SMTP Status Codes

This document describes the set of extended status codes for use within the SMTP mail system for delivery status reports, tracking, and improved diagnostics. In combination with other information provided in the Delivery Status Notification (DSN) delivery report, these codes facilitate media and language independent rendering of message delivery status.

- These codes are documented in RFC 3463

Status Code Structure

This document defines a new set of status codes to report mail system conditions. These status codes are used for media and language independent status reporting. They are not intended for system specific diagnostics.

The syntax of the new status codes is defined as:

```
status-code = class "." subject "." detail
```

```
class = "2"/"4"/"5"
subject = 1*3digit
detail = 1*3digit
```

White-space characters and comments are NOT allowed within a status-code. Each numeric sub-code within the status-code MUST be expressed without leading zero digits.

Status codes consist of three numerical fields separated by “.”. The first sub-code indicates whether the delivery attempt was successful. The second sub-code indicates the probable source of any delivery anomalies, and the third sub-code indicates a precise error condition.

Example: 2.1.23

The code space defined is intended to be extensible only by standards track documents. Mail system specific status codes should be mapped as close as possible to the standard status codes. Servers should send only defined, registered status codes. System specific errors and diagnostics should be carried by means other than status codes.

New subject and detail codes will be added over time. Because the number space is large, it is not intended that published status codes will ever be redefined or eliminated. Clients should preserve the extensibility of the code space by reporting the general error described in the subject sub-code when the specific detail is unrecognized.

Status Codes

Error Code	Meaning	Notes

1.0.1	Cannot open connection	Typically your SMTP server or email program is unable to even start an SMTP session. Typical replies will be “SMTP Error 101, Error opening connection” or “SMTP Error 101, cannot open SMTP stream”. All SMTP Error 101 errors usually point to a configuration problem, such as an incorrectly spelt SMTP server, or an IP address that does not exist, or an SMTP port that does not exist or which the recipient will not accept SMTP connections on, or some other process is already using the default SMTP port, port 25.
1.1.1	Connection refused	Typically from Linux based email systems such as SquirrelMail and Mailman. The message will usually go like this : “Connection refused, 111 Can’t open SMTP stream”. All SMTP Error 111 errors usually point to an inability of your server to communicate with the remote SMTP server (either the recipient’s SMTP server or your ISP’s SMTP server) or to a Linux/SMTP software configuration problem, typically /etc/hosts not being world readable, or a newly installed or reconfigured firewall preventing connection to the remote SMTP server, or incorrect hostnames and/or domains (e.g. does your sending hostname match your IP address in a reverse lookup?), or exim not running. Telnet and logs should help you home in on the problem.
Status Code 2.X.X - Success Messages		
2.1.1	System Status message or System Help Reply	SMTP status 211 prefaces a message about the Mail Server status or a System Help reply to the user requesting help information. You might for example issue a command to the mail server to display a list of commands you can use and the server replies with an SMTP Reply 211 followed by the list you requested.
2.1.4	Help Reply message	SMTP status 214 is usually in reply to the “HELP” command.It displays information about the server, usually a URL to the FAQ page of the SMTP software running on the server. As a result this “error” is normally called a reply, as in SMTP Reply 214.
2.2.0	<Server Name> service is running	This is normally the first message you will get back from the server. It means the mail service is running (ie. your mail server is running). It will normally contain a welcome message and/or the title of the SMTP software and, sometimes, the version number of the mail server software.SMTP Reply 220 is effectively a “Hi There, I have just this second finished starting up – I am ready to go and at your command” informational message.
2.2.1	The domain service is closing the transmission channel	The server is ending the mail session – it is closing the conversation with the ISP as it has no more mail to send in this sending session. SMTP Status 221 is often misconstrued as an error condition, when it is in fact nothing of the sort. The mail server is simply telling you that it has processed everything it was given in this particular session, and it is now going back into waiting mode. Because SMTP status 221 is often misinterpreted, with some mail servers the Network Administrators have changed the default text of SMTP Reply 221 to something more meaningful and less alarming. For example, a typical SMTP reply 221 might say “221 Goodbye” or “221 Closing connection”, or the most irritating one we’ve seen “221 Bye”, Arrrgghh–can you blame anyone for thinking there might be a problem? Of course not! So some Network Administrators are these days being quite imaginative by changing the default text of SMTP reply 221 to more user friendly messages like : “221 Thank you for your business”(I love that one!),or “221 All messages processed successfully in this session, SMTP connection is closing”.
2.1.4	Help Reply message	SMTP status 214 is usually in reply to the “HELP” command. It displays information about the server, usually a URL to the FAQ page of the SMTP software running on the server. As a result this “error” is normally called a reply, as in SMTP Reply 2.1.4.

