Unit OS A: Windows Networking

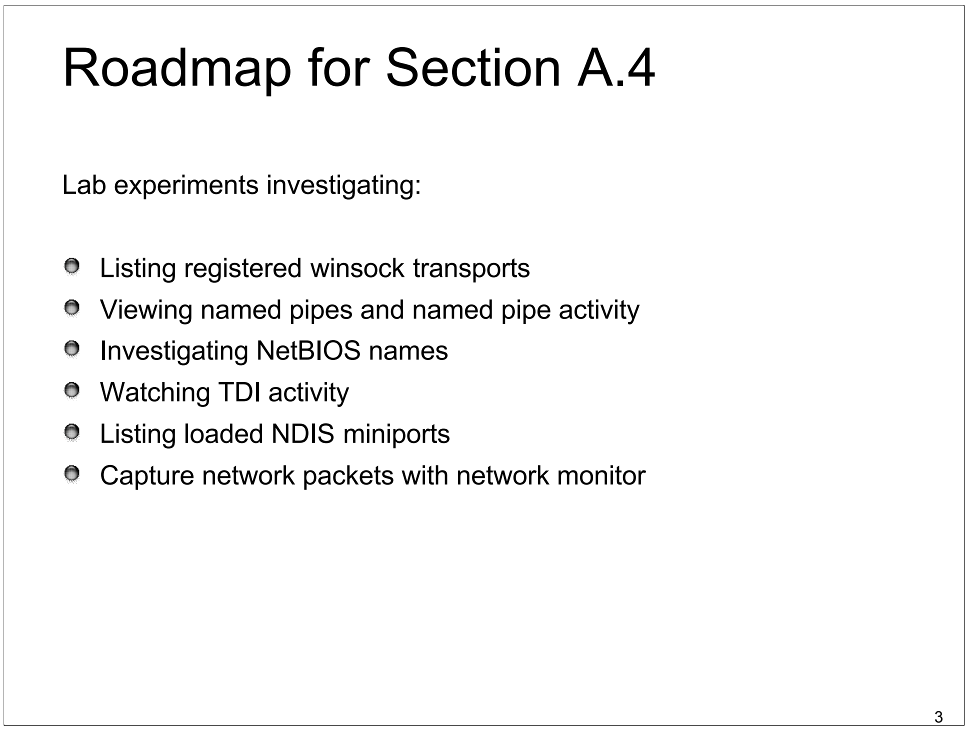
A.4. Lab Manual

Copyright Notice

© 2000-2005 David A. Solomon and Mark Russinovich

- These materials are part of the *Windows Operating System Internals Curriculum Development Kit,* developed by David A. Solomon and Mark E. Russinovich with Andreas Polze
- Microsoft has licensed these materials from David Solomon Expert Seminars, Inc. for distribution to academic organizations solely for use in academic environments (and not for commercial use)

2



Roadmap for Section A.4

Lab experiments investigating:

- Listing registered winsock transports
- Viewing named pipes and named pipe activity
- Investigating NetBIOS names
- Watching TDI activity
- Listing loaded NDIS miniports
- Capture network packets with network monitor

3

This LabManual includes experiments investigating the networking mechanisms and concepts implemented inside the Windows operating system. Students are expected to carry out Labs in addition to studying the learning materials in Unit OS A.

A thorough understanding of the concepts presented in Unit OS A: Windows Networking is a prerequisite for these Labs.

