Exchange 2003 Mailflow – Part II Troubleshooting

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article I will show you how to Troubleshoot Message flow within the Exchange Organization. This is part two of a two part article. Part one deals with the basics of message delivery and transmitting from Outlook to Exchange and between Exchange Servers, part two of the article will try to help you troubleshooting e-mail delivery and message flow.

Let's begin

There are several places and tools which could help you to find the reason for failed or delayed message delivery. I will show you some basic steps that should be your first place where to start Troubleshooting. After reading this article and playing with these tools you should be able to troubleshoot E-Mail message delivery.

Queues

If you are looking for E-Mail messages which was not delivered to their recipients, one of your first places to look where the Message is gone is the Queue Viewer. You can find the Queue Viewer in the Exchange System Manager directly under the Server Node.
There are several Queues from interest and you should have a look at the State of the Queues and the Number of messages in the Queue. If there are any messages in the Queue you can select the Queue and you will see more information about possible problems in the Info pane. If you right click the Queue you can force the connection if the problem is temporarily.

Explanation of the Queue Types

Here is an explanation of the Queue Types from Henrik Walthers article about Exchange 2003 Queue Viewer improvements.

DSN messages pending submission
This folder contains Delivery Status Notifications awaiting delivery. Its primarily used for NDR's – Non Delivery Reports.

Failed message retry queue
Contains outbound messages which couldn't be delivered to their destination but will be given another attempt.

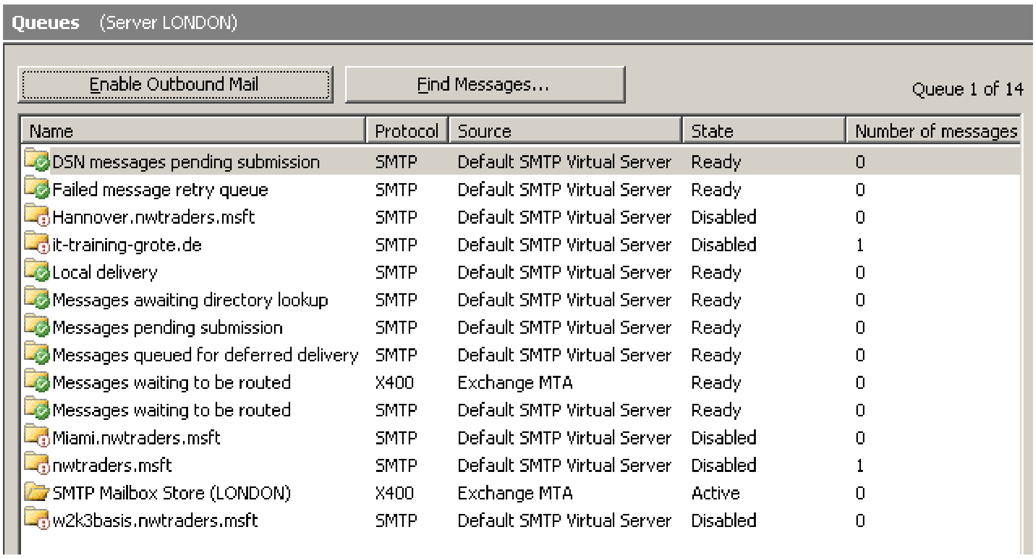
Local delivery
Contains inbound messages for delivery to mailboxes on the Exchange server.

Messages awaiting directory lookup
Contains inbound messages awaiting recipient lookup in Active Directory.

Messages pending submission
Contains messages accepted by the SMTP virtual server, but hasn't yet been processed.

Messages queued for deferred delivery
Contains messages queued for deferred delivery (later time).

Messages waiting to be routed
Contains outbound SMTP/X400 messages still waiting to be routed to their destination server, when it has been determined the message will be sent.



