Introduction to Email technology

You depend on email and can't work without it. However, most users (except IT professionals) still feel about email as something confusing and sometimes miraculous. You just need to write a message on

You depend on email and can't work without it. However, most users (except IT professionals) still feel about email as something confusing and sometimes miraculous. You just need to write a message on your computer, click Send and then a few minutes, it appears in the recipient's mailbox regardless of where they are. Great!

Email seems invisible. On the surface, you cannot know that email distribution is indeed a complex system with lots of operations to perform. Is that really an interesting story? However, if you have to be responsible for email distribution or heavy work management as email administrators, then you need to know the minimum issues about this technology.

In this article we will focus on introducing you to the technology of email. We will not go into the issue of mail management as well as company policies or issues related to human behavior. This article is also not aimed at the main issues in the fight against spam, although the spam fight is gradually becoming an important job for email administrators today. There are many other articles with the above mentioned topic that we have mentioned before.

This article also estimates that it will not go into technical expertise: with ABC knowledge, it doesn't mean everything from A to Z. Administrators probably understand that explaining the full concept can cost up to 40 dense pages of technical definitions; Most of them are too difficult to understand for the majority of users. However, if email is important to your business, you have to make sure that your employees have certain knowledge about email with some important people with it. This article will introduce the technological foundations so you will have an understanding of how it works and what can happen.

How does the email reach the recipient's mailbox?

Perhaps the first platform is email that is not managed by any kind of server or technology. It is a protocol package that is served by separate processes. We will consider these processes after understanding the overview.

You used to write in your email client - software applications that can be used on the desktop to help edit and organize mail, such as Microsoft Outlook, Apple Mail or Thunderbird programs. Email experts call these client applications the mail user agent (MUA).

BUYING may not be a desktop application; It can be a "Web mail" application that runs on a Web server and this server allows you to control using a browser. Web mail client, whether via Gmail, Yahoo or the front end of the company to another system, is handled in the same way as the BUYER of the desktop client in the rest of the email transmission process.

When you click on the Send button, the mail will not appear on the screen and set up a series of mail transfers. After clicking on the Send button, the mail is transmitted to your outgoing mail server (the mail server), this mail server can be named as ***mail.tencongty.com*** . Mail server - formerly known as a mail transport agent (MTA) - approves mail, because you are in a trusted network or because you have provided a username and password (usually stored in configuration files Picture of BUY). This network process is accomplished using a simple mail transfer protocol - Simple Mail Transfer Protocol (SMTP), and the sender security process is trusted called SMTP authentication.

When your mail is in the queue, the mail server needs to send it. The mail server communicates with the recipient's mail server and the mail download server using SMTP protocol. But with millions of mail servers, what is the mail server that it needs to contact? Your mail server will search on the DNS server (domain name server), these servers are understood as a type of library card catalog of the Internet, to find out who signed to accept mail for the domain of the person. receive. DNS for your mail server mail exchange (MX) records have been registered for that domain. From there give your mail server a server to contact and it begins to transmit on it.

Messages are sent on the Internet via TCP / IP (Transmission Control Protocol / Internet Protocol).

The process of communicating between the server and the server is somewhat different from what it did when talking to the BUYER client, although both use SMTP. Another difference is that between the administrator's settings and the pre-established code program, each mail server will acknowledge that the mail has been formatted incorrectly (like a postal rejection for a letter lacks a full street address), because it is not in line with the principle of sending spam or viruses.

Mostly to prevent spam, most mail servers handle mail through a process of many small steps before they accept the data, not even saving it and forwarding it to the user. These steps will be briefly introduced below.

Note that we are simplifying the communication process here.

Know that there are many steps in a process and each step is managed by standards. For example, RFC 2821 provides the SMTP standard, which includes how to send mail on the network. RFC 2822 offers a basic format for email notifications, including headers (To :, Cc :, Subject: .). Your email administrators will probably understand these issues very well.

When the mail reaches the destination mail server, this server will be responsible for delivering to the recipient (such as ***mail.tencongtykhachhang.com***), it is prepared to distribute to individuals waiting for your mail. There are also many options for mail administrators, how the mail will be saved and how it is forwarded to users. Each organization (or its email administrators) decides which method is best for their needs. Mostly, the main protocol used in our organization is Internet Message Access Protocol (IMAP), which allows to keep all incoming mail servers, neatly categorized into messages User's item. Today companies often use Post Office Protocol (POP3). Using POP3 e-mail, the 'Download new mail' command in your PURCHASE allows the application to download all correspondence to your computer. Under any circumstances, email messages using POP3 are then deleted on the mail server.

The recipient goes through a 'Download new mail' command on their own BUY . and gets the message you sent. The miracle is that your correspondence can travel around the world through 5 or 6 single computers. However, in many cases, your mail reaches the recipient's computer within a minute or two. All of that work is done very quickly when the system works. So what happens when the system has a problem?

How can emails be kept slow or lost?

The hype before said that Internet is like an 'electronic highway'. In this case, though, a freeway network is similar to the different highways in reality. If you do not find a vehicle on your way to your office, it may take about 20 minutes to reach the office. But if the road has too many cars, you can take up to 5 minutes to get through each intersection or intersection. Good engine structure cannot help you in this case. Then it will take more than 20 minutes for you to spend time in the office.

Understand the same for 'email highway'. The email server is fast, but the messages are very much and are full in

the queue. Internet traffic may require messages to be rerouted through unambiguous paths. Sometimes the problem may be caused by servers that are disconnected from the Internet, have a network cable unplugged, changed their BUY settings, or sent a PowerPoint file of up to 10MB. This is a common problem for your mail server. As with postal services, correspondence can be transferred from one location to another before they are distributed. These emails are managed from machine to machine under a 'save and forward' model involving many computers, so the delivery speed can change very quickly.

