Layering

- Per gestire la complessità delle comunicazioni e l'estrema eterogeneità di hardware, software e tecnologie di canale si adotta un approccio a strati (layered)
- Il modello di riferimento è ISO/OSI
  - Inizialmente concepito come implementazione state-of-the-art, ora rimane di interesse esclusivamente come modello teorico

Layering

- ISO/OSI propone un'architettura di soluzione per arrivare a descrivere una comunicazione ICT complessa
  - L'architettura si basa sul principio dell'astrazione che richiede di nascondere dettagli e mostrare solo le entità utili significative per l'utente finale (cliente)
- Avendo un problema complesso, si introducono una serie di astrazioni, i livelli, che consentono di risolvere il problema separando gli ambiti in modo ordinato e ben identificato
- Si definiscono una serie di livelli per decomporre il problema e affrontare le complessità separatamente
- Il "divide et impera" è il principio ingegneristico 0 per la gestione di complessità ed eterogeneità ed è di fondamentale importanza per le reti di calcolatori

Vantaggi dell'approccio layered

- L'approccio layered permette a progettisti e sviluppatori che realizzano soluzioni di livello X di non curarsi dei protocolli di livello sottostante
  - È sufficiente rispettare le interfacce fornite dai protocolli di livello sottostante
- A ogni livello possiamo ragionare indipendentemente
  - È possibile impilare i protocolli come vogliamo, purché soddisfino i vincoli di interfacciamento
  - Questo consente di **sostituire, sviluppare, e aggiornare i singoli protocolli singolarmente senza modificare il resto dello stack**

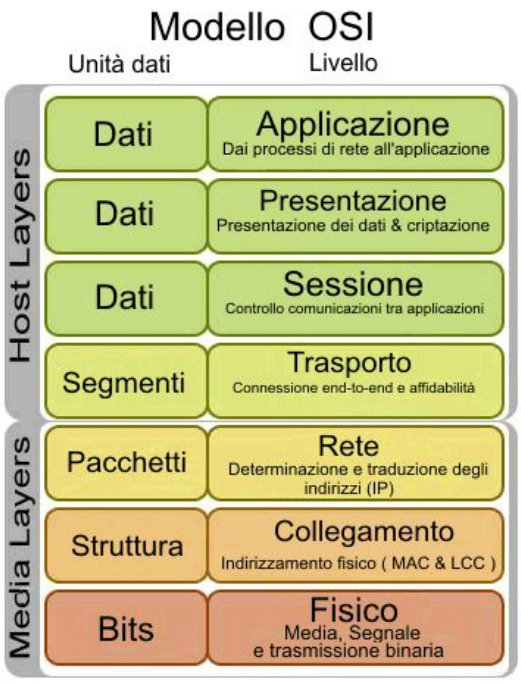
Il Modello ISO/OSI

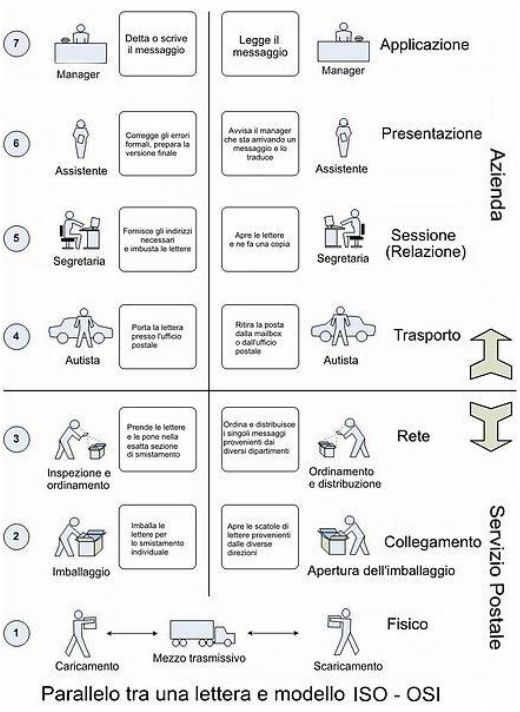
- Modello a 7 layer basato su IBM SNA
- Partendo dal livello applicazione (top-down), ogni livello ha l'obiettivo di comunicare con il pari, e lo realizza tramite un protocollo, ossia un insieme di passi, che realizza usando il servizio sottostante
- Ogni livello fornisce un servizio specificato e disponibile al livello superiore
- Ogni sistema a livelli si basa sul **principio della separazione dei compiti (delega) e della trasparenza della realizzazione (astrazione)**

Il Modello ISO/OSI

- In genere, per un'azione di invio informazioni, possiamo avere:
  - **Mittente**: entità che ha la responsabilità di iniziare la comunicazione
  - **Ricevente**: entità che accetta la comunicazione e poi la sostiene
  - **Intermediari**: eventuali nodi intermedi (access point, bridge, switch, router) che devono partecipare alla comunicazione - e fornire risorse per sostenerla
- Il mittente manda dei dati a un ricevente che può anche rispondere all'invio con un'azione applicativa conseguente
- Ogni azione comporta una comunicazione che passa attraverso i livelli da applicativo a fisico, del mittente e ricevente e almeno fino al livello di rete per gli intermediari