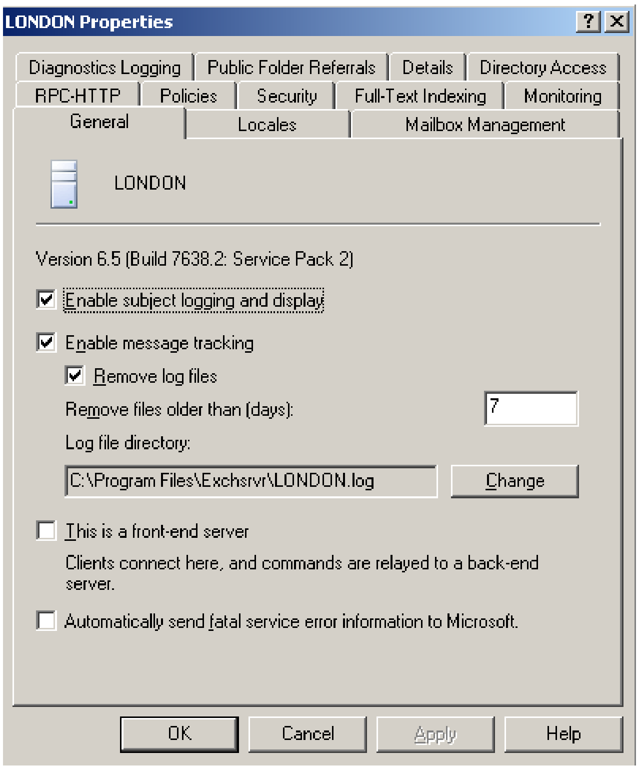
Name	Protocol	Source	State	Number of messages
DSN messages pending submission	SMTP	Default SMTP Virtual Server	Ready	0
Failed message retry queue	SMTP	Default SMTP Virtual Server	Ready	0
Hannover.nwtraders.msft	SMTP	Default SMTP Virtual Server	Disabled	0
it-training-grote.de	SMTP	Default SMTP Virtual Server	Disabled	1
Local delivery	SMTP	Default SMTP Virtual Server	Ready	0
Messages awaiting directory lookup	SMTP	Default SMTP Virtual Server	Ready	0
Messages pending submission	SMTP	Default SMTP Virtual Server	Ready	0
Messages queued for deferred delivery	SMTP	Default SMTP Virtual Server	Ready	0
Messages waiting to be routed	X400	Exchange MTA	Ready	0
Messages waiting to be routed	SMTP	Default SMTP Virtual Server	Ready	0
Miami.nwtraders.msft	SMTP	Default SMTP Virtual Server	Disabled	0
nwtraders.msft	SMTP	Default SMTP Virtual Server	Disabled	1
SMTP Mailbox Store (LONDON)	X400	Exchange MTA	Active	0
w2k3basis.nwtraders.msft	SMTP	Default SMTP Virtual Server	Disabled	0

Figure 1: Queue Viewer

For Troubleshooting reasons it is also possible to Stop all Outbound Mail if you click the Symbol in the Queue viewer. Please note that the picture above has already stopped Outgoing Mail. I stopped Outbound E-Mail delivery for this article because i would like to show you some Messages in the Queues.

Message Tracking

In my opinion one of the fundamental settings that every Exchange Server should have enabled is the Message Tracking option. The Message Tracking option enables the logging for every E-Mail message and if you enabled it for the message subject too. You should enable message subject tracking only on low utilized Servers. Message subject logging can also be a problematic in Data Security so you should talk with your law department before you implement this feature.



LONDON

Version 6.5 (Build 7638.2: Service Pack 2)

☑ Enable subject logging and display

☑ Enable message tracking

☑ Remove log files

Remove files older than (days): 7

Log file directory: C:\Program Files\Exchsrvr\LONDON.log

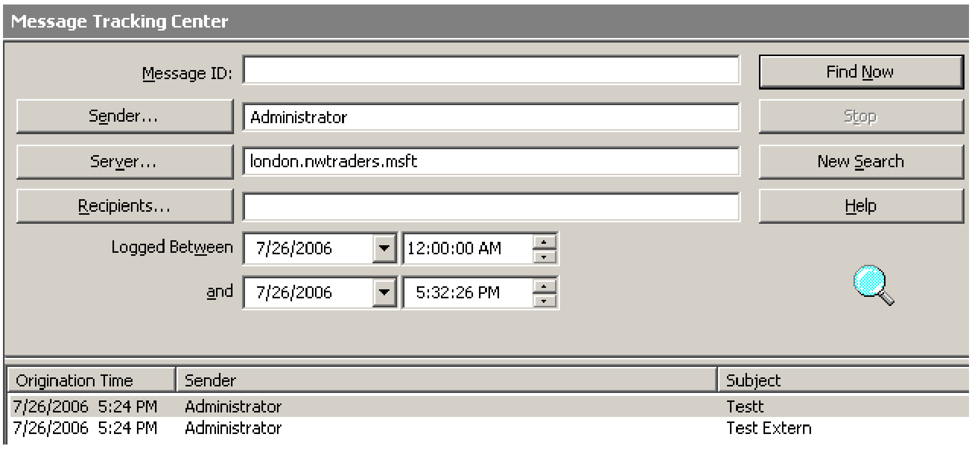
□ This is a front-end server

Clients connect here, and commands are relayed to a back-end server.

