

Integrating Sendmail with Teamware Office

Integrating Sendmail with Teamware Office

October 2001
Document Version: 3.1

This document was produced by TeamWARE Group Oy in Helsinki, Finland.
We welcome and consider all comments and suggestions.

Please send them to:
TeamWARE Group Oy
P.O. Box 135
FIN-00381 Helsinki
Finland
Fax number: +358 9 5128 2705
Internet address:
office.team@teamware.com

Teamware Group endeavors to ensure that the information in this document is correct, but accepts no liability for any error or omission in the same.

The development of Teamware Group products and services is continuous and published information may not be up to date. Any particular issue of a product may contain part only of the facilities described in this document or may contain facilities not described herein. It is important to check the current position with Teamware Group.

Specifications and statements as to performance in this document are Teamware Group estimates intended for general guidance. They may require adjustments in particular circumstances and should therefore not be taken as formal offers or commitments.

This document is not part of a contract or license save insofar as may be expressly agreed.

Further information can primarily be obtained through Teamware partners. Contact you local Teamware contact for further details. Teamware can also offer support and other services on a consultancy fare basis. Alternatively support for answering questions of technical nature can be handled through Teamware Incident Database when agreement between the parties exist.

Teamware is a registered trademark in the USA and other countries. Microsoft, MS-DOS and Windows are registered trademarks of Microsoft Corporation in the USA and other countries. UNIX is a registered trademark of The Open Group. Sendmail is a trademark of Sendmail Inc. in the USA and other countries.

Disclaimer, warranty and terms of distribution

These publications are partly based on and contains pre-release or other vendor software that may vary at the level of performance, functionality or compatibility. The purpose of the publications is to give the Teamware users the opportunity to take a look of what can be done and explore these features. Teamware Group shall have no obligation to maintain, correct, update, change, modify or otherwise support the software components and documents mentioned in this publication.

Teamware Group expressly disclaims any warranty for the publication. The publication is provided "as is" without warranty of any kind, including, without limitation, the implied warranties of fitness for a particular purpose. In no event shall Teamware Group be liable for any damages whatsoever including, damages for loss of business profit, business interruption, loss of business information, or any other loss, occurring during the use of, or inability to use the software.

Contents

1 Document history	4
2 Introduction	5
3 Routing outgoing mail	6
3.1 Check if Sendmail accepts relaying for Teamware Office	6
3.2 Configure Sendmail to relay Teamware Office mail.....	7
4 Processing incoming mail	9
4.1 Delivering incoming messages through SMTP	9
4.1.1 Configuring MIME Connector	10
4.1.2 Instructing Sendmail to accept Teamware Office mail	10
4.1.3 Declaring the delivery agent.....	10
4.1.4 Selecting the messages to be delivered to Teamware Office	12
4.1.4.1 Deliver all mail to Teamware Office.....	13
4.1.4.2 Deliver based on base address	13
4.1.4.3 Deliver based on the user name	14
4.1.4.4 Deliver based on aliases.....	15
4.1.4.5 Deliver using LDAP lookups.....	16
4.1.5 What to do when Sendmail and MIME Connector are running on different machines	19
4.1.5.1 Using default Sendmail relaying.....	20
4.1.5.2 Using special mailer for relaying to Teamware Office	21
4.2 Delivering incoming messages with torecvm.....	21
4.2.1 Configuring MIME Connector	22
4.2.2 Configuring Sendmail	22
4.2.3 Preventing "Relayed" DSN reports from Sendmail.....	24
5 Additional notes	25
5.1 The 0, A and C optional flags for delivery agents	25
5.1.1 0 – Turn off MX lookups.....	25
5.1.2 A – Lookup user again in the aliases database	26
5.1.3 C – Add @domain to recipient.....	26
5.2 Modifying base address for outgoing messages	26
5.3 Format of the From: header	27
5.4 Testing sendmail.cf without disturbing others.....	28
5.5 Creating backup mail servers.....	29
5.6 Beef up your security and anti-spam policy	30
5.7 Using alias base addresses for Teamware Office	31
5.8 Preventing routing of Teamware addresses to Internet	32
5.9 Locating the source of the problems.....	32

1 Document history

Here is a list with what has changed from the previous versions of the document:

Version 3.1: 12th October 2001

- Corrected some typos

Version 3.0: 1st June 2001

- Corrected typo on rewriting rule at 4.1.4.2 (\$3 was incorrect, must be \$2)
- Added section 4.1.4.5 about using LDAP lookups for delivering messages
- Added section 5.2 about modifying the base address for outgoing messages
- Added section 5.5 about creating backup mail servers

Version 2.0: 6th April 2001

- Amended the rulesets definitions. The previous version of the document had a dot (.) after the domain that has to be matched. However, although it is very rare, some base addresses will not have the trailing dot after the address is tokenized

Version 1.0: 3rd April 2001

- First released version of the document

2 Introduction

In many situations it is needed that the Mail service of Teamware Office to coexist with other mail systems inside the same organization. The present document presents a number of methods for integrating Teamware Office with one of the most used mail servers in the Internet, Sendmail.

However, this document is not intended to replace the Teamware Office and Sendmail documentation, which you are encouraged to study before reading this document.

Although the document tries to cover as many situations as possible, it would be impossible to cover all the possibilities. Please consider this document as a starting point for tailoring your system according to your specific requirements.

The following three chapters present the following issues:

Chapter 2: Routing outgoing mail originating from Teamware Office.

Chapter 3: Routing incoming mail intended for Teamware Office.

Chapter 4: Additional notes about Teamware Office and Sendmail Integration.

3 Routing outgoing mail

Teamware Office doesn't know by itself how to deliver outgoing Internet e-mail to the recipient servers, it needs an SMTP server that would accept to relay this messages to their final destination. You can use for that an SMTP server that already exists in your company, or an external SMTP server (such as one from your ISP) which accepts to relay messages for you. This server can run any software (Sendmail, Qmail etc.), as long as it understands the SMTP protocol.

If you will be using an external SMTP server, or one that you cannot administer yourself, you will need to ask his administrator to enable relaying for you.

If you have an internal Sendmail server that you can administer, this chapter will explain how to do it yourself.

First, you will need to specify in Teamware Office the IP address or machine name of the SMTP server. You can do this:

- During installation.
- Using `to config` command. Go to `3.Services` and then to `11.Connector for MIME`. When asked about `SMTP host`, enter the machine name or IP address of the SMTP server.
- With the Admin client, in the Connector for MIME -> Connection and message handling section.

First of all, make sure that your modifications will not affect other systems using that Sendmail server. It is highly advisable to make a backup copy of the all configuration files that you will modify.

