

SMB – a protocol example

... of which one implementation is SaMBa

David Morgan

© David Morgan 2003

SMB

- “Server Message Block”
- an application layer protocol
- implements file (“resource”) sharing
- built in to Windows

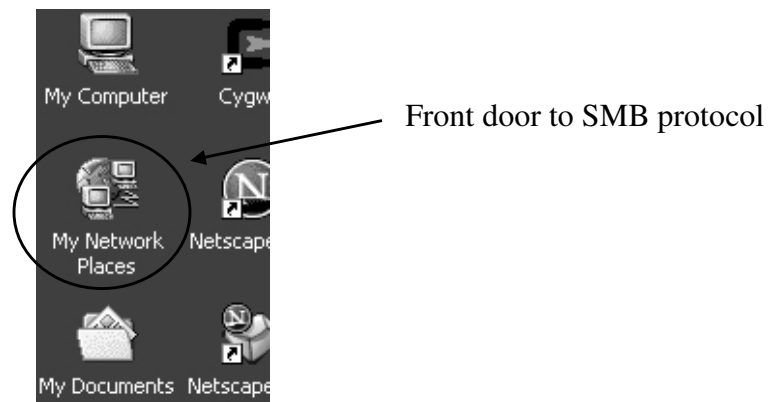
© David Morgan 2003

SMB historical lineage

- from early work by IBM, 3Com, Intel, Microsoft
- the native file-sharing protocol in Windows, since Win95
- fueled by market dominance of Windows
- latter-day version is CIFS (Common Internet File System)

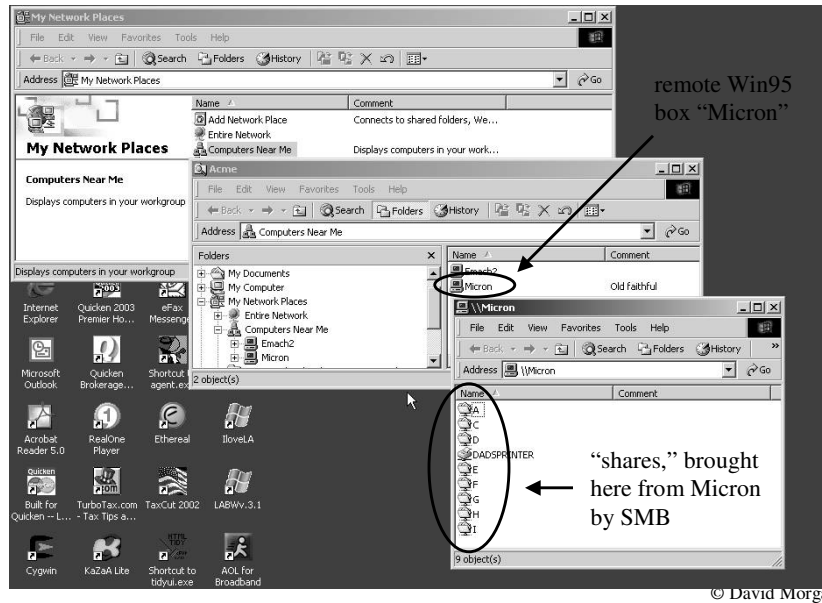
© David Morgan 2003

Where can I find SMB?

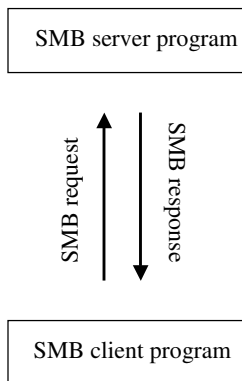


© David Morgan 2003

SMB in action (on machine EMACH2)

