Click Here

Simple Mail Transfer Protocol (SMTP) is an application layer protocol used for exchanging email messages between servers. It is essential in the email communication process and operates at the application layer of the TCP/IP stack.To send an email, the client opens a TCP connection to the SMTP server. The server, which is always listening on port 25, initiates the connection as soon as it detects a client. Once the TCP connection is established, the client sends the email across the connection.SMTPTypes of SMTP ProtocolThe SMTP model supports two types of email delivery methods: end-to-end and store-and-forward.End-to-end delivery is used between organizations. In this method, the email is sent directly from the sender's SMTP client to the recipient's SMTP server without passing through intermediate servers.Store-and-forward is used within organizations that have TCP/IP and SMTP-based networks. In this method, the email may pass through several intermediate servers (Message Transfer Agents, or MTAs) before reaching the recipient.With end-to-end delivery, the SMTP client waits until the email is successfully copied to the recipient's SMTP server before sending it. This is different from the store-and-forward method, where the email might stop at multiple intermediate servers before reaching its destination. In store-and-forward systems, the sender is notified as soon as the email reaches the first server, not the final destination.SMTPBefore diving deeper into the Model of SMTP System, it's important to understand how SMTP is leveraged by service providers like SMTP.com in the real-world scenario.SMTP.com is a platform that caters to all your transaction, email relay and email delivery needs at a very affordable price. With decades of experience, SMTP.com is regarded as the most trusted sender in the industry by ISPs. SMTP.com had been trusted by over 100,000 customers over the years. SMTP.com is extremely intuitive and easy to set up. It can be integrated seamlessly into your current business system. If you need to migrate from another provider, SMTP.com make it effortless.FeaturesDedicated IPEmail API: Integrating SMTP.com with your business can be easy with the email API feature. They have complete API documentation on their website that can help you integrate your business in just 5 minutes.24x7 Customer Support: The round-the-clock support is one of the best features of SMTP.com. Support is available both on the website and also for paid customers. 24x7, all human support is available for all customers across all plans. No third party is involved and solutions are provided fast for easy implementation. Online chat support is also available for those who are looking for more information about SMTP.comHigh Volume Sending Solutions: This newly launched feature is great for those businesses who want to send more than 250 million emails a month. Customized quotations and solutions are available.Reputation Defender: This is an add-on feature that helps clean up your email lists. It doesnt need any integration but actively monitors your lists and provides a report.PricingSMTP.com offers affordable delivery services and caters to all kinds of businesses. Their plans range from $25 to $500 and above. The best part about this platform is that all the features are available in all the plans. The prices change only based on the volume of emails sent monthly. Even with the lowest price pack, users can get access to 24x7 customer support and all the SMTP tools. The Reputation Defender for list cleaning is an add-on feature available for all users.Model of SMTP SystemSMTP ModelIn the SMTP model user deals with the user agent (UA), for example, Microsoft Outlook, Netscape, Mozilla, etc. To exchange the mail using TCP, MTA is used. The user sending the mail doesn't have to deal with MTA as it is the responsibility of the system admin to set up a local MTA. The MTA maintains a small queue of mail so that it can schedule repeat delivery of mail in case the receiver is not available. The MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.Components of SMTPMail User Agent (MUA): It is a computer application that helps you in sending and retrieving mail. It is responsible for creating email messages for transfer to the mail transfer agent(MTA).Mail Submission Agent (MSA): It is a computer program that receives mail from a Mail User Agent(MUA) and interacts with the Mail Transfer Agent(MTA) for the transfer of the mail.Mail Transfer Agent (MTA): It is software that has the work to transfer mail from one system to another with the help of SMTP.Mail Delivery Agent (MDA): A mail Delivery agent or Local Delivery Agent is basically a system that helps in the delivery of mail to the local system.How does SMTP Work?SMTP1. Sending Email:When a user wants to send an email, they use a User Agent (UA), like Outlook or Gmail.The email is handed over to the MTA, which is responsible for transferring the email to the recipients mail server.2. SMTP Client and Server:Sender-SMTP (Client): The email senders MTA initiates the connection to the recipients MTA (Receiver-SMTP).Receiver-SMTP (Server): The receiving MTA listens for incoming connections and receives the email from the sender-SMTP.This communication happens over TCP port 25.3. Relays and Gateways:Relays: In some cases, the email may pass through several intermediate MTAs before reaching the destination server. These MTAs act as relays.Gateways: If the sending and receiving systems use different