2.2.0	<Server Name> service is running	This is normally the first message you will get back from the server. It means the mail service is running (ie. your mail server is running). It will normally contain a welcome message and/or the title of the SMTP software and, sometimes, the version number of the mail server software. SMTP Reply 220 is effectively a “Hi There, I have just this second finished starting up – I am ready to go and at your command” informational message.
2.2.1	The domain service is closing the transmission channel	The server is ending the mail session – it is closing the conversation with the ISP as it has no more mail to send in this sending session. SMTP Status 221 is often misconstrued as an error condition, when it is in fact nothing of the sort. The mail server is simply telling you that it has processed everything it was given in this particular session, and it is now going back into waiting mode. Because SMTP status 221 is often misinterpreted, with some mail servers the Network Administrators have changed the default text of SMTP Reply 221 to something more meaningful and less alarming. For example, a typical SMTP reply 221 might say “221 Goodbye” or “221 Closing connection”, or the most irritating one we’ve seen “221 Bye”, Arrrgghh – can you blame anyone for thinking there might be a problem ? Of course not ! So some Network Administrators are these days being quite imaginative by changing the default text of SMTP reply 221 to more user friendly messages like: “221 Thank you for your business” (I love that one!), or “221 All messages processed successfully in this session, SMTP connection is closing”.
2.5.0	Requested mail action OK completed	The mail server has successfully delivered the message! This is the best SMTP reply (250) to receive - your message has been accepted and transmitted OK ! :) Yippee. 250 is effectively a status code rather than an error code – there is no such thing as an SMTP error 250.
2.5.1	User not local will forward	
2.5.2	Cannot VRFY (verify) the user – the server will accept the message and attempt to deliver it	The user account appears to be valid but could not be verified, however the server will try to deliver the message. There are sometimes circumstances where an email address appears to be valid but cannot be verified as definitely valid during the SMTP session between the sending server (your server) and the next server to accept your message. This can happen for example in very large corporation where the first email receiving server might only be an email exchanger server, a gateway server to the eventual server which holds the user mailboxes and which can verify if the intended recipient exists in that organization. When this happens the gateway server will reply with an SMTP Error 252 telling your sending server that it cannot verify the user part of the email address, that the domain part is OK, and that it will forward your email to a server which can do the checking and eventually deliver to the user mailbox if it exists.
Status Code 3.X.X - Informational		
3.5.4	Start mail input end with <CRLF>.<CRLF>, or, as a less cryptic description – “FROM and TO information received, now please provide message body and mark its end with <CRLF>.<CRLF>”	This is normally in response to the DATA command. The server has received the From and To information and is now asking for the “Message Body”, the main part of the message which should be ended by two blank lines separated by a dot (period). Therefore, on receiving an SMTP Reply 354 the sending server should send the body of the message to the receiving server and indicate the end of the message body with <CRLF>.<CRLF> (note the full stop between the two Carriage_Return-Line_Feed’s).
Status Code 4.X.X - Persistent Transient Failure		

