W3D1 Pratica 2: invio di un file.

Nota: in questa prima parte vengono descritti i passaggi per il trasferimento di un file di grandi dimensioni tra due computer di una stessa azienda, collegati da una rete LAN. Il trasferimento di un file tramite una rete privata aziendale viene preso in considerazione nell'esercizio facoltativo.

Il modello ISO/OSI aiuta a comprendere come viene trasferito un file da un computer A ad un computer B in una rete LAN aziendale. A livello fisico, il passaggio dei dati avviene via wireless o tramite cavi, mentre nel layer del data link la comunicazione avviene grazie al MAC address, ovvero l'indirizzo fisico che identifica in modo univoco un device e che viene assegnato alla sua scheda di rete. Lo switch utilizza il MAC address per mettere in contatto computer nella stessa rete e sarebbe sufficiente se il computer B si trovasse nella stessa rete di A. Immaginando però che il computer B si trovi in una sottorete diversa da quella in cui si trova A, è necessario l'utilizzo di un router, ovvero di un dispositivo del livello di rete, il layer 3, che serve a instradare i pacchetti di dati anche su reti diverse. Il router si basa sugli indirizzi IP e utilizza la routing table per capire verso quale rete inviare i pacchetti di dati. Il computer A crea quindi un pacchetto con l'indirizzo IP di B come destinatario e l'indirizzo MAC dell'interfaccia di rete dello switch, il quale riceve il pacchetto e lo invia al router, indicando il proprio indirizzo MAC come sorgente e l'indirizzo MAC dell'interfaccia del router ad esso collegato come destinatario. Il router consulta la routing table ed indirizza i dati verso la rete giusta, creando un pacchetto datagram con l'indirizzo della sua interfaccia come origine e l'indirizzo MAC dell'interfaccia dello switch dell'altra rete come destinazione. Lo switch della rete di B riceve il pacchetto e lo indirizza verso il computer B, creando un pacchetto che ha come indirizzo MAC sorgente quello dell'interfaccia dello switch e l'indirizzo MAC di B come indirizzo MAC di destinazione. È importante ricordare che mentre gli indirizzi IP restano invariati durante tutto il processo, gli indirizzi MAC cambiano ad ogni hop per riportare l'indirizzo MAC esatto della scheda di rete sorgente e di destinazione. Con il protocollo ARP, address resolution protocol, è possibile ricostruire le associazioni tra IP e MAC address, utili per esempio per conoscere il MAC address di un computer nella stessa rete del quale si conosce l'IP. Trattandosi di file di grandi dimensioni e probabilmente di documenti importanti, nel layer del trasporto è necessario scegliere il protocollo TCP, transmission control protocol. Il livello di trasporto crea un canale di collegamento tra i due computer e il protocollo TCP è adatto per trasferire file importanti perché è connection oriented, per cui stabilisce un canale di comunicazione fin da subito e prevede dei meccanismi per il controllo dei dati, garantendo la consegna di tutti i pacchetti senza perdite ed avvisando in caso di perdita di qualche pacchetto. TCP stabilisce il canale di contatto tra i due computer tramite il three-way-handshake. Il livello di sessione va a creare una sessione necessaria per la comunicazione tra due computer e il livello della presentazione prepara i dati prima del loro transito. In questo livello è possibile cifrare i dati, assicurandosi così che solo i soggetti interessati possano accedervi in sicurezza. La cifratura a chiave simmetrica è più rapida della cifratura a chiave asimmetrica, ma è fondamentale che la chiave simmetrica venga scambiata in totale sicurezza, mentre la cifratura a chiave asimmetrica è più lenta ma

più sicura, specialmente se la chiave privata rimane riservata. Il layer dell'applicazione interagisce direttamente con le applicazioni dell'utente, fornendo servizi di interfaccia per gli applicativi. Trattandosi del trasferimento di un file, si utilizza FTP, file transfer protocol che gestisce il trasferimento di dati come file anche di grandi dimensioni tra host e che è basato sul protocollo di trasporto TCP. Il file di grandi dimensioni, che era stato precedentemente suddiviso in pacchetti più piccoli, giunge quindi a destinazione nel computer B.

Esercizio facoltativo: la rete privata aziendale rappresenta una scelta sicura per collegare più sedi distanti di una stessa azienda, come se tutti i computer fossero collegati alla stessa LAN, e per far sì che la connessione di chi lavora da remoto sia sicura come se si trovasse fisicamente in ufficio. Tra i vantaggi di una VPN c'è il fatto che l'indirizzo IP viene nascosto al provider di servizi internet e ad altre parti terze, inoltre i dati sono protetti perché viaggiano in tunnel sicuri grazie al tunnelling, che consiste nella creazione di una connessione temporanea autenticata nella quale viaggiano pacchetti IP protetti. Per il caso proposto dall'esercizio è utile pensare ad una VPN site-to-site, usata soprattutto per connettere più filiali tra loro, ognuna delle quali possiede la propria LAN, e per creare uno spazio di condivisione di file sicuro, come se tutti gli host si trovassero nella stessa LAN. Nel layer fisico non ci sono cambiamenti da segnalare, la connessione avviene principalmente via wireless o via cavo. A livello del data link e della rete, nel caso dell'esercizio proposto è necessario descrivere la connessione dei due host al server VPN, tramite switch al livello 2 e tramite router al livello 3. Il Pc A nella sede principale si connette al server VPN tramite lo switch della rete aziendale e tramite il router a livello di rete, seguendo un procedimento simile a quello descritto precedentemente. Anche il computer B della sede remota si collega alla VPN aziendale, utilizzando lo switch e successivamente il router. Ora che entrambi gli host sono connessi al server VPN, quando il PC A invia il proprio file, passa dallo switch della sua sottorete e raggiunge il router, che instrada i pacchetti verso il server VPN. Il server VPN crea un canale sicuro per l'invio di questo file, in cui i vari pacchetti sono protetti durante il transito da un host all'altro. Dal server i dati vanno al router, poi allo switch e infine raggiungono l'host della sede remota, connesso alla VPN proprio come se si trovasse in ufficio. Per quanto riguarda il layer del trasporto, il protocollo da usare è sempre TCP, come nel caso precedente e non vi sono cambiamenti nei layer della sessione e della presentazione. Per quanto riguarda il livello dell'applicazione, il trasferimento avviene tramite protocollo FTP, file transfer protocol, basato sul protocollo TCP e che consente l'arrivo di tutti i pacchetti a destinazione.