

# Index

## A

- access types, 59
- ActivePerl, 5
- Address Resolution Protocol (ARP), 78
- archiving event logs, 45, 158
- ARP tables, 85–88
  - capabilities, 87
  - resources for further reading, 87
- arp.exe utility, 86
- at command, 8
- at.exe utility, 8
- attrib.exe utility, 43
- auditing, 58–61
  - access types, 59
  - audit events, 59
  - main features, 61
- Autolog.exe utility, 10
- autologon, 9–19
  - registry keys, 16
  - security implications, 26
  - setting with Regedt32, 15–17
  - starting with Perl, 17–19
- automated configuration/maintenance, 3

## B

- backup directories, 46
- batch processing functions, 128–131

## C

- changing (see configuring)
- clearing event logs, 158

- closing registry keys, 148
- CLSID (Class ID) registry keys, 104
- code
  - for the MaintainAndConfigure module, 132–143
  - guidelines for writing and testing, 113
- command-line interface, 8
- command-line utilities, 48
  - attrib.exe utility, 43
  - net.exe utility, 54–57
- computer name
  - domain and, 108
  - finding, 73–77, 93–96
- ComputerName registry key, 97
- configuration files, 130
- configuration functions, 123–128
- configuring
  - automated configuration, 3
  - error control values, 68
  - IP addresses, 98–103
  - MaintainAndConfigure module
    - for, 121–143
  - My Computer icon, 103
  - NetBIOS name, 96–98
  - network identity, 91–110
    - for multiple workstations, 91–93
  - SIDs, 105–108
- control panels
  - Drivers Control Panel, 57
  - Hardware Profiles Control Panel, 69
  - Network Control Panel, 74, 96, 99
  - Services Control Panel, 8, 22–23, 57

controlling drivers, 63–72  
  reasons for, 53  
creating  
  registry keys, 13, 149  
  registry values, 14, 148

**D**

Data Link Control (DLC), 78  
data, sending, 154  
default gateway, 100, 102  
deleting  
  files from temporary directories, 42–45  
  registry keys, 13  
  registry values, 15, 149  
dependency, 67  
deployment methods for scripts, 114  
difference files, 62  
domain  
  joining, 108–110  
  SIDs and, 106  
DOS network drivers, 79  
drivers  
  controlling, 53, 63–72  
  vs. services, 57  
Drivers Control Panel, 57

**E**

email sent by scripts, 48, 151–155  
enabling/disabling network  
  connectivity, 69–72  
%ENV Perl variable, 76  
environment table, 76  
environment variables, 76  
error control values, 68  
Ethernet cards, 77–78  
event ID field, 66  
event log objects, constructing, 155  
event logs  
  archiving, 45, 158  
  clearing, 158  
  managing, 65  
  reading entries, 156  
  reporting problems, 49–52  
  resources for further reading, 52  
event module functions, 155–158  
Event Viewer utility, 2, 60, 65–72  
execution, successful, 56  
extracting (see finding)

**F**

finding  
  computer name, 73–77, 93–96  
  IP addresses, 93–96  
  MAC addresses  
    via ARP tables, 85–88  
    with a DOS network driver, 79  
    with getmac.exe utility, 81  
    with ipconfig.exe utility, 79  
    via lookup table, 88–90  
    via the registry, 82  
  machine identifier, 73–77, 93–96  
  registry entries  
    by auditing the registry, 58–61  
    with Regmon.exe utility, 63–65  
    with sysdiff.exe utility, 62  
  workstation names, 73–77  
fully qualified hostnames, 88  
functions  
  function names, 146  
  module functions, 121–131  
  Perl module functions, 145–158

**G**

gateway, default, 100, 102  
getmac.exe utility, 81  
  capabilities, 82  
GUID (globally unique identifier), 104  
guidelines for script development, 112

**H**

hackers, security against, 115–118  
handles, 11, 18, 20, 147  
hardware, enabling/disabling, 69  
Hardware Profiles Control Panel, 69  
Hardware Profiles registry key, 60  
hash tables, 37, 47  
help files, 8  
hives, 11, 147  
HKEY\_CLASSES\_ROOT key, 12, 147  
  CLSID subkey, 104  
HKEY\_CURRENT\_CONFIG key, 12, 147  
HKEY\_CURRENT\_USER key, 12, 147  
HKEY\_LOCAL\_MACHINE key, 12, 17,  
  59–61, 74, 83, 124–125, 130, 147  
HKEY\_PERFORMANCE\_DATA key, 147  
HKEY\_PERFORMANCE\_NLSTEXT key, 147  
HKEY\_PERFORMANCE\_TEXT key, 147