Il Modello ISO/OSI



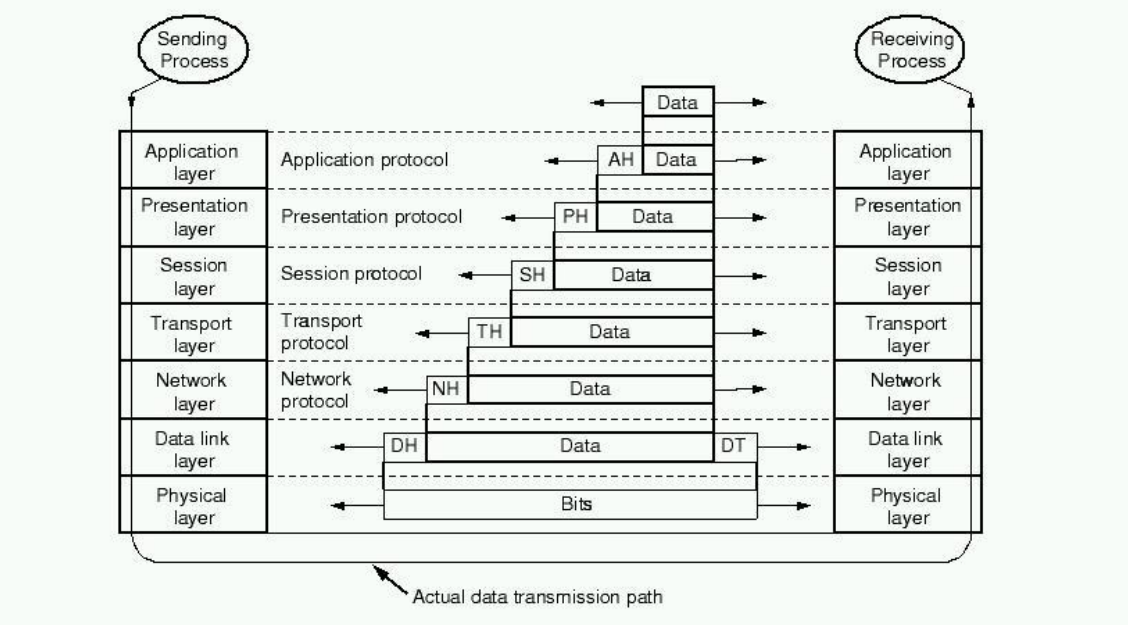


Courtesy: Wikipedia

Incapsulamento

- I 7 layer interagiscono tra loro solo tramite un set di interfacce rigorosamente definite
- I layer di livello più basso offrono dei servizi ai layer di livello superiore
- Incapsulamento delle informazioni di controllo di ciascun layer all'inizio del pacchetto di dati trasmesso

Incapsulamento



Livello 7 - Applicazione

- Il livello 7 fornisce protocolli utilizzati direttamente dalle applicazioni
- Esempio:
  - Trasferimento di file
  - Terminale virtuale
  - Posta elettronica

Livello 6 - Presentazione

- Il livello 6 si occupa della rappresentazione delle informazioni in modo standard e di implementare servizi come la compressione e la cifratura delle informazioni
- Diverse modalità di rappresentazione delle informazioni
  - Astratta (o formale)
  - Concreta (o locale)
  - Di trasferimento

Livello 5 - Sessione

- Il livello 5 coordina il dialogo tra gli utenti basandosi sul servizio offerto dal livello di Trasporto
- Funzioni svolte: gestione dialogo, sincronizzazione, gestione attività
- La principale funzione del livello 5 è quella di stabilire tra gli utenti delle sessioni di lavoro (gestione dialogo). Una sessione di lavoro fa uso di una connessione di trasporto, con diverse possibilità di mapping (es. una sessione su due connessioni L4).
- Supporto a sincronizzazione e rollback

Livello 4 - Trasporto

- Il livello 4 permette il trasferimento di dati tra due nodi
- È il primo livello della pila ISO/OSI che opera in modo end-to-end
- Il livello 4 si occupa di:
  - Stabilire e mantenere connessioni tra i nodi in comunicazione
  - Implementare meccanismi di affidabilità end-to-end
  - Controllo di congestione

Livello 3 - Rete

- Il livello 3 permette il trasferimento di pacchetti oltre la rete locale (LAN)
- Reponsabile di:
  - Instradamento (routing) dei pacchetti
  - Conversione dei pacchetti tra vari protocolli di livello 2
  - Frammentazione dei pacchetti

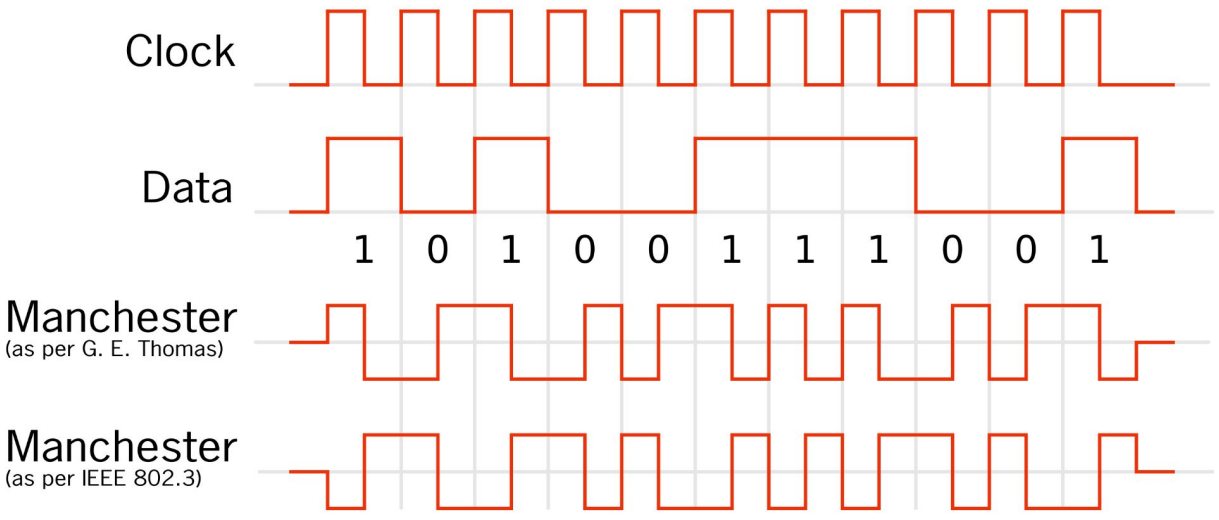
Livello 2 – Collegamento (Link)

