Protocolo: POP3: Post Office Protocol Versión 3.

Es un protocolo para la ***gestión de correo en Internet***. Es el más utilizado junto con SMTP, porque aunque en algunos nodos menores de Internet normalmente es poco práctico mantener un sistema de transporte de mensajes (MTS), es posible que una estación de trabajo no tenga recursos suficientes (espacio en disco, entre otros) para permitir que un servidor de SMTP [RFC821] y un sistema local asociado de entrega de correo estén residentes y continuamente en ejecución. De forma similar, puede ser caro (o incluso imposible) mantener una computadora personal interconectada a una red tipo IP durante grandes cantidades de tiempo (el nodo carece el recurso conocido como "connectivity").

A pesar de esto, a menudo es muy útil poder administrar correo sobre estos nodos, y frecuentemente soportan un user agent (UA agente de usuario) para ayudar en las tareas de manejo de correo. Para resolver el problema, un nodo que sí sea capaz de soportar un MTS ofrecerá a estos nodos menos dotados un servicio de maildrop. Se entiende por maildrop, el "lugar" en el sistema con el MTS donde el correo es almacenado para que los otros nodos puedan trabajar con él sin necesidad de mantener su propio MTS. El Protocolo de oficina de correos - Versión 3 (POP3) está destinado a permitir que una estación de trabajo acceda dinámicamente a un maildrop en un host servidor de forma útil y eficiente. Esto significa que el protocolo POP3 se usa para permitir a una estación de trabajo recobrar correo que el servidor tiene almacenado.

POP3 no está destinado a proveer de extensas operaciones de manipulación de correo sobre el servidor; normalmente, el correo es transmitido y entonces borrado. IMAP4 es un protocolo más avanzado y complejo y es tratado en [RFC1730] y revisado en [RFC 2060].

De aquí en adelante el termino (host) cliente se refiere a un host haciendo uso del servicio POP3 y host servidor al que ofrece este servicio. Inicialmente, el host servidor comienza el servicio POP3 leyendo el puerto 110 TCP. Cuando un host cliente desea de hacer uso del servicio, establece una conexión TCP con el host servidor. Cuando la conexión se establece, el servidor POP3 envía un saludo. Entonces, el cliente y el servidor de POP3 intercambian comandos y respuestas respectivamente hasta que la conexión se cierra o es abortada.

Los comandos en el POP3 consisten en una palabra clave (keyword), posiblemente seguida de uno o más argumentos. Todos los comandos terminan con un par CRLF. Las palabras clave y los argumentos consisten en caracteres ASCII imprimibles. Las palabras clave y los argumentos están cada uno separados por un único carácter de espacio. Las palabras clave son de una longitud de tres o cuatro caracte-

res, mientras que cada argumento puede ser de hasta 40 caracteres de longitud.

Las respuestas en el POP3 consisten de un indicador de estado y una palabra clave posiblemente seguida de información adicional. Todas las respuestas acaban en un par CLRF. Las respuestas pueden ser de hasta 512 caracteres de longitud, incluyendo el CRLF de terminación. También existen dos indicadores de estado: positivo o afirmativo ("+OK") y negativo ("-ERR"). Los servidores deben enviar el "+OK" y el "-ERR" en mayúsculas.

Las respuestas a ciertos comandos son multilínea (una respuesta compuesta de varias líneas). En estos casos, que se indican claramente más adelante, después de enviar la primera línea de la respuesta y un CRLF, se envía cualquier línea adicional, cada una terminada en un par CRLF. Cuando todas las líneas de la respuesta han sido enviadas, se envía una línea final, que consiste en un octeto de terminación (en decimal 046,".") Y un par CRLF. Si alguna línea de la respuesta multilínea comienza con el octeto de terminación, se ponen bytes de relleno precedidos por el byte de terminación en esa línea de la respuesta. De aquí en adelante una respuesta multilínea termina con los cinco bytes "CRLF.CRLF". Al examinar una respuesta multilínea, el cliente comprueba si la línea comienza con el byte de terminación. Si es así y si siguen otros bytes a excepción del CRLF, el primer byte de la línea (el byte de terminación) es ignorado. De este modo si el CRLF sigue inmediatamente al carácter de terminación, entonces la respuesta desde el servidor POP termina y la línea conteniendo "CRLF " no es considerada como parte de la respuesta multilínea.