□ Automatically send fatal service error information to Microsoft.

Figure 2: Enabling Message Tracking

After you enabled the Message Tracking feature you can use the Message Tracking Feature in the Exchange System Manager to find Messages send to recipients.



Message ID:

Sender: Administrator

Server: london.nwtraders.msft

Recipients:

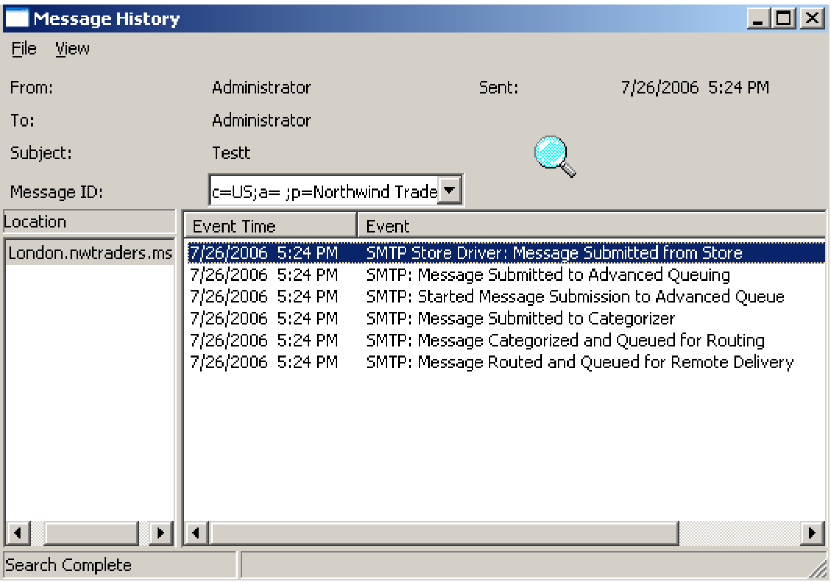
Logged Between 7/26/2006 12:00:00 AM

and 7/26/2006 5:32:26 PM

Origination Time	Sender	Subject
7/26/2006 5:24 PM	Administrator	Testt
7/26/2006 5:24 PM	Administrator	Test Extern

Figure 3: Message Tracking Center

If you select one E-Mail message you can click the Message to see the details about Message Delivery status.



From: Administrator
To: Administrator
Subject: Testt
Sent: 7/26/2006 5:24 PM
Message ID: c=US;a= ;p=Northwind Trade

Location: London.nwtraders.ms

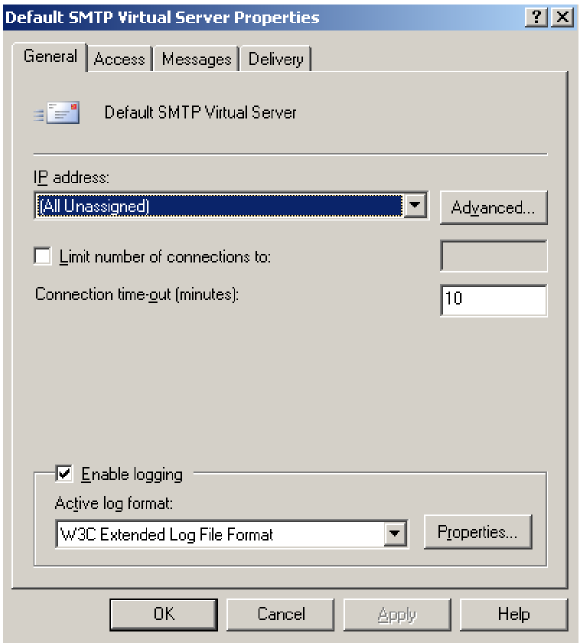
Event Time	Event
7/26/2006 5:24 PM	SMTP Store Driver: Message Submitted from Store
7/26/2006 5:24 PM	SMTP: Message Submitted to Advanced Queuing
7/26/2006 5:24 PM	SMTP: Started Message Submission to Advanced Queue
7/26/2006 5:24 PM	SMTP: Message Submitted to Categorizer
7/26/2006 5:24 PM	SMTP: Message Categorized and Queued for Routing
7/26/2006 5:24 PM	SMTP: Message Routed and Queued for Remote Delivery

Figure 4: Message History

As you can see in the picture above the Message was Submitted from Store, delivered to the AQE, submitted to the Categorizer, Queued for Routing and Queued for Remote Delivery. For an explanation of these terms read my first article about Exchange message flow.