- Il livello 2 permette il trasferimento di pacchetti al di sopra di un canale (link) di comunicazione
- Il livello 2 si occupa di:
  - Coordinamento all'accesso del canale da parte di più nodi
  - Controllo errori e ritrasmissioni (per implementare comunicazioni affidabili)
  - Controllo di flusso (per evitare che trasmissioni troppo veloci mettano in difficoltà macchine lente)

Livello 1 - Fisico

- Il livello 1 si occupa di definire come i bit di informazione vengono trasmessi sul canale fisico (fibra ottica, rame, radio, ecc.)
- Ad esempio:
  - Livelli di tensione
  - Durata del segnale che identifica un bit
  - Modulazione e codifica
  - Trasmissione half- e full-duplex

Es. Livello 1: Manchester Coding

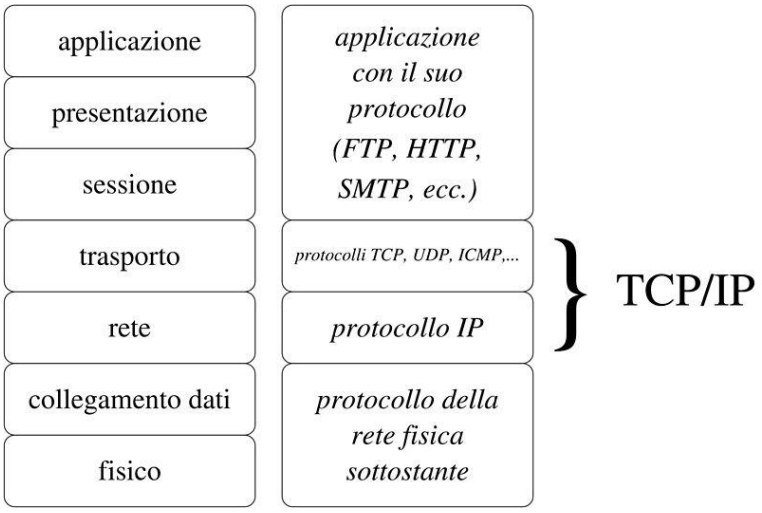


Courtesy: Wikipedia

Il Modello TCP/IP

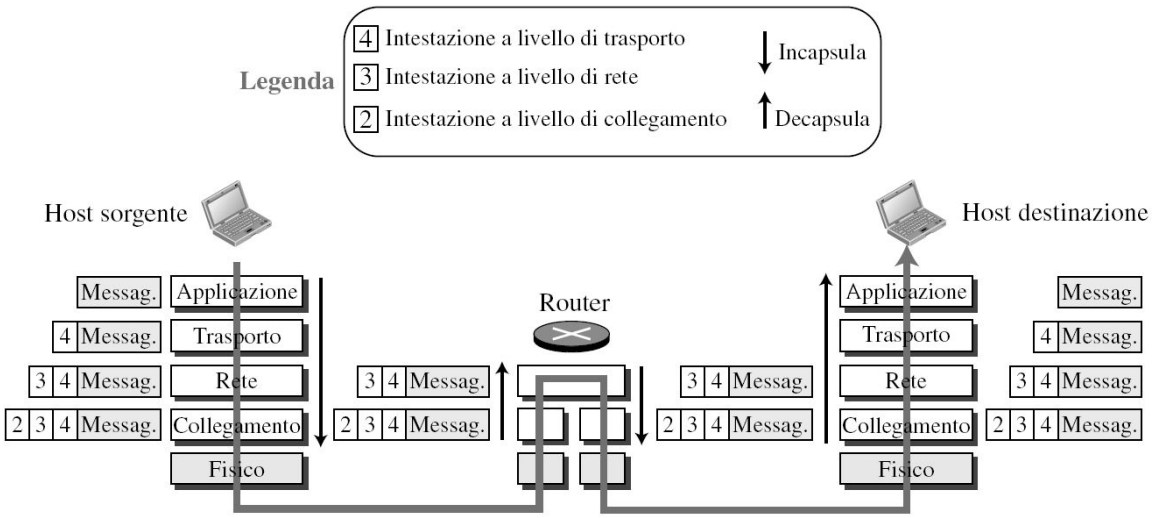
- Per diversi motivi (complessità, distribuzione sbilanciata delle funzioni tra i vari layer, ecc.) il protocollo OSI non ha mai visto la luce
- La suite di protocolli TCP/IP, invece, che regge Internet, ha avuto un successo incredibile e rappresenta la tecnologia (e quindi anche il modello) più importante nel campo delle reti di comunicazioni

ISO/OSI e TCP/IP a confronto

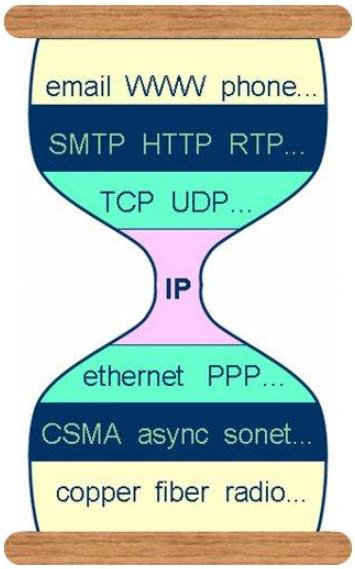


Il modello TCP/IP è privo dei livelli di sessione e presentazione. (Vedremo come questo complichi significativamente lo sviluppo delle applicazioni.)

