

Windows Vista™ Resource Kit

*Mitch Tulloch, Tony
Northrup, Jerry Honeycutt
with the MSWinVista Team*

9780735622838
Publication Date: April 2007

Microsoft®
Press

Table of Contents

<i>Acknowledgments</i>	xxvii
<i>System Requirements</i>	xxix
<i>Introduction</i>	xxxix

Part I Overview

1 Overview of Windows Vista Improvements	3
What's New	3
User Interactions	5
Performance	13
Mobility	16
Tablet PC	20
Deployment	22
Reliability and Supportability	23
Troubleshooting	28
Architecture Improvements	30
Windows Vista Editions	32
Windows Vista Starter	34
Windows Vista Home Basic	35
Windows Vista Home Premium	35
Windows Vista Business	35
Windows Vista Enterprise	36
Windows Vista Ultimate	36
Choosing Hardware	37
Windows Vista Logos	37
Hardware Requirements	38
Summary	38
Additional Resources	39
2 Security in Windows Vista	41
Addressing Specific Security Concerns with Windows Vista	41
Wireless Networks	42
Help Desk Calls Related to Malware	42
Data Theft	47
New and Improved Windows Vista Security Features	50
User Account Control (UAC)	50
Windows Defender	54
Windows Firewall	55

 **What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

	Internet Explorer Security Features	58
	BitLocker	60
	Encrypting File System (EFS)	63
	Auditing Enhancements	64
	Smart Card Improvements	65
	Credential Manager Enhancements	66
	Architectural and Internal Windows Vista Security Improvements	66
	Code Integrity (CI)	67
	Windows Resource Protection (WRP)	68
	Kernel Patch Protection	70
	Required Driver Signing	71
	Windows Service Hardening	71
	Authorization Manager	73
	Network Access Protection Client	74
	Web Services for Management	74
	Crypto Next Generation (CNG) Services	74
	Data Execution Prevention (DEP)	75
	Address Space Layout Randomization (ASLR)	76
	New Logon Architecture	76
	Rights Management Services (RMS)	77
	Multiple Local Group Policy Objects	78
	Summary	78
	Additional Resources	79
Part II	Deployment	
3	Deployment Platform	83
	Tools Introduction	83
	Windows Vista Deployment Terminology	85
	Platform Components	87
	Windows Imaging	88
	Answer Files	89
	Windows SIM	90
	Windows Setup	91
	Sysprep	91
	Windows PE	92
	Other Tools	93
	Windows DS	94
	ImageX	95
	Basic Deployment Process	96
	BDD 2007 Deployment Process	97
	Summary	102
	Additional Resources	102
4	Planning Deployment	105
	Using BDD 2007 for Deployment Planning	105
	Planning Guide	107
	Feature Team Guides	112
	Solution Framework	114
	Job Aids	114

Planning Low-Volume Deployment	115
Scope and Objectives	116
Current Environment	116
Configuration Plan	117
Testing and Piloting	117
Rolling Out	118
Windows Vista Requirements	119
Hardware Requirements	119
Upgrade Paths	119
Preparing for Development	120
Application Compatibility	120
Application Management	122
Computer Imaging System	123
Deployment	124
Infrastructure Remediation	125
Operations Readiness	125
Security	126
User State Migration	126
Installing BDD 2007	127
Program Folders	129
Distribution Share	129
Starting Deployment Workbench	130
Updating BDD 2007 Components	130
Summary	132
Additional Resources	132
5 Automating Installation	133
Deployment Scenarios	133
Upgrade Computer Scenario	134
New Computer Scenario	135
Replace Computer Scenario	135
Understanding Setup	136
Preinstallation Phase	137
Online Configuration Phase	138
Windows Welcome Phase	139
Preparing the Environment	141
Planning Installation	141
Configuring the Technician Computer	143
Using Windows SIM	145
Building Distribution Shares	147
Creating an Answer File	150
Adding Files to Answer Files	153
Converting Windows XP Answer Files	155
Unattend.txt	155
Sysprep.inf	156
WinBOM.ini	156
OEMInfo.ini	156
Oobeinfo.ini	156

Choosing Installation Methods	157
Staging Distribution Shares	157
Using Windows DS	157
Using SMS OSD and BDD	157
Summary	157
Additional Resources	158
6 Developing Disk Images	159
Getting Started	160
Prerequisite Skills	161
Lab Requirements	161
Capturing Images with BDD 2007	164
Navigating Deployment Workbench	165
Configuring the Lab Distribution Share	166
Adding Windows Vista	167
Adding Applications	169
Adding Packages	175
Adding Out-of-Box Drivers	177
Creating Image Builds	179
Editing a Build's Task Sequence	183
Configuring Group and Task Properties	186
Configuring the Options Tab	186
Creating the Lab Deployment Point	191
Configuring the Deployment Point	193
Updating the Deployment Point	197
Capturing a Disk Image for LTI	197
Capturing a Disk Image for ZTI	199
Creating an Image Capture CD	199
Preparing the Image for Capture	199
Capturing the Image	201
Manually Preparing Images	201
Customizing BDD 2007	203
Summary	203
Additional Resources	204
7 Migrating User State Data	207
Evaluating Migration Technologies	208
Windows Easy Transfer	208
User State Migration Tool	208
Microsoft IntelliMirror	209
Using Windows Easy Transfer	209
Planning User State Migration Using USMT	210
Choosing Subject Matter Experts	211
Identifying User State Data	212
Prioritizing Migration Tasks	213
Choosing a Data Store Location	214
Automating USMT	215
Installing USMT	216
Local Installation	217

Network Staging	218
BDD 2007	218
SMS 2003 OSD	218
Understanding USMT Components	218
Scanstate.exe	219
Loadstate.exe	220
XML Migration Files	220
Developing Migration Files	221
Customizing USMT	221
Control File Syntax	221
Deploying Migration Files	222
Using USMT in BDD 2007	222
Downloading USMT Components	223
Specifying the Data Store Location	224
Adding Custom Migration Files	226
Summary	227
Additional Resources	227
8 Deploying Applications	229
Preparing the Lab	230
Planning Deployment	231
Priorities	232
Categories	233
Installation Methods	234
Subject Matter Experts	235
Configurations	236
Mitigating Compatibility Issues	236
Choosing a Deployment Strategy	239
Thick Images	240
Thin Images	241
Hybrid Images	243
Automating Installation	243
Windows Installer	244
FLEXnet InstallShield	246
Legacy InstallShield	246
Legacy InstallShield PackageForTheWeb	247
Legacy Wise Installation System	247
Windows Script Host	248
Repackaging Legacy Applications	248
The Repackaging Process	249
Repackaging Tools	249
Injecting in a Disk Image	250
Adding Applications	251
Creating Dependencies	253
Installing Applications	254
Installing from an Answer File	256
Adding Applications in Audit Mode	257
Summary	258
Additional Resources	258

- 9 Preparing Windows PE 261**
 - Exploring Windows PE 262
 - Capabilities 263
 - Limitations 265
 - New Features 266
 - Setting up the Environment 267
 - Installing the Windows AIK 267
 - Configuring the Build Environment 268
 - Removing the Build Environment 269
 - Working with Windows PE 270
 - Applying Windows PE 270
 - Adding Optional Components 270
 - Copying Applications 273
 - Adding Device Drivers 273
 - Installing Updates 273
 - Prepping the Image 273
 - Capturing the Image 274
 - Creating Bootable Media 275
 - Customizing Windows PE 278
 - Automating Windows PE 280
 - Automating with Unattend.xml 280
 - Adding Images to Windows DS 280
 - Using Windows PE with BDD 281
 - Summary 283
 - Additional Resources 284

- 10 Deploying with Windows DS 285**
 - Introducing Windows DS 286
 - Service Architecture 286
 - Operating Modes 291
 - Planning for Windows DS 293
 - Server Requirements 293
 - Client Requirements 294
 - DHCP Requirements 295
 - Routing Requirements 296
 - Capacity Requirements 296
 - Installing Windows DS 297
 - Windows Server 2003 297
 - Windows Server Code Name "Longhorn" 298
 - Configuring Windows DS 299
 - Preparing Discover Images 301
 - Importing Images 302
 - Importing Boot Images 303
 - Importing Install Images 303
 - Managing Image Security 304
 - Installing Windows Vista 307
 - Capturing Custom Images 308
 - Using Windows DS with BDD 2007 309

	Summary	311
	Additional Resources	311
11	Using Volume Activation	313
	Introduction	313
	Volume Activation	314
	Activation Options	315
	Activation Terminology	319
	Planning an Activation Infrastructure	320
	Analyzing Activation Options	321
	Mapping Computers to Activation Options	322
	Implementing OEM Activation	322
	Installing Volume-Licensed Images on OEM Systems	323
	OEM Imaging of Volume Editions	324
	Implementing MAK Activation	324
	Obtaining MAKs	324
	Managing MAKs	324
	Obtaining Additional MAK Activations	325
	Assigning MAKs to Windows Vista Systems	325
	Volume Activation Management Tool	327
	Implementing KMS Activation	328
	Installing a KMS Computer	329
	Installing KMS Client Computers	332
	KMS Integration with the Deployment Workbench	333
	KMS Reporting	333
	Configuring KMS Activation	334
	Using SImgr.vbs to Configure KMS	334
	Using Registry Entries to Configure KMS	335
	KMS Computer Configuration	335
	KMS Client Configuration	336
	Using WMI to Configure KMS	336
	Activation in BDD 2007	337
	Using the Windows Deployment Wizard	338
	Automating the Windows Deployment Wizard	339
	Troubleshooting Volume Activation	339
	Common Problems	339
	Event Log Entries	341
	Resolving RFM	341
	Summary	344
	Additional Resources	345
12	Deploying with BDD 2007	347
	Introducing BDD 2007 Deployment	348
	Deployment Scenarios	348
	Comparing LTI and ZTI	348
	Preparing the Distribution Share	349
	Creating the Additional Deployment Points	350
	Preparing Windows PE for ZTI	355
	To Prepare the Windows PE Images	355
	Customizing Windows PE	356

- Providing Access to Windows PE Image 359
- Importing Windows PE in to SMS 2003 OSD 360
- Creating the SMS 2003 OSD Image Installation CD 360
- Preparing Windows DS 361
 - Selecting an Operational Mode 362
 - Adding Images to Windows DS 362
 - Pre-staging Destination Computers 363
- Configuring Resource Access 364
 - Creating Shared Folders 364
 - Configuring Share Permissions 364
 - Configuring Other Resources 365
 - Configuring ZTI Package Selection 367
- Configuring SMS 2003 for ZTI 368
 - Configuring the ZTI Operating System Image 368
 - Creating a ZTI User State Migration Package 372
- Customizing BDD 2007 Deployment 374
 - Configuring Multiple Computers 374
 - Configuring Individual Computers 377
 - Customizing CustomSettings.ini 378
 - Customizing BootStrap.ini 379
 - Using the BDD 2007 Database 380
- Configuring for Common Scenarios 385
 - Typical Settings for LTI 385
 - Typical Settings for ZTI 387
 - Automated Settings for LTI 388
- Performing LTI Deployments 391
- Performing ZTI Deployments 401
- Summary 402
- Additional Resources 402

Part III Desktop Management

- 13 Managing the Desktop Environment 407**
 - Understanding Group Policy in Windows Vista 407
 - Group Policy Issues on Earlier Versions of Windows 408
 - New Group Policy Features in Windows Vista 410
 - New Group Policy Settings in Windows Vista 411
 - Understanding ADMX Template Files 417
 - Understanding Multiple Local Group Policy 422
 - Managing Windows Vista Computers Using Group Policy 424
 - Configuring the Central Store 424
 - Creating and Editing GPOs 426
 - Using ADMX Migrator 430
 - Configuring Group Policy Processing 432
 - Using Advanced Group Policy Management 432
 - Troubleshooting Group Policy 433
 - Using Event Viewer 433
 - Enabling Debug Logging 435
 - Using GPLogView 435

