



Microsoft Exchange: Internet Mail Service and SMTP

**Vincent Valdez
Support Professional
Premier Support
Department
Microsoft Corporation**

Agenda

- ◆ **What is Simple Mail Transfer Protocol (SMTP)?**
- ◆ **What is the Internet Mail Service?**
- ◆ **Basic configuration**
 - **Common problems**
 - **Review recent Knowledge Base articles**
- ◆ **Advanced configuration**
 - **Best practices**
- ◆ **Test your knowledge**
- ◆ **Q & A**

What Is SMTP?

- ◆ RFCs
 - 821 The envelope and stamp
 - 822 The body (actual message)
- ◆ Extensions
- ◆ Jonathan B. Postel (founder of SMTP)



“There we were, designing TCP in this 56-kilobit world, saying things like, ‘well, a reasonable-sized data pack is maybe 500 bytes.’ ”

821 and 822 – SMTP Message

Envelope

From: Bob

To: someone@microsoft.com

Actual Message

From: Bob

To: someone@microsoft.com; George

Subject: Test

Hello!

What Is the Internet Mail Service?

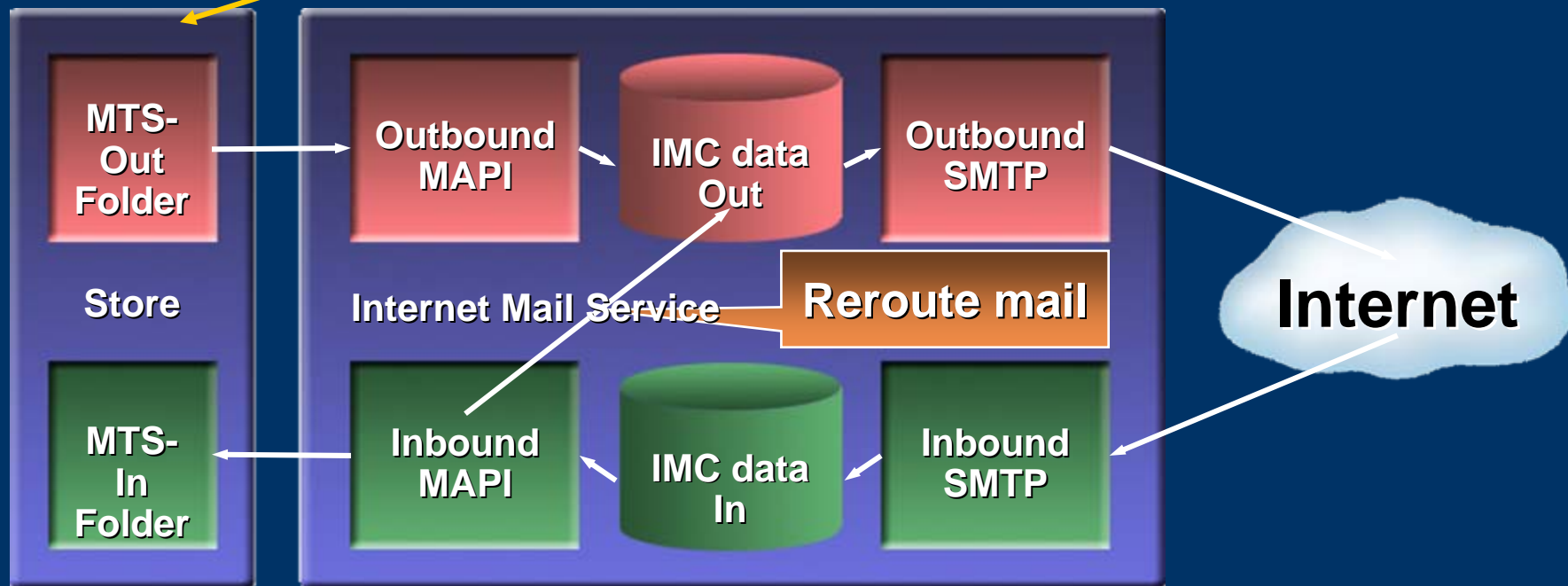
- ◆ **Microsoft Exchange SMTP Provider**
 - **Internet Mail Service = Exchange 5.5 Internet Mail Service with SP3**
- ◆ **Relationship to other Microsoft software**
 - **NTOP (Mail Enable Web Applications)**
 - **MCIS (Built for ISPs)**

What Is the Internet Mail Service? (continued)

◆ Design

- Queues
- Importance of the information store

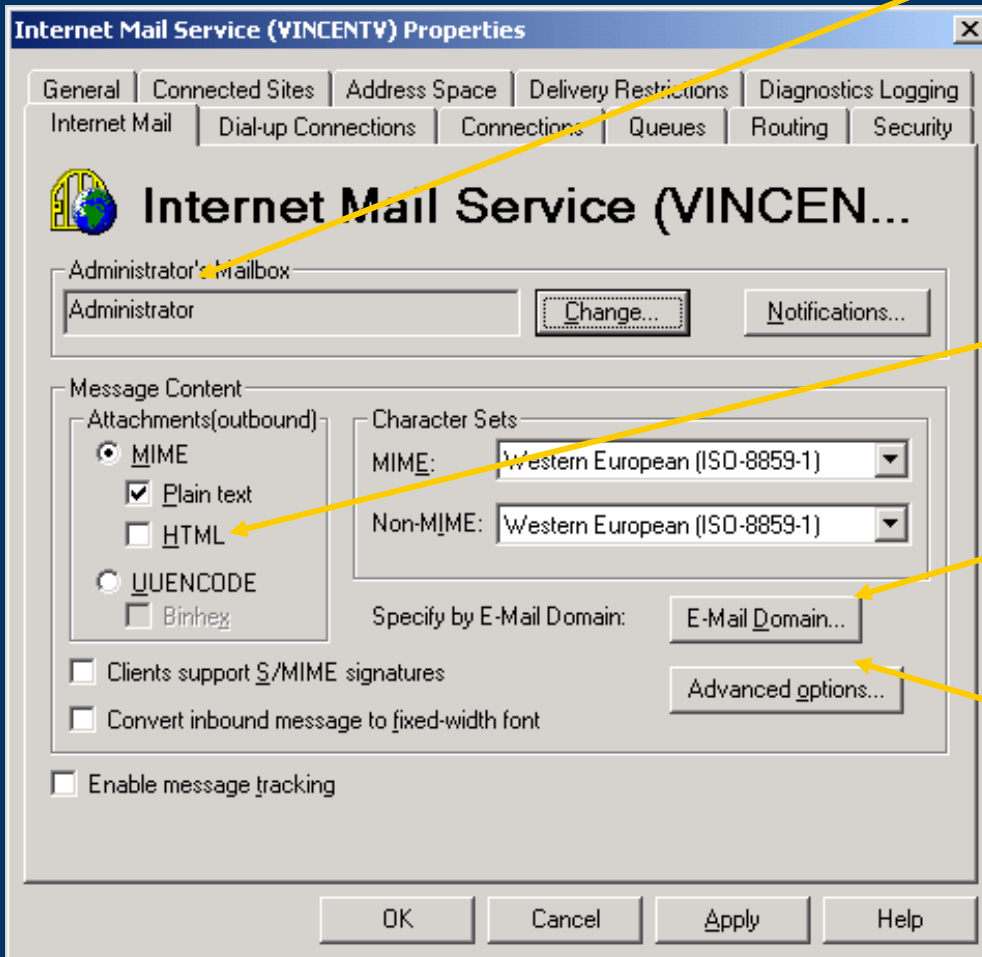
Q233353 – OLE attachments are replaced with <<...>> when sent