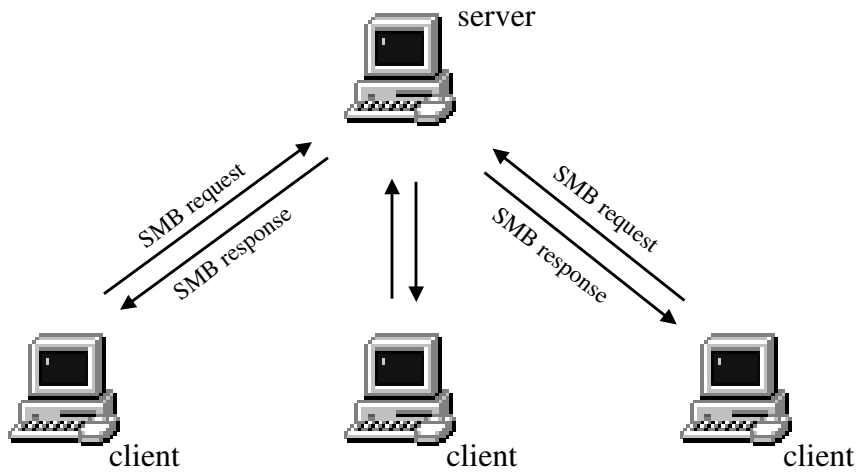


An SMB conversation



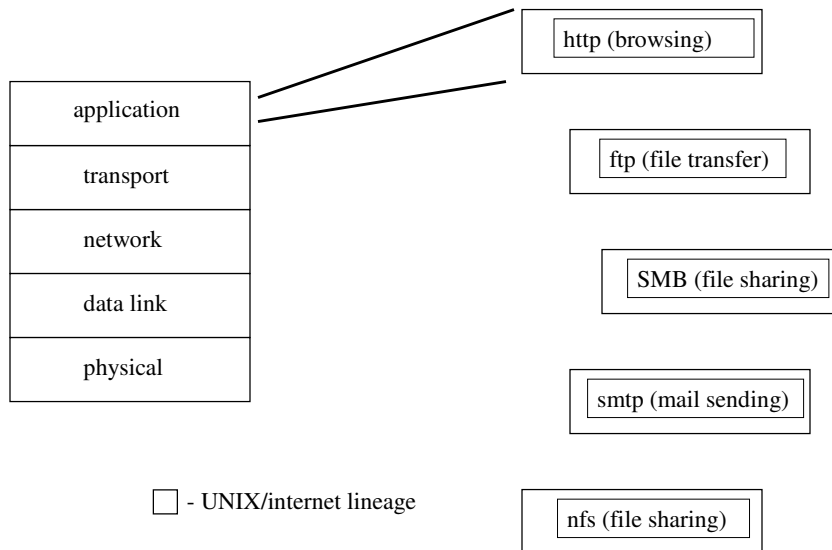
© David Morgan 2003

Typical configuration...



