

Modulo 11 – Livelli Transport e Application del modello TCP/IP

Upon completion of this module, the student will be able to perform tasks related to the following:

11.1 TCP/IP Transport Layer

11.2 TCP/IP Application Layer

11.1 TCP/IP Transport Layer

11.1.1 Introduzione al transport layer

Lo scopo primario del livello transport, livello 4 del modello OSI, è di trasportare e regolare il flusso di informazioni (velocità) dalla sorgente alla destinazione in modo accurato ed affidabile. Questo è raggiunto tramite le finestre variabili (sliding windows), i numeri di sequenza e le conferme (acknowledgment). Il livello transport stabilisce una connessione logica tra i 2 dispositivi che devono passarsi i dati, segmenta i dati in trasmissione e li riassume in ricezione. I servizi del livello transport comprendono:

- Segmentation of upper-layer application data
- Establishment of end-to-end operations
- Transport of segments from one end host to another end host
- Flow control provided by sliding windows
- Reliability provided by sequence numbers and acknowledgments

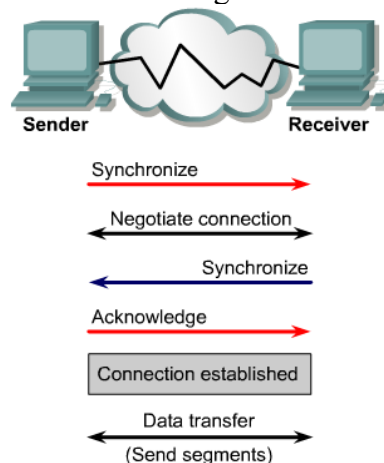
TCP/IP è una combinazione di 2 protocolli: IP opera a livello 3 ed è connectionless, TCP opera a livello 4 ed è connection oriented, fornisce il controllo di flusso e l'affidabilità. Assieme costituiscono la base di un'intera suite di protocolli.

11.1.2 Controllo di flusso

Il controllo di flusso evita che i dati arrivino al ricevente ad una velocità maggiore di quanto esso riesca a sopportare, per cui i dati andrebbero persi. I 2 host comunicano tra di loro e stabiliscono una velocità di trasferimento dei dati adeguata per entrambi.

11.1.3 Panoramica sullo stabilimento, mantenimento e terminazione di una sessione

Più applicazioni possono condividere contemporaneamente lo stesso livello transport, questo è detto multiplexing delle conversazioni dei livelli superiori. Prima che inizi il trasferimento dei dati occorre che si stabilisca la connessione e che avvenga la sincronizzazione.



La congestione può avvenire durante il trasferimento dei dati per vari motivi:

- Un computer veloce può trasmettere ad una velocità maggiore di quella consentita dalla rete
- Se molti computer mandano dati allo stesso computer, questi non riesce a seguire tutte le comunicazioni

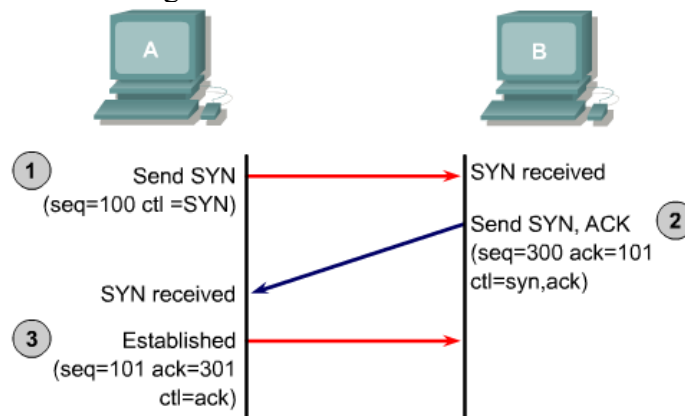
Quando i pacchetti arrivano troppo velocemente sono salvati temporaneamente in memoria, se il traffico prosegue a lungo la memoria si esaurisce e i pacchetti in eccesso vengono buttati.

Invece di perdere dati il livello transport invia un messaggio “not ready” al trasmettitore il quale cessa di trasmettere finché non riceve un messaggio “ready”.

Alla fine del trasferimento dei dati l’host che trasmette invia un segnale che indica la fine delle trasmissioni ed il termine della connessione.