3.1 Check if Sendmail accepts relaying for Teamware Office

Before doing any modifications, check if the Sendmail server isn't already accepting relaying from your Teamware Office server. Run the command:

```
sendmail -bt
```

You have now entered in the Sendmail testing mode. At the new prompt, enter the command:

```
$(=R
```

This will list the content of the `$$=R` class macro, which holds the list of servers from which relaying is accepted. Zero or more IP addresses and/or host names will be listed.

If the list contains the IP address or name of the machine running the Teamware Office Connector for MIME, you don't need to modify anything. If not, read the next section.

3.2 Configure Sendmail to relay Teamware Office mail

You will have to add the IP address or the name of the machine running MIME Connector to the `$$=R` Sendmail class macro (which acts basically as a list of values). The values of a class macro can be directly in `sendmail.cf` or can be listed in a file. The `$$=R` class macro contains the machines for which Sendmail accepts to relay mail.

Open `sendmail.cf` with a text editor and search for one or more lines starting with the capital letters `CR` or `FR`, followed by a machine name, an IP address or file name. There might or might not be a space after `CR` or `FR`, but there is no between `C` or `F` and `R`. For example:

```
CR mailhub.company.com
FR-o /etc/mail/relay-domains
```

The first letter (`C` or `F`) signals the beginning of a class macro definition, what follows is the value to be added to the class macro (`C`) or the name of a file from which the values are to be read (`F`)

If, for example, the machine running MIME Connector has the IP address `172.30.1.3` or the name `mime.company.com`, you can insert in `sendmail.cf` lines like:

```
CR 172.30.1.3
CR mime.company.com
```

Please note that the class macro definitions are case sensitive, so don't use `"cR"`, `"Cr"` or `"cr"`. If you can't find a `CR` or `FR` line in `sendmail.cf`, just add your line(s) before the first line that starts with a `C` character (usually it is `Cwlocalhost`).

If your MIME Connector machine has more IP addresses or names and you don't know which one is used when talking to the Sendmail server, just add similar lines for all addresses. Do not list more addresses in one line, it won't work. However, you should try to determine the correct address later and keep only the corresponding line in `sendmail.cf`.

You can also add these IP addresses or machine names to the file indicated by the `FR` declaration, one per line. You can also create a new `FR` declaration and file, if you want. The `-o` following `F` means "optional" and prevents Sendmail from complaining if the file does not exist.

Please note that if you are modifying `sendmail.cf` or a file accessed by it (such as `/etc/mail/relay-domains`), you will need to restart Sendmail in order for the new configuration to become effective.

Reading the values of a class macro (such as `$_R`) from a file makes administration more simple, avoiding the need of modifying `sendmail.cf`.

After you have updated the contents of `$_R` and restarted Sendmail, it will accept to relay outgoing and incoming messages on behalf of Teamware Office.

4 Processing incoming mail

There are two methods in which Teamware Office can receive e-mail from Internet.

The first method is to make Teamware Office receive the mail directly. In order to do that, the Teamware Office server must be visible from the Internet (it must have a public IP address) and you must setup proper MX records for its base addresses. If you will be using this method, answer "No" when asked if Sendmail is installed on your server, during the installation or when using `to config` to modify the Connector for MIME service configuration. This will determine Teamware Office to start it's own SMTP receiving service (SMTP Responder).

The second method is to configure your Sendmail server to receive the messages intended for Teamware Office users, and then make Sendmail to deliver those messages to the Teamware Office server, either with SMTP deliveries or using the `to recvm` program.

In the following paragraphs you will see different ways to implement this second method. Please read them all and choose the one that best suits your needs.

4.1 Delivering incoming messages through SMTP

If you will be using the methods described in this section, Sendmail will deliver mail to Teamware Office using SMTP connections. This can be used regardless if MIME Connector and Sendmail are installed on the same machine or not.

There are two main advantages in using SMTP deliveries instead of using `to recvm` deliveries:

- Sendmail doesn't treat `to recvm` as an DSN-aware mailer. But using SMTP ensures that delivery and receipt reports will be properly handled.
- It is easier to reconfigure your network, for example if you want to move MIME Connector from the machine running Sendmail to a different machine.

If Teamware Office and Sendmail are running on different machines, you will have to make certain modifications to the Ruleset 0 rewriting rules that are presented further in this section. Please see 4.1.5.2 for details.

4.1.1 Configuring MIME Connector

If you will be using SMTP deliveries, you will have to configure the Connector for MIME as if Sendmail is not installed on the same machine, even if they are actually running on the same machine.

This can be specified at installation time or using `to config`. Start `to config`, go to section `3.Services` then `11.Connector for MIME`. When asked if Sendmail is installed in this server, answer **NO** (even if Sendmail is actually running on the same machine). This will determine Teamware Office to start the SMTP Responder service, which will listen for incoming SMTP connections.

Additionally, if MIME Connector and Sendmail are running on the same machine, you will have to modify the port number used by SMTP Responder, because the default port 25 will be used by Sendmail. This is done with in the Admin client, Connector for MIME -> Miscellaneous section, by modifying the value in the SMTP Port number text box. You will need to restart Teamware Office in order for this setting to become effective.

4.1.2 Instructing Sendmail to accept Teamware Office mail

If you configured Sendmail as described at 3.2, it will accept to receive and relay incoming messages for Teamware Office.

4.1.3 Declaring the delivery agent

You will then have to instruct Sendmail how and what e-mails have to be delivered to Teamware Office. First, define the Teamware Office delivery agent in `sendmail.cf`, by adding the mailer definition below after the other mailer definitions (the lines starting with `M`):

```
Mtwu,          P=[IPC], F=8aAFmMnPuX, S=0, R=0, E=\r\n, L=2040,  
              T=DNS/RFC822/SMTP, A=IPC $h 2025
```

The parameters have the following meaning:

<code>Mtwu</code>	The name of the mailer (<code>twu</code>). There must be no spaces or tabs before or after <code>M</code> .
<code>P=[IPC]</code>	TCP/IP communication will be used when talking with the delivery agent.
<code>F=8aDFmMnPuX</code>	Delivery flags. Except <code>8</code> and <code>u</code> , all others are required in our case. Briefly, the meaning of flags is:

8: Convert all unlabeled 8 bit mail to MIME labeled mail. (V8.7 and above)
a: Run extended SMTP protocol (ESMTP). (V8 and above)
D: Need Date: in header.
F: Need From: in header.
m: Delivery agent allows delivery to multiple recipients.
M: Need Message-ID: in header.
n: Don't use Unix-style From in header. Don't confuse with the From: above. This flag must be set always when not dealing with Unix-style mailboxes.
P: Need Return-Path: in header.
u: Preserver uppercase for username.
x: Need RFC821 hidden dot. In case a line of the message contain only a dot, that dot will be doubled, in order not to confuse it with the dot signaling the end of message.

