




 POLITECNICO DI MILANO

# Impianti Informatici



## Reti




Cos'è una rete

2

Rete: insieme di sistemi per l'elaborazione delle informazioni interconnessi tra loro

Obiettivi:

- condividere il software
- consultare archivi comuni
- comunicare dati fra i sistemi stessi




Impianti Informatici

POLITECNICO DI MILANO

Uno degli aspetti più evidenti della rivoluzione Informatica e delle Telecomunicazioni è stata la nascita e la diffusione delle reti,

- Per rete si intende un insieme di apparati interconnessi tra loro. Le reti possono essere di svariato tipo: ad esempio la rete telefonica classica include apparati quali le centraline telefoniche, i telefoni stessi, connessi tra loro mediante cavi. In ambito prettamente informatico una rete serve per collegare fra loro svariati computer con l'obiettivo di:
  - condividere il software, consultare archivi comuni, comunicare dati fra i sistemi stessi. In generale una rete di computer permette lo scambio di informazioni, e quindi la condivisione delle risorse della macchine coinvolte (che vengono denominate host) o di periferiche (ad esempio di una stampante)



Tipologie di reti

3

LAN (Local Area Network)

- Estensione limitata, elevata velocità di trasferimento dei dati (edificio, edifici adiacenti, ~100m)

MAN (Metropolitan Area Network)

- Trasferimento dati ad alta velocità (città, ~ 10 Km), ad esempio utilizzando cavi in fibra ottica
- Può connettere varie LAN all'interno della stessa città

WAN (Wide Area Network)

- Consiste solitamente in più LAN e MAN distribuite in un'ampia area geografica
- La più ampia è Internet

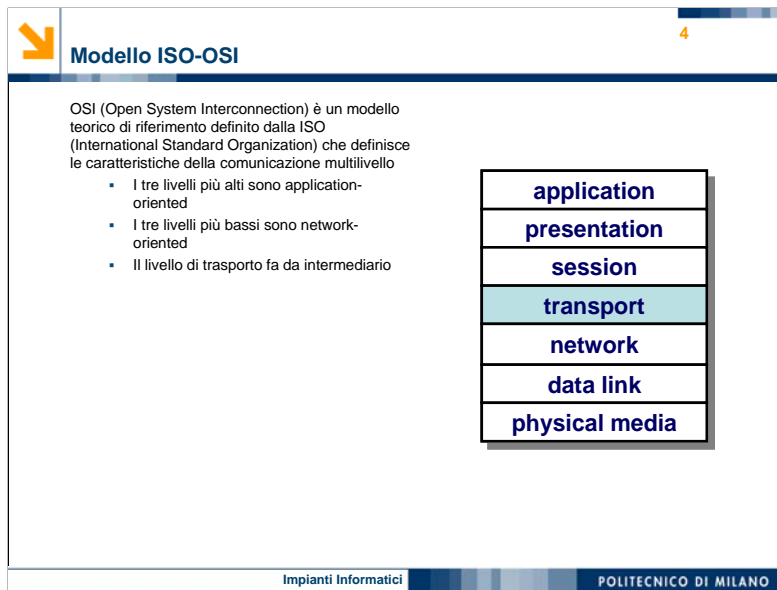
Impianti Informatici

POLITECNICO DI MILANO

Oggi la dimensione di una rete va dalla rete locale di un'azienda alla rete globale attraverso Internet, a seconda delle esigenze dell'utente di condividere dati solo con il proprio ufficio o con persone che stanno a decine o migliaia di chilometri di distanza. In una rete compaiono computer di vario tipo, computer di produttori diversi e computer che possono utilizzare sistemi operativi diversi tra loro.

In base alla tecnologia utilizzata le reti possono raggiungere differenti distanze di trasmissione:

- La più piccola è la LAN, la classica rete aziendale; essa ha estensione limitata (minore di 100m), ma elevata velocità di trasferimento.
- La MAN, come dice il nome, copre una area metropolitana: la sua estensione non supera la decina di chilometri e la velocità di trasferimento dei dati è molto elevata. Può comprendere all'interno diverse Lan
- La WAN può essere composta da reti LAN e MAN, connesse da apposite apparecchiature (ad esempio mediante router) e copre un'ampia area geografica. Internet è la più ampia delle WAN



In una rete gli apparati sono interconnessi tra loro per scambiarsi le informazioni; affinché sistemi diversi possano comunicare è però necessario stabilire delle regole di comunicazione.

- L'International Standard Organization ha definito un modello teorico di riferimento, denominato OSI, che definisce le caratteristiche della comunicazione multilivello. Tale framework aggiunge dei livelli di astrazione alla comunicazione consentendo lo scambio di informazioni tra sistemi eterogenei.
- Il modello OSI è composto da 7 livelli; non è necessario che tutti e 7 compaiano necessariamente in ogni sistema
- Nella pila protocollare i tre livelli alti sono application-oriented, quindi basati sulle esigenze dell'applicazione da eseguire
- Mentre i tre livelli più bassi sono network-oriented, cioè dipendono dalle caratteristiche del mezzo di trasmissione
- Tra loro la comunicazione avviene mediante il livello di trasporto, che opera da intermediario

➤
Stratificazione
5


---

**Protocollo:** insieme di regole per gestire la comunicazione tra entità che scambiano informazioni  
 Il livello  $n$  di un sistema comunica **virtualmente** con il livello  $n$  di un altro

Impianti Informatici
POLITECNICO DI MILANO

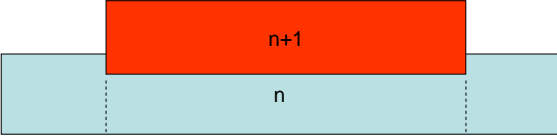
Nelle reti informatiche la comunicazione avviene attraverso entità che risiedono nei diversi sistemi. Un'entità è un dispositivo capace di inviare e ricevere informazioni; va osservato, comunque, che due entità non possono semplicemente scambiare sequenze di bit sperando di essere comprese.

- Affinché la comunicazione sia efficace le entità devono essere d'accordo su un protocollo. Un protocollo definisce cosa va comunicato, oltre a come e quando vada comunicato.
  - Due entità di pari livello comunicano virtualmente tra loro e sono in grado di interpretare correttamente i dati provenienti dall'altra entità perché utilizzano lo stesso protocollo
- Un protocollo può comprendere un intero livello del modello ISO-OSI, oppure una sua parte o anche includere più livelli.

 **Principio dell'incapsulamento** 6

Principio dell'**incapsulamento**

- i messaggi dei livelli superiori vengono *incapsulati* nel campo dati del livello inferiore e trasmessi in maniera *trasparente*
  - non vengono né interpretati né modificati
- Garantisce l'**indipendenza tra layer**

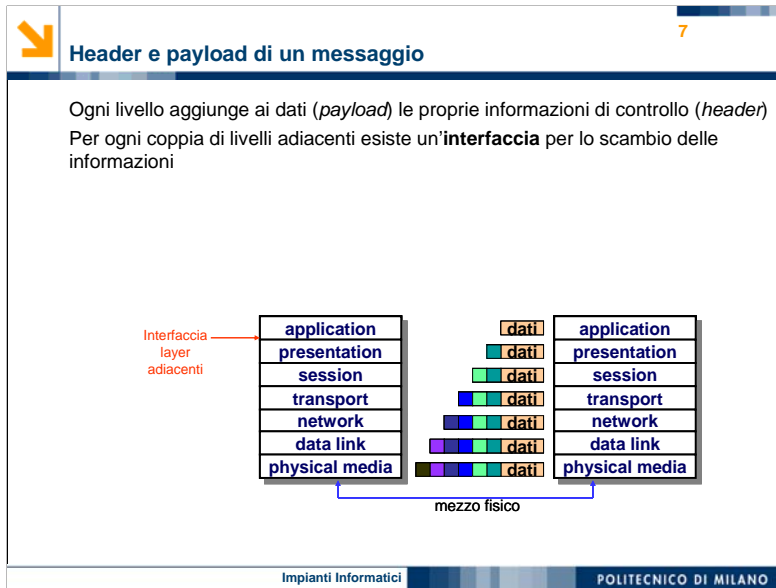


Impianti Informatici POLITECNICO DI MILANO

Virtualmente la comunicazione avviene tra entità di pari livello; realmente tale comunicazione è invece tra l'entità di livello  $n+1$  e l'entità inferiore di livello  $n$ .