	Summary	437
	Additional Resources	437
14	Managing Users and User Data	439
	Understanding User Profiles in Windows Vista	439
	Types of User Profiles	439
	User Profile Namespace	441
	Application Compatibility Issues	446
	Implementing Corporate Roaming	450
	Understanding Roaming User Profiles and Folder Redirection	450
	Implementing Folder Redirection	454
	Implementing Roaming User Profiles	466
	Working with Offline Files	475
	How Offline Files Works in Windows Vista	477
	Managing Offline Files	479
	Summary	483
	Additional Resources	483
15	Managing Disks and File Systems	485
	Overview of Partitioning Disks	486
	How to Choose Between MBR or GPT	486
	Converting from MBR to GPT Disks	487
	GPT Partitions	488
	Choosing Basic or Dynamic Disks	489
	Working with Volumes	489
	How to Create a Simple Volume	489
	How to Create a Spanned Volume	490
	How to Create a Striped Volume	491
	How to Resize a Volume	492
	How to Delete a Volume	493
	File System Fragmentation	494
	Backup and Restore	496
	How File Backups Work	498
	File and Folder Backup Structure	499
	How Complete PC Backups Work	501
	How to Start a Complete PC Backup from the Command Line	501
	How to Restore a Complete PC Backup	502
	Complete PC Backup Structure	505
	Best Practices for Computer Backups	505
	How to Manage Backup Using Group Policy Settings	506
	Previous Versions and Shadow Copies	508
	Windows ReadyBoost	513
	BitLocker Drive Encryption	516
	How BitLocker Encrypts Data	516
	How BitLocker Protects Data	517
	BitLocker Phases	520
	BitLocker Requirements	522
	How to Configure BitLocker Partitions	523
	How to Enable the Use of BitLocker on Computers Without TPM	523
	How to Enable BitLocker Encryption	524

	How to Manage BitLocker Keys on a Local Computer	527
	How to Manage BitLocker from the Command Line	527
	How to Recover Data Protected by BitLocker	529
	How to Disable or Remove BitLocker Drive Encryption	530
	How to Permanently Decommission a BitLocker Drive	531
	How to Prepare Active Directory for BitLocker	532
	How to Manage BitLocker with Group Policy	532
	The Costs of BitLocker	533
	Encrypting File System	534
	How to Export Personal Certificates	534
	How to Import Personal Certificates	535
	How to Grant Users Access to an Encrypted File	535
	Symbolic Links	536
	How to Create Symbolic Links	537
	How to Create Relative or Absolute Symbolic Links	538
	How to Create Symbolic Links to Shared Folders	539
	How to Use Hard Links	541
	Disk Quotas	541
	How to Configure Disk Quotas on a Single Computer	542
	How to Configure Disk Quotas from a Command Prompt	543
	How to Configure Disk Quotas by Using Group Policy Settings	544
	Summary	545
	Additional Resources	545
16	Managing Devices and Services	547
	Managing Devices	547
	Changes to Device Management in Windows Vista	547
	Understanding Device Installation in Windows Vista	549
	Managing Devices Using Group Policy	558
	Troubleshooting Device Installation	568
	Understanding Power Management	574
	Configuring Power Management Settings	576
	Understanding Services	586
	Changes to Services in Windows Vista	587
	Managing Services	589
	Summary	593
	Additional Resources	593
17	Managing Sharing	595
	Managing File Sharing	595
	Understanding Local Sharing	596
	Understanding Network Sharing	600
	Implementing File Sharing	607
	Managing File Sharing Using Group Policy	624
	Creating and Managing Shares Using the Net Commands	624
	Creating and Managing Shares Using Scripts	626
	Troubleshooting File Sharing	632
	Best Practices for Implementing File Sharing in a Workgroup Environment	634

	Best Practices for Implementing File Sharing in a Domain Environment	635
	Managing Media Sharing	636
	Media Sharing and Windows Firewall	638
	Media Sharing and Windows Firewall in Windows XP	639
	Limitations of Media Sharing	640
	Media Sharing and Network Categories	641
	Using Media Sharing	642
	Managing Media Sharing with Group Policy	645
	Troubleshooting Media Sharing	646
	Best Practices for Media Sharing	647
	Summary	647
	Additional Resources	647
18	Managing Windows Meeting Space	649
	Understanding How Meeting Space Works	650
	Meeting Space and Microsoft P2P Collaboration Services	650
	Meeting Space and IPv6	651
	Meeting Space and the Peer Name Resolution Protocol (PNRP)	653
	Meeting Space and People Near Me	654
	Meeting Space Services	655
	Meeting Space and Windows Firewall	655
	Meeting Space and Security	657
	How a Meeting Works	659
	Limitations of Meeting Space	660
	Deploying and Managing Meeting Space	662
	Managing Meeting Space in a Workgroup Environment	662
	Managing Meeting Space in a Domain Environment	662
	Managing Meeting Space in an Ad-Hoc Wireless Environment	664
	Using Meeting Space	664
	Setting Up Meeting Space	665
	Configuring People Near Me	667
	Starting a New Meeting	670
	Joining a Meeting	670
	Inviting Others to Your Meeting	672
	Collaborating Within a Meeting	673
	Troubleshooting Meeting Space	673
	Summary	674
	Additional Resources	674
19	Managing Printing	677
	Enhancements to Printing in Windows Vista	677
	Understanding Printing in Windows Vista	679
	Understanding the XML Paper Specification	679
	Understanding the Windows Vista Print Subsystem	680
	Understanding Print Management	683
	Enhancements to Print Management in Windows Vista	683
	The Print Management Console	684
	Adding and Removing Print Servers	686
	Adding Printers Using the Network Printer Installation Wizard	687

Creating and Using Printer Filters	688
Managing Printers Using Print Management	690
Configuring Properties of Printers	690
Publishing Printers in Active Directory	691
Managing Printer Drivers	692
Exporting and Importing Print Server Configurations	694
Performing Bulk Actions Using Print Management	695
Client-Side Management of Printers	696
Installing Printers Using the Printers CPL	697
Searching for Printers	698
Installing Printers Using Point and Print	700
Using Printers Explorer	701
Using the Color Management CPL	701
Managing Client-Side Printer Experience Using Group Policy	702
Configuring the Add Printer Wizard	702
Disable Client-Side Printer Rendering	704
Configuring Package Point and Print Restrictions	705
Deploying Printers Using Group Policy	707
Preparing to Deploy Printers	707
Deploying a Printer Connection	708
Limitations of Deploying Printers Using Group Policy	710
Assigning Printers Based on Location	710
Migrating Print Servers	712
Migrate Print Servers Using Print Management	712
Migrating Print Servers Using Printbrm.exe	714
Monitoring and Troubleshooting Printers	714
Configuring E-Mail Notifications	715
Configuring Print Server Notifications	715
Configuring Script Actions	716
Configuring Detailed Event Logging	716
Summary	717
Additional Resources	717
20 Managing Search	719
Search and Indexing Enhancements in Windows Vista	719
Issues in Previous Windows Platforms	719
Design Goals and New Features	720
How Search and Indexing Works in Windows Vista	721
Understanding Search Engine Terminology	722
Windows Search Engine Processes	723
Windows Search Engine Architecture	726
Understanding the Catalog	727
Understanding the Indexing Process	732
Understanding Remote Search	740
Managing Indexing	741
Configuring the Catalog	741
Configuring Offline Files Indexing	743
Configuring Indexing of Encrypted Files	744
Configuring Indexing of Similar Words	744

Other Configuration Options	745
Using Search	746
Configuring Search Using Folder Options	746
Search Integration in the Shell	748
Using Instant Search	748
Using the Search Explorer	750
Other Search and Organization Features	753
Troubleshooting Search	753
Summary	754
Additional Resources	754
21 Managing Internet Explorer	757
Non-Security Internet Explorer Improvements	757
User Interface Changes	757
Tabbed Browsing	758
Search Bar	758
RSS Feeds	760
Improved Standards Support	761
Expanded Group Policy Settings	762
Internet Explorer 7 Security Features	762
Defending Against Malware	765
Protecting Against Data Theft	774
Security Zones	784
Managing Internet Explorer with Group Policy	788
Using the Internet Explorer Administration Kit	791
Troubleshooting Internet Explorer Problems	792
Internet Explorer Does Not Start	793
An Add-on Does Not Work Properly	793
Some Webpages Do Not Display Properly	794
An Unwanted Toolbar Appears	796
The Home Page or Other Settings Have Changed	796
Summary	797
Additional Resources	797

Part IV Desktop Maintenance

22 Maintaining Desktop Health	801
Monitoring Reliability and Performance	801
Component Binaries	802
Opening the Reliability and Performance Monitor	802
Using Resource Overview	803
Using Performance Monitor	806
Using Reliability Monitor	824
Understanding Windows Eventing	831
Overview of Windows Eventing	831
Windows Eventing Capabilities	832
Event Viewer User Interface	838
Understanding the Windows System Assessment Tool	851
Overview of WinSAT	851

How Desktop Window Manager Performs Composition	855
Troubleshooting Aero Glass	857
Overriding Windows Vista Automatic Detection Mechanisms	858
Using Performance Information And Tools	860
Accessing Performance Information And Tools	860
Configuring Performance Information And Tools Using Group Policy	862
Understanding Each Section of the Tool	862
Understanding Windows Error Reporting	865
Overview of Windows Error Reporting	866
Error Reporting Cycle	867
Report Data Overview	868
Conceptual Components	869
Architecture of Windows Error Reporting	873
Configuring Windows Error Reporting	875
Using the Problem Reports And Solutions Control Panel	879
Using Task Scheduler	884
Task Scheduler Enhancements and Improvements	884
Operational Overview	886
Task Scheduler Architecture	886
Task Scheduler Security	888
AT and Task Scheduler v1.0 Compatibility Modes	889
Task Scheduler User Interface	890
Creating New Tasks	891
Managing Tasks	901
Using the SchTasks.exe Command	903
Scheduled Tasks Events	906
Troubleshooting Task Scheduler	906
Interpreting Result and Return Codes	908
Summary	909
Additional Resources	909

23 Supporting Users Using Remote Assistance 911

Understanding Remote Assistance	911
Improvements to Remote Assistance in Windows Vista	912
How Remote Assistance Works	913
Using Remote Assistance in the Enterprise	922
Interoperability with Remote Assistance in Windows XP	924
Implementing and Managing Remote Assistance	925
Initiating Remote Assistance Sessions	925
Scenario 1: Offering Remote Assistance Using DCOM	927
Scenario 2: Soliciting Remote Assistance by Creating RA Tickets and Saving Them on Monitored Network Shares	929
Managing Remote Assistance Using Group Policy	933
Additional Registry Settings for Configuring Remote Assistance	936
Summary	941
Additional Resources	942

24	Managing Software Updates	943
	Update Improvements to Windows Vista	944
	Methods for Deploying Updates	946
	Windows Update Client	946
	Windows Server Update Services	947
	Systems Management Server	949
	Manually Installing, Scripting, and Removing Updates	950
	Overview of Windows Vista Update Files	950
	How to Script Update Installations	951
	How to Remove Updates	951
	Deploying Updates to New Computers	952
	Managing BITS	956
	BITS Behavior	956
	BITS Group Policy Settings	957
	The BITSAdmin.exe Tool	959
	Windows Update Group Policy Settings	963
	Configuring Windows Update to Use a Proxy Server	965
	Tools for Auditing Software Updates	966
	The MBSA Console	966
	MBSACLI	968
	SMS	970
	Troubleshooting the Windows Update Client	970
	The Process of Updating Network Software	973
	Assembling the Update Team	973
	Inventorying Software	974
	Creating an Update Process	976
	How Microsoft Distributes Updates	981
	Security Updates	982
	Update Rollups	983
	Service Packs	983
	Microsoft Product Life Cycles	985
	Summary	985
	Additional Resources	986
25	Managing Client Protection	987
	Understanding the Risk of Malware	987
	User Account Control	988
	UAC for Standard Users	991
	UAC for Administrators	992
	UAC User Interface	993
	How Windows Vista Determines Whether an Application Needs Administrative Privileges	995
	UAC Virtualization	998
	UAC and Startup Programs	999
	Compatibility Problems with UAC	999
	How to Configure User Account Control	1002
	How to Configure Auditing for Privilege Elevation	1007
	Other UAC Event Logs	1008
	Best Practices for Using UAC	1008

Using Windows Defender	1009
Understanding Windows Defender	1010
Windows Defender Alert Levels	1013
Understanding Microsoft SpyNet	1014
Configuring Windows Defender Using Group Policy	1015
Configuring Windows Defender on a Single Computer	1017
Windows Defender Tools	1017
How to Determine if a Computer Is Infected with Spyware	1019
Best Practices for Using Windows Defender	1020
How to Troubleshoot Problems with Unwanted Software	1021
Microsoft Forefront Client Security	1022
Summary	1024
Additional Resources	1025

Part V Networking

26	Configuring Windows Networking	1029
	Usability Improvements	1029
	Network And Sharing Center	1030
	Network Explorer	1032
	Network Map	1035
	Networking Icons in the System Tray	1036
	The Set Up A Connection Or Network Wizard	1037
	Manageability Improvements	1037
	Network Access Protection (NAP)	1038
	Network Location Types	1039
	Policy-based QoS	1041
	Windows Firewall and IPsec	1044
	Windows Connect Now	1044
	Core Networking Improvements	1045
	Efficient Networking	1046
	Improved Reliability	1050
	IPv6 Support	1051
	802.1X Network Authentication	1053
	Server Message Block (SMB) 2.0	1056
	Strong Host Model	1056
	Wireless Networking	1057
	Improved APIs	1059
	Network Awareness	1059
	Improved Peer Networking	1060
	EAPHost Architecture	1062
	Layered Service Provider (LSP)	1063
	Windows Sockets Direct Path for System Area Networks	1064
	How to Configure Wireless Settings	1065
	Manually Configuring Wireless Settings	1065
	Using Group Policy to Configure Wireless Settings	1067
	Configuring Wireless Settings from the Command Line or a Script	1069
	How to Configure TCP/IP	1071
	DHCP	1071