Other flags that you can use are `o`, `A` and `c`, but read first the section 5.1 to see if you really need them:

`o`: Turns off MX lookups for delivery agent. (V8.8 and above)

`A`: Lookup recipient (`$u`) in aliases database. (V8.7 and above; prior to V8.7 it was a default)

`c`: Add @domain part to address if it doesn't have one.

`S=0, R=0` Specify additional rulesets to be applied to the sender and recipient respectively. In our case we specified 0, which means no additional ruleset processing.

`E=\r\n` Use CR/LF combination at the end of line.

`L=2040` The maximum accepted line length, in bytes. Lines longer than that will be split.

`T=DNS/RFC822/SMTP` Used for composing DSN responses.

`A=IPC` The list of arguments for this delivery agent. For SMTP delivery agents, it is always IPC.

`$h` The IP address or machine name to which the machine has to connect. It is set by the `$@` part of the delivery agent. In certain conditions, you can also use the IP address directly. See sections 5.1.1 for details.

2025 The SMTP port number used by MIME Connector (2025 in our example). See section 4.1.1 for details.

Please note that there must be TAB character before P=. Also, if your mailer definition will span on more lines (as in the example above), the second and following lines MUST start with a TAB character, so Sendmail will know that they belong to the same mailer definition.

4.1.4 Selecting the messages to be delivered to Teamware Office

You have defined in the above section HOW Sendmail delivers messages to Teamware Office. Now you have to instruct Sendmail WHAT messages must delivered to Teamware Office.

This is done in the `Ruleset 0` of `sendmail.cf`. If you don't know what "rulesets" and "rewriting rules" mean, just open `sendmail.cf` and search a line containing the string "Ruleset 0" (without the quotation marks). A couple of lines below you should see a line containing `S0`. This marks the beginning of the `Ruleset 0`, where you will add the configurations you need.

Primarily, `Ruleset 0` is responsible for selecting the delivery agent to be used for a specific message based on the recipient address. If needed, the recipient address might also be modified by a rule in `Ruleset 0`.

The following configuration methods are presented in this document:

- Deliver all mail to Teamware Office (4.1.4.1): Use this method if you want all mail received by Sendmail to be automatically delivered to Teamware Office.
- Deliver based on base address (4.1.4.2): Messages will be delivered to Teamware Office if the recipient has specific base address(es). This implies that the base address(es) used by your Teamware Office server are not used by other mail servers.
- Deliver based on the user name (4.1.4.3): Messages will be delivered to Teamware Office if they have a specific string in the user part of the recipient address.
- Deliver based on aliases (4.1.4.4): You will use Sendmail's `aliases` file to specify mail for which recipients has to be delivered to Teamware Office. This is useful when you have no other way of distinguishing between Teamware Office recipients and other recipients. The downside is that you will need to update the `aliases` file every time you modify the e-mail address of a Teamware Office user or create a new user.

Of course, these are not all the possible options. As you will learn more about Sendmail, you can discover new methods that are maybe more suitable for your needs.

4.1.4.1 Deliver all mail to Teamware Office

Add the following rule at the beginning of Ruleset 0. Please note that you **MUST** have a TAB character before \$#:

```
R$+ < @ $=R . > $*      $#twu $@ $w $: $1 < @ $2 > $3
```

Here is a short explanation of this rule:

- | | |
|-----------------------|--|
| R | Declares the beginning of a rewriting rule. |
| \$+ < @ \$=R . > | The recipient address filter to decide to which messages this rule applies. It will select all addresses that have something both in front and after the @ character, and whose base addresses are listed in the \$=R class (the list of host names for which Sendmail receives mail; see 3.2 for details).
Note: The dot that follows after \$=R is not always required |
| \$* | This is used to match everything that might follow the base address, for example the requests for DSN reports (e.g. NOTIFY=SUCCESS,FAILURE). |
| \$#twu | The delivery agent to be used – twu.
Note: You MUST have a TAB character before \$#. |
| \$@ \$w | The host to which the message should be delivered. \$w is the name of the localhost. This is suitable if Sendmail and MIME Connector are running on the same machine. Section 4.1.5.2 shows the modifications needed when MIME Connector and Sendmail are on different machines. |
| \$: \$1 < @ \$2 > \$3 | The rewritten address to which the mail should be delivered. \$1 means the first match of the filter (\$+ above), and \$2 the second match of the filter (\$=R above). If you want, you can state in clear the new base address part, by replacing \$2 with it. \$3 matches anything that might follow after the base address (e.g. DSN requests). |

4.1.4.2 Deliver based on base address

Let's say that your Teamware Office base address is @two.domain.com, and that this base address is used **ONLY** for Teamware Office users. In this case you will want to instruct Sendmail to deliver all messages with that base address to Teamware Office. The rule that you have to add at the beginning of Ruleset 0 is (don't forget the TAB character before \$#):

```
R$+ < @two.domain.com. > $*          $#twu $@ $w $: $1 < @ two.domain.com >
$2
```

The rule is very similar with the one defined at 4.1.4.1, we just replaced `$=R` with an explicit domain, and we specified in clear the base address to be used in the rewritten address. If Teamware Office is using more base addresses, add similar lines for each such base address.

If MIME Connector and Sendmail are NOT running on the same machine, you will also have to modify the `$@ $w` part. See 4.1.5.2 for details.

4.1.4.3 Deliver based on the user name

If both Teamware Office and non-Teamware Office users in your system share the same base address, you can make the distinction between them by making all the Teamware Office e-mail addresses to have a certain string in the user part that is not used by non-Teamware Office users.

This string could be, for example, `.twu` or a single character such as `.` (dot) or `_` (underscore). Of course, that string must NOT appear in any other non-Teamware addresses that are handled by Sendmail.

Let's say that all Teamware Office addresses have a dot (`.`) in them before `@`, for example: `john.smith@company.com`. The rule that you have to add to Ruleset 0 is:

```
R$+.$+ < @ $=R . > $*          $#twu $@ $w $: $1.$2 < @ $3 > $4
```

This will make all messages containing a dot (`.`) before the `@` sign to be delivered to Teamware Office. Recipient addresses such as `joe@company.com` or `smith@company.com` will be ignored by this rule, so the rule will not interfere with other e-mail addresses handled by your Sendmail server.

If instead of a dot you want to use, for example, `.twu` as distinctive mark, the rule will look like:

```
R$+.twu < @ $=R . > $*          $#twu $@ $w $: $1.twu < @ $2 > $3
```

In this case, all your Teamware Office addresses should be in the form of:

```
<name>.twu@<yourdomain.com>.
```

If Teamware Office and Sendmail are NOT running on the same machine, you will also have to modify the `$@ $w` part. See 4.1.5.2 for details.