• Perciò i messaggi dell'entità  $n+1$  di un sistema, pur destinati all'entità  $n+1$  di un altro sistema, non giungono direttamente all'entità di destinazione, ma vengono incapsulati nel livello  $n$  e trasmessi in maniera trasparente, ovvero senza essere né interpretati né modificati

• Il principio dell'incapsulamento garantisce l'indipendenza tra i layer: in linea teorica è quindi possibile utilizzare un certo protocollo per un dato livello, qualsiasi siano i protocolli utilizzati nei livelli superiori ed inferiori.

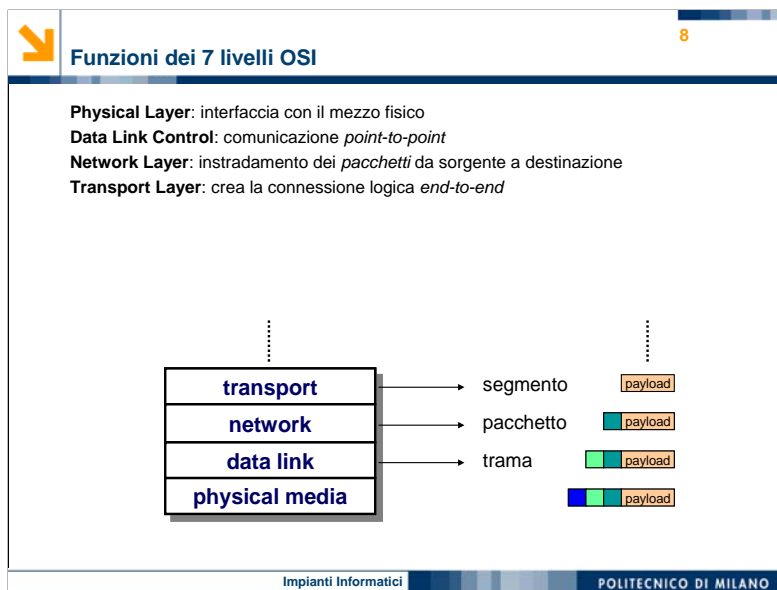


Si consideri la figura. Quando l'application layer del sistema di sinistra vuole comunicare con l'application layer di destra, genera un certo messaggio in base al protocollo utilizzato dalle due entità. Esso viene ricevuto dal livello inferiore, il presentation, il quale genera un nuovo messaggio, destinato al presentation layer di destra:

- Il nuovo messaggio è composto dai dati provenienti dal layer superiore che costituiscono il payload, più una serie informazioni di controllo, dette header, necessarie presentation layer di destra per interpretare i dati

Ogni livello aggiunge quindi il proprio header, finché il messaggio non viene inviato tramite il mezzo fisico. I livelli del sistema di destra operano al contrario: di ogni messaggio estraggono l'header più esterno e mandano al layer superiore la restante parte del messaggio, fino a giungere all'application layer.

- Lo scambio di informazioni tra livelli adiacenti avviene mediante un'opportuna interfaccia.

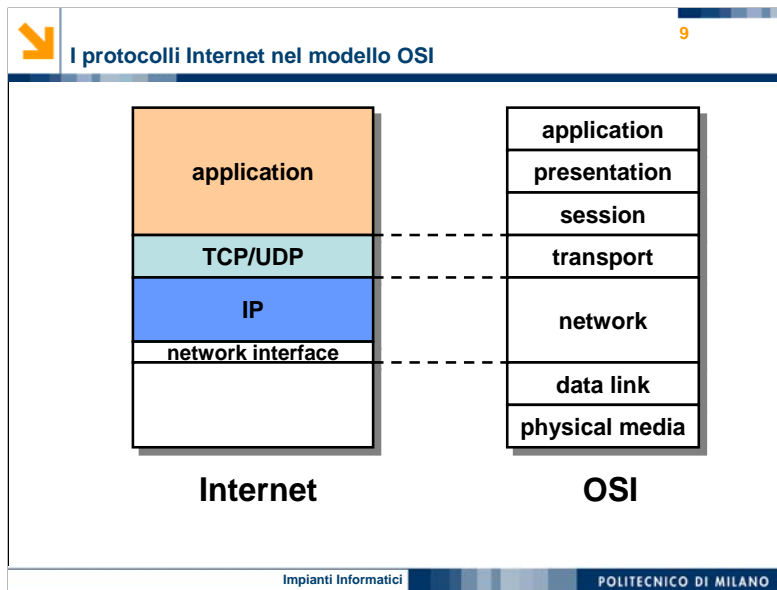


Analizziamo le funzioni principali dei livelli inferiori dello stack protocollare ISO-OSI:

- Il livello Fisico descrive le modalità di trasmissione e ricezione dei segnali che trasportano le informazioni.
- Il livello Data link controlla il flusso di dati fra due nodi intercomunicanti. Una delle sue funzioni originarie era l'Automatic Retrasmission Request, cioè l'uso di codici per il controllo degli errori. I mezzi fisici odierni hanno una probabilità d'errore decisamente inferiore rispetto a qualche decina di anni fa, così da rendere inutile tale controllo, che viene effettuato dai livelli superiori. Un'evoluzione di tali codici è tuttora usata nei collegamenti radio, molto più soggetti ad errori di trasmissione.
- Il livello di Rete descrive le modalità di instradamento dei dati, ovvero specifica come avviene l'attraversamento delle reti interconnesse. Si dice che il livello di rete crei il percorso tra sorgente e destinazione.
- Il livello di Trasporto comprende tutte le operazioni necessarie al corretto trasferimento dei dati dall'applicazione sorgente all'applicazione destinazione, provvedendo al controllo degli errori o alla ritrasmissione in caso di errore.

I messaggi a livello di trasporto vengono detti segmenti, a livello rete pacchetti e a livello data link trame.





Lo stack TCP/IP è la suite di protocolli di utilizzati in Internet.

Come si può vedere dall'immagine nel protocollo TCP/IP alcuni strati sono stati fusi in un unico layer:

Application - presentation - session si sono fusi nell'application layer

Il Trasport è stato semplicemente rinominato in TCP/UDP, due alternativi protocolli di trasporto

Il Network è stato disaccoppiato in IP e network interface

Il livello fisico ed il Data link non vengono definiti in maniera diretta dallo stack.



Indirizzo IP

10

Ogni nodo della rete è identificato da un indirizzo IP.

- Un nodo che è collegato a più reti (multi homed host) ha un indirizzo per ogni interfaccia

Un indirizzo è una stringa lunga 32 bit (nel caso IPv4)

L'indirizzo IP è solitamente espresso nella notazione decimale a gruppi di 8 bit (*dotted decimal notation*):

8 bit . 8 bit . 8bit . 8 bit

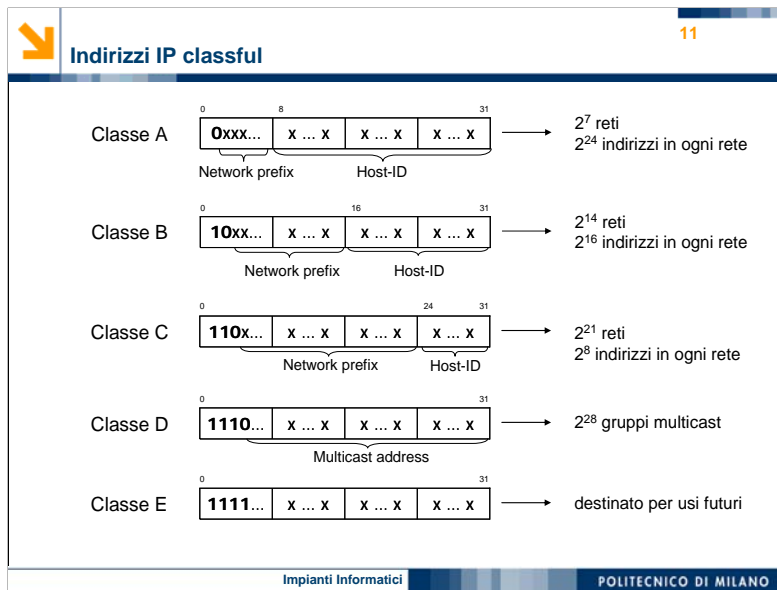
- Ad esempio: 131.175.54.140



Impianti Informatici


POLITECNICO DI MILANO

- L'indirizzo ip consente di identificare i vari nodi di una rete. Nodi collegati a più reti (detti multi-homed host), hanno un indirizzo ip x ogni interfaccia.
- Praticamente l'indirizzo ip è una stringa che, nel caso di IP versione 4, è lunga 32 bit.
- Solitamente si usa indicare tale stringa nella dotted decimal notation, ovvero raggruppando i 32 bit in 4 gruppi da 8 e convertendo il valore di ciascun gruppo in numero decimale. Un tipico indirizzo ip avrà quindi una struttura del tipo 131.175.54.140



Esistono tipologie di indirizzi detti classful, che hanno una struttura ben definita. Mentre qualche decina di anni fa si usavano praticamente solo indirizzi classful, a causa della loro rigidità oggi sono poco usati. In essi l'indirizzo è diviso in due campi, il campo network che individua la rete, ed il campo host che individua il nodo all'interno di una rete. A seconda di quanti bit sono dedicati al network prefix e quanti all'host-id si parla di indirizzi di classe A, B o C: i primi bit dell'indirizzo consentono di identificare la classe.