SMTP Logging

With Exchange Server 2003 it is possible to use extended SMTP Logging for Troubleshooting purposes. If SMTP Logging is enabled, Exchange will write every Outgoing Mail through SMTP in a special Logfile located by default in \Windows\System32\Logfiles\SMTPSVC1 where SVC1 is the first Virtual SMTP Server.
You must enable this feature in the Exchange System Manager under the Protocol container from the Exchange Server object.



Default SMTP Virtual Server

IP address: (All Unassigned)

□ Limit number of connections to:

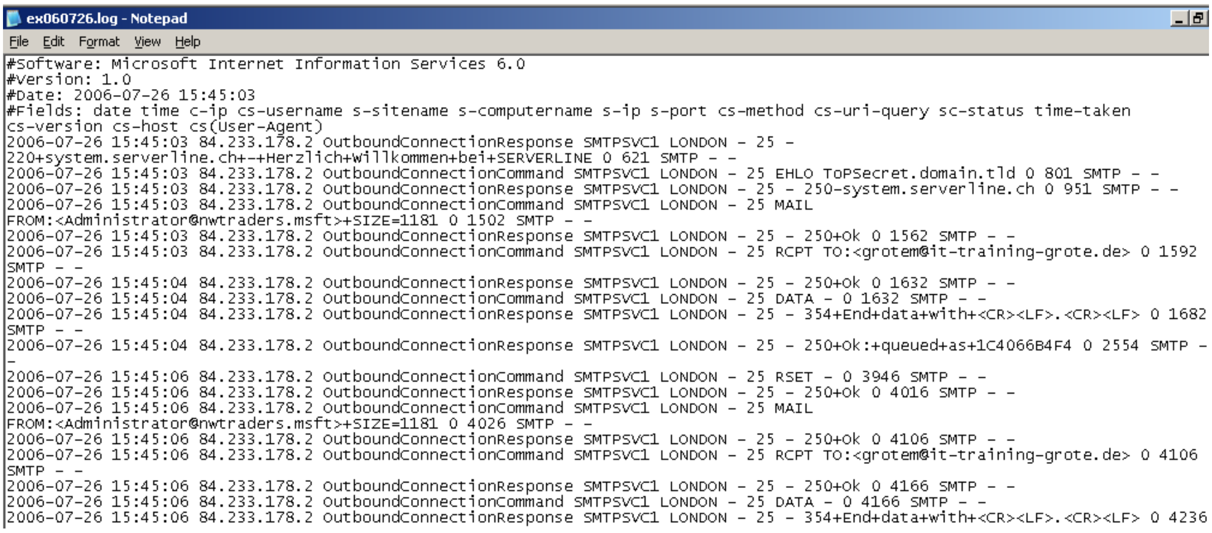
Connection time-out (minutes): 10

☑ Enable logging

Active log format: W3C Extended Log File Format

Figure 5: SMTP Logging

After enabling this feature you can open the generated Logfile and see the detailed steps in the SMTP connection process.
For better viewing and analyzing it is possible to import the Logfile into Microsoft Excel. With Microsoft Excel you can format the Logfile so that it is easier to analyze the Logfile content.



```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2006-07-26 15:45:03
#Fields: date time c-ip cs-username s-sitename s-computername s-ip s-port cs-method cs-uri-query sc-status time-taken
cs-version cs-host cs(User-Agent)
2006-07-26 15:45:03 84.233.178.2 OutboundConnectionResponse SMTPSVC1 LONDON - 25 -
220+system.serverline.ch+-+Herzlich+Willkommen+bei+SERVERLINE 0 621 SMTP - -
2006-07-26 15:45:03 84.233.178.2 OutboundConnectionCommand SMTPSVC1 LONDON - 25 EHLO TOPSecret.domain.tld 0 801 SMTP - -
2006-07-26 15:45:03 84.233.178.2 OutboundConnectionResponse SMTPSVC1 LONDON - 25 - 250-system.serverline.ch 0 951 SMTP - -
2006-07-26 15:45:03 84.233.178.2 OutboundConnectionCommand SMTPSVC1 LONDON - 25 MAIL
