

ESERCIZIO W3D2

Un'azienda sta cercando di inviare un file di grandi dimensioni da un computer all'altro attraverso una rete.

Utilizzando il modello ISO/OSI, descrivi i passaggi che il file deve attraversare per essere trasferito correttamente.

7- Application: Nel livello applicazione andiamo a concentrarci sulle applicazioni in grado di connettersi alla rete. Non avendo un quadro della natura del file inviato definisco sommariamente quali protocolli possono venir utilizzati:

- HTTP(Hypertext Transfer Protocol): Il protocollo utilizzato per il caricamento di una pagina web. Nel caso voglia caricare un file in una piattaforma, ad esempio di posta elettronica, E-learning, forum o blog innanzitutto è necessario che tale protocollo metta in comunicazione browser e server. Dal Client l'azienda invia una richiesta POST al server per trasferire i dati su internet.
- SFTP(SSH File Transfer Protocol): Il protocollo applicativo usato per il trasferimento dei file. A differenza del più semplice FTP, SFTP offre possibilità di manipolazione, grazie al trasferimento sicuro offerto dal protocollo SSH. Trattandosi di dati inviati da un'azienda, è logico pensare che quest'ultima voglia proteggere al meglio le sue risorse.
- SMTP(simple mail transfer protocol): Questo protocollo viene usato per trasferire un email da un utente ad un altro grazie al sostegno di un User Agent(Yahoo, Gmail, servizi di posta nativi al sito web etc), indipendentemente dalle caratteristiche hardware e software. Visto che un'azienda vuole inviare un file da un computer ad un altro, si affida al servizio di posta elettronica.
- DNS(domain name system): Tale protocollo si occupa di convertire il nome di dominio digitato nel browser aziendale in IP. Tutto ciò è possibile grazie alle associazioni name:IP(Record A) contenute nel database del server DNS.

6- Presentation: Nel livello presentazione il file inviato dall'azienda, che può essere di formato JPG, RAW, MP4, SVG, ZIP, PDF, DOCX verrà convertito in linguaggio comune per tutte le macchine. Un esempio di codifica può essere ad esempio ASCII, che traduce i messaggi testuali digitati dal computer aziendale. I dati infine vengono compressi e criptati da protocolli come:

- HTTPS: Questo protocollo a differenza di HTTP offre un canale di comunicazione sicuro protetto dalla crittografia asimmetrica.
- TLS(Transport Layer Security): Questo protocollo protegge i dati sensibili inerenti alle connessioni internet e ai link condivisi tra clients e server.
- PGP(Pretty Good Privacy): Una standard di crittografia che supporta in modo sicuro autenticazione e privacy.
- S/MIME(Secure Multipurpose Internet Mail Extensions): Un altro standard per la crittografia asimmetrica e la firma digitale di messaggi di posta elettronica. Esso supporta il servizio SMTP con la possibilità di trasferire dati non testuali, come immagini, video e audio.

5- Session: Il livello presentazione si occupa di aprire, mantenere ed infine chiudere la sessione tra client e server. Quest'ultima può essere inizializzata tra il client aziendale e, per esempio, un server DNS, HTTP oppure User Agent. La sincronizzazione inoltre salverà dei checkpoint intermedi per non perdere le informazioni nel caso di interruzione. Esempi di protocolli usati nel livello sono:

- ISO-SP(OSI Session Layer Control): In caso di perdita connessione, questo protocollo cercherà di recuperare la sessione perduta.
- SCP(Session Control Protocol): Permette a client e server di intrattenere numerose conversazioni lungo un canale TCP.

4- Transport: Il livello trasporto segmenterà il grande file in pezzi più piccoli per facilitare il trasporto, dopo di che instaurerà un canale

logico tra le parti in comunicazione. Trattandosi di un file aziendale sappiamo già quale potrebbe essere la scelta migliore, però è sempre meglio specificare i canali disponibili:

- UDP(User Datagram Protocol): Detto anche protocollo connectionless, UDP non ha bisogno di instaurare un canale di comunicazione. Risulta più leggera e veloce del TCP, ma non garantisce che i dati arrivino a destinazione.
- TCP(Transmission Control Protocol): Detto anche protocollo connection oriented, TCP crea un canale di scambio prima ancora di procedere all'invio dei dati, inoltre controlla il flusso per assicurare il file al destinatario. Molti protocolli superiori, come HTTPS e S/MIME, si affidano all'SCP, che utilizza come canale proprio il TCP.

