

CCNA_1 (Versione 3.1) Networking basics

Cap. 11 Livelli Trasporto e Applicazione

ithum

Marco Ciampi
m.ciampi@ithum.it



Cap. 11 Livelli Trasporto e Applicazione

Ithum Learning License

Licenza d'uso del materiale didattico

Questo documento e tutto il materiale prodotto da Ithum S.r.l. e dai suoi collaboratori in qualità di autori originari costituisce una "opera" intellettuale protetta dal diritto d'autore e/o dalle altre leggi applicabili.

Tale opera (si veda anche l'appendice *Materiale allegato*) è messa a disposizione sulla base dei termini della presente *Ithum Learning License* ovvero della *Licenza concessa da Ithum Srl per l'utilizzo del materiale prodotto*.

È proibita ogni utilizzazione dell'opera che non sia autorizzata ai sensi della presente licenza o del diritto d'autore.

Ithum Srl e gli autori originari, in qualità di licenzianti, concedono l'utilizzo dell'opera con i diritti ed i doveri di seguito elencati.

Con il semplice esercizio sull'opera di uno qualunque dei diritti di seguito elencati, si accetta e ci si impegna a rispettare integralmente ed a far rispettare a terzi i termini e le condizioni della presente licenza.

L'opera può essere riutilizzata così come è oppure riadattata alle proprie esigenze come specificato da quanto segue.

Ithum S.r.l. e gli autori originari concedono:

- L'utilizzo dell'opera per fini educativi ed informativi personali;
- La riproduzione, distribuzione, comunicazione e/o esposizione in pubblico, rappresentazione, esecuzione o recitazione dell'opera;
- La creazione di opere derivate;

Alle seguenti imprescindibili condizioni:

1. riconoscere sempre e comunque il contributo di Ithum S.r.l. e dell'autore originario, dandone sempre evidenza scritta o comunque documentabile;
2. tener traccia sempre e comunque dei soggetti cui l'opera viene distribuita e comunicarla tempestivamente ad Ithum ed all'autore originario;
3. chiarire e far sottoscrivere agli altri sempre e comunque, in occasione di ogni atto di utilizzo o distribuzione, i termini della presente licenza;
4. contattare preventivamente sempre Ithum S.r.l. e l'autore originario per negoziarne coinvolgimento e compensi in caso di utilizzo ai fini commerciali;
5. Se si ottiene il permesso documentato dal titolare del diritto d'autore (Ithum S.r.l. e l'autore originario) è possibile rinunciare ad alcune o tutte le precedenti condizioni.

Le utilizzazioni libere e gli altri diritti non sono in nessun modo limitate da quanto sopra.

Per qualsiasi informazione è possibile scrivere a formazione@ithum.it.



Il primo compito del layer di trasporto è di trasportare e regolare il traffico di informazioni dalla sorgente alla destinazione, in modo accurato ed affidabile.

Questo controllo ed affidabilità sono dati dalle sliding window, i sequencing numbers e gli acknowledgments.

Il transport layer fornisce servizi di trasporto dall'host sorgente a quello di destinazione, stabilendo una connessione logica tra gli end point di una rete.

I transport service segmentano e riassemblano diversi stream di applicazioni nello stesso data stream del transport layer. Quest'ultimo è colui che garantisce dei servizi per il trasporto end-to-end.

Reliable transport can accomplish the following:

- Ensure that segments delivered will be acknowledged to the sender
- Provide for retransmission of any segments that are not acknowledged
- Put segments back into their correct sequence at the destination
- Provide congestion avoidance and control

Il transport service include i seguenti servizi di base:

- Segmentazione dei dati di applicazione dei layer superiori
- Instaurazione delle operazioni end-to-end
- Trasporto dei segmenti da un end host ad un altro
- Controllo di flusso fornito dalle sliding windows
- Affidabilità data dai sequence numbers e gli acknowledgments

TCP/IP è la combinazione di due protocolli individuali; l'IP opera al layer 3 ed è connectionless e fornisce best-effort delivery nella rete; il TCP opera al livello 4, è connection oriented ed è colui che si occupa della reliability e del flow control.



