

### 5.2.1.1 Überblick

In den folgenden Seiten werden zwei Protokolle die in den höheren Layern arbeiten beschrieben. Anhand von POP und SMTP wird der Session Layer 5 per Skript bedient und dann noch etwas vom Layer 6 um die anzuzeigen oder auszuwerten.

| Protokoll | Lang Text                      | IP-Typ | Port  | Transfer | Layer | Funktion         | RFC  |
|-----------|--------------------------------|--------|-------|----------|-------|------------------|------|
| SNTP      | Simple Network Time Protokoll  | TCP    | 123   | TelNet   | 4     | Uhrzeit abfrage  | 2030 |
| SMTP      | Simple Mail Transfer Protokoll | TCP    | 25    | Telnet   | 4     | Email Versand    | 821  |
| POP3      | Post Office Protokoll          | TCP    | 110   | Telnet   | 5     | Email abfrage    | 1939 |
| HTTP      | Hyper Text Transfer Protokoll  | TCP    | 80    | Telnet   | 4     | WEB Zugriff      | 822  |
| FTP       | File Transfer Protokoll        | TCP    | 20/21 | FTP      | 5     | Dateiübertragung | 959  |
| IMAP      | Internet Message Access Prot.  | TCP    | 143   | TelNet   | 5     | Div. z.B. POP... | 2060 |

Was ist nun an den beiden Protokollen speziell? Speziell ist, dass es Protokolle der höheren Layer sind, die somit auf weiteren niedrigeren Layern aufbauen. Weiter haben höhere Layer meist viel höhere Time-outs (Zeit bis zu Protokoll Abbruch) was diese Protokolle für Demonstrationszwecke gerade zu ideal macht. Z.B. die Bytes der Pakete des ICMP Protokolls sind so schnell, dass man diese nur mit Hilfsmittel abspeichern und darstellen kann. Nicht so bei POP und SMTP wenn nach einem Byte eine Pause von 100 Sekunden eingelegt wird, so ergeben sich noch keine Abbrüche! Die unteren Protokolle wie beispielsweise das Telnet Protokoll das für POP und SMTP Verwendet wird, überträgt jedes getippte Zeichen einzeln und erzeugt dafür jeweils ein Paket das sofort versendet wird. Sehr von Vorteil ist auch, dass diese Protokolle im Klartext aufgebaut sind (also Text orientiert und sogar Wortbasierend).

Übrigens alle RFC sind bei RIPE (den europäischen Internet Göttern) zu finden <ftp://ftp.ripe.net/rfc/>

#### Noch was zu den Layern:

Weiter sind die Layer zu beachten, denn nicht alle Protokolle haben eine Authentifizierung (Passwort-abfrage) also arbeiten diese Protokolle nur bis zum Layer 4. Alles mit Passwortabfrage braucht also auch einen Layer 5. Allerdings ist zu sagen, dass auch ein Layer 4 Protokoll wie SMTP eine Session erzeugt, d.h. es ist ein Verbindungsaufbau-, ein Datenaustausch- und ein Verbindungsabbau vorhanden.

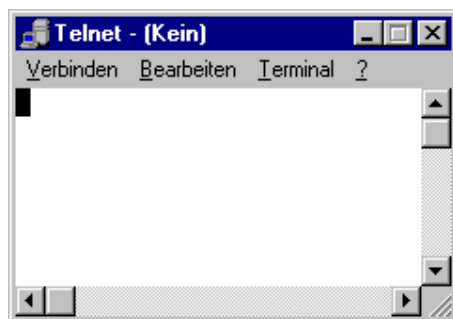
Wobei die meisten dieser Protokolle auch eine Präsentations Schicht (Layer 6) und Programm Schicht (Layer 7) brauchen, damit wir vernünftig damit arbeiten können. HTTP>(Web-Browser), POP3>(eMail-Client), SMTP>(eMail-Client)