Layering e incapsulamento in TCP/IP



TCP/IP: il Modello a Clessidra



Il modello TCP/IP viene detto “a clessidra” perché è essenzialmente basato sull'idea di convogliare tutte le comunicazioni attraverso un protocollo di comunicazione comune e onnipresente: IP.

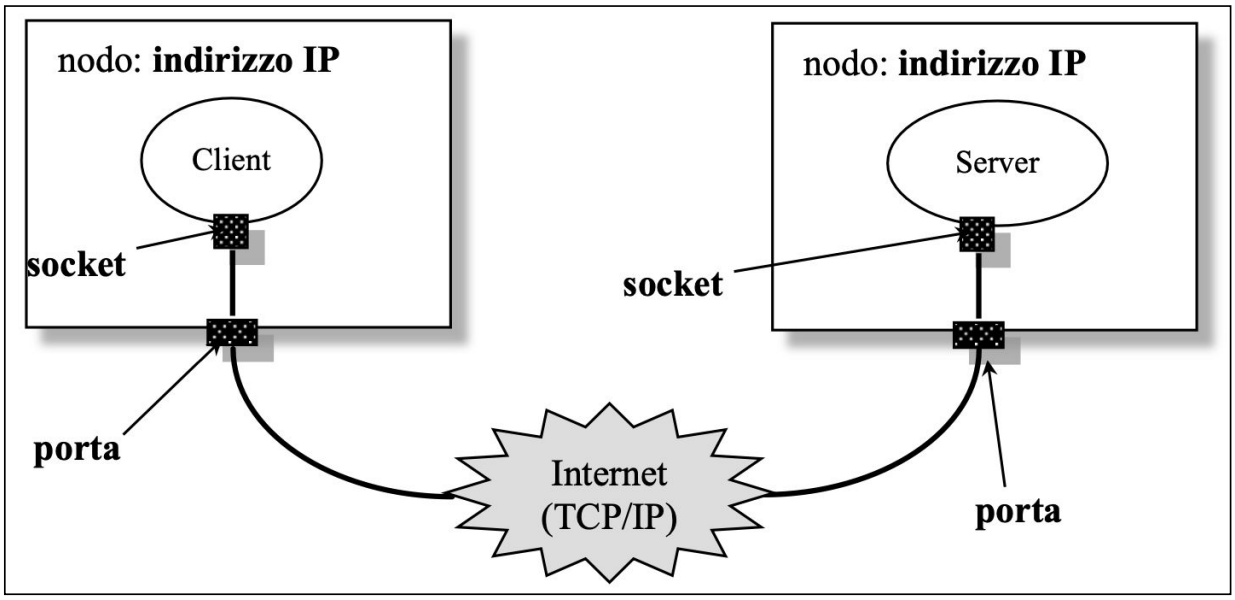
Servizi TCP/IP

- In TCP/IP, ogni servizio è associato a un ID, che si chiama *porta*
- Per accedere a un servizio, dobbiamo specificare IP e porta su cui il servizio è in attesa di richieste
- Per interagire con il fornitore di servizio dobbiamo rispettare uno specifico protocollo di comunicazione, ovverosia il protocollo di livello applicazione (es. HTTP per il Web)

Servizi TCP/IP

- Tipicamente, a ogni tipologia di servizio è associato un protocollo di comunicazione unico
- Ad esempio:
  - per il Web si usano il protocollo HTTP (L7) sulla porta 80 al di sopra di TCP (L4) e IP (L3)
  - per il DNS si usano il protocollo DNS (L7) sulla porta 53 al di sopra di UDP (L4) e IP (L3)