email protocols (e.g., SMTP and non-SMTP), an email gateway can convert the email to the appropriate format for delivery.4. Email Delivery:The senders MTA sends the email to the receivers MTA, either directly or through relays.The MTA uses the SMTP protocol to transfer the message. Once its delivered to the destination MTA, the email is placed in the recipients mailbox.The recipients User Agent (UA) can then download the email.SMTP EnvelopePurposeThe SMTP envelope contains information thatguides email deliverybetween servers.It isdistinct from the email headers and bodyand isnot visible to the email recipient.Contents of the SMTP EnvelopeSender Address: Specifies where the email originates.Recipient Addresses: Indicates where the email should be delivered.Routing Information: Helps servers determine the path for email delivery.Comparison to Regular MailThink of the SMTP envelope as theaddress on a physical envelopefor regular mail.Just like an envelope guides postal delivery, the SMTP envelope directs email servers on where to send the email.SMTP CommandsS.No.KeyworCommand formDescriptionUsage1.HELOHELOIt provides the identification of the sender i.e. the host name.Mandatory2.MAILMAILFROM : It specifies the originator of the mail.Mandatory3.RCPTRCPTTO : It specifies the recipient of mail.Mandatory4.DATADATAIt specifies the beginning of the mail.Mandatory5.QUITQUITIt closes the TCP connection.Mandatory6.RSETRSETIt aborts the current mail transaction but the TCP connection remains open.Highly recommended7.VRFYVRFYIt is use to confirm or verify the user name.Highly recommended8.NOOPNOOPNo operationHighly recommended9.TURNTURNIt reverses the role of sender and receiver.Seldom used10.EXPNEXPNIt specifies the mailing list to be expanded.Seldom used11.HELPHELPIt send some specific documentation to the system.Seldom used12.SENDSENDFROM : It send mail to the terminal.Seldom used13.SOMLSOMLFROM : It send mail to the terminal if possible; otherwise to mailbox.Seldom used14.SAMLSAMLFROM : It send mail to the terminal and mailbox.Seldom usedSMTP PortsPort 587: This is the most commonly used port for secure SMTP submission using TLS (Transport Layer Security). It is recommended for client-to-server communication, as it ensures the security of the email transmission.Port 465: Previously used for secure SMTP (SMTPS), this port is no longer considered an official standard and is generally not recommended anymore. Many email providers have moved away from port 465 in favor of port 587.Port 25: This port is traditionally used for SMTP relay between mail servers, not for email submission from clients. It is often blocked by ISPs for outgoing mail due to its frequent use for spam and malicious activities.Port 2525: Although not an official SMTP port, it is sometimes used as an alternative for SMTP submission, especially in cases where port 25 is blocked or restricted. Many email providers support this port as an alternative for secure communication.Difference Between SMTP and Extended SMTPSMTPExtended SMTPUsers were not verified in SMTP as a result of massive-scale scam emails being sent.In Extended SMTP, authentication of the sender is done. We cannot attach a Multimedia file in SMTP directly without the help of MMIE.We can directly attach Multimedia FIle in ESMTP.We cannot reduce the size of the email in SMTP.We can reduce the size of the email in Extended SMTP.SMTP clients open transmission with the command HELO.The main identification feature for ESMTP clients is to open a transmission with the command EHLO (Extended HELLO).Advantages of SMTPIf necessary, the users can have a dedicated server.It allows for bulk mailing.Low cost and wide coverage area.Offer choices for email tracking.Reliable and prompt email delivery.Disadvantages of SMTPSMTP's common port can be blocked by several firewalls.SMTP security is a bigger problem.Its simplicity restricts how useful it can be.Just 7-bit ASCII characters can be used.If a message is longer than a certain length, SMTP servers may reject the entire message.Delivering your message will typically involve additional back-and-forth processing between servers, which will delay sending and raise the likelihood that it won't be sent.SMTP vs POP vs IMAPSMTP POP IMAPStands for Simple mail transfer protocolStands for Post Office Protocol.Stands for Internet Message Access Protocol.Used for sending mail.Used for retrieving mail.Used for retrieving mail.it is pushprotocol.it is pull protocol.it is pull protocol.It work between senders mail server to receivers mail server and sender and senders mail server.It work between receiver and receivers mail server.It works between receiver and receivers mail server.It does not store mail on server it just send the mail.It download all the mail when it connected to internet.It store all mail on server and download when it get request to download.Works on TCP port number 25.Works on TCP port number 110.Works on TCP port number 143.Connection oriented protocol.Connection oriented protocol.Connection oriented protocol.It has persistence TCP connection.It has persistence TCP connection.It has persistence TCP connection.Statelessprotocol.Stateful protocol.Stateful protocol.It is in band protocol.It is in band protocol.It is in band protocol.Not used at receiver side.Used at receiver side.Used at receiver side. Share copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits. You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation . No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. Whether