11.1.4 Three-way handshake

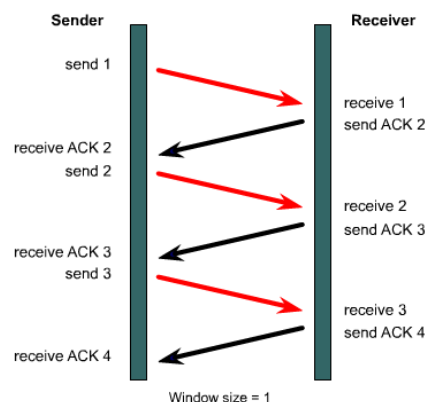
TCP è un protocollo connection-oriented per cui richiede che venga stabilita una connessione prima che inizi il trasferimento dei dati. Per far questo i 2 host devono sincronizzare i loro ISN (Initial Sequence Number): mandano dei segmenti con un bit di controllo detto SYN ed il numero ISN.



La sincronizzazione richiede che ogni parte invii il proprio ISN e riceva una conferma (ACK). Lo scambio delle informazioni avviene come nella foto precedente ed è detto three-way handshake.

11.1.5 Windowing

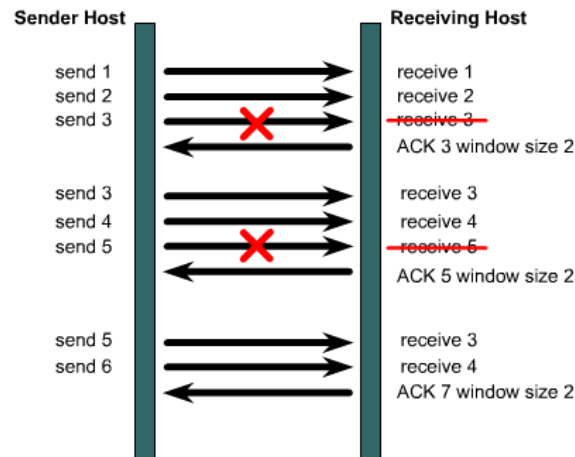
I pacchetti di dati potrebbero essere trasmessi in sequenza uno per volta e prima di inviare il successivo aspettare la conferma.



Se per ogni pacchetto occorre aspettare la conferma si rallenta la trasmissione, per cui molti protocolli connection-oriented permettono la trasmissione di più pacchetti assieme. Il numero di pacchetti che si possono trasmettere prima di ricevere la conferma è detto window size o semplicemente window. TCP aspetta una conferma (ACK) con un numero che rappresenta il successivo pacchetto che il ricevitore si aspetta di ricevere. Windowing si riferisce al fatto che la window size è negoziata dinamicamente durante la sessione TCP. Windowing è un meccanismo di controllo di flusso. Se la window size fosse 3 il trasmettitore invia 3 pacchetti dopodiché si ferma

ad aspettare ACK, se i 3 pacchetti sono arrivati correttamente l'ACK contiene il numero del 4° pacchetto.

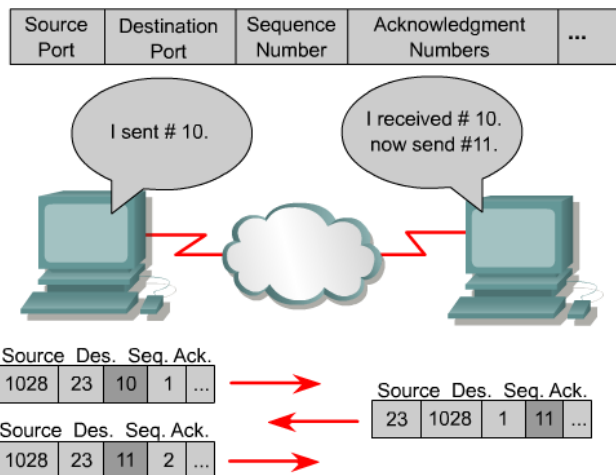
La window size può variare durante la connessione, ogni ACK contiene il numero di bytes che il ricevente può accettare. TCP mantiene anche una finestra di controllo della congestione, all'inizio ha le stesse dimensioni di quella del ricevitore, se un pacchetto viene perso, forse a causa della congestione della rete, la finestra viene dimezzata, per cui questa finestra viene espansa o contratta come necessario.



11.1.6 Acknowledgment

La trasmissione affidabile garantisce che un insieme di dati siano spediti ad un altro dispositivo senza duplicati, modifiche o perdite. L'ACK positivo con la ritrasmissione sono una tecnica per garantire l'affidabilità. Quando il trasmittente invia un pacchetto avvia un timer, al suo scadere se non è arrivato l'ACK il pacchetto viene ritrasmesso.