Servizi Internet



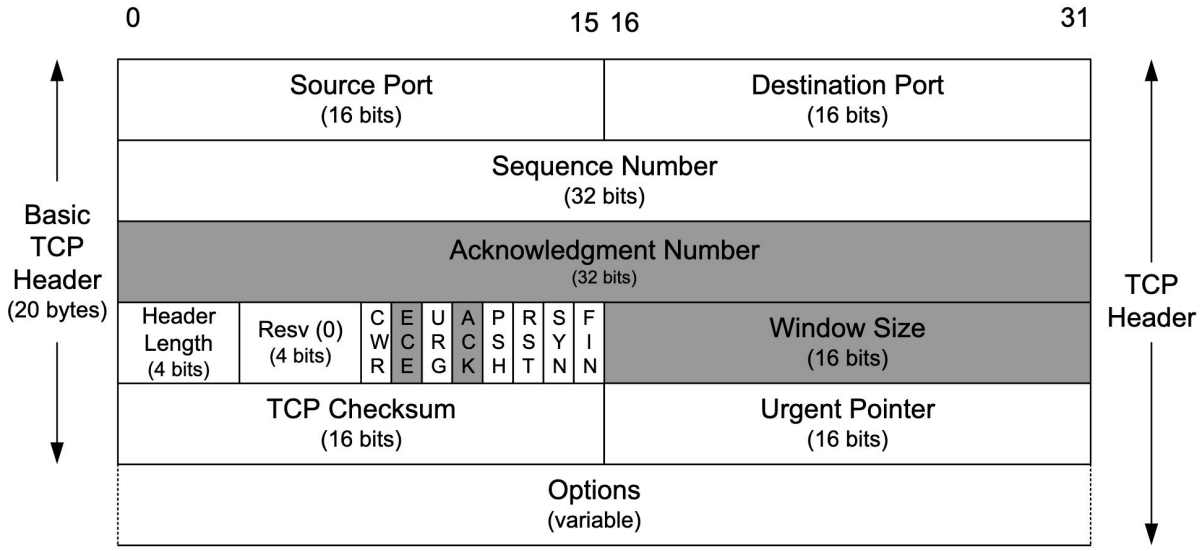
Livello Trasporto in TCP/IP

- Al di sopra di IP, vi sono diversi protocolli di livello trasporto, ma i principali sono TCP e UDP:
  - TCP permette di stabilire dei flussi di comunicazione bidirezionali affidabili tra due nodi
  - UDP permette a un nodo di mandare dei messaggi a un altro nodo. (In pratica, UDP è un semplicissimo protocollo costruito per poter sfruttare la consegna di messaggi best effort fornita da IP.)
- Usando TCP o UDP, e il livello IP sottostante, è possibile costruire applicazioni (o servizi)

Transmission Control Protocol (TCP)

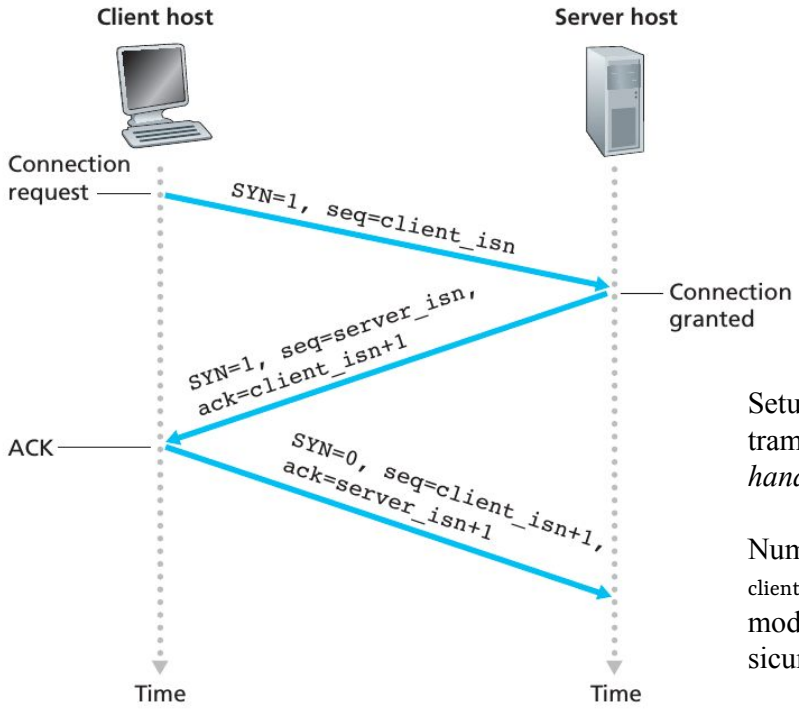
- TCP offre un servizio CON CONNESSIONE e AFFIDABILE
  - connessione bidirezionale
  - consegna sequenziale
    - ordine corretto dei byte
    - ritrasmissione messaggi persi
    - possibilità di trasmissione dati prioritari (out of bound)
    - non rispetta separazione tra messaggi (se richiesto dalla semantica di servizio, il framing va implementato a livello applicativo)
  - controllo di flusso e bufferizzazione
  - controllo di congestione
  - multiplexing
  - semantica at-most-once

TCP header



Courtesy: K. Fall, W. R. Stevens, G. Wright, “TCP/IP Illustrated Volume 1: The Protocols”, 2nd Edition, Addison-Wesley Professional, Pearson, Year: 2012

TCP: Setup connessione

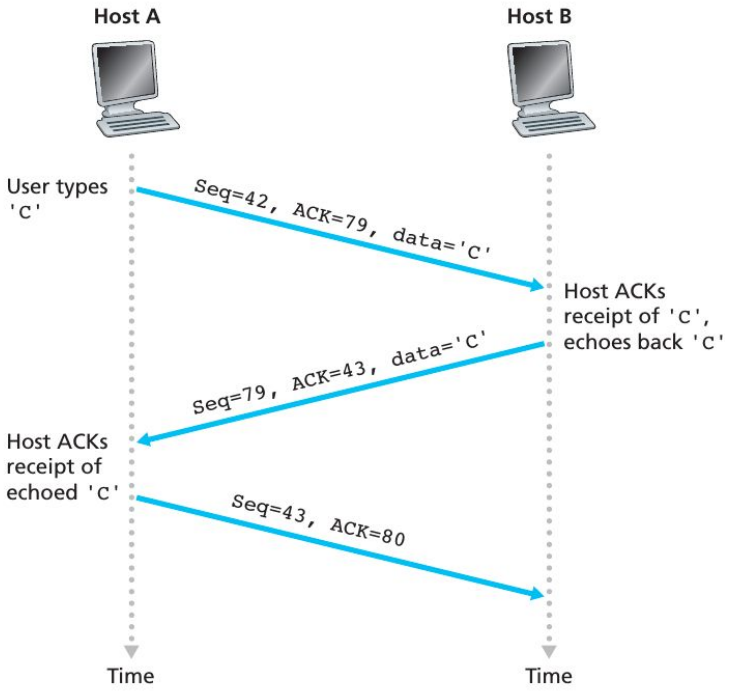


Setup della connessione tramite il noto *3-way handshake*

Numeri di sequenza iniziali client_isn e server_isn scelti in modo casuale per motivi di sicurezza