Internet Mail Tab

Q201072 – Postmaster @ domain.com

Q245041 – Postmaster incorrectly receives SMTP messages

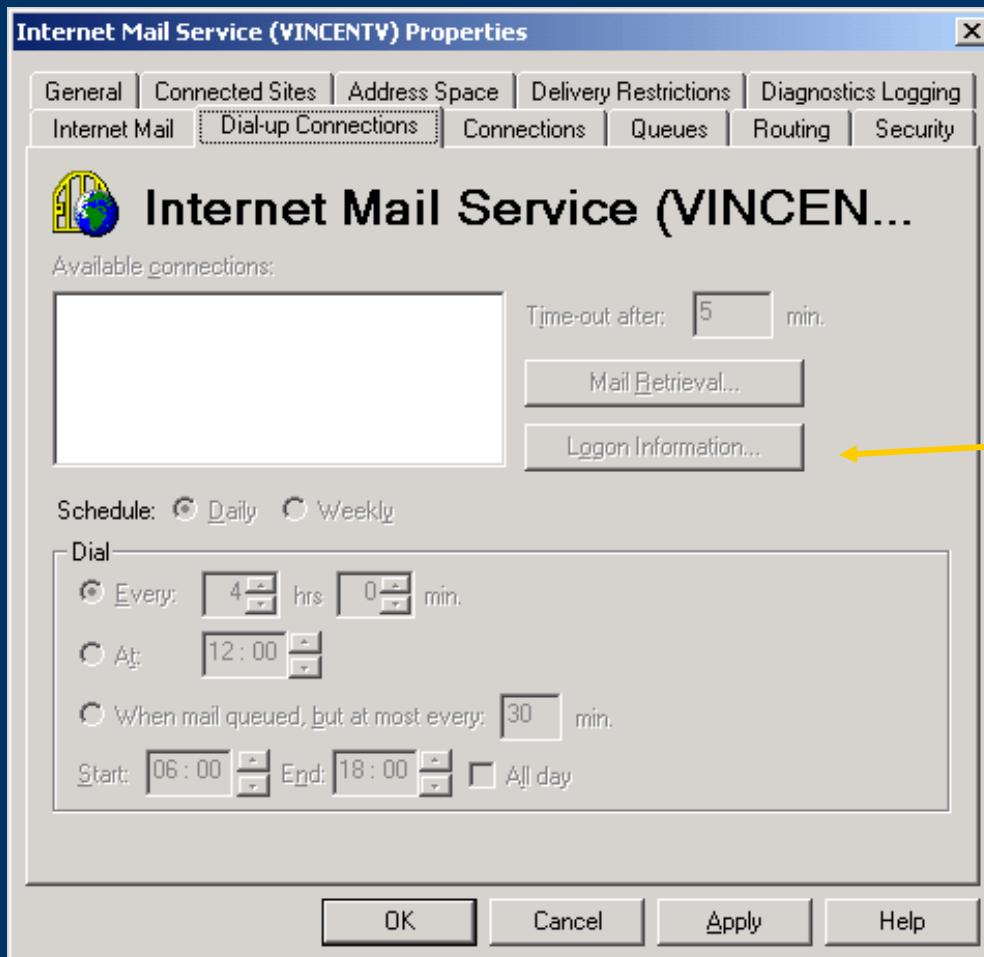


Q251006 – HTML pages sent outside organization

Q243822 – UI problem with e-mail domains button

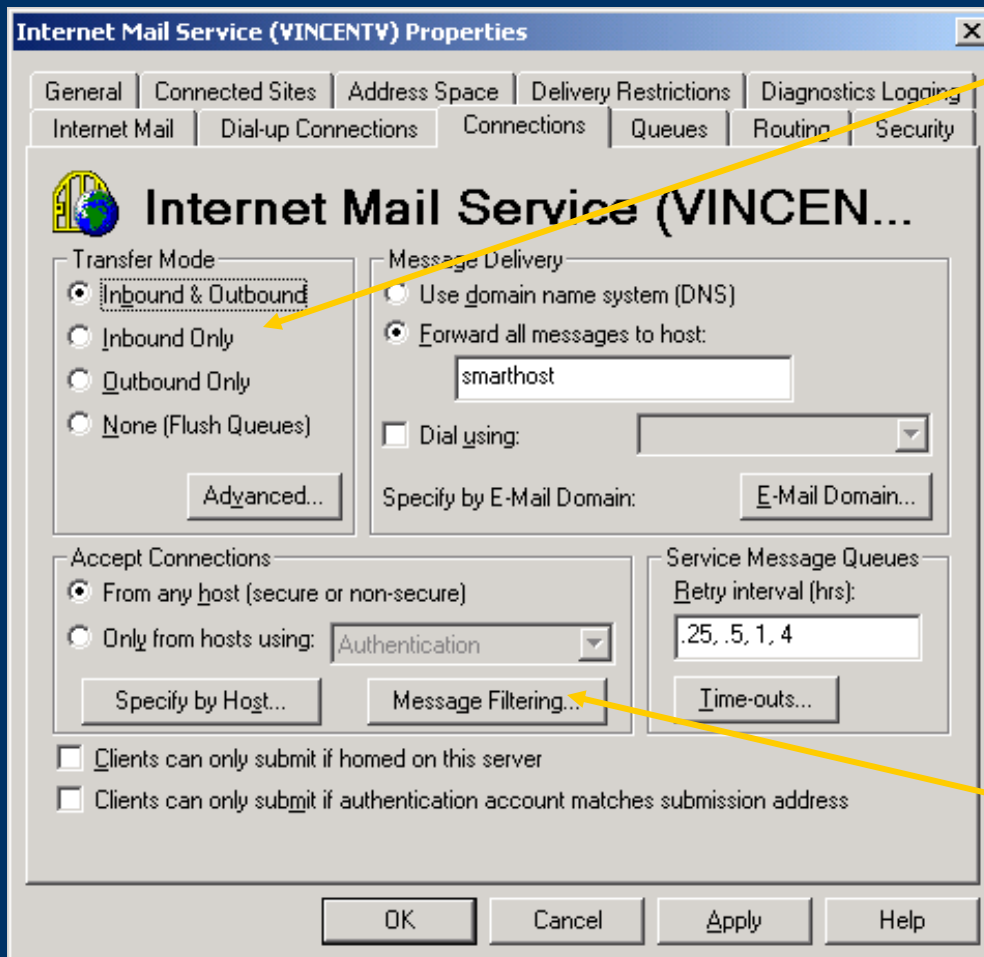
Q216397 – Auto Forward may cause a loop

Dial-up Connections Tab



Q236910 – Cannot open Internet Mail Service Dial-Up Connections Tab on Windows 2000

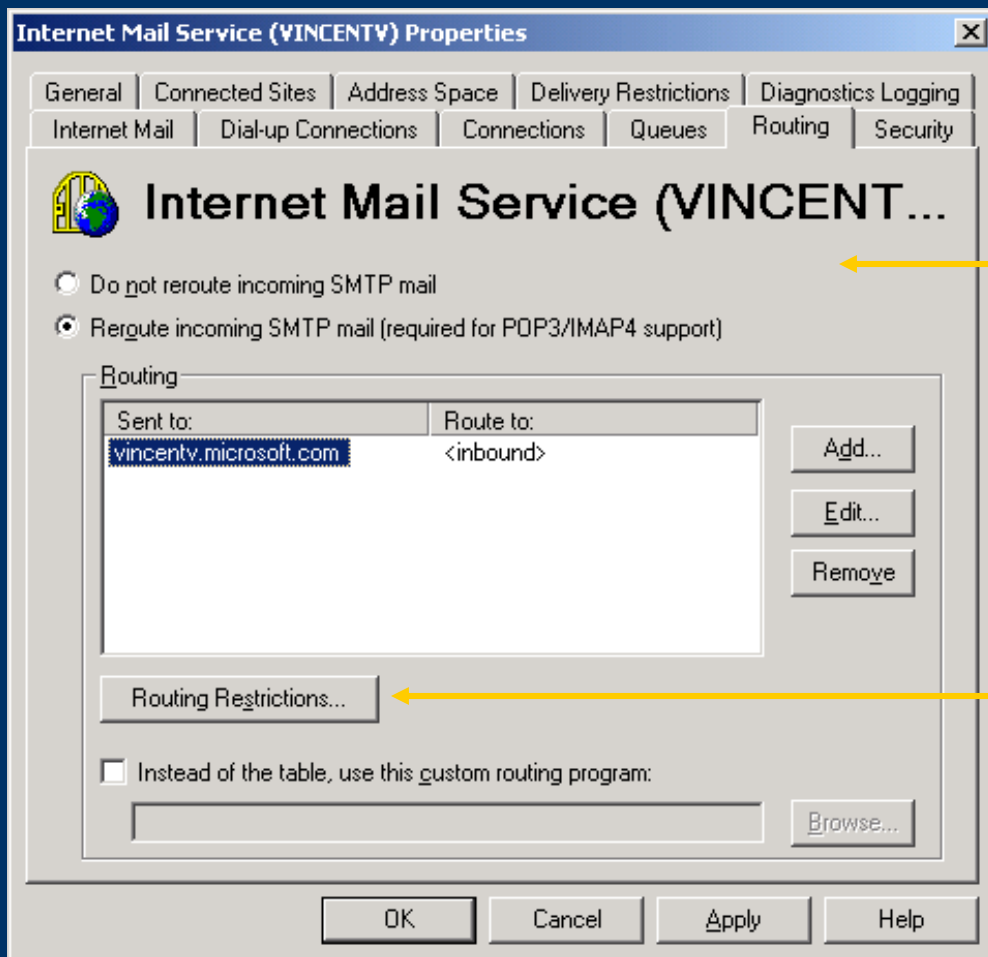
Connections Tab



Q238719 – Inbound only, queues outgoing mail

Q245465 – How to configure message filtering

Routing Tab



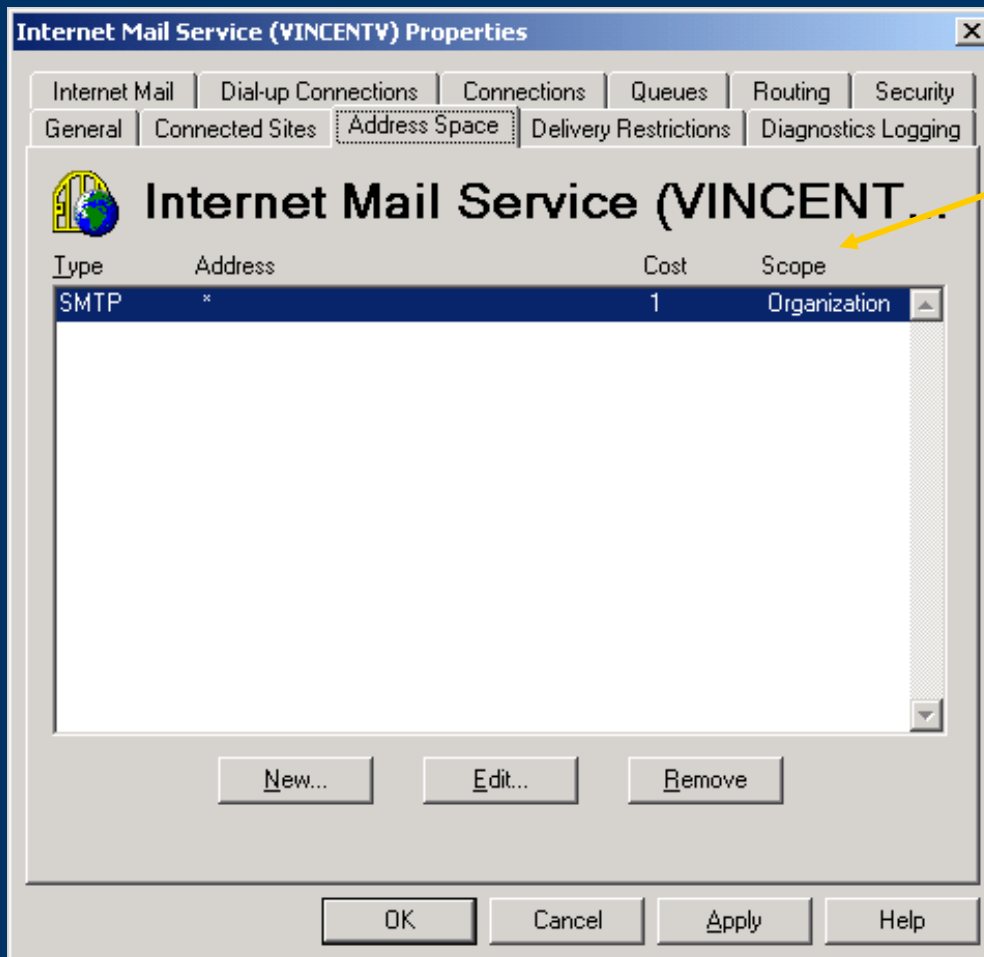
Q174351 – How to create a virtual secondary SMTP address