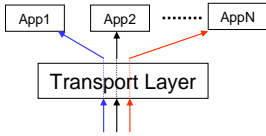
Gli indirizzi di classe D sono dedicati ai gruppi multicast, ovvero insieme di nodi identificati da un unico indirizzo ip. Un messaggio destinato a tale indirizzo verrà instradato a tutti gli host del gruppo. Infine gli indirizzi di classe E sono tutt'oggi inutilizzati.

 **Protocolli di trasporto**
12

---

Creano una connessione logica (end-to-end) tra sorgente e destinazione  
 La sorgente, così come la destinazione, è identificata da un *socket* (indirizzo IP + porta)


- L'IP identifica il nodo
- La porta identifica il servizio richiesto
  - il livello di trasporto esegue la *demultiplazione* (e *multiplazione*) per inviare i dati alla corretta applicazione



Impianti Informatici
POLITECNICO DI MILANO

Il protocollo di trasporto è il livello intermedio tra i 3 livelli application-oriented e i 3 network-oriented

- Esso crea una connessione logica end-to-end tra l'applicazione sorgente e l'applicazione destinazione
- Sorgente e destinazione sono, ciascuna, identificate univocamente da un socket, composto da un indirizzo ip ed un numero di porta
- L'indirizzo ip individua l'host
- La porta identifica il servizio richiesto, cioè la particolare applicazione. E' questo livello che si occupa di multiplazione e demultiplazione dei messaggi tra i diversi servizi, quindi di permettere a differenti applicazioni di appoggiarsi allo stesso protocollo di trasporto.



Protocolli TCP e UDP

13

La connessione logica è descritta in modo completo da una coppia di socket

**UDP** (User Datagram Protocol):

- *Segmentazione*
- Multiplazione/demultiplazione

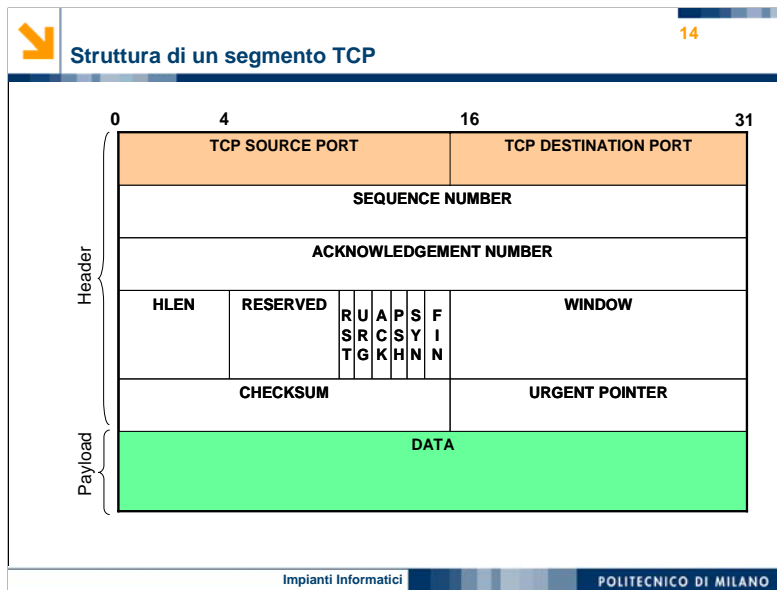
**TCP** (Transmission Control Protocol):

- È *connection-oriented* (virtual circuit)
- Offre le stesse funzioni di UDP + un servizio *reliable*:
  - Controllo di flusso
  - Controllo di sequenza
  - Controllo di congestione
  - Correttezza delle informazioni (gestisce perdite e duplicazioni)

Impianti Informatici

POLITECNICO DI MILANO

- La connessione logica tra due applicazioni è descritta in modo completo da una coppia di socket
  - I due protocolli di trasporto utilizzati su internet sono il TCP e l'UDP
  - Quest'ultimo offre un servizio connection-less, quindi non affidabile. Le sue principali funzionalità sono la multiplazione e demultiplazione, oltre alla segmentazione dei messaggi in parti più piccole
  - Il protocollo TCP è invece connection-oriented, perciò, a differenza di UDP, offre un servizio affidabile per mezzo di controllo di flusso, di sequenza e di congestione, andando, ad esempio, ad adattare la velocità di trasmissione in base allo stato attuale sia del nodo di destinazione che della rete
- Il TCP è quindi più affidabile di UDP, ma come controparte è un protocollo meno leggero, con un maggiore overhead.



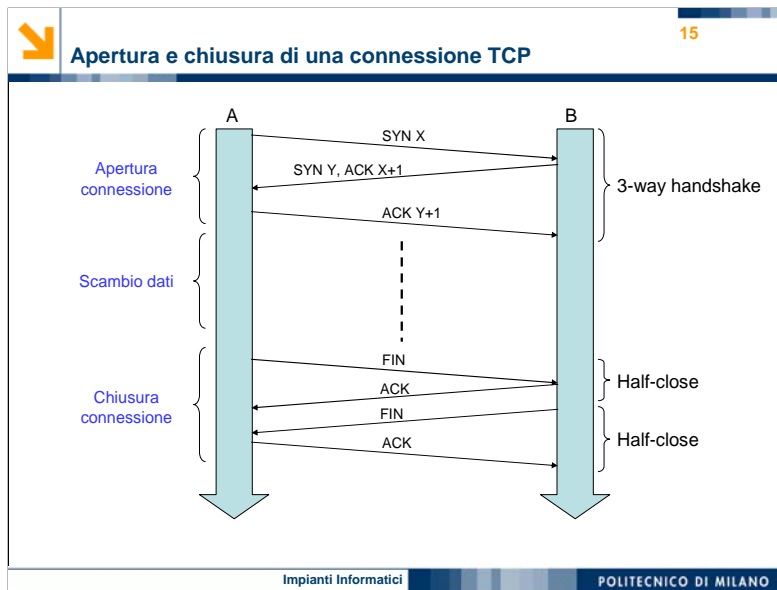
La figura mostra la struttura di un segmento TCP:

Le prime 5 parole di 32 bit sono l'header del messaggio, il resto è costituito dal payload.

I campi principali sono i numeri di porta sorgente e destinazione, ciascuno da 16 bit. Il sequence e l'acknowledgement number vengono utilizzati dal tcp x garantire il controllo di flusso, sequenza e congestione.

I 6 flag individuano il tipo di segmento: ad esempio un segmento di tipo SYN viene utilizzato x indicare l'inizio della connessione, FIN x indicare la chiusura della connessione.

La Window viene usata x sincronizzare le due applicazioni remote.



A fronte di una maggior affidabilità, il protocollo TCP richiede che venga creato un circuito virtuale prima di poter inviare i dati.

L'apertura della connessione viene detta 3-way handshake, in quanto prevede lo scambio di 3 messaggi tra sorgente e destinazione, necessari per sincronizzare le due applicazioni.

Una volta aperta la connessione è possibile l'effettivo scambio dei dati.

Al termine occorre chiudere la connessione. Questo avviene mediante una doppia half-close, ovvero una delle due applicazioni, poniamo la A, richiede la chiusura, l'applicazione B risponde con un riscontro, dopo di che invia un msg di chiusura, e solo quando l'applicazione A risponde con un riscontro viene chiusa definitivamente la connessione da parte di entrambe.