Cap. 11 Livelli Trasporto e Applicazione

Flow Control

Il transport layer mentre manda segmenti dati prova ad assicurarsi che niente vada perso.

L'host ricevente, qualora fosse incapace di processare i dati alla velocità con cui arrivano, potrebbe essere una causa di perdita di dati, in quanto è obbligato a scartarli.

Il flow control evita il problema di overflow del buffer del receiving host.

TCP dà lo strumento per controllare il flusso attraverso la comunicazione tra gli host mittente e destinatario.

I due host quindi stabiliscono un data transfer rate che è raggiungibile da entrambi.

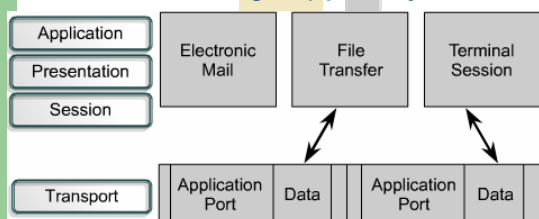


Cap. 11 Livelli Trasporto e Applicazione

Multiplexing delle "conversazioni"

Più applicazioni possono condividere la stessa transport connection, ovvero possono spedire segmenti dati su base primo arrivato, primo servito.

Questi segmenti possono essere instradati verso la stessa destinazione o verso differenti destinazioni; ci si riferisce a tale situazione come al multiplexing delle conversazioni degli upper-layer.



Una delle funzioni del transport layer è stabilire una sessione tra device similari al layer di applicazione. Un nodo inizializza la connessione che deve essere accettata dall'altro. La connessione si reputa stabilita solo dopo che la sincronizzazione è terminata.

Durante un trasferimento lo scambio di info è costante, proprio per verificare il corretto recapito dei dati.



Cap. 11 Livelli Trasporto e Applicazione

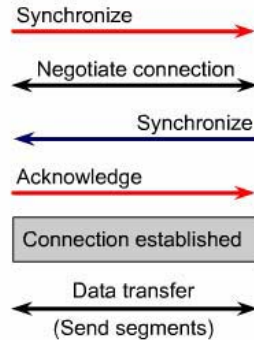
Perché ci sono le congestioni?

La figura mostra la tipica connessione, a cui precede una fase di instaurazione definita three-way handshake.

Le congestioni possono presentarsi durante un data transfer per due ragioni:

- Un computer “veloce” può generare traffico più rapidamente di quanto la rete non possa smaltirlo
- Più computer potrebbero voler spedire dati ad uno stesso computer

Se dei datagrammi arrivano troppo rapidamente all’host per essere processati “al volo” esso li mette in memoria. Se però il traffico continua fino all’esaurimento della memoria, allora i datagrammi che arriveranno in seguito saranno scartati.



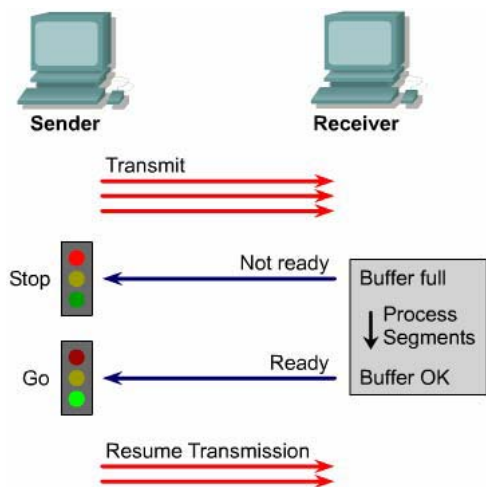
Cap. 11 Livelli Trasporto e Applicazione

Segnale di Not Ready

Invece di permettere la perdita di dati il layer di trasporto può mandare un’indicazione “non pronto”.

