chỉ IP tĩnh khi vận hành mạng WiFi trong chế độ Ad-Hoc (nghĩa là router WiFi không hiện diện để cung cấp các địa chỉ IP). Khi bạn đã cấu hình tất cả mục này một cách chính xác, máy tính có thể duyệt mạng cho các thành viên workgroup khác và truy cập các dịch vụ mạng.

38. Chạy Network Setup Wizard

Trước khi bạn bắt đầu

37. Bàn về việc cấu hình các PC

Để nối mạng để máy tính thật sự gia nhập workgroup Microsoft, bạn phải cấu hình nó dưới dạng một thành viên workgroup, như đã được đề cập trong phần trước. Điều này có nghĩa rằng máy tính phải được cấu hình với một tên NetBIOS nhất và cũng phải là một thành viên của workgroup (nghĩa là workgroup phải được tạo).

Khi đặt tên cho máy tính, chọn các tên dễ nhận biết để một người dùng trên mạng biết máy tính nào mà người dùng thật sự đang kết nối (bạn có tối đa 15 ký tự), và bạn có thể sử dụng các ký tự chữ - số và ký tự số, nhưng bạn không thể sử dụng các ký tự đặc biệt, chẳng hạn như các khoảng trống, @, #, $. Khi đặt tên cho máy tính, bạn cũng được cung cấp tùy chọn để đưa vào một phần mô tả cho máy tính. Sử dụng kết hợp tên và phần mô tả để cung cấp tất

cả thông tin cần thiết cho những người dùng khác trên mạng gia đình (workgroup) nhận dạng một máy tính cụ thể sao cho họ có thể truy cập các tài nguyên, chẳng hạn như các file hoặc máy in được chia sẻ bởi máy tính cụ thể đó.

Mạng gia đình hoặc workgroup cũng được ấn định bằng một tên. Tên mặc định được thiết lập bởi Microsoft là MSHOME. Bạn sẽ muốn tạo tên mạng riêng của bạn để nhận dạng workgroup, tên workgroup phải giống nhau trên tất cả máy tính trên mạng gia đình (nghĩa là workgroup). Bản thân tên workgroup nên ngắn và có tính mô tả. Nó không thể chứa khoảng trống hoặc những ký tự đặc biệt như @, # hoặc $. Bởi vì tên workgroup thật sự là một tên mạng "riêng" (bạn sẽ không có những người kết nối mà không phải là một phần của mạng gia đình WiFi của bạn), bạn có thể sử dụng bất kỳ tên nào bạn muốn.

Sau cùng, để một máy tính có thể chia sẻ các tài nguyên (chẳng hạn như một máy in và các folder) trong một workgroup, nó phải được cấu hình bằng dịch vụ File and Printer Sharing for Microsoft Networks. Có hai cách để tiến hành việc cấu hình các xác lập khác nhau này nhằm làm cho một máy tính trở thành thành viên của một workgroup. Cách dễ nhất để tạo workgroup là chạy Network Setup Wizard.

Tuy nhiên, để hiểu đầy đủ những gì wizard thật sự thực hiện đối với máy tính của bạn, bạn cần phải am hiểu một chút về cách cấu hình các thuộc tính cho hệ thống (chẳng hạn như tên máy tính và tư cách thành viên workgroup của nó) trong hộp thoại System Properties. Bạn cũng cần hiểu các client, dịch vụ và giao thức mạng được sử dụng như thế nào để giao tiếp workgroup và chia sẻ các tài nguyên mạng, chẳng hạn như các máy in, folder.

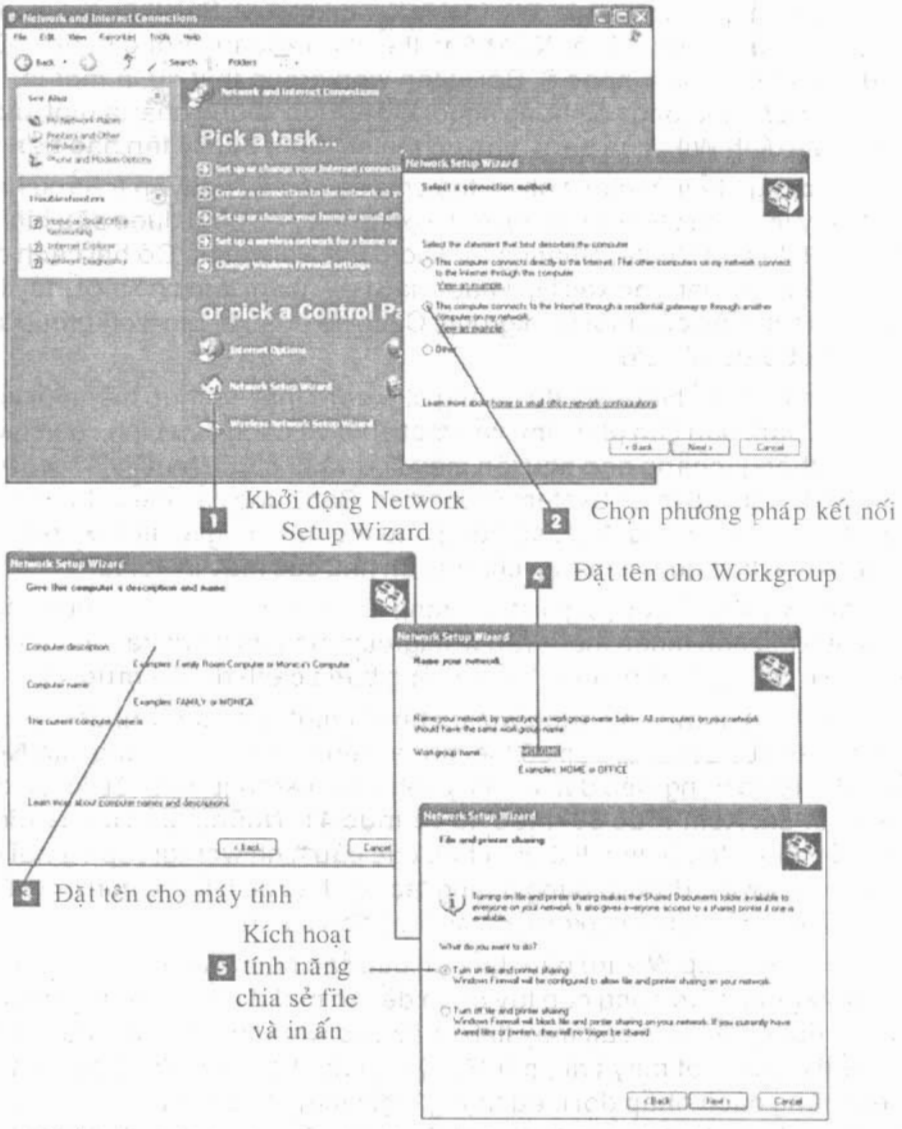
Chạy wizard như được giải thích trong tác vụ này. Lặp lại các bước cho mỗi máy tính mà bạn muốn thêm vào workgroup. Sau đó kiểm tra nhanh xem các máy tính có "nằm trên mạng" hay không bằng cách đi đến **mục 44**.

Tuy nhiên, thay vì sử dụng wizard như là một cách xử lý nhanh và sau đó tiếp tục sử dụng mạng, bạn có thể muốn hiểu rõ hơn chức năng của Network Setup Wizard trong việc đặt tên máy tính và workgroup và thiết lập sự chia sẻ file và in ấn. Xem **mục 39**, **mục 40** và **mục 41**. Những tác vụ này trình bày các hộp thoại thuộc tính thật sự chứa các cấu hình workgroup và nối mạng. Do đó chạy wizard và sử dụng những tác vụ khác để hiểu rõ hơn (và nếu cần, xử lý sự cố) cấu hình workgroup cho máy tính của bạn

Network Setup Wizard dẫn dắt bạn qua các bước đặt tên cho máy tính và tạo workgroup. Nó cung cấp tùy chọn để tạo một đĩa mềm mạng mà bạn có thể sử dụng để thêm các máy tính khác vào workgroup. Bạn chèn đĩa mềm vào ổ đĩa của một máy tính, mở My Computer từ menu Start, truy cập ổ đĩa mềm bằng cách nhấp đôi biểu tượng ổ đĩa mềm trong My Computer và sau đó nhấp đôi netsetup.exe trên một đĩa mềm để chạy một chương trình cấu hình máy tính để nối mạng workgroup.

Bạn có thể sử dụng đĩa mềm hoặc (nếu bạn đã không tạo đĩa mềm mạng), chạy Network Setup Wizard trên những máy tính khác tham gia mạng workgroup WiFi của bạn. Hãy nhớ rằng mỗi máy tính sẽ tham gia workgroup phải được cấu hình với cùng một tên workgroup (một tên duy nhất và những xác lập mạng khác) mà bạn nhập vào khi bạn chạy wizard trên máy tính đầu tiên.

38. Chạy Network Setup Wizard



1. Khởi động Network Setup Wizard

Trong cửa sổ Network and Internet Connections (mở nó từ Control Panel), nhấp biểu tượng Network Setup Wizard. Trang đầu tiên của wizard mở ra; nhấp Next để bỏ qua màn hình ban đầu. Một màn hình

checklist (danh sách kiểm tra) xuất hiện, nhắc nhở bạn cài đặt các adapter mạng và kết nối máy tính với Internet, nghĩa là bạn phải thiết lập nối kết cáp vật lý với router WiFi hoặc một adapter WiFi được cấu hình nối kết với router bằng tín hiệu vô tuyến. Nhấp Next để bỏ qua màn hình này.

2. Chọn phương pháp kết nối

   Màn hình wizard kế tiếp đề nghị ban chọn cách kết nối với mạng và Internet. Bởi vì bạn sử dụng một router WiFi làm môt gateway với băng tần rộng, chọn tùy chọn This computer connects to the Internet through a residential gateway or through another computer on my network. Sau đó nhấp Next để tiếp tuc.

3. Đặt tên cho máy tính.

   Trên màn hình kế tiếp, gõ nhập phần mô tả và tên cho máy tính. Nếu bạn hài lòng với tên mà bạn đã gán trước đó cho máy tính, gõ nhập tên này trong hộp text. Phần mò tả thì tùy chọn. Sau đó nhấp Next để tiếp tục.

4. Đặt tên cho workgroup.

   Trên màn hình kế tiếp, gõ nhập một tên cho workgroup mà bạn đang tạo. Giữ cho tên được đơn giản, nhưng cũng làm cho nó có tính mô tả. Không sử dụng tên mặc định (vốn là MSHOME). Khi quyết định một tên workgroup, không sử dụng các khoảng trống hay bất kỳ ký tự đặc biệt. Sau khi nhập một tên cho workgroup, nhấp Next.

5. Kích hoạt tính năng chia sẻ file và in ấn.

   Trên màn hình kế tiếp, hãy chắc chắn tùy chọn Turn on file and print sharing được chọn và sau đó nhấp Next.

   Bây giờ máy tính được cấu hình dưới dạng một thành viên workgroup mà bạn vừa đặt tên. Màn hình kế tiếp cho bạn tùy chọn để tạo một Network Setup Disk; nếu bạn quyết định tạo đĩa, làm theo các hướng dẫn của wizard. Khi bạn hoàn thành tiến trình, nhấp Finish.

THỦ THUẬT: Bạn có thể sử dụng đĩa mềm được tạo bởi Network Setup Wizard để thêm các máy tính khác vào workgroup. Đây là việc mang đĩa đến mỗi máy tính và chạy Network Setup Wizard với đĩa được đặt trong ổ đĩa mềm của máy tính. Bởi vì nhiều máy tính mới không có các ổ đĩa, bạn có thể chạy wizard trên mỗi máy tính và thêm nó vào workgroup.

---

39. Đặt tên cho máy tính và gia nhập Workgroup

Trước khi bạn bắt đầu

37. Bàn về việc cấu hình các PC để nối mạng

38. Chạy Network Setup Wizard

Nếu bạn chạy Network Setup Wizard như được mô tả trong mục 38 và bạn có thể xem và truy cập những máy tính khác trên workgroup (như được trình bày trong mục 44), bạn không cần thực hiện bất kỳ thay đổi nào đối với hộp thoại System Properties như đã nêu trong tác vụ này. Tác vụ này trình bày cho bạn cách thay đổi tên của một máy tính và chi nhánh workgroup của nó mà không cần chạy lại Network Setup Wizard. Nếu bạn muốn thay đổi tên của một máy tính hoặc tên của workgroup, sử dụng hộp thoại System Properties là một cách đơn giản để hoàn thành những tác vụ này.

Hộp thoại System Properties cho bạn truy cập tên của máy tính và tên của workgroup mà máy tính hiện thuộc về. Như bạn biết mọi máy tính trên mạng phải được cấu hình với một tên dài tối đa 15 ký tự. Bạn có thể sử dụng các ký tự chữ - số và các ký tự số nhưng bạn không thể sử dụng các khoảng trống hoặc những ký tự đặc biệt chẳng hạn như @, #, $...trong tên.

39. Đặt tên cho máy tính và gia nhập một Workgroup



1. Mở hộp thoại System Properties

   Nhấp menu Start và sau đó nhấp phải biểu tượng My Computer. Chọn Properties từ menu ngữ cảnh vừa xuất hiện. Hộp thoại System Properties mở ra.

THỦ THUẬT: Nếu biểu tượng My Computer nằm trên desktop Windows, bạn có thể nhấp phải nó để truy cập hộp thoại System Properties.

2. Mở hộp thoại Computer Name Changes

   Trên tab Computer Name của hộp thoại System Properties, nhấp nút Change. Hộp thoại Name Changes mở ra.

3. Nhập tên máy tính.

   Gõ nhập một tên mới cho máy tính trong hộp text Computer name.

4. Nhập tên Workgroup

   Gõ nhập một tên mới cho workgroup trong hộp text Workgroup. Thậm chí nếu đây là máy tính đầu tiên sẽ là một thành viên của workgroup, gõ nhập tên workgroup. Về cơ bản, hành động này sẽ tạo workgroup mới. Sau đó nhấp OK. Một hộp thông báo xuất hiện chào đón bạn đến với workgroup mà bạn vừa tạo. Nhấp OK để đóng hộp thông báo. Một hộp thông báo khác mở ra cho bạn biết rằng bạn phải khởi động lại máy tính, nghĩa là hệ thống cần khởi động lại để các xác lập có hiệu lực. Nhấp OK và hệ thống sẽ khởi động lại sang Windows. Bây giờ bạn có thể duyệt workgroup bằng cách sử dụng My Network Places.

Ghi chú

Hộp thoại Name Changes có một nút More mở một hộp thoại nơi để bạn nhập hậu tố (suffix) DNS cho tên của máy tính. Bởi vì bạn sử dụng workgroup làm cấu trúc mạng, thông tin DNS (Domain Name System) chẳng hạn như hậu tố (.com, .net, .biz) không bắt buộc; chúng ta không xây dựng một mạng công ty đòi hỏi hệ thống phân cấp DNS. Tóm lại, bạn không cần nhấp nút More.

5. Khởi động lại máy tính

   Nhấp OK trong hộp thông báo Computer Name Changes. Sau đó nhấp OK để đóng hộp thoại Properties. Một hộp thông báo System Settings xuất hiện; nhấp OK để khởi động lại máy tính. Máy tính sẽ khởi động lại. Sau khi Windows tải, máy tính sẵn sàng chia sẻ các tài nguyên với những máy tính khác trong workgroup.

Để thêm những máy tính khác vào mạng (workgroup), lặp lại các bước 1 -5. Mỗi máy tính phải có một tên duy nhất và phải là một thành viên của workgroup (bằng cách nhập tên workgroup).

40. Mở các thuộc tính nối kết và bật các client, giao thức và dịch vụ

Trước khi bạn bắt đầu

37. Bàn về việc cấu hình các PC để nối mạng

Control Panel cho phép bạn truy cập các nối kết cục bộ. Bạn có thể xem các nối kết và hiển thị những thuộc tính cho một adapter mạng cụ thể chẳng hạn như adapter WiFi. Thuộc tính cho một adapter gồm những xác lập mạng Windows cho adapter WiFi và được truy cập từ hộp thoại Local Area Connection Properties. Hộp thoại này là nơi bạn cấu hình các dịch vụ (service) chẳng hạn như chia sẻ file và in và các giao thức mạng chẳng hạn như TCP/IP, vốn cung cấp địa chỉ IP cho adapter.

Để một máy tính gia nhập mạng (chẳng hạn như một workgroup Windows), adapter mạng WiFi phải được cấu hình như sau:

Client. Client là phần mềm cho phép bạn thật sự đăng nhập và tham gia một loại mạng cụ thể. Trong một workgroup, phần mềm trên một máy tính có thể giao tiếp với phần mềm client trên một máy tính khác. Bởi vì chúng ta xây dựng một workgroup Windows bạn chỉ cần một client: client Microsoft Network.

Ghi chú

Có các client mạng ngoại trừ client Microsoft Network. Ví dụ, các máy tính gia nhập mạng Novell (sử dụng phần mềm nối mạng Novell) thì sử dụng client Novell.

- ***Service***. *Service (dịch vụ) là một tính năng mạng bổ sung được cấu hình cho nối kết cục bộ. Một dịch vụ thông thường được sử dụng trong nối mạng workgroup là dịch vụ File and Printer Sharing for Microsoft Networks. Dịch vụ này cho phép các máy tính trong workgroup chia sẻ các file và máy in với những thành viên khác của workgroup.*
- ***Network Protocol***. *Network protocol (giao thức mạng) cung cấp hệ thống địa chỉ được sử dụng bởi các máy tính giao tiếp trên mạng. Tối thiểu mỗi giao thức mạng phải được mở và được cấu hình cho adapter mạng. TCP/IP là giao thức duy nhất mà bạn cần để khởi động và chạy mạng workgroup và cũng cho phép các máy tính trên mạng Wi-Fi truy cập Internet thông qua router WiFi.*

Để cấu hình máy tính được bật Wi-Fi sao cho nó có thể tham gia workgroup Windows, nó phải được cấu hình với Client for Microsoft Network (một client). File and Printer Sharing for Microsoft Networks (một dịch vụ) và TCP/IP Network Protocol. Được cấu hình nghĩa là không chỉ được cài đặt trên máy tính mà còn kích hoạt trong hộp Properties. Do đó, bạn sẽ thấy một client chẳng

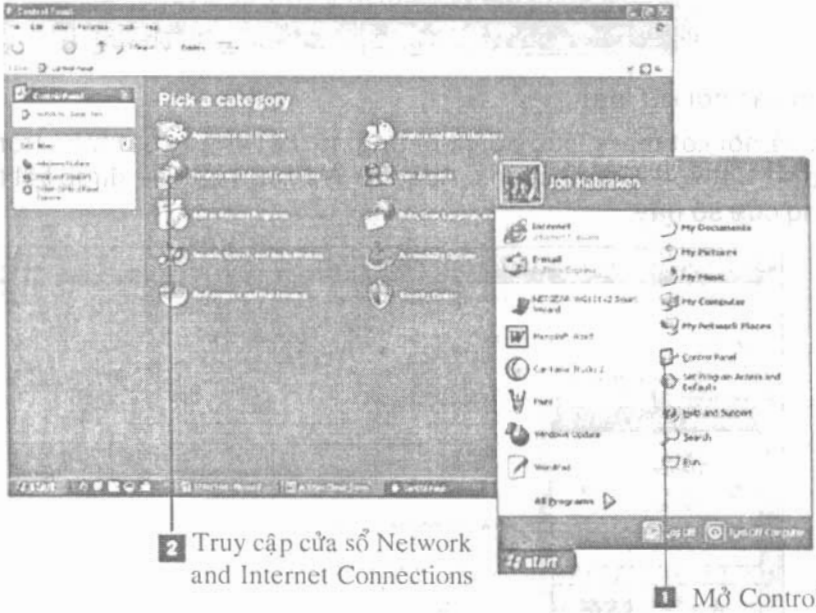
hạn như Client for Microsoft Networks được liệt kê trong hộp thoại Properties nhưng có thể không được kích hoạt (hộp kiểm cho client không được chọn).

Tác vụ này xem xét hộp thoại Properties cho adapter WiFi, bạn truy cập bất kỳ client hoặc service nào mà bạn có thể cần thêm vào và cũng kích hoạt bất kỳ service, client hoặc giao thức (protocol) vốn được cài đặt nhưng hiện không được kích hoạt.

Ghi chú

Bạn có thể có nhiều nối kết cục bộ trên một máy tính. Ví dụ, một máy tính có một nối kết trên một adapter mạng cho một mạng hữu tuyến thì cũng có một adapter WiFi cho một mạng không dây. Bạn có thể disable (tắt) bất kỳ adapter mạng mà bạn không sử dụng trong Device Manager vốn được truy cập bằng hộp thoại System Properties. Tuy nhiên, bạn không tiết kiệm bất kỳ năng lượng hệ thống và bạn không tăng tính có sẵn của nguồn tài nguyên hệ thống một cách đáng kể như vậy bằng việc tắt một thiết bị không sử dụng. Do đó tắt một thiết bị không sử dụng là tùy thuộc vào bạn. Nếu thiết bị chẳng hạn như một adapter WiFi USB được tháo ra khỏi máy tính, bạn cũng không cần phải tắt thiết bị này trong Device Manager.

40. Mở các thuộc tính nối kết và bật các Client, giao thức và dịch vụ



1. Mở Control Panel

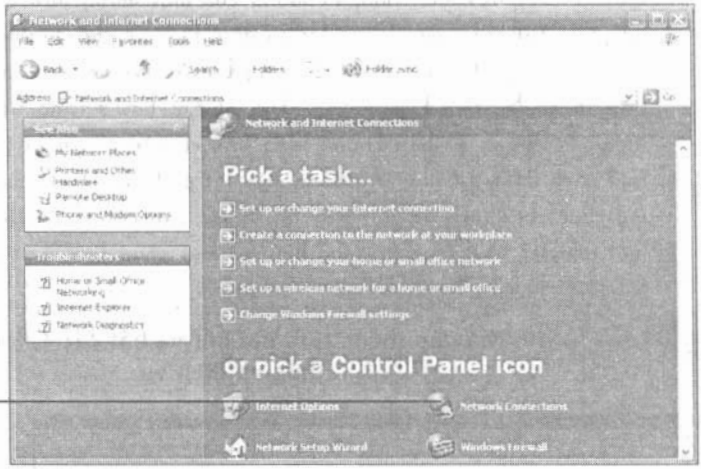
   Nhấp Start và sau đó nhấp biểu tượng Control Panel trên menu Start. Control Panel mở ra.

2. Truy cập cửa sổ Network and Internet Connections

   Trong Control Panel, nhấp link Network and Internet Connections. Cửa sổ Network and Internet Connections mở ra.

3. Mở cửa sổ Network Connections.

   Để mở cửa sổ Network Connections, nhấp biểu tượng Network Connections (gần cuối cửa sổ Network and Internet Connections).



3. Mở cửa sổ Network Connections

4. Xem các nối kết mạng

   Tất cả nối kết mạng cục bộ và những nối kết khác xuất hiện trong cửa sổ Network Connections. Adapter WiFi của bạn sẽ được liệt kê trong cửa sổ này.



4. Xem các nối kết mạng.

Ghi chú

Nếu bạn có nhiều adapter mạng trên một máy tính (thậm chí nếu một adapter mạng hữu tuyến không được nối kết), bạn có thể thấy một cầu nối (bridge) mạng được liệt kê trong cửa sổ Network Connections. Một cầu nối được tạo để liên kết các mạng khác nhau lại với nhau. Do đó các máy tính có nhiều adapter mạng có thể có một cầu nối nhằm cung cấp một nối kết giữa hai nối kết cục bộ khác nhau được tạo ra bởi hai adapter.

Nhấp phải biểu tượng nối kết cục bộ của adapter WiFi trong cửa sổ Network Connections và chọn Properties. Hộp thoại Local Area Connection Properties mở ra cho adapter WiFi.

5. Xem các thuộc tính và bật các thành phần được cài đặt



Điều quan trọng là bạn phải kiểm kê (viết nó ra hoặc chỉ việc nhớ các xác lập) các client, service (dịch vụ) và giao thức được cài đặt cho nối kết LAN hiện được chọn (adapter WiFi của bạn). Sử dụng thanh cuộn để cuộn qua các mục trong hộp thoại xem các mục trong danh sách properties. Hãy chắc chắn các mục sau đây xuất hiện trong danh sách properties:

- ***Client for Microsoft Networks.*** *Client này cần để máy tính truy cập một mạng Microsoft (chẳng hạn như một workgroup). Nếu mục này được liệt kê nhưng không được mở, nhấp hộp kiểm của client. Nếu mục này không được liệt kê, bạn phải thêm client.*
- ***File and Printer Sharing for Microsoft Networks.*** *Dịch vụ này cho phép bạn chia sẻ các folder trên máy tính với những máy*

tính khác kết nối với workgroup của bạn. Dịch vụ cũng cho phép bạn chia sẻ một máy in được nối với máy tính của bạn bằng workgroup. Nếu mục này không được liệt kê, bạn phải thêm nó.

- ***Internet Protocol (TCP/IP).*** *Mục này xuất hiện trong danh sách hộp thoại Properties bởi vì nó là giao thức mặc định cho hệ điều hành Windows XP. Bạn không thể giao tiếp trong workgroup hoặc trên Internet nếu không có giao thức này. Mặc dù nó không thể được loại bỏ khỏi danh sách, nhưng nó có thể được tắt. Nhấp hộp kiểm cho Internet Protocol (TCP/IP) để mở giao thức nếu cần.*

Nếu một mục được liệt kê chẳng hạn như Client for Microsoft Networks được cài đặt nhưng không được mở, (nghĩa là hộp kiểm ở bên trái client nằm bên trái client chứa một dấu kiểm), nhấp một dấu kiểm của mục để mở nó. Nếu thiếu bất kỳ mục được liệt kê (client hoặc service), bạn phải thêm client hoặc dịch vụ (service) mạng như được trình bày chi tiết trong **mục 41**.

41. Thêm một client hoặc dịch vụ mạng

Trước khi bạn bắt đầu

40. Mở các thuộc tính nối kết và bật các Client, giao thức và dịch vụ

Như được thảo luận trong **mục 40**, bạn phải cấu hình adapter mạng WiFi để máy tính có thể tham gia một workgroup. Điều này có nghĩa rằng Local Area Connection (từ này đồng nghĩa với adapter WiFi) phải được cấu hình với Client for Microsoft Networks (client cho phép truy cập workgroup) và dịch vụ File and Printer Sharing for Microsoft Networks (vốn cho phép chia sẻ file và in trên máy tính). Sau cùng, máy tính phải được cấu hình với một giao thức mạng. Bạn sẽ sử dụng giao thức TCP/IP cung cấp cho máy tính khả năng giao tiếp trong workgroup và trên Internet (vốn đòi hỏi TCP/IP). Điều cốt yếu là ba mục này phải được liệt kê trong hộp thoại Local Area Connection Properties của adapter WiFi. Không được phép thay thế nếu bạn muốn máy tính thật sự gia nhập mạng.

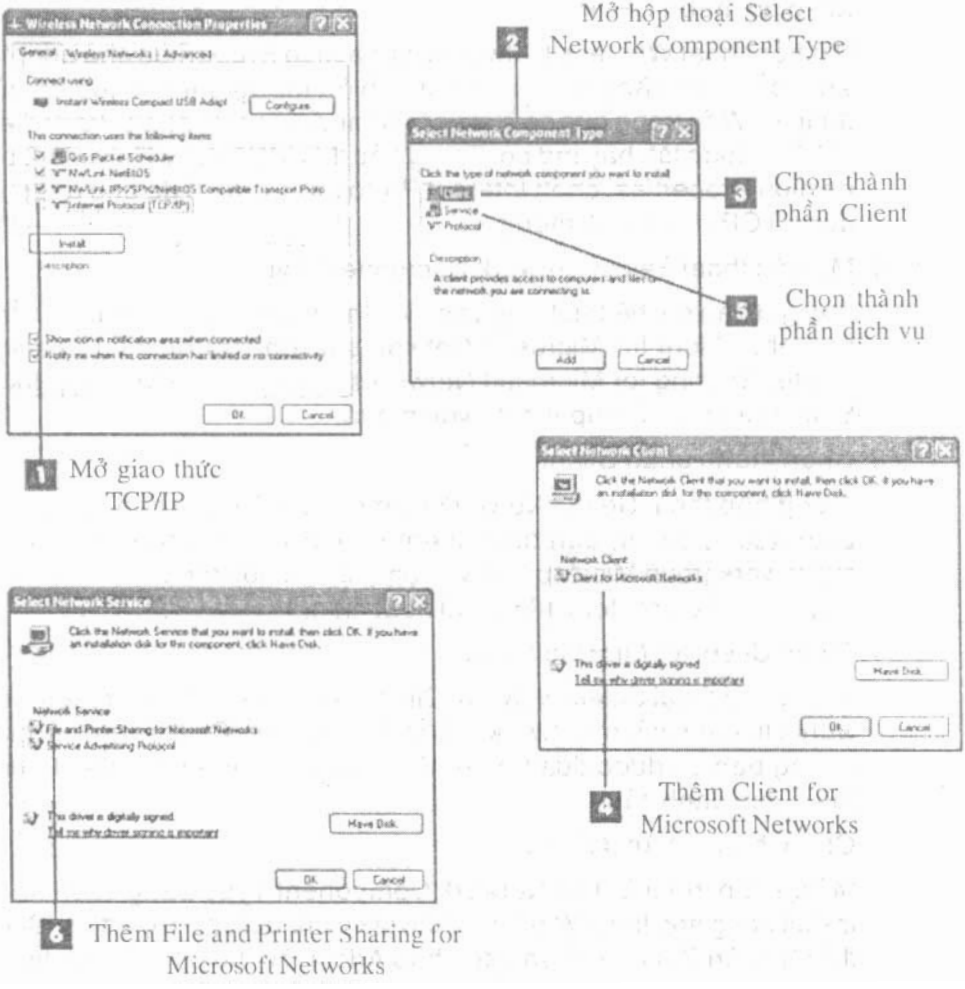
Trong một số trường hợp, phụ thuộc vào ai đã cấu hình các xác lập mạng máy tính (và việc các xác lập đó đã được thay đổi từ khi bạn mua máy tính hay không), ba mục này có thể đã được cấu hình trong hộp thoại Wireless Network Connection Properties. Bởi vì TCP/IP là giao thức mặc định cho Windows XP, nó đã được cài đặt trên hệ thống; thực tế Windows XP không cho phép bạn gỡ bỏ TCP/IP ra khỏi hộp thoại Wireless Network Connection Properties. Tuy nhiên, bạn có thể tắt (disable) giao thức bằng cách xóa dấu kiểm kế bên mục Internet Protocol (TCP/IP) trong danh sách properties.

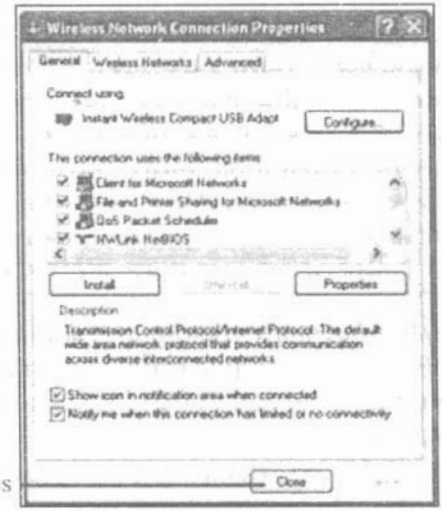
Bởi vì TCP/IP sẽ xuất hiện trong danh sách properties theo mặc định (chúng ta đang nói về Windows XP), bạn phải bảo đảm nó được mở, nghĩa là có một dấu kiểm trong hộp kiểm Internet Protocol (TCP/IP). Sau đó, bạn có thể tập trung vào việc thêm Client for Microsoft Networks (client) và dịch vụ File and Printer Sharing for Microsoft Networks.

THỦ THUẬT: Bạn cần tiến hành tác vụ này chỉ khi nào thiếu một trong các mục bắt buộc này trong cấu hình của adapter WiFi. Xem trở lại danh sách kiểm kê cấu hình mà bạn đã làm trong tác vụ trước để thấy có thiếu bất kỳ thành phần bắt buộc nào để nối mạng workgroup hay không hoặc TCP/IP đã được tắt cho nối kết hay không. Nếu vậy, sử dụng tác vụ này để thêm thành phần cụ thể đó hoặc mở giao thức TCP/IP.

Mọi máy tính gia nhập workgroup phải được cấu hình để nối mạng workgroup Microsoft. Điều này có nghĩa rằng tất cả mục cấu hình được trình bày chi tiết trong tác vụ này phải được cấu hình trên một máy tính vốn sẽ là một thành viên của workgroup.

41. Thêm một Client hoặc dịch vụ mạng





Đóng hộp thoại Wireless Network Connection Properties

1. Mở giao thức TCP/IP

   Mở hộp thoại Wireless Network Connection Properties cho adapter WiFi của bạn bằng cách nhấp phải biểu tượng nối kết cục bộ của adapter WiFi trong cửa sổ Network Connections và chọn Properties. TCP/IP được tắt, hãy mở nó. Trong hộp thoại Wireless Network Connection Properties, chọn Internet Protocol (TCP/IP) để cho phép sử dụng TCP/IP trên hệ thống.

2. Mở hộp thoại Select Network Component Type

   Bây giờ bạn có thể tập trung vào việc thêm các mục bắt buộc chẳng hạn như Client for Microsoft Networks (client) và dịch vụ File and Printer Sharing for Microsoft Networks. Nhấp nút Install. Hộp thoại Select Network Component Type mở ra.

3. Chọn thành phần Client

   Trong hộp thoại Select Network Component Type, chọn loại thành phần (component) cần được thêm vào. Bởi vì chúng ta cần thêm client workgroup Microsoft, hãy chọn client từ hộp thoại và nhấp Add. Hộp thoại Select Network Client xuất hiện.

4. Thêm Client for Microsoft Networks

   Trong hộp thoại Select Network Client, chọn Client for Microsoft Networks từ danh sách Network Client và nhấp OK. Có thể mất vài giây nhưng bạn sẽ được đưa trở về hộp thoại Properties và client được thêm vào danh sách.

5. Chọn thành phần dịch vụ

   Mở lại hộp thoại Select Network Component Type bằng cách nhấp Install trong hộp thoại Wireless Network Connection Properties. Chọn thành phần Service và sau đó nhấp Add. Hộp thoại Select Network Service mở ra.

6. Thêm File and Printer Sharing for Microsoft Networks

Trong hộp thoại Select Network Service, nhấp File and Printer Sharing for Microsoft Networks và nhấp OK. Dịch vụ này được thêm vào danh sách configuration trong hộp thoại Wireless Network Connection Properties.

THỦ THUẬT: Bạn có thể thấy các client và service (dịch vụ) khác có sẵn cho hệ thống của bạn chẳng hạn như Service Advertising Protocol hoặc giao thức NWLink. Những mục này được sử dụng trên các mạng triển khai Novell NetWare. Bạn không cần phải thêm hoặc thật sự làm bất cứ điều gì với bất kỳ client hoặc service có sẵn ngoại trừ client Client for Microsoft Networks và dịch vụ File and Printer Sharing for Microsoft Networks bắt buộc để nối mạng workgroup.

---

7. Đóng hộp thoại Wireless Network Connection Properties.

Sau khi TCP/IP được mở và Client for Microsoft Networks và dịch vụ File and Printer Sharing for Microsoft Networks được mở, bạn có thể đóng hộp thoại bằng cách nhấp Close.

THỦ THUẬT: Trong một số trường hợp Client for Microsoft Networks hoặc dịch vụ File and Printer Sharing for Microsoft Networks sẽ được cài đặt trong danh sách properties của adapter WiFi nhưng đã được tắt. Nếu một trong hai mục này được liệt kê nhưng đã được tắt, nhấp dấu kiểm nằm bên trái mục để mở client hoặc dịch vụ.

THỦ THUẬT: Có thể bạn không chắc chắn một số mục được liệt kê trong hộp thoại Wireless Network Connection Properties có cần thiết hay không. Bạn có thể chọn một mục từ danh sách và nhấp nút Uninstall để gỡ bỏ các client, dịch vụ hoặc giao thức không mong muốn. Tuy nhiên, nếu bạn không chắc chắn chức năng của một mục hoặc việc nó có cần thiết hay không, không gỡ cài đặt nó. Việc gỡ bỏ các dịch vụ hoặc giao thức cần thiết có thể ảnh hưởng đến khả năng máy tính giao tiếp trên mạng.

42. Cấu hình các xác lập TCP/IP

Trước khi bạn bắt đầu

40. Mở các thuộc tính nối kết và bật các Client, giao thức và dịch vụ

41. Thêm một Client hoặc dịch vụ mạng

Nối kết cục bộ (adapter mạng WiFi) phải được cấu hình với những xác lập TCP/IP thích hợp để giao tiếp trên mạng và tận dụng nối kết Internet tốc độ cao. Bởi vì sách này giả định bạn đã thêm một router WiFi vào mạng để tận dụng nối kết Internet băng tần rộng, bạn có thể để router phân phối các xác lập TCP/IP cho những máy tính khác nhau trên mạng WiFi.

Để router WiFi tự động cấu hình các xác lập TCP/IP cho một máy tính (kể cả địa chỉ IP), nối kết cục bộ trên một máy tính phải được cấu hình dưới dạng một client Dynamic Host Configuration Protocol (DHCP). Điều này có nghĩa máy tính yêu cầu một địa chỉ IP và thông tin cấu hình TCP/IP khác khi nó khởi động. Router WiFi phản hồi bằng thông tin cần thiết.

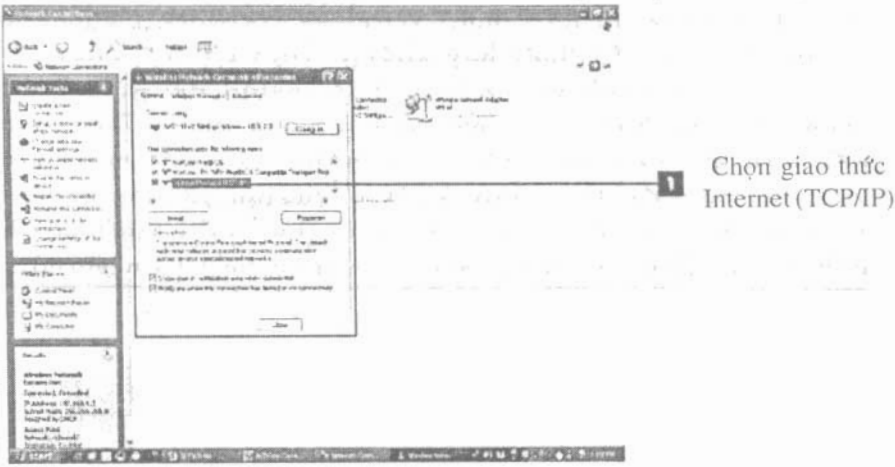
THUẬT NGỮ CHÍNH

Dynamic Host Configuration Protocol (DHCP). Một giao thức được sử dụng bởi các server và client DHCP để thương lượng việc gán động các địa chỉ IP trên một mạng. Server DHCP (chẳng hạn như một router WiFi) cung cấp cho client DHCP địa chỉ IP.

Client DHCP. Một máy tính đã được cấu hình cho giao thức TCP/IP để địa chỉ IP (và subnet mask) được tự động gán vào máy tính bởi một thiết bị chẳng hạn như router WiFi vốn có chức năng như một server DHCP.

Bạn cấu hình một máy tính dưới dạng một client DHCP trong hộp thoại Internet Protocol (TCP/IP) Properties mà bạn có thể truy cập từ hộp Wireless Network Connection Properties. Theo mặc định, các máy tính Windows đã được cấu hình dưới dạng DHCP. Tuy nhiên, xem qua các bước về cách cấu hình các thuộc tính TCP/IP cho một adapter WiFi thì không có hại gì cả.

42. Cấu hình các xác lập TCP/IP





2. Xác lập các thuộc tính tổng quát (general)



3. Xác lập cấu hình luân phiên.

1. Chọn giao thức Internet (TCP/IP)

Trong hộp thoại Wireless Network Connection Properties cho adapter WiFi, cuộn xuống danh sách các client, dịch vụ và giao thức và chọn Internet Protocol (TCP/IP), sau đó nhấp nút Properties. Hộp thoại Internet Protocol (TCP/IP) Properties mở ra.

2. Xác lập các thuộc tính khái quát (General)

Để cấu hình adapter dưới dạng một client DHCP, chọn tùy chọn Obtain and IP address automatically được đặt trên tab General của hộp thoại Internet Protocol (TCP/IP) Properties. Cũng chọn tùy chọn Obtain DNS server address automatically. Sau đó nhấp tab Alternate Configuration.

3. Xác lập cấu hình luân phiên (Alternate Configuration)

Tab Alternate Configuration thì tùy chọn, nhưng nó có thể hữu dụng nếu bạn sử dụng máy tính trong chế độ Ad Hoc (chế độ computer-to-computer) vốn đòi hỏi một địa chỉ IP và subnet mask cố định. Chọn tùy chọn User Configured và sau đó gõ nhập một địa chỉ IP và subnet mask trong các hộp thích hợp. Bạn có thể sử dụng bất kỳ dãy địa chỉ IP riêng cho những địa chỉ IP này (**xem mục 37**). Bạn không cần phải nhập gateway, các server DNS hoặc server WINS mặc định. Chỉ các địa chỉ IP cần cho chế độ Ad Hoc (vì nối kết Ad Hoc chỉ hiện hữu giữa các máy tính vốn được cấu hình cho chế độ Ad Hoc).

Khi bạn xác lập xong các thuộc tính TCP/IP cho adapter, đóng hộp thoại Internet Protocol (TCP/IP) Properties bằng cách nhấp OK. Bạn quay trở về hộp thoại Wireless Network Connection Properties.

43. Kiểm tra trạng thái Adapter WiFi

Trước khi bạn bắt đầu

40. Mở các thuộc tính nối kết và mở các client, giao thức và dịch vụ

41. Thêm một client hoặc dịch vụ mạng

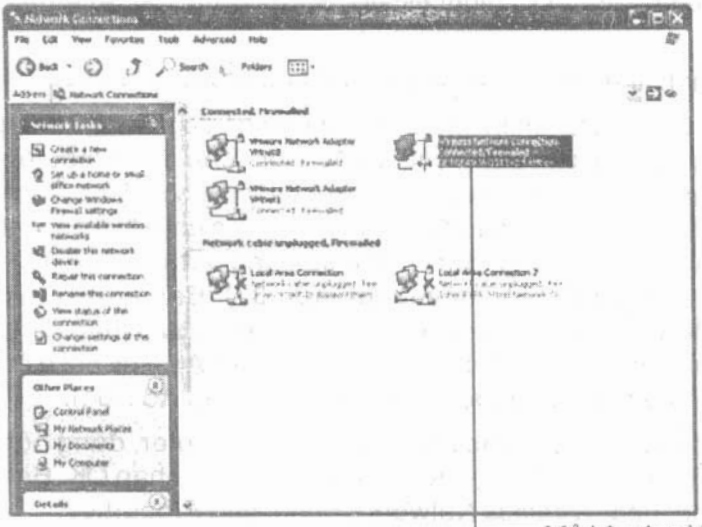
42. Cấu hình các xác lập TCP/IP

Bây giờ bạn đã cấu hình máy tính để truy cập mạng và các xác lập TCP/IP, bạn có thể muốn kiểm tra trạng thái của adapter mạng WiFi trong hộp thoại Wireless Network Connection Status. Hộp thoại này không chỉ cho phép bạn kiểm tra thời hạn nối kết và cường độ tín hiệu mà nó còn cho phép bạn xem địa chỉ IP đã được router WiFi gán vào adapter.

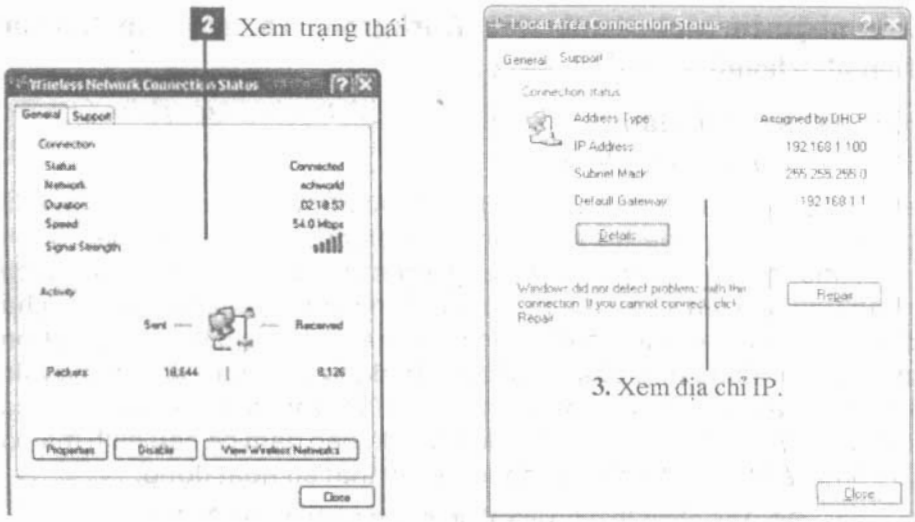
Khả năng xem trạng thái (status) cho bạn biết adapter có hoạt động tốt hay không. Mặc dù thời hạn nối kết không phải là một xác lập quan trọng như thế (trừ khi bạn gặp phải sự biến mất tín hiệu và mất nối kết), việc biết xem router WiFi đã gán một địa chỉ IP vào adapter hay không là điều quan trọng. Và khả năng xem nhanh cường độ tín hiệu của nối kết sẽ cho bạn biết PC có thể thu các tín hiệu video từ router WiFi tốt như thế nào.

THỦ THUẬT: Hoặc, bạn có thể nhấp phải biểu tượng nối kết WiFi trong vùng Notification ở đầu phải của taskbar và chọn status từ menu ngữ cảnh để xem trạng thái của adapter WiFi. Nếu bạn sử dụng một tiện ích cấu hình đi kèm với adapter WiFi, việc chọn tùy chọn Status có thể mở tiện ích đó, được sử dụng để xem trạng thái và xác lập IP của adapter WiFi.

43. Kiểm tra trạng thái adapter WiFi



1 Mở hộp thoại Wireless Network Connection Status.



1. Mở hộp thoại Wireless Network Connection Status.

   Trong cửa sổ Network Connections (được mở từ Control Panel), nhấp đôi biểu tượng cho nối kết mạng WiFi. Hộp thoại Wireless Network Connection mở ra.

2. Xem trạng thái

   Tab General của hộp thoại cung cấp trạng thái hiện hành của nối kết của adapter WiFi và cường độ tín hiệu hiện hành cho nối kết. Thời hạn của nối kết có thể được sử dụng để quyết định xem đã có một sự cố gần đây với nối kết thật sự hay không, cường độ tín hiệu cho phép bạn đánh giá adapter WiFi của máy tính kết nối với access point của router WiFi như thế nào.

   Nhấp tab Support để mở trang thứ hai của hộp thoại.

3. Xem địa chỉ IP

   Tab Support của hộp thoại Wireless Network Connection Status hiển thị địa chỉ IP và subnet mask được gán vào adapter bởi router WiFi. Nó cũng hiển thị địa chỉ IP của gateway mặc định còn được gọi là router WiFi (nó là gateway giữa mạng WiFi riêng của bạn và mạng công cộng, Internet). Nhấp Close để đóng hộp thoại.

THUẬT NGỮ CHÍNH

Gateway. Một thiết bị làm trung gian giữa hai loại mạng khác nhau. Trong trường hợp này, chúng ta xem xét thiết bị: router WiFi vốn kết nối mạng workgroup riêng và Internet công cộng. Router WiFi là gateway.

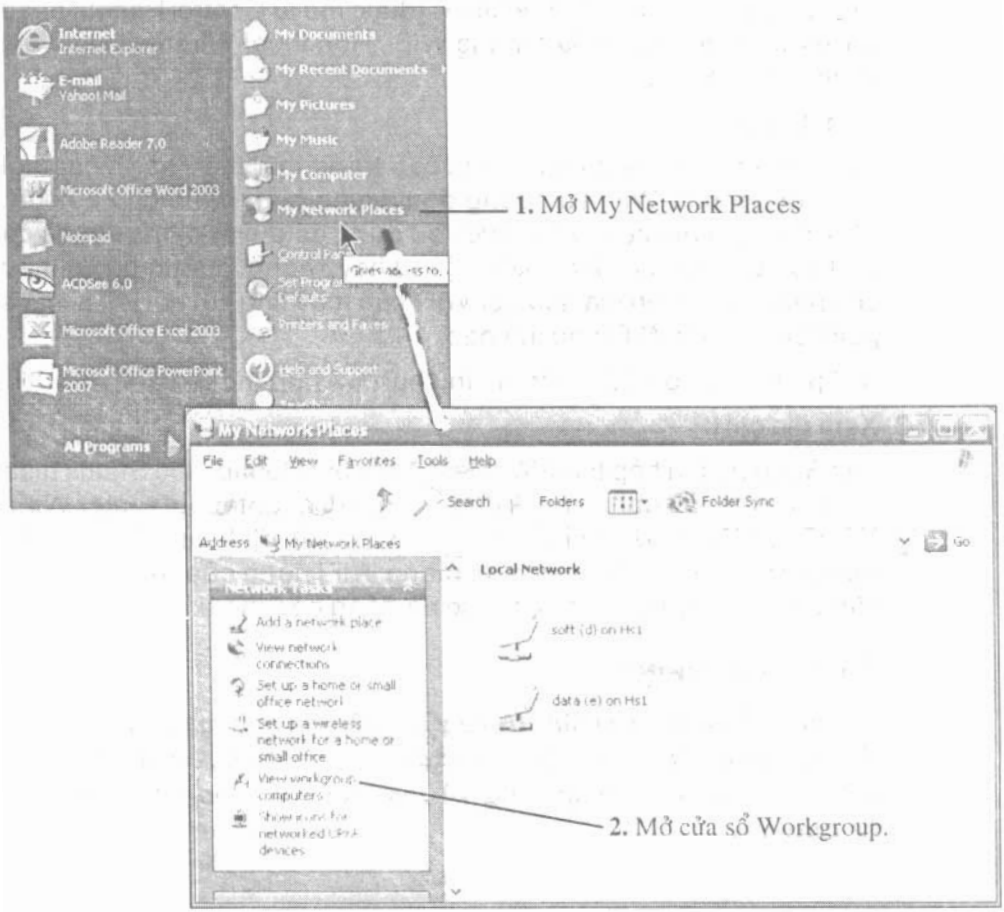
44. Xác nhận tư cách thành viên Workgroup và truy cập Network Neighborhood

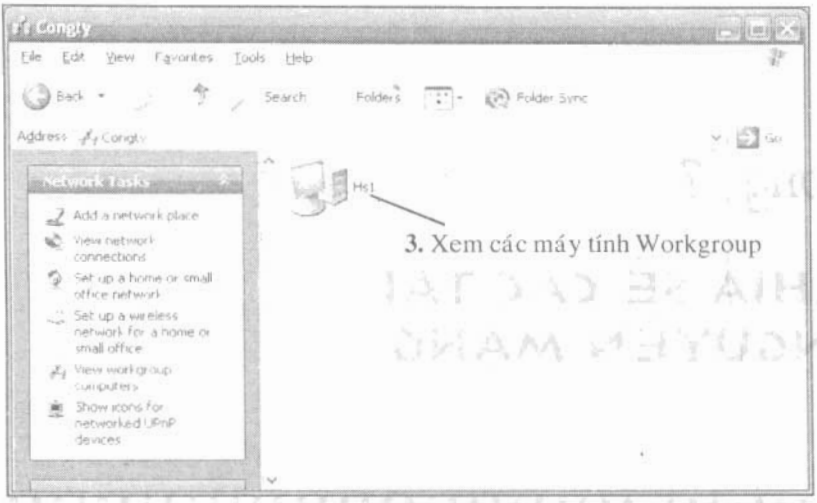
Trước khi bạn bắt đầu

38. Chạy Network Setup Wizard.

Sau khi bạn đã cấu hình các máy tính được bật WiFi (hoặc các máy tính mạng được nối cứng) để trở thành thành viên của workgroup, bạn có thể duyệt tìm những máy tính này trên mạng. Định vị những máy tính này sẽ cho phép bạn truy cập bất kỳ tài nguyên chia sẻ mà chúng có thể có chẳng hạn như các file và máy in. Nếu bạn không thể thật sự thấy các máy tính trong workgroup, bạn đang gặp phải một loại vấn đề kết nối nào đó với máy tính mà bạn đang làm việc hoặc với những máy tính workgroup khác. Xem các máy tính workgroup trong cửa sổ Workgroup để bảo đảm cả cấu hình mà bạn đã tạo trong các tác vụ trước của chương này thật sự hoạt động.

44. Xác nhận thành viên Workgroup và truy cập Network Neighborhood





1. Mở My Network Places.

   Nhấp nút Start và sau đó chọn My Network Places trên menu Start. Cửa sổ My Network Places mở ra. Cửa sổ này cho bạn thấy bất kỳ vị trí mạng mà bạn đã thiết lập một nối kết với. Để biết thêm thông tin về việc thêm Network Places vào máy tính, **xem mục 53**.

2. Mở cửa sổ Workgroup

   Trong danh sách Network Tasks nằm phía bên trái cửa sổ, nhấp View workgroup computer. Cửa sổ workgroup mở ra.

3. Xem các máy tính Workgroup

   Tất cả máy tính trong workgroup xuất hiện trong cửa sổ workgroup. Bạn có thể truy cập bất kỳ tài nguyên được chia sẻ trên những máy tính này bằng cách nhấp đôi một máy tính riêng biệt. Để biết thêm chi tiết về việc chia sẻ truy cập các tài nguyên workgroup, **xem mục 45.**

Chương 7

CHIA SẺ CÁC TÀI NGUYÊN MẠNG

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *45. Bàn về việc chia sẻ các tài nguyên mạng*
- *46. Chia sẻ một máy in*
- *47. Chia sẻ một Folder*
- *48. Bàn về việc truy cập các tài nguyên mạng*
- *49. Truy cập các Folder chia sẻ và mở các File chia sẻ*
- *50. Ánh xạ một ổ đĩa mạng*
- *51. Kết nối một máy in chia sẻ*
- *52. Tìm các máy tính mạng*
- *53. Thêm một vị trí mạng*

Sau khi đã thiết lập router WiFi và cấu hình các máy tính được bật WiFi cũng như các máy tính được "nối dây" trên mạng để nối mạng workgroup, bạn sẵn sàng chia sẻ các tài nguyên mạng, chẳng hạn như các folder và máy in. Sau khi một tài nguyên được chia sẻ, nó có thể được chia sẻ bởi những máy tính khác trong workgroup. Chương này sẽ xem xét cách chia sẻ một tài nguyên cụ thể, chẳng hạn như một máy in trong một workgroup và xem những người dùng trong workgroup có thể truy cập các tài nguyên có sẵn như thế nào.

45. Bàn về việc chia sẻ các tài nguyên mạng

Trước khi bạn bắt đầu

4. Duyệt tìm các File và Folder
5. Bàn về My Network Places

37. Bàn về việc cấu hình các PC để nối mạng

44. Xác nhận tư cách thành viên Workgroup và truy cập Network Neighborhood.

Từ network resources (tài nguyên mạng) là một từ rộng để chỉ các mục mà bạn có thể chia sẻ trên mạng. Trong một workgroup Windows, bạn có thể chia sẻ các ổ đĩa, folder (và các file trong các folder) và máy in. Bởi vì chúng ta sẽ làm việc trong một workgroup không có server trung tâm, các loại mục mà chúng ta có thể chia sẻ thì giới hạn. Mặc dù chúng ta có thể chia sẻ sự truy cập đến một folder vốn chứa một chương trình cài đặt phần mềm và cài đặt phần mềm này bằng cách truy cập folder chia sẻ, nhưng điện toán workgroup không cung cấp các ứng dụng. Do đó bạn không thể chạy phần mềm được cài đặt trên một máy tính qua mạng trên một máy tính khác ngay cả nếu bạn chia sẻ folder và các file thực thi cho chương trình đó. Nó cũng vi phạm hợp đồng phần mềm để chạy các ứng dụng đồng thời trên hai máy tính trừ khi bạn có nhiều license (bản quyền) cho phần mềm.

Một ổ đĩa hoặc folder chia sẻ được gọi là một share. Sự truy cập đến share được điều khiển bởi người thật sự chia sẻ ổ đĩa hoặc folder trên máy tính của mình.

Thuật ngữ chính

Share. Một ổ đĩa hoặc folder vốn được chia sẻ trên mạng.

Ghi chú

Các máy tính chạy Windows XP có thể chia sẻ các mục chẳng hạn như các máy in và folder khi chúng đã được cấu hình để nối mạng workgroup. Điều này đòi hỏi Client for Microsoft Networks được cài đặt và được mở trên máy tính và rằng File and Printer Sharing for Microsoft Networks cũng được cài đặt và được mở. Bạn có thể cấu hình những mục này trong hộp thoại Wireless Network Connnection Properties. Xem mục 41 để biết thêm thông tin.

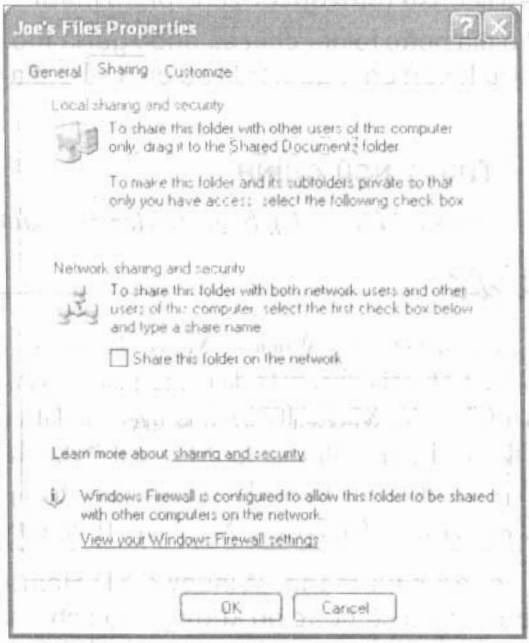
Đối với an ninh mạng, Windows XP Home Edition thì hơi lỏng lẻo. Một share được chia sẻ hoặc nó không được chia sẻ. Một khi một share đã được làm cho có sẵn đối với workgroup, nó có thể được thấy bởi tất cả thành viên trong workgroup của nó. Vấn đề an ninh liên quan đến việc những người dùng truy cập các share có thật sự thực hiện các thay đổi đối với các file trong share hay không; quyết định về việc những người dùng mạng có thể chỉnh sửa các file chia sẻ hay không tùy thuộc vào người đã tạo share lúc ban đầu

Do đó, nối mạng workgroup được phân quyền nghĩa là mỗi người dùng trên một máy tính trong workgroup có thể chia sẻ (hoặc không chia sẻ) các nguồn tài nguyên. Nối mạng peer-to-peer phân quyền chẳng hạn như nối mạng workgroup Microsoft chắc chắn tiện lợi trong việc chia sẻ các tài nguyên giữa những người dùng máy tính workgroup. Tuy nhiên, nó không cung cấp

môi trường an toàn của một mạng tập trung vốn đòi hỏi người dùng truy cập các tài nguyên trên một server mạng tập trung và an toàn.

Điều này có nghĩa bảo vệ an toàn workgroup không chỉ là bảo vệ mạng hơi không an toàn khỏi sự xâm nhập bên ngoài, mà bạn còn phải bảo vệ mạng WiFi bằng cách sử dụng những tính năng an ninh được cung cấp bởi router WiFi (bạn bảo vệ an toàn phương tiện mạng, các sóng vô tuyến WiFi, thay vì cơ cấu phần mềm mà hệ điều hành Windows sử dụng để chia sẻ các tài nguyên). Tiếp theo thông tin về việc bảo vệ an toàn hạ tầng mạng, **xem mục 72**.

Việc chia sẻ các folder và máy in trong môi trường Windows thì cực kỳ đơn giản. Mỗi mục chẳng hạn như một máy in hoặc folder có một hộp thoại Properties (**mục 46** và **mục 47** sẽ trình bày cách truy cập những hộp thoại này). Các hộp thoại Properties này, mỗi hộp thoại cung cấp một tab Sharing với các xác lập để chia sẻ các tài nguyên cụ thể đó.



Tab Sharing của một folder được sử dụng để cấu hình một folder dưới dạng một tài nguyên chia sẻ trong workgroup.

Ghi chú

Khi nhiều người dùng sử dụng cùng một máy tính, mỗi người có một user profile kiểm soát sự truy cập đến các folder được tạo cho người đó trên máy tính đó. Để chia sẻ một folder với người mà bạn dùng chung máy tính (ở đây không nói về việc chia sẻ một folder với các máy tính workgroup khác), bạn chỉ việc rê folder từ cửa sổ My Computer (nhấp nút Start và sau đó chọn My Computer để mở cửa sổ) đến folder Share Documents vốn cũng xuất hiện trong cửa sổ My Computer. Bất kỳ người dùng trên máy tính chia sẻ sau đó có thể truy cập các file trong folder mà bạn đã chia sẻ bằng cách rê nó đến folder Shared Documents. Kiểu chia sẻ này (giữa những người dùng khác nhau trên cùng một máy tính)

có thể xảy ra thậm chí khi một máy tính không được cấu hình để nối mạng. Do đó, đừng nhầm lẫn việc chia sẻ các folder cục bộ trên một máy tính với việc chia sẻ các folder trên một mạng workgroup. Để biết thêm thông tin về việc tạo nhiều tài khoản người dùng trên cùng một máy tính, xem mục 11.

46. Chia sẻ một máy in

Trước khi bạn bắt đầu

45. Bàn về việc chia sẻ các tài nguyên mạng

Một người dùng máy tính có một máy in được nối với máy tính có thể chia sẻ máy tính với những người dùng khác trong workgroup. Chia sẻ một máy in cho phép những người dùng trên một máy tính trong mạng in sang một máy in. Một máy in được nối trực tiếp là một máy in được nối với máy tính nối kết USB hoặc một nối kết parallel thường là LPT1, đây là cổng máy in parallel mặc định. Bởi vì USB đã trở thành cách phổ biến nhất để nối các thiết bị ngoại vi, chẳng hạn như các máy in với các máy tính, có lẽ bạn sử dụng một máy in USB (hầu hết các máy in không còn cung cấp một cổng parallel để nối kết với máy tính nữa).

Cho dù máy in được nối với máy tính (USB hoặc parallel) như thế nào thì nó cũng được gọi là máy in cục bộ. Người dùng máy tính chia sẻ máy in cục bộ của mình với những người dùng khác trong workgroup mà thật sự xem máy in là một máy in từ xa (remote printer).

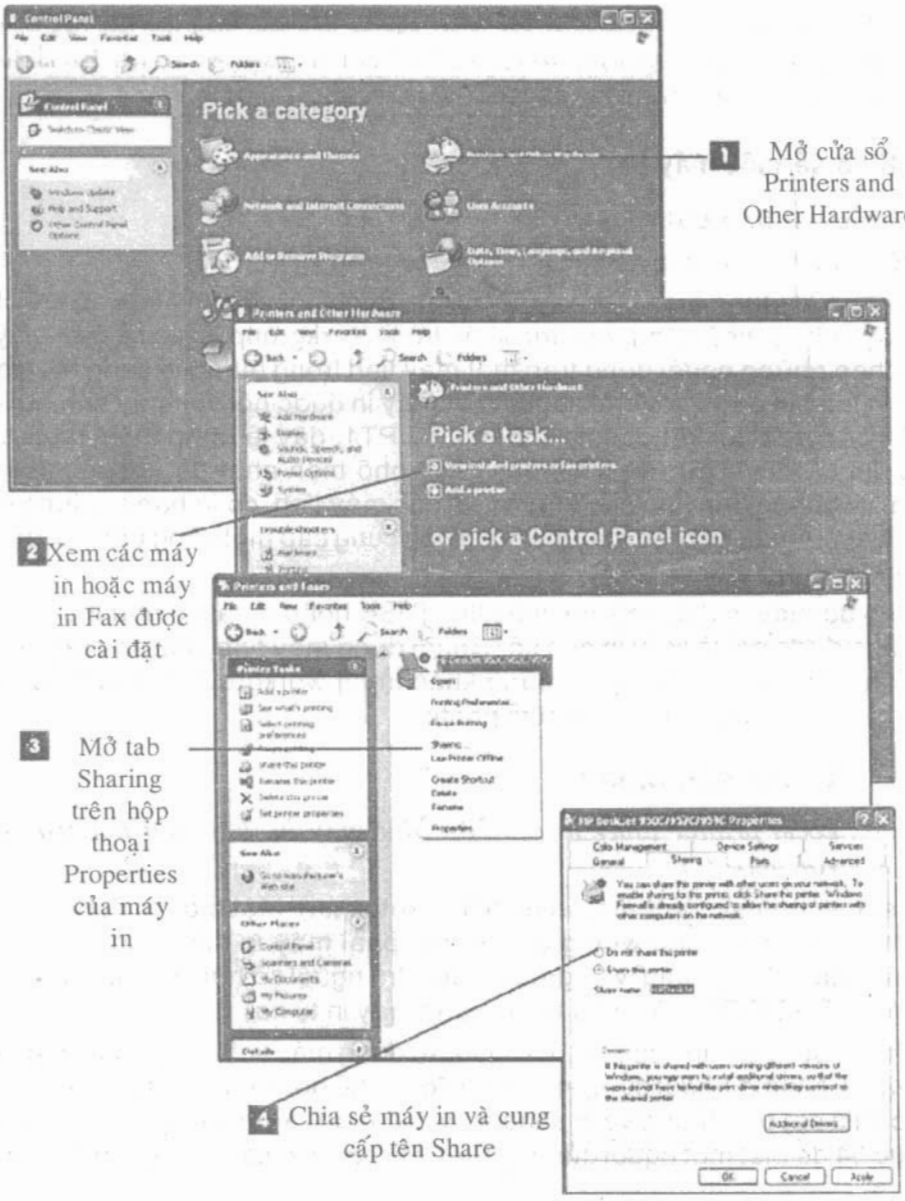
Thuật ngữ chính

Local printer (máy in cục bộ). Một máy in được nối kết trực tiếp với máy tính.

Remote printer. (Một máy in được nối kết từ xa). Một máy in được nối kết với một máy tính trong workgroup không phải máy in hiện được sử dụng. Những người dùng trong workgroup, ngoại trừ người sở hữu máy tính mà máy in được nối kết bằng vật lý có thể in sang máy in từ xa.

Máy in cục bộ được chia sẻ bởi người sử dụng máy tính mà máy in được kết nối vật lý. Những người dùng khác sau đó có thể nối kết với máy in từ xa (vốn được chia sẻ) trên mạng và in sang máy in đó. Hãy xem cách chia sẻ máy in, ở **mục 54** để biết một người dùng nối kết với máy in chia sẻ từ xa như thế nào.

46 Chia sẻ một máy in



1. Mở cửa sổ Printers and Other Hardware

   Chúng ta cần đào sâu qua các cửa sổ Control Panel để có thể mở hộp thoại Properties cho máy in mà bạn muốn chia sẻ. Mở Control Panel bằng cách nhấp Start và chọn Control Panel, sau đó nhấp link Printers and Other Hardware. Cửa sổ Printers and Other Hardware mở ra.

