SUPPORT NOTE

SN-134

Common Errors Mapping to a Shared Folder

Introduction

This note addresses some common errors when a logical drive on a DOS Test Controller is mapped to a shared folder on an RDS Intranet Test Client or on a Lab Edition Workstation. Some of the issues arise when a shared folder on any Windows file server is mapped from an MS-DOS computer.

For this note, MS-DOS 6.22 and MS Client 1.00 are assumed to be the operating system and networking client on the DOS Test Controller. It is also assumed that network software in C:\NET is used when booting into RDS DOS and that network software in C:\NETSLV is used when booting into RDS Intranet.

Error 53: The Computer Name…

The most frequent message, "The computer name specified in the network path cannot be located", can be caused by several different problems.

Name of Test Client Does Not Exist

This failure happens when the names of the test client or the server being mapped do not exist or when the server cannot be "seen" by the networking software. In some cases, incorrect or missing data is the culprit.

1) Typographical errors in the batch files invoked during boot-up (Autoexec.bat and Startxxx.bat) and the network initialization file (System.ini) are easy to check and eliminate.
2) The Test Client name must be identified in both LMHOSTS and HOSTS.
3) Test Client name must be 12 characters or less in length and start with an alpha character.

If there are no data errors, the Test Client can be pinged by its IP address and computer name.

1) Not being able to ping by IP address is an indicator of a network connectivity or firewall issue.
2) Not being able to ping by name is an indicator of a typo in SYSTEM.INI or LMHOSTS.

Invalid Permission w/Server or Folder

Networking client will report error 53 if the logged in user does not have privilege to access that file server and/or shared folder. In the case of a Test Client acting as a server, the default is to have a local user login from the DOS controller. Both security and share permissions need to be checked on the folder being shared (TCSHARE is default share of RDS Intranet) to ensure the desired users have permission.

If Test Client is part of a workgroup instead of a domain, the folder must be shared with permission for network clients to have full control.

Password Not Complex Enough

Error 53 also occurs if the user was not able to logon even though it appeared as if the login was successful. This usually occurs when the password in Username.PWL in the network folder does not match that on the Test Client. It can also occur when passwords match but security settings of the Test Client and/or domain are such that the password being used isn't valid. For example, the password being used isn't long enough or is missing special characters.

In other words, even a local user password must conform to a password acceptable to the domain.

Password errors also occur because of security differences that are resolved by changing the Test Client security policies found in the security options folder:

Start → Programs → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Options

1) Domainmember: Digitally encrypt or sign secure channel data (always)—Set to Disabled.
2) Microsoft network server: Digitally sign communications (always)—Set to Disabled.

Error 86: The Specified Network…

Error "The specified network password is not correct", usually occurs because of incorrect passwords:

1) The Username.PWL file in the network folder does not have the correct password or domain information. A new PWL is created by deleting the existing one and re-logging in.
2) Username and/or password used to login does not match what exists on the Test Client. A local user with the correct password must have been set-up on the Test Client.

Error 36: The System Has…

Error 36, "The system has detected an overflow in the sharing buffer", is caused by a security policy conflict between DOS and Windows that is resolved by changing the Test Client security policies found in the security options folder:

Start→Programs→Administrative Tools→ Local Security Policy→Security Settings→ Local Policies→Security Options

1) Microsoft network client: Digitally sign communications (always)—Set to Disabled.
2) Microsoft network server: Digitally sign communications (always)—Set to Disabled.
3) Microsoft network server: Digitally sign communications (if client agrees)—Set to Disabled.