*Apparati di rete*

# Impianti Informatici

 POLITECNICO DI MILANO



Reti







## HUB (livello 1)

17

Opera al livello fisico dello stack ISO-OSI

È un semplice *ripetitore* di segnale

- Anche denominato *accentratore di rete*

Unisce LAN perfettamente identiche tra loro (con stesso protocollo MAC)



application
presentation
session
transport
network
data link
physical media

Impianti Informatici

POLITECNICO DI MILANO

L'hub è un apparato che

- Opera al livello più basso dello stack protocollare ISO-OSI, cioè a quello fisico
- Esso è un semplice ripetitore di segnale, ovvero replica su tutte le sue interfacce la sequenza di bit in ingresso
- Viene anche denominato accentratore di rete, nel senso che rappresenta una sorta di accentratore "elettrico", dove i segnali presenti su tutta la linea vengono mescolati assieme; ogni scheda di rete collegata all'hub sente tutto il traffico presente
- Funzionando a livello fisico, è in grado di unire solamente LAN perfettamente identiche.
- Dato che il livello Datalink può essere suddiviso in due componenti, quello superiore è il logical link control, mentre quello inferiore è il Medium Access Control, detto MAC,...
- l'hub può unire reti che utilizzano lo stesso protocollo MAC



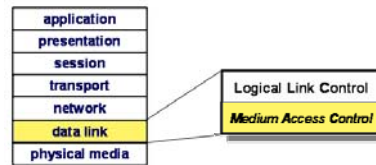
## BRIDGE/SWITCH (livello 2)

18

Opera a livello MAC (Medium Access Control) del Data Link Layer

Ha nozioni di *trama*, quindi non replica semplicemente il segnale

Unisce LAN che usano gli stessi protocolli nei layer superiori a quello MAC

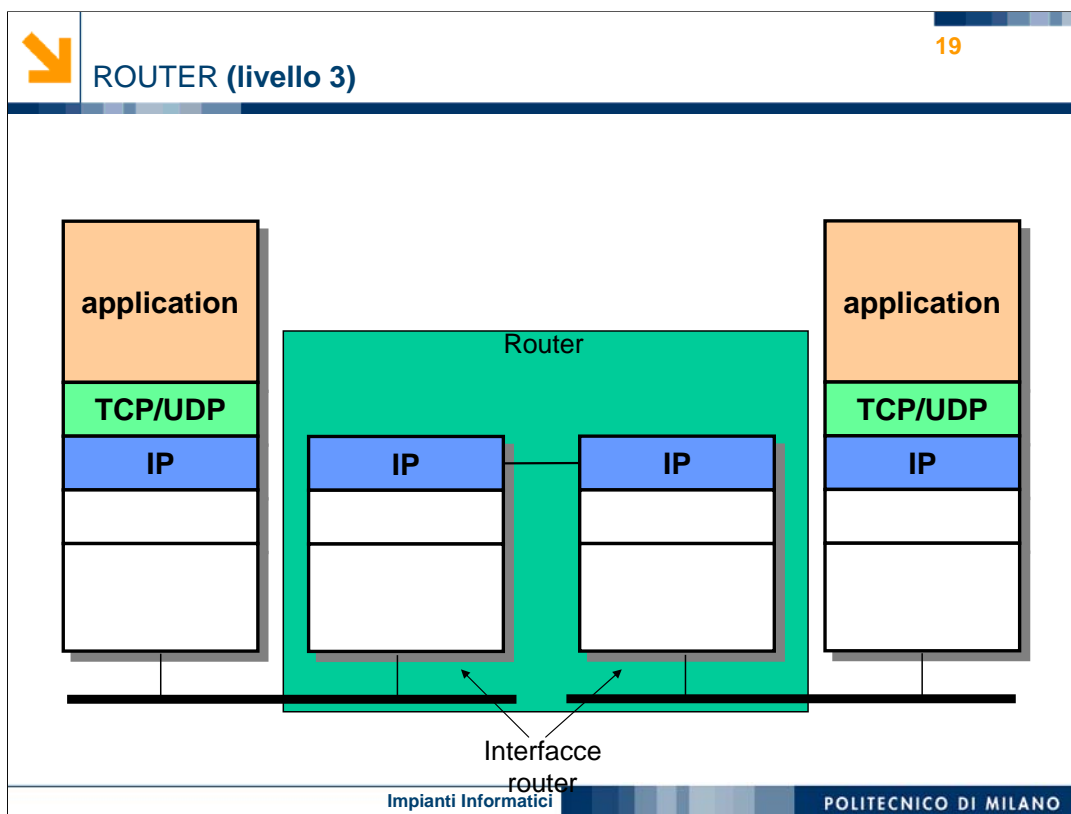


Impianti Informatici

POLITECNICO DI MILANO

Il bridge è un apparato di interconnessione più evoluto rispetto all'hub.

- Osservando lo stack protocollare, il bridge
  - Opera a livello di Medium Access Control. La conseguenza principale, e che lo differenzia dall'hub, è il fatto che il bridge
  - non si limita a ripetere puramente il segnale su tutte le interfacce, ma, avendo nozioni di trama, è in grado di replicarlo verso quella corretta, ovvero quella che consente di raggiungere l'host di destinazione
  - Le tipologie di reti che è in grado di connettere sono quelle che utilizzano gli stessi protocolli nei livelli superiori a quello MAC
- A livello notazionale, solitamente si usano i termini bridge se l'apparato collega solamente due reti, switch se ne collega un numero superiore.



### Il router

- consente di interconnettere reti anche molto differenti. I due host in figura si appoggiano entrambi sullo stack TCP/IP
- I protocolli inclusi nel router includono i livelli ISO-OSI fino a quello di rete.
- La funzione principale del router è infatti quella di instradare i pacchetti dal nodo sorgente a quello destinazione.
- Il router dispone di molteplici interfacce; vi è un'interfaccia per ogni rete a cui è collegato
- Il router riceve i pacchetti da una certa interfaccia e li inoltra verso
- una delle interfacce di uscita in base a determinate politiche, che consentano di giungere, anche passando da differenti router, alla rete cui è collegato l'host di destinazione

➤
20

## Funzionalità dei router

I router eseguono il routing dei pacchetti IP tra le reti ad essi connesse:

- Rimuovono l'intestazione di livello 2
- Esaminano l'intestazione di livello 3 per eseguire l'instradamento
- Modificano l'intestazione di livello 3 (ad es. TTL)
- Inseriscono una nuova intestazione di livello 2

Impianti Informatici
POLITECNICO DI MILANO

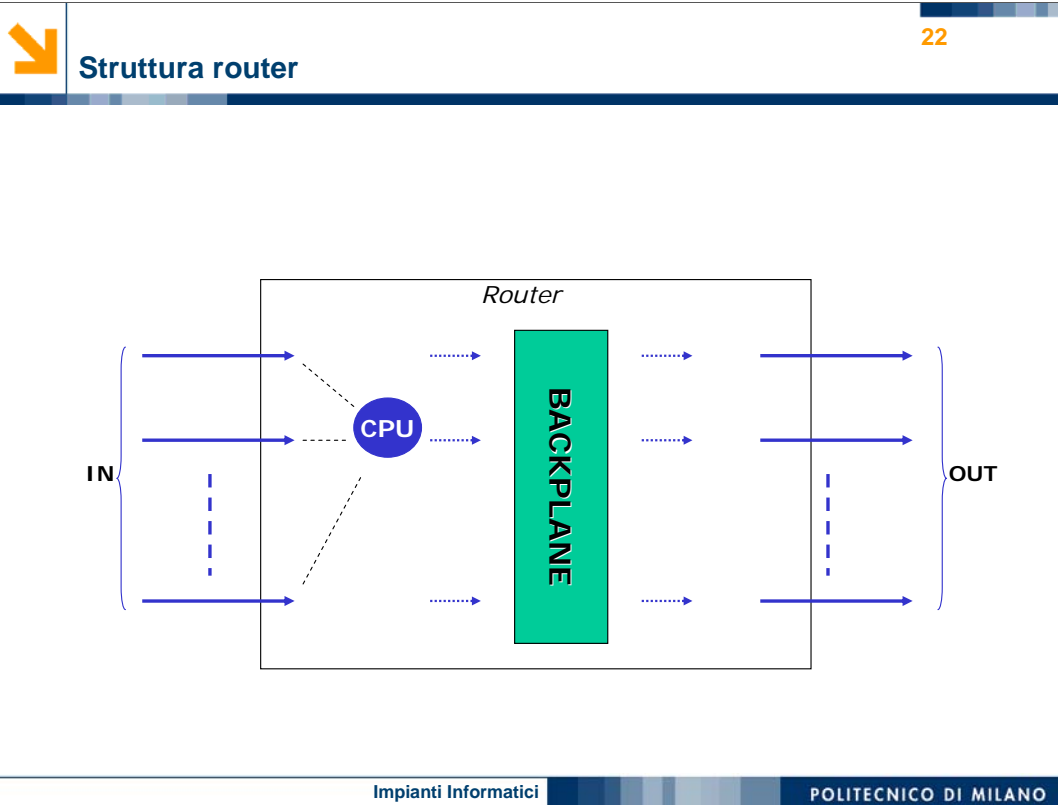
La funzione principale dei router è

- L'instradamento dei pacchetti IP tra le reti ad essi connesse. Praticamente, quando un router riceve un pacchetto,
- Le principali operazioni che compie sui pacchetti in arrivo sono
- rimuovere l'intestazione del Data Link Layer
- Esaminare quella del livello IP, in particolare decidere, in base all'indirizzo dell'host di destinazione, all'algoritmo di routing utilizzato e alla tabella di instradamento, come inoltrare il pacchetto
- Vengono quindi modificati alcuni campi dell'header IP, ad esempio viene decrementato il campo TimeToLive, ed il pacchetto viene inviato verso la rete di destinazione
- Aggiungendo un opportuno header di livello 2.