Q190710 – How to use Internet Mail Service to reroute messages

Q243045 – UI...Problem / routing restrictions are enabled, but are dimmed

Q254214 – Routing restrictions do not work with some antivirus solutions

Address Space Tab



Q229961 – Syntax and address space

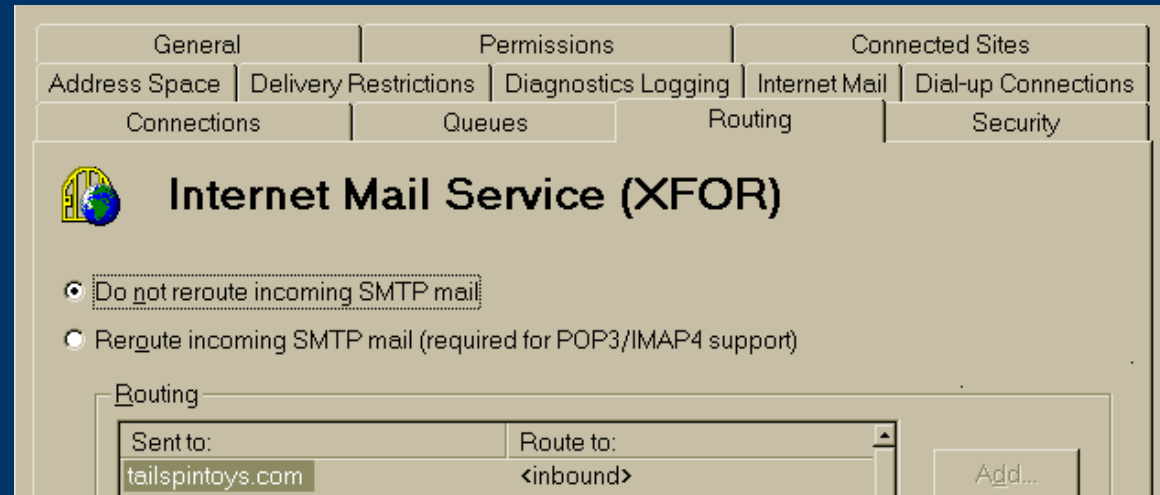
Q239228 – Internet Mail Service that has restrictions does not work

Q152471 – Difference between SMTP:* and SMTP: address space

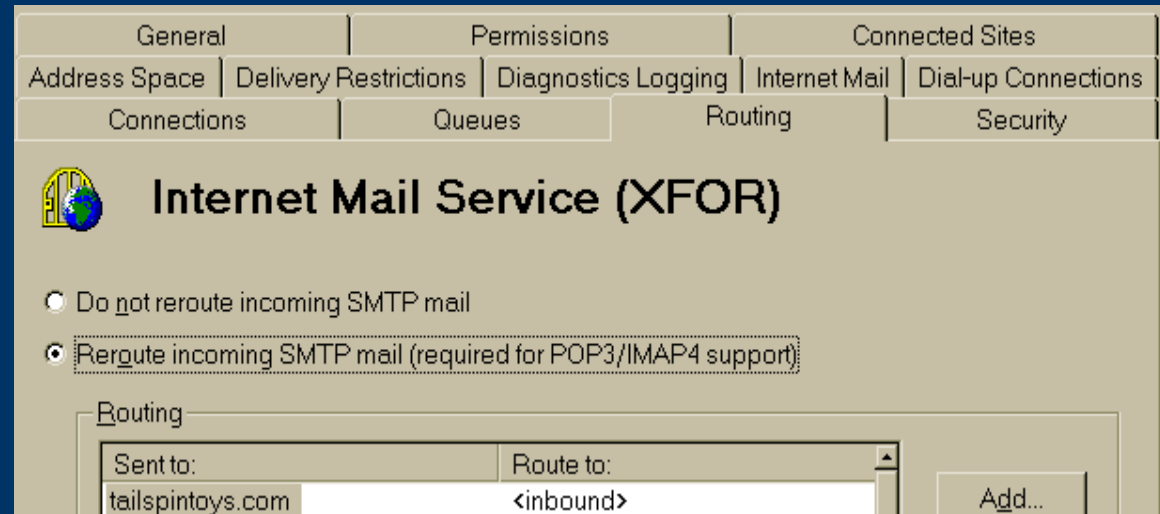
How to Disable Relay

Step 1

Before



After



How to Disable Relay

Step 2

Routing Restrictions...



Routing Restrictions [X]

Specify the hosts and clients that can route mail when the following conditions are met

- Hosts and clients that successfully authenticate
- Hosts and clients with these IP addresses
 - IP Address | Mask
 - Add...
 - Edit...
 - Remove
- Hosts and clients connecting to these internal addresses
 - Internal Address
 - Add...
 - Edit...
 - Remove

Specify the hosts and clients that can NEVER route mail

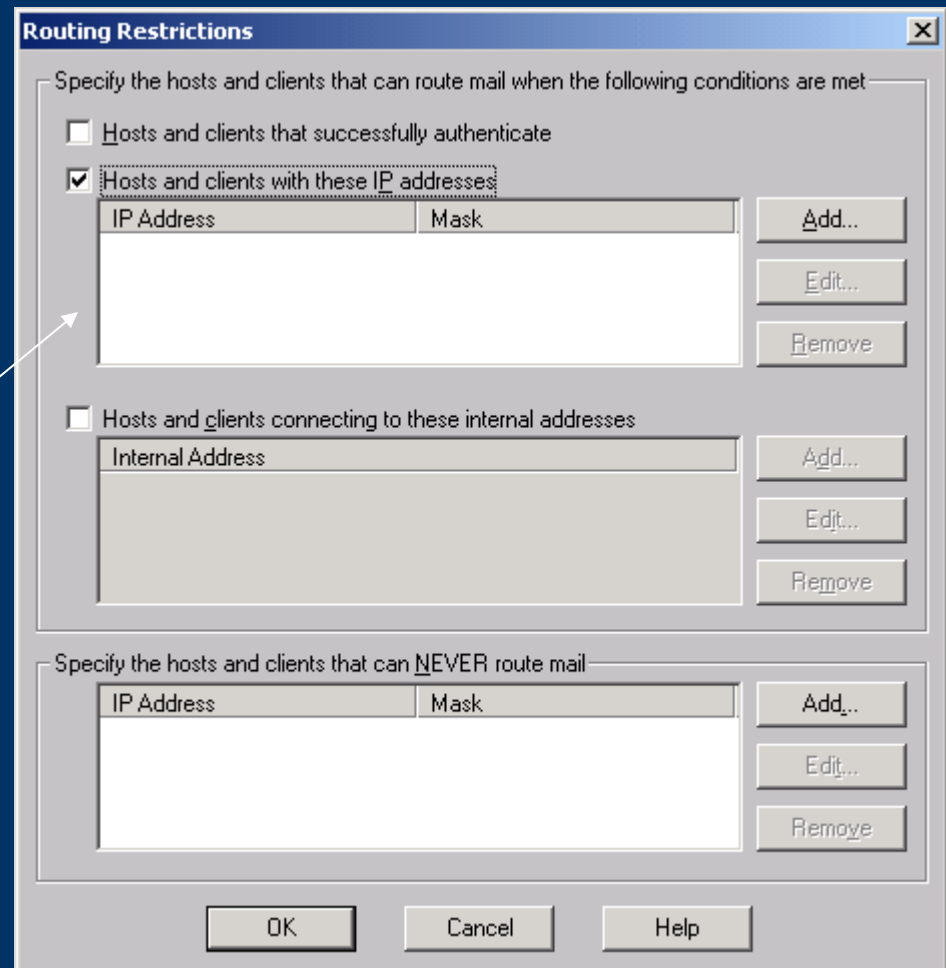
- IP Address | Mask
- Add...
- Edit...
- Remove

OK Cancel Help

How to Disable Relay

Step 3

By selecting **Hosts and clients with these IP addresses**, the Internet Mail Service is configured to allow only IP addresses in the box to relay. This means no one is allowed to relay.



The image shows a Windows dialog box titled "Routing Restrictions". It contains three sections for specifying hosts and clients that can route mail. The first section, "Specify the hosts and clients that can route mail when the following conditions are met", has two options: "Hosts and clients that successfully authenticate" (unchecked) and "Hosts and clients with these IP addresses" (checked). Below the checked option is a table with columns "IP Address" and "Mask", and buttons "Add...", "Edit...", and "Remove". The second section, "Hosts and clients connecting to these internal addresses" (unchecked), has a table with column "Internal Address" and buttons "Add...", "Edit...", and "Remove". The third section, "Specify the hosts and clients that can NEVER route mail", has a table with columns "IP Address" and "Mask", and buttons "Add...", "Edit...", and "Remove". At the bottom are "OK", "Cancel", and "Help" buttons.

