

# Contents

## Windows Internals, Sixth Edition, Part 1

---

<i>Introduction</i> .....	<i>xvii</i>
<b>Chapter 1 Concepts and Tools</b> .....	<b>1</b>
Windows Operating System Versions .....	1
Foundation Concepts and Terms .....	2
Windows API .....	2
Services, Functions, and Routines .....	4
Processes, Threads, and Jobs .....	5
Virtual Memory .....	15
Kernel Mode vs. User Mode .....	17
Terminal Services and Multiple Sessions .....	20
Objects and Handles .....	21
Security .....	22
Registry .....	23
Unicode .....	24
Digging into Windows Internals .....	24
Performance Monitor .....	25
Kernel Debugging .....	26
Windows Software Development Kit .....	31
Windows Driver Kit .....	31
Sysinternals Tools .....	32
Conclusion .....	32
<b>Chapter 2 System Architecture</b> .....	<b>33</b>
Requirements and Design Goals .....	33
Operating System Model .....	34
Architecture Overview .....	35
Portability .....	37
Symmetric Multiprocessing .....	38

---

**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:

[microsoft.com/learning/booksurvey](http://microsoft.com/learning/booksurvey)

Scalability . . . . .	40
Differences Between Client and Server Versions . . . . .	41
Checked Build . . . . .	45
Key System Components . . . . .	46
Environment Subsystems and Subsystem DLLs . . . . .	48
Ntdll.dll . . . . .	53
Executive . . . . .	54
Kernel . . . . .	57
Hardware Abstraction Layer . . . . .	60
Device Drivers . . . . .	63
System Processes . . . . .	68
Conclusion . . . . .	78

**Chapter 3 System Mechanisms 79**

Trap Dispatching . . . . .	79
Interrupt Dispatching . . . . .	81
Timer Processing . . . . .	112
Exception Dispatching . . . . .	123
System Service Dispatching . . . . .	132
Object Manager . . . . .	140
Executive Objects . . . . .	143
Object Structure . . . . .	145
Synchronization . . . . .	176
High-IRQL Synchronization . . . . .	178
Low-IRQL Synchronization . . . . .	183
System Worker Threads . . . . .	205
Windows Global Flags . . . . .	207
Advanced Local Procedure Call . . . . .	209
Connection Model . . . . .	210
Message Model . . . . .	211
Asynchronous Operation . . . . .	213
Views, Regions, and Sections . . . . .	214
Attributes . . . . .	215
Blobs, Handles, and Resources . . . . .	215
Security . . . . .	216
Performance . . . . .	217
Debugging and Tracing . . . . .	218

Kernel Event Tracing .....	220
Wow64 .....	224
Wow64 Process Address Space Layout .....	224
System Calls .....	225
Exception Dispatching .....	225
User APC Dispatching .....	225
Console Support .....	225
User Callbacks .....	226
File System Redirection .....	226
Registry Redirection .....	227
I/O Control Requests .....	227
16-Bit Installer Applications .....	228
Printing .....	228
Restrictions .....	228
User-Mode Debugging .....	229
Kernel Support .....	229
Native Support .....	230
Windows Subsystem Support .....	232
Image Loader .....	232
Early Process Initialization .....	234
DLL Name Resolution and Redirection .....	235
Loaded Module Database .....	238
Import Parsing .....	242
Post-Import Process Initialization .....	243
SwitchBack .....	244
API Sets .....	245
Hypervisor (Hyper-V) .....	248
Partitions .....	249
Parent Partition .....	249
Child Partitions .....	251
Hardware Emulation and Support .....	254
Kernel Transaction Manager .....	268
Hotpatch Support .....	270
Kernel Patch Protection .....	272
Code Integrity .....	274
Conclusion .....	276