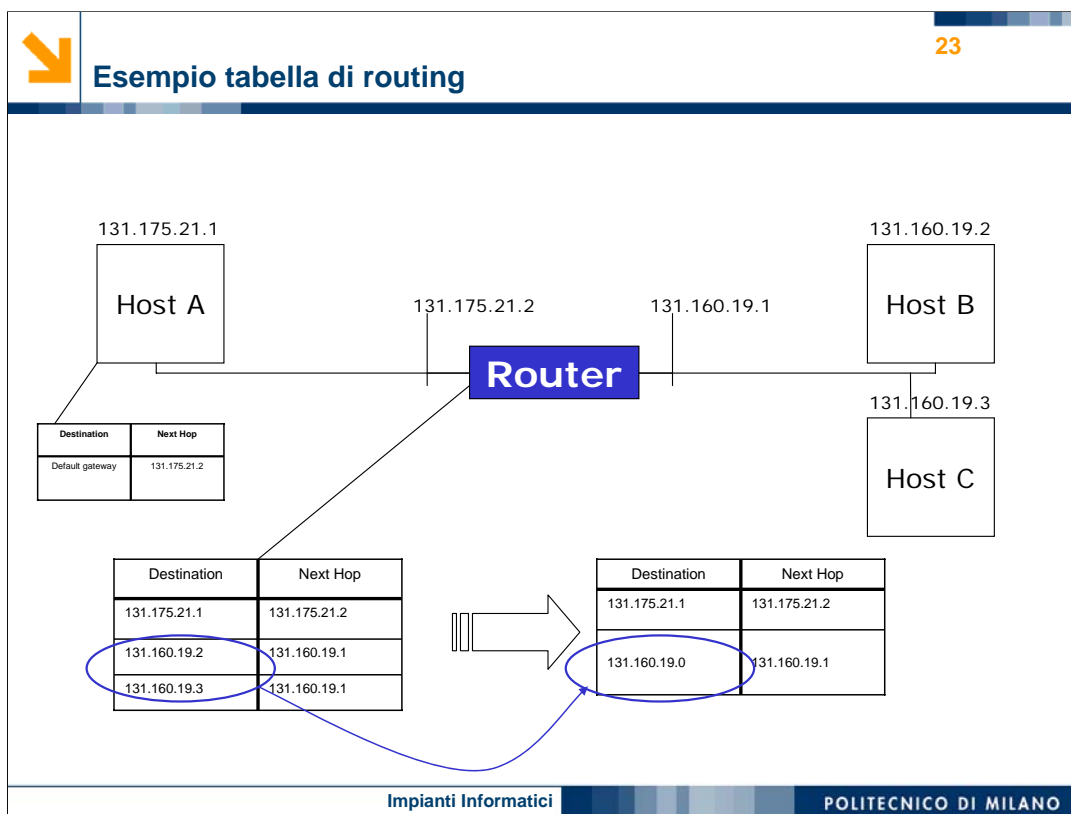
- Hanno algoritmi di instradamento sofisticati
- Se necessario, frammentano ulteriormente i pacchetti per adattarsi alla rete fisica su cui trasmette
- Si utilizzano solitamente per interconnessioni MAN/WAN
- I router attuali offrono generalmente anche funzioni aggiuntive al puro instradamento,
  - Esse richiedono l'integrazione di protocolli superiori al livello di rete (ad esempio quando fungono da NAT-BOX)

- I router implementano sofisticati algoritmi di instradamento per effettuare il routing dei pacchetti; solitamente questi algoritmi sono destination-based, ovvero la scelta del percorso dipende dall'indirizzo ip del nodo di destinazione.
- Dato che implementano il protocollo ip, possono eventualmente frammentare i pacchetti per adattarsi alla rete fisica su cui vengono inviati
- Essi sono utilizzati come apparati di interconnessione tra reti di medie o grandi dimensioni, quindi MAN o WAN
- I router in commercio offrono spesso anche delle funzionalità aggiuntive al semplice instradamento dei pacchetti. Lo stack protocollare che essi implementano integra perciò anche protocolli superiori all'IP.
- Quando, ad esempio, il router opera da NAT-BOX, necessita perlomeno del livello di trasporto, in quanto deve accedere all'header per modificarne la porta.



Un router è collegato a due o più reti mediante

- una serie di Interfacce di ingresso e di Interfacce di uscita
  - I pacchetti in ingresso giungono ad una CPU, oppure ad un banco di CPU, che controlla gli header dei pacchetti e, tramite l'algoritmo di routing, determina la corretta interfaccia di uscita
  - E' quindi compito del BACKPLANE smistare i pacchetti
- Le specifiche di un router si definiscono in termini di pacchetti al secondo,
- le cui prestazioni sono dipendenti dalla CPU, ed in termini di bit/secondo
  - dipendenti dalle capacità del backplane. Per pacchetti lunghi il bottleneck è quindi rappresentato da questa componente, mentre per pacchetti di limitate dimensioni è rappresentato dalla CPU.



Consideriamo un router che interconnetta due reti.

- Alla prima rete è connesso l'host A

- Alla seconda gli host B e C

La tabella di instradamento del router deve consentire la comunicazione tra tutti e tre i nodi. Una possibile tabella sarà quindi del tipo mostrato in figura

- In cui, per ogni destinazione, viene indicata l'interfaccia di uscita su cui inoltrare il pacchetto.

- Affinché gli host possano inviare pacchetti all'esterno della loro rete, è necessario che contengano almeno una mini tabella di routing, in cui venga specificata l'interfaccia di default verso cui inviare i pacchetti

- Con l'obiettivo di ridurre il più possibile il numero di entry,

- la tabella del router può essere compattata andando ad

- identificare gli host B e C tramite l'indirizzo della rete a cui appartengono



Migrazione istantanea non fattibile

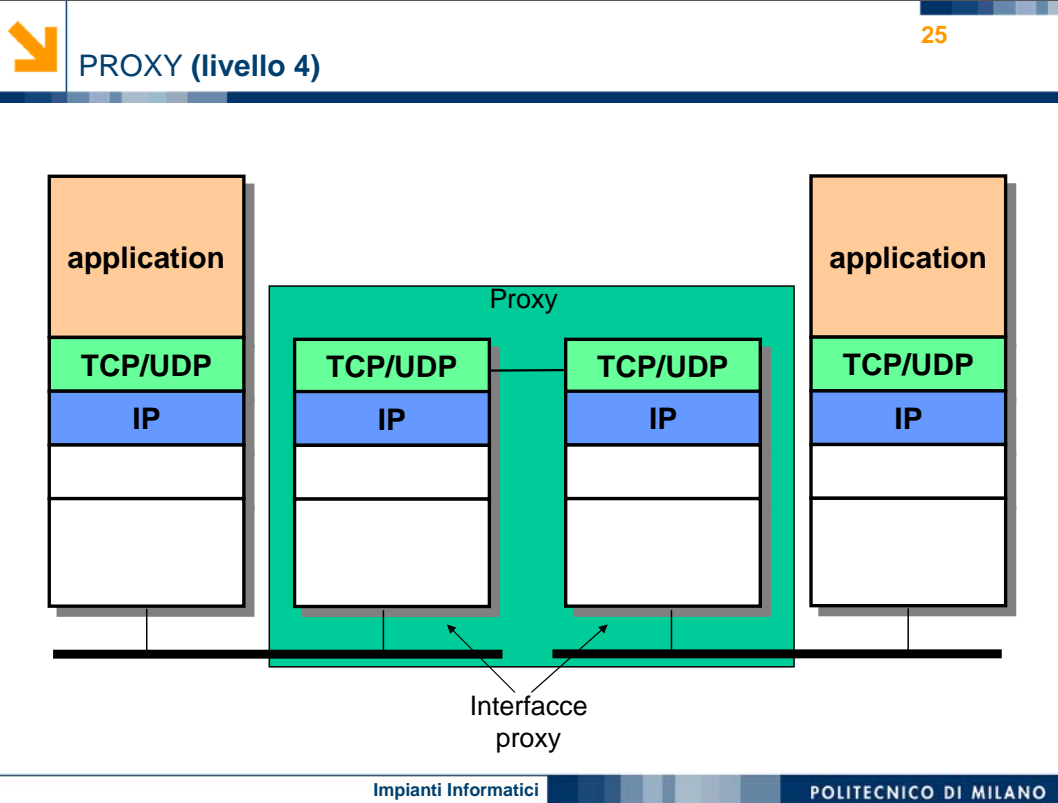
Tecniche di migrazione:

- Dual Protocol
  - Ogni nodo deve implementare sia IPv4 che IPv6
- IPv4 Tunnelling
  - Edge router con stack IPv4 e IPv6
- Protocol Translation
  - Impossibilità di usare i nuovi campi di IPv6

Le difficoltà nella migrazione di tutta la rete Internet dall'IPv4 all'IPv6 è uno dei motivi che ha rallentato l'espansione di questo protocollo.