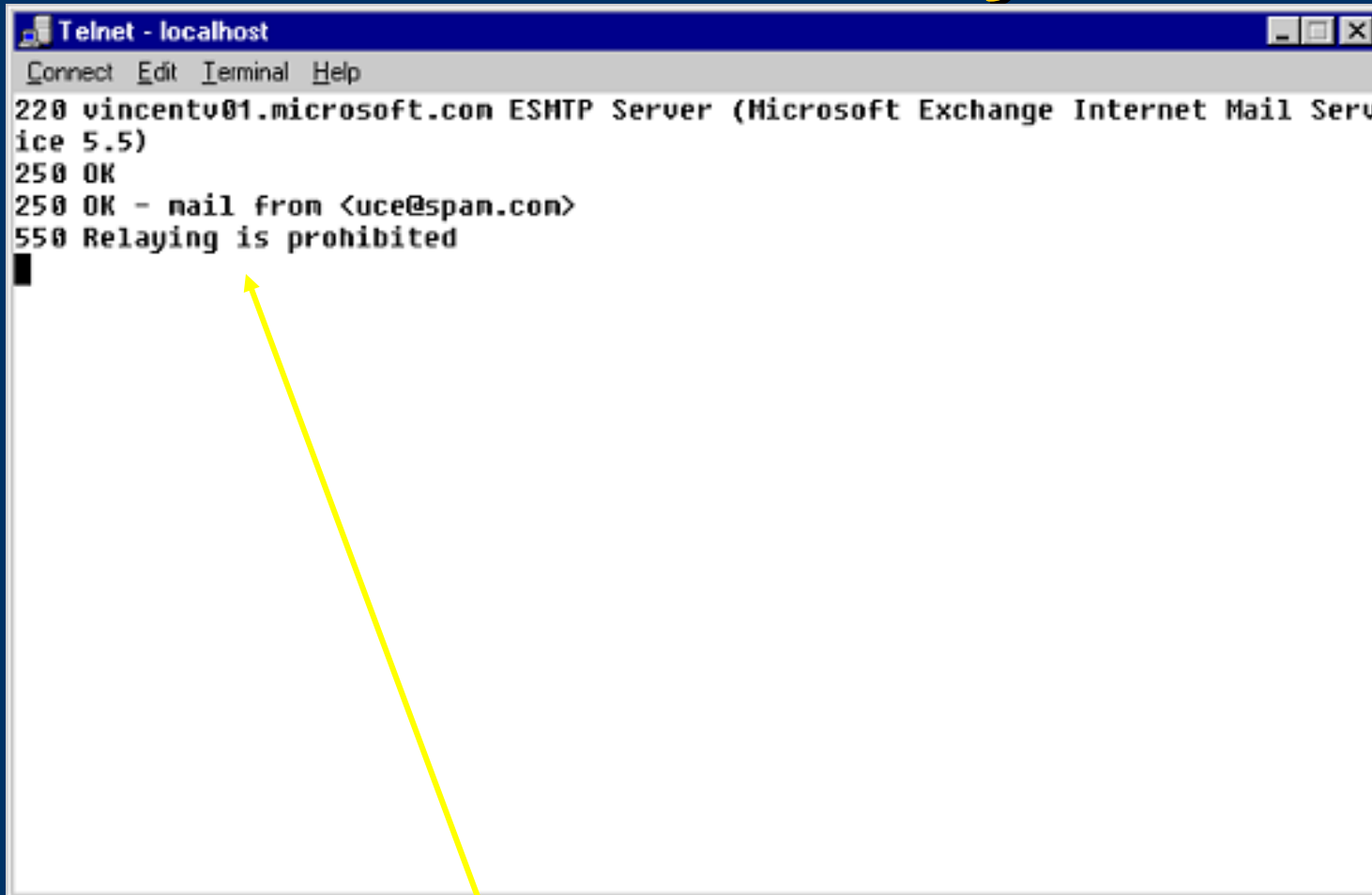
| IP Address | Mask |
|------------|------|
|------------|------|

| Internal Address |
|------------------|
|------------------|

| IP Address | Mask |
|------------|------|
|------------|------|

How to Disable Relay

Step 4

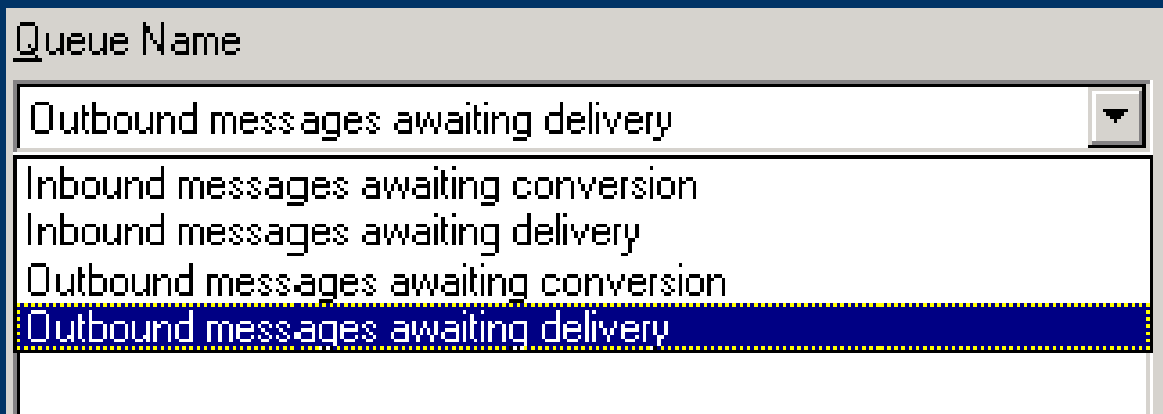


A screenshot of a Telnet terminal window titled "Telnet - localhost". The window has a menu bar with "Connect", "Edit", "Terminal", and "Help". The terminal output shows the following text: "220 vincentv01.microsoft.com ESMTP Server (Microsoft Exchange Internet Mail Service 5.5)", "250 OK", "250 OK - mail from <uce@span.com>", and "550 Relaying is prohibited". A yellow arrow points from the bottom of the terminal to the text "Attempting to relay to another SMTP domain" below the screenshot.

```
Telnet - localhost
Connect Edit Terminal Help
220 vincentv01.microsoft.com ESMTP Server (Microsoft Exchange Internet Mail Service 5.5)
250 OK
250 OK - mail from <uce@span.com>
550 Relaying is prohibited
```





Attempting to relay to another SMTP domain

Server Considerations



Four Queues:

Queues tab in Internet Mail Service

| Color | Scale | Counter | Instance |
|--|-------|-----------------|----------|
|  | 1.000 | Queued Inbound | --- |
|  | 1.000 | Queued MTS-IN | --- |
|  | 1.000 | Queued MTS-OUT | --- |
|  | 1.000 | Queued Outbound | --- |

Perfmon View

Server Considerations (continued)

- ◆ **After Exchange Server 4.0 SP4, the most common issue we resolve is a corrupted message problem:**
 - ***Reason:*** The conversion from MDBEF to SMTP takes place as the message is moved to and from the store (MTS-IN and MTS-OUT).
 - ***Best Practice:*** For enterprise networks, do not put an Internet Mail Service on a mailbox server.

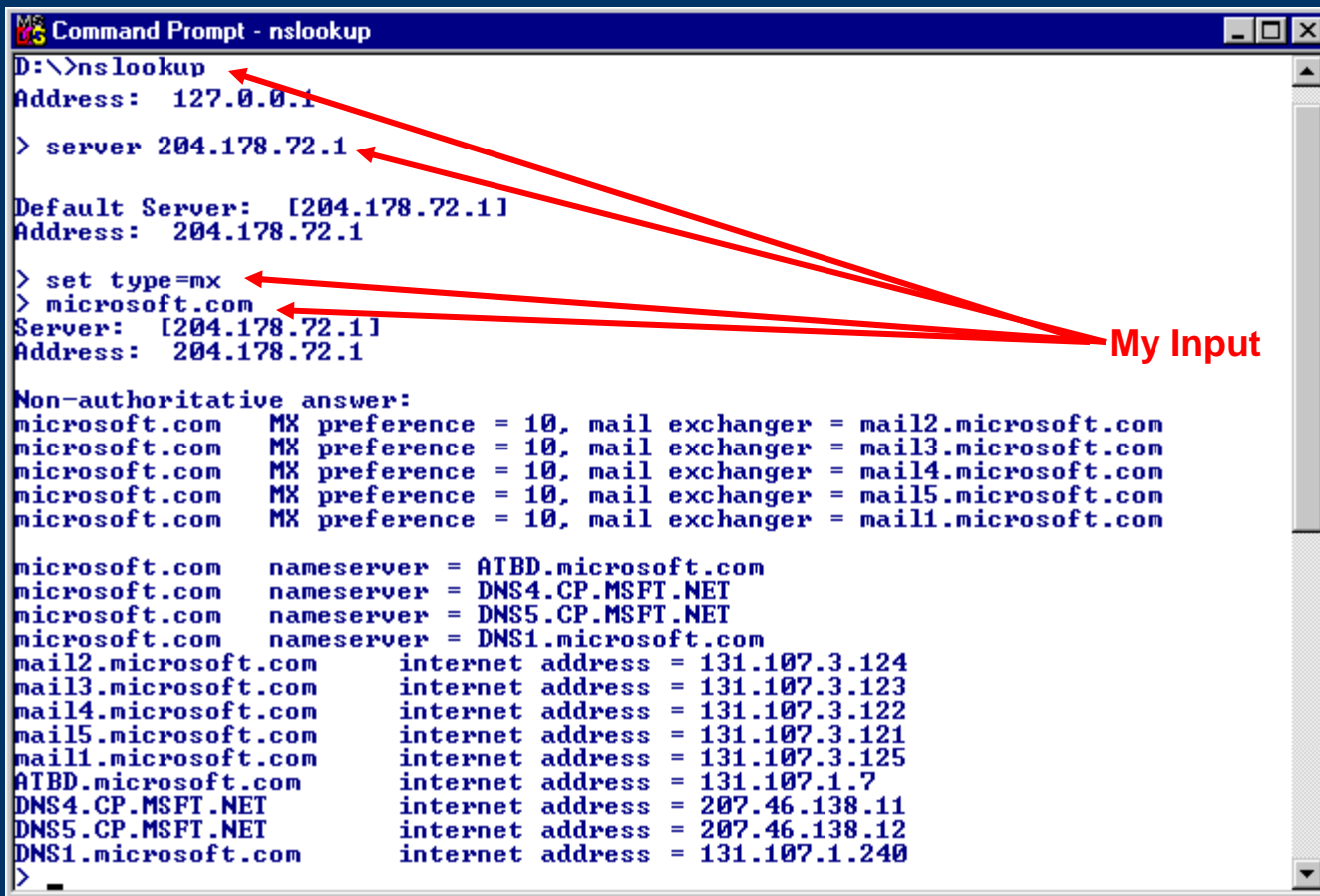
Tools of the Job

| | |
|------------------|------------------------------------|
| Ping | Name resolution and layer 3 |
| Nslookup | DNS reports |
| Telnet | Application layer tests |
| PathPing* | Router tests |
| Netmon | What is really going on? |
| Perfmon | Set alerts for problems |