	Manually Configuring IP Addresses	1074
	Command Line and Scripts	1075
	How to Connect to Active Directory Domains	1078
	Summary	1079
	Additional Resources	1080
27	Configuring Windows Firewall and IPsec	1083
	Understanding Windows Firewall	1083
	Understanding the Windows Filtering Platform	1085
	Understanding Windows Service Hardening	1087
	Understanding Windows Firewall Profiles	1090
	Understanding Windows Firewall Policy Storage and Rule Merge Logic	1093
	Understanding Windows Firewall Rules	1094
	Understanding IPsec Integration	1115
	Understanding Windows Firewall Logging and Auditing	1128
	Managing Windows Firewall	1131
	Managing Windows Firewall Using the Windows Firewall With Advanced Security Snap-in	1133
	Managing Windows Firewall Using Group Policy	1137
	Managing Windows Firewall Using netsh	1140
	Managing Windows Firewall Using Scripts	1140
	Common Management Tasks	1142
	Summary	1145
	Additional Resources	1145
28	Connecting Remote Users and Networks	1147
	Understanding Connection Types	1147
	Outgoing Connection Types	1148
	Incoming Connection Types	1149
	Deprecated Connection Types	1149
	Configuring Virtual Private Network Connections	1150
	Supported Tunneling Protocols	1150
	Enhancements to VPN Security in Windows Vista	1150
	VPN Connection Negotiation Process	1155
	Creating and Configuring VPN Connections	1156
	Configuring Dial-up Connections	1170
	Creating a Dial-up Connection	1171
	Configuring a Dial-up Connection	1172
	Advanced Connection Settings	1173
	Configuring Incoming Connections	1173
	Managing Connections Using Group Policy	1175
	Using Remote Desktop	1178
	Understanding Remote Desktop	1178
	Steps for Using Remote Desktop	1182
	Enabling Remote Desktop and Authorizing Users on a Single Computer	1182
	Enabling Remote Desktop using Group Policy	1185
	Configuring and Deploying Remote Desktop Connection	1185

Establishing a Remote Desktop Session	1193
Improving Remote Desktop Performance	1193
Troubleshooting Remote Desktop	1194
Summary	1195
Additional Resources	1195

29 Deploying IPv6 1197

Understanding IPv6	1197
Understanding IPv6 Terminology	1198
Understanding IPv6 Addressing	1199
Understanding ICMPv6 Messages	1204
Understanding Neighbor Discovery	1204
Understanding Address Autoconfiguration	1206
Understanding Name Resolution	1208
IPv6 Enhancements in Windows Vista	1211
Configuring and Troubleshooting IPv6 in Windows Vista	1214
Displaying IPv6 Address Settings	1214
Configuring IPv6 in Windows Vista Using the User Interface	1218
Configuring IPv6 in Windows Vista Using Netsh	1219
Other IPv6 Configuration Tasks	1220
Troubleshooting IPv6 Connectivity	1224
Planning for IPv6 Migration	1226
Understanding ISATAP	1227
Migrating an Intranet to IPv6	1228
Summary	1231
Additional Resources	1231

Part VI Troubleshooting

30 Configuring Startup and Troubleshooting Startup Issues 1235

What's New with Windows Vista Startup	1235
Boot Configuration Data	1236
System Recovery	1239
Windows Boot Performance Diagnostics	1240
Understanding the Startup Process	1241
Power-on Self Test Phase	1242
Initial Startup Phase	1242
Windows Boot Manager Phase	1245
Windows Boot Loader Phase	1246
Kernel Loading Phase	1247
Logon Phase	1251
Important Startup Files	1253
How to Configure Startup Settings	1254
How to Use the Startup And Recovery Dialog Box	1254
How to Use the System Configuration Tool	1254
How to Use BCDEdit	1256
How to Remove the Windows Vista Boot Loader	1261
The Process of Troubleshooting Startup	1262
Startup Troubleshooting Before the Progress Bar Appears	1262

	Startup Troubleshooting After the Progress Bar Appears	1272
	Troubleshooting Startup Problems After Logon	1284
	Summary	1288
	Additional Resources	1289
31	Troubleshooting Hardware, Driver, and Disk Issues	1291
	Windows Vista Improvements for Hardware and Driver Troubleshooting	1291
	Windows Memory Diagnostics	1292
	Disk Failure Diagnostics	1292
	Self-Healing NTFS	1293
	Reliability Monitor	1294
	Improved Driver Reliability	1294
	Improved Error Reporting	1295
	The Process of Troubleshooting Hardware Issues	1295
	How to Troubleshoot Problems That Prevent Windows from Starting	1295
	How to Troubleshooting Problems Installing New Hardware	1295
	How to Troubleshooting Problems with Existing Hardware	1296
	How to Troubleshoot Unpredictable Symptoms	1298
	How to Diagnose Hardware Problems	1299
	How to Use Device Manager to Identify Failed Devices	1299
	How to Check the Physical Setup of Your Computer	1300
	How to Check the Configuration of Your Hardware	1301
	How to Verify That System Firmware and Peripheral Firmware Are Up to Date	1302
	How to Test Your Hardware by Running Diagnostic Tools	1302
	How to Simplify Your Hardware Configuration	1303
	How to Diagnose Disk-Related Problems	1304
	How to Use Built-in Diagnostics	1305
	How to Use Problem Reports and Solutions	1305
	How to Use Reliability Monitor	1305
	How to Use Event Viewer	1306
	How to Use Data Collector Sets	1306
	How to Use Windows Memory Diagnostics	1307
	How to Troubleshoot Disk Problems	1315
	How to Prepare for Disk Failures	1315
	How to Use Chkdsk	1316
	How to Use the Disk Cleanup Wizard	1322
	How to Disable Non-volatile Caching	1322
	How to Troubleshoot Driver Problems	1323
	How to Find Updated Drivers	1323
	How to Roll Back Drivers	1324
	How to Use the Driver Verifier	1324
	How to Use the File Signature Verification	1326
	How to Use Device Manager to View and Change Resource Usage	1327
	How to Use System Restore	1328
	How to Troubleshoot USB Problems	1329
	How to Troubleshoot Bluetooth Problems	1333
	Summary	1334
	Additional Resources	1334

32	Troubleshooting Network Issues	1337
	Tools for Troubleshooting	1337
	Arp	1340
	Event Viewer	1341
	Ipconfig	1342
	Nbtlookup	1343
	Nbtstat	1344
	Net	1346
	Netstat	1348
	Network Monitor	1349
	Nslookup	1351
	PathPing	1354
	Performance Monitor	1357
	Ping	1360
	Portqry	1361
	Reliability and Performance	1363
	Resource Monitor	1365
	Route	1366
	Task Manager	1368
	Telnet Client	1370
	Test TCP	1372
	Windows Network Diagnostics	1374
	The Process of Troubleshooting Network Problems	1374
	How to Troubleshoot Network Connectivity Problems	1376
	How to Troubleshoot Application Connectivity Problems	1381
	How to Troubleshoot Name-Resolution Problems	1384
	How to Troubleshoot Performance Problems and Intermittent Connectivity Issues	1388
	How to Troubleshoot Joining or Logging on to a Domain	1391
	How to Troubleshoot Network Discovery	1394
	How to Troubleshoot File and Printer Sharing	1395
	How to Troubleshoot Wireless Networks	1397
	How to Troubleshoot Firewall Problems	1399
	Summary	1401
	Additional Resources	1401
33	Troubleshooting Stop Messages	1403
	Stop Message Overview	1403
	Identifying the Stop Error	1404
	Finding Troubleshooting Information	1404
	Stop Messages	1405
	Types of Stop Errors	1408
	Memory Dump Files	1408
	Configuring Small Memory Dump Files	1410
	Configuring Kernel Memory Dump Files	1411
	Configuring Complete Memory Dump Files	1412
	How to Manually Initiate a Stop Error and Create a Dump File	1413
	Using Memory Dump Files to Analyze Stop Errors	1413

Being Prepared for Stop Errors	1419
Prevent System Restarts After a Stop Error	1419
Record and Save Stop Message Information	1420
Check Software Disk Space Requirements	1421
Install a Kernel Debugger and Symbol Files	1421
Common Stop Messages	1421
Stop 0x0A or IRQL_NOT_LESS_OR_EQUAL	1421
Stop 0x1E or KMODE_EXCEPTION_NOT_HANDLED	1423
Stop 0x24 or NTFS_FILE_SYSTEM	1425
Stop 0x2E or DATA_BUS_ERROR	1426
Stop 0x3F or NO_MORE_SYSTEM_PTES	1427
Stop 0x50 or PAGE_FAULT_IN_NONPAGED_AREA	1428
Stop 0x77 or KERNEL_STACK_INPAGE_ERROR	1429
Stop 0x7A or KERNEL_DATA_INPAGE_ERROR	1430
Stop 0x7B or INACCESSIBLE_BOOT_DEVICE	1432
Stop 0x7F or UNEXPECTED_KERNEL_MODE_TRAP	1434
Stop 0x9F or DRIVER_POWER_STATE_FAILURE	1436
Stop 0xBE or ATTEMPTED_WRITE_TO_READONLY_MEMORY	1437
Stop 0xC2 or BAD_POOL_CALLER	1437
Stop 0xCE or DRIVER_UNLOADED_WITHOUT_CANCELLING_PENDING_OPERATIONS	1439
Stop 0xD1 or DRIVER_IRQL_NOT_LESS_OR_EQUAL	1440
Stop 0xD8 or DRIVER_USED_EXCESSIVE_PTES	1440
Stop 0xEA or THREAD_STUCK_IN_DEVICE_DRIVER	1441
Stop 0xED or UNMOUNTABLE_BOOT_VOLUME	1441
Stop 0xFE or BUGCODE_USB_DRIVER	1442
Stop 0xC000021A or STATUS_SYSTEM_PROCESS_TERMINATED	1443
Stop 0xC0000221 or STATUS_IMAGE_CHECKSUM_MISMATCH	1444
Hardware Malfunction Messages	1445
Stop Message Checklist	1445
Check Your Software	1446
Check Your Hardware	1448
Summary	1450
Additional Resources	1450
Part VII Appendices	
A Appendix A	1453
B Appendix B	1461
C Appendix C	1471
Glossary	1481
Index	1499

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Supporting Users Using Remote Assistance

In this chapter:

Understanding Remote Assistance	911
Implementing and Managing Remote Assistance	925
Summary	941
Additional Resources	942

Remote Assistance (RA) in Windows Vista includes a number of improvements in connectivity, performance, usability, and security along with feature enhancements that make it even more useful than RA in Windows XP. With increased Group Policy support, command-line scripting capabilities, session logging, bandwidth optimization, and more, Remote Assistance is now an essential tool for enabling enterprises to support users in Help Desk scenarios. This chapter examines how Remote Assistance works in Vista, how to use it to support end users, and how to manage it using Group Policy and scripts.

Understanding Remote Assistance

Supporting end users is an essential function of IT departments and the corporate Help Desk. Unfortunately, conventional technical support provided over the telephone or using chat tools is generally cumbersome and inefficient. As a result, supporting users is often both time-consuming and costly for large enterprises to implement. For example, end users often have difficulty describing the exact nature of the problem they are having. Because of their general inexperience and lack of technical knowledge, end users may try to describe their problem using non-technical, inexact language. As a result, Help Desk personnel are generally reduced to asking a series of simple questions to try and isolate the problem the user is having. The methodical nature of these questions sometimes causes users to feel as if Help Desk personnel are being condescending, and such misunderstanding can reduce the effectiveness of the support experience and can make users tend to avoid contacting support personnel when future problems arise.

End users also often have difficulty following instructions given to them by Help Desk personnel who are trying to assist them. Well-trained support personnel will try to avoid using technical jargon when communicating with end users, but although using plain language can improve the support experience, it may also mean that resolution steps become long and tire-

some. For example, telling a user how to use Disk Cleanup from System Tools in Accessories can require several sentences or more, and this kind of communication can add time to support incidents, making them more costly to the company.

Remote Assistance (RA) solves these problems by enabling support personnel to view the user's desktop in real time. The user seeking assistance can demonstrate the nature of the problem to the support person. This is a quicker and more efficient way to communicate a problem than using words or e-mail. If necessary, the user can also give the support person permission to assume shared interactive control of the user's computer to show the user how to resolve the problem. The result of using Remote Assistance is faster problem resolution, an improved support experience, and a lower Total Cost of Ownership (TCO) for supporting end users in large, corporate environments.

