Laurea specialistica in Fisica

Anno accademico 2010/11

Uso e funzionamento della rete

Leandro Lanzi

26 ottobre 2010

Premessa

Questi pochi appunti non sono delle vere *dispense* sull'argomento, ma sono solo poco di più di un elenco di informazioni.

Si tratta di un semplice promemoria su Internet che penso possa essere di aiuto ad un fisico, prossimo alla laurea, per conoscere i concetti fondamentali delle reti informatiche e gli strumenti che queste offrono in modo da poterli usare al meglio nel loro futuro lavoro di ricerca.

26 ottobre 2010 Leandro Lanzi

Reti informatiche

- Con il termine "**Rete**" si indica una qualsiasi interconnessione fra dispositivi, detti **nodi della rete**.
- In una rete informatica i nodi della rete sono degli elaboratori che permettono ad una popolazione distribuita di utenti lo scambio e la condivisione di risorse (sia hardware che software).

Classificazione delle reti informatiche

- Le reti informatiche possono essere classificate secondo diversi criteri:
  - il **canale trasmissivo**;
  - l'**estensione geografica**;
  - la **topologia**.

Canale trasmissivo

- Cominciamo con l'esaminare i tipi di collegamenti che permettono di mettere in comunicazione computer, stampanti, modem, router e tutti gli apparecchi che possono far parte di una rete.
- Le informazioni da trasportare sono delle sequenze di bit, quindi si possono usare
  - coppie di conduttori per trasportare un segnale elettrico;
  - fibre ottiche per trasportare un segnale luminoso;
  - lo spazio libero per trasportare onde elettromagnetiche.
- Cercando su Internet ci sono anche soluzioni curiose tipo trasduttori per realizzare reti informatiche tramite onde sonore che ovviamente non hanno un'applicazione pratica.
- Nel Dipartimento di Fisica, per esempio, si trovano rami di rete che usano tutti e tre i tipi di canali trasmissivi:
  - il cablaggio strutturato di tutto l'edificio è realizzato tramite cavi UTP (unshielded twisted pair, cioè doppino intrecciato non schermato), tipicamente di categoria 5 o superiore;
  - i collegamenti fra particolari dispositivi di rete che trovate nei corridoi (gli switch) sono realizzati in fibra ottica;
  - inoltre è disponibile praticamente ovunque l'accesso wi-fi, quindi tramite onde elettromagnetiche.
- La categoria in un cavo UTP indica la qualità del cavo: più alta è la categoria e maggiore è la velocità di trasmissione che il cavo può reggere.
- Ogni mezzo trasmissivo ha pregi e difetti nonché limiti di funzionamento dovuti agli aspetti fisici che riguardano la propagazione del segnale.
- Per esempio il doppino in rame costa poco, si maneggia facilmente, è resistente ma è fortemente influenzato dal fenomeno dell'interferenza elettromagnetica e dell'attenuazione del segnale.
- Le fibre ottiche non sono soggette all'interferenza elettromagnetica e scarsamente all'attenuazione del segnale, ma hanno costi molto più alti (soprattutto per i connettori, cioè i trasduttori ottici), sono meno maneggevoli e più delicate.
- Le onde elettromagnetiche possono avere il problema delle zone d'ombra e, usando un mezzo condiviso, possono avere forti implicazioni riguardo alla riservatezza dei dati trasmessi. Un altro aspetto da considerare per le onde elettromagnetiche è l'aspetto di congestione della comunicazione tipico dei mezzi condivisi.

- Viene scelto di usare uno dei mezzi trasmissivi a disposizione in base ai parametri fisici che li caratterizzano come ad esempio
  - la frequenza massima di trasmissione del segnale,
  - l'attenuazione del segnale,
  - il ritardo nella propagazione del segnale,
  - la distorsione del segnale.

Estensione geografica

Reti personali (Personal Area Network, PAN)

- Il collegamento ethernet o wi-fi fra il vostro pc e il vostro router ADSL è un esempio di collegamento di una rete PAN.
- Le reti PAN si estendono per decine di metri per esempio in un appartamento, in uno o più uffici o in un locale pubblico.
- Tipicamente una PAN è realizzata tramite cavi UTP oppure tramite wi-fi, ma possono essere utilizzati anche cavi USB o IEEE1394 (firewire) oppure il bluetooth o il collegamento a infrarossi (IrDA).
- Un cavo UTP può attualmente reggere una frequenza di trasmissione fino ad 1 Gbps mentre le reti wi-fi tipicamente lavorano intorno ai 10 Mbps.
- Nelle reti Fast Ethernet la velocità nominale di trasferimento è 100Mbps e si realizzano o con cavi UTP (Cat 5) oppure in fibra ottica.
- La frequenza di trasmissione del Bluetooth 2.0 è di 3 Mbps e funziona nel raggio di pochi metri.
- Per quanto riguarda il collegamento ad infrarossi (IrDA) si raggiungono frequenze di 16 Mbps ma emettitore e ricevitore devono "guardarsi" entro un angolo di accettazione tipicamente di una decina di gradi.

Reti locali (Local Area Network, LAN)

- Le LAN si estendono per centinaia di metri o qualche chilometro.
- Si sviluppano all'interno di singoli edifici o edifici adiacenti.
- Attualmente usano per la maggior parte cavi UTP con RJ-45 oppure fibra ottica soprattutto per i collegamenti principali.
- Negli ultimi anni le soluzioni wireless sono state particolarmente apprezzate, tra queste il wi-fi (standard IEEE 802.11) e recentemente il WiMAX (standard IEEE 802.16).
- Velocità tipiche per i collegamenti in fibra ottica sono 1Gbps (IEEE 802.3z) e dal 2007 10Gbps (IEEE 802.3-2005).

Campus e reti universitarie (Campus Area Network, CAN)

- Le LAN di università o campus prendono anche il nome di CAN.

Reti metropolitane (Metropolitan Area Network, MAN)

- Si estendono su aree di decine di chilometri, cioè sulle dimensioni metropolitane.
- I canali trasmissivi maggiormente usati attualmente sono la fibra ottica o i ponti radio o [?> Fast

Ethernet, tipo di cavi e velocità <?].

- Un ponte punto-punto in tecnologia laser può usare tranquillamente una frequenza di trasmissione di 1 Gbps.
- I collegamenti tramite modem V92 reggono frequenze massime di 56 Kbps.
- Il servizio telefonia digitale ISDN (Integrated Services Digital Network) ha frequenze di 64 Kbps (o 128 Kbps usando due canali in parallelo).
- La tecnologia ADSL (Asymmetric Digital Subscriber Line) uas il normale doppino telefonico che è in grado di trasmettere segnali a frequenze molto maggiori di quelle utilizza nella comunicazione telefonica. Per farlo necessita di nuovi apparati di commutazione nelle centrali telefoniche e di filtri negli impianti telefonici domestici. Le frequenze di trasmissione possono raggiungere i 12 Mbps (o i 24 Mbps con la ADSL2+).

Reti geografiche (Wide Area Network, WAN)

- Tutte le reti che si estendono su dimensioni maggiori delle aree metropolitane sono WAN.
- Quindi si estendono su distanze da decine di chilometri fino a migliaia di chilometri e collegano l'intero pianeta.
- I canali trasmissivi usati sono la fibra ottica e i ponti radio sia terrestri che satellitari.
- Frequenze di trasmissione tipiche sono di 10 Gbps ed oltre.

Topologia

Rete a stella

- È caratterizzata da un punto centrale, centro-stella, che può essere uno switch o un elaboratore e diversi host connessi ad esso.
- La rete a stella diventa **a stella estesa** quando al posto di un host collegato al centro stella c'è un altro apparato attivo, switch o hub, con a sua volta altri host collegati ad esso.
- Pregi
  - un guasto ad un host non compromette le comunicazioni degli altri;
  - comunicazioni sicure e difficilmente intercettabili tra un host e l'altro (con l'uso dello switch);
  - basso traffico di pacchetti per gli host (con l'uso dello switch).
- Difetti
  - elevato traffico sul centro-stella;
  - rottura del centro-stella con conseguente interruzione delle comunicazioni per tutti gli host.

Rete a bus

- Ogni host è collegato in modo lineare attraverso un cavo (linea, dorsale o segmento).
- Pregi
  - reti semplici da realizzare e poco costose.
- Difetti
  - ogni computer può intercettare le comunicazioni altrui;
  - elevato traffico in tutta la rete;

- sensibile ai guasti;
- difficile trovare il guasto.

Rete ad anello

- La più famosa rete ad anello è la rete **Token Ring**, ovvero una rete ad anello con passaggio del testimone, in cui la determinazione di quale calcolatore abbia diritto a trasmettere avviene tramite un particolare messaggio, detto token.
- Ogni calcolatore è collegato ad altri due formando complessivamente un cerchio.
- All'interno di questa rete solo un calcolatore alla volta può trasmettere e cioè quello in possesso del token. Esso avvia la trasmissione dei dati trasferendoli al calcolatore vicino, il quale li prende in consegna se è il destinatario, oppure ripete a sua volta il segnale verso l'altro calcolatore ad esso collegato, così fino a raggiungere il destinatario. Il destinatario legge i dati ma non li toglie dalla rete, perché i dati torneranno al mittente. Sarà il mittente ad eliminare i suoi dati dalla rete e a rimettere in circolo il testimone.
- Quando il calcolatore che è in possesso del token ha terminato la trasmissione dei dati passa il token a quello vicino. Quest'ultimo se deve trasmettere dati inizia la comunicazione, altrimenti cede immediatamente il token senza impegnare il canale. Ogni calcolatore, ogni volta che riceve il token, può trasmettere al massimo un solo frame[1], quindi deve consegnare il token al terminale vicino.
- I dispositivi di rete garantiscono la presenza di un solo token sull'anello, e provvedono a rigenerarne uno qualora questo venga perso a causa di guasti nella rete o al calcolatore che l'ha preso in consegna. Quando un host non trova il token invoca un segnale in cui reclama il token (claim token). Se non riceve il testimone, allora ne crea uno nuovo e diventa il monitor della rete.
- Nelle reti Token Ring, a differenza di altre, un computer malfunzionante viene automaticamente escluso dall'anello consentendo agli altri di continuare a funzionare regolarmente in rete. In altri tipi di reti ad anello, un computer che non funziona può provocare il blocco di tutta la rete.
- Pregi
  - può coprire distanze maggiori di quelle consentite da altre reti senza l'aggiunta di amplificatori di segnale.
- Difetti
  - esiste il rischio che gli host possano intercettare comunicazioni altrui;
  - elevato traffico in tutta la rete;
  - il guasto di un host può compromette la trasmissione di dati a seconda del tipo di rete (non nelle reti Token Ring).

Rete mesh

- Nelle reti mesh non esiste infrastruttura: ogni nodo che fa parte della rete deve anche provvedere ad instradare i dati che non sono diretti ad esso, si comporta a grandi linee come un router[2].
- Molte tecnologie (Bluetooth, WiFi,WiMAX) permettono di creare reti mesh.
- Pregi
  - reti semplici da realizzare, non hanno bisogno di infrastruttura, quindi possono essere create ad-hoc per uno scopo e poi spostate;
  - facilmente estendibili.

1 Vedi dopo: definizione di frame nella sezione "Livelli di protocollo di Internet (stack TCP/IP)".
2 Vedi dopo: "Sistemi intermedi".

- Difetti
  - usano protocolli di routing, gestione e sicurezza molto complicati;
  - il mezzo fisico (normalmente wireless) è condiviso, il che riduce la banda.