4.2.0	Timeout communication problem encountered during transmission. This is a Novell GroupWise SMTP error	In our experience only Novell GroupWise servers use this error (we use GroupWise!). You will get a GroupWise GWIA (GroupWise Internet Agent) 420 TCP Write Error or 420 TCP Read Error if there are communication problems during transmission of the actual message after the sending and receiving servers have actually connected. A small number of 420 SMTP errors is normal as occasional peaks of Internet usage may delay the transmission of an email with attachment so much that a timeout occurs. When a timeout occurs on a GWIA send, the message is queued up in the <Domain>\WPGATE\DEFER directory for processing at a later time (as defined in ConsoleOne or GWIA.CFG). If you experience 420 errors only with specific recipient then it is quite likely that the recipient's antispam firewall does not like your server, your server's external IP address, or that your server's HELO command uses an outbound identification that does not match your server's external IP address (check that your sending domain's DNS is set up correctly). In an ideal world a well behaved recipient server should really be issuing your GroupWise server with a 554 error rather than timing out and causing the GroupWise GWIA to fault with a 420 error. If you experience too many 420 errors with all email communications, then you have a physical communication problem somewhere. This could be your server's network card, the network point that your server is plugged into, your switch(es), your router(s), your firewall, or your Internet line – problems caused by routers with different MTU sizes is a classic issue. Unless the logs of all those various problem points can give you an instant answer, the only way you will get to the bottom of the problem is to use a packet tracing and inspection program like Ethereal or Wireshark, its successor, if you're running GroupWise on a Windows or Linux server; on NetWare your only choice is PacketScan which you can get here http://support.novell.com/docs/Readmes/InfoDocument/2967287.html. In the final analysis, if the tracing of packets, and the changing of hardware does not help then do not discount a slightly faulty hard disk being the cause of all your problems (even if your RAID controller or your hard disk testing software does not detect any problem!).
4.2.1	The SMTP service/server you use has a limit on the number of concurrent SMTP streams your server can use	The Mail transfer service is unavailable because of a transient event. SMTP reply 421 can be caused by many things but generally indicates that the mail server which returns this status code is currently unavailable but may be available later. For example, the server administrator may have stopped the mail service to troubleshoot a problem, or the mail server is right in the middle of rebooting, or the mail server is currently processing too many incoming messages or incoming requests, etc... Note : "Mail Server" in this case can be any of the mail servers on the message's route – the sending server (your server), the ISP SMTP server, or the recipient's mail server. Clearly, if you repeatedly receive an SMTP status 421 then the problem is no longer of a transient nature and you need to investigate or inform the relevant network administrator, ISP tech support, or the recipient. SMTP Response 421 can also be received as a result of your message server sending an email where the total number of TO, CC, and BCC users results in a number of simultaneous SMTP connections that is in excess of the number of connections your ISP or SMTP service allows. A typical error message for this situation would be : "421 Too many concurrent SMTP connections from this IP address; please try again later". Typically, when this happens your server will have sent some of the messages (note that for all servers, each email sent by a user always gets broken down into individual separate emails to each of the recipients in the TO, CC, and BC fields), and will automatically retry a little later to send the remaining messages.