Una sesión POP3 progresa a través de una serie de estados a lo largo de su vida. Una vez la conexión TCP ha sido abierta y el servidor de POP3 ha enviado el "saludo" (línea especial que se utiliza cuando se establece la conexión), la sesión entra en el estado de autorización (AUTHORIZATION). En este estado, el cliente debe identificarse al servidor de POP3. Una vez el cliente ha hecho esto satisfactoriamente, el servidor adquiere los recursos asociados al maildrop del cliente, y la sesión entra en el estado de transacción (TRANSACTION). En este estado, el cliente realiza una serie de solicitudes al servidor de POP3. Cuando el cliente ha emitido el comando de finalización (QUIT), la sesión entra en el estado de actualización (UPDATE). En este estado, el servidor de POP3 libera cualesquiera recursos adquiridos durante el estado de transición, "dice adiós" y la conexión TCP se cierra.

Un servidor debe responder a comandos no reconocidos, no implementados, o sintácticamente incorrectos con un indicador negativo de estado (respuesta negativa). También debe responder con un indica-

dor negativo de estado cuando la sesión se encuentra en un estado incorrecto. No hay un método general para que el cliente distinga entre un servidor que no implementa un comando opcional y un servidor que no esta dispuesto o es incapaz de procesar el comando.

Un servidor de POP3 puede disponer de un temporizador o cronómetro de inactividad (autologout inactivity timer). Tal cronómetro debe ser de por lo menos 10 minutos de duración. La recepción de cualquier comando desde el cliente durante este intervalo reinicia la cuenta de este cronómetro. Cuando el cronómetro llega a los diez minutos, la sesión no entra en el estado de actualización. Entonces, el servidor debería cerrar la conexión TCP sin eliminar ningún mensaje y sin enviar ninguna respuesta al cliente.

USER nombre
Argumentos: una cadena identificando un mailbox, el cual solo tiene significado para el servidor
Restricciones: solo puede darse en el estado de autorización después del saludo o de los comandos USER o PASS sin éxito.
Definición: Para autentificar usando la combinación de los comandos USER y PASS, el cliente debe primero emitir el comando USER. Si el servidor responde afirmativamente (+OK), entonces el cliente puede responder con el comando PASS para completar la autentificación, o el comando QUIT para finalizar con la conexión. Si el servidor responde negativamente (-ERR) al comando USER, el cliente puede emitir un nuevo comando de autenticación o bien el comando QUIT.
El servidor puede devolver una respuesta afirmativa incluso a pesar de que no exista ningún mailbox. El servidor puede devolver una respuesta negativa si el mailbox existe, pero no permitir la autenticación.

PASS cadena
Argumentos: palabra de acceso al mailbox
Restricciones: solo puede darse en el estado de autorización inmediatamente después de un comando USER satisfactorio.
Definición: Cuando el cliente el comando PASS, el servidor utiliza el par de argumentos de los comandos USER y PASS para determinar si al cliente se le debe dar acceso al maildrop apropiado.
Ya que el comando PASS tiene exactamente un argumento, un servidor de POP3 puede tratar los espacios como parte del password en lugar de cómo separadores de argumentos.