2. Xem các máy in hoặc máy in Fax được cài đặt.

Nhấp link View Installed printers or fax printers trong cửa sổ Printers and Other Hardware. Cửa sổ Printers and Faxes mở ra.

3. Mở tab Sharing trên hộp thoại Properties của máy in.

   Nhấp phải biểu tượng của máy in cục bộ mà bạn muốn chia sẻ (nhãn biểu tượng không nói rằng máy in là cục bộ, nhưng nếu bạn nói rằng máy in đã nối kết từ xa, nó sẽ thường đặt tên cho máy in vốn chia sẻ máy in). chọn Sharing từ menu ngữ cảnh vừa xuất hiện. Hộp thoại Properties cho máy in được chọn mở ra với tab Sharing được chọn.

THỦ THUẬT: Nếu tùy chọn Share this Printer không có sẵn trên tab Sharing của hộp thoại Properties của máy in, bạn thấy text cho biết tính năng chia sẻ máy in phải được mở, bạn phải cài đặt và kích hoạt File and Printer Sharing for Microsoft Networks. Cách dễ nhất để bảo đảm dịch vụ này có sẵn là chạy Network Setup Wizard được mô tả trong mục 38.

---

4. Chia sẻ máy in và cung cấp tên Share.

   Trên tab Sharing trong hộp thoại Properties của máy in, nhấp nút tùy chọn Share this printer. Tên share là một dạng rút gọn tên thật sự của máy in (chẳng hạn như Deskjet 950C), tên này được tự động đặt trong hộp text Share name. Bạn có thể giữ lại tên tự động hoặc tên riêng của bạn. Vấn đề tên share của bạn là để người dùng trên mạng có thể biết máy in nào mà họ đang kết nối khi họ nối kết từ xa với máy in. Do đó, hãy làm cho tên share càng có tính mô tả càng tốt. Tên share không nên dài hơn 31 ký tự (một chiều dài tối đa mà Microsoft được đề nghị). Mặc dù các khoảng trống được cho phép trong tên, nhưng bạn nên sử dụng các khoảng trống đặc biệt nếu một máy tính trong workgroup chạy một hệ điều hành trước Windows XP (chẳng hạn như Windows XP hoặc Windows Me hoặc Windows 98). Những hệ điều hành này không cho phép các tên share (chẳng hạn như các tên cho các máy in chia sẻ) có các khoảng trống hoặc có hơn 12 ký tự.

Sau khi bạn đã gõ nhập tên shared cho máy in, nhấp OK. Bạn quay trở về cửa sổ Printers and Faxes. Bây giờ biểu tượng của máy in có một bàn tay khum lại, cho thấy máy in được chia sẻ trên mạng (workgroup).

47. Chia sẻ một Folder

Trước khi bạn bắt đầu

45. Bàn về việc chia sẻ các tài nguyên mạng

Bạn có thể chia sẻ một folder hoặc một ổ đĩa với những người dùng khác trên mạng. Chia sẻ một đối tượng chứa chẳng hạn như một folder hoặc ổ đĩa

cho phép những người dùng truy cập bất kỳ file trên ổ đĩa đó hoặc trong folder đó. Thường không nên chia sẻ toàn bộ một ổ đĩa bởi vì chúng ta thường có nội dung mà chúng ta muốn truy cập độc quyền. Việc đặt các file riêng biệt trên folder Shared Documents (vốn được chia sẻ tự động trên mạng) hoặc chia sẻ các folder riêng lẻ thì sẽ hợp lý hơn. Giới hạn các file và folder chia sẻ theo cách này sẽ cho bạn thêm khả năng kiểm soát các file vốn thật sự có thể được truy cập bởi những người dùng workgroup.

Đối với sự an ninh cho file và những folder mà bạn chọn chia sẻ, Windows XP Home Edition cho phép bạn ấn định việc truy cập đến các file trong một ổ đĩa hoặc folder chia sẻ là chỉ đọc (read-only). Việc gán sẽ truy cập chỉ đọc vào các file và folder chia sẻ có nghĩa rằng một người dùng trên mạng có thể truy cập, đọc những file này, nhưng họ không thể thực hiện các thay đổi đối với các file và lưu trực tiếp các thay đổi sang ổ đĩa hoặc folder mà bạn đã chia sẻ. Tuy nhiên, họ có thể sao chép file sang máy tính của mình và sau đó biên tập hoặc chia sẻ file khi cần thiết kể cả đổi tên file.

Thuật ngữ chính

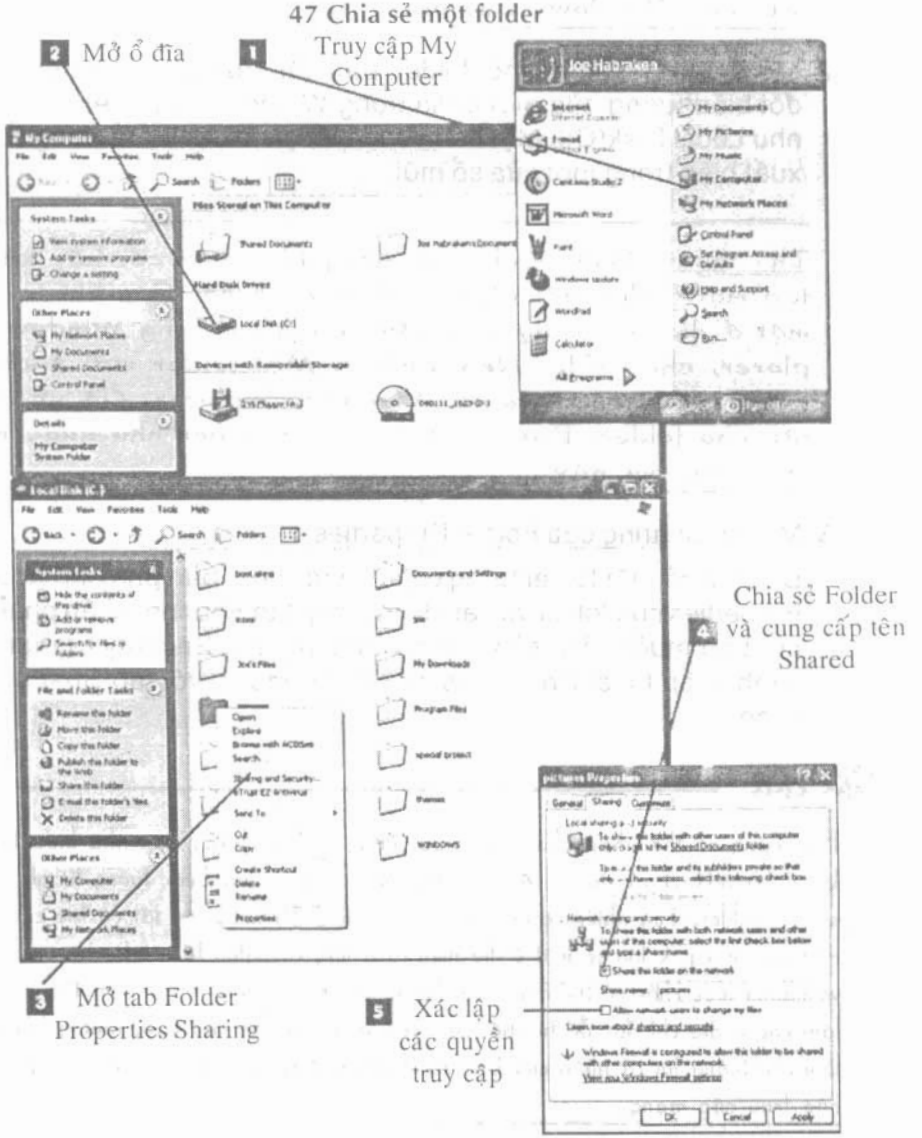
Truy cập chỉ đọc (read-only). Một file hoặc folder có thể truy cập, được mở và được đọc nhưng không thể được thay đổi và được lưu trực tiếp sang ổ đĩa hoặc folder nguồn. Tuy nhiên các file và folder như vậy có thể được sao chép và sau đó được biên tập hay thay đổi.

Chia sẻ các tài nguyên folder và file cho một workgroup đòi hỏi các người dùng trên mạng "chơi đẹp". Bởi vì không có nhà quản trị nào kiểm soát sự truy cập đến các tài nguyên mạng, mọi người phải hành xử theo một cách nhằm làm cho việc chia sẻ các ổ đĩa, folder và file trở thành một ưu thế cho tất cả người dùng mạng thay vì là một cơn ác mộng của các file bị xóa vô ý, các share bị mất và những sự cố tài nguyên khác.

Đối với phương tiện (media) tháo rời được và các ổ đĩa USB "di động", bạn có thể chia sẻ các ổ đĩa CD/DVD và các ổ đĩa USB tháo rời được. Tuy nhiên, nếu một người dùng tháo một ổ đĩa USB ra khỏi máy tính, nó không còn có sẵn trên mạng nữa. Đối với việc chia sẻ các ổ đĩa CD/DVD, bạn có thể truy cập các folder (và các file được chứa) cho bất kỳ CD hoặc DVD vốn được đặt trong ổ đĩa chia sẻ. Kỹ thuật này được sử dụng khi cần cài đặt phần mềm cho nhiều máy tính. CD cài đặt có thể nằm trên ổ đĩa CD chia sẻ và sau đó chương trình cài đặt có thể được truy cập từ bất kỳ máy tính trong workgroup. Tuy nhiên, hãy lưu ý rằng cài đặt phần mềm trên mạng chậm hơn cài đặt trực tiếp thật sự phần mềm trên máy tính sử dụng ổ đĩa CD/DVD riêng của nó.

Thủ thuật: Mặc dù bạn có thể chia sẻ các folder vốn chứa các file thực thi cho một ứng dụng, nhưng bạn không thể chạy ứng dụng trên mạng. Các ứng dụng được thiết kế để cài đặt và sau đó chạy từ cùng một máy tính, do đó

mặc dù bạn có thể truy cập file thực thi cho một ứng dụng trong một folder chia sẻ nhưng máy tính của bạn không được cấu hình để thật sự chạy ứng dụng (và do đó ứng dụng không chạy). Bởi vì user license (bản quyền người dùng) cho hầu hết các máy tính từ chối việc sử dụng đồng thời một ứng dụng, bạn không nên cố bắt đầu chạy nhiều instance của một gói phần mềm người dùng. Có các phiên bản "network" của các ứng dụng phần mềm, nhưng những phiên bản này được thiết kế để chạy trên một mạng vốn cung cấp các server cụ thể chia sẻ những ứng dụng với những máy tính người dùng cuối trên mạng.



1. Truy cập My Computer

   Nhấp nút Start và sau đó chọn My Computer từ menu Start (bạn cũng có thể nhấp đôi biểu tượng My Computer trên desktop nếu nó hiện diện). Windows Explorer mở ra, hiển thị tất cả ổ đĩa của máy tính.

Thủ thuật: Nếu bạn không có biểu tượng My Computer trên desktop Windows XP, nhấp nút Start và sau đó nhấp phải biểu tượng My Computer trong menu Start. Chọn Show on Desktop từ menu ngữ cảnh vừa xuất hiện. Bây giờ biểu tượng trên desktop vừa xuất hiện và có thể sử dụng để truy cập Windows Explorer.

---

2. Mở ổ đĩa để chia sẻ một folder, bạn cần truy cập folder này. Nhấp đôi biểu tượng của một ổ đĩa trong Windows Explorer, chẳng hạn như Local Disk(C:). Một danh sách tất cả folder chứa trong ổ đĩa đó xuất hiện trong một cửa sổ mới.

Thủ thuật: Thay vì chia sẻ một folder hiện có, hãy xem xét tạo một folder mới và sau đó chia sẻ nó. Sau khi truy cập một ổ đĩa trên máy tính bằng cách sử dụng Windows Explorer, chọn File, New Folder. Một folder mới xuất hiện cho ổ đĩa trong cửa sổ Windows Explorer. Gõ nhập một tên cho folder. Bạn có thể chia sẻ folder như được mô tả trong tác vụ này.

---

3. Mở tab Sharing của Folder Properties

   Để chia sẻ một folder trong ổ đĩa được chọn, bạn phải mở hộp thoại Properties của folder và sau đó truy cập tab Sharing: nhấp phải folder mà bạn muốn chia sẻ và chọn Sharing and Security từ menu ngữ cảnh. Hộp thoại Properties của folder mở ra với tab Sharing được chọn.

Ghi chú

Bạn cũng có thể nhấp phải một biểu tượng ổ đĩa, chẳng hạn như biểu tượng Local Drive(C:) và chia sẻ ổ đĩa bằng cách sử dụng các bước tương tự như chia sẻ một folder. Tuy nhiên, chia sẻ toàn bộ một ổ đĩa mở rộng tất cả file của bạn ra trước mạng. Chia sẻ một ổ đĩa theo cách này có nghĩa tất cả tài liệu của bạn và những mục khác có thể được xem bởi những người khác trên mạng. Bạn có thể làm cho ổ đĩa chỉ đọc để từ chối việc xóa vô ý các file của bạn, nhưng bạn vẫn làm cho thông tin cá nhân của bạn trở thành một cuốn sách mở cho bất kỳ người nào truy cập mạng.

4. Chia sẻ Folder và cung cấp tên Share

   Trên tab Sharing, nhấp hộp kiểm Share this folder on the network. Một tên share mặc định xuất hiện trong hộp text Share name (tên mặc định dựa vào tên folder). Nếu bạn muốn thay đổi tên share, chọn text mặc định và gõ nhập một tên mới. Nếu tất cả máy tính trong workgroup chạy Windows XP, bạn có thể sử dụng 31 ký tự (kể cả các khoảng trống) cho tên share. Nếu các máy tính workgroup chạy hỗn hợp các hệ điều hành (chẳng hạn như Windows XP và Windows 98), sử dụng tối đa 12 ký tự cho tên share và không sử dụng các khoảng trống.

5. Xác lập các quyền truy cập

   Nếu bạn muốn cho phép những người dùng mạng thay đổi (nghĩa là biên tập, xóa,...) các file trong folder chia sẻ, nhấp hộp kiểm Allow network users to change my files. Nếu bạn muốn các file trong folder chia sẻ (cũng như chính folder) có sự truy cập chỉ đọc (read-only), hủy chọn hộp kiểm Allow network users to change my files.

Khi bạn sẵn sàng hoàn tất tiến trình chia sẻ folder, nhấp OK. Hộp thoại Properties đóng lại và bạn quay trở về cửa sổ Windows Explorer. Bây giờ folder được đánh dấu bằng một biểu tượng chia sẻ (một bàn tay ôm giữ folder). Folder và nội dung của nó có thể được truy cập bởi những người dùng khác trong workgroup. **Xem mục 48** để biết thông tin về việc truy cập các file và folder chia sẻ trên mạng.

48. Bàn về việc truy cập các tài nguyên mạng

Trước khi bạn bắt đầu

3. Duyệt tìm các file và folder

4. Bàn về My Network Places

44. Xem tư cách thành viên Workgroup và truy cập Network Neighborhood.

45. Bàn về việc chia sẻ các tài nguyên mạng

Sau khi các tài nguyên mạng (chẳng hạn như các máy in và folder) đã được chia sẻ, bạn và những thành viên workgroup khác có thể truy cập những tài nguyên này. Truy cập bất kỳ tài nguyên workgroup có sẵn bằng cách mở My Network Places. Cửa sổ My Network Places hiển thị các share (folder) đang có sẵn cho workgroup. Nó cũng nhận dạng host của mỗi share qua tên máy tính. Các thành viên workgroup có thể truy cập các máy in được chia sẻ bởi một máy tính workgroup cụ thể bằng cách mở cửa sổ My Network Places và chọn link View workgroup computers. Từ cửa sổ này, bạn có thể xem các tài nguyên được chia sẻ bởi một máy tính cụ thể kể cả các máy in.

Nếu bạn không thấy một share cụ thể mà bạn hy vọng truy cập, điều này có nghĩa máy host hiện được tắt và không có sẵn. Trong một số trường hợp, máy host có thể được mở nhưng share không xuất hiện trong cửa sổ My

Network Places bởi vì sự hiện diện của máy host trên mạng đã không tiếp cận được máy tính của bạn. Các máy tính "quảng cáo" sự hiện diện của chúng trên mạng và cũng quảng cáo share mà chúng cung cấp. Một máy tính đã được mở, nó có thể không xuất hiện trong cửa sổ My Network Places bởi vì "quảng cáo' đã chưa tiếp cận được máy tính của bạn. Trong những trường hợp, bạn không thấy một tài nguyên mà bạn biết có ở đó, bạn có thể tìm kiếm nhanh máy tính này bằng cách sử dụng tính năng Windows Search (có sẵn trong menu Start). Nếu bạn vẫn không thể định vị và truy cập các share của máy tính kia, có thể bạn đang gặp phải một sự cố kết nối. Để biết thông tin về việc giải quyết các sự cố kết nối mạng, **xem mục 91**.

Để làm việc với các share máy in, vấn đề truy cập máy in chia sẻ từ xa là in. Do đó bạn kết nối với máy in một lần (và chỉ một lần), điều này làm cho máy in có sẵn đối với bạn (và máy tính của bạn), như thể máy in được nối kết trực tiếp với máy tính của bạn. Máy in thật sự được thêm vào danh sách Printer trên máy tính. Một khi máy in từ xa được "cài đặt" trên máy tính của bạn (nghĩa là khi bạn đã nối kết với nó qua "như được giải thích trong **mục 51**), máy in xuất hiện trong cửa sổ Printer and Faxes (được truy cập từ Control Panel) như bất kỳ máy in cục bộ được nối kết trực tiếp. Sau khi bạn đã thiết lập nối kết ban đầu (thông qua My Network Places), máy in có sẵn cho bạn từ thời điểm đó trở đi hoặc cho đến khi bạn xóa máy in ra khỏi xác lập máy in. Khuyết điểm duy nhất của việc in máy in trên một máy in từ xa là máy tính chia sẻ máy in phải được mở và máy in phải được mở và máy in phải mở để bạn in trên mạng.

Các folder chia sẻ như đã được đề cập có thể được truy cập từ cửa sổ My Network Places. Bạn có thể xúc tiến việc truy cập các folder chia sẻ bằng cách ánh xạ một folder chia sẻ dưới dạng một ổ đĩa mạng (như được thảo luận trong mục 50). Bạn cũng có thể tạo một vị trí mạng (network places) cho các folder chia sẻ từ xa như được thảo luận trong **mục 53**.

49. Truy cập các Folder chia sẻ và mở các File chia sẻ

Trước khi bạn bắt đầu

4. Bàn về My Network Places

44. Xác nhận tư cách thành viên Workgroup và truy cập Network Neighborhood.

48. Bàn về việc truy cập các tài nguyên mạng

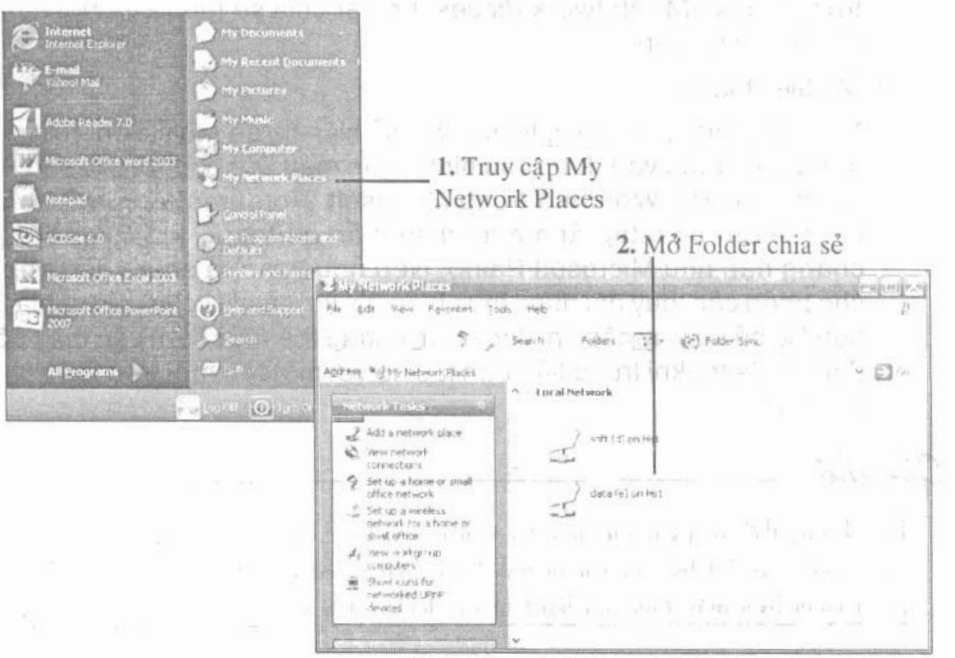
Các folder chia sẻ có thể được truy cập nhanh từ cửa sổ My Network Places. Biểu tượng My Network Places có sẵn trên menu Start, nhấp nó để mở cửa sổ My Network Places (tương tự như cửa sổ My Computer; cả hai đều được mở bằng cách sử dụng ứng dụng Windows Explorer vốn được sử dụng để duyệt nội dung của máy tính hoặc mạng). Nếu bạn muốn đặt My Network Places trên desktop Windows XP, nhấp phải biểu tượng My Network Places trên menu Start và chọn Show on Desktop từ menu ngữ cảnh vừa xuất hiện.

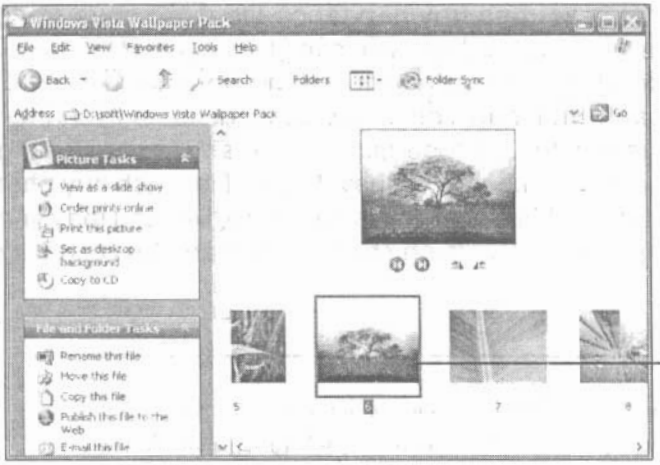
Sau khi mở một folder chia sẻ, bạn truy cập tất cả file được chứa trong folder đó. Bạn có thể chỉnh sửa, xóa và di chuyển các file trong một folder chỉ khi người dùng chia sẻ folder đã cho phép các người dùng workgroup thay đổi các file trong share bằng cách chọn hộp kiểm Allow network users to change my file trên tab Sharing của hộp thoại Properties của folder. Hãy lưu ý rằng nếu các file đã được chia sẻ để bạn không thể thay đổi các file, cách duy nhất mà bạn có thể chỉnh sửa một file chia sẻ chỉ đọc là sao chép file sang máy tính của bạn nơi mà sau đó bạn có thể xử lý file như bạn thường làm đối với bất kỳ file khác trên máy tính.

Ghi chú

Mặc dù bạn có thể truy cập các file trong một folder chia sẻ, nhưng bạn không thể thay đổi bất kỳ xác lập chia sẻ liên quan đến folder chia sẻ. Ví dụ, nếu người dùng đã chia sẻ folder không chọn hộp kiểm Allow network users to change my files khi share được tạo, không có cách nào để thay đổi thuộc tính share này. Chỉ người dùng trên máy tính tạo share mới thay đổi được các thuộc tính share. Điều này cũng có nghĩa rằng người đã tạo share là người duy nhất có thể "tắt" tính năng chia sẻ trên một folder chia sẻ cụ thể. Bởi vì việc chia sẻ các folder trong một workgroup được phân quyền (nghĩa là mỗi máy tính và người dùng của máy tính đó điều khiển các tài nguyên mà nó chia sẻ) và bởi vì các workgroup không có các server hoặc các nhà quản trị mạng, không có cách nào để ghi đè những preferences (lựa chọn theo sở thích) chia sẻ được gởi trên một máy tính riêng lẻ hoặc host trên workgroup.

49. Truy cập các folder chia sẻ và mở các file chia sẻ





1. Truy cập My Network Places

   Nhấp nút Start và sau đó chọn My Network Places. Điều này mở ra cửa sổ My Network Places. Các share có sẵn trên các máy tính workgroup sẽ xuất hiện trong cửa sổ. Bạn có thể biết cái nào là các biểu tượng cho các share từ xa (các share không nằm trên máy tính) bằng việc chúng có một "T" mạng nhỏ. (một chữ T ngược biểu thị một tài nguyên mạng, ở đáy biểu tượng. Các share mà bạn đã chia sẻ trên máy tính xuất hiện dưới dạng các folder bình thường trong cửa sổ My Network Places.

2. Mở Folder chia sẻ

   Để mở một share (folder) cụ thể, nhấp đôi biểu tượng cho folder đó trong cửa sổ My Network Places. Folder chia sẻ mở ra và nội dung của folder hiển thị.

3. Mở file chia sẻ.

   Nhấp đôi bất kỳ file trong folder chia sẻ hiển thị để mở file đó. File mở trong ứng dụng vốn được cấu hình trong máy tính cho kiểu file đó. Ví dụ một tài liệu Word mở trong Microsoft Word; một ảnh mở trong phần mềm biên tập ảnh mặc định (vốn có thể là một ứng dụng, chẳng hạn như Microsoft Paint). Nếu người tạo ra share đã không cho phép các thay đổi được thực hiện đối với các file chia sẻ (nghĩa là nếu file có sự truy cập chỉ đọc), bạn không thể thực hiện các thay đổi đối với file trừ khi trước tiên bạn lưu nó với một tên mới trên máy tính của bạn.

Ghi chú

Bạn không thể chạy các file thực thi trên mạng. Bạn không thể chạy các chương trình được cài đặt trên một máy tính khác (ngoại trừ các chương trình cài đặt phần mềm trên máy tính của bạn) từ các folder chia sẻ.

50. Ánh xạ một ổ đĩa mạng

Trước khi bạn bắt đầu

44. Xác nhận tư cách thành viên Workgroup và truy cập Network Neighborhood

48. Bàn về việc truy cập các tài nguyên mạng

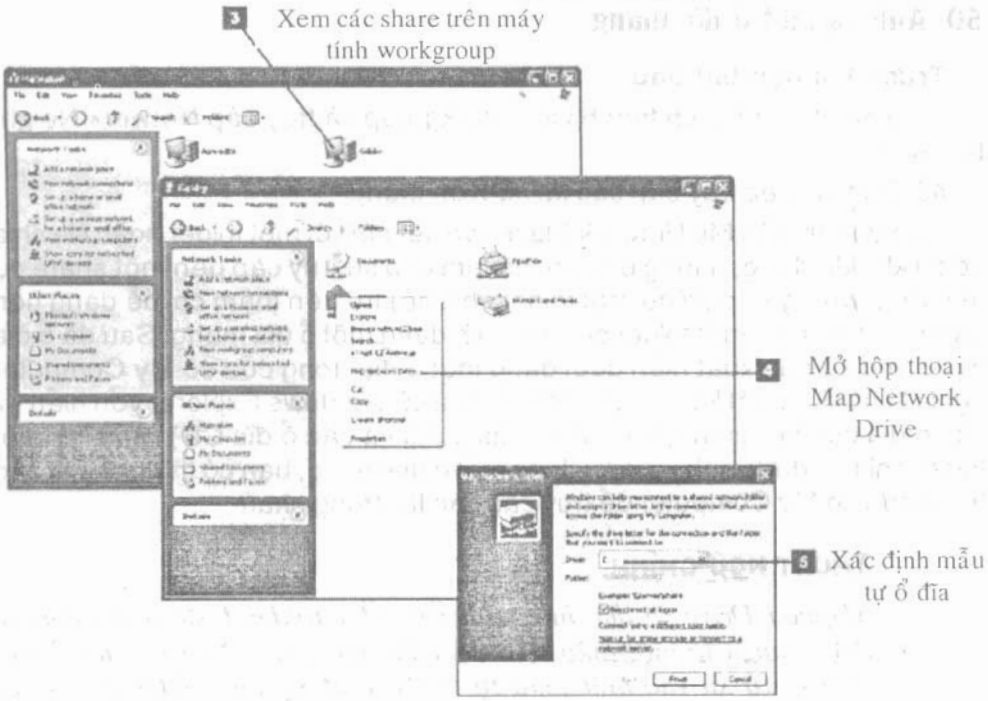
Mặc dù truy cập My Network Places và kết nối với một folder hoặc file chia sẻ thì khá dễ dàng, nhưng bạn có thể làm cho sự truy cập đến một share cụ thể trong workgroup (ví dụ một folder chia sẻ) trở nên thậm chí dễ dàng hơn bằng cách ánh xạ một folder chia sẻ dưới dạng một ổ đĩa mạng. Sau đó ổ đĩa được ánh xạ này xuất hiện dưới dạng một ổ đĩa trong cửa sổ My Computer nghĩa là nó được liệt kê trong cùng một cửa sổ Windows Explorer vốn hiển thị các ổ đĩa cục bộ (chẳng hạn như ổ đĩa cứng và các ổ đĩa CD). Sau khi một folder chia sẻ được ánh xạ dưới dạng một ổ đĩa mạng, bạn có thể nhấp đôi nó trong cửa sổ My Computer để truy cập các file trong share.

THUẬT NGỮ CHÍNH

Mapped Drive (ổ đĩa được ánh xạ). Một folder hoặc ổ đĩa chia sẻ được cung cấp một mẫu tự ổ đĩa trên máy tính. Ánh xạ một folder chia sẻ từ xa vào một mẫu tự ổ đĩa sẽ cho phép folder chia sẻ có thể truy cập từ My Computer.

50. Ánh xạ một ổ đĩa mạng





1. Mở My Network Places

   Cửa sổ My Network Places cho phép truy cập nhanh đến link View workgroup computers nhằm cho phép bạn xem tất cả máy tính đang có sẵn trong workgroup. Truy cập một máy tính cụ thể sẽ cho phép bạn xem tất cả tài nguyên chia sẻ được cung cấp bởi máy tính đó. Cửa sổ My Network Places cũng cho phép truy cập nhanh đến cửa sổ My Computer, folder Shared Documents và những vị trí khác trên máy tính bằng các link nằm ở phía bên trái cửa sổ. Để mở My Network Places, nhấp nút Start và nhấp My Network Places.

2. Mở các máy tính Workgroup

   Trong cửa sổ My Network Places, nhấp link View workgroup computers trong khung nằm ở phía bên trái cửa sổ. Có thể mất trong giây lát để tất cả máy tính workgroup xuất hiện trong cửa sổ workgroup nằm bên phải.

3. Xem các Share trên máy tính Workgroup

   Để xem các share được cung cấp bởi một máy tính workgroup hiển thị trong cửa sổ workgroup, nhấp đôi biểu tượng cho máy tính đó. Có thể mất một chút thời gian để tất cả share cho máy tính đó mở trong cửa sổ mới.

4. Mở hộp thoại Map Network Drive

   Sau khi bạn đã định vị folder chia sẻ mà bạn muốn tạo một ổ đĩa mạng, nhấp phải folder chia sẻ và nhấp Map Network Drive từ menu ngữ cảnh. Hộp thoại Map Network Drive mở ra.

5. Xác định mẫu tự ổ đĩa

Một mẫu tự ổ đĩa mặc định được cung cấp cho ổ đĩa mạng mới mà sẽ được tạo cho folder chia sẻ. Bạn có thể sử dụng mẫu tự ổ đĩa mặc định hoặc chọn một mẫu tự ổ đĩa có sẵn khác từ danh sách xổ xuống Drive. Sau khi chọn mẫu tự ổ đĩa, nhấp Finish. Ổ đĩa mạng mới mở ra, hiển thị nội dung của folder chia sẻ. Bây giờ bạn có thể truy cập ổ đĩa mạng từ danh sách ổ đĩa được tìm thấy trong cửa sổ My Computer (mở My Computer bằng cách nhấp nút Start và sau đó nhấp My Computer). Hoặc nếu muốn, bạn có thể rê biểu tượng ổ đĩa được ánh xạ từ cửa sổ My Computer lên trên desktop Windows để tạo một cửa sổ desktop shortcut đến tài nguyên từ xa đó.

51. Kết nối với một máy in chia sẻ

Trước khi bạn bắt đầu

44. Xác nhận tư cách thành viên Workgroup và truy cập Network Neighborhood

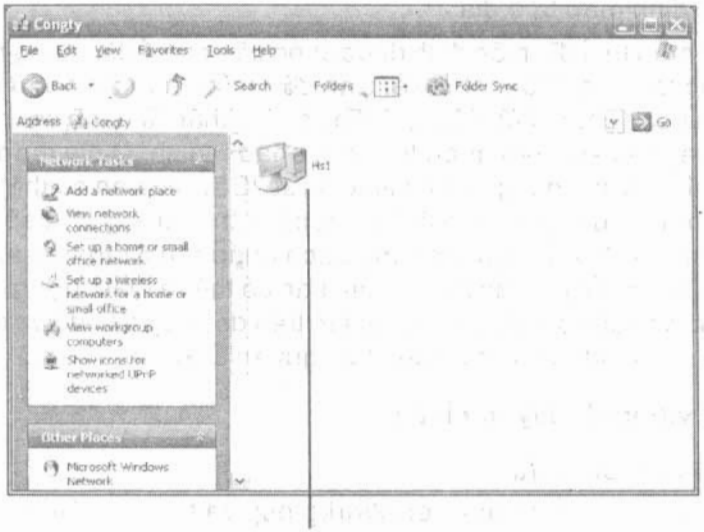
48. Bàn về việc truy cập các tài nguyên mạng

Bạn có thể tận dụng workgroup WiFi bằng cách chia sẻ các máy in trên mạng. Chia sẻ một máy in sẽ cho phép những người dùng trên mạng sử dụng một máy in, loại bỏ nhu cầu mua một máy in cho mỗi máy tính trên mạng. Sau khi người dùng trên một workgroup kết nối với một máy in chia sẻ, máy in có thể được cấu hình trên máy tính của họ và được truy cập khi cần thiết trong tương lai từ những ứng dụng trên máy tính. Mặc dù hệ thống Help của Windows XP đề nghị bạn cài đặt máy in từ xa mới bằng cách sử dụng cửa sổ Printer and Faxes (được truy cập từ Control Panel), nhưng kết nối với một máy in chia sẻ "bằng trực quan" bằng cách mở workgroup từ cửa sổ My Network Palces và truy cập các share cho một máy tính cụ thể sẽ dễ dàng hơn. Trong trường hợp này là máy tính chia sẻ máy in. Sau đó bạn có thể kết nối trực tiếp với máy in trong cửa sổ của máy tính workgroup.

51. Kết nối với máy in chia sẻ







3. Truy cập các Shares trên máy tính Workgroup

1. Mở My Network Places

   Để mở cửa sổ My Network Places, nhấp nút Start và sau đó nhấp My Network Places.

2. Truy cập các máy tính Workgroup

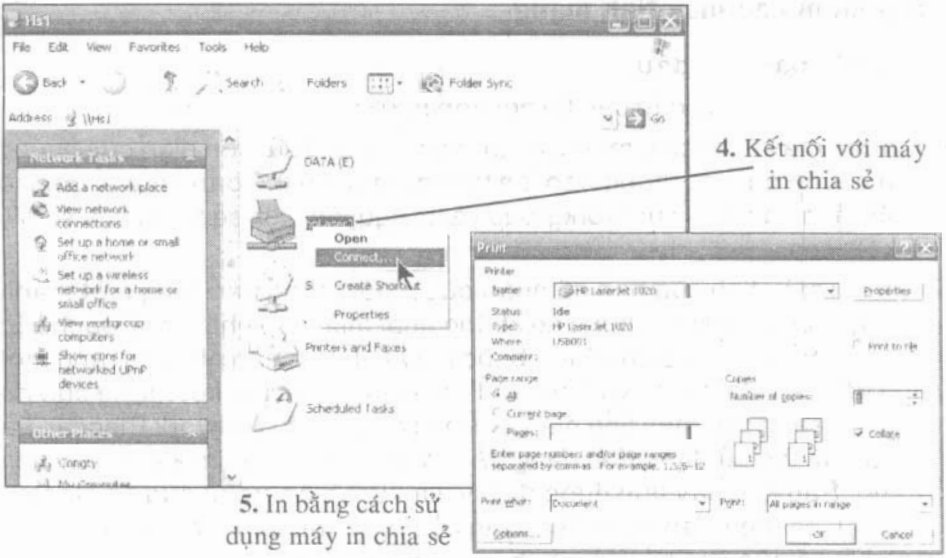
   Nhấp link View workgroup computer nằm ở phía bên trái cửa sổ My Network Places để xem tất cả máy tính trong workgroup đang kết nối với mạng.

3. Truy cập các Share trên máy tính Workgroup.

   Sau khi biểu tượng cho các máy tính workgroup xuất hiện trong cửa sổ workgroup, nhấp đôi máy tính vốn chia sẻ máy in mà bạn muốn kết nối. Các tài nguyên chia sẻ và các folder và máy in cho máy tính đó xuất hiện trong cửa sổ.

4. Kết nối với máy in chia sẻ

   Nhấp phải biểu tượng máy in chia sẻ và chọn biểu tượng connect từ menu ngữ cảnh. Một hộp thông báo xuất hiện cho bạn biết rằng một Driver máy in trên máy tính sẽ được cài đặt để bạn biết rằng bạn có thể in sang máy in chia sẻ . Driver được cài đặt và máy in được thêm vào cấu hình Printers and Faxes mà bạn có thể truy cập từ Control Panel



5. In bằng cách sử dụng máy in chia sẻ

Bạn có thể in sang máy in từ bất kỳ ứng dụng nào trên máy tính của bạn. Nếu đây là máy in duy nhất được cấu hình trong máy tính của bạn, nó sẽ được ấn định trong máy tính của bạn và tất cả ứng dụng sẽ in sang máy in bằng mặc định. Nếu bạn có một máy in cục bộ khác được cài đặt trên máy tính, bạn có thể in sang nó hoặc máy in workgroup (được cài đặt) mới kết nối. Từ hầu hết các ứng dụng, chọn File, Print để mở hộp thoại riêng. Từ hộp danh sách sổ xuống Printer Name ở phần trên cùng của hộp thoại, chọn máy in mà bạn muốn sử dụng (cho dù là máy in cục bộ hay máy in chia sẻ từ xa) và nhấn OK để in. Nếu muốn bạn có thể chọn máy in chia sẻ là máy in mặc định trong cửa sổ Printers and Faxes.

Chú ý

Trong một số trường hợp, Driver máy in sẽ không được download một cách tự động xuống máy tính từ máy tính vốn cung cấp máy in chia sẻ. Một thông báo có thể sẽ xuất hiện, giải thích rằng driver không được sao chép và yêu cầu vị trí của CD hoặc media khác vốn chứa Driver phần mềm cho máy in. Nếu điều này xảy ra, bạn sẽ cần cài đặt driver cho máy tính của bạn bằng cách sử dụng CD hoặc đĩa mềm gốc đi kèm với máy in. Sau khi bạn đã cài đặt driver, bạn có thể in sang máy in từ xa. Để test máy in, nhấp phải biểu tượng máy in trong cửa sổ Printers and Faxes (mở cửa sổ từ Control Panel) và chọn Properties từ menu ngữ cảnh. Trên tab General của hộp thoại Properties, nhấp nút Print Test Page. Một trang test sẽ in trên máy in. Nếu bạn không nhận được một bản in, hãy chắc chắn rằng máy in online và đã kết nối với máy tính chia sẻ máy in. Nếu bạn vẫn gặp trục trặc khi in, xóa máy in ra khỏi cửa sổ Printers and Faxes và làm theo các bước trong tác vụ này để kết nối lại với máy in.

52. Tìm kiếm các máy tính mạng

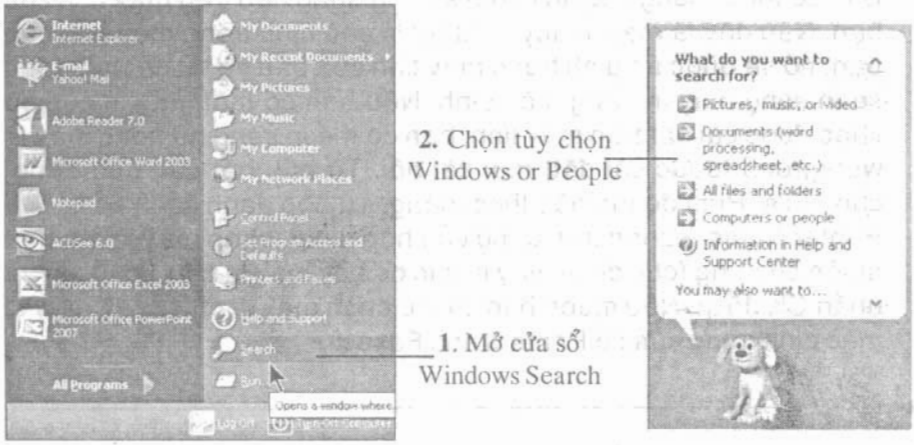
Trước khi bạn bắt đầu

48. Bàn về việc truy cập các tài nguyên mạng

Bởi vì các máy tính trong một workgroup thông báo sự hiện diện của chúng (nghĩa là chúng gửi các thông báo lên trên mạng), có thể bạn không luôn có một danh sách các máy tính workgroup và tài nguyên chia sẻ trong cửa sổ My Network Places.

Thậm chí máy tính của bạn đã nhận được một thông báo rằng một thành viên workgroup đã online, nhưng nó không nhất thiết cập nhật danh sách các máy tính kết nối của nó. Bạn có thể buộc máy tính của bạn nhận ra rằng một máy tính gần đây đã online và cập nhật danh sách các nối kết mạng của nó (vốn là danh sách các máy tính hiển thị trong cửa sổ My Network Places), và sau đó bạn có thể sử dụng tính năng Windows Search để tìm kiếm máy tính trên mạng. Sau khi máy tính được định vị và xuất hiện trong cửa sổ Search Results, bạn có thể nhấp đôi biểu tượng của máy tính để xem các nguồn tài nguyên chia sẻ của nó chẳng hạn như các folder và máy in.

52. Tìm kiếm các máy tính mạng



1. Mở cửa sổ Windows Search

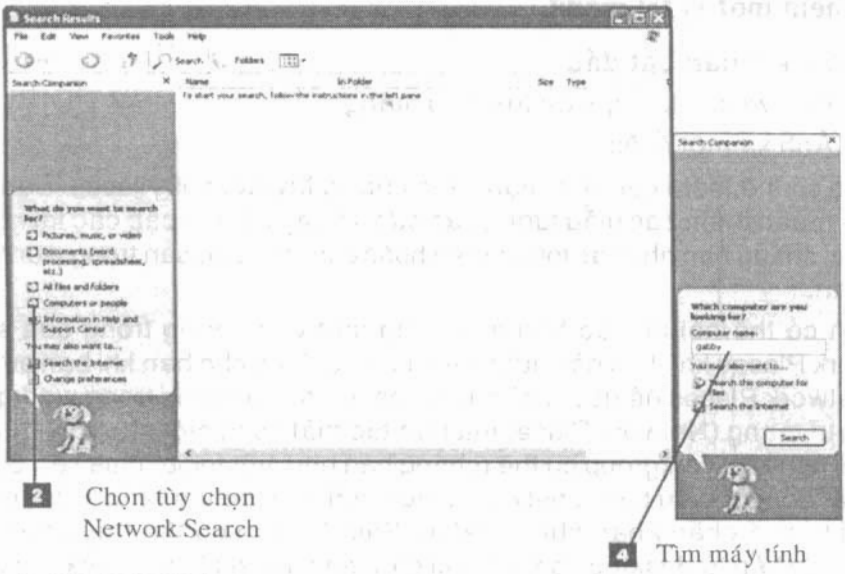
   Nhấp nút Start và sau đó nhấp biểu tượng Search trên menu Start. Cửa sổ Search Result mở.

2. Chọn tùy chọn Windows or People

   Để tìm kiếm các máy tính trong workgroup, chọn link Computers or people trong khung Search Companion nằm phía bên trái của cửa sổ Search Results.

3. Chọn tùy chọn Network Search

   Để tìm kiếm một máy tính trong workgroup, chọn link A Computer on the network trên khung Search Companion của cửa sổ Search Results.



4. Tìm máy tính

   Gõ nhập tên của máy tính mà bạn tìm trong hộp text Computer name và nhấp nút Search. Tên và biểu tượng của máy tính sẽ xuất hiện ở khung bên phải của cửa sổ Search Results nếu máy tính thật sự mở và kết nối với workgroup. Để truy cập các share trên máy tính này (các folder chia sẻ và máy in của nó) nhấp đôi biểu tượng của máy tính.

Ghi chú

Nếu máy tính mà bạn đang tìm không xuất hiện trong danh sách Search Results, có hai điều mà bạn có thể làm. Đầu tiên bạn hãy chắc chắc gõ đúng tên của máy tính trong hộp text Computer name. Nếu bạn chỉ nhớ một phần tên của máy tính bạn có thể sử dụng phần này trong hộp Search. Nếu bạn biết vài mẫu tự đầu tiên của tên, gõ nhập các ký tự đó. Nếu bạn nhớ phần cuối của tên, gõ nhập một dấu * và sao đó gõ phần còn lại của tên. Dấu sao được sử dụng làm ký tự đại diện (wildcard) cho bất kỳ ký tự nào xuất hiện trước các ký tự được cung cấp. Một dấu sao có thể được sử dụng làm ký tự đại diện ở đầu hoặc cuối một tên máy tính để tượng trưng cho bất kỳ số ký tự. Nếu bạn cần một ký tự đại diện tượng trưng cho một ký tự đơn, sử dụng dấu hỏi (?). Ví dụ, nếu bạn không thể nhớ tên của máy tính là bill hay bull, hãy sử dụng từ tìm kiếm b?ll. Cũng phải bảo đảm rằng máy tính thật sự mở và được kết nối với mạng. Nếu bạn vẫn không thể thấy máy tính hãy kiểm tra xem máy tính đó có thật sự là một thành viên của workgroup hay không (sử dụng hộp thoại System Properties trên máy tính đó để kiểm tra chi nhánh workgroup của nó, nhấp phải biểu tượng My computer để mở hộp thoại System Properties) Nếu tất cả xác lập dường như đúng mà bạn vẫn không thể thấy máy tính trên mạng, hãy xem chương 13.

53. Thêm một vị trí mạng

Trước khi bạn bắt đầu

48. Bàn về các tài nguyên truy cập mạng

50. Ánh xạ một ổ đĩa

Bạn có thể thêm các vị trí mạng vào cửa sổ My Netwok Places. Bạn cũng có thể muốn thêm các biểu tượng vào cửa sổ này để truy cập các tài nguyên Internet chẳng hạn như các folder Web hoặc các share có sẵn trong workgroup của bạn.

Bạn có thể hỏi tại sao bạn muốn tao một vị trí mạng trong cửa sổ My Network Places khi điều này được thực hiện tự động cho bạn khi bạn sử dụng My Network Places để duyệt các máy tính đang hoạt động trong workgroup. Một vị trí mạng (Network Place) mà bạn tạo thật sự là một shortcut dẫn đến một tài nguyên workgroup cụ thể (chẳng hạn như một folder chia sẻ). Sau khi bạn đã tạo một biểu tượng network place mới, bạn có thể rê biểu tượng đến một vị trí mới chẳng hạn như desktop. Sau đó, bạn có thể truy cập nhanh share trực tiếp từ desktop, loại bỏ nhu cầu mở cửa sổ My Network Places.

Một network place tương tự như một ổ đĩa được ánh xạ, trong đó bạn tạo một pointer dẫn sang một tài nguyên riêng biệt tại một vị trí riêng biệt trên mạng. Network Places mà bạn tạo xuất hiện trong cửa sổ My Network Places và có thể được rê lên desktop Windows dưới dạng các shortcut. Các ổ đĩa được ánh xạ xuất hiện trong cửa sổ My Computer và cũng có thể được rê lên desktop dưới dạng các shortcut. Việc bạn sử dụng Network Places hoặc các ổ đĩa được ánh xạ đều tùy thuộc vào bạn. Tuy nhiên, bạn chỉ có sẵn 26 mẫu tự ổ đĩa (các mẫu tự của bảng chữ cái). Nếu bạn muốn tạo nhiều shortcut dẫn đến các folder chia sẻ, xem xét sử dụng network places vốn không đòi hỏi một mẫu tự ổ đĩa nào.

1. Mở Add a Network Place Wizard

   Mở cửa sổ My Network Places bằng cách nhấp Sart và sau đó nhấp My Network Places. Nhấp link Add a network place trong khung Network Tasks nằm phía bên trái của cửa sổ Add a network Place Wizard mở ra. Nhấp Next để bỏ qua màn hình wizard ban đầu.

2. Chọn vị trí

   Nhấp biểu tượng Choose another network location trên cửa sổ wizard. Tùy chọn này cho phép bạn tạo các vị trí mạng cho ổ đĩa và folders chia sẻ trong workgroup. Nó cũng có thể cho phép bạn tạo các vị trí mạng cho các servers mà bạn có thể truy cập trên Internet chẳng hạn như các site FTP (File Transfer Protocol) và các website vốn cung cấp các bản download file. Những shares từ xa (trên Internet) này được xem như các share mà bạn có thể truy cập từ mạng cục bộ. Sau khi nhấp biểu tượng, nhấp Next.

53. Thêm một vị trí mạng



3. Duyệt tìm vị trí

   Như đã đề cập, một vị trí mạng có thể là một website Internet hoặc site FTP. Trong trường hợp của một website, bạn nhập tên của một website chẳng hạn như HTTP://website/share. Đối với một site FTP, tên chia sẻ tương tự như FTP://ftpsite.com. Bạn không thể duyệt tìm các website hoặc các share site FTP; bạn phải nhập chính xác URL của chúng, tuy nhiên bạn có thể duyệt tìm một share workgroup cục bộ. Nhấp nút Browse để duyệt tìm một share mà bạn muốn sử dụng cho vị trí mạng mới. Cửa sổ Browse for Folder mở ra. Bạn sẽ duyệt mạng cục bộ (workgroup) để tìm folder hoặc ổ đĩa chia sẻ mà bạn muốn chỉ định là một vị trí mạng.

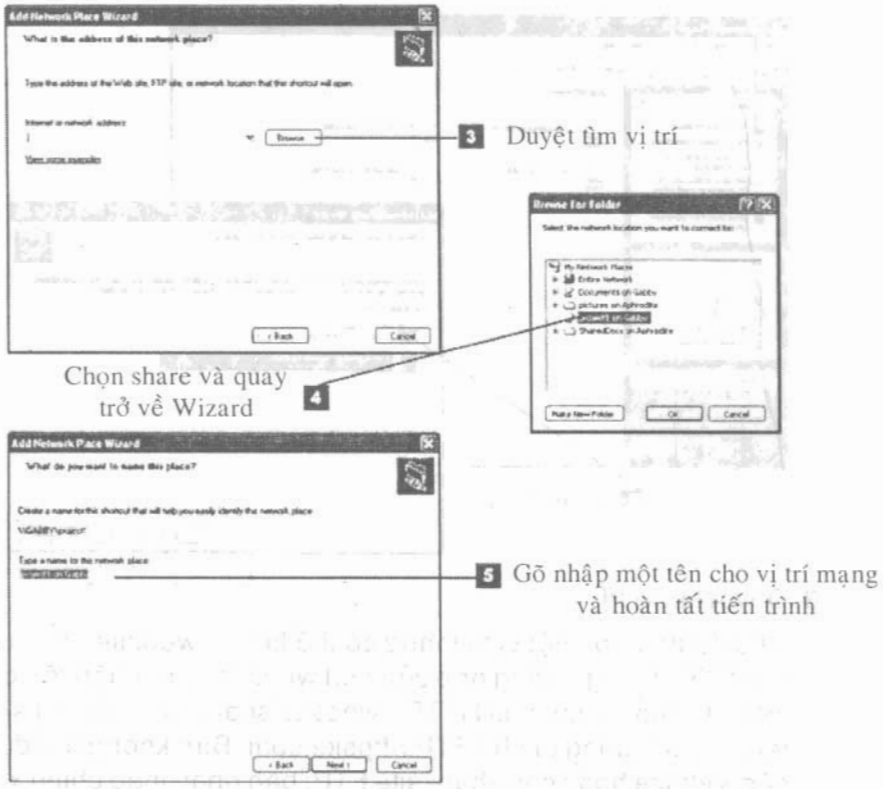
4. Chỉ định Share và quay về Wizard

   Nhấp một share workgroup vốn xuất hiện trong cửa sổ Browse for Folder để chỉ định share mà bạn muốn tạo vị trí mạng. Kế đó nhấp OK. Bạn quay trở về wizard và tên share mà bạn đã chọn xuất hiện trong hộp text Internet or network address. Nhấp Next để tiếp tục.

5. Nhập một tên cho vị trí mạng và hoàn tất tiến trình.

   Màn hình Wizard kế tiếp đề nghị bạn gõ một tên cho vị trí mạng mới. Một tên mặc định được tạo dựa vào tên của máy tính và tên của một share (hoặc tên của share trong trường hợp của một website hoặc một site FTP) nhưng bạn có thể gõ nhập một tên khác trong hộp text Type a name for the network place. Nhấp Next để di chuyển đến màn hình Wizard cuối cùng, sau đó nhấp Finish. Biểu tượng vị trí mạng mới xuất hiện trong cửa sổ My Network Places và share kết

hợp mở trong một cửa sổ mới. Đóng cửa sổ vốn hiển thị nội dung của share.



Để đặt biểu tượng vị trí mạng mới trên desktop dưới dạng một shortcut đến share, rê biểu tượng từ cửa sổ My Network Places đến desktop. Sau đó bạn có thể đóng cửa sổ My Network Places. Bây giờ bạn có thể truy cập trực tiếp share từ desktop Windows bằng cách nhấp đôi biểu tượng của share.

Chương 8

LỌC NỘI DUNG VÀ MỞ CÁC DỊCH VỤ GAME

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *54. Bàn về việc lọc nội dung và mở các cổng*
- *55. Ngăn chặn truy cập đến các website*
- *56. Ngăn chặn truy cập đến các dịch vụ Internet*
- *57. Thiết lập một thời biểu lọc*
- *58. Cấu hình Port Forward và Port Triggering*

Bạn sẽ thấy router WiFi có một số tính năng cho phép kiểm soát nội dung Internet có sẵn cho những người dùng mạng WiFi. Việc kiểm soát này bao gồm ngăn chặn (block) các site Internet cụ thể cũng như sự truy cập đến các dịch vụ Internet như gửi thông điệp tức thì (instant messaging). Dù việc ngăn chặn sự truy cập Internet và lọc nội dung tùy thuộc vào bạn đối với mạng gia đình, nhưng router wifi cũng có thể được cấu hình để những người dùng trên mạng có thể tận dụng việc chơi game online mà không gây ra sự cố an ninh lớn cho mạng gia đình. Chương này xem xét việc truy cập vào các dịch vụ trong khi vẫn cho phép truy cập các dịch vụ đặc biệt chẳng hạn như các tùy chọn chơi game thông qua port forwarding.

54. Bàn về việc lọc nội dung và mở các cổng

Trước khi bạn bắt đầu	Xem thêm
21. Bàn về việc cấu hình Router không dây	**Mục 71**
22. Truy cập cấu hình Router	**Mục 70**
37. Bàn về việc cấu hình các PC để nối mạng	

Vì Router WiFi nằm giữa mạng gia đình hoặc workgroup và nối kết Internet tốc độ cao nên router được cấu hình để kiểm soát việc truy cập nội dung web. Điều này có nghĩa nội dung nhất định có thể được ngăn chặn tại Router, từ chối truy cập đến một máy tính cụ thể trong workgroup hoặc từ chối sự truy cập đó đến tất cả máy tính trong workgroup. Hầu hết các router WiFi cũng có thể được cấu hình để từ chối truy cập đến các dịch vụ Internet chẳng hạn như truyền file, chơi game và gửi thông báo tức thì.

Ghi chú

Khả năng ngăn chặn nội dung web và các dịch vụ Internet chẳng hạn như email hoặc gửi thông báo tức thì cung cấp cho bạn hai cách để kiểm soát sự truy cập mà những người dùng của bạn có theo những đường truyền Internet khác nhau (chẳng hạn như Web). Khi bạn ngăn chặn nội dung web, nội dung được ngăn chặn cho tất cả máy tính trên mạng WiFi của bạn. Tuy nhiên bạn có thể nhập địa chỉ IP của một máy tính (được biết là máy tính "đáng tin cậy") trong cấu hình ngăn chặn nội dung web của router, điều này sẽ cho phép máy tính đó vẫn truy cập nội dung. Khi bạn từ chối hoặc ngăn chặn các dịch vụ (service) trên mạng, bạn có thể chỉ định một hoặc một số máy tính được miễn bị ngăn chặn một dịch vụ hay các dịch vụ. Do đó để cho phép các ngoại lệ (exceptions), bạn sẽ có thêm sự linh hoạt khi bạn ngăn chặn các dịch vụ thay vì nội dung web.

Bạn không những có thể ngăn chặn sự truy cập đến nội dung web và các dịch vụ Internet mà bạn có thể thiết kế một thời biểu nhằm ấn định khi nào nội dung hoặc các dịch vụ thật sự được ngăn chặn. Tóm lại các tính năng lọc web và ngăn chặn dịch vụ này cho router WiFi cho phép bạn chọn những gì bạn muốn ngăn chặn về nội dung Internet và những dịch vụ và khi nào bạn muốn ngăn chặn nó.

Ghi chú

Điều quan trọng là phải hiểu sự khác biệt giữa Internet và những nơi giao tiếp khác nhau chẳng hạn như World Wide Web và các dịch vụ gửi thông báo tức thì vốn hoạt động trên Internet. Internet là hạ tầng hoặc xa lộ thật sự cho phép chúng ta tận dụng các giao thức Internet hoặc những chiến lược khác nhau để giao tiếp trên hạ tầng Internet. Một dịch vụ chẳng hạn như web hoặc gửi thông báo tức thì là một chiến lược giao tiếp chạy trên hạ tầng Internet. Web chỉ là một trong vài chiến lược giao tiếp có thể truy cập các dữ liệu được cung cấp bởi các web server cũng kết nối với Internet. Một ví dụ khác về một dịch vụ giao tiếp sử dụng hạ tầng Internet là gửi thông báo tức thì có sẵn từ một số nhà cung cấp dịch vụ chẳng hạn như Microsoft (MSN Messenger), Yahoo! (Yahoo Instant Messaging) và AOL (AIM hoặc AOL Instant Messenger).

Vậy thì router thật sự có thể ngăn chặn người dùng truy cập một website nhất định như thế nào? Đó là do các hoạt động của web và Internet. Ví dụ World Wide Web hoặc "Web" là một môi trường client/server. Nội dung được yêu cầu bởi những người dùng kết nối với Internet sử dụng các trình duyệt web (client) và sau đó được "phục vụ" bởi các web server (server). Hãy nhớ World Wide Web chỉ là một dịch vụ sử dụng hạ tầng Internet để giao tiếp.

Chính sự giao tiếp giữa web client và phần mềm web server cho phép bạn lướt web và xem nội dung. Bởi vì các yêu cầu từ phần mềm client (trình duyệt web của một người dùng chẳng hạn như Interr et Explorer) phải đi qua router để đi đến Internet và các web server đợi bên ngoài trên Internet để nhờ các yêu cầu nội dung, Router có thể kiểm tra các yêu cầu được thực hiện bởi client. Nếu yêu cầu client đòi hỏi nội dung mà Router đã được cấu hình để ngăn chặn, router không chuyển tiếp (forward) đến web. Điều này có nghĩa yêu cầu về nội dụng bị ngăn chặn. Hãy xem các chi tiết cụ thể về việc nội dung web bị ngăn chặn bởi router WiFi như thế nào và sau đó xem cách bạn ngăn chặn các dịch vụ Internet chẳng hạn như chơi game hoặc gửi thông báo tức thì.

Ngăn chặn nội dung

Khi bạn cấu hình router để ngăn chặn nội dung web, bạn thật sự ngăn chặn các website dựa vào các từ khóa hoặc các tên website riêng biệt, nghĩa là tên domain hoặc URL (uniform resource locator) cho site. Nói cách khác để thật sự ngăn chặn nội dung từ các website, bạn phải tạo một danh sách các từ khóa và các tên domain (miền) thật sự.

Danh sách từ khóa được router dùng làm tham chiếu; khi một người dùng trên mạng yêu cầu một website bằng cách sử dụng một trình duyệt web, router xem danh sách từ khóa và so sánh nó với tên website được yêu cầu. Nếu một từ khóa hoặc tên domain trong danh sách khớp với tên website (tên domain) đang được yêu cầu, website bị ngăn chặn.

Rõ ràng việc ngăn chặn các website bằng tên website thì khá dễ dàng. Ví dụ thêm URL www.pornographic.com vào danh sách từ khóa và site trên router sẽ ngăn chặn file cụ thể đó. Việc lập một danh sách từ khóa để ngăn chặn các site là một vấn đề khác đòi hỏi suy nghĩ một chút.

Ví dụ, bạn nhập từ violence trong danh sách từ khóa. Bây giờ tất cả các websites có từ violence trong tên website sẽ bị ngăn chặn. Tuy nhiên, cách sắp xếp này cũng sẽ ngăn chặn một trang web mang tên www.stop-violence.org. Khi suy xét một danh sách từ khóa để ngăn chặn các loại website nhất định chẳng hạn như các website đồi trụy, danh sách từ khóa của bạn phải phản ánh loại ngôn ngữ sử dụng trong các tên website. Điều này có nghĩa danh sách từ khóa sẽ bao gồm nhiều từ bạn sẽ không sử dụng công khai (hoặc thậm chí riêng tư trong hết các trường hợp.)

Rõ ràng bất kỳ danh sách từ khóa mà bạn tạo sẽ được biên tập theo thời gian vì bạn không muốn một từ khóa trong danh sách ngăn chặn các site "tốt" Hầu hết các router WiFi cung cấp một tính năng log nhằm cho phép bạn xem những website đã được "cho phép" và đã bị "từ chối" bởi danh sách từ khóa và URL của bạn để ngăn chặn nội dung. Xem log theo thời gian để thấy những gì bị ngăn chặn và những gì được cho phép sẽ cho bạn cơ hội biên tập từ khóa sao cho bộ lọc ngăn chặn nội dung làm tốt công việc của nó.

Một điều nữa liên quan tới việc ngăn chặn nội dung: khi bạn ngăn chặn nội dung, bạn ngăn chặn nội dung cho tất cả các máy tính trên mạng. Bạn có thể ngăn chặn nội dung trên cơ sở từng máy tính. Router WiFi sẽ được cấu hình để sao cho một máy tính trên mạng được miễn ngăn chặn và lọc nội dung. Máy tính này được gọi là máy tính đáng tin cậy trong cách xác lập cấu hình nội dung web cho một router Netgear (cấu hình của Router có thể xem máy tính là exempt hoặc sử dụng một từ khác nào đó). Máy tính đáng tin cậy đơn giản là nó có thể truy cập một nội dung vốn bị ngăn chặn cho những máy tính khác trên mạng bởi router.

Thuật ngữ chính

Máy tính đáng tin cậy (trusted computer). Máy tính được xác lập trong cấu hình của một Router là miễn ngăn chặn nội dung web.

Việc xác lập một máy tính đáng tin cậy trên mạng đạt kết quả tốt nếu mọi người sử dụng có máy tính riêng của mình. Nếu bạn chia sẻ máy tính với người khác chẳng hạn như con của bạn, bạn có thể phải sử dụng tính năng thời biểu của một router để ngăn chặn nội dung trong những thời điểm nhất định trong ngày.

Ngăn chặn các dịch vụ

Sử dụng router WiFi để ngăn chặn các dịch vụ Internet thì phức tạp hơn ngăn chặn nội dung nhưng chỉ vì bạn phải hiểu các dịch vụ khác nhau như email phải gửi thông điệp tức thì và web thật sự giao tiếp và di chuyển thông tin trên Internet như thế nào.

Mục 37 đã thảo luận giao thức trên TCP/IP và việc lập địa chỉ IP, giao thức TCP/IP thật sự là một nhóm hoặc "ngăn xếp" các giao thức nhỏ hơn được sử dụng để quản lý các khía cạnh giao tiếp khác nhau giữa các máy tính trên một mạng. IP hoặc Internet Protocol xử lý phương pháp lập địa chỉ IP được sử dụng trên mạng. Một máy tính được gán một địa chỉ IP duy nhất mà qua đó một máy tính được nhận biết trên mạng khi gửi hoặc nhận dữ liệu.

Ngăn xếp giao thức TCP/IP cung cấp hai giao thức vốn thật sự thương lượng và quản lý việc di chuyển dữ liệu giữa các máy tính; những giao thức này là Transmission Control Protocol (TCP) và User Datagram Protocol (UDP). Các dịch vụ Internet hoặc ứng dụng sử dụng TCP hoặc UDP hoặc cả hai để điều khiển sự di chuyển dữ liệu giữa một client chẳng hạn như instant messenger hoặc web client (trình duyệt web của bạn) và server Internet vốn cung cấp loại dịch vụ mà bạn đang cố tận dụng.

Ví dụ khi hai người dùng máy tính đang "chat" với nhau bằng cách sử dụng tính năng gửi thông báo tức thì (sử dụng một client chẳng hạn như AOL, Instant Messenger AIM), dữ liệu (chat) đi từ client gửi thông báo tức thì đến một server gửi thông bảo. Sau đó dữ liệu chuyển tiếp từ server gửi thông báo đến người nhận. Dữ liệu được gửi và được nhận bởi client gửi thông báo tức thì (sử dụng server gửi thông báo) được di chuyển trên Internet bằng giao thức TCP. TCP/IP không chỉ cung cấp giao thức vận chuyển, trong trường hợp này TCP (một số phần mềm khác sử dụng UDP thay vì TCP) di chuyển dữ liệu. Để di chuyển dữ liệu mỗi ứng dụng (chẳng hạn như phần mềm gửi thông báo tức thì, hoặc web hoặc email client) thương lượng việc di chuyển dữ liệu từ máy tính này đến máy tính khác bằng cách sử dụng một kênh riêng biệt, được gọi là port (cổng). Ví dụ cổng mà tất cả máy tính sử dụng cho web là cổng 80. Số cổng được sử dụng cho việc gửi thông báo tức thì AOL là 5190. Số cổng cho Real Audio (Real Player) là một dãy cổng từ 6970 đến 7170.

Ghi chú

Các cổng được sử dụng trên các thiết bị để giao tiếp trên một mạng IP không hiện hữu về khía cạnh vật lý. Chúng là các tên trong mã phần mềm hướng dẫn các ứng dụng giao tiếp trên một cổng cụ thể khi dữ liệu được gửi hoặc được nhận.

THUẬT NGỮ CHÍNH

Port (cổng). Một kênh giao tiếp được đánh số hoặc điểm cuối (end point) được sử dụng bởi một ứng dụng Internet. Làm con đường hoặc cửa ngõ để thương lượng các cuộc truyền dữ liệu giữa hai máy tính.