Remote Assistance vs. Remote Desktop

Remote Assistance and Remote Desktop are different features of Vista that have entirely different uses. Remote Desktop is based on Microsoft's Terminal Services and is a tool for remotely logging on to remote computers. When you use Remote Desktop to connect to a remote computer, a new user session is established. Remote Desktop can also establish sessions with computers that have no interactive sessions running (no users logged on locally) such as headless servers. For more information on Remote Desktop, see Chapter 28, "Connecting Remote Users and Networks."

Remote Assistance, on the other hand, is a tool for interactively helping users troubleshoot problems with their computers. To use Remote Assistance, both the User (also called the Novice) and the Helper must be present on their computers. Unlike Remote Desktop, Remote Assistance does not create a new session. Instead, Remote Assistance allows the Helper to work in the existing session of the User. The User's desktop gets *remoted* to the Helper, who can then view the User's desktop and, with the User's consent, share control of the desktop.

Here is another way to summarize the difference between these two features: In Remote Assistance, both users involved are looking at the same desktop using the same logon credentials (those of the interactively logged-on User) and can share control of that desktop; in Remote Desktop, when the remote person logs on, the interactively logged-on user (if there is one) is logged out.

Improvements to Remote Assistance in Windows Vista

Windows Vista includes a number of new features and enhancements for Remote Assistance compared to the Remote Assistance available in Windows XP, including:

- Connectivity improvements with transparent NAT traversal using Teredo and IPv6.

- An improved user interface that is easier to launch and use.
- A standalone executable (`msra.exe`) that accepts command-line arguments and can easily be scripted.
- Improved overall performance with a smaller footprint, quicker startup and connect times, and optimized bandwidth usage for screen updates.
- Enhanced security with mandatory password and integration with UAC.
- New Offer RA via IM scenario and an open API for integration with peer-to-peer applications.
- Additional Group Policy settings for improved manageability.

Remote Assistance in Vista deprecates the following features that were available on XP:

- No more support for the MAILTO method of solicited Remote Assistance
- No more support for voice sessions

For information on interoperability between the XP and Vista versions of Remote Assistance, see the section titled “Interoperability with Remote Assistance in Windows XP” later in this chapter.

How Remote Assistance Works

In Remote Assistance, the person needing help is referred to as the *User* (or *Novice*) and the support person providing assistance is called the *Helper* (or *Expert*). RA is launched from the Start Menu by navigating to All Programs, clicking Maintenance, and then selecting Windows Remote Assistance. It can also be launched from a command prompt by typing **msra.exe**.

Remote Assistance has two basic modes of operation:

- **Solicited RA** In *Solicited RA* (also known as *Escalated RA*) the User requests assistance from the Helper by initiating the RA session using e-mail, instant messaging, or by providing the Helper with a saved copy of an invitation file (*.MsRcIncident). Each of these methods uses a different underlying mechanism:
 - **Solicited RA using e-mail** This method requires that the e-mail clients being used by the User support Simple Mail Application Programming Interface (SMAPI). An example of an e-mail client that supports SMAPI is Windows Mail, which is included with Windows Vista. Other examples of SMAPI-compliant e-mail clients include Microsoft Outlook and other third-party clients. In this approach, the User launches the RA user interface to create an email message that has an RA invitation file (*.MsRcIncident) attached to the message. The User must enter a password for the RA session, which must be communicated to the Helper using an out-of-band (OOB) method such as calling the Helper on the telephone. When the Helper receives the User’s RA invitation, she opens the attached ticket, enters the

password that was conveyed by the User, and the RA session starts. The Helper must respond to the invitation from the User within a specified time limit (default is 6 hours) or the invitation will expire and a new one will need to be sent. In a domain environment this ticket lifetime can also be configured using Group Policy. See the section titled “Managing Remote Assistance Using Group Policy” later in this chapter.

- ❑ **Solicited RA using file transfer** This method requires that both the User and Helper have access to a common folder (such as a network share on a file server) or that they use some other method for transferring the file (for example, by using a USB key to manually transfer the file or by uploading the file to an FTP site). The user creates an RA invitation file and saves it in the shared folder. The User must provide a password that must be communicated to the Helper using an out-of-band (OOB) method such as a telephone call. The Helper retrieves the ticket from the shared folder, opens it, enters the password, and the RA session starts. Again, the Helper must respond to the invitation within a specified time or the invitation will expire and a new one will be needed (the expiration time is configurable using Group Policy).
- ❑ **Solicited RA using Instant Messaging** This method for soliciting assistance requires that the instant messaging (IM) applications being used by both the User and the Helper support Microsoft’s new Rendezvous API. Windows Live Messenger is an example of an IM application that supports Rendezvous. Windows Live Messenger is available as a download. In this approach, the User requests assistance from someone on his buddy list. To ensure that the remote person is really the User’s buddy (and not someone masquerading as the buddy), Remote Assistance requires that a password be relayed from the User to the Helper by other means (such as a phone call) before the Helper can connect. For more information on the Rendezvous API, see the Windows SDK on MSDN at <http://windowsdk.msdn.microsoft.com/en-us/library/default.aspx>.
- **Unsolicited RA** In Unsolicited RA (also known as Offer RA) the Helper offers help to the User by initiating the RA session.
 - ❑ **Offer RA using DCOM** This is a typical corporate Help Desk scenario in which all the users are in a domain. The Helper enters either the fully qualified name (FQDN) or IP address of the User’s computer to connect to the User’s computer. This method requires that the Helper has been previously authorized a domain administrator to be able to offer Remote Assistance to the Users. (For information on how to authorize Helpers for offering RA, see the section titled “Managing Remote Assistance Using Group Policy” later in this chapter.) This method also requires that the Helper either knows the name (the host name on a local subnet; the fully qualified name otherwise) or address (IPv4 or IPv6) of the User’s computer.
 - ❑ **Offer RA using Instant Messaging** This method for soliciting assistance requires that the instant messaging (IM) applications being used by both the User and the

Helper support the Rendezvous API. In this approach, the Helper offers assistance to someone on her buddy list. If the buddy agrees, then he must enter a password to be used by the Helper. The password must be relayed by an OOB mechanism to ensure that the remote person is really the User's buddy (and not someone masquerading as the buddy). For more information on the Rendezvous API, see the Windows SDK on MSDN at <http://windowssdk.msdn.microsoft.com/en-us/library/default.aspx>.

How It Works: RA Invitation Files

Remote Assistance invitation files (.MsRcIncident) are XML-formatted file documents that include information used by the Helper's computer that will attempt to connect. This ticket information is encrypted to prevent unauthorized users from accessing the information should e-mail or file transfer be used to send the invitation over an unsecured network.

If the e-mail method is used to send the invitation file to the Helper, the invitation file is sent as an e-mail attachment with a file name of RATicket.MsRcIncident. If the file transfer method is used instead, the invitation file is created by default on the desktop of the User's computer and the file name of the invitation is Invitation.MsRcIncident.

Remote Assistance Operational States

Remote Assistance has three operational states:

- **Waiting For Connect** This state occurs when either:
 - ❑ The Helper has offered RA to the User but the User has not yet agreed to allow the Helper to connect to his computer.
 - ❑ The User has sent the Helper an invitation but the Helper has not yet responded by opening the invitation, or the Helper has opened the invitation and the User has not yet agreed to allow the Helper to connect to his computer.

In the Waiting For Connect state, the Helper cannot view or control the screen of the User's computer until an RA connection has been established and both computers have entered the Screen Sharing state. Once the RA application has been started and is running in the Waiting For Connect state, the application should not be closed until the other party responds and establishes the connection. For example, if the User uses the Solicit RA Using E-mail method and sends an invitation file to a Helper, the RA application opens on the User's computer and waits for the Helper to accept the invitation. If the User closes RA on her computer before the Helper accepts the invitation, the Helper will not be able to connect to the User's computer and the User will need to send a new invitation.

- **Screen Sharing** This state occurs when the User has consented to allow the Helper to connect to his computer—either after the User has sent the Helper an invitation or the Helper has offered RA to the User. In the Screen Sharing state, an RA session has been established and the Helper can view—but not control—the screen of the User’s computer.

When the User is prompted for consent to allow the Helper to connect to his computer, a warning message appears on the User’s computer saying that the Helper wants to connect to his computer. This warning message is customizable using Group Policy. See the section titled “Managing Remote Assistance Using Group Policy” later in this chapter for more information.

- **Control Sharing** This state occurs after the Screen Sharing state, when the Helper has requested control of the User’s computer and the User has consented to allow the Helper to have shared control of his computer. In the Control Sharing state, the Helper has the same level of access to the User’s computer that the User has and the Helper can use his own mouse and keyboard to remotely perform actions on the User’s computer. Specifically:
 - If the User is a standard user on his computer, the Helper will only be able to perform actions on the User’s computer that can be performed by a standard user on that computer.
 - If the User is a local administrator on his computer, the Helper will be able to perform any actions on the User’s computer that can be performed by a local administrator on that computer.

For more information on the level of control that a Helper has on a User’s computer, see the section titled “Remote Assistance and the Secure Desktop” later in this chapter.

User vs. Helper Functionality

Once an RA connection has been established and both computers have entered the Screen Sharing state, the User and Helper are able to perform the tasks listed in Table 23-1.

Table 23-1 Tasks That Can Be Performed by User and Helper During an RA Session

Description of task	User?	Helper?
Chat	Yes	Yes
Send files	Yes	Yes
Save a log of session activity	Yes (default)	Yes (default)
Configure bandwidth usage	Yes	No
Pause (temporarily hide screen)	Yes	No
Request shared control	No	Yes
Give up shared control	Yes	Yes
Disconnect	Yes	Yes
Disconnect using Esc key	Yes	No

Remote Assistance and NAT Traversal

Remote Assistance works by establishing a peer-to-peer connection between the User's computer and the Helper's computer. One challenge this poses is that it can be difficult to establish peer-to-peer connections if one or both of the computers involved are behind a gateway or router that uses Network Address Translation (NAT). NAT is an IP routing technology described by RFC 1631 that is used to translate IP addresses and TCP/UDP port numbers of packets being forwarded. NAT is typically used to map a set of private IP addresses to a single public IP address (or to multiple public addresses). Home networks using a wireless or wired router also use NAT technology.

To overcome this difficulty, Vista includes built-in support for Teredo, an IPv6 transition technology described in RFC 4380 that provides address assignment and automatic tunneling for unicast IPv6 connectivity across the IPv4 Internet. The NAT traversal capability provided by Teredo in Vista allows RA connectivity when one or both of the users involved in an RA session are hidden behind a NAT. The RA experience is transparent from the perspective of the users involved, regardless of whether NAT is being used on either user's network. For most small business and home user environments, Vista's RA will seamlessly traverse a NAT-enabled router with no additional router configuration required. For information on enterprises that need to remotely support users who work from home, see the section titled "Other Possible Remote Assistance Usage Scenarios" later in this chapter.



Note Offering RA using DCOM is not usually a Teredo scenario because enterprise users are behind a corporate firewall and not separated from each other by NATs.

Remote Assistance will not connect in certain configurations. Specifically:

- Teredo cannot traverse a symmetric NAT. Remote Assistance can only connect across restricted NATs and cone NATs. In most cases, this is not a significant limitation because the large majority of deployed NATs are either the restricted or cone variety. For more information on NAT traversal support in Vista, see Chapter 29, "Deploying IPv6."
- RA will not work if the NAT-enabled router is configured to block the specific ports used by RA. See the section titled "Remote Assistance and Windows Firewall" later in this chapter for more information.
- Remote Assistance will not work if the user's NAT-enabled router is configured to block all UDP traffic.



Note To determine the type of NAT a network is using, open an elevated command prompt and type **netsh interface teredo show state**.

For more information on IPv6 support in Windows Vista, including built-in client support for Teredo and other IPv6 transition technologies, see Chapter 29.

Remote Assistance and IP Ports Used

The ports used by a Remote Assistance session depend on whether the session is between two Vista computers or between a Vista computer and a downlevel Windows XP computer. Specifically:

- **Vista to Vista RA Session** Dynamic ports allocated by the system in the range TCP/UDP 49152–65535
- **Vista to XP RA Session** Port 3389 TCP (local/remote)

In addition, the Offer RA via DCOM scenario uses Port 135 (TCP).

Remote Assistance and Windows Firewall

The Windows Firewall is configured with a group exception for Remote Assistance. This group exception has multiple properties that are grouped together as part of the RA exception. The RA exception properties will change depending on the network location of the computer (private, public, or domain). For example, the default RA exception when the computer is in a public location is stricter than when the computer is in a private location. In a public location (such as an airport), the RA exception is disabled by default and does not open ports for Universal Plug-and-Play (UPnP) and Simple Service Discovery Protocol (SSDP) traffic. In a private network (a home or work network, for example) the RA exception is enabled by default and uPnP and SSDP traffic is permitted.