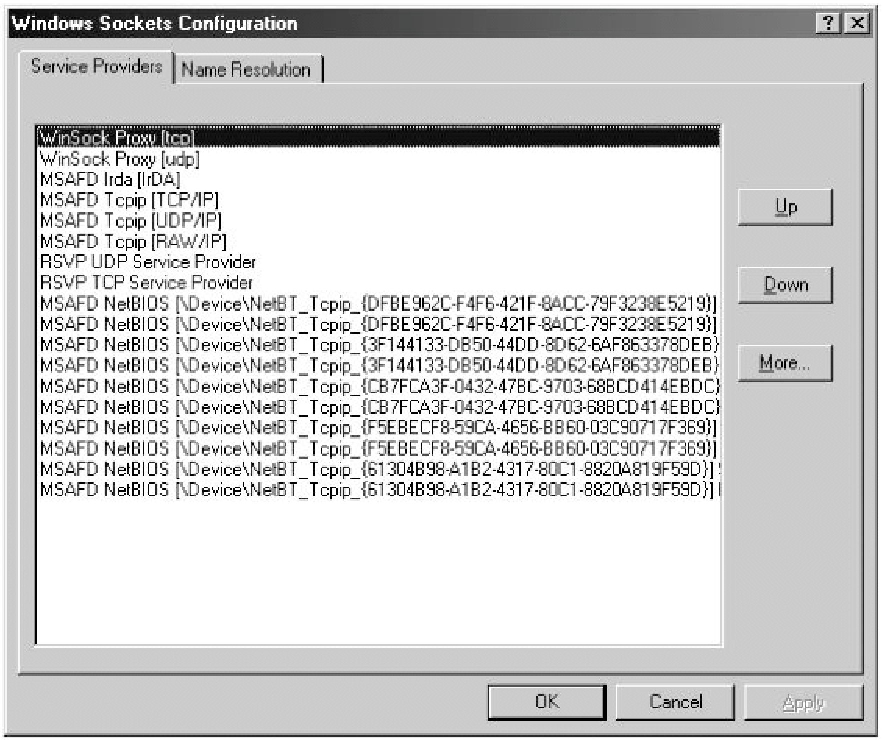
List Registered Winsock Transports

- Winsock integrates with the Windows I/O model and uses file handles to represent sockets
  - Kernel-mode Ancillary Function Driver (AFD - \Windows\System32\Drivers\Afd.sys) implements socket-based functions
  - AFD is a TDI client and executes network socket operations by sending TDI IRPs to protocol drivers
  - AFD isn't coded to use particular protocol drivers; user-mode Msafd.dll informs AFD of the name of the protocol used for each socket
  - AFD opens the device object representing the protocol
- **Windows Sockets Configuration(Sporder.exe)** utility shows registered Winsock transport providers

4

Lab objective: Looking at Winsock Service Providers

The Windows Sockets Configuration utility (Sporder.exe) included with the Platform SDK shows the registered Winsock transport and namespace providers and allows you to change the order in which transport service providers are enumerated. For example, if there are two TCP/IP transport service providers, the first one listed is the default provider for Winsock applications using the TCP/IP protocol.



```
WinSock Proxy [tcp]
WinSock Proxy [udp]
MSAFD Irda [IrDA]
MSAFD Tcpip [TCP/IP]
MSAFD Tcpip [UDP/IP]
MSAFD Tcpip [RAW/IP]
RSVP UDP Service Provider
RSVP TCP Service Provider
MSAFD NetBIOS [\Device\NetBT_Tcpip_{DFBE962C-F4F6-421F-8ACC-79F3238E5219}]
MSAFD NetBIOS [\Device\NetBT_Tcpip_{DFBE962C-F4F6-421F-8ACC-79F3238E5219}]
MSAFD NetBIOS [\Device\NetBT_Tcpip_{3F144133-DB50-44DD-8D62-6AF863378DEB}
MSAFD NetBIOS [\Device\NetBT_Tcpip_{3F144133-DB50-44DD-8D62-6AF863378DEB}
MSAFD NetBIOS [\Device\NetBT_Tcpip_{CB7FCA3F-0432-47BC-9703-68BCD414EBDC}
MSAFD NetBIOS [\Device\NetBT_Tcpip_{CB7FCA3F-0432-47BC-9703-68BCD414EBDC}
MSAFD NetBIOS [\Device\NetBT_Tcpip_{F5EBECF8-59CA-4656-BB60-03C90717F369}]
MSAFD NetBIOS [\Device\NetBT_Tcpip_{F5EBECF8-59CA-4656-BB60-03C90717F369}]
MSAFD NetBIOS [\Device\NetBT_Tcpip_{61304B98-A1B2-4317-80C1-8820A819F59D}]
MSAFD NetBIOS [\Device\NetBT_Tcpip_{61304B98-A1B2-4317-80C1-8820A819F59D}]
```