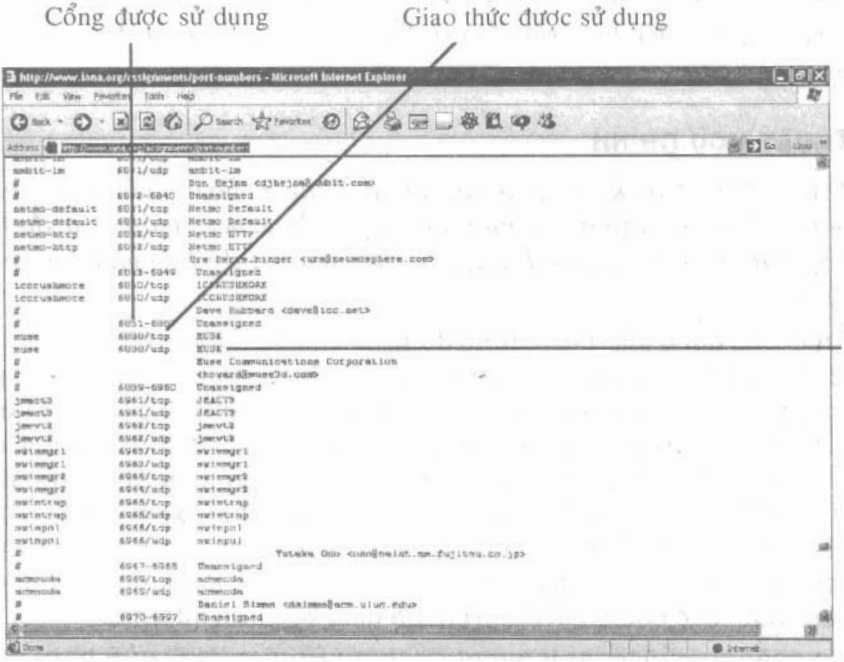
Tóm lại mỗi ứng dụng Internet phải sử dụng một giao thức vận chuyển (TCP, UDP, hoặc cả hai trong một số trường hợp) và việc thương lượng truyền dữ liệu xảy ra trên một cổng. Danh sách các cổng thật sự có sẵn được bảo trì bởi Internet Engineering Task Force. Số cổng có thể bắt đầu từ 0 đến 65536. Các cổng từ 1 đến 1024 được dành riêng cho các dịch vụ Internet nhất định chẳng hạn như Web (HTTP) và email (các giao thức POP3) và được xem là các cổng phổ biến. Các nhà phát triển phần mềm tạo một chương trình mới cho Internet chọn một cổng từ danh sách này (một cổng không được sử dụng từ chương trình Internet khác) sao cho phần mềm có thể giao tiếp trên Internet.

Để ngăn chặn một dịch vụ Internet sử dụng Router WiFi của bạn, bạn chọn dịch vụ cụ thể chẳng hạn như gửi thông báo tức thì hoặc web (HTTP) từ một danh sách các dịch vụ được cung cấp trong cấu hình của router. Số dịch vụ được liệt kê phụ thuộc vào router (và nhà sản xuất của router). Khi bạn chọn một dịch vụ từ danh sách, giao thức vận chuyển và cổng cho ứng dụng được cấu hình tự động.

Nếu bạn muốn ngăn chặn một dịch vụ vốn không được liệt kê trong danh sách dịch vụ của một router, hầu hết các router WiFi cho phép bạn cấu hình một dịch vụ " do người dùng ấn định" để cấu hình một dịch vụ ngay từ đầu, bạn cần biết giao thức vận chuyển cho ứng dụng (TCP, UDP hoặc cho cả hai) và số cổng hoặc dãy số cổng mà dịch vụ ứng dụng.

Bạn có thể dò tìm giao thức vận chuyển (TCP hoặc UDP) và số cổng cho nhiều dịch vụ Internet bằng cách sử dụng danh sách được cung cấp tại http://www.jana.org/assignments/port-numbers. Bạn có thể cuộn qua danh sách hoặc sử dụng tính năng Find của trình duyệt web để tìm kiếm một công ty hoặc tên ứng dụng nào đó. Trong các trường hợp danh sách IANA không cung cấp cho bạn thông tin bạn cần, bạn có thể lấy thông tin từ website của nhà phát triển phần mềm hoặc website của công ty bán sản phẩm.

Như bạn có thể khi ngăn chặn nội dung, bạn có thể ngăn chặn các dịch vụ vào một thời điểm nào đó trong ngày bằng tính năng lập thời biểu (scheduling) được cung cấp bởi router WiFi. Bạn có thể ngăn chặn một dịch vụ cho tất cả máy tính trên mạng hoặc bạn có thể xác định địa chỉ IP của những máy tính mà bạn muốn dịch vụ bị ngăn chặn.



Đi đến website IANA nếu bạn cần biết giao thức vận chuyển và số cổng được sử dụng bởi một dịch vụ mà bạn muốn ngăn chặn bằng cách sử dụng router WiFi.

Các vấn đề về chơi Game và sự truy cập Workgroup

Router WiFi được thiết kế để giữ cho mạng nội bộ (workgroup của bạn) an toàn khỏi sự xâm nhập bên ngoài. **Mục 70** và **mục 71** thảo luận những tính năng an ninh mà router mang lại. Nhưng trong một số trường hợp, bạn muốn cho phép những người dùng bên ngoài truy cập các dịch vụ từ mạng riêng của bạn. Ví dụ, bạn có phần mềm với server chạy trên một máy tính và muốn những người dùng trên Internet có thể xem trang web của bạn. Điều này cũng rất hữu dụng (và cần thiết) trong các tình huống chơi game dành cho nhiều người chơi nơi mà bạn muốn những game thủ khác có thể truy cập máy tính của bạn để chơi game peer-to-peer (ngang hàng).

Do đó bạn muốn cho phép sự truy cập bên ngoài đến mạng của bạn, nhưng chắc chắn bạn không muốn mở toang mạng nội bộ riêng của bạn ra trước những mối đe dọa bên ngoài. Router WiFi có thể cho phép và kiểm soát sự truy cập đến một tài nguyên trên mạng của bạn (chẳng hạn như một web server) bằng cách sử dụng port fowarding. Port forwarding mở một cổng (port) trên router và router chuyển tiếp các yêu cầu bên ngoài cho một dịch vụ "bên trong" cụ thể, chẳng hạn như một web server hoặc mail server (server FTP) sử dụng cổng đó. Port forwarding làm cho máy tính trên mạng (máy tính có phần mềm web server trên đó) nhìn thấy được đối với những máy tính bên ngoài mạng (nghĩa là các máy tính trên Internet) sao cho những người dùng có thể truy cập dịch vụ hoặc nội dung nội bộ của bạn.

Thuật ngữ chính

Port forwarding. Một phương pháp mở các cổng trên router WiFi nhằm cho phép các yêu cầu về các dịch vụ bên ngoài truy cập các máy tính cung cấp những dịch vụ đó trên mạng nội bộ chẳng hạn như một web server. Khi bạn sử dụng port forwarding, địa chỉ IP nội bộ của bạn có thể được theo dõi bởi các server trên Internet, đây có thể là mối quan tâm an ninh.

Nếu bạn thích chơi game dành cho nhiều người chơi và muốn chơi các game chẳng hạn như Quake hoặc Starcraft trên mạng của bạn, bạn phải cấu hình port triggering. Port triggering tạm thời mở một cổng và cũng không đòi hỏi địa chỉ IP của bạn được theo dõi bởi các server trên Internet. Port triggering không tạo một cổng mở toang như port forwarding (port forwarding mở và đóng cổng khi cần thiết) và cũng giữ bí mật địa chỉ IP nội bộ của bạn. Nhưng port triggering cho phép những máy tính khác truy cập dịch vụ và kết nối với máy tính của bạn, điều này cần thiết cho việc chơi game dành cho nhiều người chơi.

Thuật ngữ chính

Port forwarding. Một cách để tạm thời mở một cổng trên router WiFi khi một yêu cầu bên ngoài về cổng đó được nhận bởi router. Port triggering không để mở các cổng (như port forwarding) và không cho biết địa chỉ IP của máy tính nội bộ cung cấp dịch vụ. Port triggering được sử dụng để cấu hình máy tính cho các dịch vụ chẳng hạn như chơi game trực tuyến.

55. Ngăn chặn sự truy cập đến các Website

Trước khi bạn bắt đầu

22. Truy cập cấu hình Router

24. Bàn về việc lọc nội dung và mở các cổng

Bạn có thể ngăn chặn sự truy cập đến website từ những máy tính trong workgroup (thông qua router đến Internet) bằng địa chỉ web (tên miền) hoặc sử dụng một danh sách từ khóa. Số mục nhập mà bạn có thể có trong danh sách phụ thuộc vào router WiFi mà bạn đã mua. Ví dụ, router WiFi Netgear WGR614 cho phép bạn tạo một danh sách từ khóa/tên miền vốn có thể chứa 255 mục nhập.

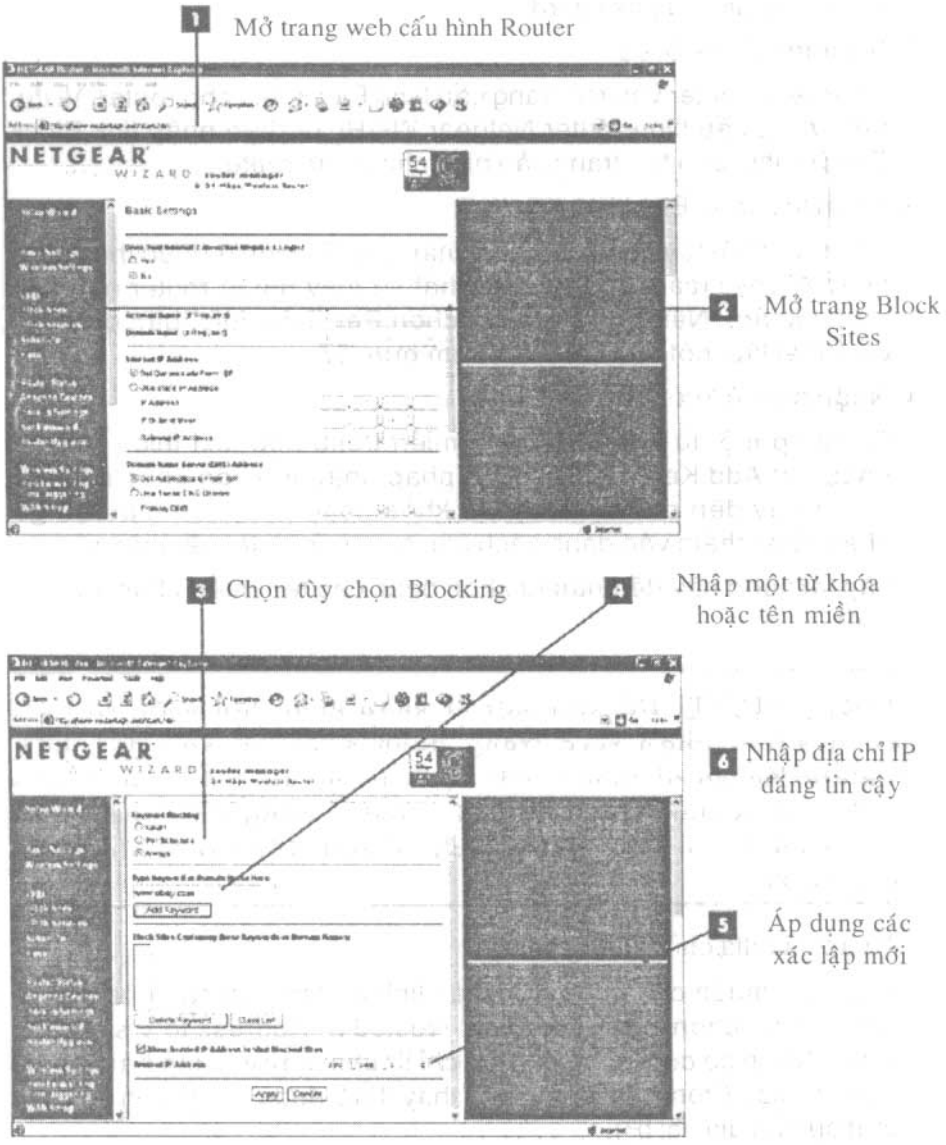
Nếu bạn có một router Netgear WGR614, bạn có thể nhập 255 tên miền trong danh sách từ khóa để ngăn chặn 255 website. Tuy nhiên, nếu bạn sử dụng các từ khóa để ngăn chặn các site, bạn có thể lập một danh sách các từ khóa vốn có thể ngăn chặn hàng ngàn file xấu hoặc không phù hợp. Nếu ban biết các website cụ thể mà bạn muốn ngăn chặn, bằng mọi giá phải nhập tên miền cho các site đó trong danh sách. Tuy nhiên, các từ khóa mà bạn nhập trong danh sách cung cấp những khả năng có tầm ảnh hưởng rộng nhất cho việc ngăn chặn hầu hết các site.

Để lập một danh sách từ khóa ngăn chặn sự truy cập, xem xét những điều sau đây:

- *Tôi muốn ngăn chặn các loại website nào?*
- *Các từ khóa nào thường xuất hiện trong các tên miền cho những website này?*
- *Danh sách từ khóa của tôi có thể ngăn chặn các website nào mà tôi không muốn ngăn chặn?*

Khi bạn bắt đầu ngăn chặn các website bằng cách sử dụng một danh sách các tên miền hoặc từ khóa, bạn sẽ phải giám sát log của router để quyết định xem tính năng ngăn chặn truy cập có thật sự thực thi như bạn mong đợi hay không. Để biết thông tin về việc xem log của router, **xem mục 98**. Có thể bạn phải biên tập danh sách từ khóa theo thời gian để đạt được kết quả bạn tìm kiếm.

55. Ngăn chặn sự truy cập đến các website



1. Mở trang web cấu hình Router.

   Mở trang web cấu hình router (nhập địa chỉ web đã được chỉ định cho router khi bạn cài đặt nó và sau đó gõ nhập tên đăng nhập administrator và password cho router).

   Nếu bạn quên địa chỉ web hoặc URL cho router, hãy xem tài liệu đi kèm router WiFi. Tài liệu này cũng cung cấp tên đăng nhập và password mặc định cho router. Tất cả thông tin này được xác định bởi nhà sản xuất router và thường như nhau cho tất cả router được sản xuất bởi một nhà cung cấp cụ thể. Ví dụ router Netgear sử dụng URL

http://www.routerlogin.net/start.htm. Tên đăng nhập là admin và password mặc định là password.

2. Mở trang Block Sites

   Chọn lệnh router vốn mở trang cấu hình Block Site cho router. Ví dụ, trên trang cấu hình router Netgear WGR614, bạn nhấp link Block Sites ở phía bên trái trang cấu hình chính của router.

3. Chọn tùy chọn Blocking

   Chọn một nút tùy chọn để ngăn chặn Per Schedule (theo thời biểu) hoặc Always (các tên tùy chọn thật sự thay đổi từ router này đến router khác). Nếu bạn chọn tùy chọn Per Schedule, bạn cũng sẽ cần thiết lập một thời biểu lọc, **xem mục 57**.

4. Nhập một từ khóa hoặc tên miền

   Gõ nhập một từ khóa hoặc tên miền trong hộp text thích hợp và nhấp nút Add Keyword (phương pháp nhập từ khóa khác nhau từ router này đến router khác). Từ khóa hoặc tên miền mà bạn gõ nhập được thêm vào danh sách các mục mà router sẽ ngăn chặn.

   Lặp lại bước này để nhập từ khóa hoặc các tên miền khác khi cần thiết.

THỦ THUẬT: Để xóa một từ khóa hoặc tên miền ra khỏi danh sách, chọn mục trong danh sách và sau đó nhấp Delete Keyword (hoặc một lệnh tương tự trên trang cấu hình của router). Hầu hết các router cũng cho phép bạn xóa sạch hoàn toàn danh sách và bắt đầu lại từ đầu nếu cần thiết.

---

5. Nhập các địa chỉ IP đáng tin cậy

   Nếu bạn muốn cho phép một máy tính cụ thể truy cập các site bị ngăn chặn, chọn hộp kiểm Allow Trusted IP Address to Visit Block Sites. Nhập số cuối cùng của địa chỉ IP cho máy tính mà bạn muốn được tin cậy (trong ví dụ này, bạn thay đổi 0 được cho thành số cuối thật sự của địa chỉ IP).

THỦ THUẬT: Để quyết định địa chỉ IP của máy tính (địa chỉ được gán bởi router WiFi có chức năng như một server DHCP, bạn có thể sử dụng lệnh ipconfig/all vốn hiển thị địa chỉ IP (và subnet mask của máy tính và thông tin khác). Trên máy tính mà bạn tin cậy, nhấp nút Start và sau đó chọn Run. Trong hộp thoại Run, gõ nhập Command và nhấn Enter. Tại dòng nhắc lệnh, gõ nhập config/all. Lệnh này trả về địa chỉ IP, subnet mask và thông tin khác về

máy tính chẳng hạn như địa chỉ IP của gateway mặc định và server DHCP (vốn là router WiFi). Để đóng hộp thoại lệnh, gõ nhập Exit và nhấn Enter. Để tìm hiểu thêm thông tin về lệnh ipconfig, xem mục 96 và mục 97.

6. Áp dụng các xác lập mới

   Sau khi nhập các tham số khác nhau cho tính năng blocked content, bạn phải áp dụng các xác lập cho cấu hình của router. Nhấp nút Apply (hoặc nút áp dụng và lưu các xác lập từ router). Các xác lập mới sẽ có hiệu lực ngay tức thì; sự truy cập đến các website từ những máy tính trên mạng sẽ bị ngăn chặn theo danh sách tên miền và từ khóa mà bạn đã tạo.

Khi một người dùng cố mở một website vốn bị ngăn chặn bởi router (sử dụng một trình duyệt khác chẳng hạn như Internet Explorer), một màn hình mở ra trong trình duyệt web cho người dùng biết rằng site bị ngăn chặn.

56. Ngăn chặn sự truy cập đến các dịch vụ Internet

Trước khi bạn bắt đầu	**Xem thêm**
22. Truy cập cấu hình Router	**Mục 57**
54. Bàn về việc lọc nội dung và mở các cổng	

Ngăn chặn các dịch vụ chẳng hạn như FTP và gởi thông báo tức thì (instant messaging) cho phép bạn kiểm soát việc mạng sử dụng các loại ứng dụng cụ thể trên Internet. Ví dụ, việc ngăn chặn dịch vụ FTP (File Transfer Protocol) cho mạng sẽ có nghĩa rằng những người dùng trên mạng không thể download các site từ các file FTP (được thiết kế là những nơi lưu trữ nội dung có thể download). Việc ngăn chặn các dịch vụ FTP sẽ ngăn chặn những đứa con của bạn download các file nhạc bất hợp pháp từ một site FTP nghịch ngợm. Nếu bạn không muốn việc gởi thông báo tức thì xảy ra trên mạng sau 8 giờ tối, bạn có thể ngăn chặn dịch vụ AIM trên cơ sở thời biểu (như được giải thích trong **mục 57**).

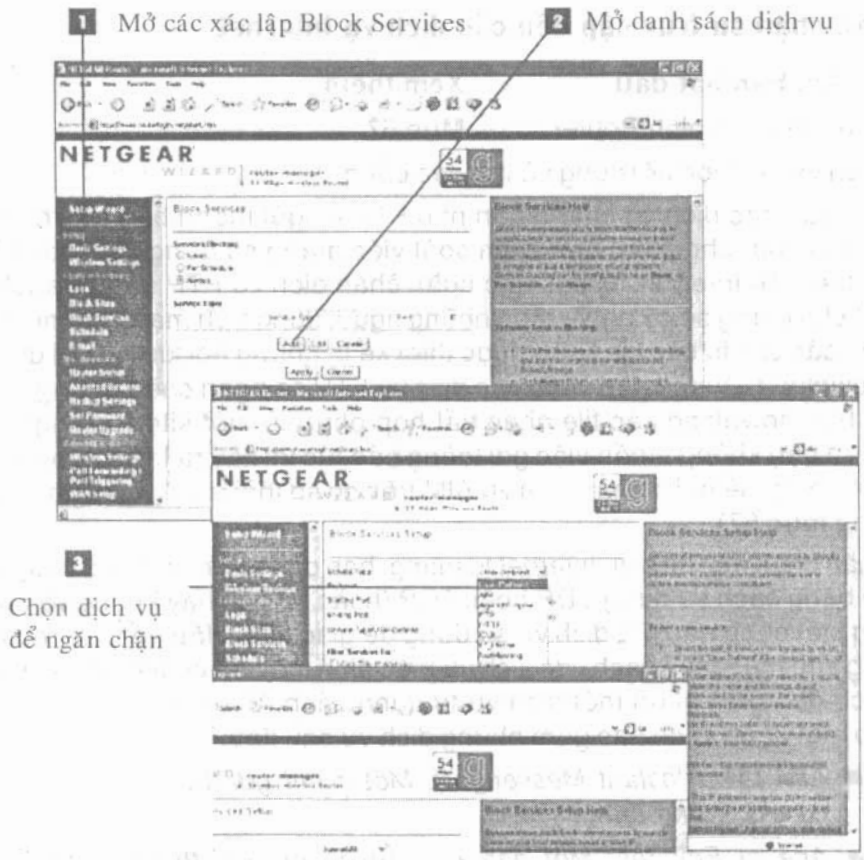
Để ngăn chặn một dịch vụ Internet từ mạng, bạn cần biết dịch vụ có chuyển thông tin bằng cách sử dụng UDP hoặc TCP (hoặc cả hai) hay không và bạn cũng cần biết cổng nào mà dịch vụ sử dụng để giao tiếp. Hầu hết các router WiFi cung cấp một danh sách các dịch vụ mặc định mà bạn có thể ngăn chặn bằng cách đơn giản chọn một dịch vụ từ danh sách. Ví dụ, router Netgear cung cấp một danh sách bao gồm những dịch vụ sau đây:

- *AIM (AOL Instant Messenger): Một client gởi thông điệp tức thì cực kỳ thông dụng.*
- *Age of Empires: Một game nhiều người chơi thông dụng của Microsoft có thể chơi trên một mạng.*
- *FTP (File Transfer Protocol): Một giao thức được sử dụng để truyền các file trên Internet.*

- *HTTP (Hypertext Transfer Protocol): Giao thức cho phép trình duyệt web giao tiếp với các web server và ngược lại. Nếu bạn ngăn chặn FTP, các máy tính trên mạng sẽ không thể duyệt các website. Điều này có nghĩa bạn có thể chắc chắn rằng không ai lướt web sau 9 giờ tối nếu bạn ngăn chặn dịch vụ FTP với một thời biểu lọc.*

Chọn một dịch vụ từ danh sách được cung cấp bởi router sẽ từ chối việc bạn phải tìm kiếm cổng và giao thức được sử dụng bởi dịch vụ cụ thể đó. Thông tin cổng và giao thức được điền vào cho bạn. Danh sách các dịch vụ được cung cấp bởi router thay đổi từ router này đến router khác. Bất kỳ dịch vụ khác mà bạn muốn ngăn chặn (các dịch vụ vốn không được cung cấp trên một danh sách) phải được thiết lập bằng tay (nghĩa là bạn phải cung cấp giao thức UDP hoặc TCP hoặc cả hai và số cổng được sử dụng bởi dịch vụ mà bạn muốn ngăn chặn).

56. Ngăn chặn sự truy cập đến các dịch vụ Internet





1. Mở các xác lập Block Services

   Mở trang web cấu hình chính của router (gõ nhập URL của router, chẳng hạn như routerlogin.net rồi nhập tên đăng nhập và password quyền quản trị; tất cả thông tin này nằm trong tài liệu do nhà sản xuất router cung cấp). Mở tính năng Block Services bằng cách chọn link Block Services (hoặc lệnh tương tự) trên danh sách lệnh của router.

2. Mở danh sách dịch vụ

   Chọn một trong các nút tùy chọn Service Blocking. Ví dụ đối với router Netgear, chọn Always hoặc Per Schedule (trang cấu hình của router sẽ có những tùy chọn tương tự). Để mở danh sách dịch vụ được cung cấp bởi router, nhấp nút Add hoặc lệnh tương tự (ví dụ trên một router Linksys là một danh sách cuộn thay vì một danh sách xổ xuống, nhưng bạn vẫn sử dụng nút Add để thêm dịch vụ).

3. Chọn dịch vụ để ngăn chặn

   Nhấp danh sách xổ xuống Service Type để hiển thị một danh sách các dịch vụ mà router biết đến. Từ danh sách này, chọn dịch vụ cần ngăn chặn (chẳng hạn như AIM, FTP hoặc RealAudio). Nếu bạn muốn ngăn chặn một dịch vụ không có trên danh sách, chọn tùy

chọn User Defined, sau đó nhập giao thức vận chuyển (UDP hoặc TCP) và số cổng cho dịch vụ. Bạn phải nhập số cổng đầu và cuối cho dịch vụ (ví dụ, nếu số cổng là 2600, cổng đầu là 2600 và cổng cuối cũng là 2600). Trong hộp text Service Type/User Defined, gõ nhập một tên cho dịch vụ do người dùng ấn định này (ví dụ, nếu bạn ngăn chặn một dịch vụ truyền thông có tên là "glowworm", bạn gõ nhập glowwom làm loại dịch vụ).

THỦ THUẬT: Website JANA là một thích hợp tốt để tìm các số cổng cho những dịch vụ không được liệt kê trong danh sách dịch vụ mà router cung cấp. Kiểm tra http://www.iana.org/assignments/port-numbers. Website này cũng cung cấp giao thức (UDP hoặc TCP) được sử dụng bởi dịch vụ cụ thể. Thông tin cổng và thông tin giao thức vận chuyển cho một dịch vụ cụ thể cũng có thể được tìm thấy bằng cách tìm kiếm Web. Để biết thêm thông tin về số cổng và giao thức vận chuyển, xem mục 54.

---

4. Cấu hình bộ lọc dịch vụ cho các địa chỉ IP riêng biệt

   Sau khi bạn đã chọn một dịch vụ để ngăn chặn, bạn có thể nhập một địa chỉ IP hoặc một dãy địa chỉ IP cho các máy tính trong mạng mà bạn muốn router ngăn chặn dịch vụ. Chọn một trong các nút tùy chọn sau đây:

THỦ THUẬT: Để xác định địa chỉ IP của một máy tính, địa chỉ được gán bởi router WiFi có chức năng như một server DHCP, bạn có thể sử dụng lệnh ipconfig. Trên máy tính mà bạn cần thông tin này, nhấp nút Start và sau đó chọn Run. Trong hộp thoại Run, gõ nhập một lệnh và nhấn Enter. Tại dòng nhắc lệnh, gõ nhập ipconfig/all.

Lệnh này trả về địa chỉ IP, subnet mask và thông tin khác về máy tính chẳng hạn như địa chỉ IP của gateway mặc định và server DHCP (vốn là router WiFi) để đóng hộp thoại lệnh, gõ nhập Exit và nhấn Enter. Để biết thêm thông tin về lệnh ipconfig, xem mục 96 và mục 97.

- ***Only This IP Address***. *Chọn tùy chọn này nếu bạn muốn ngăn chặn dịch vụ đã chọn cho một máy tính trong mạng. Sau đó nhập địa chỉ IP cho máy tính đó.*
- ***IP Address Range***: *Chọn tùy chọn này nếu bạn muốn ngăn chặn dịch vụ được chọn từ một dãy máy tính trong mạng (chẳng hạn cho tất cả máy tính được sử dụng bởi những đứa con của bạn). Sau đó, nhập địa chỉ IP đầu và cuối của dãy máy tính.*

- ***All IP Addresses**: Chọn tùy chọn này nếu bạn muốn ngăn chặn dịch vụ hiện hành cho tất cả máy tính trên mạng.*

5. Thêm dịch vụ vào danh sách Blocked

   Sau khi chọn hoặc nhập dịch vụ và các tùy chọn liên quan đến các địa chỉ IP mà bạn muốn chặn dịch vụ này, nhấp Add để thêm dịch vụ vào danh sách blocked.

   Lặp lại các bước 3-5 khi cần thiết để thêm những dịch vụ khác vào danh sách các dịch vụ bị ngăn chặn.

6. Áp dụng các xác lập Blocked Services

   Sau khi thêm các dịch vụ mà bạn muốn ngăn chặn, nhấp Apply để áp dụng các xác lập ngăn chặn dịch vụ vào cấu hình của router.

57. Thiết lập một thời biểu lọc

Trước khi bạn bắt đầu

22. Truy cập thông tin Router

54. Bàn về việc lọc nội dung và mở các cổng

55. Ngăn chặn sự truy cập đến các website

56. Ngăn chặn sự truy cập đến các dịch vụ Internet

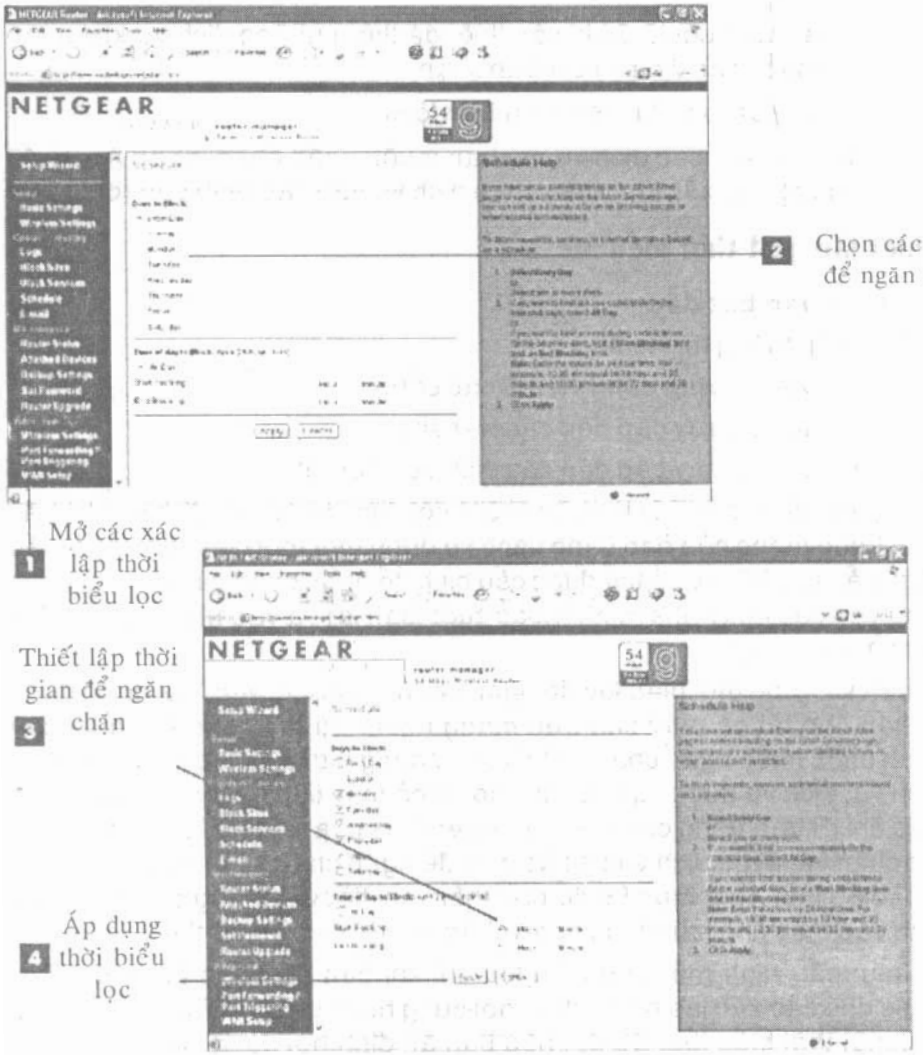
Nếu bạn muốn lọc (nghĩa là ngăn chặn) nội dung hoặc các dịch vụ cho các máy tính trong mạng của bạn bằng cách sử dụng một thời biểu, bạn phải cấu hình thời biểu lọc. Bộ lọc có thể được cấu hình để ngăn chặn các dịch vụ hoặc nội dung vào các ngày nhất định (hoặc suốt tuần lễ) và vào những thời điểm nhất định trong ngày.

Khi bạn sử dụng thời biểu lọc để ngăn chặn nội dung web, nội dung được ngăn chặn cho tất cả máy tính trên mạng ngoại trừ máy tính đáng tin cậy (máy tính được miễn ngăn chặn). Khi bạn sử dụng thời biểu lọc để ngăn chặn một dịch vụ, dịch vụ được ngăn chặn cho tất cả máy tính mà bạn đã xác định bằng địa chỉ IP trên trang cấu hình block services của router. Tất cả nội dung bị ngăn chặn và tất cả dịch vụ đã xác định để ngăn chặn sẽ bị ngăn chặn bởi một thời biểu lọc. Xem mục 56 để biết thêm chi tiết về những cách mà bạn xác định các máy tính cần được ngăn chặn từ một dịch vụ cụ thể.

Bạn cần cấu hình một thời biểu lọc chỉ khi bạn đã chọn tùy chọn Per Schedule cho các xác lập ngăn chặn nội dung hoặc dịch vụ. Bạn có thể cấu hình chỉ một thời biểu lọc. Do đó, nếu bạn ấn định nội dung web nên được ngăn chặn "per schedule" và các dịch vụ đã chọn nên được ngăn chặn "per schedule", tất cả nội dung và các dịch vụ theo cùng một thời biểu sẽ luôn ngăn chặn đúng nội dung (ví dụ, bạn không muốn hình ảnh đồi trụy có sẵn cho những đứa con của bạn dựa vào một thời biểu); để luôn ngăn chặn nội dung, xác định Always khi bạn cấu hình router để ngăn chặn nội dung web. Sau đó, bạn sử dụng thời biểu lọc một cách thích hợp hơn để ngăn chặn các dịch vụ nhất định, bạn không muốn con của bạn sử dụng vào đêm khuya (chẳng hạn như các tính năng gởi thông báo tức thì hoặc chơi game).

Thời biểu lọc mặc định cho hầu hết các router WiFi là Every Day, nghĩa là các nội dung và dịch vụ mà bạn đã chọn để ngăn chặn 7 ngày một tuần; thời gian mặc định mà nội dung và các dịch vụ bị ngăn chặn là All Day, nghĩa là nội dụng và các dịch vụ bị ngăn chặn 24 giờ mỗi ngày.

57. Thiết lập một thời biểu lọc



1. Mở các xác lập thời biểu lọc

   Mở trang web cấu hình chính của router (gõ nhập URL của router chẳng hạn như routerlogin.net, sau đó nhập tên đăng nhập và password quản trị). Mở tính năng Schedule bằng cách chọn link Schedule (hoặc lệnh tương tự) trên danh sách lệnh router. Ví dụ trên router

Netgear, nhấp Schedule trên danh sách lệnh nằm ở phía bên trái trang web.

2. Chọn các ngày để ngăn chặn

Xác lập mặc định cho những ngày nào mà nội dung và các dịch vụ sẽ được ngăn chặn là Every Day. Hủy chọn hộp kiểm cho Every Day nếu bạn không muốn ngăn chặn 7 ngày một tuần và thay vào đó bạn muốn ngăn chặn các ngày cụ thể và sau đó chọn hộp kiểm cho các ngày mà bạn muốn ngăn chặn nội dung hoặc các dịch vụ (hoặc cả hai nếu bạn đã cấu hình cả hai).

3. Xác lập thời gian để ngăn chặn

Nếu bạn muốn xác định một dãy thời gian để ngăn chặn vào các ngày ma bạn đã chọn, chọn hộp kiểm All Day và nhập thời gian Start Blocking và End Blocking trong các hộp text thích hợp. Hầu hết các router sử dụng một hệ thống thiết lập thời gian 24 giờ; thời gian vào buổi sáng (am) là giờ thật sự (8 giờ sáng là 8 giờ trên đồng hồ 24 giờ). Các giờ sau buổi trưa (p.m) được xác lập bằng cách cộng 12 (giờ) với thời gian, do đó 8 p.m được nhập là 20 (giờ) trên đồng hồ 24 giờ.

4. Áp dụng thời biểu lọc

Sau khi bạn đã chọn các ngày và thiết lập một dãy thời gian, nhấp OK để thêm thời biểu lọc vào cấu hình của router.

58. Cấu hình Port Forwarding và Port Triggering

Trước khi bạn bắt đầu

22. Truy cập cấu hình router

24. Bàn về việc lọc nội dung và mở các cổng

Việc mạng của bạn nằm đằng sau một router có nghĩa là các router bảo vệ máy tính của bạn khỏi sự xâm nhập từ thế giới bên ngoài. Nhưng có thể có những trường hợp bạn muốn chạy các server hoặc dịch vụ khác từ một máy tính trên mạng cục bộ của bạn và làm cho dịch vụ đó có sẵn đối với những người bên ngoài mạng (nghĩa là Internet).

Một số game máy tính (chẳng hạn như Quake, Starcraft, Kali và những game từ các nhà cung cấp game trên wẹb chẳng hạn như Ultima Online và MSN Gaming Zone) có thể được cấu hình dưới dạng các game nhiều người chơi ở nơi mà có nhiều người tham gia đấu với nhau trên một mạng. Những game này không chỉ được chơi bởi nhiều người dùng trên mạng cục bộ mà một số game còn cung cấp khả năng chơi các session nhiều người chơi trên Internet.

Để những người dùng bên ngoài truy cập một website hoặc game nội bộ được chơi trên mạng của bạn (họ cũng phải cài đặt game này trên máy tính của họ), bạn phải cung cấp một đường dẫn cho dữ liệu để di chuyển qua lại giữa các máy tính chạy game Bởi vì các router WiFi thật sự được thiết kế để ngăn các yêu cầu dữ liệu từ bên ngoài mạng, bạn phải cấu hình router WiFi

để nó cho phép giao tiếp giữa các máy tính chơi game. Điều này được thực hiện bằng cách sử dụng port forwarding hoặc port triggering. Như đã thảo luận, port forwarding lý tưởng cho những tình huống bạn muốn chạy dịch vụ chẳng hạn như một web server trên một máy tính trong mạng của bạn và làm cho dịch vụ đó có sẵn đối với những người dùng bên ngoài mạng, port triggering được sử dụng cho việc chơi game nhiều trò chơi, nơi mà có tối thiểu một trong những người chơi ở bên ngoài mạng WiFi của bạn.

Để port forwarding và port triggering hoạt động tốt, đặc biệt trong những trường hợp chơi game dành cho nhiều người chơi, bạn cũng phải cho phép router sử dụng UPnP (Universal Plug and Play). Tính năng này giúp các máy tính trên mạng phát hiện các dịch vụ đang được cung cấp bởi những máy tính khác trên mạng hoặc những máy tính bên ngoài mạng.

Thuật ngữ chính

UPnP (Universal Plug and Play). Một cấu trúc mạng hỗ trợ sự giao tiếp giữa các thiết bị tương thích UPnP, chẳng hạn như các máy tính trên các mạng và Internet. UPnP được hỗ trợ trên tất cả hệ điều hành và bởi hơn 400 nhà cung cấp phần cứng và thiết bị ngoại vi máy tính, những công ty thiết kế thiết bị để tương thích với UPnP trở lên.

Ghi chú

UPnP giúp các máy tính giao tiếp trên mạng để quyết định các dịch vụ nào đang được cung cấp bởi những máy tính khác trên mạng. Các máy tính thật sự truyền phát các thông báo trên mạng, cho những máy tính khác trên mạng biết các dịch vụ nào đang được cung cấp. Một router thường ngăn chặn lưu lượng truyền phát này. Khi UPnP được mở trên router của mạng, router không ngăn chặn các thông báo truyền phát khác nhau được gởi đi bởi các máy tính trên mạng. Nếu bạn sử dụng các ứng dụng gởi thông báo tức thì trên các máy tính mạng WiFi (chẳng hạn như AOL Instant Messenger AIM), bạn sẽ muốn mở UPnP thậm chí nếu bạn không cấu hình port forwarding hoặc port triggering.

58. Cấu hình Port Forwarding và Port Triggering



1. Truy cập xác lập UPnP

   Mở trang web cấu hình chính của router (gõ nhập URL của router, chẳng hạn như routerlogin.net, sau đó nhập tên đăng nhập và password quản trị; URL, tên đăng nhập và password mặc định đều được được xác lập bởi nhà sản xuất router, do đó hãy tham khảo tài liệu của router để biết thông tin này). Mở tính năng UPnP của router bằng cách chọn link UPnP (hoặc lệnh tương tự) trên danh sách lệnh của router. Ví dụ trên router Netgear, nhấp UPnP trên danh sách lệnh nằm ở phía bên trái trang web.

2. Mở và áp dụng xác lập UPnP

   Nhấp hộp kiểm Enable UPnP (hoặc mở UPnP bằng cách sử dụng lệnh hoặc lựa chọn thích hợp trên trang cấu hình của router). Sau khi chọn tùy chọn cho UPnP nhấp Apply (hoặc một xác lập tương tự) để áp dụng xác lập vào cấu hình của router.

   Một số router WiFi cũng cho phép truy cập thêm các xác lập liên quan đến UPnP chẳng hạn như Advertisement Time to Live (time to live có thể được viết tắt thành TTL), những xác lập này có thể được để lại tại các thiết lập mặc định của chúng trong hầu hết các trường hợp. Một số router chỉ cho phép bạn mở UPnP và không cho phép bạn điều chỉnh thời hạn (period) quảng cáo hoặc thời gian để sống (time to live).

   UPnP Portmap Table trình bày các địa chỉ IP của những máy tính truy cập router và cũng hiển thị các cổng đã được mở bởi các máy tính trên mạng. Portmap Table không cung cấp dữ liệu về mạng của bạn

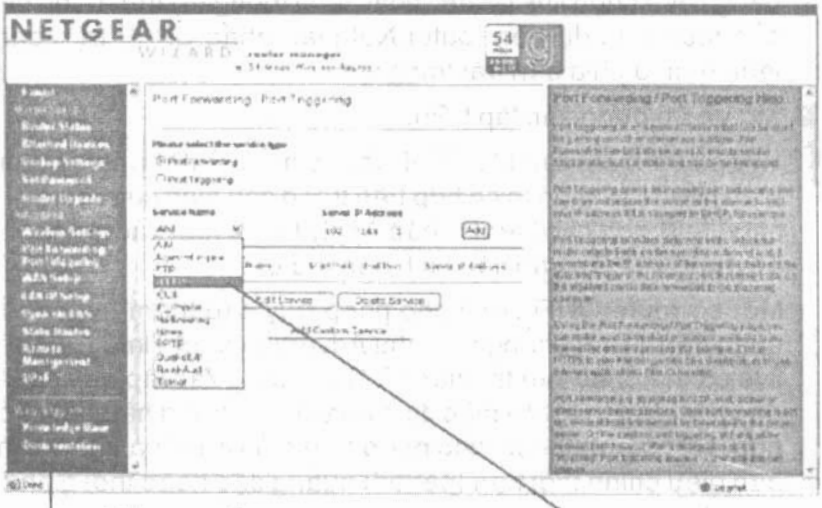
cho đến khi bạn đã cấu hình port forwarding hoặc port triggering trên router (portmap table UPnP không có sẵn trên router).

Ghi chú

Các thiết bị UPnP chẳng hạn như các máy tính sử dụng các thông báo hoặc quảng cáo để cho những máy tính khác biết những dịch vụ mà chúng đang cung cấp, chẳng hạn như một dịch vụ chơi game. Thời hạn quảng cáo cho các UPnP là mức độ thường xuyên mà một router thông báo rằng một dịch vụ cụ thể đang được cung cấp bởi một máy tính trên mạng. Thời hạn mặc định là cách 30 phút. Thời gian quảng cáo (advertisement time to live) được đo bằng các bước nhảy (hop) là số router mà quảng cáo có thể di chuyển qua (nó nhảy từ router này đến router khác) trước khi chúng bị loại bỏ khỏi một router. Đối với hầu hết các mạng nhỏ, các xác lập advertisement period và advertisement time to live mặc định làm việc tốt. Nếu bạn thấy rằng một số dịch vụ đang gặp trục trặc khi kết nối với một dịch vụ nào đó, bạn có thể tăng số bước nhảy cho xác lập time to live.

3. Mở trang cấu hình Port Forwarding/Port Triggering

Chọn link hoặc lệnh Port Forwarding/Port Triggering trên trang cấu hình của router (những lệnh này có thể nằm trên các trang riêng biệt trên một số router, do đó có thể bạn phải chọn Port Triggering, quay trở về lệnh/danh sách cấu hình và sau đó chọn Port Triggering để truy cập đúng các trang) để mở trang cấu hình Port Forwarding/Port Triggering.



4. Cấu hình Port Forwarding

Cấu hình Port Forwarding cho một dịch vụ được cung cấp bởi một máy tính trên mạng, chọn dịch vụ từ danh sách xổ xuống Service Name. Các dịch vụ mà các router cung cấp có thể khác nhau nhưng tất cả chúng đều liệt kê các dịch vụ thường được sử dụng, chẳng hạn như FTP hoặc HTTP, và các game online phổ biến (chẳng hạn như Age of Empires (từ Microsoft) và Quake (từ ID Software). Sau đó nhập octet sau cùng (số cuối cùng) của địa chỉ IP cho máy tính cung cấp dịch vụ. Hãy nhớ, bạn có thể sử dụng lệnh ipconfig trên một máy tính để xác định địa chỉ IP của nó. Sau đó, nhấp Add để thêm tên dịch vụ vào danh sách dịch vụ.

Nếu bạn muốn thêm một dịch vụ tùy ý, nhấp nút Add Custom Service và cung cấp tên của dịch vụ, các số cổng đầu và cuối để mở (đối với một dịch vụ chỉ có một số cổng, nhập số này dưới dạng cổng đầu và cổng cuối). Giao thức vận chuyển cho dịch vụ (TCP hoặc UDP hoặc cả hai) và địa chỉ IP của máy tính trên mạng sẽ cung cấp dịch vụ. Sau đó nhấp Apply. Bạn sẽ được đưa trở về trang cấu hình Port Forwarding/ Port Triggering. Các dịch vụ mà bạn đã thêm xuất hiện trong danh sách dịch vụ.

Bạn có thể chọn những dịch vụ khác từ danh sách dịch vụ thêm các dịch vụ tùy ý khi cần thiết. Hãy nhớ bất cứ lúc nào bạn cấu hình một máy tính để cung cấp một dịch vụ và sau đó cấu hình router để cho phép một cổng mở truy cập dịch vụ đó, bạn đang làm ảnh hưởng tới sự an ninh trên mạng. Về cơ bản, Port Forwarding cung cấp một nối kết ổn định và nhất quán cho một cổng cụ thể mà có thể được sử dụng để xâm nhập mạng.

THỦ THUẬT: Bạn có thể xóa hoặc chỉnh sửa một dịch vụ mà bạn đã thêm vào danh sách dịch vụ. Chọn dịch vụ và sau đó nhấp nút Delete Service để xóa dịch vụ ra khỏi danh sách, nhấp nút Edit Service để thay đổi các tham số dịch vụ chẳng hạn như số cổng và giao thức vận chuyển cho dịch vụ.

---

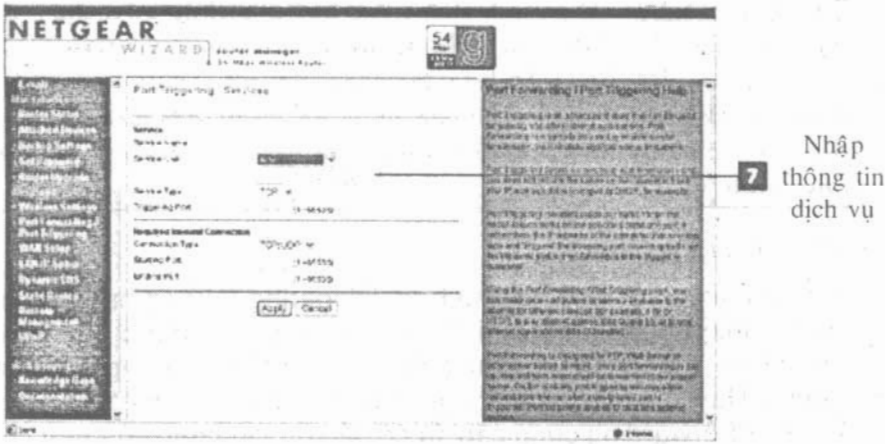
5. Chọn Port Triggering

Để cấu hình một dịch vụ cho Port Triggering (chẳng hạn như một game nhiều người chơi chạy trong các máy tính được nối mạng), chọn Port Triggering trên trang cấu hình Port Forwarding/ Port Triggering. Hãy nhớ rằng Port Triggering tạm thời mở chỉ một cổng trong khi Port Forwarding cung cấp sự có sẵn ổn định hơn của một cổng mở. Rõ ràng port triggering là một cách an toàn hơn để cho phép truy cập một cổng trên một máy tính cung cấp dịch vụ.



6. Thêm một dịch vụ Port Triggering

Bạn đã thấy một số cổng được cấu hình để kích khởi trên router chẳng hạn như dịch vụ điện thoại Dialpad Internet và Starcrafft. Những cổng này được kích khởi bởi vì chúng là các cổng được sử dụng bởi các dịch vụ chơi game phổ biến nhất trên các mạng gia đình. Danh sách thay đổi từ router này đến router khác và cũng phụ thuộc vào khi nào bạn đã mua router. Để thêm một dịch vụ vào danh sách port triggering, nhấp nút Add Service.



7. Nhập thông tin dịch vụ

Trên trang Port Triggering Services (hoặc một trang tương tự trên router), bạn được yêu cầu nhập thông tin liên quan đến dịch vụ chẳng

hạn như giao thức vận chuyển được sử dụng (TCP/UDP) và cổng được sử dụng bởi dịch vụ (thường là một game trực tuyến). Tất cả thông tin mà bạn cần để cấu hình một dịch vụ cho port triggering có sẵn trên website của nhà sản xuất game hoặc dịch vụ. Thông tin được yêu cầu để cấu hình một dịch vụ mới port triggering như sau:

- ***Service Name**: Đây là tên của game.*
- ***Service User**: Tùy chọn mặc định là Any (nghĩa là bất cứ người nào trên Internet có thể truy cập game của bạn trên máy tính mạng) hoặc bạn có thể chọn địa chỉ từ danh sách xổ xuống Service User. Sau đó bạn nhập địa chỉ IP của người dùng dịch vu (người sẽ kết nối với máy tính) trong các hộp địa chỉ.*
- ***Service Type**: Chọn giao thức vận chuyển cho dịch vụ (TCP hoặc UDP).*
- ***Triggering Port**: Đây là cổng ngoại biên cho game. Bạn có thể nhận được cổng ngoại biên cho game từ tài liệu game hoặc website game.*

Ghi chú

Router lắng nghe cổng ngoại biên để tìm lưu lượng từ máy tính chơi game của bạn, khi nó phát hiện sự truyền dữ liệu, nó mở ra cổng nội biên để cho phép giao tiếp từ máy tính bên ngoài mạng.

- ***Connection Type**: Đây là giao thức vận chuyển được sử dụng cho nối kết nội biên. Chọn UDP, TCP hoặc cả hai (UDP/TCP). Thông tin này có sẵn trong tài liệu hoặc website của game.*
- ***Starting Port**: Nhập cổng bắt đầu cho dãy số cổng sẽ được mở trên router cho lưu lượng nội biên. Thông tin này có sẵn trong tài liệu của game hoặc trên website.*
- ***Ending Port**: Nhập cổng kết thúc cho dãy số cổng sẽ được mở trên router cho lưu lượng nội biên. Nếu game sử dụng chỉ một số cổng , nhập số này trong Starting Port hoặc Ending Port.*

Nhấp Apply. Dịch vụ mới được thêm vào danh sách port triggering trên trang Port Forwarding/ Port Triggering.

Bạn có thể thêm dịch vụ khác vào danh sách port triggering khi cần thiết bằng cách lặp lại các bước 5 đến 7.

Chương 9

TẬN DỤNG CÁC HOTSPOT KHÔNG DÂY

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *59. Bàn về các Hotspot không dây*
- *60. Sử dụng Web để định vị các Hotspot*
- *61. Xác định các Hotspot WiFi và kết nối*
- *62. Tinh chỉnh các tham số nối kết Hotspot*
- *63. Bàn về Wardriving*

Việc sở hữu một máy tính notebook có tính năng WiFi sẽ cho phép tận dụng tối đa các nhà hàng, tiệm cà phê, khách sạn và những doanh nghiệp khác vì đây là những nơi thường cung cấp cho khách hàng sự truy cập miễn phí Internet thông qua một Hotspot không dây. Chương này sẽ xem xét các hotspot WiFi là gì cách tìm kiếm và kết nối chúng.

59. Bàn về các Hotspot không dây

Trước khi bạn bắt đầu	Xem thêm
32. Bàn về việc cấu hình Adapter không dây	**Mục 63**
	Mục 76

Sự truy cập công cộng đến Internet thông qua hotspot đã trở thành một công cụ tiếp thị cho những doanh nghiệp và là một thành phần quan trọng của quy hoạch đô thị và nông thôn. Mặc dù nhiều người trong chúng ta tận dụng các hotspot WiFi trong các tiệm cà phê và khách sạn (một hotspot là một doanh nghiệp hoặc cơ sở khác cung cấp nối kết "công cộng" đến Internet thông qua một access point WiFi), nhưng các mạng WiFi được xây dựng cho toàn bộ các thành phố chẳng hạn như San Francisco cũng được thực thi trong các dãy núi Appalachia ở vùng nông thôn bởi các cơ quan phi lợi nhuận.

Đối với tính có sẵn của các hotspot WiFi, nhiều doanh nghiệp bây giờ cung cấp sự truy cập không dây miễn phí đến Internet. Tất cả những gì bạn phải làm là khởi động máy tính notebook có tính năng WiFi trong phạm vi giới hạn của doanh nghiệp và kết nối với access point thông qua WiFi.

THUẬT NGỮ CHÍNH

Hotspot. Một điểm kết nối với Internet được cung cấp bởi một doanh nghiệp hoặc cơ sở khác. Điểm kết nối thường là một router WiFi hoặc access point được cung cấp bởi một doanh nghiệp cụ thể chẳng hạn như một tiệm cà phê hoặc khách sạn.

Một số doanh nghiệp cung cấp sự truy cập "hoàn toàn miễn phí" đến Internet thông qua một hotspot WiFi; những doanh nghiệp khác đòi hỏi bạn đăng ký một nhà cung cấp cụ thể để sử dụng hotspot trong các cơ sở của họ hoặc trả tiền cho dịch vụ theo giờ (các tiệm cà phê Internet thường tính phí cho các nối kết WiFi). Ví dụ, Starbucks đòi hỏi bạn đăng ký dịch vụ Hotspot T-Mobile nếu bạn muốn kết nối với Internet trong khi nhấm nháp ly cà phê.

Tài nguyên Web

http://www.starbucks.com/retail/wireless.asp.

Không phải mọi địa điểm Starbucks đều cung cấp các nối kết WiFi. Để biết thêm thông tin về Starbucks, dịch vụ hotspot T-Mobile tại Startbucks, và một bộ định vị để tìm các vị trí Starbucks cung cấp website, hãy đi đến website này.

Rõ ràng, một số doanh nghiệp cung cấp sự truy cập WiFi như là một ưu đãi cho các khách hàng của mình và sử dụng nối kết WiFi làm phương tiện để đưa bạn vào cửa sao cho bạn sẽ mua sản phẩm mà họ bán (chẳng hạn như một phòng khách sạn). Nhiều khách du lịch kinh doanh mong đợi các khách sạn cung cấp các hotspot WiFi có các nối kết Internet tốc độ cao. Các khách sạn cung cấp hotspot WiFi thường dùng phương pháp bảo vệ bằng password để ngăn những người bên ngoài khách sạn ngốn hết tất cả băng thông WiFi vốn dành riêng cho các khách hàng của khách sạn. Những người ở khách sạn được cung cấp một tên đăng nhập người dùng và password hàng ngày để họ có thể kết nối với hotspot WiFi.

Tuy nhiên, nhiều doanh nghiệp không đòi hỏi một sự (logon) để kết nối với WiFi. Bạn có thể đi vào cơ sở, mua phần cơm trưa của mình và kết nối với hotspot WiFi bằng việc cho phép adapter WiFi của bạn phát hiện tín hiệu không dây gần nhất (và mạnh nhất). Như bạn biết, các access point WiFi (chẳng hạn như các access point được lắp sẵn vào các router WiFi) cung cấp một phạm vi hoạt động hơn 100 feet, do đó bạn có thể thật sự đỗ xe trong khu vực đỗ xe của một doanh nghiệp cung cấp hotspot WiFi và kết nối mà không đi vào doanh nghiệp hoặc mua một thứ nào đó. Lẫn nữa các hotspot WiFi do các doanh nghiệp cung cấp được xem là những công cụ tiếp thị, do đó nếu bạn cảm thấy có lỗi, đôi khi bạn có thể muốn hoàn trả cho doanh nghiệp bằng cách mua bất cứ những gì mà nó bán.

Các tốc độ nối kết Hotspot

Khi bạn sử dụng một hotspot WiFi để kết nối với Internet, bạn có thể ngạc nhiên trước thông lượng thật sự mà bạn được cung cấp. Hầu hết các adapter WiFi 802.11g cung cấp một tốc độ nối kết tiềm năng là 56Mbps; một số adapter nổi tiếng cung cấp các tốc độ nối kết có thể có là 108Mbps. Trên mạng WiFi gia đình của bạn, bạn có thể nhận ra các tốc độ tối đa nếu bạn có một router cho phép tốc độ kết nối là 56Mbps trở lên.

Tuy nhiên, bạn sẽ thấy rằng các hotspot WiFi cung cấp ít băng thông hơn nhiều bởi vì mục đích của hotspot là kết nối với Internet chứ không phải cung cấp băng thông để nối mạng cục bộ.

Các hotspot không nhất thiết cung cấp cho bạn thông lượng tối đa vốn có thể được nhận biết bởi adapter WiFi.



Thậm chí 10 (tốc độ cho một nối kết 802.11b) hoặc 11Mbps là quá mức cần thiết đối với tốc độ nối kết nếu bạn nghĩ về nó, bởi vì toàn bộ vấn đề của nối kết WiFi là truy cập Internet. Thậm chí nối kết Internet nhanh nhất hiếm khi vượt quá 700Kbps, do đó nối kết 11Mbps thật sự nhiều hơn mức để tận dụng đầy đủ băng thông của nối kết Internet mà hotspot cung cấp.

An ninh hotspot

Bởi vì nhiều hotspot công cộng cung cấp cho bất cứ người nào sự truy cập Internet, cho nên an ninh của dữ liệu trên một nối kết như vậy có thể là một vấn đề. Nếu người nào đó cũng được nối kết với hotspot đang giám sát mạng bằng cách sử dụng phần mềm nghe lén nhằm thu thập các gói dữ liệu, bạn có thể truyền phát thông tin quan trọng vào tay của những người sẽ sử dụng nó không cho mục đích tốt đẹp gì cả.

Ghé tạt vào một địa điểm phục vụ cơm trưa có cung cấp hotspot và ăn bữa cơm trưa trong khi trả hóa đơn trực tuyến trên Internet thì cực kỳ thỏa đáng.

Tuy nhiên, dữ liệu của bạn có thể di chuyển trên mạng WiFi không được bảo vệ. Các hotspot WiFi không nhất thiết cung cấp bất kỳ chiến lược mã hóa hoặc an ninh.

Do đó, sự thật là bạn nhận được những gì bạn trả tiền. Các hotspot yêu cầu trả tiền cho dịch vụ chẳng hạn như nối kết T-Mobile thường thấy trong nhiều tiệm cà phê Starbucks tận dụng sự xác thực người dùng (user authentication) và giao thức an ninh WPA. Nếu bạn không cần phải trả tiền để truy cập hotspot, hãy giả định nối kết không an toàn và sử dụng nối kết Internet của bạn thông qua nối kết đó một cách thích hợp. Trong hầu hết các trường hợp, khi bạn thiết lập một nối kết với một mạng WiFi không an toàn, một thông báo mở ra cho bạn biết rằng nối kết WiFi không được bảo vệ an toàn, kết nối mà bản thân bạn phải gánh lấy mọi rủi ro.

Một vấn đề an ninh tiềm ẩn khác khi bạn sử dụng các hotspot công cộng là những xác lập trên máy tính của bạn liên quan đến việc chia sẻ file và máy in. Nếu bạn chia sẻ các file và máy in trên mạng gia đình của bạn, dịch vụ File and Print Sharing for Microsoft Networks sẽ được mở trên máy tính của bạn. Do đó, bất kỳ người nào kết nối với cùng một hotspot khi bạn có thể duyệt tìm các máy tính được kết nối và cố truy cập bất kỳ folder chia sẻ trên các máy tính được kết nối với nó. Bạn nên tắt dịch vụ File and Print Sharing for Microsoft Networks trên máy tính khi bạn sử dụng các dịch vụ công cộng để kết nối với Internet. Xem mục 40 để biết các bước để mở/tắt dịch vụ này.



Tắt dịch vụ File and Print Sharing for Microsoft Networks khi bạn sử dụng các File and Print Sharing for Microsoft Networks WiFi.

Ghi chú

Nếu bạn phải tiến hành các giao dịch và truyền dữ liệu quan trọng khác trên các hotspot công cộng, bạn có thể xem xét một sản phẩm phần mềm giúp bảo vệ an toàn dữ liệu của bạn. Có một số sản phẩm trên thị trường. Ví dụ, kiểm tra http://www.jiwire.com/spotlock.htm. JiWire cung cấp một sản phẩm an ninh

WiFi có tên là Spotlock, vốn mã hóa dữ liệu di chuyển qua lại máy tính khi bạn sử dụng một nối kết hotspot WiFi công cộng.

60. Sử dụng Web để định vị các Hotspot

Trước khi bạn bắt đầu

59. Bàn về các hotspot không dây

Bạn có thể sử dụng Web để định vị các hotspot WiFi trong khu vực của bạn. Việc tìm kiếm trực tuyến trước khi rời khỏi nhà sẽ loại bỏ nhu cầu lái xe xung quanh để cố kết nối với các hotspot. Nó cũng cho bạn biết các hotspot "công cộng" có sẵn thay vì các hotspot vốn là các mạng WiFi riêng không được bảo vệ. Các hotspot mà các quán cà phê, khách sạn và những doanh nghiệp khác được thiết kế để giải quyết nhiều kết nối trên các mạng của họ. Các mạng WiFi riêng không được bảo vệ chỉ mở rộng cho nối kết bởi vì mạng đã không được bảo vệ an toàn bởi nhà quản trị mạng. Các hotspot công cộng mong đợi bạn kết nối; các mạng riêng không an toàn không mong đợi bạn kết nối (và bạn không nên kết nối với các mạng riêng không an toàn mà bạn phát hiện; việc làm như vậy thì không đúng nguyên tắc và có thể bất hợp pháp trong một số trường hợp).

Bởi vì các trang tài nguyên liệt kê các hotspot dường như đến và đi trên web, bạn nên định kỳ tìm kiếm bằng cách sử dụng bộ máy tìm kiếm ưa thích để định vị các danh sách hotspot cập nhật nhất trong khu vực của bạn hoặc trong một khu vực mà bạn sẽ ghé thăm hoặc đi qua.

1. Tìm kiếm các hotspot WiFi

   Mở trình duyệt Web và định hướng sang trang tìm kiếm ưa thích. Nhập từ tìm kiếm hotspot WiFi và chạy cuộc tìm kiếm.

2. Chọn link hotspot List

   Một số kết quả sẽ được liệt kê khi bạn tiến hành tìm kiếm. Nhấp một trong các link để truy cập tài nguyên đó. Ví dụ, bạn có thể chọn kết quả tìm kiếm cho http://www.wififreespot.com/.

2. Chọn một tiểu bang

   Hầu hết các website cung cấp một danh sách các hotspot WiFi sẽ cho phép bạn xem các hotspot theo tiểu bang hoặc có thể cung cấp một bộ máy tìm kiếm nhằm cho phép bạn tìm kiếm theo tiểu bang và thành phố. Trong trường hợp của site www.wififreespot.com, nhấp một tiểu bang cụ thể trong danh sách được cho.

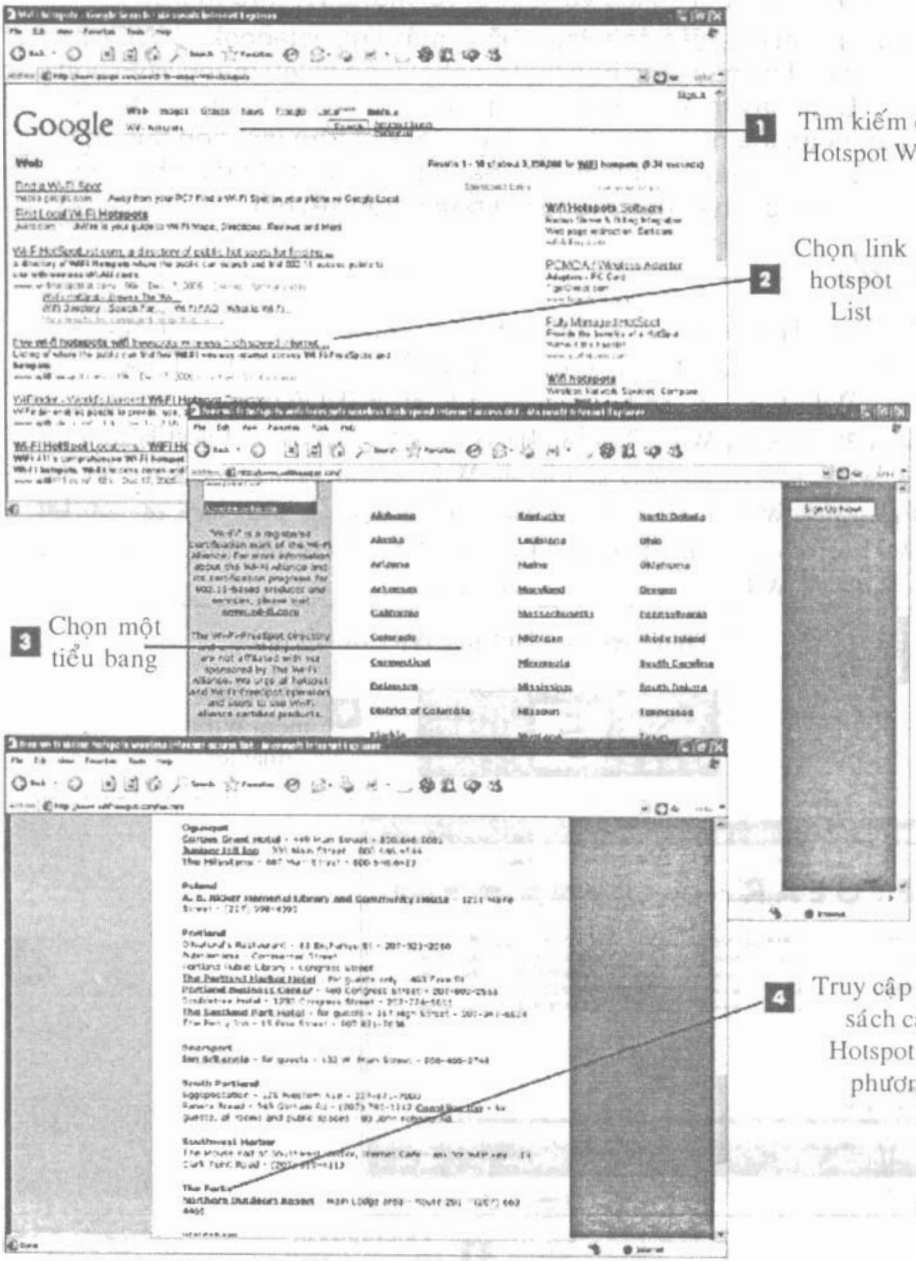
3. Truy cập danh sách Hotspot địa phương

   Các hotspot địa phương được chọn thường được liệt kê theo thành phố. Ví dụ, bạn có thể cuộn xuống danh sách các hotspot trong tiểu bang Maine và xem các hotspot trong thành phố Portland,ME. Thật không may, hầu hết các danh sách hotspot cung cấp chỉ vị trí của

hotspot và thường không chứa thông tin về chính hotspot (chẳng hạn như việc nối kết WiFi có được bảo vệ an toàn hay không và việc nối kết là miễn phí hay tính phí).