3- **Network:** Il livello rete metterà in comunicazione il computer aziendale con qualsivoglia server o end Host. Per farlo si affiderà all'indirizzo IP(Internet Protocol) assegnato ai vari dispositivi. Grazie alla routing table, il router della LAN o WAN aziendale sceglierà il percorso di rete più appropriato per inviare i datagrammi a destinazione. I protocolli usati nel livello 3 possono essere:

- IPV4(Internet Protocol V4): La versione più utilizzata al momento della suite di protocolli internet. Tale indirizzo è composto da 32 bit divisi in 4 otteti ed identifica i dispositivi durante i vari hop.
- ICMP(Internet Control Message Protocol): Tutti i dispositivi di rete fanno uso di questo protocollo. Si occupa di testare la connettività tra indirizzi IP, inviando messaggi di errore o di avvenuta ricezione.
- ARP(Address Resolution Protocol): In un rete Lan, l'ARP identifica il MAC di un dispositivo connesso utilizzando come indizio il suo IP. Invia una richiesta ad un dominio broadcast fino a che non gli ritorna indietro una risposta.
- RIP(Routing Information Protocol): Si tratta di un protocollo di routing di tipo distance vector. Esso previene il looping durante gli Hop, andando a settare il limite massimo di 15 hop.

2- Data Link: Il livello Data Link si occupa della connettività Node to Node, controlla il flusso di dati e rileva gli errori. Riceve i datagrammi del livello 3 e li trasforma in frame. Il MAC address, trovato tramite messaggi ARP, guiderà ulteriormente i vari pacchetti. Alcuni protocolli del Data Link sono:

- **MAC(Media Access Control):** Definito anche BIA(burned in address), è un indirizzo che identifica univocamente le schede di rete dei dispositivi. Il MAC rappresenta lo standard per inviare i pacchetti di una rete su un mezzo fisico.
- **ARP:** In teoria sarebbe un protocollo di livello 2, ma collabora attivamente con il livello 3 per identificare i dispositivi durante i salti.
- **HDLC (High level data link control):** Sarebbe un protocollo a riempimento di bit. Per evitare le sequenze di terminazione inserisce tra le sequenze degli 0 aggiuntivi. Permette la comunicazione multipunto tra due dispositivi.
- **LLC(Logical Link Control):** Una versione più semplice di un HDLC. Controlla i dati, conferma le ricezioni e rivela gli errori se li trova.
- **802.3(Ethernet Protocol):** Permette la comunicazione tra due dispositivi collegati tramite LAN o rete cablata. L'ethernet è ciò che consente lo scambio di pacchetti frame con lo strato fisico.

1- Physical: Una volta raggiunto il livello più basso del modello OSI, i frame vengono convertiti in onde radio(WIFI) o Bit(connessione cablata), a seconda del mezzo trasmissivo. Tra i protocolli usati abbiamo:

- **802.3:** La famiglia 802.3 ovviamente compare qui. A seconda della tipologia di cavo avremo una qualità trasmissiva differente. La fibra ottica singlemode 802.3an, ad esempio, distribuisce 10 gbs su ben 30km di cavo.
- **802.11:** Definisce gli standard di trasmissione per le reti WLAN.

Una volta superati tutti i livelli del mittente, i file viaggiano in formato elementare fin dentro il livello fisico del ricevente. Da qui in poi parte lo spaccettamento dei dati.

- 1- Physical: Il file viaggia attraverso il mezzo fisico del ricevente. Da bit o onde radio, i dati vengono convertiti in pacchetti frame, pronti ad essere inviati al secondo livello.
- 2- Data Link: Nel secondo livello i frame vengono controllati per eventuali errori di trasmissione o indirizzamento.
- 3- Network: Il livello network collabora con il data link per assicurare la trasmissione dei datagrammi tramite indirizzo IP.
- 4- Transport: Nel livello trasporto viene aperto il canale di comunicazione tra mittente e ricevente. Il protocollo TCP assicura che i dati arrivino senza perdite. I segmenti di dati sono ricomposti in un file di grandi dimensioni.
- 5- Session: Il livello sessione mantiene aperto il canale di comunicazione tra client aziendale/user agent e ricevente, assicurandosi di salvare dei check point durante lo scambio.
- 6- Presentation: I dati provenienti da session sono convertiti in un formato comprensibile al ricevente (caratteri testuali, JPG, MP4, PDF etc). Quest'ultimi inoltre vanno incontro a decompressione e decriptazione.
- 7- Application: Il file aziendale raggiunge finalmente il computer del ricevente attraverso le applicazioni di rete.