Viewing Named Pipes and Named Pipe Activity

- Run Pipelist (Sysinternals) to see the named pipes on a system
- Run Filemon (Sysinternals) to watch named pipe activity in real-time

5

Lab objective: Listing the Named Pipe Namespace and Watching Activity

It is not possible to use the Windows API to open the root of the named pipe FSD and perform a directory listing, but you can do this by using native API services. The PipeList tool from www.sysinternals.com shows you the names of the named pipes defined on a computer as well as the number of instances that have been created for a name and the maximum number of instances as defined by a server's call to CreateNamedPipe. Here's an example of PipeList output:

```
C:\>pipelist
PipeList v1.01  byMark Russinovich  http://www.sysinternals.com
Pipe Name                       Instances        Max Instances
---------                       ---------        -------------
TerminalServer\AutoReconnect    1                1
InitShutdown                    2                -1
lsass                           4                -1
protected_storage               2                -1
ntsvcs                          58               -1
scerpc                          2                -1
net\NtControlPipe1              1                1
net\NtControlPipe2              1                1
ExtEventPipe_Service            1                30
...
```

The Filemon file system filter driver from www.sysinternals.com is able to attach to either the Npfs.sys or Msfs.sys file system drivers and to therefore see all named pipe or mailslot activity occurring on a system. Select the Named Pipes or Mail Slots menu entries from Filemon's Drives menu to have Filemon attach to the corresponding driver.

Investigating NetBIOS names

- NetBIOS relies on a naming convention
  - computers and network services are assigned a 16-byte name called a NetBIOS name
  - Only one instance of a unique NetBIOS name can be assigned to a network
  - A client can broadcast messages by sending them to a group
- Windows automatically defines a NetBIOS name for a domain
  - the first 15 bytes of the left-most DNS name
  - support interoperability with Windows NT 4 systems as well as Consumer Windows
- **Nbtstat.exe -n** shows NetBIOS-to-TCP/IP mappings

6

Lab objective: Using Nbtstat to See NetBIOS Names

You can use the Nbtstat command, which is included with Windows, to list the active sessions on a system, the NetBIOS-to-TCP/IP name mappings cached on a computer, and the NetBIOS names defined on a computer. Here's an example of the Nbtstat command with the –n option, which lists the NetBIOS names defined on the computer:

```
C:\>nbtstat -n

Local Area Connection:
Node IpAddress: [192.168.131.65] Scope Id: []
                NetBIOS Local Name Table
       Name               Type         Status
    ---------------------------------------------
    FIN            <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    FIN            <20>  UNIQUE      Registered
    FIN            <03>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered
    ANDREAS        <03>  UNIQUE      Registered
```

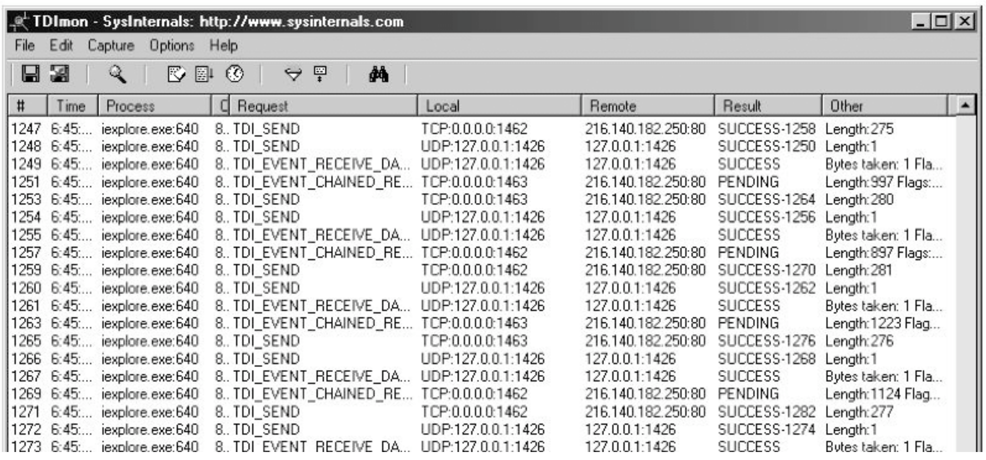
Watching TDI Activity

- Run TDIMon (Sysinternals) to watch TDI activity
  - Access any network resource
  - TDImon sees every IRP that TDI clients issue to network protocols.
  - By intercepting TDI client event callback registration, it also monitors event callbacks.