Table 23-2 summarizes the state of the Remote Assistance firewall inbound exception for each type of network location. The RA exception has outbound properties as well; however, the Windows Firewall is not by default configured to enable outbound properties.

Table 23-2 Default State Of Remote Assistance Firewall Inbound Exception for Each Type of Network Location

Network location	State of RA exception	Default properties of the RA exception
Private (Home or Work)	Enabled by default	<ul style="list-style-type: none"> ■ Msra.exe application exception ■ uPnP enabled for communications with uPnP NATs ■ Edge traversal enabled to support Teredo
Public	Disabled by default— must be enabled by user with Admin credentials	<ul style="list-style-type: none"> ■ Msra.exe application exception ■ Edge traversal enabled to support Teredo

Table 23-2 Default State Of Remote Assistance Firewall Inbound Exception for Each Type of Network Location

Network location	State of RA exception	Default properties of the RA exception
Domain	Disabled by default—typically enabled by Group Policy	<ul style="list-style-type: none"> ■ Msra.exe application exception ■ RAServer.exe (the RA COM server) application exception ■ DCOM Port 135 ■ uPnP enabled for communications with uPnP NATs

In other Windows Firewall profiles, the default configuration of the Remote Assistance exception is as follows:

- **Private profile** The RA exception in the Windows Firewall is enabled by default when the computer location is set to “private.” It is configured for NAT traversal using Teredo by default so that users in a private networking environment (for example, the home environment) can solicit help from other users who may also be behind NATs. The private profile includes the appropriate exceptions needed to allow communication with uPnP NAT devices. If there is a uPnP NAT in this environment, Remote Assistance will attempt to use the uPnP for NAT traversal. Offer RA via DCOM is not configured in this profile.
- **Public profile** The RA exception is disabled by default and no inbound RA traffic is permitted. Windows Firewall is configured this way by default to better protect users in a public networking environment (such as a coffee shop or airport terminal). When the RA exception is enabled, NAT traversal using Teredo is enabled. However, traffic to uPnP devices is not enabled and Offer RA via DCOM is not enabled.
- **Domain Profile** The RA exception when the computer is in a domain environment is geared towards the Offer RA scenario. This exception is disabled by default and is typically enabled via Group Policy. Teredo is not enabled in this profile because corporate networks typically have a corporate firewall that blocks Teredo UDP traffic. However, uPnP is enabled so that uPnP NATs can be communicated with.

Remote Assistance and the Secure Desktop

When a User consents to having a Helper share control of her computer during a Remote Assistance session, the User has the option of allowing the Helper to respond to UAC prompts (Figure 23-1). Typically, User Account Control (UAC) prompts appear on the Secure Desktop (which is not remoted) and consequently the Helper cannot see or respond to Secure Desktop prompts. The Secure Desktop mode is the same mode that a user sees when she logs on to her computer or presses the Secure Attention Sequence (SAS) keystroke (Ctrl+Alt+Delete). UAC elevation prompts are displayed on the Secure Desktop instead of the user’s normal desktop to protect the user from unknowingly allowing malware to run with elevated privileges on her computer. The user must provide consent to a UAC prompt to return to her

normal desktop and continue working. This consent requires either clicking Continue (if the user is a local admin on her computer) or by entering local admin credentials (if she is a standard user on her computer).

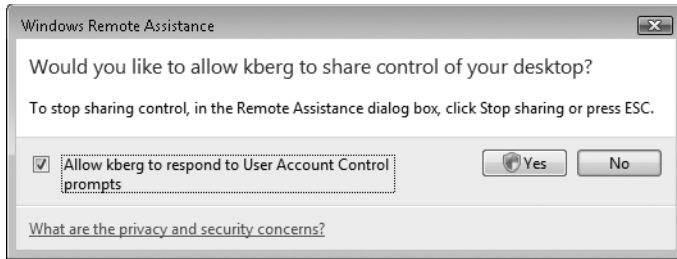


Figure 23-1 The User has the option of allowing the Helper to respond to UAC prompts when the RA session is in Control Sharing State.

It is important to understand that the Secure Desktop on the User's computer is not remoted to the Helper's computer. In other words, the Helper can only respond to UAC prompts on the User's computer using the User's own credentials. This means that if the User is a standard user on her computer while the Helper is a local administrator on the User's computer, the Helper can only have administrative privileges on the User's computer if the User can first supply those credentials.

Enforcing this limitation is essential to ensure the security of Vista desktops. The reason behind this design decision is that if RA was architected to allow the Helper to remotely elevate the User's privileges, the User would be able to terminate the RA session and thus steal local admin credentials from the Helper.

Remote Assistance Logging

Remote Assistance can generate a session log of RA-associated activity. Session logging is enabled by default and consists of time-stamped records that identify RA-related activities on each computer. Session logs only contain information about activities that specifically relate to RA functionality, such as who initiated the session, whether consent was given to a request for shared control, and so on.

Session logs do not contain information on actual tasks that the User or Helper performed during a session. For example, if the Helper is given Shared Control privileges, starts an Admin command prompt, and performs steps to reconfigure the TCP/IP configuration on the User's computer during an RA session, the session logs will not contain a record of this action.

Session logs do include any chat activity performed during an RA session. The log generated during a session is also displayed within the chat window so that both the User and the Helper can see what is being logged during the session. Session logs also include any file

transfer activity that occurs during the session, and also record when the session has been paused.

Purpose of RA Session Logging Session logs for RA are mainly intended for enterprises that are required to maintain records of system and user activity for record-keeping purposes. They are not intended as a way to record every action performed by Help Desk personnel when troubleshooting problems with users' computers. A typical environment in which session logging might be required would be in a banking environment, where a financial institution is required by law to maintain records of who accessed a computer and at what time.

Because the ACLs on these session logs grant the User full control over logs stored on her own computer, by default session logs are generated on both the User's computer and Helper's computer so that the Helper can protect and archive them from tampering. The logs created on each side of an RA session are similar but not identical. This is because session logs are generated from the perspective of the computer involved—whether the User's computer or the Helper's computer—and therefore complement each other instead of being identical.

In an enterprise environment, Group Policy can be used to enable or disable session logging. If session logging is not configured using Group Policy, both the User and Helper are free to disable session logging on their own computers. For more information, see the section titled "Managing Remote Assistance Using Group Policy" in this chapter.

Session Log Path and Naming Convention Session logs are XML-formatted documents so that they can be easily integrated into other data sets—for example, by importing them into a database managed by Microsoft SQL Server 2005. All session logs are stored under each user's Documents folder within the following path:

Users*user_name*\Documents\Remote Assistance Logs

A unique session log file is created for each RA session on the computer. Log files stored within this folder are formatted using XML and are named using the convention *YYYYMMD-DHHMMSS.xml*, where the time format is 24-hour. For example, a session log created at 3:45:20 p.m. on August 13, 2006, would be named 20060813154520.xml.

The XML content of a typical session log looks like this:

```
<?xml version="1.0" ?>
<SESSION>
  <INVITATION_OPENED TIME="3:24 PM" DATE="Wednesday, August 09, 2006" EVENT="A Remote Assistance invitation has been opened." />
  <INCOMING_IP_ADDRESS TIME="3:26 PM" DATE="Wednesday, August 09, 2006">fe80::2856:e5b0:fc18:143b%10</INCOMING_IP_ADDRESS>
  <CONNECTION_ESTABLISHED TIME="3:26 PM" DATE="Wednesday, August 09, 2006" EVENT="A Remote Assistance connection has been established.">jdow</CONNECTION_ESTABLISHED>
  <EXPERT_REQUEST_CONTROL TIME="3:27 PM" DATE="Wednesday, August 09, 2006" EVENT="jdow has requested to share control of the computer." />
  <EXPERT_GRANTED_CONTROL TIME="3:27 PM" DATE="Wednesday, August 09, 2006" EVENT="jdow has been granted permission to share control of the computer." />
```

```
<EXPERT_CONTROL_STARTED TIME="3:27 PM" DATE="Wednesday, August 09, 2006" EVENT="jdow is sharing control of the computer." />
<EXPERT_CONTROL_ENDED TIME="3:27 PM" DATE="Wednesday, August 09, 2006" EVENT="jdow is not sharing control of the computer." />
<CHAT_MESSAGE TIME="3:30 PM" DATE="Wednesday, August 09, 2006">jdow: test</CHAT_MESSAGE>
<CHAT_MESSAGE TIME="3:30 PM" DATE="Wednesday, August 09, 2006">jchen: ok</CHAT_MESSAGE>
<CONNECTION_ENDED TIME="3:30 PM" DATE="Wednesday, August 09, 2006" EVENT="The Remote Assistance connection has ended." />
<INVITATION_CLOSED TIME="3:30 PM" DATE="Wednesday, August 09, 2006" EVENT="A Remote Assistance invitation has been closed." />
</SESSION>
```

Using Remote Assistance in the Enterprise

The main Remote Assistance scenario within a corporate networking environment is supporting desktop computers that are on the corporate network and joined to a domain. Users' machines must be configured appropriately before they can be offered RA. This is done via Group Policy, as explained in the section of this chapter titled "Managing Remote Assistance Using Group Policy." Additionally, the Remote Assistance exception in the Windows Firewall must be enabled. For more information, see the section titled "Remote Assistance and Windows Firewall" earlier in this chapter .

Because most corporate networks have a perimeter firewall blocking access from outside the internal network, supporting remote users who are connecting from outside the corporate network can be more difficult. However, most enterprises now use virtual private network (VPN) technologies to allow remote users to connect to their corporate networks over the Internet, and this kind of scenario generally poses no problem to RA functionality.

Using Remote Assistance in the Corporate Help Desk Environment

The standard approach to using Remote Assistance in an enterprise environment is for Help Desk personnel to offer Remote Assistance to users who telephone in to request assistance. A typical scenario might be as follows:

1. User Jane Dow (the User) is having problems configuring an application on her computer. She phones Help Desk, explains her problem briefly, and asks for help.
2. A Help Desk person named Jacky Chen (the Helper) asks Jane for the fully qualified name or IP address of her computer. She responds with the information, which she can get from computer properties or by running `ipconfig`.
3. Jacky starts Remote Assistance on his computer and uses the Offer RA feature to offer help to Jane. This causes a dialog to appear on Jane's computer, asking her if she would like to allow Jacky to connect to her computer.
4. Jane accepts the offer, and at this point Jane's desktop may temporarily change to conserve network bandwidth used by the Remote Assistance session. The Remote Assistance window that opens on Jane's screen tells her that she is being helped by Jacky.

5. At this point, Jacky can see Jane's screen but he can't control it. Jane then explains the problem she is having, either by using the Chat feature of Remote Assistance, or more likely over the telephone. Jacky asks Jane to perform a series of steps to correct the problem and watches her screen in his own Remote Assistance window as she does this.
6. If the instructions Jacky provides are too complex or if time is limited, Jacky can ask Jane if he can share control of her computer. If Jane agrees, Jacky clicks the Request Control button at the top of his Remote Assistance window. A dialog appears on Jane's desktop asking her if she wants to allow Jacky to share control of her desktop. Jane accepts the prompt, and also selects the option to allow Jacky to respond to User Account Control (UAC) prompts on Jane's computer.
7. Jacky is now connected to Jane's computer using Jane's credentials, and he can both view her screen and interact with it using his own mouse and keyboard. Jacky then proceeds to perform the steps needed to resolve the problem, either correcting the issue or demonstrating to Jane how to fix the problem if it occurs again in the future. If at any time Jane wants to force Jacky to relinquish control of her computer, she can click the Stop Sharing button, the Disconnect button, or press the Panic key (Esc).



Note Offer RA needs preconfiguration of the User's machine via Group Policy. See the section titled "Managing Remote Assistance Using Group Policy" later in this chapter for more information.

Other Possible Remote Assistance Usage Scenarios

Other types of Remote Assistance scenarios are also possible for businesses ranging from large enterprises to Small Office/Home Office (SOHO) environments. Examples of possible usage scenarios include:

- A user who is having a problem with configuring an application on her computer can phone Help Desk for assistance. A support person can then use Offer RA to connect to the user's computer, ask for control of her screen, and show the user how to configure her application. This scenario is the standard one for enterprise Help Desk environments and is described in more detail in the section titled "Using Remote Assistance in the Corporate Help Desk Environment" later in this chapter.
- A user who is having trouble installing a printer sends an RA invitation to Help Desk using Windows Mail. A support person who is monitoring the Help Desk e-mail alias reads the message, opens the attached invitation file, and connects to the user's computer. The support person asks for control of the user's computer and walks him through the steps of installing the printer.
- A user is on the road and is connected to the internal corporate network using a VPN connection over the Internet. The user is having problems configuring Windows Mail on her computer, so she opens Windows Messenger and notices that someone she

knows in Corporate Support is currently online. She sends an RA invitation to the support person using Windows Messenger, who responds to the invitation, asks for control, and shows the user how to configure Windows Mail.