* PathPing is a Windows 2000 command-line utility

Tools of the Job

Nslookup



```
Command Prompt - nslookup
D:\>nslookup
Address: 127.0.0.1

> server 204.178.72.1

Default Server: [204.178.72.1]
Address: 204.178.72.1

> set type=mx
> microsoft.com
Server: [204.178.72.1]
Address: 204.178.72.1

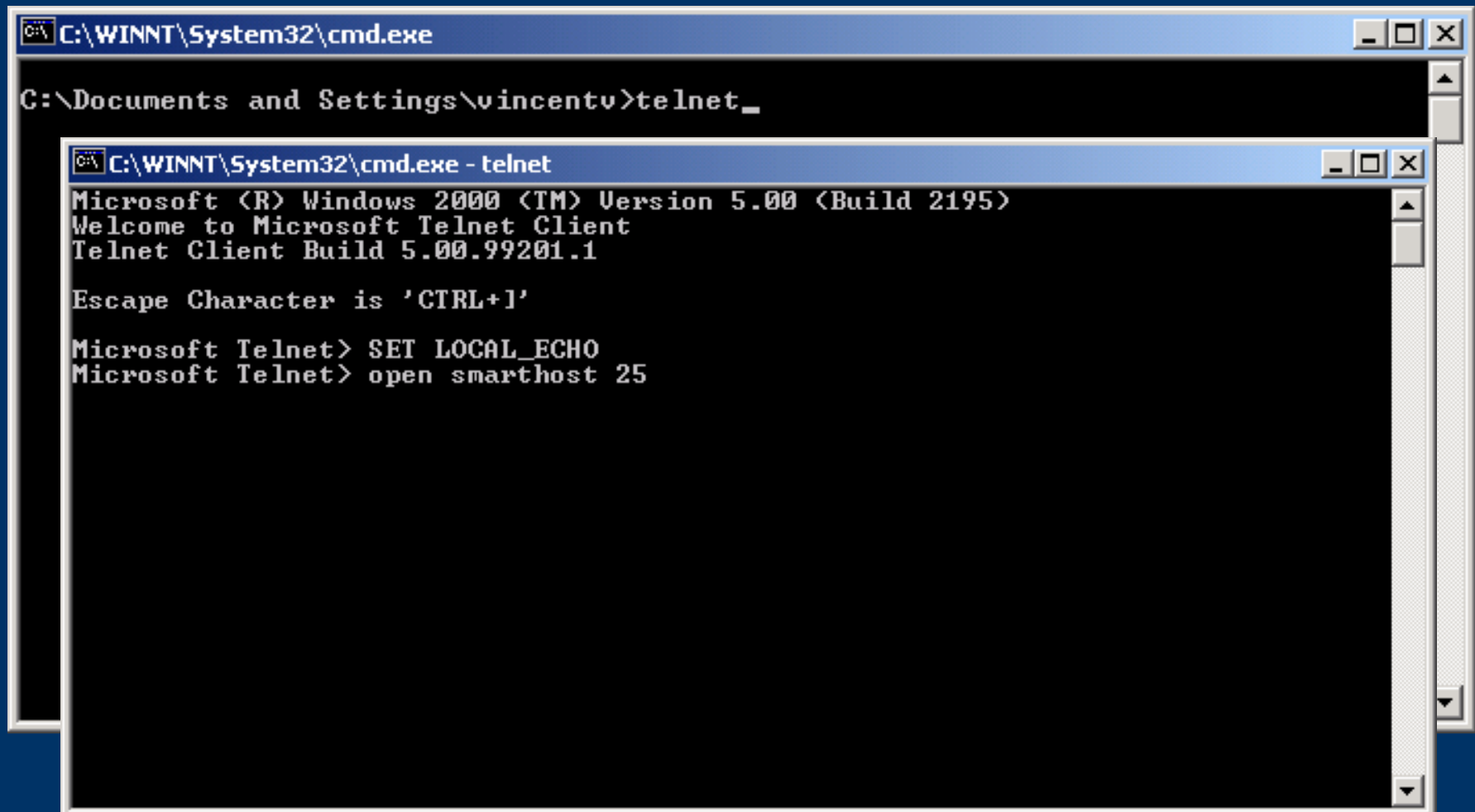
Non-authoritative answer:
microsoft.com MX preference = 10, mail exchanger = mail2.microsoft.com
microsoft.com MX preference = 10, mail exchanger = mail3.microsoft.com
microsoft.com MX preference = 10, mail exchanger = mail4.microsoft.com
microsoft.com MX preference = 10, mail exchanger = mail5.microsoft.com
microsoft.com MX preference = 10, mail exchanger = mail1.microsoft.com

microsoft.com nameserver = ATBD.microsoft.com
microsoft.com nameserver = DNS4.CP.MSFT.NET
microsoft.com nameserver = DNS5.CP.MSFT.NET
microsoft.com nameserver = DNS1.microsoft.com
mail2.microsoft.com internet address = 131.107.3.124
mail3.microsoft.com internet address = 131.107.3.123
mail4.microsoft.com internet address = 131.107.3.122
mail5.microsoft.com internet address = 131.107.3.121
mail1.microsoft.com internet address = 131.107.3.125
ATBD.microsoft.com internet address = 131.107.1.7
DNS4.CP.MSFT.NET internet address = 207.46.138.11
DNS5.CP.MSFT.NET internet address = 207.46.138.12
DNS1.microsoft.com internet address = 131.107.1.240
>
```

My Input

Tools of the Job

Telnet



```
C:\WINNT\System32\cmd.exe
C:\Documents and Settings\vincentv>telnet_

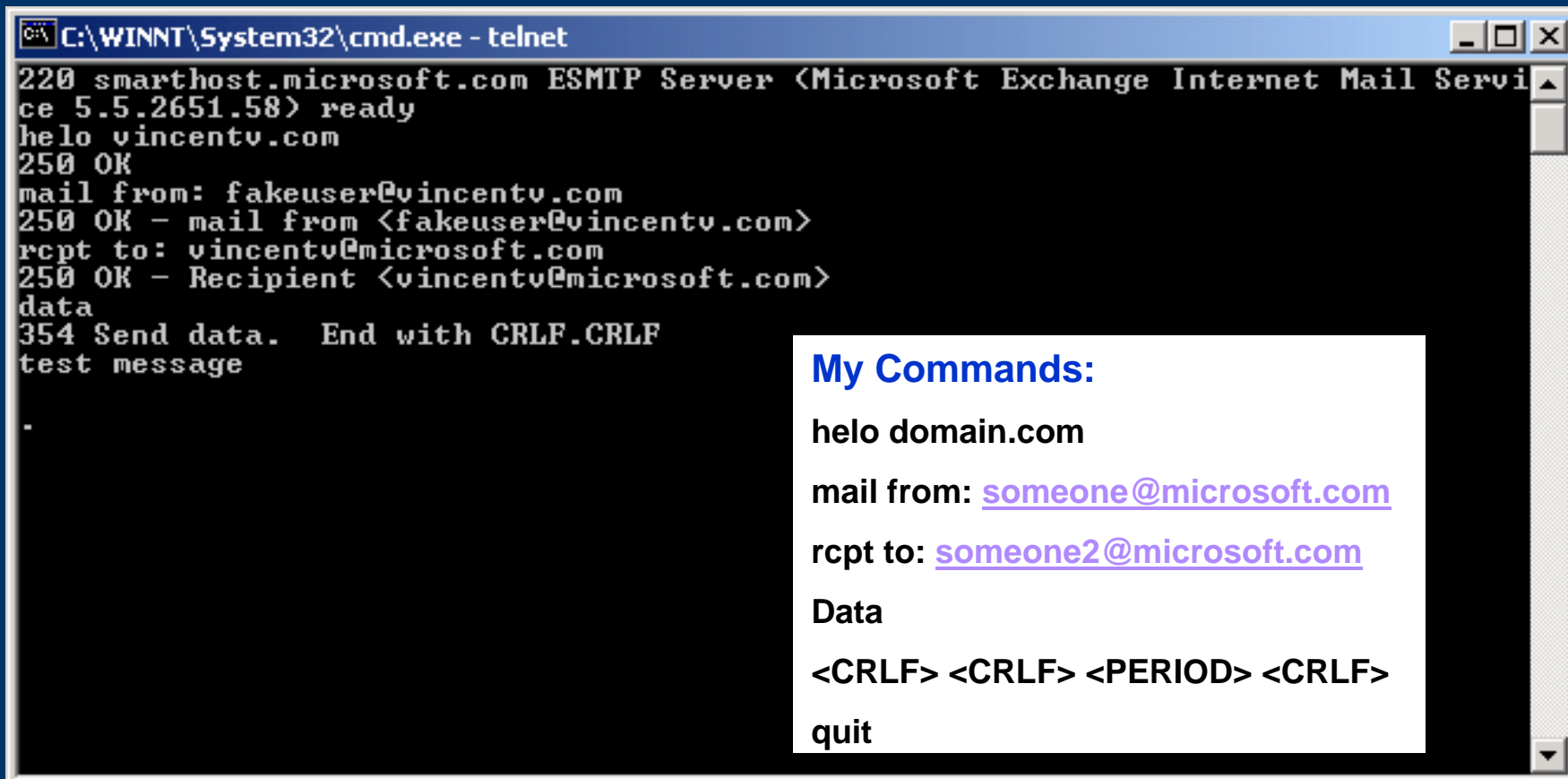
C:\WINNT\System32\cmd.exe - telnet
Microsoft (R) Windows 2000 (TM) Version 5.00 (Build 2195)
Welcome to Microsoft Telnet Client
Telnet Client Build 5.00.99201.1

Escape Character is 'CTRL+]'

Microsoft Telnet> SET LOCAL_ECHO
Microsoft Telnet> open smarthost 25
```