Interconnessioni di reti

- Dopo aver parlato di reti isolate, passiamo a considerare reti interconnesse.
- La cosa può sembrare banale, ma in realtà comporta tutta una serie di problemi legati essenzialmente al fatto che reti differenti possono parlare "linguaggi differenti".

  Per esempio due reti possono
  - comunicare a frequenze diverse,
  - usare protocolli di comunicazione diversi.
- Si può presentare la necessità di collegare una LAN (rete locale) privata ad Internet attraverso un host (gateway) sulla rete pubblica attraverso un NAT (Network Address Translation). Questo meccanismo permette agli host della rete locale privata di accedere a tutto Internet. Quando un host della rete privata cerca di contattare un host di Internet invia la richiesta al gateway che si occupa di inoltrare tale richiesta al destinatario e, una volta ricevuta la risposta, di renderla all'host che ha generato la richiesta.

Internet

- Con il termine internetwork (o internet) si indica una "rete di reti".
- La più grande internetwork è **Internet** (con la "I" maiuscola), che connette un numero enorme di reti su scala planetaria.

Utenti di Internet

- Attualmente (31/12/2008) gli utenti di Internet sono 1.57×10^9 e rappresentano il 23% della popolazione mondiale, 6.71×10^9.
- In Europa la percentuale di utenti rispetto alla popolazione è il 49%, mentre in Italia è il 60%.
- La distribuzione degli utenti di Internet nel mondo segue fortemente la distribuzione della ricchezza.

Cenni storici

- I primi progetti di realizzazione di reti fra calcolatori risalgono alla fine degli anni cinquanta.
- Nel 1962 il Dipartimento della Difesa statunitense creò un'agenzia di carattere scientifico ARPA (Advanced Research Project Agency) che coordinasse le informazioni e ottimizzasse le comunicazione tra i vari reparti dell'esercito, marina ed aviazione.
- Uno dei progetti di ARPA fu quello di creare una rete informatica decentrata (in seguito fu denominata ARPA Net) che fosse in grado di mantenere le comunicazioni fra computer in caso di una guerra nucleare.
- Alla fine degli anni '**50** i computer già esistevano ma erano molto diversi da quelli che usiamo oggi.
  - Innanzitutto non era ancora stata sviluppata la microelettronica: i calcolatori occupavano intere stanze.
  - In secondo luogo i sistemi di archiviazione informazioni erano delle schede perforate in cartone

(o bobine di carta) o delle grandi bobine di nastro magnetico.

- Inoltre non esisteva uno standard per il sistema operativo: ogni calcolatore aveva il proprio.

- In queste condizioni si muovevano i ricercatori che hanno sviluppato i primi nodi della rete ARPA Net.
- All'interno del progetto ARPA Net vennero sviluppati e realizzati i primi protocolli di rete alla base di Internet e le prime infrastrutture di rete.
- L'applicazione pratica iniziò alla fine degli anni sessanta quando questa tecnologia è stata usata per collegare i principali centri universitari americani.
- Il **28 ottobre 1969** venne realizzato il primo collegamento (a commutazione di pacchetto) fra i due computer dell'Università della California (UCLA) e dell'Istituto di Ricerca di Stanford e nei mesi successivi si aggiunsero l'Università di Santa Barbara e l'Università dello Utah.
- Nel **1971** i computer collegati in rete erano 23.
- Nel **1973** l'Inghilterra e la Norvegia si unirono alla rete con un computer ciascuno.
- Tutto era pronto per il cruciale passaggio ad Internet, compreso il primo virus telematico: sperimentando sulla velocità di propagazione delle e-mail, a causa di un errore negli header del messaggio, ARPA Net venne totalmente bloccata. Era il **27 ottobre 1980**.
- Nel **1981** nacque in Francia la rete Minitel, che diventerà in breve tempo la più grande rete di computer al di fuori degli USA.
- La nascita della moderna Internet può esser fatta coincidere con il **primo di gennaio del 1983** quando fu resa operativa la prima WAN basata sul protocollo TCP/IP (definito nel 1982) che è quello attualmente usato da Internet (TCP - Transmission Control Protocol, IP - Internet Protocol). Tutti gli host di ARPA Net passarono al nuovo protocollo abbandonando i vecchi protocolli NCP.
- Il **23 giugno 1983** fu ideato il DNS[3] (Domain Name System).
- Dagli **anni '80** le tecnologie che oggi costituiscono la base di Internet cominciarono a diffondersi in tutto il globo (Italia compresa).
- Nel corso degli **anni '90** la popolarità della rete è divenuta massiva in seguito al lancio, nel **1990**, del World Wide Web ad opera di un ricercatore *(a contratto)* del CERN.
- Da allora l'infrastruttura di Internet si è espansa in tutto il mondo per creare la rete mondiale globale di computer che conosciamo oggi.

Descrizione di Internet

- Per descrivere internet si può parlare:
  - dei suoi **componenti hardware** (host, router, switch, hub, ...)
  - delle sue **infrastrutture** (che forniscono servizi alle applicazioni distribuite);
  - dei **protocolli** e dei loro modelli di servizio.
  - della sua **tecnologia alla base della trasmissione dati** (rete a commutazione di pacchetto a datagrammi);
  - di come viene fornito l'**accesso** (reti di accesso, ISP e dorsali Internet);

3 Vedi dopo: “Nomi di dominio e servizio DNS”.

Componenti hardware di Internet

Host e link

- Fino a qualche anno fa si poteva dire che Internet fosse la "Rete mondiale di calcolatori".
- Attualmente possono essere connessi ad internet:
  - calcolatori,
  - strumenti di gestione remota di esperimenti e strumenti di acquisizione dati,
  - sistemi di monitoraggio ambientale,
  - strumentazione industriale,
  - webcam, sistemi di sicurezza,
  - telefoni, PDA, televisori, elettrodomestici,
  - ...
- Per questa varietà di panorama delle utenze di Internet non si parla più di "Rete di calcolatori", ma genericamente di una rete costituita da **host** (ospite) o end-system (sistema terminale).
- Gli host si possono distinguere in due categorie:
  - client,
  - server.
- Si indica con **client** (spesso desktop, laptop, PDA, …) gli host su cui girano uno o più programmi client.
- Un **programma client** è un'applicazione che chiede e riceve un servizio da un programma server in esecuzione su un altro host.
- La distinzione fra client e server non è così netta. Un peer (cioè un host che usa un programma P2P) è client quando richiede dati ad un altro peer, è server quando invia dati ad un altro peer.
- Gli host sono connessi tramite **collegamenti** (**communication link**): cavi coassiali, fili di rame, fibre ottiche, onde elettromagnetiche.
- Collegamenti diversi possono trasmettere dati a frequenze diverse.

Packet switch

- Non tutti gli host sono connessi direttamente uno con l'altro: tipicamente sono connessi fra loro tramite dispositivi di commutazione (switching device) chiamati in TCP/IP anche **packet switch** (**commutatori di pacchetto**).
- Un packet switch prende un elemento di informazione, detto **pacchetto** (**packet**), da un collegamento in ingresso, e lo ritrasmette su uno o più collegamenti in uscita.
- Ogni pacchetto è formato da un'**intestazione (header)** e dal **contenuto (content)**. A seconda del livello nello stack TCP/IP il pacchetto prende nomi specifici[4].
- I packet switch si dividono in tre principali tipologie (a seconda del livello a cui operano[5]):
  - **router**,
  - **switch** (più propriamente **link-layer switch**),

4 Vedi dopo: "Livelli di protocollo di Internet (stack TCP/IP)".
5 Vedi dopo: "Livelli di protocollo di Internet (stack TCP/IP)".

- **hub**.

- La sequenza di collegamenti e commutatori di pacchetto attraversati dal singolo pacchetto da un host ad un altro viene detto **route** (percorso).
- Il collegamento fra due host non avviene con un percorso dedicato, ma viene usata la tecnica nota come **packet switching** (**commutazione di pacchetto**) che consente a più host di condividere uno stesso percorso o parte di esso.

Servizi offerti alle applicazioni distribuite

- Internet può essere descritta tramite i servizi che offre alle applicazioni distribuite sulla rete.
- Internet consente alle applicazioni distribuite eseguite sui singoli host di scambiarsi dati.
- Tali applicazioni comprendono:
  - navigazione sul web,
  - messaggistica istantanea,
  - straming audio e video,
  - telefonia su Internet,
  - giochi distribuiti,
  - condivisione di file tramite peer-to-peer (P2P),
  - autenticazione remota,
  - posta elettronica,
  - …
- Internet fornisce essenzialmente due tipi di servizi alle proprie applicazioni distribuite:
  - un **servizio affidabile orientato alla connessione** (**connection-oriented**) che garantisce che i dati trasmessi da un mittente a un destinatario vengano consegnati in ordine e nella loro completezza;
  - un **servizio non affidabile senza connessione** (**connectionless**) che non dà alcuna garanzia di consegna.
- Normalmente le applicazioni distribuite fanno uso dell'uno o dell'altro servizio, ma non di entrambi.
- Attualmente Internet non fornisce un servizio che dia garanzia sul tempo di consegna dei dati.
- Non è possibile per l'utente ottenere un servizio migliore (per esempio con ritardi limitati) per esempio pagando di più, ad eccezione della frequenza di collegamento con il proprio ISP.

Servizi orientati alla connessione (connection-oriented)

- Il programma client e il programma server (che risiedono su host differenti) si scambiano pacchetti di controllo prima di inviare i packet di dati reali da trasferire. Questa procedura viene detta **handshaking** (stretta di mano).
- Si dice servizio orientato alla connessione piuttosto che servizio con connessione perché la connessione è estremamente lasca e non si realizza fisicamente. In particolare, solo gli host terminali sono consapevoli di questa “connessione”, mentre tutti i packet switch che si trovano sul percorso ne sono completamente all'oscuro.
- In altre parole i packet switch non mantengono nessuna informazione sullo stato della connessione.
- Il servizio connection-oriented di Internet è fornito dal protocollo detto **Trasmission Connection**

Oriented (TCP) che è stato definito nella sua versione finale nella RFC 793[6].

- I servizi forniti da TCP alle applicazioni includono
  - il **trasferimento dati affidabile**,
  - il **controllo di flusso**,
  - il **controllo di congestione**.
- Queste tre caratteristiche (il trasferimento dati affidabile, il controllo di flusso e il controllo di congestione) benché siano integrate in TCP, non sono in alcun modo componenti essenziali del servizio connection-oriented in generale. In altre parole un tipo diverso di rete di calcolatori che non usa TCP può fornire alle proprie applicazioni un servizio connection-oriented senza mettere a disposizione queste tre caratteristiche.
- Le applicazioni si preoccupano soltanto della fornitura dei servizi e non del modo con cui TCP effettivamente implementi l'affidabilità, il controllo di flusso e di congestione.
- La maggior parte delle applicazioni Internet più consuete fa uso di TCP, per esempio:
  - Telnet (per la comunicazione bidirezionale generalizzata),
  - SMTP, IMAP e POP3 (per la posta elettronica),
  - FTP (per il trasferimento di file),
  - HTTP (per il Web),
  - ...
- **Trasferimento di dati affidabile**
  - Con trasferimento di dati affidabile si intende che un'applicazione possa far affidamento sulla connessione per trasportare tutti i dati senza errori e nell'ordine corretto.
  - L'affidabilità di Internet viene conseguita tramite l'uso di acknowledgement (avvisi di ricezione) e ritrasmissioni.
  - Per esempio.
    - Si considera un'applicazione che ha stabilito una connessione fra due host A e B.
    - Quando B riceve un pacchetto da A, B invia ad A un acknowledgement.
    - Quando A riceve tale messaggio, sa che il pacchetto corrispondente è stato ricevuto in maniera definitiva.
    - Se A non riceve un acknowledgement, A assume che il pacchetto non sia stato ricevuto da B e lo ritrasmette.
- **Controllo di flusso**
  - Il controllo di flusso assicura che nessuna estremità della connessione soffochi l'altro partecipante inviando troppi pacchetti ravvicinati net tempo.
  - Internet implementa il controllo di flusso usando buffer di invio e ricezione negli host terminali comunicanti.
- **Controllo della congestione**
  - Il servizio di controllo della congestione di Internet evita che la rete entri in uno stato di ingorgo.
  - Quando il traffico in un packet switch raggiunge una certa soglia, i suoi buffer possono andare in overflow (cioè si possono saturare) e si può verificare perdita di pacchetti.
  - In tali circostanze, se ogni coppia di host terminali continuasse ad inviare pacchetti alla massima

6 RFC: vedi dopo.

frequenza si renderebbe ancora più critico l'ingorgo di dati.