The preceding list is not intended to be complete—other corporate support scenarios using RA are possible. Generally speaking, however, corporate environments will use Offer RA to provide assistance to users who phone Help Desk when they have problems. Some enterprises may also allow users to submit RA invitations either via e-mail or by saving invitation files to network shares that are monitored by support personnel. Others may use instant messaging applications that support Remote Assistance within the corpnet.



Note Helpers can have multiple RA sessions open simultaneously—one session for each User they are supporting. However, Users can have only one RA session in the Waiting For Connect state. The invitation that was created could be sent to multiple recipients—any of whom may connect. All subsequent connect attempts will be blocked until the first helper disconnects, after which another helper may connect. If the user disconnects the session, the RA application terminates and no further connections will be allowed.

Interoperability with Remote Assistance in Windows XP

Remote Assistance in Vista is backward-compatible with Remote Assistance in Windows XP, with the following limitations:

- Offer RA from Vista to XP is supported, but Offer RA from XP to Vista is not supported. This means that enterprises who want to implement Offer RA as a support solution for their Help Desk departments should ensure that computers used by support personnel who will help users running Vista are themselves running Vista. (and not XP).
- NAT traversal using Teredo and IPv6 is supported on Vista to Vista RA only, and not on Vista to XP.
- Voice support for RA in XP is not supported by RA in Vista, and any attempt by a User on an XP computer to use this feature during an RA session with a Helper on a Vista computer will cause a notification message regarding this limitation to appear.
- The MAILTO method of soliciting assistance that is supported by RA in XP is not supported by RA in Vista.
- Windows Messenger (which shipped with XP) does not ship with Vista. Users of RA with Windows Messenger in XP will need to migrate to an IM vendor that supports Vista and Remote Assistance. Windows Live Messenger currently supports XP, Vista, and Remote Assistance.
- Offer RA via Messenger is a new feature in Vista and is not available in Windows XP.

Implementing and Managing Remote Assistance

Remote Assistance is a powerful and flexible feature that can be used in many different ways to support users within large enterprises, medium-sized businesses, and SOHO environments. This section outlines how to initiate Remote Assistance sessions from both the UI and the command line. The section also demonstrates how to use Remote Assistance in an enterprise Help Desk environment involving two common scenarios:

- Helper offers RA to User who has telephoned Help Desk with a problem.
- User creates an RA invitation and saves it on a network share that is monitored by Help Desk personnel.

For information on other scenarios for implementing Remote Assistance, including sending invitations with Windows Mail and Windows Messenger, search for the topic “Remote Assistance” within Windows Help and Support.

Initiating Remote Assistance Sessions

Remote Assistance sessions can be initiated either from the user interface or the command line. A significant usability enhancement, from the perspective of support personnel, is that Offer RA is no longer buried within Help And Support as it was in Windows XP, but is instead easily accessible now from the GUI.

Initiating Remote Assistance From the GUI

Initiating Remote Assistance sessions from the GUI can be done using any of several available methods:

- From the Start menu, click Start, then All Programs, then Maintenance, and then Windows Remote Assistance. This launches the RA app.
- Click Start, then Help And Support, and then under the Ask Someone heading click Windows Remote Assistance.
- Click Start, type **assistance**, and when Windows Remote Assistance appears in the Programs list, click it.

Any of these methods will open the initial Remote Assistance screen, shown in Figure 23-2.

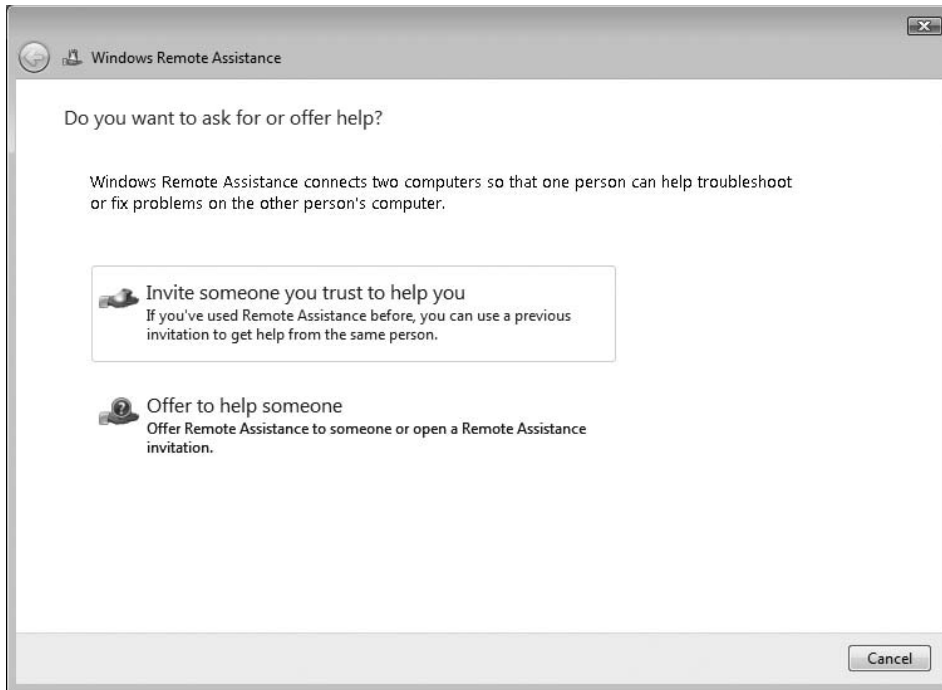


Figure 23-2 The initial screen of Windows Remote Assistance.

Initiating Remote Assistance From the Command Line

Remote Assistance in Vista is implemented as a standalone executable called `msra.exe`. You can initiate RA sessions directly from the command line or by using scripts. The syntax and usage for this command is explained in Table 23-3.

Table 23-3 Syntax and Usage for Command-Line Remote Assistance (`msra.exe`)

Option	Description
<code>/novice</code>	Launches Remote Assistance as Novice in Solicited RA mode and presents the user with the choice of either sending an RA ticket using a SMAPI-enabled e-mail application such as Windows Mail or by saving the invitation as a file. Once this choice has been made, Windows Remote Assistance opens on the Novice's computer in the Waiting For Connect state.
<code>/expert</code>	Launches Remote Assistance in the Helper mode and presents the user with the choice of either specifying the location of an RA ticket to open or specifying the Novice's computer name or address (Offer RA). The computer name can be either a host name (if the Novice is on the local subnet) or a fully qualified name (DNS name), and the address can be either an IPv4 address or an IPv6 address. Unsolicited RA without an invitation requires preconfiguration of the remote machine being helped.

Table 23-3 Syntax and Usage for Command-Line Remote Assistance (msra.exe)

Option	Description
<i>/offerRA computer</i>	Launches Remote Assistance as Helper in Unsolicited (Offer) RA mode and uses DCOM to remotely open Remote Assistance on the Novice's computer and then connect to the Novice's computer to initiate an RA session. The Novice's computer can be specified using either its computer name or address. The computer name can be either a host name (if the Novice is on the local subnet) or a fully qualified name (DNS name), and the address can be either an IPv4 address or an IPv6 address. This method is demonstrated in more detail in the section titled "Scenario 1: Offering Remote Assistance to Novices" later in this chapter.
<i>/email password</i>	Launches Remote Assistance as Novice in Solicited RA mode and creates a password-protected RA ticket that is attached to a new RA invitation message opened by the default SMTP-enabled e-mail client (which by default is Windows Mail). The password must be six characters or more and must be relayed separately to the Helper. The e-mail client application launches a window with the invitation file attached. The User must enter the e-mail address of the Helper in the To field to send the message to the Helper.
<i>/saveasfile path password</i>	Launches Remote Assistance as Novice in Solicited RA mode and creates a password-protected RA ticket that is saved at the path specified. The path may be either a local folder or network share and the User must have appropriate permissions on the destination folder to create the file. The path must include a file name for the ticket. (The .MsRcIncident file extension will be automatically added to the file name.) The password must be six characters or more. Use of this method is demonstrated in more detail in the section titled "Scenario 2: Soliciting Remote Assistance by Creating RA Tickets and Saving Them on Monitored Network Shares" later in this chapter.
<i>/openfile path password</i>	Launches Remote Assistance as Helper in Solicited RA mode and opens a previously created RA ticket that was saved within the path specified. The path may be either a local folder or network share and the Helper must have appropriate permissions on the destination folder to open the file. The path must include the file name of a valid ticket that has the .MsRcIncident file extension. The password must be the same password that was used by the User to secure the ticket when it was created.



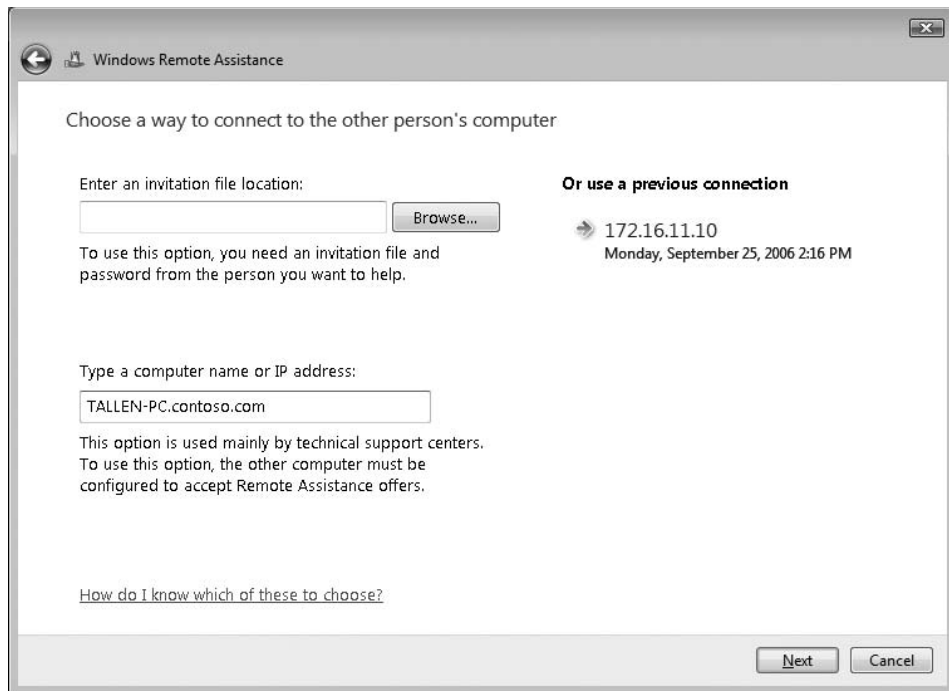
Note There is no support for Windows Managing Instrumentation (WMI) scripting of msra.exe.

Scenario 1: Offering Remote Assistance Using DCOM

Before you can offer Remote Assistance to other users, your user account must be authorized as a Helper on the user's computer. You can use Group Policy to do this in an enterprise environment. (See the section titled "Managing Remote Assistance Using Group Policy" in this chapter for information on how to do this.)

Once a support person (or group of individuals) has been configured as a Helper for all Vista computers in a domain or OU, the support person can offer RA to users of those computers when they need assistance. For this scenario, let's say that Tony Allen (tallen@contoso.com) is a Vista user who needs assistance with an issue on his computer. Tony telephones the Help Desk department and the call is taken by Karen Berg (kberg@contoso.com) who asks Tony for the name or IP address of his computer. Tony provides Karen with his fully qualified computer name (TALLEN-PC.contoso.com) or IP address, and Karen then offers assistance to Tony by following these steps:

1. Start Remote Assistance using any of the methods described previously.
2. Click Offer To Help Someone.
3. Enter **TALLEN-PC.contoso.com** in the field labeled Type A Computer Name Or IP Address.



4. Click Next.

At this point a dialog box will appear on Tony's computer asking if he would like to allow Karen to connect to his computer and view his desktop. Tony has two minutes to respond to this dialog before the offer times out and the dialog box disappears, which will cause a message saying "The person you are trying to help isn't responding" to appear on Karen's computer. If the offer to Tony times out, Karen can resubmit the offer by selecting it from the list of previous connections that are displayed in her RA application (Figure 23-3). If Tony accepts

the offer (grants consent), the Remote Assistance session begins and Tony's desktop will be viewable by Karen in a Remote Assistance application window.

