1 Post Office Protocol 3

.. anhand RFC 1939.

1.1 Allgemeines zu POP3:

1. ist ein Kommunikationsprotokoll, um Emails von einem POP-Server abzuholen
2. Kommunikation erfolgt zwischen einem Email Client und einem Email Server

1.2 Funktionsweise des POP3:

1. per Fernzugriff werde gespeicherte Emails abgerufen und lokal gespeichert
2. POP sieht Prinzip der Offline-Verarbeitung von E-Mails vor
3. Online werden E-Mails vom POP-Server des Clients heruntergeladen
4. erst nach erfolgreichem und vollstndigem Zugriff werden Emails am Server gelscht
5. Bearbeitung der Emails erfolgt lokal (offline) ohne Verbindunge zum POP-Server

1.3 Anmeldung bei Mailserver:

1. Server host startet den POP3-Server,in dem es den TCP Port 110 abhrt
2. mchte ein Client den Service verwenden -¿ Client erstellt TCP Verbindung mit dem Server Host her
3. nach erfolgreicher Verbindung -¿ POP3 Server sendet Gru aus
4. Session kommt in die AUTHORIZATION State
5. Client muss sich zuletzt identifizieren

1.4 Abrufen von Nachrichten:

1. Client fhrt hierbei einen Command aus -¿ Server antwortet auf dieses
2. Nachrichten werden von Server lokal am Computer abgespeichert, d.h. es wird einfach eine Kopie der Nachricht am Computer abgespeichert, wobei diese Mail am Server gelscht wird und nur mehr lokal erreichbar ist

1.5 Wie ist das POP3-Protokoll grundstzlich aufgebaut?

The Post Office Protocol - Version 3 (POP3) is intended to permit a workstation to dynamically access a maildrop on a server host in a useful fashion. Usually, this means that the POP3 protocol is used to allow a workstation to retrieve mail that the server is holding for it. POP3 is not intended to provide extensive manipulation operations of mail on the server - normally, mail is downloaded and then deleted.

Initially, the server host starts the POP3 service by listening on TCP port 110. When a client host wishes to make use of the service, it establishes a TCP connection with the server

host. When the connection is established, the POP3 server sends a greeting. The client and POP3 server then exchange commands and responses (respectively) until the connection is closed or aborted.

Commands in the POP3 consist of a case-insensitive keyword, possibly followed by one or more arguments. All commands are terminated by a CRLF pair. Keywords and arguments consist of printable ASCII characters. Keywords and arguments are each separated by a single SPACE character. Keywords are three or four characters long. Each argument may be up to 40 characters long.

Responses in the POP3 consist of a status indicator and a keyword possibly followed by additional information. All responses are terminated by a CRLF pair. Responses may be up to 512 characters long, including the terminating CRLF. There are currently two status indicators: positive ("+OK") and negative ("-ERR"). Servers MUST send the "+OK" and "-ERR" in upper case. Responses to certain commands are multi-line.

Sessions progresses through a number of states during its lifetime. Once the TCP connection has been opened and the POP3 server has sent the greeting, the session enters the AUTHORIZATION state. In this state, the client must identify itself to the POP3 server. Once the client has successfully done this, the server acquires resources associated with the client's maildrop, and the session enters the TRANSACTION state. In this state, the client requests actions on the part of the POP3 server. When the client has issued the QUIT command, the session enters the UPDATE state. In this state, the POP3 server releases any resources acquired during the TRANSACTION state and says goodbye. The TCP connection is then closed.

1. Starten des POP3 Servers
2. Indentifizieren des Users innerhalb der AUTHORIZATION State:
   (a) User muss Benutzernamen sowie Passwort eingeben -¿ hat Server Daten geprft und ein entsprechendes Maildrop geffnet ,wechselt POP3 Session in die TRANSACTION State
   (b) Client kann nun Kommandos ausfhren, auf welche POP3 Server antwortet
3. TRANSACTION State:
   (a) nachdem Client erfolgreicht identifiziert wurde, kann Client kommandos ausfhren
   (b) nach jedem Kommando gibt der Server eine Antwort
   (c) ist die Sitzung zur Anforderung und bermittlung der Emails
   (d) alle Befehle zur Bearbeitung von Emails werden hier ausgefhrt
4. UPDATE State:
   (a) alle vom Client angegebenen Anforderungen werden hier ausgefhrt
   (b) Verbindung zu TCP ist zu diesem Zeitpunkt schon beendet
   (c) fhrt der Client innerhalb dieser State den QUIT Befehl aus, so wechselt die Session zur UPDATE State
   (d) terminiert die Session ohne das Client QUIT ausgefhrt hat, so kommt die Session nicht in den UPDATE Zustand und weiters muss keine Nachricht aus dem Maildrop entfernt werden

(e) letzter Vorgang stellt sicher, dass Emails nur auf dem Server gelscht werden, wenn Verbindung ordnungsgem beendet wurde

1.6 Ist POP3 ein sicheres Protokoll? Warum, Warum nicht?

1. POP3 setzt Authentifizierung ber Benutzername und Passwort voraus
2. Benutzername und Passwort werden ungeschtzt als Klartext bertragen
3. ermglicht Angreifern den unbemerkten Zugriff auf die Mailbox -¿ Sicherheitslcke

1.7 Was ist der Unterschied zwischen single-line und multi-line response?

1. Singlie-Line Response:
   (a) es wird eine Zeile als Response zurckgegeben
   (b) terminiert durch CRLF
2. Multi-Line Response:
   (a) nachdem die erste Line und ein CRLF gesendet wurde, werden die restlichen hinterher gesendet, welche ebenfalls durch ein CRLF terminiert werden
   (b) sind alle Lines verschickt worden so wird eine letzte Line, die aus einem "." und einem CRLF-Paar besteht, versendet -¿ Ende der Multi-Line mit CRLF.CRLF gekennzeichnet

1.8 Vergleiche POP3 mit IMAP und beschreibe wesentliche Unterschiede.

1. POP3:
   (a) hier werden ledigliche die Emails aus dem Ordner des Posteingangs vom Server heruntergeladen
   (b) Nutzer kann selbst whlen, ob diese vom Server gelscht oder behalten werden sollen
   (c) Meldet man sich an einem anderen Ort an, kann es sein, dass all ihre Emails erneut heruntergeladen werden, da diese nicht gelscht werden (kann nach einiger Zeit in die Tausende gehen und viel Speicherplatz/Zeit beanspruchen)
   (d) nicht erkennbar, welche Emails gelesen, beantwortet oder gelscht wurden
   (e) Synchronisation zwischen Endgert und Email-Konto geschieht nicht !!
2. IMAP:
   (a) hierber wird der komplette Inhalt des Email Kontos stets mit dem Mail-Programm auf dem Computer oder Smartphone synchronisiert
   (b) wird z.B. eine Nachricht mittels Outlook gesendet, so landet diese im Ordner "Gesendet" sowohl in Outlook, als auch auf dem Server und anderen Gerten wie dem Smartphone
   (c) alle Bewegungen des Email-Kontos sind auf allen Gerten gleich