### 5.2.1.2 Kommunikation

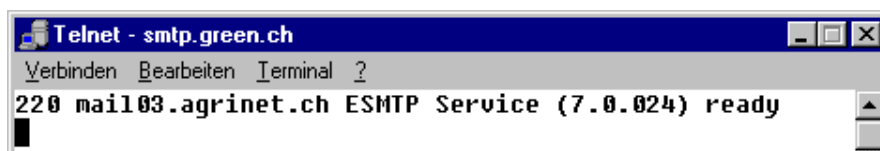
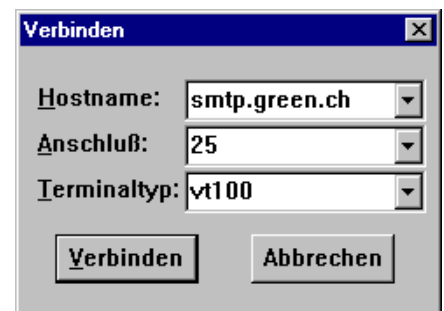
Um eine Kommunikation mit POP oder SMTP aufzubauen ist also ein Telnet Programm notwendig, das sowohl in Windows als auch bei UNIX Welt als Bestandteil integriert ist. Achtung bei Win2k und WinXP kann beim Telnet Programm der Port nicht mehr vom Standard Telnet Port 23 umgestellt werden. In diesen Fällen verwenden Sie bitte PuTTY Telnet Client ab folgender URL:

<ftp://ftp.clinch.ch/NetzWerk/Telnet/puttytel.exe> . Die Datei muss beim Downloaden nicht auf der Festplatte gespeichert werden, sondern kann direkt geöffnet werden.

Mit dem Windows TelNet sieht es folgender massen aus: [Start], [Ausführen], **TELNET**, [OK]



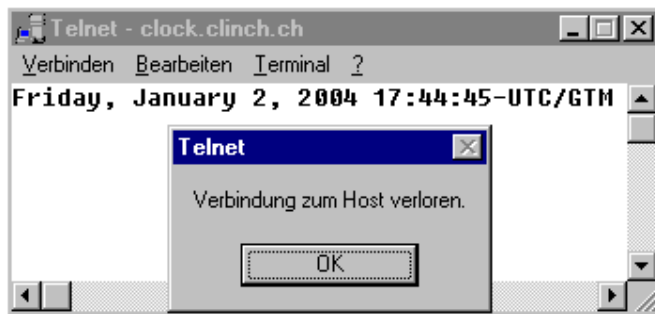
[Verbindung], [Netzwerk]



Jetzt meldet sich der Mail Server mit seinem Namen, Funktion und Version und wartet auf weitere Kommandos...

### 5.2.1.3 SNTP

Ein sehr einfaches Protokoll ist SNTP (Simple Network Time Protokoll) mit dem ein SNTP Zeit Server abgefragt werden kann.



Gegen Ende dieses Kapitels, bei den Script's, werden wir noch eine Synchronisierung programmieren.

Für Win2k und WinXP sind bereits SNTP Client's im Lieferumfang vorhanden. Mit folgendem Befehl lässt sich die Zeit auf dem Client aktualisieren: **NET TIME /setsntp:clock.clinch.ch** . Oder zur Sicherheit mit zwei Servern: **net time /setsntp:"swisstime.ethz.ch tick.usnogps.navy.mil info1.rrze.uni-erlangen.de"** Starten des Windows Zeit Synchronisations Dämon: **net start W32Time** .

Oder zur Abfrage der aktuellen Einstellungen ist folgender Befehl zu verwenden: **NET TIME /querysntp**

Unter folgender URL ist ein SNTP Client Service für alle Windows Versionen als FreeWare zum Downloaden bereit: [ftp://ftp.clinch.ch/NetzWerk/Net-Clock/NetTime-2b6\\_easy.exe](ftp://ftp.clinch.ch/NetzWerk/Net-Clock/NetTime-2b6_easy.exe)

### Stratum

Mit den SNTP Protokollen muss auch noch das Wort Stratum erklärt werden. Die oberste Instanz eines Zeitsystem ist das ZeitNormal, dies ist zum Beispiel eine Cäsium Atom Uhr (Stratum 0 System). Jetzt folgen die direkt angeschlossenen SNTP Server (Stratum 1). Das sind SNTP Server die Ihre Uhrzeit direkt von einem Stratum 0 System (Atom Uhr) erhalten.

Jetzt folgen die SNTP Systeme die Ihre Uhrzeit, über Internet, von verschiedenen Stratum 1 Quellen beziehen. Z.B. Clock.clinch.ch ist ein Stratum 2 NTP Server der in Zürich in der Schweiz im Rechenzentrum von SYSTEM-CLINCH Internet Services GmbH installiert ist. Dieser SNTP Server ist in der Hierarchie ein zentrales System das die Uhrzeit ausschliesslich über Internet von mehreren Quellen bezieht. Wobei diese alle Quellen nach verschiedenen Kriterien bewertet werden und immer der mit der geringsten Korrektur Notwendigkeit verwendet wird (und natürlich auch mit dem geringsten Jitter).