4.1.4.4 Deliver based on aliases

When you can't distinguish between Teamware Office and non-Teamware Office addresses in the ways described before, you can use Sendmail's aliases database to specify which are the Teamware Office users. The aliases database is specified by the `O AliasFile` or `OA` lines in `sendmail.cf` (usually `/etc/aliases`).

The main disadvantage of this method is that every time you add, delete or modify a user's e-mail address, you have to update the aliases database accordingly. However, you don't have to restart sendmail to do that, it is enough to run the command `newaliases`, which will rebuild the aliases database.

Let's say you have a Teamware Office user whose e-mail address is `john@company.com`. Add to `/etc/aliases` the following line:

```
john:      john.twu
```

Then add in `sendmail.cf`, at the beginning of Ruleset 0, the following two rewriting rules:

```
R$+ .twu < @ $+ > $*      $#twu $@ $w $: $1 < @ $2 > $3  
R$+ .twu $*              $#twu $@ $w $: $1 < @ company.com > $2
```

You will notice that these rules are similar with the ones described at 4.1.4.3, the same principle applies here.

Why two rules? If your Teamware Office server is using only one base address, then you will need only the second rule. Keep in mind that Sendmail will strip off the domain part from any recipient addresses that have the base addresses in the `$=w` class macro. Also, remember that only recipients that have such base addresses will be looked up in `/etc/aliases`.

But if Teamware Office was configured with multiple base addresses, you will have to use in `/etc/aliases` lines like:

```
mary:      mary.twu@sales.company.com
```

This way you explicitly specify the base address to be used for each aliased user. In this case, the first rewriting rule will be used.

As an example of alternative method, you could create in `/etc/aliases` lines like:

```
john:      john.twu_company  
mary:      mary.twu_sales  
mark:      mark.twu_sales
```

And the rewriting rules will become:

```
R$+ .twu_company $*      $#twu $@ $w $: $1 < @ company.com > $2
```

```
R$+ .twu_sales $*           $#twu $@ $w $: $1 < @ sales.company.com >  
$2
```

This way, you don't have to specify the base addresses in `/etc/aliases`, you will specify them in `sendmail.cf`.

Please also note that, if Sendmail and MIME Connector are running on different machines, you have to modify the `$@ $w` part from the rewriting rules. See 4.1.5.2 for details.

4.1.4.5 Deliver using LDAP lookups

One of the nice features in Sendmail is that it can perform lookups in LDAP servers. Such LDAP lookups can be used by Sendmail to check if a specific recipient address exists in a Teamware Office LDAP server and to select the correct MIME Connector destination machine for delivery.

It is especially suitable when the recipient addresses of all the incoming messages for users on different servers have the same base address (e.g. `@company.com`). Instead of maintaining big aliases databases (as was described on 4.1.4.4), it is more convenient to use LDAP lookups, since the LDAP servers hold up to date information about the users. Of course, this flexibility comes at a price: for each recipient, one or more LDAP lookups must be performed. It is advisable to make some performance tests on your systems before actually implementing this method.

The first step is to declare in `sendmail.cf` the connection information for the LDAP server. Add somewhere at the beginning of `sendmail.cf` a line like:

```
Ktwo_ldap ldap -k"mail=%s" -v"mail" -h"172.30.1.3" -b"o=Company, c=FI"
```

The meaning of the arguments is:

<code>Ktwo_ldap</code>	Declares a lookup database called <code>two_ldap</code>
<code>ldap</code>	Declares the type of the database (<code>ldap</code>). Please note that in Sendmail version prior to 8.10, the type was <code>ldapx</code> .
<code>-k"mail=%s"</code>	Specifies the search argument. In our case, the search will be done for LDAP entries that have the value of the <code>mail</code> field equal to the argument used in search (<code>%s</code>).
<code>-v"mail"</code>	Specifies the LDAP attribute whose value will be returned by the search. In our case, we want the search to return the e-mail address (the value of <code>mail</code> attribute).
<code>-h"172.30.1.3"</code>	Specifies the IP address of the LDAP server.
<code>-b"o=Company, c=FI"</code>	Specifies the search base in the LDAP server. To speed up the searches, you might want to use a narrower search base, for example <code>-b"l=Helsinki, o=Company, c=FI"</code> .

Please note that, in order for Sendmail to be able to perform LDAP lookups, you must allow anonymous binds to the Teamware Office LDAP server. You can enable them using the `toxldconf` program.

If you have multiple Teamware Office LDAP servers, you will to use similar declarations for them as well. Just make sure to use unique names (e.g. `two_ldap1`, `two_ldap2` etc.)

After you have declared your LDAP servers, you will have to define a ruleset that will perform the LDAP lookups. You can insert this ruleset anywhere in the `sendmail.cf` file, as long as it is not in the middle of another ruleset. To be sure, search for the first line that starts with an S (usually it is S3, the beginning of Ruleset 3) and insert your new ruleset before that line.

Let's say you have two Teamware Office LDAP servers, identified in `sendmail.cf` by `two_ldap1` and `two_ldap2`. Let's also say that the users in the first server have base addresses like `@tw1.company.com` and the users in the second server have base addresses like `@tw21.company.com` and `@tw22.company.com`. Finally, let's say that all the incoming mail, for all Teamware Office users, will have only `@company.com` as base address, without the distinguished parts `tw1`, `tw21` or `tw22`.

In this case, your ruleset will have to look like:

```
STWO_LDAP
R$+ < @ $=R . >      $: $(two_ldap1 $1 @ tw1 . $2 $: $1 < @ $2 . > $)
R$+ < @ $=R . >      $: $(two_ldap2 $1 @ tw21 . $2 $: $1 < @ $2 . > $)
R$+ < @ $=R . >      $: $(two_ldap2 $1 @ tw22 . $2 $: $1 < @ $2 . > $)
R$+@$+               $: $1 < @ $2 . >
R$+ < < @ $+ . > . > $: $1 < @ $2 . >
```

Please note that there must be at least one TAB character before the first `$:` symbol.

The first line declares the beginning of a ruleset called `TWO_LDAP`. The next three lines define how the LDAP lookups will be actually performed. Let's take a closer look at the rules.

```
R$+ < @ $=R . >      $: $(two_ldap1 $1 @ tw1 . $2 $: $1 < @ $2 . > $)
```

You will need such a line for each Teamware Office LDAP server that you intend to use and for each base addresses declared in those servers.

The part before the TAB character is the matching pattern. It will match any standard Internet e-mail address that has the domain part (the base address) listed in the `$=R` class macro (the list of domains accepted for relaying).

The `$:` symbol following the TAB character means that the address rewriting should be performed only once. If this symbol would not be present, Sendmail would try to match again the result of the rewriting with the string before TAB, which could lead to an

endless loop. Please note that this symbol, in this context, does not have the same meaning as the `$:` symbol from the rules in the Ruleset 0 which were presented earlier.