FROM:<Administrator@nwtraders.msft>+SIZE=1181 0 1502 SMTP - -
2006-07-26 15:45:03 84.233.178.2 OutboundConnectionResponse SMTPSVC1 LONDON - 25 - 250+Ok 0 1562 SMTP - -
2006-07-26 15:45:03 84.233.178.2 OutboundConnectionCommand SMTPSVC1 LONDON - 25 RCPT TO:<grotem@it-training-grote.de> 0 1592
SMTP - -
2006-07-26 15:45:04 84.233.178.2 OutboundConnectionResponse SMTPSVC1 LONDON - 25 - 250+Ok 0 1632 SMTP - -
2006-07-26 15:45:04 84.233.178.2 OutboundConnectionCommand SMTPSVC1 LONDON - 25 DATA - 0 1632 SMTP - -
2006-07-26 15:45:04 84.233.178.2 OutboundConnectionResponse SMTPSVC1 LONDON - 25 - 354+End+data+with+<CR><LF>.<CR><LF> 0 1682
SMTP - -
2006-07-26 15:45:04 84.233.178.2 OutboundConnectionResponse SMTPSVC1 LONDON - 25 - 250+Ok:+queued+as+1C4066B4F4 0 2554 SMTP -
-
2006-07-26 15:45:06 84.233.178.2 OutboundConnectionCommand SMTPSVC1 LONDON - 25 RSET - 0 3946 SMTP - -
2006-07-26 15:45:06 84.233.178.2 OutboundConnectionResponse SMTPSVC1 LONDON - 25 - 250+Ok 0 4016 SMTP - -
2006-07-26 15:45:06 84.233.178.2 OutboundConnectionCommand SMTPSVC1 LONDON - 25 MAIL
FROM:<Administrator@nwtraders.msft>+SIZE=1181 0 4026 SMTP - -
2006-07-26 15:45:06 84.233.178.2 OutboundConnectionResponse SMTPSVC1 LONDON - 25 - 250+Ok 0 4106 SMTP - -
2006-07-26 15:45:06 84.233.178.2 OutboundConnectionCommand SMTPSVC1 LONDON - 25 RCPT TO:<grotem@it-training-grote.de> 0 4106
SMTP - -
2006-07-26 15:45:06 84.233.178.2 OutboundConnectionResponse SMTPSVC1 LONDON - 25 - 250+Ok 0 4166 SMTP - -
2006-07-26 15:45:06 84.233.178.2 OutboundConnectionCommand SMTPSVC1 LONDON - 25 DATA - 0 4166 SMTP - -
2006-07-26 15:45:06 84.233.178.2 OutboundConnectionResponse SMTPSVC1 LONDON - 25 - 354+End+data+with+<CR><LF>.<CR><LF> 0 4236
```