Tools of the Job

Telnet (continued)



```
C:\WINNT\System32\cmd.exe - telnet
220 smarthost.microsoft.com ESMTP Server (Microsoft Exchange Internet Mail Servi
ce 5.5.2651.58) ready
helo vincentv.com
250 OK
mail from: fakeuser@vincentv.com
250 OK - mail from <fakeuser@vincentv.com>
rcpt to: vincentv@microsoft.com
250 OK - Recipient <vincentv@microsoft.com>
data
354 Send data.  End with CRLF.CRLF
test message
.
```

My Commands:

helo domain.com

mail from: someone@microsoft.com

rcpt to: someone2@microsoft.com

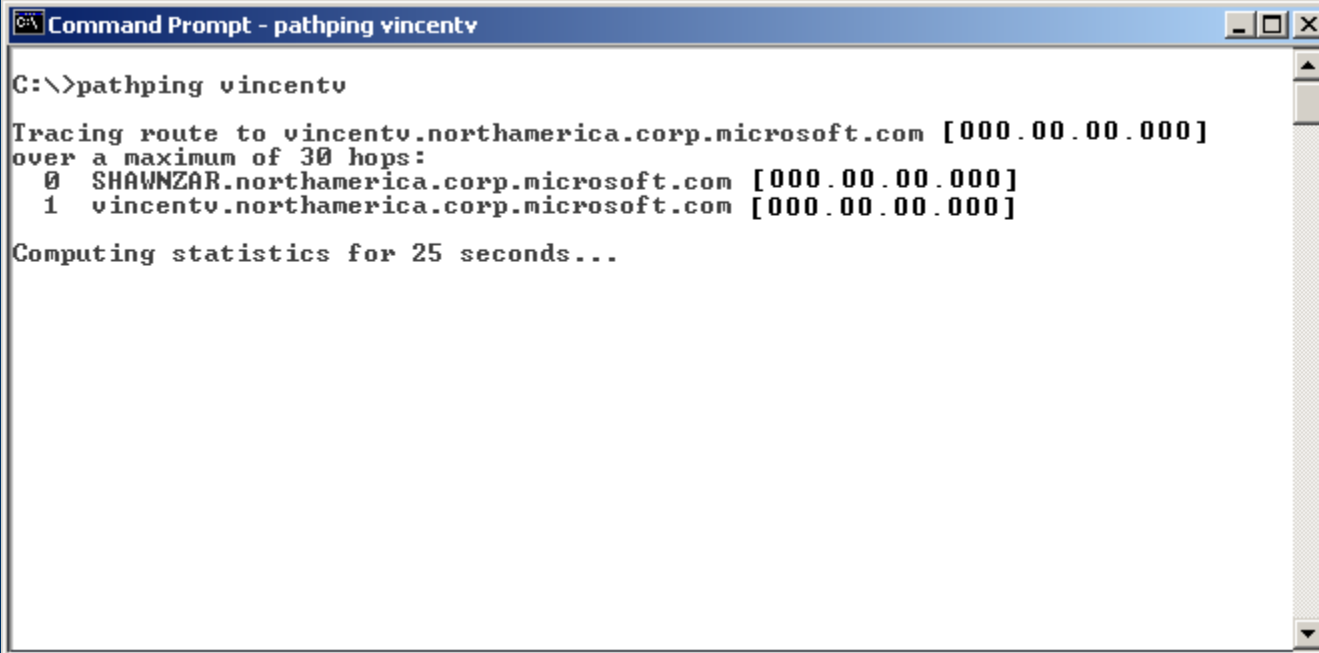
Data

<CRLF> <CRLF> <PERIOD> <CRLF>

quit

Tools of the Job

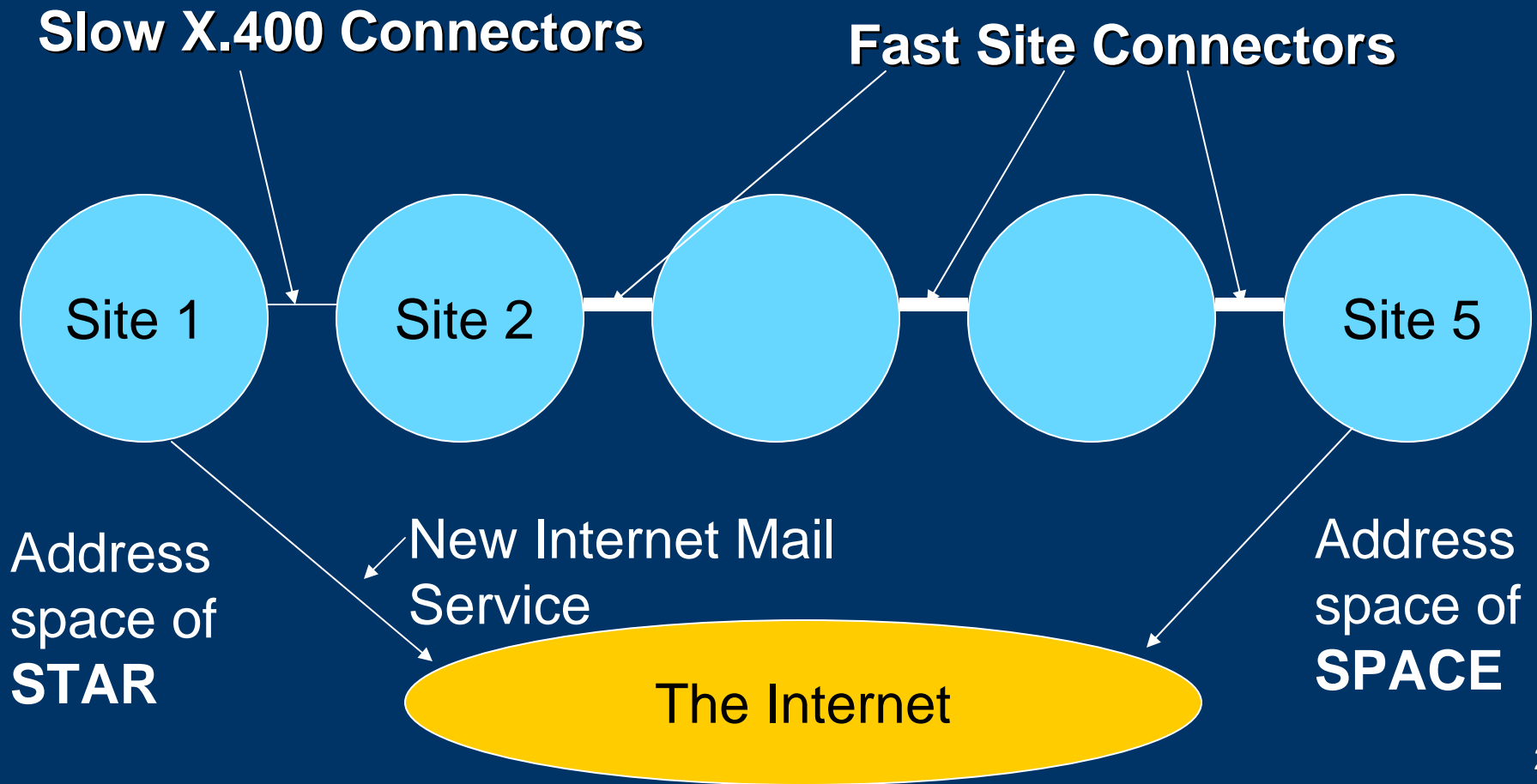
PathPing



```
Command Prompt - pathping vincentv
C:\>pathping vincentv
Tracing route to vincentv.northamerica.corp.microsoft.com [000.00.00.000]
over a maximum of 30 hops:
  0  SHAWNZAR.northamerica.corp.microsoft.com [000.00.00.000]
  1  vincentv.northamerica.corp.microsoft.com [000.00.00.000]
Computing statistics for 25 seconds...
```