| Stratum   | Zeit-Funktion        | Typ           | Beschreibung                                 |
|-----------|----------------------|---------------|----------------------------------------------|
| Stratum 0 | Atom Uhr             | Master        | Hoch genaue Atom Uhr                         |
| Stratum 1 | SNTP-Server          | Primär        | Direkt an Stratum 0 angeschlossen & Internet |
| Stratum 2 | SNTP-Server & Client | Sekundär      | Synchronisiert zu mehreren Stratum 1         |
| Stratum 3 | SNTP-Client          | Local-Srv./PC | Server in Unternehmen (oder einzel PC)       |
| Stratum 4 | SNTP-Client          | PC            | Client eines LAN's                           |

### SNTP Statistik eines Stratum 2 Servers (show ntp associations)

```

address      ref clock      st  when  poll reach  delay  offset  disp
~127.127.7.1  127.127.7.1    7   31    64  377    0.0    0.00    0.0
~131.188.3.36  0.0.0.0       16   -    1024  0     0.0    0.00   16000.
+~204.34.198.40 .USNO.        1   21    64  377   164.9   -4.35    0.6
*~129.132.2.21 .DCFa.        1    8    64  377   10.4   -1.39    0.6
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured

```

### 5.2.1.3 SMTP

Die Emails das wohl meist verbreitete elektronische Kommunikationsmittel. Wie funktioniert das denn? Meinem Email Client ist unter anderem ein SMTP Server meines ISP's (Internet Service Provider /zu deutsch Internet Dienst Verteiler) hinterlegt. D.h. alle meine ausgehende Post wird zu diesem Server gesendet. Dieser SMTP Server übernimmt dann die Zustellung zum Ziel ISP oder genauer zum Server der die Domäne und das entsprechende Postfach unterhält. Dort wird somit die elektronische Post bis zur Abholung gelagert (im elektronischen Postfach). Zur Übermittlung der elektronischen Post zum ISP gibt's eine Liste von Befehlen die im RFC des SMTP Protokolls definiert sind. Im folgenden eine Liste der Kommandos:

| Kommando   | Argument / Beschreibung                           |
|------------|---------------------------------------------------|
| HELO       | Systemname Beginn, Name des sendenden Systems     |
| MAIL From: | Absenderadresse Beginn der Übermittlung           |
| RCPT To:   | Empfängeradresse Adressat der Email               |
| DATA       | Brieftext, Ende durch eine Zeile mit "."          |
| HELP       | Topic Hilfestellung                               |
| VERFY      | Mailadresse Mailadresse verifizieren              |
| EXPN       | Mailadresse Mailadresse expandieren (z. B. Liste) |
| RSET       | Senden abbrechen, Zurücksetzen                    |
| NOOP       | nichts tun                                        |
| QUIT       | Verbindung beenden                                |

Wichtig ist, dass das Postfach des Empfänger der Email auf dem selben SMTP Server vorhanden ist. Da ansonsten Fehlermeldungen erscheinen (550 no Relaying) usw...

Wir versenden nun eine Email, via Telnet, direkt auf den Server der das Email Konto unterhält.

[Start], [Ausführen], **TELNET**, [OK], [Verbinden], [Hostname:]**smtp.clinch.ch**, [Anschluss:]**25**, [OK]

| Eingabe                            | Antwort:                                                                 |
|------------------------------------|--------------------------------------------------------------------------|
| Der SMTP Server meldet beim Start: | 220 X1 NT-ESMTP Server clinch.ch (IMail 9.07 123456-1)                   |
| HELP                               | 211 DATA EXPN HELO MAIL NOOP QUIT RCPT RSET SAML<br>SEND SOML TURN VERFY |
| HELO mail.niemand.ch               | 250 hello clinch.ch                                                      |
| MAIL From: info@niemand.ch         | 250 ok                                                                   |
| RCPT To: info@clinch.ch            | 250 ok its for <info@clinch.ch>                                          |
| DATA                               | 354 ok, send it; end with <CRLF>.<CRLF>                                  |
| Test Email via Telnet versendet    | -                                                                        |
| .                                  | 250 Message queued                                                       |
| NOOP                               | 250 ok                                                                   |
| QUIT                               | 221 Goodbye<br>Telnet Session wird beendet                               |

Wie am Protokoll Ablauf oben zu sehen ist, ist kein Passwort notwendig? Ja, das ist klar, es muss ja weltweit auf alle Server funktionieren. Dies ist aber auch ein Sicherheitsrisiko dem mit einigen Tricks nachgeholfen wird. Erstens - Die IP-Adresse des Absenders muss im IP Range des ISP's liegen (könnte auch falsch angegeben werden). Zweitens - Mindesten eine der Email Adressen Sender oder Empfänger muss auf dem Mail Server als Konto vorhanden sein liegen (könnte auch falsch angegeben werden). Drittens - (Option) Von der selben Absender IP-Adresse muss zuvor eine POP3 Konto mit User-Name und Passwort authentifiziert worden sein. Viertens - (Option) SMTP Empfang einer Email von einem Client nur mit SMTP Passwort (Keine übliche Methode).