Courtesy: Kurose-Ross

TCP: Consegna ordinata

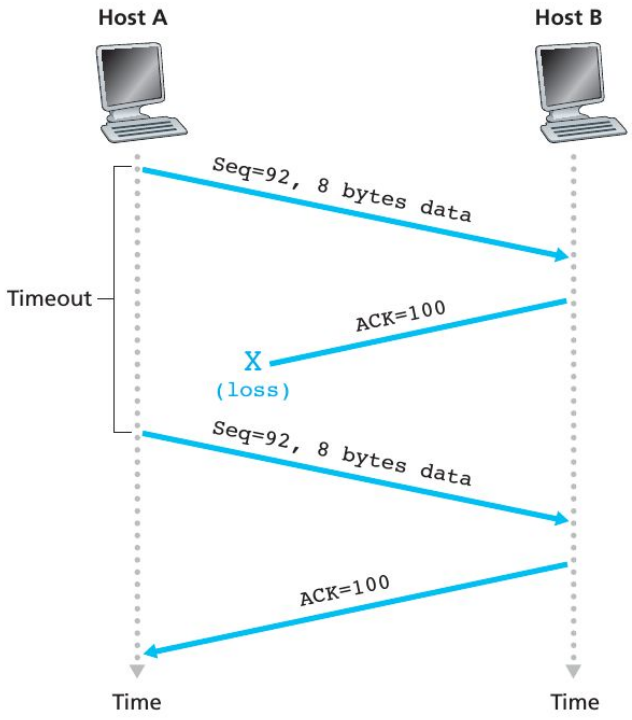


TCP ordina i byte da trasmettere in sequenza e tiene traccia del numero di sequenza dei byte trasmessi e ricevuti.

Uso di acknowledgement per confermare all'altro endpoint la corretta avvenuta ricezione dei messaggi.

Courtesy: Kurose-Ross

TCP: Consegna affidabile



TCP implementa la consegna affidabile dei messaggi effettuando la ritrasmissione automatica dei messaggi in caso non venga ricevuto un acknowledge entro un certo tempo massimo.

Uso di timeout con backoff esponenziale.

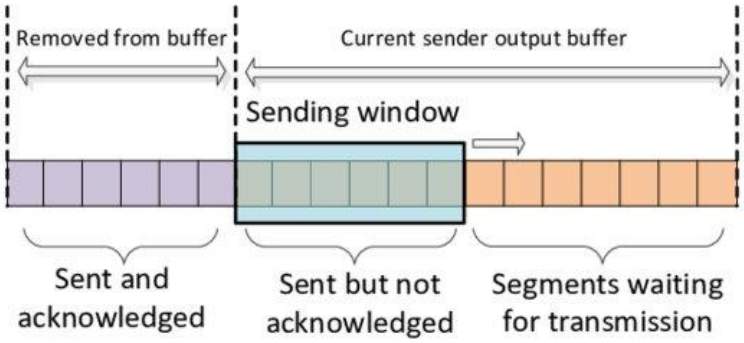
Inizialmente meccanismo di affidabilità GO-BACK-N, successivamente estensione per SELECTIVE ACK.

Courtesy: Kurose-Ross

TCP: Controllo di flusso

- Il controllo di flusso è fondamentale per Internet in cui sono presenti macchine molto diverse fra loro.
- Un server molto lento potrebbe essere saturato di messaggi inviati da client più veloci (e perdere quindi messaggi).
- Il controllo di flusso serve per permettere a un ricevitore lento di rallentare l'invio dei messaggi da parte del mittente.
- Il meccanismo fondamentale per il controllo di flusso è la *finestra scorrevole (sliding window)*.

TCP: finestra scorrevole



R. Al-Saadi, G. Armitage, J. But and P. Branch, "A Survey of Delay-Based and Hybrid TCP Congestion Control Algorithms," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3609-3638, Fourthquarter 2019, doi: 10.1109/COMST.2019.2904994.