APOP nombre digest
Argumentos: una cadena identificando un mailbox y una cadena digest MD5
Restricciones: solo puede darse en el estado de autorización después del saludo o de los comandos USER o PASS sin éxito.
Definición: Normalmente, cada sesión POP3 comienza con intercam-

bio USER/PASS. Esto tiene como resultado una clave de acceso específica enviada a través de la red. Para un uso intermitente del POP3, no conlleva un riesgo considerable. Sin embargo, muchas implementaciones de cliente POP3 conectan al servidor regularmente para comprobar si hay correo nuevo. Además, el intervalo de iniciación de la sesión puede ser del orden de 5 minutos. Por lo tanto, el riesgo de que la clave de acceso sea capturada es alto.
Se requiere un método alternativo de autenticación que no implique el envío de claves de acceso a través de la red. Esta funcionalidad la proporciona el comando APOP.
Un servidor que implemente el comando APOP incluirá una marca de tiempo (timestamp) en sus "saludos". La sintaxis de la marca de tiempo corresponde al "msg-id" en la RFC 882 (actualizada por RFC 973 y después por RFC 1982), y debe ser diferente cada vez que el servidor envía un saludo. Por ejemplo, en una implementación UNIX en la cual un proceso UNIX separado es el encargado de cada instancia de servidor, la sintaxis de la marca de tiempo podría ser: process-ID.clock@hostname, donde process ID es el valor decimal del PID del proceso, clock es el valor decimal del reloj del sistema, y hostname es el nombre de dominio del host donde el servidor está funcionando.
El cliente recibe esta marca de tiempo y emite un comando APOP. El parámetro nombre tiene el mismo significado que el parámetro nombre del comando USER. EL parámetro digest se calcula aplicando el algoritmo MD5 (RFC 1321) a una cadena consistente en una marca de tiempo (incluyendo <) seguido de un secreto compartido. Este secreto compartido es una cadena conocida solo por el cliente y el servidor. Se debe tener un gran cuidado para prevenir una revelación no autorizada del secreto, ya que su conocimiento puede permitir a cualquier entidad hacerse pasar por el usuario. El parámetro digest es un valor de 16 bytes que se envía en formato hexadecimal, utilizando caracteres ASCII en minúsculas.
Cuando el servidor recibe el comando APOP, verifica el digest proporcionado. Si el digest es correcto, el servidor envía una respuesta afirmativa y la sesión entra en el estado de transacción. Si no, envía una respuesta negativa y la sesión permanece en el estado de autorización.
Notar que conforme incrementa la longitud de los secretos compartidos, aumenta la dificultad de derivarlos. Como tales, los secretos compartidos deben ser cadenas largas (considerablemente más largas que el ejemplo de 8 caracteres mostrado abajo).

AUTH mecanismo

Argumentos: una cadena que identifique un mecanismo de autenticación IMAP4 (definición en IMAP4-AUTH).
Restricciones: sólo puede darse en el estado de autorización.
Definición: El comando AUTH se refiere a un mecanismo de autenticación al servidor por parte del cliente. Si el servidor soporta este mecanismo, lleva a cabo el protocolo para la identificación del usua-

rio. Opcionalmente, también procede con un mecanismo de protección para las subsiguientes interacciones del protocolo. Si este mecanismo de autentificación no es soportado, el servidor debería rechazar el comando AUTH enviando una respuesta negativa.
El protocolo de autentificación consiste en una serie de cuestiones por parte del servidor y de unas respuestas del cliente, específicas de este mecanismo de autentificación. Una pregunta del servidor, es una línea que consiste en un carácter "+" seguido de un espacio y una cadena codificada en base 64. La respuesta del cliente es una línea que contiene otra cadena codificada en base 64. Si el cliente desea cancelar la autentificación, debe emitir una línea con un único "*". Si el servidor la recibe, rechazará el comando AUTH.
Un mecanismo de protección proporciona integridad y privacidad a la sesión del protocolo. Si se utiliza un mecanismo de protección, este será aplicado a todos los datos que se envíen en la conexión. El mecanismo de protección tiene efecto inmediatamente después de que un CLRF concluya con el proceso de autenticación del cliente y de la respuesta positiva del servidor. Una vez el mecanismo de protección se hace efectivo, el flujo de bytes de comandos y respuestas se procesa en buffers de ciphertext (texto cifrado). Cada buffer es transferido en la conexión como un flujo de bytes seguidos de un campo de 4 bytes que representan la longitud de los siguientes datos. La longitud máxima de los bufferes de ciphertext se define en el mecanismo de protección.
No es necesario que el servidor soporte algún mecanismo de autentificación, y tampoco es necesario que los mecanismos de autentificación soporten mecanismos de protección. Si un comando AUTH falla, la sesión permanece en el estado de autorización y el cliente puede probar con otro AUTH o bien con otro mecanismo como la combinación USER/PASS, o el comando APOP. En otras palabras, el cliente puede pedir tipos de autentificación en orden decreciente de preferencia, con USER/PASS o APOP como últimos recursos.
Si el cliente completa la autentificación satisfactoriamente, el servidor de POP3 emite una respuesta afirmativa y se entra en el estado de transacción.