youre testing a new email service, diagnosing a problem between a client program and SMTP service, looking to write a script to send automated emails, or just wanting to learn more about how SMTP works, this SMTP 101 post is the first in a series designed to help you interact with open, text-based, protocols in common use within the email industry.But before we get into the how-to, lets start with the basics What is SMTP?Simple Mail Transfer Protocol (SMTP) is an internet standardforelectronic mail(email) transmission. First defined byRFC821in 1982, it was updated in 2008 withExtended SMTPadditions byRFC5321, which is the protocol in widespread use today.Although electronicmail servers and other mail transfer agentsuse SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server forrelaying. For retrieving messages, client applications usually use eitherIMAPorPOP.SMTP communication between mail servers uses TCP port 25.Mail clientson the other hand, often submit the outgoing emails to a mail server on port 587 or 465. The latter port was previously deprecated, but this changed withRFC 8314and its use is now recommended to ensure security. SMTP connections on port 25 or 587 can be secured using an extra command (STARTTLS).Although proprietary systems and [some] webmailsystemsuse their own non-standard protocols to access mail box accounts on their own mail servers, all use SMTP when sending or receiving email from outside their own systems. SourceSMTP is a plaintext protocol,so you can just type commands from your keyboard and send an email.In this posts example, we use the atmail cloud, but it is equally applicable to any SMTP service. Connecting to SMTPThe three options for connecting to SMTP (dependant on your installation) are:plaintext (or Telnet)SSLTLSLets walk through each option 1. Plaintext or TelnetThe easiest method to connect (if your SMTP server supports plaintext connections) is via the program Telnet(short for Terminal Network). If you dont have telnet installed and cant have it installed (like on your locked down production system), you might see if netcat is installed.In this example, I am using Linux, but you could equally use PuTTY on Windows.The port will typically be either port 25 or 587. (Port 465 is typically used for SSL connections.)Example:$ telnet smtp-us.atmailcloud.com 25Trying 204.145.97.24...Connected to smtp-us.atmailcloud.com.Escape character is '^]'.220 us11-011mrc - SMTP readyNow we can type commands.Now the same thing with netcat or nc if telnet isnt available:$ nc --crlf --verbose smtp-us.atmailcloud.com 25Ncat: Version 7.50 ( )Ncat: Connected to 204.145.97.22:25.220 us11-012mrc - SMTP readyquit221 ByeNcat: 6 bytes sent, 39 bytes received in 7.90 seconds.2. SSLSome people get confused between SSL and TLS.To make it clear, SSL (Secure Sockets Layer) is used to encrypt the TCP channel before any SMTP protocol is presented to the client.TLS, on the other hand, encrypts the channel during the SMTP session (i.e. it starts as plaintext but then switches to an encrypted channel).The easiest way to initiate an SSL encrypted channel is via the OpenSSL s_client command.Example:$ openssl s_client -connect smtp-us.atmailcloud.com:465 -crlf -quietdepth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2verify return:1depth=1 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = RapidSSL TLS RSA CA G1verify return:1depth=0 CN = *.atmailcloud.comverify return:1220 us11-011mrc - SMTP readyThe option -crlf just means to issue a carriage return and a line feed on enter and -quiet means not to spit out a bunch of details about the encrypted channel.Feel free to drop -quiet to view the output, or if you are keen, add -debug for even more detail. 3. TLSAs I said above, TLS (Transport Layer Security) starts after connecting with plaintext.You could start a TLS session (like my Telnet, but then you need to negotiate a binary encrypted channel with Telnet.The ports for TLS are going to be either 25 or 587 and will depend on your installation.Starting a TLS session over Telnet:$ telnet smtp-us.atmailcloud.com 25Trying 204.145.97.22...Connected to smtp-us.atmailcloud.com.Escape character is '^]'.220 us11-010mrc - SMTP readyEHLO example250-us11-010mrc.dh.atmailcloud.com Hello example [101.165.155.220]250-SIZE 52428800250-8BITMIME250-PIPELINING250-AUTH LOGIN PLAIN250-CHUNKING250-STARTTLS250 HELPSTARTTLS220 TLS go aheadYou can see that I introduced the command ehlo some-name.This just asks the SMTP server which extended options are supported.One of those returned is STARTTLS, so I executed that and at that point, the TCP connection switched to binary and I needed to negotiate an encrypted channel.The easiest way to do this is using OpenSSL s_client again, like so:$ openssl s_client -connect smtp-us.atmailcloud.com:25 -crlf -quiet -starttls smtpdepth=0 C = UK, O = Exim Developers, CN = us11-011mrc.dh.atmailcloud.comverify error:num=18:self signed certificateverify return:1depth=0 C = UK, O = Exim Developers, CN = us11-011mrc.dh.atmailcloud.comverify error:num=9:certificate is not yet validnotBefore=Sep 12 11:29:24 2018 GMTverify return:1depth=0 C = UK, O = Exim Developers, CN = us11-011mrc.dh.atmailcloud.comnotBefore=Sep 12 11:29:24 2018 GMTverify return:1250 HELPNow I issue some new commands, for example the EHLO we introduced earlier.250 HELPEHLO example250-us11-010mrc.dh.atmailcloud.com Hello example [101.165.155.220]250-SIZE 52428800250-8BITMIME250-PIPELINING250-AUTH LOGIN PLAIN250-CHUNKING250 HELPYou can see, for