- Internet evita questo problema forzando i sistemi terminali a decrementare la frequenza di invio di pacchetti nei momenti di traffico intenso.
- I sistemi terminali assumono l'esistenza di traffico intenso quando smettono di ricevere gli acknowledgement dei pacchetti inviati.

Servizi senza connessione (connectionless)

- Il servizio connectionless (senza connessione) di Internet non prevede né handshaking né acknowledgement.
- Quando un'applicazione vuole trasmettere pacchetti, il programma d'invio non fa altro che spedirli direttamente all'altra parte.
- Pertanto la consegna dei dati può essere più rapida.
- Questo rende il servizio connectionless particolarmente indicato per applicazioni multimediali quali la fonia via Internet o la videoconferenza.
- Il servizio connectionless:
  - in assenza di un trasferimento di dati affidabile, il mittente non sa quali pacchetti siano arrivati a destinazione;
  - non mette a disposizione il controllo di flusso;
  - non mette a disposizione il controllo di congestione.
- Il servizio connectionless di Internet è fornito dal protocollo detto **User Datagram Protocol (UDP)** ed è definito nella RFC 768[7].

Protocolli

- Tutti i componenti di Internet (host, packet switch) fanno uso di **protocolli** che controllano l'invio e la ricezione di pacchetti.
- Un **protocollo di rete** definisce il formato e l'ordine dei messaggi scambiati tra due o più entità in comunicazione, così come le azioni intraprese in fase di trasmissione e/o di ricezione di un messaggio o di un altro evento.
- In generale in Internet si usano protocolli diversi per realizzare compiti diversi .
- Attualmente i due più importanti protocolli di Internet sono:
  - **Transmission Control Protocol (TCP)**;
  - **Internet Protocol (IP)**.
- Tutti i protocolli di Internet sono noti con il nome collettivo di **TCP/IP**.
- Tutte le caratteristiche e le funzioni di ogni singolo protocollo sono definite dagli standard Internet.
- Gli standard Internet vengono sviluppati dall'**Internet Engineering Task Force (IETF)**.
- La documentazione degli standard Internet viene detta **Request for Comment (RFC)**.
- Inizialmente le RFC erano appunto delle richieste generiche di commento per risolvere problemi di architettura sulle reti precedenti a Internet. Attualmente sono documenti tecnici molto dettagliati con tutte le specifiche per ogni aspetto della rete.
- Fra le RFC si trovano:

7 RFC: vedi dopo.

- le specifiche dei protocolli di Internet, tra cui:
  - **DHCP (Dynamic Host Configuration Protocol)**, RFC 2131, RFC 1534, RFC 2132;
  - **HTTP (Hyper Text Transfer Protocol)**, RFC 1945, , RFC 2616;
  - **HTTPS (HTTP Over TLS)**, RFC 2818;
  - **SMTP (Simple Mail Transfer Protocol)**, RFC 821, RFC 1123, RFC 1425, RFC 1651 (rimpiazza RFC 1425), RFC 1869 (rimpiazza RFC 1651), RFC 1891 (corregge RFC 1869), RFC 2821 (rimpiazza RFC 821, RFC 1123, RFC 1869), RFC 2822;
  - **POP3 (Post Office Protocol)** , RFC 937 (POP versione 2), RFC 1939 POP versione 3, RFC 1734, RFC 1957, RFC 3206;
  - **IMAP (Internet Message Access Protocol)**, RFC 4551, RFC 4549, RFC 4469, RFC 4467, RFC 4466, RFC 4315, RFC 4314, RFC 3691, RFC 3656, RFC 3516, RFC 3503, RFC 3502, RFC 3501, RFC 3348, RFC 3028, RFC 2971, RFC 2821, RFC 2683, RFC 2595, RFC 2359, RFC 2342, RFC 2244, RFC 2221, RFC 2195, RFC 2193, RFC 2192, IMAP4, RFC 2177, RFC 2095, RFC 2088, RFC 2087, RFC 2086, RFC 2062, RFC 2061, RFC 1939, RFC 1733, RFC 1732, RFC 1731.
  - **FTP (File Transfer Protocol)**, RFC 959, RFC 2228, RFC 2640, RFC 4217;
  - **DNS (Domain Name System)**, RFC 882, RFC 883, RFC 1034, RFC 1035;
  - **SSH (Secure SHell)**, RFC 4250, RFC 4251, RFC 4252, RFC 4253, RFC 4254;
  - **IRC (Internet Message Access Protocol)**, RFC 1459;
  - **SNMP (Simple Network Management Protocol)**, RFC 1157, RFC 1441, RFC 3410, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, RFC 3418, RFC 3584, RFC 3512;
  - **SIP (Session Initiation Protocol)**, RFC 3261;
  - **RTSP (Real Time Streaming Protocol)**, RFC 2326, RFC 3550;
  - **Telnet (per la comunicazione bidirezionale)**, RFC 854, RFC 855;
  - **HSRP (Hot Standby Router Protocol)**, RFC 2281;
  - **RTP (Real-time Transport Protocol)**, RFC 3550, RFC 1889;
  - **BGP (Border Gateway Protocol)**, RFC 4271, RFC 3392, RFC 3065, RFC 2918, RFC 2796, RFC 1965, RFC 1772, RFC 1771, RFC 1657, RFC 1655, RFC 1654, RFC 1105;
  - **RIP (Routing Information Protocol)**, RFC 2453, RFC 2082, RFC 1058, RFC 2080;
  - ...
- i protocolli eseguibili dagli **host** (RFC 1122, RFC 1123);
- i protocolli eseguibili dai **router** (RFC 1812);
- gli standard per **componenti hardware** di rete o per i **collegamenti di rete**; per esempio IEEE 802 LAN/MAN Standard Committee (IEEE 802 2004) specifica lo standard Ethernet e wireless Wi-Fi.

- Le RFC sono in continua evoluzione: oltre a quelle che affrontano nuovi argomenti, escono sempre nuove RFC che approfondiscono, modificano o sostituiscono vecchie RFC.
- Ad oggi ci sono circa 5500 RFC.

Tecnologia alla base della trasmissione dati

- Esistono due fondamentali approcci per costruire un metodo di comunicazione fra due nodi terminali di una rete:
  - la **commutazione di circuito**,
  - la **commutazione di pacchetto**.
- Diversamente da altre reti di comunicazione, come ad esempio quella telefonica che usa una comunicazione a commutazione di circuito, Internet usa una comunicazione a commutazione di pacchetto.

Commutazione di circuito

- Nella commutazione di circuito le risorse richieste lungo un percorso per consentire la comunicazione fra host terminali sono riservate per l'intera durata della sessione di comunicazione.
- Prima di poter comunicare si deve creare un ben preciso collegamento fra i due host detto circuito.
- Quando viene stabilito un circuito viene riservata una frequenza di trasmissione costante nei collegamenti per tutta la durata della connessione: il mittente può trasferire dati ad una frequenza di trasmissione costante e garantita. In altre parole viene garantita una certa larghezza di banda.
- Tutti i nodi della rete che rendono disponibile il circuito fra host terminali sono informati dello stato della connessione.
- Le reti telefoniche sono esempi di reti a commutazione di circuito.

Commutazione di pacchetto

- Nella commutazione di pacchetto le risorse non sono riservate: i messaggi di una sessione usano le risorse su richiesta e di conseguenza possono dover attendere (cioè mettersi in coda) per accedere ad un collegamento.
- **Internet è una rete a commutazione di pacchetto.**
- Quando un host invia un pacchetto ad un altro host, il pacchetto segue un certo percorso attraverso una serie di collegamenti senza che gli sia riservata alcuna frazione di banda.
- Se un collegamento è congestionato, allora il pacchetto in questione dovrà attendere in un opportuno buffer e subirà un ritardo.
- Internet dà un servizio **best effort** (massimo sforzo possibile) per consegnare i pacchetto in modo temporizzato ma non garantisce il successo.
- In particolare, Internet è una rete a **commutazione di pacchetto a datagramma** (esistono anche le reti a commutazione di pacchetto a circuito virtuale).
- Il funzionamento delle reti a datagrammi è assimilabile a quello del servizio postale, che usa il recapito del messaggio per instradarlo verso la sua destinazione in modo gerarchico. Per il servizio postale la struttura gerarchica che definisce il destinatario è rappresentata dallo stato, il capoluogo di provincia, il comune, la via ed infine il numero civico.
- Ogni pacchetto che attraversa una rete a datagrammi contiene nella sua intestazione l'indirizzo del destinatario che presenta una struttura gerarchica.
- I pacchetti vengono trasmessi in rete indipendentemente l’uno dall’altro; ogni nodo intermedio elabora l’intestazione e inoltra il pacchetto al nodo successivo verso la destinazione secondo una tabella di instradamento che mappa gli indirizzi di destinazione (o loro parti) verso un collegamento uscente. In questo modo viene determinato il percorso attraverso la rete (**instradamento**).

- In altre parole, quando un pacchetto giunge ad un commutatore di pacchetto, questo esamina la destinazione del pacchetto e la confronta con la propria tabella di instradamento per determinare il collegamento uscente da usare.
- Le reti a datagrammi non mantengono informazioni sullo stato delle connessioni nei propri commutatori per cui i pacchetti possono seguire percorsi differenti attraverso la rete, possono arrivare in un ordine diverso da quello di partenza e si possono perdere.
- In una rete a commutazione di pacchetto non si hanno risorse dedicate ma condivise e sono soggette a **problemi di congestione** al variare istantaneo del traffico.
- I nodi hanno delle code (buffer) in cui immagazzinano i pacchetti in arrivo (in attesa di essere elaborati); queste code si possono riempire provocando la perdita di alcuni pacchetti.

Accesso ad Internet

- Quando si parla di accesso alla rete si considera il collegamento o i collegamenti fisici che connettono un host al proprio **edge router**, cioè al primo router sul percorso dall'host ad un qualsiasi altro host distante.
- In altre parole, si considera l'infrastruttura che permette il collegamento di un host ad Internet, detta la **rete d'accesso**.
- Le reti d'accesso possono essere catalogate in tre categorie estremamente non rigide:
  - **accesso residenziale**, connette le residenze private alla rete;
  - **accesso aziendale**, connette host di uffici, istituti, università, … alla rete;
  - **accesso wireless**, connette host (che spesso sono in movimento) alla rete via etere.

Accesso di tipo residenziale .

- **Modem dial-up V92** (tipicamente a 56 Kbps) su doppino telefonico.
- **Modem ISDN (Integrated Services Digital Network)** su linea telefonica digitale.
- Digital Subscriber Line (DSL).

