**Scopul protocolului SMTP**

Simple Mail Transfer Protocol (prescurtat, **SMTP**; în traducere aproximativă *Protocolul simplu de transfer al corespondenței*) este un protocol simplu din [suită de protocoale de Internet](https://ro.wikipedia.org/w/index.php?title=Suit%C4%83_de_protocoale_de_Internet&action=edit&redlink=1" \o "Suită de protocoale de Internet — pagină inexistentă), care este folosit la transmiterea mesajelor în format electronic în rețea de calculatoare. SMTP folosește [portul de aplicație](https://ro.wikipedia.org/w/index.php?title=Port_de_aplica%C8%9Bie&action=edit&redlink=1" \o "Port de aplicație — pagină inexistentă) 25 TCP („smtp”) și determină adresa unui server SMTP pe baza înregistrării MX (*Mail eXchange*, „schimb de corespodență”) din configurația serverului DNS.

**Cum se poate verifica dacă serverul SMTP funcționează utilizînd linia de comandă?**

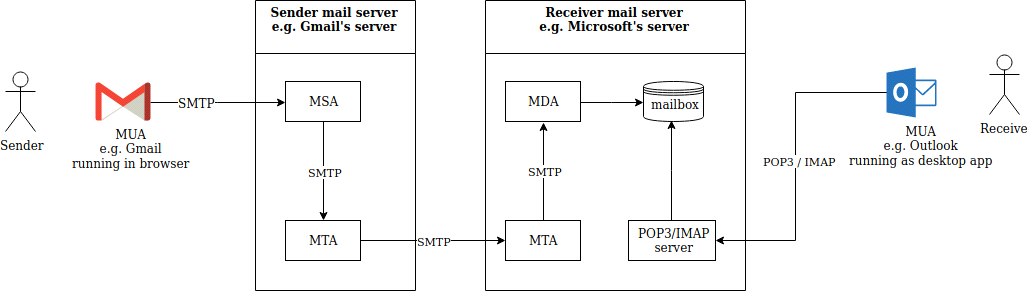
telnet smtp.gmail.com 465

**Care sunt comenzile SMTP**

* HELO - identificare computer expeditor;
* EHLO - identificare computer expeditor cu cerere de mod extins;
* MAIL FROM - specificarea expeditorului;
* RCPT TO - specificarea destinatarului ;
* DATA - conținutul mesajului;
* RSET – Reset;
* QUIT - termină sesiunea;
* HELP - ajutor pentru comenzi;
* VRFY - verifica o adresa;
* EXPN - expandează o adresa;

VERB - informatii detaliate.

**Pentru ce este nevoie de MUA, MSA, MTA și MDA**



**MUA (agent utilizator de e-mail)**

Aplicație client care permite primirea și trimiterea de e-mailuri. Poate fi o aplicație desktop cum ar fi Microsoft Outlook / Thunderbird / ... sau bazată pe web, cum ar fi Gmail / Hotmail / ... (aceasta din urmă se numește și Webmail).

**MSA (Agent de trimitere prin poștă)**

Un program de server care primește mail de la un MUA, verifică eventualele erori și îl transferă (cu SMTP) către MTA găzduit pe același server.

**MTA (agent de transfer de poștă)**

O aplicație server care primește mail de la MSA sau de la un alt MTA. Acesta va găsi (prin servere de nume și DNS) înregistrarea MX din zona DNS a domeniului destinatar pentru a ști cum să transferați poșta. Se transferă apoi poșta (cu SMTP) către un alt MTA (cunoscut sub numele de retransmisie SMTP) sau, dacă a fost atins serverul destinatarului, către MDA.

Exemple de MTA sunt Postfix, Exim, Sendmail, qmail, ...

**MDA (agent de livrare prin poștă)**

Un program de server care primește mail de la MTA-ul serverului și îl stochează în căsuța poștală. MDA este, de asemenea, cunoscut sub numele de LDA (Local Delivery Agent).

Un exemplu este Dovecot, care este în principal un server POP3 și IMAP care permite unui MUA să recupereze poștă, dar include și un MDA care preia poștă de la un MTA și îl livrează la căsuța poștală a serverului.