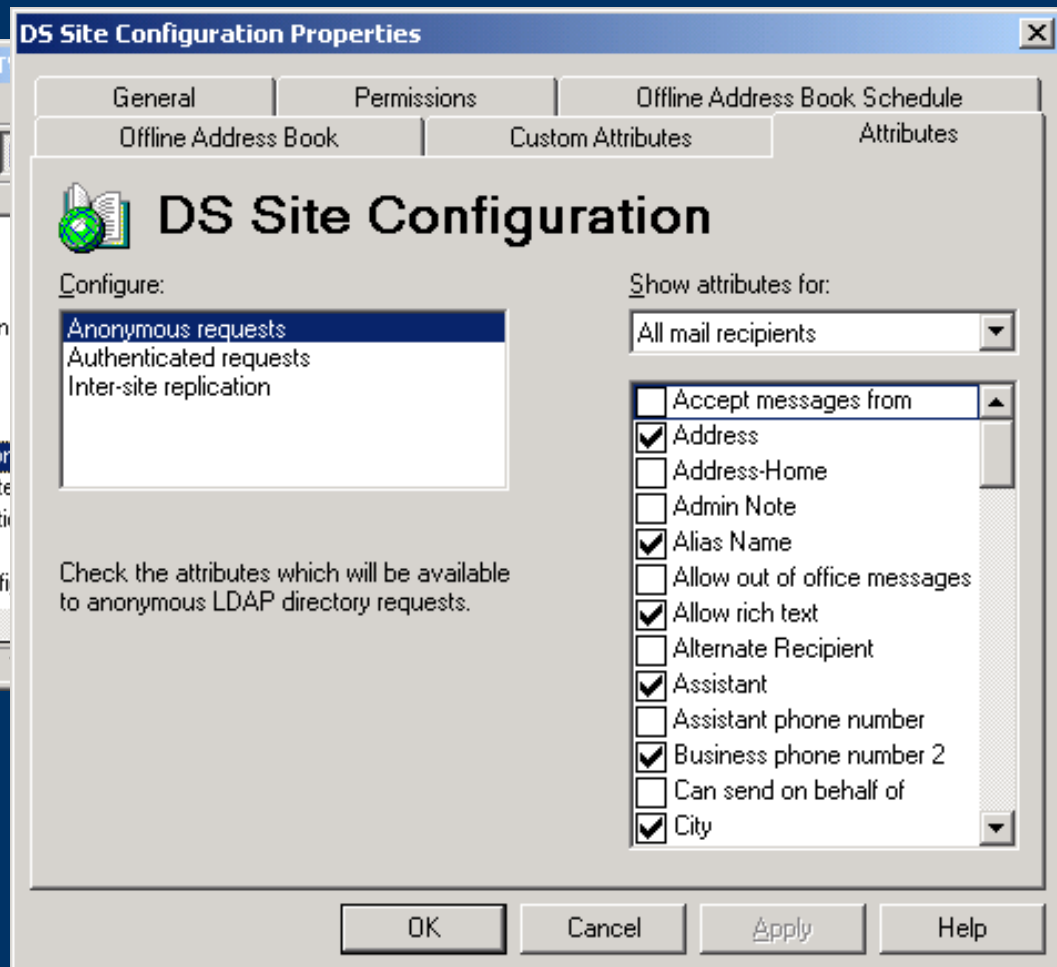
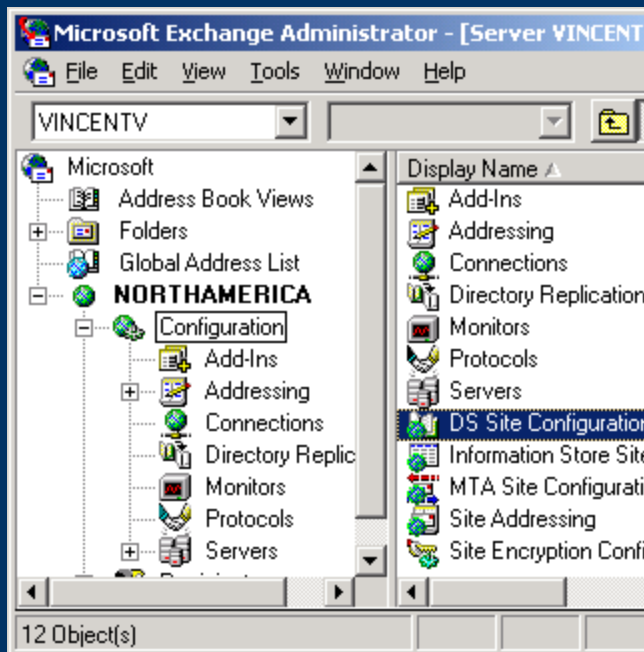
Address Space

(Space vs. Star)



LDAP Configuration

Closing LDAP for Anonymous – Step 1



LDAP Configuration

Closing LDAP for Anonymous – Step 2

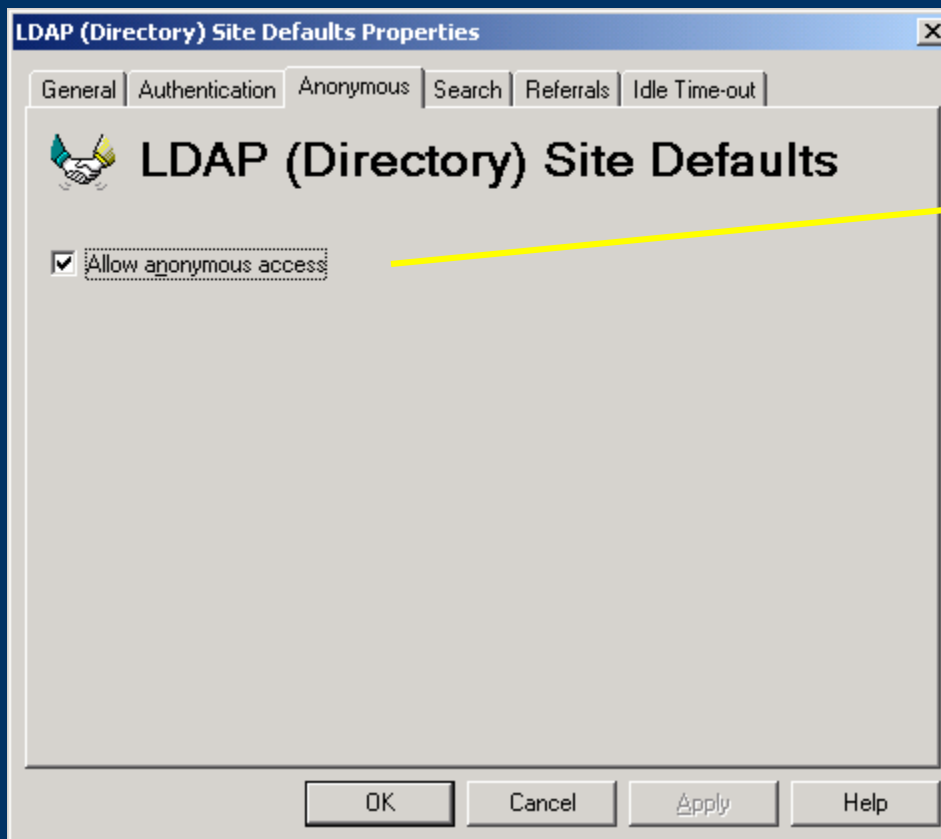
Data that can be collected by an anonymous user by default with LDAP



- ◆ Direct reports
- ◆ Fax number
- ◆ Home phone number
- ◆ Manager
- ◆ Mobile number
- ◆ Pager number
- ◆ SMTP address

LDAP Configuration

Closing LDAP for Anonymous – Step 3



Check box is selected by default.

Hardware - Performance

I/O Recommendations

- ◆ RAID 5 with as many spindles as possible
- ◆ Logs and databases on different physical disks

Network - Performance

Disable Reverse Lookups

The screenshot shows a Microsoft Internet Explorer window displaying the Microsoft Exchange Server help page for "Reverse Resolution". The page title is "Reverse Resolution" and it explains that reverse resolution is used to resolve the host name of the sender in an SMTP message header. It includes a sample message header and instructions on how to disable reverse resolution to improve performance.

Reverse Resolution

You can disable reverse resolution lookup for SMTP mail sent to the Internet Mail Service. Reverse resolution is when the name of the host that delivered an incoming SMTP message is resolved and placed into the message header by the Internet Mail Service.

When an SMTP message is received, the host address is contained in the message header. The header describes the path of the message as it traveled from the host that sent the message to the host that received the message. The following is a sample SMTP message header with return path and time stamps.

```
Received: from GHI.COM by JKL.COM : 27 Oct 96 15:27:39 PST
Received: from DEF.COM by GHI.COM : 27 Oct 96 15:15:13 PST
Received: from ABC.COM by DEF.COM : 27 Oct 96 15:01:59 PST
Date: 27 Oct 96 15:01:01 PST
From: JOE@ABC.COM
Subject: Upgraded Mail System
To: SAM@JKL.COM
```

Disabling Reverse Resolution

You can increase Internet Mail Service performance by disabling reverse resolution. When reverse resolution is disabled, the Internet Mail Service will not resolve the host name in the upper most Received From portion of the SMTP message header. If the address is in Internet Protocol (IP) form, the address will remain as such.

1. Open Regedit.exe or Regedit32.exe.
2. Open the following registry keys: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeIMC\Parameters
3. If you are using Regedit.exe, choose **Edit**, and then choose **New DWORD Value**. If you are using Regedit32.exe, choose **Edit**, and then choose **Add Value**.
4. If you are using Regedit.exe, type **DisableReverseResolve**, under **Value data**, type 1. If you are using Regedit32.exe, type **DisableReverseResolve**; under **Data Type**, choose REG_DWORD.
5. If you are using Regedit32.exe, under **Data**, type 1.

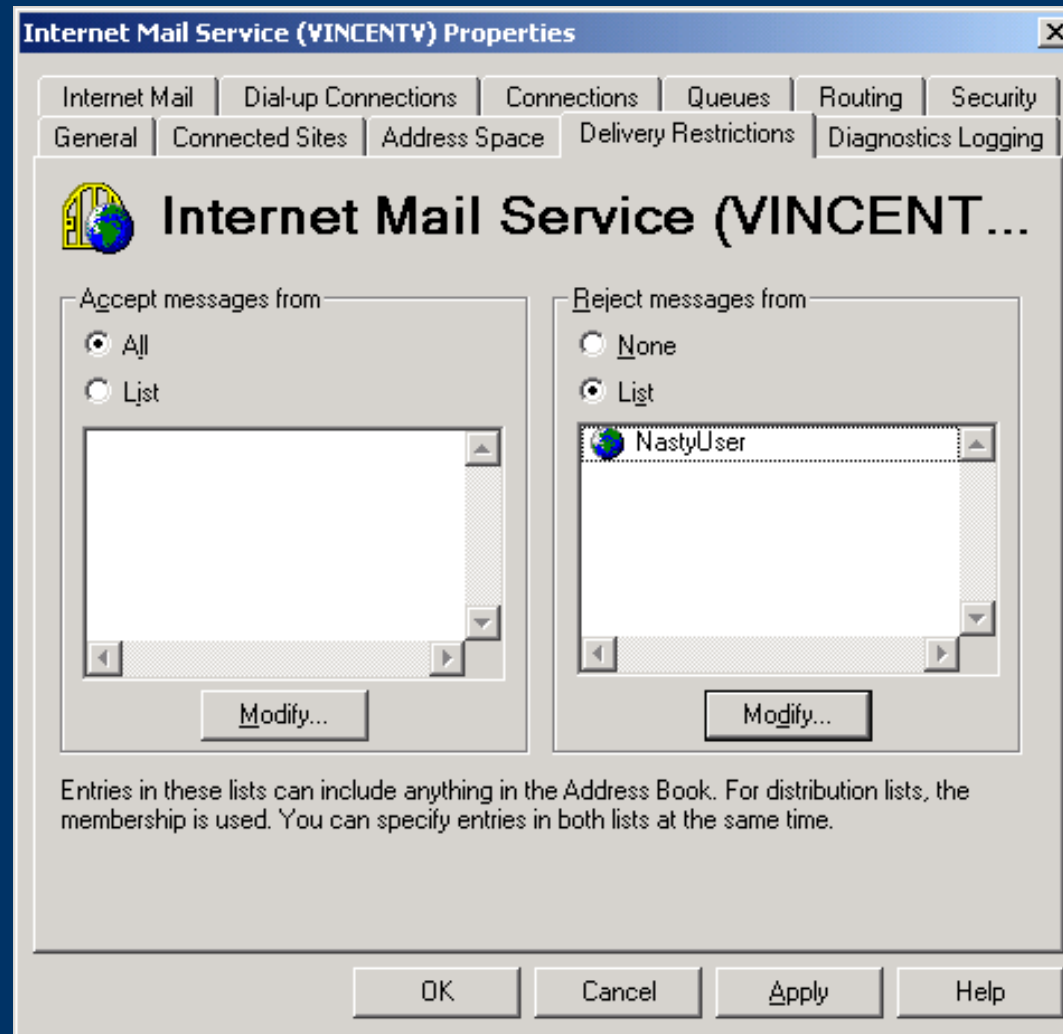
The screenshot shows the Windows Registry Editor window. The left pane shows the tree structure expanded to "My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIMC\Parameters". The right pane shows a list of registry values, with "DisableReverseResolve" selected. The value is a DWORD with a data type of REG_DWORD and a value of 1.