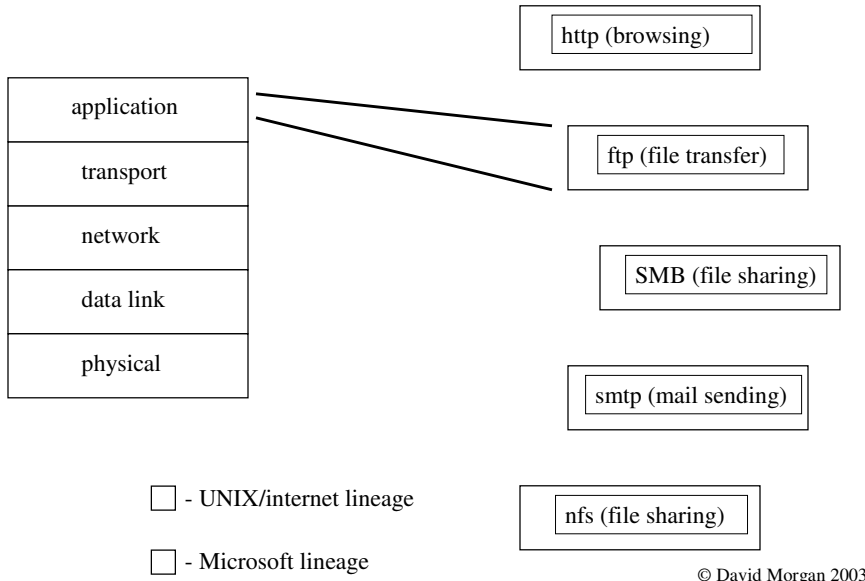
© David Morgan 2003

Application layer protocols

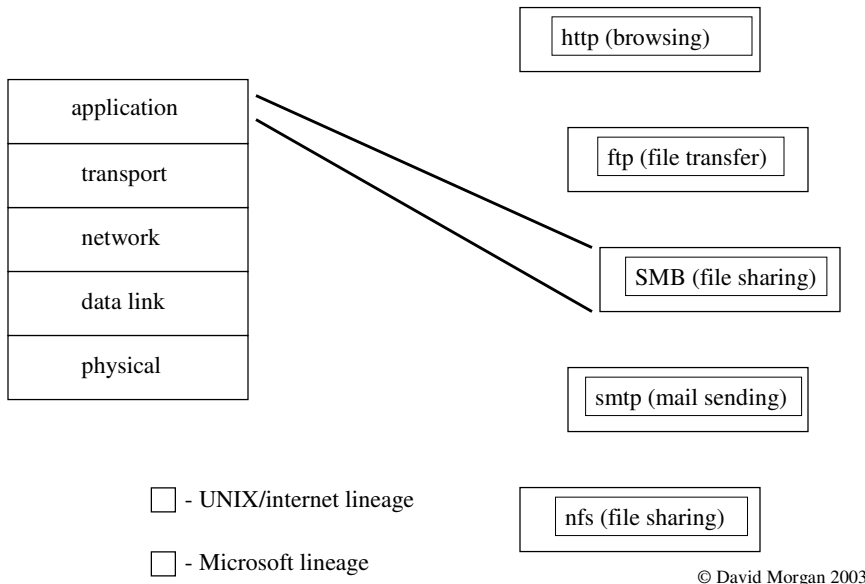


© David Morgan 2003

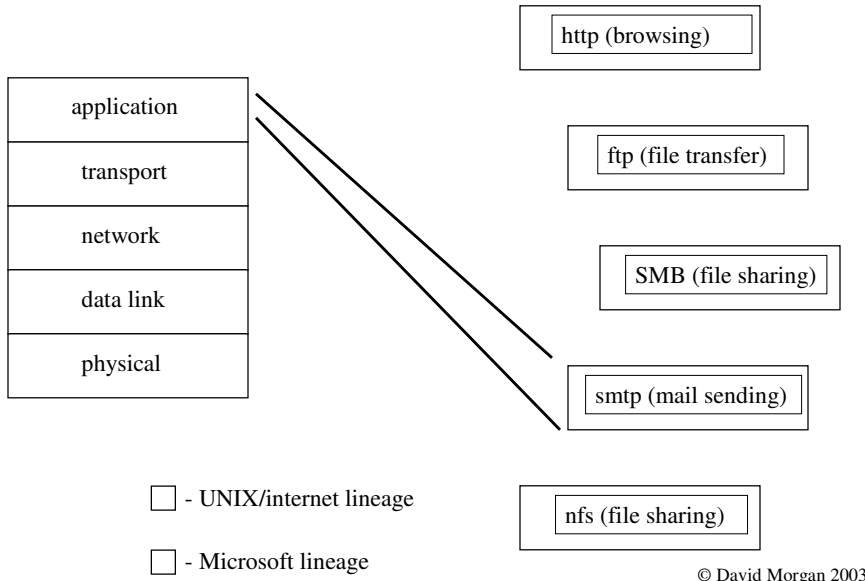
Application layer protocols



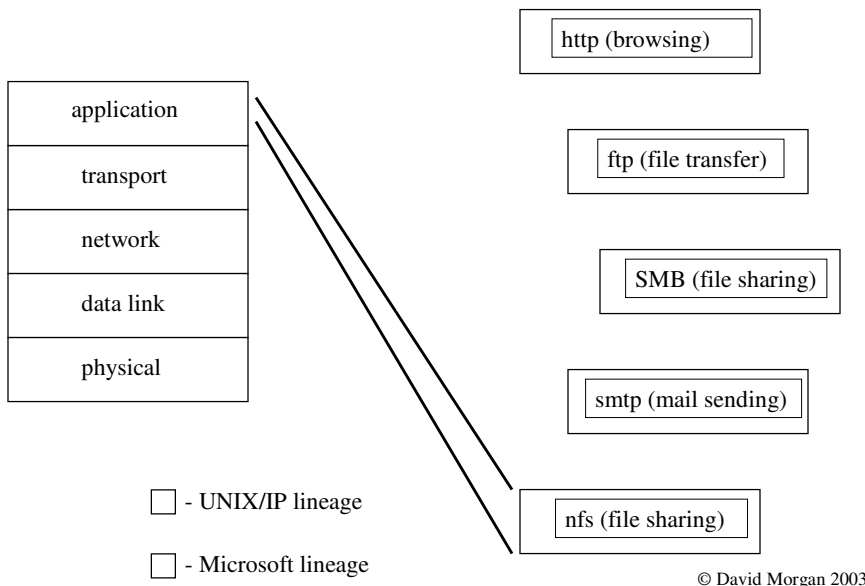
Application layer protocols



Application layer protocols



Application layer protocols



TCP transport supporting different apps

ftp (file transfer)	SMB (file sharing)	http (browsing)
TCP or UDP	TCP or UDP	TCP or UDP
IP	IP	IP
data link	data link	data link
physical	physical	physical