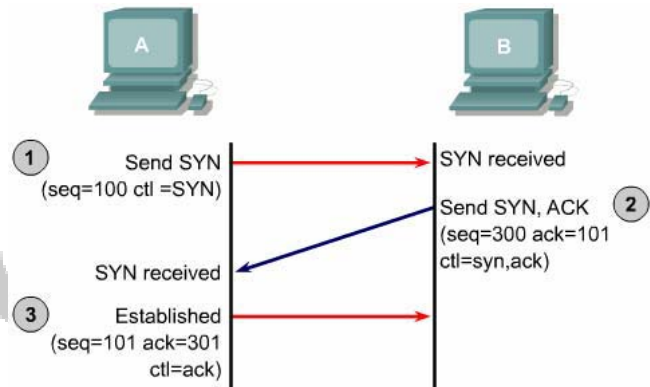
Nel momento in cui il destinatario sarà in grado di accogliere altri dati allora il mittente potrà trasmettere ancora.

Alla fine del trasferimento di dati il mittente manda un segnale di termine della trasmissione, che sarà appreso dal destinatario in modo che la connessione venga terminata.



Three-Way Handshake

1. A → B SYN—(A) la sequenza ha numero d'inizio X, il numero ACK è 0, Il bit di SYN è settato, quello di ACK no
 2. B → A ACK—(A) il numero della sequenza è X+1, il numero d'inizio sequenza di B è Y, il bit di SYN e di ACK sono settati
 3. A → B ACK—(B) il numero di sequenza di B è Y+1, il numero di sequenza di A è X+1, il bit di ACK è settato, quello di SYN no
- I numeri X ed Y sono detti ISN, Initial Sequence Number



Perché si usa il three-way handshake?

- Il three-way handshake è necessario perché i sequence number non sono collegati ad un clock generale della rete e i protocolli superiori supportati da TCP possono avere differenti meccanismi su come prendere gli ISN.
- Colui che riceve il SYN (B) non ha modo di sapere se il segmento arrivato è di una vecchia connessione, a meno che non ricordi l'ultimo numero di sequenza usato in una connessione, cosa non sempre possibile.



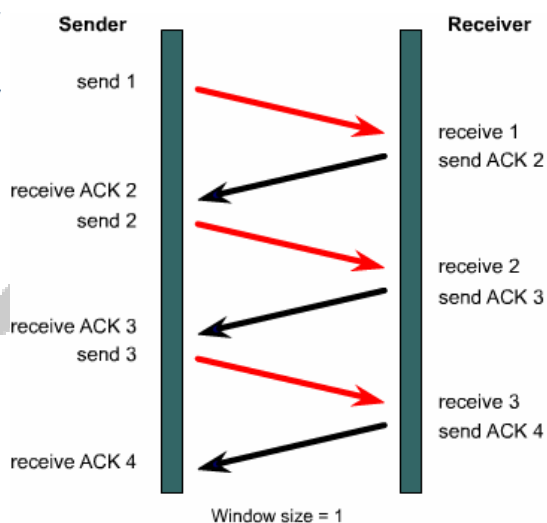
Spiegazione del protocollo TCP

- Al fine di avere un data transfer affidabile e connection-oriented i "pacchetti" devono essere recapitati tutti e nell'ordine corretto.
- Se il mittente dovesse aspettare un ack per ogni segmento la portata sarebbe molto bassa; ecco perché molti dei protocolli connection oriented affidabili permettono a più di un pacchetto "inrisolto" di stare in rete. Il numero di pacchetti dati che il mittente è autorizzato a spedire pur non ricevendo un ack è detto finestra o dimensione della finestra (window size).
- Il TCP usa expectational ack, ovvero i numeri di ack si riferiscono al pacchetto che si aspetta per prossimo.
- Il windowing si riferisce al fatto che la window size si negozia dinamicamente durante la sessione TCP.



Il Windowing

- Il windowing è un meccanismo di flow control. Richiede che la sorgente riceva un ack dal destinatario dopo aver trasmesso una certa quantità di dati.
- Il processo TCP in ricezione riporta una finestra al processo mittente. Questa finestra specifica il numero di pacchetti, partendo dal numero ack, che il processo ricevente è attualmente in grado di accettare.
- Se la window size è 3 la sorgente deve aspettare un ack prima di continuare a spedire. Se l'ack non arrivasse si deve ritrasmettere, ad un rate più lento però.