4.2.2	The recipient's mailbox is over its storage limit (OR) The size of the message exceeds the recipient's size limits for incoming email	Either the recipient's mailbox is over its storage limit or the message delivery directory (folder) on the recipient's mail server is currently over a size limit imposed by the Network Administrator (e.g. possibly as a result of the mail server having been down for some time, having been repaired, and currently in the process of collecting thousands of queued up messages). However, SMTP response 422 can also be received if the email being sent is larger than the incoming emails size limit in operation at the recipient's mail server (particularly when that recipient's mail server is Exchange Server).
4.3.1	The recipient's mail server is experiencing a Disk Full condition	The recipient's mail server is experiencing a Disk Full error condition, or an Out of Memory (too many file handles) error condition (Microsoft Exchange).
4.3.2	The recipient's Exchange Server incoming mail queue has been stopped	This is an SMTP status response specific to Microsoft Exchange Server. It indicates that the recipient's mail queue on their Exchange Server has been stopped (frozen), probably while the Network Administrator troubleshoots some problem.
4.4.1	The recipient's server is not responding	This is an error emanating from your server indicating that the recipient's server is not responding. Your server will automatically try again a number of times – how many depends on how your server has been configured.
4.4.2	The connection was dropped during transmission	Your server started delivering the message but the connection was broken during transmission. This may be an unusual transient error – however, if it keeps happening you should investigate possible problems with your server's network card, your Internet routers, processes hogging the resources of your server, and anything else which could result in a network connection being broken.
4.4.6	The maximum hop count was exceeded for the message	The maximum hop count was exceeded for your message. The most likely cause of this error status code is that your message is looping internally on your server, internally between two of your organisation's servers, or, sometimes, looping between your server and the recipient's server.
4.4.7	Your outgoing message timed out.	Your outgoing message timed out because of problems with the receiving server who objected to your message. Typically there is a problem with the message header (such as too many recipients, in most cases, or a protocol timeout between the two servers).
4.4.9	Routing error	This is a Microsoft Exchange Server specific error code. As per Microsoft's documentation this error code is returned when either of the following conditions occurs: an SMTP connector is configured to use DNS without a smart host and also uses a non-SMTP address space (e.g. X.400), or A message was sent to a recipient who was identified as a member of a routing group that was deleted.

4.5.0	Requested action was not taken – The mailbox was unavailable at the remote end. A secondary SMTP error code may follow “450” to refine the reason for the failure to transmit the message, e.g. “SMTP Error 450”.	The server could not access the mailbox to deliver the message. This could be caused by a process on the remote server tidying up the mailbox, or the remote mailbox could be corrupt, or the remote mailbox may be stored on another server which is currently offline, or the network connection went down while sending, or the remote mail server does not want to accept mail from your server for some reason (IP address, blacklisting, etc..). In general SMTP Error 450 is a transient error at the remote end (the destination), or at one of the routers or servers en route to the remote end, and should induce your mail server to retry after it’s preset retry interval. Example of an SMTP Error 450 reply message: “450 Please try again later”, or a classic Novell GroupWise 450 status message: “The message that you sent has been delayed. The reason given for the delay: 450 Host down (relay.clara.net)”. SMTP Error 450 is often followed by a second SMTP error code to refine the reason for the email not reaching its destination. For example: “SMTP Error 450 5.2.3 Msg Size greater than allowed by Remote Host”. When that is the case and If the error message is not as clearly worded as in this example, then simply search this document for the secondary error code. In this case searching this document for SMTP Error 523 or SMTP Error 5.2.3 would yield an explanation identical to the wording above.
4.5.1	Requested action aborted – Local error in processing. (OR) Requested action delayed – Local problem (OR) <IP_Address> has recently sent spam	The action has been aborted by the ISP’s server. “Local” (Local Problem, Local Error) refers to the next server that your message will go through after leaving your server, typically your ISP’s server, or the SMTP relaying service you are using, or, if your mail server is sending directly to the destinations, the destination mail server. This error is usually due to overloading at your ISP or your SMTP relaying service from [temporarily] too many messages or some other similar transient failure. Typically some [hopefully] temporary event prevents the successful sending of the message. The next attempt to send by your server may prove successful. If this error keeps occurring to the point that it has effectively lost its transient nature and has become... frequent (!!), then the problem is at your end and you should check your own mail server (if you email out of a corporate network), communications on your side (router, server network card), or inform your ISP if your mail server relays through your ISP or if you are a home user emailing out through Outlook, Outlook Express, Windows Mail, or similar email program. Examples of typical SMTP Error 451 return messages: “SMTP error 451 Unable to complete command, DNS not available or timed out” or “451 Domain of sender address does not resolve” or “451 Error getting LDAP results in map”, or “451 ” 4.7.1 Greylisting in action, please come back in 00:02:00 [minutes]” or “The message that you sent has been delayed. The reason given for the delay : 451 Temporary local problem - please try later.”. With the original SMTP standards having been invented before spam became the scourge of the Internet, there are no SMTP error codes dedicated to anti-spam errors. As a result, SMTP Error 451 is now increasingly also used to indicate that a message has been rejected by the remote server because of anti-spam measures. A typical error might be, for example: “SMTP error from remote mail server after end of data, host <host_address>: 451 <ip_address> has recently sent spam. If you are not a spammer, please try later.”. If all anti-spam related SMTP 451 errors are as descriptive as the one above, then the error itself will tell you what you need to do. As a general rule, however, you will most times need to take some measures to have either your server, or your ISP’s server, taken off some Internet blacklist used by the recipient.