| Name | Data |
|------------------------------|-----------------|
| SMTPWaitForBanner | 0x0000012c (30) |
| SMTPWaitForDataBlock | 0x00000258 (60) |
| SMTPWaitForDataInitiation | 0x00000078 (12) |
| SMTPWaitForDataTermina... | 0x00000258 (60) |
| SMTPWaitForEtrn | 0x0000012c (30) |
| SMTPWaitForMailFrom | 0x0000012c (30) |
| SMTPWaitForRcpt | 0x0000012c (30) |
| SMTPWaitForStartTLS | 0x0000012c (30) |
| SMTPWaitForTurn | 0x0000012c (30) |
| ThreadsPerProcessor | 0x00000003 (3) |
| UseRTFText | 0x00000001 (1) |
| WarnedAboutTCPIPConfig | 0x00000001 (1) |
| DisableReverseResolve | 0x00000001 (1) |

Speed increases but logs are harder to decipher.

1. Test your Knowledge

How do I restrict a specific user's mail from coming in to the Internet Mail Service?

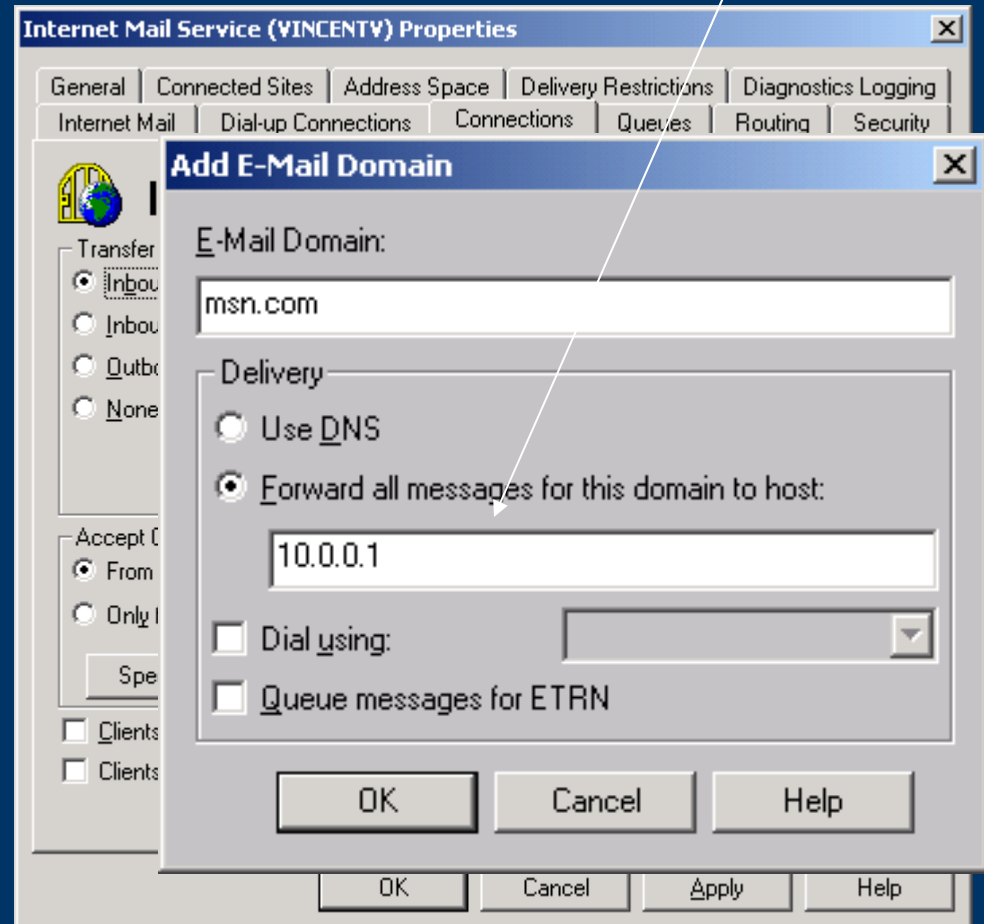
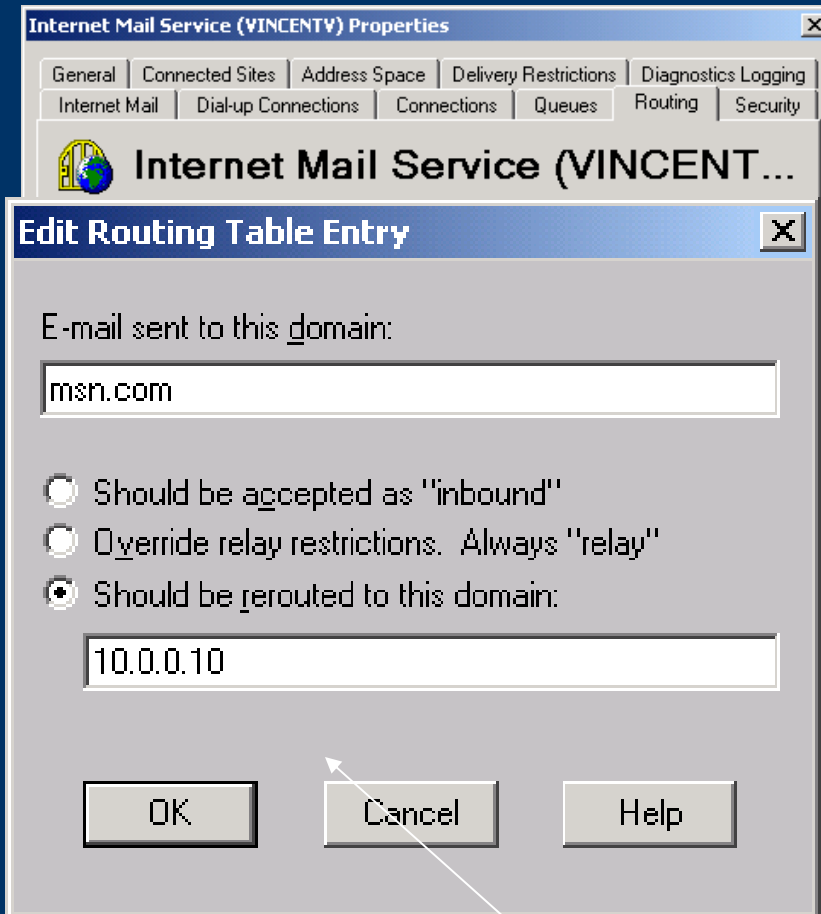


Answers at the end.

3. Test Your Knowledge

Where do you configure all mail for a certain domain to go to a certain host?

Connections tab



Answers at the end.

Routing tab

4. Test Your Knowledge

- ◆ What do the following SMTP errors (reply codes) mean?
 - 442
 - 552
 - 550
 - 454

Answers at the end.

5. Test Your Knowledge

- ◆ **What can NTLM be used for on an Exchange-to-Exchange Internet Mail Service connection?**
 - **Authentication**
 - **Encryption**
 - **Both**

Answers at the end.

Test Your Knowledge: Answers

Answers:

1. Use the Message Filtering button on the Connections tab. See article Q245465 for more information.
2. The answer is number 6. The alias someone@microsoft.com would only allow mail for someone@microsoft.com to go through. Numbers 1-4 would all be valid for the user called “someone,” but Number 5 would not be valid for any address.
3. For special routing for a certain domain, use the Connections tab – E-Mail Domains button.
4. Reply Codes
 - 4xx means temporary problem
 - 5xx means permanent problem
 - x4x means system issue
 - x5x Means mail issue
5. The answer *Both*. NTLM can provide RC4 level encryption.

References

- ◆ **White paper: “Inside Exchange Internet Mail Service”**
<http://www.microsoft.com/exchange/55/whpprs/InsideIMS.doc>
- ◆ **How to Replicate Exchange Server Directories Using the Internet Mail Service**
<http://www.microsoft.com/TechNet/exchange/technote/imsrep.asp>
- ◆ **Security Fix for Routing Vulnerability**
<http://www.microsoft.com/TechNet/exchange/tools/imcfix.asp>

References (continued)

- ◆ **Windows NT Magazine: Is Your Exchange Server Relay-Secure?**
<http://www.microsoft.com/TechNet/exchange/relay.asp>
- ◆ **Chapter 10 from *Exchange Server 24Seven*, published by Sybex Inc. - Exchange Internet Interoperability**
<http://www.microsoft.com/TechNet/exchange/2505ch10.asp>



Where do you want to go today?®