

Kofax Communication Server

TCLINK-SM / TC/LINK-OC Technical Manual

Version: 10.2.0.1



© 2018 Kofax. All rights reserved.

Kofax is a trademark of Kofax, Inc., registered in the U.S. and/or other countries. All other trademarks are the property of their respective owners. No part of this publication may be reproduced, stored, or transmitted in any form without the prior written permission of Kofax.

Contents

1. OVERVIEW	7
1.1 SMTP / MIME BASICS	7
1.2 KEY FEATURES OF TC/LINK-SM	7
1.3 KEY FEATURES OF TC/LINK-OC	7
1.4 MODULES OF TC/LINK-SM.....	8
2. MAIL BACKGROUND.....	9
2.1 ADDRESSING	9
2.1.1 <i>Message Addressing from SMTP to KCS</i>	10
2.1.2 <i>Message Addressing from KCS to SMTP</i>	10
2.1.3 <i>Configuring a Different Separator Sign</i>	11
2.1.4 <i>User Authentication</i>	11
2.1.5 <i>Message Relaying</i>	12
2.2 MESSAGE CONTENT	12
2.2.1 <i>The Basic SMTP Protocol</i>	12
2.2.2 <i>SMTP Protocol Extensions (ESMTP)</i>	13
2.2.3 <i>RFC822 Message Format</i>	13
2.2.4 <i>MIME Message Format</i>	14
2.2.5 <i>Non-Standard Extensions</i>	14
2.2.6 <i>Delivery / Non-Delivery Notifications</i>	14
2.2.7 <i>Message Conversion from SMTP to KCS</i>	16
2.2.8 <i>Message Conversion from KCS to SMTP</i>	16
2.2.9 <i>Supporting SSL Connections (RFC2487)</i>	17
2.2.10 <i>Supporting "Fax over IP" to NetMoves (mail.com)</i>	20
2.3 MAIL DELIVERY IN THE INTERNET.....	21
2.3.1 <i>Routing from KCS to SMTP</i>	22
2.3.2 <i>The "Direct Delivery" Feature of TC/LINK-SM</i>	23
2.3.3 <i>Routing from SMTP to KCS</i>	23
2.3.4 <i>Message / Notification Loops</i>	24
3. INSTALLATION	25
3.1 PREREQUISITES	25
3.2 COMMON INSTALLATION STEPS	26
3.2.1 <i>Installation Steps on KCS Server</i>	26
3.2.2 <i>TC/LINK-SM "Easy Installation"</i>	26
3.2.3 <i>TC/LINK-SM "Advanced Installation"</i>	28
3.2.4 <i>TC/LINK-OC "Easy Installation"</i>	31
3.2.5 <i>TC/LINK-OC "Advanced Installation"</i>	32
3.2.6 <i>Final Installation Steps</i>	32
3.3 TC/LINK-SM FOR CONNECTING AN EXISTING KCS SYSTEM TO THE INTERNET.....	32
3.4 TC/LINK-OC FOR USE WITH TC/WEB	33
3.5 TC/LINK-SM FOR CONNECTING A PROPRIETARY MAIL SYSTEM TO KCS.....	34
3.6 TC/LINK-SM FOR CONNECTING MANY PROPRIETARY MAIL SYSTEMS TO KCS	35
3.7 TC/LINK-SM FOR USE AS AN INTRANET SMTP BACKBONE.....	35
3.8 MULTIPLE TC/LINK-SM INSTALLATIONS	37
3.8.1 <i>Multiple TC/LINK-SMs in Parallel / Load Balancing</i>	37
3.8.2 <i>Multiple TC/LINK-SMs in Parallel / Fail-Save Design</i>	37
3.8.3 <i>Multiple TC/LINK-SMs on the Same Workstation – Single IP Address</i>	38
3.8.4 <i>Multiple TC/LINK-SMs on the Same Workstation – Multiple IP Addresses</i>	38
3.8.5 <i>Windows NLB Cluster Installation – with TCSRVR NLB Support</i>	50
3.9 SPECIAL FEATURES	54
3.9.1 <i>User Profiles Setup for SMTP Aliases</i>	54
3.9.2 <i>User Profiles Setup for Special Originator Address</i>	55
3.9.3 <i>Enhanced Originator Mapping</i>	55

3.9.4	“Direct Delivery” Feature	55
3.9.5	Operation over a One-Way Dialup Line	56
3.9.6	“Single Text Block” Operation	57
3.9.7	Large Message Size Operation.....	57
3.9.8	Implementing Different Recipient Addressing Syntax	58
3.9.9	Configuring MIME Types for Attachments.....	58
3.9.10	Configuring Display Mode for Special Attachments	59
3.9.11	Changing the Address Separator Character	60
3.9.12	Active Polling of Remote Mail Queues (ETRN Feature).....	60
3.9.13	Separate TCP Ports for Send and Receive	60
3.9.14	Originator Alias Configuration.....	61
3.9.15	Reject Invalid Recipient Addresses.....	62
3.9.16	Customizable Codepage Conversion.....	62
3.9.17	Support of Japanese Text	63
3.9.18	Support of UNIX “LF Instead of CRLF” Behavior.....	63
3.9.19	Support of T.37 (“Fax over SMTP”).....	63
3.9.20	Additional Recipient Check	64
3.9.21	Filtering of Attachments (Inbound: SMTP->KCS).....	64
3.9.22	Enhanced Spam Filter.....	64
3.9.23	Handling of Multipart/Alternative.....	65
3.9.24	Restricted UTF-8 Support	66
3.9.25	Support of the Windows-1253 Character Set	66
3.9.26	Support of ISO-2022-CN and GB2312 Character Set.....	66
3.9.27	Support of ISO-8859-15 Character Set	66
3.9.28	SMTP Authentication	67
3.9.29	DNS File Lookup	68
3.9.30	“Reply-To” Support	69
3.9.31	Ignore the “Date:” Header Field.....	70
3.9.32	Support of the Thai Character Set “Windows-874”.....	71
3.9.33	Support of “Message/Partial” Attachments	71
3.9.34	Support of Custom Header Fields	71
3.9.35	Support of Additional TC MIME Header Fields	71
3.9.36	Message Sensitivity.....	72
3.9.37	Option to Remove Prefix from SMTP Recipient Address	73
3.9.38	Create Multipart Alternative with XSLTTransform from PS.....	73
3.9.39	Transparent SMTP Relaying	73
3.9.40	Special MIME Header Fields Written by TC/LINK-SM	74
3.9.41	Support of TC SMIME	75
3.9.42	Setting the HTML Character Set	75
3.9.43	Enable Signed Mails to Exchange Feature	75
3.9.44	Store SMTP Server Response in KCS Send Order	75
3.9.45	Synchronous Operation.....	76
3.9.46	Email Header in Body Text	76
3.9.47	Performance Improvement Using DNSCACHE File.....	79
3.10	USEFUL INSTALLATION HINTS	80
3.10.1	Templates.....	80
3.10.2	The Role of the Postmaster.....	80
3.11	TROUBLESHOOTING.....	80
3.11.1	Windows Tools for Checking TCP/IP and SMTP Environment	80
3.11.2	How to View Message Source in the Trace File.....	83
3.11.3	What to Do When	83
4.	OPERATION.....	85
4.1	VIEWING AND CHANGING TC/LINK-SM SETUP.....	85
4.2	SMTP SECURITY CONSIDERATIONS	85
4.2.1	Restricted Privacy of SMTP	85
4.2.2	Viruses via SMTP?	85

4.2.3	<i>Denial-of-Service Attacks</i>	85
4.3	MONITORING TC/LINK-SM OPERATION	86
4.4	SUMMARY OF ERROR CONDITIONS AND RETRIES BEHAVIOR	86
4.4.1	<i>KCS to SMTP</i>	86
4.4.2	<i>SMTP to KCS</i>	87
4.5	TEMPORARY FILES	87
4.5.1	<i>Intermediately Stored Messages</i>	87
4.5.2	<i>Temporary Files Used During Message Conversion</i>	87
5.	PERFORMANCE	88
5.1	TEST ENVIRONMENT	88
5.2	SENDING.....	88
5.2.1	<i>Plain Text 4 KB 1 Page</i>	88
5.2.2	<i>Word Attachment 27 KB 1 Page</i>	88
5.2.3	<i>Word Attachment 653 KB 51 Pages</i>	88
5.3	RECEIVING WITHOUT DOCUMENT CONVERSION	89
5.3.1	<i>Plain Text 4 KB 1 Page</i>	89
5.3.2	<i>Word Attachment 27 KB 1 Page</i>	89
5.3.3	<i>Word Attachment 653 KB 51 Pages</i>	89
5.4	RECEIVING WITH DOCUMENT CONVERSION	89
5.4.1	<i>HTML to PDF using KFXConverter - HTML 1 Page</i>	89
5.4.2	<i>DOCX to PDF using KFXConverter - Word Attachment 22KB 1 Page</i>	90
5.4.3	<i>DOCX to PDF using KFXConverter - Word Attachment 332KB 70 Pages</i>	90
5.5	CONCLUSIONS TO SPEED UP LINK-SM.....	90
5.5.1	<i>General Information About LINK-SM</i>	90
5.5.2	<i>How to Speed Up LINK-SM</i>	90
6.	RESTRICTIONS	91
6.1	GENERAL RESTRICTIONS	91
6.2	KNOWN PROBLEMS	91
6.2.1	<i>"X-..." Header Fields Can Only Be 256 Characters Long</i>	91
6.2.2	<i>Using Password Authentication</i>	91
6.2.3	<i>Bcc: Recipients Not Visible to the Postmaster</i>	91
6.2.4	<i>Microsoft Exchange 5.0 Internet Mail Service</i>	91
6.2.5	<i>Case-Sensitive rr99 Process Prior to TCOSS 7.07</i>	92
6.2.6	<i>Non-Delivery Notification Does Not Work on TC/LINK-OC</i>	92
6.2.7	<i>Different Recipient Addresses in RCPT and DATA Field Cause Wrong Sending Type</i>	92
7.	APPENDIX	93
7.1	REGISTRY KEYS USED BY TC/LINK-SM.....	93
7.2	COMPLEX MIME MESSAGE TRANSFER EXAMPLE.....	96
7.3	OVERVIEW OF THE DNS CONCEPT	97
7.3.1	<i>"A" Records</i>	97
7.3.2	<i>"MX" Records</i>	98
7.3.3	<i>Reverse Lookup – "IN-ADDR.ARPA" Entries</i>	98
7.4	TC/LINK-SM AND ANTI-SPAMMING MEASURES.....	99
7.4.1	<i>Mail Is Routed Only If Sent from a Known Subnet</i>	99
7.4.2	<i>Mail Is Routed Only If a Valid MX Record Is Available</i>	99
7.4.3	<i>Mail Is Routed Only If Double Reverse Lookup Is Successful</i>	99
7.5	SHORT INTRODUCTION TO FIREWALLS	99
7.5.1	<i>Understanding Firewalls</i>	99
7.5.2	<i>Types of Firewalls</i>	100
7.5.3	<i>Drawbacks with Firewalls</i>	100
7.5.4	<i>Masquerading</i>	100
7.5.5	<i>Copyright for the Linux Firewall Howto</i>	101
7.6	CONFORMANCE TO RECOMMENDATIONS AND DIRECTIONS	102
7.7	CHECKLIST FOR SETUP	103

7.8 SSL – VERIFICATION ERROR CODES 103

7.9 GLOSSARY..... 105

1. OVERVIEW

1.1 SMTP / MIME Basics

First, SMTP (Simple Mail Transfer Protocol) was the mail transfer protocol for the Internet. Due to the recent rise of the Internet/Intranet and the implementation of Internet standards (e.g. TCP/IP) in private networks, SMTP became the most used mail transfer protocol.

SMTP defines the protocol between SMTP servers (bi-directional). It relies on an existing TCP/IP infrastructure.

However, Internet Mail clients (like Netscape Messenger, MS Outlook Express or Eudora) also use SMTP to send messages to SMTP servers. (To get mail from servers, the POP3 or IMAP4 protocol is used.)

SMTP was originally defined as a pure ASCII (7bit) text transmission protocol, MIME was added later. MIME defines encoding methods for attachments and for message parts which are not plain text.

SMTP is a so-called “open standard” meaning that the protocol is described in publicly available documents, and anybody can use this standard (no patent protection or similar). Almost everything that is related to Internet Mail is documented in the “RFCs” (Request for comment). See chapter *Conformance to Recommendations and Directions* for a listing of all applicable RFCs!

Important! The Kofax Communication Server and its components formerly used the name TOPCALL. Some screen shots and texts in this manual may still use the former name.

1.2 Key Features of TC/LINK-SM

- TC/LINK-SM connects Kofax Communication Server to the messaging service of the Internet. Any KCS user or user on connected propriety mail systems, can have one (or more) Internet mail address(es) assigned. This enables sending and receiving Internet Mail without the need to change the user’s working environment.
- TC/LINK-SM enables all SMTP clients, and also the JAVA client, to use all KCS services, e.g. fax or sms. Reception to these clients is usually done via POP3 or IMAP4 protocol.
- TC/LINK-SM offers full SMTP/MIME support, including binary attachments, extended character sets and enhanced delivery status notifications.
- Notifications are always sent back to the originating user or application regardless of the user’s mail system.
- TC/LINK-SM supports more than one simultaneous incoming SMTP session, the maximum number can be configured.
- Configurable polling cycle for automatic, periodical opening of one-way dial-up connections to the Internet Service Provider
- TC/LINK-SM is member of the TC/LINK family, and therefore has a unified architecture and all the common features (like document conversion with learn mode, configurable covers and templates, configurable address mapping, and so on).
- Support of Kofax Communication Server features like printing all incoming email, auto-forward feature, least cost routing, delayed sending, alerts (via shadow user profiles).
- TC/LINK-SM is a full 32 bit Windows implementation, with high performance, easy maintenance, and excellent stability.

Note: TC/LINK-SM must not be used for connecting to MFP devices. Use TC/LINK-MFP instead.

1.3 Key Features of TC/LINK-OC

TC/LINK-OC is a special TC/LINK-SM configuration that supports Internet Mail Clients. When installed and started as “OC”, no license is required by TC/LINK-SM.

Restrictions of this configuration:

- Requires TC/SP 7.08 or higher (the first release with open client support)
- Only supported for directly connected SMTP/POP3/IMAP, or TC/JAVA client access.
- Some image conversions still need licenses if installed (same as for all Links).

- TC/LINK-OC must be installed on the same machine as the Internet Information Server for TC/JAVA!

1.4 Modules of TC/LINK-SM

TC/LINK-SM and TC/LINK-OC take advantage of all common files of the KCS links. In addition, they use the following modules:

Module	Main tasks
TCLSM.DLL	Receiving from Internet to temporary file Transmission to the Internet Polling feature Loop detection
TCMIME.DLL	Message conversion from / to MIME
SMTP.MAP	Address mapping rules for SMTP

2. MAIL BACKGROUND

There are some important points to make mail systems work. In this chapter, we will discuss:

- message addressing
- message content
- mail delivery procedure

2.1 Addressing

In general, any SMTP address comes in the format <localpart@mail-domain>. The “mail-domain” is used to route the message to the destination server, while the “localpart” usually identifies a single recipient mailbox on this server. Not only is this a simplification, it also helps understanding the basic operation of mail delivery.

SMTP Addressing Character Set

SMTP addresses suffer from a very limited character set: RFC 822 restricts the user-allowed characters to the ones not shaded in the following table:

HEX	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.A	.B	.C	.D	.E	.F
0.																
1.																
2.	SP	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3.	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4.		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5.	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6.	'	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7.	P	q	r	s	t	u	v	w	x	y	z	{		}	~	

Note:

- If you need to use any shaded characters in the local part of the address, this is allowed by putting the complete local part into double quotes. But even within the quotation marks, only US-ASCII characters are allowed.
- In general, the local part of the address is case sensitive while the mail-domain is not. But any server may choose to accept the local part as well (TC/LINK-SM does, if operated together with TCOSS 7.07 or higher).

Examples of SMTP Addresses

Address (localpart@domain)	Remarks
support@microsoft.com	Valid address for user mailbox “support” at mail server for the domain “microsoft.com”
max.mustermann@sample.com	Valid address for user mailbox “max.mustermann” at mail server for the domain “sample.com”
Max Mustermann@sample.com	Not valid because of the blank (“ ”) in the localpart
“Max Mustermann”@sample.com	Not valid because the complete local part must be quoted
“Max Mustermann”@sample.com	Valid because the complete local part is quoted
“Schütz”@sample.com	Not valid because of the non-US-ASCII character in the localpart (“ü”)
AI@(sub).sample.com	Not valid because of the brackets “()” in the mail-domain
AI@(sub).sample.com”	Not valid because the “mail-domain” is not allowed to be quoted.
<“X400#C=at;A=umi-at;S=autoanswer”@sample.com>	A valid X.400 address

Maximum SMTP Address Length

RFC822 limits the local part and the mail domain to a maximum of 64 characters each.

Total length of an Internet mail address must not exceed 256 characters (critical especially for embedded X.400 addresses)

Note:

Some of the given restrictions may not apply to special environments (e.g. addresses with non-US-ASCII characters or very long SMTP addresses may work in some scenarios). However, it is strongly recommended to keep the RFC 822 addressing specifications to guarantee interoperability.

2.1.1 Message Addressing from SMTP to KCS

As TC/LINK-SM is a mail server with an associated mail domain, all mail addressed to this domain will be routed to it by the external infrastructure. E.g., if TC/LINK-SM serves the mail domain <kofax.com>, all messages addressed to <AI@kofax.com>, <"12345#99"@kofax.com> or <"AI@Notes"@kofax.com> will be routed to TC/LINK-SM.

TC/LINK-SM is responsible for resolving the local part to make the final delivery. Therefore, it is necessary to embed the complete KCS addressing information in the local part of the email address. The general syntax is

[fullname#][service#]number[#answerback]@mail-domain

Examples (for default address mapping):

Address	Mail will be delivered to ...
AI@kofax.com	KCS User "AI"
"M. Meier"@kofax.com	KCS address book entry "M. Meier" (as long as no user with the same name exists)
FAX#12345@kofax.com	Fax number "12345"
TLX#12345#TCINT@kofax.com	Telex number "12345" with answerback "TCINT"
"Mr. Kerg#FAX#12345#876"@kofax.com	Fax number "12345" with answerback "876"; recipient full name is "Mr. Kerg"
"NOTES#KAichner@KFX"@kofax.com	Via TC/LINK-LN to address "KAichner@KFX" on Lotus Notes

Note that "FAX", "TLX", "NOTES" are services that must be configured on Kofax Communication Server.

2.1.2 Message Addressing from KCS to SMTP

Sending a message to SMTP is like addressing to any other service. If you want to send a message to <nobody@nowhere.com>, and SMTP is your service defined for TC/LINK-SM, simply type "SMTP,nobody@nowhere.com" in the To: field of TCfW.

The address must consist of a local part (one or more characters before the @) and a domain. With default configuration, TC/LINK-SM accepts any domain name. TC/LINK-SM can be configured to reject messages to root domains – so that the domain name must contain one or more dot (.) characters.

If the recipient address does not conform to these restrictions, TC/LINK-SM does not send the message.

To make replies work, TC/LINK-SM automatically builds a valid SMTP originator address for your message. There are two basic ways to configure your originator address:

2.1.2.1 Originator Address from the KCS User Profile

This applies if the originator of a message to SMTP is a KCS user (or, when sending from a connected propriety mail system, has a shadow user assigned):

The originator address is the first SMTP address configured in the user profile. (To be exact: the first address with a prefix matching the TC/LINK-SM default queue.) See chapter 3.9.2 "User Profiles Setup for Special Originator Address" for an example user profile setup.

2.1.2.2 Originator Built via Address Mapping

If the originator is not a KCS user, or the user profile does not hold a SMTP address, the originator address is built according to the same syntax as for the addressing to KCS:

[fullname#][service#]number[#answerback]@mail-domain

Examples (for default address mapping):

Originator	Resulting SMTP Originator Address
KCS user "FS"	FS@company.com Note: Full name is NOT inserted for KCS user IDs!
Fax from "12345", no full name, no AB	#FAX#12345#@kofax.com
Lotus Notes User "KAichner@KFX", sending via TC/LINK-LN w/o shadow user	`#NOTES#KAichner@KFX"@kofax.com

Note that "FAX" and "NOTES" are services that must be configured on KCS.

2.1.3 Configuring a Different Separator Sign

It is possible to configure another separator than "#" via the registry.

Name	Type	Default	Remarks
TCLSM\Separator	REG_SZ	"#"	Be careful in choosing another separator, as some characters are reserved for other purposes

2.1.4 User Authentication

As the KCS system may offers access to many services (e.g. fax, telex, X.400), it is very important to control access to these capabilities. This access control is mainly based on the originator of a message, which is either a KCS user or it is not.

2.1.4.1 Originator has a KCS User Profile

If TC/LINK-SM encounters an originator address that exactly matches a KCS user ID or alias address (originator mail-domain matches TC/LINK-SM mail-domain, and originator local part matches the KCS user Id), all rights settings, templates, etc., are taken from this user profile. In the user profile, you can control e.g. the restricted access to some services, the right to enter a number directly, or mandatory authorizers from the user template. A detailed description for the possible setup is given in the TC/LINK-Manual.

2.1.4.2 Originator has no KCS User Profile

If the search for a matching KCS shadow user fails, the rights and password setup will be taken from the configured "guest" user profile. You can, e.g.:

- configure this guest user to need authorization for sending faxes while all KCS users do not need it
- configure it to use the service "TOPCALL" only (only sending to KCS users will be allowed)
- configure limited rights and empty password while KCS users have full rights but need a password (++)PW). See 2.1.4.4 "Authentication via User Password" for details.

2.1.4.3 Authentication via Originator IP Address

As most Internet Mail clients give the possibility to enter any originator address without any verification (... therefore passing by the originator rights check), it may be necessary to configure additional access restrictions. This can be done by configuration of all IP addresses that are allowed to connect to TC/LINK-SM.

IP addresses are usually fixed for a workstation or at least taken dynamically from a fixed IP address range.

This feature is very useful, e.g., to allow only client PCs within the customer's LAN to access the TC/LINK-SM. See 3.2.3.3 "IP Authentication Setup" for details on the configuration.

2.1.4.4 Authentication via User Password

For additional security, TC/LINK-SM can be configured to require the user password embedded into the message (++PW). See the TC/LINK Manual for a detailed description.

Hint:

No password is needed for originators without shadow profile if the “guest” user profile has an empty password. This enables you to set up different levels of security for shadow users and guests. E.g., even though ++PW is enabled, guest users can send to KCS users, but cannot send faxes (for restricted rights in “guest” user profile: service “TOPCALL” is allowed, service “FAX” needs authorization).

2.1.5 Message Relaying

Usually, all mails arriving at TC/LINK-SM from the Internet have a matching mail-domain. But there are scenarios (especially 3.4 “TC/LINK-OC for Use with”) where any other destination mail domain occurs in messages to KCS. This means: A message arrives at TC/LINK-SM that shall be delivered to any other destination.

There are two configurations how TC/LINK-SM should handle this:

- Routing is disabled: TC/LINK-SM does not accept this message. It is up to the sending SMTP host, what to do with this message (it will try a different route, or send a non-delivery notification back to the originator).
- Routing is enabled: TC/LINK-SM posts this message to KCS by adding its own service prefix. If no reroute (via rr99) is done, this will cause the message to reappear and be sent out either directly to the destination (via DNS) or to the configured smart host (“messaging server”). The smart host is then responsible for further delivery.

With routing enabled, TC/LINK-SM is fully transparent for Internet Mail!

Example:

- An Internet Mail client is directly connected to TC/LINK-SM. It sends a message addressed to <nobody@nowhere.com> that will arrive at TC/LINK-SM.
- With routing enabled, TC/LINK-SM finds out that the destination domain (“nowhere.com”) does not match the own mail-domain (“company.com”), and therefore it will post the message addressed to “SMTP, nobody@nowhere.com”.
- If no reroute is found on KCS (e.g., if a user has an inactive SMTP alias address of “nobody@nowhere.com”, the message will be delivered to this address), the message will be sent out again by TC/LINK-SM to the configured smart host.
- The smart host is then responsible for further delivery of this message.

2.2 Message Content

To send mail via an Internet connection, all involved mail hosts must keep unified protocols and message formats (defined in various RFCs). For example, a fax received via KCS can only be forwarded to Internet Mail if it is embedded into a MIME message.

2.2.1 The Basic SMTP Protocol

SMTP provides an envelope for all mail sent via the Internet. It is a fully text-based, bi-directional (peer-to-peer) protocol; therefore, it is easy to handle, but not very secure (see 4.2 “SMTP Security Considerations”).

The most important SMTP commands are

Command	Meaning	Example
HELO	Identification of sending host	HELO mail.microsoft.com
MAIL	Originator mailbox	MAIL FROM:<Klaus.Aichner@company.x.com>
RCPT	Destination mailbox	RCPT TO:<nobody@nowhere.com>
DATA	Start of data transmission	(no parameters)
CRLF.CRLF	End of data	(no parameters)
QUIT	End of transmission	(no parameters)

For a real-life example of SMTP taken from the TC/LINK-SM trace file, see 7.2 “Complex MIME Message Transfer Example”. There you can also see that the message is transferred between the “DATA” and the “End of data” commands.

2.2.2 SMTP Protocol Extensions (ESMTP)

To expand the possibilities of SMTP, an extension mechanism was defined in RFC1869.

- To negotiate capabilities of the receiving host, the sender issues an “EHLO” command (“extended HELO”) instead of the initial HELO.
- If the recipient does not support extensions, it will respond with an “unknown command” error message; the sender will resume with an ordinary HELO, and disable any ESMTP features.
- If the recipient does support ESMTP, it will respond with a list of supported features (any feature has a special keyword assigned, and is described in a separate RFC).
- The sender now parses the list of supported features and chooses the necessary ones for transmission.

Example:

```
11:35:22.767 (a0/a1) TCP<-220 link.company.com (KOFAX TC/LINK-SM Version 2.05.13) ESMTP service ready
11:35:22.767 (a0/a1) TCP->EHLO lotus.com
11:35:22.767 (a0/a1) TCP<-250-link.company.com
11:35:22.767 (a0/a1) TCP<-250-DSN
11:35:22.767 (a0/a1) TCP<-250-SIZE 5000000
11:35:22.767 (a0/a1) TCP<-250 HELP
11:35:22.767 (a0/a1) TCP->MAIL From:<xyz@lotus.com> SIZE=1159
...
```

In this example, the receiving host <link.company.com> declares

- its capability of enhanced notifications (DSN),
- a maximum message size of 5MB (SIZE 5000000),
- and support of the HELP command.

The sender only takes advantage of the SIZE feature and indicates the size of the message to be transmitted.

ESMTP Features Supported By TC/LINK-SM – Overview

Keyword	Defined in	Short description
DSN	RFC1891-1894	Enhanced delivery notifications; see 2.2.6.4 “Advanced Notifications (According to RFC1891..1894)”
SIZE	RFC1870	Maximum message size negotiation; see 3.9.7 “Large Message Size Operation”
HELP	RFC 821	Gives a short description of supported commands
ETRN	RFC 1985	Active polling of remote mail queues; see 3.9.12 “Active Polling of Remote Mail Queues (ETRN Feature)”
STARTTLS	RFC 2487	Enables SSL connection over TCP

2.2.3 RFC822 Message Format

Similar to physical mail, there is a letter (... a message) within the (SMTP) envelope. Only the final destination needs to understand the message format within the envelope; all relaying stations only need to deal with the SMTP protocol (... the envelope).

The first message format for Internet Mail was defined in RFC822. It consists of a message header and a plain-text message body, separated by a single blank line.

The most important header keywords are:

Keyword	Meaning	Example
From	Originator	From: <xy@abc.com>
To	Primary recipient(s)	To: <nobody@nowhere.com>, <AI@company.com>, <BM@company.com>
Cc	Copy recipient(s)	Cc: <FAX#12345@company.com>

Bcc	Blind copy recipient(s)	Bcc: <HA@company.com>
Subject	Subject of the message	Subject: Meeting announcement
Date	Creation date (including time zone)	Date: Mon, 05 May 1997 19:16:03 +0200

The main limitations of this message format are

- No binary attachments possible (except e.g. UUencode, which is not an Internet standard)
- Restricted to 7 bit text (no vowel mutations like äüÄÖÜß, etc possible).

2.2.4 MIME Message Format

To overcome the limitations of the RFC822 message format, this new standard was created. MIME messages support

- binary attachments
- several character sets
- alternative contents
- embedded messages,
- multimedia (graphics, audio, video)

The basic message structure is still the same as with RFC822 (message header and body, separated by single blank line); therefore, it is somewhat compatible to this older message format.

Major differences are

- Several additional header fields, e.g.

Keyword	Meaning	Examples
Content-Type	What is the following message part	Content-Type: text/plain -> indicates simple text Content-Type: image/gif -> indicates image Content-Type: multipart/mixed -> multiple message parts to follow, separated by boundary
Content-Transfer-Encoding	How the content is encoded	Content-Transfer-Encoding: 7Bit -> the following message part is not encoded Content-Transfer-Encoding: base64 -> base64 encoded message part follows

- Definition of encodings (for transferring binary data over all kinds of text-based gateways): base64, quoted-printable.

Note: Encoded message parts are NOT encrypted! They can be decoded by anybody knowing the encoding algorithm.

- Sub-headers for every part of a multipart message (delimited by boundaries)
- Possibility for recursive structuring, meaning that an attached message within a MIME message can, e.g. contain an attached message.

See 7.2 “Complex MIME Message Transfer Example” for an example of a MIME message (taken from the TC/LINK-SM trace file).

2.2.5 Non-Standard Extensions

MIME is an encoding standard that provides mechanisms for non-standard extensions. For example, the TC/POP3 server uses “Content-Type: image/x-tci” to send TCI files.

Any incoming non-standard attachment types are saved as binary attachments by TC/LINK-SM.

2.2.6 Delivery / Non-Delivery Notifications

Unfortunately, the SMTP standard (RFC821) does not state how to request notifications. The only thing mentioned is that “*the originator must be notified if a message could not be delivered*”.

But there is the strong demand to get also notifications for successful message delivery. So, several possibilities – of which one standardized way – to request delivery notifications were developed. The most important ones are supported by TC/LINK-SM.

The following 5 types can be used for requesting notifications by setting the registry key “TCLSMIMENotifFormat” (see chapter 7.1 for the exact values).

2.2.6.1 Standard Notifications (According to RFC 821)

Of course, TC/LINK-SM supports the user readable notifications requested by the SMTP standard (plain-text messages in case of delivery problems). They are built by using the SMNONDEL CVR on the Kofax Communication Server.

Disadvantages:

- Only non deliveries are sent. No mechanism to request also delivery notifications!
- No automatic sending status update
- No generalized message format (you may, e.g., get a Japanese non-delivery, although original message and recipient are located on English servers ...)

2.2.6.2 Additional “Return-Receipt-To” Header Field

As non-delivery notifications are standard for SMTP, there is the need for requesting delivery notifications. This is done by entering an additional header field into the message, giving the address that should be notified as soon as the message has been delivered.

Example:

```
Return-Receipt-To: <support@kofax.com>
```

This has two major disadvantages:

- It is a non-standard method. This means: There is no way to prove whether the receiving host really sends a delivery notification or not. Furthermore, there are hosts that send a notification as soon as the message has been delivered to the recipient's inbox, and others that wait until the message has been read.
- The notification to be sent back is not standardized. This means that it is user readable, but cannot be parsed programmatically; thus, it is not possible get an automatic status update (which is one of the most important KCS notification features).

2.2.6.3 Additional “Rr” Header Field

This is a method mainly used in the UNIX world. It works the same way as the “Return-Receipt-To” field.

Example:

```
Rr: <support@kofax.com>
```

2.2.6.4 Advanced Notifications (According to RFC1891..1894)

This is a relatively young standard but supported by an increasing number of hosts (estimated around 50% in 1997).

It basically consists of two items:

- How to request a notification level
- How to build a machine-readable notification

Requesting notifications: This is done via an ESMTP feature called “DSN” (see 2.2.2 “SMTP Protocol Extensions”). Immediately after connecting, the sending host checks for advanced capabilities of the receiving host. If it finds the RFC1891..1894 notification capability (by checking the ESMTP response for the Keyword “DSN”), it will add some special parameters to the SMTP envelope.

Example:

```
11:35:22.767 (a0/a1) TCP<-220 mail.austria.eu.net ESMTP service ready
11:35:22.767 (a0/a1) TCP->EHLO kofax.com
11:35:22.767 (a0/a1) TCP<-250 OK
11:35:22.777 (a0/a1) TCP<-250-mail.austria.eu.net, pleased to meet you
11:35:22.777 (a0/a1) TCP<-250-SIZE
11:35:22.777 (a0/a1) TCP<-250-DSN
11:35:22.777 (a0/a1) TCP<-250 HELP
11:35:22.777 (a0/a1) TCP->MAIL FROM:<AI@kofax.com> ENVID=00000654517@kofax.com
11:35:22.777 (a0/a1) TCP<-250 OK
11:35:22.777 (a0/a1) TCP->RCPT TO:<nobody@nowhere.com> NOTIFY=SUCCESS,FAILURE
11:35:22.777 (a0/a1) TCP<-250 OK
```

11:35:22.777 (a0/a1) TCP->DATA

- The **DSN** keyword in the EHLO response indicates that the server is capable of handling RFC1891... 1894 notifications.
- The **ENVID** parameter gives a unique identification of the message. This parameter is returned in the notification in order to enable a match between message and corresponding notification.
- The **NOTIFY** parameter gives the desired notification level for a recipient. "SUCCESS,FAILURE" requests positive and negative notifications; "NEVER" would request no notifications at all.

Special Notifications Format: Notifications according to RFC1894 consist of three parts:

- a human-readable notification text (for compatibility with non-conform hosts)
- a machine-readable status report (containing key information of the original message, like the ENVID parameter, and numerical status codes like "delivered", "relayed" or "failed")
- a part of – or the complete original message.

TC/LINK-SM uses the ENVID parameter to identify the original send order, and the status code to update its status. This makes automatic status update (e.g. "at next node") work.

2.2.6.5 Supporting of Disposition Notification Requests (RFC2298)

Currently, following restrictions have to be considered:

- RFC 2298 is not implemented symmetric, only client role available (LINK-SM requests message disposition notifications (mdn). No server role, i.e. mdn requests will be ignored)
- mdn is globally activated (not dependent on recipient)
- no filtering (send options, target SMTP server)

2.2.6.6 Additional Notification Settings

The registry key "TCLSM\SMNotifLevel" sets the default notification handling on receiving messages. This is important, if the clients are not requesting RFC1891 notifications.

The registry key "TOPCALL\NotifMail" generally specifies, whether notifications are requested for messages from KCS. So this should be always set to 1, if you want to use the MIMENotifFormat key.

The registry key "TCLSM\NotifyMailFrom" triggers a non-empty sender address in case of a notification. The reason for this feature is, that some mail server do not accept an empty "MAIL FROM:<>".