HKEY\_USERS key, 12, 59, 147  
HKLM\SOFTWARE\Description\Microsoft\  
Rpc\UuidTemporaryData key, 83  
HKLM\SOFTWARE\Microsoft\Windows NT  
keys  
Windows key, 69  
Winlogon key, 15  
HKLM\SOFTWARE\Microsoft\Windows\  
CurrentVersion\RunOnce key, 10  
HKLM\SYSTEM\CurrentControlSet keys, 70  
ComputerName key, 97  
HardwareProfiles key, 60  
Lsa key, 46  
Services key, 20–21, 67, 101  
srvname key, 22  
Start key (Tcpip), 64  
hostnames, 74, 100  
fully qualified, 88  
IP hostname, 97  
housekeeping, 42–47

**I**

information events, 66  
instrv.exe utility, 21–23  
Internet Control Message Protocol  
(ICMP), 86  
internet protocol (IP), 98  
IP addresses, 98  
configuring via Network Control  
Panel, 99  
finding, 93–96  
registry settings for, 100–103  
IP hostname, 97  
IP networking  
resources for further reading, 98  
setting up, 98–103  
ipconfig.exe utility, 79  
capabilities, 80

**L**

LegalNotice registry keys, 19  
Local Security Authority (LSA), 108  
lookup table, compiling, 88–90  
Lsa registry key, 46

**M**

MAC addresses, 78, 92  
finding, 78–90, 93–96  
via ARP tables, 85–88  
with a DOS network driver, 79  
with getmac.exe utility, 81  
with ipconfig.exe utility, 79  
via lookup table, 88–90  
via the registry, 82–85  
machine identifier, finding, 73–77, 93–96  
MaintainAndConfigure module, 121–143  
batch processing functions, 128–131  
code for, 132–143  
configuration functions, 123–128  
script control functions, 122  
maintenance, 41–52  
automated, 3  
MaintainAndConfigure module  
for, 121–143  
managing event logs, 65  
Media Access Control (MAC) addresses (see  
MAC addresses)  
modules  
custom  
advantages of, 120, 133  
MaintainAndConfigure module (see  
MaintainAndConfigure module)  
importing, 145  
Perl module functions, 145–158  
monitoring (see auditing)  
My Computer icon, configuring, 103

**N**

native functions, 145  
nested subdirectories, 44  
Net::SMTP module, 48  
functions of, 151–155  
NetBIOS name  
configuring, 96–98  
replacing using NewSID.exe utility, 107  
Netdom.exe utility, 109  
net.exe utility, 54–57, 109  
machine identifier extraction, 75  
Network Basic Input/Output System (see  
NetBIOS)

- Network Control Panel
    - configuring IP addresses, 99
    - finding computer name, 74
    - setting NetBIOS name, 96
  - network identity, configuring, 91–110
    - for multiple workstations, 91–93
  - Network-disabled Hardware Profile, 69
  - networks
    - connectivity, enabling/disabling, 69–72
    - disruption of, 30
    - identity (see network identity)
  - NewsSID.exe utility, 106
  - NTFS (NT file system), 2
- O**
- object-oriented interface, 146
  - open keys, 147
- P**
- packet-sniffers, 118
  - Perl, 4, 145–147
    - case sensitivity, 147
    - %ENV variable, 76
    - MaintainAndConfigure module, 121–143
    - module functions, 145–158
    - Net::SMTP module, 48
    - recursive functions, 44
    - saving time with, 24
  - Primary Domain Controller (PDC), 108
  - print spooler services,
    - starting/stopping, 55–56
  - process module functions, 149–151
  - processes, creating, 150
  - purgable directories, 43
- R**
- recipients, 153
  - reconfiguration scripts, 93–96
  - recursive functions, 44
  - RegCreateKey function, 71
  - Regedit, 2, 12, 97
  - Regedt32, 13–17, 58, 74, 97
  - registry
    - access types, 59
    - audit event, 59
    - auditing, 58–61, 97
      - main features, 61
      - in real time, 65
    - enabling/disabling network connectivity
      - via, 69
    - finding entries, 58–65
      - by auditing, 58–61
      - with Regmon.exe utility, 63–65
      - with sysdiff.exe utility, 62
    - finding MAC address via, 82–85
      - capabilities of the technique, 85
    - IP addresses settings, 100–103
    - keys (see registry keys)
    - machine identifier extraction, 74
    - module functions, 147–149
    - NetBIOS name settings, 97
    - object-oriented versions, 146
    - overview, 11–13
    - Regedt32, 58
    - resources for further reading, 11
    - TCP/IP parameter settings, 100–103
    - value types, 14
    - values (see registry values)
  - registry keys, 11–14, 147–149
    - autologon registry keys, 16
    - closing, 148
    - CLSID (Class ID) registry keys, 104
    - creating, 13, 149
    - deleting, 13
    - opening, 147
    - root keys, 12
    - traversing, 13
  - registry values, 12, 68
    - creating, 14, 148
    - deleting, 15, 149
    - modifying, 148
    - types of, 14
  - Regmon.exe utility, 58, 63–65
    - main features, 65
    - vs. auditing or the sysdiff.exe utility, 65
  - relative identifier, 105
  - reporting, 47–52
    - disk overload, 48
    - event log problems, 49–52
  - resources for further reading
    - ARP tables, 87
    - event logs, 52
    - internet protocol, 98
    - maintenance tools, 2
    - Perl, 5
    - Windows NT Registry, 11