  Solitamente fornito da una compagnia telefonica, talvolta in partnership con un ISP[8] indipendente. Si tratta di un accesso tramite modem su doppino telefonico progettati per sfruttare la vicinanza fisica fra host e ISP.
- Hybrid fiber-coaxial Cable (HFC) .

  Sono l'estensione delle normali reti per la televisione via cavo.

  Tipicamente si connette con fibre ottiche l'ISP e i nodi a livello di quartieri. Le singole abitazioni sono collegate tramite cavo coassiale ai nodi in fibra ottica.
- ADSL (Asymmetric Digital Subscriber Line)

  Usa il normale doppino telefonico che è in grado di trasmettere segnali a frequenze molto maggiori di quelle usate nella comunicazione telefonica. Per farlo necessita di nuovi apparati di commutazione nelle centrali telefoniche e di filtri negli impianti telefonici domestici.

Accesso aziendale

- Nelle aziende, università, istituti, edifici pubblici si usa normalmente una **rete locale (LAN, Local Area Network)** per collegare gli host all'edge router.

8 Vedi dopo: ISP e dorsali Internet

- Attualmente la **tecnologia Ethernet** è la più diffusa.
- I collegamenti fisici fra host e edge router sono realizzati tipicamente tramite cavi UTP o fibra ottica.

Accesso wireless

- In una **Wireless local area network** (Wireless LAN, rete locale wireless) gli host sono in collegamento con una stazione base, detta **wireless access point**, tipicamente entro poche decine di metri.
  - Gli access point sono generalmente connessi ad Internet tramite una rete cablata.
  - Una Wireless LAN basata sullo standard **IEEE 802.11** è nota come **Wireless Ethernet** o **Wi-Fi**.
- In una **Wide-Area Wireless Access Network** (rete d'accesso wireless geografica) tipicamente un provider di telecomunicazioni serve utenti in un raggio di chilometri.
  - In passato è stata usata la tecnologia **WAP (Wireless Access Protocol)** per collegare per esempio cellulari ad Internet.
  - In Europa il protocollo WAP è interfacciato con i protocolli **GSM**.
  - **WAP 2.0** opera su una pila di protocolli TCP/IP[9].
  - Attualmente la tecnologia **3G** usa accesso a commutazione di pacchetto.

ISP e dorsali Internet

- Nell'Internet pubblica le reti di accesso (che connettono il singolo host ad Internet) sono connesse al resto della rete tramite una struttura gerarchica di **ISP (Internet Service Provider)**.
- Gli ISP che forniscono la rete d'accesso ad Internet sono all'estremo inferiore di questa struttura gerarchica.
- All'altro estremo, cioè a capo della struttura gerarchica degli ISP, ci sono i **tier-1 ISP (ISP di livello 1)**.
- Gli ISP di livello 1 sono caratterizzati da:
  - esser connessi a ciascuno degli altri ISP di livello 1,
  - esser connessi a un gran numero di ISP di livello 2,
  - avere copertura internazionale.
- Gli ISP di livello 1 sono anche detti **reti dorsali di Internet (Internet Backbone Network)**. Tra queste ci sono:
  - AT&T ,
  - Global Crossing (GBLX) ,
  - Level 3 Communications (L3) ,
  - NTT Communications (Verio) (in origine TLGnet) ,
  - Qwest ,
  - Sprint ,
  - Verizon Business (precedentemente UUNET) ,
  - SAVVIS ,
  - TeliaSonera International Carrier.

9 Vedi dopo: “Livelli di protocollo di Internet (stack TCP/IP)”.

- Gli ISP di livello 2 hanno una copertura distrettuale o nazionale.
- Gli ISP di livello 2 si connettono solo ad alcuni ISP di livello 1.
- Per raggiungere una grande porzione della rete globale un ISP di livello 2 deve instradare il traffico attraverso un ISP di livello 1.
- Un ISP di livello 2 viene detto **cliente (customer)** dell'ISP di livello 1 cui si connette, mentre quest'ultimo viene detto **fornitore (provider)** del primo.
- Molte grandi aziende, istituti, università collegano direttamente la propria rete LAN ad ISP di livello 2 o di livello 1.
- Al di sotto del livello 2 ci sono altri ISP che si collegano ad Internet tramite uno o più ISP di livello 2.
- Al gradino più basso si trovano gli **ISP d'accesso ad Internet** .
- Quando due ISP dello stesso livello sono direttamente interconnessi sono detti pari grado (**peer**).
- In una rete di ISP, il punto in cui un ISP si collega ad altri (inferiori, superiori o paritari) è detto punto di presenza (**POP, Point of Presence**).
- Un ISP di livello 1 ha tipicamente molti POP in varie locazioni geografiche della propria rete.

  Le reti client di altri ISP si collegano a questi POP.
- Per connettersi ad un ISP fornitore, di solito un ISP client affitta un collegamento ad alta velocità da una terza parte fornitrice di connettività e collega direttamente un proprio router al POP del fornitore.
- Due ISP di livello 1 possono connettersi fra loro con uno, due o più coppie di POP, cioè possono presentare **più punti di peering**.
- Oltre a collegarsi vicendevolmente in punti privati di peering, gli ISP spesso si collegano presso **punti di accesso alla rete (NAP, Network Access Point)** ciascuno dei quali è di proprietà e viene gestito da una terza parte (tipicamente che si occupa di telecomunicazioni o da un fornitore di dorsale Internet).
- I NAP scambiano grandi quantità di traffico con molti ISP.
- La tendenza per gli ISP di livello 1 è quella di interconnettersi direttamente tramite POP privati.
- La tendenza per gli ISP di livello 2 è quella di interconnettersi direttamente tramite POP privati ad ISP di livello 2 e tramite NAP ad ISP di livello 1.

Livelli di protocollo di Internet (stack TCP/IP)

- Per capire quale sia l'importanza di una progettazione di comunicazione a livelli consideriamo un semplice esempio di comunicazione fra due persone: consideriamo che il Sig. Rossi (italiano) voglia inviare una comunicazione a Mr. Smith (inglese).
- Il Sig. Rossi dà un testo in italiano ad un interprete che traduce il testo in francese e lo passa ad un segretario che invia un fax al segretario di Mr. Smith.
- Il segretario di Mr. Smith passa il fax in francese al suo interprete che traduce il testo dal francese all'inglese e lo consegna a Mr. Smith.
- Nell'analogia tra questo esempio e i livelli di protocolli in Internet ciascun individuo rappresenta un livello di Internet.
- Si possono fare le seguenti osservazioni riguardo all'esempio.
    - la lingua usata dai due interpreti (così come il metodo di trasmissione usato dai segretari) può essere cambiata senza problemi per gli altri livelli.

      Se gli interpreti decidessero di usare il tedesco anziché il francese, o i segretari decidessero di usare il telefono anziché il fax, non sarebbe necessaria nessuna modifica negli altri livelli (l'unica cosa che non deve cambiare è l'interfaccia verso i livelli superiori o inferiori).
    - In trasmissione, ogni livello riceve i dati dal livello superiore, aggiunge delle informazioni di controllo (ad esempio l'interprete scrive che lingua ha usato) e passa il tutto al livello inferiore.
    - In ricezione ogni livello interpreta le informazioni di controllo, le elimina, e passa i dati al livello superiore.
- L'esempio suggerisce che una comunicazione strutturata a livelli presenta **numerosi vantaggi concettuali e strutturali**:
    - ogni livello del mittente comunica, indipendentemente dai livelli superiori ed inferiori, con il rispettivo livello del destinatario;
    - anche se è definito un protocollo di un certo livello, nessun dato è trasferito direttamente da un livello all'altro su un diverso sistema (ad eccezione del livello più basso);
    - ogni livello può essere sviluppato e aggiornato indipendentemente dagli altri livelli, sempre mantenendo inalterate le interfacce con il livello superiore ed inferiore.
- La comunicazione fra host in Internet è affidata a protocolli che sono organizzati a **livelli (layer)**.
- Ciascun protocollo appartiene ad un livello.
- Sono di interesse i servizi che un livello offre a quello superiore: si tratta del così detto **modello dei servizi (service model) di un livello**.
- Ogni livello fornisce il suo servizio
    - effettuando determinate azioni all'interno del livello stesso,
    - usando i servizi del livello inferiore.
- Per esempio i servizi offerti dal livello N possono includere la consegna affidabile dei messaggi da un lato all'altro della rete.

  Questo può essere implementato usando un servizio di consegna dei messaggi non affidabile al livello N-1 e aggiungendo al livello N la funzionalità di determinare e ritrasmettere i messaggi persi.
- Un livello di protocollo può essere implementato via software, hardware o in modo combinato.
- I **protocolli a livello di applicazione** (come HTTP, per la comunicazione fra client e server Web, e

SMTP, per lo scambio di posta elettronica) sono solitamente implementati solo tramite software.

- Anche il **livello del trasporto** è implementato via software.
- I livelli più bassi, **fisico e di collegamento**, sono implementati nell'hardware.
- Il livello intermedio, di **rete**, è implementato in modo misto hardware e software.
- La **pila dei protocolli (protocol stack)** di Internet consiste di 5 livelli (in realtà si parla di 3 o 4 o 4+1 o 5 livelli a seconda degli autori e delle RFC)..

N	Livello	Layer	Protocolli	Unità trasmessa (pacchetto)	Usa	Commutatore di pacchetto
5	Applicazione	Apllication	DHCP, HTTP, HTTPS , SMTP, POP3, IMAP, FTP, SFTP, DNS, SSH, IRC, SNMP, SIP, RTSP, RTP, ...	Messaggio	FQDN o IP	- - -
4	Trasporto	Transport	**TCP**, **UDP**, SCTP, DCCP ...	Segmento TCP Datagramma UDP Segmento	Porta	- - -
3	Rete	Network	**IPv4**, IPv6, ICMP, ICMPv6, IGMP, IPsec...	Datagramma	IP	Router
2	Collegamento	Link	**Ethernet**, **WiFi**, PPP, Token ring, ARP, ATM, FDDI, LLC, SLIP, WiMAX, HSDPA, OSPF, MPLS ...	Frame	(in Ethernet) Mac address	Switch
1	Fisico	Physical	- - -	- - -	- - -	Hub

(5) Livello di applicazione (application layer)

- Il livello più alto è il **livello di applicazione (Application layer)**.
- Il livello di applicazione è la sede delle applicazioni di rete e dei relativi protocolli.
- Fra i protocolli del livello applicazione ci sono
  - **DHCP (Dynamic Host Configuration Protocol),** usato dagli host per ottenere la configurazione di rete in modo automatico;
  - **HTTP (Hyper Text Transfer Protocol) e HTTPS (HTTP Over TLS)**, per la comunicazione fra client e server Web;
  - **SMTP (Simple Mail Transfer Protocol)**, per lo scambio di posta elettronica;
  - **POP3 (Post Office Protocol)** e **IMAP (Internet Message Access Protocol)**, per l'accesso agli account di posta elettronica;
  - **FTP (File Transfer Protocol)**, per la trasmissione dati;
  - **IRC (Internet Message Access Protocol)**, per la messaggistica istantanea;

        - **SNMP (Simple Network Management Protocol)**, per l'amministrazione e la supervisione di apparati collegati in rete;
        - **SIP (Session Initiation Protocol)**, per applicazioni di telefonia su IP o VoIP;
        - **RTSP (Real Time Streaming Protocol)**, per streaming (flusso di dati) audio e video;
        - **RTP (Real-time Transport Protocol)**, per servizi che necessitano di trasferimento in tempo reale (come l'interattività audio e video);
        - ...
- Il livello di applicazione ospita determinate funzioni come ad esempio la traduzione dei nomi degli host in indirizzi IP[10] di rete a 32 bit avviene tramite il protocollo **DNS (Domain Name System)**[11].