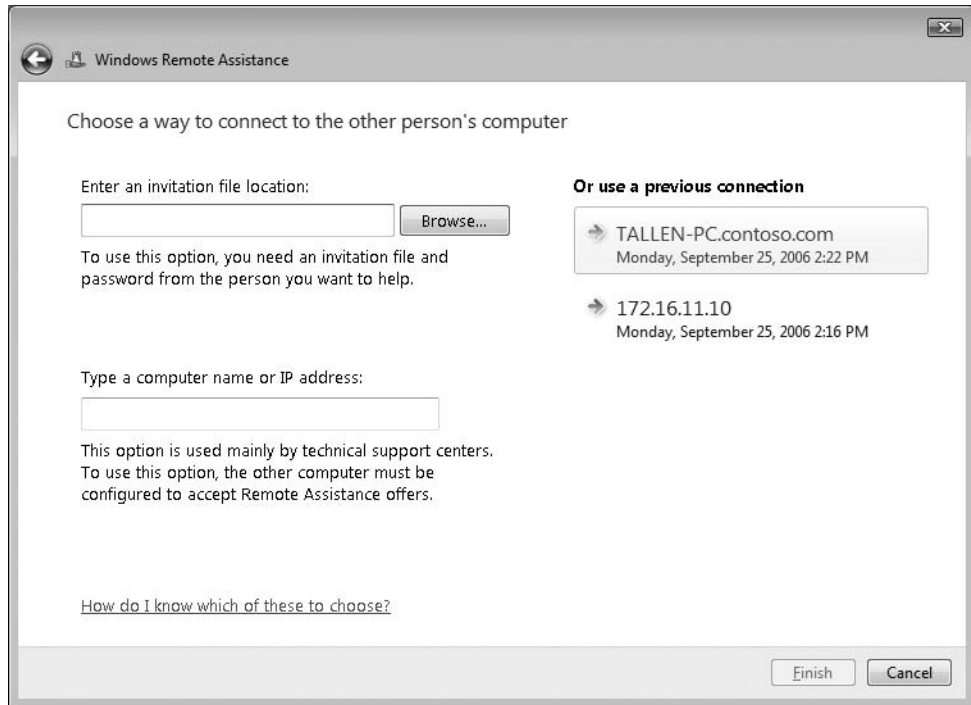


Figure 23-3 Recent RA invitations and offers listed under Or Use A Previous Connection can be reused.

At this point the desktop properties of Tony's desktop may change (based on configurable settings) to optimize the network bandwidth used by RA for screen updates on Karen's computer. Karen can now request control from Tony, send files to Tony or receive files from him, chat with Tony, or disconnect the session. Tony can send and receive files, chat, or pause or disconnect the session.



Note If you are a User and a Helper has shared control of your computer, you can immediately terminate shared control and return the session to Screen Sharing state by pressing the Panic key (Esc).

Scenario 2: Soliciting Remote Assistance by Creating RA Tickets and Saving Them on Monitored Network Shares

Another way that you can use Remote Assistance in an enterprise environment is by having users create invitation files and save them on a network share that is monitored by Help Desk personnel. This way, when Help Desk determines that a new ticket has been uploaded to the

share, a support person can call the user on the telephone to obtain the password for the ticket and then use the ticket to establish an RA session with the user who needs help.

To make procedure easier, administrators can first deploy a script on users' desktops that uses command-line Remote Assistance (msra.exe) to create the invitation file and save it on the network share. For example, let's say that users' invitation files should be uploaded to \\FILESRV3.contoso.com\Support\IncomingTickets, a folder in the Support share on the file server named FILESRV3. The following script, named SubmitTicket.vbs, could be deployed on each user's desktop to accomplish this task:

```
dim strPassword
dim strUser
dim strTicketName

strPassword = InputBox("Enter a password for your ticket")
Set wshShell = wscript.CreateObject("wscript.Shell")
strUser = wshShell.ExpandEnvironmentStrings("%username%")
strTicketName = strUser & "-" & Year(Now) & "-" & Month(Now) & "-" & Day(Now) & _
    "-" & Hour(Now) & "-" & Minute(Now) & "-" & Second(Now)
strRA = "msra.exe /saveasfile \\FILESRV3\Support\IncomingTickets\" & _
    strTicketName & " " & strPassword
wshShell.Run strRA
```

When the user double-clicks on this script to run it, an Input box appears asking the user to provide a password to be used to secure the invitation. After the user supplies a password, a new RA ticket is created and saved in the target folder on the file server. The name of the ticket is unique and consists of the user's name followed by the date and time, such as tallen-YYYY-MM-DD-HH-MM-SS.MsRcIncident. Once the support person monitoring the share has obtained the ticket's password using an OOB method such as a telephone call, the support person opens the ticket. After the User grants consent, the RA connection is established.

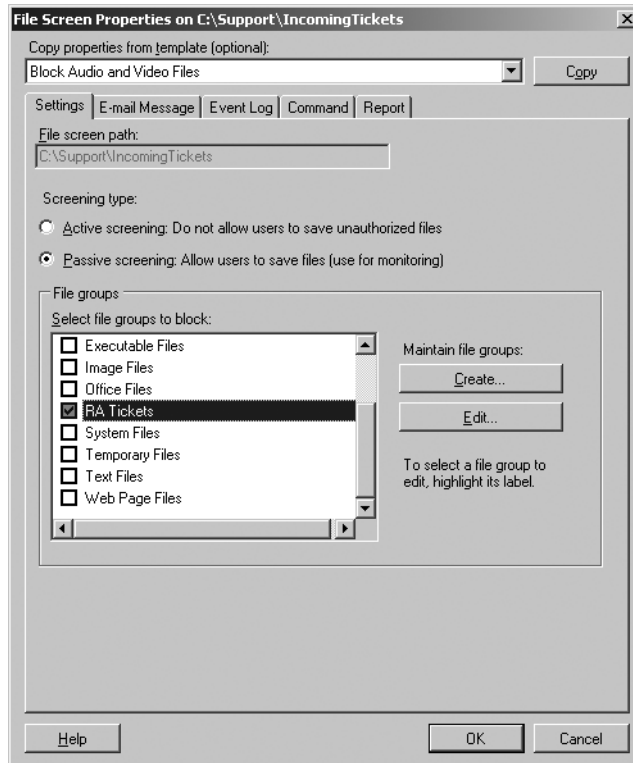
To monitor the IncomingTickets folder in the network share, Help Desk personnel can use the file-screening capabilities of Windows Server 2003 R2 file servers. To do this, you can create a passive file screen that monitors the folder and sends an e-mail alert to a Help Desk alias whenever a new ticket is uploaded to the folder. The steps for doing this are:

1. Install or upgrade the File Server role on the Windows Server 2003 R2 computer where the Support folder is located.
2. Start the File Server Resource Manager console from Administrative Tools, right-click the root node, and select Configure Options.
3. Specify the DNS name of the IP address of an SMTP host that can be used to forward alert e-mails generated by the file screen you will create.
4. Click OK to close File Server Resource Manager Options, and expand the console tree to select File Screens under File Screening Management.
5. Select the option Create File Screen in the Action pane.

6. Click Browse to select the Incoming folder for the File Screen Path.
7. Select the option labeled Define Custom File Screen Properties and click Custom Properties.
8. Choose the option for Passive Screening so that uploaded tickets will only be monitored and not blocked by the screen.
9. Click Create to create a new file group called RA Tickets and use the Add button to add files of type *MsRcIncident to the group.



- Click OK to return to the properties sheet for the new file screen, and select the check box for the RA Tickets file group you just created.



- Click the Email tab and specify a support alias (such as support@contoso.com) that will be notified whenever a new ticket is uploaded to the folder. Configure a suitable subject and body for the message.
- Click Create to create the new file screen and then choose the option to save the screen without creating a template.
- Test the new file screen by opening a command prompt on a user's computer and typing **msra.exe /saveasfile path password** where *path* is the UNC path to the Incoming folder within the Support share on the file server, and *password* is any password of six or more characters that you specify.

For more information on how to implement file screening in Windows Server 2003 R2, see the topic "Screening Files" on the Microsoft Windows Server TechCenter at <http://technet2.microsoft.com/WindowsServer/en/library/de035087-2e9c-4b98-af4c-07d2d690ad6c1033.msp>.

Managing Remote Assistance Using Group Policy

In an enterprise environment, Remote Assistance can be managed using Group Policy. The policy settings for Remote Assistance are all machine settings and are found in the following policy location:

Computer Configuration\Administrative Templates\System\Remote Assistance

When these policy settings are written to the registry on targeted computers, they are stored under the following registry key:

HKLM\SOFTWARE\Policies\Microsoft\WindowsNT\Terminal Services

Remote Assistance policy settings are summarized in Table 23-4.

Table 23-4 Group Policy Settings for Remote Assistance

Policy	Description
Solicited Remote Assistance	<p>Enabling this policy allows users of targeted computers to use Solicited RA to request assistance using e-mail, file transfer, or instant messaging. Disabling this policy prevents users from using Solicited RA. The default setting is Not Configured, which allows users to change their Remote Assistance settings using the Remote tab of the System CPL in Control Panel.</p> <p>If the policy is Enabled, you can further configure whether Helpers can be prevented from sharing control of the User's computer, the maximum ticket lifetime, and the method used for sending invitations my e-mail. (Windows Vista does not support the MAILTO method—select SMAPI instead if the targeted computers are running Windows Vista.) Ticket lifetime applies only to RA invitations sent by e-mail or file transfer. The default ticket lifetime when Group Policy is not being used is 6 hours.</p> <p>If this policy is Enabled, you must also enable the Remote Assistance exception in Windows Firewall to allow Solicited RA to work.</p> <p>In an unmanaged environment, this setting can also be configured using the Remote tab of the System CPL in Control Panel.</p> <p>This policy is also supported on Windows XP Professional and Windows Server 2003.</p>
Offer Remote Assistance	<p>Enabling this policy allows designated Helpers to use Offer RA to offer assistance to users of targeted computers. Disabling this policy or leaving it Not Configured prevents Offer RA from being used to offer assistance to users of targeted computers.</p> <p>If the policy is Enabled, you can further configure whether Helpers can view or control the Users' computers, and you must specify a list of Helpers who are allowed to Offer RA to the users of the targeted computers. Helpers can be either users or groups and must be specified in the form <i>domain_name\username</i> or <i>domain_name\groupname</i>.</p> <p>If this policy is Enabled, you must also enable the Remote Assistance exception in Windows Firewall to allow Offer RA to work.</p> <p>This policy is also supported on Windows XP Professional and Windows Server 2003. See the Explain tab of this policy setting for more details.</p>

Table 23-4 Group Policy Settings for Remote Assistance

Policy	Description
Allow Only Vista Or Later Connections	<p>The default Vista invitation file includes a XP-specific node for backward compatibility. This node is not encrypted and allows XP machines to connect to the Vista machine that created the ticket. Enabling this policy causes all RA invitations generated by users of targeted computers to <i>not</i> include the XP node, thereby providing an additional level of security and privacy. Disabling this policy or leaving it Not Configured leaves information such as IP address and port number unencrypted in RA invitations. This policy setting only applies to RA invitations sent using e-mail or file transfer, and has no effect on using instant messaging to solicit assistance or on using Offer RA to offer assistance.</p> <p>In an unmanaged environment, this setting can also be configured by clicking Advanced from the Remote tab of the System Properties dialog.</p> <p>This policy is supported only on Windows Vista and later platforms.</p>
Customize Warning Messages	<p>Enabling this policy causes a specified warning to be displayed on targeted computers when a Helper wants to enter Screen Sharing State or Control Sharing State during an RA session. Disabling this policy or leaving it Not Configured causes the default warning to be displayed in each instance.</p> <p>If the policy is Enabled, you can further specify the warning message to be displayed in each instance.</p> <p>This policy is supported only on Windows Vista and later platforms.</p>
Turn On Session Logging	<p>Enabling this policy causes RA session activity to be logged on the targeted computers. For more information, see the section titled “Remote Assistance Logging” earlier in this chapter. Disabling this policy causes RA auditing to be disabled on the targeted computers. The default setting is Not Configured, in which case RA auditing is automatically turned on.</p> <p>This policy is supported only on Windows Vista and later platforms.</p>
Turn On Bandwidth Optimization	<p>Enabling this policy causes the specified level of bandwidth optimization to be used to enhance the RA experience over low-bandwidth network connections. Disabling this policy or leaving it Not Configured allows the system defaults to be used.</p> <p>If the policy is Enabled, you must specify the level of bandwidth optimization you want to use from the following options:</p> <ul style="list-style-type: none"> ■ No Optimization ■ No Full Window Drag ■ Turn Off Background ■ Full Optimization (Use 8-Bit Color) <p>If No Optimization is selected, the User’s computer will use the Windows Basic theme with full background, and during a shared control session the Helper will be able to drag full windows across the User’s screen. Additional optimization turns off effects to allow a more responsive experience for the Helper.</p> <p>This policy is supported only on Windows Vista and later platforms.</p>



Note In Windows XP, members of the Domain Admins group were implicitly granted Helper privileges even if they were not added to the Helpers list of the Offer Remote Assistance policy setting. This is no longer the case in Vista, where the Domain Admins group must now be explicitly added to the Helpers list to grant them Helper privileges for Offer RA.