Nếu bạn không cảm thấy website đã cung cấp một danh sách đầy đủ hoặc bạn muốn xem những khả năng khác, hãy sử dụng nút Back của trình duyệt để quay trở về danh sách tìm kiếm ban đầu và bắt đầu lại tiến trình.

60. Sử dụng Web để định vị các Hotspot



61. Phát hiện các hotspot WiFi và kết nối

Trước khi bạn bắt đầu

59. Bàn về các hotspot không dây
60. Sử dụng Web để định vị các Hotspot

Sau khi bạn đã sử dụng Web để định vị các hotspot WiFi trong khu vực của bạn (hoặc trong một thành phố mà bạn dự định ghé thăm), bạn có thể thật sự đi đến một vị trí hotspot cụ thể và kết nối với mạng WiFi và Internet.

Khi bạn cố kết nối với một hotspot bằng máy tính notebook có WiFi, bạn có thể ngạc nhiên khi thấy rằng bạn thật sự phát hiện nhiều mạng WiFi hơn bạn mong đợi. Điều này thường đúng trong những khu vực đô thị lớn, nơi một số khách sạn hoặc tòa nhà văn phòng được đặt khít trên một con đường thành phố. Nếu bạn đối mặt với tình huống hạnh phúc là phát hiện nhiều hotspot mạng WiFi, bạn có thể chọn mạng mà bạn muốn kết nối.

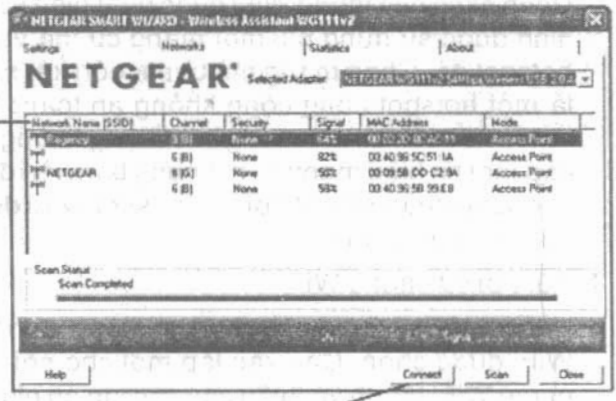
Ghi chú

Nếu bạn không muốn kéo lê theo laptop của bạn để phát hiện các hotspot, các dịch vụ khác có sẵn để phát hiện các hotspot WiFi. Ví dụ, bất kỳ Palm có tính năng WiFi hoặc máy hỗ trợ cá nhân kỹ thuật số (PDA) khác có thể được sử dụng để nối mạng WiFi. Nếu bạn không muốn trả tiền cho một thiết bị xách tay có WiFi, bạn có thể mua một bộ dò WiFi có giá không quá $50. Ví dụ, Kensington WiFi Finder Plus có thể được sử dụng để phát hiện các nối kết WiFi và có giá khoảng $30. Để biết thêm thông tin về các máy tính xách tay và máy dò WiFi, kiểm tra www.handtops.com.

61. Phát hiện các Hotspot WiFi và kết nối







1. Mở phần mềm WiFi Adapter

   Nhấp phải biểu tượng adapter WiFi trong System Tray và chọn Open từ menu ngữ cảnh. Phần mềm của adapter WiFi hoặc Windows Wireless Connection Monitor mở ra.

2. Quét để tìm các Hotspot có sẵn

   Nhấp nút Scan (hoặc chọn một lệnh tương tự) để yêu cầu adapter quét tìm các mạng WiFi có sẵn. Các kết quả xuất hiện trong cửa sổ phần mềm của adapter WiFi.

   Các hotspot miễn phí và luôn có sẵn nếu bạn kết nối không có xác lập an ninh. Do đó bên dưới cột Security, bạn sẽ xác lập None. Nếu một mạng xuất hiện trên danh sách Scan và liệt kê WEP hoặc WPA như là xác lập an ninh, điều này có nghĩa rằng là bạn sẽ cần khóa an ninh chia sẻ hoặc passphrase để kết nối với mạng. Sự hiện diện của an ninh WEP hoặc WPA thường có nghĩa rằng đây là mạng riêng an toàn. Tuy nhiên, trong trường hợp của các hotspot công cộng an toàn chẳng hạn như các hotspot T-Mobile tại các tiệm cà phê Starbucks, bạn thấy mạng được bảo vệ an toàn bằng WPA. Khi bạn đăng ký T-Mobile, bạn được đăng ký tên thông tin và passphrase để cấu hình máy tính WiFi kết nối với máy tính. Do đó mặc dù T-Mobile cung cấp một hotspot công cộng có sẵn tại một số địa điểm, nhưng nó thật sự là một mạng riêng mà bạn phải đăng ký để sử dụng.

   Kênh mà bạn được kết nối cũng xuất hiện trong cửa sổ Scan khi adapter WiFi quét để tìm các nối kết, nó duyệt qua tất cả kênh WiFi có sẵn. Mặc dù thật thú vị khi biết kênh nào mà bạn đang làm việc trên đó, nhưng xác lập channel (kênh) được điều khiển bởi access point WiFi.

3. Chọn mạng WiFi

Danh sách các mạng WiFi được phát hiện cũng sẽ cung cấp kiểu an ninh được sử dụng bởi một mạng cụ thể và cường độ tín hiệu của hotspot đó. Chọn mạng mà bạn muốn kết nối trong trường hợp này là một hotspot công cộng không an toàn. Mặc dù bạn có thể rất muốn kết nối với một trong các mạng không an toàn khác vốn cung cấp một tín hiệu mạnh hơn, nhưng bạn nên để yên các mạng "riêng" không an toàn và kết nối với hotspot WiFi được cung cấp bởi cơ sở nơi ban đang đứng.

4. Kết nối với mạng WiFi

Nhấp nút Connect hoặc chọn một lệnh tương tự để kết nối với mạng WiFi được chọn. Các xác lập mới cho nối kết chẳng hạn như tên mạng WiFi (kênh và thiếu các xác lập an ninh) sẽ được hiệu lực hóa (bạn không cần phải làm bất cứ điều gì để hiệu lực hóa những xác lập này) và sau đó kết nối sẽ trở nên có sẵn. Bây giờ bạn có thể lướt Web hoặc sử dụng công cụ Internet khác chẳng hạn như email khi cần thiết.

62. Điều chỉnh các tham số nối kết Hotspot

Trước khi bạn bắt đầu

59. Bàn về các hotspot không dây

61. Phát hiện các hotspot WiFi và kết nối

Bạn có thể thấy cường độ tín hiệu và chất lượng nối kết của một hotspot WiFi ít lý tưởng hơn. Cường độ tín hiệu có thể thay đổi trong khoảng thời gian kết nối phụ thuộc vào bao nhiêu người dùng khác đang kết nối với hotspot.

Ghi chú

Rất có khả năng bạn đã định vị router WiFi gia đình của bạn và thiết bị khác để được một nối kết và cường độ tín hiệu khi bạn kết nối với mạng WiFi gia đình. Bạn sẽ thấy thế giới của hotspot WiFi không lý tưởng như môi trường gia đình của bạn. Các tín hiệu hotspot WiFi có thể yếu và thậm chí có thể ngắt nối kết trong khi bạn đang online. Nhưng điều đó chung quy là bạn nhận được những gì bạn trả tiền và nhiều hotspot hoàn toàn miễn phí.

Bạn có thể tinh chỉnh một số xác lập nối kết WiFi để tăng tối đa một nối kết yếu. Tuy nhiên, hãy lưu ý một số xác lập nâng cao cho một nối kết WiFi cũng có thể làm cho nối kết bị hỏng. Sau đây là những xác lập mà bạn có thể tinh chỉnh (nếu bạn cẩn thận).

- ***Power Saving***: *Nếu bạn sử dụng một laptop bằng năng lượng pin, bạn nên mở tính năng Power Saving của adapter. Điều này sẽ giúp bảo toàn việc sử dụng năng lượng của adapter và do đó duy trì pin của laptop. Trên adapter USB Netgear WG111, các tùy chọn tiết kiệm điện có thể là Off, Maximum hoặc Dynamic Xác*

lập Maximum tương đương như adapter luôn mở; xác lập dynamic cho phép mở và tắt chế độ tiết kiệm điện. Bạn nên sử dụng xác lập dynamic chỉ trong những tình huống bạn biết pin laptop của bạn yếu. Đôi khi việc sử dụng xác lập dynamic có thể khiến cho adapter rớt nối kết.

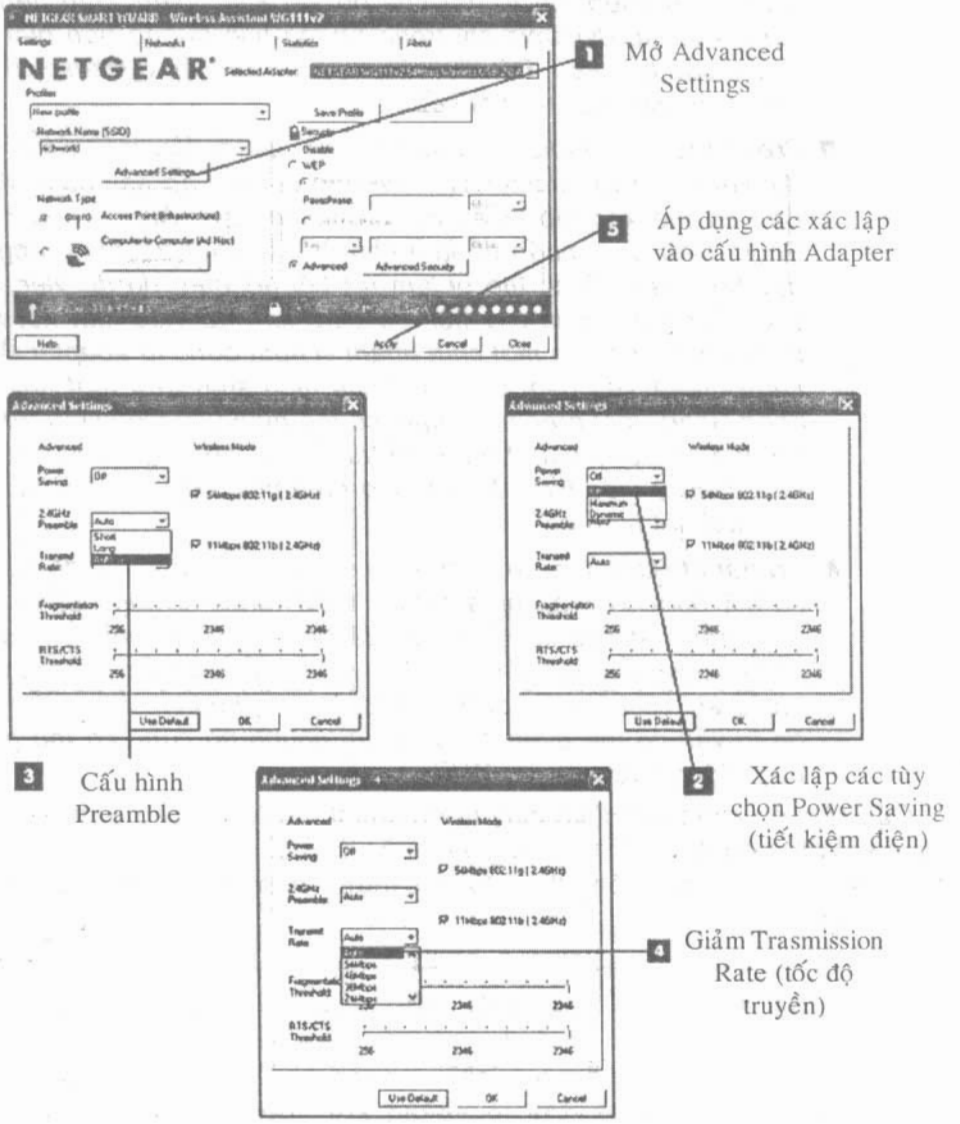
- ***Preamble**: Preamble là dòng bit được gởi ở đầu một cuộc trao đổi kết nối giữa adapter WiFi và một kết nối access point WiFi. Bạn có thể xác lập chiều dài preamble sang Auto, Long hoặc Short. Nếu bạn muốn cố làm cho một nối kết trở nên đáng tin cậy hơn (kết nối có thể bị làm rớt bởi adapter, do đó việc làm cho chúng đáng tin cậy hơn sẽ giúp loại bỏ việc mất kết nối) hoặc có được thêm một chút phạm vi hoạt động từ adapter WiFi, chọn preamble Long. Để tinh chỉnh hiệu suất trên một nối kết, chọn Short (một preamble ngắn có thể mang lại hiệu suất truyền tốt hơn, nghĩa là toàn bộ tốc độ truyền có thể được tăng cho nối kết). Chú ý việc thay đổi xác lập preamble có thể vô hiệu hóa một nối kết hiện có.*
- ***Transmit Rate**: Đối với một adapter WiFi 54Mbps, tốc độ truyền có thể được xác lập giữa 1Mbps và 54Mbps. Trong trường hợp này, hầu hết các xác lập nên để tại Auto. Tuy nhiên, nếu có nhiều access point trên một khu vực nhỏ, bạn có thể thấy sự nhiễu khi cố kết nối với một hotspot địa phương. Việc giảm tốc độ truyền có thể giảm đi sự nhiễu, nhưng nó cũng có thể giảm hoạt động của adapter WiFi.*

Các xác lập khác được tìm thấy trong hộp thoại Advanced Settings cho adapter WiFi nên được để tại các giá trị mặc định của chúng. Việc thay đổi những xác lập này sẽ không thay đổi các thông số hiệu suất hoặc phạm vi hoạt động.

THỦ THUẬT: Các xác lập power-saving, preamble và transfer rate có thể được ghi nhãn một cách khác nhau phụ thuộc vào adapter WiFi mà bạn sử dụng. Các xác lập được thảo luận ở đây là những xác lập được cung cấp cho adapter USB wireless G Netgear WG111. Hãy chắc chắn bạn đọc tài liệu đi kèm adapter WiFi trước khi thay đổi bất kỳ xác lập "nâng cao".

---

62. Điều chỉnh các thông số nối kết Hotspot



1. Mở Advanced Settings

   Nhấp phải biểu tượng adapter WiFi trong System Tray và chọn Open từ menu ngữ cảnh để mở cửa sổ cấu hình của adapter. Nhấp nút Advanced Settings để mở hộp thoại Advanced Settings (lệnh này thay đổi giữa các adapter khác nhau).

2. Xác lập các thiết lập Power Saving (tiết kiệm điện)

   Từ danh sách xổ xuống Power Saving, chọn Maximum hoặc Dynamic. Xác lập mặc định là Off. Xác lập Dynamic tiết kiệm cho bạn nhiều điện nhất nhưng có thể khiến cho adapter ngắt nối kết khi có năng lượng pin rất thấp.

3. Cấu hình Preamble

   Xác định hộp xổ xuống Preamble. Xác lập mặc định là Auto. Nếu bạn muốn tăng phạm vi hoạt động của adapter, thay đổi xác lập này thành Long. Nếu bạn muốn tinh chỉnh hiệu suất, chọn Short.

4. Giảm Transmission Rate (tốc độ truyền)

   Xác định danh sách xổ xuống Transmission Rate. Xác lập mặc định là Auto. Nếu bạn muốn tinh chỉnh nối kết với một hotspot (ví dụ, nếu bạn đã bị ngắt nối kết do sự nhiễu, bạn có thể giảm tốc độ truyền để giảm đi sự nhiễu cục bộ. Đi xuống mỗi lần một lựa chọn menu (ví dụ từ 54Mbps xuống 48Mbps) bởi vì việc giảm tốc độ truyền cũng giảm đi phạm vi hoạt động của adapter.

   Sau khi điều chỉnh các xác lập nâng cao, nhấp OK để quay trở về cửa sổ cấu hình chính.

5. Áp dụng xác lập vào cấu hình Adapter

   Nhấp nút Apply trong cửa sổ các xác lập adapter chính để áp dụng các xác lập nâng cao mới vào cấu hình của adapter WiFi. Nếu bạn thấy việc tinh chỉnh các xác lập đã không thật sự giải quyết bất kỳ vấn đề mà bạn đã gặp phải, hãy quay trở về hộp thoại Advanced Settings và thử các lựa chọn khác. Bạn có thể quay trở về giá trị mặc định nếu cần thiết.

THỦ THUẬT: Nếu việc tinh chỉnh bất kỳ xác lập nâng cao cho adapter WiFi gây ra các sự cố kết nối, hãy trở về hộp thoại Advanced Settings và chọn nút Use Default (hoặc lệnh tương tự) để quay trở về các xác lập nâng cao mặc định của router.

---

63. Bàn về Wardriving

Trước khi bạn bắt đầu	Xem thêm
59. Bàn về các Hotspot không dây	**Mục 76**
61. Phát hiện các hotspot WiFi và kết nối	

Với ngày càng nhiều mạng WiFi công cộng và tư nhân online, những người đam mê máy tính đã bắt đầu định vị và sau đó ánh xạ các nối kết WiFi không an toàn. Tiến trình này được gọi là wardriving, về cơ bản có nghĩa là một người nào đó lái xe xung quanh thành phố hoặc thành thị với một máy tính laptop được bật wireless để cố tìm kiếm và kết nối với các mạng wireless không an toàn. Các wardriving thường trang bị cho phương tiện của họ một anten không dây ngoài để giúp dễ dàng tìm các hotspot không dây. Một thiết bị Global Positioning System (GPS) xách tay cũng thường được sử dụng để giúp lập bản đồ (map), các ranh giới thật sự hotspot, làm cho việc sử dụng hotspot sau này trên Internet trở nên cực kỳ dễ dàng.

Ghi chú

Trong hầu hết các trường hợp, nếu một mạng không an toàn được phát hiện bởi adapter WiFi, bạn sẽ có thể kết nối với nó. Không an toàn, nghĩa là các access point WiFi không sử dụng sự an ninh WEP hoặc WPA. Trong một số trường hợp các hotspot có thể sử dụng sự an ninh thứ cấp vẫn đòi hỏi một tên đăng nhập và password khi bạn cố sử dụng nối kết không an toàn để duyệt Web. Trong trường hợp của các hotspot không an toàn hoặc các mạng WiFi cụ thể được tìm thấy bằng cách sử dụng một tiến trình quét adapter WiFi các mạng an toàn chẳng hạn như một hostpot T-Mobile tại một tiệm cà phê Starbuck sẽ cho thấy mạng đó được bảo vệ an toàn (ví dụ các ký tự WPA sẽ xuất hiện trong cột Security setting cho mạng được phát hiện).

THUẬT NGỮ CHÍNH

Wardriving. Tiến trình lái xe khắp thành phố với mục đích nhận biết và lập bản đồ các hotspot WiFi không an toàn.

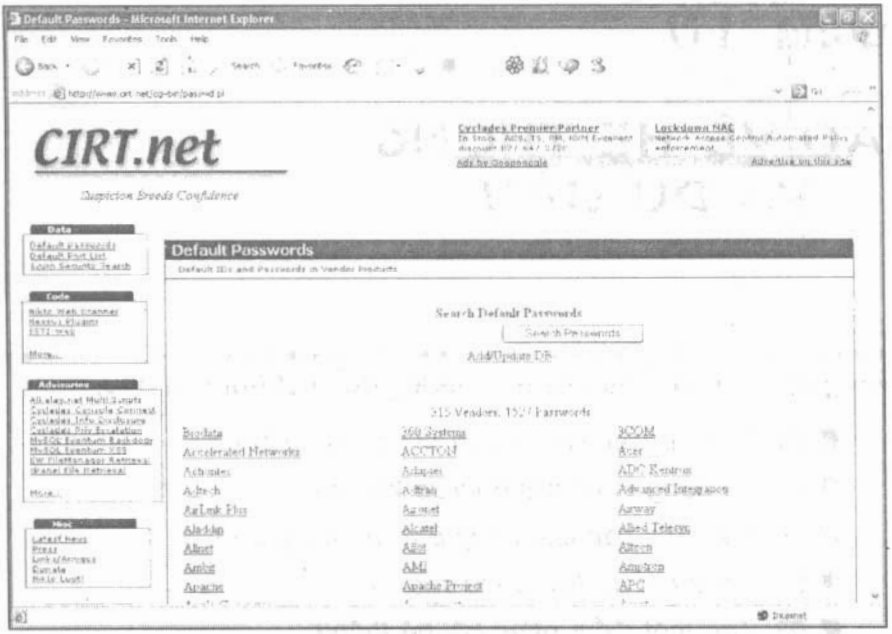
Wardriving đã trở thành một mốt nhất thời đến nỗi nhiều người tham gia để cố định vị các hotspot không dây không an toàn. Những người có thú đam mê này tìm kiếm sự truy cập Internet miễn phí và sẵn sàng chia sẻ thông tin về các hotspot được lập bản đồ với những wardriver khác lên một số site trên Web. Một số wardriver hoặc war walker (nghĩa là bạn đi bộ thay vì lái một phương tiện để phát hiện các hotspot) sử dụng một hệ thống các dấu phấn trên vỉa hè để đánh dấu các tòa nhà có sự truy cập không an toàn và công cộng đến Internet thông qua một hotspot WiFi. Tìm một hình tròn có chữ W bên trong để định vị một hotspot đã được đánh dấu bởi một war walker.

Vấn đề với wardriving là nó sẵn sàng nhận dạng các mạng WiFi không an toàn. Điều này có nghĩa về cơ bản, các hacker đã đưa ra một bản đồ đường dẫn đến các mạng không dây không an toàn. Nếu bạn đã không làm điều này, mối đe dọa mà các wardriver có thể định vị mạng không an toàn của bạn sẽ làm cho bạn bảo vệ an toàn mạng WiFi, đặc biệt nếu bạn sống trong một trung tâm đô thị (nơi wardriving phổ biến hơn) với giao thức WPA. Để biết thêm thông tin về WPA, **xem mục 76** và **mục 78**.

Các wardriver biết rằng cấu hình mặc định cho một access point làm cho cực kỳ dễ nối kết với một mạng không dây vốn truyền phát SSID của nó mà không sử dụng WEP hoặc WPA để bảo vệ an toàn mạng. Thậm chí nếu không có sự truyền phát SSID, các wardriver có thể kết nối với một mạng WiFi không an toàn bằng cách sử dụng SSID mặc định cho các access point phổ biến khác nhau. Ví dụ, SSID mặc định cho một access point được sản xuất bởi Linksys là linksys.

Bạn có thể tìm thấy website kể cả các hotspot không nhất thiết phải được thiết kế để sử dụng công cộng. Các website khác liên quan đến wardriving cung cấp các SSID mặc định, các password mặc định và thông tin khác cho

các router WiFi và access point; ví dụ kiểm tra http://www.cirt.net. Danh sách này cho thấy có 315 nhà cung cấp phần cứng WiFi chẳng hạn như các access point và router WiFi. Mỗi nhà cung cấp có các SSID và password mặc định riêng của nó.



Các site wardriving chẳng hạn như www.cirt.net cung cấp các SSID mặc định và các password mặc định của phần cứng WiFi.

Do đó trong khi các wardriver nói rằng mục đích của wardriving là lập danh mục các hotspot WiFi có sẵn, nhưng wardriving cũng cung cấp thông tin dùng để truy cập các mạng WiFi đã không được bảo vệ an toàn. Có sẵn một số công cụ hack được sử dụng để giám sát lưu lượng mạng và cố phá vỡ sự an ninh của các hotspot WiFi. Hãy tuyệt đối bảo vệ mạng WiFi của bạn khỏi sự truy cập trái phép.

Chương 10

BẢO VỆ HỆ THỐNG VÀ DỮ LIỆU

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *64. Bàn về việc sao lưu và phục hồi dữ liệu*
- *65. Sử dụng Windows Backup Wizard*
- *66. Sử dụng các tính năng Backup nâng cao*
- *67. Phục hồi dữ liệu được sao lưu*
- *68. Tạo một điểm phục hồi hệ thống*
- *69. Phục hồi hệ thống*

Bảo vệ dữ liệu, nghĩa là các tài liệu, hình ảnh và những file quan trọng khác, là một khía cạnh quan trọng trong việc quản lý một máy tính cho dù máy tính đó được kết nối với mạng hay không. Bởi vì chia sẻ các file trên một mạng workgroup làm tăng khả năng một file bị xóa do vô ý, bạn nên sao lưu dự phòng dữ liệu quan trọng trên máy tính. Sau đó, nếu có một sự cố hoặc dữ liệu quan trọng bị mất, bạn có thể phục hồi các file đó.

Và bởi vì các file hệ thống Windows cũng như các file khác có thể bị hỏng hoặc bị nhiễm virus, bạn nên tận dụng tối đa tính năng System Restore của Windows, tính năng này cho phép bạn phục hồi nhanh hệ thống nếu nó bắt đầu bị trục trặc. Chương này sẽ xem xét việc sao lưu dự phòng và phục hồi dữ liệu và sử dụng tính năng System Restore.

64. Bàn về việc sao lưu dự phòng và phục hồi dữ liệu

Trước khi bắt đầu

1. Bàn về môi trường Windows XP
7. Nhận sự trợ giúp trong Windows
60. Ánh xạ một ổ đĩa mạng

Phương pháp hiệu quả nhất để bảo vệ các file quan trọng trên máy tính là sao lưu đều đặn các file này. Bản sao lưu của một folder hoặc ổ đĩa là một file nén có thể phục hồi sang máy tính nếu cần thiết. Bạn có thể sao lưu các file sang các ổ đĩa khác nhau chẳng hạn như một ổ đĩa flash USB hoặc một ổ đĩa sao lưu USB ngoài chuyên dụng. Nhiều ổ đĩa sao lưu ngoài bây giờ cũng cung cấp khả năng kết nối FireWire. FireWire (còn được gọi là IEEE 1394) là một giao diện tốc độ cao có sẵn trên nhiều máy tính mới có khả năng truyền dữ liệu với tốc độ lên đến 800 Mbps.

THUẬT NGỮ CHÍNH

Ổ đĩa Flash. Một ổ đĩa bộ nhớ Flash di động có thể được gắn với một máy tính qua cổng USB. Các ổ đĩa Flash nhỏ và sử dụng một chip để chứa dữ liệu. Chúng cung cấp một cách hoàn hảo để chuyển các lượng dữ liệu giới hạn giữa các máy tính.

Ổ đĩa cứng ngoài. Một thiết bị lưu trữ đĩa cứng ngoài có thể được nối kết với máy tính bằng cách sử dụng một nối kết USB hoặc FireWire. Các ổ đĩa cứng ngoài USB là các ổ đĩa cứng giống như ổ đĩa cứng bên trong máy tính (nghĩa là chúng chứa phương tiện từ xoay với tốc độ cao). Các ổ đĩa cứng đã được điều chỉnh để làm việc trong một case (thùng máy) ngoài và để truyền dữ liệu bằng cách sử dụng một nối kết USB hoặc FireWire.

Bạn có thể sao lưu các file xác lập hệ thống sang một đĩa mềm (nếu bạn có một ổ đĩa mềm trên máy tính). Các file sao lưu dữ liệu được lưu trữ trong một ổ đĩa cục bộ (chẳng hạn như ổ đĩa C:) và bạn có thể sao lưu dữ liệu được lưu trữ trong một máy tính khác trên workgroup chẳng hạn như một share mà bạn đã ánh xạ dưới dạng ổ đĩa. Tuy nhiên, việc đặt bản sao lưu trên máy tính của người khác không nhất thiết có nghĩa là bản sao lưu của bạn an toàn không bị hỏng hoặc bị xóa do vô ý.

Có một bản sao lưu của dữ liệu máy tính sẽ giúp phục hồi dữ liệu nếu dữ liệu tình cờ bị xóa (một sự cố phổ biến với các folder chia sẻ trong một workgroup) hoặc nếu bạn gặp các sự cố phần cứng chẳng hạn như một ổ đĩa cứng bị hỏng. Ví dụ, nếu ổ đĩa cứng bị hỏng, bạn có thể đặt một ổ đĩa cứng mới trong máy tính, cài đặt Windows vào phần mềm khác mà bạn sử dụng rồi sau đó phục hồi các file dữ liệu được sao lưu sang ổ đĩa cứng mới. Tất cả những gì bạn đã mất là thời gian cần để đặt ổ đĩa cứng mới và phục hồi các file. Dữ liệu quan trọng vốn đã được sao lưu cũng được phục hồi sang một máy tính hoàn toàn khác, điều này đặc biệt hữu dụng nếu bạn nâng cấp lên một máy tính mới.

Để sao lưu dữ liệu trên mạng, bạn có hai lựa chọn, các bản sao lưu cục bộ hoặc các bản sao lưu qua mạng WiFi. Bởi vì mạng workgroup là một nhóm các máy tính peer chia sẻ các tài nguyên giữa những máy tính riêng lẻ, các bản sao lưu cục bộ cho phép mỗi người dùng máy tính chọn và sao lưu các file mà mình cảm thấy quan trọng. Sao lưu cục bộ sang một thiết bị sao lưu và được nối trực tiếp với một máy tính là tiến trình khá nhanh và không chiếm

băng thông mạng; việc sao lưu trên mạng có thể làm giảm đi tốc độ mạng.

Lựa chọn còn lại là có một thiết bị trên mạng dành riêng cho tiến trình sao lưu, chẳng hạn như một máy tính được chỉ định là file server hoặc ổ đĩa sao lưu mạng nối trực tiếp với mạng WiFi. Tuy nhiên, nếu bạn sao lưu sang một máy tính khác trên mạng, bạn sẽ xiết chặt khả năng xử lý trên máy tính đó trong quá trình sao lưu. Và bởi vì dữ liệu phải truyền trên mạng, việc sao lưu sẽ mất thời gian hơn sao lưu trên một ổ đĩa được nối kết trực tiếp.

Ví dụ, một ổ đĩa cứng USB được nối trực tiếp có thể cung cấp một tốc độ truyền 480Mbps (Megabit/giây), trong khi mạng WiFi có thể truyền dữ liệu với chỉ tốc độ tối đa 56 Mbps (trừ khi bạn sử dụng một loại công nghệ tăng tốc độ nào đó trên router và các adapter cung cấp thông lượng nhanh hơn nhưng vẫn không nhanh bằng một ổ đĩa được nối kết). Do đó các thiết bị sao lưu được nối kết trực tiếp sẽ luôn nhanh hơn và đáng tin cậy hơn (bởi vì dữ liệu không được gởi qua mạng).

Ghi chú

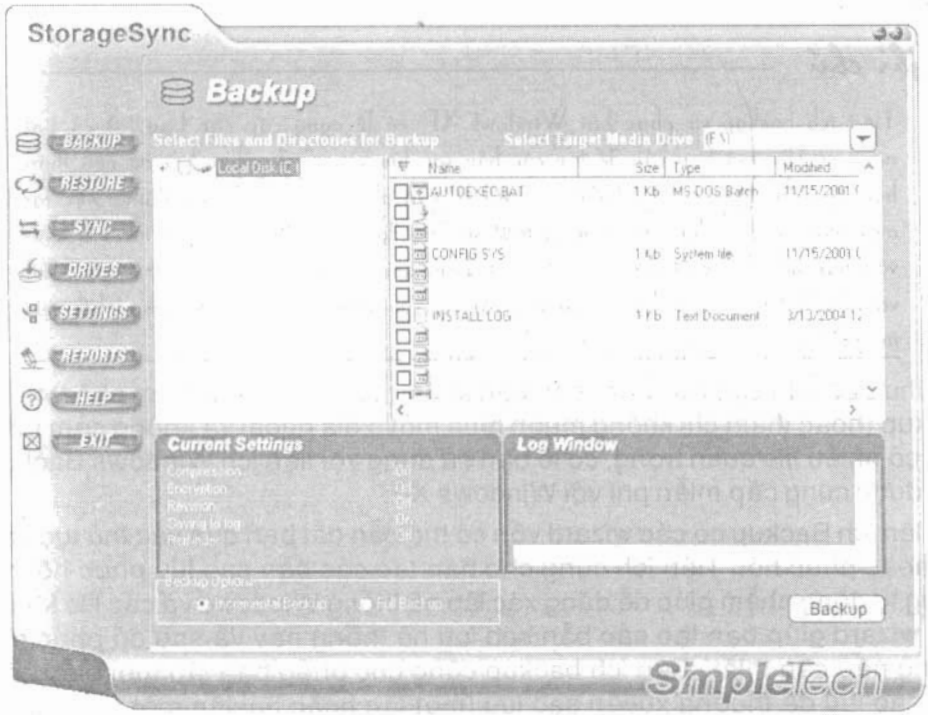
Các mạng máy tính doanh nghiệp lớn sử dụng các file server trung tâm làm nơi lưu trữ file cho tất cả người dùng trên mạng. Sao lưu những file này thì dễ dàng bởi vì nhà quản trị mạng có thể sao lưu toàn bộ server. Nhà quản trị mạng nối trực tiếp một thiết bị sao lưu với file server để bảo đảm sự sao lưu nhanh và không gặp trục trặc bởi vì dữ liệu di chuyển trực tiếp sang thiết bị lưu trữ và không cần phải di chuyển qua mạng. Trong một môi trường workgroup, các file được phân bố qua các máy tính trong workgroup. Do đó mỗi người dùng máy tính nên sao lưu các file riêng của mình; sao lưu các file cục bộ bằng cách sử dụng một ổ đĩa cứng ngoài hoặc một ổ đĩa CD-RW, nghĩa là bạn có được một bản sao lưu khá nhanh và không cần phải ngồi đợi trong khi sao lưu các file gởi trên mạng đến một thiết bị sao lưu trung tâm. Sao lưu qua mạng không phải là cách sử dụng tốt thời gian hoặc tài nguyên mạng và máy tính. Tuy nhiên, nếu cách duy nhất để sao lưu nhiều máy tính được nối mạng là sử dụng một ổ đĩa chia sẻ trên mạng thì hãy làm như vậy, bởi vì việc sao lưu các file cần thiết đối với bạn thì cực kỳ quan trọng.

Có nhiều khả năng phần mềm và phần cứng để sao lưu dữ liệu trên một PC đối với phần mềm sao lưu và thiết bị lưu trữ phần cứng mà bạn sử dụng để chứa các file sao lưu. Đầu tiên, hãy nói về những khả năng phần mềm.

Phần mềm Backup

Mặc dù có nhiều công ty bán các sản phẩm phần mềm sao lưu (backup) khác nhau nhưng trong hầu hết các trường hợp, bạn không cần mua thêm bất kỳ phần mềm nào. Nếu bạn đã mua một ổ đĩa USB ngoài, hầu hết những ổ đĩa này đính kèm phần mềm backup riêng của chúng. Ví dụ, ổ đĩa cứng ngoài SimpleDrive (một ổ đĩa USB) cung cấp phần mềm backup có tên là

StorageSync Professional. Phần mềm backup này cho phép vừa nén vừa mã hóa file cùng với một giao diện rất dễ sử dụng.



Hầu hết các ổ đĩa cứng USB cung cấp phần mềm backup để sao lưu sang ổ đĩa ngoài được nối kết cục bộ.

Khuyết điểm của phần mềm backup đi kèm với các ổ đĩa cứng ngoài USB (chẳng hạn như SimpleDrive) là nó được thiết kế để phát hiện các ổ đĩa được nối với USB và sau đó sử dụng chúng làm đích sao lưu. Phần mềm thường không cung cấp các tùy chọn để sao lưu trên mạng hoặc thậm chí sao lưu sang ổ đĩa cứng cục bộ trên máy tính.

Nếu bạn không muốn sử dụng phần mềm backup đi kèm với một ổ đĩa USB ngoài hoặc nếu bạn đã mua một ổ đĩa không cung cấp phần mềm backup, bạn có thể bắt đầu với tiện ích Windows Backup. Nó là một tiện ích sao lưu và phục hồi đầy đủ và sẽ cung cấp cho bạn hầu hết các tùy chọn mà bạn cần để định kỳ sao lưu các file quan trọng.

Nếu sau khi đã đọc các tác vụ trong chương này bạn muốn mua một gói phần mềm backup "có đầy đủ tính năng hơn", bạn sẽ thấy có sẵn nhiều gói phần mềm backup. Ví dụ, Roxio (www.sonic.com) bán Backup MyPC Deluxe với chức năng sao lưu và phục hồi dữ liệu, nó cũng cung cấp những tính năng nâng cao để phục hồi các hệ điều hành và sao chép các CD và DVD. Phần mềm backup cao cấp hơn chẳng hạn như Norton Ghost (www.symantec.com) được sử dụng để tạo "ảnh" sao lưu của toàn bộ ổ đĩa cứng máy tính. Hầu hết

các ổ đĩa USB ngoài (các ổ đĩa USB dung lượng lớn hơn 60 Gigabyte) đính kèm một CD chứa phần mềm backup và phục hồi mà bạn có thể sử dụng với ổ đĩa.

Ghi chú

Tiện ích backup và phục hồi Windows XP có lẽ cung cấp cho bạn tất cả tính năng cơ bản mà bạn cần để tạo các bản sao lưu và sau đó phục hồi nó nếu thảm họa ập đến. Bạn có thể kiểm tra một số sản phẩm khác có sẵn, nhưng việc tạo một bản sao lưu đơn giản không thật sự bảo đảm chi phí của phần mềm backup và phục hồi đặc biệt. Bạn sẽ phải tự đánh giá những nhu cầu cụ thể của mình và những tính năng khác nhau mà các gói phần mềm backup và phục hồi này mang lại.

Như được đề cập trước đó, nếu bạn không cần phải mua thêm phần mềm backup (hoặc thậm chí không muốn mua một ổ đĩa ngoài và không cảm thấy bạn có nhiều file quan trọng, có lẽ bạn sử dụng vội tiện ích Windows Backup vốn được cung cấp miễn phí với Windows XP.

Tiện ích Backup có các wizard vốn có thể dẫn dắt bạn qua các thủ tục sao lưu hoặc phục hồi. Tiện ích cũng cho bạn tạo các bản sao lưu phục hồi hệ thống tự động nhằm giúp dễ dàng xác lập hệ thống Windows và các file khác. Một wizard giúp bạn tạo các bản sao lưu hệ thống này và sau đó phục hồi chúng nếu cần thiết. Tiện ích backup cũng cho phép bạn lập thời biểu các bản sao lưu để thường xuyên sao lưu (một lần hoặc hai lần một tuần hoặc thường xuyên hơn nếu cần thiết).

THỦ THUẬT: Vấn đề lớn nhất với các tiện ích chẳng hạn như tiện ích Windows Backup là người ta không sử dụng chúng. Khi hệ thống của họ bị đổ vỡ, họ than vãn về việc họ đã không bao giờ sao lưu các file quan trọng của mình.

Khi hầu hết người ta nghĩ về việc sao lưu hệ thống của mình, họ giả định rằng họ phải để yên máy tính trong khi tiến trình sao lưu đang xảy ra. Tuy nhiên, tiện ích backup của Windows XP tạo một bản sao volume shadow của dữ liệu khi nó tạo bản sao lưu. Điều này có nghĩa các file được sao lưu trên volume đã xác định, nghĩa là trên ổ đĩa cứng hoặc vị trí khác nào đó) là những bản sao có trạng thái hiện hành của các file. Chỉ có các file mà bạn mở và làm việc thật sự được sao lưu hoặc được sao chép trong trạng thái mà tiện ích backup tìm thấy chúng trong quá trình sao lưu. Ví dụ, nếu bạn gõ nhập một bức thư cho Microsoft Word và đã hoàn thành 2/3 bức thư (và mở file để làm việc) trong khi việc sao lưu xảy ra, 2/3 bức thư được gõ nhập sẽ được lưu trong file sao lưu. Tính năng backup của Windows XP cho bạn sao lưu "thời gian thực" các file mà bạn đã chọn để lưu cho dù chúng hiện đang mở hay không

Phần cứng Backup

Đối với phần cứng mà bạn sẽ cần để lưu trữ các bản sao lưu, những gì bạn thật sự cần phụ thuộc vào số file mà bạn muốn sao lưu. Nếu bạn muốn sao lưu cả một ổ đĩa cứng 100GB, rõ ràng nội dung sẽ không nằm vừa trên một ổ đĩa Flash USB 512MB (ngay cả nếu các file được nén). Các file lưu trữ sao lưu được tạo bởi tiện ích Windows Backup được nén ở một mức độ nhất định để chiếm ít khoảng trống hơn nhưng một số kiểu file, chẳng hạn như các file âm thanh (các file MP3) và các file ảnh kỹ thuật số thật sự không nén bởi vì chúng được lưu theo định dạng mà thường sử dụng một kiểu nén nào đó. Để an toàn (và thực tế), hãy nghĩ về một mối quan hệ một đối một giữa kích cỡ các file cần sao lưu và khoảng trống cần để chứa file sao lưu. Nếu bạn đã sao lưu 20GB dữ liệu, bạn nên có 20GB khoảng trống trở lên trên ổ đĩa mà bạn sẽ sử dụng để lưu trữ bản sao lưu.

THỦ THUẬT: Để xác định kích cỡ của một folder cụ thể (về cơ bản là kích cỡ nội dung của folder), mở My Computer bằng cách nhấp nút Start rồi chọn My Computer, sau đó nhấp đôi ổ đĩa (chẳng hạn như C:) chứa folder mà bạn quan tâm. Nhấp phải folder và chọn Properties từ menu ngữ cảnh. Trên tab General của hộp thoại Properties của folder, số liệu thống kê Size on disk cho bạn số byte mà folder trên ổ đĩa cứng chiếm. Biết kích cỡ của một folder sẽ giúp bạn ước tính lượng khoảng trống mà bạn cần để sao lưu các file trong folder hoặc các folder đó.

Một vấn đề cần xem xét trong việc chọn một thiết bị sao lưu (chẳng hạn như một ổ đĩa cứng USB) là thiết bị phải đủ lớn (xét về khoảng trống đĩa có sẵn) để đáp ứng nhu cầu sao lưu của bạn. Và bởi vì các file có thể được sao lưu trên mạng workgroup Windows, nên hãy xem xét việc mua một thiết bị chia sẻ trên mạng và được sử dụng để sao lưu tất cả file quan trọng từ những máy tính khác nhau trong workgroup. Mặc dù sao lưu trên mạng thì chậm và tốn băng thông mạng, nhưng nó có thể tiện lợi bởi vì mọi người trên mạng có thể sử dụng ổ đĩa mạng. Nếu sự tiện lợi quan trọng hơn thời gian và băng thông mạng (bởi vì một bản sao lưu mạng vừa chậm hơn vừa sử dụng băng thông mạng), hãy xem xét một ổ đĩa ngoài có một cổng Ethernet hoặc sử dụng một ổ đĩa cứng của máy tính và một card WiFi làm một file server và nơi lưu trữ. Mỗi cá nhân trên mạng có thể sao lưu các file quan trọng trên một thiết bị chia sẻ vốn được host bởi một trong các máy tính trên mạng. Để biết thêm chi tiết về việc chia sẻ ổ đĩa và folder trong một workgroup, **xem mục 47**.

Một số công ty chẳng hạn như Seagate và Western Digital bán các ổ đĩa cứng USB. Những ổ đĩa này có dung lượng lên đến 400 GB và cung cấp nhiều khoảng trống để mở rộng không gian lưu trữ có sẵn cho một máy tính và cũng được sử dụng làm các thiết bị sao lưu hoàn hảo. Bởi vì chúng là các ổ đĩa USB, chúng riêng biệt với máy tính thậm chí nếu máy tính bị hỏng, ổ đĩa USB (vốn có nguồn điện riêng của nó) vẫn hoạt động. Điều này có nghĩa nếu các file quan trọng đã được sao lưu sang ổ đĩa USB thì sẽ được phục hồi sang một máy tính khác nếu cần thiết ngay tức thì.



Các ổ đĩa cứng USB chẳng hạn như ổ đĩa Western Digital này là các thiết bị di động có dung lượng lớn, rất hữu dụng cho việc lưu trữ bản sao lưu file máy tính.

Các ổ đĩa cứng USB (các ổ đĩa flash và ổ đĩa cứng thật sự) không phải là những thiết bị duy nhất có sẵn để sao lưu dữ liệu. Một số phần mềm Backup (tuy nhiên không phải tiện ích Windows Backup) cho phép sao lưu dữ liệu sang một đầu ghi CD hoặc DVD trên máy tính. Các ổ băng (như các ổ đĩa sử dụng DAT) và các ổ đĩa có dung lượng lớn chẳng hạn như Zip và Jaz của Iomega (www.iomega.com) là một tùy chọn khác. Bạn có thể tháo phương tiện sao lưu băng hoặc đĩa ra khỏi ổ đĩa và cất giữ nó ở một nơi an toàn. Các công ty lớn thường sử dụng một ổ đĩa băng tốc độ cao nào đó để lưu trữ các file sao lưu bởi vì sau đó các băng có thể mang đến nơi khác để bảo vệ nhằm ngăn ngừa một thảm họa do hỏa hoạn hoặc thiên nhiên. Để sao lưu máy tính gia đình, các ổ đĩa USB có lẽ sử dụng có tính kinh tế nhất và dễ dàng. Bạn sẽ còn phải đem các bản sao của các file sao lưu ra bên ngoài (cách xa nhà bạn), nhưng bạn bảo vệ dữ liệu cá nhân và quan trọng cho máy tính của mình như thế nào là tùy thuộc vào bạn.

Nếu nhu cầu sao lưu của bạn tối thiểu, nghĩa là bạn sao lưu chỉ một vài file quan trọng trong folder My Documents hoặc bạn muốn sao lưu chỉ các file trạng thái hệ thống Windows (các file điều khiển cấu hình Windows), bạn có thể chọn một ổ đĩa flash USB (có sẵn với nhiều kích cỡ khác nhau, điển hình là từ 256MB đến 2GB trở lên).

Các loại sao lưu

Khi bạn sao lưu các file từ máy tính, bạn cần sao lưu chỉ các file mà bạn đã tạo (lý lịch, sổ séc, danh sách thiệp giáng sinh,...). Sao lưu các file phần mềm thì lãng phí thời gian và không gian lưu trữ bởi vì phần mềm luôn có thể cài đặt lại từ các CD phần mềm gốc.

Bạn có thể nghĩ rằng bạn phải sao lưu hoàn toàn tất cả các file mỗi lần bạn chạy tiện ích backup. Tuy nhiên, bạn có thể cấu hình tiện ích backup sao cho nó sao lưu chỉ các file mới hoặc đã thay đổi trong các folder mà bạn đã xác định. Tiện ích Windows backup cho phép bạn tùy biến tiến trình sao lưu và giảm thiểu lượng thời gian cần thiết để sao lưu các file của bạn.

Tóm lại lần đầu tiên bạn sao lưu tất cả file trong folder hoặc các folder mà bạn chọn, đối với các lần sao lưu tiếp theo, bạn sao lưu chỉ các file đã thay đổi hoặc mới. Các loại sao lưu khác nhau được hỗ trợ bởi tiện ích Windows Backup như sau:

- ***Normal backup***: *Loại sao lưu mặc định cho tiện ích Windows Backup. Sử dụng tùy chọn này lần đầu tiên bạn sao lưu các file trên máy tính. Tất cả file được sao lưu trong một tiến trình sao lưu bình thường được tạo thẻ bằng điện tử (với một file switch) là đã được sao lưu. Khi bạn biên tập hoặc chỉnh sửa một file được tạo thẻ là đã sao lưu, thẻ (tag) bị loại bỏ file không còn được tạo thẻ là đã được sao lưu nữa). Việc tạo thẻ cho các file thì quan trọng đối với việc sử dụng các loại sao lưu khác chẳng hạn như daily (hàng ngày) và differential.*

THUẬT NGỮ CHÍNH

Normal backup. Một phương pháp sao lưu tất cả file được chọn sang file lưu trữ và đánh dấu các file là đã được sao lưu.

- ***Daily backup***: *Loại sao lưu này sao chép các folder được chọn sang file sao lưu. Chỉ các file được chỉnh sửa vào ngày đó mới được sao lưu. Những file mới được sao lưu không được đánh dấu là đã được sao lưu. Điều này có nghĩa rằng là nếu bạn đã phục hồi các file được sao lưu gần đây, bạn phải phục hồi các file từ bản sao lưu bình thường và sau đó phục hồi các file từ bản sao lưu hàng ngày.*

THUẬT NGỮ CHÍNH

Daily backup. Một phương pháp sao lưu tất cả file đã thay đổi hoặc mới được tạo vào ngày đó trong các folder được chọn.

- **Differential backup**: *Loại sao lưu này sao chép các file vốn đã thay đổi (nghĩa là các file đã được sao lưu trước đó) hoặc bạn đã tạo kể từ lần sao lưu normal hoặc incremental cuối cùng. Các file không được đánh dấu là đã sao lưu. Loại sao lưu này tương tự như loại sao lưu hàng ngày (daily backup), nhưng nó sao lưu tất cả file được thay đổi và mới được tạo trong các folder được chọn.*

THUẬT NGỮ CHÍNH

Differential backup. Một phương pháp sao lưu tất cả file trong một folder và hầu hết các folder được chọn vốn đã thay đổi hoặc đã được tạo gần đây từ lần sao lưu normal hoặc incremental sau cùng. Loại sao lưu này không "tạo thể" cho các file là đã được sao lưu.

- **Incremential backup**. *Loại sao lưu này sao lưu chỉ các file mới hoặc đã được thay đổi kể từ lần sao lưu normal sau cùng. Các file được sao lưu trong lần sao lưu incremental được đánh dấu là đã được sao lưu nghĩa là thuộc tính archive được loại bỏ ra khỏi file trong tiến trình sao lưu incremental.*

THUẬT NGỮ CHÍNH

Incremental backup. Một phương pháp sao lưu tất cả các file trong một folder hoặc các folder được chọn vốn đã thay đổi hoặc mới được tạo kể từ lần sao lưu normal cuối cùng. File đã sao lưu được tạo thể là đã được sao lưu.

- **Copy backup.** *Loại sao lưu này sao chép tất cả file trong các folder được chọn. Các file được sao chép sang một file lưu trữ cho dù các file đã được sao lưu trước đó hay không.*

THUẬT NGỮ CHÍNH

Copy backup. Một phương pháp sao chép tất cả file trong một folder được chọn bất kể chúng đã được sao lưu trước đó hay không.

Một điểm cuối cùng liên quan đến việc sử dụng tiện ích Windows Backup: Tiện ích này không phải là một phần của bản cài đặt mặc định Windows XP Home Edition. Trong một số trường hợp, tiện ích có lẽ đã được cài đặt trên máy tính. Nhưng điều đó tùy thuộc vào Windows XP Home Edition được nhà sản xuất máy tính cài đặt như thế nào (hoặc nếu bạn đã nâng cấp máy tính lên Windows XP). Để xem tiện ích Backup được cài đặt hay không, nhấp nút Start và chọn All Programs, Accessories, System Tools. Tiện ích Backup xuất hiện dưới dạng một biểu tượng trong folder con System Tools. Nếu bạn không thấy biểu tượng Backup, bạn cần cài đặt tiện ích này.

Chèn CD Windows XP Home Edition vào ổ đĩa CD. Mở My Computer bằng cách nhấp nút Start và sau đó nhấp My Computer. Nhấp phải biểu tượng ổ đĩa CD chứa CD Windows và chọn Explorer từ menu ngữ cảnh để mở CD Windows XP. Nhấp đôi folder VALUEADD để mở nó. Sau đó, nhấp đôi folder MSFT bên trong folder VALUEADD. Nhấp đôi folder NTBACKUP bên trong folder MSFT rồi nhấp đôi biểu tượng cài đặt NTBACKUP. Một wizard cài đặt mở ra, làm theo các bước của wizard này để cài đặt tiện ích backup. Sau đó bạn có thể lấy CD Windows XP ra khỏi ổ đĩa CD. Bây giờ bạn có thể chạy Backup Wizard như được thảo luận trong mục 65.

65. Sử dụng Windows Backup Wizard

Trước khi bạn bắt đầu

64. Bàn về việc sao lưu và phục hồi dữ liệu

Tiện ích Windows Backup hoạt động trong hai chế độ khác nhau, chế độ wizard và chế độ advanced. Khi bạn sử dụng chế độ wizard, tiện ích cung cấp Backup or Restore Wizard vốn dẫn dắt bạn qua tiến trình sao lưu hoặc phục hồi các file của bạn.

Chế độ advanced cho phép bạn điều khiển những xác lập khác nhau liên quan đến tiến trình sao lưu và phục hồi chẳng hạn như chọn kiểu sao lưu (normal, daily hoặc incremental) hoặc chọn không ghi đè các file hiện có khi phục hồi. Chế độ advanced cũng cho bạn khả năng lập thời biểu các tác vụ sao lưu sao cho các bản sao lưu tự động chạy.

Khi bạn chạy tiện ích Backup bằng cách sử dụng tiện ích Backup or Restore Wizard, kiểu mặc định được thực hiện là sao lưu bình thường (normal backup) tất cả các file trong các folder được chọn. Nếu bạn muốn thay đổi kiểu sao lưu lần kế tiếp sao lưu các file (chẳng hạn như thay đổi các file thành incremental), bạn phải sử dụng chế độ advanced.

Khi bạn sử dụng tiện ích Backup từ menu Start, phần mềm quét hệ thống để tìm các ổ đĩa sao lưu, chẳng hạn như các ổ đĩa cứng USB hoặc ổ đĩa flash USB tháo rời được. Hãy chắc chắn ổ đĩa mà bạn muốn sử dụng làm ổ đĩa đích cho file lưu trữ được gắn vào máy tính (chẳng hạn như một ổ đĩa USB ngoài) trước khi khởi động tiện ích backup. Nếu bạn đã sao lưu sang một máy tính trên mạng chia sẻ một ổ đĩa hoặc folder hoặc sao lưu sang một ổ đĩa mạng ngoài, hãy chắc chắn máy tính hoặc ổ đĩa trên mạng có sẵn (miễn là máy tính chia sẻ vị trí sao lưu đang chạy trên mạng).

Bạn có thể sao lưu dữ liệu từ một vị trí mạng sang một ổ đĩa đích trên máy tính mà bạn xác định và bạn cũng có thể sao lưu dữ liệu cục bộ (dữ liệu trên máy tính) qua mạng sang một share hoặc ổ đĩa từ xa. Di chuyển ổ đĩa qua mạng sẽ mất thời gian và bạn sẽ tự quyết định xem việc sao lưu dữ liệu trên mạng hoặc từ máy tính sang một ổ đĩa được nối kết chẳng hạn như một ổ đĩa ngoài USB có phải là tùy chọn tốt hơn hay không.

Tiện ích Backup được thiết kế để chuẩn bị một hệ thống Windows (tuy nhiên không phải Windows XP Home Edition) cho việc phục hồi tự động bằng cách sử dụng Automated System Recovery (ASR) Wizard. Bởi vì tiện ích wizard ban đầu được thiết kế dành cho các phiên bản Windows trước đây, nó không thể phục hồi chính xác các file phục hồi hệ thống sang một máy tính chạy Windows XP Home Edition. Do đó về cơ bản, bạn có thể bỏ qua wizard ASR và hoạch định sử dụng tiện ích System Restore, được thảo luận trong **mục 68** và **mục 69**.

THỦ THUẬT: Nếu bạn muốn tiện ích Backup tự động khởi động trong chế độ advanced vào lần kế tiếp bạn khởi động nó, hãy hủy chọn hộp kiểm Always start in wizard mode trên màn hình wizard ban đầu.

---

65. Sử dụng Windows Backup Wizard

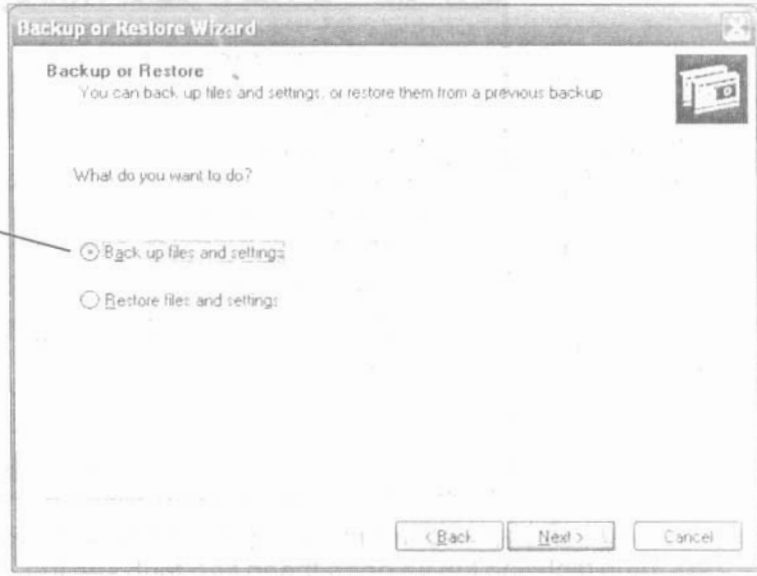


1. Khởi động Backup or Restore Wizard

   Nhấp nút Start và chọn All Programs, Accessories, System Tools. Trong folder System Tools, chọn Backup. Backup or Restore Wizard. Nhấp Next để bỏ qua màn hình ban đầu trên wizard.

2. Chọn một tùy chọn sao lưu File

   Màn hình wizard kế tiếp hỏi bạn có muốn sao lưu hoặc phục hồi các file không. Nhấp nút tùy chọn Back up files and settings và sau đó nhấp Next để đi đến màn hình kế tiếp.



2. Chọn một tùy chọn sao lưu File

3. Chọn những gì cần sao lưu

Màn hình kế tiếp cung cấp các tùy chọn liên quan đến những gì bạn muốn sao lưu. Chọn một trong những tùy chọn sau đây:

- ***My documents and settings***. *Tùy chọn này sao lưu My Documents (kể cả các folder con chẳng hạn như My Pictures) và cũng sao lưu các xác lập liên quan đến Windows desktop và Internet Explorer (chẳng hạn như các cookie và web favorites).*
- ***Everyone's documents and settings***. *Tùy chọn này sao lưu folder My Documents cho tất cả người dùng trên máy tính chẳng hạn như các file hệ thống của họ liên quan đến desktop cookie, ...*
- ***All information on this computer***. *Tùy chọn này tạo một đĩa phục hồi hệ thống và sao lưu tất cả thông tin trên ổ cứng của máy tính. Đĩa phục hồi hệ thống và file sao lưu được tạo từ kiểu sao lưu này có thể được sử dụng để phục hồi hệ thống Windows phòng hờ một sự cố lớn. Kiểu sao lưu này đòi hỏi một ổ đĩa đích có nhiều không gian lưu trữ và cũng mất nhiều thời gian nhất trong các kiểu sao lưu được liệt kê ở đây.*
- ***Let me choose what to back up***. *Tùy chọn này cho phép bạn di chuyển đến thêm một màn hình wizard, nơi bạn có thể xác định ổ đĩa và các folder mà bạn muốn sao lưu. Đây là tùy chọn tốt nhất nếu bạn sao lưu chỉ các folder cụ thể chứa các file quan trọng.*

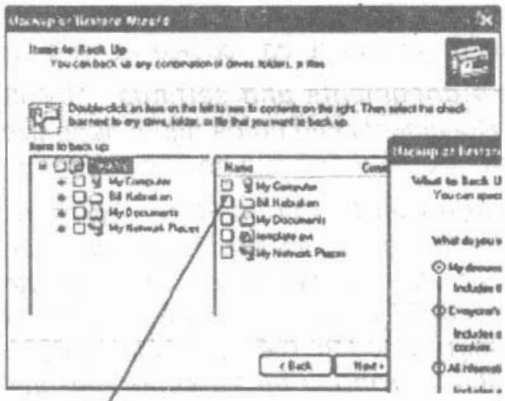


3. Chọn những gì cần sao lưu

Nếu bạn chọn một trong các tùy chọn đầu tiên, đi đến bước 5 để xác định đích sao lưu và hoàn thành tiến trình sao lưu. Nếu bạn chọn tùy chọn All information on this computer, bạn cũng phải có sẵn một đĩa mềm để hoàn tất việc sao lưu. Nếu bạn chọn tùy chọn Let me choose what to back up as your backup, đi đến bước 4.

Sau khi chọn một trong các tùy chọn What to Back Up, nhấp Next để tiếp tục.

4. Chọn các mục cụ thể để sao lưu



4. Chọn các mục cụ thể để sao lưu

Nếu bạn đã chọn tùy chọn Let me choose what to back up ở bước 3, bạn phải chọn các vị trí thật sự trên máy tính mà bạn muốn sao lưu. Trong màn hình Items to Back Up của wizard, chọn hộp kiểm cho ổ đĩa, folder hoặc folder con mà bạn muốn sao lưu. Để mở rộng ổ đĩa hoặc folder để xem nội dung của nó, nhấp dấu cộng nằm bên trái

tên ổ đĩa hoặc folder. Bạn có thể chọn nhiều folder bằng cách chọn các hộp kiểm cho các folder.

Nếu bạn dự định sao lưu dữ liệu từ mạng (nghĩa là bạn sao lưu dữ liệu từ một vị trí từ xa sang một đích sao lưu mà bạn đã xác định ở bước 5), nhấp biểu tượng My Network Places để mở rộng nó và sau đó tìm xem (theo tên) và chọn nó. Bạn thật sự có thể sao lưu bất kỳ file chứa trong một share từ xa. Chọn một folder chia sẻ sẽ sao lưu dữ liệu trên mạng. Do đó hãy nhớ rằng việc sao lưu dữ liệu qua mạng sẽ mất nhiều thời gian hơn sao lưu sang một thiết bị backup được nối kết trực tiếp.

Cho dù bạn sao lưu dữ liệu cục bộ hoặc dữ liệu trong một share, hãy nhớ đặt một dấu kiểm kế bên folder, share hoặc tên file. Khi bạn hoàn tất chọn lựa, nhấp Next để tiếp tục.

5. Chọn đích sao lưu và hoàn tất việc sao lưu

Màn hình kế tiếp cung cấp một hộp danh sách xổ xuống Choose a place to save your backup, mà bạn có thể sử dụng để xác định ổ đĩa đích (chẳng hạn như ổ đĩa USB) hoặc vị trí khác để sao lưu. Hoặc, nhấp nút Browse và duyệt sang vị trí sẽ lưu trữ file sao lưu của bạn.

5. Chọn đích sao lưu và hoàn tất việc sao lưu



Nếu bạn muốn sao lưu dữ liệu cục bộ (các ổ đĩa hoặc folder được chọn ở bước 4 được đặt trên máy tính) sang một share mạng từ xa các biểu tượng My Network Places vốn xuất hiện trong hộp thoại Save As (vốn mở ra khi bạn nhấp nút Browse). Tìm và chọn share từ xa trong cửa sổ My Network Places.

Bạn cũng phải xác định tên file cho bản sao lưu. Tên file mặc định là Backup, nhưng bạn nên đặt một tên có tính mô tả hơn (ví dụ bạn có thể đưa vào ngày tháng, chẳng hạn như backup 11-20-05). Sau khi xác định tên file sao lưu và

chọn vị trí để sao lưu, nhấp Next (nếu bạn đã sử dụng tùy chọn Browse, xác định một tên cho file sao lưu và nhấp Save trong hộp thoại Save As để quay trở về wizard). Sau đó, bạn có thể nhấp Next để tiếp tục.

Ghi chú

Phần mềm Backup chẳng hạn như tiện ích Windows XP Backup không thật sự thấy được bất kỳ sự khác biệt giữa các folder cục bộ (trên máy tính) và các folder chia sẻ trên mạng. Điều này có nghĩa bạn có thể sao lưu dữ liệu được đặt từ xa trên mạng chẳng hạn như một share hoặc trên một máy tính khác, bạn cũng có thể sao lưu dữ liệu cục bộ trên một vị trí từ xa trên những máy tính khác.

Một màn hình kế tiếp xuất hiện tổng kết các bước mà bạn đã hoàn tất. Nhấp Next để hoàn tất tiến trình. Hộp thoại Backup Process mở ra, thể hiện tiến độ sao lưu. Khi tiến trình hoàn tất, bạn có thể đóng hộp thoại Backup Process bằng cách nhấp Close. Sau khi sao lưu dữ liệu, bạn an toàn cho đến khi gặp một sự cố; sau đó bạn sẽ phục hồi dữ liệu như được giải thích trong **mục 67**.

THỦ THUẬT: Nếu bạn muốn xem một báo cáo liên quan đến một bản sao lưu mà bạn đã hoàn tất bằng cách sử dụng tiện ích Backup, nhấp nút Report trong hộp thoại Backup Process. Báo cáo cung cấp ngày tháng và thời gian sao lưu (thời gian và ngày tháng bắt đầu và thời gian và ngày tháng kết thúc), tên của file sao lưu được tạo và kiểu sao lưu đã được chạy (chẳng hạn như một normal backup). Báo cáo cũng bao gồm số folder và file được sao lưu. Nó không cung cấp một danh sách các file hoặc folder được sao lưu.

66. Sử dụng các tính năng sao lưu cao cấp

Trước khi bạn bắt đầu

64. Bàn về việc sao lưu và phục hồi dữ liệu

65. Sử dụng Windows Backup Wizard

Tiện ích Windows Backup mang lại nhiều sự dư thừa trong việc chạy các tiến trình sao lưu và phục hồi. Bạn có thể sử dụng Backup or Restore Wizard mở ra khi bạn chọn tiện ích Backup từ menu Start hoặc bạn có thể chọn các xác lập cho các bản sao lưu và phục hồi bằng cách sử dụng tiện ích advanced.