4.5.2	Requested action not taken – Insufficient storage.	The ISP server's disk system has run out of storage space, so the action had to be cancelled. Unless you are with an ISP which is so slack that they have not implemented Disk Full Alerts, this error usually indicates that your ISP's mail server is overloaded from too many messages. This can happen even to the best ISPs when, for example, there have been problems and none of the ISP's customers could send mail; as soon as the problems are fixed there is almost always a situation where thousands of users and organizations are trying to send mail all at the same time, and those numbers can occasionally result in the ISP's mail servers' hard disks temporarily filling up, with SMTP Error 452 being the result. The next attempt to send by your server may prove successful.
4.6.5	Code Page unavailable on the recipient server	This is an Exchange Server-specific error code. This error is returned by the recipient's server if the incoming email specifies a Code Page that is not installed on the recipient's server, normally because not all language files were installed on the server during either the installation of Windows or of Exchange Server.
4.7.1	This is a local error with the sending server and is often followed with "Please try again later"	This is always a local error with your own mail server. SMTP Error 471 (or 4.7.1) is usually tagged onto a primary SMTP error code, for example "SMTP Error 450 4.7.1", or "SMTP Error 451 4.7.1", or "SMTP Error 550 4.7.1"; example: "451 4.7.1 Greylisting in action, please come back in 00:02:00 [minutes]". In all the cases that we have seen SMTP Error 471 is usually caused by anti-spam or virus scanning software on your server (the sending server) getting into problems through a bug in the software, or because of a bad automatic update from the antivirus/anti-spam manufacturer, because of lack of memory on your server, or because of hard disk problems.
Status Code 5.X.X - Errors		
5.0.0	Syntax error command not recognized.	SMTP Error 500 : The last command sent by your server was not recognized as a valid SMTP or ESMTP command, or is not formatted in the way the server expected. This includes situations where the command is too long. Note that commands that are recognized, but not implemented, are handled by different status messages (see 502 and 504). Note: A "500 unrecognized command" server response is often a case of antivirus software and/or firewall interfering with incoming and/or outgoing SMTP communications. Read your antivirus / firewall software documentation thoroughly to solve the problem. Examples of SMTP Error 500 error messages: SMTP Permanent Error: 500 Access Denied By Port Access" or "SMTP Error 500 Line too long.
5.0.1	Syntax error in parameters or arguments (e.g. invalid email address) Can sometimes also be indicative of communication problems.	The command was correct and recognised, but the parameters (the arguments, e.g. email address) were not valid. For example, the following email address will definitely give an SMTP Error 501 with most mail servers, happy_larry@hotmail.com, as "\" is not allowed in email addresses, which makes this email address invalid. In the vast majority of cases SMTP Error 501 is caused by invalid email addresses, an invalid domain name recipient, or a Unix / Linux SEND MAIL command which does not follow the established standards. For example, a typical return error message might be: "<remote-server-ip-address> does not like recipient. Remote host said: 501 Invalid Address". In cases where the error is not caused by an invalid email address, or by the failure to assign a valid email address to the mandatory "From" property, an SMTP Error 501, particularly if repeated, can be indicative of communications problems, such as a noisy line, intermittent drops in network connections, etc…
5.0.2	Command not implemented	The command or function issued by your mail server is valid but has not been activated (typically, it is not supported on this particular server).