Configuring Remote Assistance in Unmanaged Environments

Users of unmanaged computers can enable and configure Remote Assistance using the Remote tab of the System CPL in Control Panel (Figure 23-4). Enabling or disabling Remote Assistance and configuring its settings this way requires local administrator credentials on the computer, so a UAC prompt will appear when the user tries to do this.

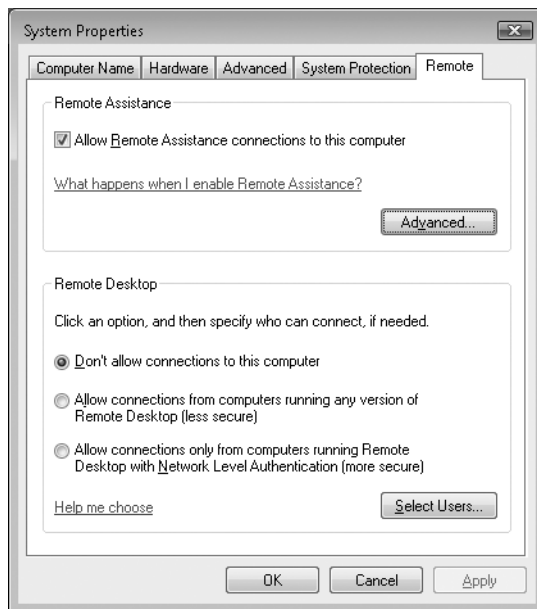


Figure 23-4 Configuring RA from the Remote tab of the System CPL in Control Panel.

Note that settings changes made this way will affect all users on the system. The per-machine registry settings for Remote Assistance are found under the following key:

HKLM\SYSTEM\CurrentControlSet\Control\Remote Assistance

In managed environments, when the following Group Policy setting is Enabled, the Control Panel settings for configuring Remote Assistance become unavailable (are grayed out).

Computer Configuration\Administrative Templates\System\Remote Assistance\Solicited Remote Assistance



Note Group Policy settings always prevail over locally configured settings when they overlap.

Additional Registry Settings for Configuring Remote Assistance

Additional behavior for Remote Assistance can be configured by modifying certain registry settings. Specifically, per-user registry settings for Remote Assistance are found under the following key:

HKCU\Software\Microsoft\Remote Assistance

These settings are changeable when in the Waiting To Connect mode or when in the connected mode from the Settings button.



Caution If Group Policy is used to manage Remote Assistance settings and any configured policy settings overlap these registry settings, the policy settings prevail.

Direct from the Source: Troubleshooting Remote Assistance

The following are some tips for troubleshooting Remote Assistance in Windows Vista:

1. *When I attempt to create an invitation with e-mail or save-to-file, I see a warning message that says that the Windows Firewall is currently blocking Remote Assistance.*

The Remote Assistance firewall exception will change depending upon your network location (private, public, or domain). If you are at home, your network location type should be set to “private” since this enables the Remote Assistance firewall exception automatically. If your network location is set to “public,” the Remote Assistance firewall exception is not enabled automatically for security purposes. It will need to be enabled by an Administrator.

If you are connected to a managed network (for example when you are within a corporate domain) the network location is categorized as “domain” and the Remote Assistance exception is not enabled automatically. It is expected to be configured by Group Policy by your System Administrator.

2. *I cannot use RA to connect from my home computer to a work computer.*

RA uses Teredo (IPv6) to traverse NATs. However, Teredo cannot be used to traverse corporate edge firewalls that provide NAT for intranet clients and blocks dynamic ports or outbound UDP traffic. Since you do not have a globally reachable IPv4 address within the corpnet, RA cannot make a connection to you from outside the corpnet.

3. *If I disable the Windows Firewall I cannot make an RA connection in certain cases. This is counter-intuitive since I expect connectivity to be less restrictive with the firewall disabled.*

In Vista, the Windows Firewall is IPv6-aware. The RA exception in the Windows Firewall enables Teredo for edge traversal. If the Windows Firewall is disabled, the ability to use Teredo for NAT traversal is also disabled. The Windows Firewall must be running with the RA exception enabled for RA to be able to traverse NATs using Teredo.

4. *I cannot use RA to connect from my work to my home computer.*

Your corporate firewall may be configured to block outbound peer-to-peer connections. In a managed environment (domain-joined computers), which is typically found in a corporate network, the RA exception does not enable Teredo (edge traversal) since corporate firewalls typically block outbound UDP traffic. NAT traversal using Teredo is disabled by default in this scenario. If the person you are trying to help is behind a UPnP NAT or directly connected to the Internet, you should be able to make a connection. Check with your network administrator to see if outbound peer-to-peer connections through the corporate firewall can be enabled.

5. *When I move my laptop (or change my home network location) from a “private” to “public” location, I am not able to connect to certain computers.*

If you have a laptop that moves between work and home, the properties of the RA firewall exception in the Windows Firewall will change depending on whether your network location is classified as “private,” “public,” or “domain”. In a private location, the RA exception is enabled by default, and if you are using a UPnP NAT, the RA exception will allow communications with the UPnP NAT to enable RA connections that make use of UPnP. In a public network the RA exception is not enabled by default and will need to be enabled using Administrator credentials. In addition, the default “public” profile does not permit UPnP communication for security purposes, thereby restricting RA connectivity in certain cases.

6. *I am on a low bandwidth connection and the person helping me is experiencing slow screen refreshes.*

Set the Bandwidth Usage under Settings to “Low” to reduce the bandwidth used during a Remote Assistance connection. Keep in mind that display quality decreases as bandwidth usage is limited.

7. *Why can't I connect to XP machines that are behind a NAT as easily as I can connect to Vista machines?*

RA in XP does not support Teredo for NAT traversal. Consequently, a Vista-to-XP RA connection attempt may fail in cases where both computers are behind non-UPnP NATs.

8. *How does RA make a connection?*

When the RA invitation is created, the User's computer will set itself as a listener on all of its IP addresses (IPv4 and IPv6), including its Teredo address. All these listeners are waiting for a connection from the Helper's computer. The address and port information associated with these different listeners is relayed to the Helper's computer using the RA invitation (which gets transported by Messenger when Messenger is used to launch RA). The Helper's computer then tries to connect concurrently on all the address/port pairs in the invitation. The first successful connection that is made is used for the RA session and the rest of the connection attempts are terminated.

9. *How do I troubleshoot a connection failure between two home-based Vista machines that are behind NATs?*

Refer to the RA Connectivity information in Tables 23-5 and 23-6 to verify that the network configuration you have is supported for RA connectivity. Then do the following:

- ❑ Confirm that the Windows Firewall on the computer of the person that is being helped is running and configured for RA.
 - The Windows Firewall is IPv6 compatible and must be running to enable NAT traversal using Teredo.
 - The network location of the computer must be set to "private" or "public" since Teredo is not enabled in "domain" or "managed" settings.
 - The Remote Assistance exception in the firewall must be enabled to allow RA connections.
- ❑ Check that there is no edge firewall between User and Helper since it may block peer-to-peer applications like RA.
- ❑ Confirm that the User and Helper are not behind a symmetric NAT and that Teredo is able to get to the "qualified" state on both machines. To determine this, do the following:
 1. First, initiate Teredo by forcing RA into the "waiting to connect" state. You can do this by typing `msra.exe /saveasfile myinvitation mypassword` at a command prompt.
 2. Then, check to see if Teredo can be activated on both machines and goes into the "qualified" state. Open an elevated command prompt window and type `netsh interface teredo show state` at the command prompt. The output should show Teredo in the "qualified" state. If Teredo does not go to the "qualified" state on both machines, an RA

connection may not be possible between these two computers. Teredo will not go into the qualified state if one of these 2 conditions exists:

- A global Teredo server could not be reached at `teredo.ipv6.microsoft.com`.
- The computer is behind a symmetric NAT. To verify this, look at the output of `netsh interface teredo show state` and check the output on the “NAT :” line which specifies NAT type.

10. *When I am helping someone who is a Standard user, I cannot run a program that needs Administrator privileges even though I have Administrator privileges to the user’s computer.*

RA allows a User to share control of their computer with a remote Helper. If the User is a Standard user, the remote Helper is given the same privileges as the Standard user. If the Helper attempts to launch a program that requires Administrator credentials, these credentials must be entered *locally* (on the Secure Desktop) by the User and cannot be entered remotely by Helper. This is required in order to prevent a security loophole where Admin programs launched by a remote Helper could be hijacked by the local User by simply terminating the RA session.

Table 23-5 RA Connectivity for Expert on Windows XP

		Expert on XP			
		Directly Connected	Behind UPnP NAT	Behind non UPnP NAT	Behind corporate Edge Firewall**
Novice on XP	Directly Connected	Yes	Yes	Yes	Yes
	Behind UPnP NAT	Yes	Yes	Yes	Yes
	Behind non UPnP NAT	Yes using Msgr Only	Yes using Msgr Only	No	No
	Behind corporate Edge Firewall**	Yes using Msgr Only	Yes using Msgr Only	No	Yes - if both are behind same firewall No - if both are behind different firewalls

Table 23-5 RA Connectivity for Expert on Windows XP

		Expert on XP			
		Directly Connected	Behind UPnP NAT	Behind non UPnP NAT	Behind corporate Edge Firewall**
Novice on Vista	Directly Connected	Yes	Yes	Yes	Yes
	Behind UPnP NAT	Yes	Yes	Yes	Yes
	Behind non UPnP NAT	Yes using Msgr Only	Yes using Msgr Only	No	No
	Behind corporate Edge Firewall**	Yes using Msgr Only	Yes using Msgr Only	No	Yes - if both are behind same firewall No - if both are behind different firewalls

Table 23-6 RA Connectivity for Expert on Windows Vista

		Expert on Vista			
		Directly Connected	Behind UPnP NAT	Behind non UPnP NAT	Behind corporate Edge Firewall**
Novice on XP	Directly Connected	Yes	Yes	Yes	Yes
	Behind UPnP NAT	Yes	Yes	Yes	Yes
	Behind non UPnP NAT	Yes using Msgr Only	Yes using Msgr Only	No	No
	Behind corporate Edge Firewall**	Yes using Msgr Only	Yes using Msgr Only	No	Yes - if both are behind same firewall No - if both are behind different firewalls

Table 23-6 RA Connectivity for Expert on Windows Vista

		Expert on Vista			
		Directly Connected	Behind UPnP NAT	Behind non UPnP NAT	Behind corporate Edge Firewall**
Novice on Vista	Directly Connected	Yes	Yes	Yes	Yes
	Behind UPnP NAT	Yes	Yes	Yes	Yes
	Behind non UPnP NAT	Yes using Teredo*	Yes using Teredo*	Yes using Teredo*	None
	Behind corporate Edge Firewall**	No	No	No	Yes - if both are behind same fire-wall No - if both are behind different firewalls

* Teredo connectivity is not available if either computer is behind a "symmetric NAT"

** Edge Firewall must permit outbound connection (e.g. using the Microsoft ISA Firewall Client)

John Thekkethala

Program Manager for Remote Assistance and the Remote Assistance team at Microsoft

Summary

Remote Assistance has been enhanced in Windows Vista to provide better performance, improved usability, NAT-traversal flexibility, and increased security. Best practices for implementing Remote Assistance in an enterprise environment include:

- Use Group Policy to enable users of targeted computers in a domain or OU to receive offers of RA from Help Desk personnel.
- Use Group Policy to enable the RA exception in the Windows Firewall.
- Use Group Policy to deploy scripts to enable users to run the msra.exe executable if you want to customize how they launch RA sessions—for example, to upload an invitation to a network share monitored by support personnel.
- If all of your support computers are running Vista, use Group Policy to encrypt RA tickets to hide sensitive information such as users' IP addresses and computer names.
- If corporate policy requires RA records for auditing purposes, use Group Policy to enable RA logging on your company's desktop computers and run scripts to periodically move both Helper and User RA logs to a safe storage.

- To meet corporate privacy and security requirements, use Group Policy to customize the text message that users see before they allow the Helper view their screens or share control.

Additional Resources

The following resources contain additional information and tools related to this chapter.

Related Information

- Remote Assistance FAQ from Windows Vista Help and Support can be found at <http://windowshelp.microsoft.com/Windows/en-US/help/398b5eda-aa7f-4078-94c5-1519b697bfa01033.mspx>.
- Remote Assistance Rendezvous API reference from the Windows SDK can be found at <http://windowssdk.msdn.microsoft.com/en-us/library/aa359213.aspx>.