(4) Livello di trasporto (transport layer)

- Il livello di trasporto trasferisce i messaggi a livello di applicazione tra il modulo client e server di un'applicazione.
- A questo livello i pacchetti, per essere instradati verso una destinazione contengono nell'header il numero di porta di destinazione[12] (oltre al numero di porta d'origine da usare nell'eventuale risposta).
- In Internet si trovano principalmente due protocolli di trasporto:
    - **TCP (Transmission Control Protocol) - RFC 793**
        - fornisce alle applicazioni un servizio orientato alla connessione,
        - include la consegna garantita dei messaggi a livello di applicazione,
        - include il controllo di flusso,
        - fraziona i messaggi troppo lunghi in segmenti più brevi,
        - favorisce un meccanismo di controllo della congestione;
    - **UDP (User Datagram Protocol) - RFC 768**
        - fornisce alle applicazioni un servizio senza connessione.
- I pacchetti a livello di trasporto vengono chiamati **segmenti**.
- Per essere più precisi solo i pacchetti TCP vengono chiamati segmenti, mentre i pacchetti UDP sono chiamati datagrammi UDP.

(3) Livello di rete (network layer)

- I pacchetti a livello di rete sono detti **datagrammi**.
- Il protocollo a livello di trasporto (TCP o UDP) in un host origine passa al livello di rete un segmento e un indirizzo IP di destinazione, che server per instradare i pacchetti.
- Nell'intestazione del pacchetto è presente anche lP sorgente per instradare un'eventuale risposta o una segnalazione di errore.
- L'IP di destinazione può essere anche l'indirizzo IP di broadcast.
- Il livello di rete mette a disposizione il meccanismo di consegna del segmento allo strato di trasporto nell'host di destinazione.
- Il livello di rete presenta due principali componenti.

10 Vedi dopo: “Identificazione degli host: mac address, indirizzo IP, FQDN” e “Indirizzi IP”.
11 Vedi dopo: “Nomi di dominio e servizio DNS”.
12 Vedi dopo: “Numero di porta”.

- Possiede un protocollo (il **protocollo IP**) che definisce i campi del datagramma e come gli host e i router agiscano su tali campi. Esiste un solo protocollo IP e tutti i componenti di Internet che presentano un livello di rete lo devono supportare.
- Possiede protocolli di instradamento che determinano i percorsi che i datagrammi devono seguire. Internet è una rete di reti e ognuna può scegliere il protocollo di instradamento che preferisce.

(2) Livello di collegamento (link layer)

- Il livello di collegamento instrada un datagramma attraverso una serie di commutatori di pacchetto tra l'origine e la destinazione.
- Per trasferire un pacchetto da un nodo (host o commutatore di pacchetto) a quello successivo sul percorso, lo strato di rete passa il datagramma al livello sottostante (collegamento) che lo trasporta al nodo successivo.
- I servizi forniti dallo strato di collegamento dipendono dallo specifico protocollo a livello di collegamento usato.

  Per esempio, alcuni protocolli garantiscono la consegna affidabile sulla base del collegamento, ossia dal nodo che trasmette a quello che riceve. È da notare che questa consegna affidabile non ha niente a che vedere con quella implementata nel TCP, che garantisce la consegna da un host terminale sorgente ad uno di destinazione.
- Un esempio di protocollo del livello di collegamento è **Ethernet**, che instrada i pacchetti in base al mac address del destinatario.
- Dato che i datagrammi devono attraversare diversi collegamenti nel loro viaggio, un datagramma potrebbe essere gestito da differenti protocolli a livello di collegamento lungo le diverse tratte del percorso.
- I pacchetti a livello di collegamento vengono chiamati **frame**.

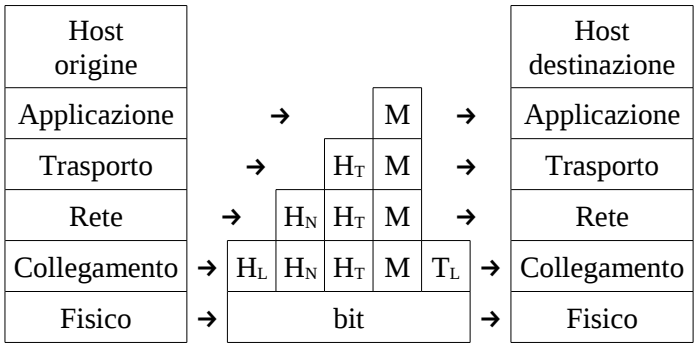
(1) Livello fisico (physical layer)

- Mentre il livello di collegamento si occupa di di spostare interi frame da un elemento della rete a quello adiacente, il ruolo dello strato fisico è quello di **trasferire ogni singolo bit** del frame da un nodo a quello successivo.
- I protocolli a questo livello dipendono sia dal protocollo del livello superiore (di collegamento) che dal mezzo trasmissivo di collegamento.
- Per esempio Ethernet presenta diversi protocolli a livello fisico per
  - il doppino intrecciato,
  - il cavo coassiale,
  - la fibra ottica.

Incapsulamento

- Consideriamo un host di origine che invia un **messaggio (M)** ad un'host di destinazione.
- Presso l'host di origine il messaggio a livello di applicazione viene passato al livello di trasporto.
- Nel caso più semplice il livello del trasporto prende il messaggio e gli concatena informazioni aggiuntive, cioè un'intestazione (header) di livello di trasporto (H_T) che sarà usata dal livello di trasporto dell'host di destinazione, per esempio il **numero di porta**.

- Il messaggio (M) più l'intestazione del livello di trasposto (H_T) costituiscono il **segmento a livello di trasporto (transport-layer segment)** che incapsula il messaggio a livello di applicazione.
- Le informazioni contenute nell'intestazione H_T potrebbero includere
  - dati che consentono allo strato di trasporto sull'host di ricezione di consegnare il messaggio all'applicazione desiderata,
  - bit per il rilevamento di errori.
- Il livello di trasporto passa il segmento al livello di rete che aggiunge una nuova intestazione propria del livello di rete (H_N), come gli **indirizzi IP** degli host di origine e di destinazione creando un **datagramma** a livello di rete.
- Il datagramma a livello di rete viene passato al livello di collegamento, il quale aggiungerà le sue intestazioni (H_L) che, per esempio per Ethernet è il **mac address**, e, diversamente dai livelli più alti, anche una coda (T_L) che identifica la fine del pacchetto creando un **frame** a livello di collegamento.
- Il processo di incapsulamento appena descritto è il più semplice possibile.
- In generale il processo di incapsulamento può essere più complicato, ad esempio un messaggio grande può essere **diviso** in più segmenti a livello di trasporto, i quali possono essere a loro volta divisi in più datagrammi a livello di rete.
- Al momento della ricezione il messaggio originale deve essere ricostruito percorrendo il processo inverso a partire dai frame, per ricostruire i datagrammi e successivamente i segmenti.



Identificazione degli host: mac address, indirizzo IP , FQDN

- Deve esistere un metodo di identificazione univoco per permettere a due host di comunicare fra loro. In altre parole se l'host A vuole comunicare con l'host B deve affidarsi ad un metodo che permetta di identificare in modo univoco l'host B e viceversa.
- Partendo dai livelli più bassi, ogni tipo di rete ha i suoi indirizzi (detti **indirizzi fisici**) che vengono usati al livello 2 (livello di collegamento) per identificare i singoli host connessi alla rete.

  Ad esempio su ethernet si usano indirizzi **MAC address** di 48 bit (per cui gli indirizzi teoricamente disponibili sono 2^{48}, cioè circa 300 mila miliardi), solitamente rappresentati in formato esadecimale ottetto per ottetto, separati da due punti (":").

  Per esempio: 00:1d:09:5d:7d:f2.
- Ogni porta ethernet di ciascun host è identificata in modo univoco dal proprio MAC address che è registrato nel proprio hardware.
- I primi tre numeri del MAC address identificano il costruttore dell'hardware quindi si possono registrare fino a 2^{24} costruttori e ciascuno di essi può produrre 2^{24} dispositivi di rete.

Per esempio: 00:1d:09 identifica Intel®.

Per conoscere i MAC address assegnati ai costruttori di hardware si può consultare la pagina web al link: `http://standards.ieee.org/regauth/oui/index.shtml`

- Quando un host viene messo in rete gli viene assegnato (via software) a livello 3 (livello di rete) un indirizzo IP che identifica in modo univoco il singolo host nella rete.
- Un indirizzo IP è una sequenza di 32 bit (per cui gli indirizzi teoricamente disponibili sono 2^{32}, cioè circa 4,3 miliardi), di solito scritta in decimale ottetto per ottetto (separati da un punto), ad esempio:

  11000000 10101000 00001010 00000001

  192 . 168 . 10 . 1

  Questa notazione è detta **dotted-decimal notation (notazione decimale puntata)**.
- A questo punto si incomincia ad avere più chiaro il motivo della struttura a livelli dei protocolli di Internet.
  - Infatti, già il semplice problema dell'identificazione di un host nella rete, viene risolto in maniera molto versatile usando il **MAC address a livello 2** per identificare la scheda di rete e l'**indirizzo IP a livello 3** per identificare l'host in una rete.
  - Questa prima stratificazione permette per esempio di sostituire la scheda di rete in un host della rete senza dover propagare la notizia all'intera Internet oppure di usare un portatile in reti differenti senza doverne dare notizia al mondo intero.
  - Infatti queste due situazioni vengono risolte localmente a livello di LAN dove ci sono meccanismi efficaci per associare MAC address a IP e viceversa (protocollo ARP[13]).
  - Senza la stratificazione a livelli la soluzione alle due precedenti situazioni non sarebbe così semplice.
- A livello 4 (trasporto) non c'è bisogno di identificare l'host, quanto piuttosto la singola applicazione di rete in esecuzione sull'host, poiché ci possono essere più applicazioni in esecuzione e quando si riceve un pacchetto è necessario sapere a quale applicazione è indirizzato. A tal scopo si utilizza il numero di porta.
- A livello 5 (livello di applicazione) per indicare un host solitamente si usa il suo **nome FQDN (Fully Qualified Domain Name)**, per esempio: `www.fi.infn.it`
- Per associare l'indirizzo IP al FQDN e viceversa, ogni dominio ha un **servizio di DNS (Domain Name System[14])**.
- Ricapitolando, l'identificazione degli host e, con più precisione, di applicazioni in esecuzione sugli host avviane secondo meccanismi differenti a seconda del livello che si sta considerando.
  - A livello d'applicazione (livello 5) il singolo host viene indicato di solito con il suo nome FQDN (Fully Qualified Domain Name), per esempio: www.fi.infn.it.
  - In ogni dominio è attivo un DNS, cioè un servizio usato per la risoluzione di nomi di host in indirizzi IP e viceversa.
  - A livello di trasporto (livello 4) viene usato il numero di porta per identificare le applicazioni di rete interessate alla comunicazione.
  - A livello di rete (livello 3) viene usato l'indirizzo IP, per esempio:192.84.145.12
  - A livello di collegamento (livello 2) viene usato, per esempio dal protocollo ethernet, il MAC address.

13 Vedi dopo: “Protocollo per la risoluzione degli indirizzi (ARP)”
14 Vedi dopo: “Nomi di dominio e servizio DNS”

Sistemi intermedi

- Non sempre lo scambio delle informazioni avviene direttamente tra i due host finali che contengono le applicazioni
- Può anche implicare l'attraversamento di alcuni **sistemi intermedi (IS, Intermediate Systems)**.
- Di questi sistemi intermedi, che servono ad instradare il pacchetto dall'host d'origine a quello di destinazione, ne esistono di vari tipi a seconda del livello dello stack TCP/IP in cui agiscono.