Ogni pacchetto viene numerato prima dell'invio in modo che il ricevitore possa riassemblare i segmenti. Se un segmento manca ne viene richiesta la ritrasmissione.



11.1.7 TCP (Transmission Control Protocol)

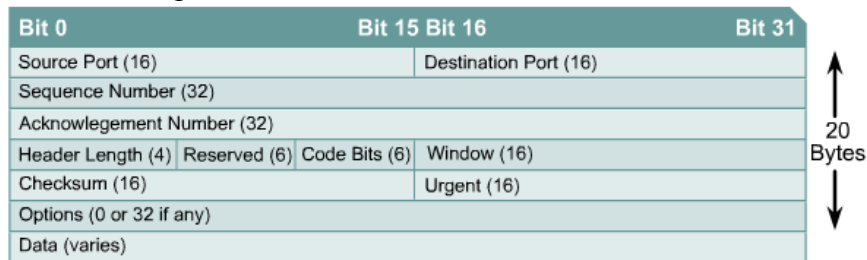
TCP è un protocollo connection-oriented di livello 4 che fornisce una trasmissione dati affidabile in modo full-duplex. Essendo connection-oriented viene stabilita una connessione tra i dialoganti prima che inizi il trasferimento dei dati. TCP è responsabile per dividere i messaggi in segmenti, riassemblarli a destinazione, ritrasmettere quello che non è stato ricevuto. TCP fornisce un circuito virtuale tra le applicazioni degli utenti finali.

I protocolli che TCP include sono:

- FTP (File Transfer Protocol)

- HTTP (Hypertext Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- Telnet

Un segmento TCP è così composto:



- **Source port** – Number of the calling port
- **Destination port** – Number of the called port
- **Sequence number** – Number used to ensure correct sequencing of the arriving data
- **Acknowledgment number** – Next expected TCP octet
- **HLEN** – Number of 32-bit words in the header
- **Reserved** – Set to zero
- **Code bits** – Control functions, such as setup and termination of a session
- **Window** – Number of octets that the sender is willing to accept
- **Checksum** – Calculated checksum of the header and data fields
- **Urgent pointer** – Indicates the end of the urgent data
- **Option** – One option currently defined, maximum TCP segment size
- **Data** – Upper-layer protocol data

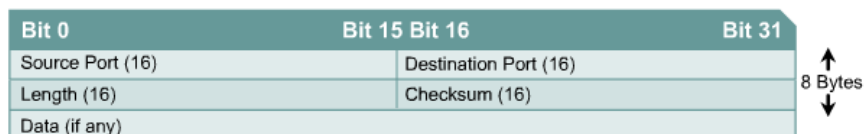
11.1.8 UDP (User Datagram Protocol)

UDP è un protocollo connectionless di livello 4, è un protocollo semplice che scambia datagrammi senza ACK e senza garanzia di affidabilità. Il rilevamento di errori e la ritrasmissione deve essere gestita da protocolli di livello più alto. UDP non ha windowing o ACK. UDP è fatto per applicazioni che non necessitano di avere sequenze di segmenti.

UDP include:

- TFTP (Trivial File Transfer Protocol)
- SNMP (Simple Network Management Protocol)
- DHCP (Dynamic Host Control Protocol)
- DNS (Domain Name System)

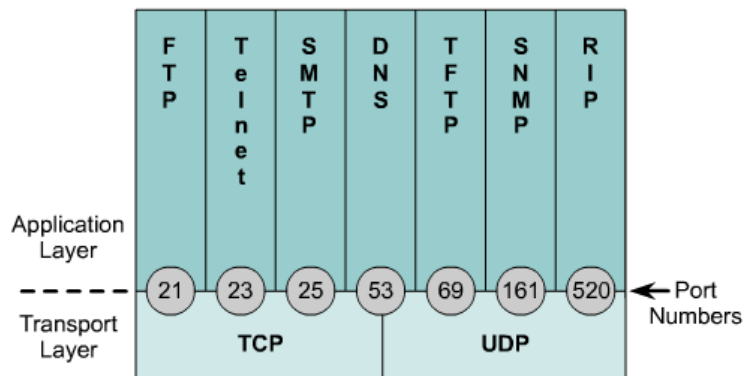
Un segmento UDP è così composto:



- **Source port** – Number of the calling port
- **Destination port** – Number of the called port
- **Length** – Number of bytes including header and data
- **Checksum** – Calculated checksum of the header and data fields
- **Data** – Upper-layer protocol data

11.1.9 Numeri di porta TCP e UDP

Sia TCP che UDP usano i numeri di porta (socket) per passare informazioni ai livelli superiori. I numeri di porta servono per tener traccia di conversazioni differenti che passano nella rete contemporaneamente. I numeri di porta sono stabiliti da IANA (Internet Assigned Numbers Authority). Ad esempio le applicazioni FTP usano i numeri 20 e 21, 20 per i dati e 21 per i controlli.