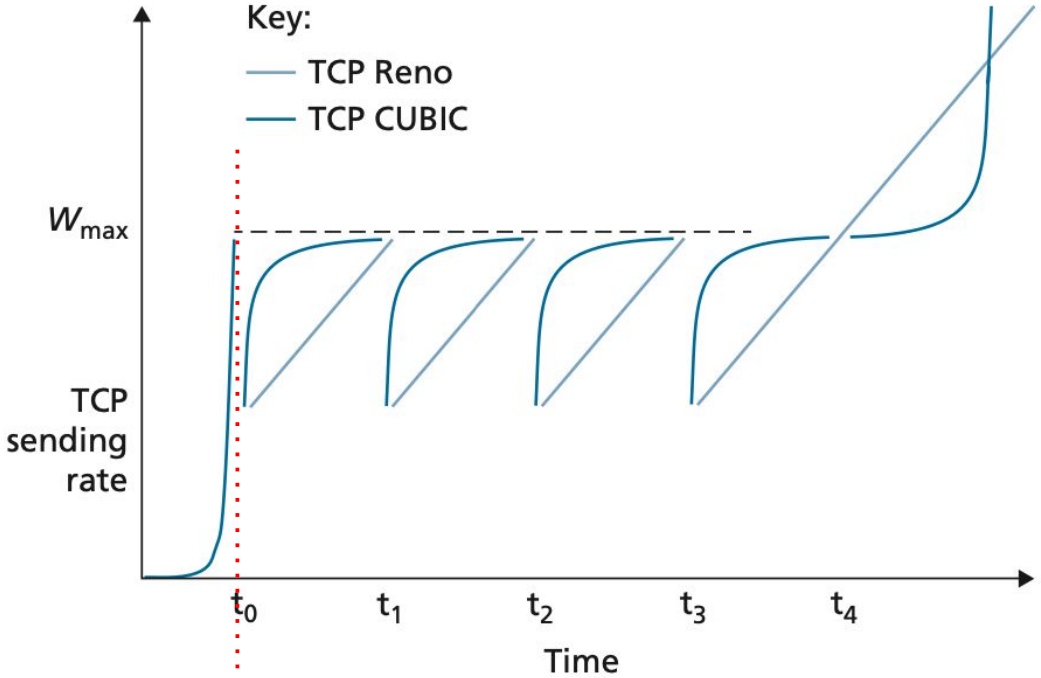
TCP: Controllo di flusso

- Il ricevente comunica al mittente la dimensione della propria finestra (ovverosia la dimensione della parte ancora disponibile nel proprio buffer di ricezione)
- **Meccanismo di retroazione efficace che permette di modulare la velocità di trasmissione del mittente sulla base delle risorse del destinatario**
- Alcuni aspetti interessanti del problema:
  - Initial window size (10 segments, RFC6928)
  - Window scaling (RFC7323)

TCP: Controllo di congestione

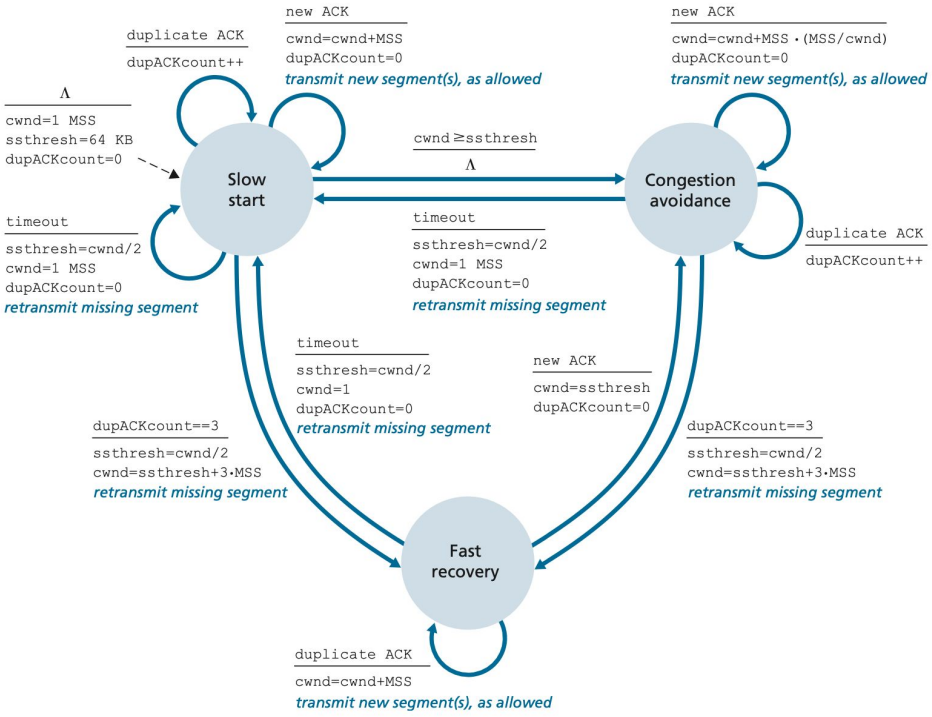
- In seguito all'immissione di un numero maggiore di pacchetti rispetto a quanto (una parte) dell'infrastruttura di rete riesca a gestire si possono verificare *congestioni della rete*
- Per risolvere una congestione è indispensabile che i nodi comunicanti rallentino la velocità di trasmissione
- TCP fornisce un meccanismo di *congestion control*, che cerca di inferire la presenza di congestioni lungo il percorso di comunicazione e in tal caso rallenta la velocità di trasmissione