Figure 6: SMTP Logfile

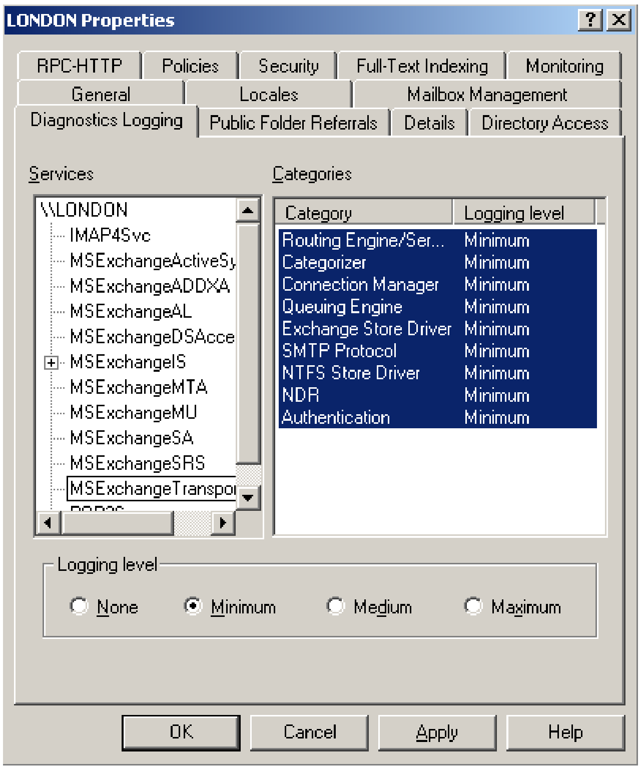
Diagnostic Logging

One other Troubleshooting helper is the Diagnostic Logging of Exchange Server 2003. Diagnostic Logging sets the details that are logged in the Event Viewer about specific Exchange components to a higher Level so more information will be logged in the Application Log of the Event Viewer.

You should enable Diagnostic Logging only for the Time where you troubleshoot specific problems because Diagnostic Logging quickly fills the Event Log. You can set the Logging Level from None to Maximum in the GUI but there is also a Registry Key for setting the Logging Level to Level 7 for SMTP Logging purposes.

You must enable Diagnostic Logging in the Exchange System Manager under the Exchange Server object.

After enabling the Diagnostic Logging feature you can analyze the Event Viewer for specific problems.



Category	Logging level
Routing Engine/Ser...	Minimum
Categorizer	Minimum
Connection Manager	Minimum
Queuing Engine	Minimum
Exchange Store Driver	Minimum
SMTP Protocol	Minimum
NTFS Store Driver	Minimum
NDR	Minimum
Authentication	Minimum

Logging level

○ None ● Minimum ○ Medium ○ Maximum

Figure 7: Diagnostic Logging

Telnet for SMTP

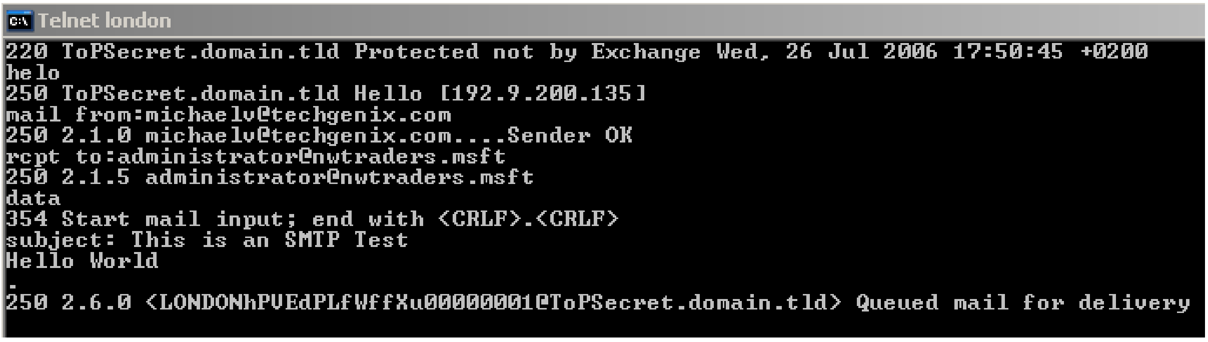
In my opinion is Telnet a great tool to analyze problems with the SMTP Service specially for Message delivery.

If you Telnet into the Exchange Servers SMTP Port you can see every Step that is necessary to establish a communication with the SMPT Service on Exchange.

To start a Telnet session with the Exchange Server open a command prompt and enter:

Telnet Server.Domaene.TLD 25

The following picture shows every Step that is necessary to establish an SMTP connection and to send an E-Mail.



```
220 ToPSecret.domain.tld Protected not by Exchange Wed, 26 Jul 2006 17:50:45 +0200
helo
250 ToPSecret.domain.tld Hello [192.9.200.135]
mail from:michaelv@techgenix.com
250 2.1.0 michaelv@techgenix.com....Sender OK
rcpt to:administrator@nwtraders.msft
250 2.1.5 administrator@nwtraders.msft
data
354 Start mail input; end with <CRLF>.<CRLF>
subject: This is an SMTP Test
Hello World
.
250 2.6.0 <LONDONhPUEdPLfWffXu00000001@ToPSecret.domain.tld> Queued mail for delivery
```

Figure 8: Telnet for SMTP Tests

For more information about Telnet and SMTP read my article.

SMTPDIAG

SMTPDIAG is a simple Tool for testing the SMTP Message flow from Exchange Servers to outside SMTP or Exchange Servers.