Following settings are recommended to get the best result:

- TCLSM\MIMENotifFormat = 3
- TCLSM\SMNotifLevel = 1
- TOPCALL\NotifMail = 1

2.2.7 Message Conversion from SMTP to KCS

Plain text parts of incoming messages are converted to the KCS character set as good as possible. When the text cannot be converted without loss, the text in original form is kept as a binary attachment within the message.

Attachments (e.g. HTML pages, GIF or JPEG images, or also text attachments) are converted at the Document Converter if necessary (if any of the recipients does not have binary capabilities, e.g. fax). Attachments need an appropriate application installed capable of printing them via the KCS printer driver.

Embedded Messages are either converted to a plain structure, or kept as embedded messages according to the TC/LINK-SM setup (registry value "...TCLINKSM\General\EmbeddedMessages"). See the TC/LINK-Manual for details!

2.2.8 Message Conversion from KCS to SMTP

Text parts of the message are delivered as text and are converted to the best-fitting MIME character set.

Attachments are simply MIME encoded, without further conversion.

Image parts (e.g. incoming fax pages) are delivered in any of GIF, TIFF, BMP, PCX, DCX, MODCA and TCI formats, according to the TC/LINK-SM setup.

2.2.9 Supporting SSL Connections (RFC2487)

Security has become more and more an important factor in SMTP transfers. A possibility to achieve security is to use the SSL, respectively TLS (RFC standard) protocol. With the exception of TC/LINK-OC, all SMTP based link types support secure connections over this protocol. The following registry keys control SSL support:

(Location HKEY_LOCAL_MACHINE\Software\TOPCALL\TCLINKSM\TCLSM\...)

Registry Key	Type	Default	Possible Values / Meaning
SMSendSecure	DWORD	0	0 ... SSL only used, if mail server requests it 1 ... SSL connection mandatory, when sending to domains from SMSendSecDomains 2 ... SSL connection always mandatory
SMSendSecDomains	Multistring	""	List of domains, for which a SSL connection must be used
SMRcvSecure	DWORD	0	0 ... SSL disabled 1 ... SSL connection mandatory, when receiving from domains from SMRcvSecDomains 2 ... SSL connection always mandatory 3 ... SSL only used, if client requests is
SMRcvSecDomains	Multistring	""	List of domains, for which a SSL connection must be used
SMSDDMode	DWORD	0	1 ... SSL supported, detailed settings defined in other registry values 0 ... SSL disabled
CertificatePath	SZ	C:\TOPCALL\SHARED	Folder holding PEM files for SSL connections. The files must be called rootcerts.pem, private.pem, certificate.pem

To use SSL, a certificate and private key is needed. There are two possibilities: Either use the test certificate and key, which are included in the package or use any others from a CA (=certificate authority).

To verify certificates, root certificates are needed. Setup will install the root certificates from Thawte into the directory "C:\Topcall\Shared", if SSL is enabled during Setup. If you get additional root certificates, just open "rootcerts.pem" and append the text from your new certificates to this one. You can add information lines between the certificates, like in this example:

```
-----END CERTIFICATE-----
original filename: thawteCp.pem
-----BEGIN CERTIFICATE-----
```

If the verification of a certificate fails, you will find an error code in the trace file. You can find a list of the error codes in the appendix (7.8).

The SSL connection is established via the OpenSSL library, which is under open source license, so it can be used for free.

2.2.9.1 SSL Security Details

TC/LINK-SM supports secure connection via the SSL protocol (RFC standard: TLS). The following table shows an example, how the SSL connection is established and what happens:

Client (KCS)	Server (e.g. NetMoves)	Comments
SMTP command: STARTTLS	replies ok	The client initiates the SSL protocol by sending the STARTTLS command in the SMTP protocol. If the server is able to use SSL, he will send an acknowledgement.
Client Hello	Server Hello	The Hello messages establish the following attributes: protocol version, session ID, used ciphers and compression method.
	send server cert. (*)	Next the server sends his certificate, which includes the public key and requests the client certificate.
send client cert. (*) verify server cert. (*)		The client sends its certificate and verifies the server certificate. At this moment the client is finished. It will return to the SMTP protocol and now the connection is encrypted.
	verify client cert. (*)	The server verifies the client certificate and it will return to the SMTP protocol.

(*) ... These steps are optional in the SSL protocol. In fact our implementation does not request a client certificate as this could lead to problems, if the client certificate is only a server certificate.

It is important to mention, that SSL is integrated into the SMTP protocol as an extension. It does not change the port, like the https protocol, which is the SSL extension from the http protocol. So regarding firewall issues no additional port-forwarding is required.

To use SSL, a certificate and the private key are needed. The certificate holds the public key and the whole data about the server and the private key is self-explanatory. Now there are two possibilities: You can either use the self-signed certificate included in the latest TC/LINK-SM version (should be only used for testing) or use any others from a CA (=certificate authority).

To use the self-signed certificate delivered with TC/LINK-SM, rename the files PRIVATE_SELF_SIGNED.PEM and CERTIFICATE_SELF_SIGNED.PEM in the TOPCALL\SHARED folder to PRIVATE.PEM and CERTIFICATE.PEM. This test certificate is valid until 2027, but has two disadvantages:

- It is self-signed, therefore it will not be accepted if the remote server tries to verify the certification authority against a list of allowed authorities.
- It contains a hard-coded domain name (tclink-sdd-test-cert.topcall.com). If the remote server compares this domain name with the domain name assigned to TC/LINK-SM, it will not accept the certificate.

To request a new certificate from a CA, use the OpenSSL tool (delivered with TC/LINK-SM; located in C:\TOPCALL\SHARED).

Hint for Windows Server 2012: The path variable for OPENSSL must be set: Start the Command Prompt as an administrator and run the following command:

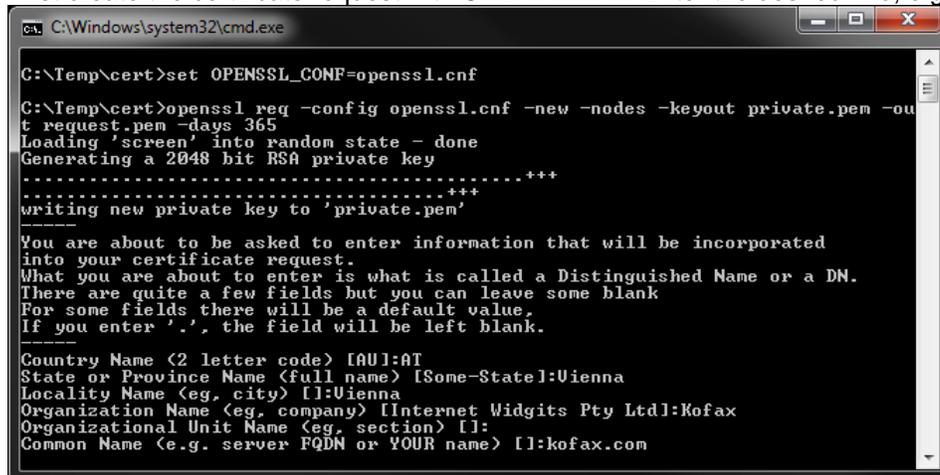
```
set OPENSSL_CONF=c:\topcall\shared\bin\openssl.cfg
```

Edit the OpenSSL configuration file, openssl.cnf, in a text editor. Change the value of the parameter default_bits from 1024 to 2048. (1024-bit certificates are no longer considered safe enough.)

File CREATE.BAT contains a sample command line for OpenSSL. This command create a certificate request file, named "request.pem" and a private key file, named "private.pem". You have to enter some data in this procedure, whereas the most important is the "Common Name". This should be the full domain name assigned to TC/LINK-SM (e.g. support.kofax.com).

You can put the "private.pem" file immediately into the "TOPCALL\SHARED" directory. After that you have to contact e.g. Thawte (www.thawte.com) and follow the online instructions to request a test SSL certificate. You have to provide some information about the company and the desired certificate. It is sufficient to request a standard server certificate. See following print-screens for an example procedure to get a test certificate:

First create the certificate request with CREATE.BAT. Enter the desired info, e.g.



```
C:\Windows\system32\cmd.exe
C:\Temp\cert>set OPENSSL_CONF=openssl.cnf
C:\Temp\cert>openssl req -config openssl.cnf -new -nodes -keyout private.pem -out request.pem -days 365
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
writing new private key to 'private.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AT
State or Province Name (full name) [Some-State]:Uienna
Locality Name (eg, city) []:Uienna
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Kofax
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:kofax.com
```

Afterwards, you can enter an optional password, which will protect the certificate. This is not mandatory.

The file content will look something like this:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICmDCCAYACAQAwUzELMAkGA1UEBhMCVQVXQzANBgNVBAMgMBIzpzW5uYTEPMA0G
A1UEBwwGVml1bm5hMQ4wDAYDVQQKDAVLb2ZheDESMBAGA1UEAwJhZj29mYXguY29t
MIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvlvUxQyhcbSBsXh1FZYH
/rigovKpWEd1l/zFM40i3EjtzuNoeQPsmYhWYaUR3Mq8AzfvrseDm2yLqu5lU/0f
1GVJzUN9qaDjLmWm94vJPRKz+CT5L2vTS/fmnl1B2IUfshNVAPXoeTOFqL0eRG63
9TbQn6aRgY6cv5QgJ0jN1jfeG16hZMRI0X0902RoovknQHTPHIXNgj/qZHvcvkh
JHz6yj9b5FNz0icrN5R8ymT7ovOmAYRXzhan1ZAIUV8C1Em4nsmzekzASAwwZQGw
AMgnuUuu/pRTSBxMY5I+mrhfEgJ9gudc1CEGT4XIR7lk6qzaulCW/ktmVZzKAjN
JQIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAKK2h3QKq7GFzG57xbgw5mV0Ssb
BVZ1KC9QbE0JEiHrkkKgcA3nuN9dCPCaaA7vvV5TahFWGTQKGOftWi+PvZAE
9sVeknBs48sWHfTxwstOoYga0/oLg1mlkzxikaqfPBjclB8PMdv7i0P6z0JpwcGt
eJUwgoFv/Bjs/J5xQ8a2gxR3ec0A0SbZpDGsvwBU5WLx2RtDe68VP4X5u/SjwbTb
+nw9ZSHKMGA53ekhw6Ixaq0j2gu/8HGwayj03T/QsbQkdY3cds0cBLZ6fGqzm
fJxTxutvN6YpImGfc3aPRNVZCGXQ/56Pt6j5KcZ82rOpqrT1kiJrYp3dRg=
-----END CERTIFICATE REQUEST-----
```

Go to www.thawte.com and request a free test SSL certificate.

Thawte, Inc. (US) | https://ssl-certificate-center.thawte.com/process/retail/trial_capture_csrd

Trial SSL Certificate ▶ 1) Options ▶ 2) Technical Contact ▶ 3) CSR ▶ 4) Summary

Enter Certificate Signing Request (CSR)

Select server platform: ?
 Server not listed

Server not listed ?
 other platform

What does a CSR look like?
 -----BEGIN CERTIFICATE REQUEST-----
 MIB2CQAUJMCAGWzGzAJBgnVBAytMrowFOYDVOQIEv5O63J0acBDBYXlv
 8SiuYTEOQMAcA1UEBxMHUreFZWmndEdMBSA1UECHMUUVShndRIENwanN1bH
 RpbmcyZ2MxGzAZBgNVBAsTEiRic3RpbmciRQWwYXU0WVudEiMCEGA1UEAxMadm
 idS9yWfFnb29keWVyLnRoYX0z55jb20wZm9uZDQYKozZhvchNAQEBBQADgY0AMGU
 XosBMMNjDvYmV2ZjwEGUvpm8BA1H1h5H5YKtTbP5Wc+heUoo03Lg092ScZUeM
 DJ4sbTZQn07Tu7ZA0JhoexlyhMpe2FwH0NhPJRPEeZrQFYaqOmqtH+wr9Jw5W4cE
 FoQ3MxYhHdJAGCjB9XReVuz5YNPwdrq36hx1Hrd7vAgMBAAGgADANBgkqhkiG9w0B
 AQQFAwQBgQIEI49xkeJuxuz.1FwQ9KCEU6UmEw1JagugCrs3Su1Zsh1Nv99q
 HTqAUC+PcCLM1Fb46GvH2EDFtzyvPHZwKKDzxNGetKn5500RhT8FIP3tn7sqsc
 401D7gmatWVR29kZKmpQLJgdYINz5Ou27iVE6MFw==
 -----END CERTIFICATE REQUEST-----

Paste Certificate Signing Request (CSR): ?

```
-----BEGIN CERTIFICATE REQUEST-----
MIICmDCCAYACAQAwUzELMAkGA1UEBhMCVQVXQzANBgNVBAMgMBIzpzW5uYTEPMA0G
A1UEBwwGVml1bm5hMQ4wDAYDVQQKDAVLb2ZheDESMBAGA1UEAwJhZj29mYXguY29t
MIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvlvUxQyhcbSBsXh1FZYH
/rigovKpWEd1l/zFM40i3EjtzuNoeQPsmYhWYaUR3Mq8AzfvrseDm2yLqu5lU/0f
1GVJzUN9qaDjLmWm94vJPRKz+CT5L2vTS/fmnl1B2IUfshNVAPXoeTOFqL0eRG63
9TbQn6aRgY6cv5QgJ0jN1jfeG16hZMRI0X0902RoovknQHTPHIXNgj/qZHvcvkh
JHz6yj9b5FNz0icrN5R8ymT7ovOmAYRXzhan1ZAIUV8C1Em4nsmzekzASAwwZQGw
AMgnuUuu/pRTSBxMY5I+mrhfEgJ9gudc1CEGT4XIR7lk6qzaulCW/ktmVZzKAjN
JQIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAKK2h3QKq7GFzG57xbgw5mV0Ssb
BVZ1KC9QbE0JEiHrkkKgcA3nuN9dCPCaaA7vvV5TahFWGTQKGOftWi+PvZAE
9sVeknBs48sWHfTxwstOoYga0/oLg1mlkzxikaqfPBjclB8PMdv7i0P6z0JpwcGt
eJUwgoFv/Bjs/J5xQ8a2gxR3ec0A0SbZpDGsvwBU5WLx2RtDe68VP4X5u/SjwbTb
+nw9ZSHKMGA53ekhw6Ixaq0j2gu/8HGwayj03T/QsbQkdY3cds0cBLZ6fGqzm
fJxTxutvN6YpImGfc3aPRNVZCGXQ/56Pt6j5KcZ82rOpqrT1kiJrYp3dRg=
-----END CERTIFICATE REQUEST-----
```

Total: US \$0 (Free Trial) < Back Cancel Continue

Paste the certificate request from the "request.pem" file into the text field and click Continue.

After that you need to agree to Thawte terms of service and you receive the test certificate via email.

Copy the text into a file in the "TOPCALL\SHARED" directory and rename it to "certificate.pem". If you request a real SSL server certificate, additional info about the company must be entered.

Ordering a real certificate will last approximately one week and don't get confused, if the web-page always mentions your "Web-Server" and not "Mail-Server". This is because, the main usage of such an SSL certificate is for a "Web-Server". But in reality there is no difference in the certificate, as it secures a server-name.

If you want to have a certificate, which is longer valid than one year, you have to change the "-days" parameter in the CREATE.BAT file. In the case of a certificate renewal you don't have to use CREATE.BAT anymore. It is sufficient to

order a renewal from your CA. There you will have to provide some info, like the order number and contact info. After some time (approx. a week), you will get the renewed certificate.

Currently if a certificate is no longer valid, this will only be viewable in the LINK-SM trace. Also if something goes wrong with the certificate verification, only error-codes are written in the trace. A complete list of error-codes will be appended in the next LINK-SM manual. Additionally there exists a future enhancement, that these errors will be listed as events in the event-viewer.

The SSL connection is established via the OpenSSL library, which is under OpenSource license, so it can be used for free.

As soon as the SSL connection is established, the data exchanged is encrypted. The procedure works this way: The sender encrypts the data with the public key of the recipient. The data can only be decrypted with the private key of the recipient. The public key is part of the certificate. This means after exchange of the certificates sender and recipient know each others public key. Furthermore anyone who sniffs between the connections will get the public key, but will not be able to decrypt the data, because of the absence of the private key.

You can configure TC/LINK-SM to support only secured connections to the Internet by setting registry keys TCLSM\SMSendSecure and TCLSM\SMRcvSecure to 2. This means that the message cannot be sent via email if the remote SMTP server does not support SSL, or does not accept the CA or TC/LINK's certificate.

You can also configure just a list of domains that shall only be contacted via secure connections, by setting registry keys TCLSM\SMSendSecure and TCLSM\SMRcvSecure to 1, and writing the domain names to registry keys TCLSM\SMSendSecDomains and TCLSM\SMRcvSecDomains. Each registry key can hold up to 1000 bytes of information (approx. 30 – 40 domains). If larger lists of domains are needed, you can use 2 links with different services (e.g. "SMTP" and "SMTPSSL"), configure one of them to require SSL always and use the recipient service for a decision whether SSL shall be used.

TC/LINK-SM verifies the remote certificate against one or more root certificates. These root certificates, which must be located in one file ("rootcerts.pem"), must also be installed on the link server. You can make commentaries between the root certificates, but not between the "---BEGIN" and "---END" lines. TC/LINK-SM Setup copies the file, which contains the root certificate from Thawte to "C:\TOPCALL\SHARED", which is the most distributed SSL certifier. If a customer encounters a partner with a different certifier, contact the partner to get the root certificate and copy it into the "rootcerts.pem" file.

If multiple link instances are installed, each of them can use its own SSL certificate. The folder where TC/LINK-SM looks for the PEM files is configurable in registry value TCLSM\CertificatePath.

If a message cannot be sent via a secure connection, the (optional) alternative fax address is used for sending. To make sure that SSL is used for the complete path that the message takes, configure TC/LINK-SM for direct delivery (TCLSM\UseDNS = 1 or 2, TCLSM\SMFixedRecipient = "").

2.2.10 Supporting "Fax over IP" to NetMoves (mail.com)

It is now possible to send a fax out of TCfW to NetMoves. The following prerequisites have to be met:

- HKLM\TOPCALL\TCLINKSM\TOPCALL\IncludeCover must be set to 1
- HKLM\TOPCALL\TCLINKSM\General\CompatibilityNoCover must be set to 0
- HKLM\TOPCALL\TCLINKSM\TCLSM\AcceptNetMoves must be created (DWORD) and must be set to 1
- Create a cover sheet for your fax. This sheet MUST look that way:

```
++MIME_START
X-TSI:+43-1-66133-8$UAdd0FXI$, $UTxt$
X-USERCODE:$Correl$
++MIME_END
```

(The telephone-number in the X-TSI field is only an example.)

Afterwards, it is now possible to send a fax to NetMoves using TCfW.

Example:

Sending a fax to 431661338272@faxes.com (keep in mind, NOT to send to +431... or to 00431....) with the subject "This is my first fax" (DO NOT FORGET TO INCLUDE YOUR COVER!)

This subject of the message will be converted to "#000012340003456789# This is my first fax"

If NetMoves can deliver this fax, you will get a notification with the subject
"Deliver notice: #000012340003456789# This is my first fax"
or, on failure (e.g.: wrong fax number, Destination-fax not online, etc)
"Non-deliver notice: #000012340003456789# This is my first fax"
or if you have no authorization to send a fax
"Failure notice: #000012340003456789# This is my first fax"

Note:

New registry key:

"HKLM\TOPCALL\TCLINKSM\TCLSM\SMFaxDomain" (STRING) **Default:** "faxesav.com"

NetMoves is sending a notification according to RFC1891. This notification will be ignored. See the next paragraph for more details.

Message Flow:

- When sending a message to NetMoves it will request an RFC notification if the recipient domain (which means the part after the "@" is in the recipient's email address) is the configured SMFaxDomain.
- Additionally, if the NetMoves functionality is switched on (TCLSM\AcceptNetMoves=0x1), the TC/LINK-SM will also alter the subject of the message. At the beginning of the subject it will add the correlation parameters (CifID, CifNr), which are enclosed then between hash symbols:
Subject: #000017640024956280# /SMC/YMACS1014 /20061109/001619
- The reason for doing this is that the final notification (which is sent back from NetMoves as a normal mail) will include the subject of the original message and based on this information the TC/LINK-SM can then find the appropriate KCS send order.
- Because of requesting the RFC 1891 notifications, the NetMoves server will send back also those RFC notifications. But it is important to understand that it will send back the notifications as soon as it took over the document, i.e. before the fax was really sent out via NetMoves fax channels, so it will always be a delivery notification, even if it points out later on that the fax number was wrong.
- Normally, when receiving such a notification, the TC/LINK-SM will set the status of the send order in TCOSS to "Sent OK" or "Cancelled", depending on whether it was a delivery or a non-delivery notification.
- **In case NetMoves is activated (TCLSM\AcceptNetmoves=0x1) and this notification contains anywhere (typically in the email address of the "From:" mime header field) the configured TCLSM\SMFaxDomain, the behavior will be different. It will ignore this RFC notification and it will not change the status of the KCS send order (so the status remains on "Active forwarded"). So you have to make sure to set the SMFaxDomain to the correct domain. If you do not know the domain, please contact support, who can help you finding it out with the help of TCP traces.**
- Later on, when NetMoves has sent the fax it will send a real notification (informing about success/failure of the real fax sending). This notification is received as a normal incoming mail and the subject will be the same as the original subject (containing the cifID, CifNr within # characters).

2.3 Mail Delivery in the Internet

In the following example, KCS user AI uses TCFW to send a message to the email address <nobody@nowhere.com>.

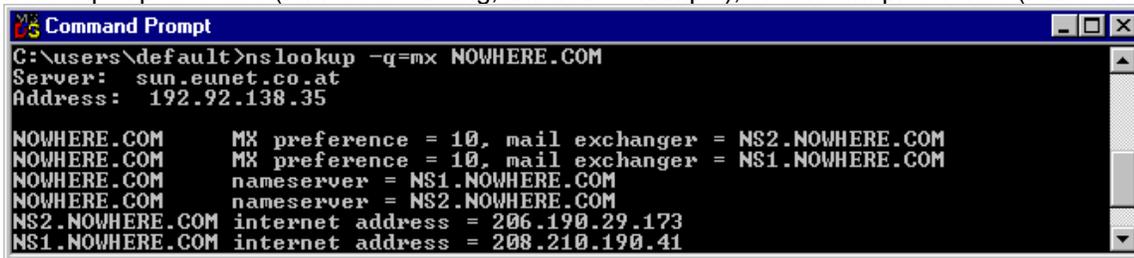
2.3.1 Routing from KCS to SMTP

2.3.1.1 Step 1: KCS -> TC/LINK-SM -> External Mail Server

- In TCFW, the destination address is "SMTP, nobody@nowhere.com".
- As soon as the user clicks the "send" button in TCFW, the message is put into the TC/LINK-SM queue.
- When TC/LINK-SM polls the queue next time, the message is taken.
- TCLINK.EXE does the address mapping, and conversion from TCI to the desired graphics format if required (e.g. for incoming faxes).
- TCMIME.DLL converts the message to RFC822 or MIME format. Output goes to a temporary file.
- TCLSM.DLL connects to the configured mail server ("smart host") and transmits the message file.
- After transmission, the message is notified according to the requested notification level, and the temporary file is removed.

2.3.1.2 Step 2: External Mail Server (Smart Host) -> Destination Host -> Final Mailbox

- The smart host checks the desired recipient domain from the SMTP envelope (<nowhere.com> in our example).
- It starts a DNS query for mail exchanger records ("MX" records) assigned to that domain.
- If successful, it gets one or more IP addresses that are responsible for mail delivery to the given domain. They may have equal preference (for load balancing, like in the example), or different preference (fallback configuration):



```

C:\users\default>nslookup -q=mx NOWHERE.COM
Server: sun.eunet.co.at
Address: 192.92.138.35

NOWHERE.COM      MX preference = 10, mail exchanger = NS2.NOWHERE.COM
NOWHERE.COM      MX preference = 10, mail exchanger = NS1.NOWHERE.COM
NOWHERE.COM      nameserver = NS1.NOWHERE.COM
NOWHERE.COM      nameserver = NS2.NOWHERE.COM
NS2.NOWHERE.COM  internet address = 206.190.29.173
NS1.NOWHERE.COM  internet address = 208.210.190.41
  
```

The configuration file on the DNS server for this example (omitting the "NS" record for responsible name server, which is not important here) will look like this:

nowhere.com	MX	ns2.nowhere.com	10
nowhere.com	MX	ns1.nowhere.com	10
ns2.nowhere.com	A	206.190.29.173	
ns1.nowhere.com	A	208.210.190.41	

- The smart host first takes the returned address that has the lowest preference value (or the first one, if there are more with the same priority) ... <ns2.nowhere.com>
- It tries to connect to the SMTP port of that host.
- If the connection can be established, the message is transmitted.
- If the connection fails, retries may be done for the same host (depending on the error).
- If the retries fail, then all the other mail host addresses are tried (in increasing preference order; <ns1.nowhere.com> in the example).
- If all that fails, the smart host may either look for any private routing tables, seek for any destination domain aliases (... to send the message to another smart host), or send a non-delivery notification back to the originator.

<nowhere.com> is the **mail-domain** while <ns1.nowhere.com> and <ns2.nowhere.com> are **host names**.

The difference in short:

- All email is always addressed to the mail-domain.
- "MX" records map mail domains to one or more host names (like in the example). Their names may also be the same (e.g. the host <microchip.com> may serve the mail domain <microchip.com>.)
- Host names are names for physical servers
- so-called "A" records map host names to IP addresses (in the example, <ns1.nowhere.com> to <208.210.190.41>)

The time between sending the message and receiving the non delivery notification may be quite long (in the range of several days; e.g. failure reason "Your mail could not be delivered for five days").

2.3.2 The “Direct Delivery” Feature of TC/LINK-SM

If “Direct delivery” is enabled, TC/LINK-SM does no longer require an external smart host. The complete DNS address resolution is done by TC/LINK-SM instead; the destination host is contacted directly.

2.3.3 Routing from SMTP to KCS

The delivery from distant originator to TC/LINK-SM is similar to the other direction (DNS lookup, delivery to TC/LINK-SM). However, inbound routing (from TC/LINK-SM to the KCS!) is a rather complicated process with many options and inbound routing was subject to frequent changes in the previous TC/LINK-SM and TCOSS releases.

2.3.3.1 Default Inbound Routing

Any email sent to <UserID@mail-domain> is routed to the KCS user’s Inbox.

Example:

TC/LINK-SM mail-domain is <company.com>, the KCS User ID is “user1”:
The only email address of user1 is <user1@company.com>!

When the same user sends from e.g. TCfW to the Internet, the originator address is composed from the KCS user ID and the link’s domain.

With the user from the previous example, this leads to
user1@company.com ... bingo.

2.3.3.2 Multiple Addresses for Receiving Email

If the user’s email address differs from his KCS User ID or if the user is to have more than one email address, this can be configured via inactive SMTPIN aliases the user profile. See 3.9.1 “User Profiles Setup for SMTP Aliases” for an example.

Background:

All inactive address entries are appended to the end of the rr99 **NODES section. Although they are not visible there, you can check all aliases on your system by using TCfW 3.01 or higher (Admin / User Profiles / Address View)

Example: (TCOSS below 7.08.00):

- TC/LINK-SM serves the mail domain “company.com” (defined in registry “...TCLINKSM\TCLSM\SMLinkDomain”)
- The user “MM” has an inactive address “SMTPIN,Max.Mustermann” (SMTPIN prefix is “postmaster:”)
- This gives a new (invisible) entry in the rr99 below the **NODES section:
postmaster:Max.Mustermann~,MM:~,
- So, if the TC/LINK-SM receives a message for Max.Mustermann@company.com, it will find a matching mail domain but no shadow user. Therefore, the address is mapped to use the local part of the Internet address, plus the default KCS service (from registry “...\TCLINKSM\Topcall\TCService”). The resulting address is
SMTPIN,Max.Mustermann
- The rr99 process replaces the service against the prefix of the service: the result is
postmaster:Max.Mustermann
- ... which matches the invisible entry in the rr99 memory image. The message is routed to the KCS user “MM”.

In the end, the message it is routed to the mailbox “MM”, i.e. a SMTP alias address for the user “MM” was created.

If there is no match (no user has this email alias address), the user “postmaster” receives this message. That is the reason to define the prefix of the SMTPIN service to be “postmaster:”!

Remarks:

- All inactive SMTPIN addresses in the user profiles provide Internet mail aliases on the **same** mail domain (the one configured with TC/LINK-SM); therefore, you need not enter a domain with SMTPIN addresses.
- All inactive SMTP addresses in the user profiles provide Internet mail aliases on any domain; therefore, you must always enter full Internet addresses (including domain!) with SMTP addresses.
- The rr99 process was changed to exact match in TCOSS 7.08.00. The invisible rr99 entry will look like:
postmaster:Max.Mustermann,MM:,
(Note there are no ~ !)

This may influence all addresses that did not match exactly (they did work in prior TCOSS releases, but fail as TCOSS is upgraded. Make sure to enter exact aliases in the user profile.)

- TCOSS 7.08.00 and higher have a new rr99 section: **INBOUND. This section MUST be modified for inbound routing via SMTPIN:

```
**INBOUND
```

```
postmaster:~, ,search for SMTPIN aliases; non-matching to postmaster!
```

```
,, no default required because prefix already is existent user
```

Please refer to the TCOSS 7.08.02 release description for details.

2.3.4 Message / Notification Loops

As mail routing in the Internet can be quite complex, loops may occur.

Example 1:

- A message is sent from an invalid originator address (e.g. typing mistake in a mail client setup) to a non-existing recipient.
- The mail server finds out that the recipient does not exist and sends back a non delivery notification to the (invalid!) originator address.
- As this notification is a plain-text message to an invalid address, it may cause another non-delivery notification to be generated, and so on, leading to looping notifications.

Example 2:

- A message is sent from a valid originator to a valid recipient.
- One of the DNS entries on the way to the recipient is wrong; therefore, the message is delivered back to the original mail server.
- The original mail server makes a DNS query, gets the same result as before, attempts delivery again → looping message.

TC/LINK-SM loop detection:

- The hop count is checked by means of counting the number of time stamps. If the configured maximum hop count is exceeded, the message is sent to the local postmaster.
- Notifications are detected by an empty "MAIL FROM:<>" address (as recommended by RFC821)
- Notifications for notifications are never sent; they are reported to the local postmaster instead.
- In addition, as some originators are known as misbehaving, you can configure a list of originators that shall never be notified. Simply add them (full address, "localpart@domain") to the Registry Multistring "...TCLINK-SM\TCLSM\NeverNotify"!

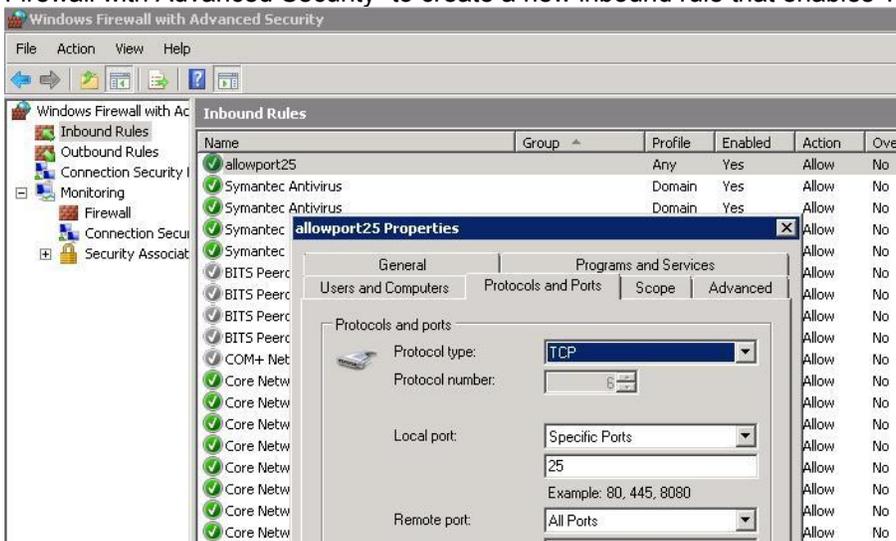
3. INSTALLATION

As SMTP is an open, bi-directional mail transfer protocol, there are many different scenarios it can be used. The most important ones will be described on the following pages but almost any combination of them is also possible. Therefore, installation of TC/LINK-SM may become quite complex.

3.1 Prerequisites

Please consult the *TC/LINK Manual* for all general requirements (KCS, operating system, and so on)! TC/LINK-SM additionally needs the following:

- For identification of TC/LINK-SM, select a **mail-domain** (e.g. <company.com>) first. This must be unique in the area TC/LINK-SM is reachable (for the Internet, you obtain this mail domain name from your ISP (Internet Service Provider); for Intranets, contact the network administrator).
- Optionally, the TC/LINK-SM host name may be different to the mail-domain (e.g. <link.company.com> – see 3.3 “TC/LINK-SM for Connecting an Existing KCS System to the Internet” for details).
- Obtain a **fixed IP address** for the TC/LINK-SM host name. This is a major difference to most private internet accounts as they get a dynamically allocated IP address (for Internet access, contact the ISP; for Intranets the network administrator).
- Find out the default router IP address (e.g. <193.81.166.126>), and the subnet mask (e.g. <255.255.255.0> for a class C address range)
- SMTP requires a TCP/IP connection between the SMTP servers and clients. Set up the TCP/IP stack on the Link Server (Control Panel / Network / TCP/IP) and enter the data collected above (IP address, domain name, default router, subnet mask).
- Winsock 2 support is required (delivered with Windows). TC/LINK-SM may not work with TCP/IP stacks from different (non-Microsoft) vendors.
- Make sure that the firewall (if installed) enables SMTP connections to and from the designated TC/LINK-SM server IP address. You can check this with Telnet to “smtp”; if this does not work, contact the local firewall administrator. Note: On Windows Server 2008/2012, input via port 25 is by default disabled. Use the administrative tool “Windows Firewall with Advanced Security” to create a new inbound rule that enables TCP input via port 25.



- Edit the HOSTS file (in Windows\System32\drivers\etc); add the external mail server (“smarthost”):

Sample hosts file:

127.0.0.1	localhost	# local PC
193.154.160.101	mail.austria.eu.net smarthost	# remote mail server (smarthost)

Notes on HOSTS file:

- Every time a message is sent out to SMTP, TC/LINK-SM needs to resolve the distant hostname. This could be done via DNS but would reduce performance. Therefore, it is recommended to have these entries locally (in the HOSTS file).
 - Every host can also have multiple alias names (separated by white space; in the example above, “mail.austria.eu.net” and “smart host” will both resolve to “193.154.160.101”).
- The TC/LINK-SM needs a dedicated temporary directory which is not used by any other application (“c:\temp” is NOT a valid choice). It is essential that this directory is not cleared automatically at link start (a folder below “C:\TCOSS\TCLP\TMP” is NOT a valid choice). The default value is C:\TCOSS\TCLP\WORK\TCLINKSM. Set the permissions to Full Control for the TC/LINK-SM Windows User account.
 - As with all other TC/LINKs, this Windows user account needs the ‘Log On As A Batch Job’ special user right when the TC/LINK-SM is started via TCSRVD (recommended).
 - After all that, do not forget to reboot the TC/LINK-SM server to make all these settings become effective.

3.2 Common Installation Steps

There are some configuration steps needed for all scenarios. These are described here.

3.2.1 Installation Steps on KCS Server

With the release 1.09, TC/LINK-SM automatically creates most of its dependencies on KCS (SMTP and SMTPIN service, link queues, guest and “postmaster” users, notification and “onlyimg” covers, default templates). Only the following steps are required:

- Create the Link user (“TCLINK”); this user is automatically present with new TCOSS installations (TCOSS 7.23.xx or higher).
- Set up rr99 to reroute all SMTP messages for the local mail-domain. Otherwise, you may get bad performance and open send orders for messages sent via SMTP to local recipients. Example for TCOSS 7.08 or higher (all “TCLSMxxx” entries apply for TC/LINK-SM, all “TCLOCxxx” are for TC/LINK-OC):