Hub

- Gli hub sono dispositivi hardware dotati di un certo numero di porte e agiscono a **livello fisico (livello 1)**.
- La loro azione è quella di propagare il segnale elettrico proveniente da una porta su tutte le altre porte.
- Non blocca le tempeste di broadcast.

Switch

- Uno switch è un dispositivo hardware che agisce sui pacchetti ethernet e quindi è un dispositivo di **livello 2 (collegamento)** dello standard TCP/IP.
- Trovandosi a livello 2, lavorano sui **mac address**[15].
- Gli switch sono dei commutatori di pacchetto che usano l'indirizzo LAN di destinazione per filtrare e inoltrare i pacchetti.
- Per **filtraggio (filtering)** si intende la possibilità dello switch di inoltrare o scartare un pacchetto.
- L'**inoltro (forwarding)** consiste nell'individuazione dell'interfaccia verso cui un pacchetto deve essere inviato.
- Le operazioni di filtraggio e inoltro sono eseguite mediante una **tabella di commutazione (switch table)** che contiene le seguenti voci
  - l'indirizzo mac del nodo,
  - l'interfaccia dello switch che conduce al nodo,
  - data e ora di inserimento della voce nella tabella di commutazione.
- La tabella di commutazione di uno switch è diversa dalla tabella di instradamento di un router[16] non solo per i contenuti (quelle dei router contengono gli IP, mentre quelle degli switch contengono i mac address) ma anche per il modo in cui viene creata e mantenuta.
- Consideriamo un pacchetto indirizzato al mac address AA:AA:AA:AA:AA:AA giunga allo switch sull'interfaccia x.
- Lo switch cerca nella sua tabella l'indirizzo AA:AA:AA:AA:AA:AA e trova che è associato all'interfaccia y.
- Se x è uguale ad y allora il pacchetto appartiene ad un segmento della LAN che contiene il mac address AA:AA:AA:AA:AA:AA; non occorre inoltrare il pacchetto a un'altra interfaccia dello switch e quindi il pacchetto viene scartato.
- Se x è diverso da y il pacchetto deve essere inoltrato dall'interfaccia x all'interfaccia y. Lo switch

15 Vedi dopo: "Identificazione degli host: mac address, indirizzo IP, FQDN".

16 Vedi dopo: "Router".

pone il pacchetto nel buffer che precede l'interfaccia y e quando è possibile invia il pacchetto dall'interfaccia y.

- **Autoapprendimento**
  - Le tabelle di commutazione sono costruite e mantenute in modo dinamico e automatico.
  - La tabella è inizialmente vuota.
  - Quando giunge un mac address su un'interfaccia il suo indirizzo di destinazione non è contenuto nella tabella, lo switch invia copie del pacchetto ai buffer di uscita di tutte le altre interfacce che lo inoltrano sui rispettivi segmenti della LAN usando il protocollo CSMA/CD.
  - Il **protocollo CSMA/CD** è un **protocollo del livello 2 (di collegamento)** che ha le seguenti caratteristiche:
    - l'adattatore **può iniziare a trasmettere in qualsiasi momento**, cioè non usa slot (come i protocolli TDM, come slot ALHOA);
    - usa la **rilevazione della portante**, cioè non può trasmette se altri adattatori stanno già trasmettendo;
    - usa la **rilevazione delle collisioni**, cioè blocca la trasmissione nel momento in cui rileva che un altro adattatore sta trasmettendo;
    - prima di trasmettere l'adattatore **resta in attesa** per un tempo random più breve rispetto alla durata del pacchetto.
  - Di ogni pacchetto in ingresso, lo switch archivia nella sua tabella l'indirizzo mac sorgente del pacchetto, l'interfaccia da cui proviene il pacchetto, data e ora della ricezione.
  - Quando tutti i nodi della LAN avranno inviato un pacchetto la tabella di commutazione sarà completa.
- Se su un'interfaccia arriva un pacchetto il cui indirizzo di destinazione è presente nella tabella di commutazione, questo pacchetto viene inoltrato all'interfaccia appropriata.
- Quando dopo un dato periodo di tempo detto **aging time (tempo di invecchiamento)**, lo switch non riceve pacchetti da un determinato indirizzo sorgente, lo cancella.
- Non blocca le tempeste di broadcast.

Router

- Un **router** è un dispositivo hardware che agisce sui **datagrammi IP** (pacchetti IP) e quindi è un dispositivo di **livello 3 (rete)** dello standard TCP/IP.
- Il ruolo del livello di rete (livello 3) è quello di trasferire pacchetti da un host ad un altro in base all'indirizzo IP.
- Differentemente dagli switch di livello 2 che sono dei dispositivi plug-and-play, nel senso che inoltrano i pacchetti in base alle risposte alle interrogazioni che mandano sulla rete, **i router prendono delle decisioni in base alla loro configurazione**.
- Esistono due importanti funzioni che vengono eseguite a questo livello:
- **inoltro (forwarding)**
  - quando un router riceve un pacchetto lo trasferisce all'appropriato collegamento d'uscita.
- **instradamento (routing)**
  - tramite algoritmi di instradamento vengono determinati i percorsi che devono compiere i pacchetti.

- Gli elementi della **tabella di instradamento (o Routing Table)** non sono quindi singoli calcolatori ma intere reti, ovvero sottoinsiemi anche molto ampi dello spazio di indirizzamento. Questo è fondamentale per la scalabilità delle reti, in quanto permette di gestire reti anche molto grandi facendo crescere le tabelle di instradamento in modo meno che lineare rispetto al numero di host.
- Per l'instradamento i router usano **tabelle di instradamento** i cui elementi sono blocchi di indirizzi IP, che sono detti **route (o rotte)**. Questo metodo è pertanto più scalabile, in quanto un singolo elemento della tabella di instradamento può gestire un numero anche molto alto di host.
- Le tabelle di instradamento possono essere popolate con una combinazione di diversi metodi:.
  - **Routing per reti direttamente connesse**: quando una interfaccia di rete di un host IP viene configurata con un indirizzo IP ed una maschera di sotto-rete, l'host conosce automaticamente la rotta per raggiungere tutti gli host di quella sotto-rete.

    Nel caso molto semplice di una rete costituita da diverse sotto-reti connesse ad un solo router, questo automatismo è sufficiente a popolare la tabella di routing di quel singolo router con tutti gli elementi necessari.
  - **Routing statico**: le rotte possono essere configurate manualmente sui vari router. Questo metodo è poco scalabile, difficile da gestire per reti più che banali, e non consente alla rete di usare percorsi multipli quando questi sono disponibili.
  - **Routing dinamico**: le tabelle di instradamento vengono popolate da appositi protocolli di routing, eseguiti sui router, che permettono ai router di scambiarsi informazioni circa la topologia attuale della rete, e quindi di costruire automaticamente le tabelle di instradamento. Questi protocolli permettono alla rete di adattarsi automaticamente ad eventuali modifiche (aggiunta o caduta di nodi e di collegamenti), ed in particolare di re-instradare il traffico in caso di caduta di un collegamento.

    Per fare questo sono stati messi a punto dei protocolli di routing appositi, come **OSPF**, **RIP** e **BGP**, attraverso i quali i router si scambiano informazioni sulle reti raggiungibili.
- Un router può **interconnettere reti di livello 2 eterogenee**, come ad esempio una LAN ethernet con un collegamento geografico in tecnologia Frame Relay o ATM.
- Rispetto ad uno switch o ad un hub, un router blocca le tempeste broadcast.
- Alcuni router possiedono anche un firewall incorporato, poiché il punto di ingresso/uscita di una rete verso l'esterno è ovviamente il luogo migliore dove effettuare controlli sui pacchetti in transito.
- I router possono essere normali computer che fanno girare un software apposito (**gateway**), o - sempre più spesso - apparati specializzati, dedicati a questo solo scopo. I router di fascia più alta sono basati su architetture hardware specializzate per ottenere prestazioni **wire speed** (letteralmente alla velocità della linea). Un router wire speed può inoltrare pacchetti alla massima velocità delle linee a cui è collegato.

Nomi di dominio e servizio DNS

- La possibilità di attribuire un nome testuale facile da memorizzare a un server (ad esempio un sito world wide web) migliora molto l'uso del servizio, in quanto gli individui trovano solitamente più facile ricordare nomi testuali (mentre gli host e i router sono raggiungibili usando gli indirizzi IP numerici). Per questo, il DNS è fondamentale per l'ampia diffusione di internet anche tra utenti non tecnici, ed è una delle sue caratteristiche più visibili.
- L'operazione di convertire un nome in un indirizzo IP è detta **risoluzione DNS**, convertire un indirizzo IP in nome è detto **risoluzione inversa**.
- È possibile attribuire più nomi allo stesso indirizzo IP (o viceversa) per rappresentare diversi servizi o funzioni forniti da uno stesso host (o più host che erogano lo stesso servizio).

- Questa flessibilità risulta utile in molti casi:
  - Nel caso il server debba sostituire il server che ospita un servizio, o si debba modificare il suo indirizzo IP, è sufficiente modificare il record DNS, senza dover intervenire sui client.
  - usando nomi diversi per riferirsi ai diversi servizi erogati da un host, è possibile spostare una parte dei servizi su un altro host, e spostare i client su questo nuovo host modificando il suo record nel DNS.
  - Facendo corrispondere più indirizzi IP a un nome, il carico dei client viene distribuito su diversi server, ottenendo un aumento delle prestazioni complessive del servizio e una tolleranza ai guasti (ma è necessario assicurarsi che i diversi server siano sempre allineati, ovvero offrano esattamente lo stesso servizio ai client).
- Il DNS viene usato da numerose tecnologie in modo poco visibile agli utenti, per organizzare le informazioni necessarie al funzionamento del servizio.

Nomi DNS

- Un nome a dominio è costituito da una serie di stringhe separate da punti, ad esempio it.wikipedia.org. A differenza degli indirizzi IP, dove la parte più importante del numero è la prima partendo da sinistra, in un nome DNS la parte più importante è la prima partendo da destra. Questa è detta **dominio di primo livello (o TLD, Top Level Domain)**, per esempio **.org** o **.it**.
- Un **dominio di secondo livello** consiste in due parti, per esempio **wikipedia.org**, e così via. Ogni ulteriore elemento specifica un'ulteriore suddivisione. Quando un dominio di secondo livello viene registrato all'assegnatario, questo è autorizzato a usare i nomi di dominio relativi ai successivi livelli come **it.wikipedia.org** (**dominio di terzo livello**) e altri come **some.other.stuff.wikipedia.org** (**dominio di quinto livello**) e così via.

Database distribuito e gerarchico

- Non è pensabile di gestire in modo efficiente un unico database per la risoluzione di tutti gli IP di Internet (potenzialmente 2^{32} indirizzi IP).
- Per trattare il problema della scalabilità il DNS usaza un gran numero di **server organizzati in modo gerarchico e distribuiti** in tutto il mondo.
- Nessun server DNS contiene le corrispondenze FQDN - IP per tutti gli host di Internet: queste informazioni sono distribuite su tutti i server DNS del mondo.
- In prima approssimazione esistono tre classi di server DNS:
  - i server **radice (root server)**;
  - i server **top-level domain (TLD)**;
  - i server **di competenza (authoritative server)**.
- In Internet esistono 13 server radice DNS (**root DNS server**) etichettati da A a M.
- In realtà per garantire sicurezza, efficienza e affidabilità ciascun root server è costituito da un **cluster di server replicati**.
- I server **top-lever domain (TLD)** si occupano dei domini di alto livello come com, org, net, edu, gov e di tutti i domini locali di alto livello come it, uk, fr, us.
- Ogni organizzazione dotata di host Internet pubblicamente accessibili deve fornire server record DNS di pubblico dominio che mappino i nomi di tali host in indirizzi IP. I server **di competenza (authoritative server) sono i server DNS** che mantengono questi record. Un'organizzazione può scegliere di implementare il proprio server di competenza o di pagare un certo fornitore di servizi per

ospitare questi record su un server.