### 5.2.1.4 POP3

Das Post Office Protokoll - Abfrage eines Postfaches mittels Telnet und POP3. Wie funktioniert das denn? Ja, da die meisten PCs nicht dauernd am Internet sind und auch meistens keine öffentliche, Fixe IP-Adresse besitzen, muss ein Postfach her, das die elektronische Post aufbewahrt. Dieser Dienst wird im Normalfall durch den ISP gestellt, oder auch durch diverse Web-eMailer wie yahoo.ch oder gmx.ch uvm...

Kommandos:

| Kommando | Argument | Beschreibung                                                                                            |
|----------|----------|---------------------------------------------------------------------------------------------------------|
| USER     | Konto    | Das Argument identifiziert eine Mailbox.                                                                |
| PASS     | Passwort | Das Passwort enthält ein Mailbox-spezifischen Code (Passwort).                                          |
| STAT     |          | Liefert die Anzahl der gespeicherten Mails und die Grösse der Mailbox zurück (in Byte).                 |
| LIST     |          | Liefert die Nummer und Grösse (in Bytes) aller Mails zurück.                                            |
| LIST     | Nummer   | Liefert die Grösse (in Bytes) dieser Mail.                                                              |
| RETR     | Nummer   | Gibt die Mail mit der als Argument übergebenen Nummer aus.                                              |
| DELE     | Nummer   | Löscht die Mail mit der übergebenen Nummer.                                                             |
| NOOP     |          | Bewirkt die Antwort "+OK". Dient zur Aufrechterhaltung der Verbindung, ohne dass ein Time-out auftritt. |
| RSET     |          | Setzt die aktive Verbindung zurück. Noch nicht ausgeführte Änderungen werden verworfen.                 |
| QUIT     |          | Beendet die Verbindung und führt alle gespeicherten Änderungen aus.                                     |

Wir empfangen nun eine Email, via Telnet, durch die direkte Abfrage des Postfaches auf den Server der das Email Konto unterhält.

[Start], [Ausführen], **TELNET**, [OK], [Verbinden], [Hostname:]**pop.clinch.ch**, [Anschluss:]**110**, [OK]

| Eingabe                            | State | Antwort:                                               |
|------------------------------------|-------|--------------------------------------------------------|
| Der POP3 Server meldet beim Start: | A     | +OK X1 NT-POP3 Server clinch.ch (IMail 9.07 1234567-1) |
| USER info                          | A     | +OK welcome                                            |
| PASS xxxxxxxxxxxxxxxx              | A     | +OK maildrop locked and ready                          |
| HELP                               | T     | +OK Normal POP3 commands allowed                       |
| XYZ                                | T     | -ERR illegal command                                   |
| LIST                               | T     | +OK 1 136<br>2 259                                     |
|                                    |       | .                                                      |
| STAT                               | T     | +OK 2 395                                              |
| LIST 1                             | T     | +OK 1 136                                              |
| RETR 1                             | T     | .... Text der Mail mit Header, MIME und allem ....     |
| DELE 1                             | T     | +OK                                                    |
| NOOP                               | T     | +OK                                                    |
| QUIT                               | U     | +OK POP3 Server saying Good-Bye                        |
|                                    | U     | Telnet Session wird beendet                            |

A = Authentisierungs Modus, T = Transaktions Modus, U = UpDate Modus

Der Server führt das Kommando DELE nicht unmittelbar aus. Die entsprechenden Emails werden als gelöscht markiert und erst bei beenden der Verbindung endgültig vom Server gelöscht. Hat man eine Nachricht zum Löschen gekennzeichnet, möchte dies jedoch rückgängig machen, führt man das Kommando RSET aus. Der Server verwirft alle noch nicht ausgeführten Operationen.

Sendet der Client das QUIT-Kommando, wechselt die Verbindung in den "Update State". Der Server trennt die TCP-Verbindung und führt alle gespeicherten Änderungen aus.

### 5.2.1.5 Telnet Abfrage per Batch Skript