The part following the first `$:` specifies how the LDAP lookup is performed:

```
$(two_ldap1 $1 @ tw1 . $2 $: $1 < @ $2 . > $)
```

The `$()`, `$:` and `$)` symbols act like an IF-THEN-ELSE structure. The part between `$()` and `$:` tell Sendmail to perform a lookup in the database with the name `two_ldap1`, using `$1 @ tw1 . $2` as search criteria.

Let's say that the address being processed is `john@company.com`. By the time it reaches our ruleset, the address will be in the tokenized form `john < @ company . com . >`

When matching this address against our rewriting rule, `$1` will have the value `john`, and `$2` will have the value `company.com`. So Sendmail will search in the LDAP server for a user with the e-mail address `john@tw1.company.com`.

If the search is successful, the rule will rewrite the address with what the LDAP search has returned (the e-mail address `john@tw1.company.com` in our example).

If the search is not successful, the address will be replaced with what is written between `$:` and `$)`. In our case, it will return `john < @ company .com . >`, which is the original form of the address that was passed to the rewriting rule. We need to preserve this original form, because this is the form needed in `sendmail.cf`.

If the lookup was unsuccessful, the next rules will try, in a similar manner, to lookup the address in the other server, using the two possible forms of the Teamware Office base addresses.

It is a good idea to place first in the ruleset the rules corresponding to the LDAP server that receives the biggest amount of mail. This way you can reduce the number of unsuccessful LDAP lookups.

In case of a successful lookup, the next rules in the ruleset will not perform LDAP lookup, because the address in this case was rewritten as `john@tw1.company.com` (without the angle brackets `<` and `>` surrounding the base address).

And this also explains the role of the last two rules in the ruleset:

```
R$+@$+ $: $1 < @ $2 . >  
R$+ < < @ $+ . > . > $: $1 < @ $2 . >
```

The first adds the angle brackets in the address. The second deletes a pair of brackets if now there are two of them in the address.

A possible optimization of this ruleset would be that, instead of doing LDAP lookups for all the addresses with base address contained in the `$$=R` class macro, to do lookups only for addresses that have a specific base address. For example, instead of the rule:

```
R$$+ < @ $$=R . >          $: $(two_ldap2 $1 @ tw21 . $2 $: $1 < @ $2 . > $)
```

you could use a rule like (everything must go in one line):

```
R$$+ < @ company . com . > $: $(two_ldap2 $1 @ tw21 . company . com $: $1 < @ company . com . > $)
```

Now, that the LDAP lookup mechanism is defined, Sendmail must know when to use it. For this, add at the beginning of the Ruleset 0 (just after the line saying `s0`), a line like:

```
R$$*                        $: $>TWO_LDAP $1
```

This rule will determine that, prior to trying to identify the delivery agent for a recipient address, that address should be first parsed (and rewritten, if needed) by the `TWO_LDAP` ruleset that we previously defined.

After the recipient address passes through the `TWO_LDAP` ruleset, it will contain its Teamware Office base address and you can use domain-based delivery methods, as the ones discussed in the chapters 4.1.4.2 or 4.1.5

If no matching user has been found in the Teamware Office LDAP servers, Sendmail will try to find other suitable delivery agents (e.g. deliver to a local user). If it can't find any suitable delivery agents, it will return a failure notification to the sender.

4.1.5 What to do when Sendmail and MIME Connector are running on different machines

If Sendmail and MIME Connector are running on different machines, you have two main configuration options:

- MIME Connector to receive mail directly from Internet. You will have to assign a public IP address for the MIME Connector machine, and define proper MX records for the Teamware Office base addresses used by it.
- Sendmail to receive the mail for Teamware Office users and then pass it to the MIME Connector.

If you want to use the second option, there are again two options:

- Use the default Sendmail relaying – see 4.1.5.1
- Use special mailer definition for relaying to Teamware Office – see 4.1.5.2

4.1.5.1 Using default Sendmail relaying

Let's say that Sendmail receives a message with the base address `@sales.company.com`, which is listed in `=$R` (the list of domains for which Sendmail accepts relaying, see 3.1 and 3.2), but is not listed in `=$w` (the list of names for the `localhost`). In this case, Sendmail will try to send the message to its destination server.

First, Sendmail tries to resolve the name `sales.company.com` to an IP address, using DSN lookups, the `/etc/hosts` file or any other method configured in your server for resolving host names. Then it will connect to the IP address it found, on port 25 and will try to deliver the message.

So, if `@sales.company.com` is one of your Teamware Office base addresses, you will have to make sure that it is resolved to the IP address of the machine running MIME Connector.

Important note regarding the use of canonical names: There is a potential problem if the Teamware Office base addresses are resolved through DNS lookups to canonical names. Let's say you have defined in your DNS configuration records like:

```
sales      IN CNAME    mime
marketing  IN CNAME    mime
```

In this case, Sendmail, when using default relaying, will automatically rewrite the base addresses of incoming mail from `@sales.company.com` and `@marketing.company.com` to `@mime.company.com`. So mail addressed to `john@sales.company.com` will never reach its recipient.

There are more workarounds for this, choose the one that better fits your needs.

First option is not to use `IN CNAME`, or not to declare at all in the DNS the names corresponding to Teamware Office base addresses.

The second option is to define in Teamware Office that `@mime.company.com` is an alias for the Teamware Office base address (see 5.7 for details). But this will work only if you have a single Teamware Office base address.

The third option to disable name canonification in Sendmail. Search in `sendmail.cf` a line like:

```
#O DontExpandCnames
```

If you activate this option (by removing the comment sign #), Sendmail won't convert the base addresses to their canonical names. But before activating this option check very carefully that it won't affect other users of this Sendmail server.

The fourth option is to declare customized rewriting rules and mailers in `sendmail.cf` that will bypass the name canonification. This method is explained in the following section, 4.1.5.2

4.1.5.2 Using special mailer for relaying to Teamware Office

Even if Sendmail and MIME Connector are installed on different machines, you can still use the rulesets defined at 4.1.4.1 – 4.1.4.4. You will only have to modify the `$@ $w` part from the rulesets. Specifically, you will have to replace `$w` (the name of the localhost) with the IP address or name of the machine running MIME Connector, for example:

```
$@ mime
$@ mime.company.com
$@ 172.30.1.3
```

Important note: It is better to disable MX lookups (see 5.1.1 for details) if you will use IP addresses. You can disable MX lookups when using machine names as well, but only if you really need to.