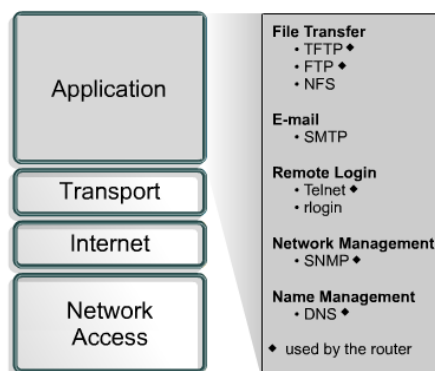
I numeri di porta sotto 1024 sono riservati per determinate applicazioni, mentre quelli sopra 1024 sono assegnati dinamicamente a quelle applicazioni che non hanno un numero di porta specifico.

11.2 Il livello application

11.2.1 Introduzione al livello application TCP/IP

Quando fu progettato il modello TCP/IP i livelli presentation e session del modello OSI furono inglobati nel livello application. Questo fornisce maggiore flessibilità agli sviluppatori di software del livello application. I protocolli principali del livello application sono:

- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
- Telnet



11.2.2 DNS

Internet è costruito su uno schema di indirizzamento gerarchico per cui il routing si basa non su un indirizzo singolo ma su classi di indirizzi. Il problema che si crea per l'utente è associare ad un ito Internet il suo indirizzo IP. Il DNS (Domain Name System) è un sistema usato su Internet per tradurre i nomi dei domini e i loro nodi pubblici in indirizzi IP. Un dominio è un gruppo di computer associati dalla loro posizione geografica o dal tipo di business. Un nome di dominio è una

stringa di caratteri, numeri o entrambi. Ci sono più di 200 domini top-level su Internet, ad esempio .us per gli Stati Uniti, .it per l'Italia. Ci sono anche nomi generici, ad esempio:

- .edu – educational sites
- .com – commercial sites
- .gov – government sites
- .org – non-profit sites
- .net – network service

11.2.3 FTP e TFTP

FTP è un servizio connection-oriented affidabile che usa TCP per trasferire i file tra sistemi che supportano FTP. Lo scopo principale di FTP è copiare file, FTP stabilisce prima una connessione di controllo, quindi stabilisce una seconda connessione per trasferire i dati. Il trasferimento dei dati è o in modo ASCII o in modo binario, questi modi determinano la codifica usata per i dati, che nel modello OSI appartiene al livello presentation. Alla fine del trasferimento del file la connessione dei dati è terminata automaticamente, quando l'intera sessione di copia o trasferimento è completa, viene terminata anche la prima connessione e finisce la sessione.

TFTP è un servizio connectionless che usa il protocollo UDP. TFTP è usato dai router per trasferire i file di configurazione ed i sistemi operativi (Cisco IOS image). TFTP è un sistema piccolo e facile da implementare, per cui mancano molte possibilità di FTP: può leggere, scrivere o inviare file da o verso un server remoto, ma non può listare le directory o autenticare gli utenti. Opera a velocità più alta di FTP.

11.2.4 HTTP

HTTP (Hypertext Transfer Protocol) lavora con il World Wide Web, che è la parte di Internet che è più usata e che è cresciuta più velocemente. Un Web browser è un'applicazione client-server che preenta i dati in formati multimediali sulle pagine Web. Le pagine Web sono create con un formato chiamato HTML (Hypertext Markup Language). Gli hyperlinks permettono una facile navigazione, quando si fa clic su un hyperlink dirige il browser su una nuova pagina. Ogni pagina Web ha un suo URL (Uniform Resource Locator), ad esempio <http://www.cisco.com/edu/>, la parte http:// dice al browser il protocollo da usare, la seconda parte è il nome della macchina specifica con uno specifico indirizzo IP. Per determinare l'indirizzo IP corrispondente al nome usa il DNS. Quando si vuole leggere una pagina i livelli superiori del client iniziano una sessione col Web server. Il client fa la richiesta della pagina che vuole, il server risponde inviando tutto il testo, l'audio, il video, i file grafici di quella pagina. Il client riassume il tutto e chiude la sessione.

http://	www.	cisco.com	/edu/
Identifies to the browser what protocol should be used.	Identifies the hostname or name of a specific machine	Represents the domain entity of the web site.	Identifies the folder where the web page is located on the server. Also since no name is specified, the browser will load the default page identified by the server

11.2.5 SMTP

I server di e-mail comunicano usando il protocollo SMTP (Simple Mail Transfer Protocol) per inviare e ricevere posta. SMTP trasporta i messaggi in formato ASCII usando TCP.