obvious reasons, that STARTTLS is now missing. Authenticating to SMTPSometimes you may want to authenticate to the SMTP server (eg. if it is your outbound mail server).But you may not always need to authenticate (eg. if you are connecting to an MX server of a particular domain you wont be able to authenticate).But if you do want to authenticate, this is how:You can see above, in response to the EHLO, we get the line:250-AUTH LOGIN PLAINThis means this server supports both LOGIN and PLAIN methods. Authenticating via Login MethodThe login method means we send the username and password separately as base64 encoded strings.SMTP servers tell you this by encoding the question. (Why? Not sure. Probably, just to be clever.)We issue the command AUTH LOGIN and we receive:AUTH LOGIN334 VXNlcm5hbWU6Now, if we decode that base64 string, we get:$ echo "VXNlcm5hbWU6" | openssl base64 -dUsername:The same applies for the next prompt, which is Password:.So how do you encode your username and password to send in base64?This is my preferred way:$ echo -en "" | openssl base64c29tZXVzZXJAZXhhbXBsZS5hdG1haWxjbG91ZC5jb20=$ echo -en "my^Passw0rd" | base64bXleUGFzc3cwcmQ=Now putting this all together to actually authenticate:EHLO example250-us11-011mrc.dh.atmailcloud.com Hello o [101.165.155.220]250-SIZE 52428800250-8BITMIME250-PIPELINING250-AUTH LOGIN PLAIN250-CHUNKING250 HELPAUTH LOGIN334 VXNlcm5hbWU6c29tZXVzZXJAZXhhbXBsZS5hdG1haWxjbG91ZC5jb20=334 UGFzc3dvcmQ6bXleUGFzc3cwcmQ=235 Authentication succeeded Authenticating using the Plain MethodUsing the Plain method, we provide the username and password as single base64 encoded string, separated by the NUL character.Here is how to generate the base64 on a Linux machine:$ echo -en '\\0my^Passw0rd' | openssl base64AHNvbWV1c2VyQGV4YW1wbGUuYXRtYWlsY2xvdWQuY29tAG15XlBhc3N3MHJkWe will address the leading NUL in the next section, but for basic user authentication, that is the format you need.Here is an authenticating session:AUTH PLAIN 334AHNvbWV1c2VyQGV4YW1wbGUuYXRtYWlsY2xvdWQuY29tAG15XlBhc3N3MHJk235 Authentication succeededWe are now authenticated and can issue commands as a trusted user. Special Credit: Authenticating via SASL PLAIN as an Admin UserNow, back to that leading NUL in the previous section. The SASL PLAIN, which is really the Plain method above, defines the ability to authenticate as one user but actually perform the session as if another user authenticated. The typical use case is for an administrator to authenticate as themselves, but access the service as another user.We dont use an admin password for the atmail cloud, but I do have a lab box where I have atmail on-prem running, so Ill switch to that for the purposes of this section.The format is:authcidNULauthzidNULpasswordSo generate this we can use Linux:$ echo -en '\\0admin1\0admin1234' | openssl base64dGlnZXJAemV1cy5wAGFkbWluAGFkbWluMTIzNA==Hereauth plain 334dGlnZXJAemV1cy5wAGFkbWluMQBhZG1pbjEyMzQ=235 Authentication succeeded Sending an EmailNow that were connected (possibly via SSL/TLS) and weve optionally authenticated,we can send an email.As far as the SMTP server is concerned, an email consists of three parts:Who the message is from (MAIL FROM);Who the message is to (RCPT TO); andThe message (DATA).At the SMTP layer, the message header and body are just considered the message (or more correctly, the DATA).You can only have a single MAIL FROM, but many RCPT TOs (up to the limit configured by the server administrator).Note: Some SMTP servers enforce the SMTP protocol more strictly than others. So, while in the examples below I just use the email address form as , some SMTP servers will insist on the RFC specified format of using brackets (i.e.). Please bear this in mind when you are testing.MAIL FROM: 250 OK RCPT TO: 250 Accepted Recipient RCPT TO: 250 Accepted Recipient DATA 354 Enter message, ending with "." on a line by itself From: Some User To: Some Other User Cc: Subject: HelloHello my friends..250 OK id=1g040I-0008DT-GGSo what I did above was:I issued a MAIL FROMThen a couple of RCPT TOsThen the DATAI then entered the email as I wished to sendTold the server I was finished by issuing a single . on a line by itself.The server accepted the message.A couple of points worth noting:The format of the DATA is up to you, you can include some headers and not others.The indicator of where message headers stop and the message body begins is a single blank line.There is no direct relationship between the From and To/CC fields in the DATA and the envelope MAIL FROM and RCPT TO. Basically, the envelopes need to be real and exist and the message body can be pure fantasy, this is also known as spoofing (some mail servers will re-write the DATA headers to align with the envelope, but this is not super-common practice). A Complete ExampleHere is a complete SMTP session, including some spoofing, as an example.