Take for example the rewriting rule from 4.1.4.1:

```
R$+ < @ $=R . > $*          $#twu $@ $w $: $1 < @ $2 > $3
```

If MIME Connector is installed on the machine `mime.company.com`, the rule in this case will become:

```
R$+ < @ $=R . > $*          $#twu $@ mime.company.com $: $1 < @ $2 > $3
```

4.2 Delivering incoming messages with `torecvm`

This method is suitable only if Sendmail and MIME Connector are running on the same machine. Instead of Sendmail using SMTP connections to deliver the messages to Teamware Office, the messages will be piped to a program – `torecvm`.

Please note that this method allows less functionality than the SMTP deliveries presented in section 4.1.

Also, a big disadvantage is that Sendmail considers any program delivery agent (such as `torecvm` in our case) to be non-DSN aware, and there is no method to tell it otherwise.

Therefore, upon delivering a message to Teamware Office (`torecvm`), Sendmail will send a "Relayed to non-DSN aware MTA" notification back to the message originator. Even if Teamware Office will generate afterwards DSN notifications (such as Delivered, or even Undeliverable) those notifications will be ignored by most of the sender mail clients. See 4.2.3 for a partial workaround.

Worst case scenario: someone misspells a Teamware Office recipient address. Sendmail will pass it to `torecvm` and return to sender a notification "Delivered to non-DSN aware MTA". The sender's mail client will get this notification and set the message status to Delivered. Later, Teamware Office will determine that the message can't be delivered and will try to send a Delivery Failure report back to originator. But most mail clients (including Teamware Mail) will ignore this second report (because they already received one report) and will not inform the sender about the failed delivery.

Having said that, here is the configuration method for `torecvm` deliveries.

4.2.1 Configuring MIME Connector

When configuring the Connector for MIME, you have to answer YES when asked if Sendmail is installed on the same machine. This will prevent Teamware Office from starting the SMTP Responder.

4.2.2 Configuring Sendmail

The configurations presented in the sections 4.1.2, 4.1.3 and 4.1.4 for SMTP deliveries are valid for `torecvm` deliveries as well, except the mailer definition from 4.1.3, which will become:

```
Mtwu,      P=/usr/bin/torecvm, F=DFMnPu, S=0, R=0, E=\r\n, L=2040,  
           T=DNS/RFC822/X-Unix,  
           A=torecvm -d/to/smtp -pA -f$f -r$u
```

The parameters are, as follows:

`P=/usr/bin/torecvm` Path to delivery agent. It also signals to sendmail that the delivery agent is a program.

`F=DFMnPu` Delivery flags. Except `u` and `-pA` all others are required in our case. Briefly, the meaning of flags is:

D: Need Date: in header.

F: Need From: in header.

M: Need Message-ID: in header.

n: Don't use Unix-style From in header. Don't confuse with the From: above. This flag must be set always when not dealing with Unix-style mailboxes.

P: Need Return-Path: in header.
u: Preserver uppercase for username.

Other flags that you might use are A and C flags, but read first the section 5.1 to see if you really need them:

A: Lookup recipient ($\$u$) in aliases database. (V8.7 and above; prior to V8.7 it was a default)

C: Add @domain part to address if it doesn't have one.

S=0, R=0 Specify additional rulesets to be applied to the sender and recipient address respectively. In our case we specified 0, which means no additional rulesets processing.

E=\r\n Use CR/LF combination at the end of line.

L=2040 The maximum accepted line length, in bytes. Lines longer than that will be split.

T=DNS/RFC822/X-Unix Used for composing DSN responses.

A=torecvm The list of arguments for this delivery agent. The parameters are explained below (these are Teamware Office specific, not Sendmail).

-d/to/sntp The `torecvm` parameter specifying the path for storing incoming messages. `/to` represents the installation path of Teamware Office. Modify it to match your configuration.

-pA `Torecvm` switch specifying what kind of DSN must be produced by Teamware Office. A means "All reports". Other possible options are F and N, to indicate "Failure reports" or "No reports" (default setting). Please note that this setting will be applied to all incoming messages, regardless what DSN requests the originator have set, because Sendmail will not inform `torecvm` about these requests.

-f\$f `Torecvm` parameter indicated the originator of the message ($\$f$ is the Sendmail macro specifying the message originator).

-r\$u `Torecvm` parameter indicating the intended recipient. $\$u$ is generated by Sendmail from the part following $\$:$ in

the rewriting rule that determined the selection of this mailer.

4.2.3 Preventing "Relayed" DSN reports from Sendmail

As mentioned above, Sendmail will generate a "Relayed to non-DSN aware MTA" DSN report upon delivering the message to `troecvm`, if the originator requested a DSN report.

One possible workaround would be to include `noreceipts` in the `PrivacyOptions` setting. Search in `sendmail.cf` a line starting with:

```
O PrivacyOptions=          (in V8.7 and above; or)
Op=                        (prior to V8.7)
```

Add `noreceipts` (without the quotation marks) to the list of options following `PrivacyOptions=` or `p=`. This will determine Sendmail to ignore any DSN requests. The message originators will be informed about the status of the delivery only if you instruct Teamware Office to send such requests, by using the `-pA` or `-pF` switches for `troecvm` in the mailer definition.

The major drawbacks are:

- Sendmail DSN reports will be disabled for all users, including non-Teamware users of this Sendmail server. Fortunately, the DSN requests will be relayed, so if the outgoing messages from Teamware Office will request DSN reports, the recipient server will be informed about these requests.
- The `-p` switch for `troecvm` in the mailer definition will be applied to all the messages, regardless of what DSN requests were actually made by the message originator – even if the originator explicitly specifies the it doesn't want to receive DSN reports.

5 Additional notes

This section contains different things that you need to check on your system or that could help you in certain circumstances.

5.1 The 0, A and C optional flags for delivery agents

When the mailer definitions were presented in 4.1.3 and 4.2.2, it was said that a number of flags are optional in the `F=` equate. Below they will be detailed, in order to help you determine if they are needed or not in your configuration:

5.1.1 0 – Turn off MX lookups

When using SMTP delivery agents, Sendmail will try first to use DNS queries in order to locate an MX record for the destination server (`$h`). If the DNS query returns a canonical name for the destination server, it will re-iterate the DNS query, using the canonical name. If it cannot resolve the destination server in this way, it will then try to use other resolving mechanism on that machines (such as using `/etc/hosts`).

Specifying the flag 0 in the `F=` equate will prevent Sendmail from using DSN and MX record lookups.

Let's say you are using the rewriting rule:

```
R$+ < @ $=R . > $*      $#twu $@ mime.company.com $: $1 < @ $2 > $3
```

You can declare then in `/etc/hosts` the IP address of the machine `mime.company.com`, so Sendmail will know how to contact it.