Bạn có thể truy cập chế độ advanced của tiện ích Backup bằng cách sử dụng link Advanced Mode trên màn hình đầu tiên của Backup or Restore Wizard. Chế độ Advanced cho phép truy cập một Backup Wizard (Advanced) và Restore Wizard (Advanced). Hai wizard này cực kỳ giống như Backup or Restore Wizard đã thảo luận trong tác vụ trước. Lợi ích duy nhất của việc sử

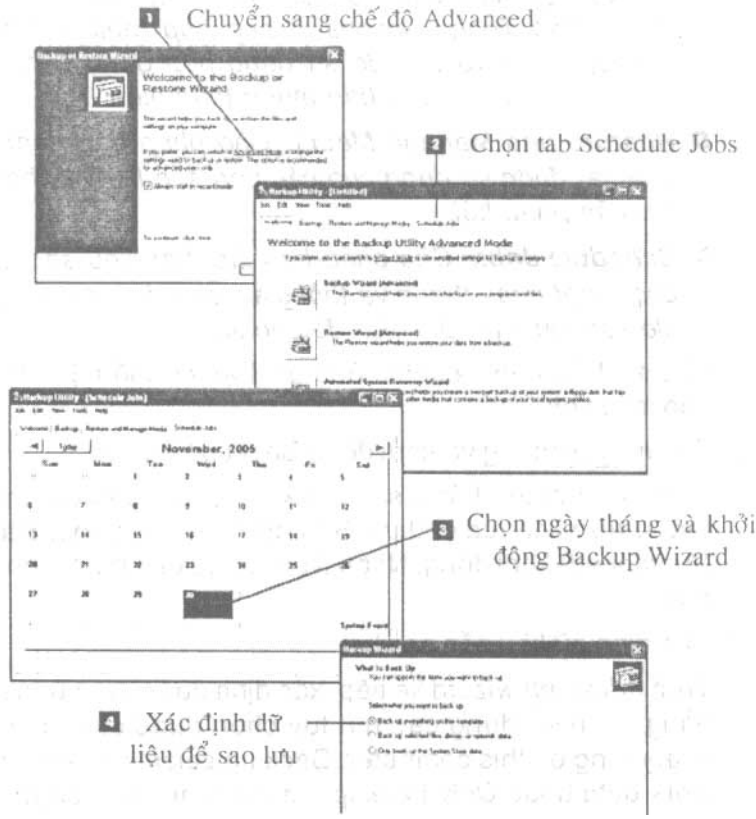
dụng các wizard cao cấp là chúng cho bạn điều khiển việc kiểm tra dữ liệu khi dữ liệu được sao lưu hoặc phục hồi và backup wizard cao cấp cho bạn khả năng chọn kiểu sao lưu mà bạn muốn thực hiện (normal, daily, incremental,...).

Ghi chú

Chế độ advanced cũng cho phép truy cập Automated System Recovery Wizard. Tuy nhiên, tính năng này không làm việc chính xác với Windows XP Home Edition và không nên được sử dụng (mà nên sao lưu thông tin hệ thống bằng cách sử dụng tính năng System Restore; xem mục 68).

Bởi vì các wizard cao cấp cho phép điều khiển thêm một chút một hoạt động sao lưu hoặc phục hồi và bởi vì Automated System Recovery Wizard không ổn định với Windows XP Home Edition, bạn có thể tự hỏi tại sao bạn từng muốn sử dụng chế độ advanced. Giá trị thật sự của chế độ advanced là nó cho phép bạn lập thời biểu các bản sao lưu. Bạn có thể xác định các tham số cho bản sao lưu chẳng hạn như kiểu sao lưu, các file cần sao lưu, đích sao lưu và cũng lập thời biểu một ngày tháng và thời gian khi việc sao lưu xảy ra. Tác vụ này giải thích cách lập thời biểu sao lưu (việc phục hồi được thảo luận trong **mục 67**).

66. Sử dụng các tính năng Backup cao cấp



1. Chuyển sang chế độ Advanced

   Khởi động tiện ích Backup bằng cách nhấp nút Start và chọn All Programs, Accessories, System Tools, Backup. Trên màn hình đầu tiên của Backup or Restore Wizard, nhấp link Advanced Mode. Cửa sổ Backup Advanced Mode mở ra.

2. Chọn tab Schedule Jobs.

   Cửa sổ Advanced Mode của tiên ích backup liệt kê Backup Wizard (Advanced), Restore Wizard (Advanced) và Automated System Recovery Wizard. Sự khác biệt duy nhất giữa các wizard cao cấp được cung cấp trên màn hình này và wizard mà bạn đã sử dụng trong **mục 65** là các wizard cao cấp cho bạn kiểu sao lưu (normal, incremental, daily,...) và chọn hiệu lực hóa dữ liệu sau khi hoàn tất việc sao lưu.

   Bốn tab được cung cấp trên cửa sổ Advanced Mode của tiện ích Backup:

   - ***Welcome:*** *Liệt kê các wizard cao cấp, được khởi động bằng cách nhấp nút thích hợp.*
   - ***Backup:*** *Cho phép xác định các file cần sao lưu và đích sao lưu; cũng cung cấp một nút Start Backup để bắt đầu sao lưu. Bạn có thể xác lập kiểu sao lưu trước khi chạy tiến trình sao lưu bằng cách chọn Tools, Options. Trong hộp thoại Options, chọn tab Backup Type và sau đó sử dụng hộp danh sách xổ xuống để chọn kiểu sao lưu mà bạn muốn thực hiện.*
   - ***Restore and Manage Media:*** *Cho phép bạn chọn phương tiện (media) được sử dụng cho các bản sao lưu và chọn các file sao lưu cần phục hồi.*
   - ***Schedule Jobs:*** *Cho phép bạn lập thời biểu sao lưu bằng cach chọn một ngày tháng và thời gian, sau đó chọn kiểu sao lưu, tên file sao lưu và ổ đĩa đích để sao lưu.*

   Nhấp tab Schedule Jobs. Bây giờ bạn có thể lập thời biểu sao lưu cho máy tính.

3. Chọn ngày tháng và khởi động Backup Wizard.

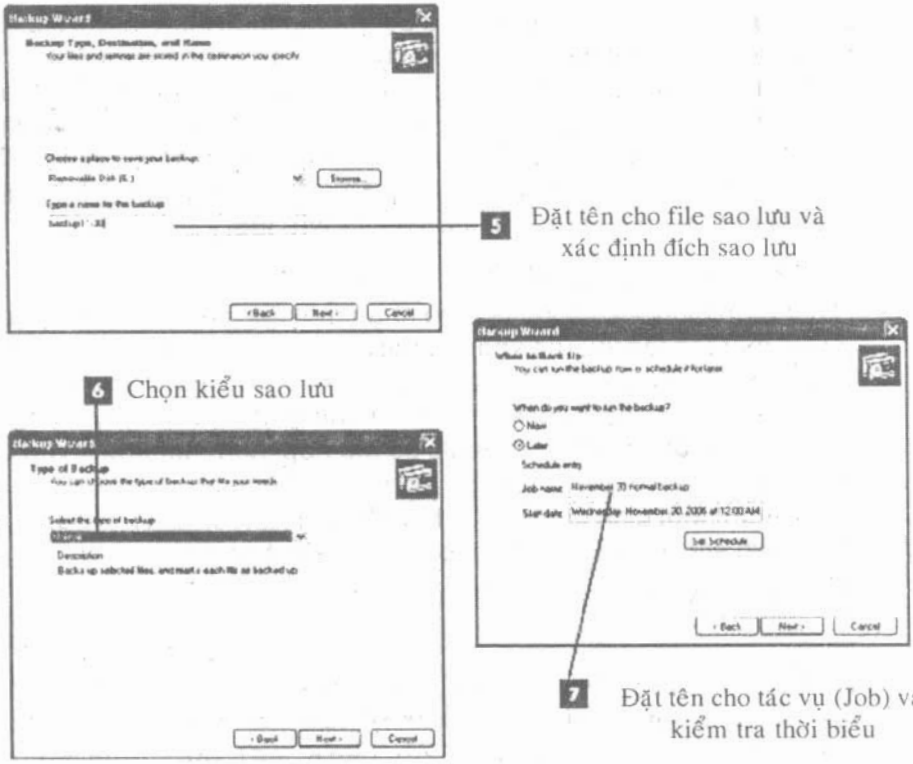
   Chọn một ngày tháng sao lưu kế tiếp bằng cách nhấp một ngày tháng trên lịch (calendar). Sau đó nhấp Add Job. Backup Wizard (Advanced) khởi động. Nhấp Next để bỏ qua màn hình ban đầu wizard.

4. Xác định dữ liệu cần sao lưu

   Trên màn hình wizard kế tiếp, xác định dữ liệu mà bạn muốn sao lưu bằng cách sử dụng các nút tùy chọn được cung cấp (Backup up everything on this computer, Back up selected files, driver hay network data hoặc Only backup the System State data). Nếu bạn đã

chọn tùy chọn Back up selected files, drivers, or network data, nhấp Next và xác định các file bằng cách sử dụng các hộp kiểm ổ đĩa và folder được cung cấp. Sau đó, nhấp Next lần nữa.

5. Đặt tên cho File sao lưu và xác định đích sao lưu



Trên màn hình kế tiếp, cung cấp một tên cho file sao lưu và cũng xác định đích sao lưu.

Sử dụng danh sách xổ xuống Drive để xác định ổ đĩa cho đích sao lưu (tùy chọn này liệt kê bất kỳ ổ đĩa ngoài được nối với máy tính đã được nhận biết khi bạn khởi động tiện ích Backup). Nếu bạn muốn xác định một vị trí từ xa làm đích sao lưu (chẳng hạn như bất kỳ ổ đĩa chia sẻ bao gồm các ổ đĩa flash và share trên những máy tính khác trong workgroup hoặc một folder riêng biệt trên bất kỳ ổ đĩa cục bộ, nhấp nút Browse. Trong hộp thoại Save As vốn mở ra khi bạn nhấp Browse, nhấp biểu tượng My Network Places và sau đó tìm share từ xa mà bạn muốn sử dụng làm đích sao lưu.

Sau khi bạn đặt tên file sao lưu và xác định đích sao lưu (nhấp Save để đóng hộp thoại Save As, nếu bạn đã duyệt tìm một vị trí), nhấp Next để tiếp tục.

6. Chọn kiểu sao lưu

   Trên màn hình kế tiếp, sử dụng danh sách xổ xuống Select the type of backup để xác định kiểu sao lưu mà bạn muốn lập thời biểu; mặc định là Normal. Những tùy chọn khác được mô tả trong phần "các kiểu sao lưu" của **mục 64**.

   Khi bạn đã chọn kiểu sao lưu mà bạn muốn thực hiện, nhấp Next để tiếp tục. Màn hình wizard kế tiếp cung cấp tùy chọn để kiểm tra dữ liệu sau khi sao lưu để có thể quyết định xem việc sao lưu đã thành công hay không. Việc bạn muốn kiểm tra dữ liệu sao lưu hay không tùy thuộc vào bạn; quyết định của bạn thật sự phụ thuộc vào dữ liệu quan trọng đối với bạn như thế nào. Để sử dụng nó, chọn hộp kiểm Verify data after backup và nhấp nó để tiếp tục.

7. Đặt tên cho tác vụ (Job) và kiểm tra thời biểu

   Trên màn hình wizard kế tiếp, gõ nhập một tên job, tên bắt buộc này chỉ là một tên tác vụ, (nó không phải là tên file sao lưu). Job được lập thời biểu để xảy ra sau đó (later) và ngày tháng mà việc sao lưu sẽ được thực hiện được liệt kê. Nếu bạn muốn thay đổi ngày tháng và thời gian, nhấp nút Set Schedule để mở hộp thoại Schedule vốn cho phép ban lập thời biểu một ngày tháng cụ thể hoặc ngày sao lưu lập lại với một thời gian cụ thể. Khi bạn đã xác lập xong thời biểu, kể cả thời gian sao lưu và các lần sao lưu lặp lại, nhấp OK.

   Bạn sẽ quay trở về wizard. Nhấp Next.

THỦ THUẬT: Khi bạn xác lập một thời biểu sao lưu lặp lại bằng cách sử dụng hộp thoại Set Schedule, bạn chọn một ngày cụ thể của tuần rồi chọn một thời gian cụ thể của ngày đó. Chọn một ngày của tuần và thời gian mà bạn sẽ mở máy tính nhưng không cần sử dụng máy tính. Sao lưu các file sẽ làm chậm đi tốc độ hệ thống và làm cho bạn khó tiếp tục làm việc hơn trong khi việc sao lưu đang tiến hành. Lần nữa, chọn một ngày và thời gian mà hệ thống khởi động và chạy nhưng vào lúc mà bạn chắc rằng mình sẽ không sử dụng máy tính.

Màn hình wizard cuối cùng xuất hiện với một bảng tổng kết các xác lập cho tác vụ sao lưu. Nhấp Finish. Bạn quay trở về calendar trên tab Schedule Jobs của tiện ích Backup; job mới xuất hiện dưới dạng một biểu tượng vào ngày tháng mà bạn đã xác định. Khi bạn đã làm việc xong với cửa sổ chế độ advanced, bạn có thể đóng nó lại.

Job sẽ chạy như đã được lập thời biểu. Hãy chắc chắn ổ đĩa mà bạn sử dụng làm đích để sao lưu được nối với hệ thống (chẳng hạn như một ổ đĩa Flash hoặc ổ đĩa USB ngoài được cắm vào một ổ đĩa USB trên máy tính) và

được mở trước khi việc sao lưu được lập thời biểu chạy. Nếu bạn sao lưu trên mạng sang một share từ xa, hãy chắc chắn máy tính mở và có sẵn trên mạng.

THỦ THUẬT: Nếu bạn muốn chỉnh sửa một tác vụ sao lưu mà bạn đã lập thời biểu (biểu tượng của nó xuất hiện trên lịch trên tab Schedule Jobs của cửa sổ tiện ích Backup), nhấp đôi biểu tượng Job trên ngày lịch. Hộp thoại Options cho job mở ra. Để thay đổi thời gian hoặc ngày tháng cho job, nhấp nút Properties trên tab Scheduled Data của hộp thoại Options. Hộp thoại Schedule Job mở ra. Sử dụng tab Schedule để thay đổi ngày tháng hoặc thời gian và sau đó nhấp OK để quay trở về hộp thoại Options cho job được lập thời biểu. Nếu bạn muốn xóa một job được lập thời biểu, nhấp nút Delete trên tab Scheduled data trong hộp thoại Options của job. Job bị xóa khỏi lịch.

67. Phục hồi dữ liệu được sao lưu

Trước khi bạn bắt đầu

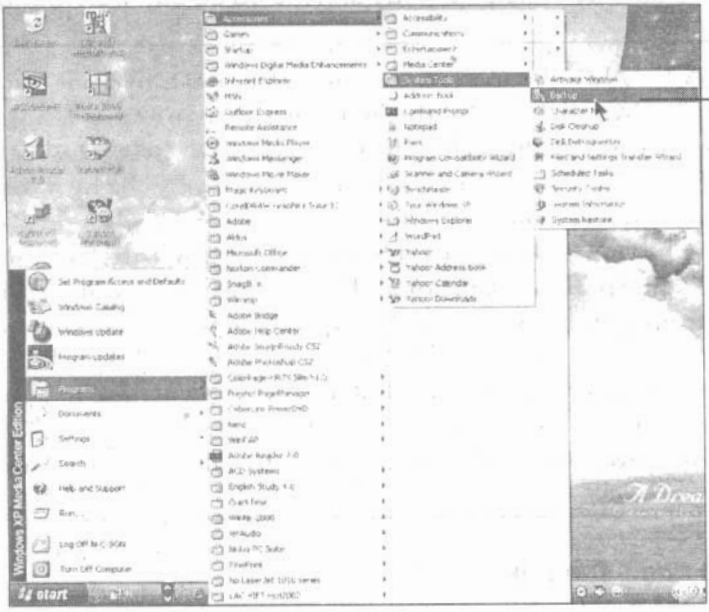
64. Bàn về việc sao lưu và phục hồi dữ liệu

66. Sử dụng Windows Backup Wizard

Cũng có lúc bạn cần thật sự sử dụng các file sao lưu mà bạn đã tạo bằng cách sử dụng tiện ích backup. Có thể bạn phải phục hồi dữ liệu sang máy tính vốn bị mất do một sự cố hệ thống hoặc bị xóa do vô ý (điều này xảy ra quá thường xuyên khi bạn chia sẻ các folder lên một mạng).

Cách dễ nhất để phục hồi dữ liệu sang ổ đĩa cứng của máy tính là sử dụng Backup or Restore Wizard, vốn mở ra khi bạn khởi động tiện ích Backup. Nếu muốn, bạn cũng có thể sử dụng Restore Wizard được cung cấp bởi chế độ advanced của tiện ích backup. Bất kể cách nào bạn chọn, các bước để phục hồi dữ liệu thì tương tự: chỉ định file sao lưu cần sử dụng trong tiến trình phục hồi rồi chỉ định các file thật sự cần phục hồi. Trong những trường hợp bạn đã sử dụng các normal backup và incremental backup, bạn sẽ muốn phục hồi dữ liệu theo thứ tự. Điều này có nghĩa trước tiên bạn phục hồi normal backup gần đây nhất và sau đó phục hồi từng incremental backup (theo thứ tự ngày tháng). Sử dụng chiến lược này để phục hồi dữ liệu sẽ bảo đảm rằng bạn có các phiên bản cập nhật nhất của các file trên máy tính khi việc phục hồi hoàn tất.

67. Phục hồi dữ liệu được sao lưu



1. Khởi động Backup or Restore Wizard

   Nhấp nút Start và chọn All Programs, Accessories, System Tools, Backup. Khi màn hình ban đầu của Backup or Restore Wizard mở ra, nhấp Next để tiếp tục.

2. Chọn Restore.

   Trên màn hình wizard kế tiếp, nhấp nút tùy chọn Restore files and settings. Sau đó nhấp Next để tiếp tục.

3. Chọn File sao lưu

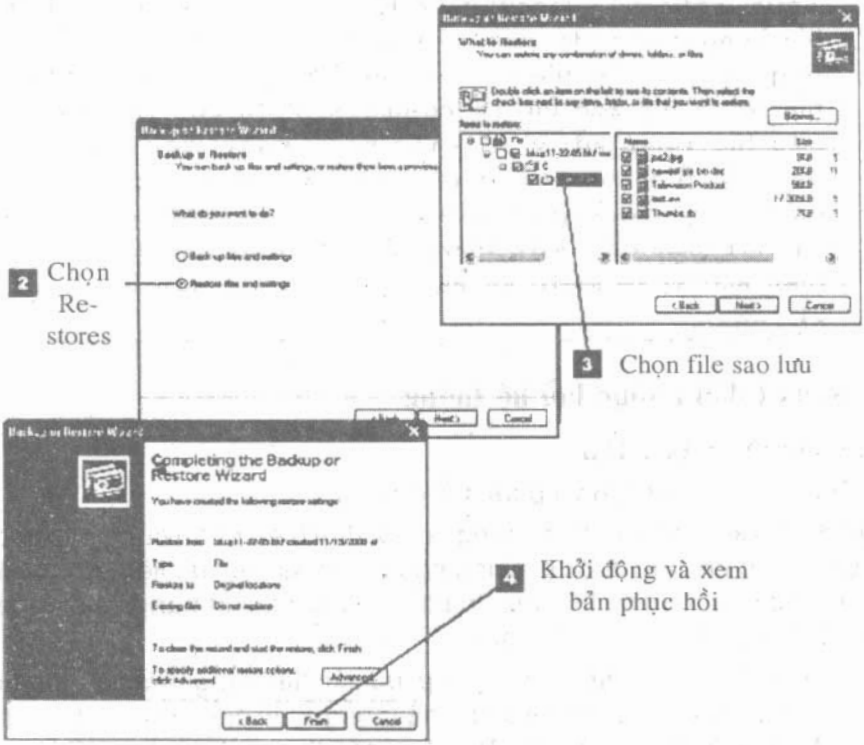
   Trên màn hình wizard kế tiếp, chọn file sao lưu mà bạn muốn phục hồi máy tính.

   Bạn có thể nhấp tiêu đề file và mở rộng nội dung của nó để xem một danh sách các bản sao lưu gần đây. Để xem nội dung của một file sao lưu cụ thể, mở rộng file sao lưu (sử dụng các dấu cộng nằm bên trái các ổ đĩa và folder). Sử dụng hộp kiểm kế bên một mục chẳng hạn như một ổ đĩa, folder hoặc file để xác định các mục mà bạn muốn phục hồi sang máy tính.

   Nếu file sao lưu mà bạn không muốn phục hồi không nằm trên màn hình wizard hoặc trên một share trên một máy tính khác trong workgroup, nhấp nút Browse. Hộp thoại Open Backup File mở ra; nhấp lại Browse để mở hộp thoại Select File to Catalog. Sử dụng biểu tượng My Computer nằm phía bên trái hộp thoại để tìm các file sao lưu trên máy tính. Để định hướng sang các file sao lưu chứa trong các share mạng trên những máy tính khác, nhấp biểu tượng My Net-

work Places. Khi bạn đã tìm thấy file mà bạn muốn mở, chọn nó (cho dù nó nằm trên ổ đĩa cục bộ hoặc một share trên mạng) và nhấp Open trong hộp thoại Select File to Catalog. Sau đó nhấp OK để đóng hộp thoại Open Backup File và quay trở về wizard.

Bây giờ bạn có thể chọn các mục riêng lẻ mà bạn muốn phục hồi bằng cách sử dụng các hộp kiểm thích hợp (hoặc bạn có thể chọn toàn bộ file sao lưu). Khi bạn đã chọn các file cần phục hồi, nhấp Next để tiếp tục.



THỦ THUẬT: Bạn có thể chọn phục hồi tất cả file trong một file sao lưu hoặc nhắm vào bản phục hồi bằng cách chọn các file riêng biệt. Mở rộng file sao lưu bằng cách nhấp đôi nó để xem nội dung của nó. Nếu bạn muốn phục hồi tất cả file trong file sao lưu, chọn hộp kiểm cho file đó. Nếu bạn muốn phục hồi chỉ các file nhất định, tìm các file đó và chọn các hộp kiểm để chọn các file khi cần thiết.

4. Khởi động và xem bản phục hồi

Màn hình wizard cuối cùng cung cấp một bảng tổng kết các xác lập phục hồi. Nhấp nút Finish để bắt đầu phục hồi. Hộp thoại Restore

Progress mở ra. Một chỉ báo tiến độ cho bạn biết tiến độ phục hồi. Khi tiến trình hoàn tất, bạn có thể xem một báo cáo cho bản phục hồi bằng cách nhấp nút Restore. Báo cáo cung cấp thời gian bắt đầu và hoàn thành cho tiến trình phục hồi và cũng liệt kê số mục đã được phục hồi (nó không cung cấp một danh sách các folder hoặc file được phục hồi). Để đóng hộp thoại Restore Progress, nhấp nút Close.

THỦ THUẬT: Backup or Restore Wizard phục hồi các file sang các vị trí gốc của chúng theo mặc định. Nó cũng thay thế bất kỳ file mà nó tìm thấy tại vị trí đó bằng các file trong file sao lưu có cùng tên. Nếu bạn muốn phục hồi các file sang một vị trí khác hoặc ngăn việc phục hồi ghi đè các file hiện có, nhấp nút Advanced trên màn hình cuối cùng Backup or Restore Wizard. Hành động này mở ra một loạt các màn hình dẫn dắt bạn qua tiến trình xác định một vị trí khác và chọn các file có nên bị ghi đè hay không.

---

68. Tạo một điểm phục hồi hệ thống

Trước khi bạn bắt đầu

64. Bàn về việc sao lưu và phục hồi dữ liệu

Mặc dù đôi khi các sự cố hệ thống là một dấu hiệu phần cứng sắp bị hỏng (mà bạn không thể làm được gì nhiều ngoài việc sao lưu dữ liệu) nhưng trong nhiều trường hợp, bạn có thể làm cho hệ thống chạy tốt bằng cách sử dụng tính năng Windows System Restore.

Tính năng System Restore cho phép lưu các file trạng thái hệ thống dưới dạng các điểm phục hồi (restore point) hệ thống. Các điểm phục hồi hệ thống được lưu trên hệ thống và sau đó được truy cập theo ngày tháng. Khi bạn bắt đầu gặp một sự cố với hệ thống, bạn có thể sử dụng System Restore để chọn một điểm phục hồi hệ thống từ thời điểm bạn đã không gặp bất kỳ sự cố với máy tính. Phục hồi sang điểm phục hồi hệ thống máy tính có thể giúp làm cho một hệ thống ốm yếu trở nên mạnh khỏe trở lại.

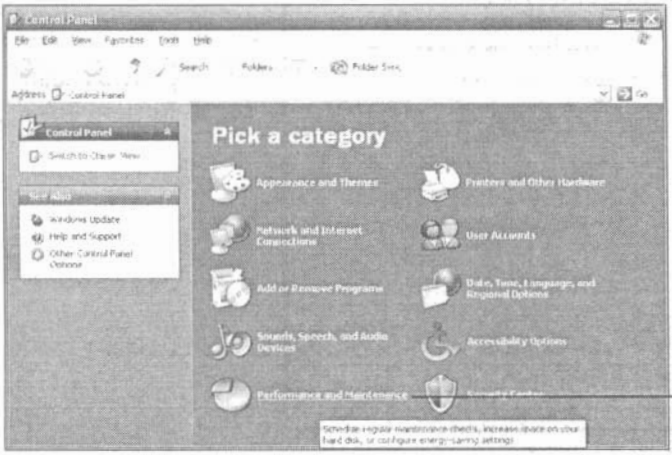
THUẬT NGỮ CHÍNH

Restore point. Một snapshot (ảnh chụp nhanh) của các xác lập và phần mềm được cài đặt của máy tính vốn có thể được phục hồi sang hệ thống. Các restore point (điểm phục hồi) có thể được sử dụng để sửa chữa các sự cố trên hệ thống bằng cách phục hồi máy tính trở về thời điểm trước đó khi nó đã hoạt động tốt.

System Restore tự động lưu các điểm phục hồi hệ thống theo định kỳ. Bạn cũng sẽ thấy các điểm phục hồi hệ thống được thêm vào khi bạn cài đặt một

phần mềm nào đó trên hệ thống. Chú ý rằng System Restore sẽ không giúp chống các virus hoặc spyware hoặc phần mềm xâm nhập khác bởi vì đôi khi những thực thể tấn công này được lưu trong một điểm phục hồi hệ thống. Bạn vẫn phải có một chương trình phần mềm chống virus tốt trên hệ thống.

68. Tạo một điểm phục hồi hệ thống



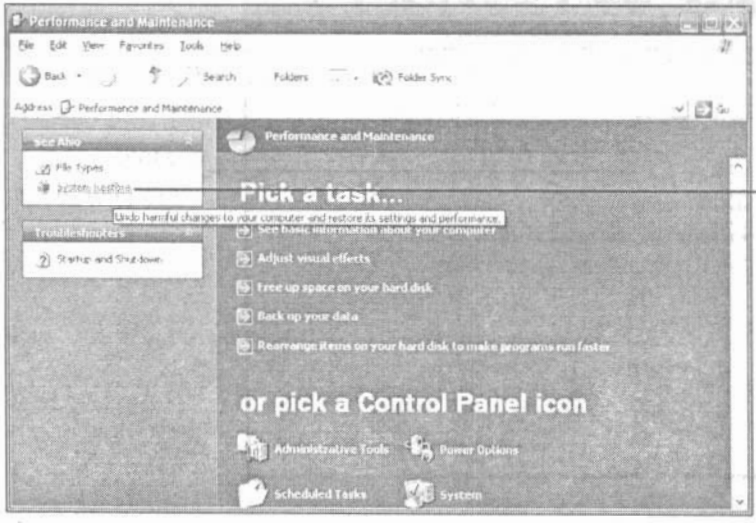
1. Mở cửa sổ Performance and Maintenance của Control Panel

1. Mở cửa sổ Performance and Maintenance của Control Panel

   Mở cửa sổ Control Panel bằng cách nhấp nút Start và sau đó nhấp Control Panel. Chọn biểu tượng Performance and Maintenance để mở cửa sổ Performance and Maintenance.

2. Mở cửa sổ System Restore

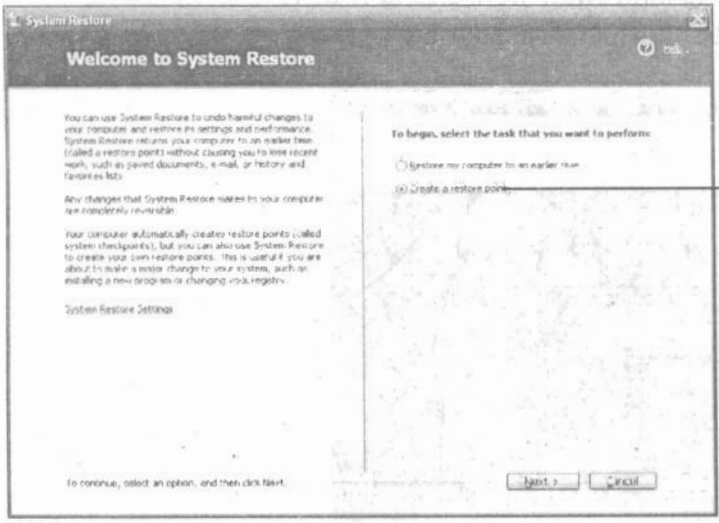
   Ở phía bên trái cửa sổ Performance and Maintenance, nhấp link System Restore. Cửa sổ System Restore mở ra.



2. Mở cửa sổ System Restore

3. Chọn Create Restore Point

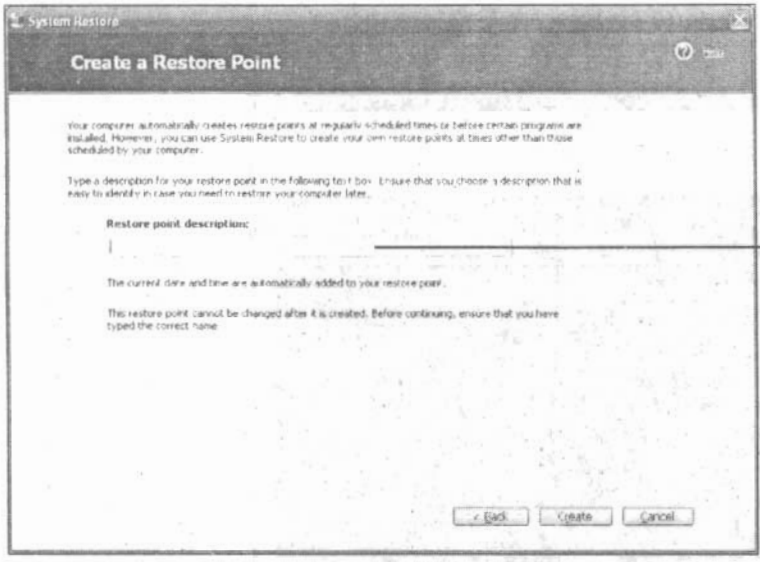
Trong cửa sổ Welcome to System Restore, nhấp nút tùy chọn Create a restore point và sau đó nhấp Next.



3. Chọn Create Restore Point

4. Mô tả và tạo điểm phục hồi

Gõ nhập một phần mô tả cho điểm phục hồi hệ thống. Bạn có thể đưa vào ngày tháng hoặc thông tin hữu ích khác trong phần mô tả khi cần thiết. Bạn có thể sử dụng ngày tháng và text chẳng hạn như before scanner installation để thấy điểm phục hồi đã được tạo trước khi cài đặt một scanner trên máy tính của bạn. Sau khi gõ nhập phần mô tả, nhấp Create.



4. Mô tả và tạo điểm phục hồi

Điểm phục hồi hệ thống sẽ được tạo. Bạn có thể đóng cửa sổ System Restore.

Nếu bạn cần tận dụng điểm phục hồi mà bạn vừa tạo, hãy quay trở về **mục 69** để được trợ giúp.

THỦ THUẬT: Trong một số tình huống chẳng hạn như khi bạn cố loại bỏ một virus hoặc worm đã lây nhiễm sang hệ thống của bạn, các hướng dẫn mà bạn nhận được có thể cho biết rằng bạn nên tắt System Restore để loại bỏ virus hoặc worm. Để tắt System Restore, nhấp nút Start, nhấp phải biểu tượng My Computer và chọn Properties từ menu ngữ cảnh. Trong hộp thoại System Properties, nhấp tab System Restore và sau đó chọn hộp kiểm Turn Off System Restore. Khi bạn đã loại bỏ virus, mở System Restore bằng cách lặp lại các bước này. Để biết thêm chi tiết về việc xử lý các virus, worm và malware khác, xem mục 82.

---

69. Phục hồi hệ thống

Trước khi bạn bắt đầu

68. Tạo một điểm phục hồi hệ thống

Bạn có thể biết được khi nào bạn đang gặp một sự cố hệ thống: hệ thống chạy chậm, bạn nhận được các thông báo lỗi nói rằng các cửa sổ phần mềm cần đóng lại hoặc phần mềm không chịu khởi động. Trong một số trường hợp, Windows không khởi động thành công và hệ thống liên tục khởi động lại.

Trong những trường hợp hệ thống khởi động lại mà không tắt đúng cách, hệ thống sẽ khởi động và cung cấp cho bạn tùy chọn để khởi động Windows trong chế độ Safe Mode. Safe Mode sử dụng một cấu hình Windows cơ bản và không tải tất cả driver mà bạn đã cài đặt cho các thành phần phần cứng khác nhau. Safe Mode hữu dụng bởi vì nó cho phép Windows tải tối thiểu sao cho bạn có thể giải quyết sự cố.

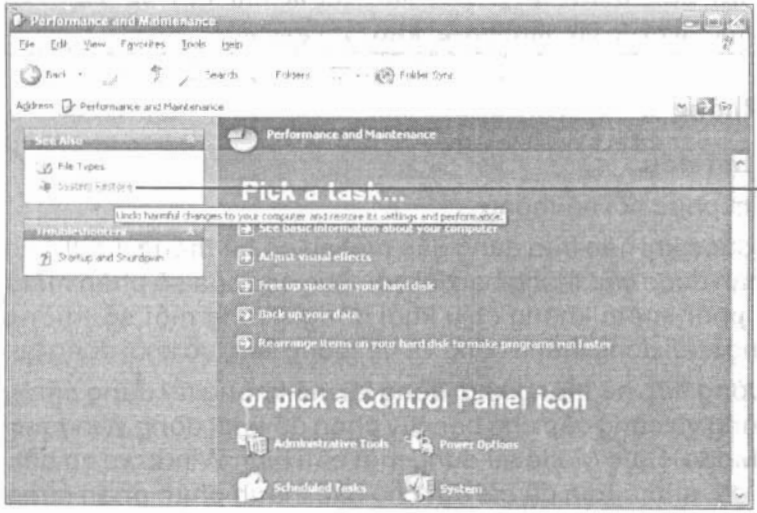
Sau khi hệ thống khởi động và chạy cho dù bạn đã khởi động sang Safe Mode hoặc khởi động Windows một cách bình thường, bạn có thể sử dụng System Restore để phục hồi các file hệ thống trở về thời điểm trước đó. Bạn nên chọn một điểm phục hồi có một ngày tháng trước khi hệ thống đã bắt đầu chạy kém và bạn bắt đầu thấy rằng đã có một loại sự cố nào đó.

Hãy lưu ý rằng về cơ bản System Restore "xác lập lại" hệ thống trở về một thời điểm trước đó. Điều này có nghĩa các driver và những hệ thống xác lập khác được xác lập sang thời điểm trước đó. Có thể bạn phải cài đặt lại các driver cho một số phần cứng nếu bạn sử dụng System Restore. Ví dụ, nếu bạn đã thêm một driver và đã cấu hình một adapter WiFi trên hệ thống, sau đó phải phục hồi hệ thống trở về thời điểm trước đó, bạn sẽ phải cài đặt lại driver cho adapter. Các xác lập mạng bị ảnh hưởng bởi sự phục hồi hệ thống bao gồm

client mạng và các xác lập TCP/IP mặc định. Ví dụ, nếu bạn đã cấu hình hệ thống để sử dụng một địa chỉ IP cụ thể trước đây, nhưng sau đó thay đổi các xác lập để địa chỉ IP được nhận động từ router WiFi, có thể bạn phải "redo" các xác lập gần đây nếu bạn phục hồi sang một thời điểm trước đó vốn đã sử dụng các xác lập. System Restore được thiết kế để làm cho máy tính bị trục trặc khởi động và chạy lại; việc phải cấu hình lại một số xác lập hệ thống thật sự là một cái giá nhỏ phải trả.

Bất kỳ bản cập nhật Windows mà bạn đã thêm vào hệ thống sau ngày tháng của điểm phục hồi cũng được phục hồi trở lại bởi System Restore. Do đó, bạn nên sử dụng System Restore chỉ khi bạn gặp phải một sự cố xảy ra với hệ điều hành Windows. Các file mà bạn đã tạo hoặc đã lưu, chẳng hạn như các bức ảnh mà bạn đã download hoặc những tài liệu mà bạn đã tạo và lưu, không bị ảnh hưởng bởi System Restore; những file này sẽ vẫn nằm trên máy tính nơi bạn đã lưu chúng sau khi chạy System Restore.

69. Phục hồi hệ thống

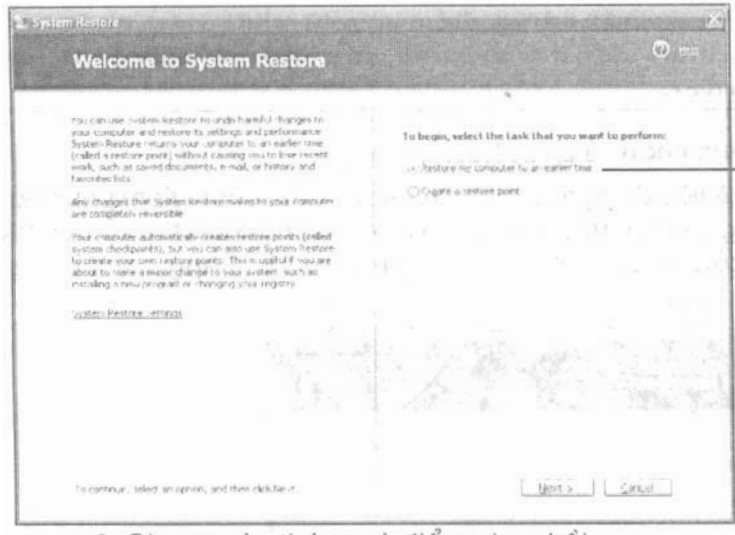


1. Mở cửa sổ System Restore

   Mở cửa sổ Performance and Maintenance bằng cách nhấp nút Start và nhấp Control Panel. Sau đó nhấp biểu tượng Performance and Maintenance để mở cửa sổ Performance and Maintenance. Chọn link System Restore nằm ở phía bên trái cửa sổ để mở cửa sổ System Restore.

2. Chọn Restore My Computer

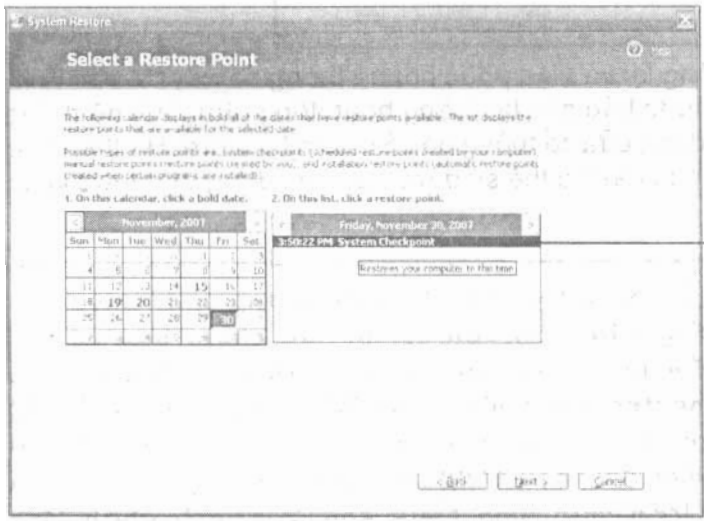
   Nhấp nút tùy chọn Restore my computer to an earlier time và sau đó nhấp Next.



2. Chọn Restore My Computer

3. Chọn ngày tháng và điểm phục hồi

Sử dụng lịch (calendar) để chọn một ngày tháng chứa điểm phục hồi. Ngày tháng có các điểm phục hồi được in đậm trong lưới của lịch. Sau khi chọn một ngày tháng trong lịch, một danh sách các điểm phục hồi được tạo trong ngày đó xuất hiện ở phía bên phải cửa sổ; chọn một trong các điểm phục hồi từ danh sách và sau đó nhấp Next để tiếp tục.



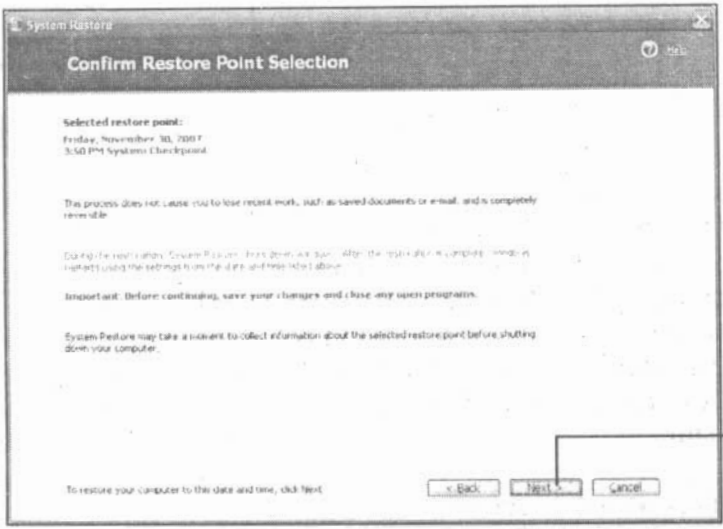
3. Chọn ngày tháng và điểm phục hồi

THỦ THUẬT: Khi có nhiều điểm phục hồi cho một ngày tháng, bạn nên chọn một điểm phục hồi đã được tạo trước khi bạn bắt đầu gặp phải sự cố. Bạn cũng nên chọn điểm phục hồi gần giống với vẻ bề ngoài của sự cố (nhưng

không chứa sự cố) bởi vì điều này từ chối việc phải thực hiện nhiều thay đổi đối với các xác lập hệ thống và bản cài đặt driver.

4. Xác nhận lựa chọn và phục hồi hệ thống

Màn hình kế tiếp đề nghị bạn xác nhận việc lựa chọn điểm phục hồi. Ngày tháng điểm phục hồi và tên điểm phục hồi xuất hiện ở bên trái phía trên cửa sổ System Restore. Khi bạn sẵn sàng bắt đầu tiến trình, nhấp Next.



4. Xác nhận lựa chọn và phục hồi hệ thống

Máy tính sẽ khởi động lại và việc phục hồi hệ thống sẽ xảy ra. Khi Windows khởi động, bạn được báo cho biết rằng hoạt động phục hồi hệ thống hoàn tất. Nhấp OK để đóng cửa sổ thông báo System Restore. Hệ thống sẽ hoàn tất tải và một lần nữa bạn có thể sử dụng các ứng dụng Windows khác nhau.

THỦ THUẬT: Nếu System Restore không giải quyết sự cố với hệ thống của bạn, bạn có hai lựa chọn: bạn có thể chọn một điểm phục hồi khác hoặc bạn có thể sử dụng các troubleshooter khác nhau mà Windows cung cấp để giúp giải quyết các sự cố phần mềm và phần cứng. Nhấp nút Start và sau đó chọn Help and Support. Từ danh sách Pick a Task trên màn hình Help and Support, chọn Use tools to view your computer information and diagnose problems. Tùy chọn này sẽ dẫn dắt bạn qua những khả năng khác nhau để xử lý sự cố mà bạn đang gặp phải với hệ thống.

Nếu bạn gặp phải một sự cố trên một máy tính và bạn thấy rằng một driver phần cứng chẳng hạn như driver cho một adapter mạng WiFi là thủ phạm (và bạn đã thay driver bằng một driver mới của nhà sản xuất), hãy thay driver đó trên bất kỳ máy tính khác trên mạng vốn có thể sử dụng cùng một nhãn hiệu adapter. Thay driver thậm chí nếu máy tính khác dường như không gặp cùng một sự cố mà bạn đã gặp phải trên máy tính ban đầu.

Chương 11

BẢO VỆ AN TOÀN MẠNG KHÔNG DÂY

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *70. Bàn về an ninh mạng cơ bản*
- *71. Bàn về các Firewall*
- *72. Cấu hình các xác lập Firewall của Router*
- *73. Thay đổi xác lập của Router*
- *74. Sao lưu cấu hình Router*
- *75. Tắt các Broadcast Server Set ID (SSID)*
- *76. Bàn về các chiến lược an ninh 802.11*
- *77. Cấu hình an ninh Wired Equivalent Privacy (WEP)*
- *78. Cấu hình an ninh WiFi Protected Access (WPA)*
- *79. Bàn về các địa chỉ MAC giao diện mạng*
- *80. Tạo một danh sách truy cập MAC mạng WiFi*
- *81 Cấu hình Remote Management*

Các mạng WiFi đối mặt với hai con đường xâm nhập tiềm ẩn: bản thân phương tiện WiFi (các tín hiệu vô tuyến) và nối kết Internet thường trực từ mạng gia đình được kết nối với một router DSL hoặc modem băng tần rộng. Bảo vệ mạng không dây (wireless) đòi hỏi bạn bảo vệ an toàn phương tiện mạng và bảo vệ mạng nội bộ khỏi cuộc tấn công bởi người nào đó bên ngoài mạng, nghĩa là người nào đó tấn công mạng trên Internet.

Chương này sẽ trình bày cách bảo vệ an toàn mạng WiFi bằng cách sử dụng chiến lược an ninh wireless vốn sử dụng sự mã hóa và các khóa an ninh. Chương cũng trình bày router WiFi cung cấp một firewall nhằm giúp bảo vệ an toàn mạng khỏi cuộc tấn công bên ngoài.

70. Bàn về an ninh mạng

Trước khi bạn bắt đầu	Xem thêm
11. Tạo một tài khoản người dùng	**Mục 82**
45. Bàn về việc chia sẻ các tài nguyên mạng	
64. Bàn về việc sao lưu và phục hồi dữ liệu	

An ninh mạng bao gồm an ninh cho một mạng workgroup gia đình xoay quanh việc bảo vệ thông tin, nghĩa là dữ liệu mạng. Trên một mạng doanh nghiệp lớn, dữ liệu có thể là các số an sinh xã hội (social security) và các số thẻ tín dụng (credit card) cho hàng ngàn người. Trên mạng gia đình của bạn, dữ liệu có thể là file ngân sách gia đình hoặc một danh sách các địa chỉ cho các thiệp giáng sinh năm nay.

Dữ liệu và những nguồn tài nguyên mạng khác phải được bảo vệ khỏi sự xâm nhập bên trong (chẳng hạn như một người dùng mạng hợp pháp xóa các file quan trọng) và sự xâm nhập bên ngoài (chẳng hạn như một virus máy tính hoặc hacker bất hợp pháp trên Internet). Các mạng doanh nghiệp chi ra vô số tiền cho những biện pháp an ninh khác nhau nhằm bảo vệ mạng của họ. Và mặc dù an ninh mạng cũng quan trọng đối với mạng gia đình, nhưng bạn không cần phải cố lặp lại biện pháp được tiến hành trên các mạng lớn nhằm bảo vệ thông tin quan trọng.

An ninh mạng, thậm chí an ninh trên một mạng gia đình được tập trung vào sự truy cập mạng và sự truy cập nguồn tài nguyên. Để bảo vệ dữ liệu mạng, bạn phải bảo vệ sự an toàn mạng khỏi sự truy cập trái phép (từ bên ngoài) và cũng bảo vệ dữ liệu khi nó được truy cập bởi một người dùng khi nó được cho phép (từ bên trong).

- ***Thay đổi Password router WiFi.*** *Mặc dù điều này không ngăn chặn các cuộc xâm nhập mạng, nhưng việc định kỳ thay đổi password của router sẽ làm cho việc truy cập đến cấu hình của router trở nên an toàn hơn. Các password mặc định để quản lý router thường là những password chung chung quen thuộc chẳng hạn như password; bạn càng sớm thay đổi password đi kèm với router của bạn thì bạn sẽ càng an toàn. Xem mục 73 để biết thêm thông tin.*
- ***Mở/tắt SSID Broadcast:*** *Mặc dù tắt việc truyền phát đại chúng (broadcast), Server Set ID (SSID) hoặc tên mạng bằng router WiFi sử dụng một tín hiệu vô tuyến sẽ không thật sự bảo vệ an toàn mạng khỏi sự xâm nhập bên ngoài, nhưng nó cũng ngăn router WiFi quảng cáo rằng mạng WiFi hiện hữu cho bất kỳ người nào ở trong phạm vi hoạt động vốn đang cố lắng nghe. Để biết thêm thông tin,* ***xem mục 75****.*
- ***Các xác lập Firewall:*** *Một firewall có thể bảo vệ một mạng nội bộ khỏi các cuộc tấn công từ bên ngoài trên nối kết Internet thường trực. Số xác lập firewall có sẵn cho bạn phụ thuộc vào*

router mà bạn đã mua. Để biết thêm thông tin, ***xem mục 71*** *và* ***mục 72.***

- ***Danh sách truy cập card WiFi:*** *Router WiFi có thể cấu hình để chỉ các máy tính vốn có MAC (Media Access Control) hoặc địa chỉ phần cứng cho adapter mạng WiFi của chúng được ghi trong danh sách truy cập của router sẽ được phép kết nối với mạng WiFi. Để biết thêm chi tiết về các địa chỉ MAC và danh sách truy cập card router,* ***xem mục 79*** *và* ***mục 80.***
- ***Xác thực bằng khóa (Key Authentication)*** *và mã hóa dữ liệu (DataEncryption): Một cách để bảo vệ mạng WiFi khỏi sự xâm nhập trên phương tiện mạng (các tín hiệu vô tuyến) là đòi hỏi các máy tính cố kết nối với mạng được xác thực (hoặc được chấp thuận) bởi router WiFi. Dữ liệu di chuyển trên phương tiện mạng vốn bị chặn cũng có thể được bảo vệ nếu trước tiên bạn mã hóa dữ liệu đó. Hầu hết các router WiFi cung cấp hai loại chiến lược an ninh WiFi khác nhau: WEP và WPA. Để biết thêm chi tiết về WEP và WPA,* ***xem mục 76, mục 77*** *và* ***mục 78.***

Khi bạn tận dụng những cách khác nhau để bảo vệ workgroup của bạn khỏi những cuộc tấn công bên ngoài (kể cả các sự cố liên quan đến các virus và malware khác như được giải thích trong **mục 82**), bạn vẫn sẽ cần bảo vệ dữ liệu khỏi những cuộc phá vỡ an ninh bên trong mạng. Đây thường là một vấn đề với việc vô ý xóa các file quan trọng hoặc việc dữ liệu quan trọng đã bị hỏng hoặc không thể sử dụng được.

Trên các mạng lớn, dữ liệu được bảo vệ bởi một nhà quản trị mạng vốn gán cho mỗi người dùng một tập hợp quyền liên quan đến việc nhập dữ liệu. Tuy nhiên, bởi vì dữ liệu chia sẻ được phân tán qua một số máy tính (các folder chia sẻ thường trú trên các máy tính riêng lẻ và được quản lý bởi những người dùng trên các máy tính đó), bạn thật sự không thể xem xét những người dùng trên một workgroup như cách các nhà quả trị có thể kiểm soát những nguồn tài nguyên mạng trên những server tập trung. Do đó bảo vệ dữ liệu khỏi những sự cố vốn phát sinh từ bên trong mạng chẳng hạn như một file bị xóa do vô ý hoặc bị hỏng, được xử lý tốt nhất bằng cách sao lưu dữ liệu trên một máy tính riêng lẻ (**xem mục 64**).

Một vấn đề khác với các mạng workgroup là nếu một folder được chia sẻ trong một workgroup, nó có sẵn cho mọi người trong workgroup đó. Do đó, điều quan trọng là những người dùng trên mạng phải có hành động trách nhiệm khi làm việc với các folder chia sẻ và nội dung của những folder này. Điều cũng quan trọng là mỗi máy tính trên mạng nên được cài sản phẩm phần mềm chống virus cập nhật bởi vì khá dễ lây lan một virus hoặc malware khác trong một môi trường nối mạng workgroup (**xem mục 83** để biết thêm chi tiết về phần mềm chống virus).

71. Bàn về các Firewall

Trước khi bạn bắt đầu	Xem thêm
54. Bàn về việc lọc nội dung và mở các cổng	**Mục 96**
70. Bàn về an ninh mạng cơ bản	**Mục 97**

Các firewall (tường lửa) được thiết kế để đặt giữa mạng và Internet và bảo vệ mạng nội bộ khỏi cuộc tấn công bên ngoài. Các firewall có thể bao gồm phần cứng và phần mềm, chẳng hạn như firewall được cung cấp bởi router WiFi. Các router cũng có thể bao gồm chỉ phần mềm chẳng hạn như Windows Firewall của Windows XP.

Thuật ngữ chính

Firewall. Phần mềm, phần cứng hoặc cả phần mềm lẫn phần cứng được thiết kế để ngăn sự truy cập trái phép đến một mạng riêng. Một firewall có thể được sử dụng để ngăn chặn lưu lượng dữ liệu đến và đi.

Các firewall vốn là một sự kết hợp phần cứng và phần mềm (ví dụ, firewall của router WiFi) có thể kiểm tra các gói dữ liệu rời khỏi và đi vào mạng nội bộ. Đây là lý do tại sao firewall có thể được sử dụng để ngăn chặn sự truy cập đến nội dung web và các dịch vụ như được giải thích trong **mục 54**. Quan trọng hơn, firewall được thiết kế để từ chối những cuộc xâm nhập và cuộc tấn công từ bên ngoài, nghĩa là Internet. Vậy thì làm thế nào firewall xác định được khi nào các gói dữ liệu từ bên ngoài là một cuộc tấn công thay vì lưu lượng dữ liệu thông thường?

Trên thị trường có một số lớn các sản phẩm firewall. Firewall chỉ phần mềm chẳng hạn như Windows Firewall (một sự bổ sung miễn phí cho OS Windows XP) và Zone Alarm (để biết thêm chi tiết về Zone Alamr, một Firewall cá nhân tuyệt vời, xem http://www.zonealarm.com) được thiết kế làm các Firewall cá nhân để bảo vệ máy tính mà chúng được cài đặt trên đó. Các firewall cao cấp hơn được thiết kế để bảo vệ một mạng nhỏ được cài sẵn vào nhiều router WiFi từ các nhà sản xuất chẳng hạn như Linksys và Netgear. Các mạng doanh nghiệp sử dụng các firewall thậm chí tinh vi hơn, phức tạp hơn, được thiết kế để bảo vệ các mạng lớn. Những firewall chuyên dụng này (chúng thường không phục vụ bất kỳ chức năng khác, tương tự như router WiFi đa năng) cung cấp nhiều tùy chọn cấu hình hơn và số xác lập an ninh nhiều hơn so với các firewall đơn giản cho nối mạng gia đình và văn phòng nhỏ.

Firewall được cài sẵn vào router WiFi kiểm tra tất cả lưu lượng dữ liệu đi vào và đi ra mạng cục bộ. Mỗi gói dữ liệu được kiểm tra sao cho nó có thể được kết hợp với một dịch vụ Internet riêng biệt chẳng hạn như http (Web) hoặc FTP (một sự truyền file). Nếu một gói dữ liệu không thể được kết hợp với một nối kết dịch vụ thật sự (chẳng hạn như dịch vụ duyệt Web) đã khởi đầu trên mạng cục bộ, firewall sẽ loại bỏ gói đó và bất kỳ gói khác không thể được kết hợp với một nối kết cụ thể. Do đó, bất kỳ lưu lượng dữ liệu (các gói

thực sự) không khởi nguồn từ một dịch vụ nội bộ sẽ được ngăn chặn bởi firewall.

Kiểu kiểm tra gói (packet) này được gọi là Stateful Packet Inspection (SPI). Đây là lý do tại sao firewall cài sẵn vào router WiFi được gọi là firewall SPI trong tài liệu của router.

THUẬT NGỮ CHÍNH

Stateful Packet Inspection (SPI). Các gói dữ liệu được kiểm tra bởi firewall và được phân tích để quyết định sự kết hợp của chúng với các nối kết mạng và các yêu cầu dịch vụ hiện hành.

Các firewall sử dụng SPI đã quyết định xem các gói dữ liệu đi vào mạng cục bộ từ Internet có phải là kết quả của một cuộc tấn công hoặc xâm nhập tiềm ẩn trên mạng cục bộ hay không. Một trong những kiểu tấn công phổ biến nhất được sử dụng trên Internet là tấn công từ chối dịch vụ: kẻ tấn công làm tràn ngập mạng cục bộ (thường là một máy tính đơn) bởi rất nhiều dữ liệu đến nỗi máy tính hoặc mạng bị quá tải và tắc máy. Kiểu tấn công này được sử dụng liên tục để làm ngừng hoạt động các Web site trên Internet và cũng có thể được sử dụng để phá rối các máy tính và dịch vụ trên một mạng gia đình nhỏ. Một firewall SPI có thể bảo vệ mạng khỏi cuộc tấn công từ chối dịch vụ, do đó nên tận dụng tối đa firewall được cung cấp bởi router firewall.

72. Cấu hình các xác lập firewall của router

Trước khi bạn bắt đầu

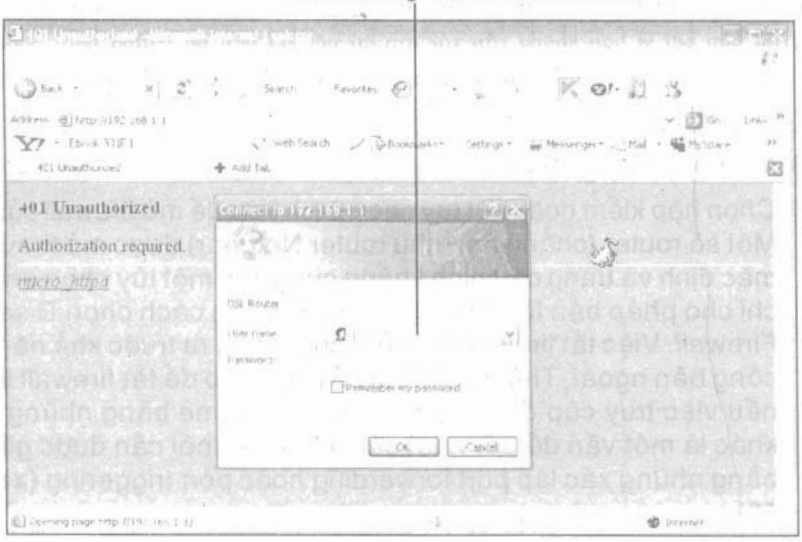
22 Truy cập cấu hình Router

71 Bàn về các Firewall

Các xác lập thực sự có sẵn cho firewall của router WiFi mà bạn đã mua. Trong hầu hết các trường hợp, các xác lập firewall cho router WiFi gia đình khá đơn giản; chúng có thể chỉ cho phép bạn mở hoặc tắt firewall và cấu hình một máy tính để chạy bên ngoài firewall trong những gì được gọi là vùng phi quân sự (DMZ). Các Web server và gaming server có thể chạy trong vùng DMZ, do đó bạn không cần phải sử dụng port forwarding hoặc port triggering để cho phép người dùng bên ngoài mạng kết nối với server. Port forwarding hoặc port triggering được thảo luận trong **mục 58**.

Những xác lập khác mà bạn có thể điều khiển đối với các xác lập firewall liên quan đến việc giao diện router có thể được ping từ Internet hay không (ping hữu dụng như một công cụ chẩn đoán nhưng có thể mở mạng ra trước các cuộc tấn công tiềm ẩn). Lệnh ping được thảo luận trong **mục 96** và **mục 97**. Các xác lập firewall của router cũng có thể cho phép bạn xác lập kích cỡ gói (packet) tối đa vốn có thể được truyền lên mạng. Đây được gọi là kích cỡ Maximum Transmit Unit (MTU); nó thường được cấu hình tại 1500 bytes nhưng được điều chỉnh thành một kích cỡ nhỏ hơn nếu được yêu cầu bởi nhà cung cấp dịch vụ Internet.

72. Cấu hình các xác lập firewall của router



1. Mở trang Web cấu hình router

   Đăng nhập vào router bằng quyền quản trị administrator bằng cách sử dụng trình duyệt Web, gõ nhập URL cho router trong hộp Address của trình duyệt và sau đó cung cấp tên đăng nhập và password cho router khi được nhắc về thông tin này. Bạn có thể tìm thấy URL cho router trong tài liệu đi kèm router; các router cũng thường có một trang khởi động nhanh cung cấp URL hoặc địa chỉ Web cho router cùng với tên đăng nhập và password mặc định. Nếu bạn không truy cập một trong hai trang thông tin này, đi đến Web site của nhà sản xuất router và truy cập trang hỗ trợ của họ tìm các link dẫn đến các trang sản phẩm riêng biệt nơi bạn có thể download tài liệu cho router WiFi.

2. Truy cập các xác lập firewall

   Trên Web site cấu hình của router, chọn link dẫn bạn đến các xác lập firewall của router. Ví dụ, trên trang cấu hình của router WiFi Netgear, các xác lập firewall nằm trên trang WAN Setup do đó nhấp link WAN Setup nằm ở phía bên trái trang. Các trang Setup của mỗi router khác nhau do đó hãy tham khảo tài liệu của router và sách hướng dẫn để biết thêm thông tin.

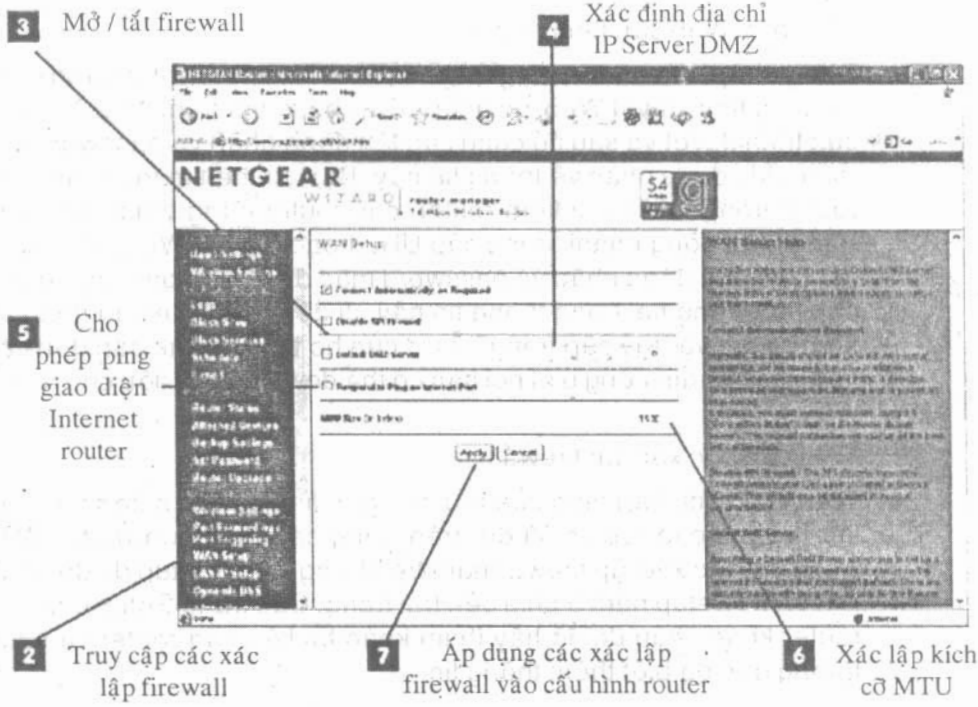
Ghi chú

Các xác lập firewall thường được tìm thấy trên trang cấu hình thiết lập WAN của router bởi vì nối kết WAN (mạng diện rộng) là nối kết với Internet (Internet là mạng diện rộng). Một số router cho phép thay đổi nối kết giữa mạng của bạn

và Internet từ automatic (nghĩa là nó xảy ra tự động qua router) sang manual. Một nối kết manual (thủ công) đòi hỏi bạn sử dụng tính năng thủ công trên router để thiết lập và chạy nối kết Internet. Xác lập automatic connection thật sự tốt hơn bởi vì bạn không cần xác lập lại nối kết nếu nó ngừng hoạt động hoặc bị gián đoạn. Khi xác lập automatic được bắt buộc, router tự động kết nối với Internet khi cần truy cập.

3. Mở hoặc tắt các firewall

Chọn hộp kiểm hoặc nút tùy chọn thích hợp để mở firewall của router. Một số router (chẳng hạn như router Netgear) được mở firewall theo mặc định và trang cấu hình không cung cấp một tùy chọn enable; nó chỉ cho phép bạn tắt (disable) firewall bằng cách chọn Disable SPI Firewall. Việc tắt firewall sẽ mở toang mạng ra trước khả năng bị tấn công bên ngoài. Thật sự không có lý do nào để tắt firewall thậm chí nếu việc truy cập đến các dịch vụ chơi game bằng những dịch vụ khác là một vấn đề bởi vì tất cả vấn đề kết nối cần được giải quyết bằng những xác lập port forwarding hoặc port triggering **(xem mục 58).**



4. Xác định địa chỉ IP Server DMZ

Nếu bạn muốn vận hành một máy tính hoặc server (chẳng hạn như máy tính có chức năng như một Web server hoặc gaming server) bên ngoài firewall, bạn có thể yêu cầu router đặt máy tính đó trong

vùng DMZ. Điều này có nghĩa là mạng được bảo vệ khỏi cuộc tấn công nhưng máy tính DMZ có thể bị tấn công. Để đặt một máy tính trên của bạn trong vùng DMZ sử dụng một router Netgear, chọn hộp kiểm Default DMZ Server và sau đó nhập địa chỉ IP của máy tính vốn sẽ được đặt trong vùng DMZ. Nếu bạn cần tìm địa chỉ IP của một máy tính, đi đến máy tính đó và nhấp nút Start, sau đó chọn Run. Gõ nhập command trong hộp Run và nhấp OK. Trong cửa sổ command vừa mở ra, gõ nhập ipconfig/all và nhấn Enter. Bạn sẽ được cung cấp địa chỉ IP và nhận xác lập IP khác cho máy tính.

5. Cho phép ping giao diện Internet router

   Ping là một công cụ dòng lệnh được sử dụng để xác định xem một nối kết có hiện hữu giữa máy tính hoặc những thiết bị mạng khác hay không. Ví dụ nếu bạn dường như không thể kết nối với các máy tính khác trên mạng vốn có một folder chia sẻ, bạn có thể ping máy tính này bằng cách sử dụng địa chỉ IP của nó để xem có một sự cố kết nối hay không. Theo mặc định, hầu hết các router WiFi được cấu hình để giao diện hoặc nối kết của router với Internet không thể được ping. Giao diện Internet cho router thực sự được gán địa chỉ IP của nó bởi nhà cung cấp dịch vụ Internet. Do đó giao diện Internet trên router thực sự là giao diện công cộng. Việc cho phép giao diện công cộng ping có thể mở toang router ra trước sự tấn công vì nó có thể "bị ping đến chết". Một cá nhân có ý đồ xấu trên Internet có thể gởi tới tấp các gói ping hoặc các gói ping quá cỡ để thật sự làm ngừng hoạt động giao diện công cộng của router. Kiểu tấn công này được gọi là "ping tử thần".

   Mở giao diện Internet của router để ping chỉ khi nhà cung cấp dịch vụ Internet (hoặc bạn) cần ping giao diện đó để xác định xem có một sự cố kết nối hay không. Ví dụ đối với router Netgear, chọn tùy chọn Respond to Ping on Internet Port để mở tính năng này. Khi bạn quyết định rằng giao diện có thể được truy cập bởi một Ping (từ bạn hoặc kỹ thuật viên ISP), bạn nên tắt tính năng này.