- Una transizione istantanea non è praticabile perché occorrerebbe configurare milioni di nodi contemporaneamente.
- La migrazione impatta anche su uno degli apparati basilari utilizzati in Internet: il router.
- La più semplice è l'uso di una doppia stack protocollare all'interno di ogni nodo, e quindi di ogni router,
- con relative conseguenze in termini di costi di implementazione, configurazione e amministrazione
- L'uso del tunnelling su IPv4 prevede che solo
- gli edge router, posti a confine tra una rete IPv4 ed una IPv6, contengano il doppio stack protocollare, in modo da fare il tunnel dei pacchetti IPv6
- Un'ulteriore tecnica è l'uso di convertitori protocollari.
- Le difficoltà emergono dal fatto che gli header delle due versioni non contengono le stesse informazioni.





Il proxy

- offre dei servizi alla rete
- Dato che implementa lo stack protocollare fino al livello di trasporto, è in grado di analizzare il flusso informativo in transito
- Dispone di molteplici interfacce, una per ogni rete a cui è collegato

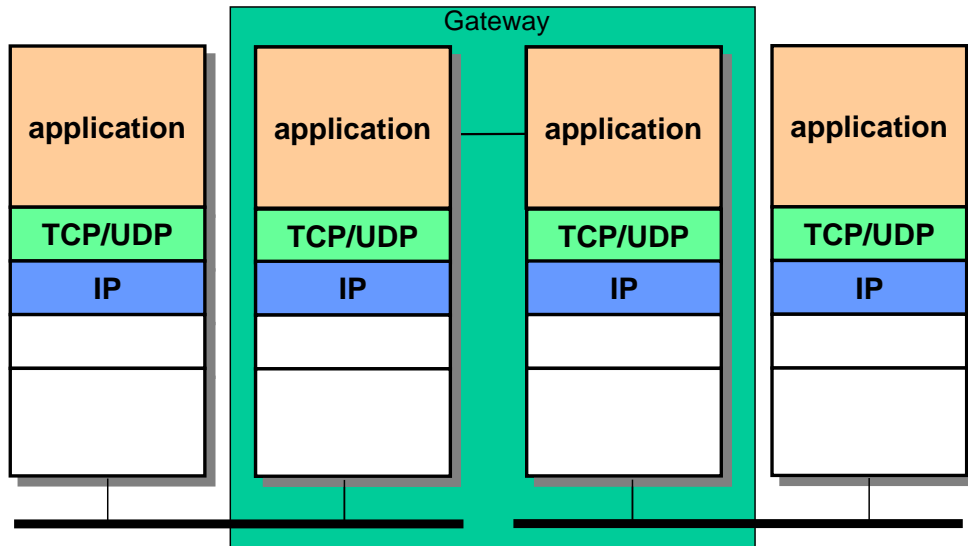


Sono in grado di ricostruire un intero messaggio o flusso di dati scambiato tra due reti

Possono (limitatamente) analizzare e modificare il flusso informativo tra due reti o stazioni

- a livello di proxy è possibile applicare un antivirus alle e-mail in transito
- a livello di proxy è possibile decidere se un utente ha il diritto di visualizzare una certa pagina Web
- intermediario tra nodi
  - caching

- I proxy, operando a livello di trasporto, sono apparati che permettono di ricostruire un intero messaggio o flusso di dati
- Possono, anche se in modo limitato, oltre ad analizzare il flusso di informazioni, modificarne il contenuto, andando, ad esempio,
- ad applicare un antivirus alle email in transito, oppure
- Decidere se un utente ha il diritto o meno di visualizzare una determinata pagina web
- Una delle funzionalità che hanno reso noto il termine proxy è la possibilità di fare caching delle risorse, ponendosi da intermediario tra due host.



L'ultimo apparato che analizziamo è il gateway applicativo. La sua principale funzionalità è quella di interconnettere tra loro due applicazioni remote differenti.

- Lo stack protocollare che implementano comprende tutti i livelli fino a quello applicativo.



I gateway applicativi interconnettono applicazioni diverse (agiscono da interfaccia tra protocolli differenti)

Esempio: posta elettronica (via web mail)

- L'e-mail si avvale di protocolli applicativi (SMTP, POP, IMAP) e di applicazioni client/server adatte a questi protocolli
- Un gateway Web permette di leggere e inviare e-mail usando un protocollo applicativo totalmente diverso (HTTP) e applicazioni client/server totalmente diverse (Web browser/Web server)

- Il gateway permette l'interconnessione di due applicazioni che utilizzano protocolli differenti, fungendo così da interfaccia
- Un classico esempio è la web mail
- La posta elettronica utilizza sia applicazioni client/server, come ad esempio il client di posta elettronica, che si avvalgono di protocolli applicativi, quali SMTP, POP, IMAP
- Un gateway web permette di interagire con la casella di posta elettronica leggendo ed inviando email tramite HTTP pagine Web, quindi protocollo applicativi e linguaggi completamente diversi, e utilizzando browser anziché client di posta. E' il gateway che agisce da interfaccia tra questi diversi protocolli.



Il gateway opera a livello 7 dello stack ISO-OSI


- È in grado di interpretare i dati ricevuti e in parte di modificarli prima di trasmetterli

Il router opera a livello 3 dello stack ISO-OSI

- Instrada i pacchetti
- Non modifica il flusso di dati


Spesso il termine gateway viene comunemente utilizzato, in modo improprio, come sinonimo di router.

- Tuttavia con gateway si individua un dispositivo che svolge funzioni di livello più elevato rispetto al router, con la possibilità di interpretare e modificare i dati prima di ritrasmetterli.
- Il router è invece limitato ad inoltrare i pacchetti, non disponendo di funzionalità per modificare il flusso di informazioni.

 Internet Protocol 30

È un protocollo di rete (livello 3 modello OSI) a pacchetto


- Si occupa della consegna dei pacchetti tra due nodi della rete
- È un protocollo di *interconnessione tra reti* (*Inter-Networking Protocol*), nato per collegare reti eterogenee per tecnologia, prestazioni, gestione.



Impianti Informatici POLITECNICO DI MILANO

l'Internet Protocol fa parte dello stack protocollare TCP/IP.

- In particolare opera a livello di rete del modello OSI
- consentendo la consegna dei pacchetti tra un nodo sorgente ed un nodo destinazione della rete
- Il nome deriva dalla contrazione di Internetworking protocol, richiamando la capacità di interconnettere reti anche molto eterogenee tra loro.

Caratteristiche Internet Protocol31

Servizio *unreliable*

- È compito dei livelli superiori fornire particolari garanzie

Funzioni di *instradamento e indirizzamento*

- Identifica i nodi sorgente e destinazione mediante un indirizzo IP
- Consente ad un pacchetto di circolare dalla sorgente alla destinazione

Esegue *frammentazione* e riassetramento dei pacchetti

Impianti InformaticiPOLITECNICO DI MILANO

L'IP è un protocollo connection-less, che offre perciò un

- Servizio non affidabile, senza garantire la corretta consegna dei messaggi. E' quindi compito dei livelli superiori, in particolare di quello di trasporto, fornire eventualmente delle funzionalità aggiuntive. L'esigenza o meno di tali servizi deriva dai requisiti richiesti dalla particolare applicazione che sta utilizzando lo stack protocollare.
- Le funzioni principali dell'ip sono l'instradamento dei pacchetti dal nodo sorgente al nodo destinazione e l'indirizzamento della rete
- E' inoltre in grado di eseguire frammentazione e riassetramento dei pacchetti, cioè di suddividere un pacchetto in più parti: il livello inferiore ha infatti una dimensione massima di dati che può inviare alla volta ed il protocollo ip garantisce che non gli arrivino messaggi più grandi.