Or you can specify the IP address of the machine running MIME Connector directly in the mailer definition, for example

```
Mtwu,      P=[IPC], F=08aDFmMnPuX, S=0, R=0, E=\r\n, L=2040,  
           T=DNS/RFC822/SMTP, A=IPC 172.30.1.2 2025
```

However, you are encouraged to use this alternative only as a last resort. If you can define proper MX lookups for your MIME Connector machine and for the Teamware Office base addresses, please do so and do avoid using the 0 flag.

5.1.2 A – Lookup user again in the aliases database

Normally, user names are looked up in the aliases database before they are passed to the delivery agent. The aliases database is specified by the `O AliasFile` or `OA` lines in `sendmail.cf` (usually `/etc/aliases`).

However, if you specify the `A` flag in the `F=` equate, the user passed to the delivery agent will be looked up again in the aliases database before the delivery is made. If a matching entry is found, that entry will replace the user name in the recipient address and Sendmail will go again through the rulesets, including Ruleset 0, which could cause a new delivery agent to be selected.

Please note that only local user recipients are looked up in the aliases database. If a recipient address, after passing through rulesets, still has a base address attached to it (e.g. `user@company.com`), it will not be considered local.

The decision of using the `A` flag or not depends entirely on your specific requirements.

5.1.3 C – Add @domain to recipient

If the recipient address passed to that delivery agent doesn't have a `@domain` part, one will be automatically added, the one defined as the primary base address for Sendmail.

You might want to use this flag if there are chances that, after passing through the rulesets, the recipient address might lack the domain part. However, in that case you must make sure that Sendmail's default base address is the same as the one used by Teamware Office.

The decision of using the `C` flag or not depends entirely on your specific requirements.

5.2 Modifying base address for outgoing messages

If multiple base addresses are used (possible from multiple Teamware Office servers), you might want to convert them all to a single base address, so the external recipients will see only one base address (e.g. `@company.com`) instead of multiple base addresses (e.g. `@tw1.company.com`, `@tw2.company.com` etc.) in your outgoing messages.

First, at the beginning of `sendmail.cf`, initiate the class macro `$=M`, which holds the list of domains (base addresses) that must be masqueraded, for example:

```
CM tw1.company.com tw2.company.com
```

Then add at the beginning of Ruleset 94 (envelope name masquerading), just after the line saying "S94", a line such as:

```
R$* < @ $=M . > $*           $: $1 < @ company . com . > $3
```

For example, if the user `john@tw1.company.com` sends a message, the recipient will see it as coming from `john@company.com`.

Instead of `@company.com`, you can use predefined macros, such as `$j` (the fully qualified name of the Sendmail server) or `$m` (the domain to which the Sendmail server belongs), for example:

```
R$* < @ $=M . > $*           $: $1 < @ $m . > $3
```

To be sure that this technique works, you must also check that indeed the Ruleset 94 is used in your case for sender address rewriting. To do this, look at the definitions of the delivery agents used for delivering mail to external addresses. They should contain a setting `S=11` or `S=11/31`, which set the ruleset (usually 11) that is applied to sender address before the delivery is made.

Then look at the Ruleset 11 (search for a line containing "s11"). In that ruleset you should see a line like:

```
R$*                           $: $>94 $1
```

This line calls the Ruleset 94, which performs the actual domain masquerading. If the line doesn't exist, or if the Rulesets 11 or 94 don't exist, you can create them yourself. You can also add the `S=11` parameter to any delivery agent definition you want - including the Teamware Office specific delivery agents (see chapter 4.1.3 for details).

Of course, if you will implement this method, you won't be able to implement domain-specific delivery methods for incoming messages (e.g. the one described in 4.1.4.2), you will have to implement user-based or LDAP-based delivery techniques (e.g. 4.1.4.3, 4.1.4.4 or 4.1.4.5).

5.3 Format of the From: header

In some older versions of Sendmail, the definition of the `From:` header for outgoing messages was:

```
H?F?From:$q (where $q means the default format of sender's address)
```

This determined that, if a mail was sent by a Teamware Office user to a non-Teamware Office user having the same base address, the base address part was deleted from the sender's address in the MIME `From:` header. As a consequence, if that recipient wanted to reply to such a message, the reply didn't reach the Teamware Office user.

The newest versions of Sendmail are defining the `From:` header to be something like:

```
H?F?From:$?x$x <$g>$|$g$.
```

This translates as:

<code>\$?x, \$, \$.</code>	Condition: if the macro <code>\$x</code> (the full name of the sender) has a value, include in output whatever is specified between <code>\$?x</code> and <code>\$ </code> . Otherwise include in output the part between <code>\$ </code> and <code>\$.</code>
<code>\$g</code>	Sender's full return address.
<code>< , ></code>	Symbols used to delimit the address.

In human language: "IF the sender's full name is defined, THEN insert the full name followed by the address in angle brackets, ELSE insert only the sender's address."

You are encouraged to use this format. To locate in `sendmail.cf` this line, search for a line starting with `H` and containing `From:` (there might be various parameters, such as `?F?`, between `H` and `From:`).

5.4 Testing sendmail.cf without disturbing others

It's not always trivial to get your `sendmail.cf` right from the first time. That's why it is better to be able to test it without disturbing the normal mail processing of your server – your colleagues will definitely appreciate it.

Create a working copy of `sendmail.cf`, let's say `sendmail.cf.test`, and do all the modifications you need in this one. When you want to test the delivery process of a message addressed to, let's say, `user@company.com`, run the command:

```
sendmail -C/etc/sendmail.cf.test -bv -d21.1 user@company.com
```

Where:

<code>-C/etc/sendmail.cf.test</code>	Tells sendmail what configuration file to use.
<code>-bv</code>	Tells Sendmail to run in testing mode, without doing any actual delivery.
<code>-d21.1</code>	Tells sendmail to output trace information.
<code>user@company.com</code>	The recipient address for which you want to test the delivery.

When you run the command, you will see a lot of tracing, showing how the originator (the user who run the command) and the recipient addresses are parsed by the various rulesets invoked. This will tell you exactly what is the effect of your rulesets. On the last line you will see what would be the outcome: if the message is deliverable or not, which mailer will be used and the rewritten recipient address.

Test all possible recipient types: Teamware Office users, non-Teamware users, external recipients etc. After you are satisfied with the test results, move the original `sendmail.cf` to a backup location and replace it with your test configuration file

(renamed now to `sendmail.cf`, of course). Restart sendmail (with `killall -HUP sendmail` for example).

After that, monitor closely if all is well. If, despite your tests, the new configuration file doesn't work as expected, revert to the backup copy of `sendmail.cf` and restart Sendmail.

5.5 Creating backup mail servers

What happens when your receiving mail server (Sendmail or MIME Connector) becomes unavailable for one reason or another? The servers that want to deliver messages to you will store the messages in their queues until your server is back online or until the time-out period of the messages in the queue expires (usually it is a few days).