Quando un server mail riceve un messaggio per un client, lo memorizza ed aspetta che il client lo scarichi. I più popolari protocolli usati dai client per scaricare la posta sono POP3 e IMAP4, entrambi usano TCP per trasportare i dati. Invece per inviare la posta un client in genere usa SMTP. E' bene testare la posta sia in trasmissione che in ricezione, perché a volte funziona solo 1 dei 2.

Il protocollo SMTP non offre molta sicurezza e non richiede autenticazione.

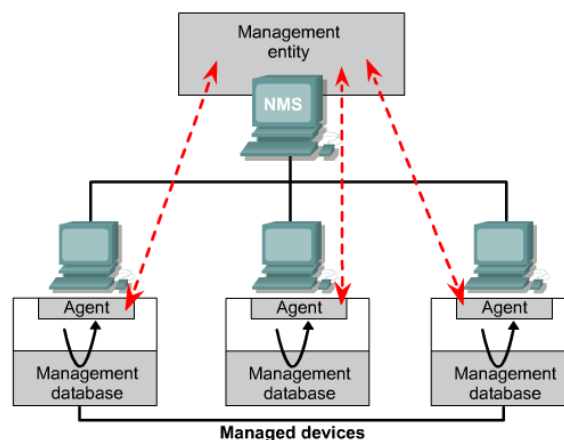
11.2.6 SNMP

SNMP (Simple Network Management Protocol) è un protocollo di livello application che facilita lo scambio di informazioni di gestione tra dispositivi di rete.

SNMP permette agli amministratori di rete di gestire le performance della rete, trovare e risolvere problemi di rete e pianificare la crescita della rete. SNMP usa UDP come protocollo di livello 4.

Una rete gestita da SNMP consiste di 3 componenti chiave:

1. NMS (Network Management System): esegue applicazioni che fanno il monitoraggio e controllano i dispositivi. In una rete possono esserci più NMS.
2. Managed devices: sono nodi della rete che contengono un agente SNMP, collezionano e memorizzano informazioni e le rendono disponibili a NMS usando SNMP. I managed devices possono essere router, server, switch, hub, computer o stampanti.
3. Agents: sono moduli software che risiedono nei managed devices. Un agent ha una conoscenza locale delle informazioni e le traduce in una forma compatibile con SNMP.



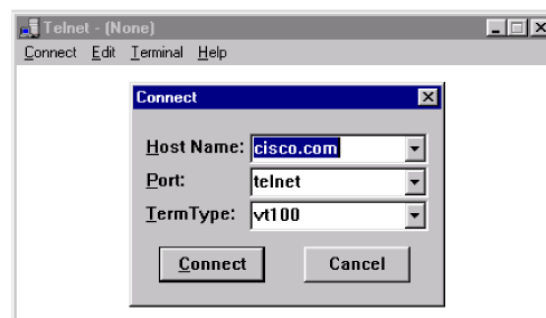
11.2.7 Telnet

Un client Telnet dà la possibilità di fare il login con un server Telnet remoto e quindi eseguire comandi tramite una linea di comando. Il server Telnet usa un software speciale detto demone.

Per fare una connessione da un client in genere si apre una dialog box dove viene chiesto l'host name e il tipo di terminale. L'host name è l'indirizzo IP o il nome DNS del computer remoto. Il tipo di terminale descrive il tipo di emulazione di terminale che Telnet deve usare.

Telnet invia i tasti premuti dal client e invia le schermate risultanti sul monitor locale.

Telnet lavora a livello application del nodello TCP/IP e ai 3 livelli superiori del modello OSI: il livello application tratta i comandi, il livello presentation si occupa del formato, in genere ASCII, il livello session trasmette.



A Telnet session starts like any other communication program: with an address to connect to a host computer. The address may be an IP address (192.168.10.11) or a domain name.