Cap. 11 Livelli Trasporto e Applicazione

Sulla finestra

Durante tutto il tempo della connessione la dimensione della finestra può variare. Ogni ack contiene un window advertisement che indica il numero dei byte che il destinatario può ricevere.

TCP mantiene anche una finestra per il controllo delle congestioni; solitamente tale window è della stessa dimensione sia nel destinatario che nella sorgente. Appena si perde un pacchetto, magari proprio per una congestione, questa finestra è divisa a metà. Questo approccio gestisce la finestra nella maniera consona alle situazioni che vi sono nella rete.

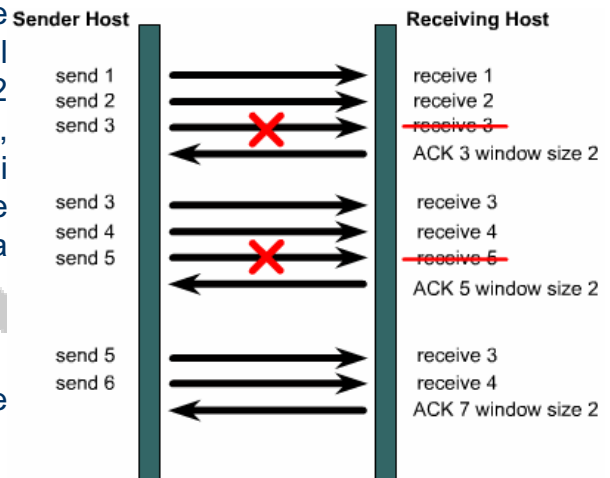


Cap. 11 Livelli Trasporto e Applicazione

Esempio

Nella figura l'host trasmittente manda tre pacchetti e poi aspetta un ack. Se il destinatario può gestire solamente 2 pacchetti allora il terzo è scartato, specificando mediante ack che si aspetta il terzo pacchetto come prossimo, nonché che per lui la dimensione di finestra è 2.

Errata corregge bel Receive 3 e 4 invece di 5 e 6.....



Cap. 11 Livelli Trasporto e Applicazione

Alcune funzioni del TCP

| Bit 0 | Bit 15 | Bit 16 | Bit 31 |
|-----------------------------|--------------|-----------------------|-------------|
| Source Port (16) | | Destination Port (16) | |
| Sequence Number (32) | | | |
| Acknowledgement Number (32) | | | |
| Header Length (4) | Reserved (6) | Code Bits (6) | Window (16) |
| Checksum (16) | | Urgent (16) | |
| Options (0 or 32 if any) | | | |
| Data (varies) | | | |

20
Bytes

TCP è un protocollo di layer 4 connection-oriented che fornisce trasmissioni full-duplex affidabili. In ambiente connection-oriented la connessione è stabilita

prima che si mandino dei dati. TCP è il responsabile della segmentazione come del riassemblamento, della spedizione se qualcosa si è perso e della numerazione dei segmenti prima che inizi la trasmissione.

TCP crea un circuito virtuale tra le applicazioni end-user.

I protocolli che usano TCP sono:

- FTP
- HTTP
- SMTP
- Telnet



Cap. 11 Livelli Trasporto e Applicazione

Campi del pacchetto TCP

I campi del pacchetto TCP sono:

- Source port – numero della porta chiamante
- Destination port – numero della porta
- Sequence number
- Acknowledgment number – prossimo ottetto TCP atteso
- HLEN – numero di parole da 32 bit nell'header
- Reserved – posto a zero
- Code bits – funzione di controllo come il setup o la terminazione della sessione
- Window – numero di ottetti che il mittente può accettare
- Checksum – calcolata sull'header e il campo dati
- Urgent pointer – indica la fine dei dati urgenti
- Option – unica opzione esistente massima size del segmento TCP
- Data – Upper-layer protocol data



Cap. 11 Livelli Trasporto e Applicazione

L'UDP

Il protocollo UDP è connectionless. Esso è un protocollo semplice che scambia datagrammi senza ack o garanzie sulla consegna. Error processing o ritrasmissioni devono essere gestite dai protocolli di livello superiore.