6. Xác lập kích cỡ MTU

   Giá trị Maximum Transmit Unit (MTU) cho các mạng Ethernet chẳng hạn như mạng WiFi là 1500 bytes. Để xác lập MTUtại giá trị mặc định trừ phi nhà cung cấp dịch vụ Internet đòi hỏi sử dụng một xác lập khác. Nếu bạn không chắc chắn về giá MTU, hãy liên lạc với ISP của bạn. Ví dụ để thay đổi MTU trên router Netgear, nhấp hộp text MTU và gõ nhập giá trị khác. Mỗi router cung cấp một màn hình cấu hình hơi khác nhau để xác lập MTU.

   Nhà cung cấp dịch vụ Internet quyết định MTU tối ưu cho mạng mà nó dịch vụ bằng phương pháp thử và sai. Cách duy nhất mà bạn có thể cảm nhận được rằng bạn không có đúng xác lập MTUcho nối kết

ISP là nối kết với Internet hơi chậm và điều này thường chỉ xảy ra trong những tình huống mà MTU được xác lập cao hơn MTU của ISP và các gói dữ liệu phải được phân chia thành các cụm nhỏ hơn để truyền. Do đó, kết quả cuối cùng là hãy gọi ISP và xem nó có sử dụng MTU đặc biệt nào hay không.

7. Áp dụng các xác lập firewall vào cấu hình router

   Khi bạn đã xác lập cấu hình firewall cho router, bạn phải áp dụng hoặc lưu các xác lập mới (cho dù bạn áp dụng hoặc lưu các xác lập hay không đều tùy thuộc vào router WiFi). Ví dụ đối với router Netgear WGR 614, nhấp nút Apply để áp dụng và lưu các xác lập firewall

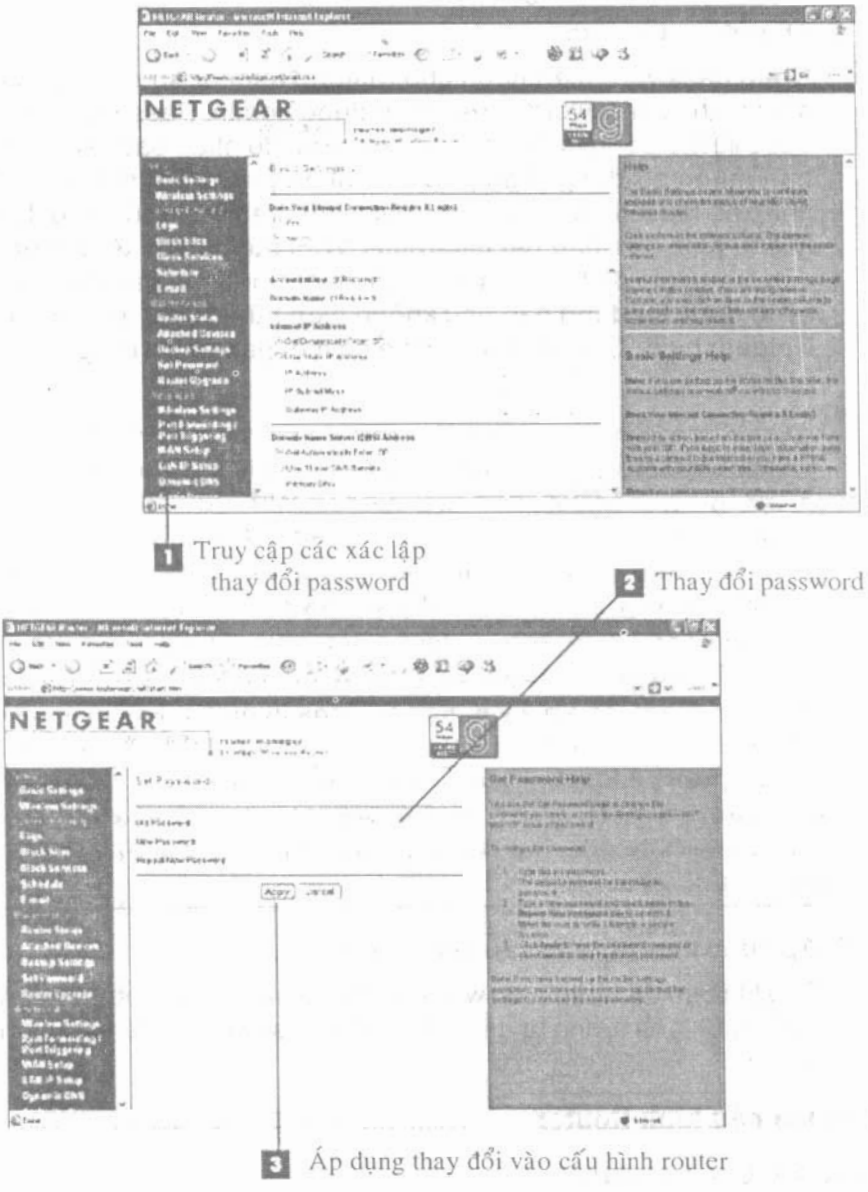
73. Thay đổi Password của Router

Trước khi bạn bắt đầu	Xem thêm
22 Truy cập cấu hình Router	**Mục 74**

Bạn có thể tự hỏi nên thay đổi password router như thế nào để bảo vệ an toàn mạng. Trước tiên, hầu hết các router sử dụng một password mặc định mà bất kỳ người nào có thể đoán. Ví dụ Netgear sử dụng password làm password mặc định của nhà quản trị. Do đó, các xác lập của router liên quan đến firewall và những tính năng khác chẳng hạn như ngăn chặn nội dung và dịch vụ chỉ an toàn như cấu hình của router. Nếu bất kỳ người nào trong gia đình của bạn nhảy vào máy tính được kết nối trực tiếp với router (hoặc nếu bạn đã mở chức năng quản lý từ xa cho router như được giải thích trong **mục 81**) và truy cập cấu hình của router, bạn có thể sẽ gặp phải một sự phá vỡ an ninh lớn, nhất là khi các thành viên gia đình tắt firewall bởi vì game online mà họ đang cố chơi không hoạt động tốt.

Trước khi bạn thay đổi password của router, bạn có thể muốn sao lưu cấu hình của router. Hầu hết các router firewall có khả năng sao lưu file cấu hình cho router phòng ngừa có một sự cố chẳng hạn như một password quản trị bị quên (để biết thêm chi tiết về việc sao lưu cấu hình, hãy **xem mục 74).**

73. Thay đổi password của Router



1. Truy cập các xác lập thay đổi password

Đăng nhập vào router bằng quyền administrator bằng cách sử dụng trình duyệt Web, gõ nhập URL cho router trong hộp Address của trình duyệt và sau đó cung cấp tên đăng nhập và password cho router khi được nhắc về thông tin này. Bạn có thể tìm thấy URL và tên đăng nhập và password mặc định cho router của bạn trong tài liệu đi kèm với router. Nếu bạn đã mất tất cả tài liệu cho router, đi đến Web site của nhà sản xuất và download tài liệu này.

Từ trang cấu hình chính của router, truy cập xác lập trên password cho router. Ví dụ, Netgear WGR14 cung cấp link lệnh Set password.

2. Thay đổi password

Nhập password hiện hành cho router (Netgear sử dụng password mặc định là password; Linksys sử dụng admin. Password mặc định được liệt kê trong tài liệu cho router). Sau đó nhập password mới mà bạn muốn sử dụng. Bạn phải xác nhận password mới bằng cách nhập nó lần thứ hai. Bởi vì một giao diện Web được sử dụng để quản lý cấu hình của hầu hết các router WiFi được thiết kế cho hầu hết các mạng gia đình, các quy tắc chi phối chiều dài password và các ký tự được sử dụng hầu như không hiện hữu. Ví dụ trên một router Netgear hoặc Linksys, bạn có thể có một password chỉ gồm một ký tự đơn.

THỦ THUẬT: Điểm mấu chốt của việc có một password là để giúp bảo vệ an toàn router WiFi do đó bạn nên sử dụng tối thiểu ó ký tự (bạn có thể sử dụng bất kỳ ký tự nào trên bàn phím) và bạn sử dụng kết hợp các ký tự chữ và số. Không dùng tên của vợ hoặc chồng, con chó, con cái hay bất kỳ những gì khác mà người ta có thể dễ dàng đoán. Đừng quên rằng bạn đang cố bảo vệ an toàn router khỏi sự xâm nhập bên ngoài (password của bạn nên có một mức độ phức tạp nào đó) và cũng để bảo vệ an toàn router khỏi những người trong nhà của bạn (chẳng hạn như con cái của bạn), những người có thể muốn cấu hình lại router sao cho nó không còn ngăn chặn các Web site nhất định nữa.

---

3. Áp dụng thay đổi vào cấu hình router

Sau khi bạn đã nhập password cũ và password mới, nhấp nút Apply hoặc một lệnh tương tự để lưu thay đổi password sang cấu hình của router.

74. Sao lưu cấu hình Router

Trước khi bạn bắt đầu

22 Truy cập cấu hình router

Bạn có thể sao lưu file cấu hình của router. Điều này hữu dụng trong những tình huống bạn muốn thử các xác lập mới nhưng sau đó muốn phục hồi trở lại cấu hình của router sang các xác lập đã thử và đúng của bạn. Việc sao lưu file cấu hình router sẽ mang đến cho bạn khả năng đưa router trở về cấu hình ưu tiên nếu người nào đó trong nhà bạn đã sửa đổi các xác lập của router.

Trang Backup Settings cho router sẽ cho phép bạn sao lưu cấu hình của router và cũng phục hồi cấu hình nếu cần thiết (sử dụng lệnh Restore). Bạn chỉ cần sao lưu router khi bạn thay đổi cấu hình của router (chẳng hạn như sau khi thiết lập cấu hình ban đầu). Thực hiện các sao lưu tiếp theo chỉ sau khi bạn thay đổi cấu hình của router. Bạn nên sao lưu các thay đổi mà bạn thực hiện đối với cấu hình của router chỉ sau khi bạn đã quyết định rằng các xác lập mới hoạt động. Nếu các xác lập mới không hoạt động, bạn có thể phục hồi các xác lập trở lại bằng cách phục hồi một phiên bản trước đó của cấu hình router. Bạn có thể lưu bao nhiêu file khác nhau tùy thích, điều này cho phép bạn giữ các phiên bản cấu hình khác nhau của router. Hầu hết các router cũng cung cấp một lệnh nhằm cho phép bạn xóa cấu hình của router và phục hồi cấu hình trở về cấu hình các xác lập factory.

74 Sao lưu cấu hình Router



1. Truy cập các xác lập Backup

Đăng nhập vào router bằng quyền administrator bằng cách sử dụng trình duyệt Web; các nhà URL cho router của bạn trong hộp Address của trình duyệt, sau đó cung cấp tên đăng nhập và password cho router khi được nhắc về thông tin này. Bạn có thể tìm thấy URL cho router trong tài liệu đi kèm router. Nếu bạn đã thay đổi password cho router như được thảo luận trong mục 73, hãy sử dụng password mới mà bạn xác lập.

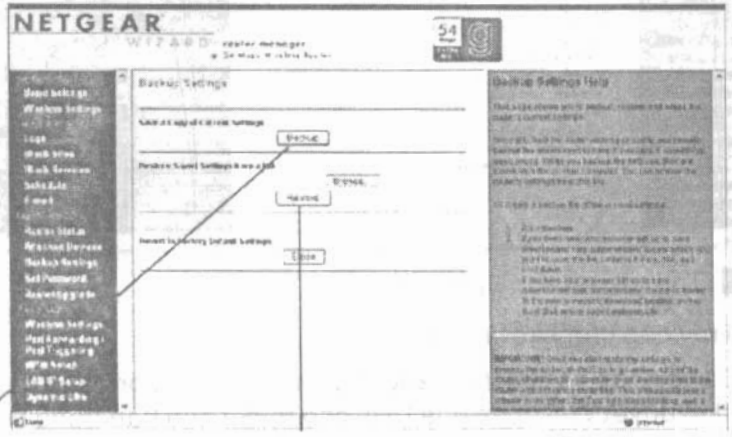
THỦ THUẬT: Khi bạn truy cập URL cho router, hãy lưu trang dưới dạng một trong các favorites trong trình duyệt Web. Sau đó bạn có thể mở trang Web của router bất cứ lúc nào bằng cách nhấp link favorites mà bạn đã tạo. Bạn cũng có thể nhập tên user và password trong hộp text

logon và chọn hộp kiểm Remember my password. Windows sẽ nhớ tên user và password, giúp bạn dễ dàng truy cập router. Tuy nhiên, nếu Windows nhớ password cho bạn, bất kỳ người nào tiếp cận máy tính của bạn có thể truy cập router. Nếu bạn thay đổi password mặc định, hãy bảo đảm bạn nhớ nó hoặc ghi nó ra ở một nơi an toàn phòng ngừa bạn cần nó.

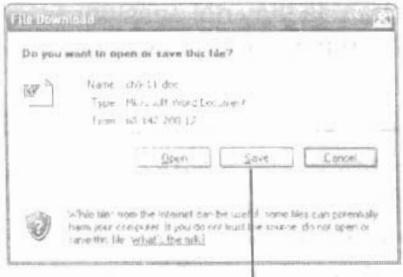
Từ trang cấu hình chính của router, nhấp link Backup Settings hoặc lệnh tương tự để truy cập trang mà từ đó bạn có thể cấu hình tiến trình sao lưu cho router của bạn.

2. Bắt đầu tiến trình sao lưu

Trên trang cấu hình Backup Settings, nhấp nút Backup hoặc lệnh tương tự. Một hộp thoại File Download mở ra. Đây cũng là loại hộp thoại download vốn mở khi bạn cố download một file từ bất kỳ trang Web. Ví dụ nếu bạn download một file ảnh hoặc file âm thanh từ một trang Web (hãy nhớ rằng router được cấu hình) bằng cách sử dụng một giao diện Web, các trang cấu hình router thực tế là các trang Web như bất kỳ trang Web khác.



2 Bắt đầu tiến trình sao lưu



3. Chọn tùy chọn Save File



4. Chọn vị trí và lưu bản sao lưu

3. Chọn tùy chọn Save File

   Nhấp Save trong hộp thoại Save File Download. Một hộp thoại Save As mở ra.

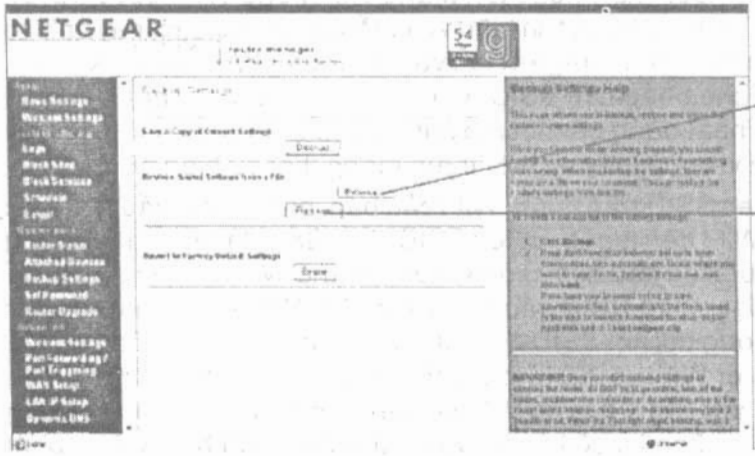
4. Chọn vị trí và lưu bản sao lưu

   Sử dụng một hộp thoại Save As để chọn một vị trí cho file đã lưu (bạn có thể lưu nó trong folder My Documents trong máy tính của bạn hoặc một vị trí khác nào đó nếu bạn thích hơn). Bạn có thể thay đổi tên mặc định cho file sao lưu của bạn (Netgear đối với một router Netgear) thành một tên nào đó hơi mang tính mô tả hơn sao cho bạn có thể tìm thấy file nếu cần trong tương lai. Sau khi xác định một vị trí và một tên cho file, nhấp Save. File sao lưu sẽ được lưu sang đĩa cứng của máy tính.

5. Mở file sao lưu

   Bây giờ bạn có thể phục hồi file sao lưu trong tương lai (nếu cần) bằng cách sử dụng lệnh Restore trên trang cấu hình Backup Settings.

   Ví dụ, bạn đã sao lưu router và cần phục hồi file cấu hình đó. Nhấp nút Browse ở trên nút Restore trên trang Backup Settings của cấu hình router. Sau đó, tìm file trong hộp Choose file vừa mở ra. Khi bạn đã tìm thấy file sao lưu thích hợp, nhấp Open để quay trở về màn hình cấu hình router.



6. Phục hồi file sao lưu

   File sao lưu mà bạn đã mở ở bước 5 xuất hiện trong hộp text filename kế bên nút Browse. Nhấp Browse để phục hồi file cấu hình sang router. Một hộp thông báo xuất hiện cho bạn biết rằng các xác lập hiện hành sẽ được thay thế bởi các xác lập đã phục hồi. Nhấp OK để đóng hộp xác nhận.

Cấu hình router sẽ được phục hồi (điều này có thể mất một thời gian) và sau đó bạn sẽ được đưa trở về trang Web cấu hình router.

THỦ THUẬT: Nếu bạn cần reset (xác lập) lại router và bắt đầu lại từ đầu, router cung cấp lệnh Erase hoặc lệnh tương tự nhằm cho phép bạn xóa cấu hình của router và bắt đầu lại từ đầu. Ví dụ, nếu tất cả người dùng đang gặp trục trặc khi truy cập Web hoặc những dịch vụ Internet khác bởi vì bạn đã không cấu hình chức năng ngăn chặn dịch vụ hoặc port triggering một cách chính xác, bạn có thể muốn reset router và bắt đầu lại từ đầu. Việc có một bản sao lưu cấu hình trước đây của router (vốn đã thực sự hoạt động tốt) sẽ loại bỏ nhu cầu về lệnh Erase bởi vì bạn có thể phục hồi router trở về một cấu hình trước đó, chỉ sử dụng Erase như là một giải pháp cuối cùng.

---

75. Tắt các Broadcast Server Set ID (SSID)

Trước khi bạn bắt đầu

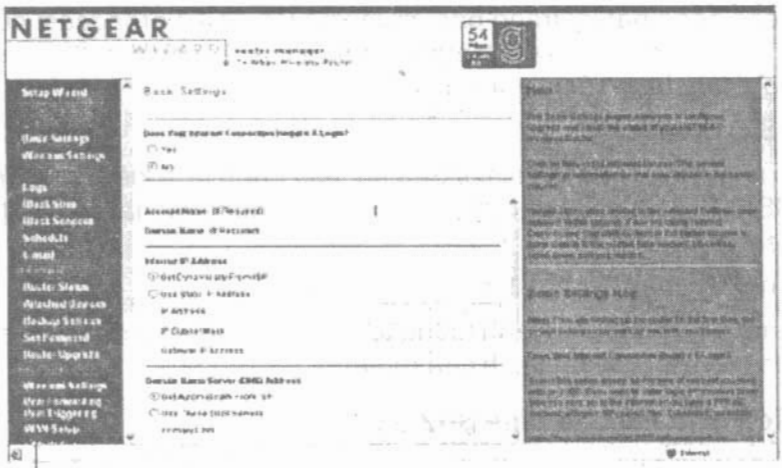
21 Bàn về việc cấu hình Router

22 Truy cập cấu hình router

SSID (service set identifier) hoặc tên mạng cho mạng WiFi được truyền phát đại chúng bởi router qua một tín hiệu vô tuyến, giúp cho các máy tính có tính năng WiFi trên mạng dễ dàng kết nối với các router WiFi và workgroup. Tuy nhiên khi bạn cho phép các SSID truyền phát đại chúng, bất kỳ người nào trong phạm vi hoạt động có một máy tính được bật WiFi có thể cố truy cập mạng WiFi bởi vì người này có thể "thấy" mạng thật sự hiện hữu.

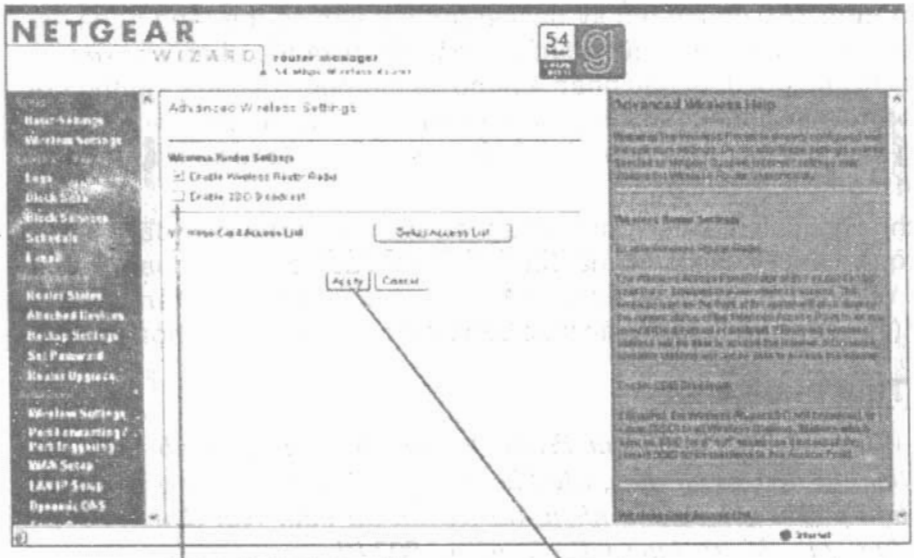
Bởi vì bạn biết các SSID trên mạng WiFi của bạn, bạn có thể cấu hình các máy tính được bật WiFi trên mạng với tên SSID. Tên SSID là một trong những xác lập được bắt buộc để cấu hình một Adapter mạng WiFi. Xem mục 33 để biết thông tin về việc nhập SSID và những xác lập WiFi khác cho Adapter WiFi. Bởi vì bạn không đòi hỏi SSID được truyền phát đại chúng (bạn có thể cấu hình các Adapter WiFi với SSID bằng thủ công), việc tắt các thông báo đại chúng (broadcast) SSID ít ra có thể bảo vệ mạng của bạn khỏi "những hacker nghiệp dư", những kẻ cố kết nối với mạng WiFi của bạn khi họ phát hiện mạng do sự truyền phát đại chúng SSID.

75. Tắt các Broadcast Server Set ID (SSID)



1. Truy cập các xác lập Wireless nâng cao

Đăng nhập vào router bằng quyền administrator bằng cách sử dụng trình duyệt web bằng cách gõ nhập URL cho router trong hộp Address của trình duyệt và sau đó cung cấp tên đăng nhập và password cho router khi được nhắc về thông tin này. Bạn có thể tìm thấy URL cho router của bạn trong tài liệu đi kèm router hoặc bạn có thể đi đến Web site của nhà sản xuất router và download tài liệu cho router của bạn để biết cách truy cập site cấu hình của router.



Từ trang cấu hình chính cho router, truy cập các xác lập wireless nâng cao hoặc bất kỳ trang nào chứa xác lập SSID broadcast của router. Ví dụ đối với router Netgear, nhấp link Advanced Wireless Setting trong danh sách lệnh của router.

2. Tắc SSID Broadcast

   Trên trang Advanced Wireless Setting, hãy chọn hộp kiểm cho Enable SSID Broadcast (hoặc chọn xác lập trên router để tắt các SSID Broadcast).

3. Áp dụng các thay đổi cấu hình

   Nhấp nút OK (hoặc một lệnh tương tự) để áp dụng thay đổi mà bạn đã thực hiện đối với cấu hình của router.

76. Bàn về các chiến lược an ninh 802.11

Trước khi bạn bắt đầu	Xem thêm
70 Bàn về an ninh mạng cơ bản	Mục 77
	Mục 78

Khi các chuẩn Ethernet 802.11 để nối mạng WiFi được thiết lập bởi IEEE (viện kỹ sư điện và điện tử), rõ ràng các chuẩn an ninh đã được thiết lập để nối mạng wireless. Bởi vì phương tiện mạng là những tín hiệu vô tuyến, bất kỳ người nào muốn "lắng nghe" bằng một máy tính được bật WiFi chẳng hạn như một laptop hoặc một số phần mềm bổ sung để thu nhập các gói dữ liệu có thể nghe lén trên một mạng WiFi.

Rõ ràng bạn có thể tắt SSID broadcast để giúp che giấu mạng WiFi của bạn (**xem mục 75**), nhưng bất kỳ hacker tận tụy vẫn có thể lắng nghe lưu lượng mạng vô tuyến trên những tần số khác nhau và thu nhập các gói dữ liệu. Sau khi các gói được thu nhập, chúng có thể được giải mã, những gói này chứa thông tin chẳng hạn như các địa chỉ IP, username, password và tất cả những thứ mà hacker sau đó có thể sử dụng để đạt được sự truy cập trái phép đến mạng WiFi của bạn.

Giao thức an ninh đầu tiên được phát triển cho các mạng WiFi đã là WEP (Wired Equivalent Privacy). Nó đã được phát triển để bảo vệ an toàn chuẩn 802.11b. WEP sử dụng hai chiến lược để bảo vệ dữ liệu truyền trên phương tiện WiFi (các sóng vô tuyến): xác thực bằng khóa chia sẻ và mã hóa dữ liệu.

Thuật ngữ chính

WEP (Wired Equivalent Privacy): Một giao thức an ninh WiFi mã hóa dữ liệu và sử dụng các khóa chia sẻ để mã hóa và giải mã dữ liệu ở đầu gởi và đầu nhận khi truyền dữ liệu. Ban đầu WEP đã được tạo để sử dụng với các mạng 802.11b.

Một chuỗi ký tự thập lục phân được sử dụng để hiệu lực hóa một user hoặc thiết bị như là điểm nối kết hoặc người nhận luồng dữ liệu.

Xác thực bằng khóa chia sẻ nghĩa là một khóa xác thực được cấu hình trên router WiFi. Khóa xác thực là số thập lục phân dài 64 bit hoặc 128 bit. Số bit càng dài khóa càng an toàn do đó bạn sẽ muốn sử dụng một khóa 128 bit nếu bạn sử dụng sự an ninh WEP.

Khóa xác thực có thể được tạo tự đông bởi router hoặc bạn có thể tư nhập số này (khóa xác thực có dạng thập lục phân nếu bạn không biết cách nhập các số thập lục phân, bạn có thể sử dụng tính năng tự động tạo khóa hơn). Để một máy tính đươc bật WiFi kết nối với mang đươc host bởi router WiFi, máy tính đó phải được cấu hình bằng cùng một mã khóa xác thực vốn được cấu hình trên router. Nếu một máy tính được bật WiFi cố truy cập mạng WiFi mà không có adpater WiFi trên máy tính được cấu hình bằng khóa xác thực chia sẻ, router từ chối máy tính đó truy cập mạng.

Mã hóa dữ liệu sao cho nó có thể được đọc cho đến khi nó được giải mã tại nơi đến cuối cùng của nó. Do đó khi WEP được kích hoạt trên mạng (trên các adapter WiFi cho các máy tính riêng lẻ và trên router WiFi), dữ liệu được mã hóa bởi máy tính gởi và sau đó được giải mã bởi máy tính nhận. WEP mã hóa chỉ dữ liệu, nó không mã hóa các khóa xác thực chia sẻ. Thật không may sự mã hóa chỉ có hiệu lực khi dữ liệu được gởi trên tín hiệu WiFi. Dữ liệu không được mã hóa nếu nó di chuyển từ hạ tầng WiFi đến một mạng hữu tuyến. Nếu người nào đó nghe lén trên mạng WiFi của bạn (phần mềm có sẵn cho phép thu nhập dữ liệu truyền trên một mạng WiFi), người đó có thể xem luồng dữ liệu và cuối cùng quyết định các khóa xác thực là gì. Một khi hacker có khóa xác thực, người này có thể ngăn chặn dữ liệu và giải mã nó như thể người này là người nhận đã định.

WEP cũng không có khả năng tạo một khóa xác thực mới sau một lượng thời gian xác định. WEP cũng không đòi hỏi sự xác thực người dùng (user authentication khi dữ liệu được nhận và được giải mã). Không phải việc xác thực người nhận ở đầu kia của tiến trình truyền dữ liệu mở rộng việc truyền dữ liệu ra trước khả năng bị chặn và được giải mã bởi người nào đó không phải người nhận đã được chỉ định.

Thuật ngữ chính

Encryption (mã khóa). Biến dịch một thông báo thành một mật mã. Sau khi một thông báo được mã hóa, một khóa (key hoặc phương thức nhận dạng khác chẳng hạn như một password) được cần đến để giải mã thông báo.

Bây giờ có lẽ bạn nghĩ rằng với việc mã hóa dữ liệu và sự xác thực bằng khóa chia sẻ, không có cách nào để một hacker có thể phá hỏng hệ thống an ninh mạng của bạn. Tuy nhiên, WEAP của bạn sử dụng một khóa tĩnh (static key), nghĩa là khóa xác thực được truyền với mỗi tập hợp dữ liệu (khóa thường được lặp lại). Do đó khi ngày càng nhiều dữ liệu được gởi trên mạng, một hacker có thể giải mã các vùng mã khóa bởi vì khóa không thay đổi. Hacker thu thập càng nhiều dữ liệu bằng việc giám sát mạng (người ta có thể giám sát mạng thậm chí nếu họ không thể đăng nhập) thì họ có thể lắp ghép lại

càng nhiều thông tin theo thời gian. Cuối cùng hacker sẽ có đủ thông tin để xác định khóa và giải mã dữ liệu mà bạn giả định là an toàn. Thực tế người ta ước tính rằng một hacker giám sát một mạng chưa tới một ngày là để tích lũy đủ thông tin về các khóa để bắt đầu giải mã các thông báo được mã hóa.

Để khắc phục một số khuyết điểm của WEP (đã có sẵn khi các thiết bị WiFi 802.11b có mặt vào năm 2000), một giao thức an ninh WiFi mới được phân phối vào năm 2002: WPA (WiFi Protected Access). WPA xáo trộn các khóa xác thực chia sẻ, tạo các khóa mới vào một khoảng thời gian nào đó và cũng có những tính năng để kiểm tra xem một khóa đã bị sửa đổi hay không. WPA cũng cho phép mã hóa dữ lieae3u được truyền trên mạng WiFi và sử dụng một thuật toán mã hóa mạnh hơn thuật toán WAP. WPA cũng đòi hỏi sự xác thực người dùng (user authentication) trong tiến trình gởi và nhận dữ liệu trên mạng. Do đó, WPA giải quyết hầu hết những điểm yếu của WEP.

THUẬT NGỮ CHÍNH

WPA (WiFi Protected Access). Một giao thức an ninh WiFi và mã hóa dữ liệu xáo trộn các khóa chia sẻ được gởi qua mạng WiFi. WPA cũng đòi hỏi sự xác thực người dùng, cung cấp mức độ an ninh cao hơn WEP.

Bạn có thể cấu hình router WiFi để sử dụng WEP và WPA. Chọn cái này hoặc cái kia, bạn không thể chạy cả hai giao thức cùng một lúc. Nếu bạn chọn WPA, tất cả thiết bị WiFi trên mạng WiFi phải được cấu hình để sử dụng QPA. Nếu bạn có một số thiết bị cũ hơn không hỗ trợ WPA, có thể bạn sẽ chọn WEP để đáp ứng những thiết bị đó.

Nếu bạn thực sự muốn mạng WiFi được bảo vệ, bạn sẽ muốn sử dụng WPA. Cấu hình của WPA và WEP tương tự do đó bạn nên sử dụng WPA. **Xem mục 77** và **78** để biết các hướng dẫn về việc cấu hình hai giao thức an ninh này trên router của mạng.

77. Cấu hình an ninh Wired Equivalent Privacy (WEP)

Trước khi bạn bắt đầu

22 Truy cập cấu hình Router

33 Cấu hình Adapter và kết nối với Router không dây

Khi bạn cấu hình WEP trên router, bạn có tùy chọn để sử dụng khóa xác thực 64 bit hoặc 128 bit. Càng nhiều bit trong một khóa thì khóa càng khó giải mã (ví dụ bởi một hacker). Khóa có thể được tạo tự động bởi router (router có thể thực sự tạo nhiều khóa và bạn có thể chọn khóa mà bạn muốn sử dụng). Bạn cũng có thể xác lập kiểu xác thực mà bạn muốn sử dụng với việc mã hóa WEP. Có 3 loại xác lập authentication (xác thực):

- ***Open System Authentication**: Loại xác thực này cho phép một máy tính được bật WiFi giao tiếp với router WiFi (access point) và sau đó kết nối với mạng WiFi. Nó không đòi hỏi bất kỳ sự xác thực người dùng để máy tính kết nối.*

- ***Shared Key:*** *Kiểu xác thực này sử dụng một khóa chia sẻ. Máy tính được bật WiFi phải được cấu hình cùng một khóa chia sẻ với router WiFi trước khi nó kết nối với access point của router và mạng WiFi. Sử dụng khóa chia sẻ sẽ từ bỏ việc xác thực hệ thống mở trên mạng.*
- ***Automatic****: Một số router cho phép bạn xác lập sự xác thực ở dạng "automatic". Điều này có nghĩa là một máy tính cố kết nối với mạng có thể sử dụng sự xác thực hệ thống mở (open system authentication) hoặc sự xác thực bằng khóa chia sẻ (shared key) phụ thuộc vào adapter WiFi của máy tính đã được cấu hình như thế nào.*

Phụ thuộc vào router WiFi mà bạn đã mua, bạn cũng có thể xác định một passphrase cho cấu hình WEP. Sau đó passphrase có thể được sử dụng để cấu hình adapter WiFi trên các máy tính (làm việc tốt nhất với những adapter từ cùng một nhà sản xuất với router). Gõ nhập passphrase vào cấu hình của adapter WiFi sẽ cho phép các adapter download khóa chia sẻ từ router.

Điều này có nghĩa bạn không cần phải gõ nhập bằng tay khóa WEP chia sẻ vào cấu hình của adapter, vì điều đó có thể gây thất vọng nếu bạn sử dụng một khóa 128 bit dài 26 chữ số.

Thuật ngữ chính

Passphrase. Một chuỗi text tương tự như password được sử dụng để cấu hình thiết bị WiFi cho an ninh WEP hoặc WPA. Bởi vì passphrase được tạo bởi router WiFi, passphrase được sử dụng trong các xác lập của router WiFi để cấu hình thiết bị bằng đúng khóa mã hóa. Việc sử dụng passphrase để cấu hình adapter sẽ từ chối nhu cầu gõ nhập toàn bộ khóa (vốn không có sẵn cho WPA) trong các xác lập cấu hình của adapter WiFi.

Để cấu hình mạng được sử dụng trong WEP, đầu tiên bạn phải thay đổi các xác lập của router và sau đó bạn phải cấu hình adapter mạng cho từng máy tính trên mạng.

- ***Shared Key:*** *Kiểu xác thực này sử dụng một khóa chia sẻ. Máy tính được bật WiFi phải được cấu hình cùng một khóa chia sẻ với router WiFi trước khi nó kết nối với access point của router và mạng WiFi. Sử dụng khóa chia sẻ sẽ từ bỏ việc xác thực hệ thống mở trên mạng.*
- ***Automatic****: Một số router cho phép bạn xác lập sự xác thực ở dạng "automatic". Điều này có nghĩa là một máy tính cố kết nối với mạng có thể sử dụng sự xác thực hệ thống mở (open system authentication) hoặc sự xác thực bằng khóa chia sẻ (shared key) phụ thuộc vào adapter WiFi của máy tính đã được cấu hình như thế nào.*

Phụ thuộc vào router WiFi mà bạn đã mua, bạn cũng có thể xác định một passphrase cho cấu hình WEP. Sau đó passphrase có thể được sử dụng để cấu hình adapter WiFi trên các máy tính (làm việc tốt nhất với những adapter từ cùng một nhà sản xuất với router). Gõ nhập passphrase vào cấu hình của adapter WiFi sẽ cho phép các adapter download khóa chia sẻ từ router.

Điều này có nghĩa bạn không cần phải gõ nhập bằng tay khóa WEP chia sẻ vào cấu hình của adapter, vì điều đó có thể gây thất vọng nếu bạn sử dụng một khóa 128 bit dài 26 chữ số.

Thuật ngữ chính

Passphrase. Một chuỗi text tương tự như password được sử dụng để cấu hình thiết bị WiFi cho an ninh WEP hoặc WPA. Bởi vì passphrase được tạo bởi router WiFi, passphrase được sử dụng trong các xác lập của router WiFi để cấu hình thiết bị bằng đúng khóa mã hóa. Việc sử dụng passphrase để cấu hình adapter sẽ từ chối nhu cầu gõ nhập toàn bộ khóa (vốn không có sẵn cho WPA) trong các xác lập cấu hình của adapter WiFi.

Để cấu hình mạng được sử dụng trong WEP, đầu tiên bạn phải thay đổi các xác lập của router và sau đó bạn phải cấu hình adapter mạng cho từng máy tính trên mạng.

77. Cấu hình an ninh Wired Equivalent Privacy (WEP)



1 Truy cập các xác lập Wireless

1. Truy cập các xác lập Wireless

Đăng nhập vào router bằng quyền administrator bằng cách sử dụng trình duyệt Web, gõ nhập URL của router trong hộp Address của trình duyệt, sau đó cung cấp tên đăng nhập và password cho router khi bạn được nhắc về thông tin này. Bạn có thể tìm thấy URL cho router trong tài liệu đi kèm router. Từ trang cấu hình chính cho router WiFi, nhấp link Wireless Setting hoặc lệnh tương tự để mở trang cấu hình cho các xác lập an ninh của router.

2. Mở WEP

Nhấp nút tùy chọn WEP (Wired Equivalent Privacy) trên trang Wireless Setting (hoặc bằng lệnh trên trang cấu hình của router vốn mở chức năng an ninh WEP).

3. Xác lập kiểu xác thực

Nhấp danh sách Authentication Type và chọn Automatic Open System Authentication hoặc Shared Key. Xác lập mà bạn chọn phụ thuộc vào các yêu cầu cấu hình của các adapter WiFi được sử dụng trên mạng.

Nếu bạn chọn Automatic, router sẽ tạo khóa chia sẻ (nó thật sự tạo 3 khóa và bạn có thể thật sự chọn một trong ba khóa này). Bạn có thể gõ nhập một password mà sau đó bạn có thể sử dụng để cấu hình các adapter WiFi bằng khóa đó (bạn gõ nhập passphrase trong các xác lập của adapter WiFi và khóa được gởi đến các adapter bởi router). Bạn có thể sử dụng xác lập Automatic nếu adapter WiFi cho phép bạn nhập một passphrase cho các cấu hình WEP.





Nếu bạn chọn Open System Authentication, khóa không được bắt buộc do đó các adapter WiFi được cấu hình cho WEP nhưng không được cấu hình bằng một passphrase hoặc một khóa chia sẻ. Bất kỳ máy tính được bật WiFi có thể kết nối với router mà không vẫn xác thực nhưng router sẽ mã háo luồng dữ liệu gởi trên các thiết bị. Khóa chia sẻ không được bắt buộc để giải mã dữ liệu đã mã hóa tại đầu nhận (nghĩa là máy tính).

Nếu các adapter WiFi không cho phép sử dụng một passphrase để cấu hình adapter cho WEP, bạn vẫn phải cấu hình adapter bằng cùng một Shared Key với router WiFi trước khi nó có thể kết nối với các access point của router và mạng WiFi. Hãy chắc chắn bạn nhập khóa trong các xác lập cấu hình của router một cách chính xác để nó xuất hiện trong cấu hình của router.

Để dễ dàng cấu hình và sử dụng WEP với một khóa chia sẻ, lựa chọn tốt nhất là automatic, nghĩa là bạn phải sử dụng một passphrase để cấu hình các adapter WiFi. Lựa chọn tốt nhất thứ hai cho xác lập này là Shared Key (nhưng bạn phải gõ nhập khóa thập lục phân chia sẻ trên màn hình cấu hình adapter WiFi một cách chính xác như nó xuất hiện trên màn hình cấu hình router).

4. Chọn cường độ mã hóa

Bạn có thể chọn sử dụng sự mã hóa 64 bit hoặc 128 bit. Số bit càng lớn thì một hacker càng khó tìm ra nó. Khóa 128 bit mạnh hơn khóa 64 bit. Tuy nhiên nếu bạn phải cấu hình router WiFi trên mạng bằng khóa thật sự (nếu chúng không cho phép bạn sử dụng một passphrase), bạn có thể sử dụng khóa ngắn hơn để tiện lợi (nó có ít ký tự hơn). Thực hiện lựa chọn của bạn từ danh sách sổ xuống được cung cấp.

5. Tạo khóa mã hóa và tạo passphrase

Để tạo một tập hợp khóa mã hóa, nhấp nút Generate. Bốn khóa được tạo để mã hóa bằng WEP (chiều dài của khóa phụ thuộc vào việc bạn đã chọn sự mã hóa 64 bit hoặc 128 bit). Tất cả router WiFi cung cấp một màn hình tương tự để tạo khóa mã hóa. Nhiều khóa mã hóa được tạo để bạn có thể thay đổi khóa theo thời gian nhằm giúp bảo vệ an toàn mạng. Bởi vì passphrase được kết hợp với bất kỳ một trong các khóa, bạn có thể thay đổi bất cứ lúc nào mà không phải cấu hình lại các adapter WiFi (trừ khi bạn có các adapter không cho phép cấu hình passphrase WEP). Chọn nút radio của khóa mà bạn muốn sử dụng.

Để kết hợp một passphrase với các khóa mã hóa, gõ nhập một passphrase trong hộp passphrase. Passphrase có thể dài từ 8 đến 63 ký tự. Thực tế passphrase là một password. Số ký tự càng dài thì người ta càng khó đoán password. Ngoài ra các password vốn sử dụng kết hợp các ký tự chữ và số khó đoán hơn. Password không thể chứa các khoảng trống nhưng nó có thể chứa bất kỳ ký tự có sẵn trên bàn phím.

6. Áp dụng các xác lập WEP

Nhấp nút Apply để áp dụng các xác lập WEP vào các công cụ router.

7. Cấu hình các Adapter WiFi cho WEP

Sau khi bạn đã cấu hình router để sử dụng an ninh WEP, bạn phải cấu hình các adapter WiFi trên từng máy tính mạng cho WEP. Trên một trong các máy tính trong mạng, mở phần mềm cấu hình cho adapter WiFi (nhấp phải biểu tượng adapter WiFi trong System tray và chọn Open từ menu ngữ cảnh).

Chọn nút tùy chọn WEP trên màn hình cấu hình của adapter. Sau đó, nhấp nút tùy chọn Create with Passphrase và gõ nhập cùng một

passphrase bạn đã định nghĩa ở bước 5 trong hộp text. Cả hai router Netgear và Linksys cho phép sử dụng các passphrase. Nếu router của bạn không cho phép sử dụng một passphrase cho WEP hoặc tự động tạo các khóa WEP, bạn phải gõ vào khóa được cấu hình trên router. Nếu bạn không có tùy chọn để xác lập một passphrase trên router, nhấp nút radio Enter Key Manually (hoặc lệnh tương tự) và nhập khóa mã hóa được cấu hình trên router. Sau khi nhập passphrase hoặc khóa, áp dụng các xác lập mới vào adapter WiFi của máy tính. Bây giờ máy tính này có thể kết nối với router. Làm lại bước 7 cho mỗi máy tính trên mạng. Để biết thêm chi tiết về việc cấu hình adapter WiFi **xem mục 33**

78. Cấu hình an ninh WiFi Protected Access (WPA)

Trước khi bạn bắt đầu

22 Truy cập cấu hình Router

33 Cấu hình Adapter và kết nối với Router không dây

An ninh WPA (WiFi Protected Access) cung cấp sự mã hóa và xác thực mạnh mẽ nhằm bảo vệ an toàn mạng WiFi. Khi bạn cấu hình WPA trên router WiFi, các xác lập thực sự duy nhất mà bạn có thể thực hiện là chọn tùy chọn để mở WPA và xác định một passphrase để cấu hình các adapter WiFi trên các máy tính mạng vốn sẽ kết nối với router. Các khóa xác thực an ninh được tạo bởi router WiFi tại một khoảng thời gian đã xác định, do đó bạn cũng sẽ phải xác lập khoảng thời gian khi bạn chọn WPA làm giao thức an ninh. Khoảng thời gian càng ngắn thì mức độ an ninh càng lớn bởi vì một khoảng thời gian ngắn hơn được cung cấp cho một hacker vốn có thể đang giám sát mạng và đang cố giải mã khóa an ninh.

Để cấu hình mạng nhằm sử dụng tính năng an ninh WPA, trước tiên bạn phải thay đổi các xác lập của router và sau đó bạn phải cấu hình adapter mạng cho từng máy tính trên mạng.

78. Cấu hình an ninh WiFi Protected Access (WPA)



1 Truy cập các xác lập Wireless

1. Truy cập các xác lập Wireless

   Đăng nhập vào router bằng quyền administrator bằng cách sử dụng trình duyệt Web, gõ nhập URL cho router trong hộp Address của trình duyệt và sau đó cung cấp tên đăng nhập và password cho router khi được nhắc về thông tin này. Bạn có thể tìm thấy URL cho router trong tài liệu đi kèm router. Hoặc đi đến Web site của nhà sản xuất router, download tài liệu và tham khảo nó để tìm URL và tên đăng nhập cùng với password mặc định.

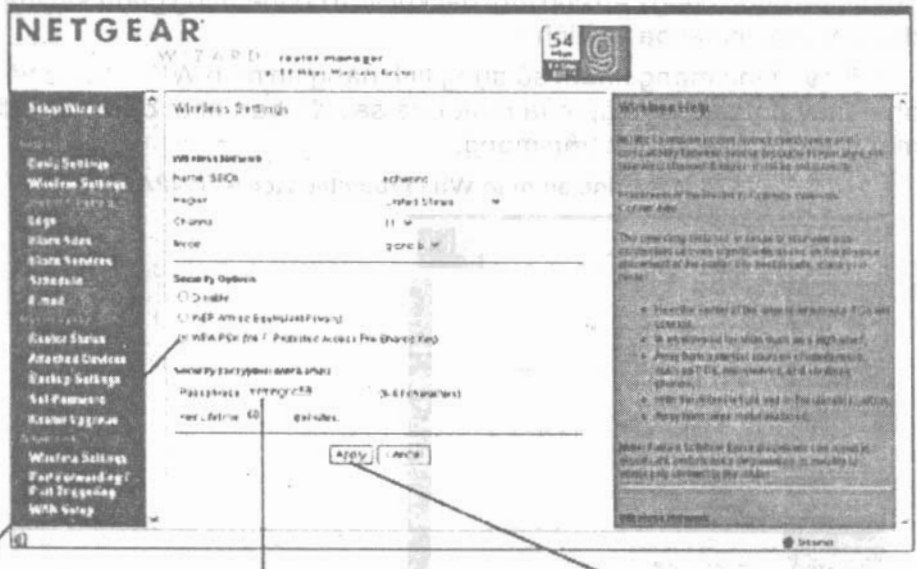
   Từ trang cấu hình chính cho router WiFi, nhấp link Wireless Setting hoặc tương tự để mở trang cấu hình cho các xác lập an ninh của router chẳng hạn như WEP và WPA.

2. Mở WPA

   Nhấp nút tùy chọn WPA-PSK (WiFi Protected Access Pre-Shared Key) trong phần Security Option của trang Wireless Setting (hoặc trang tương tự trên Web site cấu hình của router).

3. Tạo passphrase

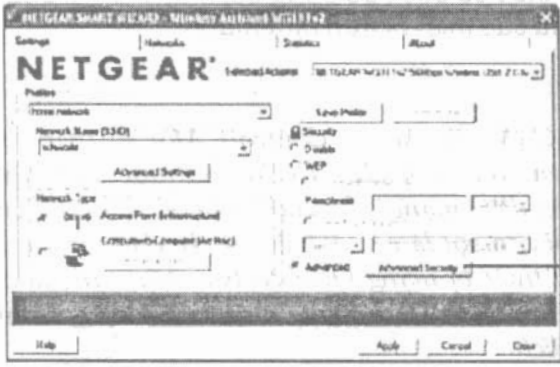
   WPA tự động tạo các khóa chia sẻ và duyệt chúng tại một khoảng thời gian đã xác định. Bạn cấu hình adapter WiFi và những cấu hình khác trên mạng cho WPA, sử dụng cùng một passphrase khi cấu hình router WiFi. Việc sử dụng passphrase phải nhất quán giữa tất cả router WiFi đối với cấu hình WPA. Thậm chí bạn không thấy các khóa được tạo do đó bạn phải sử dụng một passphrase để cấu hình các adapter WiFi.



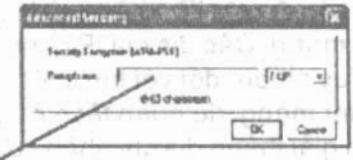
Gõ nhập một passphrase (từ 8 đến 63 ký tự). Nếu bạn muốn thay đổi khoảng thời gian mặc định cho thời gian tồn tại của khóa, nhấp trong hộp text Key Lifetime và gõ nhập một giá trị (tính bằng phút). Thời gian tồn tại của khóa càng ngắn thì mạng WiFi càng an toàn. Giá trị mặc định cho hầu hết các router là một thời gian tồn tại quá 60 phút. Bởi vì có lẽ mạng WiFi sẽ không là mục tiêu của một số kẻ vô loại WiFi (bạn là một con cá nhỏ trong vùng biển mạng WiFi), bạn có thể để cho thời gian tồn tại của khóa được xác lập theo mặc định của nó. Nếu nó giúp bạn ngủ ngon hơn, hãy giảm thời gian tồn tại của khóa thành 30 phút. Một thời gian tồn tại ngắn hơn sẽ không ảnh hưởng tiêu cực đến dòng chảy dữ liệu trên mạng nhưng một hacker sẽ mất hơn một giờ để giải mã một khóa chia sẻ (và sau đó khóa đó sẽ được thay đổi bằng cách nào đó).

4. Áp dụng các xác lập

Sau khi chọn các xác lập cho an ninh WPA, nhấp Apply (hoặc một lệnh tương tự trên router) để lưu các xác lập an ninh mới dưới dạng một phần cấu hình của router.



5 Xác lập Advanced Security cho một Adapter WiFi



6 Nhập Passphrase và áp dụng các xác lập mới

5. Xác lập Advanced Security cho một Adapter WiFi

Sau khi bạn đã cấu hình router để sử dụng loại an ninh WPA, bạn phải cấu hình các adapter WiFi trên từng máy tính mạng cho WPA. Trên một trong các máy tính trên mạng, mở phần mềm cấu hình cho adapter WiFi (nhấp phải biểu tượng của adapter WiFi trong system và chọn Open từ menu ngữ cảnh). Để xác lập an ninh nâng cao cho adapter WiFi, chọn nút tùy chọn Advanced và sau đó nhấp nút Advanced Security. Hộp thoại Advanced Security mở ra.

6. Nhập Passphrase và áp dụng các xác lập mới.

   Nhập passphrase mà bạn đã xác định ở bước 3 cho router trong hộp thoại Advanced Security (hoặc hộp thoại tương tự sử dụng cấu hình phần mềm của adapter; ví dụ nếu bạn sử dụng hộp thoại Windows Wireless Networking Properties cho adapter, password được nhập trong tab Association). Nhấp OK. Quay trở về màn hình cấu hình chính cho adapter WiFi, sau đó bạn có thể áp dụng các xác lập mới cho adapter bằng cách nhấp Apply.

79. Bàn về các địa chỉ MAC giao diện

Trước khi bạn bắt đầu

22 Truy cập cấu hình Router

27 Cấu hình Adapter và kết nối với Router không dây

Mọi adapter (hữu tuyến hoặc không dây) có một địa chỉ phần ứng duy nhất được ghi lên trên một chip ROM (Read Only Memory) bởi nhà sản xuất adapter. Địa chỉ duy nhất này được gọi là địa chỉ phần cứng MAC (Media Access Control). Những địa chỉ duy nhất này thực sự được sử dụng bởi máy tính và phần cứng nối mạng để gởi dữ liệu giữa các thiết bị trên một mạng.

THUẬT NGỮ CHÍNH

Địa chỉ phần cứng MAC (Media Access Control). Một số thập lục phân 48 bit được ghi lên trên một chip ROM cho một máy tính trên mạng hoặc kẹt giao diện mạng (cho một router). Các địa chỉ phần cứng MAC đôi khi còn gọi là các đại chỉ vật lý được sử dụng bởi các máy tính và các thiết bị mạng khác để bảo đảm rằng dòng bit dữ liệu di chuyển trên phương tiện mạng được nhận dạng chính xác đối với nguồn và đích.

Có lẽ bạn đang nghĩ rằng các địa chỉ IP, không phải các địa chỉ MAC cung cấp hệ thống lập địa chỉ cho mạng. Các địa chỉ IP cung cấp hệ thống lập địa chỉ cho các mạng TCP/IP. Tuy nhiên, đối với hai thiết bị chẳng hạn như các máy tính được trang bị adapter mạng, để hoàn tất một giao tác dữ liệu (hoặc truyền), địa chỉ IP được phân giải thành địa chỉ phần cứng MAC trên adapter mạng của máy tính. Tiến trình này bảo đảm dữ liệu được truyền trên đúng thiết bị mạng bởi vì địa chỉ MAC là duy nhất trên mỗi thiết bị. Sau đây là những ví dụ về địa chỉ phần cứng MAC: 00-50-56-C0-00-1.

Hầu hết các router WiFi liệt kê các máy tính hiện được kết nối và các địa chỉ phần cứng MAC của chúng trên các thiết bị được nối kết hoặc màn hình có tên tương tự, điều này làm cho dễ dàng thêm những máy tính này vào một danh sách truy cập MAC. Danh sách truy cập MAC được tìm thấy trên cấu hình của router bằng cách nhấp Wireless Card Access Setup hoặc lệnh tương tự.

Nếu một máy tính được kết nối xuất hiện trên màn hình các thiết bị được nối kết, bạn có thể thật sự cắt và dán MAC mà bạn muốn tạo sang danh sách truy cập MAC mặc dù bạn sẽ phải di chuyển từ danh sách các thiết bị được nối kết đến danh sách truy cập MAC bằng cách sử dụng lệnh router thích hợp (thường được tìm thấy qua phía bên trái các trang Web được sử dụng để cấu hình và giám sát router). Thật là lạ, bạn có thể thấy một máy tính được kết nối không được liệt kê bởi router mặc dù bạn biết rằng máy tính được kết nối. Trong trường hợp này bạn nên xem địa chỉ MAC trên máy tính và sau đó nhập nó bằng tay vào danh sách truy cập MAC của router.

Để xem địa chỉ phần cứng MAC cho adapter mạng của một máy tính, nhấp nút Shared và lệnh Run. Trong hộp thoại Run gõ nhập command và nhấn Enter. Một cửa sổ dòng nhấp lệnh mở ra. Gõ nhập lệnh ipconfig/all và nhấn Enter. Địa chỉ IP và subnet mask cho adapter được liệt kê, tương tự như địa chỉ vật lý (địa chỉ phần cứng MAC) cho adapter. Khi bạn nhập địa chỉ phần cứng MAC trong danh sách truy cập MAC, bạn cũng sẽ cần tên của máy tính (tên host). Tên host được liệt kê cùng với thông tin IP và địa chỉ MAC khi bạn chạy lệnh ipconfig/all.

Việc chuyển đổi các địa chỉ IP thành các địa chỉ MAC hoặc ngược lại là điều xảy ra trong khi dữ liệu di chuyển trên mạng. Tuy nhiên, bởi vì các địa chỉ MAC hoàn toàn duy nhất, bạn có thể sử dụng chúng làm một cách khác để mạng WiFi của bạn an toàn hơn. Bạn có thể tạo một danh sách truy cập MAC trên router WiFi. Danh sách truy cập này gồm các địa chỉ MAC từ những máy tính mà bạn muốn có thể kết nối với mạng WiFi của bạn. Mặc dù các danh sách truy cập MAC không phải là hệ thống an toàn để bảo vệ mạng WiFi, nhưng chúng từ chối việc xâm nhập của các hacker "ít tận tâm hơn".

80. Tạo một danh sách truy cập MAC mạng WiFi

Trước khi bạn bắt đầu

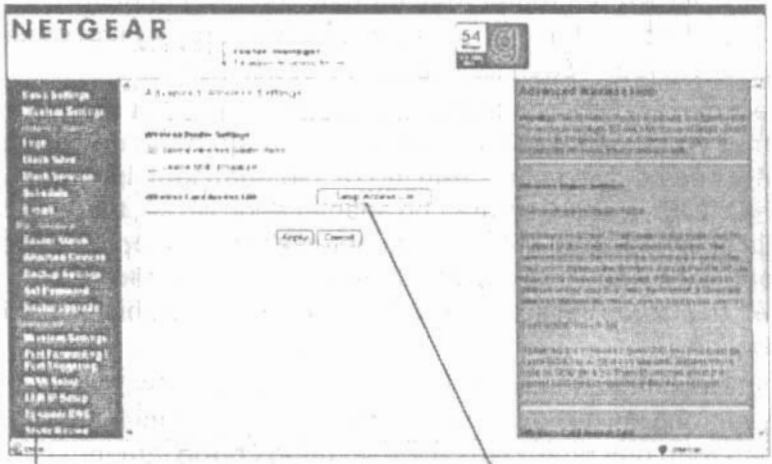
22 Truy cập cấu hình Router

79 Bàn về các địa chỉ MAC giao diện mạng

Hầu hết các router WiFi cung cấp cho bạn một danh sách các máy tính kết nối nhằm cho bạn dễ dàng thêm các máy tính được liệt kê vào chính danh sách truy cập MAC. Nếu bạn không có một danh sách đầy đủ các máy tính được kết nối (điều này đôi khi có thể xảy ra vì lý do không rõ ràng) hoặc bạn muốn thêm một máy tính vào danh sách hiện không được liệt kê, bạn phải biết các tên host và địa chỉ MAC hoặc phần cứng vật lý cho những máy tính mà bạn muốn đưa vào danh sách. Trên từng máy tính mà bạn muốn đưa vào danh sách truy cập MAC, hãy mở một dòng nhấp lệnh (nhấp Start, chọn Run, gõ nhập command và nhấn Enter). Tại dòng nhắc lệnh, gõ nhập ipconfig/all và nhấn Enter. Lệnh này liệt kê tên host, thông tin IP cho adapter mạng của máy tính và cũng là MAC / địa chỉ vật lý cho máy tính.

THỦ THUẬT: Để xóa sạch cửa sổ dòng nhắc lệnh các kết quả của các lệnh gần đây nhất, gõ nhập clear và nhấn Enter. Để đóng cửa sổ nhắc lệnh, gõ nhập Exit và nhấn Enter.

80. Tạo một danh sách truy cập MAC mạng WiFi



1. Truy cập các xác lập Wireless nâng cao

   Đăng nhập vào router bằng quyền administrator bằng cách sử dụng trình duyệt Web, gõ nhập URL cho router trong hộp Address của trình duyệt và sau đó cung cấp tên đăng nhập và password cho router khi được nhắc về thông tin này. Bạn có thể tìm thấy URL cho router trong tài liệu đi kèm router. Hoặc đi đến Web site của nhà sản xuất router, download tài liệu. Web site của nhà sản xuất cung cấp một trang hỗ trợ vốn sẽ giúp bạn tìm và download tài liệu cho router. Từ bất kỳ trang cấu hình của router, chọn lệnh Advanced Wireless Setting (hoặc lệnh tương tự trên trang Web của router). Link này cho phép truy cập một lệnh để thiết lập một danh sách truy cập MAC.

THỦ THUẬT: Lệnh thiết lập danh sách truy cập nằm trên cùng một trang cấu hình với lệnh để mở các broadcast SSJD của router.

2. Chọn lệnh Setup Access List
3. Mở chức năng kiểm soát truy cập

   Để router thực sự sử dụng danh sách mà bạn sẽ tạo là một cách để chấp nhận hoặc từ chối sự truy cập đến mạng WiFi, bạn phải mở tính năng kiểm soát truy cập. Chọn hộp kiểm Turn Access Control

On (hoặc lệnh tương tự). Bây giờ bạn có thể tạo danh sách các máy tính được phép truy cập mạng WiFi thông qua router.

4. Mở danh sách thiết bị

Nhấp nút Add để mở danh sách thiết bị. Một danh sách các máy tính hiện được kết nối và các địa chỉ MAC của các card mạng xuất hiện trên trang Wireless Card Access Setup.



3 Mở chức năng kiểm soát truy cập

4 Mở danh sách thiết bị

5. Chọn thiết bị và thêm vào danh sách truy cập



5 Chọn thiết bị và thêm vào danh sách truy cập

Chọn một thiết bị từ danh sách bằng cách chọn nút radio cho thiết bị. Nếu một máy tính (hoặc các máy tính) không được liệt kê trong danh sách thiết bị nhưng bạn biết rằng máy tính được kết nối với mạng WiFi, gõ nhập tên host và địa chỉ MAC cho máy tính đó trong các hộp text thích hợp. Nhấn nút Add. Máy tính (hoặc các máy tính nếu bạn đã chọn nhiều máy tính trong danh sách thiết bị) được thêm vào danh sách truy cập.

THỦ THUẬT: Danh sách truy cập sử dụng các nút radio để chọn một thiết bị cụ thể cho danh sách. Nhấp nút radio cho một thiết bị trong danh sách và sau đó bạn có thể xóa thiết bị ra khỏi danh sách bằng cách sử dụng lệnh Delete, nhấp lệnh Edit để chỉnh sửa địa chỉ MAC hoặc tên thiết bị được chọn. Bạn có thể chọn mỗi lần chỉ một thiết bị.

6. Áp dụng các xác lập danh sách truy cập

Danh sách truy cập được cập nhật và hiển thị mỗi lần bạn thêm một máy tính vào danh sách. Bạn có thể sử dụng nút Add để bổ sung thêm các máy tính vào danh sách. Khi bạn đã nhập xong các máy tính vào danh sách truy cập, áp dụng các xác lập vào router bằng cách nhấp nút Apply để lưu danh sách truy cập sang cấu hình của router.



THỦ THUẬT: Để loại bỏ một máy tính ra khỏi danh sách truy cập, chọn nút tùy chọn của máy tính và nhấp nút Delete. Sau đó nhấp nút Apply để áp dụng bất kỳ thay đổi mà bạn thực hiện đối với bất kỳ danh sách truy cập (chẳng hạn như các máy tính mới được bổ sung hoặc các máy bị được loại bỏ).

81. Cấu hình Remote Management

Trước khi bạn bắt đầu

22 Truy cập cấu hình Router

Khi bạn đã cài đặt và cấu hình router WiFi, bạn cần nối trực tiếp vào máy tính với router bằng một card mạng "hữu tuyến". Cấu hình của router sau đó được xử lý từ máy tính được nối trực tiếp. Sử dụng một máy tính được nối dây

với router dưới dạng configuration console cho router thì rất hợp lý về khía cạnh an ninh bởi vì chỉ máy tính được nối trực tiếp mới có thể được sử dụng để truy cập cấu hình của router, thậm chí nếu password của nhà quản trị router được biết bởi người nào đó ngoại trừ nhà quản trị.

Tuy nhiên, đôi khi bạn hãy xem những thông lệ an ninh và quyết định xem một thông lệ nào đó có trở nên bất tiện hay không. Bạn có thể cấu hình router để truy cập từ xa, nghĩa là router có thể được truy cập bởi bất kỳ một máy tính hoặc Internet. Bạn có thể chọn địa chỉ IP của máy tính hoặc các máy tính truy cập từ xa cho cấu hình của router hoặc bạn có thể cho phép tất cả máy tính truy cập cấu hình của router. Dĩ nhiên, bất kỳ người nào cố đăng nhập vào router thì phải cung cấp đúng tên đăng nhập và password.

Router được truy cập từ xa bằng địa chỉ IP "thật" mà nhà cung cấp dịch vụ internet đã cho (router nhận được tự động địa chỉ IP khi nó được kết nối với router DSL hoặc modem cable). Địa chỉ IP đầy đủ và phần mở rộng số cổng phải được gõ nhập vào một trình duyệt Web để truy cập router qua Internet thì nằm trên trang cấu hình nơi bạn thiết lập sự truy cập từ xa. Số cổng 8080 phải được đi cùng với địa chỉ IP để thiết lập kết nối với router, do đó nếu địa chỉ IP của router là 192.168.1.1, bạn phải gõ nhập 192.168.1.1:8080 vào hộp address của trình duyệt. Sau đó, gõ nhập tên đăng nhập và password để truy cập cấu hình của router.

Mặc dù sự truy cập từ xa chắc chắn có thể hữu ích khi ngồi tại bất kỳ máy tính và cấu hình nhanh router, nhưng nó có thể mở router ra trước một con đường tấn công khác. Nếu các hacker "biết được" cấu hình của router, họ có thể thay đổi password, cho phép những máy tính "ngoài vòng pháp luật" truy cập mạng của bạn và tắt hoàn toàn tín hiệu radio WiFi, tắt mạng của bạn. Do đó, bạn phải quyết định xem sự truy cập từ xa có phải là một điều tốt hay không. Chắc chắn bạn không được bắt buộc thiết lập sự truy cập từ xa nếu bạn nghĩ hóa ra nó gây ra vấn đề hơn là tiện lợi.

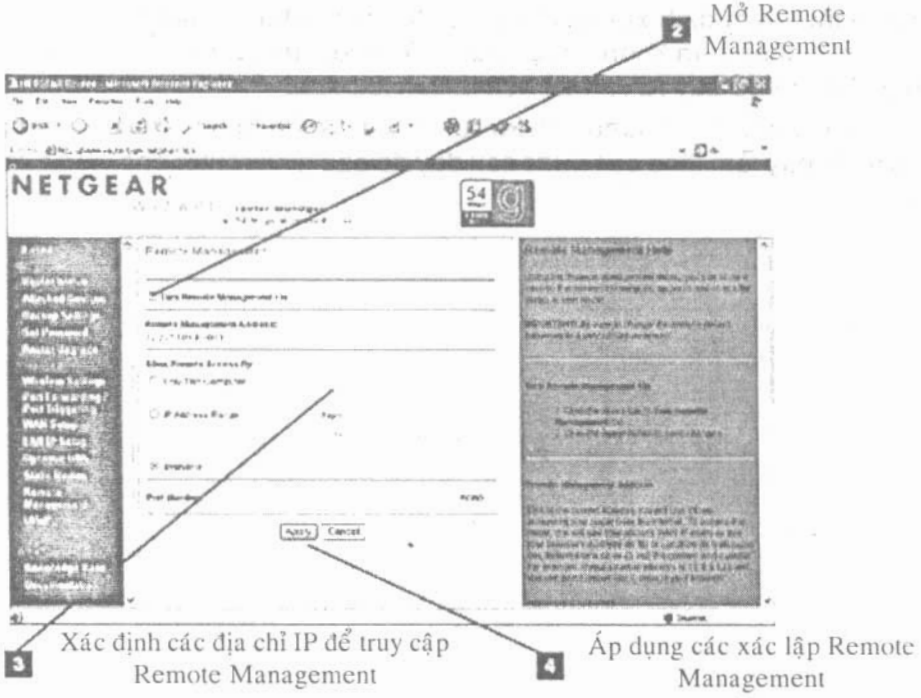
Nếu bạn quyết định những tiện lợi của router nhiều hơn những mối quan tâm an ninh, hãy làm theo các bước sau đây để cấu hình router cho việc quản lý từ xa:

81. Cấu hình Remote Management



1. Truy cập các xác lập Remote Management

Đăng nhập vào router bằng quyền administrator bằng cách sử dụng trình duyệt Web, gõ nhập URL cho router trong hộp Address của trình duyệt và sau đó cung cấp tên đăng nhập và password cho router khi được nhắc về thông tin này. Bạn có thể tìm thấy URL cho router trong tài liệu đi kèm router. Hoặc đi đến Web site của nhà sản xuất router và download thông tin này.