7

Lab objective: Watching TDI Activity

TDImon, a utility from www.sysinternals.com, is a form of filter driver that attaches to the \Device\Tcp and \Device\Udp device objects that the TCP/IP driver creates. After attaching, TDImon sees every IRP that TDI clients issue to these protocols. By intercepting TDI client event callback registration, it also monitors event callbacks. The TDImon driver sends information about the TDI activity for display in its GUI, where you can see the time of an operation, the type of TDI activity that took place, the local and remote addresses of a TCP connection or the local address of a UDP endpoint, the resulting status code of the IRP or event callback, and additional information such as the number of bytes sent or received. Here's a screen shot of TDImon watching the TDI activity that is generated when Microsoft Internet Explorer browses a Web page:


TDImon - SysInternals: http://www.sysinternals.com
File Edit Capture Options Help

#	Time	Process	C	Request	Local	Remote	Result	Other
1247	6:45:...	iexplore.exe:640	8..	TDI_SEND	TCP:0.0.0.0:1462	216.140.182.250:80	SUCCESS-1258	Length:275
1248	6:45:...	iexplore.exe:640	8..	TDI_SEND	UDP:127.0.0.1:1426	127.0.0.1:1426	SUCCESS-1250	Length:1
1249	6:45:...	iexplore.exe:640	8..	TDI_EVENT_RECEIVE_DA...	UDP:127.0.0.1:1426	127.0.0.1:1426	SUCCESS	Bytes taken: 1 Fla...
1251	6:45:...	iexplore.exe:640	8..	TDI_EVENT_CHAINED_RE...	TCP:0.0.0.0:1463	216.140.182.250:80	PENDING	Length:997 Flags:...
1253	6:45:...	iexplore.exe:640	8..	TDI_SEND	TCP:0.0.0.0:1463	216.140.182.250:80	SUCCESS-1264	Length:280
1254	6:45:...	iexplore.exe:640	8..	TDI_SEND	UDP:127.0.0.1:1426	127.0.0.1:1426	SUCCESS-1256	Length:1
1255	6:45:...	iexplore.exe:640	8..	TDI_EVENT_RECEIVE_DA...	UDP:127.0.0.1:1426	127.0.0.1:1426	SUCCESS	Bytes taken: 1 Fla...
1257	6:45:...	iexplore.exe:640	8..	TDI_EVENT_CHAINED_RE...	TCP:0.0.0.0:1462	216.140.182.250:80	PENDING	Length:897 Flags:...
1259	6:45:...	iexplore.exe:640	8..	TDI_SEND	TCP:0.0.0.0:1462	216.140.182.250:80	SUCCESS-1270	Length:281
1260	6:45:...	iexplore.exe:640	8..	TDI_SEND	UDP:127.0.0.1:1426	127.0.0.1:1426	SUCCESS-1262	Length:1
1261	6:45:...	iexplore.exe:640	8..	TDI_EVENT_RECEIVE_DA...	UDP:127.0.0.1:1426	127.0.0.1:1426	SUCCESS	Bytes taken: 1 Fla...
1263	6:45:...	iexplore.exe:640	8..	TDI_EVENT_CHAINED_RE...	TCP:0.0.0.0:1463	216.140.182.250:80	PENDING	Length:1223 Flag...
1265	6:45:...	iexplore.exe:640	8..	TDI_SEND	TCP:0.0.0.0:1463	216.140.182.250:80	SUCCESS-1276	Length:276
1266	6:45:...	iexplore.exe:640	8..	TDI_SEND	UDP:127.0.0.1:1426	127.0.0.1:1426	SUCCESS-1268	Length:1
1267	6:45:...	iexplore.exe:640	8..	TDI_EVENT_RECEIVE_DA...	UDP:127.0.0.1:1426	127.0.0.1:1426	SUCCESS	Bytes taken: 1 Fla...
1269	6:45:...	iexplore.exe:640	8..	TDI_EVENT_CHAINED_RE...	TCP:0.0.0.0:1462	216.140.182.250:80	PENDING	Length:1124 Flag...
1271	6:45:...	iexplore.exe:640	8..	TDI_SEND	TCP:0.0.0.0:1462	216.140.182.250:80	SUCCESS-1282	Length:277
1272	6:45:...	iexplore.exe:640	8..	TDI_SEND	UDP:127.0.0.1:1426	127.0.0.1:1426	SUCCESS-1274	Length:1
1273	6:45:...	iexplore.exe:640	8..	TDI_EVENT_RECEIVE_DA...	UDP:127.0.0.1:1426	127.0.0.1:1426	SUCCESS	Bytes taken: 1 Fla...