UDP non usa windowing o ack per cui la affidabilità anche è demandata ai layer di livello superiore.

Si basano sui servizi dell'UDP:

- TFTP
- SNMP
- DHCP
- DNS

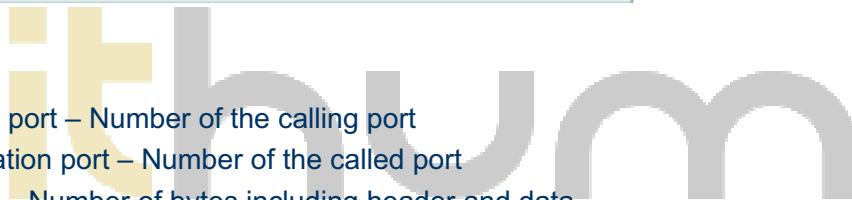


Cap. 11 Livelli Trasporto e Applicazione

Formato del segmento UDP

| Bit 0 | Bit 15 | Bit 16 | Bit 31 |
|------------------|-----------------------|--------|-------------------|
| Source Port (16) | Destination Port (16) | | 8 Bytes ↑ ↓ |
| Length (16) | Checksum (16) | | |
| Data (if any) | | | |

- 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



Cap. 11 Livelli Trasporto e Applicazione

Le porte

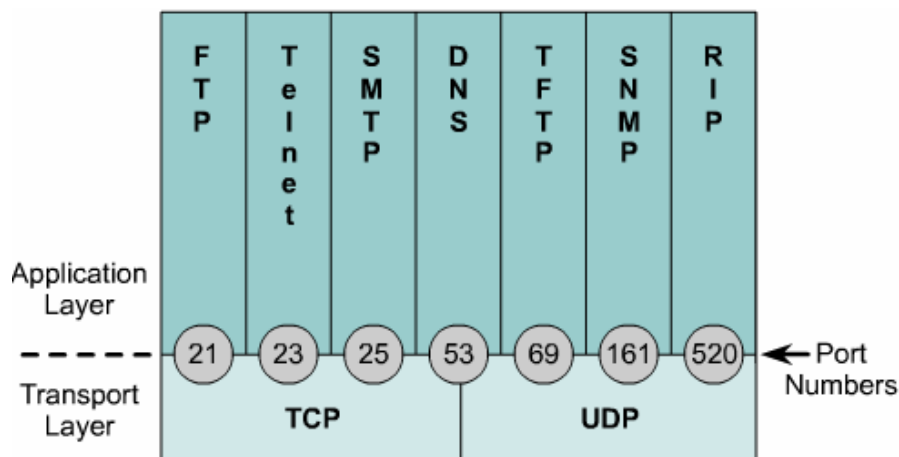
Sia il TCP che l'UDP usano le porte (o socket) per passare le informazioni ai layer superiori. I numeri delle porte sono mantenuti per tenere traccia delle conversazioni che attraversano la rete nello stesso momento (Internet Assigned Numbers Authority (IANA)). I numeri delle porte hanno i seguenti range assegnati:

- Numeri sotto al 1024 sono considerati come port number ben noti
- Numeri sopra al 1024 porte assegnate dinamicamente
- Le porte registrate sono di applicazioni specifiche di determinati vendor; la maggior parte sono sopra al numero 1024
- Gli end system usano numeri di porta per selezionare l'applicazione appropriata.