- UNIX/IP lineage

- Microsoft lineage

© David Morgan 2003

SMB app supported by different transports

OSI	SMB				TCP/IP
Application					Application
Presentation					
Session	NetBIOS		NetBIOS	NetBIOS	
Transport	IPX ¹	NetBEUI	DECnet	TCP&UDP	TCP/UDP
Network				IP	IP
Link	802.2, 802.3,802.5	802.2 802.3,802.5	Ethernet V2	Ethernet V2	Ethernet or others
Physical					

© David Morgan 2003

SMB operation

- connection established by lower level protocol (pre-W2K involves netbios, post-W2K can be straight TCP)
- SMBs negotiate common version level
- client sends user/pass to “log in”
 - server returns a UID (id for user)
- client connects to a share
 - server returns a TID (“tree” id for share)
- client embeds UID & TID in future messages for transparent unimpeded access

© David Morgan 2003

SMB commands

- SMB has about 75 commands
- in SMB header's a 1-byte command field
- command categories
 - session control
 - file commands
 - create, open, read, write, close, etc
 - print commands
 - message commands

© David Morgan 2003

Samba and SMB

- Samba implements SMB
- indistinguishable from other implementations
- turns linux box into another windows box from viewpoint of windows boxes

© David Morgan 2003

“Host Announcement” by Win95

Win95 box

SMB stuff, manufactured by Win95

```

No.   Time   Source                                Destination  Protocol  Info
-----
1    0.000  192.168.3.1                          192.168.3.255  BROADCAST Host Announcement MICRON, workstation, Server, Print Queue
2    0.000  192.168.3.1                          192.168.3.255  BROADCAST Host Announcement EMACHI, workstation, Server, Print Queue

Frame 1 (255 on wire, 255 captured)
Ethernet II
Internet Protocol, Src Addr: 192.168.3.1 (192.168.3.1), Dst Addr: 192.168.3.255 (192.168.3.255)
User Datagram Protocol, Src Port: 138 (138), Dst Port: 138 (138)
NetBIOS Datagram Service
Microsoft Message Block Protocol
SMB Header
Transaction Request (0x25)
SMB Mailslot Protocol
Opcode: write Mail slot (1)
Priority: 1
Class: Unreliable & Broadcast (2)
Size: 62
Mailslot Name: \MAILSLOT\BROWSE
Microsoft Windows Browser Protocol
Command: Host Announcement (0x01)
Update Count: 7
Update Periodicity: 5 minutes
Host Name: MICRON
OS Major version: 4
OS Minor version: 0
Server Type: 0x00412203
Browser Protocol Major version: 21
Browser Protocol Minor version: 4
Signature: 0xa35
Host Comment: old faithful

0070  41 43 41 43 41 43 41 43 41 43 41 43 41 42 46 00 ff 53 48 42  acacacac abn, smb
0080  ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  8a.....
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  2d.....
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  3e.....
00b0  00 00 00 23 00 00 00 00 00 01 00 02 00 00 00 00 00  3e.....
00c0  00 5c 48 41 49 4c 53 4c 4f 54 5c 42 52 4f 57 53  5c.....
00d0  45 00 01 07 60 93 04 00 48 49 43 52 4f 4e 00 00  45.....
00e0  00 00 00 00 00 00 00 00 04 00 03 25 41 00 13 04  25.....
00f0  55 aa 4f 8c 64 20 66 01 69 74 68 66 75 8c 00  55aa4f8c6420660169746866758c00
  
```

© David Morgan 2003

“Host Announcement” by samba

linux
box

The screenshot shows a Wireshark capture of a Host Announcement packet. The packet list pane shows two packets from 192.168.3.255 to 192.168.3.255, both identified as BROWSER Host Announcement. The packet details pane for the selected packet (No. 2) shows the following structure:

- Frame 2 (261 on wire, 261 captured)
- Ethernet II
- Internet Protocol, Src Addr: 192.168.3.8 (192.168.3.8), Dst Addr: 192.168.3.255 (192.168.3.255)
- User Datagram Protocol, Src Port: 138 (138), Dst Port: 138 (138)
- NetBIOS Datagram Service
- SMB (Server Message Block Protocol)
 - SMB Header
 - Transaction Request (0x25)
 - SMB Mailslot Protocol
 - Opcode: write Mail slot (1)
 - Priority: 1
 - Class: Unreliable & Broadcast (2)
 - Size: 68
 - Mailslot Name: \MAILSLOT\BROWSE
 - Microsoft Windows Browser Protocol
 - Command: Host Announcement (0x01)
 - Update Count: 0
 - Update Periodicity: 1 minute
 - Host Name: EMACH1
 - OS Major version: 4
 - OS Minor version: 5
 - Server Type: 0x00019a03
 - Browser Protocol Major version: 15
 - Browser Protocol Minor version: 1
 - Signature: 0xaa55
 - Host Comment: Linux Samba Server

The packet bytes pane shows the raw data, with a hex dump and ASCII representation. A bracket on the right side of the packet details pane points to the SMB section with the text "SMB stuff, manufactured by samba".