You can download SMTPDIAG on the Microsoft Exchange 2003 Tools Website.

After downloading and extracting the SMTPDIAG Tool you can open a command prompt and start SMTPDIAG.

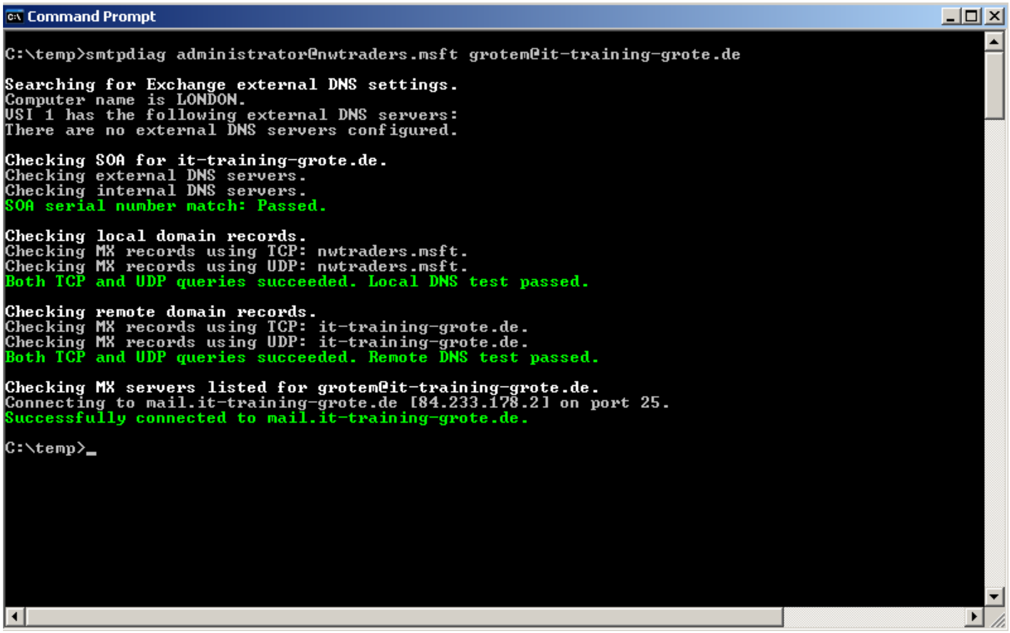
SMTPDIAG has a very simple Syntax as you can see in the following picture.

SMTPDIAG administrator@mwtraders.msft grotem@it-training-grote.de starts the SMTPDIAG process. SMTPDIAG now checks DNS settings and initiate a SMTP connection to the destination system without sending a mail.

SMTPDIAG has only two options.

/V = enables Verbose Mode and shows some more details which are hidden in Standard Mode

[-d target DNS] = This parameter is optional. You can specify the IP address of the target DNS server to use to look up remote MX records. This is often configured as an external DNS server in Exchange. You can configure an external DNS at the Exchange virtual server level but not for the Internet Information Services SMTP service.



```
C:\temp>smtpdiag administrator@nwtraders.msft grotem@it-training-grote.de

Searching for Exchange external DNS settings.
Computer name is LONDON.
VSI 1 has the following external DNS servers:
There are no external DNS servers configured.

Checking SOA for it-training-grote.de.
Checking external DNS servers.
Checking internal DNS servers.
SOA serial number match: Passed.

Checking local domain records.
Checking MX records using TCP: nwtraders.msft.
Checking MX records using UDP: nwtraders.msft.
Both TCP and UDP queries succeeded. Local DNS test passed.

Checking remote domain records.
Checking MX records using TCP: it-training-grote.de.
Checking MX records using UDP: it-training-grote.de.
Both TCP and UDP queries succeeded. Remote DNS test passed.

Checking MX servers listed for grotem@it-training-grote.de.
Connecting to mail.it-training-grote.de [84.233.178.2] on port 25.
Successfully connected to mail.it-training-grote.de.

C:\temp>_
```

Figure 9: SMTPDIAG

For more information about SMTPADIAG read my article.

Conclusion

In this article I tried to show you some Troubleshooting tips if you have problems with E-Mail delivery in your Exchange Organization and to external recipients. The first part of this article should show you the Basics of Message Flow and Delivery in your Exchange Organization.