5.0.3	Bad sequence of commands. (OR) This mail server requires authentication.	In the original standards SMTP Status 503 indicates that the commands have been sent in the wrong order, for example your mail server has sent the “Hello” command before sending the “Mail” command. This can often be caused by a drop in network connection just as your server was sending a command, resulting in the ISP’s server not receiving it and consequently not understanding the command that followed it. SMTP Reply Code 503 is nowadays more often an indicator that the SMTP server you are trying to use requires authentication and you tried to send a message without authentication (username + password). This SMTP Error 503 is permanent in that the SMTP server will not log any errors in its log and it will not retry – you will have to resend the email using authentication. Example of such an error : “SMTP Error (state 13): 503 This mail server requires authentication when attempting to send to a non-local e-mail address. Please check your mail client settings or contact your administrator to verify that the domain or address is defined for this server”.
5.0.4	Command parameter not implemented.	The command and parameter are both valid, but the parameter is not implemented on the ISP server, or an additional parameter or action is missing. For example, an often encountered SMTP Error 504 is : “504 Need to authenticate first”
5.1.0	Bad Email Address	Bad email address. This status code is generated by the sender’s local mail server. If the email was addressed internally, then it means that the addressee, as written in the email’s TO, CC, or BCC fields, does not exist in your organization’s email system. If the email was addressed externally, then the recipient’s email address was misspelt.
5.1.1	Bad Email Address	Bad email address. This error is similar to error 510 and as with error 510, this status code is generated by the sender’s local mail server. If the email was addressed internally, then it means that the addressee, as written in the email’s TO, CC, or BCC fields, does not exist in your organization’s email system. If the email was addressed externally, then the recipient’s email address was misspelt.
5.1.2	The host server for the recipient’s domain name cannot be found (DNS error)	This SMTP reply code is received when one of the servers on the way to the destination is unable to resolve the domain name of a recipient email address. Said differently : one of the servers on the way to the destination, including your server or your ISP, has a DNS problem or, possibly correctly, does not like one of the email addresses in the message’s TO, CC, and BCC fields. The first check you should perform to resolve a 5.1.2 reply code is to check all the recipient email addresses for incorrect domain names (misspelt domain names, or, maybe, totally non-existent domain names) – remember, error code 512 is very specifically an error with the domain name of one of the recipient email addresses. You can call the recipient(s) or use the WHOIS tool of The Ultimate Troubleshooter. If all the recipient email addresses check out as regards the domain part of the email addresses, then one of the servers on the way to the recipient(s) has DNS problems – usually this will be one of the first 2 servers in the chain, your own mail server (or your network) or your ISP’s mail server. Examples of typical SMTP error 512 messages : “5.1.2 - Bad destination host 'DNS Hard Error looking up domain”, or “SMTP Error 550 5.1.2 Host unknown – host cannot be found”, or how about this fantastically informative error message “5.1.2 The message could not be delivered because the recipient's destination email system is unknown or invalid. Please check the address and try again, or contact your system administrator to verify connectivity to the email system of the recipient.”.