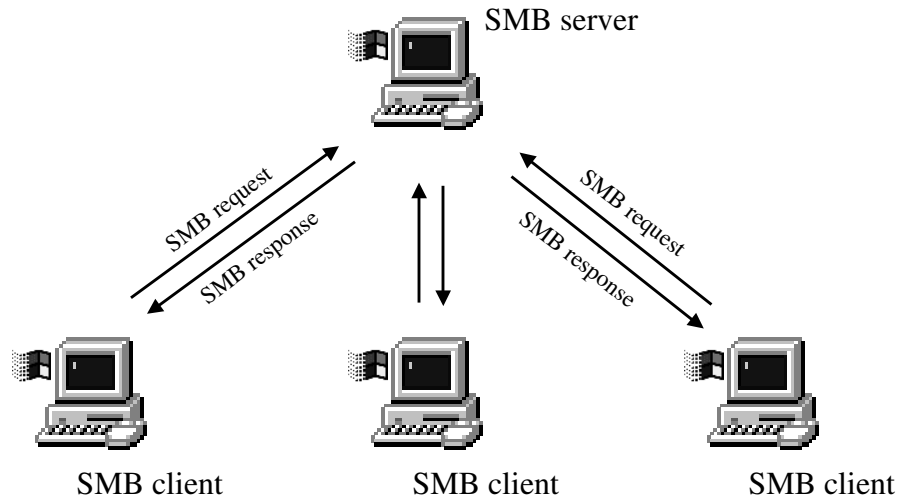
© David Morgan 2003

SMB and nfs

- nfs – network file system
 - originated by Sun Microsystems
- SMB is to Windows as nfs is to UNIX
 - SMB is native file-sharing protocol in Windows
 - nfs is native file-sharing protocol in UNIX
- cross-operability via appropriate drivers
 - samba, for SMB under UNIX
 - Windows Services for UNIX, for nfs under Windows