**Care este diferența dintre porturile 25, 465 și 587 ?**

Toate sunt porturi SMTP doar ca portul 25 este blocat sau restrictionat de majoritatea providerilor, pentru a reduce numarul de emailuri nedorite din reteaua lor; portul 465 nu a fost inregistrat ca un canal oficial de transmisie de catre IEFT ci de IANA, este sigur deoarece utilizeaza SSL. Portul 587 va reduce numarul de mesaje respinse

**Care este diferența dintre porturile 110 și 995 ?**

110- pop3 port necriptat

995- POP3 criptat

**Care este diferența dintre porturile 143 și 993 ?**

143- IMAP port nesecurizat

993- IMAP port securizat

**Cum funcționează protocolul SMTP ?**

Comunicarea intre client și server se realizeaza prin texte ASCII. Inițial clientul stabilește conexiunea către server și așteaptă ca serverul să-i răspundă cu mesajul “220 Service Ready” . Dacă serverul e supraîncărcat, poate să întarzie cu trimirea acestui raspuns. Dupa primirea mesajului cu codul 220 , clientul trimite comanda HELO prin care isi va indica identitatea. In unele sisteme mai vechi se trimite comanda EHLO, comanda EHLO indicand faptul că expeditorul mesajului poate sa proceseze extensiile serviciului și dorește să primească o listă cu extensiile pe care le suportă serverul. Dacă clientul trimite EHLO iar serverul îi răspunde ca aceasta comandă nu e recunoscută, clientul va avea posibilitatea să revină și să trimită HELO.

Odată ce comunicarea a fost stabilită, clientul poate trimite unul sau mai multe mesaje, poate incheia conexiunea sau poate folosi unele servicii precum verificarea adreselor de e-mail. Serverul trebuie să raspundă după fiecare comandă indicand astfel dacă aceasta a fost acceptată, dacă se mai asteaptă comenzi sau dacă există erori în scrierea acestor comenzi.

**Scopul protocoalelor POP3 și IMAP**

IMAP și POP sunt două metode pentru a accesa e-mailul

**Diferența dintre POP3 și IMAP**

IMAP este metoda recomandate atunci când aveți nevoie pentru a verifica e-mailurile din mai multe dispozitive diferite, cum ar fi un telefon, tabletă și laptop.

POP3 doar pe un dispozitiv.

**Cum să verificați dacă există o adresă de e-mail fără a trimite un e-mail ?**

Cu comanda smtp VERIFY

**Diferență dintre SSL și TLS**

SSL și TLS sunt adesea folosite interschimbabil deoarece sunt strâns legate. Ambele sunt protocoale de comunicare online și servesc aceluiași scop, acela de criptare a comunicațiilor între un server web și browser-ul utilizatorului prin schimb de chei publice și private pentru a stabili o sesiune sigură. Singura diferență dintre cele două este faptul că TLS a evoluat din tehnologia SSL și este o versiune mai sigură a SSL. De fapt, este TLS (și nu SSL) care este utilizat astăzi pentru a asigura comunicațiile online, dar chiar și atunci ne referim la acesta ca SSL, deoarece numele a rămas și este folosit mai frecvent.

**Schimbarea de la SSL la TLS**

SSL 2.0 a fost proiectat de Netscape (SSL 1.0 nu a fost niciodată publicat din cauza unor erori grave de securitate) și lansat în 1995. Cu toate acestea, datorită vulnerabilităților care au afectat această versiune, Netscape a fost forțat să proiecteze un SSL 3.0 mai bun și mai sigur, un an mai târziu. SSL 3.0 a fost folosit pe scară largă până de curând – pentru a fi mai precis, până în 2014 – când o vulnerabilitate majoră găsită de echipa de securitate Google l-a închis definitiv.

**În acel moment TLS a intrat în scenă**

Deși SSL 3.0 a fost utilizat pe scară largă până recent, TLS, care reprezintă Transport Layer Security, a ieșit din umbra tehnologiei SSL (Secure Sockets Layer). În total, patru versiuni diferite ale TLS au fost lansate până în prezent, cel mai recent TLS 1.3 aflat încă în stadiul de dezvoltare. Din punctul de vedere al securității, TLS 1.3 este considerat un progres major, deoarece este de așteptat să elimine diferite tehnici criptografice cunoscute a fi exploatabile. De exemplu, sursele sugerează că TLS 1.3 va permite cifrele numai dacă acetsea oferă Criptare autentificată cu date suplimentare (AEAD).

**TLS oferă mai multe avantaje**

TLS 1.3 este de așteptat să fie extrem de eficient și din acest motiv se așteaptă să scape de „reluarea sesiunii și renegocierea”, ambele fiind cunoscute ca reprezentând mai multe amenințări distincte legate de securitate în trecut. De asemenea, se sugerează că va renunța complet la compresia la nivel de TLS ca urmare a atacurilor de securitate precum CRIME, TIME și BREACH. Luând în considerare toți acești factori, se poate spune că TLS 1.3 va fi „mult mai sigur” decât versiunile anterioare și predecesorul său SSL.