$ openssl s_client -connect smtp-us.atmailcloud.com:25 -crlf -quiet -starttls smtp depth=0 C = UK, O = Exim Developers, CN = us11-012mrc.dh.atmailcloud.com verify error:num=18:self signed certificate verify return:1 depth=0 C = UK, O = Exim Developers, CN = us11-012mrc.dh.atmailcloud.com verify return:1 250 HELP EHLO EXAMPLE 250-us11-012mrc.dh.atmailcloud.com Hello 27-33-184-51.static.tpgi.com.au [27.33.184.51] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH LOGIN PLAIN 250-CHUNKING 250 HELP AUTH PLAIN 334 AHNvbWV1c2VyQGV4YW1wbGUuYXRtYWlsY2xvdWQuY29tAG15XlBhc3N3MHJk 235 Authentication succeeded MAIL FROM: 250 OK RCPT TO: 250 Accepted Recipient DATA 354 Enter message, ending with "." on a line by itself From: To: Subject: Hello everyone! A little spoofed message from someone pretending to be the I hope you enjoyed this blog post..250 OK id=1g0eWC-0003vH-SuQUIT221 Bye Find this SMTP post useful?Were taking ideas for future email-related 101 posts. If youd like to make a request, we invite you to drop us a line here.Meanwhile, we invite you to check out some of our other how-to posts: New to atmail?If email is not your core business and youd like someone else to worry about SMTP, we can help.With 20 years of global, white label, email expertiseserving telecommunications and hosting providers across every continent,you can trust us to deliver white label, email solutions that are stable, secure and scalable.We power 170 million mailboxes and offer user-friendly,cloud hosted emailwith 99.99% uptime and your choice of US or (GDPR compliant) EU data centres.Or, if you want to stay in-house, we offeron-premises webmail and/or mail server options.Talk to us today. On January 11, 2025 By Zakhar Yung Learn everything you need to know about SMTP server. Find out what it is, how it works, what its types are, and much more. On February 17, 2023 By Piotr Malek There are various ports available for SMTP transmission but not all should be used these days. Learn what works and what doesnt. Interested in learning about how SMTP works?While sending and receiving emails through an email client seems simple, theres a lot happening behind the scenes to deliver an email from the sender to the receiver.The entire process is carried out via various email protocols, and many email systems use SMTP (a specific protocol) for sending emails.In this article, Ill cover what SMTP is, how it works with email providers, and its differences from other email protocols.Ill also show you how to set up SMTP on your email server.This Article Contains: Lets get started.What Is SMTP?Simple Mail Transfer Protocol (SMTP) is an email protocol used to send email messages from one email account to one or more email addresses. Its part of the application layer of the TCP/IP (Transmission Control Protocol/Internet Protocol) network model.But waitwhats a protocol?An email protocol is a set of rules that help you exchange information between email accounts. While there are several different protocols in place today, SMTP is one of the most widely used outgoing email protocols.How Does SMTP Work?Lets take a quick look at how the SMTP email protocol works:Note: The following sections can be slightly technical, as understanding how SMTP works can be quite complicated. Fortunately, you dont have to know how SMTP works to use it. So if you just want to learn how to set up your own SMTP settings, click here to skip this section and jump to my walk-through guide.However, for those of you interested in learning what goes on behind the scenes every time you click Send, read on:A. The Fundamentals of SMTPHeres all the information you need to know about the Simple Mail Transfer Protocol:1. How Does SMTP Send Email?When a user wants to send an email, the email client (an email application like Gmail, Yahoo, or Outlook) opens an SMTP connection to the domains SMTP server. It finds the domains SMTP server by doing an MX record lookup on the domain.Once the SMTP connection (which uses a TCP connection) is established with the mail server, an SMTP session begins.During this session, the SMTP client communicates with the outgoing server using various SMTP commands, like HELO. An SMTP command consists of alphabetic characters, and the server responds with numeric codes.During the TCP connection, the mail client transfers the following information to the server:Senders email addressRecipients email addressMessage body and attachmentsThen, the Mail Transfer Agent (also known as a Message Transfer Agent) checks to see if the email addresses of the sender and receiver originate from the same domain. If they do, the email is sent immediately to the receivers inbox, and the email can be retrieved via POP3 or IMAP.However, if the two domains are different, the server will communicate with the Domain Name System (DNS) and obtain the receiving domains MX record via a DNS lookup. The MX record points to the receivers mail server. Then, the senders server connects to the receivers server and transfers the mail.The receiving SMTP server verifies the incoming mail. Once the domain and username are recognized, the email message is forwarded to the recipients POP3 mail server or IMAP server.2. The Multiple Ways That SMTP Works:The Simple Mail Transfer Protocol model consists of two types:Store-and-forwardEnd-to-endThe store-and-forward method is used to communicate with email addresses within an organization, such as coworkers or students whose email addresses are part of the same domain (e.g., @company.com or @school.edu).The end-to-end method is used for outgoing messages to addresses based on a mail server outside the organization.While this means most of the emails you write are sent using the end-to-end method, theres one particular type of business email that benefits from this:Using the end-to-end method with SMTP servers really helps if your business regularly sends transactional emails. A transactional email is an email that automatically sent when a user action (e.g., account creation, feedback/comment, purchase receipt, download, etc.) happens on your website.3. What Type of Emails Can You Send with SMTP?SMTP can only transfer text it cant send