```
**ROUTE
,, reroute local domain to SMTPIN service
TCLSMQI:~@company.com,postmaster:~, for TCLINKSM
TCLOCQI:~@company.com,postmaster:~, for TCLINKOC

**INBOUND
TCLSMQI:~, ,search for local SMTP aliases (full SMTP addresses)
,, not found: no inbound routing, send to SMTP

postmaster:~, ,search for SMTPIN aliases; non-matching to postmaster!
,, no default required because prefix already is existent user

TCLOCQI:~, ,search for local SMTPOC aliases (full address)
TCLOCQI:~, invalid, address not found locally -> nondelivery
```

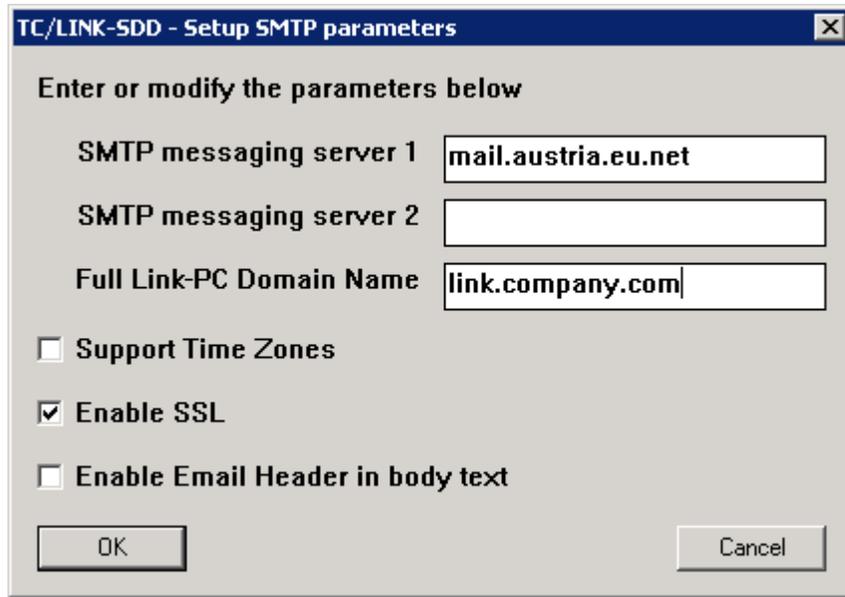
- If you want to use any aliases for KCS user names on the local domain, enter all user aliases as inactive SMTPIN addresses (“localpart” only).

A short example for inbound routing is given in 2.3.3.2 “Multiple Addresses for Receiving Email”.

3.2.2 TC/LINK-SM “Easy Installation”

Links come with a special “Easy Installation” setup mode. This mode enters useful defaults for almost every parameter and helps to get the Link running in a very short time.

See the TCLINK Manual for all common setup screens; TC/LINK-SM requires the following special parameters:



TC/LINK-SDD - Setup SMTP parameters

Enter or modify the parameters below

SMTP messaging server 1

SMTP messaging server 2

Full Link-PC Domain Name

Support Time Zones

Enable SSL

Enable Email Header in body text

OK Cancel

SMTP messaging server 1: Host name of the server to deliver all messages to SMTP (“smarthost”). You can enter the name or the IPv4 address of the smart host. Optionally, a port number can be added, separated via a colon, e.g. mail.austria.eu.net:25. The specified port number then overrides the globally defined port number for sending to the internet (*TCLSMPort2SMTP*).

If you specify the host name, it is recommended to add an IP address mapping for this host into the local HOSTS file (for better performance).

SMTP messaging server 2: Here you can configure an alternative smarthost, which will be contacted if the main smarthost is not reachable.

Full Link-PC Domain name: This must be the mail domain name of the Link server. (Exactly the same string must also be entered in the local HOSTS file and, if used, in the DNS server MX record.)

Support Time Zones: Here you can enable multiple time zone support as described in the TC/LINK manual.

Enable SSL: This should be checked, if SSL should be available (see chapter 2.2.9 for more details). The checkbox is not available for TC/LINK-OC.

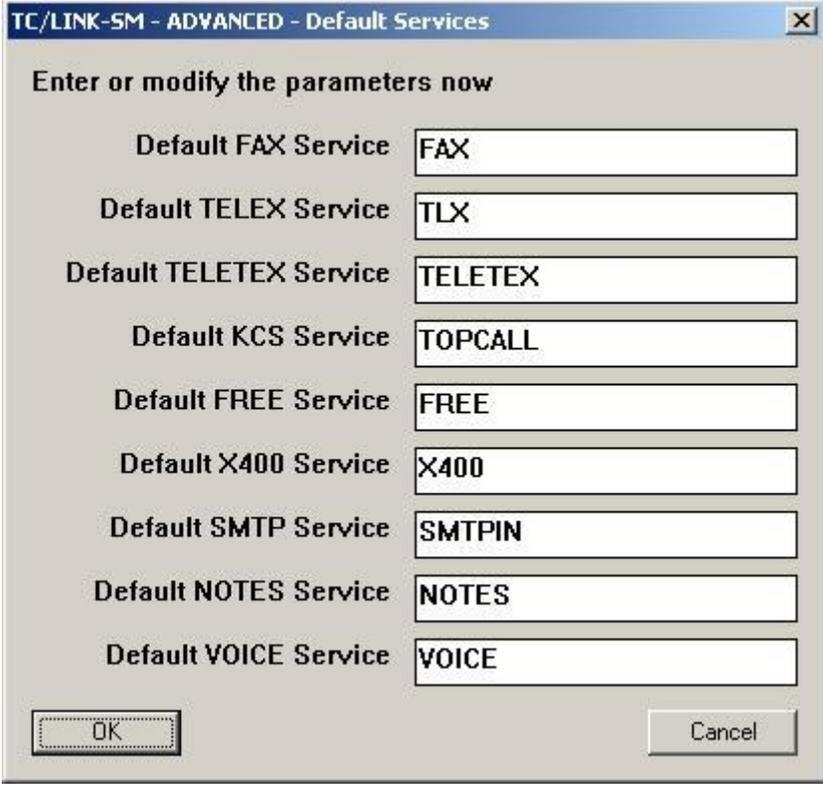
Enable Email Header in body text: Check if you want to prefix the body text of incoming mails with email header information. Only for TC/LINK-SM, TC/LINK-SDD and TC/LINK-MX7. For details see section Installation - Special Features – Email Header in Body Text.

3.2.3 TC/LINK-SM “Advanced Installation”

If you got TC/LINK-SM running, it is possible to fine-tune some parameters by running “Advanced Setup”. Please see the *TCLINK Manual* for all common configuration data.

3.2.3.1 Default Services Setup

This screen has an important difference compared to the standard TC/LINK setup:



TC/LINK-SM - ADVANCED - Default Services

Enter or modify the parameters now

Default FAX Service	FAX
Default TELEX Service	TLX
Default TELETEX Service	TELETEX
Default KCS Service	TOPCALL
Default FREE Service	FREE
Default X400 Service	X400
Default SMTP Service	SMTPIN
Default NOTES Service	NOTES
Default VOICE Service	VOICE

OK Cancel

You must enter “SMTPIN” as the default KCS service if you want to use the special inbound routing with SMTPIN alias names.

3.2.3.2 TC/LINK-SM Advanced SMTP Parameters Setup

After the "Easy Installation" SMTP setup screen, the following mail-specific parameters can be configured:

Direct delivery: you can select the level of DNS address resolution done by TC/LINK-SM. "Disabled" is the compatible setting to all releases prior to 1.09.00; "Hosts lookup" only resolves "A" records, and "MX" lookup is a fully-featured address resolver.

Temporary directory: is used for intermediate storage of messages.

- Must be exclusively used by TC/LINK-SM.
- If you install multiple TC/LINK-SMs on the same workstation, you must enter different directories for each TC/LINK!

Maximum connections: Gives the maximum number of possible simultaneous incoming connections. It is internally limited to a maximum of 20.

Preferred MIME text coding: Select the standard coding for non-ASCII text (should always be "quoted-printable" ... see NOTE!). This parameter applies only for sending from KCS to SMTP.

Preferred MIME binary coding: Select the standard coding for binary attachments (should always be "base64" ... see NOTE!). This parameter applies only for sending from KCS to SMTP.

Preferred notifications format: Select which notifications format TC/LINK-SM shall use. For optimum performance, double-check with your provider which format the used smart host supports (Standard Notifications, "Return-Receipt-To", "Rr", or RFC1891...1894; see 2.2.6 "Delivery / Non-Delivery Notifications" for details)!

"Open Line" cycle: This value determines how often the SMTP messaging server is polled. A zero entry or an empty field disables polling. See 3.9.5 "Operation over a One-Way Dialup Line" for details!

IP masking option: TC/Link-SM gives the possibility for access restriction via IP authentication. You can select

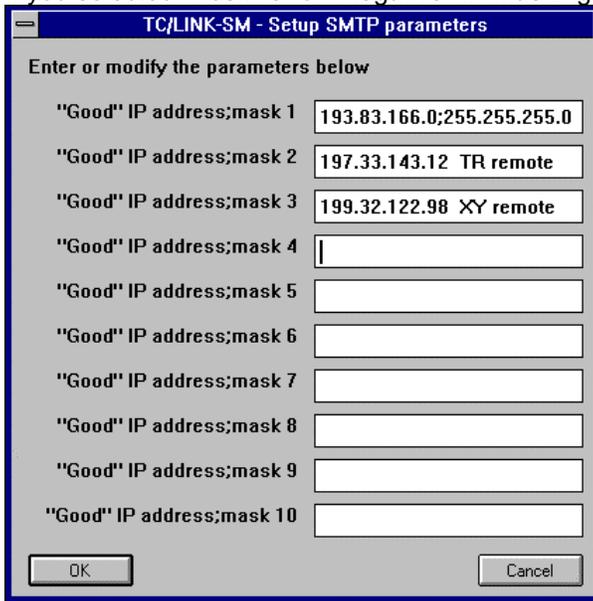
- "Positive" (only IP addresses and -ranges entered in the next screen can access KCS)
- "Negative" (all IP addresses except the ones given in the next screen can access KCS)
- Disable IP authentication

If a user wants to connect to TC/LINK-SM with an IP address not allowed to do so, then TC/LINK-SM sends an SMTP error message and does not accept the connection.

NOTE: 8Bit encoding is **NOT** supported anymore due to earlier problems. It will not be used even if you select it in the setup.

3.2.3.3 IP Authentication Setup

If you selected "Positive" or "Negative" IP Masking, an additional screen is displayed (example for "Positive" setting):



Please enter all IP addresses and ranges that should be allowed to access KCS.

- The content of the list is of the form Format <Address>;<mask>;<domain>
- The <mask> operates similar to the "subnet mask" in the TCP/IP setup
- <mask> defaults to "255.255.255.255"
- <domain> defaults to "" (originator domain is not checked if this setting is empty)
- Do not enter leading zeroes (197.033.143.012 does NOT work!)
- Comments may be entered after the <domain> separated by at least one whitespace! Do not enter any blanks in or between IP addresses. For line comments, <Space> should exist only at the beginning of the line. String after <Space> should not contain any spaces.
- If only domain name is required (without IP address or subnet mask) then start the line with a semi-colon.

Examples (Positive authentication):

Entry	Effect
193.83.166.0;255.255.255.0 Text	only users in the range 193.83.166.xxx can access KCS; "Text" is comment
197.33.143.12	allows this single IP address to access KCS
0.0.0.0;0.0.0.0	any IP address can access KCS
193.83.166.4;255.255.255.251	Allows only 193.83.166.4 and 193.83.166.0 to access KCS
193.0.0.0;255.0.0.0;kofax.com	Any IP address in 193.x.x.x with originator domain "kofax.com" can access KCS

Example (Negative authentication):

Entry	Effect
0.0.0.0;0.0.0.0;spam.com	Does not accept any mail originated by <spam.com>

If you need to have more than ten entries, you can enter them via REGEDT32 (The registry Multi-string "...TCLINKSM\TCLSM\SMIPList"). The complete list is limited to 5000 characters in total, and it is ignored if it is longer.

It is also possible to specify whole email addresses and to use a text file instead of the registry. The file name is configurable via registry value "...TCLINKSM\TCLSM\SMIPListFile. You can either specify the file name only (if the file is in directory C:\TCOSS\TCLP) or a complete path name.

The default location is C:\TCOSS\TCLP\domainlist.txt.

An entry in the domain list file can have either the syntax explained above, or can simple be the domain name or the complete email address. Leading spaces are not allowed.

Example for a “domainlist.txt” file:

```
193.83.166.0;255.255.255.0 Kfx
;john@hotmail.com
;coolmail.com
```

If this file does not exist, the values in registry key SMIPList will be used. The functionality of the key “SMIPMasking” applies to both configuration mechanisms. So you can specify whether this list is to be used as a “good” or “bad” IP list.

3.2.3.4 TCP Trace / Hop Count / Message Limits Setup:

Enable TCP trace: Yes ... writes all data from / to the Internet to the trace file. If switched on and with the general trace level set to 0x0, a plain SMTP/MIME trace will be created.

Maximum hop count: Indicates the maximum number of hops before a message originally sent to SMTP is re-routed to the local post master as a problem report. Hops are counted by means of the MIME “Received:” timestamps.

Maximum message size from SMTP: configures a limit for messages received from SMTP. Note that the limit is only applied if the connected client/host supports the EHLO/SIZE SMTP extension (RFC 1870).

Maximum message size to SMTP: configures a limit for messages sent to SMTP. If a MIME-encoded message is larger, it will be negatively terminated on KCS.

Combine all text blocks to a single block: If checked, TC/LINK-SM will put all text of the message to SMTP together and position it at the beginning of the message. All attachments follow after the text block.

3.2.4 TC/LINK-OC “Easy Installation”

In “Easy Installation” mode, TC/LINK-OC requires no mail-specific configuration inputs.

Special defaults are

- Link domain name is taken from the TCP/IP setup (workstation name only)
- Smart host setting empty
- DNS delivery disabled
- Sending without shadow user disabled
- Polling of smart host disabled

Note:

If you try to change the defaults listed above (e.g. by regedt32), then TC/LINK-OC will be started as TC/LINK-SM and therefore require a license.

3.2.5 TC/LINK-OC “Advanced Installation”

In “Advanced installation” mode, you can change some mail-specific parameters. These are the same as for the TC/LINK-SM “Advanced Installation”, except for the special defaults listed in 3.2.4 “TC/LINK-OC “Easy Installation””.

To install TC/LINK-SM, run the setup program on the link PC and fill in all required parameters. Please see the TC/LINK Manual for the general parts of the installation procedure.

3.2.6 Final Installation Steps

After performing scenario-specific setup steps, you should do the following:

- Set the trace level to a low value for optimum performance
- Configure access rights if necessary
- For high reliability, configure TC/LINK-SM to run as a service (controlled by TCSRVR); be sure to configure automatic start-up for TCSRVR.
- Reboot the TC/LINK-SM server to check for automatic start-up.

3.3 TC/LINK-SM for Connecting an Existing KCS System to the Internet

This is probably the most common scenario for using TC/LINK-SM.

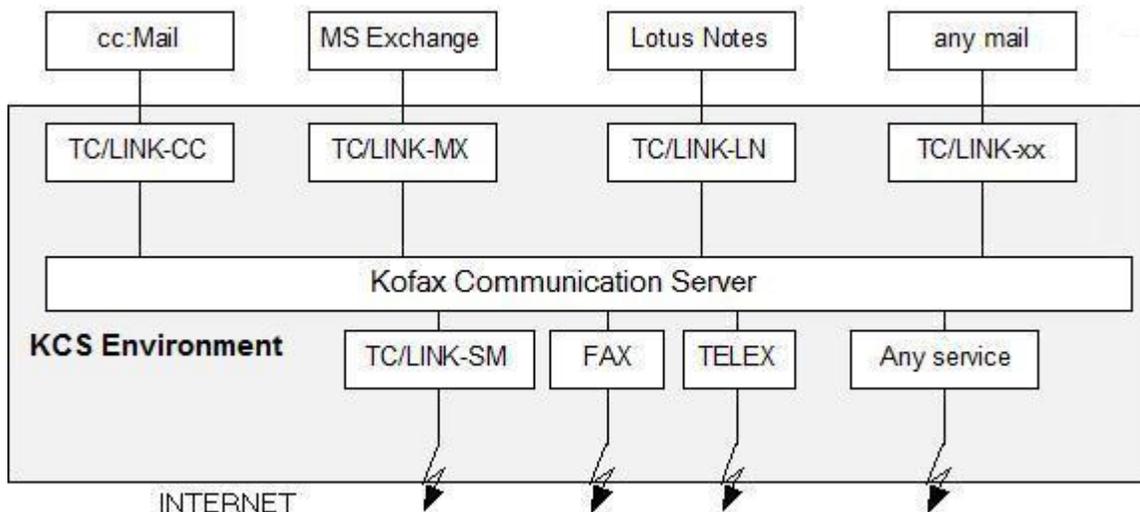
3.3.1.1 Scenario

- A customer with an existing KCS system wants to get access to Internet mail for all systems connected to KCS.
- User profiles are set up already. Every KCS user shall get his own email address, with a single common mail-domain (in our example, <kofax.com>)
- All undeliverable mail shall be sent to the local user "postmaster".

3.3.1.2 Solution

- Get Internet access from any Internet Service Provider (ISP).
- install TC/LINK-SM, and
- configure it to use the ISP's smart host.

The KCS server becomes an MTA and handles all Internet Mail addresses of the company's mail domain.



3.3.1.3 Required Additional Setup:

- Make sure that an Internet account is available. This may either be a dial-up connection or a leased line, according to your needs for throughput and security. Remember that you need a fixed IP address for TC/LINK-SM.
- Find out the domain name and IP address of the ISP's smart host (e.g. <mail.austria.eu.net> / <193.154.160.101>). This is necessary to deliver messages to SMTP.
- Find out the IP address(es) of your ISP's DNS servers. Enter them at the TCP/IP setup on the TC/LINK-SM server (Control Panel / Network / Protocols / TCP/IP / DNS).
- Get an "A" and "MX" resource record in the ISP's DNS server, pointing to the TC/LINK-SM server. Check this setup with the "nslookup" tool (see 3.11.1.3 "Nameserver Configuration – nslookup"). This is necessary to receive messages addressed to the Link domain.
- Assign a mail queue at your ISP if you have a one-way dialup connection (see 3.9.5 "Operation over a One-Way Dialup Line"). This is necessary to avoid loss of messages if anybody from outside wants to send mail while TC/LINK-SM is offline.
- Check for the notifications format supported by your ISP's smart host (see 2.2.6 "Delivery / Non-Delivery Notifications" for available formats); configure TC/LINK-SM to use this.

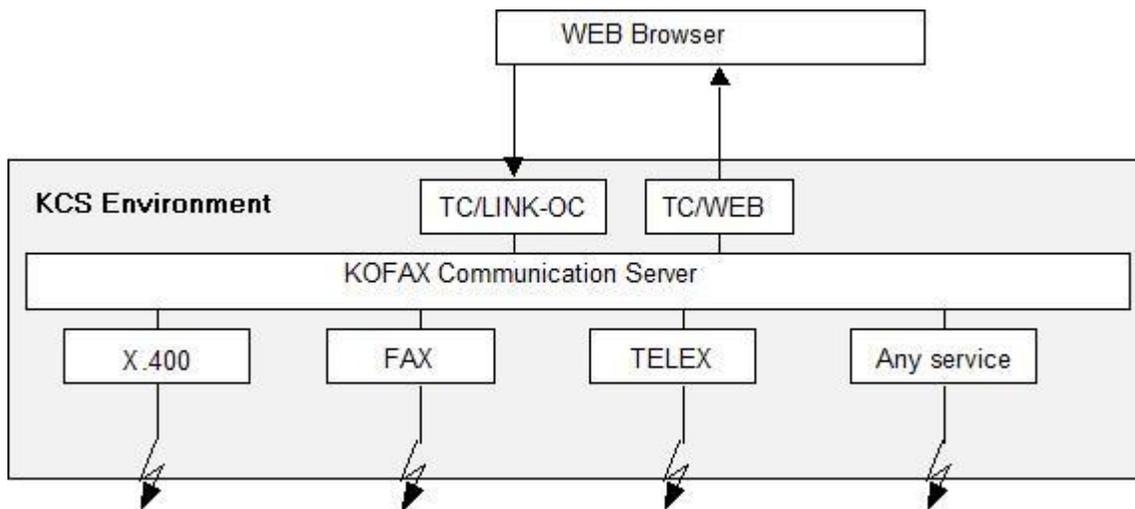
3.4 TC/LINK-OC for Use with TC/Web

3.4.1.1 Scenario:

- Customer already uses (or wants to use) Web Browser based mail access in his Intranet and intends to add additional services via web access to a KCS server.

3.4.1.2 Solution:

- Install TC/LINK-OC
- Install TC/WEB from the Kofax Communication Server setup. During TC/WEB setup, enter the TC/LINK-OC PC name and the link domain name, as described in the TC/WEB manual.



3.4.1.3 Required Additional Setup:

- Create a KCS user profile for every user.
- Configure user rights according to your needs.

3.4.1.4 Addressing Shortcut

In this scenario, you can use an addressing shortcut: Instead of addressing your mail e.g. to "FAX#123@company.com", you can use simply "FAX#123".

Note:

- No "@" is allowed in shortcut addresses (e.g. <"NOTES#KAichner@KFX"> is not allowed as a shortcut. You must use the full form <"NOTES#KAichner@KFX"@company.com> instead.)
- With TCOSS releases prior to 7.23, shadow users are only found if the originator address is given in the format "KCS UserId@domain". If you need to match shadow users by SMTP aliases, you need a TCOSS upgrade to 7.23 or higher (See the *TC/LINK Manual* for a detailed description of the new "Enhanced Originator Mapping" feature.).

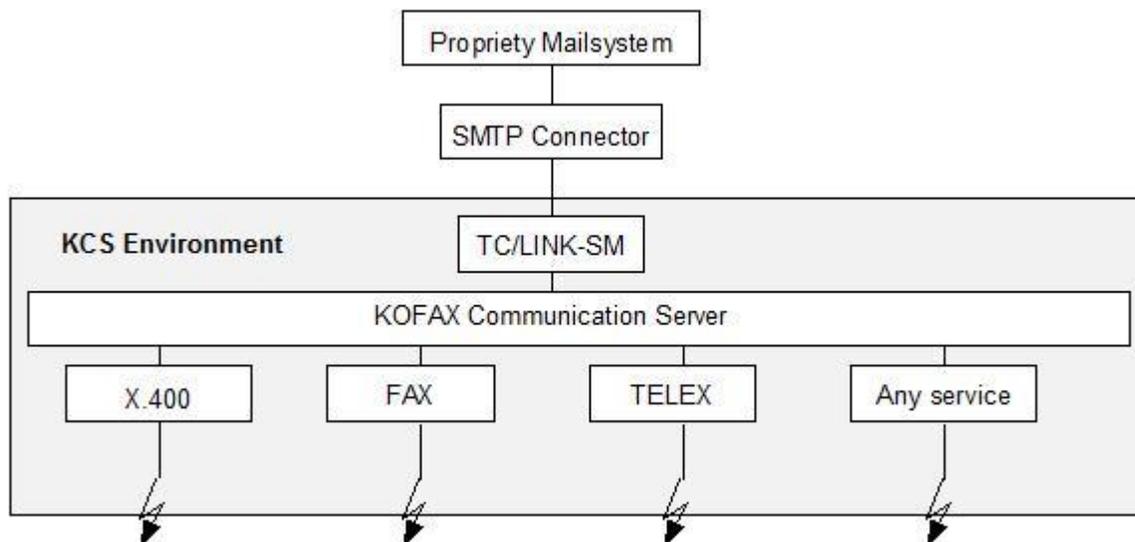
3.5 TC/LINK-SM for Connecting a Proprietary Mail System to KCS

3.5.1.1 Scenario:

Customer has a proprietary mail system and wants to connect it to a KCS server to get use of all available services, but no TC/LINK is currently available for this mail system.

3.5.1.2 Solution:

If a SMTP connector is available for the proprietary mail system, you can use this to connect to KCS via TC/LINK-SM.



3.5.1.3 Required Additional Setup:

- Enter the TC/LINK-SM hostname in the messaging server configuration of the proprietary SMTP connector. This is required for sending to Kofax Communication Server.
- Enter the proprietary SMTP connector hostname as "messaging server" in the TC/LINK-SM setup. This is required for sending from KCS (e.g. incoming faxes, notifications to the mail system).
- Select the notifications format according to the capabilities of the proprietary SMTP connector.
- Configure the proprietary SMTP connector's user rights, message format options, etc. to fit the needs of TC/LINK-SM.

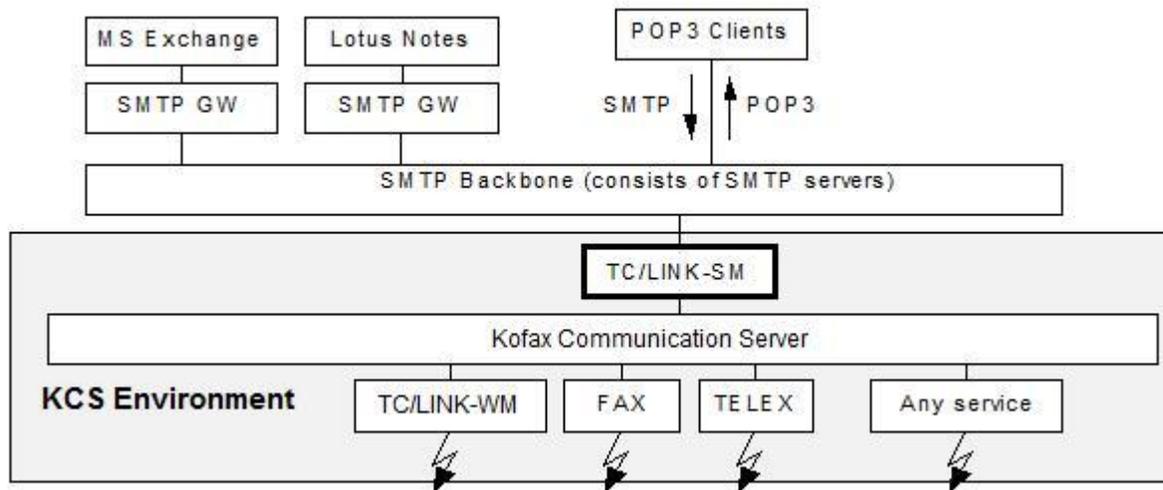
3.6 TC/LINK-SM for Connecting Many Proprietary Mail Systems to KCS

3.6.1.1 Scenario:

Customer has already an existing internal SMTP backbone that interconnects his proprietary mail systems. The routing between the mail systems is set up already; additional services shall be made available to all users on all mail systems by installing a KCS server.

3.6.1.2 Solution:

TC/LINK-SM can be installed to connect the KCS system to the existing SMTP backbone. Then, all users with access to this backbone can use SMTP to access the KCS server to send faxes, telexes, Internet messages. In this case, SMTP is being used INSTEAD OF numerous TC/LINKs to different email systems.



3.6.1.3 Required Additional Setup:

- Enter the SMTP backbone server (the server that does all the mail routing) in the “messaging server” setup of TC/LINK-SM.
- Configure the SMTP backbone server for routing to and from the TC/LINK-SM mail-domain (depends on the used backbone; may e.g. be a “A” and “MX” record like in 3.3 “TC/LINK-SM for Connecting an Existing KCS System to the Internet”)

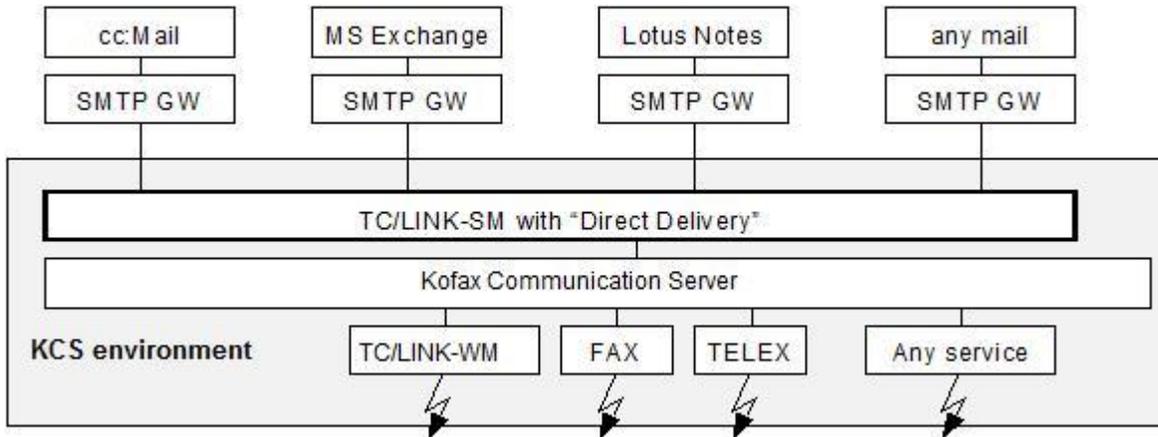
3.7 TC/LINK-SM for Use as an Intranet SMTP Backbone

3.7.1.1 Scenario:

A customer has multiple different propriety mail systems, and wants to connect them via their SMTP connectors by setting up an SMTP backbone. Additional services should be made available by connection to a KCS server.

3.7.1.2 **Solution:**

All propriety mail systems can be tied together using the SMTP protocol. The KCS system including TC/LINK-SM can serve as an SMTP backbone.



3.7.1.3 **Required Additional Setup:**

- Enable the "Direct Delivery" feature during TC/LINK-SM "Advanced Installation".
- Make sure that all distant server host names are either entered to the local HOSTS file or are available via DNS.
- If you decided to use DNS, configure your DNS server(s) in the TCP/IP setup on the TC/LINK-SM PC.
- Enable the routing feature (SMRouteEnable = 1) on TC/LINK-SM.
- Configure all connected SMTP gateways to send mail to TC/LINK-SM (enter the TC/LINK-SM hostname into their setup). If name resolution is done via DNS, enter an "A" and "MX" record for TC/LINK-SM.
- If you maintain shadow users on KCS, make sure that they have at least one inactive SMTP address (full address, including domain). This is required as that the SMTPIN aliases will only work for users on the local domain (<company.com>).

3.8 Multiple TC/LINK-SM installations

3.8.1 Multiple TC/LINK-SMs in Parallel / Load Balancing

If your scenario uses DNS for name resolution, you can configure the “MX” records of your domain to distribute mail to several parallel mail servers.

Example: load balancing to five parallel mail servers

company.com	MX	mail1.company.com	10
company.com	MX	mail2.company.com	10
company.com	MX	mail3.company.com	10
company.com	MX	mail4.company.com	10
company.com	MX	mail5.company.com	10
mail1.company.com	A	193.81.166.6	
mail2.company.com	A	193.81.166.8	
mail3.company.com	A	193.81.166.19	
mail4.company.com	A	193.81.166.33	
mail5.company.com	A	193.81.166.47	

Up-to-date DNS servers rotate the order of MX records with equal preference in every query response. Therefore, any time mail will be delivered to <company.com>, it will in fact be delivered to a different TC/LINK-SM.

Note:

- To maximize throughput, all instances of TC/LINK-SM must be installed on separate PCs.
- All TC/LINK-SMs must have exactly the same setup (the configured Link mail-domain is always <company.com>.). The only difference is the HOSTS file: all will have an entry for <company.com> pointing to the local IP address. Therefore, the HOSTS file must be local; shared HOSTS files via network will NOT work.
- The TCP/IP connection to your ISP must be fast enough to handle this increased traffic. It does not make sense to implement load balancing for a slow modem connection.

3.8.2 Multiple TC/LINK-SMs in Parallel / Fail-Save Design

You can use the MX records to configure two (or more) TC/LINK-SMs for a fail-safe design.

Example: one primary mail server, one backup server

company.com	MX	mail1.company.com	10
company.com	MX	mail2.company.com	100
mail1.company.com	A	193.81.166.33	
mail2.company.com	A	193.81.166.47	

As long as <mail1.company.com> is running, all mail will be delivered to it. As soon as it fails, mail will be delivered to <mail2.company.com> as a fallback.

Note:

- For fail-save design, both TC/LINK-SMs should run on a separate PC.
- Both TC/LINK-SMs must have exactly the same setup (except for the local HOSTS file that must have the entry <company.com> pointing to the local machine IP address.)
- Make sure that you are always online. Otherwise, it will be better to configure an external fallback server (see e.g. 3.9.5 “Operation over a One-Way Dialup Line”).

3.8.3 Multiple TC/LINK-SMs on the Same Workstation – Single IP Address

To allow different configurations parameter for SMTP (e.g. different originator domains), several instances of TC/LINK-SM can be run in parallel on the same machine.

For the setup, the following steps are required:

- Edit the Defaults.ini file for every Instance of TC/LINK-SM as described in the TC/LINK manual.
- Run the setup for every instance of TC/LINK-SM. Make sure to enter different temporary directories for every Link.
- Enable incoming connections only on one single Link (all other must have the "maximum connections" parameter set to zero).
- If required, set up routing between the different link queues (rr99).

Note: It is theoretically possible to enable multiple listeners by configuring different TCP/IP port numbers (every TC/LINK-SM uses different Port number). However, as this port must be known by all distant stations, it is **not recommended** (every SMTP server usually uses the so-called "well-known port" 25 for SMTP).

3.8.4 Multiple TC/LINK-SMs on the Same Workstation – Multiple IP Addresses

If multiple TC/LINK-SMs are installed on a PC with multiple LAN adapters or multiple IP addresses, you can bind any instance of TC/LINK-SM to a unique IP address directly. Therefore, one receiving Link can be installed per available IP address of the server.

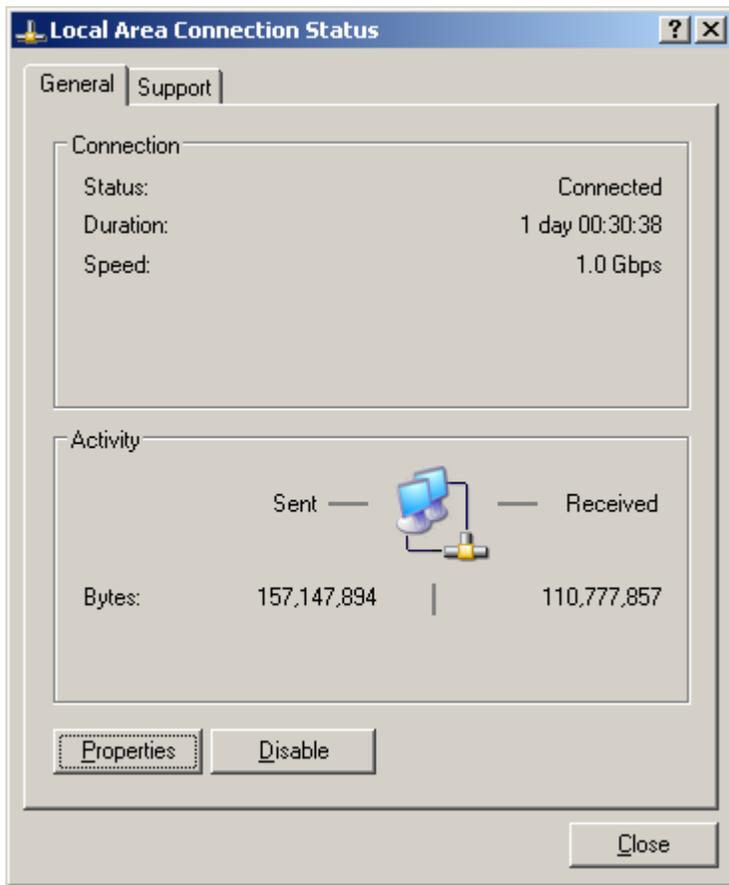
To do this, fill the registry key ". . \TCLSM\OwnIPAddress" of every installed instance with the desired IP address.

3.8.4.1 Configuration for Multiple IP Addresses on Single LAN Adapter

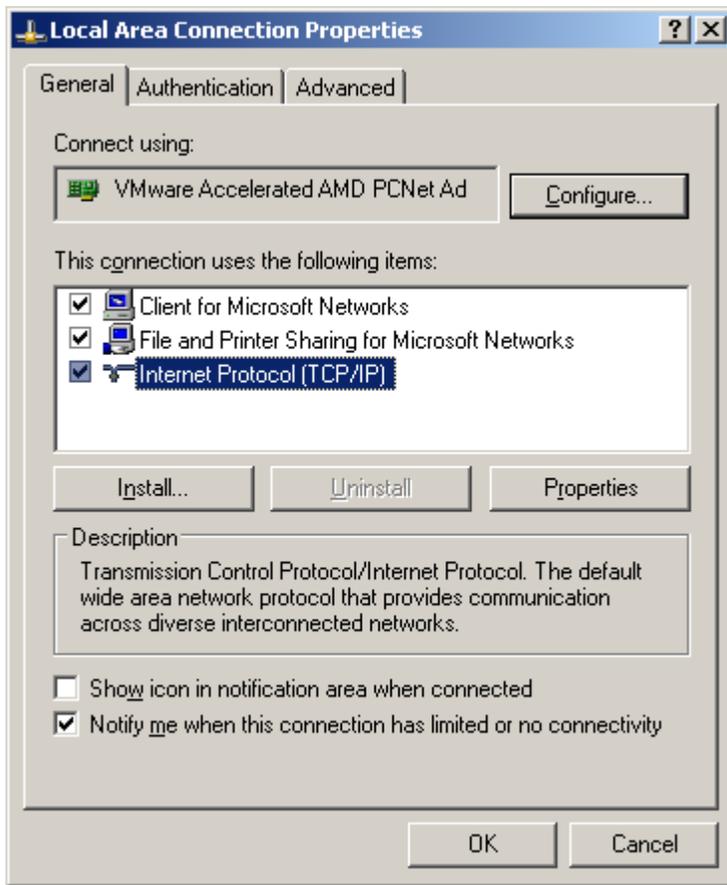
In the "Control Panel/Network/Protocols/TCP/IP Protocol/Properties/IP Address/Advanced" screen, there is a possibility to configure multiple IP addresses for a single LAN adapter. For this purpose, DHCP must be disabled.

Configuring multiple IP addresses in Windows 2003:

Click the **Start** button on bottom of the screen and select **Control Panel | Network Connections | Local Area Connection**.



Click on **Properties**.

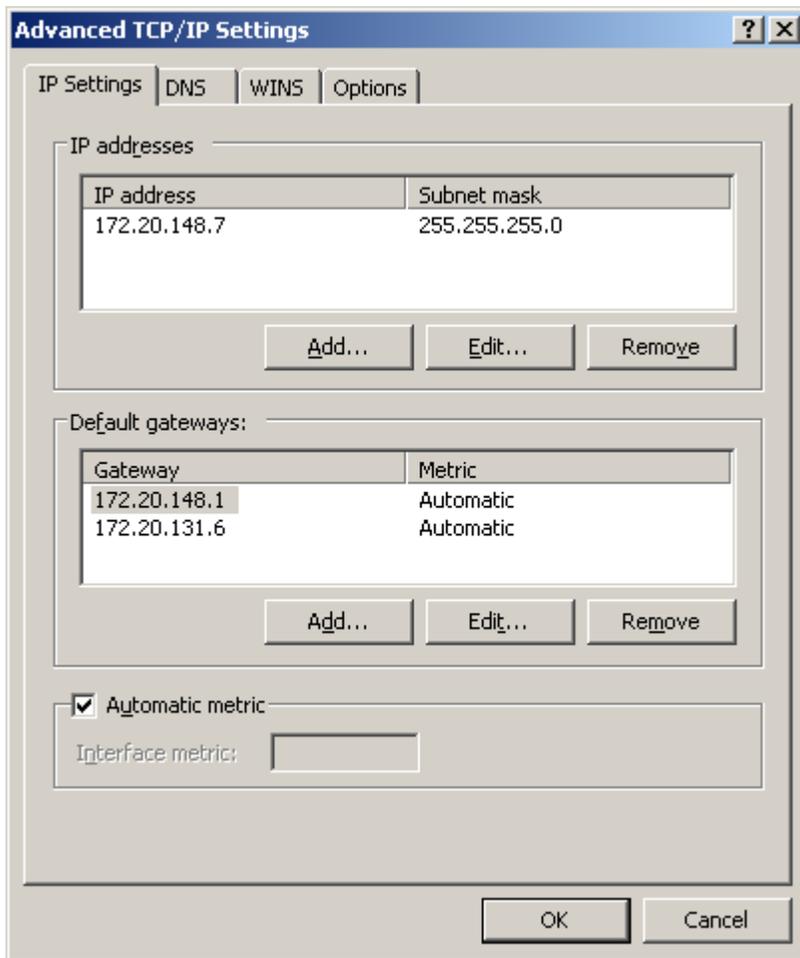


Select **Internet Protocol (TCP/IP)** and click on **Properties**.

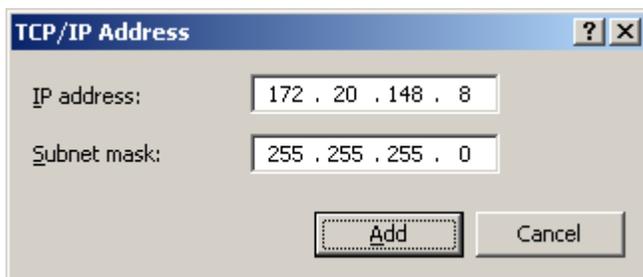
The screenshot shows the 'Internet Protocol (TCP/IP) Properties' dialog box with the 'General' tab selected. The dialog contains the following elements:

- Title Bar:** 'Internet Protocol (TCP/IP) Properties' with help and close buttons.
- General Tab:** A tab labeled 'General'.
- Text:** 'You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.'
- Radio Buttons:**
 - Obtain an IP address automatically
 - Use the following IP address:
- IP Address Fields:**
 - IP address: 172 . 20 . 148 . 7
 - Subnet mask: 255 . 255 . 255 . 0
 - Default gateway: 172 . 20 . 148 . 1
- Radio Buttons (DNS):**
 - Obtain DNS server address automatically
 - Use the following DNS server addresses:
- DNS Server Fields:**
 - Preferred DNS server: 172 . 20 . 148 . 7
 - Alternate DNS server: 172 . 20 . 131 . 5
- Buttons:** 'Advanced...', 'OK', and 'Cancel'.

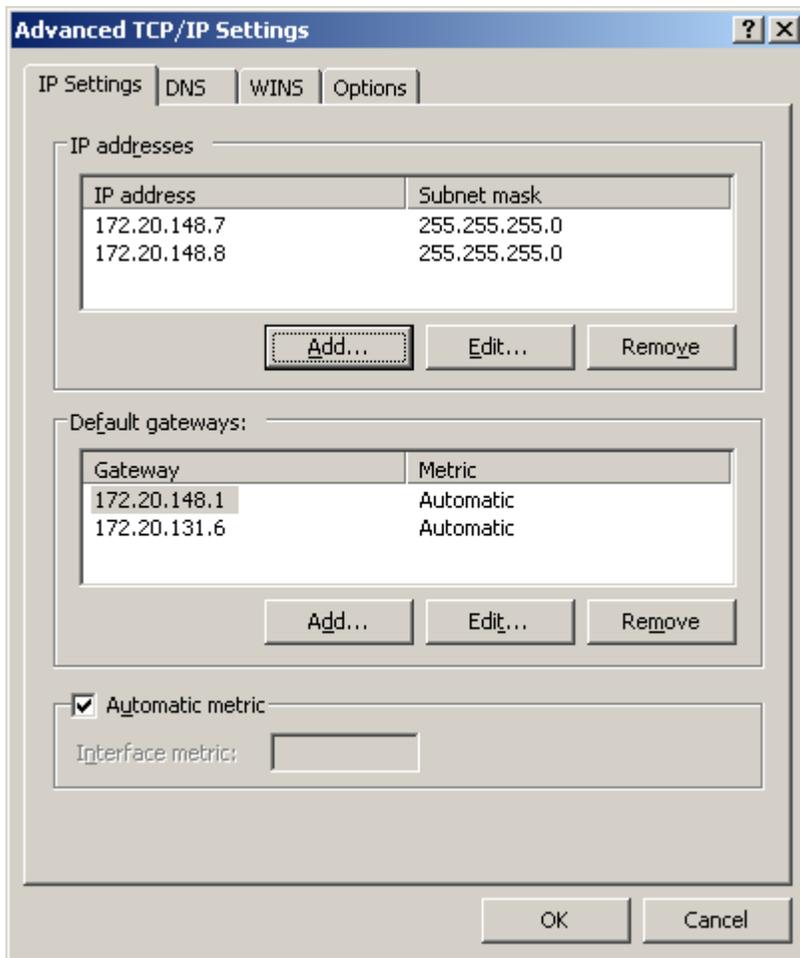
Select **Use the following IP address** to enter the first IP address and subnet mask (if not yet configured). The option **Obtain an IP address automatically** is not supported in this scenario. Click on **Advanced**.



In the **IP addresses** area, click **Add** to configure additional IP addresses.



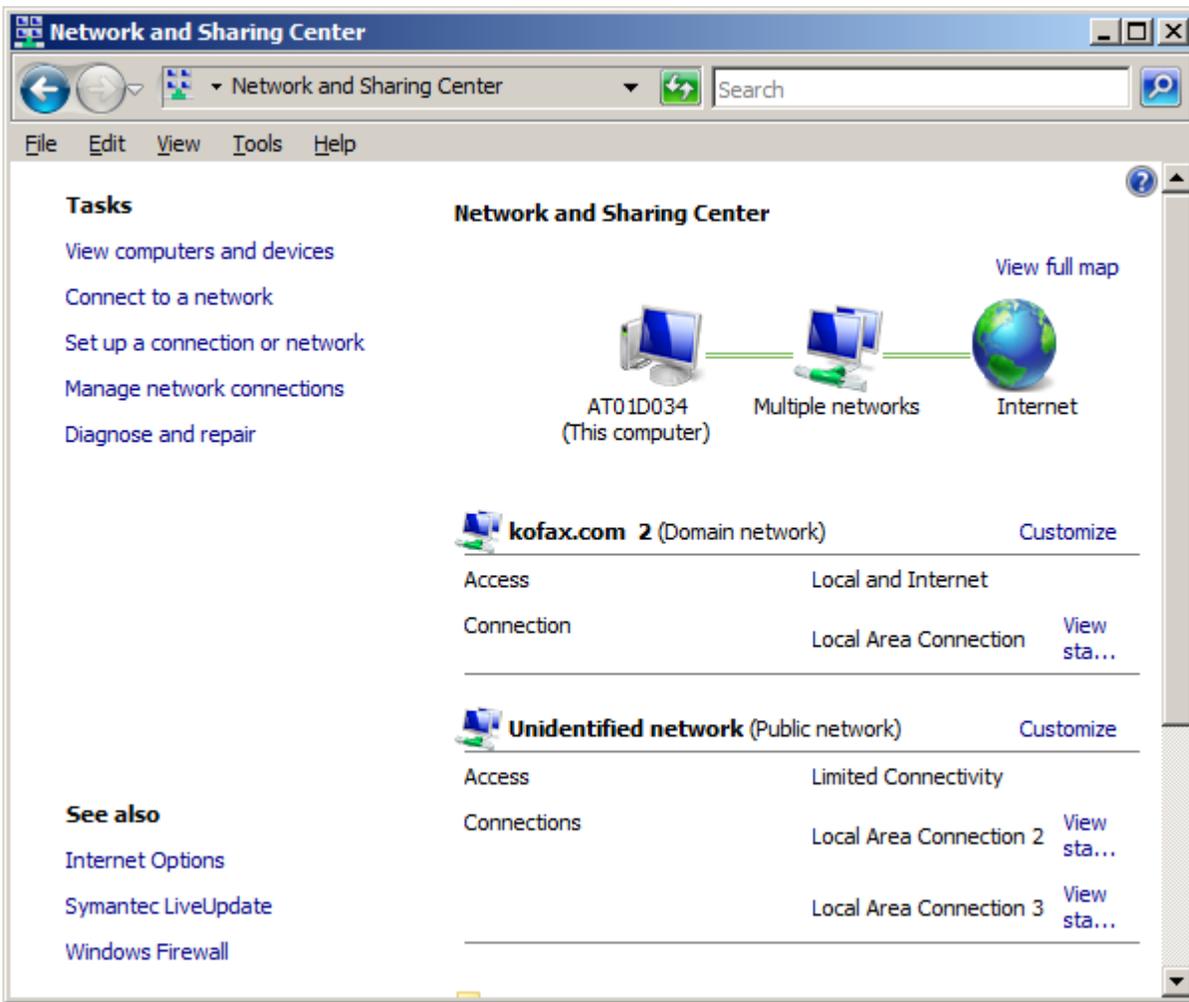
Enter **IP address** and **Subnet mask** and click **Add** to store the new address.



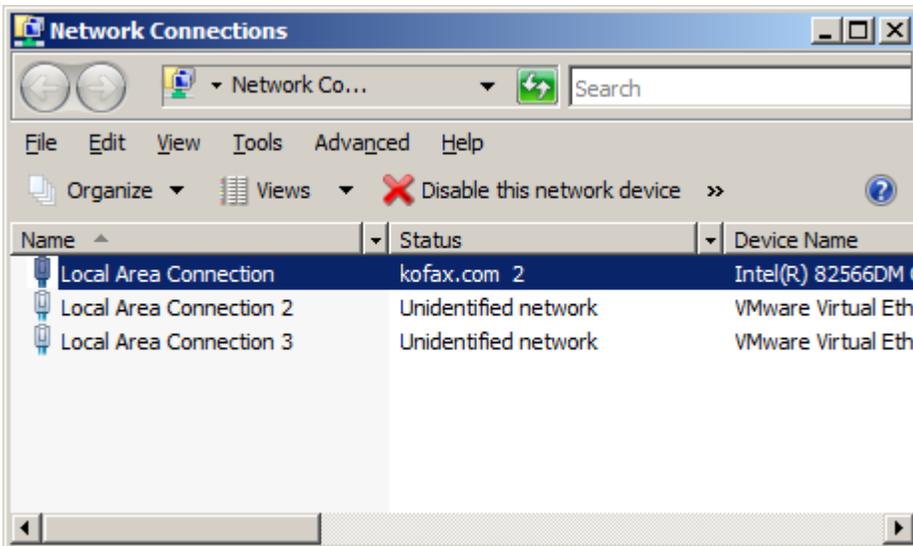
Click **Add** to configure additional IP addresses or **OK** to store the settings. Leave all other dialogs by clicking **OK**.

Configuring multiple IP addresses in Windows 2008:

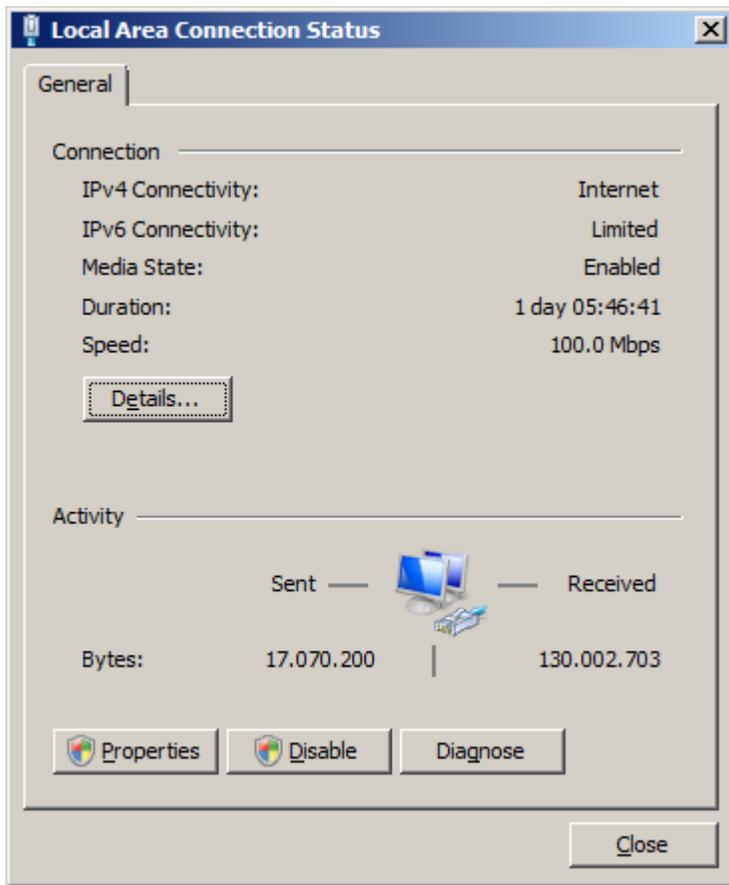
Click the **Start** button on bottom of the screen and select **Control Panel | Network and Sharing Center**.



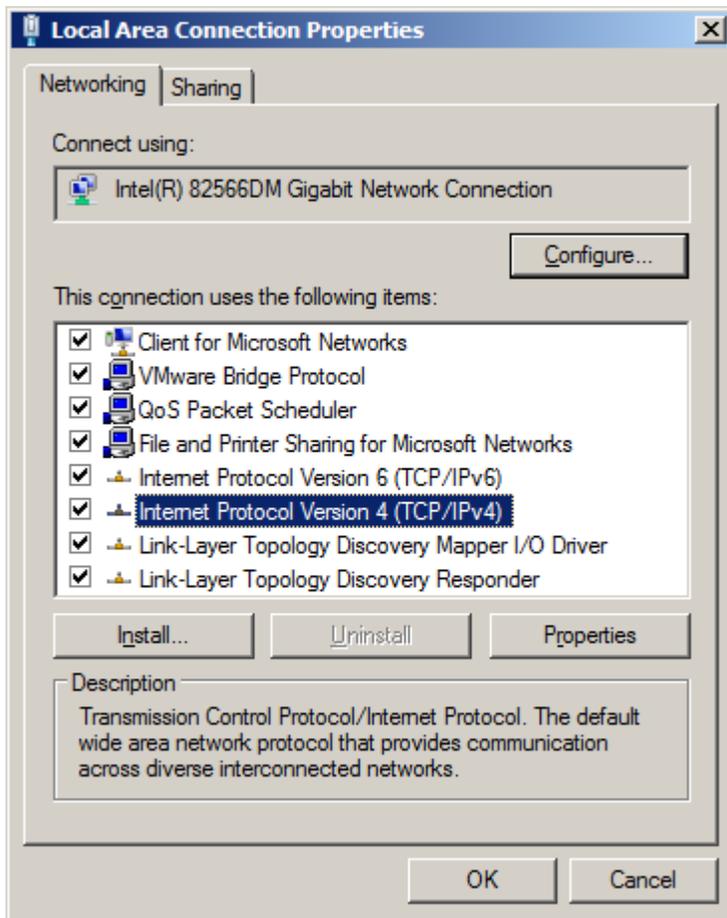
Select the task **Manage network connections**.



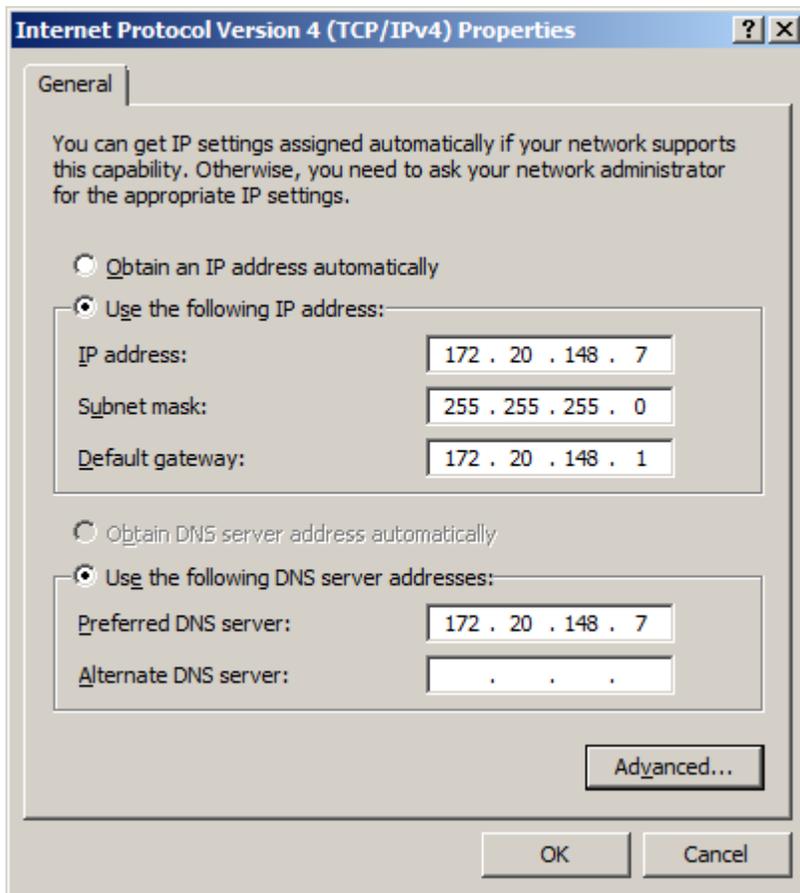
Double-click the connection you want to configure.



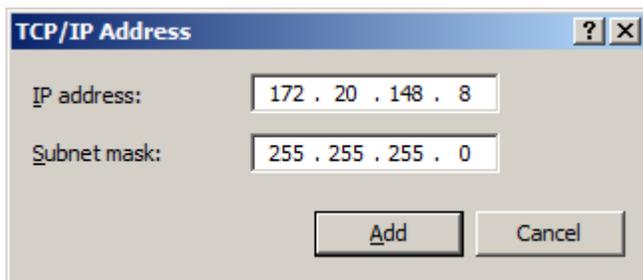
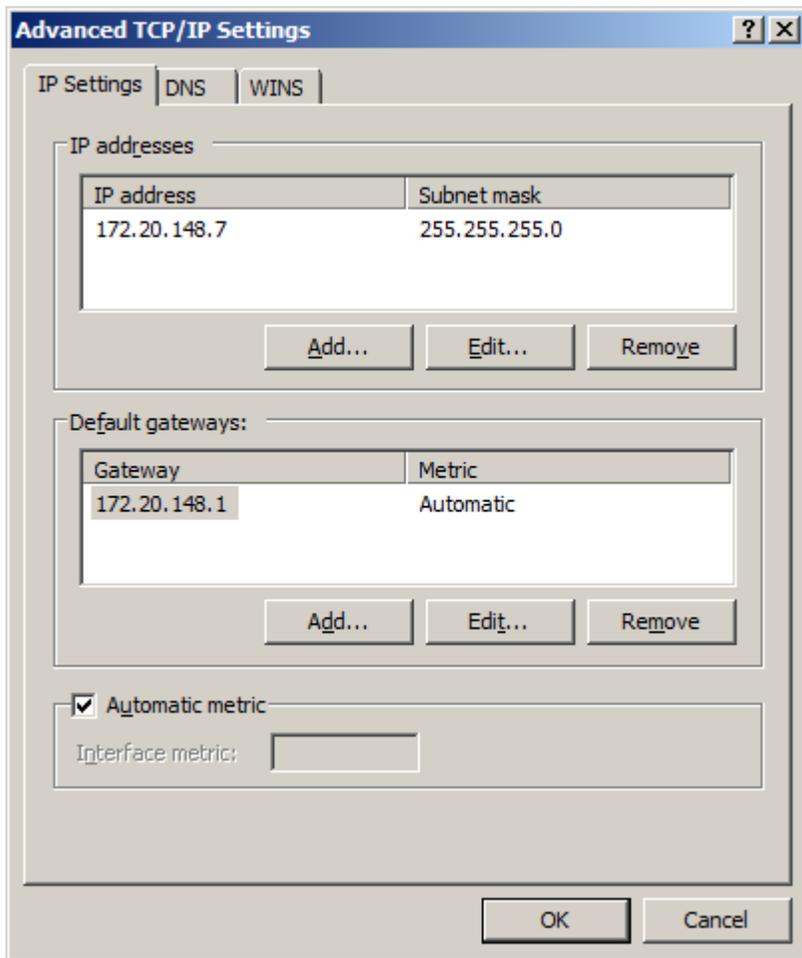
Click on Properties.



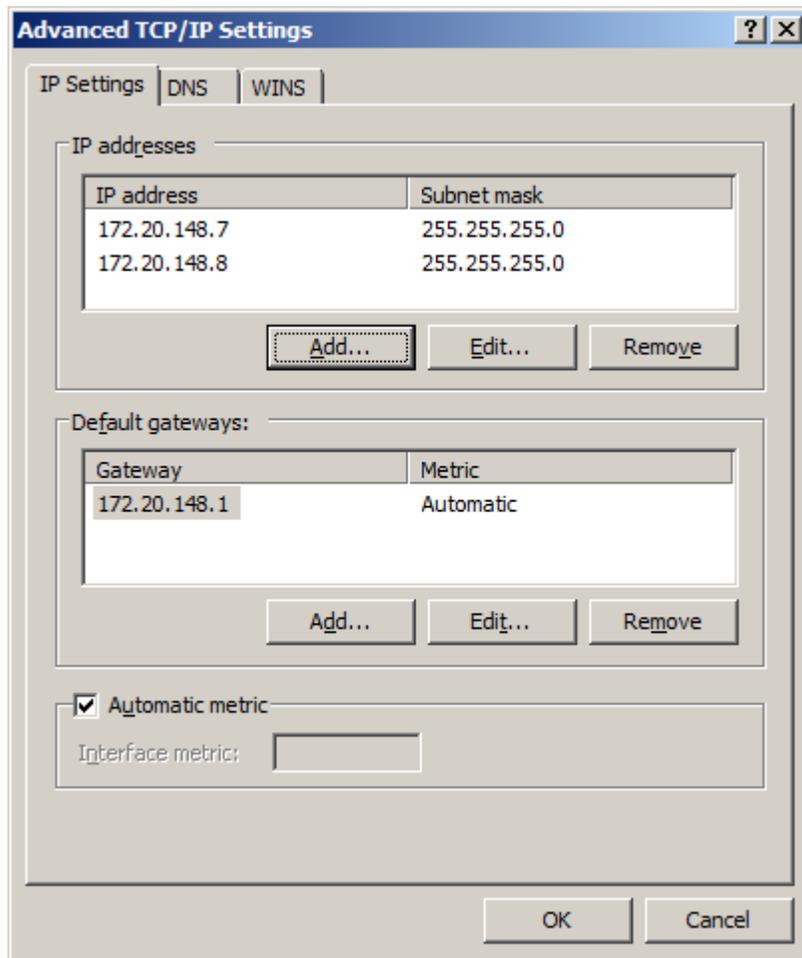
Select **Internet Protocol Version 4 (TCP/IPv4)** and click on **Properties**.



Select **Use the following IP address** to enter the first IP address and subnet mask (if not yet configured). The option **Obtain an IP address automatically** is not supported in this scenario. Click on **Advanced**.



Enter **IP address** and **Subnet mask** and click **Add** to store the new address.



Click **Add** to configure additional IP addresses or **OK** to store the settings. Leave all other dialogs by clicking **OK**.

Example:

- TC/LINK-SM (for connecting KCS to the Internet), and TC/LINK-OC (for connecting from the intranet via TC/WEB) shall be installed on the same machine.
- The IP address “172.20.148.7” shall be used for the Internet mail; therefore, it needs an MX record, and it must be bound to the TC/LINK-SM serving the “public” network.
- The IP address “172.20.148.8” shall be used by TC/WEB. Therefore, it must be bound to the TC/LINK-OC.

Resulting “OwnIPAddress” registry keys:

```
“...\TCLINKSM\TCLSM\OwnIPAddress”= “172.20.148.7”
“...\TCLINKOC\TCLSM\OwnIPAddress”= “172.20.148.8”
```

3.8.4.2 Configuration for Multiple LAN Adapters

In the same control panel screen, you can configure different IP addresses for different network adapters (use the “Adapter” drop-down list).

Configuration for TC/LINK-SM or -OC is quite the same: Simply enter the desired IP address to the registry key “...\TCLSM\OwnIPAddress”.

3.8.4.3 Notes on “Multi-Homed” Operation

- Make sure that the used IP addresses are really available on the connected network! Any IP address conflicts will prevent TC/LINK-SM from proper operation. Any problems will be reported in the Eventlog and the TC/LINK trace file.

- Do not enter leading zeros or blanks for the IP addresses.
- Note that the assigned IP address is used for all mail activity of the corresponding TC/LINK-SM (DNS queries, SMTP traffic, “open line” feature). It does not have any influence on the TCTI connection to the Kofax Communication Server.
- Missing, empty or invalid “OwnIPAddress” entries result in behavior described in 3.8.3 “Multiple TC/LINK-SMs on the Same Workstation – Single IP Address”.

3.8.5 Windows NLB Cluster Installation – with TCSRV NLB Support

Overview:

TC/LINK-SM NLB cluster installation can be used to add scalability, load balancing and fault-tolerance / high availability to the TC/LINK-SM SMTP service (=mail transmission in Mail->KCS direction) in scenarios, where the sender SMTP client, e.g. SAPconnect or certain MFPs, can only be configured to send to a particular SMTP server machine defined by a single IP address. (That is, it does not provide MX record lookup routing or other failover / load-balancing switch mechanism.)

The Windows NLB (=Network Load Balancing) cluster feature is included in the supported Windows Server versions free of charge. However, the Windows NLB alone does not provide complete fault-tolerance because it is not aware of the TC/LINK-SM process health state. To solve this problem, TCSRV was extended with NLB support for TC/LINK-SM and derived links. That is, the TCSRV “NLB port control” feature monitors permanently the health state of the supervised TC/LINK-SM process(es) and directs the incoming traffic only to those NLB nodes where the TC/LINK-SM process is healthy. This makes sure that the unavailability periods are restricted only to the switch-over intervals (in case of failures or planned service stops), in 1 to 10 seconds range.

Configuration:

The NLB cluster can contain 2 to 32 machines (=cluster nodes). Each node is a link server with one or more TC/LINK-SM instances. In any case, all NLB cluster nodes must have exactly the same TC/LINK-SM configuration; each node is a mirror of any other node. When more than one TC/LINK-SM instances are running on the cluster nodes, then every TC/LINK-SM instance on the node must have an individual unique SMTP listener port number (configured in <link>/TCLSM/Port2TC).

The TCSRV NLB port control feature has to be activated for all TC/LINK-SM instances with the registry setting <link>/TCLSM/NLBPortControl=1. (This setting takes effect only after TCSRV restart.) To get more details on the TCSRV NLB port control feature, please refer to the TCSRV manual / chapter “Windows NLB Port Control for TC/LINK-SM”.

The sender SMTP client(s), e.g. SAPconnect SMTP node or MFPs, must be configured to send to the common NLB IP address.

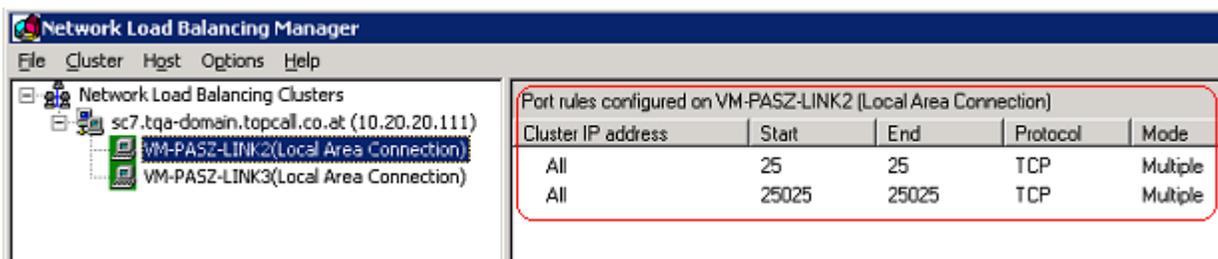
NLB configuration parameters:

Cluster operation mode: Multicast

Port rules:

- Port range from = Port range to = value of <link>/TCLSM/Port2TC (or 25 if Port2TC is 0)
- Protocols: TCP
- Filtering mode: Multiple host
- Affinity: none
- Load weight: equal

If multiple TC/LINK-SM instances are running on each cluster node, then every different SMTP listener port number must have its own individual NLB port rule. Reason: The TCSRV NLB port control manipulates the ports through the port rules. So, to enable individual port-control for each listener port, each listener port must map to an individual port rule.



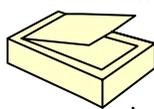
TC/LINK-SM NLB cluster installation plan:

All SMTP clients are configured to send to the common NLB IP address

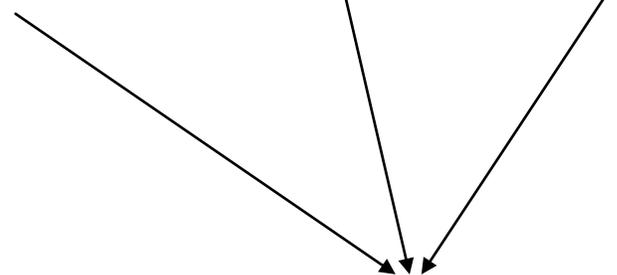
Sender SMTP client (e.g. MFP)

SMTP client

SMTP client

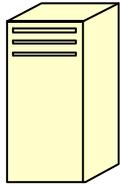
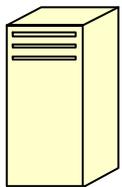


.....

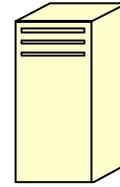


NLB configuration:
 Multicast mode,
 Port range-from: TCLSM/Port2TC
 Port range-to: TCLSM/Port2TC
 Protocol: TCP
 Filtering mode: Multiple host
 Affinity: none
 Load weight: equal →
NLB distributes the message traffic on all link servers approximately equally. (=Load balancing)

Windows Network Load Balancing (NLB) cluster (common IP address)



.....



Link server 1

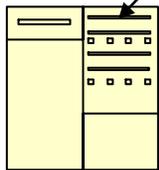
Link server 2

Link server n

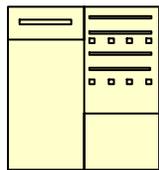
- TCSR process with "NLB port control" functionality
- TC/LINK-SM (=SMTP server, its listener port is supervised by the TCSR NLB port control)

- TCSR process with "NLB port control" functionality
- TC/LINK-SM (=SMTP server, its listener port is supervised by the TCSR NLB port control)

- TCSR process with "NLB port control" functionality
- TC/LINK-SM (=SMTP server, its listener port is supervised by the TCSR NLB port control)

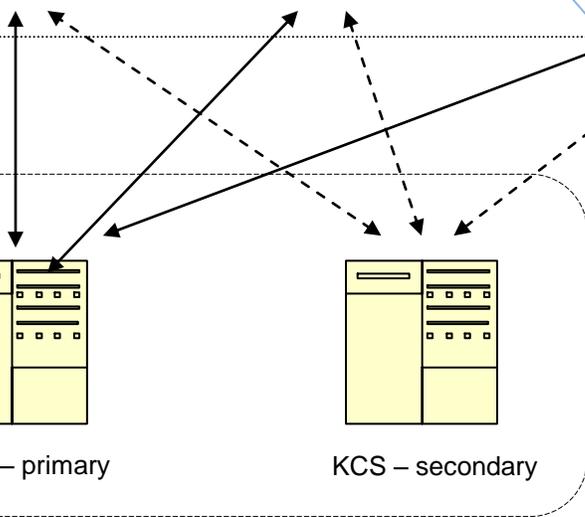


KCS – primary



KCS – secondary

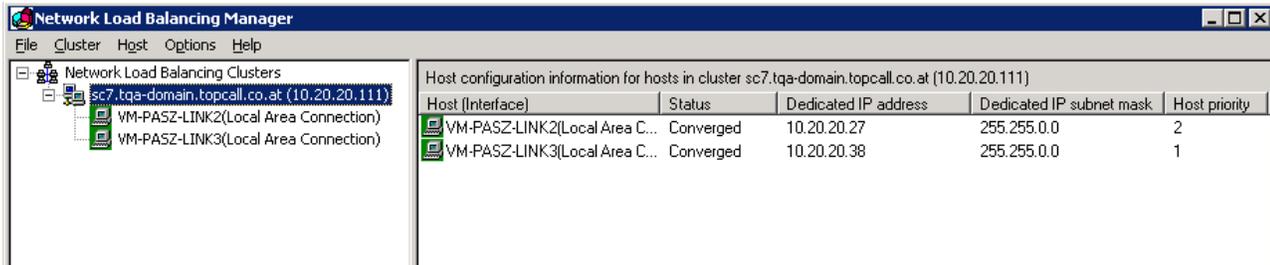
Kofax Communication Server (=TCOSS) – tandem



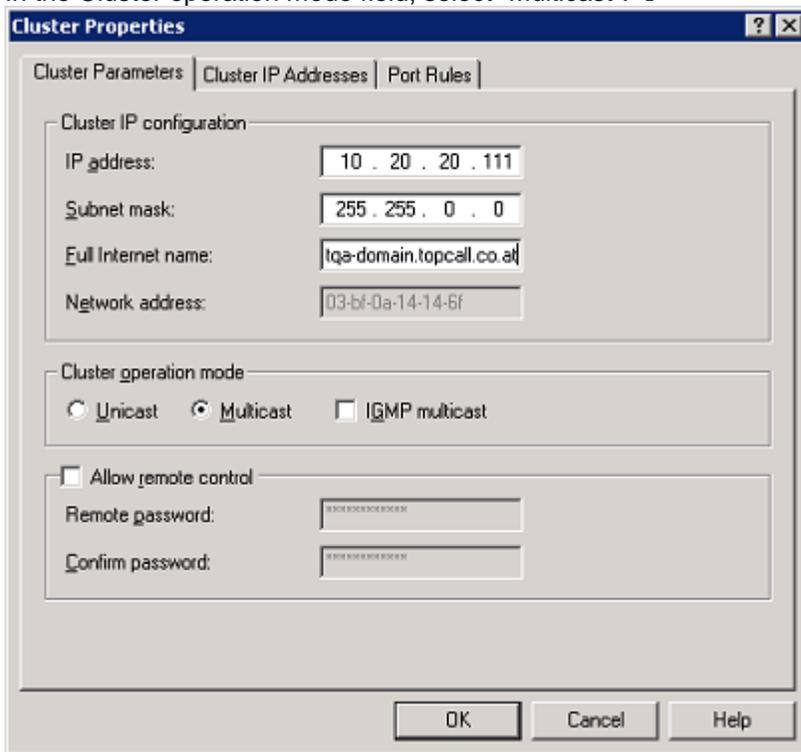
On each link server run TC/LINK-SM process(es) and the TCSR process. TCSR supervises the TC/LINK-SM process(es) on each machine. TCSR provides NLB support ("NLB port control" feature): It NLB enables / disables the listener port according to the health state of the TC/LINK-SM process. Effect: When some TC/LINK-SM link process is not ready or some link machine is down, then the NLB routes the SMTP message to some other NLB member link server. (=Failover)

Creating a Windows NLB cluster:

The Windows NLB Manager tool (start: %SystemRoot%\system32\nlbmgr.exe or Start/Programs/Administrative Tools/Network Load Balancing Manager) since Windows Server 2003 SP2 provides an easy way to setup NLB in the local network. It is recommended to run this tool on a machine which is not a part of the NLB. It is also recommended to define a higher cluster IP address number than either of the local IP addresses.

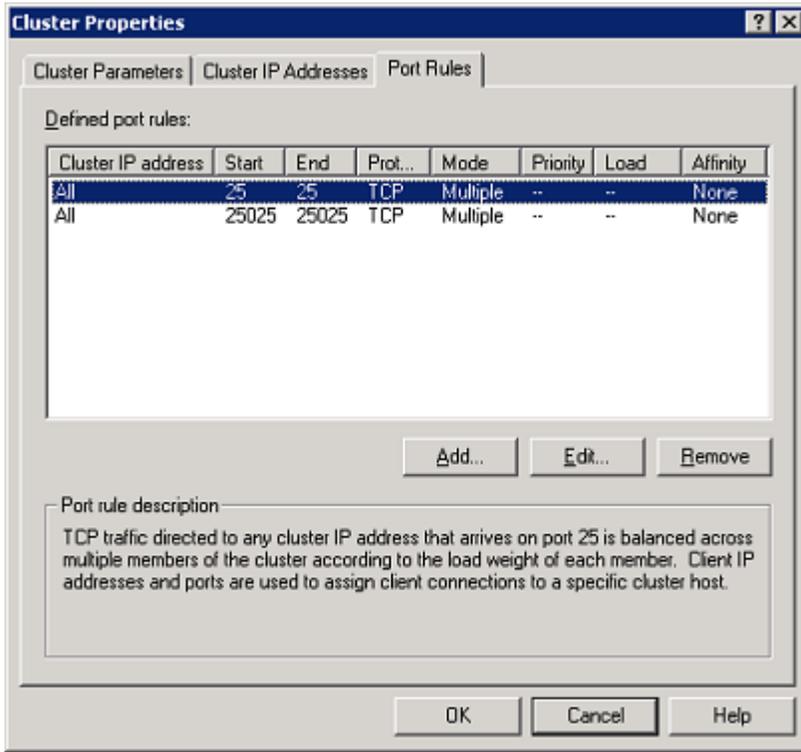


The common cluster IP address is set in the Cluster IP configuration | IP address field. In the Cluster operation mode field, select "Multicast". ➔



When multiple parallel TC/LINK-SM instances are running on each NLB node, then an individual port rule has to be defined for each such TC/LINK-SM instance(-group).

("group": consists of TC/LINK-SM instances running on different NLB nodes but with the same configuration.)



Port rule configuration. Port number 25 below is only an example. Start Port = End Port = as defined at the according link instance(-group) in the registry setting <link>/TCLSM/Port2TC. Otherwise, the settings shown on the picture below have to be used. ➔

Add/Edit Port Rule ? X

Cluster IP address
[] or All

Port range
From: 25 To: 25

Protocols
 ICP UDP Both

Filtering mode
 Multiple host Affinity: None Single Class C
 Single host
 Disable this port range

OK Cancel

3.9 Special Features

There are some special installation features that can be applied to almost every scenario described above.

3.9.1 User Profiles Setup for SMTP Aliases

If you want your users to have more than a single SMTP address in the default format <UserId@mail-domain>, you can edit their user profiles as follows:

- To give a user alias addresses on the local mail-domain, you can enter inactive SMTPIN addresses ('localpart' only! Entering SMTPIN addresses with domain will NOT work.)
- To give a user aliases with a different domain, enter the complete address ('localpart' AND 'mail_domain!') as an inactive SMTP address.
- Note that the first SMTP address in a user profile will be used as the originator address when this user sends mail to SMTP.

Example user setup:

User Profile - LL

Queue Length/Age/Pages alerting | Queue Length/Age/Pages logging | TC/WEB | TC/WEB Identity Rights

General | Address | Event | Rights | Manual Fax | Distributor | Authorize/Sign

Service: **SMTP** | Addr. no.: **6** | Active

Free address: | |

Active	No	Service	Number:
X	1	TOPCALL	LL,
	2	FXI	848,
	3	SMTP	Lisa.Lustig@comany.com,
	4	SMTPIN	Lisa Lustig,
	5	SMTPIN	LLustig,
	6	SMTP	lustig@gmx.com,

| |

This gives the following aliases:

- <LL@company.com> (the default UserId@domain)
- <Lisa.Lustig@company.com>
- <LLustig@company.com>
- <lustig@gmx.com>

Note:

- To enable aliases with different mail-domains, TC/LINK-SM must be configured to allow routing (Registry "...TCLINKSM/TCLSM/SMRouteEnable" = 1)!

3.9.2 User Profiles Setup for Special Originator Address

As already mentioned above, the first SMTP address will be taken as originator for all mail sent from this user to SMTP. In the example above, <Lisa.Lustig@company.com> will be the originator address (instead of the default <UserId@mail_domain> that would have been <LL@company.com>).

3.9.3 Enhanced Originator Mapping

With TC/LINK-SM/OC 1.09 or higher, and TCOSS 7.23 or higher, the KCS user profile aliases are checked to find a matching originator user profile ("shadowuser").

Example (using the configuration example from 3.9.1):

- With TC/LP prior to 1.09, the SMTP originator address must have been "LL@company.com" (UserId@domain) for getting the full shadow user functionality (message visible in users outbox, user template applied, passing of the "disable sending for mail users" check, etc.).
- Now, also the originator addresses "Lisa.Lustig@company.com" and "lustig@gmx.com" (in fact, all inactive SMTP aliases; the SMTPIN aliases do NOT.) will give full shadow user functionality!

See the TCLINK Manual for a detailed description of this feature.

3.9.4 "Direct Delivery" Feature

This feature is required for the scenario described in 3.7 (“TC/LINK-SM for Use as an Intranet SMTP Backbone”); but it may also be useful for other scenarios.

Direct mail delivery (according to RFC974, RFC1034 and RFC1035) is supported by TC/LINK-SM. In short, the following happens when mail is sent to SMTP:

- TC/LINK-SM takes the destination domain from the recipient address
- It starts a DNS query to find out the responsible mail server (“MX” record) for that domain
- Another query is done to find out the IP address (“A” record) of the responsible mail server
- TC/LINK-SM directly contacts that server and delivers the message
- As a fallback for any direct delivery failure, TC/LINK-SM attempts sending the message to the configured smart host (if available)
- To keep the query overhead low for often used domains, a cache is maintained locally in the TC/LINK-SM temporary directory.

There are three levels of delivery (configured during “Advanced Installation”):

- Smarthost delivery: All mail sent to the configured smart host
- “HOSTS lookup”: Direct delivery using “A” record lookup. Very useful in Intranets with all other mail servers entered to the local “HOSTS” file
- “MX lookup”: this is more effort, therefore slower but works for the whole Internet (no need to enter mail servers to the local “HOSTS” file)

Fallback:

- If “MX” lookup (UseDNS = 2) is configured, and “MX” resolution fails, then “A” record resolution is tried. If this also fails, then the message is sent to the smart host (if configured).
- If “A” lookup (UseDNS = 1) is configured, and “A” resolution fails, then the message is sent to the smart host (if configured).

Note:

- Due to the lookup overhead, the TC/LINK-SM throughput is decreased for DNS delivery. If you have problems with throughput, the “smarthost” delivery is the preferred choice.
- Like in all prior releases, a message is sent for every single active recipient. This applies to all delivery modes.

3.9.5 Operation over a One-Way Dialup Line

If you connect to the Internet over a one-way dialup line, you are not always reachable from the Internet. Only if you are online, mail can be delivered directly to TC/LINK-SM.

To avoid message loss in this situation, you need an external mail queue assigned, with an MX record preference higher than the one of TC/LINK-SM. Most ISP offer this service of mail buffering.

Example:

company.com	MX	link1.company.com	10
company.com	MX	queue1.isp.net	100
link1.company.com	A	193.81.166.101	
queue1.isp.net	A	192.88.117.5	

What happens if mail shall be delivered to <company.com>?

- First of all, the sending host looks up the MX records and tries to contact the server with the lowest preference (<link1.company.com>).
- Because this one has a one-way dialup line and is currently offline, connection will fail.
- As a fallback, the sending host tries to connect to the alternative server (... the one with the higher preference <queue1.isp.net>). As this server is located at the ISP and is always online, message delivery will succeed.
- Next time <link1.company.com> goes online; this must be detected by <queue1.isp.net>. Then, all mail currently in the queue will be forwarded to <link1.company.com> ... the final destination host.

To allow operation over a one-way dial up line, a poll cycle may be configured on TC/LINK-SM so that the line is periodically opened for incoming mail. (Configuring a poll cycle of e.g. 3600 means that TC/LINK-SM will check for new messages every hour).

Note:

- Basic polling simply opens the line to the other SMTP mail server (similar to e.g. ping). The alternative mail server (mail queue) at the ISP must recognize the opened line and forward its mail to TC/LINK-SM.
- See 3.9.12 “Active Polling of Remote Mail Queues (ETRN Feature)” on an advanced polling possibility.

3.9.6 “Single Text Block” Operation

When you send a message containing multiple text blocks via SMTP to e.g. MS Exchange, only the first text block is displayed as plain text. All other will show up as text attachments.

This is a bad behavior of MS Exchange (not sticking to RFC1806). However, as the same problem also appears with some clients fetching mail via TC/POP3, the TC/LINK-SM can be configured (“Advanced Installation”) to put all text blocks together in a single text block at the first position in the message.

Note:

- This applies only for messages from Kofax Communication Server to SMTP.
- The position of attachments is lost if this switch is enabled. All attachments appear at the end of the text lines.
- Due to additional conversion overhead, performance is reduced if this switch is enabled.

3.9.7 Large Message Size Operation

As the Internet is generally not very stable for transmission of very large files (several Megabytes), the same thing applies to large mail messages. There are no fixed limits, but generally: The larger the message, the higher the risk of rejection.

3.9.7.1 Connection Timeouts

TC/LINK-SM can be configured for several timeouts, message size limits, and also a watchdog feature. See 7.1 “Registry Keys Used by TC/LINK-SM” for a description of involved registry values!

3.9.7.2 SMTP Protocol Extension for Maximum Message Size

Older versions of TC/LINK-SM did not check the message size before sending a message. Therefore, it could happen that somebody sends a very large message; connection broke or timed out during transmission; and the following retries blocked TC/LINK-SM for quite a long time.

Since 1.09, TC/LINK-SM supports the ESMTP feature “SIZE” (defined in RFC1870).

- Together with the direct delivery feature, this gives the opportunity to check the maximum size capability of the destination mail server, therefore avoiding send attempts on messages that are too large to be transmitted.
- The own message size capabilities can be defined during “Advanced Installation”
- Incoming messages larger than the configured inbound limit will not be accepted (the sender gets a “552 message size exceeds fixed maximum message size” response).
- outgoing messages which exceed the outbound size or which are larger than the destination server’s capabilities, are not transmitted at all. They are negatively terminated, with a response message like “message too large” or similar.

Note:

- This feature must be supported by the connected client/host. It will e.g. not work for some older Internet mail clients (check the TCP trace for the “SIZE” keyword to find out about your client).
- The MIME message size (not the TCOSS message size) is used for this “SIZE” handshake. If you send a 1MByte attachment, this will result in about 1.4 MByte MIME message size due the encoding overhead.
- Size determination is optimized to be fast; therefore, accuracy is only around +/- 1kByte.

3.9.7.3 TC/LINK Watchdog

TCLSM.DLL resets the TCLINK watchdog timer as long as sending is in progress successfully. If there is any TCP/IP problem during transmission (like "connection lost"), this will be reported to KCS, initiating retries according to the failure condition.

3.9.8 Implementing Different Recipient Addressing Syntax

If the customer does not like the default addressing described in 2.1 "Addressing", you can configure different types of address syntax. Note that this is a very advanced setup; it should be used only if absolutely necessary.

Scenario:

The service information is to be embedded into the "mail-domain" part of the SMTP address:

<number@service.domain> - e.g. <66133899@fax.company.com>

Solution:

- Enable the routing feature for TC/LINK-SM
- Edit the rr99 on KCS, add a line in the **ROUTE section for every service needed (reroute the message to the service-specific channel or queue):

```
**ROUTE
TCLSMQI:~@fax.company.com,05:~,SMTP to FAX
TCLSMQI:~@telex.company.com,01:~,SMTP to Telex
TCLSMQI:~@exchange.company.com,TCLMXQI:~,SMTP to Exchange
```

Remarks: "05:" is the fax channel, "01:" is the telex channel, and "TCLMXQI" is the queue polled by TC/LINK-MX!

If you want to use this addressing style in DNS-based scenarios (like 3.3 "TC/LINK-SM for Connecting an Existing KCS System to the Internet"), you need MX records pointing to TC/LINK-SM for all used services!

Example:

fax.company.com	MX	link1.company.com	10
telex.company.com	MX	link1.company.com	10
exchange.company.com	MX	link1.company.com	10
link1.company.com	A	193.81.166.101	

Note:

All messages to these "service-domains" are posted to KCS as SMTP addresses; this means that the document converter will not be activated with the default SMTP service definition. If you need a document conversion, you may either remove the "binary" capability of the SMTP service, or request a customized MAP file from Kofax.

3.9.9 Configuring MIME Types for Attachments

3.9.9.1 Sending Binary Attachments to SMTP

Several clients do resolve the attachment type not by filename extension (... as most of the clients do), but by the MIME type/subtype header information. As this is "application/octet-stream" in the default TC/LINK-SM configuration for all binary attachments in messages to SMTP, these clients did not correctly display attachments.

Therefore, you can configure by a registry Multi-string which MIME type/subtype field should be used according to the filename extension. The syntax for every entry is:

```
<Filename extension>,<MIME Type/Subtype>
```

Example:

```
"HKEY_LOCAL_MACHINE\SOFTWARE\TOPCALL\TCLINKSM\TCLSM\MIMETypes"
```

Data:	GIF, Image/gif TIF, Image/tiff DOC, Application/msword TCI, image/x-tci
-------	--

If you send a message from TCfW to SMTP with an attached Word document "test.doc", this leads to a default MIME sub header

```
Content-Type: Application/octet-stream; name=test.doc
```

With the list configured above, TC/LINK-SM takes the filename extension ("doc"), scans the list, and finds a matching entry. Therefore, the sub header will be

```
Content-Type: Application/msword; name=test.doc
```

Note:

- The extensions are not case-sensitive, i.e. "DOC" matches "Doc", "doc" or even "DoC".
- If no match is found, the default "application/octet-stream" is inserted (as with all older releases).

3.9.9.2 Receiving Binary Attachments from SMTP

In order to select the right application for the KCS document converter, it is important that all binaries received from the Internet have a valid filename extension assigned.

If messages from SMTP have binary attachments with valid type/subtype information, but without a valid filename, the MIMETypes registry list is used to build a file name.

Example (using the MIMETypes configuration from above):

If the incoming attachment subheader is

```
Content-Type: Image/tiff
```

, (not holding a filename!), then TC/LINK-SM will look up the MIMETypes list for "Image/tiff", and finds the extension "TIF" to be used. It will build a filename using that information; equivalent MIME sub header line would be

```
Content-Type: Image/tiff; name="unknown.TIF"
```

This will make the document conversion work (if required).

Note:

- The mime-types are not case-sensitive! So, "Image/Tiff" matches also "iMaGe/tifF".
- If no match is found in the registry list, the filename is built in the syntax "<Type>.<Subtype>" (e.g. "Content-Type: text/html" will result in a filename "text.html")

3.9.10 Configuring Display Mode for Special Attachments

By default, TC/LINK-SM converts all documents that are not "text/plain" as MIME attachments (This is done with the "Content-Disposition:" header parameter, described in RFC1806).

If TCLINK-SM receives a HTML text document and forwards this document to another SMTP mail server, this document is sent as an attachment. The user that finally receives the message needs to double-click this document to view the message.

To work around that unwanted effect, you can configure a list of content types that shall be displayed inline. This is done by filling the registry list "HKLM\Software\Topcall\TCLINKSM\TCMIME\InlineContentTypes" with all content types that shall be displayed inline.

Example:

```
InlineContentTypes:  
  Text/plain  
  Text/enriched
```

Text/html

Note:

- The registry key is created, and filled with the default values automatically when this version of TC/LINK is started the first time.
- Entries are not case-sensitive.
- The registry list is restricted to a total length of 5000 characters.
- When you are using the TC/POP3 or TC/IMAP server on the same machine, you must upgrade them to release 7.23.02 or higher. Reason is the TCMIME.DLL that is shared by multiple applications.
- Even when setting a content type to be displayed inline, it is still depending on the client capabilities whether this part of a message will really be displayed inline.

3.9.11 Changing the Address Separator Character

The TC/LINK-SM allows to be operated as a switch between SMTP and all other KCS services by using the following syntax in the email address:

```
<fullname#service#number#answerback@mail_domain>
```

If the “#” is not appropriate for any reason and another character (which must be allowed in email addresses, see 2.1 “Addressing”!) shall be used, the SMTP.MAP file must be edited: replace any occurrence of “#” against the new separator character, and restart TC/LINK-SM.

3.9.12 Active Polling of Remote Mail Queues (ETRN Feature)

In earlier releases of TC/LINK-SM, the polling feature was limited to simple “open line” functionality. The distant SMTP mail queue must detect the open line, and start sending the queue by itself. RFC 1985 describes a standardized possibility to actively start sending of an external mail queue. This feature is widely supported in the UNIX world (sendmail 8.x standard feature), and also by Microsoft Exchange (5.0 or higher).

TC/LINK-SM issues the “ETRN” command when polling the distant mail queue (after checking if the command is supported). This will result in

- Better interoperability with any kind of mail server (as now a standardized way of polling is used)
- Faster delivery to the end user (active request via ETRN is usually faster than the polling for “open line”).
- Better detection of errors on the distant mail server: The distant mail server will respond with either an “OK”, or an error indication (e.g. “459 Mailqueue currently unavailable”). Error conditions are reported to the TC/LINK-SM trace file and Windows event log.

Note:

- This feature is only activated if you use the “open line” feature (if you configure a poll cycle).
- Only error responses are written to the Windows event log. Successful polling is not reported.

3.9.13 Separate TCP Ports for Send and Receive

When using a firewall with ports translation, it is sometimes desired to use separate ports for sending and receiving from / to the Internet.

The desired ports for sending and reception can be put to two registry values:

```
“...\TCLSMTPort2SMTP” ... gives the port number used for sending and polling  
“...\TCLSMTPort2TC” ... gives the port number for reception (listener)
```

You may change these port numbers via registry editor.

Note:

- TC/LINK-SM must be restarted to make changes effective.

- Make sure to use the port numbers fitting your environment; otherwise, sending or reception via TC/LINK-SM may be impossible.

3.9.14 Originator Alias Configuration

By default, KCS users sending to SMTP get the following originator address:

```
From: "Fullname" (Freetext) <UserId@Linkdomain>
```

Three parameters (Fullname, Freetext and UserId) are taken from the KCS user profile.

However, some Internet mail clients only display the part in the brackets (the 'Freetext' in the default MAP file) as the originator. In this case, it may be desirable to put a different string to this position. This can be done by simply un-commenting some lines in the SMTP.MAP file:

Standard SMTP.MAP:

```
ENTRY ----- (KCS address: UserID@domain without blanks)
*
SET_TC_ADDRESS
*
SET_FREE_ADDRESS

COPYAPPEND
DST.TS_FREE_ADDR
SRC.TS_TC_USERID
"@ "
REG.TCLSM\SMLinkDomain

REM Optionally, write special alias string:
REM To get alias same as eMail address, uncomment the following 3 lines
REM COPYAPPEND
REM DST.TS_FREETEXT
REM DST.TS_FREE_ADDR

REM to get alias same as fullname, uncomment the following 3 lines
REM COPYAPPEND
REM DST.TS_FREETEXT
REM SRC.TS_FULLNAME
```

Adapted to put the Fullname to the Alias:

```
ENTRY ----- (KCS address: UserID@domain without blanks)
*
SET_TC_ADDRESS
*
SET_FREE_ADDRESS

COPYAPPEND
DST.TS_FREE_ADDR
SRC.TS_TC_USERID
"@ "
REG.TCLSM\SMLinkDomain

REM Optionally, write special alias string:
REM To get alias same as eMail address, uncomment the following 3 lines
REM COPYAPPEND
REM DST.TS_FREETEXT
REM DST.TS_FREE_ADDR

REM to get alias same as fullname, uncomment the following 3 lines
COPYAPPEND
DST.TS_FREETEXT
SRC.TS_FULLNAME
```

Note:

- These lines occur twice in the TO_MAIL_ORIG section; make sure to change both occurrences.

- TC/LINK-SM must be restarted to make changes effective.
- As the alias field usage is not standardized, you may get different originator address display on different clients. So, in general, it is a trial-and-error approach to find the best solution in your special environment.

3.9.15 Reject Invalid Recipient Addresses

In the TC/LINK-SM standard configuration, all incoming mail will be accepted. If there is an invalid local part (not matching any KCS User Id or SMTPIN alias), the message is rerouted to the postmaster. If requested, a delivery notification will be sent.

This behavior can easily be changed to reject such messages (send a non-delivery notification) by changing the rr99 entry for the SMTPIN alias lookup. The default ****INBOUND** section looks like this:

```
postmaster:~, ,search for SMTPIN aliases; non-matching to postmaster!
,, no default required because prefix already is existing user
```

If you change that to

```
postmaster:~, ,search for SMTPIN aliases
postmaster:~, invalid, Disable reroute! Send non-delivery instead ...
```

... all incoming mail with an invalid address will be rejected.

Note:

- All rejected messages will get a "TCLINK cannot post" notification. There is currently no detailed indication what went wrong.
- The use of the ****INBOUND** section requires TCOSS 7.08.xx or higher.

3.9.16 Customizable Codepage Conversion

In some environments, 8-bit messages are sent containing characters that are not matched by any TCOSS character. Therefore, it is sometimes required to add custom code conversion rules.

TCMIME 1.14.00 or higher makes use of the character set conversion routine included in TCSI32.DLL 2.19.00 or higher. New code conversions may be added or existing conversions modified by providing the conversion table as ASCII file in the Shared directory ("C:\TOPCALL\SHARED").

Conversion Table File Name:

For the conversion from code page A to code page B the conversion table's file name is "AtoB.cnv",

A and B can be the following numbers:

```
0 ... TCOSS codepage 0
1 ... TCOSS codepage 1
100 ... MIME charset=USASCII (or no char set specified)
101 ... MIME charset=ISO-8859-1
102 ... MIME charset=ISO-8859-2
...
110 ... MIME charset=ISO-8859-10
115 ... MIME charset=ISO-8859-15
```

Filename examples:

"100to0.cnv" replaces the built-in USASCII-to-TCOSS 0 conversion

"0to101.cnv" replaces the built-in TCOSS 0-to-ISO-8859-1 conversion

Conversion Table Format:

A conversion table contains 256 hexadecimal values in 2-Byte ASCII notation, letters 'A' .. 'F' may be in upper or lower case. Comments may be added after the conversion values.

Example (“100to0.cnv”)

```

00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f
20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f
30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d 3e 3f
40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f
50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d 5e 5f
60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f
70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e d7
b1 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f
90 91 92 93 94 95 96 97 98 99 9a 9b 9c 9d 9e 9f
20 ad 9b 9c d1 9d 7c c1 bd 43 a6 ae aa 2d 52 b5
ba f1 fd c9 b2 e6 f3 bc be 31 a7 af ac ab db a8
41 41 41 41 8e 8f 92 80 45 90 45 45 49 49 49 49
c2 a5 4f 4f 4f 4f 99 c5 ed 55 55 55 9a 59 cc e1
85 a0 83 61 84 86 91 87 8a 82 88 89 8d a1 8c 8b
d2 a4 95 a2 93 6f 94 f6 d9 97 a3 96 81 79 dc 98
(Comment: This is the USASCII-to-TCOSS 0 conversion table)

```

The character value in the source code page is used as an index into the conversion table to retrieve the code point in the destination code page.

Conversion Table Trace:

The loading of custom defined or built-in code tables may be traced by setting a new switch in “... \TCS\DebugLevel”: 0x8000 ... conversion table trace

Note:

- As the 7-bit character range (0x00 ... 0x7f; the first 8 line in the .cnv files) is used by the SMTP/MIME encoding, you must never change this. Only the upper half of the tables can be customized.
- Remember that Internet addresses (the From: and the To: parameters) must always consist entirely of 7-bit characters. Otherwise, delivery may fail.
- As TCMIME is a shared module, customized conversion tables affect all applications using TCMIME on the same PC (e.g. TC/POP3 and TC/LINK-SM).
- In the direction KCS to SMTP, only USASCII, ISO-8859-1/2/7 and utf-8 are used. TC/LINK-SM uses utf-8 only if the TCOSS code page is 0 or 1 and the text cannot be converted without errors to ISO-8859-1/2/7, e.g. for the Euro character.

3.9.17 Support of Japanese Text

It is now possible to send and receive Japanese subjects and body text. This is achieved by supporting the “iso-2022-jp” character set in MIME messages. You have to set following registry keys to turn on the language support (Shift-JIS 932 Codepage):

```

“TCLINKSM\Topcall\CodePage=0x3a4”
“TCLINKSM\General\PCCodePage=0x3a4”

```

3.9.18 Support of UNIX “LF Instead of CRLF” Behavior

This means that TC/LINK-SM supports UNIX and Windows text line behavior. In the UNIX world lines are separated with only a LF (=LineFeeds). In the Windows world a CR (=Carriage Return) and a LF is used. E.g. this is important during the parsing of the MIME header.

3.9.19 Support of T.37 (“Fax over SMTP”)

With T.37 support (as standardized by ITU) KCS can send and receive fax over SMTP in its “simple mode” (RFC 2305). This is done by attaching the fax as a TIFF Profile S image (RFC 2301) to a standard email and using a special addressing syntax (RFC 2303/2304). As KCS already provides a gateway to Internet mail (TC/LINK-SM), changes are only needed in supporting the new image format and mapping of the new address format. There are following possible ways to use the T.37 support:

Direction	Usage
Fax -> KCS -> T.37 gateway	KCS is used as fax gateway. Fax will be sent with LINK-SM to the T.37 gateway. Originator address is in RFC2304 style. MUST change SMTP.MAP file (see below for more information).
T.37 gateway -> KCS -> Fax	KCS is used as fax gateway. Fax will be received with LINK-SM from the T.37 gateway. Originator will be T.37 address.
Mail System -> KCS -> T.37 gateway	KCS is used as mail gateway. Mail will be sent with LINK-SM to the T.37 gateway. Originator will be mail address. No changes needed in MAP file.

If you want to use the first case you have to change the SMTP.MAP file. Please remove the "REM" headers of the T.37 entry in the TO_MAIL_ORIG section.

Addressing syntax of T.37 messages:

FAX=<faxnumber>@<domain>

For example:

FAX=+4318635321@company.com

FAX=018635321@company.com

3.9.20 Additional Recipient Check

Following registry key forces the TC/LINK-SM to check the recipient already, when the "RCPT TO:" command is sent from a distant SMTP client. If the link receives an email, it will check first whether the recipient is a KCS user. Otherwise, the link will reject the "RCPT TO:" command from the SMTP client. If the key is not set, the default behavior is not changed and the recipient is checked later, where a non-delivery will be sent if the recipient is not a KCS user.

Name	Type	Default	Remarks
TCLSM\SMRecipientCheck	DWORD	0	Set to 1: SMTPIN service type is "Free Format". Set to 2: SMTPIN service type is "Topcall"

If set to 1, then the additional check is forced and the LINK searches for SMTPIN addresses with service type "Free Format", i.e. local part of the email address is equal to the SMTPIN address. If set to 2, then the LINK searches for SMTPIN addresses with service type "TOPCALL", i.e. the local part of the email address is appended with a ".".

3.9.21 Filtering of Attachments (Inbound: SMTP->KCS)

It is now possible to remove attachments from emails. This is done, by setting following registry keys:

Name	Type	Default	Remarks
TCMIME\AttachmentFilter	Multi-String	""	Here you can specify the file endings, which should be removed, e.g. "exe vbs bat"
TCMIME\FilterText	String	"An attachment was removed due to mail restrictions!"	Here you can specify the alternative text, which is inserted into the mail, to explain the missing attachment.

3.9.22 Enhanced Spam Filter

In previous versions it was possible to specify the "good" respectively "bad" address list only in the registry ("SMIPList"). Also, it was only possible to specify domain addresses and not whole email addresses. This is now changed. First the LINK-SM checks, if the file "domainlist.txt" exists in the C:\TCOSS\TCLP directory. If it is so, then the IP list is read from there.

Note: Comments may be entered after the <domain> separated by at least one whitespace! Do not enter any blanks in or between IP addresses. For line comments, <Space> should exist only at the beginning of the line. String after <Space> should not contain any spaces.

Example for a "domainlist.txt" file:

```
;john@hotmail.com
;trash.com
;dr.makegood@internet_medicine.com
;spam.com
```

If this list does not exist, the old registry key will be used. The functionality of the key "SMIPMasking" has not changed. So you can now specify whether this list is used as a "good" or "bad" IP list.

3.9.23 Handling of Multipart/Alternative

Many email client applications send the message body as a multipart/alternative content consisting of a plain text version and an HTML version.

With former TC/LINK-SM versions, it was already possible to configure a preferred alternative content, so that the resulting message contained either plain text, or HTML text or both (if no preferred alternative was configured). If no alternative content was configured, the recipient got the message text twice.

Now, TC/LINK-SM can be configured to render the message body as a single object with HTML as binary content and additionally text and (if needed) image alternatives. This is handled similar to rich text processing in TC/LINK-MX and TC/LINK-LN.

Setup installs document conversion scripts for file extensions HTM and HTML. These scripts use the Internet Explorer.

You can configure TC/LINK-SM to start the HTML message body on the fax cover sheet. The table below shows the recommended value for registry key *General\AltImgOnFirstPage*, assuming that the default script is used. If a different document conversion script shall be used, it must be copied manually to C:\TCOSS\TCLP\SCRIPT after running KCS setup, and the page margins configured in the *General\AltImgOnFirstPage* must be adjusted. Please consult the TCLINK manual for a detailed description.

The following registry values decide how text and html alternatives of the message body are handled:

Name	Type	Default	Remarks
TCMIME\HTMLAsAlternative	Dword	0	0: take text or html or both, as configured in PreferredAltContent 1: create 1 html object with text alternative 2: create html or mht object with text alternative (mht is created if the body contains embedded images)
TCMIME\PreferredAltContent	String	""	For compatibility with old versions, use one of the following values: "plain" ... for only the text message "html" ... for only the html message "" ... text and html This setting is only valid if HTMLAsAlternative is 0.

General\Support\MultipartRelatedHtml	Dword	0	1: Any references to graphical objects, like icons or screen shots, within the HTML text are resolved before document conversion. The resulting image contains the graphics. Only valid if HTMLAsAlternative is nonzero. 0: No references are resolved, graphic elements are rendered as separate attachments. 2: No binary attachments for the pictures
General\AltImgOnFirstPage	Multi-String	""	To start the HTML message body on the cover sheet, set the following values: HTML,100,100,4 HTML,100,100,4
General\AltForceBodyToTCI	Dword	0	1: Force document conversion for the HTML message body, even if recipients support binary attachments

3.9.24 Restricted UTF-8 Support

The character set "utf-8" is now supported. But this is restricted. The TC/LINK-SM does only recognize the keyword and translates it to the configured TCOSS codepage (e.g.: 0, 1, 874, 930, 932, 936). The full "utf-8" support is currently not possible as TCOSS does not support this.

3.9.25 Support of the Windows-1253 Character Set

The TC/LINK-SM now understands the Windows-1253 (Greek) codepage. It is recommended to run the whole KCS system under the Greek Windows codepage to get the best results because the TCOSS codepage 0 do not contain all Greek characters.

3.9.26 Support of ISO-2022-CN and GB2312 Character Set

It is now possible to send and receive Chinese subjects and body text. This is achieved by supporting the iso-2022-cn char set in MIME messages. You have to set following registry keys to turn on the language support ("Simplified Chinese" 936 Codepage or "Traditional Chinese" 930 Codepage):

```
"TCLINKSM\Topcall\CodePage=0x3a8"  
"TCLINKSM\General\PCCodePage=0x3a8"
```

or

```
"TCLINKSM\Topcall\CodePage=0x3a2"  
"TCLINKSM\General\PCCodePage=0x3a2"
```

3.9.27 Support of ISO-8859-15 Character Set

TC/LINK-SM supports the ISO-8859-15 character set in messages received via SMTP. Subjects and body text using this character set are correctly converted to TCOSS characters.

3.9.28 SMTP Authentication

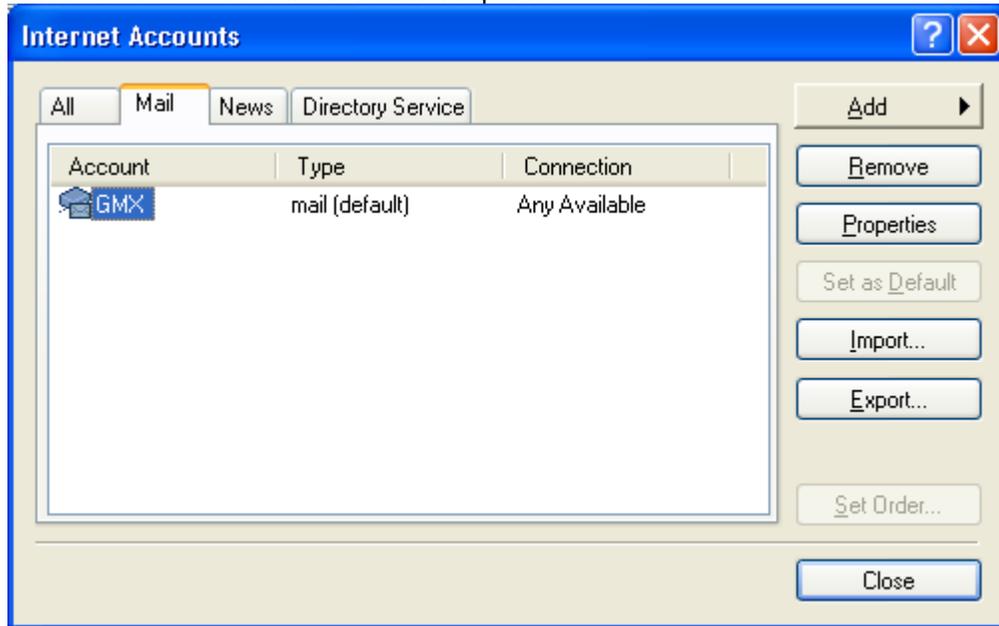
TC/LINK-SM supports the SMTP AUTH functionality. This often-used RFC standard enables the link to request a user/password login from the SMTP client (like Outlook). To use this feature you have to create the following new registry key:

Name	Type	Default	Remarks
TCLSM\Authentication	DWORD	0	Set the key to 1 to enable the feature.

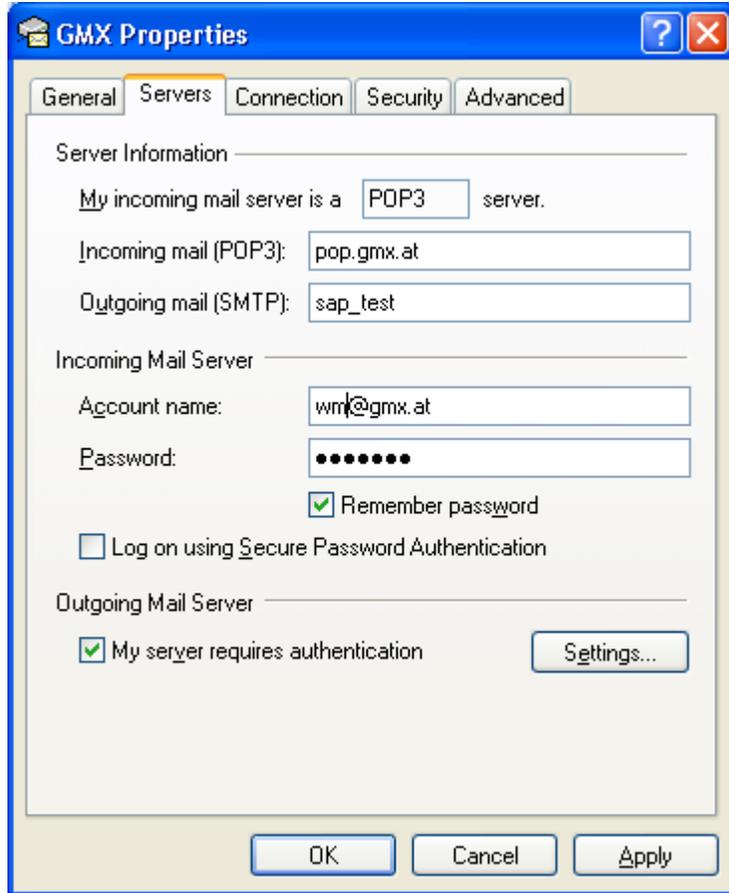
The TC/LINK-SM awaits an existing KCS user as login information. If the client does not support SMTP Authentication, then you should disable this feature. See following example for the configuration of a mail client to use this feature (Outlook Express):

Go to "Tools->Accounts"

Select the correct account and click "Properties"



Go to the “Servers” tab:



Select “My server requires authentication” and change the settings to a valid account name and password:



Important: TC/Web does currently **NOT** support SMTP authentication. So if you enable this feature on the TC/LINK-SM, which receives the messages from TC/Web, then it will not work.

3.9.29 DNS File Lookup

It is now possible to use a text file for DNS lookups. This means that every message sent from KCS to SMTP gets checked for a matching recipient in the DNS file. In case a recipient matches, the mail server from the file will be used. To use this feature first create following new registry value

Name	Type	Default	Remarks
TCLSM\DNSFile	String	""	The full file name of the DNS file (including path)

If a DNS file is configured in registry value TCLSM\DNSFile and can be opened, TC/LINK-SM uses this file to search for a mail server name. The registry value TCLSM\UseDNS is not relevant for this search.

The format of each line in the DNS file must be the following:

```

    email_address      <TAB>  mail_server[:port]
e.g.
    hugo@kofax.com      xyserv.kofax.com
    fred@kofax.com      10.20.127.1:1025
    nurejew@gmx.at      mx0.gmx.de

```

The mail_server can be either a server name or an IPv4 address. Additionally, a port number can be specified.

You can use wildcards in the email addresses specified in the DNS file. One wildcard character * can be used in the local part of the address, either at the beginning or at the end. Additionally, one wildcard character * can be used in the domain part of the address, either at the beginning or at the end.

Examples:

```

*@kofax.com
*_mueller@kofax.com
Hugo_*@kofax.com
*@*.microsoft.com
support@*.microsoft.com

```

TC/LINK-SM uses the first matching line only.

To find the IP address for the mail server specified in the DNS file, TC/LINK-SM does an A record lookup, including the local hosts file.

Registry value TCLSM\UseDNS is consulted if no matching mail server was found in the DNS file.

3.9.30 “Reply-To” Support

With TC/MIME version 1.18.00 it is possible to configure a “Reply-To” address in the user profile. This is done by defining a special service (e.g. “REPLYTO”), for which an address must be entered in the user profile for the users who want to use the special “Reply-To” email address. In the TC/MIME registry you have to specify the defined service.

Name	Type	Default	Remarks
TCMIME\ReplyToService	String	""	The name of the service, which will be searched for in the user profile.

If a user has such an address configured, then the “Reply-To:” header field will be added in the email, so that every reply to that message will be sent to the configured email address and not to the original email address of the sender.

Currently, you have to create the service manually:

Services

Service: Type:

Description: Prefix:

Image Restricted Text Delete
 Text Binary Save
 OCR Conversion

Service	Descrip	Docum	Prefix	Address
EXCHANGE	Exchar	TIB	EXCHANGE:	Free Format
FAX	Fax	RTI	F:	Fax
FREE	Free	RTIB		Free Format
FXI	Fax	RTI	FXI:	Fax
GWFA2	Fax	TI	F:	Fax
GWSEMA	Groupw	RTIB	TCLGW2QI:	Free Format
MYSMTP	Internet	RTIB	TCLSM5QI:	Free Format
NOTES	Lotus	TIB	NOTES:	Free Format
REPLYTO	reply to	TIB		Free Format
RESOLVE	TEST	TIB		Free Format
SAPSMTP	Internet	RTIB	SAPSMQI:	Free Format

Then you have to create the address entry in the user profile:

User Profile - CS1

Queue Length/Age | TC/Broadcast | FaxPlus | TC/WEB | TC/WEB Identity Rights
 General | Address | Event | Rights | Manual Fax | Distributor | Authorize/Sign | Alert

Service: Addr. no.: Active

Free address:

Active	No	Service	Number:
	5	VOICE	111,
	6	VOICE_F	111,
	7	VOICE_S	111,
	8	SMT PIN	hello,
	9	REPLYTO	gore69@a1.net,

3.9.31 Ignore the “Date:” Header Field

It is now possible to ignore the “Date:” header field, so that instead the TCOSS time will be used as the “time_created” date. This can be important for time zone problems.

Name	Type	Default	Remarks
TCMIME\IgnoreDate	DWORD	0	Set to 1, if the feature shall be activated.

3.9.32 Support of the Thai Character Set “Windows-874”

It is possible to send and receive Thai subjects and body text. This is achieved by supporting the “Windows-874” char set in MIME messages. You have to set following registry keys to turn on the language support:

```
"TCLINKSM\Topcall\CodePage=0x36a"      (= decimal "874")
"TCLINKSM\General\PCCodePage=0x36a"
```

3.9.33 Support of “Message/Partial” Attachments

The “message/partial” content-type, which is defined in the RFC standard 2046, allows the email sender to split up an attachment into several parts, which are then sent in single emails.

The TC/LINK-SM is now able to concatenate those received “message/partial” attachments, by rebuilding the attachment accordingly to the RFC standard.

Attention: If the link is configured for synchronous mode, any partial message reception will fall into a timeout.

3.9.34 Support of Custom Header Fields

This feature allows the TC/LINK-SM to relay custom MIME header fields. This configurable header field will be recognized by the TCMIME.DLL and stored in a “ts_xfield” of the TCSI message. It will be written by the TC/LINK-SM in the MIME header, when sending this message out again as an email and in the notification back.

The name of the header field must be specified in the following new registry key:

```
"TCLINKSM\TCMIME\CustomHeader" (REG_SZ)
```

You have to specify the name **with** the colon (e.g. “MyField:”). Additionally, you need at least the version 2.12.01 of the TCLINK.EXE

Example MIME Header:

```
To: kristina.wilewska@ibx.se
Subject: Purchase Order Number: IBXTestKristina2
Mime-Version: 1.0
Content-Type: multipart/mixed; boundary="2418004.1115106125045.JavaMail.SYSTEM@pra46xpc1"
IBX-Message-ID: IBXTestKristina2
Date: Tue, 3 May 2005 09:42:06 +0200 (CEST)
X-BTI-AntiSpam: sta:false/12/019,dcc:passed,rbl:passed,wlbl:none
Return-Path: ibxemailservice@ibxnordic.com
X-OriginalArrivalTime: 03 May 2005 07:45:26.0270 (UTC) FILETIME=[11E2A1E0:01C54FB4]
```

In this example you would configure “IBX-Message-ID:” in the registry value, so that the LINK-SM stores the value of this custom MIME header field (“IBXTestKristina2”) in the KCS message.

3.9.35 Support of Additional TC MIME Header Fields

The LINK-SM supports additional MIME header fields, which sets different KCS send options. Here is the list:

Enhanced “X-Priority”:	Possible values are
1	High
3	Normal
5	Low

11	Superior1
12	Superior2
.	
.	
18	Superior8.

“X-PriorityCC”:	Possible values are
1	High
3	Normal
5	Low
11	Superior1
12	Superior2
.	
.	
18	Superior8.

“X-TCRegistered”:	possible values are
1	Registered Message

“X-TCFaxResolution”:	possible values are
1	High Resolution

“X-TCAuthorization”:	here you can specify KCS user ids, which must authorize the message. If you have more than one authorizer, you must use the comma as a separator
-----------------------------	--

- ..

3.9.36 Message Sensitivity

When sending from KCS to a remote mail server, TC/LINK-SM can optionally specify the message sensitivity (MIME tag Sensitivity).

In TC/LINK-SM configuration, you can assign a sensitivity level for all messages or for messages with certain priority values. By default, no such mapping exists, and no sensitivity information is included in the message.

Registry value: TCLINKSM\TCMIME\Sensitivity (MULTI_SZ)

The registry value is created automatically when TC/LINK-SM starts. Its default value is empty; this means no sensitivity information is written.

Only the first four lines in this multi-string value are evaluated.

Each line can contain a mapping between priority and sensitivity, in syntax: <Priority>=<Sensitivity>

e.g.: SUPERIOR_1=Private

If a line contains only a sensitivity value, this value is used where the previous mappings did not match.

Example:

Values in TCMIME\Sensitivity	Description
SUPERIOR_20=Company-Confidential Private	In messages with priority SUPERIOR_20, set Sensitivity: Company-Confidential In all other messages, set Sensitivity: Private

Possible priority values are: LOW, NORM, HIGH, SUPERIOR_1, SUPERIOR_2 up to SUPERIOR_27. These priority constants are evaluated in a case-insensitive way, e.g. Superior_1 is also accepted.

Leading and trailing blanks are ignored. If the sensitivity string contains a blank character, it must be set between double quotes.

3.9.37 Option to Remove Prefix from SMTP Recipient Address

TC/LINK-SM can optionally remove a prefix from the SMTP recipient address.

This feature was needed for a customer using a “SunOne messaging server 5.2 sp2” to forward messages to TC/LINK-SM. The server added a virtual IP address prefix to the recipient address.

For example: **@10.11.143.4:FAX#0691254847@faxserver.interno.it**
Instead of the real address: **FAX#0691254847@faxserver.interno.it**

A new registry value TCLSM\IgnoredPrefix (REG_SZ) defines which address prefix should be removed from recipient addresses.

The value can be the exact prefix or can use one wildcard character (*). Trailing wildcard characters are ignored.

Examples:

@10.11.143.4: complete prefix specified
@*: prefix starts with @ and ends with :
*: prefix ends with :

The registry value TCLSM\IgnoredPrefix must be created manually. If it does not exist or is empty, the feature will be disabled.

3.9.38 Create Multipart Alternative with XSLTTransform from PS

In combination with the XSLTTransform link exit from Professional Services the TCMIME.DLL is now able to generate multipart-alternative attachments. This means that as a prerequisite XSLTTransform must be installed and configured to use a specific XSLT transformation. Please contact PS for further information. As soon as you have configured it, you just have to set the following registry value:

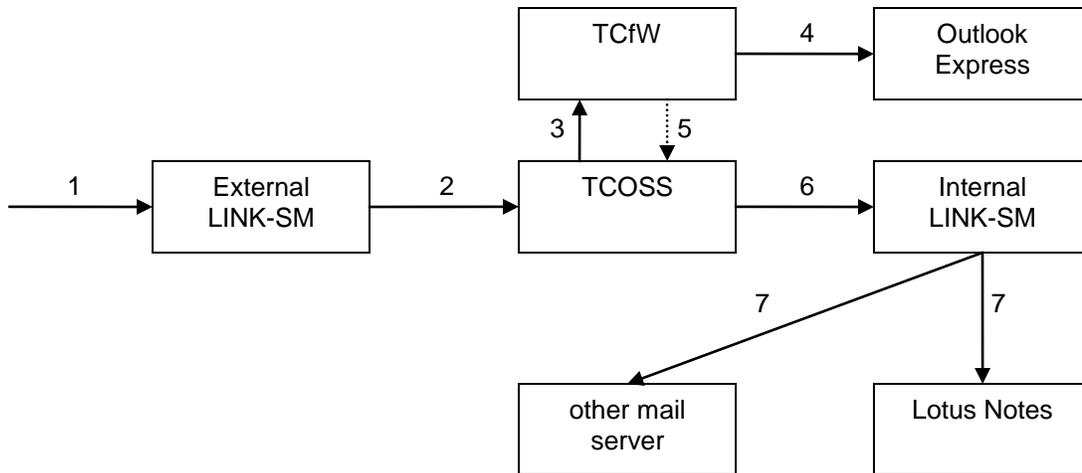
TOPCALL\TCLINKSM\TCMIME\CreateAltContent (DWORD) = 1

3.9.39 Transparent SMTP Relaying

This feature allows TC/LINK-SM to store the MIME content as Outlook Express messages on TCOSS. The advantages of using Outlook Express are the following:

- It is free and preinstalled on almost every Windows OS.
- Outlook Express files (they have the extension “.EML”) are simple text files, which contain the MIME encoded content. No special API needed.

Additionally, TCfW already provides the possibility to open attachments within TCfW. The following diagram displays the supported workflow. Please keep in mind that if you do not have any other link to forward the message, the EML attachment will be part of the message and will not be removed:

**Workflow:**

1. Receive email.
2. TC/LINK-SM creates an additional Outlook Express (=".EML") attachment and puts the message into TCOSS.
3. The message will be opened with TCfW.
4. By double-clicking, the ".EML" attachment can be opened with Outlook Express. This is only needed if the email is not readable.
5. The distributor sends the email to a KCS user who has an In-Event to his SMTP address, or he sends it to any other SMTP recipient. The dashed line represents the fact that changed content will not be part of the forwarded email.
6. The LINK-SM gets the send order from TCOSS.
7. The LINK-SM sends the original email to the specified email recipient (either Lotus Notes or any other mail server).

This feature can be enabled by setting the following registry value (do not forget to set it in both links):

```
TOPCALL\TCLINKSM\TCLSM\KeepOriginalMIME (DWORD) = 1
```

Restrictions:

- If the distributor changes the content of the email within TCfW, the recipient will not receive the changes. This also applies for ++commands.
- The transparent relaying is only implemented within the LINK-SM. No other KCS applications were changed during this implementation.
- TCfW will still display the MIME decoded message, even if there was a decoding problem.

3.9.40 Special MIME Header Fields Written by TC/LINK-SM**3.9.40.1 X-Priority**

The TC/LINK-SM supports the usage of X-Priority in both directions. It is set in the MIME header to 1, 3 or 5 according to the KCS priorities High, Normal or Low. The special priorities High1 – Highest are mapped to 1. Additionally, the header field "Importance" is set. This is used by Lotus Notes, where the possible values are "High", "Normal" and "Low". They are mapped in the same way as the X-Priority value.

3.9.40.2 X-OriginalArrivalTime

TC/LINK-SM stores the UTC-based send time in the field X-OriginalArrivalTime.

This field contains the same time as the "Date:" field, but the value is based on UTC time, i.e. the time zone offset is -0000.

Example:

Date: Wed, 24 Oct 2007 09:47:44 +0200

X-OriginalArrivalTime: 24 Oct 2007 07:47:44 -0000

3.9.41 Support of TCSMIME

TCSMIME is a Professional Services product. It is able to sign outgoing emails. To use it together with TC/LINK-SM you have to create manually the following registry key:

TOPCALL\TCLINKSM\TCLSM\SMIMELibrary (RegSZ)

Set this value to the location (path) of the TCSMIME.DLL (e.g. "C:\TOPCALL\SHARED\TCSMIME.DLL"). As soon as the value is set, TC/LINK-SM will always call this DLL before sending out an email. If the signing fails, you will find a warning in the TC/LINK-SM trace file, but still the message will be sent.

3.9.42 Setting the HTML Character Set

Some applications send out HTML text without specifying the used character set within the HTML header. Instead the MIME header is used to store the information. This can lead to the problem, if the HTML text needs to be faxed out. The TCDC uses only the HTML file and has no access to the additional information from the MIME header.

To solve this problem TC/LINK-SM can add the character set information to the HTML header, if this information is missing. To turn on this feature, set the following registry value to 1:

TOPCALL\TCLINKSM\TCLSM\SetHTMLCharSet (DWORD)

3.9.43 Enable Signed Mails to Exchange Feature

TC/LINK-SM can support specific signed emails that are routed to Microsoft Exchange via LINK-MX. This feature is disabled by default. If enabled, it can lead to a problem as soon as the TC/LINK-SM receives other signed email. To enable this feature set the following registry value to 1:

TOPCALL\TCLINKSM\TCLSM\SignedMailsToExchange (DWORD)

3.9.44 Store SMTP Server Response in KCS Send Order

The SMTP protocol defines that the receiving SMTP server has to send a positive completion reply when it accepts the received message data. See the red line in the following example:

```
TCP<- .
TCP->250 2.6.0 <20070622_155957_C1_02e2f8e7_C2_0000004b_Name_00048429285@link.te3domain.com>
Queued mail for delivery
TCP<-QUIT
TCP->221 2.0.0 te3ms.TE3DOMAIN.COM Service closing transmission channel
```

By default, this information is not stored anywhere.

But you can configure TC/LINK-SM to store the first 80 characters of this response in the TCOSS send order. The response is then visible in the TCFW outbox in column **Response**.

To enable this feature, set the following registry value to 1:

TOPCALL\TCLINKSM\TCLSM\KeepOriginalSMTPResponse (DWORD)

Restriction:

If TC/LINK-SM requests a (non-textual) notification for this message (MIMENotifFormat = 3 or 4), the error text is overwritten as soon as the notification arrives.

3.9.45 Synchronous Operation

Caution: Synchronous operation shall not be used if the link instance must support partial messages (messages of type message/partial).

By default, TC/LINK terminates the SMTP conversation as soon as the received message has been stored in a temporary file (LSM file in the TEMP folder). This can lead to information loss if the link computer is damaged before the LSM file could be processed.

Optionally, the link waits until the message has successfully posted or an error or timeout has occurred.

This is configured via registry value TCLSM\WaitTillPosted (REG_DWORD, default is 0).

If the value is nonzero, it is interpreted as the number of minutes that the receiving thread waits until the message has been posted.

If this timeout expires, the SMTP transaction fails with an error (554 Timeout) and the message is not posted to KCS. If a non-delivery notification was requested, TC/LINK additionally returns a non-delivery notification. The additional non-delivery notification provides more information about the error than the SMTP error code. For scenarios where the typical sender cannot handle SMTP messages (e.g. if the sender is a simple client like TC/Web, or an MFP device), the additional non-delivery notification can be disabled by setting registry value Topcall\NonDelNfImmediate to 0.

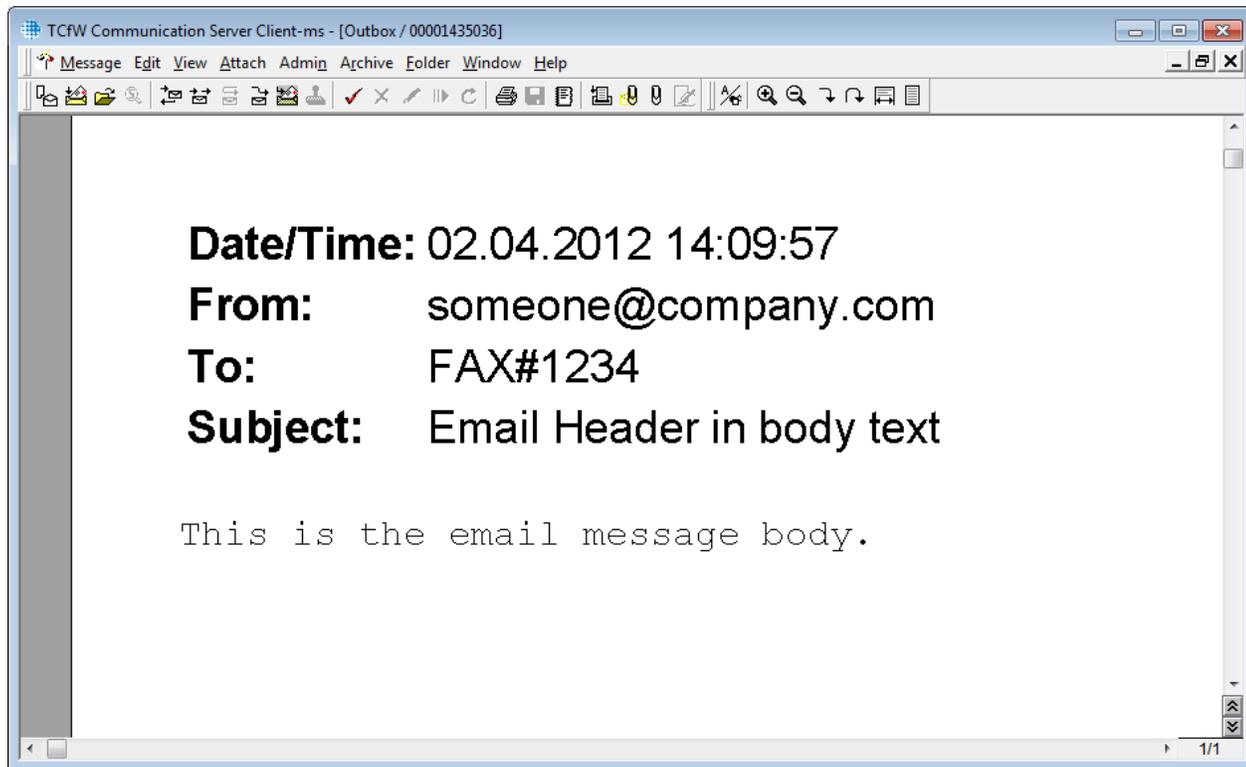
If the link crashes in between, the remote computer interprets the connection loss as an error.

Note: When running in this mode, TC/LINK ignores any LSM files found at link startup.

3.9.46 Email Header in Body Text

During setup, you can select to put email header information like date, from, to and subject in front of the body text in messages from SMTP to KCS.

This feature is available for TC/LINK-SM, TC/LINK-SDD and TC/LINK-MX7.



If this feature is enabled, the header data is put as HTML in front of the email body. If it is a plain text message, the text is put to an basic HTML structure. After that the Document Converter is called (if applicable) and the HTML body including the email header is converted to the configured type of image. If you have VRS processing enabled for HTML content, the HTML header is converted by VRS as well.

3.9.46.1 Configuration of TC/LINK-SM

The following configuration is written during setup if “Email Header in body text” is enabled:

HKEY_LOCAL_MACHINE\Software\TOPCALL\TCLINKSM

Registry Key	Type	Value	Description
General\ExitDll	STRING	EEH2.dll (Version earlier than KCS 10.1 has value <i>ExitEmailHeader.dll</i>)	TC/LINK Exit DLL that enables the feature
General\SupportMultiPartRelatedHtml	DWORD	2	HTML body is created with embedded images. Set to 1 if embedded images have to be added as attachments as well.
TCMIME\HtmlAsAlternative	DWORD	1 (default)	1... Create HTML object with text alternative 2... Create HTML object with MHT alternative (<i>ExitEmailHeader.dll</i> does not support this)

Note: Support of TCMIME\HtmlAsAlternative=2 is introduced in KCS 10.1. If you are upgrading from KCS 10.0.1 or an earlier version, change the value of registry key General\ExitDll from *ExitEmailHeader.dll* to *EEH2.dll* and restart TC/LINK-SM. After the restart, make sure the newly created registry keys are set to the values mentioned in the following table.

HKEY_LOCAL_MACHINE\Software\TOPCALL\TCLINKSM\EEH2

Registry Key	Type	Default	Description
ScriptFile	STRING	exit_mailheader.kps	Internal file that describes the changes of the TC/LINK messages that have to be performed. You need to specify this value in the registry key.
TempDir	STRING	c:\tcoss\tclp\tmp\EEH2	Folder for temporary files
TraceLevel	DWORD	0x10	For debugging, set the TraceLevel to 0xff

Refer section [Backward Compatibility](#) for KCS 10.0.1 and earlier versions.

3.9.46.2 Configuration of KCS Capture Connector

Configure the KCS Capture Connector to use the images created by TC/LINK-SM instead of performing an additional document conversion (this is not relevant for the email header generation, but may cause embedded images of the HTML body to be lost). See the parameter *Kofax_FetchAlternativelyAvailable* of the Capture Connector manual.

3.9.46.3 Restrictions

- No other TC/LINK Exits are supported if this feature is enabled (e.g. MetaMail, TC/LINK-MFP).
- RTF mail bodies are not supported.
- If Unicode is not enabled by TCOSS or TC/LINK, plain text body content and content of the email header (e.g. the subject) is converted to the TCOSS code page before the HTML UTF-8 content is created, therefore only characters of the TCOSS code page will be displayed correctly.
- If you use text directives (++ commands) to modify e.g. message subject, the subject is not exchanged in the generated email header in body text.

3.9.46.4 Backward Compatibility

For versions KCS 10.0.1 & earlier, the following configuration is written during setup if “Email Header in body text” is enabled:

HKEY_LOCAL_MACHINE\Software\TOPCALL\TCLINKSM

Registry Key	Type	Value	Description
General\ExitDll	STRING	ExitEmailHeader.dll	TC/LINK Exit DLL that enables the feature
General\SupportMultiPartRelatedHtml	DWORD	2	HTML body is created with embedded images. Set to 1 if embedded images have to be added as attachments as well.
TCMIME\HtmlAsAlternative	DWORD	1	Create HTML object with text alternative

Note: For this feature to work, it is essential that registry value *TCMIME\HtmlAsAlternative* is 1. (Value 2 is not supported, as the exit DLL does not support MHT content).

The email header is created by the TC/LINK extension module *ExitEmailHeader.dll* (*EEH2.dll* from KCS 10.1). This is called before the general TC/LINK conversion and document conversion. Enabling *ExitEmailHeader* always creates a HTML body text that is UTF-8 encoded.

The TC/LINK Exit module has the following additional configuration:

HKEY_LOCAL_MACHINE\Software\TOPCALL\TCLINKSM\ExitEmailHeader

Registry Key	Type	Default	Description
ConfigFile	STRING	ExitEmailHeaderConfig.txt	Configuration file for HTML header
ScriptFile	STRING	ExitEmailHeader.txt	Internal file that describes the changes of the TC/LINK messages that have to be performed
TempDir	STRING	c:\tcoss\tclp\tmp\ExitEmailHeader	Folder for temporary files
TraceLevel	DWORD	0x10	For debugging, set the TraceLevel to 0xff

These values are only created after start-up if the Email Header feature is enabled. The default locations for files is the c:\tcoss\tclp folder.

Note: If you are upgrading from KCS 10.0.1 or earlier version, EEH2.dll is used instead of *ExitEmailHeader.dll*. (Refer sections- Configuration of TC/LINK-SM)

3.9.46.5 Configuration of HTML Header

From KCS 10.1, ExitEmailHeaderConfig.txt is not used by EEH2.dll & thus, the registry key *ConfigFile* is not needed and not created. Email Header configuration is part of the script file configured in the key 'ScriptFile'.

Example:

Date format of header can be changed from script file (exit_mailheader.kps) by commenting the existing line with "//" and adding a similar line with new format