This also means that 'travel' correspondence through computers may or may not know the recipient and sender. The save and forward model is an important model in the email delivery method, because it allows secondary routes to change paths and recreate connections when certain problems occur.

These are all things that have not touched the annoying issues like spam and viruses. Add to that a huge amount of bandwidth consumption; Viruses, spam and Trojan horses can cause a lot of time and effort for network administrators to build traps to prevent unwanted risks from entering the user's mailbox. Every gateway takes time, like a highway, but its speed is slow. Previously, mail servers were not much interested in technical aspects. But in the current world, the ability to distribute mail may be compromised by other technical problems such as incorrect domain name servers (DNS), reckless adjustment of timeout parameters and mail format. abnormal.

Then the burden shifted to address spam, fake attacks and viruses. There will be no such thing when doing spam protection. While these filters will be increasingly improved, you may still have to keep in mind because not many real messages are included in the spam folder, and in such a situation if you don't check the spam folder you will assume That letter is lost.

Other barriers come from failure to configure the client and the email owner (as if it were you) according to the rules; More generally, this mail is rejected by the recipient's mail servers. If that happens, the message will be delayed or lost. This means that companies must enforce standards-based mail technology (such as ensuring that email addresses are closely tied to RFC), and that users must have behaviors to do with email correctly. Some other reasons include incompatibility between mail servers of recipients and senders. In this case the mail will be slowed down or lost. Therefore companies often have to force mail technology based on common standards and users pay attention in using email addresses correctly and necessary.

What is the difference between IMAP / POP protocols and why need to care about them?

As mentioned earlier, email can use a lot of Internet protocols, which are the industry standard method for data transmission. At the very least, you must have the protocol used by incoming mail servers - also known as 'recipient servers', usually POP3 and IMAP. Mail servers go (outgoing) - those servers are responsible for sending mail to a certain mailbox - using SMTP. A company may have a separate authentication server (LDAP) and perhaps provide other components such as schedules (often related to SQL databases), Web mail (using Web browsers). , with it the equivalent protocols are HTTP and IMAP), and centralized repository of client configuration (ACAP).

Each protocol serves a completely different need. For example, POP3 is designed to support disconnected and lightly loaded clients. IMAP provides server storage of mail folders. LDAP provides authentication not only for mail systems but also for other applications. Each protocol involves a particular problem.

However, most of these protocols are important, and it depends on which protocol suits you. Maybe your company thinks IMAP is more practical than POP3 because IMAP is more commonly used today than POP3, though both have their own advantages and disadvantages. So let's take a look at these advantages and

disadvantages.

IMAP is more popular because mail is still in the server. Most mail clients (MUA) allow users to synchronize data with the local hard drive - the need for mobility, such as on flights - however, the main location of the messages Credit is on the server. IMAP allows administration to be easier for IT managers because there is only one computer for backup and it is easy to control the amount of disk space consumed by restricting mailbox sizes. Users appreciate the ability to access their mail from any computer that is using MUA appropriately, and because IMAP can save the mail status (such as whether a message has been read or answered well). not yet) and keep the sent messages.

IMAP (separate SSL IMAP, with additional new features) can also enable bandwidth usage effectively. Instead of downloading messages to users' mailboxes, IMAP sends the header of the message by default (sender, recipient and subject line, etc.). Only selected messages are sent to the mailbox and the client can retrieve the text without retrieving the attachments.

However, IMAP also has drawbacks. If a company keeps all mail on one server, in case of no backup in time plus the number of emails can be very large, typically attachments or embedded images; Many companies solve this problem by creating guidelines for disk space (such as a maximum of 100MB), which will be annoying for users, especially those who really need a lot of needs.

Obviously, IMAP email cannot be accessed without an Internet connection or synchronization with a local computer. Many debate among experts about POP email is just one aspect of IMAP. Because the messages are downloaded to a separate computer, the mailbox size is limited by the user's available disk space, and messages can be viewed at any time when downloaded - however it can only be viewed from the downloaded device itself if the user does not have a specific setting to save the downloaded mail on the server. It also gives users a sense of privacy, POP3 is widely used for dial-up connections and it works with an older email client (kept by the user).

How is spam filtering conducted?

Email can be filtered at any point in the mailing process. It is not the same as what happens at the top of the

sender (probably because spam attackers know about what they're doing). Receiving emails can be checked on the server (companies should do so).

At the mail server level, mail can be checked by specialized devices or software (software with anti-virus tools), or with features built into the email server itself (via one Custom number required or add-on utilities).

When server filters work, there is no need to install a client filter. However, if no company installs a server filter or they do not perform well in maintaining the software, it could make commercial ISP registrations less control.
.

Fortunately, most email client applications, both web mail and desktop applications, have the type of spam filtering; In addition, you can also buy add-ons to select mail and classify them into a folder or vice versa marking them as carefully checked. Here are some of the methods used:

1. Filter header verifies the message headers - threads, incoming addresses, sending addresses, relay chains of servers - to see if they are fake or not. Some anti-spam programs can detect fake headers, based on that to distinguish spam. Filter languages ??to exclude messages that are not the language you normally use.
2. There is also content filtering, this is the least effective method. There is also a method for filtering permissions, which requires the sender to verify themselves.

There are indeed a lot of email issues that we need to discuss in this brief overview. In this article some topics are not mentioned here such as mail storage, encryption and mail administration. Because of that, we will deliver it to you as soon as possible.