As evidence that TDI operations are inherently asynchronous, the PENDING codes in the Result column indicate that an operation initiated but that the IRP defining the operation hasn't yet completed.

Listing Network Driver Interface Specification (NDIS) miniports

- NDIS-conforming network adapter drivers are called NDIS miniport drivers
  - NDIS library (\Windows\System32\Drivers\Ndis.sys) implements the NDIS boundary that exists between TDI transports (typically) and NDIS drivers
  - a helper library that NDIS driver clients use to format commands they send to NDIS drivers
- Kernel debugger shows miniports:
  - !miniports and !miniport commands
  - ndiskd extension needs to be loaded

8

Lab objective: Listing the Loaded NDIS Miniports

The Ndiskd kernel debugger extension library includes the !miniports and !miniport commands, which let you list the loaded miniports using a kernel debugger and, given the address of a miniport block (a data structure Windows uses to track miniports), see detailed information about the miniport driver. The following example shows the !miniports and !miniport commands being used to list all the miniports and then specifics about the miniport responsible for interfacing the system to a PCI Ethernet adapter. (Note that WAN miniport drivers work with dial-up connections.)

```
kd> .loadndiskd
 Loaded ndiskd extension DLL
kd> !miniports
Driver verifierlevel: 0
Failed allocations: 0
MiniportDriverBlock: 817aa610
  Miniport: 817b1130RAS Async Adapter
Miniport Driver Block: 81a1ef30
  Miniport: 81a1ea70 Direct Parallel
Miniport Driver Block: 81a21cd0
  Miniport: 81a217f0 WAN Miniport (PPTP)
Miniport Driver Block: 81a23290
  Miniport: 81a22130 WAN Miniport (L2TP)
Miniport Driver Block: 81a275f0
  Miniport: 81a25130 Intel 8255x-based PCI Ethernet Adapter(10/100)
kd>!miniport81a25130
  Miniport81a25130 :Intel 8255x-based PCI Ethernet Adapter(10/100)
     Flags :20413208
…
```

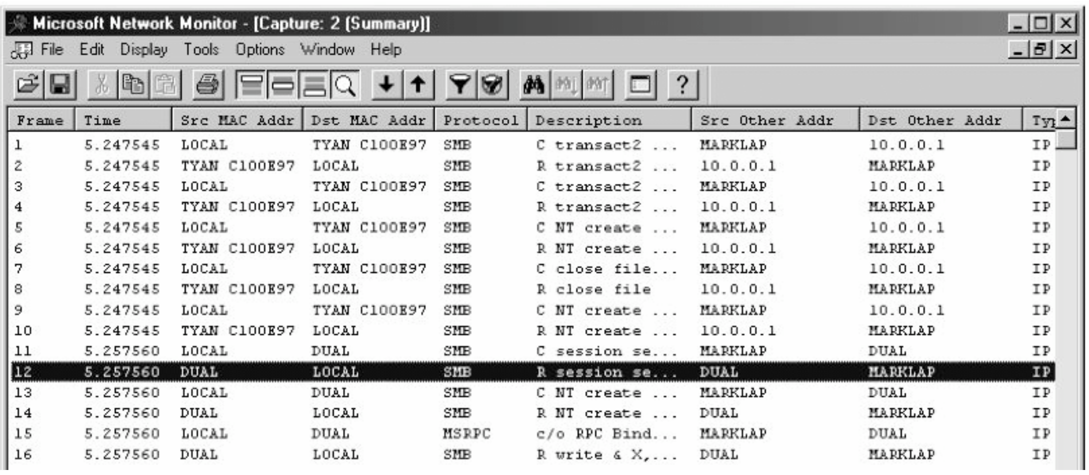
Using Network Monitor to Capture Network Packets