```
//time "dd.MM.yyyy HH:mm:ss", $createdtime
time "MM/dd/yyyy HH:mm:ss", $createdtime
```

For KCS 10.0.1 & earlier versions, the HTML header is defined in the file ExitEmailHeaderConfig.txt in the c:\tcoss\tclp folder. This UTF-8 text file consists of internal variables defining the HTML snippets of the header that is to be created.

You may change the HTML between the quotes to customize the header. If using non-western code page characters it is recommended to escape them. If not, the header characters may not be displayed correctly if an email with HTML in another code page is received and the code pages do not match.

The file is not overwritten by setup.

3.9.47 Performance Improvement Using DNSCACHE File

Every time an outbound message is sent to a specific mail domain, the TC/LINK-SM needs to identify the IP address of the mail server handling e-mails for this specific mail domain. To get this information, the TCLINK will do a DNS Server query and the result of this query is stored in a DNSCACHE file. Next time when a message is sent to the same mail domain, the IP address for establishing the SMTP connection is fetched from the DNSCACHE file. This results in improved performance and message throughput.

Each entry in DNSCACHE file only has a specific TimeToLive (TTL) that is one hour (TimeToLive entry is calculated in seconds since 1.1.1970, 00:00). Therefore, all entries older than TTL are removed from this file. This cleanup of entries prevent TC/LINK-SM to send messages to an old IP address in case the IP of a domain is changed. If TC/LINK-SM does not find an entry for a specific mail domain in the DNSCACHE file, it will do a DNS query and add the results of this DNS query to the DNSCACHE file.

To enable this feature, set the value of TCLSM\UseDNS registry key to 2. The DNSCACHE file is created at the TC/LINK-SM directory. Default location of this file is: C:\TCOSS\TCLP\WORK\TCLINKSM. This location is defined in *TCLINKSM\TCLSM\SMTempDir* registry key.

Each line of the DNSCACHE file has the following information:
maildomain IPAddress Preference TimeToLive

For example,
hotmail.com 104.47.46.33 2 1518430278

When TC/LINK-SM sends a message, it will parse through the DNSCACHE file and remove all the entries where TTL is already expired. When old entries are removed for a domain, a new DNS query is run when sending mail to this mail domain. The result of this query are again added to the DNSCACHE file.

If you delete the DNSCACHE file, it will be created again, but the existing cache information will be lost. If the IP addresses of frequently used domains are changed periodically (or regularly), disable this feature. To disable this feature, create registry sub-key under TCLSM with name DnsCacheDisable (REG_DWORD type) and set its value to 1.

3.10 Useful Installation Hints

3.10.1 Templates

For sending to SMTP from TCfW or another TC/LINK, it is recommended to use text-only templates. Any graphical part such as a company logo or a signature will be converted to the graphical format of the TC/LINK-SM queue for this send order.

3.10.2 The Role of the Postmaster

All error messages (e.g. hop count exceeded, conversion from/to SMTP failed) and messages which cannot be routed correctly will go to the postmaster's in box. Also administrative messages from postmasters of other mail domains or users will often be sent to the postmaster.

- Make sure to check this mailbox regularly.
- Make sure that the postmaster has no events set in his user profile. Otherwise, there is the chance of message looping!

3.11 Troubleshooting

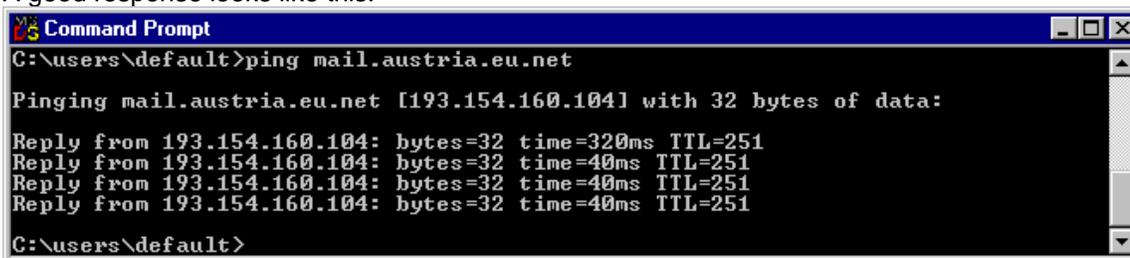
3.11.1 Windows Tools for Checking TCP/IP and SMTP Environment

There are some tools delivered with Windows that are very useful for checking the working environment of TC/LINK-SM. All of them should be run on the TC/LINK-SM PC, using TC/LINK-SMs user account, to test the real operating conditions of TC/LINK-SM.

There are three basic levels of checking environment:

3.11.1.1 TCP/IP Connectivity – “Ping” and “Tracert”

This is the basic level of connectivity. It can be tested by “ping <smarthost>” from the command line: A good response looks like this:



```
Command Prompt
C:\users\default>ping mail.austria.eu.net

Pinging mail.austria.eu.net [193.154.160.104] with 32 bytes of data:

Reply from 193.154.160.104: bytes=32 time=320ms TTL=251
Reply from 193.154.160.104: bytes=32 time=40ms TTL=251
Reply from 193.154.160.104: bytes=32 time=40ms TTL=251
Reply from 193.154.160.104: bytes=32 time=40ms TTL=251

C:\users\default>
```

Possible problems are

- irresolvable target addresses:



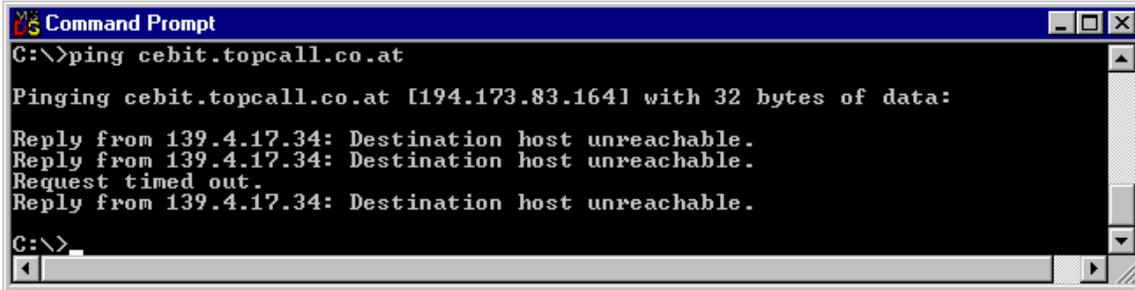
```

Command Prompt
C:\users\default>ping xyz.nonex.com
Bad IP address xyz.nonex.com.
C:\users\default>

```

In this case, you forgot to enter the smart host to the local HOSTS file (see 3.1 “Prerequisites”)

- Destination host unreachable:



```

Command Prompt
C:\>ping cebit.topcall.co.at

Pinging cebit.topcall.co.at [194.173.83.164] with 32 bytes of data:

Reply from 139.4.17.34: Destination host unreachable.
Reply from 139.4.17.34: Destination host unreachable.
Request timed out.
Reply from 139.4.17.34: Destination host unreachable.

C:\>

```

In this case, TCP/IP connectivity to the host is missing. Use the “tracert <smarthost>” tool to find out where connectivity lacks. You will see whether the bad hop is inside your Intranet (contact your network administrator), or outside (like in this example ... contact your ISP)



```

Command Prompt
C:\>tracert cebit.topcall.co.at

Tracing route to cebit.topcall.co.at [194.173.83.164]
over a maximum of 30 hops:

  0  <10 ms    <10 ms    10 ms    ISDN_ROUTER [193.81.166.126]
  1  30 ms     30 ms     30 ms    Vienna1821.Vienna.AT.EU.net [193.154.182.11]
  2  30 ms     40 ms     30 ms    e2.Vienna18.Vienna.AT.EU.net [193.154.182.11]
  3  30 ms     30 ms     30 ms    e3.Vienna14.Vienna.AT.EU.net [193.154.180.2]
  4  80 ms     40 ms     40 ms    Vienna1.AT.EU.net [134.222.51.1]
  5  120 ms    70 ms     120 ms   Amsterdam12.NL.EU.net [134.222.228.113]
  6  80 ms     70 ms     70 ms    Amsterdam2.NL.EU.net [134.222.186.2]
  7  120 ms    100 ms    100 ms   Dortmund2.DE.EU.net [134.222.1.2]
  8  110 ms    90 ms     100 ms   cr2.Dortmund.DE.EU.net [139.4.17.34]
  9  cr2.Dortmund.DE.EU.net [139.4.17.34] reports: Destination host unreachable

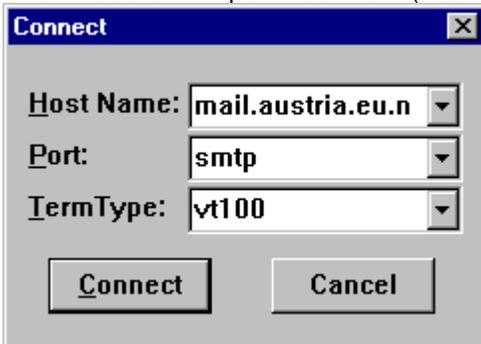
Trace complete.

C:\>

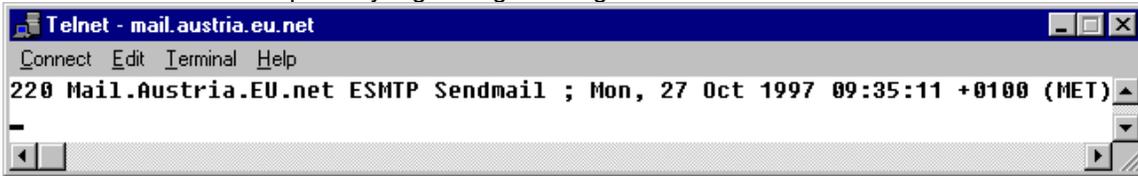
```

3.11.1.2 SMTP Connectivity – “Telnet”

If TCP/IP connectivity is ok, but TC/LINK-SM is still not working, type “telnet” from the command line. Connecting to the smart hosts SMTP port must work (Terminal type does not really matter):



The smart host must respond by a greeting message like:



```
Telnet - mail.austria.eu.net
Connect Edit Terminal Help
220 Mail.Austria.EU.net ESMTP Sendmail ; Mon, 27 Oct 1997 09:35:11 +0100 (MET)
```

If the “ping” is ok, but telnet connection fails, then

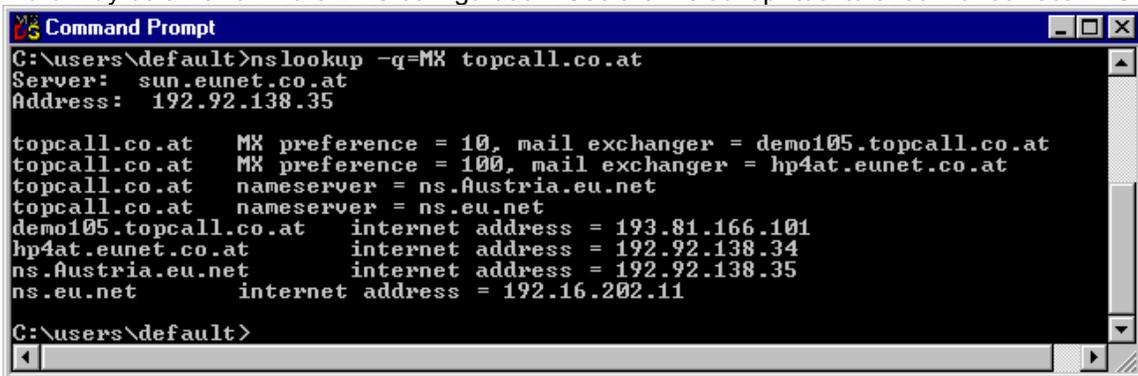
- check the providers mail server name
- ask the provider which port number he is using for mail (standard is 25 or “smtp”)
- check your local “services” file (WinNT\system32\drivers\etc\services) for a correct “smtp” entry matching the port the provider is using:

...		
smtp	25/tcp	mail
...		

3.11.1.3 Nameserver Configuration – nslookup

Note: This section applies only to scenarios using DNS for mail routing! It is not applicable e.g. for scenario 3.4 “TC/LINK-OC for Use with”.

If the two tests above are successful, then TC/LINK-SM should be able to send to SMTP. If reception is not working, there may be an error in the DNS configuration. Use the “nslookup” tool to check for correct DNS entries:



```
Command Prompt
C:\users\default>nslookup -q=MX topcall.co.at
Server: sun.eunet.co.at
Address: 192.92.138.35

topcall.co.at MX preference = 10, mail exchanger = demo105.topcall.co.at
topcall.co.at MX preference = 100, mail exchanger = hp4at.eunet.co.at
topcall.co.at nameserver = ns.Austria.eu.net
topcall.co.at nameserver = ns.eu.net
demo105.topcall.co.at internet address = 193.81.166.101
hp4at.eunet.co.at internet address = 192.92.138.34
ns.Austria.eu.net internet address = 192.92.138.35
ns.eu.net internet address = 192.16.202.11

C:\users\default>
```

- Responsible mail exchanger (“MX” record) for the mail-domain <topcall.co.at> is the host <demo105.topcall.co.at>, with a fallback (higher preference value!) to <hp4at.eunet.co.at>.
- Hostname <demo105.topcall.co.at> resolves to <193.81.166.101> (“A” record). If this machine is the one TC/LINK-SM is running on, this setup is ok.
- The fallback mail queue <hp4at.eunet.co.at> resolves to <192.92.138.34>. Check with your ISP if this is ok.
- The “responsible nameserver” setup (“NS” record) is not used by TC/LINK-SM, but must be a valid hostname.

If either the MX record, or the mail queue entry (only for dialup connections) is missing, contact your ISP.

Note:

- It may take several hours until new or changed DNS entries are spread to all Name Servers in the world. Therefore, even if the “A” and “MX” records are ok, it takes some time until TC/LINK-SM is reachable from anywhere in the world.
- If the “MX” and “A” records setup is ok, but connection is still refused from outside, check if the dial-up line is open, and your firewall enables SMTP access to and from the TC/LINK-SM server.

3.11.2 How to View Message Source in the Trace File

If you want to see the message source (including SMTP envelope), enable the TCP trace for TC/LINK-SM (by running Advanced Setup, or setting the registry "...\\TCLINKSM\\TCLSM\\TCPDebug" to 1), and disable all other trace output. Then, you get the information written to the TC/LINK-SM trace file.

This trace file setting is useful especially for debugging message conversion errors. There are some clients that do not exactly keep the MIME standard; to localize the problems, a MIME trace is necessary.

A complex example of a MIME message, consisting of three message parts (a text block followed by two binary attachments), is written in the Appendix (7.2 "Complex MIME Message Transfer Example").

3.11.3 What to Do When...

3.11.3.1 TC/LINK-SM Does not Start

If TC/LINK-SM does not start correctly, proceed as follows:

- Check the event log for error messages
- Set the trace level to 0xFF
- Restart TC/LINK-SM, and check the trace file (c:\tross\trace\TCLINKSMx.TRC).

The most common error codes are

- 608: TCOSS server not reachable (for native TCTI configuration); check KCS name and path settings.
- 612: TCOSS server not reachable (for RPC TCTI configuration); check KCS name and path settings.
- 609: User not existing; check the Link user setup.
- 610: Invalid password; check Link user password.
- 621: Missing Registrations! Use the Licenses.exe tool to enter a valid TC/LINK-SM license.
- (no code): Temporary directory for TC/LINK-SM not accessible! Create it, accord full access rights.

3.11.3.2 TC/LINK-SM Cannot Send Messages

Congratulation! You got TC/LINK-SM running.

But if you prepare a message in TCfW now and send it to TC/LINK-SM but the message is not sent, check the following:

- Set the trace level to 0xFF
- Enable TCSI and Mail trace
- Check the trace file to see what's happening!

Symptom	Check ...
Although message is sent from TCfW, no message occurs in the TCSI trace	<ul style="list-style-type: none"> • Addressing Correct? (e.g. "SMTP,user@gmx.at") • Service "SMTP" defined correct (Type FREE, prefix = Queueuser + ":-")? • Queue user(s) existing? Must NOT have any address in user profile. • Queues polled correct (see trace file!)? • Message re-routed? Check in TCfW outbox where it goes!
Message occurs in TCSI trace, but conversion fails	<ul style="list-style-type: none"> • Temporary directory existing? Full access rights provided? • Enough free hard disk space available? (min. 50MB)
Message conversion ok, but SMTP protocol does not start (no HELO etc)	<ul style="list-style-type: none"> • Check if external mail server is reachable from PC (Telnet) • Check if external mail server correctly entered to setup and HOSTS file • Check the TCP/IP stack setup: Local IP address, Default router, etc. • Check the configured port number (see trace file)
SMTP protocol starts, but does not succeed	<ul style="list-style-type: none"> • Check the trace file to find out the error. (May e.g. be "invalid hostname" for a bad address, "Access denied" for invalid rights). • Contact your ISP for assistance.

3.11.3.3 TC/LINK-SM Cannot Receive Messages

If TC/LINK-SM is successfully set up to send messages, but unable to receive messages from the Internet, check the following:

- Did you enable at least one listener (Maximum connections > 0)? Check with “telnet” on the local machine (when connecting to “localhost”, port 25, you must get a greeting message).
- Does your TC/LINK-SM server have an “A” and “MX” record assigned, with proper preference setup? Check with “nslookup”!
- Check if your dial-up line is really open during this test!
- Check if your company's firewall enables SMTP access to and from the TC/LINK-SM server! Call your ISP to check via Telnet from outside the company!
- Check for correct setup of the “smtp” port (trace file)!

3.11.3.4 Improper Sending/Reception of Non-ASCII Text and Binaries

If you get scrambled messages from the Internet, check the following:

- This may occur if the transport does not support 8bit transmission. Set TC/LINK-SMs default coding to quoted-printable and base64.
- This can also occur if a Mail client is not set up properly. Enable MIME coding on your client, select ISO-8859-1 codepage for best compatibility, check client's manual for details.
- If your clients or relaying host relies on MIME type/subtype information to display attachments, fill the ...TOPCALL\TCLSM\MIME\Types Registry list according to your needs (this is usually not necessary as most of the clients use the filename extension to display attachments).

4. OPERATION

4.1 Viewing and Changing TC/LINK-SM Setup

The current configuration of TC/LINK-SM can easily be viewed and modified by running its Setup program again. Some advanced settings are only available via registry editor; see 7.1 "Registry Keys Used by TC/LINK-SM" for a complete listing!

Please consult the TC/LINK Manual for general configuration items.

4.2 SMTP Security Considerations

4.2.1 Restricted Privacy of SMTP

As SMTP is a text-based protocol, all SMTP messages pass as either plain text, or simple Base64/Quoted-printable encoding through the Internet.

This means: Anybody having access to any of the hosts involved in the message transfer has the chance to read your mail.

4.2.2 Viruses via SMTP?

The story about an email virus having "GOOD TIMES" in its subject (it is said to cause physical damage to your PC) is NOT TRUE. But what about other possible security risks of SMTP?

- SMTP does not give any connected client or server access to the TC/LINK-SM PC file system.
- SMTP offers no possibility to start any process on the host.
- Problems may arise mainly from TCDC which tries to convert files that may contain harmful macros.
- Binary attachments holding scripts or executables are another source of danger. If they are started by the recipient, anything can happen ...

Countermeasures (improving TCDC security):

- Disable macro execution in the applications installed on the TCLINK server (usually possible via applications setup).
- For several applications, you can get a viewer that does not execute any macros. Install this viewer to print attachments.
- Restrict access to services without binary capability (e.g. by means of the guest user profile) as only these services need document conversion.

4.2.3 Denial-of-Service Attacks

As the SMTP service is usually public available, it is possible for a hacker to occupy all the CPU or network resources of the SMTP server. This makes the host unreachable for all other users.

For TC/LINK-SM, this means:

- As TC/LINK-SM has a limited number of receiver threads, it can be made unreachable by opening and keeping alive a large number of connections simultaneously. Sending to SMTP is not interrupted by this attack.

Countermeasure: Get the IP address of the attacker (by means of TC/LINK-SM trace file or network trace), and add this to the "Bad" IP list; or configure your firewall to reject connection requests from this address!

- As TC/LINK-SM puts received messages into a temporary file first, and as hard disk space is never unlimited, it is theoretically possible to stop TC/LINK-SM by putting in an extremely large message.

Countermeasure: As soon as TC/LINK-SM is restarted by either TCSRVS or the hardware watchdog, the large temporary file is deleted, and TC/LINK-SM is up again. Nevertheless, make sure that TC/LINK-SM has enough hard disk space available.

4.3 Monitoring TC/LINK-SM Operation

There are currently four possibilities to watch TC/LINK-SM operation:

- On the local machine only: Configure the “Interact with desktop” right for TCSRVS (Control Panel / Services / TCSRVS / Properties). Then you will see the console window of TC/LINK-SM on the desktop.
- On local and remote machine: The KCS monitor (TCMON32) can be used to view operation of TC/LINK-SM. It gives also an indication of messages sent/received and notifications sent/received.
- On local and remote machine: The Windows performance monitor can be used to monitor TC/LINK-SM operation, if Performance counters are enabled for it.
- On remote machine: If you install TC/SNMP on the TC/LINK-SM workstation, you can watch operation of TC/LINK-SM via SNMP tools like HP OpenView. See the TC/SNMP documentation for details!

As all of them are implemented in the general part of the Link, see the general TC/LINK Manual for details.

4.4 Summary of Error Conditions and Retries Behavior

4.4.1 KCS to SMTP

There are certain error conditions when a message cannot be delivered to SMTP or a notification is received indication any delivery problem. Some of them are temporary – therefore, retries should be done. Some are definitely permanent – retries do not make sense.

Error Condition	Action	TCfW Outbox “Response” field (TS_LAST_MDA_NOTE)
Message coding to MIME failed	No retries; “inactive – problems”	“Message coding error”
Tempfile write error	TCOSS Retries (BREAK2)	“Disk Write Error”
Error connecting to mailserver	TCOSS Retries (BREAK2)	Winsock error code (e.g. “10061” ... connection refused)
Any temporary SMTP error (code 4xx)	TCOSS Retries (BREAK2)	SMTP error message (e.g. “access denied”)
Any fatal SMTP error (code 5xx)	No retries; “inactive-problems”	SMTP error message (e.g. “unknown recipient”)
Looping message detected	No retries; forward to postmaster	“Hop count exceeded”
Looping notification detected	No retries; forward to postmaster	“Notification loop detected”
DNS resolution failed (temporary)	TCOSS Retries (BREAK2)	DNS error message (e.g. “Nameserver failed”)
DNS resolution failed (fatal)	No retries; “inactive-problems”	DNS error message (e.g. “nonexisting domain”)
a message is too large for transmission	No retries; “inactive – problems”	“message too large”
RFC1894 notification arrived (temporary failure)	TCOSS Retries (BREAK2)	From notification (e.g. “connection failed”)
RFC1894 notification arrived (fatal failure)	No retries; “inactive – problems”	From notification (e.g. “host unknown”)

In addition, the general part of the Link fills the "Error" field with a more general error indication ("LV ... message cannot be delivered to mail recipient"). This string comes from the language file, while all "Response" messages either come from a distant host (language unknown), or are hard coded English messages.

4.4.2 SMTP to KCS

For any errors during message transmission, the sending host is responsible for initiating retries. If any error occurs in the special modules after the message is acknowledged by TC/LINK-SM (... the "250 OK" after transmission), then the MIME source text of the message is forwarded to the local postmaster as a "SMTP problem report".

4.5 Temporary Files

Temporary files used by TC/LINK-SM can be grouped into two categories, with a dedicated folder for each category. All temporary files are removed automatically, no manual cleanup is needed.

4.5.1 Intermediately Stored Messages

TC/LINK-SM uses one or more background threads for SMTP reception. The received MIME messages are stored as text files (extension "LSM") in the folder configured in registry value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TOPCALL\TCLINKSM\TCLSM\SMTempDir
```

By default, this is folder "C:\TCOSS\TCLP\WORK\TCLINKSM".

The main thread of TC/LINK-SM reads these temporary files one by one. After message conversion, the corresponding file is deleted.

MIME messages sent from KCS to the internet are also stored for a short time in this folder (extension "TSM"). These files are automatically removed after message transfer.

It is vital for the TC/LINK-SM operation that this folder is only used by this TC/LINK-SM instance and is not automatically emptied after a link restart.

4.5.2 Temporary Files Used During Message Conversion

Attachments converted by TC/LINK-SM are temporarily copied to folder "C:\TCOSS\TCLP\TMP\TCLINKSM". Under normal conditions, these files are deleted immediately after document conversion. After a link start, TCLINK.EXE removes all files from this folder, in order to get rid of files left over by an irregular link stop.

5. PERFORMANCE

5.1 Test Environment

- TCOSS Computer with 2 Link-SM instances: Xeon E5-2630v3 - 4 CPUs 2.40GHz - 2 CPUs - 4 cores, 4 GB RAM
- Link server with 1 Link-SM: Xeon E5-2630v3 - 4 CPUs 2.40GHz - 4 CPUs - 4 cores, 4 GB RAM
- Microsoft Windows Server 2016 Datacenter. Link running via TCMON in Background – interact with desktop enabled
- 1st Link-PC 2 Link-SM installed (and either 1st or both links running, dependent on the test)
- 2nd Link-PC 1 Link-SM installed
- All Links polling same Link-Queue
- Poll cycle: 10 seconds
- Trace level: 50
- TCOSS running via TCMON in Background – interact with Desktop enabled

5.2 Sending

Following settings were used for sending tests:

- Stopped all Link-SM instances and deleted the traces after every test.
- All default registry settings were used except the server settings, default poll cycle and trace settings.
- NotifMail = 0
- Created a user with five in-events and each in-event was linked to an individual SMTP address.
- Messages were sent using MailTest using an external Link (Link-MX7 in the KCS environment was connected to the TCOSS of the performance system). 200 TOPCALL messages with plain text body and with/without small/big attachment were sent. In total, there were 5x 200 = 1000 send orders in TCOSS in waiting status
- Depending on the type of test, one or more Link-SM instances was started.
- The timestamps of first and last message was used to calculate the number of messages processed per hour.
- UseDNS=2

5.2.1 Plain Text 4 KB 1 Page

Configuration	UseDNS=2 and unknown mail domain	UseDNS=2 and known mail domain
Sending 1 Link SM	ca. 1499 msg/h	ca. 29752 msg/h
Sending 2 Link SM same PC	ca. 3003 msg/h	ca. 56697 msg/h
Sending 2 Link SM on different PCs	ca. 2963 msg/h	ca. 47525 msg/h

5.2.2 Word Attachment 27 KB 1 Page

Configuration	UseDNS=2 and unknown mail domain	UseDNS=2 and known mail domain
Sending 1 Link SM	ca. 1449 msg/h	ca. 18182 msg/h
Sending 2 Link SM same PC	ca. 2908 msg/h	ca. 36544 msg/h
Sending 2 Link SM on different PCs	ca. 2887 msg/h	ca. 35644 msg/h

5.2.3 Word Attachment 653 KB 51 Pages

Configuration	UseDNS=2 and known mail domain
Sending 1 Link SM	ca. 2326 msg/h
Sending 2 Link SM same PC	ca. 4281 msg/h
Sending 2 Link SM on different PCs	ca. 4489 msg/h

5.3 Receiving Without Document Conversion

Following settings were used for receiving tests:

- Stopped all Link-SM instances and deleted the traces after every test.
- All default registry settings were used except for the server settings, default poll cycle, trace settings.
- Sent with one or multiple MailTests. 1000 messages with plain or html body with and with/without small/big attachment were received.
- Each Link instance had its own IP address to which the messages were sent. For example, a test with two Link instances, 10 MailTests were used; Five are sending to Link 1 and the other five to Link 2.
- For tests without conversion, a TOPCALL message was sent to a user.

5.3.1 Plain Text 4 KB 1 Page

Configuration	Throughput
Receiving 1 Link SM	ca. 16667 msg/h
Receiving 2 Link SM on same PC	ca. 30393 msg/h
Receiving 2 Link SM on different PCs	ca. 27586 msg/h

5.3.2 Word Attachment 27 KB 1 Page

Configuration	Throughput
Receiving 1 Link SM	ca. 16667 msg/h
Receiving 2 Link SM on same PC	ca. 30769 msg/h
Receiving 2 Link SM on different PCs	ca. 30252 msg/h

5.3.3 Word Attachment 653 KB 51 Pages

Configuration	Throughput
Receiving 1 Link SM	ca. 4219 msg/h
Receiving 2 Link SM on same PC	ca. 5103 msg/h
Receiving 2 Link SM on different PCs	ca. 7912 msg/h

5.4 Receiving with Document Conversion

Following settings were used for receiving tests:

- Stopped all Link-SM instances and deleted the traces after every test.
- All default registry settings were used except for the server settings, default poll cycle, trace settings.
- Sent with one or multiple MailTests. 1000 messages with plain or html body with and with/without small/big attachment were received.
- Each Link instance had its own IP address to which the messages were sent. For example, a test with two Link instances, 10 MailTests were used; Five are sending to Link 1 and the other five to Link 2.
For tests with TCDC, the message got sent to a fax number (such as fax#1234).

5.4.1 HTML to PDF using KFXConverter - HTML 1 Page

Configuration	One KFXConverter instance	Two KFXConverter instance
Receiving 1 Link SM	ca. 1600 msg/h	
Receiving 2 Link SM on same PC	ca. 1840 msg/h	ca. 3226 msg/h
Receiving 2 Link SM on different PCs	ca. 3152 msg/h	

5.4.2 DOCX to PDF using KFXConverter - Word Attachment 22KB 1 Page

Configuration	One KFXConverter instance	Two KFXConverter instances
Receiving 1 Link SM (average)	ca. 859 msg/h	
Receiving 2 Link SM on same PC	ca. 952 msg/h	ca. 1760 msg/h
Receiving 2 Link SM on different PCs	ca. 1698 msg/h	

5.4.3 DOCX to PDF using KFXConverter - Word Attachment 332KB 70 Pages

Configuration	One KFXConverter instance	Two KFXConverter instances
Receiving 1 Link SM (average)	ca. 418 msg/h	
Receiving 2 Link SM on same PC	ca. 608 msg/h	ca. 832 msg/h
Receiving 2 Link SM on different PCs	ca. 825 msg/h	

5.5 Conclusions to Speed Up LINK-SM

5.5.1 General Information About LINK-SM

Link-SM can only process messages sequentially – one after one, so if one message takes longer the others have to wait. So, installing more than one link can speed up the performance.

One of the key factors in working with TC/LINK-SM is the connection to the mail server. Tests have shown that the time the TC/LINK-SM needs to establish a connection to the mail server is highly unpredictable.

During receiving messages with document conversion, document conversion is the bottleneck. So installing two links on same PC both using document conversion does not speed up the Link-SM performance. To avoid this install one link per PC.

Bottleneck during sending:

Sequential processing per link, message transfer via internet

Bottleneck during receiving:

Sequential processing per link, document conversion

Disabling interact with Desktop also speeds up the performance.

5.5.2 How to Speed Up LINK-SM

- Sending (KCS to Internet)
Install two links on same PC or one link per PC
- Receiving (Internet to KCS)
Without document conversion
Install two links on same PC or one link per PC

With document conversion
Install one link per PC

6. RESTRICTIONS

6.1 General Restrictions

- **SMTP addresses must consist only of ASCII characters.** This is a global restriction of Internet Mail. No German vowel mutations etc. are allowed.
- TC/LINK-SM does no immediate recipient check when receiving from SMTP (recommended by RFC821: When a message is sent to a non-existing recipient, it should be rejected immediately). TC/LINK-SM generates a delivery notification (if the message is passed on to the postmaster via rr99 rerouting) or a non-delivery notification (if the message is rejected) instead.
- Fragmenting of large messages on sending is not supported; incoming fragmented messages are treated like single messages.
- RFC 821 commands SEND/SOML/SAML are not supported (TC/LINK-SM cannot find out whether the recipient's terminal is active at delivery time). They will be treated the same way as the MAIL command (message is always delivered to the recipient's in box).
- Optional RFC 821 commands TURN, VRFY and EXPN are not supported
- Recursion level of attached messages (message that contains message with attached message ...) is limited to a default of 3 (by TCMIME). The rest of the message source is attached as plain text.
- The Performance Counters support built in into TCLINK.EXE does not give correct results for multithreaded parts (the SMTP listeners of TC/LINK-SM). All "Time in xxx" values are not valid for TC/LINK-SM.

6.2 Known Problems

6.2.1 "X-..." Header Fields Can Only Be 256 Characters Long

Due to an internal TCSI buffer limit the "X-..." header fields will be cut off after 256 characters. These header fields are stored in the TCSI message for relaying purposes (mail received by LINK-SM and sent out again via LINK-SM) and are not used for anything else. If you want to keep the complete information, please check the "Transparent SMTP Relaying" (3.8.42) feature.

6.2.2 Using Password Authentication

If you are using the ++PW authentication feature, the following thing can happen:

- Somebody sends a mail from TCfW via TC/LINK-SM to a SMTP address.
- This SMTP address cannot be reached due to any reason.
- As a result, a plain-text non-delivery notification is generated and sent back to TC/LINK-SM.
- As this notification does not contain a ++PW command, it will be rejected. Therefore, the TCfW user will never be notified that his mail has not been delivered!

To avoid loss of notifications, use the ++PW feature only for directly connected clients sending mail to KCS (... and fetching their INBOX e.g. via TC/WEB)!

Never use password authentication (++)PW if mail is sent from KCS to SMTP! You will never get any notifications back!

6.2.3 Bcc: Recipients Not Visible to the Postmaster

If the KCS system is set up to send all undeliverable mail to the local postmaster, it may occur that a Bcc: recipient of an incoming message cannot be reached. The postmaster finds this message in his TCfW inbox, but does not get the information of the intended recipient.

This is a problem of TCfW that does never display Bcc: recipients to any other user than the final recipient. It should be possible to configure a "full address view" for the Administrator.

6.2.4 Microsoft Exchange 5.0 Internet Mail Service

Release 5.0.1458.49 of MS Exchange IMS is said to support enhanced notifications according to RFC1891..1894. But, in fact, it does NOT generate notifications in the RFC1894-specified format.

To avoid send orders keeping in “at next node” state forever, disable the RFC1891..1894 notification capability on TC/LINK-SM when being connected to this SMTP connector.

6.2.5 Case-Sensitive rr99 Process Prior to TCOSS 7.07

Because of the case-sensitivity of TCOSS rr99 in releases prior to 7.07, the SMTP.MAP file should be changed to convert addresses to lowercase. All inactive email addresses in the KCS User Profiles must then be entered in lower case.

Please refer to the release description of TC/LINK-SM 1.05.00 for special hints.

For TCOSS 7.07.00 or higher, rr99 is no longer case sensitive (but case preserving).

6.2.6 Non-Delivery Notification Does Not Work on TC/LINK-OC

If a message is sent from a browser-based client (using TC/WEB) to TC/LINK-OC, and processing in TCLINK fails, then the non-delivery notification does not go to the sender’s KCS inbox.

Reasons:

- A message is addressed to a FAX number.
- Something goes wrong while TCLINK processing (e.g. TCDC fails).
- TCLINK builds a non-delivery notification; the FAX number is the originator of this notification, the KCS user will be the recipient (both addresses are converted to email addresses).
- TC/LINK-OC will attempt to post this notification to the configured smart host.
- BUT: As TC/LINK-OC cannot send messages to the internet, this will fail.

6.2.7 Different Recipient Addresses in RCPT and DATA Field Cause Wrong Sending Type

According to RFC822 following behavior of TC/LINK-SM is implemented: if the recipient address in the DATA section of the mail (e.g.: To: “testperson@company.com” differs from the address in the RCPT TO field (e.g.: RCPT TO: <testperson@test.company.com>), then the message will be sent as “bcc”, instead of “to”. To assure messages to be sent as “to” the addresses have to be the same.

7. APPENDIX

7.1 Registry Keys Used by TC/LINK-SM

TCLSM.DLL uses the following registry keys:

(Location HKEY_LOCAL_MACHINE\Software\TOPCALL\TCLINKSM\TCLSM\...)