<b>Chapter 4</b>	<b>Management Mechanisms</b>	<b>277</b>
	The Registry . . . . .	.277
	Viewing and Changing the Registry . . . . .	.277
	Registry Usage . . . . .	.278
	Registry Data Types . . . . .	.279
	Registry Logical Structure . . . . .	.280
	Transactional Registry (TxR) . . . . .	.287
	Monitoring Registry Activity . . . . .	.289
	Process Monitor Internals . . . . .	.289
	Registry Internals . . . . .	.293
	Services . . . . .	.305
	Service Applications . . . . .	.305
	The Service Control Manager . . . . .	.321
	Service Startup . . . . .	.323
	Startup Errors . . . . .	.327
	Accepting the Boot and Last Known Good . . . . .	.328
	Service Failures . . . . .	.330
	Service Shutdown . . . . .	.331
	Shared Service Processes . . . . .	.332
	Service Tags . . . . .	.335
	Unified Background Process Manager . . . . .	.336
	Initialization . . . . .	.337
	UBPM API . . . . .	.338
	Provider Registration . . . . .	.338
	Consumer Registration . . . . .	.339
	Task Host . . . . .	.341
	Service Control Programs . . . . .	.341
	Windows Management Instrumentation . . . . .	.342
	Providers . . . . .	.344
	The Common Information Model and the Managed Object Format Language . . . . .	.345
	Class Association . . . . .	.349
	WMI Implementation . . . . .	.351
	WMI Security . . . . .	.353
	Windows Diagnostic Infrastructure . . . . .	.354
	WDI Instrumentation . . . . .	.354
	Diagnostic Policy Service . . . . .	.354
	Diagnostic Functionality . . . . .	.356
	Conclusion . . . . .	.357

<b>Chapter 5</b>	<b>Processes, Threads, and Jobs</b>	<b>359</b>
	Process Internals . . . . .	359
	Data Structures . . . . .	359
	Protected Processes . . . . .	368
	Flow of <i>CreateProcess</i> . . . . .	369
	Stage 1: Converting and Validating Parameters and Flags. . . . .	371
	Stage 2: Opening the Image to Be Executed . . . . .	373
	Stage 3: Creating the Windows Executive Process Object ( <i>PspAllocateProcess</i> ) . . . . .	376
	Stage 4: Creating the Initial Thread and Its Stack and Context. . . . .	381
	Stage 5: Performing Windows Subsystem–Specific Post-Initialization . . . . .	383
	Stage 6: Starting Execution of the Initial Thread . . . . .	385
	Stage 7: Performing Process Initialization in the Context of the New Process . . . . .	386
	Thread Internals . . . . .	391
	Data Structures . . . . .	391
	Birth of a Thread . . . . .	398
	Examining Thread Activity. . . . .	398
	Limitations on Protected Process Threads. . . . .	401
	Worker Factories (Thread Pools) . . . . .	403
	Thread Scheduling . . . . .	408
	Overview of Windows Scheduling . . . . .	408
	Priority Levels . . . . .	410
	Thread States . . . . .	416
	Dispatcher Database . . . . .	421
	Quantum . . . . .	422
	Priority Boosts. . . . .	430
	Context Switching . . . . .	448
	Scheduling Scenarios. . . . .	449
	Idle Threads. . . . .	453
	Thread Selection. . . . .	456
	Multiprocessor Systems. . . . .	458
	Thread Selection on Multiprocessor Systems . . . . .	467
	Processor Selection . . . . .	468
	Processor Share–Based Scheduling . . . . .	470
	Distributed Fair Share Scheduling. . . . .	471
	CPU Rate Limits . . . . .	478

Dynamic Processor Addition and Replacement .....	479
Job Objects .....	480
Job Limits .....	481
Job Sets .....	482
Conclusion .....	485

**Chapter 6 Security 487**

Security Ratings .....	487
Trusted Computer System Evaluation Criteria .....	487
The Common Criteria .....	489
Security System Components .....	490
Protecting Objects .....	494
Access Checks .....	495
Security Identifiers .....	497
Virtual Service Accounts .....	518
Security Descriptors and Access Control .....	522
The AuthZ API .....	536
Account Rights and Privileges .....	538
Account Rights .....	540
Privileges .....	540
Super Privileges .....	546
Access Tokens of Processes and Threads .....	547
Security Auditing .....	548
Object Access Auditing .....	549
Global Audit Policy .....	552
Advanced Audit Policy Settings .....	554
Logon .....	555
Winlogon Initialization .....	556
User Logon Steps .....	558
Assured Authentication .....	562
Biometric Framework for User Authentication .....	563
User Account Control and Virtualization .....	566
File System and Registry Virtualization .....	566
Elevation .....	573
Application Identification (AppID) .....	581
AppLocker .....	583
Software Restriction Policies .....	589
Conclusion .....	590