Từ trang cấu hình chính cho router, nhấp lệnh Remote Management. Trang Remote Management mở ra.

2. Mở Remote Management

   Nhấp hộp kiểm Turn Remote Management On để mở chức năng quản lý từ xa.

3. Xác định các địa chỉ IP để truy cập Remote Management

   Theo mặc định, tất cả địa chỉ IP trên mạng (mọi người) có thể truy cập router (nghĩa là bạn có thể truy cập router trên Internet từ bất kỳ máy tính trên mạng). Nếu bạn muốn xác định một máy tính để truy cập từ xa, nhấp nút tùy chọn Only This Computer và sau đó nhập địa chỉ IP của máy tính. Nếu bạn muốn truy cập từ xa router từ nhiều máy tính, nhấp nút tùy chọn IP Address Range, sau đó nhập các địa chỉ IP bắt đầu và kết thúc trong dãy.

THỦ THUẬT: Nếu các máy tính không nằm trong một dãy nhất quán, tắt nguồn router và sử dụng lệnh ipconfig/release để giải phóng các địa chỉ IP hiện hành. Sau đó tắt máy tính. Mở router, đợi trong giây lát để router khởi động và chạy, sau đó khởi động từng máy tính. Router sẽ cung cấp các địa chỉ IP mới cho các máy tính và dãy địa chỉ IP nằm theo trình tự (xem mục 97 để biết thêm chi tiết về lệnh ipconfig).

   Bạn sẽ cần địa chỉ IP "thật" của giao diện công cộng của router (giao diện được kết nối với Internet băng tần rộng) để kết nối với router Internet. Nếu bạn xem trang cấu hình Remote Management cho router, bạn sẽ thấy rằng địa chỉ quản lý từ xa được liệt kê ở đó. Bạn gõ nhập địa chỉ này như được minh họa và cũng đưa vào hậu tố 8080 để mở cổng HTTP trên router. Nhập thông tin này trong hộp Address của trình duyệt Web. Ví dụ nếu địa chỉ IPCONFIG công cộng là 192.5.6.7, gõ nhập http:// 192.5.6.7:8080 để truy cập router từ xa.

4. Áp dụng các xác lập Remote Management

   Sau khi bạn đã cấu hình các xác lập Remote Management, bạn phải lưu chúng sang cấu hình của router. Nhấp Apply để thực hiện điều này.

Chương 12

BẢO VỆ MẠNG KHÔNG DÂY

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *82 Bàn về Malware*
- *83 Cài đặt và sử dụng phần mềm chống virus*
- *84 Cập nhật phần mềm chống virus*
- *85 Kích hoạt Windows XP Security Center*
- *86 Bàn về Spyware*
- *87 Cài đặt AntiSpyware*
- *88 Sử dụng AntiSpyware*
- *89 Bàn về Spam Email và Outlook Express*
- *90 Cấu hình Rule Outlook Express*

Tận dụng khả năng router WiFi để bảo vệ an toàn hạ tầng Wireless (sử dụng các giao thức an ninh chẳng hạn như WPA) và bảo vệ mạng khỏi cuộc tấn công từ Internet bằng cách sử dụng những tính năng firewall của router chỉ là một phần trong cuộc chiến bảo vệ mạng của bạn và các máy tính trên mạng. Một vấn đề lớn đối với hầu như tất cả người dùng máy tính là khả năng máy tính bị nhiễm một virus phần mềm. Những mối đe dọa bao gồm các chương trình Trojan-horse, worm, và Spyware (phần mềm gián điệp).

Chương này sẽ trình bày các loại phần mềm lây nhiễm khác nhau có thể làm hư hại hệ thống và cách ngăn chặn chúng. Những mối đe dọa phần mềm hiểm độc này thường được gọi chung là malware.

82. Bàn về Malware

Trước khi bạn bắt đầu	Xem thêm
70 Bàn về an ninh mạng cơ bản	Mục 86

Giữ cho mạng khởi động và chạy sau khi bạn cấu hình router WiFi một cách chính xác là một sự nỗ lực rất lớn. Thế nhưng, mọi nỗ lực của chúng ta sẽ tiêu tan nếu chúng ta không xử lý phần mềm độc hại mà có thể vô hiệu hóa hoặc khống chế máy tính của chúng ta. Chúng ta đang nói về các virus, Trojan-horse, worm, và spyware. Phần mềm độc hại chẳng hạn như những phần mềm này thường được gọi chung là malware. Malware có thể là bất kỳ Malware được thiết để khai thác hoặc gây thiệt hại cho máy tính. Một sự xâm nhập máy tính gây phiền toái khác mà tất cả chúng ta phải giải quyết là spam email và tuy (thư rác) không thực sự được xem là malware nhưng nó có thể gây phiền toái như nhau.

THUẬT NGỮ CHÍNH

Malware: phần mềm độc hại chẳng hạn như các virus worm, và spyware

Thật may thay sự việc gây lo lắng là có vô số virus, worm và Trojan-horse ung dung tự tại có nghĩa rằng một số công cụ phần mềm hoàn hảo đã được phát triển để bảo vệ máy tính nhằm ngăn ngừa malware. Hãy xem các loại malware khác nhau và sau đó đi qua một số tác cụ để khai thác các cách bảo vệ máy tính.

Virus

Một mối đe dọa chắc chắn đối với máy tính (hoặc các máy tính) và an ninh của mạng là Virus. Một Virus là mã phần mềm tự sao chép nghĩa là nó có thể tạo các bản sao của chính nó. Việc một Virus tự sao chép có nghĩa là nó có thể lây lan dễ dàng từ máy tính này sang máy tính khác.

THUẬT NGỮ CHÍNH

Virus. Mã phần mềm độc hại tự sao chép có thể lây nhiễm các máy tính và làm hư hại hệ thống và các file khác.

Các Virus thường đòi hỏi hành động ở bạn trước khi chúng có thể lây nhiễm hệ thống. Ví dụ nếu bạn mở một file bị nhiễm được chia sẻ bởi một người dùng khác hoặc một file đính kèm email bị nhiễm, bạn sẽ làm lây nhiễm máy tính của bạn. Sau đó, Virus được lan truyền từ máy tính này sang máy tính khác trên một mạng . Các Virus cũng có thể được lây lan trên phương tiện tháo rời được chẳng hạn như các đĩa mềm, đĩa CD và USB.

Các Virus gồm nhiều biến thể, một số loại Virus đã phát triển qua nhiều năm. Những loại Virus này đã được phân loại dựa vào việc chúng có lây nhiễm một máy tính như thế nào.

Các Virus Boot sector: đầu tiên là những Virus Boot sector lây lan qua các đĩa mềm bị nhiễm hoặc phương tiện lưu trữ tháo rời được chẳng hạn như các đĩa CD. Khi một đĩa hoặc CD khởi động bị nhiễm được để lại trong một máy tính và máy tính được bật, máy tính cố khởi động sang phương tiện tháo rời được. Lúc khởi động, boot sector tải vào bộ nhớ của máy tính. Sau đó Virus có thể làm lây nhiễm ổ đĩa cứng hay bất kỳ đĩa mà bạn đặt trong ổ đĩa mềm sau khi máy tính khởi động và chạy. Một trong những Virus Boot sector đầu tiên là Virus BRAIN, Virus này thật sự không gây hại gì cho máy tính hoặc các file bị nhiễm. Tuy nhiên Virus có thể lây lan khá nhanh bởi vì các đĩa mềm thường được sử dụng và lưu trữ dữ liệu khi Virus BRAIN xuất hiện. Ngày nay hầu hết các máy tính sẽ khởi động sang một CD trừ khi bạn biết rằng máy tính nên làm như vậy.

Các Virus file: Mặc dù bây giờ khá khác thường, nhưng các Virus file thực sự lây nhiễm một file khả thi chẳng hạn như một file EXE hoặc COM. Khi file bị nhiễm được chạy, Virus file tải vào RAM của máy tính. Sau đó nó có thể làm lây nhiễm các file thực thi khác khi chúng được chạy trên máy tính. Một dạng của Virus file là Virus ghi đè. Các ví dụ về các Virus file bao gồm Virus Dark Avenger và Virus KMIT.

Các Virus Macro: Virus Macro là một Virus khá mới. Các Virus Maro thường được viết bằng mã Visual Basic và làm lây nhiễm các tài liệu và file dữ liệu thay vì các file thực thi. Khi một tài liệu BIOS nhiễm được tải vào một tài liệu chẳng hạn như Microsoft Word, mã Virus chạy giống như bất kỳ Macro khác trong ứng dụng cụ thể đó. Một điều gây sợ hãi khác về các Virus Macro là chúng không dành riêng cho hệ điều hành. Bởi vì các Microsoft Word có thể chạy trên một PC chạy trên nền Microsoft hoặc Windows, Virus Macro thật sự có thể được lây lan giữa hai nền nếu tài liệu Word được chia sẻ. Một ví dụ về Virus Macro là Virus Melissa rất nổi tiếng, đây là một loại virus Macro Word tự lây lan qua email.

Các Virus Multipartite: Virus Multipartite có đặc điểm của một Virus boot sector và một Virus file. Nó có thể lây lan từ boot sector của một ổ đĩa sang một ổ đĩa khác và nó cũng có thể tấn công các file thực thi trên máy tính. Thậm chí một số Virus Multipartite có thể lây nhiễm các drivers thiết bị (chẳng hạn như các drivers cho card giao diện mạng). Một ví dụ về một Virus Multipartite là Pastika, được kích hoạt chỉ vào các ngày nhất định của tháng (thường là ngày 21 và 22 của tháng) và có thể thực sự ghi đè ổ đĩa cứng.

Số Virus thực sự trong môi trường "hoang dã" có thể thay đổi nhưng nói chung con số này đang tăng lên.

Cách duy nhất bạn có thể bảo vệ máy tính khỏi bị nhiễm Virus là cài đặt phần mềm chống Virus trên máy tính và cập nhật nó. Không may, việc ngăn

chặn một Virus nào đó không trở thành một phần của những tính năng phần mềm chống Virus cho đến khi Virus "được mọi người biết đến". Điều này có nghĩa là luôn có một thời gian chậm trễ giữa sự xuất hiện của Virus và khả năng phần mềm chống Virus ngăn ngừa nó.

THỦ THUẬT: Một nơi tốt để tìm thông tin liên quan đến các Virus là SANS. SANS tại http://www.sans.org cung cấp thông tin về những Virus và những vấn đề an ninh mạng khác. Bạn cũng có thể tìm thấy thông tin về Virus hiện hành và những mối đe dọa Malware khác bằng cách kiểm tra Web site của phần mềm khác chống Virus mà bạn sử dụng.

Worm và Trojan Horse

Các Virus không phải là những mối đe dọa Malware duy nhất lây nhiễm máy tính. Cũng có các worm và Trojan Horse.

Worm là chương trình tự lây lan từ máy tính này sang máy tính khác trên một mạng. Nó không cần được kích hoạt bởi bạn như đối với một Virus. Worm thường dành riêng cho một hệ điều hành (chẳng hạn như Windows) và khai thác một điểm yếu nào đó trong hệ điều hành. Các worm thường khai thác các cổng mở và có thể thật sự khống chế một máy tính và sử dụng nó trong các cuộc tấn công từ chối dịch vụ (DOS).

THUẬT NGỮ CHÍNH

Worm. Mã phần mềm Malware tự lây lan và tự kích hoạt thường khai thác một điểm yếu nào đó trong trong một hệ điều hành.

Trojan Horse. Malware mà có vẻ như là một chương trình bình thường nhưng khi được thực thi có thể khai thác một hệ thống nào đó. Việc chương trình độc hại giả dạng là một chương trình bình thường là lý do tại sao loại Malware cụ thể này được gọi là Trojan Horse (ngựa thành Troa).

Mặc khác, Trojan Horse là một chương trình có vẻ hoàn toàn vô hại chẳng hạn như một screensaver hoặc game. Ví dụ Trojan Horse HAPPY99.EXE mà khi được thực thi cung cấp một màn trình diễn pháo bông nhỏ thú vị trên màn hình và sau đó thì sử dụng các địa chỉ mail được tìm thấy trong Email client của máy tính để gởi đi các bản sao của chính nó đến những địa chỉ này (điều này tương tự như cách Virus Malware được lây lan).

Một trong những Trojan Horse sớm nhất là AIDS Information Disk Trojan vốn thực sự là một đĩa được gởi đi đến các cơ sở y tế dưới dạng một sản phẩm ý thức AIDS. Sau khi được thực thi, file Trojan Horse đã tạo một thư mục ẩn

trên ổ đĩa cứng của máy tính và cuối cùng mã hóa toàn bộ nội dung của ổ đĩa cứng làm cho nó không thể sử dụng được.

Trong những mối đe dọa lớn nhất liên quan đến các Trojan Horse là một số Trojan Horse có có thể xâm nhập vào một máy tính và cho phép kiểm soát từ xa máy tính bị lây nhiễm bởi người tạo ra Trojan Horse (hacker). Điều này cho phép hacker đánh cắp thông tin cá nhân và cũng sử dụng máy tính trong các cuộc tấn công hàng loạt trên các server Web site.

83. Cài đặt và sử dụng phần mềm chống virus

Trước khi bạn bắt đầu

82 Bàn về Malware

Nhiều chương trình chống Virus có sẵn trong hệ điều hành Windows: Norton Antivirus, Computer Associates EZ Antivirus, PC-cillin và Kaspersky Anti-Virus đó là chỉ nói đến một số tiêu biểu. Phần mềm chống Virus mà bạn thật sự sử dụng là tùy thuộc vào bạn. Mặc dù các cuộc thử nghiệm cho thấy một số chương trình chống Virus phát hiện và gỡ bỏ các Virus ít được biết đến tốt hơn, nhưng việc có bất kỳ phần mềm chống Virus cập nhật là một khía cạnh quan trọng của việc bảo vệ các phần mềm máy tính khỏi sự xâm nhập của Malware.

THỦ THUẬT: Hầu hết các nhà cung cấp nối kết Internet băng tần rộng chẳng hạn như Verizon Time Warner, AOL và những nhà cung cấp khác cung cấp cho bạn phần mềm chống Virus miễn phí. Thậm chí một số công ty cung cấp các bộ chống Malware bao gồm các sản phẩm chống Virus, chống Malware và chống ????. Hãy liên lạc với nhà cung cấp dịch vụ Internet của bạn trước khi mua phần mềm chống Virus bởi vì bạn có thể download nó miễn phí.

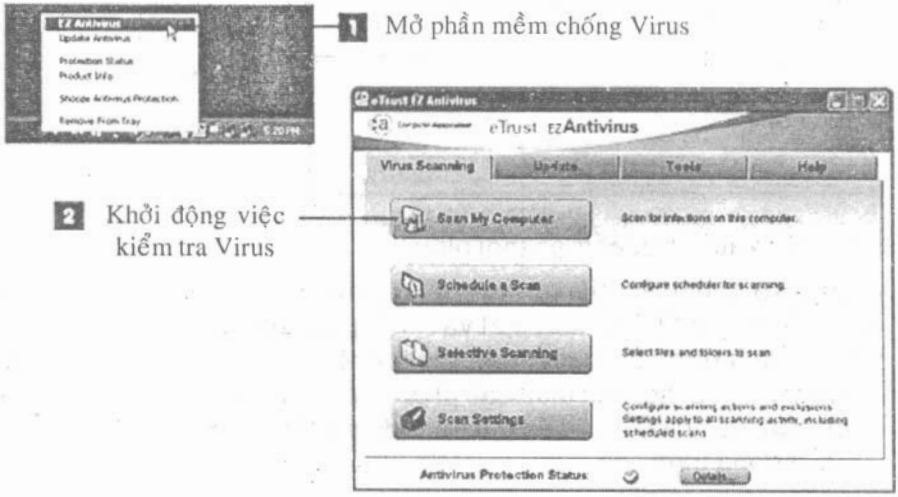
Một số chương trình chống Virus được đính kèm trong các bộ phần mềm an ninh cũng bao gồm phần mềm chống spyware, lọc spam email và thậm chí firewall. Các ví dụ bao gồm AVC, Anti-Virus cộng với firewall Edition và Nonrtoni Internet Security 2005 AntiSpyware Edition. Bởi vì Windows XP đã có một firewall cá nhân, bạn không cần phải mua một bộ phần mềm chống Virus vốn cũng cung cấp một firewall phần mềm. Tuy nhiên, mua phần mềm chống Virus có những tính năng lọc spam và chống spyware giúp bạn dễ dàng cập nhật chỉ một sản phẩm chống malware thay vì những sản phẩm riêng biệt để phát hiện Virus, malware, spyware và lọc spam.

THỦ THUẬT: Hầu hết các nhà sản xuất phần mềm chống Virus cho phép bạn download một phiên bản dùng thử của sản phẩm. Sau đó, bạn có thể mua một license để tiếp tục

sử dụng sản phẩm. Một số chương trình chống Virus cũng cho phép bạn mua giảm giá, điều này lý tưởng nếu bạn có một số máy tính trên mạng gia đình cần phần mềm chống Virus. Hãy nhớ rằng mỗi máy tính cần license riêng của nó cho phần mềm. Đừng e ngại thử phần mềm chống Virus khác nhau. Các sản phẩm khác nhau về tính sử dụng và hiệu quả do đó đây là một lựa chọn mang tính cá nhân. Xem các bài bình luận trên Web liên quan đến các phần mềm chống Virus và chọn sản phẩm mới nhất cho máy tính của bạn.

Khi bạn chạy phần mềm chống Virus, bạn có thể tiếp tục sử dụng máy tính nhưng bạn sẽ thấy máy tính chạy chậm. Việc chạy tiến trình chống Virus sẽ hợp lý hơn khi bạn không sử dụng máy tính trong một khoảng thời gian chẳng hạn như ban đêm hoặc trong giờ ăn trưa.

83. Cài đặt và sử dụng phần mềm chống virus



1. Mở phần mềm chống Virus.

   Nhấp phải biểu tượng chương trình phần mềm chống Virus trong Windows System Tray và chọn lệnh vốn mở phần mềm chống Virus chẳng hạn lệnh EZ Antivirus mở cửa sổ phần mềm EZ Antivirus.

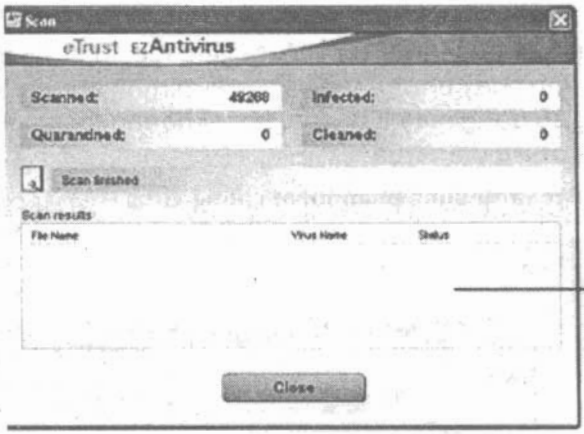
2. Khởi động việc kiểm tra Virus

   Bắt đầu kiểm tra Virus bằng cách nhấp Scan My Computer hoặc lệnh tương tự trong cửa sổ phần mềm chống Virus. Phần mềm chống Virus sẽ kiểm tra các boot sector trên ổ đĩa cứng của máy tính để tìm các Virus và sau đó kiểm tra các file của máy tính.

   Khi tiến trình quét virus hoàn tất, phần mềm cung cấp cho bạn mọi số liệu thống kê liên quan đến tiến trình quét chẳng hạn như số file

đã được quét và virus nào đã được phát hiện và được diệt. Để đóng hộp thoại liên quan đến việc hoàn tất quá trình quét, nhấp OK.

THỦ THUẬT: Bạn có thể xác định chương trình quét Virus xem chỉ các folder hoặc ổ đĩa được chọn trên máy tính. Nhấp nút Selective Scanning hoặc lệnh tương tự trong cửa sổ chính của chương trình quét Virus sau đó chọn ổ đĩa và folder mà bạn muốn trong chương trình quét.



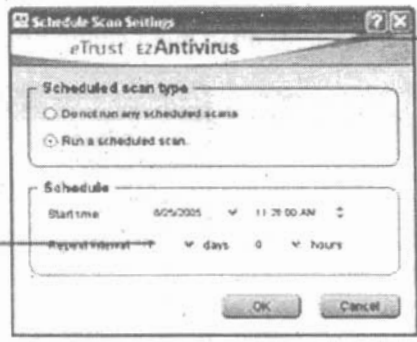
3. Mở các xác lập quét theo thời biểu

Bạn nên cấu hình phần mềm chống virus để nó chạy theo định kỳ. Bạn có thể thiết lập việc quét vào mỗi lần bạn không sử dụng máy tính. Cách bạn cấu hình phần mềm chống Virus để chạy tự động theo thời biểu thay đổi giữa các phần mềm khác nhau. Trong trường hợp của EZ Anitvirus, nhấp nút Schedule a Scan trên màn hình chính của chương trình.

4. Xác lập thời biểu quét

Để xác lập thời biểu quét, nhấp nút tùy chọn Run a Scheduled Scan hoặc một tùy chọn tương tự. Sau đó, xác lập ngày tháng bắt đầu, thời gian bắt đầu và khoảng thời gian lập lại. Nếu bạn muốn máy tính được quét mỗi lần một tuần chẳng hạn xác lập khoảng thời gian lặp lại sang 7. Xác lập khoảng thời gian để chạy tiến trình quét Virus tùy thuộc vào bạn. Hầu hết phần mềm chống Virus cung cấp khả năng chống Virus thời gian thật và báo động cho bạn biết nếu một Virus hoặc Malware khác cố xâm nhập hệ thống của bạn. Phần mềm chống Virus không nhất thiết bắt giữ nhanh tất cả malware, do đó bạn nên chạy phần mềm chống Virus tối thiểu mỗi tuần một lần. Chạy nó thường xuyên hơn nếu bạn download nhiều file từ Internet hoặc mở các phần đính kèm email, gởi đến bạn bởi những người mà bạn không quen biết.

Khi bạn đã xác lập xong các tham số lập thời biểu quét, nhấp OK để đóng hộp thoại.



THỦ THUẬT: Nếu một Virus không thể bị diệt, báo cáo được cung cấp bởi phần mềm chống Virus sẽ nêu chi tiết thông tin này hoặc cho biết tên của các file bị nhiễm. Trong một số trường hợp, có thể bạn phải cập nhật phần mềm chống Virus để xóa sạch Virus ra khỏi hệ thống. Trong những trường hợp khác, có thể bạn phải làm theo hướng dẫn được cung cấp trên Web site của công ty phần mềm chống Virus hoặc download một chương trình diệt virus, worm hoặc Trojan Horse vốn không thể diệt được bằng phần mềm chống Virus.

84. Cập nhật phần mềm chống Virus

Trước khi bạn bắt đầu

82 Bàn về Malware

83 Cài đặt và sử dụng phần mềm chống Virus

Cập nhật phần mềm chống Virus thì cực kỳ quan trọng. Các Virus mới và Malware luôn xuất hiện và các nhà sản xuất phần mềm chống Virus làm việc liên tục để nhận dạng và diệt tận gốc những mối đe dọa Malware mới. Những nhà cung cấp phần mềm thường xuyên tung ra các bảng cập nhật cho phần mềm chống Virus. Hãy nhớ rằng phần mềm chống Virus lỗi thời thì tệ như là không có phần mềm chống Virus gì cả.

Nhiều gói phần mềm chống Virus tự động kết nối với một Web site để kiểm tra tìm thông tin mới mỗi lần bạn mở máy tính và Windows chạy. Tuy nhiên, điều này không luôn như vậy do đó bảo đảm các chữ ký chống Virus (file được sử dụng để nhận dạng và diệt Virus) được cập nhật. Điều này có nghĩa bạn nên biết cách cập nhật bằng thủ công phần mềm chống Virus. Đối với mức độ thường xuyên bạn kiểm tra để tìm các bản cập nhật, việc làm điều này mỗi ngày thì chẳng hề gì cả bởi vì tiến trình download và cài đặt cho bản

cập nhật thường khá ngắn. Các Virus và malware mới xuất hiện mỗi ngày do đó tại sao không bảo đảm phần mềm chống Virus của bạn cập nhật mỗi ngày?

84 Cập nhật phần mềm chống Virus



1. Khởi động Antivirus Update

   Bạn có thể khởi động việc cập nhật phần mềm cho hầu hết các Virus từ desktop Windows XP. Tìm biểu tượng của phần mềm chống Virus trong system tray Windows và nhấp phải biểu tượng. Chọn Update Antivirus hoặc một lệnh tương tự để ở cửa sổ cập nhật chương trình chống Virus. Một số chương trình phần mềm chống Virus không đặt một biểu tượng trong system tray (khay hệ thống) nhưng sẽ cung cấp một lựa chọn menu (mà bạn có thể truy cập cho đến khi bạn khởi động phần mềm) nhằm cho phép bạn cập nhật phần mềm. Bạn sẽ thường tìm thấy lệnh này trong menu Tools (hoặc một menu có tên tương tự).

2. Download bất kỳ bản cập nhật

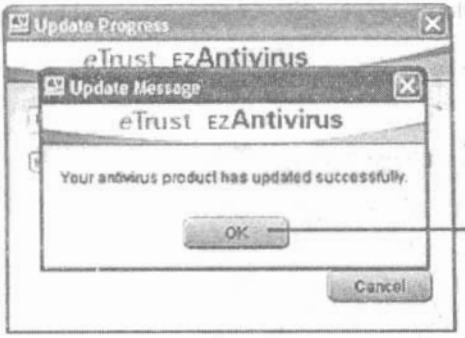
   Chương trình cập nhật chống Virus sẽ kết nối với Web site của nhà cung cấp phần mềm và download bất kỳ bản cập nhật có sẵn. Khi các file cập nhật được download, phần mềm cài đặt tự động cập nhật các file cập nhật.

3. Đóng cửa sổ Update

   Khi việc cập nhật hoàn tất, nhấp OK để đóng cửa sổ cập nhật chống Virus.

Ghi chú

Nếu phần mềm chống Virus đã cập nhật, một thông báo sẽ xuất hiện cho bạn biết rằng không có sẵn các bản cập nhật mới. Trong trường hợp này, bạn có thể đóng cửa sổ Update ngay tức thì.



85. Kích hoạt Windows XP Security Center

Trước khi bạn bắt đầu

82 Bàn về Malware

83 Cài đặt và sử dụng phần mềm chống Virus

71 Bàn về các Firewall

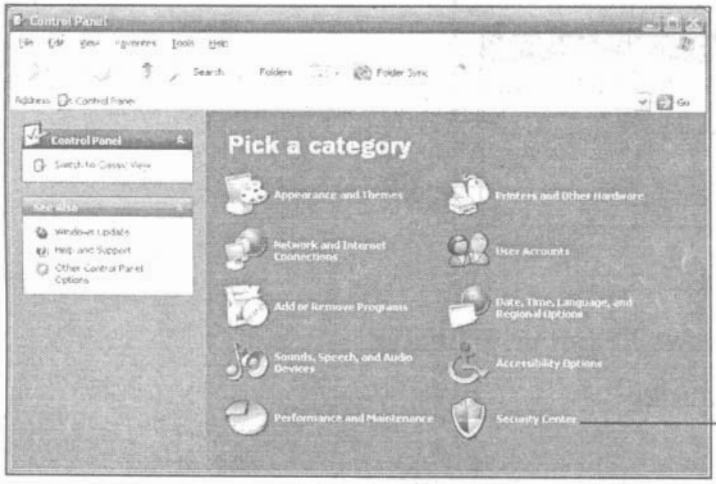
Windows XP đã trải qua nhiều chuyển biến dưới dạng các Service Pack. Với việc tung ra Service Pack 2 (SP2), một tính năng mới được thêm vào Windows XP có tên là Windows XP Security Center.

THỦ THUẬT: Nếu bạn không có Service Pack 2 (nhấp nút Start, nhấp phải tùy chọn My Computer và chọn Properties từ menu ngữ cảnh, hộp thoại Properties cho bạn biết phiên bản Windows mà bạn đang chạy kể cả bất kỳ Service Pack đã được cài đặt), đi đến www.microsoft.com và download nó. Bạn sẽ phải khởi động lại máy tính trước khi các bản cập nhật có hiệu lực. Nếu bạn đã kích hoạt Automatic Updates trong Security Center, rất có khả năng hệ thống của bạn đã được nâng cấp lên thành Service Pack 2.

Microsoft đã cố gắng giảm bớt những lỗ hổng an ninh trong hệ điều hành Windows XP ban đầu. SP2 đã cung cấp một firewall cá nhân mới cho Windows cũng như Security Center vốn giám sát những xác lập an ninh chẳng hạn như việc phần mềm chống Virus có cập nhật hay không và việc Windows automatic update có được mở hay không. Security Center có thể được cấu hình để giám sát những xác lập an ninh chẳng hạn như firewall Windows hoặc bạn có thể tắt những tính năng giám sát của Security Center.

Bạn nên sử dụng Security Center bởi vì nó giúp bạn cập nhật phần mềm chống Virus và hệ điều hành Windows. Windows firewall cũng có thể bảo vệ thêm cho máy tính của bạn cùng với firewall của router WiFi.

85. Kích hoạt Windows XP Security Center



1. Mở Security Center

   Từ Windows Control Panel (nhấp nút Start và chọn Control Panel), nhấp biểu tượng Security Center. Cửa sổ Security Center mở ra.

   Nếu bất kỳ thành phần Security Center (Firewall, Automatic Updates hoặc Virus Protection) được tắt, một nút Off màu đỏ xuất hiện kế bên thành phần đó. Nút Off xuất hiện kế bên thành phần Virus Protection chỉ khi phần mềm chống Virus không được cài đặt trên máy tính hoặc nếu Security Center không thể nhận ra phần mềm chống Virus là đã được cài đặt.

Ghi chú

Một chương trình phần mềm chống Virus không được nhận biết bởi Security Center. Nhưng điều đó không có nghĩa bạn cần cài đặt lại phần mềm hoặc mua một chương trình chống Virus khác. Chỉ hãy chắc chắn rằng bạn cập nhật phần mềm chống Virus (download và cài đặt theo định kỳ) bởi vì Security Center sẽ không thể cảnh báo cho bạn biết khi nào phần mềm chống Virus của bạn đã cũ (out of date).

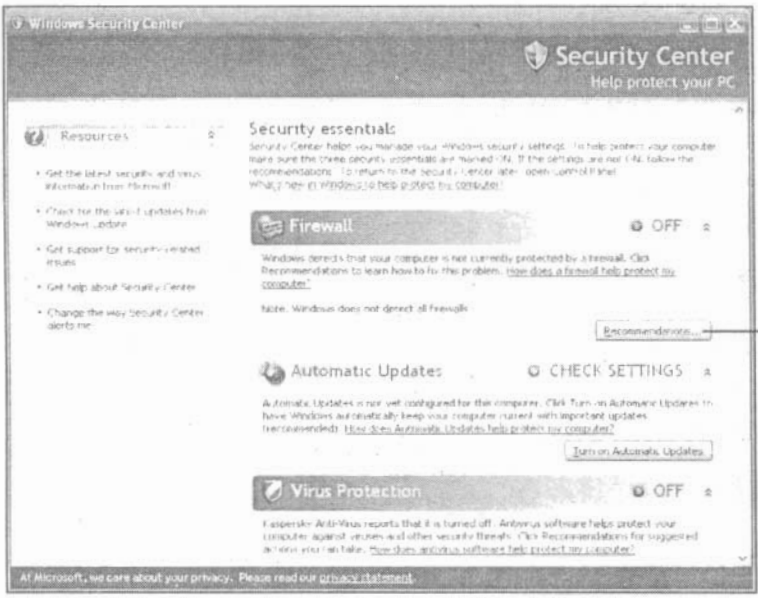
2. Mở Firewall Recommendations

   Nếu firewall được tắt (Off), bạn nên mở (On) nó. Nhấp nút Recommendations. Hộp thoại Recommendations mở ra.

Ghi chú

Nếu bạn sử dụng một firewall phần mềm khác chẳng hạn như một firewall vốn là thành phần của bộ phần mềm chống Virus, bạn có thể tắt Microsoft firewall.

Việc chạy nhiều firewall phần mềm trên một máy tính có thể làm giảm tốc độ hiệu suất và những vấn đề khác.



2. Mở Firewall Recommendations

3. Mở Firewall Windows

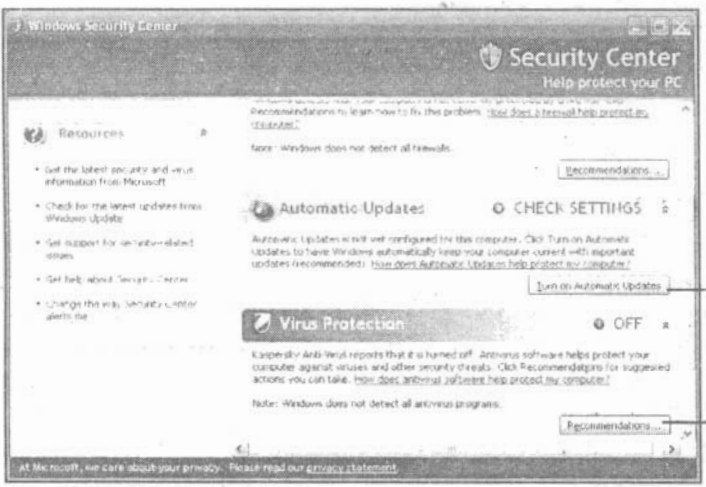
Để mở firewall, nhấp nút Enable now trong hộp thoại Recommendations. Nhấp OK để đóng hộp thông báo và sau đó nhấp OK lần nữa để đóng hộp thoại Recommendations. Nút firewall bây giờ là On trong cửa sổ Security Center.



4. Mở Automatic Updates

Chắc chắn bạn nên cập nhật phần mềm Windows bởi vì các mối đe dọa an ninh mới thường xuất hiện và Microsoft phân phối các bản sửa lỗi an ninh cho Windows để loại trừ các mối đe dọa. Nhấp nút

Turn on Automatic Updates. Bây giờ Windows sẽ đưa ra cho bạn một cảnh báo trong system tray bất cứ khi nào bản cập nhật mới đã được download và nên được cài đặt.



4. Mở Automatic Updates

5. Mở Antivirus Recommendations

Ghi chú

Nếu bạn đã cấu hình Security Center để báo cho bạn biết khi nào có sẵn một bản cập nhật Windows (nghĩa là bạn đã mở Automatic Updates), Windows đặt một biểu tượng cảnh báo trong system tray. Làm theo lời khuyên của cảnh báo bằng cách nhấp cảnh báo, bản cập nhật sẽ được cài đặt tự động trên hệ thống. Đừng e ngại những cảnh báo cập nhật. Đây không phải là một mã mánh nào đó đang cố đánh lừa bạn cài đặt malware trên máy tính. Nếu bạn thật sự không thích các bảng cập nhật tự động (Automatic Updates) thì đừng mở chúng. Trách nhiệm của bạn là định kỳ đi đến Web site Windows Updates và cho phép site quét máy tính của bạn và cài đặt bất kỳ bản cập nhật có sẵn (các bản cập nhật bất kỳ được cung cấp bởi Web site Updates luôn được cài đặt). Để đi đến Web site Windows Updates, nhấp nút Start, chọn All Programs và sau đó chọn Windows Updates.

5. Mở Antivirus Recommendations

Security Center có thể giám sát việc phần mềm chống của bạn có cập nhật hay không. Nếu Security Center thấy phần mềm của bạn không cập nhật, nó sẽ đưa ra một cảnh báo trong system tray. Bạn nên để cho Security Center theo dõi phần mềm chống Virus và các bản cập nhật của nó.

Nhấp nút Recommendations trong hộp Virus Protection của Security Center. Hộp thoại Recommendations mở ra.

6. Mở Security Center để giám sát phần mềm chống Virus

Hủy chọn hộp kiểm I have an antivirus program that i'll monitor myself và nhấp OK để đóng hộp thoại Recommendations. Bây giờ Security

Center sẽ đưa ra các cảnh báo liên quan đến các Windows firewall, Windows Updates và tình trạng của phần mềm chống Virus.



6. Mở Security Center để giám sát phần mềm chống Virus

86. Bàn về Malware

Trước khi bạn bắt đầu

82 Bàn về Malware

Mặc dù các Virus, worm, Trojan Horse gây ra những thứ nguy hiểm tiềm ẩn đối mạng gia đình của bạn, nhưng phần mềm chống Virus cập nhật và kinh nghiệm thực tế trong việc download và mở các file lạ có thể góp phần giảm thiểu mối đe dọa. Tuy nhiên, một loại malware mới được gọi là spyware đã trở thành mối đe dọa nổi bật nhất, có tính lây lan nhất và gây phiền toái nhất cho máy tính cá nhân.

Spyware là malware lén lút thu thập thông tin bằng cách sử dụng nối kết Internet của máy tính. Spyware thường được ẩn trong phần mềm miễn phí và những chương trình khác có thể download từ Web. Spyware có thể thật sự giám sát hoạt động của một người dùng trên Web và thu nhập thông tin liên quan đến các sở thích sản phẩm và lịch sử (history) duyệt. Một số malware cũng có thể thu thập thông tin liên quan đến các password và những giao dịch khác trên Web, bao gồm những giao diện nơi bạn nhập số thẻ tín dụng.

THUẬT NGỮ CHÍNH

Spyware. Malware lây nhiễm máy tính qua phần mềm miễn phí và các bản download từ các Web site. Spyware thu thập thông tin từ những người dùng chẳng hạn như những sở thích duyệt và thông tin được sử dụng trong các giao dịch web chẳng hạn như các password và số thẻ tín dụng. Một sự lây nhiễm spyware thường có

những biểu hiện chẳng hạn như chức năng máy tính chậm đi (bởi vì malware sử dụng các nguồn tài nguyên hệ thống của máy tính kể cả bộ nhớ và một nối kết Internet dường như chậm đi. Vấn đề với malware là nó thật sự chỉnh sửa với registry Windows và làm cho nó trở thành một phần của cấu hình Windows, tương tự như các chương trình "bình thường" thường làm khi chúng được cài đặt.

Một loại Malware thậm chí ngấm ngầm hơn được gọi là rootkit thật sự kích hoạt trong quá trình khởi động hệ thống; các rootkit khó phát hiện bởi vì chúng chạy trước khi phần mềm chống spyware và chống Virus tải. Các rootkit spyware có thể cài đặt tất cả loại file ẩn trên hệ thống và thậm chí chặn dữ liệu từ mạng.

Spyware đã trở thành một mối quan tâm lớn về hiệu suất lớn của máy tính (spyware làm hao mòn các tài nguyên hệ thống) và việc thông tin cá nhân có thể bị đánh cắp đặc biệt nếu bạn sử dụng máy tính để mua hàng trực tuyến. Một số gợi ý phần mềm chống spyware được cung cấp trong mục 87.

THỦ THUẬT: Máy tính của bạn cũng có thể bị nhiễm adware, phần mềm được đưa vào như là thành phần của phần mềm miễn phí hoặc một dịch vụ trên một Web site nào đó. Adware có thể tạo ra những quảng cáo pop-up gây phiền toái. Adware có thể được gỡ bỏ khỏi hệ thống bằng cách sử dụng một số công cụ tương tự vốn gỡ bỏ spyware khỏi hệ thống. Tuy nhiên, để chạy một số phần mềm miễn phí chẳng hạn như Jmesh và Morpheus (cả hai ứng dụng chia sẻ file nhạc ngang hàng vốn cài đặt adware trên hệ thống, bạn phải chịu dựng adware mà về cơ bản là một "chi phí" sử dụng phần mềm mà bạn đã không thanh toán bằng tiền.

---

87. Cài đặt Spyware

Trước khi bạn bắt đầu

82 Bàn về Malware

86 Bàn về Spyware

Nếu bạn lướt web nhiều (kể cả download các file) và bạn cũng sử dụng web để mua hàng trực tuyến, bạn nên cài đặt phần mềm chống spyware trên máy tính. Spyware có thể được cài đặt trên máy tính mà bạn không hề biết sẽ làm chậm đi hiệu suất của máy tính và trong những tình huống tột cùng dẫn đến việc đánh cắp thông tin nhận dạng đặc biệt nếu thông tin bạn nhập để mua hàng trực tuyến chẳng hạn như một số thẻ tín dụng mà spyware ghi chép được.

Có sẵn một số phần mềm chống spyware. Hầu hết sản phẩm này chạy như một chương trình chống Virus và sẽ kiểm tra Windows Registry (một cơ sở dữ liệu các xác lập Windows và phần mềm được cài đặt) để tìm xem bất kỳ spyware có thêm vào phần mềm được cài đặt hay không. Một số sản phẩm chống spyware này cũng cung cấp khả năng bảo vệ thời gian thật và ngăn chặn việc cài đặt spyware trên hệ thống. Như với các chương trình chống vi rút, bạn cần cập nhật phần mềm chống Spyware sao cho nó để gỡ bỏ hoặc ngăn chặn các dạng Spyware gần đây nhất. Một số sản phẩm chống spyware hoạt động tốt được liệt kê ở đây:

- *Spybot (Search and Destroy)*

  http://www.safer-networking.org

  Spybot là một sản phẩm chống Virus miễn phí. Spybot cung cấp những tính năng chống spyware thời gian thật và những người tạo ra nó cung cấp các bản cập nhật đúng lúc.

- *Ad-Aware*

  http://www.lavasoftusa.com/software/adaware

  Ad-Aware có ở nhiều dạng khác nhau, bao gồm ấn bản (edition) Personal miễn phí và ấn bản Plus. Phiên bản miễn phí làm tốt công việc loại bỏ spyware (và adware) đã có trên hệ thống. Tuy nhiên, bạn cần ấn bản Plus để có được thời gian thật nhằm ngăn spyware không được cài đặt trên hệ thống khi bạn duyệt web.

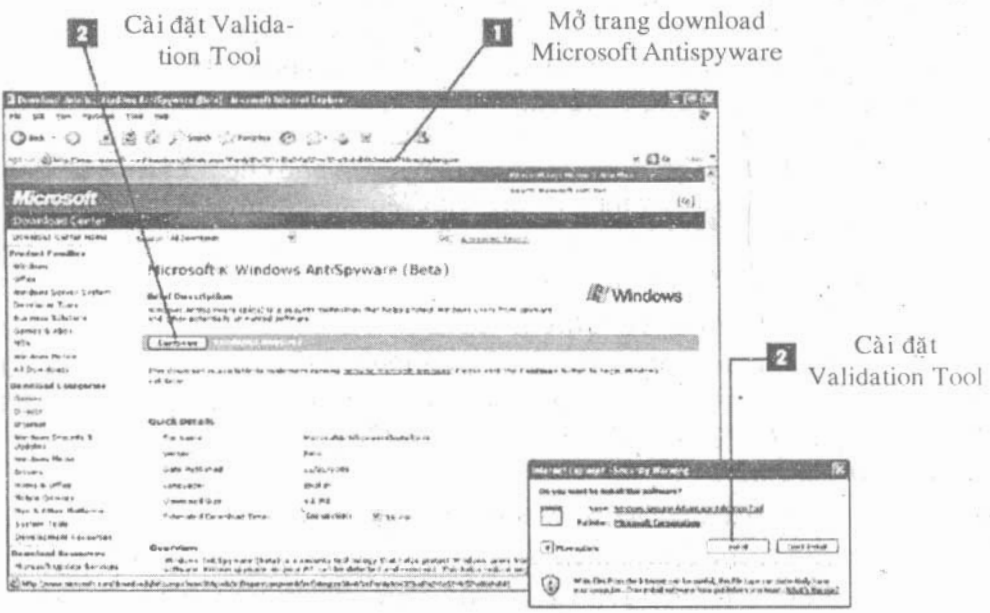
- *Microsoft Windows AntiSpyware*

  http://www.microsoft.com/downloads/

  Microsoft Windows AntiSpyware thậm chí làm tốt công việc trong phiên bản Beta và cung cấp sự bảo vệ thời gian thật và ngăn chặn spyware. Nó cũng cho phép bạn gỡ bỏ spyware đã có trên hệ thống.

Trong tác vụ này, bạn sẽ download, cài đặt và sử dụng phần mềm Windows spyware bởi vì nó hiện có sẵn cho tất cả người dùng Windows XP.

87. Cài đặt Antispyware



1. Mở trang download Microsoft Antispyware

   Mở trình duyệt web và đi đến site download Microsoft Antispyware tại http://www.microsoft.com/downloads/details.aspx?FamilyID=321cd7a2-6a57-4c57-a8bd-dbf62eda9671&displaylang=en. Bởi vì các trang download thực sự cho các add-on Microsoft có thể thay đổi theo thời gian bạn cũng có thể đi đến http://www.microsoft.com và tìm trang download Antispyware.

   Trước khi có thể download phần mềm Antispyware, bạn phải cập nhật hệ thống bằng một công cụ hiệu lực hóa (validation tool) vốn kiểm tra xem hệ thống có chạy một phiên bản "chính thức" (nghĩa là được đăng ký) từ Windows XP hay không. Nhấp nút Continue. Một hộp thoại Security Warning mở ra.

2. Cài đặt Validation Tool

   Trong hộp thoại Security Warning, nhấp nút Install. Validation Tool sẽ được cài đặt và trang download cho phần mềm Microsoft Antispyware mở ra.

3. Download Antispyware

   Nhấp nút download. Một hộp thoại file download mở ra. Nhấp Run để cài đặt phần mềm sau khi nó được download xuống hệ thống. Trong hộp thoại an ninh thứ hai vừa mở ra nhấp Run lần nữa. Microsoft Antispyware Wizard xuất hiện. Làm theo các bước để hoàn tất việc cài đặt phần mềm.



4. Cài đặt Microsoft Antispyware

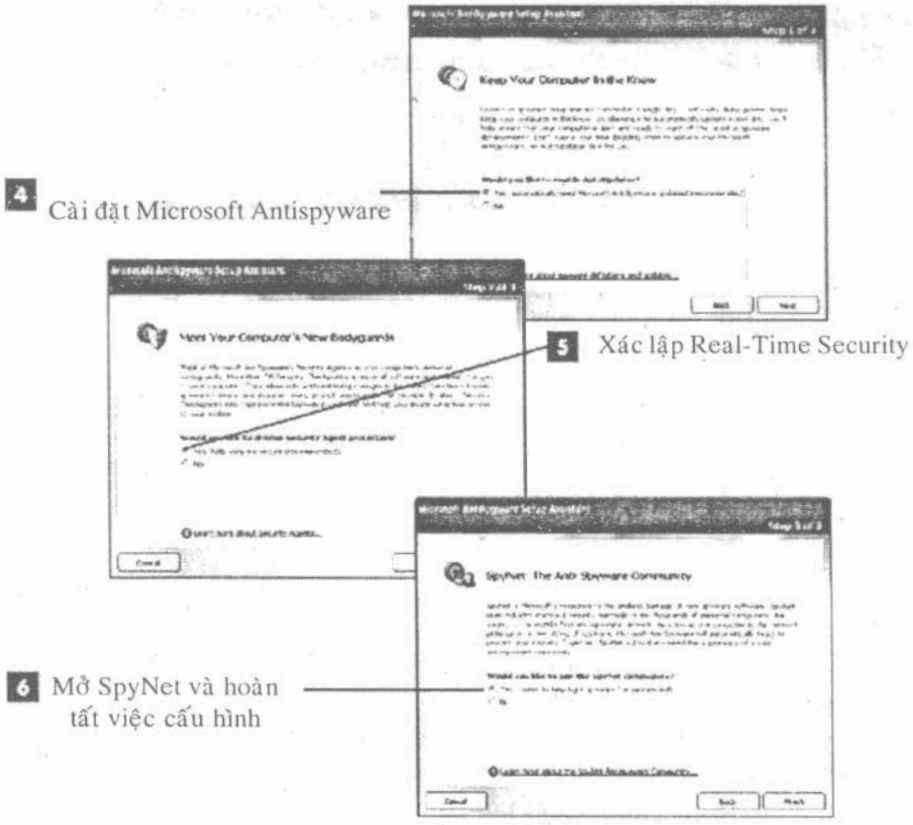
   Sau khi cài đặt, một wizard mở ra giúp bạn cài đặt Microsoft Antispyware. Nhấp nút Next để bỏ qua màn hình ban đầu. Trên màn hình kế tiếp, bạn hãy chắc chắn nút tùy chọn Yes, automatically keep Microsoft Antispyware Updates được chọn và sau đó nhấp next để tiếp tục.

5. Xác lập Real-Time Security

   Trên màn hình kế tiếp, bạn hãy chắc chắn nút tùy chọn yes, help me secure được chọn. Tùy chọn này cho phép phần mềm có khả năng ngăn chặn việc cài đặt spyware khi bạn lướt Web. Nhấp Next để tiếp tục.

6. Mở SpyNet và hoàn tất việc cấu hình

   Màn hình kế tiếp cung cấp tùy chọn để trở thành một phần spyware của Microsoft, vốn là một mạng peer-to-peer chia sẻ thông tin liên quan spyware. Về lý thuyết khi một thành viên của spyware bị đe dọa bởi spyware mới, tất cả máy tính thành viên của spyware có thể phản ứng lại mối đe dọa này bằng cách ngăn chặn nó. Nếu bạn muốn trở thành một phần này của SpyNet, hãy chắc chắn nút tùy chọn Yes, I want to help fight spyware được chọn. Sau đó, nhấp Finish. Một màn hình xuất hiện cung cấp một link mà bạn có thể nhấp để bắt đầu quét hệ thống bằng phần mềm Antispyware được cài đặt.



88. Sử dụng Antispyware

Trước khi bạn bắt đầu

82 Bàn về Malware

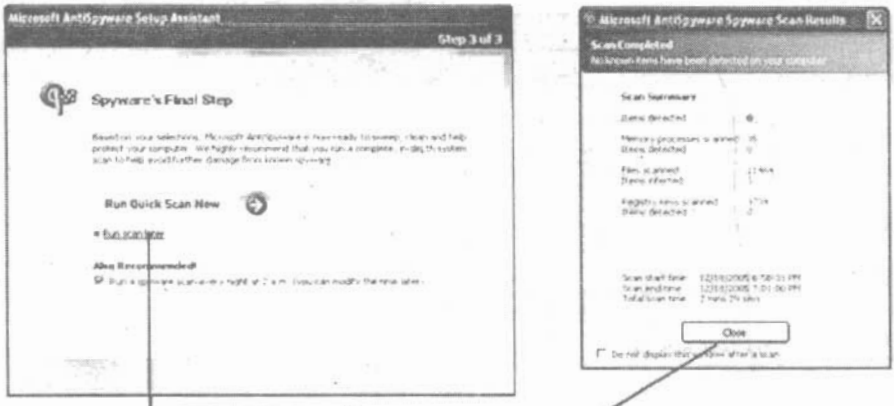
86 Bàn về Spyware

87 Cài đặt Antispyware

Sau khi bạn đã cài đặt phần mềm Microsoft Windows Antispyware, bạn có thể sử dụng nó để quét hệ thống tìm spyware đang có. Nếu spyware đã có trên hệ thống, Antispyware gỡ bỏ nó và làm sạch Registry (spyware đặt các mục trong cơ sở dữ liệu trong Windows Registry tương tự như phần mềm mà bạn cài đặt thường làm).

Bạn có thể cấu hình Antispyware để tự động kiểm tra tìm các bản cập nhật vào một khoảng thời gian mà bạn xác lập, bạn cũng có thể xác lập loại cảnh báo mà bạn muốn nhận được khi Antispyware chạy trong chế độ thời gian thật (real time).

88. Sử dụng Antispyware



1. Chạy Microsoft Antispyware

   Nhấp đôi biểu tượng Microsoft Antispyware trên desktop Windows hoặc nhấp link Run Quick Scan Now trên Setup Assistant Antispyware. Cửa sổ Antispyware mở ra và phần mềm bắt đầu quét hệ thống.

2. Đóng cửa sổ kết quả quét

   Khi việc quét hoàn tất, một kết quả Scan Results mở ra. Nó hiển thị số mục spyware được phát hiện, số process (tiến trình) và khóa registry được quét và tổng thời gian đã mất để quét. Nhấp Close để đóng cửa sổ kết quả.

Ghi chú

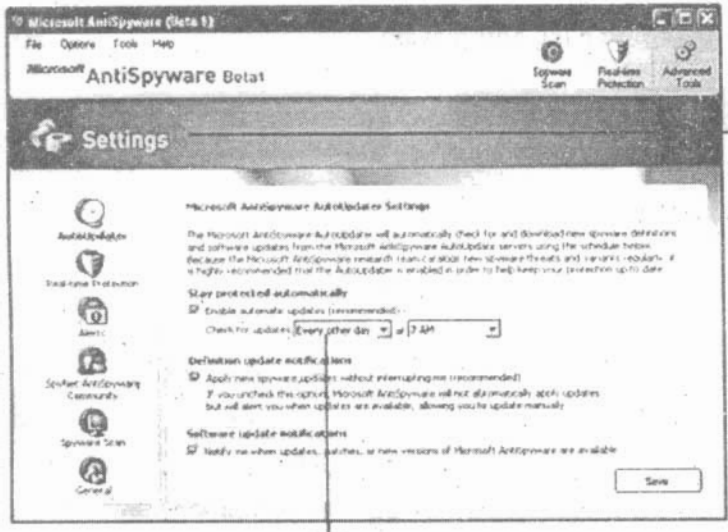
Nếu spyware bị phát hiện trong quá trình quét, chương trình Antispyware tự động gỡ bỏ spyware cùng với thông tin Registry vốn đã được nhập với spyware.

3. Mở các tùy chọn Antispyware

   Để xác lập các tùy chọn cho phần mềm Antispyware chẳng hạn như khi nào Antispyware được cập nhật, chọn Options, Settings từ menu Antispyware. Cửa sổ Settings mở ra.

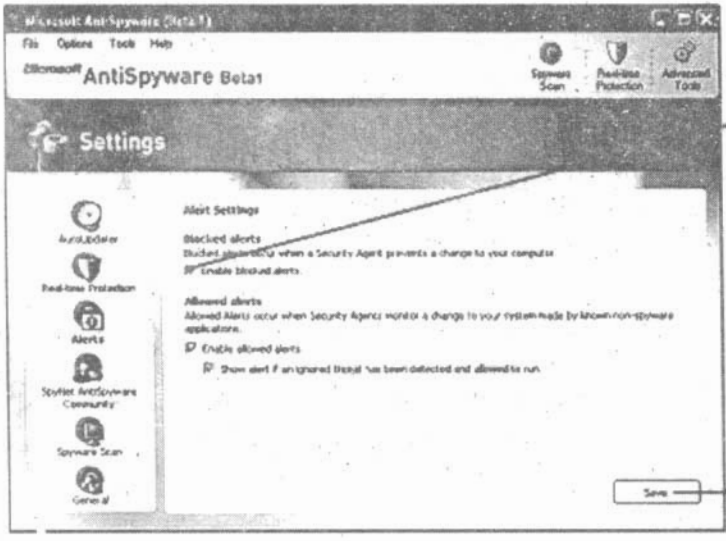
4. Xác lập các tùy chọn AutoUpdate

   Để xác lập thời gian tự động cập nhật cho Antispyware, chọn biểu tượng AutoUpdater nằm bên trái cửa sổ Setting sử dụng và sau đó các hộp xổ xuống Check for updates để xác lập khoảng thời gian mà bạn muốn chương trình kiểm tra tìm các bản cập nhật (system startup, Daily, Every other day hoặc Every week) và thời gian bạn muốn thực hiện việc cập nhật.



5. Xác lập các loại cảnh báo

Nhấp biểu tượng Alerts nằm bên trái cửa sổ Settings. Để nhận các cảnh báo (alerts) trong system tray khi spyware bị ngăn chặn, chọn hộp kiểm Enable blocked alerts. Nếu bạn muốn nhận được các thông báo khi các thay đổi được thực hiện đối với những chương trình và tiện ích mà bạn đã cài đặt trên máy tính, nhấp hộp kiểm Enable blocked alerts. Nếu bạn đánh dấu chọn tùy chọn này, bạn sẽ nhận được một cảnh báo mỗi lần phần mềm được cài đặt trên máy tính được cập nhật trên Internet. Việc bạn muốn thấy tất cả bản cập nhật này đều tùy thuộc vào bạn bởi vì chắc chắn chúng không làm lộ ra một sự cố hoặc sự lây nhiễm bởi spyware.



6. Lưu các xác lập

Khi bạn đã hoàn tất việc thực việc các thay đổi đối với những xác lập Antispyware, nhấp nút Save. Một hộp thông báo mở ra cho bạn biết rằng các xác lập đã được lưu. Nhấp OK. Bây giờ bạn có thể đóng cửa sổ Antispyware hoặc chạy một tiến trình Web khi cần thiết bằng cách nhấp biểu tượng spyware nằm ở bên trái cửa sổ ứng dụng.

89. Bàn về Spam Email và Outlook Express

Trước khi bạn bắt đầu

82 Bàn về Malware

Spam Email chắc chắn đã trở thành một điều tệ hại. Cuối cùng mọi người có tài khoản email điều nhận spam (thư rác). Và nếu bạn sử dụng địa chỉ email để đăng ký làm thành viên Web site và để down load phần mềm hoặc các file khác, địa chỉ email của bạn có thể được bán cho những người khác và sau đó sự gởi đến ồ ạt của Spam Email tăng lên theo thời gian.

Một số Spam Email có thể chứa các Virus và malware khác. Thậm chí bạn có thể nhận được Spam Email trông như nó đến từ một Web site hợp pháp yêu cầu bạn đi đến một vị trí web và cập nhật thông tin cá nhân của bạn. Trong ví dụ này Web site mà bạn đi đến không thật sự là Web site eBay, do đó khi bạn nhập thông tin của bạn, nó bị đánh cắp. Tiến trình gởi đi các email trông có vẻ chính thức và đưa bạn đến các Web site không thật sự sát nhập với công ty hoặc dịch vụ được đề cập trong email được gọi là phishing. Thực tế, Phishing dẫn đến nhiều vụ đánh cắp thông tin nhận dạng.

THUẬT NGỮ CHÍNH

Phishing. Tiến trình cố đánh lừa người ta cung cấp thông tin cá nhân, bao gồm các số thẻ tín dụng bằng cách hướng họ sang một Web site sử dụng một email trông có vẻ chính thức và tỏ ra là đến từ một Web site hoặc dịch vụ hợp pháp.

Phishing không phải là mối nguy hiểm duy nhất liên quan đến email. Spam cũng có thể được gởi chứa các Virus hoặc các phần đính kèm malware khác. Ví dụ bạn có thể nhấp một tên file để mở một bức ảnh hoặc chạy một chương trình và máy tính bị nhiễm bởi Malware đính kèm.

Các email khác nhau Outlook Express là một ví dụ cung cấp chức năng chống Spam Email. Điều này được thực hiện bằng cách nhận dạng Spam Email và tạo các Rule (quy tắc) vốn di chuyển email nghi ngờ trực tiếp sang thùng rác (trash). Email từ những người gởi nhất định cũng có thể bị ngăn chặn bằng việc cấu hình một danh sách blocked sender.

Một số email chẳng hạn như Microsoft Outlook (vốn là một phần của bộ Microsoft Office và là loại đàn anh lớn của Microsoft Outlook Express) cung cấp một bộ lọc spam cài sẵn, sử dụng các quy tắc khác nhau để nhận dạng

email là Junk (linh tinh). Sau đó Junk Email được đặt trong một folder junk nơi bạn có thể xem lại email.

Outlook Express không cung cấp một folder Junk theo mặc định nhưng bạn có thể thiết lập các quy tắc duy trì email nghi ngờ sang một folder mà bạn tạo (một folder spam) và xóa thông báo một cách tự động. Để được trợ giúp về tạo các quy tắc lọc email, **xem mục 90.**

90. Cấu hình các quy tắc Outlook Express

Trước khi bạn bắt đầu

82 Bàn về Malware

86 Bàn về Spyware

87 Cài đặt Antispyware

Email client Outlook Express chỉ chống malware ở mức tối thiểu bởi vì bạn phải tạo các quy tắc nhằm di chuyển spam từ Inbox của bạn sang một folder đã xác định hoặc sang thùng rác. Nhưng khả năng chống spam được cung cấp bởi các quy tắc Outlook Express tốt hơn là không có khả năng chống spam gì cả và bạn nên biết cách cấu hình các quy tắc email hoặc ngăn chặn những người gởi.

Để chống malware hoàn chỉnh hơn, bạn có thể mua một chương trình ngăn chặn spam. Có một số chương trình như vậy. Một số phần mềm chống Virus chẳng hạn như EZ Antivirus của Computer Associates cũng có chức năng chống spam chẳng hạn như EZ Anti-spam vốn chống spam cho Outlook Express và Outlook. Một trong những sản phẩm chống spam tốt nhất trên thị trường là Mail Frontier Desktop, cung cấp những tính năng chống spam và chống phishing cho Microsoft Outlook Express và Microsoft Outlook.

Ghi chú

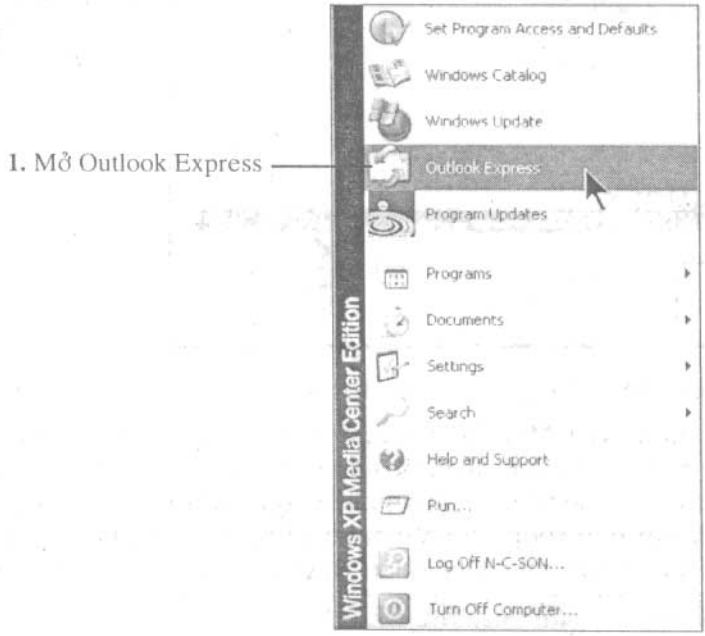
Trong môi trường Windows, Outlook Express và Outlook là hai email client thường được sử dụng nhiều nhất. Do đó bạn sẽ thấy hầu hết các sản phẩm chống spam được thiết kế để làm việc với hai email client Microsoft.

Các sản phẩm chẳng hạn như Mail Frontier Desktop cũng sử dụng một quy tắc để nhận dạng và xử lý các spam chẳng hạn như di chuyển nó đến một folder spam đặc biệt. Bởi vì các sản phẩm spam chẳng hạn như Mail Frontier Desktop được cập nhật theo định kỳ bằng những quy tắc mới và cũng có khả năng học hỏi từ sự tương tác với email của bạn (bạn có thể thêm những người gởi bị ngăn chặn và cũng xác định mail là spam), spam thật sự được xử lý càng hiệu quả khi bạn sử dụng sản phẩm chống Virus càng lâu.

Đối với các quy tắc chung liên quan đến spam bạn không bao giờ nên mở các file đính kèm email của những người gởi mà bạn không biết. Cũng không bao giờ phản hồi một spam email đặc biệt để loại bỏ email của bạn khỏi danh

sách người gởi của họ. Trong nhiều trường hợp spam được gởi dưới dạng một thông báo toàn miền và bạn nhận được nó bởi vì nó bao hàm tất cả địa chỉ email trong một miền cụ thể. Việc trả lời thông báo spam đó sẽ đặt địa chỉ email của bạn trên danh sách của họ, điều này chỉ dẫn đến nhiều spam hơn.

90. Cấu hình các quy tắc Outlook Express



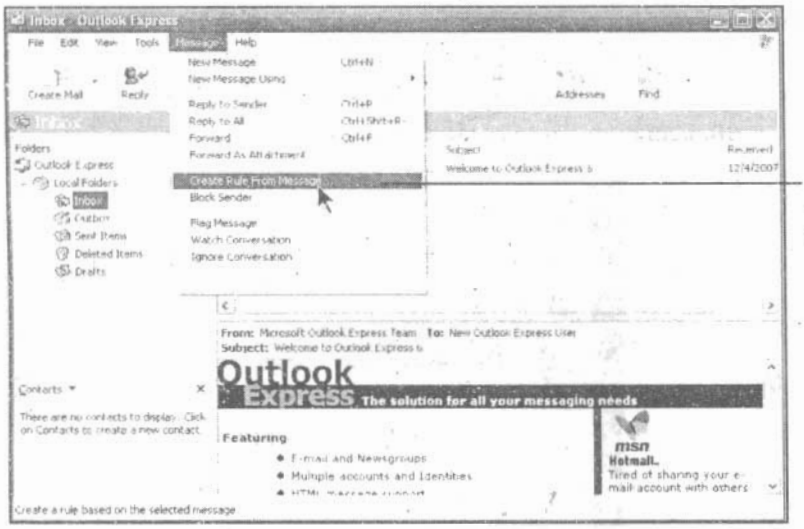
1. Mở Outlook Express

   Nhấp nút Start và sau đó chọn tùy chọn email để mở Outlook Express.

2. Chọn thông báo và mở hộp thoại New Mail Rule

   Trong inbox của Outlook Express, chọn một thông báo spam. Bạn có thể tạo một quy tắc (rule) ngăn chặn các email từ người gởi của spam email đã chọn.

   Chọn Message, Create Rule form Message từ thanh menu. Hộp thoại New Mail Rule mở ra.



2. Chọn thông báo và mở hộp thoại New Mail Rule

3. Xác định các điều kiện quy tắc và các hành động

Trong hộp thoại New Mail Rule, xác định điều kiện cho quy tắc và sau đó xác định hành động sẽ được tiến hành khi điều kiện được đáp ứng. Ví dụ hành động trên spam email từ người gởi email mà bạn đã chọn ở bước hai, nhấp hộp kiểm Where the From line contains people trong danh sách Select the Condition for your rule.



3. Xác định các điều kiện quy tắc và các hành động

Bạn cũng phải chọn một hành động cho quy tắc để tiến hành. Bạn có thể di chuyển mail được nhận dạng bởi quy tắc đến một folder đã xác định hoặc bạn có thể xóa thông báo (thông báo thật sự được di chuyển đến folder Delete Outlook Express). Chọn một hành động chẳng hạn như Delete từ danh sách Select the Condition for your rule.