images or any other attachments. However, you can easily use the SMTP protocol to send emails with attachments.How?SMTP uses an add-on protocol known as Multipurpose Internet Mail Extension, or MIME, to encode all non-text data into text format.All your images and other attachments will be converted to text before being sent through SMTP. And once they arrive at their destination, they are converted back into their original format.B. MTA vs. SMTPEarly on in this article, I mentioned that the MTA plays a part in sending email through SMTP.So how does an MTA differ from an SMTP server?A Mail Transfer Agent (also known as a mail relay) is software thats installed on an SMTP server. It communicates with the Mail Submission Agent (MSA) to obtain emails that have been sent by a Mail User Agent (MUA), which is the mail client. (Gmail and Outlook are examples of mail clients.)MTAs then pass these emails on to other MTAs if the recipient is not a local recipient (i.e., not part of the same domain). Finally, an MTA delivers the email to a Mail Delivery Agent (MDA), which sends the email to the receiving email message client (User Agent).C. What Is an SMTP Relay?Its important to note that the SMTP Relay Server and SMTP Host dont mean the same thing.An SMTP Relay is the process of transferring emails between SMTP servers. An SMTP Relay consists of the MTA and the MDA, and usually occurs when the email addresses of the sender and receiver are from different domains.Using an SMTP Relay service guarantees high rates of email deliverability ensuring that your outgoing messages arrive in the recipients inbox.The term SMTP Host only refers to the server that the email is sent through, while the SMTP relay is carried out on that server.How Does SMTP Differ from Other Email Protocols?Remember, SMTP isnt the only email protocol out there.Two other popular email protocols that are used around the world are POP and IMAP.But what do these email protocols do, and how do they differ from SMTP?Lets take a look at what POP and IMAP are, and how SMTP differs from both of them:1. What Is POP?The Post Office Protocol (POP) is used to receive incoming emails. The latest version of this email protocol is known as POP3.POP3 is the right email protocol if you use a single computer to check your email. As POP downloads all your received emails and stores them locally, its a great way to check your emails even when youre offline!2. What Is IMAP?The Internet Message Access Protocol or IMAP is another email protocol thats used to receive incoming mails.IMAP is more popular than the POP receiving server since it stores all the email messages on a cloud server. This way, a user can check their emails on whatever device they want.And since IMAP is a cloud-based electronic mail protocol, its more efficient and also faster than POP.3. SMTP vs. POP and IMAPSo how do POP and IMAP differ from SMTP?All you have to remember is that SMTP is an email protocol used for outgoing mail, while POP and IMAP are electronic mail protocols used to receive incoming emails.Why Should You Set Up an SMTP Server on GMass?Using a custom server can do wonders for your outgoing messages, especially if you send out lots of mass emails regularly.So heres a look at what GMass is and why you should set up an SMTP server (or multiple SMTP servers) on GMass:What Is GMass?GMass is a popular email outreach tool that helps people send tons of email campaigns straight from their Gmail account. Its used by employees of companies like Twitter, Uber, Google, and LinkedIn for boosting their email outreach easily.But GMass isnt just for the use of tech giants!Solopreneurs, churches, individuals, and SMBs can also use GMass to send mail to any type of audience.With GMass, you can:Send mass emails from your gmail.com inbox.Personalize your mail campaigns easily.Track how recipients are engaging with your emails.Schedule and send bulk email and follow-ups.The best part?Just download the GMass Chrome extension, and you can start sending mail campaigns instantly!How Does Setting Up SMTP in GMass Help You?While you can set up an SMTP outgoing mail server in Gmail, Outlook, AOL, or any other email message client you use, those services put limits on how many emails you can send per day.Additionally, when you use a Gmail SMTP server, your email message client can flag you as a spammer and block your email account if you send out a high number of emails at once.When you set up an SMTP account and link it to GMass, you dont have to worry about mail limits on email delivery or a blocked mail account. Since your emails pass through GMass servers, you can send tons of bulk emails to your recipients.However, if you still want to set up your SMTP server using a native email client, here are my guides on setting up: And when its time to test things and make sure theyre working perfectly, try our worlds best SMTP server testing tool!If youre an expert-level developer, you may want to look through my technical review of popular SMTP services.How to Set Up an SMTP Server on GMass (Step-by-Step Guide)I know that understanding how SMTP works can be pretty complicated. So youd probably think setting it up is like rocket science, too.But luckily, setting up an SMTP mail server in GMass super-easy!Heres a step-by-step guide on how you can set up your own SMTP server on GMass:1. Choose How You Want to Set Up Your SMTP ServerThere are three ways you can set up the SMTP server setting in GMass:A. Use the GMass SMTP ServerIf your emails are