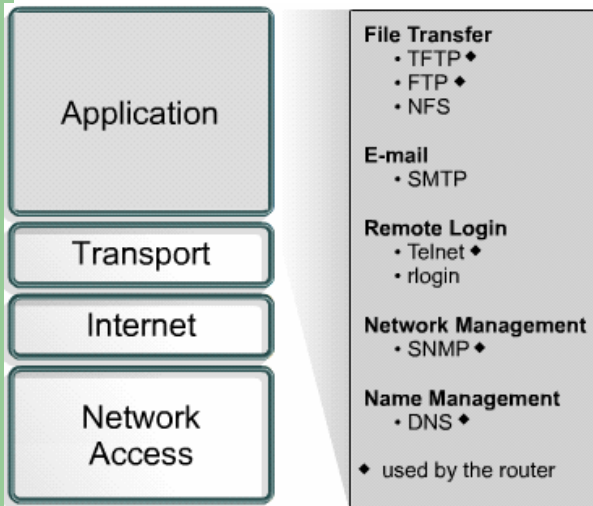
Cap. 11 Livelli Trasporto e Applicazione

I numeri di porte "famose"



Cap. 11 Livelli Trasporto e Applicazione

Application Layer del modello TCP/IP



Il livello applicazione del modello TCP/IP comprende quelli application, presentation e session del modello OSI; ecco perché esso racchiude tutto ciò che riguarda rappresentazione, encoding e dialog control. Questo design del modello assicura massima flessibilità al layer application per gli sviluppatori di software.



Cap. 11 Livelli Trasporto e Applicazione

Domain Name System

E' molto facile dimenticare un IP address per un sito se non c'è un'associazione di idee tra esso ed il contenuto del sito.

Un domain naming system è stato sviluppato per associare il contenuto del sito all'indirizzo di esso. Il DNS è il sistema usato su Internet per tradurre i "nomi" dei siti in indirizzi IP.

Un domain è un gruppo di computer associati dalla locazione geografica o l'offerta che fanno.

Il nome di un dominio è una stringa di caratteri, numeri o entrambi.

- .us – United States**
- .uk – United Kingdom**
- .edu – educational sites**
- .com – commercial sites**
- .gov – government sites**
- .org – non-profit sites**
- .net – network service**



Cap. 11 Livelli Trasporto e Applicazione

FTP e TFTP

L'FTP è un servizio affidabile, connection-oriented basato su TCP che serve a trasferire file. Se il file è copiato da un server FTP prima stabilisce un controllo di connessione; quindi si crea una seconda connessione che è il link tra i computer attraverso cui i dati sono trasferiti.

I trasferimenti di dati possono avvenire in modalità ASCII o binaria. Tali modalità determinano l'encodaggio usato per i file di dati, che è un task del presentation layer. Appena il file termina la connessione dati termina automaticamente. Quando l'intera sessione è completa allora il command link cade quando l'utente si logga fuori.

TFTP si basa su UDP; è usato sui router per trasferire file di configurazione e immagini degli IOS Cisco. Fu progettato per essere piccolo e facile da implementare e per questo manca di molte caratteristiche di FTP. Non fa autenticazione e non lista le directory, ma legge, scrive o maila files da o a un server remoto. E' utile in alcune LAN perché è più veloce dell'FTP e, in ambienti stabili, lavora in modo affidabile.



Cap. 11 Livelli Trasporto e Applicazione

HTTP

Hypertext Transfer Protocol funziona con il World Wide Web, che è la parte più usata e crescente di Internet. Un Web Browser è una applicazione client-server, il che significa che richiede ambedue i componenti per funzionare. Esso presenta le pagine Web che possono contenere suoni, immagini, video e che sono create tramite HTML, il quale in realtà indirizza il Web Browser su una particolare Web page per far apparire la pagina in una determinata maniera. Inoltre HTML specifica la locazione per il piazzamento del testo, degli oggetti o dei file che devono essere trasferiti dal Web server al Web Browser.

L'Uniform Resource Locator è una descrizione HTML nascosta. Quando si va su una pagina il browser esamina il protocollo per vedere se deve aprire un altro programma e poi stabilisce l'indirizzo IP del Web server usando DNS. A questo punto gli ultimi 4 livelli della pila OSI iniziano la sessione col Web server.