L'Università di Firenze (unifi.it) ha i propri server DNS:

- DNS primario 150.217.140.15,
- DNS secondario 150.217.1.32.

Schema di funzionamento

- Consideriamo un esempio concreto per illustrare lo schema di funzionamento di una quesry DNS.
  - Il dominio `poly.edu` ha un proprio server DNS (TLD): `dns.poly.edu`.
  - L'host `cis.poly.edu`, che appartiene al dominio `poly.edu`, vuole conoscere l'indirizzo IP dell'host `gaia.cs.umass.edu`.
  - Se l'host `cis.poly.edu` è configurato correttamente conosce l'indirizzo IP del proprio server DNS (`dns.poly.edu`).
  - L'host `cis.poly.edu` interroga il proprio DNS server `dns.poly.edu` chiedendo l'IP dell'host `gaia.cs.umass.edu`.
  - Il server locale `dns.poly.edu`, non avendo la risposta, inoltra la richiesta ad un server radice (root DNS server).
  - Il server radice prende nota del suffisso `edu` e restituisce a `dns.poly.edu` una lista di server TLD responsabili di `edu`.
  - Il server locale `dns.poly.edu` invia la richiesta ad uno di questi server TLD.
  - Il server TLD prende nota del suffisso `umass.edu` e restituisce a `dns.poly.edu` il server DNS di competenza (authoritative server) per il dominio `umass.edu`.
  - Non è detto che il server di competenza per il dominio `umass.edu` conosca l'IP di `gaia.cs.umass.edu`.

    Se lo conosce lo invia a `dns.poly.edu` che lo consegna all'host `cis.poly.edu`.

    Se non lo conosce, sarà a conoscenza del DNS di competenza di livello più basso del dominio `cs.umass.edu`. Così lo restituisce a `dns.poly.edu`. A questo punto a `dns.poly.edu` contatta quest'ultimo server DNS e, ottenuta la risposta, la consegna all'host `cis.poly.edu`.

Caching DNS

- Fino a questo punto abbiamo ignorato una caratteristica fondamentale dei server DNS e cioè il **caching DNS** che migliora le prestazioni (minimizza i ritardi nelle risposte) e riduce il numero di richieste inviate su Internet.
- Quando ad un server DNS viene richiesto un certo nome il server esegue tutte le quesry DNS per risalire all'IP associato.
- Una volta ottenuta la risposta, questa informazione viene mantenuta per un periodo di tempo definito (tipicamente 48 ore) in modo che se, in questo intervallo di tempo, arriva una nuova richiesta di risoluzione per quel nome il server può subito dare una risposta senza dover contattare altri server DNS.

Numero di porta

- Quando due applicazioni di rete su host diversi comunicano, oltre a conoscere i rispettivi IP dei due

host, le applicazioni devono conoscere i rispettivi processi destinatari.

- Questa ulteriore informazione è necessaria perché, in generale, su un singolo host possono essere in esecuzione più applicazioni di rete.
- Il **numero di porta** di destinazione risponde a questo compito.
- Di solito si utilizzano porte basse (inferiori alla 1024) per applicazioni server che stanno in ascolto, mentre si usano le porte altre (superiori alla 1024) per applicazioni client.
- Alle applicazioni più note sono stati associati numeri di porta specifici. Per esempio i server web sono identificati dal numero di porta 80, i server ssh dalla porta 22, i server di posta dalla porta 25, ...
- In totale sono disponibili 2^{16} numeri di porta identificati dai numeri interi da 0 a 65535.
- La lista di numeri di porta noti per tutti i protocolli standard di Internet può essere scaricata da `http://www.iana.org`, oppure si può consultare il fie `/etc/services`.

Indirizzi IP

- Per quanto abbiamo detto in precedenza riguardo alla numerazione degli indirizzi, in teoria un IP è un numero compreso fra 0 e 2^{32}.

  In formato binario fra

  00000000 00000000 00000000 00000000 e 11111111 11111111 11111111 11111111

  Nella notazione decimale puntata (dotted-decimal notation) fra 0.0.0.0 e 255.255.255.255.
- In realtà non si possono assegnare agli host proprio tutti gli IP fra 0.0.0.0 e 255.255.255.255 poiché alcuni sono riservati[17].
- Sia da un punto di vista organizzativo che di efficienza per l'instradamento dei pacchetti, gli IP di Internet vengono raggruppati in **sotto-reti**, chiamate anche **reti IP** o semplicemente **reti**.
- Concettualmente l'indirizzo IP si compone di due parti:
  - **identificatore di rete**, o più precisamente della sotto-rete (**Network ID**)
  - **identificatore di host** (**Host ID**),
- Gli host che appartengono alla stessa rete hanno in comune i bit più a sinistra del proprio indirizzo IP (identificativo di rete).
- Le reti vengono classificate (storicamente) in **tre classi principali** (classe A, B e C) in base al numero di host che possono contenere.
  - Rete di **classe A**: da **0**.0.0.0 a **127**.255.255.255

da	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

0	Network ID Identificatore di rete	Host ID Identificatore di host
	7 bit	24 bit

    - Numero di reti possibili: 128
    - Numero max di indirizzi host: 16'777'214

17 Vedi dopo: indirizzi particolari

- Rete di **classe B**: da **128.0**.0.0 a **191.255**.255.255

da	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

1	0	Network ID Identificatore di rete	Host ID Identificatore di host
		14 bit	16 bit

  - Numero di reti possibili: 16'384
  - Numero max di indirizzi host: 65'534

- Rete di **classe C**: da **192.0.0**.0 a **223.255.255**.255

da	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

1	1	0	Network ID Identificatore di rete	Host ID Identificatore di host
			21 bit	8 bit

  - Numero di reti possibili: 2'097'152
  - Numero max di indirizzi host: 254

- Oltre a queste tre classi di sotto-reti, ne esistono altre due un po' particolari
  - Rete di **classe D**: da 224.0.0.0 a 239.255.255.255

da	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

1	1	1	0	Multicast Group ID
				28 bit

  - Rete di **classe E**: da 240.0.0.0 a 247.255.255.255

da	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
a	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

1	1	1	1	0	Per usi futuri
					27 bit

Reti di classe A

- Una rete di classe A è una rete in cui gli tutti gli IP hanno in comune gli **8 bit più a sinistra**. Nella notazione decimale puntata tutti gli IP della rete hanno in comune il primo numero a sinistra.
- In un IP appartenente ad una rete di classe A, il primo bit a sinistra è "0", i successivi 7 bit identificano la rete (**Network ID**) ed i successivi 24 bit identificano l'host (**Host ID**).
- Per indicare che solo gli 8 bit più a sinistra restano fissi si usa la **net-mask** sia in notazione decimale puntata (255.0.0.0) sia in bit (/8).
- Per esempio la rete di classe A che comprende tutti gli IP da 100.0.0.0 a 100.255.255.255 si indica nelle due notazioni
  - IP 100.0.0.0 , net mask 255.0.0.0;
  - 100.0.0.0/8.

Reti di classe B

- Una rete di classe B è una rete in cui gli tutti gli IP hanno in comune i **16 bit più a sinistra**. Nella notazione decimale puntata tutti gli IP della rete hanno in comune il primo e il secondo numero a sinistra.
- In un IP appartenente ad una rete di classe B, i primi due bit a sinistra sono "10", i successivi 14 bit identificano la rete (**Network ID**) ed i successivi 16 bit identificano l'host (**Host ID**).
- Per indicare che solo i 16 bit più a sinistra restano fissi si usa la net mask sia in notazione decimale puntata (255.255.0.0) sia in bit (/16).
- Per esempio la rete di classe A che comprende tutti gli IP da 150.12.0.0 a 150.12.255.255 si indica nelle due notazioni
  - IP 150.12.0.0 , net mask 255.255.0.0;
  - 150.12.0.0/16.

Reti di classe C

- Una rete di classe C è una rete in cui gli tutti gli IP hanno in comune i **24 bit più a sinistra**. Nella notazione decimale puntata tutti gli IP della rete hanno in comune il primo, il secondo e il terzo numero a sinistra.
- In un IP appartenente ad una rete di classe C, i primi tre bit a sinistra sono "110", i successivi 21 bit identificano la rete (**Network ID**) ed i successivi 8 bit identificano l'host (**Host ID**).
- Per indicare che solo i 24 bit più a sinistra restano fissi si usa la net mask sia in notazione decimale puntata (255.255.255.0) sia in bit (/24).
- **Per esempio** la rete di classe C che comprende tutti gli IP da 192.84.45.0 a 192.84.145.255 si indica nelle due notazioni
  - IP 192.84.145.0 , net mask 255.255.255.0;
  - 192.84.145.0/24.

Indirizzi particolari

Sotto-rete e broadcast

- Ogni indirizzo in cui l'**identificativo host presenta tutti 0** ci si riferisce alla **rete**.

- Se tutti i bit dell'**identificativo host sono a 1** ci si riferisce ad una trasmissione **broadcast**.
- In pratica quando ad un router arriva un pacchetto in cui la parte di host dell'indirizzo presenta tutti i bit a 1, esso esegue un broadcast, cioè invia il pacchetto a tutti i nodi della sotto-rete.

Indirizzi privati

- Con indirizzi IP privati si intendono alcune classi di indirizzi IP (definite nella RFC 1918), riservate alle **reti locali** non connesse ad Internet allo scopo di ridurre le richieste di indirizzi pubblici.
- Chiunque può usare questi indirizzi per la propria rete locale, perché i pacchetti relativi a tali reti non vengono instradati dai router Internet, e quindi essi non entreranno in conflitto con analoghi indirizzi posti su altre reti locali.
- Nel caso occorra connettere ad Internet una rete locale che usa queste classi di indirizzi, si deve ricorrere al **Network Address Translation (NAT)**.[18]
- Esistono **tre classi di IP privati**
  - **10.0.0.0/8**
    - Singola rete di classe A
    - IP da **10**.0.0.0 a **10**.255.255.255
  - **172.16.0.0/12**
    - 16 reti contigue di classe B
    - IP da **172.16**.0.0 a **172.31**.255.255
  - **192.168.0.0/16**
    - 256 reti contigue di classe C
    - IP da **192.168**.0.0 a **192.168**.255.255

NAT

- Il meccanismo del **Network Address Translation (NAT)** si basa sull'uso di un **gateway**.
- In generale un gateway di una sotto-rete (con indirizzi privati o pubblici) è l'host a cui vengono inviati i pacchetti diretti ad indirizzi esterni alla sotto-rete.
- Se la sotto-rete ha solo indirizzi privati, il gateway deve fare anche da NAT e quindi deve avere almeno due collegamenti di rete: uno (con IP pubblico) verso l'Internet ed uno con (IP privato) verso la sotto-rete.
- Per implementare il NAT, un gateway ha quindi bisogno di effettuare il tracciamento delle connessioni, ovvero di tenere traccia di tutte le connessioni che lo attraversano. Per "connessione" in questo contesto si intende un flusso bidirezionale di pacchetti tra due host, identificati da particolari caratteristiche a livelli superiori a quello di rete (IP):
  - nel caso di TCP è una connessione TCP in senso proprio, caratterizzata da una coppia di porte ;
  - nel caso di UDP, per quanto UDP sia un protocollo di trasporto senza connessione, viene considerata connessione uno scambio di pacchetti UDP tra due host che usi la stessa coppia di numeri di porta.;
  - altri protocolli vengono gestiti in modo analogo, usando caratteristiche del pacchetto a livelli superiori ad IP per identificare i pacchetti che appartengono ad una stessa connessione.
- Per esempio consideriamo un host A appartenente ad una rete privata, in cui l'host G è il gateway

18 Vedi dopo: "NAT".

che fa il NAT, che tenta di connettersi alla porta 80 (server web) dell'host B di Internet. Il meccanismo del NAT è il seguente.