Instead of this, sometimes is better to create a backup mail server, that will receive messages for your site when your servers are down. The main advantages of having a backup mail server are:

- When your server comes back online, it will not be overloaded by a multitude of other servers trying to deliver all their messages at the same time. Instead, your backup mail server will deliver them to your server in a more manageable manner.
- If you have access to the mail queue of the backup server, you will be able (if needed) to read important messages directly from the queue
- You avoid the risk of losing messages because of delivery time-outs on the sender servers.

Let's say that you want to setup a backup mail server on `mail.remote.com` for your primary mail server `mail.company.com`. All you have to do is to add in your DNS server a new MX record for `mail.company.com` that points to `mail.remote.com` and which has a higher cost. So the DNS server should have the following MX records:

```
mail.company.com.    IN  MX  2      mail.company.com.  
mail.company.com.    IN  MX 100     mail.remote.com.
```

When an external mail server wants to deliver a message to `mail.company.com`, it will first try to deliver it to `mail.company.com`, which has a lower cost (2). If it cannot connect to it, it will then try to deliver it to `mail.remote.com`, which has a higher cost (100).

It is advisable that the backup server to be located on a completely different location, and on a different network, to reduce the risk that for a disaster to bring both servers down.

The backup server must be configured to accept to relay messages for your domain. The administrator of the backup server must monitor his mail queue, and notify you when messages for your site start showing up in his mail queue.

He will probably want to setup a script that will move messages from the queue to a backup directory until your server becomes available again. This will also prevent his mail server from trying to deliver messages to you while your server is down.

If the remote server is running Sendmail, the queue will contain files with names in the form of: `?f*`. The letter before `f` can be: `q` (queue control file), `d` (message body) etc. The part following `f` is a unique ID. All files from the queue that have the same ID after `f` belong to the same message.

The script mentioned above should look in the queue directory for control files `qf*` that contain your domain name in a line starting with `R` (recipient address). It then should move to the backup directory all the files containing in their names the same ID as the control files that matched the criteria.

When your server is online again, the administrator of the backup server can initiate the delivery of the messages with a command like:

```
sendmail -OQueueDirectory=/backup_queue -OTimeout.queueereturn=99d -q
```

In this example, `/backup_queue` is the directory where the backup queue files were moved. The parameter `-OTimeout.queueereturn=99d` sets the time-out of that queue directory to 99 days. If it's not used, message that stayed too long in the queue will be bounced back to sender instead of being delivered to recipient.

5.6 Beef up your security and anti-spam policy

Because Sendmail is one of the most used server software in the world, it is also one of the preferred targets for hacker attacks. Many of these attacks are successful, not necessarily because of Sendmail security bugs, but due to careless security configurations and careless users.

Sendmail security is a big topic on itself and wouldn't be possible to cover it here extensively. But there are a few pointers that you can start with:

- The default configuration that you get when installing Sendmail was intended for general-usage, therefore it doesn't provide the tight security you needed for production servers. Read your documentation and check out Internet for all security tips that can be applied to your case.
- Start with a very tight security policy and only afterwards, if really needed, relax it. This way you avoid the febrile nights of trying to patch the security holes in a hurry AFTER you have been hit.
- Firewalls are good. Sendmail needs to have port 25 open to the Internet in order to receive mail. Configure your firewall to check really well who tries to

connect to it – it could be another mail server, but it could also be hacker with a spoofed IP address.

- Instruct your users to notify you when they are hit by spam e-mails. Then try to see if you can bloke that spamming source.

There are many resources on the Internet dedicated to Sendmail security and anti-spam policies. Here are a few starting points

- www.sendmail.org – The official Sendmail site
- www.sendmail.org/antispam.html – Anti-spam provisions for Sendmail
- www.securityfocus.com – Dedicated to all kind of security issues
- www.ecompany.com/webguide – Categorized resource of web sites

5.7 Using alias base addresses for Teamware Office

It is possible to define in Teamware Office aliases for the base addresses you use. For example, if you have defined the base address of your Teamware Office users to be @company.com, you can specify that @company.net is an alias for it. The outgoing messages will have @company.com as base address, but incoming addresses like user@company.net will be accepted as well and delivered to the mailbox user@company.com.

Open the file bridge/tombsmtp.ini and search in the [DISPATCH] section for a line like:

```
own_node = company.com
```

Under that line add a new one like:

```
own_node = A:company.net
```

This will declare @company.net as an alias for @company.com. Do NOT use as an alias base address a base address that was already been declared in the Teamware Office configuration. Having multiple base addresses and having aliases for base addresses are completely different things.

Do not forget to update your MX records and Sendmail configuration for the new base address aliases.

Of course, instead of using Teamware Office aliasing for base addresses, you could use Sendmail rewriting rules to change @company.net into @company.com. Choose the method that suits you best.

Note: If you modify the bridge/tombsmtp.ini file, you will have to also change the modification date of the tomb.ini file, in order for Teamware Office to use the

new settings. In Unix you can do that with the `touch` command. In Windows, open `tomb.ini` with a text editor and then save it.

5.8 Preventing routing of Teamware addresses to Internet

Let's say that the base addresses that you defined for your Teamware Office server are not used by any other mail system. In this case it is clear that an e-mail originating from Teamware Office and having one of these base addresses as recipient should not be routed to the SMTP gateway (Sendmail).

In the file `bridge/tombsmtp.ini` there is a setting called `options`, made of a succession of digits. The first digit represents the value of the `route_to_gateway` setting. It controls what happens with an outgoing message if the recipient base address is one of the base addresses used by Teamware Office, but the user can't be found in Directory. The possible values are:

- 1 – The message is sent to the MIME Connector, which will then submit it to the SMTP gateway (Sendmail).
- 0 – An error is generated and the message is not sent to the gateway.

Setting it to 0 will reduce the traffic and the routing problems. But use it only if you are sure that the Teamware Office base addresses are not used by other mail systems.

Note: If you modify the `bridge/tombsmtp.ini` file, you will have to also change the modification date of the `tomb.ini` file, in order for Teamware Office to use the new settings. In Unix you can do that with the `touch` command. In Windows, open `tomb.ini` with a text editor and then save it.

5.9 Locating the source of the problems

When something is not working right, first thing to do is to check where the fault is: in Sendmail or in Teamware Office configuration?

Check first your Sendmail's logs (for example `/var/log/messages`, depends on your system) to see if any errors are reported and if the messages for Teamware Office users are delivered OK.

If you see that mail for Teamware is not delivered, or if mail that wasn't intended for Teamware users is delivered to MIME Connector, review your rewriting rules.

If it looks like it is a problem with Teamware Office configuration, check `to.log` for errors or warnings that would point out the problem. You can use the Admin client to setup enhanced tracing for different components (MIME Connector, Mail service etc.).