Cap. 11 Livelli Trasporto e Applicazione

HTTP (2)

- I dati che sono trasferiti al server HTTP contengono il nome della cartella della Web page. I dati possono anche contenere uno specifico file name per una pagina HTML.
- Se non c'è nessun file indicato vi è un nome di default immesso nel server.
- Il server risponde alla richiesta mandando ai Web client il testo, grafica, audio e video specificati nelle istruzioni HTML.
- I browser che sono i client riassemblano i file per creare la Web page come deve essere visualizzata, quindi terminano la sessione.



Cap. 11 Livelli Trasporto e Applicazione

SMTP

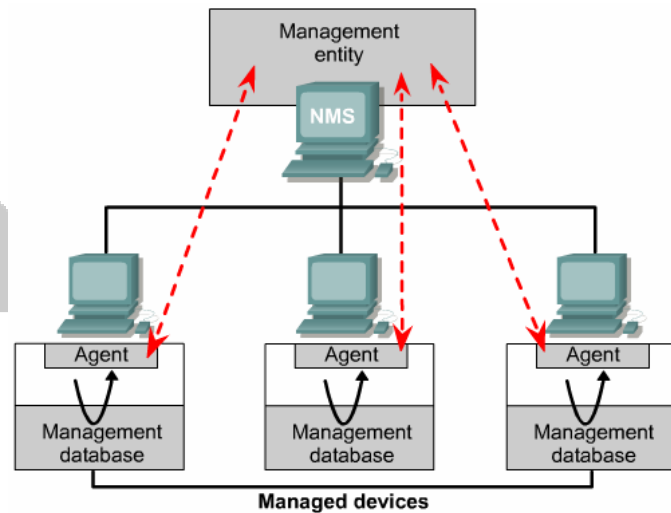
- I server e-mail comunicano tra loro con l'SMTP per spedire e ricevere mail.
- Esso usa TCP per trasportare i messaggi in formato ASCII.
- Quando un server riceve posta per un utente la registra aspettando che egli poi la scarichi.
- I protocolli client per la posta sono POP3 e IMAP4 e ambedue usano il TCP.
- I mail clients usano invece SMTP per spedire la posta. Dato che ci sono 2 protocolli distinti e 2 server distinti le operazioni possono essere fatte in maniera separata.
- Un buon test per la raggiungibilità del server di posta è usare Telnet verso la porta SMTP (porta 25) o quella POP3 (110).
- SMTP non offre un granchè come sicurezza e non richiede autenticazione: è per questo che gli amministratori di rete non permettono a host esterni di usare il server SMTP per mandare mail.



Cap. 11 Livelli Trasporto e Applicazione

SNMP

Il Simple Network Management Protocol è un protocollo di layer applicativo che facilita lo scambio di management information tra device di rete. Usa UDP e può servire agli amministratori per trovare e risolvere problemi.



Cap. 11 Livelli Trasporto e Applicazione

SNMP (2)

Un network gestito SNMP consiste di tre elementi chiave:

- Network management system – NMS esegue applicazioni per monitorare e controllare i device. Ne devono esistere diversi per ogni rete “gestita”.
- Managed devices – sono nodi della rete che contengono un agente SNMP; mantengono management information e le rendono fruibili all’NMS usando SNMP (router, switch, stampanti, host,...).
- Agents – sono moduli software che risiedono nei managed device. Esso ha la conoscenza locale delle info di management e le traduce per renderle compatibili con SNMP.



Il client software Telnet dà l'abilità di loggarsi a un host Internet remoto che sta "facendo correre" l'applicazione server Telnet.

Per compiere una connessione Telnet bisogna selezionare le opzioni, come nome host (IP address o DNS name) e tipo di terminale (indica il tipo di terminal emulation che Telnet deve compiere).

Tutto ciò che si compie con Telnet avviene sul computer remoto.

Lavora all'application layer del modello TCP/IP e agli ultimi tre livelli del modello OSI:

- Application layer – ha a che fare con i comandi
- Presentation layer – gestisce la formattazione (ASCII)
- Session layer - trasmette