- Note: requires Win2K Server or higher
- Install Network Monitor Tools
- Configure Network Monitor to attach to a network connection
- Run Network Monitor (netmon.exe)
- Press go to begin monitoring
  - Perform network activity
- Press stop to stop monitoring
- Double-click on monitor event to reveal more information

9

Lab objective: Using Network Monitor to Capture Network Packets

Windows Server comes with a tool named Network Monitor that lets you capture packets that flow through one or more NDIS miniport drivers on your system by installing an NDIS intermediate driver. Before you can use Network Monitor, you need to have the Windows Network Monitor Tools installed on your system. To install these tools, open Add/Remove Programs in Control Panel, and select Add/Remove Windows Components. Select Management And Monitoring Tools, click Details, select Network Monitor Tools, and click OK. After Network Monitor has been installed, you can launch Network Monitor by selecting it from the Administrative Tools folder. Network Monitor might ask you which network connection you want to monitor. After selecting one, begin monitoring by pressing the Start Capture button in the toolbar. Perform operations that generate network activity on the connection you're monitoring, and after you see that Network Monitor has captured packets, stop monitoring by clicking the Stop And View Capture button (the stop button that has glasses next to it).


Microsoft Network Monitor - [Capture: 2 (Summary)]
File Edit Display Tools Options Window Help

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	Src Other Addr	Dst Other Addr	Ty
1	5.247545	LOCAL	TYAN C100E97	SMB	C transact2 ...	MARKLAP	10.0.0.1	IP
2	5.247545	TYAN C100E97	LOCAL	SMB	R transact2 ...	10.0.0.1	MARKLAP	IP
3	5.247545	LOCAL	TYAN C100E97	SMB	C transact2 ...	MARKLAP	10.0.0.1	IP
4	5.247545	TYAN C100E97	LOCAL	SMB	R transact2 ...	10.0.0.1	MARKLAP	IP
5	5.247545	LOCAL	TYAN C100E97	SMB	C NT create ...	MARKLAP	10.0.0.1	IP
6	5.247545	TYAN C100E97	LOCAL	SMB	R NT create ...	10.0.0.1	MARKLAP	IP
7	5.247545	LOCAL	TYAN C100E97	SMB	C close file...	MARKLAP	10.0.0.1	IP
8	5.247545	TYAN C100E97	LOCAL	SMB	R close file	10.0.0.1	MARKLAP	IP
9	5.247545	LOCAL	TYAN C100E97	SMB	C NT create ...	MARKLAP	10.0.0.1	IP
10	5.247545	TYAN C100E97	LOCAL	SMB	R NT create ...	10.0.0.1	MARKLAP	IP
11	5.257560	LOCAL	DUAL	SMB	C session se...	MARKLAP	DUAL	IP
12	5.257560	DUAL	LOCAL	SMB	R session se...	DUAL	MARKLAP	IP
13	5.257560	LOCAL	DUAL	SMB	C NT create ...	MARKLAP	DUAL	IP
14	5.257560	DUAL	LOCAL	SMB	R NT create ...	DUAL	MARKLAP	IP
15	5.257560	LOCAL	DUAL	MSRPC	c/o RPC Bind...	MARKLAP	DUAL	IP
16	5.257560	DUAL	LOCAL	SMB	R write & X,...	DUAL	MARKLAP	IP