either:Non-commercial or100% organically developedYou can make a request to the GMass team to set up SMTP using in-house server.B. Set Up an SMTP Account of Your OwnIf your emails dont fit the criteria Ive mentioned above, dont worry!You can set up an SMTP account on a third-party SMTP service provider like SendGrid. Once you create an account with the service provider, just configure the SMTP settings and link it to GMass!C. Set Up a Private SMTP ServerIf you know your way around an email server, you can opt to set up a private server. But remember, youll need a lot of time and patience to set up a server on your own. (If youre an expert-level developer, you might be interested in my technical review of popular SMTP services.)2. Setting Up the SMTP Account to Work with GMassHeres how you can connect your GMass account to an SMTP account:Step 1The GMass email program will link to your server without TLS or SSL authentication. You can decide on which SMTP port number to use usually, its 25 or 2525.Note: Ensure that your Internet Service Provider (ISP) hasnt blocked the SMTP port number.Step 2Look for the track email opens and clicks feature in the SMTP service and turn it off. This is the preferred SMTP setting to avoid double-tracking your emails.Ensure that your outgoing server doesnt alter any emails that pass through it.Step 3Look for any outgoing email sending limits in your SMTP account. If theyre too low and will affect your mass emails, just turn them off.Step 4Remember to check the RETURN-PATH address being used by your email server. This is also known as an Envelope Form or a MAIL-FROM address.Most SMTP service providers use different domains in the from address and the MAIL-FROM address but some dont.So you might have to verify your domain name to avoid any errors.You may also need to change your DMARC, DKIM, and SPF records.Step 5Look for bounce notifications and turn them on. Set them to go to the From address. This will allow GMass to show you email bounce rates.3. Configuring GMass to Use the SMTP Server to Send EmailHeres how you can configure GMass to send email using your SMTP Server:Step 1If you dont have GMass, install the Chrome extension. Reload the Gmail email service on Google Chrome and make sure youre running the latest version of GMass.Then, click on Compose.Step 2Type in the To field.Step 3In the subject field, type the word set and wait for this form to load.Step 4Once the form loads, enter the SMTP server address (Server name) and other relevant SMTP credentials. If your SMTP setup needs no authentication, type noauth in the Username field and leave the password blank.Step 5Click on the red GMass button.Once you complete all of these steps, GMass will send a test email to your email inbox. If the test email works successfully, the SMTP server will be set for your email account.More Useful GMass FeaturesA streamlined SMTP setup process isnt the only reason to use GMass.Lets take a look at some other useful features that will benefit you:A. Advanced Personalization of EmailsRecipients dont engage with emails that look and feel generic.So to garner responses, youll have to send personalized emails to recipients.But manually customizing tons of emails will take forever, right?Dont worry!GMass has an arsenal of features like auto-detection and entry of first names, personalized images, text, attachments, and links. All of these can help personalize your outgoing email campaigns quickly.Want to learn the best ways to personalize the start of your email? Click here.B. Detailed Email MetricsWhenever you send email marketing campaigns through GMass, it generates a campaign report highlighting useful information about your campaign.These reports will show you metrics like the number of unique email opens, number of replies, number of unsubscribes, and more!C. Easily Schedule Email CampaignsIf you want the highest rates of engagement and replies, your emails need to reach recipients at the right time.GMass can help you schedule all your email campaigns to reach recipients at the best possible time. All you have to do is type your email in the Gmail webmail client, schedule it, and let GMass handle everything else!D. Easily Automate Your Follow-UpsMost recipients wont engage with your first email they might ignore it or forget to respond to it. So youll have to send follow-up emails to engage the recipient.GMass helps you automate your follow-ups to maximize your campaign interactions. It lets you choose what your follow-ups contain, when to send them, how many follow-ups to send, and it even helps you decide the gap between each follow-up email.GMass PricingAre you concerned that all this functionality comes at a steep cost?Dont worry!GMass is one of the most affordable email tools you can find. Heres a quick look at its pricing plans:Individual:Standard: $25 per month or $225 annually. Includes unlimited emails, contacts, and campaigns. Plus mail merge personalization, Spam Solver, and dozens of other features.Premium: $35 per month or $325 annually. All Standard plan features, plus auto follow-up sequences, API access and Zapier, and triggered emails.Professional: $55 per month or $525 annually. All Premium features plus GMass MultiSend for inbox rotation and high-priority support.Team:Professional: starts at $145 per month for a team of five supports all features.ConclusionIt turns out that SMTP servers are pretty important!After all, without them, you wouldnt be able to send your emails.While understanding how SMTP servers