- Poiché l'host B non appartiene alla sotto-rete, l'host A invia il pacchetto alla porta *80* dell'host G.
- Si apre una connessione fra la porta *a* dell'host A e la porta *80* dell'host G.
- L'host G modifica l'intestazione (header) di tutti i pacchetti che riceve da tale connessione modificando sia l'IP sorgente che la porta sorgente. Al posto dell'IP dell'host A usa come sorgente il proprio IP e al posto della porta *a* sceglie un'arbitraria porta *g* (tipicamente sopra la 61000) .
- L'host G tiene traccia della corrispondenza fra IP dell'host A, porta *a* e porta *g*.
- L'host G, dopo aver modificato l'intestazione dei pacchetti provenienti da A, li invia all'host B.
- L'host B riceve i pacchetti dall'host G senza sapere che provengono dall'host A.
- Invia la risposta all'host G sulla porta *g*.
- L'host G modifica le intestazioni dei pacchetti che riceve sulla porta *g*, impostando come IP di destinazione quello dell'host A e come porta di destinazione la porta *a*.

- Il gateway (host G) mantiene aggiornata una una tabella di corrispondenze tra IP della sotto-rete, porte sull'indirizzo esterno (porta *g*) e corrispondenti porte sull'indirizzo interno (porta *a*). Questa tabella serve a inoltrare indietro le risposte: quando riceve un pacchetto sull'indirizzo IP esterno, consulta la tabella per sapere a quale host interno e su quale porta inviarlo.

Protocollo per la risoluzione degli indirizzi (ARP)

Comunicazione fra due host in una sotto-rete

- Consideriamo cosa succede quando in una sotto-rete ethernet, in cui tutti gli host sono collegati tramite vari switch layer 2, un host A contatta un host B.
- I dati che caratterizzano questa situazione sono, per esempio, i seguenti.
  - Sotto-rete: 192.168.34.0/24
  - Host A, IP: 192.168.34.11
  - Host B, IP: 192.168.34.12
- Per esempio consideriamo che sull'host B sia attivo un server web e che sull'host A un browser web richieda una certa pagina web all'host B.
  1. L'host A contatta il server DNS e riceve l'indirizzo IP dell'host B (192.168.34.12).
  2. Per inviare un pacchetto (un datagramma) sulla rete l'host A deve conoscere il mac address dell'host B, ma ha a disposizione solo il suo indirizzo IP. Quindi l'host A invia sulla rete uno speciale pacchetto (**pacchetto ARP, Address Resolution Protocol**) che contiene tra l'altro gli indirizzi IP e mac address dell'host A e l'indirizzo IP dell'host B. Tale pacchetto viene inviato all'indirizzo di broadcast della rete, cioè al mac address ff:ff:ff:ff:ff:ff.
  3. Poiché il pacchetto ARP ha come destinatario l'indirizzo di broadcast, viene ricevuto da tutti gli host della rete, poiché gli switch lo propagano su tutte le loro porte.
  4. Ciascun host controlla se questo pacchetto ARP contiene il proprio IP come destinazione.
  5. L'host B è l'unico host sulla rete che ha l'indirizzo IP richiesto dal pacchetto ARP, quindi è l'unico che invia una risposta ARP all'host A.
  6. La richiesta ARP e la risposta transitano sui vari switch che hanno modo di aggiornare le proprie

tabelle ARP in modo da poter instradare i successivi pacchetti fra gli host A e B.

7. A questo punto il browser web sull'host A può richiedere una pagina HTML contattando la porta 80 dell'host B.

Esercizi

Per registrare in un file quello che fate negli esercizi e poterlo rivedere in un secondo momento vi consiglio di usare il comando script:

script [nome del file dove salvare tutto]

Per rileggere il file usare il comando”

less -r [nome del file dove è stato salvato tutto]

1. Configurazione del proprio PC per poter accedere alla rete (è necessario essere root).
   - **dhclient**
   - **ifconfig**
   - vim **/etc/resolv.conf**
   - **route**

   Oppure

   Ricavare la configurazione di rete del proprio PC (non è necessario essere root).
   - **/sbin/ifconfig**
   - **/sbin/route** oppure **netstat -rn**
   - cat **/etc/resolv.conf**
   - cat **/etc/hosts**
2. Raggiungo qualche host della rete (per esempio il DNS)?
   - cat **/etc/resolv.conf**
   - **ping**
3. Interrogare il server DNS per sapere qual è il proprio nome sulla rete
   - /sbin/ifconfig
   - **nslookup** oppure **host**
4. Qual è il mac address della scheda di rete del nostro PC? Chi ha fabbricato la scheda di rete del nostro PC?
   - /sbin/ifconfig
   - http://standards.ieee.org/regauth/oui/index.shtml
5. Consultare la tabella ARP sul proprio PC.
   - cat /proc/net/arp
6. Configurazione di un mail client.
   - Server IMAP/POP3, porta, sicurezza.
   - Server SMTP, porta, sicurezza.
7. Da root, con **tcpdump**, osservare cosa succede quando un nodo della propria sott-rete tenta di contattare un IP, che non è nella sua tabella ARP (who-has).
8. Osservare come si aggiorna la tabella ARP del proprio PC quando si contatta un nodo della propria sotto-rete o un nodo esterno alla rete.

- cat /proc/net/arp

9. Collegarsi tramite **SSH** ad un altro PC
   - ssh stufis06.fisica.unifi.it
10. Copiare un o più file e/o una o più directory dal proprio PC ad un altro tramite **SCP**
    - scp stufis06.fisica.unifi.it
11. Aprire una comunicazione fra due PC e scambiare testo/file
    - nc -l -p 12345
    - nc studenti.fisica.unifi.it 12345

      oppure
    - nc -l -p 12345 > out.txt
    - cat in.txt | nc studenti.fisica.unifi.it 12345
12. Altri utenti hanno una sessione aperta su questo PC?

    Se ci sono da quale nodo/IP si stanno collegando?

    A quale rete appartiene l'IP da cui si stanno collegando?

    Qual è il percorso per arrivare al nodo da cui si stanno collegando?
    - **who**
    - **nslookup** oppure **host**
    - **whois**
    - **traceroute**
13. La nostra rete.

    Collegarsi al sito del GARR (Gestione Ampliamento Rete Ricerca) e seguire un qualche percorso dato da traceroute (per esempio traceroute www.fi.infn.it) sulla "weather map" del GARR-NOC (Network Operation Center).
    - La home page del GARR
      - http://www.garr.it/
    - La mappa della rete GARR
      - http://www.garr.it/reteGARR/mappa.php?idmenu=rete
    - La home page del GARR-NOC
      - http://www.noc.garr.it/
    - weather map con circuiti di accesso delle sedi utente
      - http://www.noc.garr.it/mappe/
      - Router di Firenze Sesto (RT.FI.1):

        in uscita: unifi.fi.garr.net (193.206.136.85)

        in ingresso: rt-fi1-ru-unifi.fi1.garr.net (193.206.136.86)
        - http://www.noc.garr.it/mappe/rt_fi1_01.shtml
14. Consultare il traffico sul router del GARR dell'Università di Firenze (RT.FI.1)
    - http://www.noc.garr.it/mappe/rt_fi1_01.shtml

- http://www.noc.garr.it/mrtg/RT.FI1.garr.net/unifi.fi.garr.net.html

15. Quali connessioni sono attive sul mio PC e cosa stanno facendo?
    - netstat
    - netstat -n
    - netstat -aut
    - netstat -aute
    - netstat -autepnw
    - netstat -l
16. Statistiche riguardo alla rete
    - netstat -s
    - netstat -t -s
    - netstat -u -s
    - netstat -w -s
    - netstat -s
17. Quali servizi sono aperti sulle macchine nella mia rete (per esempio studenti.fisica.unifi.it)?
    - nmap
18. Parliamo direttamente con un server web, per esempio (studenti.fisica.unifi.it).
    1. nmap -p 80 studenti.fisica.unifi.it
    - telnet studenti.fisica.unifi.it 80
        - GET / HTTP/1.1 [Enter]
        - Host: stufis06.fisica.unifi.it [Enter]
        - [Enter]
19. Parliamo direttamente con un mail server , per esempio (studenti.fisica.unifi.it).
    - Apertura della **sessione telnet** con il server

      Comando da shell: telnet studenti.fisica.unifi.it 25telnet

      Risposta del server Trying 150.217.141.28...

      Connected to studenti.fisica.unifi.it.

      Escape character is '^]'.

      220 studenti.fisica.unifi.it ESMTP Postfix (Debian/GNU)
    - Ci si presenta al server dicendo da quale host ci stiamo collegando (**helo**)

      Comando da telnet: helo stufis06.fisica.unifi.it

      Risposta del server: 250 studenti.fisica.unifi.it
    - **Mittente**

      Comando da telnet: mail from: <leandro.lanzi@gmail.com>

      Risposta del server: 250 2.1.0 Ok
    - **Destinatario**

      Comando da telnet: rcpt to: <leandro.lanzi@fi.infn.it>

Risposta del server: 250 2.1.5 Ok

- **Contenuto dell'e-mail**

  Comando da telnet: data

  Risposta del server: 354 End data with <CR><LF>.<CR><LF>

- **Header** del messaggio

  Comando da telnet: from: Leandro Lanzi <leandro.lanzi@gmail.com>
  to: Leandro <leandro.lanzi@fi.infn.it>
  reply-to: Leandro Lanzi <leandro.lanzi@gmail.com>
  subject: Questa e' una prova

- **Body** del messaggio

  Comando da telnet: [Enter] (Una riga vuota indica l'inizio del Body)
  Questo e' il testo di una mail di prova.

  Saluti

  Leandro

- **Fine del messaggio**

  Comando da telnet: . (un punto “.” indica la fine del messaggio)

  Risposta del server: 250 2.0.0 Ok: queued as 2E5A526C779

- **Uscita da telnet**: quit

  Risposta del server: 221 2.0.0 Bye
  Connection closed by foreign host.

Bibliografia

- James F. Kurose, Keith W. Ross "Computer Networking: A Top-Down Approach"
  Addison-Wesley
  ISBN-10: 0321497708
  ISBN-13: 9780321497703

- W. Richard Stevens "TCP/IP Illustrated, Volume 1: The Protocols"
  Addison-Wesley
  ISBN 0-201-63346-9

- Heather Osterloh “TCP/IP Primer Plus”
  SAMS
  ISBN: 0-672-32208-0

- Charles E. Spurgeon “Ethernet - The Definitive Guide”
  O'Reilly
  ISBN 1-56592-660-9

- The Internet Engineering Task Force (IETF)
  http://www.ietf.org/

- Wikipedia
  http://wikipedia.org/

Indice