Windows NT User Administration, 9  
Windows NT Workstation Resource Kit, 10  
retrieving (see finding)  
RID (relative identifier), 105  
root keys, 11–13  
RPC registry entry, 83, 94  
RunOnce registry key, 10

**S**

safety/security  
key security issues, 115–118  
Netdom.exe utility and, 110  
running scripts without user intervention, 25–27  
scripts, 111–119  
precautions when testing, 45  
SIDs, reconfiguring, 105–108  
sc.exe utility, 22  
schedulers, 8  
security implications, 25  
script control functions, 122  
scripts  
adding/removing with stub installed, 35  
changing, danger of, 120  
criteria for usefulness, 41  
deployment methods, 114  
development guidelines, 112  
examples of use, 1  
machine-specific, 73–90  
managing remotely, 28–40  
obsolescence, 30  
Perl language for, 4  
reconfiguration scripts, 93–96  
running without user intervention, 6–27  
security implications, 25–27  
as a service, 19–25  
using autologon, 9–19  
using schedulers, 8  
safety/security, 111–119  
precautions when testing, 45  
sensitive areas, 117  
script control functions, 122  
“script talk”, 117  
self-updating, 28–30  
characteristics, 29  
disadvantages, 33

stub (see stubs)  
updating other scripts, 34  
writing, 30–34  
secure tunnels, 108  
security (see safety/security)  
self-updating scripts, 28–30  
characteristics, 29  
disadvantages, 33  
services, 19–21  
controlling with net.exe utility, 54–57  
vs. drivers, 57  
network, enabling/disabling, 69–72  
schedulers (see schedulers)  
script run as a service, 19–25  
security implications, 26  
starting from command line, 8  
starting from Services Control Panel, 22  
starting/stopping, 8, 53–72  
Win32-based, 20, 57  
Services applet, 8  
Service Control Manager, 20, 54–57, 66–67  
Services Control Panel, 8, 22–23, 57  
Services registry key, 20–21, 67, 101  
SIDs, reconfiguring, 105–108  
SMTP objects, constructing, 152  
source address, 153  
source field, 66  
svany.exe utility, 21–23  
srvname registry key, 22  
Start button (Services Control Panel), 8  
Start (Tcpip) registry key, 64  
starting/stopping services, 53–72  
using net.exe utility, 54–57  
reasons for, 53  
strings, comparing, 94  
stubs (stub scripts), 35–36, 93  
adding/removing scripts, 35  
advantages vs. self-updating scripts, 35  
safety/security, 118  
self-updating, 40  
writing, 36–40  
subdirectories, nested, 44  
subkeys, 13  
successful execution, 56  
sysdiff.exe utility, 58, 62  
main features, 63  
sysdiff.inf configuration file, 62

system maintenance, 41–52  
    MaintainAndConfigure module  
        for, 121–143  
system policy editor, 2

**T**

TCP/IP parameter settings, 100–103  
TCP/IP service, startup states for, 64  
temporary directories, cleaning, 42–45  
traversing registry keys, 13  
TweakUI.exe application, 11

**U**

uniform naming convention (UNC), 123  
user accounts (script security), 115–117  
Uuid Temporary Data registry key  
    (RCP), 83

**V**

values, registry (see registry values)  
version numbering, 30

**W**

Win32 API, 5  
Win32::Registry module, 146

Win32-based services, 20, 57  
Windows NT  
    command-line utilities, 48  
    Windows NT Registry (see registry)  
Windows registry key, 69  
Winlogon registry key, 15  
workstations  
    automated configuration/maintenance, 3  
    configuring, 78  
        automated configuration, 3  
        error control values, 68  
        network identity, 91–110  
    enabling/disabling  
        hardware, 69  
        network connectivity, 69–72  
    housekeeping, 42–47  
    names, finding, 73–77, 93–96  
        (see also MAC addresses)  
    NT domain and, 108  
    reliability, 118  
    reporting, 47–52  
    running scripts on, 6–27  
    system maintenance, 41–52