5.1.3	Address type is incorrect (most mail servers) (OR) Relaying denied or Authentication required (a small percentage of mail servers)	This status code (from the sender's mail server) is usually symptomatic, in an Exchange + Outlook environment, of the user's Outlook Contacts having been imported from another system or PST and where some of the addresses are not defined correctly. Or, in any environment it is simply that the end-user simply did enter the email address completely wrongly, such as copying it from a website and not replacing "at" with "@", e.g. : John.DoeatUCLA.edu (which should have been John.Doe@UCLA.edu), or John.Doe@UCLA.edu" (", quotes, is not allowed in email addresses and is often included in error as a result of copying and pasting an email from somewhere). The user should check all the recipient addresses in the email, including those that were inserted from Contacts.
5.2.3	The Recipient's mailbox cannot receive messages this big	This error will be received when the total size of the message you have sent (ie: message + all of its attachments) exceeds the size limits on the Recipient's server. Many companies implement the good practice of configuring their servers with limits on the size of emails they can receive to prevent their systems running out of space as a result of a spam attack where the spam emails contain large attachments, or as a result of valid but not very technically savvy senders sending enormous scans (through not knowing that scanning at 1200dpi rather than the usually perfectly usable and acceptable 300dpi, will create humongous attachments). Check the size of the email you sent, and, specifically, the size of the attachments you included, and consider splitting your email into smaller emails. If that does not work, check with the Recipient the maximum size of email they can receive, and if that is still prohibitive then consider FTP arrangements between you and the recipient.
5.3.0	Authentication is required (OR) Your server has been blacklisted by the recipient's server (OR) The recipient's mailbox does not exist	
5.4.1	Recipient Address Rejected – Access denied (typically by the recipient's antispam program / appliance)	
5.5.0	Requested actions not taken as the mailbox is unavailable. 550 is always a problem external to your own mail server. Usually it is at the recipient's end, but it could also originate from inside your own "walls" through being caused, for example, by an appliance which scans your outgoing emails once they've left your server.	
5.5.1	User not local or invalid address – Relay denied.	
5.5.2	Requested mail actions aborted – Exceeded storage allocation. or Size of the incoming message exceeds the incoming size limit.	
5.5.3	Requested action not taken – Mailbox name invalid. (OR) You are attempting to send emails through a specific ISP's SMTP server without authentication and without being connected to the Internet through that ISP's service. (OR) You are sending from an Exchange server configured to send via DNS and you do not have a public reverse DNS record pointing back to your Exchange server.	
5.5.4	Transaction failed. Nowadays SMTP status 554 is in most cases returned when the recipient server believes your email is spam or your IP address or ISP server has been blacklisted on one or more Internet blacklists. With Yahoo, on the other hand, this usually means the email address does not exist or has been disabled. (OR) With IBM's Lotus Domino this is either a Domino bug or a Disk Full error	
5.7.1	I have been told not to work with you!!!	

Collected Status Codes	
X.1.0	Other address status
X.1.1	Bad destination mailbox address
X.1.2	Bad destination system address
X.1.3	Bad destination mailbox address syntax
X.1.4	Destination mailbox address ambiguous

X.1.5	Destination mailbox address valid
X.1.6	Mailbox has moved
X.1.7	Bad sender's mailbox address syntax
X.1.8	Bad sender's system address
X.2.0	Other or undefined mailbox status
X.2.1	Mailbox disabled, not accepting messages
X.2.2	Mailbox full
X.2.3	Message length exceeds administrative limit
X.2.4	Mailing list expansion problem
X.3.0	Other or undefined mail system status
X.3.1	Mail system full
X.3.2	System not accepting network messages
X.3.3	System not capable of selected features
X.3.4	Message too big for system
X.4.0	Other or undefined network or routing status
X.4.1	No answer from host
X.4.2	Bad connection
X.4.3	Routing server failure
X.4.4	Unable to route
X.4.5	Network congestion
X.4.6	Routing loop detected
X.4.7	Delivery time expired
X.5.0	Other or undefined protocol status
X.5.1	Invalid command
X.5.2	Syntax error
X.5.3	Too many recipients
X.5.4	Invalid command arguments
X.5.5	Wrong protocol version
X.6.0	Other or undefined media error
X.6.1	Media not supported
X.6.2	Conversion required and prohibited
X.6.3	Conversion required but not supported
X.6.4	Conversion with loss performed
X.6.5	Conversion failed
X.7.0	Other or undefined security status
X.7.1	Delivery not authorized, message refused
X.7.2	Mailing list expansion prohibited
X.7.3	Security conversion required but not possible
X.7.4	Security features not supported
X.7.5	Cryptographic failure
X.7.6	Cryptographic algorithm not supported
X.7.7	Message integrity failure

From:
https://wiki.plecko.hr/ - **Eureka Moment**

Permanent link:
https://wiki.plecko.hr/doku.php?id=linux:networking:smtp_response_codes

Last update: **2019/10/31 09:05**