**Subnetting** 32

Consente di partizionare lo spazio degli indirizzi per creare delle sottoreti  
 Mediante una **subnet-mask** si allunga il *network prefix* con un nuovo campo che individua la sottorete (*subnet prefix*)  
 La lunghezza della subnet-mask viene solitamente indicata con /n (ad es. 175.16.1.5/16)

Indirizzo rete	10000010	00000101	00000000	00000000	130.5.0.0
Subnet-mask	11111111	11111111	11111000	00000000	255.255.248.0


Rete (2<sup>14</sup> reti)      Sottorete (2<sup>1</sup> sottoreti per ogni rete)      Host (2<sup>11</sup> host per ogni sottorete)

Impianti Informatici      POLITECNICO DI MILANO

Oltre all'utilizzo degli indirizzi classful, una rete può essere indirizzata, ed in maniera più efficiente, mediante l'uso del subnetting

- Esso aggiunge un ulteriore livello gerarchico, consentendo di partizionare lo spazio degli indirizzi mediante la suddivisione in sottoreti
- Praticamente si utilizza una maschera di sottorete, tramite la quale si scompone l'host-id in due gruppi di bit, uno identificante la sottorete ed uno l'host all'interno della sottorete  
 Essa è una stringa lunga quanto l'indirizzo ip: l'indirizzo della sottorete si identifica effettuando l'and bit a bit tra ip e maschera. Preso a titolo di esempio l'indirizzo ip di classe B 130.5.0.0 mostrato in figura, in cui i primi 16 bit identificano la rete, ed i successivi 16 l'host, se si applica una maschera, ad esempio la 255.255.248.0, la sottorete è identificata dai primi 21 bit, cioè i 16 bit marcati in blu della rete, più i 5 bit evidenziati in rosso riservati alla sottorete. I bit destinati ad identificare l'host all'interno della sottorete sono ora gli 11 più a destra.
- La maschera di sottorete viene sinteticamente indicata mediante una /n, dove n corrisponde al numero di 1 consecutivi nella subnet-mask: la maschera in figura è ad esempio una /21 perché i primi 21 bit sono 1.



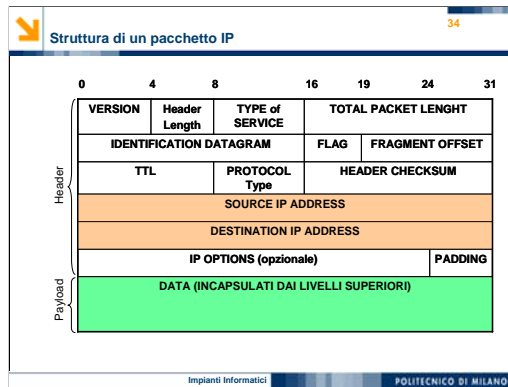
Indirizzi IP ad uso "privato"33

Esistono degli intervalli di indirizzi "privati"

- Questi indirizzi non possono essere utilizzati su internet, ma chiunque è libero di utilizzarli per una rete privata, che sia domestica o di una grande azienda:
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 169.254.0.0/16
- Un computer che utilizzi uno di questi indirizzi non potrà collegarsi direttamente ad un computer su un indirizzo pubblico, a meno di utilizzare particolari meccanismi:
  - NAT
  - Proxy

Impianti InformaticiPOLITECNICO DI MILANO

- Particolari gruppi di indirizzi sono destinati ad uso privato.
- Dato che non può esserne garantita l'univocità perché una qualsiasi rete privata può indirizzare i propri host in maniera autonoma, essi non possono venire utilizzati per navigare su internet. Sono invece liberamente utilizzabili all'interno della propria rete. A seconda dell'esigenza di partizionare in reti più o meno grandi si sceglierà l'insieme di indirizzi più adeguato, ad esempio una 10.0.0.0/8 per sistemi suddivisibili in poche reti, ma con molti nodi in ognuna, oppure una 192.168.0.0/16 per una suddivisione del sistema in più reti, ma di minori dimensioni.
- Per ovviare all'impossibilità di collegarsi ad internet da un indirizzo privato, si utilizzano particolari meccanismi. Uno di questi è l'uso di particolari proxy che, disponendo di un indirizzo pubblico, offrano come servizio quelli di effettuare le richieste sulla Rete per conto dell'host privato. Una tecnica alternativa sempre più utilizzata, e di cui vedremo successivamente il funzionamento, è l'uso del NATING.



La figura mostra la struttura di un datagramma IP. L'header minimo è composto da 5 parole da 32 bit, quindi da almeno 40 byte.


- La seconda parola da 32 bit viene utilizzata dal protocollo per la frammentazione dei pacchetti, memorizzando le opportune informazioni per effettuarne il riassetto.

- La quarta e la quinta parola sono rispettivamente riservate all'indirizzo Ip sorgente e destinazione.

Altri campi particolarmente significativi sono

- il Type Of Service, che sono 8 bit riservati alla priorità del pacchetto, rappresentando così un tentativo di QoS,

- e il Time To Live, in cui si indica il numero massimo di hop; viene utilizzato per evitare che un pacchetto cicli a vuoto a causa di inconsistenze nelle tabelle di instradamento.

 **Network Address (and Port) Translation** 35

Il NAT è una tecnica, che consiste nel modificare gli indirizzi IP di un pacchetto in transito


IP masquerading

- Particolare utilizzo del NATTING che consente ai molteplici computer di una rete privata di utilizzare un singolo indirizzo IP (pubblico) per accedere ad Internet
- Risolve il problema del "limitato" numero di indirizzi IP disponibili
- Nasconde dall'esterno la rete privata

Impianti Informatici POLITECNICO DI MILANO

Il NAT, ovvero il Network Address and Port Translation, è già stato introdotto parlando di indirizzi privati.

- Più in generale il NATTING è una tecnica che consiste nel modificare gli indirizzi ip di un pacchetto in transito
- Quando tale meccanismo viene utilizzato per permettere a molteplici host di una rete privata di accedere ad internet mediante un singolo indirizzo pubblico, si parla di IP masquerading. Si tenga inoltre conto del costo non indifferente degli indirizzi ip.
- Il suo uso ha come ulteriore effetto quello di ridimensionare il problema emergente del limitato numero di indirizzi ip disponibili.
- Inoltre il NATTING permette implicitamente di aumentare la sicurezza del sistema, bloccando i pacchetti in ingresso non attesi e nascondendo la struttura della rete privata.

 **Funzionamento di NAT** 36

Cambia alcune informazioni negli header dei messaggi:

- Source address -> Indirizzo IP pubblico
- Source port -> Una porta qualsiasi disponibile

Memorizza in apposite tabelle le modifiche apportate

- Tali informazioni vengono utilizzate per traslare i messaggi di risposta, così da farli pervenire all'host (e al servizio) corretto
- A seconda che si stia modificando l'indirizzo IP sorgente o destinazione, si parla di:
  - Source NAT
  - Destination NAT

Impianti Informatici **POLITECNICO DI MILANO**

- Concretamente il NAT modifica alcune delle informazioni presenti negli header dei messaggi. In particolare, quando un host con indirizzo privato vuole inviare un pacchetto su internet,
- la napt box modifica l'indirizzo sorgente con un indirizzo ip pubblico che ha a disposizione
- e cambia la porta sorgente con una porta qualsiasi disponibile.
- Le modifiche apportate vengono memorizzate in opportune tabelle,
- così da garantire la traslazione all'indietro dei messaggi di risposta. Infatti il pacchetto in risposta ha come indirizzo ip quello dello pubblico e come porta quella precedentemente assegnata. Occorre convertire i due campi con l'indirizzo ip privato dell'host e con la porta corretta precedentemente impostata.
- A seconda che si stiano modificando le informazioni sull'host sorgente o quelle sull'host destinazione, si parla rispettivamente di Source NAT o Destination NAT

37

**Esempio di NAT**

Private Address	Private Port	External Address	Ext. Port	Protocol Used	NAT Address	NAT Port
→ 192.168.0.1	13	81.231.110.1	80	TCP	91.168.0.15	231
192.168.0.6	66	81.231.110.1	80	TCP	91.168.0.15	115
192.168.0.4	12	211.1.9.115	21	TCP	91.168.0.15	231

Impianti Informatici      POLITECNICO DI MILANO

La figura mostra un esempio di tabella di traslazione. La situazione è quella di una classica rete aziendale indirizzata con un indirizzi privati, che dispone di un unico indirizzo ip pubblico.