work can be a little challenging, setting them up in a tool like GMass is a much simpler task.And if you set up SMTP with the right email tool, you wont have to worry about being blacklisted for spam or having your account blocked for sending too many emails. Additionally, setting up SMTP in GMass will help you enjoy lots of powerful features to streamline your mailing processes.So why not sign up for GMass today and take your email game to the next level? Email marketing, cold email, and mail merge inside Gmail Send incredible emails & automations and avoid the spam folder all in one powerful but easy-to-learn tool TRY GMASS FOR FREE Download Chrome extension - 30 second install! No credit card required Ajay is the founder of GMass and has been developing email sending software for 20 years. Love what you're reading? Get the latest email strategy and tips & stay in touch. If you think of e-mail as electronic mail, then SMTP is the mail man. Without the internets standard network protocol, sending applications documents, e-cards, and funny cat videos wouldnt be possible at all. This is because when you send an e-mail, it doesnt simply travel directly to the recipient, but goes through a complex communication process with numerous instances before it reaches its destination. SMTP stands for Simple Mail Transfer Protocol. It is a connection-oriented, text-based network protocol from the internet protocol family and is located on the seventh layer of the OSI model: the application layer. Just like any other network protocol, it contains rules for correct communication between computers in a network. SMTP is responsible for feeding and forwarding e-mails from sender to recipient.Since its release in 1982 as the successor of the Mail Box Protocol in Arpanet, SMTP has become the standard protocol for sending e-mails. For the average consumer, however, the SMTP protocol remains largely invisible, since the respective e-mail program executes it in the background. If the software, the webmail application in the browser, or the mobile mail app dont automatically define the SMTP protocol when setting up an account, you have to set it up manually to ensure smooth e-mail traffic. Sendmail was one of the first Mail Transfer Agents (MTA) that supported the SMTP protocol. Here is an overview of SMTP server addresses and SMTP ports for some of the most popular e-mail providers. E-mail provider SMTP server address SMTP port Yahoo smtp.mail.yahoo.com 465 AOL smtp.aol.com 587 Outlook smtp.live.com 587 Gmail smtp.gmail.com 587 (TLS/STARTTLS), 465 (SSL) To understand the SMTP protocol, you first have to understand e-mail. This is basically how it works: The SMTP client, i.e. the sender, loads the e-mail onto the SMTP server, i.e. the outgoing mail server of the respective e-mail provider. This is done via a webmail application in the browser or an e-mail program (technically called Mail User Agent, MUA for short) such as Windows Live Mail or Mozilla Thunderbird. The SMTP server then contacts the DNS server, and this server then searches for the IP address of the target SMTP server (also called Mail Delivery Agent, MDA for short), which is stored for the recipient address of the e-mail. The SMTP server sends the e-mail to the target SMTP server via one or more Mail Transfer Agents (MTA). Each of these forwarding processes runs according to the SMTP protocol. The target SMTP server temporarily stores the e-mail in the message store. The recipient MUA downloads the e-mail either via IMAP or POP3. Forwarding an e-mail from the SMTP client via the server to the message store of the target SMTP server is controlled by the SMTP protocol. Only then do other network protocols take effect. The interaction between the SMTP client and the SMTP server mentioned in the first step of the SMTP procedure represents the actual SMTP session. The rest of the SMTP procedure i.e. forwarding the e-mail via SMTP from the server to the recipient is covered in a separate article. Each session consists of a sequence of SMTP commands from the client and responses in the form of status codes from the server. According to the applicable SMTP specifications, each implementation of the network protocol must support at least the following eight commands, consisting of 7-bit ASCII characters: SMTP command Meaning HELO Hello. the client logs on with its computer name and starts the session MAIL FROM The client names the sender of the e-mail RCPT TO Recipient the client names the recipient of the e-mail DATA The client initiates the transmission of the e-mail RSET The client terminates the initiated transmission, but maintains the connection between client and server VRFY/EXPN Verify/Expand the client checks whether a mailbox is available for message transmission The server responds to each of these SMTP commands of the client with a three-digit status code including plain text message: Status code Plain text message Status codes that indicate that the server has successfully carried out the command: 200 (Non-standard success) 211 System status or system help reply 214 Help message 220 Server ready for SMTP session 221 Server ends the connection 250 Requested mail action OK, completed 251 User not local; mail is forwarded 252 Cannot verify (VRFY) user, but will accept message and attempt delivery 253 Pending messages for node started Status codes that indicate that the server has understood the command, but requires further information for processing: 354 Server starts mail input Status codes