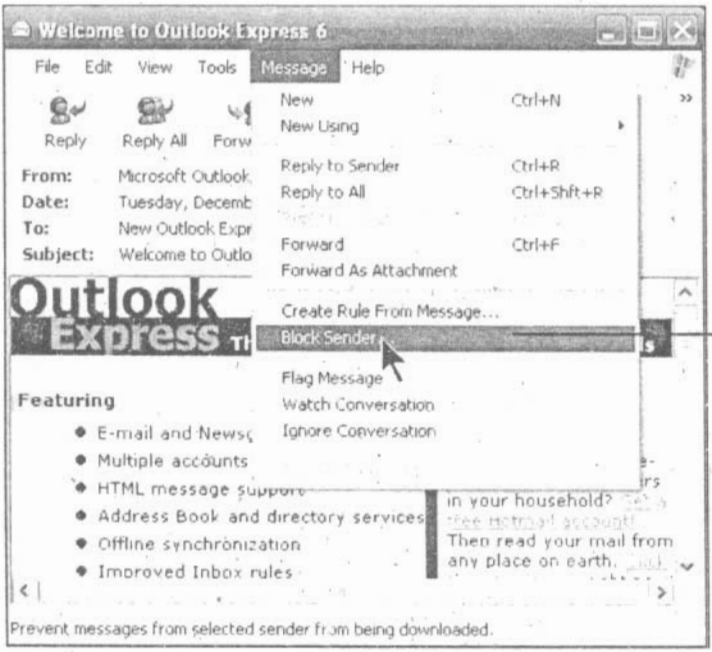
Một phần mô tả được tạo ra cho quy tắc mới và xuất hiện ở vùng dưới cùng của hộp thoại New Mail Rule.

Để chỉnh sửa tên của quy tắc mới, nhấp hộp text Name of the rule và gõ nhập một tên. Khi bạn đã tạo xong quy tắc mới, nhấp OK. Một hộp thông báo mở ra cho bạn biết rằng quy tắc đã được thêm vào. Nhấp OK lần nữa.

THỦ THUẬT: Bạn cũng có thể tạo các quy tắc ngay từ đầu trong Microsoft Outlook Express. Chọn Tool Message Rules, Mail. Bạn có thể tạo bao nhiêu quy tắc tùy mức cần thiết. Các quy tắc không nhất thiết phải được cấu hình để giúp giải quyết spam email, bạn có thể tạo các quy tắc di chuyển email từ những người gởi nhất định đến một folder đã ấn định. Điều này cho phép bạn sử dụng một quy tắc để đặt trực tiếp email kinh doanh hoặc email cá nhân trong một folder cụ thể.

---

4. Thêm người gởi vào danh sách Blocked



4. Thêm người gởi vào danh sách Blocked

Một cách khác để ngăn spam không đi vào inbox của bạn là thêm những người gởi spam vào danh sách blocked. Những email từ các người gởi trên danh sách blocked không được chấp nhận bởi Outlook Express. Bắt đầu bằng cách mở một thông báo email từ người nào đó mà bạn muốn ngăn chặn không gởi cho bạn email nữa.

Từ menu ở phần trên cùng cửa sổ thông báo, chọn Message, Block Sender. Địa chỉ email của người gởi được thêm vào danh sách BlockSender và các thông báo email từ địa chỉ email này không được phép đi vào inbox của bạn. Nhấp OK để đóng hộp thông báo để xác nhận việc người gởi đã được thêm vào danh sách blocked.

Bạn có thể lặp lại bước này khi cần thiết để thêm những người gởi khác vào danh sách blocked email.

Chương 13

XỬ LÝ SỰ CỐ VÀ GIÁM SÁT MẠNG

Trong chương này, bạn sẽ học những điểm chính sau đây:

- *91 Bàn về các sự cố nối kết mang*
- *92 Xác lập lai Adapter WiFi*
- *93 Kiểm tra trạng thái router*
- *94 Xem các thiết bị được nối kết*
- *95 Xem log Router*
- *96 Bàn về các công cụ dòng lệnh*
- *97 Sử dụng các công cụ dòng lệnh*
- *98 Bàn về việc nâng cấp firmware Router và các driver Adapter*

Làm cho một mạng WiFi gia đình khởi động và chạy đòi hỏi một số kỹ năng xử lý sự cố mạng cơ bản và kinh nghiệm thực tế. Chương này sẽ xem xét cách giám sát mạng WiFi và sử dụng những kỹ thuật xử lý sự cố để chẩn đoán và giải quyết những sự cố kết nối trên mạng.

91. Bàn về các sự cố nối kết mạng

Trước khi bạn bắt đầu

21 Bàn về việc cấu hình Router không dây

32 Bàn về việc cấu hình Adapter không dây

37 Bàn về việc cấu hình PC để nối mạng

Các sự cố kết nối mạng có thể gây khổ sở cho cả mạng nhỏ nhất, chẳng hạn như workgroup WiFi gia đình. Để xử lý sự cố nối kết và các vấn đề truy cập tài nguyên một cách hiệu quả, bạn cần tiến hành qua một loạt các bước logic nhằm cho phép loại bỏ mỗi nguyên nhân có thể có một cách hệ thống

trong một sự cố kết nối, chẳng hạn như một máy tính trong workgoup không thể truy cập Internet hoặc in sang một máy in chia sẻ. Các sự cố nối kết trên các mạng nhỏ thường gây ra do một trong ba khả năng: các sự cố phần cứng, sự cố phần mềm (kể cả các xác lập cấu hình không chính xác) và lỗi người dùng.

Giả sử lỗi người dùng không phải là một sự cố trên mạng và rằng người dùng biết cách đăng nhập vào máy tính, có thể định vị các tài nguyên mạng bằng cách sử dụng My Network Places, biết cách sử dụng Microsoft Internet Explorer để định hướng web và có thể sử dụng các email client. Cũng giả sử bạn sao lưu dữ liệu quan trọng trong folder chia sẻ (**xem mục 64**) và tận dụng Windows System Restore để bảo vệ các xác lập hệ thống Windows (**xem mục 68**).

Với lỗi người dung bị loại bỏ khỏi phương trình xử lý sự cố, bạn còn lại các sự cố phần cứng và phần mềm. Các danh sách kiểm tra phần cứng và phần mềm được trình bày dưới đây, sau đó bạn sẽ xem các cách sửa chữa adapter và router, và một số kỹ thuật xử lý sự cố liên quan đến các mạng TCP/IP.

THỦ THUẬT: Nếu bạn gặp phải sự nhiễu từ một hệ thống điện thoại kỹ thuật số (bạn cũng sẽ gặp các sự cố với các điện thoại bởi vì mạng WiFi và hệ thống điện thoại không dây "tranh dành" trên cùng một kênh), hãy thay đổi kênh mạng WiFi trên router WiFi và sau đó cấu hình các adapter mạng WiFi để kết nối với mạng trên kênh mới.

Các sự cố phần cứng

Các sự cố phần cứng thường có dạng một sự cố đơn giản và dễ sửa chữa chẳng hạn như một router WiFi được rút phích cắm; những sự cố phần cứng khác liên quan đến một thiết bị chẳng hạn như một adapter mạng WiFi bị trục trặc hoặc bị hỏng (nghĩa là nó không còn hoạt động được nữa). Nếu bạn gặp một sự cố kết nối chẳng hạn như không thể kết nối với Internet hoặc với một tài nguyên chia sẻ trên mạng chẳng hạn như một máy in, hãy thử một số gợi ý xử lý phần cứng này:

THỦ THUẬT: Nếu bạn nghĩ bạn đang gặp phải một sự cố xử lý phần cứng, hãy liên lạc với bộ phận hỗ trợ kỹ thuật để được trợ giúp cho router của bạn và họ sẽ hướng dẫn bạn chẩn đoán sự cố.

- ***Kiểm ta router WiFi***: *Router là điểm kết nối trung tâm cho toàn bộ mạng. Nếu router WiFi không hoạt động chính xác, tất cả người dùng trên mạng sẽ gặp sự cố. Sự cố của một router có thể gây ra bởi một khiếm khuyết phần cứng hoặc một router được cấu hình không đúng (**xem mục 21**).*

  Nếu đèn power của router không sáng lên, kiểm tra dây điện của router (và ổ cắm điện). Trên hầu hết các router, đèn power có một màu đồng nhất chẳng hạn như màu xanh lục (khi router được bật nguồn và bộ nguồn được kết nối chính xác). Các router WiFi cũng có các đèn cổng LAN và thường là đèn cổng Internet. Các đèn cổng LAN thể hiện hoạt động trên các cổng LAN trên switch của router. Chúng thường có màu xanh lục và được đánh số (mặc dù chúng có thể có màu vàng). Cổng Internet thể hiện hoạt động trên nối kết của router với nối kết của Internet. Đèn cổng Internet có thể là màu xanh lục hoặc một màu khác nào đó và nhấp nháy khi dữ liệu từ mạng di chuyển đến Internet (qua thiết bị băng tần rộng) và quay trở về mạng.

  Nếu những đèn này không hoạt động (nhấp nháy, và bạn gặp phải sự cố với LAN hữu tuyến hoặc nối kết Internet (nối kết với thiết bị băng tần rộng), hãy kiểm tra bất kỳ mạng được sử dụng cho nối kết này để bảo đảm chúng được nối chính xác. Bạn cũng có thể thử một cáp khác nếu bạn nghi ngờ cáp là sự cố. Mặc dù điều này nghe có vẻ ngớ ngẩn nhưng đôi khi việc rút phích cắm cáp ra khỏi cả hai thiết bị (chẳng hạn như router và thiết bị băng tần rộng), đảo ngược cáp và sau đó cắm nó trở lại các thiết bị có thể làm cho kết nối hoạt động (sự cố có thể do các bộ nối bị hư trên cáp hoặc một sự đoản mạch trên cáp).

THỦ THUẬT: Nếu bạn bật router và tất cả đèn vẫn sáng sau khi bật nguồn (nghĩa là chúng sáng ổn định không nhấp nháy) hãy tắt và sau đó bật lại nguồn. Nếu các đèn router tiếp tục vẫn sáng đều thì có lẽ bạn đang nhìn vào một thiết bị khiếm khuyết.

- ***Kiểm tra thiết bị băng tần rộng***: *Nếu bạn kết nối với Internet và router WiFi dường như hoạt động, kiểm tra các đèn trạng thái trên thiết bị băng tần rộng (modem cáp hoặc modem DSL; các đèn trên những thiết bị này thay đổi giữa các thiết bị khác nhau). Sẽ thường có một đèn chỉ báo LED nhấp nháy nghĩa là nối kết giữa router WiFi và modem băng tần rộng hoạt động. Kiểm tra adapter nguồn (và nối kết) cho thiết bị băng tần rộng và nối kết giữa router của thiết bị băng tần rộng. Nếu thiết bị băng tần rộng, bị trục trặc, router WiFi sẽ không được gán một địa chỉ IP ngoài để kết nối với Internet. Bạn có thể kiểm tra cấu hình router*

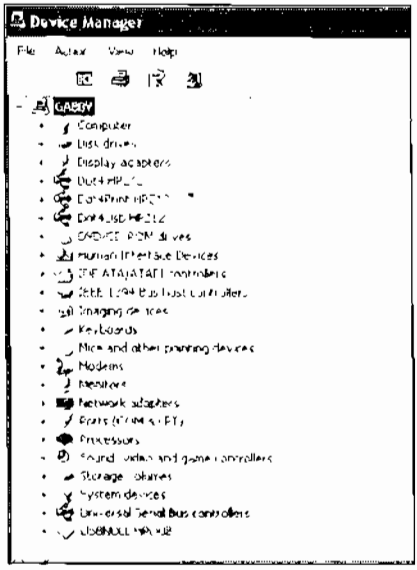
bằng cách đăng nhập vào router. Xem mục 23 để biết thêm thông tin về việc xác lập router nhằm kết nối với thiết bị băng tần rộng.

THỦ THUẬT: Một nối kết băng tần rộng cũng có thể bị trục trặc do một sự cố mà nhà cung cấp dịch vụ Internet của bạn đang gặp trục trặc. Hãy gọi số điện thoại trợ giúp của ISP; nhiều ISP cung cấp một thông báo đã ghi âm để cho bạn biết họ hiện đang gặp phải các sự cố kỹ thuật. Trong hầu hết các trường hợp, nếu bạn sử dụng một nối kết băng tần rộng từ nhà cung cấp truyền hình cáp, truyền hình và nối kết Internet sẽ ngừng hoạt động đồng thời.

- ***Kiểm tra adapter WiFi của máy tính:*** *Các adapter WiFi trong và ngoài có một đèn sẽ sáng lên khi card được bật nguồn (đèn có thể có màu hổ phách hoặc màu xanh lục phụ thuộc vào adapter và tốc độ nối kết; màu hổ phách thường được sử dụng cho các nối kết 10 Mb và màu xanh lục thường được sử dụng cho các nối kết 100 Mb trên adapter LAN 10/100 có thể chuyển mạch). Nếu bạn không thấy đèn nhấp nháy (xem adapter), adapter có thể bị một sự cố thất thường. Sự cố thất thường trở thành sự cố kinh niên, hãy thay adapter.*

  Bởi vì Windows XP là hệ điều hành plug-and-play (cắm vào là chạy), một thiết bị thật sự "bị chết" sẽ không còn được liệt kê là thiết bị được cài đặt trong Windows Device Manager nữa (để mở Device Manager nhấp nút Start, nhấp biểu tượng My Computer và chọn Properties từ menu ngữ cảnh; nhấp nút Device Manager trên tab Hardware của hộp thoại System Properties).

  Nếu một thiết bị bị trục trặc do một sự cố driver phần cứng, sẽ có một biểu tượng cảnh báo màu vàng hoặc một biểu tượng báo động màu đỏ kế bên tên của thiết bị đó trong danh sách Device Manager. Bạn có thể cố cài đặt lại driver thiết bị hoặc cập nhật driver để xử lý sự cố. ***Xem mục 30*** *và* ***31*** *để biết thêm thông tin về việc cài đặt phần mềm adapter và các driver.*



Sử dụng Device Manager để xem trạng thái của một thiết bị chẳng hạn như một adapter WiFi và để cài đặt lại, phục hồi hoặc cập nhật driver thiết bị.

Đối với các adapter mạng WiFi trong, kiểm tra để bảo đảm rằng anten được nối kết chính xác và adapter được lắp chính xác trên motherboard (bạn phải mở thùng máy tính để kiểm tra điều này). Đối với một adapter WiFi USB, kiểm tra xem thiết bị USB có được nối chắc chắn với một cổng USB trên máy tính hay không. Nếu bạn nối adapter WiFi USB với máy tính bằng một cáp USB, hãy kiểm tra các nối kết cáp và cũng kiểm tra xem cáp thay thế có giải quyết được vấn đề hay không.

THỦ THUẬT: Đôi khi các thiết bị phần cứng chẳng hạn như các router WiFi và thiết bị băng tần rộng chẳng hạn hạn như các modem cáp chỉ cần được reset. Tắt thiết bị, đợi một vài phút và sau đó bật nguồn thiết bị. Kiểm tra các đèn chỉ báo khác nhau để xem việc khởi động lại có giúp giải quyết được vấn đề hay không. Đôi khi việc khởi động lại máy tính trên mạng cũng sẽ cho phép máy tính nhận một địa chỉ IP và kết nối với mạng.

Các sự cố phần mềm

Từ nội dung thảo luận trong phần trước, bạn có thể thấy các sự cố phần cứng và phần mềm trùng lắp bởi vì tất cả thiết bị phần cứng phụ thuộc vào phần mềm để thật sự hoạt động. Do đó khi bạn loại trừ các sự cố phần cứng "vật lý" (nghĩa là những thiết bị khiếm khuyết hoặc các cáp mạng bị hỏng hoặc bị hư), bạn còn lại các vấn đề phần mềm. Các sự cố phần mềm có thể là kết quả của các xác lập cấu hình không chính xác hoặc phần mềm và các driver phần mềm được cài đặt không đúng cách.

THỦ THUẬT: Nếu bạn đã cấu hình router WiFi cho WEP hoặc WPA, một máy tính được bật WiFi sẽ không thể kết nối trừ khi nó cấu hình bằng khóa xác thực chia sẻ. Nếu một người dùng trên mạng có thể kết nối một máy tính với mạng WiFi, hãy kiểm tra cấu hình của adapter WiFi. Xem mục 32 và 33.

Về cơ bản, phần cứng trên router WiFi được cấu hình chính xác để mạng WiFi hoạt động. Một nguồn chính khác của các sự cố kết nối liên quan đến các sự cố phần mềm là những xác lập TCP/IP trên các máy tính vốn tham gia mạng WiFi.

Nếu một máy tính không được cấu hình tự động nhận địa chỉ IP của nó từ router WiFi, nó sẽ không thể gia nhập mạng IP. Trong một số trường hợp, thậm chí một PC cấu hình để tự động nhận một địa chỉ IP sẽ không có một địa chỉ IP từ router WiFi. Ví dụ nếu router tắt và một PC khởi động, Windows sẽ tự động gán một địa chỉ IP vào máy tính. Do đó, một khi router được bật nguồn PC "nghĩ" nó không cần một địa chỉ IP từ router WiFi, bạn có thể khởi động lại máy tính để giải quyết sự cố này hoặc sử dụng các lệnh ipconfig/release và ipconfig/renew tại dòng nhắp lệnh Windows (nhắp nút Start chọn biểu tượng Run, gõ nhập command và nhắp OK để đi đến dòng nhắc lệnh Windows). Để biết thêm chi tiết về việc cấu hình các xác lập TCP/IP của một PC, **xem mục 42.**

THỦ THUẬT: Nếu một PC không được cấu hình bằng Client for Microsoft Networks hoặc dịch vụ File and Printer Sharing for Microsoft Networks, PC sẽ không thể gia nhập mạng workgroup; xem mục 40 để biết thông tin về việc cấu hình một PC để nối mạng workgroup.

Nhiều adapter WiFi cũng có một số tiện ích phần mềm cũng như driver cho adapter. Nếu bạn gặp các sự cố với phần mềm, sử dụng applet Add or Remove Programs của Control Panel để gỡ bỏ bản cài đặt phần mềm. Sau đó bạn có thể cài đặt lại phần mềm. Cũng kiểm tra Web site của nhà sản xuất adapter để xem có sẵn một bản cập nhật cho phần mềm hay không hoặc có sẵn một bản cập nhật cho driver phần cứng của adapter hay không. Phần mềm kém và một driver thất thường có thể gây ra các sự cố với adapter.

THỦ THUẬT: Các thiết bị phần cứng chẳng hạn như các adapter WiFi và router WiFi cũng có phần mềm cài sẵn nhằm cho phép thiết bị hoạt động. Nếu bạn gặp các sự cố với một thiết bị, việc nâng cấp "firmware" (phần mềm cài sẵn) có thể giúp giải quyết được vấn đề. Xem

mục 98 để biết thêm thông tin về các bản nâng cấp firmware.

92. Xác lập lại Adapter WiFi

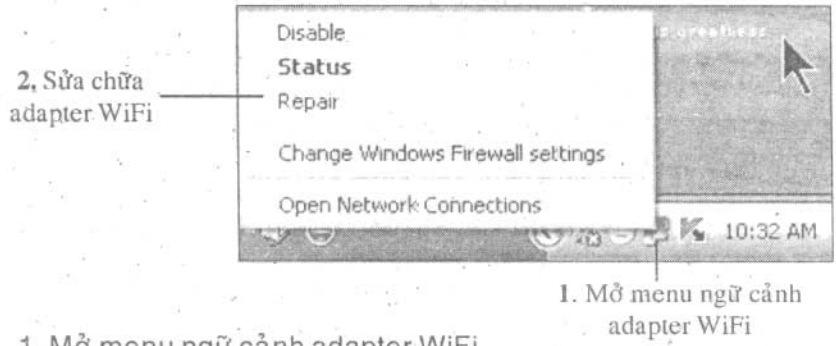
Trước khi bạn bắt đầu	Xem thêm
32 Bàn về việc cấu hình Router không dây	Mục 61
33 Cấu hình adapter và kết nối với Router không dây	

Thậm chí khi bạn biết một máy tính được cấu hình chính xác (nghĩa là các xác lập TCP/IP và WiFi của nó được xác lập thích hợp) và mạng WiFi hoạt động (nghĩa là router WiFi cho phép kết nối với mạng và Internet), bạn vẫn có thể gặp phải trường hợp máy tính không chịu kết nối với mạng. Các adapter WiFi có thể rất cầu kỳ và đôi khi bạn chỉ phải reset chúng để kết nối được.

Chính xác không nút có reset hoặc lệnh reset nhưng bạn có thể reset adapter WiFi bằng cách sử dụng lệnh Repair. Lệnh này có thể được truy cập qua menu ngữ cảnh hoặc menu tắt vốn mở ra khi bạn nhấp phải biểu tượng adapter WiFi trong system tray Windows.

Một adapter WiFi gặp sự cố kết nối với mạng WiFi có thể hiển thị một dấu chấm than màu vàng trên biểu tượng của adapter WiFi trong system tray Windows. Adapter WiFi không được kết nối hiển thị một dấu X màu đỏ trên biểu tượng adapter WiFi nghĩa là hiện không có kết nối. Bạn có thể cố thiết lập với adapter này hoặc sử dụng lệnh Run để Windows có thể kiểm tra cấu hình adapter và xác lập lại những thiết lập khác nhau trước khi cố gắng kết nối.

92. Sửa chữa adapter WiFi



1. Mở menu ngữ cảnh adapter WiFi

   Nhấp phải biểu tượng Adapter WiFi trong system tray Windows ở đầu phải của taskbar Windows. Menu ngữ cảnh mở ra.

2. Sửa chữa adapter WiFi

   Nhấp lệnh Repair trên menu ngữ cảnh. Windows tắt và sau đó mở lại adapter WiFi (các hộp thoại status xuất hiện để cho bạn biết trạng thái của tiến trình sửa chữa).

Nếu tiến trình này sửa chữa adapter, adapter sẽ kết nối với mạng WiFi mà nó được cấu hình (hoặc sẽ kết nối với mạng WiFi có sẵn đầu tiên nếu bạn đã thiết lập nó để kết nối với bất kỳ mạng).



Kiểm tra tình trạng nối kết và Adapter

Xem tình trạng Adapter và đóng hộp thoại Status

3. Kiểm tra tình trạng nối kết và Adapter

Sau khi một nối kết được thiết lập với mạng WiFi, bạn có thể kiểm tra cường độ nối kết và trạng thái của Adapter. Nhấp đôi biểu tượng Adapter trong system tray. Hộp thoại Wireless Network Connection Status mở ra.

4. Xem tình trạng Adapter và đóng hộp thoại Status

Bạn có thể kiểm tra tốc độ của nối kết và cường độ tín hiệu. Nếu tốc độ chậm hơn bạn thường gặp khi kết nối với mạng WiFi, bạn có thể gặp phải một sự cố phần cứng với adapter. Bạn có thể xem các mạng không dây có sẵn và kết nối lại nếu bạn muốn kết nối với tốc độ nhanh hơn hoặc băng thông lớn hơn. Tốc độ nối kết và cường độ tín hiệu có thể được xem nhanh bằng cách đặt chuột trên biểu tượng Adapter WiFi trong system tray Windows. Để xem những số liệu thống kê này trong cửa sổ cấu hình của adapter, nhấp đôi biểu tượng trong system tray. Để xem các mạng có sẵn, nhấp nút Scan; tất cả mạng lân cận truyền phát các SSID (các mạng WiFi an toàn và không an toàn) sẽ xuất hiện trong danh sách Scan.

Khi bạn xem xong tình trạng nối kết, nhấp Close để đóng hộp thoại Wireless Network Connection Status.

93. Kiểm tra trạng thái Router

Trước khi bạn bắt đầu

21 Bàn về việc cấu hình Router không dây

22 Truy cập cấu hình Router

92 Bàn về các sự cố nối kết mạng

Việc kiểm tra trạng thái của router sẽ cho bạn một bức ảnh chụp nhanh về cấu hình của router và tình trạng hiện hành của các nối kết WAN và LAN với router. Điều này đặc biệt hữu dụng khi bạn cố xử lý các sự cố kết nối trên mạng.

Thông tin trạng thái bao gồm đại chỉ IP "bên ngoài", được cung cấp cho adapter WiFi và LAN cũng như thông tin cổng Wireless chẳng hạn như việc router WiFi có được cấu hình dưới dạng một server DHCP (cung cấp các địa chỉ IP cho các client mạng trên mạng WiFi) hay không. Thông tin trạng thái router cũng hiển thị kênh mà mạng WiFi giao tiếp trên đó và cung cấp địa chỉ cổng LAN của router vốn có thể được sử dụng để xem một nối kết giữa máy tính và router bằng cách sử dụng lệnh ping hay không (xem mục 96 và mục 97 để biết thêm thông tin về lệnh ping và những lệnh hữu dụng khác).

Ghi chú

Vậy thì làm thế nào thông tin trạng thái router giúp chúng ta xử lý các sự cố nối kết mạng? Sau đây là một mẫu về thông tin số liệu thống kê trạng thái trên trang Connection Status của router: nếu không có một địa chỉ IP "bên ngoài" xuất hiện trong thông tin trạng thái, bạn không có một nối kết giữa router và thiết bị băng tần rộng hoặc có một sự cố với nhà cung cấp dịch vụ Internet. Nếu DHCP được tắt trên router (nghĩa là nếu xác lập là DHCP Off), bạn sẽ thấy điều này trong số liệu thống kê trạng thái router trên trang Connection Status. Điều này có nghĩa các client mạng không nhận địa chỉ IP và các xác lập cấu hình TCP/IP khác từ router ngăn những máy tính này giao tiếp trên mạng.

93. Kiểm tra trạng thái Router



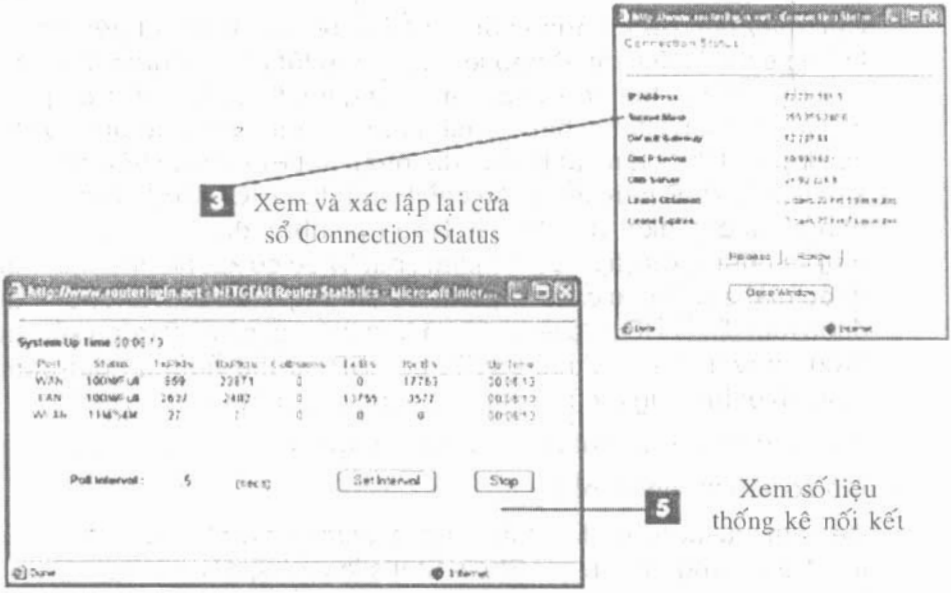
1. Truy cập màn hình trạng thái

Đăng nhập vào router bằng quyền administrator bằng cách sử dụng trình duyệt web, gõ nhập URL cho router trong hộp Address của trình duyệt, sau đó gõ đăng nhập và password cho router khi được nhắc về thông tin này. Bạn có thể tìm thấy URL cho router trong tài liệu đi kèm với router; thường có một trang thông tin khởi động nhanh đi kèm router (một tờ bướm một trang) cung cấp URL hoặc địa chỉ Web cho router và tên đăng nhập và password mặc định. Nếu bạn không truy cập một trong hai mẫu tin này, đi đến Web site của nhà sản xuất router và truy cập trang hỗ trợ. Trang này sẽ cung cấp các link dẫn đến các trang sản phẩm riêng biệt, nơi bạn có thể download dữ liệu cho router WiFi của bạn.

Từ trang router chính, chọn link router Status (hoặc một lệnh tương tự) để mở trang router Status. Trang Status thường cung cấp phiên bản hiện hành của firmware và trạng thái của cổng Internet (có khi được gọi là cổng WAN), cổng LAN và cổng Wireless.

Các địa chỉ IP và địa chỉ phần cứng MAC được liệt kê cho Internet và cổng LAN. Thông tin cổng Wireless bao gồm các SSID cho mạng WiFi, kênh đang được sử dụng và chế độ Wireless. Để xử lý sự cố nối kết, kiểm tra xem cổng Internet có một địa chỉ IP hợp lệ (một địa chỉ từ nhà cung cấp dịch vụ Internet) hay không. Cũng kiểm tra vùng Wireless port để bảo đảm rằng xác lập Wireless AP là On (nếu không sẽ không có mạng Wireless bởi vì các router không xử lý tín hiệu vô tuyến).

Nếu một xác lập không chính xác, thay đổi xác lập sao cho đúng. Ví dụ nếu tất cả adapter WiFi được cấu hình cho một mạng WiFi với một SSID là POPEYE và SSID của router là BLUTO, cấu hình là router. Nếu xác lập Wireless AP là Off, hãy mở nó (on). Nếu router được cấu hình cho an ninh WEP và bạn đã cấu hình tất cả adapter WiFi cho an ninh WPA, hãy thay đổi các xác lập của router và thay đổi tất cả xác lập của adapter.



THỦ THUẬT: Khi bạn cấu hình router và các adapter WiFi và mạng WiFi chạy tốt, hãy ghi chép các xác lập cấu hình router và adapter. Đi đến bất kỳ màn hình cấu hình router hoặc adapter và nhấn phím Print Screen (hoặc phím tương tự) trên bàn phím). Phím này chụp nhanh màn hình Desktop Windows và trang cấu hình mà bạn đang mở. Mở một chương trình xử lý văn bản chẳng hạn như Microsoft Word hoặc Windows Wordpad (nó nằm trên menu con Accessories trên menu Start) và paste (dán) ảnh chụp nhanh hoặc ảnh chụp màn hình mà bạn đã chụp bằng phím Print Screen vào một tài liệu mới. In ra trang. Làm lại tiến trình này cho các trang cấu hình khác. Bây giờ bạn có các bản in ra cấu hình của router và cấu hình cho adapter WiFi. So sánh những bản in ra này với những cấu hình thiết bị khi bạn xử lý các sự cố mạng WiFi và nghi ngờ rằng đã có một sự thay đổi không đúng đối với một cấu hình.

2. Mở cửa sổ Connection Status

Để xem thông tin liên quan đến cổng Internet, nhấp nút Connection Status (hoặc lệnh tương tự trên router).

3. Xem và xác lập lại cửa sổ Connection Status

Xem thông tin Connection Status. Nó bao gồm địa chỉ IP công cộng, subnet mask, gateway mặc định và thông tin cấu hình TCP/IP khác vốn được cung cấp cho router WiFi bởi nhà cung cấp dịch vụ Internet.

Các máy tính trên mạng không thể kết nối với Internet nếu router không có một địa chỉ IP hợp lệ (ví dụ nếu tất cả số người được liệt kê); bạn không thể cố xác lập lại những thiết lập TCP/IP trong cửa sổ Connection Status bằng cách nhấp Release để giải phóng các xác lập TCP/IP hiện hành. Sau đó, nhấp nút Renew để yêu cầu các xác lập TCP/IP mới kể cả địa chỉ IP mới từ DHCP được bảo trì bởi nhà cung cấp dịch vụ Internet. Nếu bạn nhận được một địa chỉ IP mới và những xác lập TCP/IP khác, bất kỳ sự cố kết nối Internet nên được giải quyết cho các máy tính trên mạng. Nếu bạn không nhận được một địa chỉ IP hợp lệ (nghĩa là bạn thấy tất cả số 0 trong xác lập này), server DHCP được bảo trì bởi ISP có thể ngừng hoạt động hoặc thiết bị băng tần rộng không cung cấp một kết nối với ISP.

Để đóng cửa sổ Connection Status, nhấp nút Close Windows.

4. Mở số liệu thống kê nối kết

Để xem lưu lượng dữ liệu thật sự qua lại router (nghĩa là từ các máy tính trên mạng), nhấp nút Show Statistics trong cửa sổ Router Status.

5. Xem số liệu thống kê nối kết

Số liệu thống kê nối kết cho bạn thấy số liệu nối kết và tốc độ và tình trạng nối kết cho mỗi giao diện (WAN hoặc Internet, LAN, và WLAN hoặc WiFi). Nếu một tốc độ nối kết cụ thể rất thấp hoặc bằng zero, có một sự cố trên giao diện router đó hoặc bạn đã cấu hình sai router.

TxPkts là số gói được truyền trên giao diện và TxPkts là số gói nhận được trên giao diện. Nếu bạn thấy các gói không được truyền, bạn có thể gặp một sự cố router hoặc nối kết với thiết bị băng tần rộng. Nếu các gói không được nhận trên giao diện chẳng hạn như cổng WAN, nối kết Internet có thể ngừng hoạt động.

Hầu hết số liệu thống kê router cũng sẽ cho thấy những giá trị TX B/s cho các cổng WAN và LAN vốn là lưu lượng dữ liệu ngoại biên. Rx B/s là băng thông hiện hành hoặc lưu lượng truyền nội biên trên một giao diện cụ thể. Do đó TxPkts và TX B/s thể hiện dữ liệu ngoại biên và TxPkts và Rx B/s thể hiện lưu lượng nội biên.

Nhấp nút Stop để ngừng thu thập dữ liệu trong cửa sổ Statistics vốn cho bạn một ảnh chụp nhanh về dữ liệu. Việc nhấp nút này sẽ không tắt bất kỳ giao diện router.

Ghi chú

Các mạng Ethernet (thậm chí các mạng WiFi) được thiết kế trên các máy tính và những thiết bị khác để ngồi đó lắng nghe lưu lượng dữ liệu; khi một máy tính hay thiết bị khác không phát hiện bất kỳ lưu lượng, nó truyền dữ liệu của nó. Khi nhiều thiết bị truyền cùng lúc, điều này có thể dẫn đến sự xung đột. Các xung đột thật sự phổ biến trên các mạng Ethernet, do đó nếu bạn thấy một số xung đột được liệt kê trong số liệu thống kê, đừng hoảng hốt. Nếu bạn thấy một số lớn các xung đột, bạn có thể có một card mạng bị trục trặc và phun ra các gói lên trên mạng. Điều này dẫn đến lưu lượng cao và nhiều xung đột. Bạn có thể giải quyết vấn đề này bằng cách thay card mạng bị hỏng.

Khi bạn đã xem xong số liệu thống kê của router vốn được cập nhật cách 5 phút mỗi lần theo mặc định (bạn có thể gõ nhập bất kỳ khoảng thời gian tính bằng giây vào hộp text Poll Interval), nhấp nút Close trên cửa sổ Statistics.

94. Xem các thiết bị được nối kết

Trước khi bạn bắt đầu	Xem thêm
21 Truy cập cấu hình Router	Mục 32
91 Bàn về các sự cố nối kết mạng	Mục 42

Nếu một người dùng gặp sự cố kết nối với một tài nguyên mạng chẳng hạn như folder chia sẻ hoặc Internet, bạn có thể bắt đầu tiến trình xử lý sự cố bằng cách xem máy tính đang đề cập có được kết nối với router WiFi hay không. Nếu máy tính không được kết nối với router, sự cố có thể là adapter WiFi của máy tính đang gặp trục trặc, cấu hình của nó không chính xác hoặc router WiFi được cấu hình không đúng (thậm chí nó có thể được cấu hình để ngăn chặn sự truy cập web cho máy tính đó).

Hầu hết các trang cấu hình router WiFi có màn hình cung cấp các máy tính hiện được kết nối. Màn hình này được truy cập qua trang cấu hình chính cho router.

94. Xem các thiết bị được nối kết



1. Mở trang cấu hình router

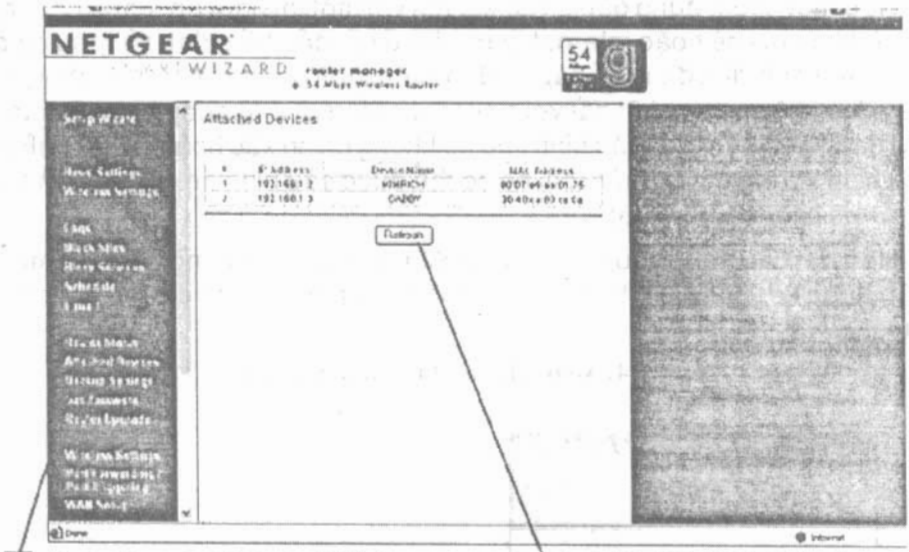
Mở trình duyệt web, nhập URL cho router trong hộp address và nhấn Enter. Sau đó, nhập tên đang nhập và password cho router. Bạn có thể tìm thấy URL cho router trong tài liệu đi kèm router. Các router thường có một trang thông tin khởi động nhanh vốn cung cấp URL hoặc địa chỉ web cho router và tên đăng nhập cùng với password mặc định. Nếu bạn không tiếp cận một trong hai nguồn thông tin này, bạn hãy đi đến Web site của nhà sản xuất router và truy cập trang hỗ trợ (support) để tìm các link dẫn đến các trang sản phẩm riêng biệt, nơi bạn có thể download tài liệu cho router WiFi của bạn.

2 Truy cập màn hình các thiết bị được nối kết

Khi bạn ở trên trang cấu hình chính của router, nhấp link Attached Devices (hoặc lệnh tương tự). Trang Attached Devices mở ra hiển thị các thiết bị đang kết nối (các máy tính được bật WiFi và máy in kết nối với router).

3 Làm mới danh sách các thiết bị được nối kết

Nếu gần đây một máy tính đã online (nghĩa là đã khởi động), bạn có thể làm mới danh sách Attached Devices để xem tất cả thiết bị đang kết nối. Nhấp nút Refresh khi cần thiết.



Nếu một máy tính được nối kết không xuất hiện trên danh sách Attached Devices, máy tính có thể có một sự cố adapter WiFi, adapter có thể không được cấu hình để nối kết với mạng hoặc có thể không có đúng các xác lập TCP/IP. Để biết cấu hình của adapter WiFi, xem mục 33. Nếu một máy tính có một nối kết hữu tuyến với router không nằm trên danh sách này, các LAN

có thể bị hư và Ethernet trên máy tính có thể được cấu hình không đúng hoặc bị lỗi. Để cấu hình các mạng workgroup và TCP/IP trên một máy tính được bật WiFi hay được nối cáp, **xem mục 41** và **42**.

95. Xem log Router

Trước khi bạn bắt đầu	Xem thêm
22 Truy cập cấu hình Router	**Mục 54**
91 Bàn về các sự cố nối kết mạng	**Mục 55**
	Mục 56

Nếu bạn sử dụng các tính năng lọc nội dung được cung cấp bởi router (xem mục 54 và mục 55 để biết thêm thông tin), bạn có thể vô tình ngăn chặn sự truy cập đến các site Internet hoặc dịch vụ phụ thuộc vào cách bạn cấu hình chức năng lọc nội dung. Chức năng lọc nội dung là con dao hai lưỡi và bạn thật sự phải suy nghĩ kỹ cách cấu hình chức năng lọc nội dung nếu bạn muốn cung cấp các mức độ truy cập khác nhau cho những người dùng trên mạng của bạn.

95. Xem log Router



Bạn có thể thấy số liệu thống kê lọc nội dung (sự truy cập đến router được cho phép hoặc được ngăn chặn như thế nào) bằng cách xem log router. Nếu bạn thấy sự truy cập đến một Web site hoặc dịch vụ nào đó chẳng hạn như email bị ngăn chặn bởi router và bạn đã không có ý định sử dụng chức năng lọc này, hãy kiểm tra các xác lập content filtering mà bạn đã cấu hình.

1 Mở trang cấu hình router

Mở trình duyệt web, nhập URL cho router trong hộp address (URL, tên đăng nhập và password có sẵn trong tài liệu của router) và nhấn Enter. Sau đó nhập tên đăng nhập và password cho router.

2 Truy cập màn hình log

- Trên trang cấu hình chính của router, nhấp link log (hoặc một lệnh tương tự trên router). Màn hình log mở ra.

3 Làm mới màn hình log và / hoặc gởi log

Để xem dữ liệu mới nhất được thu thập trong log, nhấp nút Refresh.

Nếu bạn muốn chụp một bức ảnh nhanh của log hiện hành và gởi dữ liệu đến tài khoản email của bạn để bạn có thể đọc qua nó một cách cẩn thận hơn và phát hiện bất kỳ sự cố đối với các site hoặc dịch vụ bị vô ý ngăn chặn, nhấp nút Send log (hoặc một lệnh tương tự). Hành động này sẽ gởi log đến địa chỉ email mà bạn đã cấu hình trong các xác lập email notification của router.

Log cho bạn xem tất cả lưu lượng dữ liệu giữa mạng của bạn và Internet. Nếu bạn thấy một nối kết với một Web site nhất định bị từ chối bởi router và bạn đã không dự định ngăn chặn sự truy cập đến site đó, kiểm tra cấu hình log site để xem từ khóa mà bạn đã nhập có ngăn chặn site đó hay không. Nếu bạn thấy lưu lượng gởi thông tin tức thì bắt đầu trên một máy tính sau 9 giờ tối và bạn đã đề nghị con của bạn không sử dụng chương trình gởi thông tin tức thì (instant messaging) sau 9 giờ, bạn có thể muốn xem xét sử dụng tính năng ngăn chặn dịch vụ service-blocking để ngăn chặn sự truy cập chức năng gởi thông tin tức thì và sau đó cấu hình một thời biểu cho dịch vụ bị ngăn chặn đó sao cho tính năng gởi thông tin tức thì có sẵn cho đến thời điểm bạn xác lập (và vào những ngày mà bạn xác lập). Để biết thêm chi tiết về những vấn đề cấu hình liên quan đến các site và dịch vụ bị ngăn chặn, **xem mục 55, 56** và **57**.



THỦ THUẬT: Để sử dụng tính năng email log, router phải được cấu hình cho Email Notifications. Tính năng này có thể được tìm thấy trên trang cấu hình E-mail trên màn

hình cấu hình của router vốn được mở bằng cách sử dụng link Email hoặc một lệnh tương tự. Chọn tùy chọn Email Notifications và sau đó nhập outgoing mail server (mail server mà bạn sử dụng dưới dạng smpt-mail.isp.com). Bạn cũng sẽ cần nhập địa chỉ email mà bạn muốn gởi các báo động đến. Một số router cũng có thể gởi các báo động tự động đến các địa chỉ này khi người nào đó cố truy cập một site hoặc một dịch vụ bị ngăn chặn.

96. Bàn về các công cụ dòng lệnh

Trước khi bạn bắt đầu **Xem thêm**

39 Đặt tên cho máy tính và gia nhập một Workgroup **Mục 97**

40 Mở các thuộc tính nối kết và mở các client, giao thức và dịch vụ

41 Thêm một client hoặc dịch vụ mạng

42 Cấu hình các xác lập TCP/IP

Về cơ bản các máy tính trên mạng WiFi được cấu hình tốt cho giao thức TCP/IP. Bởi vì các router WiFi cũng có chức năng như những server DHCP, chẳng hạn bạn nên cấu hình tất cả máy tính trên mạng WiFi để nhận cấu hình TCP/IP từ router (điều này bao gồm các địa chỉ IP và subnet mask). Có ba công cụ dòng lệnh liên quan đến TCP/IP mà bạn có thể sử dụng để kiểm tra nhanh cấu hình TCP/IP của máy tính, kiểm tra nối kết giữa hai thiết bị (chẳng hạn như giữa hai máy tính hoặc một máy tính và router WiFi) và truy vết đường truyền mà các gói này đi qua khi được gởi từ một máy tính đến một đích cụ thể (nghĩa là một địa chỉ IP cụ thể). Những lệnh này là:

- ***Ipconfig**: Lệnh này có thể được sử dụng để kiểm tra nhanh cấu hình IP. Lệnh ipconfig có thể được sử dụng với các khóa chuyển đổi (switch) khác nhau để hiển thị thêm thông tin cấu hình IP. Lệnh có thể được sử dụng để giải phóng và làm mới các xác lập IP hiện hành. Một số khóa ??? khác nhau mà bạn có thể sử dụng với lệnh ipconfig như sau.*

Lệnh	Mô tả
Ipconfig	Lệnh ipconfig hiển thị hậu tố DNS (domain), địa chỉ IP, subnet mask và gateway mặc định từ máy tính.
Ipconfig/all	Hiển thị thông tin được cung cấp bởi lệnh ipconfig (không có khóa chuyển đổi), địa chỉ MAC của adapter Ethernet, việc Adapter có thể được cấu hình cho DHCP và tự động cấu hình hay không, server DHCP cho máy tính, các server DNS cho máy tính, khi nào nhận được lease IP và khi nào lease IP hết hạn

Ipconfig/lease	Giải phóng (nghĩa là loại bỏ) tất cả xác lập IP cho adapter.
Ipconfig/renew	Làm cho adapter gởi đi một yêu cầu đến server DHCP để làm mới các xác lập IP.

- ***Ping***: *Một lệnh hoàn hảo để kiểm tra nối kết giữa hai máy tính hoặc những thiết bị khác trên một mạng IP là sử dụng lệnh ping. Ping là viết tắt của Pack InterNet Gopher và sử dụng các gói echo để test nối kết. Cú pháp lệnh là ping ip address, ip address là địa chỉ IP của thiết bị đích, lệnh ping cũng có thể được sử dụng với tên DNS (Fully Qualified Domain Name FQDN) của một thiết bị chẳng hạn như mycomputer.localdomain.com.*
- ***Tracert***: *Lệnh traceroute (tracert trên một máy tính Windows XP) gởi các gói dữ liệu đến một địa chỉ IP hoặc tên DNS đã xác định. Lệnh này hữu dụng ở chỗ nó cho bạn thấy cần bao nhiêu bước nhảy để dữ liệu di chuyển từ nguồn đến đích. Bởi vì bạn chỉ có một router WiFi là điểm kết nối trung tâm trên mạng nội bộ, tracert hiển thị chỉ một bước nhảy từ nguồn đến đích. Lệnh tracert cũng có thể được sử dụng để xác định bao nhiêu bước nhảy hoặc router tham gia khi bạn cố kết nối với đích mạng từ xa chẳng hạn như một địa chỉ IP trên Internet.*

Nói tóm lại, IP cho phép bạn xem (và làm mới nếu cần thiết) cấu hình một IP hiện hành cho router (bao gồm các adapter mạng WiFi). Lệnh ping cho bạn thấy việc bạn có thể kết nối với một thiết bị trên mạng hay không. Ví dụ bạn có thể ping giao diện LAN của router nếu bạn gặp một vấn đề nối kết. Lệnh tracert cho phép bạn xem đường dẫn thật sự mà dữ liệu đi qua; bạn có thể sử dụng thông tin đó để quyết định xem có một vấn đề kết nối trên mạng hay không.

97. Sử dụng các công cụ dòng lệnh

Trước khi bạn bắt đầu	Xem thêm
91 Bàn về các sự cố nối kết mạng	**Mục 43**
93 Bàn về các công cụ dòng lệnh	

Các công cụ dòng lệnh chẳng hạn như Ipconfig và ping được thực thi tại dòng lệnh Windows. Cách dễ nhất để truy cập dòng lệnh trên một máy tính Windows XP là ở hộp thoại Run (nhấp nút Start và chọn Run), gõ nhập command và sau đó nhấn Enter. Một cửa sổ command mở ra (nó trông giống như một cửa sổ DOS) mà bạn có thể sử dụng để thực thi các công cụ dòng lệnh khác nhau.

Hãy nhớ rằng toàn bộ vấn đề của việc sử dụng các công cụ này là cố hiểu tại sao một máy tính nào đó không thể kết nối với mạng cục bộ hoặc đang gặp sự cố kết nối với Internet. Hãy xem kỹ các kết quả của mỗi lệnh khi bạn chạy nó để thu. Nhập thông tin nhằm cho phép bạn giải quyết một vấn đề nối

kết cụ thể.



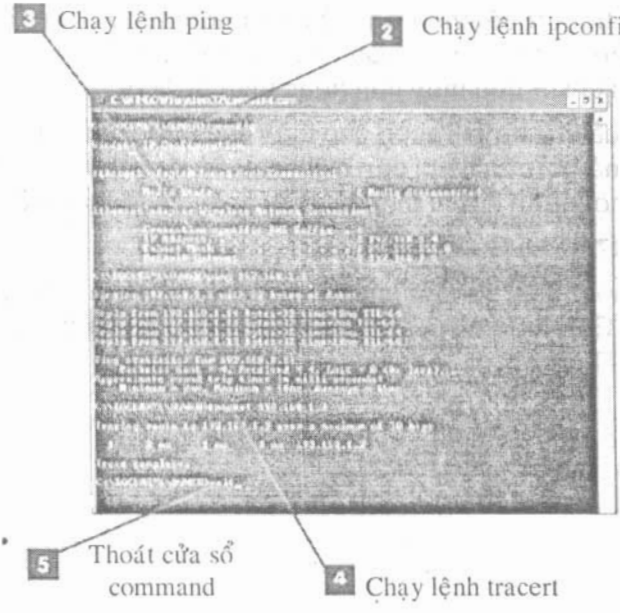
Mở cửa sổ Command

1. Mở cửa sổ Command

   Nhấp nút Start và chọn Run. Trong hộp thoại Run, gõ nhập command và nhấp OK. Cửa sổ Command mở ra.

2. Chạy lệnh ipconfig

   Tại dòng nhắc lệnh gõ nhập ipconfig hoặc ipconfig với một khóa chuyển đổi chẳng hạn như ipconfig/all và nhấn Enter. Kết quả của lệnh xuất hiện trong cửa sổ Command. Nếu bạn không thấy một gateway (cổng nối) mặc định, có thể có một sự cố với cấu hình IP trên máy tính hoặc một sự cố với server DHCP của router (bởi vì server phục vụ như gateway mặc định).



Ghi chú

Gateway mặc định cho máy tính là địa chỉ IP giao diện LAN của router WiFi. Bạn có thể kiểm tra điều này bằng cách sử dụng trong cấu hình của router.

3. Chạy lệnh ping

Để ping một máy tính hoặc một giao diện khác chẳng hạn như một LAN của router, bạn sẽ cần biết địa chỉ IP của thiết bị đó. Bạn có thể tìm thấy địa chỉ IP LAN của router bằng cách sử dụng trang cấu hình của router. Gõ nhập ping theo sau là địa chỉ IP của máy tính hoặc thiết bị mà bạn muốn kết nối. Sau đó nhấn Enter.

Kết quả của lệnh ping thể hiện số mili giây cần để thiết bị đích phản hồi lại gói ping khi bạn cần sử dụng ping trên một mạng WiFi (một mạng cục bộ), sự phản hồi đối với lệnh ping từ máy tính đích hầu như ngay tức thì. Tuy nhiên thời gian phản hồi sẽ khác nhau phụ thuộc vào lưu lượng mạng. Nếu mọi người trên mạng download các file lớn từ Internet, tất cả hoạt động đó sẽ làm chậm đi sự phản hồi đối với "thách thức ping". Tốc độ thật sự của ping (tính bằng mili giây) không quan trọng như tốc độ nhất quán.

Nếu bạn không nhận được một sự phản hồi gì cả (ping time out), có lẽ có một sự cố nối kết. Thiết bị đích không có trên mạng hoặc router đang gặp sự cố truyền yêu cầu của bạn. Kiểm tra màn hình status của router để xem các máy tính nào được kết nối với mạng. Nếu bạn không thấy máy tính mà bạn đang cố ping, máy tính đó đang gặp một sự cố kết nối mạng. **Xem mục 93** để biết thêm chi tiết về một danh sách các máy tính được kết nối với router WiFi.

4. Chạy lệnh tracert

Lệnh tracert sẽ cho bạn thấy số bước nhảy (router) cần để gói di chuyển từ máy tính của bạn đến địa chỉ đích. Gõ nhập tracert và sau đó địa chỉ IP của máy tính hoặc thiết bị đích.

Kết quả của lệnh tracert cho thấy các bước nhảy đến đích và số mili giây mà gói cần để đi đến đích; sau đó lệnh thể hiện số mili giây cần cho một phản hồi từ thiết bị đích, nghĩa là từ một máy tính.

5. Thoát cửa sổ Command

Để thoát cửa sổ Command, gõ nhập Exit tại dòng nhắc lệnh và nhấn Enter. Cửa sổ Command sẽ đóng lại và đưa bạn trở về Windows Desktop.

98. Bàn về việc nâng cấp firmware Router và các driver Adapter

Trước khi bạn bắt đầu	Xem thêm
21 Bàn về việc cấu hình router không dây	Mục 91
32 Bàn về việc cấu hình adapter không dây	
36 Bàn về việc cập nhật một driver adapter	

Nếu bạn đã loại trừ hầu hết các vấn đề phần cứng, phần mềm khi xử lý một sự cố mạng WiFi, bạn có thể muốn khai thác khả năng nâng cấp firmware của router WiFi hoặc một driver cho một adapter WiFi. Router WiFi hoạt động do một tập hợp lệnh vận hành cơ bản (mã phần mềm) vốn được ghi lên trên một chip có thể ghi lại các thiết bị. Tập hợp mã này được gọi là firmware của router. Toàn bộ khả năng vận hành của router được quyết định bởi firmware này, do đó việc có khả năng cập nhật firmware không chỉ có thể làm cho router chạy tốt mà nó còn có thể tăng toàn bộ chức năng của router, đặc biệt trong những trường hợp các giao thức an ninh và những tính năng khác đã được nâng cấp cho firmware của router bởi nhà sản xuất.

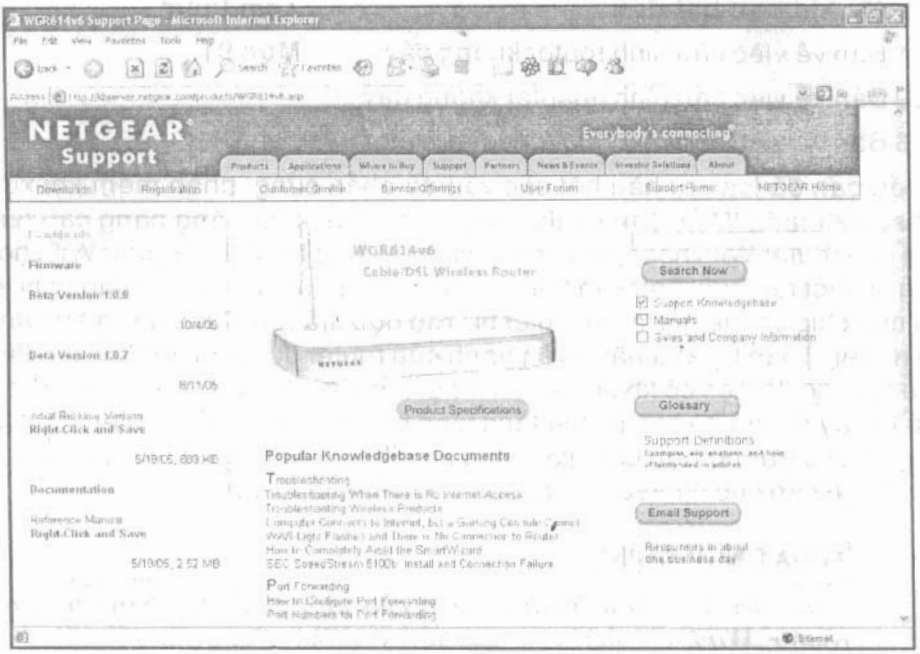
Thuật ngữ chính

Firmware Hệ điều hành cơ bản cho một thiết bị chẳng hạn như router WiFi.

Nhiệm vụ của bạn là thỉnh thoảng kiểm tra Web site của nhà router WiFi để tìm các bản cập nhật firmware. Hầu hết các router WiFi (và phần cứng khác chẳng hạn như các adapter) có một thẻ đăng ký mà bạn nên điền vào và gởi qua đường bưu điện hoặc bạn có thể gởi thiết bị với nhà sản xuất trực tuyến. Đăng ký (bao gồm thông tin chẳng hạn như địa chỉ email hợp lệ) có nghĩa là bạn sẽ nhận các email định kỳ liên quan đến bất kỳ khả năng cập nhật cho thiết bị chẳng hạn như một phiên bản mới của firmware.

Hầu hết các nhà sản xuất thiết bị nối mạng WiFi cung cấp các trang hỗ trợ và download cho những sản phẩm khác nhau mà họ sản xuất. Điều này giúp bạn dễ dàng xem các phiên bản khác nhau của firmware có sẵn cho một thiết bị. Tìm trang cho router WiFi của bạn và download khi cần thiết.

Kiểm tra trang sản phẩm cho router để xem có sẵn bản nâng cấp firmware nào hay không.

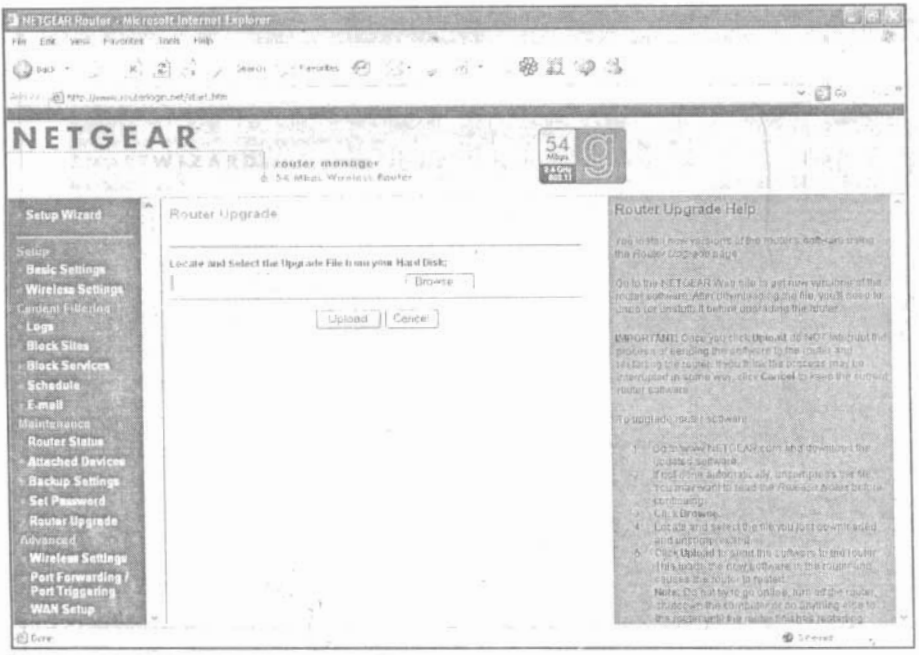


Ghi chú

Một số nhà sản xuất tung ra các phiên bản firmware beta cho các sản phẩm của họ. Việc bạn có muốn cài đặt firmware beta hay không đều tùy thuộc vào bạn. Tốt hơn là nên đợi cho đến khi một phiên bản "cuối cùng" của một bản cập nhật firmware có sẵn trước khi bạn nâng cấp router. Nhãn beta có nghĩa là phần mềm không sẵn sàng cho lần sử dụng ra mắt đầu tiên và có thể bạn làm cho sự cố router trở nên tồi tệ hơn nếu bạn sử dụng firmware beta.

Sau khi bạn download firmware mới, sử dụng file được download để nâng cấp router. Tiến trình này thay đổi giữa các router khác nhau, nhưng hầu hết các router có một trang cấu hình nhằm cho phép bạn duyệt tìm file firmware mới và sau đó nâng cấp router. Bạn nên làm theo các chi tiết cụ thể để nâng cấp router được cung cấp trong tài liệu của router.

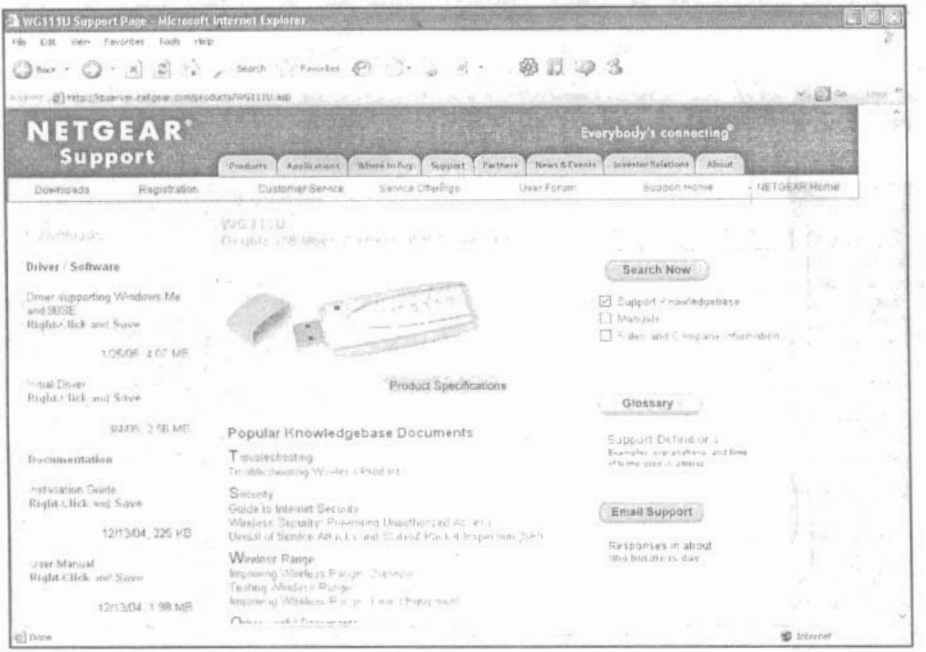
Nâng cấp firmware router bằng cách sử dụng trang cấu hình nâng cấp cho router.



Đối với các adapter WiFi (và thiết bị ngoại vi phần cứng khác mà bạn thêm vào máy tính), điều quan trọng là phải cập nhật driver cho adapter. Các nhà sản xuất cập nhật driver cho những thiết bị chẳng hạn như các adapter WiFi để giải quyết các sự cố và những vấn đề đã gặp phải với thiết bị và driver mà nó đính kèm.

Bạn có thể download các bản cập nhật driver (và những driver cho những phiên bản khác của Windows nếu bạn không chạy Windows XP) từ trang download cho adapter. Sau khi driver được download, bạn có thể cài đặt driver bằng cách sử dụng tab Device trên hộp thoại Properties cho adapter WiFi.

Kiểm tra trang download để tìm xem có các bản nâng cấp driver nào cho adapter của bạn hay không



Các thuộc tính cho bất kỳ thiết bị trên máy tính có thể được mở bằng cách sử dụng Windows XP Device Manager. **Xem mục 36** để biết thêm thông tin về việc cập nhật driver cho adapter WiFi.

Ghi chú

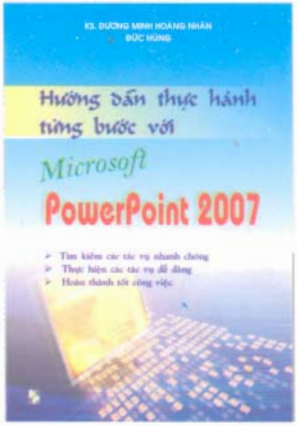
Cập nhật một driver có thể là cho một thiết bị chạy tốt bị trục trặc. Hãy nhớ rằng bạn có thể phục hồi các driver trở về phiên bản trước nếu một bản cập nhật driver gây ra các sự cố. Xem mục 30 và 36 để biết thêm chi tiết về các driver adapter WiFi.

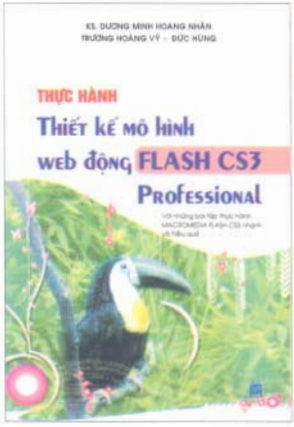
Một lời sau cùng về các bản cập nhật firmware và driver: Ở một mức độ nhất định, bạn nên tuân theo câu ngạn ngữ xưa: "Nếu nó không bị hỏng thì đừng sửa chữa nó". Nếu router WiFi của bạn hoạt động tốt và bạn không gặp bất kỳ sự cố adapter, đừng mất công nâng cấp firmware của router hoặc driver của adapter chỉ vì mục đích nâng cấp. Mặc dù nâng cấp một router WiFi có thể nâng cao an ninh và khả năng vận hành, nhưng nếu bạn hài lòng với các xác lập an ninh và hiệu suất của router, tại sao phải mức độ làm cho router trở nên không ổn định bằng việc nâng cấp firmware mới, đặc biệt là firmware beta?

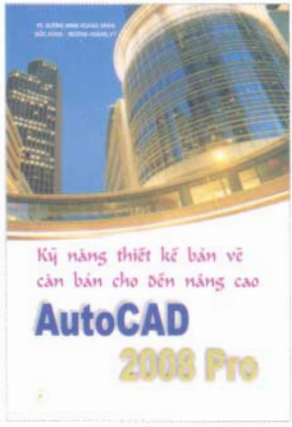
MỌI CHI TIẾT XIN LIÊN HỆ QUA ĐỊA CHỈ:

Công ty TNHH dịch vụ văn hóa KHANG VIỆT

2bisA Đinh Tiên Hoàng - P.Đakao - Q.1 - TP.HCM
ĐT : 08 9 120 915 - Fax : 08 9 111 564
email : binhthanhbookstore@yahoo.com

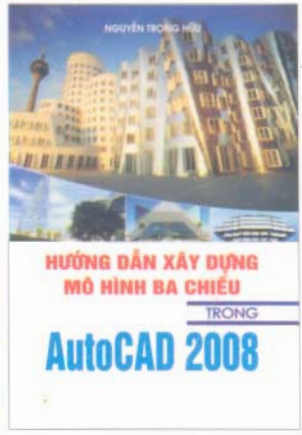












Công ty TNHH dịch vụ văn hóa KHANG VIỆT

NHÀ SÁCH KHANG VIỆT

Phát hành tại:

Nhà sách KHANG VIỆT

2bisA Đinh Tiên Hoàng - P.Đakao - Q.1 - TP.HCM
ĐT : 08 9 120 915 - Fax : 08 9 111 564
email : binhthanhbookstore@yahoo.com

Nhà sách CAO MINH

36 Nguyễn Thị Minh Khai - Q.1 - TP.HCM
ĐT : 08 8 227 346

VN 105 31

CĂN BẢN MẠNG KHÔNG DÂY
(WIRELESS)

8 935092 507101

GIÁ : 45.000