Quando un host, ad esempio il 192.168.0.1, vuole comunicare con un server esterno alla rete aziendale, ad esempio collegandosi ad una pagina web, genera uno o più pacchetti destinati a tale applicazione remota. La NAT box cambia l'ip sorgente e la porta sorgente con l'ip pubblico 91.168.0.15 e una porta a caso, ad esempio la 231

•e memorizza la traslazione nella tabella. Quando il server web risponde con un pacchetto, l'indirizzo ip di destinazione sarà 91.168.0.15, e la porta la porta 231. La NAT box riceve il pacchetto, analizza l'header ed individua nella prima riga della tabella la corretta traslazione. L'external address è infatti quello del server web, così come la external port è la porta 80; inoltre corrispondono TCP e NAT port. Mediante questi campi è possibile la corretta traslazione inversa.

•Si noti come una connessione viene identificata da molteplici campi, così da garantire che anche un numero elevato di host possa utilizzare contemporaneamente lo stesso indirizzo pubblico. Ad esempio è possibile utilizzare la stessa porta 231 per due connessioni dato che l'external address è differente.

91.168.0.15

NAPT BOX




## IPv6 (Next Generation Protocol)

38

**Limitazioni IPv4:**

- Numero di indirizzi limitato ( $2^{32}$  indirizzi non sono più sufficienti)
  - Espansione del numero di utenti della Rete
  - Sottosfruttamento degli indirizzi potenzialmente disponibili
    - le più vecchie assegnazioni disponevano solo di indirizzi classful (/8 /16 /24)
- Parte dei  $2^{32}$  indirizzi è destinata per:
  - Reti private
  - Indirizzi multicast
- Esplosione delle tabelle di routing
- Esigenza di nuove funzionalità:
  - Applicazioni Real Time
  - QoS
  - Security (autenticazione, crittografia)
  - Supporto per il roaming



Impianti Informatici
POLITECNICO DI MILANO

Il protocollo Ip versione 4 viene ormai utilizzato da una trentina di anni. Da diverse esigenze emerge la necessità di un nuovo protocollo, tale protocollo è l'IP versione 6.

• Con la sua introduzione si vuole principalmente ovviare ad alcune limitazioni della precedente versione. Una su tutte è

• Il numero limitato di indirizzi ip. Mentre originariamente  $2^{32}$  indirizzi sembravano più che sufficienti, oggi giorno tale numero risulta piuttosto ridotto. Le motivazioni sono differenti:

• Innanzitutto il numero di utenti è cresciuto enormemente

• Inoltre le prime assegnazioni di indirizzi utilizzavano solo indirizzi di tipo classful, con conseguente sottosfruttamento degli indirizzi potenziali

• Una parte dei 4 miliardi di indirizzi è destinata alle reti private e ai gruppi multicast

• Un altro problema dell'ip versione 4 è l'esplosione delle tabelle di routing

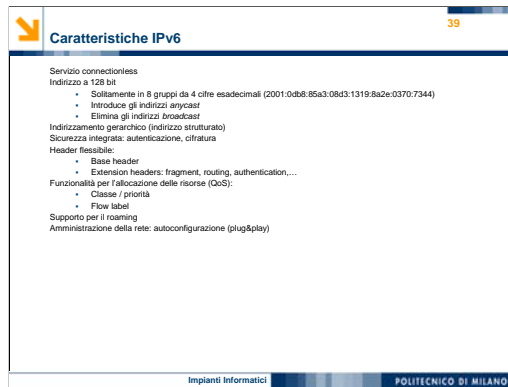
• E alla nascita di nuove esigenze, quali

• La diffusione delle applicazioni real time

• La necessità di garantire una certa Qualità del servizio


• L'integrazione di meccanismi di sicurezza

• Il supporto x il roaming da una rete all'altra




L'ip versione 6 continua ad offrire

- un servizio connection-less, Caratteristiche peculiari sono invece
  - gli indirizzi allungati a 128 bit, solitamente indicati in 8 gruppi notazione esadecimale; vengono inoltre aboliti gli indirizzi di broadcast ed introdotti quelli anycast. Un pacchetto destinato ad uno di questi indirizzi viene instradato ad uno degli host di tale gruppo, tipicamente all'host più vicino.
  - I 128 bit dell'indirizzo sono ben strutturati, garantendo un indirizzamento gerarchico delle reti, e quindi un utilizzo più efficiente delle tabelle di instradamento
  - Vengono inoltre integrati meccanismi per autenticazione e cifratura
  - L'header diventa flessibile, ed è costituito da un header di base, più eventuali header aggiuntivi, a seconda delle funzionalità richieste, quali ad esempio la frammentazione..
  - Particolari campi sono destinati all'allocazione delle risorse in termini di quality of service
  - Così come al supporto x il roaming
  - E alla semplificazione dell'amministrazione della rete mediante autoconfigurazione
- Nonostante i notevoli benefici l'ip v6 non si è diffuso ancora particolarmente diffuso, dovuto sia alle difficoltà ed ai costi di passaggio, sia al fatto che la principale motivazione, ovvero il numero limitato di indirizzi ip della versione 4, è stato parzialmente risolto con l'uso del NATING


**Domain Name System**
40

È un protocollo applicativo che si appoggia su UDP  
 Consente di utilizzare stringhe, anziché indirizzi IP, per identificare un host  
 Associa all'indirizzo numerico di un host un nome simbolico (ad esempio **www.polimi.it**) composto da una serie di label (**www**, **polimi** e **it** sono label)  
 Ogni label è assegnata da una *naming authority*


- Ciascuna di esse è strettamente inclusa in una o più authority più grandi, così da creare una gerarchia di nomi
- Tale gerarchia di inclusione va da destra a sinistra: la prima label (a sinistra) identifica il nome della macchina (o del servizio)



Impianti Informatici
 POLITECNICO DI MILANO

- Il DNS è un protocollo applicativo che si utilizza UDP come livello di trasporto.
- Esso permette identificare un host mediante l'utilizzo di stringhe alfanumeriche, anziché tramite l'indirizzo IP
- L'indirizzo ip viene infatti associato ad un nome simbolico, composto da una serie di label
- Ogni label viene assegnata dalla naming authority responsabile. Si viene perciò a creare una gerarchia di nomi, che va da destra verso sinistra. La label più a sinistra identifica la macchina o il servizio





Domain Name System
41

Ogni nome corrisponde ad un *dominio*

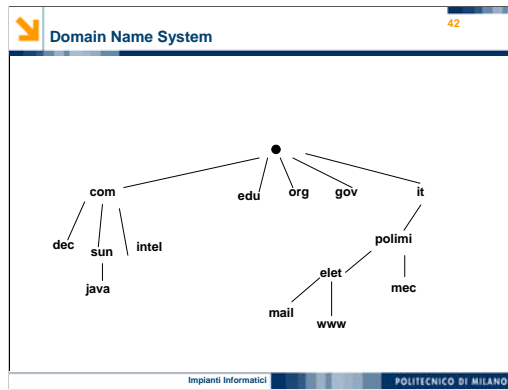
- La gerarchia dei nomi è sia geografica che organizzativa
- I domini di livello 1 sono, ad es:
  - com, edu, org, gov, it, fr, de...
- I server *DNS* consentono la risoluzione (restituendo l'indirizzo IP corrispondente ad un dato dominio)
  - Se un server DNS non sa risolvere un indirizzo manda la richiesta ad un server di livello superiore
  - La risoluzione degli indirizzi può essere:
    - Iterativa
    - Ricorsiva

Il nome di dominio va registrato presso l'InterNIC (Internet Network Information Center)

- Ciò assicura l'unicità del nome e la sua associazione ai numeri che identificano le macchine usate dal richiedente

Immagini Informatiche
POLITECNICO DI MILANO

- Ogni label corrisponde ad un dominio
- La ripartizione gerarchica dei nomi non segue rigidi schemi e può essere sia gerarchica che organizzativa. Esempio di domini di primo livello sono com, edu, org, it..
- La risoluzione di una stringa in un indirizzo ip viene effettuata da appositi server DNS. Se il server sa risolvere direttamente un dominio risponde immediatamente al richiedente, altrimenti manda la richiesta ad un server dns di livello superiore. Tale risoluzione indiretta può essere fatta sia in maniera iterativa che ricorsiva.
- Per assicurare l'unicità delle label e la corretta associazione nome-indirizzo ip, occorre registrare il dominio presso l'internet network information center.



In figura viene mostrato un esempio di gerarchia di nomi. A livello 1 si trovano i domini com, edu, org, gov e it. Ciascuno può a sua volta essere comprendere uno o più domini di livello 2: polimi è uno di questi. La gerarchia prosegue fino ai domini foglia, quale mail oppure www che individuano una precisa macchina oppure un particolare servizio offerto.