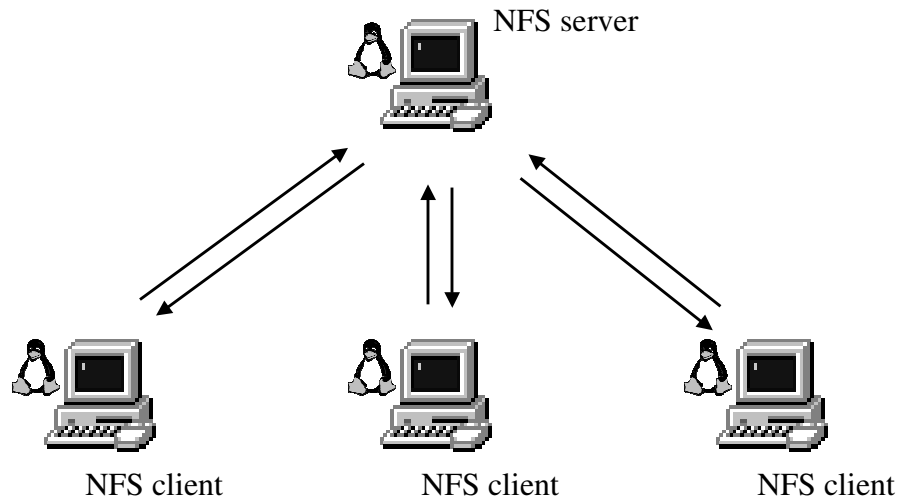
© David Morgan 2003

Pure Windows “native” scenario



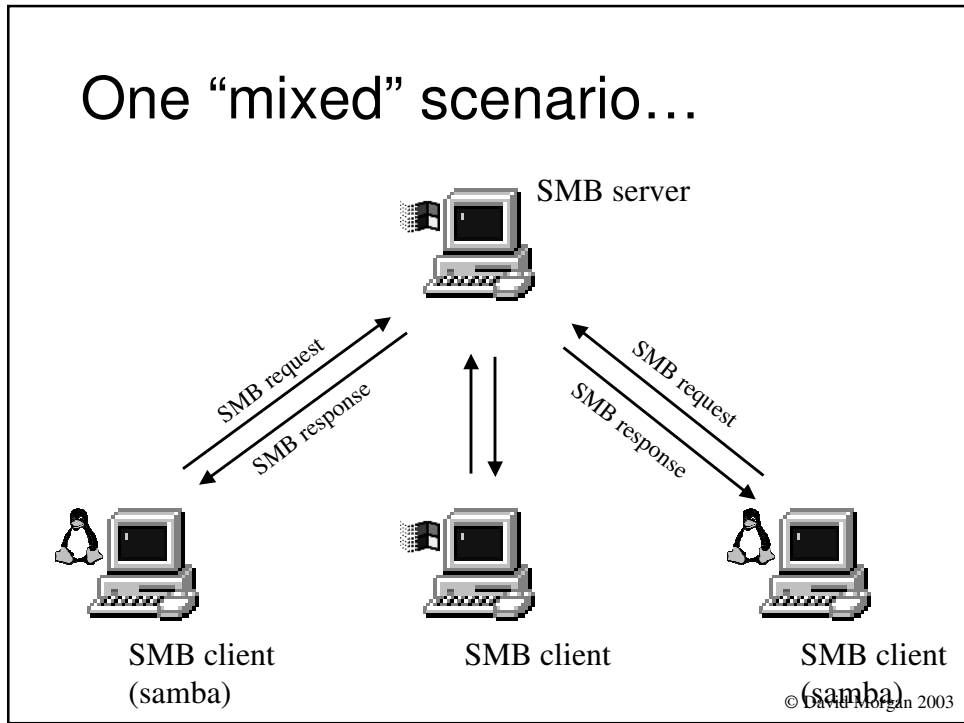
© David Morgan 2003

Pure UNIX “native” scenario

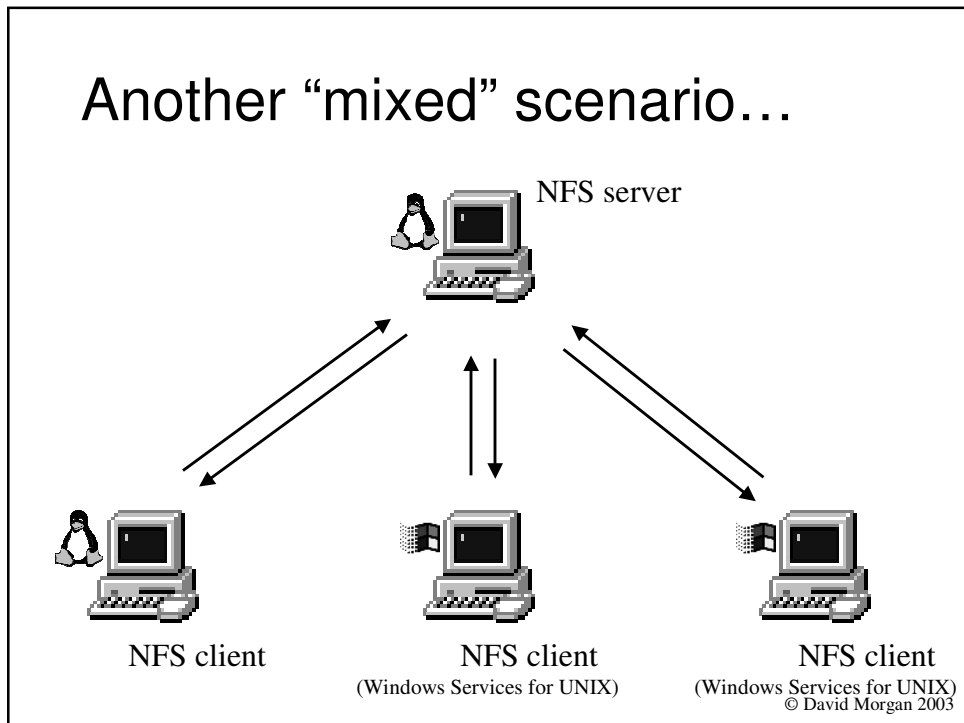


© David Morgan 2003

One "mixed" scenario...



Another "mixed" scenario...



Biblio

- <http://us1.samba.org/samba/docs/>
- Windows NT TCP/IP, Karanjit Siyan, New Riders, 1998

© David Morgan 2003