Registry Key	Type	Default	Possible Values / Meaning
AcceptRootDomains	DWORD	1	0: disallow sending to root domains, e.g. mailbox@xyz 1: allow sending to root domains
Authentication	DWORD	0	Set the key to 1 to enable this feature (see chapter 3.8.31)
DNSFile	String	""	The full filename of the DNS file (including path) (see chapter 3.8.32)
IgnoreDelNotifReq	DWORD	0	0: delivery notification request is not ignored 1: delivery notification request is ignored
KeepOriginalSMTPResponse	DWORD	0	1: response from the SMTP server is stored in TCOSS send order 0: response from the SMTP server is not stored
MaxSizeFromSMTP	DWORD	0	Max. message size accepted from SMTP (Bytes; 0 = no limit)
MaxSizeToSMTP	DWORD	0	Max. message size to be delivered to SMTP (Bytes; 0 = no limit)
MIMENotifFormat	DWORD	0	default notification format (outgoing) 0 .. plain text notifications only 1 .. Notifications using "Return-Receipt-To" 2 .. Notifications using "Rr" 3 .. Notifications according to RFC 1891..1894 4 .. Notifications according to RFC 2298
NeverNotify	Multistring	""	You may enter a list of SMTP addresses (MAIL FROM:<> parameter) that shall never be notified. If a notification is to be sent to this address, it is sent as a problem report to the local postmaster.
OwnIPAddress	String	""	Empty (or invalid) ... explicit binding disabled. Any valid IP address binds the corresponding instance of TC/LINK-SM to this address!
Port2TC	DWORD	25	Used SMTP port number for reception from SMTP
Port2SMTP	DWORD	25	Used SMTP port number for sending to SMTP
SetHTMLCharSet	DWORD	0	Set it to 1, if the TC/LINK-SM should add the character set information to the HTML header
SMFixedRecipient	Multistring	-	Smart hosts, specified via name or IPv4 address. Optionally, a port number can be added, separated via a colon. Messages to SMTP recipients will be delivered to the first available server from this list.
SMIMELibrary	String	-	Full path name of TCSMIME.DLL (provided by Professional Services). This software signs outgoing emails
SMIMEVerifyLibrary	String	-	Full path name of a certificate verification library (provided by Professional Services). This software verifies signatures in incoming emails.
SignedMailsToExchange	DWORD	0	Set it to 1 if you want to enable this old feature
SMHostName	String	-	Hostname of LINK-SM. Must be an Internet reachable name, if distant mail server uses double reverse lookup.
SMIPList	Multistring	""	A list of IP addresses for access control. See 3.2.3.3 "IP Authentication Setup" for syntax!
SMIPListFile	String	Domainlist.txt	Name of a text file with IP addresses and domain names for access control. If the file exists, it overrules the values specified in SMIPList. If no path is specified, the file must be in C:\TCOSS\TCLP.
SMIPmasking	DWORD	2	IP address access control logic 0 .. "good": only IPs/domains matching at least one entry of the list can access KCS 1 .. "bad": only IPs/domains NOT matching any list entry can access KCS 2 .. Disabled
SMLinkDomain	String	-	Mail-domain name of Link PC
SMMaxConn	DWORD	1	maximum number of simultaneous incoming connections
SMPollCycle	DWORD	0	Poll mail server (first entry in SMFixedRecipient) every <nn> seconds 0 ... disable polling

SMRouteDomains	Multistring	""	All domains listed here will be accepted. Even wildcards can be used. E.g.: domain1.* domain2.com *.domain3.* means: domain1.at will be accepted domain1.com will be accepted domain2.co.com will NOT be accepted my.link.domain3.com will be accepted domain3.it will be accepted This registry key is ignored, if SMRouteEnable is set to 0.
SMRouteEnable	DWORD	0	If this is set to "0", then TC/LINK-SM accepts only messages for the configured domain (SMLinkDomain); if set to "1", then TC/LINK-SM accepts all messages (see SMRouteDomains).
SMRTimeout	DWORD	60000	Reception Timeout from SMTP (ms) until connection is closed. The timeout is reset any time data is received from SMTP
SMTempDir	String	-	Temporary Directory for TCLSM.DLL internal message transfer (exclusively used per link!)
SMTxTimeout	DWORD	60000	Sending Timeout to SMTP (ms) until connection is closed. The timeout is reset any time data is successfully sent to SMTP.
SslContextOptions	DWORD	0x03000004	The default value disables SSLv2 and SSLv3 connections, as these protocols are considered as insecure. The registry value is a bit mask, individual bit values are defined in the OpenSSL API: https://www.openssl.org/docs/ssl/SSL_CTX_set_options.html
TCPDebug	DWORD	0	1 ... Write all data from/to SMTP to the trace file
SMNotifLevel	DWORD	2	Notification level 0 ... no notification at all 1 ... delivery notification on success 2 ... delivery notification on failure
UseDNS	DWORD	0	0 ... disable direct delivery (use smart host) 1 ... enable direct delivery via HOSTS file (A-records) 2 ... enable direct delivery via MX- and A- records
NotifyMailFrom	DWORD	0	0 ... on a notification, "MAIL FROM" is empty (MAIL FROM:<>) 1 ... MAIL FROM:<postmaster@linkdomain>
SMSendSecure	DWORD	0	0 ... SSL only used, if mail server requests it 1 ... SSL connection mandatory, when sending to domains from SMSendSecDomains 2 ... SSL connection always mandatory Only used, if link runs as LINK-SDD
SMSendSecDomains	Multistring	""	List of domains, for which a SSL connection must be used Only used, if link runs as LINK-SDD
SMRcvSecure	DWORD	0	0 ... SSL disabled 1 ... SSL connection mandatory, when receiving from domains from SMRcvSecDomains 2 ... SSL connection always mandatory 3 ... SSL only used, if client requests it Only used, if link runs as LINK-SDD
SMRcvSecDomains	Multistring	""	List of domains, for which a SSL connection must be used Only used, if link runs as LINK-SDD
SMSDDMode	DWORD	0	Indicates whether the link should run as LINK-SM or LINK-SDD. Checks the licenses accordingly. If set to 1, the SSL feature will become available.
CertificatePath	SZ	C:\TOPCALL\SHARED	Folder holding PEM files for SSL connections. The files must be called rootcerts.pem, private.pem, certificate.pem Only used, if link runs as LINK-SDD
Separator	String	"#"	This sign is used for dividing service and number. See chapter 2.1 for more info. Be careful by choosing another separator, as some characters are reserved for other purposes.
SMRecipientCheck	DWORD	0	Set to 1: SMTPIN service type is "Free Format". Set to 2: SMTPIN service type is "Topcall"
SMMaxRecipients	DWORD	100	Here the maximum recipient count can be entered. Upper limit is 1000.
SMPostmaster	SZ		if not empty, this value is used as "mail from" address for notifications
SMDebug	DWORD	0	Must be manually created. If set to 1, then the LINK-SM does not

			remove intermediary files, which are created for reception and sending, but renames them to .LS_ and .TS_. This can be used for error finding.
WaitTillPosted	DWORD	0	0 ... asynchronous reception. SMTP conversation ends when message is stored in temporary file Other values ... synchronous reception. The configured value defines the timeout (in minutes) for processing of this message. The SMTP conversation ends when the message has been posted to TCOSS (or when an error or timeout occurs).

TCMIME.DLL uses the following Registry keys:

(Location HKEY_LOCAL_MACHINE\Software\TOPCALL\TCLINKSM\TCMIME\...)

Registry Key	Type	Default	Possible Values / Meaning
BinaryCoding	DWORD	0	0 .. base64 1 .. 8 Bit (not supported anymore)
ContentDisposition- Filename	DWORD	1	0 ... do not add Filename parameter to Content-Disposition 1 ... do add Filename parameter to Content-Disposition
ConvertTextAttachmentT oUtf8	DWORD	0	0 ... do not change plain text attachments when sending to KCS 1 ... when sending to KCS, try to convert text attachments to UTF-8 with correct Byte Order Mark
InlineContentTypes	Multistring	text/plain text/html text/enriched	A list of MIME content types that shall get a "Content-Disposition: Inline" when converting messages from KCS to MIME format.
MaxLineLength	DWORD	78 (50 ... 1000 is valid)	Indicates the maximum line length of messages from KCS (if lines longer than the configured limit are found, they are encoded properly to keep SMTP line length low).
MaxRecursion	DWORD	3	Maximum level of attached message recursion (Rest is appended as plain text)
MIMETypes	Multistring	""	Gives a list of filename extensions and associated MIME type/subtypes. See 3.9.9 "Configuring MIME Types for Attachments" for details!
SingleTextBlock	DWORD	0	0 ... multiple text blocks allowed 1 ... all text put to single text block (to SMTP)
TextCoding	DWORD	0	0 .. 7 Bit (quoted-printable) 1 .. 8 Bit (not supported anymore)
MimeFileExtensions	Multistring	""	Changes File Extensions (for example: "rfc822 eml" the file "message.rfc822" will be changed to "message.eml")
ConvertSubject	DWORD	0	This key enables the mime.dll to convert special characters in the subject field. Characters which are not in the SMTP character set will be replaced with a '*'. This is necessary, because not all SMTP servers understand the "=?ISO-8859-1?Q" marker.
AttachmentFilter	Multistring	""	Here you can specify the file endings which should be removed, e.g. "exe vbs bat"
FilterText	String	"An attachment was removed due to mail restrictions!"	Here you can specify the alternative text which is inserted into the mail in order to explain the missing attachment.
HTMLAsAlternative	DWORD	0	0: render message body as configured in PreferredAltContent 1: render message body as HTML object with text (and possibly image) alternative. 2: render message body as HTML or MHT object with text (and possibly image alternative)
PreferredAltContent	String	""	Here you should specify the preferred alternative content which should not be removed.
SaveUnknownTextBlock	DWORD	1	Bitfield with significant bits 0 (= 1 decimal) and 1 (= 2 decimal). 0 ... Only converted text will be saved as body. 1 ... A text type attachment containing the unconverted body will be added in some cases when conversion is not lossless. 2 ... A binary type attachment containing the original body text as binary is always added to the message. 3 ... A combination of 1 and 2
Sensitivity	Multistring	""	Defines sensitivity levels according to message priority. If empty, no sensitivity value is written.

ReplyToService	String	""	The name of the service which will be searched for in the user profile. (see chapter 3.8.33)
IgnoreDate	DWORD	0	Set it to 1, if you want to activate this feature. (see chapter 3.8.34)
BufferSize	String	10240	To improve the performance, this key enables the mime.dll to block a specific buffer before processing the mime messages.
DefaultCharset	String	ISO-8859-1	Use this character set if the CharSet attribute is missing/not specified in the content-type field in mail.

Note:

- All TCMIME configurations (except MIMETypes and MaxRecursion) are only effective when sending from KCS to the internet! TC/LINK-SM accepts any valid text/binary coding, lines up to 1095 characters, any number of text blocks, ...
- All TCMIME configurations are reloaded per message conversion; therefore, you need not to restart TC/LINK-SM when changing TCMIME configuration.
- All TCMIME configuration values are created (and filled with default values) when TC/LINK-SM is started the first time. Existing values are not overwritten.

The most important general TCLINK registry values are

(Location HKEY_LOCAL_MACHINE\Software\TOPCALL\TCLINKSM\...)

Registry Key	Type	Default	Possible Values / Meaning
GeneralTracelevel	DWORD	-	General trace level
GeneralMailDebug	DWORD	-	1 ... dump all TCSI objects transmitted between TCLINK.EXE and special mail DLL
GeneralPCCodePage	DWORD	-	PC codepage configured on the Link server
TopcallTCSIDebug	DWORD	-	1 ... dump all TCSI objects from/to KCS
TopcallResolveService	String	RESOLVE	Service used for TC/Broadcast

Note:

- TC/LINK-SM must be stopped and restarted before these changes become effective!
- See the TC/LINK Manual for all common setup, like ++PW authentication, Performance counter support, watchdog (important for large messages) etc.

7.2 Complex MIME Message Transfer Example

```

11:35:22.767 (a0/a1) TCP<- 220 mail.austria.eu.net SMTP service ready
11:35:22.767 (a0/a1) TCP-> HELO kofax.com
11:35:22.767 (a0/a1) TCP<- 250 OK
11:35:22.777 (a0/a1) TCP-> MAIL FROM:<Klaus.Aichner@kofax.com>
11:35:22.777 (a0/a1) TCP<- 250 OK
11:35:22.777 (a0/a1) TCP-> RCPT TO:<nobody@nowhere.com>
11:35:22.777 (a0/a1) TCP<- 250 OK
11:35:22.777 (a0/a1) TCP-> DATA
11:35:22.887 (a0/a1) TCP<- 354 Start mail input, end with <CRLF>.<CRLF>
11:35:22.887 (a0/a1) TCP-> Received: from pcai.kofax.com by kofax.com with SMTP for nobody@nowhere.com; Tue,
02 Sep 1997 11:35:13 +0100
11:35:22.887 (a0/a1) TCP-> Date: 02 Sep 1997 11:35:22 +0100
11:35:22.887 (a0/a1) TCP-> From: Aichners Fullname (Ais Comment) <Klaus.Aichner@kofax.com>
11:35:22.887 (a0/a1) TCP-> To: <nobody@nowhere.com>
11:35:22.887 (a0/a1) TCP-> Subject: test for MIME message
11:35:22.887 (a0/a1) TCP-> Message-Id: 00000656624@pcai.kofax.com
11:35:22.887 (a0/a1) TCP-> MIME-Version: 1.0
11:35:22.887 (a0/a1) TCP-> Content-Type: multipart/mixed; boundary=="_NextPart_245e.742=_312"
11:35:22.887 (a0/a1) TCP-> Content-Transfer-Encoding: 7bit
11:35:22.887 (a0/a1) TCP->
11:35:22.887 (a0/a1) TCP-> ---_NextPart_245e.742=_312
11:35:22.887 (a0/a1) TCP-> Content-Type: text/plain; charset=ISO-8859-1
11:35:22.887 (a0/a1) TCP-> Content-Transfer-Encoding: 8bit
11:35:22.887 (a0/a1) TCP-> Content-Disposition: inline
11:35:22.887 (a0/a1) TCP->
11:35:22.887 (a0/a1) TCP-> this is a text part containing some 8 bit characters.
11:35:22.887 (a0/a1) TCP-> Öse, Ähre, Übel, Tür
11:35:22.887 (a0/a1) TCP->
11:35:22.897 (a0/a1) TCP-> ---_NextPart_245e.742=_312

```

```

11:35:22.897 (a0/a1) TCP-> Content-Type: application/octet-stream; name=tst.bmp
11:35:22.897 (a0/a1) TCP-> Content-Transfer-Encoding: base64
11:35:22.897 (a0/a1) TCP-> Content-Description: bitmap testfile
11:35:22.897 (a0/a1) TCP-> Content-Disposition: attachment; filename=tst.bmp
11:35:22.897 (a0/a1) TCP->
11:35:22.897 (a0/a1) TCP-> Qk3+AwAAAAAAAAAD4AAAAoAAAAZAAAADwAAAABAAEAAAAAAAAAMADAADODgAA2A4AAAAAAAAAAAAAAAA
11:35:22.897 (a0/a1) TCP-> //D/AAD///4B/D////////w/wAA///A/5////////8AAAP///wf////////AAAA=
11:35:22.897 (a0/a1) TCP->
11:35:22.897 (a0/a1) TCP-> ---_NextPart_245e.742=_312
11:35:22.897 (a0/a1) TCP-> Content-Type: Application/msword; name=test.doc
11:35:22.897 (a0/a1) TCP-> Content-Transfer-Encoding: base64
11:35:22.897 (a0/a1) TCP-> Content-Description: Relating documentation
11:35:22.897 (a0/a1) TCP-> Content-Disposition: attachment; filename=test.doc
11:35:22.897 (a0/a1) TCP->
11:35:22.927 (a0/a1) TCP-> OM8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAAABAAAAIQAAAAAAAA
11:35:23.328 (a0/a1) TCP-> AAAAAAAAAAAAAAAAAAAAAA==
11:35:23.328 (a0/a1) TCP->
11:35:23.328 (a0/a1) TCP-> ---_NextPart_245e.742=_312--
11:35:23.328 (a0/a1) TCP->
11:35:23.328 (a0/a1) TCP-> .
11:35:23.338 (a0/a1) TCP<- 250 OK receiving Data
11:35:23.338 (a0/a1) TCP-> QUIT
11:35:23.348 (a0/a1) TCP<- 221 closing transmission channel

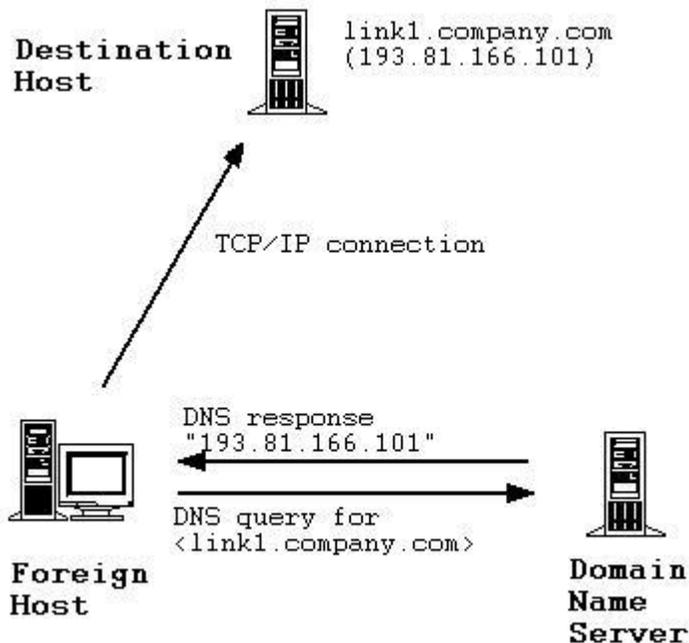
```

7.3 Overview of the DNS Concept

7.3.1 "A" Records

Every computer – client or server – on the Internet has a unique IP (Internet Protocol) address to distinguish it from other computers on the Internet. The IP address is four sets of digits separated by dots (example: <193.81.166.101>). Since this string of numbers would be hard to remember and fraught with potential keying errors, the Domain Name System (DNS) was created so people would not have to remember several confusing numbers. Domain names enable short, alphabetical nicknames to be assigned to IP addresses to describe where a computer is located. Mostly, domain names indicate who or what is located at this site and the type of organization that owns or supports the site. In the IP address example above, <link1.company.com> is the corresponding domain name for the addressed computer. This correlation between the hostname and its IP address is stored in the DNS server and referred to as "A" record.

Example: Foreign host wants to connect to link1.company.com (not knowing its IP address)



- Foreign host starts DNS query to find out the IP address of <link1.company.com> (query for the "A" record of <link1.company.com>)

- The Domain Name Server looks up the entry for link1.company.com (may be either in its own configuration, in its cache, or by recursive resolution) and returns the resulting IP address(es).
- The foreign host uses the IP address from the DNS response and can now contact the destination host.

7.3.2 “MX” Records

The example above (“A” records lookup) is not really sufficient for mail delivery in the whole Internet, as there is not too much flexibility:

- There are problems for mail domains with heavy load: No standardized way is defined to assign multiple hosts to a single domain name for load balancing.
- There are also problems with hosts that should handle mail for multiple mail-domains as there should be only one “A” record per PC.
- Fallback solutions with priority setup are impossible.

Therefore, an own resource record for mail exchangers was defined; the “MX” record. This adds a lot of flexibility by adding an additional layer of resolving mail domains.

Example:

The server <link1.company.com> shall be configured to receive mail for the mail domains <company.com> and for <another.company.at>. As a fallback for both mail domains, the backup server on <link2.company.com> shall be used. The DNS configuration will look as follows:

company.com	MX	link1.company.com	10
company.com	MX	link2.company.com	100
another.company.at	MX	link1.company.com	10
another.company.at	MX	link2.company.com	100
link1.company.com	A	193.81.166.101	
link2.company.com	A	193.81.166.6	

7.3.3 Reverse Lookup – “IN-ADDR.ARPA” Entries

By means of “A” records, you can find out the IP address for a given hostname. But, especially for authentication reasons, it may be of interest to do this the other way round (with every SMTP connection, you get the IP address of the connected client/host; you may want to check this against the sender’s domain, that comes as a parameter of the HELO command).

Therefore, “in-addr.arpa” lookup is defined: if you send a DNS query putting the IP address on the left of the “in-addr.arpa” domain, you will get the hostname for the connected client/host (if it has a valid entry, of course).

Example:

If you get a connection from the IP address “193.81.166.101”, you may issue a lookup like

```
"nslookup -q=ALL 101.166.81.193.in-addr.arpa"
```

The returned “A” Record indicates the hostname corresponding to that IP address:

```
link1.company.com | A | 193.81.166.101
```

With the Microsoft DNS server, the in-addr.arpa entries are created automatically if you enter an A record. On UNIX based DNS servers, this might need to be done manually. See the documentation of the used DNS server for more details.

7.4 TC/LINK-SM and Anti-Spamming Measures

NOTE: Neither “Mail is routed only if a valid MX record is available” nor “Mail is routed only if double reverse lookup is successful” are implemented until now.

As spamming (sending unauthorized, annoying email, abusing the ISP's mail servers) is becoming an issue, more and more ISP's are taking counter measures. This mainly effects email relaying upon which the TC/LINK-SM relies if connected to the Internet.

There are three often-used policies for the provider's mail servers:

7.4.1 Mail Is Routed Only If Sent from a Known Subnet

The mail server will accept mail for routing only if it is sent from a known IP address (or address range).

To enable TC/LINK-SM to use the provider's mail server, simply make sure that the TC/LINK-SM's IP address is in one of the ISP's known address ranges.

Note: You can also configure TC/LINK-SM for using this policy itself (see 3.2.3.3 “IP Authentication Setup”).

7.4.2 Mail Is Routed Only If a Valid MX Record Is Available

The mail server will accept mail for routing only if the sender identifies itself with a valid domain name (the parameter given with the SMTP “HELO” or “EHLO” command).

For TC/LINK-SM, there must be a MX record anyway, otherwise it would never receive mail from the Internet. You have to make sure that the SMLinkDomain (... \TCLINKSM\TCLSM\SMLinkDomain in the registry) has a valid MX record. The TC/LINK-SM uses this setting for the HELO command when opening a connection to the ISP's mail relay.

7.4.3 Mail Is Routed Only If Double Reverse Lookup Is Successful

“Double reverse lookup” is used to check if the IP address of the sender was not manipulated:

- First, a reverse lookup (see 7.3.3) is done to find out the hostname for the sender's IP address.
- Then a normal lookup is done with this hostname to test if this gives the same IP address.

If this process fails, or gives different IP addresses and hostnames than in the ones in the actual connection (hostname from the EHLO or HELO command), the connection request is denied.

For this policy, TC/LINK-SM needs the following entries in the DNS configuration:

- A MX record for all served mail domains (usually only one = SMLinkDomain). The SMLinkDomain MUST have a MX record.
- The MX record points to the TC/LINK-SM PC's hostname
- An A record for the TC/LINK-SM's hostname. This gives the IP address.
- A record for the reverse lookup (this is done by so called “in-addr.arpa” entries).

7.5 Short Introduction to Firewalls

7.5.1 Understanding Firewalls

A firewall is a term used for a part of a car. In cars, firewalls are physical objects that separate the engine from the passengers. They are meant to protect the passenger in case the car's engine catches fire while still providing the driver's access to the engine's controls.

A firewall in computers is a device that protects a private network from the public part (the internet as a whole). The firewall computer, from now on named "firewall", can reach both the protected network and the internet. The protected network cannot reach the internet and the internet cannot reach the protected network.

For someone to reach the internet from inside the protected network, they must telnet to firewall, and use the internet from there.

The simplest form of a firewall is a dual homed system (one system with two network connections). If you can TRUST ALL your users, you can simply setup a Linux (compile it with IP forwarding/gatewaying turned OFF!) and create accounts for everyone. The users can then log in to this system and telnet, FTP, read mail, and use any other service you provided. With this setup, the only computer on your private network that knows anything about the outside world is the firewall. The other system on your protected network does not even need a default route.

This needs re-stating.

Not recommended.

7.5.2 Types of Firewalls

There are two types of firewalls.

1. IP or Filtering Firewalls – that block all but selected network traffic.
2. Proxy Servers – that make the network connections for you.

7.5.2.1 IP Filtering Firewalls

An IP filtering firewall works at the packet level. It is designed to control the flow of packets based the source, destination, port and packet type information contained in each packet.

This type of firewall is very secure but lacks any sort of useful logging. It can block people from accessing private system but it will not tell you who accessed your public systems or who accessed the internet from the inside.

Filtering firewalls are absolute filters. Even if you want to give someone on outside access to your private servers you cannot without giving everyone access to the servers.

7.5.2.2 Proxy Servers

Proxy servers allow indirect internet access through the firewall. The best example of how this works is a person telneting to a system and then telneting from there to another. Only with a proxy server the process is automatic. When you connect to a proxy server with your client software, the proxy server starts its client (proxy) software and passes you the data.

Because proxy servers are duplicating all the communications they can log everything they do.

The great thing about proxy servers is that they are completely secure, when configured correctly. They will not allow someone in through them. There are no direct IP routes.

7.5.3 Drawbacks with Firewalls

The problem with filtering firewalls is that they inhibit the access to your network from the internet. Only services on systems that have pass filters can be accessed. With a proxy server users can login to the firewall and then access any system within the private network they have access to.

Also, new types of network clients and servers a coming out almost daily. When they do you must find a new way to allow controlled access before these services can be used.

7.5.4 Masquerading

Some companies which are connected to the Internet have only one Internet address or at least a very limited number of IP addresses. To be able to provide Internet access to more than one computer the masquerading router changes the IP addresses for all packets which are sent from one side to the other.

Let's look at two examples:

The customer has one "official" IP address from his ISP: 123.45.67.8

The local network side of the router has the IP address 10.0.0.1 subnet mask 255.0.0.0

Note that all addresses starting with 10 do not exist on the Internet.

The following address spaces are reserved for use with private LANs, which are not connected to the Internet, or which use masquerading to connect to the Internet:

Class A: 10.0.0.0 - 10.255.255.255
 Class B: 172.16.0.0 - 172.31.255.255
 Class C: 192.168.0.0 - 192.168.255.255

7.5.4.1 Example 1: Client Access of Internet Resources Through Masquerading Routers

The user on the PC 10.0.0.6 wants to access the well known Microsoft homepage <http://www.microsoft.com> with his Web browser. Thus the browser opens a connection to the www server's IP address at port 80 (http).

As the www server is on a different network, the IP packages are sent to the default router's IP address, which is 10.0.0.1.

When the router forwards the IP packets, it replaces the source address of the packages with its own "official" IP address: 123.45.67.8 and stores the client PC's IP address and port number as well as the www server's IP address and working port number in his memory. Now it knows that packages having those source IP/port and destination IP/port combination belong to the communication between the client and the www server. As long as this communication is established, the masquerading router continuously replacing the client's PC IP/port with its official IP address and port.

Therefore the www server thinks that it is talking to a client having the "official" IP address.

7.5.4.2 Example 2: Mail from the Internet to the Mail Server Inside the Private LAN

To be able to provide services to the Internet, connection requests to the services well known port must be forwarded to the computer with the server software installed on it. In the router's configuration a list of so called "port handlers" tells the router which computer handles requests for which port.

E.g., the TC/LINK-SM PC has the IP address 10.0.0.105 and is configured as the port handler for port 25 in the router's configuration:

```
porthandler 25 10.0.0.105
```

When the router receives a request on 123.45.67.8 port 25 on his official IP address it does not handle this request but forwards the IP packets to 10.0.0.105 port 25. When the TC/LINK-SM answers this request, again the router replaces the TC/LINK-SM's IP address and working port with its own IP address and a free working port for all packets and remembers this communication for the next IP packets.

Therefore the sending SMTP software thinks that it communicates with 123.45.67.8 on port 25.

Of course the router's name and IP address must be known to be the mail exchanger for the company's mail domain (MX record in the providers DNS server!) and not the TC/LINK-SM's IP address!

Limitation: with this configuration, it is not possible to have more than one server for each service. There can be only one SMTP server, one Web server, one FTP server, etc. At least if you want to use the standard well known ports, which is always a good idea.

It is also possible, that the masquerading router serves more than one official IP address. Then there can be multiple servers per service: one for each official IP address.

The configuration might look like

```
porthandler 123.45.67.8:25 10.0.0.105:25  
porthandler 123.45.67.9:25 10.0.0.66:25
```

Requests for 123.45.67.8 port 25 are handled by the TC/LINK-SM as before but additionally requests for 123.45.67.9 port 25 are handled by another mail server with the IP address 10.0.0.66.

Of course masquerading can be combined with an IP filtering or other types of fire walling.

7.5.5 Copyright for the Linux Firewall Howto

Parts of this chapter were taken from the Linux Firewall Howto by David Rudder.
 The Linux How-to may be re-used as long as this copyright information is included:

Copyright =====

Unless otherwise stated, Linux HOWTO documents are copyrighted by their respective authors. Linux HOWTO documents may be reproduced and distributed in whole or in part, in any medium physical or electronic, as long as this copyright notice is retained on all copies. Commercial redistribution is allowed and encouraged; however, the author would like to be notified of any such distributions.

All translations, derivative works, or aggregate works incorporating any Linux HOWTO documents must be covered under this copyright notice. That is, you may not produce a derivative work from a HOWTO and impose additional restrictions on its distribution. Exceptions to these rules may be granted under certain conditions; please contact the Linux HOWTO co-ordinator.

In short, we wish to promote dissemination of this information through as many channels as possible. However, we do wish to retain copyright on the HOWTO documents, and would like to be notified of any plans to redistribute the Howtos.

If you have any questions, please contact Mark Grennan at <markg@netplus.net>.

7.6 Conformance to Recommendations and Directions

TC/LINK-SM conforms to following RFCs:

Number	Brief description
RFC821 (also STD 0010)	SMTP Protocol Definition
RFC822 (also STD 0011)	Internet Mail Message Encoding (plain text)
RFC2045 - RFC2049 (former RFC1521, RFC1522)	Internet Mail Message Encoding (MIME)
RFC 1806	MIME-extension "Content-Disposition"
RFC 1869	SMTP service extension "EHLO"
RFC 1870	SMTP service extension "SIZE"
RFC1891 - RFC1894	Enhanced Notifications for Internet Mail
RFC 974	Mail delivery in the Internet using MX records
RFC 1034, 1035	Domain Name System (DNS)
RFC 2487	STARTTLS extension
RFC 2246	TLS protocol

7.7 Checklist for Setup

TCOSS Server CPU number1)	
Link Server CPU number	
TCOSS version	
TC/LINK-SM license1)	Key: Expire Date: Registrations:
Postscript license1) (optional)	Key: Expire Date: Registrations:
PCL5 license key (optional)	Key: Expire Date: Registrations:
GIF license key (optional)	Key: Expire Date: Registrations:
PDF license (optional)	Key: Expire Date: Registrations:
KCS Name	
Link Type to KCS, transport RPC or Native	
Secondary KCS Name (for tandem servers only)	
Link Type to secondary KCS (for tandem servers only)	
KCS Link User Name	
KCS Link User Password	
TCDCEXE User Name (foreground TCDC only)	
TCDCEXE User Password (foreground TCDC only)	
TCDCEXE User Domain (foreground TCDC only)	
Own Mail Domain Name (TC/LINK-SM only)	
Smarthost name (optional)	

1) For TCOSS < 7.08 in combination with KCS tandem servers these licenses have to be entered for both CPU numbers of the primary and the secondary KCS server.

7.8 SSL – Verification Error Codes

Error code	Description
0	ok: the operation was successful.
2	unable to get issuer certificate: the issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.
3	unable to get certificate CRL: the CRL of a certificate could not be found. Unused.
4	unable to decrypt certificate's signature: the certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value, this is only meaningful for RSA keys.
5	unable to decrypt CRL's signature: the CRL signature could not be decrypted: this means that the actual signature value could not be determined rather than it not matching the expected value. Unused.
6	unable to decode issuer public key: the public key in the certificate SubjectPublicKeyInfo could not be read.
7	certificate signature failure:

	the signature of the certificate is invalid.
8	CRL signature failure: the signature of the certificate is invalid. Unused.
9	certificate is not yet valid: the certificate is not yet valid: the notBefore date is after the current time.
10	certificate has expired: the certificate has expired: that is the notAfter date is before the current time.
11	CRL is not yet valid: the CRL is not yet valid. Unused.
12	CRL has expired: the CRL has expired. Unused.
13	format error in certificate's notBefore field: the certificate notBefore field contains an invalid time.
14	format error in certificate's notAfter field: the certificate notAfter field contains an invalid time.
15	format error in CRL's lastUpdate field: the CRL lastUpdate field contains an invalid time. Unused.
16	format error in CRL's nextUpdate field: the CRL nextUpdate field contains an invalid time. Unused.
17	out of memory: an error occurred trying to allocate memory. This should never happen.
18	self-signed certificate: the passed certificate is self-signed and the same certificate cannot be found in the list of trusted certificates.
19	self-signed certificate in certificate chain: the certificate chain could be built up using the untrusted certificates but the root could not be found locally.
20	unable to get local issuer certificate: the issuer certificate of a locally looked up certificate could not be found. This normally means the list of trusted certificates is not complete.
21	unable to verify the first certificate: no signatures could be verified because the chain contains only one certificate and it is not self-signed.
22	certificate chain too long: the certificate chain length is greater than the supplied maximum depth. Unused.
24	invalid CA certificate: a CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.
25	path length constraint exceeded: the basicConstraints pathlength parameter has been exceeded.
26	unsupported certificate purpose: the supplied certificate cannot be used for the specified purpose.
27	unsupported certificate purpose: the supplied certificate cannot be used for the specified purpose.
28	certificate rejected: the root CA is marked to reject the specified purpose.
29	subject issuer mismatch: the current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate. Only displayed when the -issuer_checks option is set.
30	authority and subject key identifier mismatch: the current candidate issuer certificate was rejected because its subject key identifier was present and did not match the authority key identifier current certificate. Only displayed when the -issuer_checks option is set.
31	authority and issuer serial number mismatch: the current candidate issuer certificate was rejected because its issuer name and serial

	number was present and did not match the authority key identifier of the current certificate. Only displayed when the -issuer_checks option is set.
32	key usage does not include certificate signing: the current candidate issuer certificate was rejected because its keyUsage extension does not permit certificate signing.
50	application verification failure: an application specific error. Unused.

7.9 Glossary

The following abbreviations and terms are frequently used in this manual:

Abbreviation	Meaning
ISP	Internet Service Provider; the company that offers you access to the Internet
SMTP	Simple Mail Transfer Protocol; The mail delivery protocol of Internet mail
MIME	Multipurpose Internet Mail Extensions; the mail format of Internet Mail
TCP	Transmission Control Protocol; stream-oriented network connection used for SMTP
IP	Internet Protocol; lowest level of connectivity objected here
DNS	Domain Name System; the system to resolve hostnames to IP addresses (the "A" record), and other so-called "resource records"
MX record	"Mail Exchanger" resource record. Part of DNS; maps a mail domain to responsible hostnames.
POP3	Post Office Protocol Version 3: Simple Protocol for Users to fetch their mail from a server
IMAP4	Internet Mail Access Protocol Version 4: Advanced Protocol for mail server access
RFC	Request For Comment. Documents for Internet standardization procedures; available e.g. from < http://www.isi.edu/publications.html >.