## Chapter 7 Networking 591

Windows Networking Architecture . . . . .	591
The OSI Reference Model . . . . .	592
Windows Networking Components . . . . .	594
Networking APIs . . . . .	597
Windows Sockets . . . . .	597
Winsock Kernel . . . . .	603
Remote Procedure Call . . . . .	605
Web Access APIs . . . . .	610
Named Pipes and Mailslots . . . . .	612
NetBIOS . . . . .	618
Other Networking APIs . . . . .	620
Multiple Redirector Support . . . . .	627
Multiple Provider Router . . . . .	627
Multiple UNC Provider . . . . .	630
Surrogate Providers . . . . .	632
Redirector . . . . .	633
Mini-Redirectors . . . . .	634
Server Message Block and Sub-Redirectors . . . . .	635
Distributed File System Namespace . . . . .	637
Distributed File System Replication . . . . .	638
Offline Files . . . . .	639
Caching Modes . . . . .	641
Ghosts . . . . .	643
Data Security . . . . .	643
Cache Structure . . . . .	643
BranchCache . . . . .	645
Caching Modes . . . . .	647
BranchCache Optimized Application Retrieval: SMB Sequence . . . . .	651
BranchCache Optimized Application Retrieval: HTTP Sequence . . . . .	653
Name Resolution . . . . .	655
Domain Name System . . . . .	655
Peer Name Resolution Protocol . . . . .	656
Location and Topology . . . . .	658
Network Location Awareness . . . . .	658
Network Connectivity Status Indicator . . . . .	659
Link-Layer Topology Discovery . . . . .	662

Protocol Drivers . . . . .	663
Windows Filtering Platform . . . . .	666
NDIS Drivers . . . . .	672
Variations on the NDIS Miniport . . . . .	677
Connection-Oriented NDIS . . . . .	677
Remote NDIS . . . . .	680
QoS . . . . .	682
Binding . . . . .	684
Layered Network Services . . . . .	685
Remote Access . . . . .	685
Active Directory . . . . .	686
Network Load Balancing . . . . .	688
Network Access Protection . . . . .	689
Direct Access . . . . .	695
Conclusion . . . . .	696
<b>Index . . . . .</b>	<b>697</b>

## **Windows Internals, Sixth Edition, Part 2** *(available Fall 2012)*

---

*Introduction*

### **Chapter 8 I/O System**

I/O System Components  
Device Drivers  
I/O Processing  
Kernel-Mode Driver Framework (KMDF)  
User-Mode Driver Framework (UMDF)  
The Plug and Play (PnP) Manager  
The Power Manager  
Conclusion

### **Chapter 9 Storage Management**

Storage Terminology  
Disk Drivers  
Volume Management  
BitLocker Drive Encryption  
Volume Shadow Copy Service  
Conclusion



## **Chapter 10 Memory Management**

- Introduction to the Memory Manager
- Services the Memory Manager Provides
- Kernel-Mode Heaps (System Memory Pools)
- Heap Manager
- Virtual Address Space Layouts
- Address Translation
- Page Fault Handling
- Stacks
- Virtual Address Descriptors
- NUMA
- Section Objects
- Driver Verifier
- Page Frame Number Database
- Physical Memory Limits
- Working Sets
- Proactive Memory Management (SuperFetch)
- Conclusion

## **Chapter 11 Cache Manager**

- Key Features of the Cache Manager
- Cache Virtual Memory Management
- Cache Size
- Cache Data Structures
- File System Interfaces
- Fast I/O
- Read Ahead and Write Behind
- Conclusion

## **Chapter 12 File Systems**

- Windows File System Formats
- File System Driver Architecture
- Troubleshooting File System Problems
- Common Log File System
- NTFS Design Goals and Features
- NTFS File System Driver
- NTFS On-Disk Structure
- NTFS Recovery Support

Encrypting File System Security  
Conclusion

## **Chapter 13 Startup and Shutdown**

Boot Process  
Troubleshooting Boot and Startup Problems  
Shutdown  
Conclusion

## **Chapter 14 Crash Dump Analysis**

Why Does Windows Crash?  
The Blue Screen  
Troubleshooting Crashes  
Crash Dump Files  
Windows Error Reporting  
Online Crash Analysis  
Basic Crash Dump Analysis  
Using Crash Troubleshooting Tools  
Advanced Crash Dump Analysis  
Conclusion

---

### **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:

[microsoft.com/learning/booksurvey](http://microsoft.com/learning/booksurvey)