Software Firewalls with SchoolLeader

If you need to program a software based firewall that runs on your computers, other than the Windows Firewall, these commands shown below illustrate the configuration necessary to program the Windows Firewall for SchoolLeader. Use these commands to translate into the appropriate commands for your own firewall software. The Windows Firewall will be programmed automatically for you by the SchoolLeader setup routines.

Windows Advanced Firewall Commands:

```
Netsh advfirewall firewall add rule name=SQL_Server dir=in action=allow protocol=tcp localport=1433
Netsh advfirewall firewall add rule name=SQL_Browser dir=in action=allow protocol=udp localport=1434
Netsh advfirewall firewall add rule name=SQL_Admin dir=in action=allow protocol=tcp localport=1434
Netsh advfirewall firewall add rule name=SQL_Broker dir=in action=allow protocol=tcp localport=4022

Netsh advfirewall firewall add rule name=FTP_Data dir=in action=allow protocol=tcp localport=20
Netsh advfirewall firewall add rule name=FTP_Control dir=in action=allow protocol=tcp localport=21

Netsh advfirewall firewall add rule name=SafePASS dir=in action=allow protocol=tcp localport=11181

Netsh advfirewall firewall add rule name=MSDTC description=""DTC"" dir=in action=allow program=""c:\windows\system32\msdtc.exe"" enable=yes
Netsh advfirewall firewall add rule name=MSDTC_EndPointMapper dir=in action=allow protocol=tcp localport=135 edge=yes
Netsh advfirewall firewall add rule name=MSDTC_UDP dir=in action=allow protocol=udp localport=any

Netsh advfirewall firewall add rule name=DNS dir=in action=allow protocol=any localport=53
```

Hardware Firewalls with SchoolLeader

SchoolLeader uses a Database management system called "*Microsoft SQL Server*". To manage traffic for multiple users it also uses a Windows service called "*Microsoft Distributed Transaction Coordinator (MSDTC)".* MSDTC uses a dynamic port allocation scheme. While this is easy to program with the Windows Firewall, it is difficult with hardware firewalls. We recommend all hardware firewalls be placed on the "outside" of the LAN switch to avoid interference and eliminate the need to program it at all. The following diagram illustrates the recommended topography