TOP mensaje

Argumentos: un número de mensaje, que si aparece no se puede referir a ningún mensaje marcado como borrado; y un número no negativo de líneas.
Restricciones: solo puede darse en el estado de transacción.
Definición: Si el servidor emite una respuesta positiva, entonces ésta es multilínea. Después del +OK inicial, el servidor envía las cabeceras del mensaje, la línea en blanco separando las cabeceras del cuerpo, y luego el número de líneas del cuerpo del mensaje.
Si el número de líneas requeridas por el cliente es mayor del número de líneas del cuerpo, el servidor envía el mensaje entero.

UIDL [mensaje]

Argumentos: un número de mensaje opcional. Si está presente no debe referirse a un mensaje marcado como borrado.

Restricciones: solo puede darse en el estado de transacción.

Definición: Si se da un argumento, el servidor emite una respuesta afirmativa con una línea que contiene información del mensaje. Esta línea se llama unique-id listing.

Si no se da ningún argumento y el servidor emite una respuesta afirmativa, la respuesta dada es multilínea. Después del +OK inicial, por cada mensaje en el maildrop, el servidor responde con una línea con información de ese mensaje.

Para simplificar el análisis, todos los servidores deben tener un mismo formato de unique-id listing, que consiste en el número de mensaje, un espacio y el unique-id del mensaje. Después no hay mas información.

El unique-id listing de un mensaje es una cadena arbitraria determinada por el servidor, que consiste en 70 caracteres entre 0x21 y 0x7E (hexadecimal), los cuales identifican únicamente un mensaje en el maildrop y los cuales permanecen a lo largo de las distintas sesiones. Esta persistencia es requerida incluso si la sesión termina sin entrar en el estado de actualización. El servidor nunca debería rehusar el unique-id en un maildrop dado a lo largo de todo el tiempo de existencia de la entidad que usa el unique-id.

Mientras que generalmente es preferible para implementaciones de servidor almacenar los unique-id en el maildrop, la especificación tiene la intención de permitir que los unique-id sean calculados como trozos del mensaje. Los clientes deberían de ser capaces de manejar una situación en la que se den dos copias idénticas de un mensaje en un maildrop con el mismo unique-id

TERRA SERVIDOR POP3

Configuración cuentas de correo.

Estos son los datos que necesitarás para configurar tu programa de correo electrónico.

	Cuentas@terra.es	**Cuentas@*tudominio.com***
Dirección de correo	*nombreBuzon*@terra.es	nombreBuzon@*tudominio.com*
Servidor correo entrante (POP3)	pop3.terra.es	pop3.dominios.terra.es
Servidor correo saliente (SMTP)	mailhost.terra.es	mailhost.dominios.terra.es
Nombre de cuenta (usuario POP3)	*nombreBuzon*.terra.es	*nombreBuzon.tudominio.com*
Contraseña	la que hayas elegido	la que hayas elegido

nombre Buzon debes sustituirlo por el nombre que hayas elegido para tu cuenta de correo.
tudominio.com debes sustituirlo por tu dominio, ya sea .com, .net, .org.

Servicio Atención al Cliente de Cuentas de Correo.
Si tiene acceso Terra Profesional o ADSL, contacte con nosotros en el 902 10 80 10, en caso contrario llame al 902 15 20 25, o en el correo Electrónico terra@terra.es. Disponibles las 24 horas del día.

807317531
www.terra.es/usuarios