TCP: Controllo di congestione



Courtesy: Kurose-Ross

TCP: Controllo di congestione



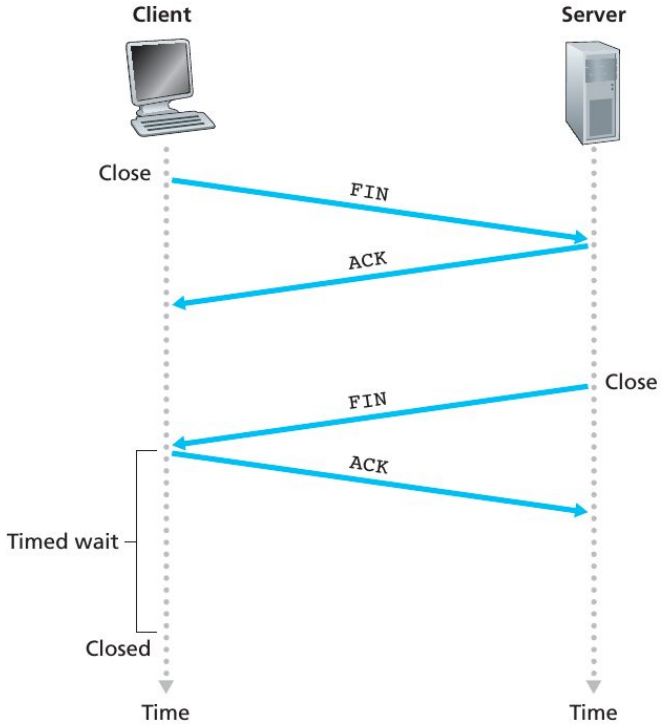
Courtesy: Kurose-Ross

TCP: Controllo di congestione

- Attenzione che il controllo di congestione potrebbe essere vicino a una rivoluzione copernicana:

M. Welzl, P. Teymoori, S. Islam, D. Hutchison and S. Gjessing, “Future Internet Congestion Control: The Diminishing Feedback Problem”, in IEEE Communications Magazine, vol. 60, no. 9, pp. 87-92, September 2022, https://arxiv.org/abs/2206.06642

TCP: Chiusura connessione



Courtesy:
Kurose-Ross

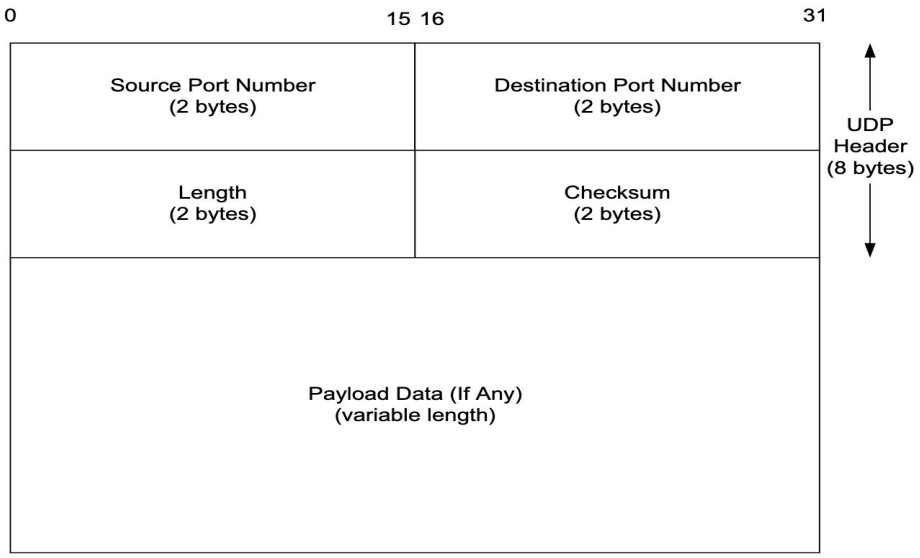
Versioni di TCP

- Diverse versioni di TCP
  - TCP Tahoe: prima versione con congestion control (seguita da TCP Reno, TCP NewReno, ecc.)
  - TCP CUBIC: versione ottimizzata per reti ad alta banda e alta latenza; default in Linux (kernel 2.6.19+), Windows 10 e Windows Server 2016
  - Data Center TCP (DCTCP): versione ottimizzata per comunicazioni tra nodi in uno stesso data center
  - TCP BBR: recente e interessante sviluppo emerso dalla ricerca sul fenomeno del "bufferbloat"
    Si veda N. Cardwell et al. "BBR: Congestion-Based Congestion Control", ACM Queue, 2016, https://queue.acm.org/detail.cfm?id=3022184

User Datagram Protocol (UDP)

- UDP offre un servizio SENZA CONNESSIONE e NON AFFIDABILE
  - non preserva ordinamento messaggi
  - non garantisce consegna di messaggi
  - non fornisce controllo di flusso
  - non fornisce controllo di congestione
  - multiplexing
  - semantica may-be
    - è anche possibile che i messaggi vengano consegnati più volte

UDP header



Courtesy: K. Fall, W. R. Stevens, G. Wright, “TCP/IP Illustrated Volume 1: The Protocols”, 2nd Edition, Addison-Wesley Professional, Pearson, Year: 2012

TCP o UDP?

- La scelta del protocollo di trasporto da usare dipende dal tipo di applicazione che devo realizzare

Application	Application-Layer Protocol	Underlying Transport Protocol
Electronic mail	SMTP	TCP
Remote terminal access	Telnet	TCP
Web	HTTP	TCP
File transfer	FTP	TCP
Remote file server	NFS	Typically UDP
Streaming multimedia	typically proprietary	UDP or TCP
Internet telephony	typically proprietary	UDP or TCP
Network management	SNMP	Typically UDP
Routing protocol	RIP	Typically UDP
Name translation	DNS	Typically UDP

TCP/IP: altri protocolli livello trasporto

- Esistono diversi protocolli di livello trasporto alternativi
  - SCTP: semantica SEQPACKET con supporto a multiflusso e multihoming, ancora in fase sperimentale, non funziona con middleboxes
  - DCCP: in pratica UDP con congestion control, non molto diffuso, non funziona con middleboxes
  - QUIC: ottica dell'ottimizzazione delle performance, innovazione “disruptive”, approccio a livello applicativo, basato su UDP
- Tuttavia, i principali protocolli rimangono TCP e UDP

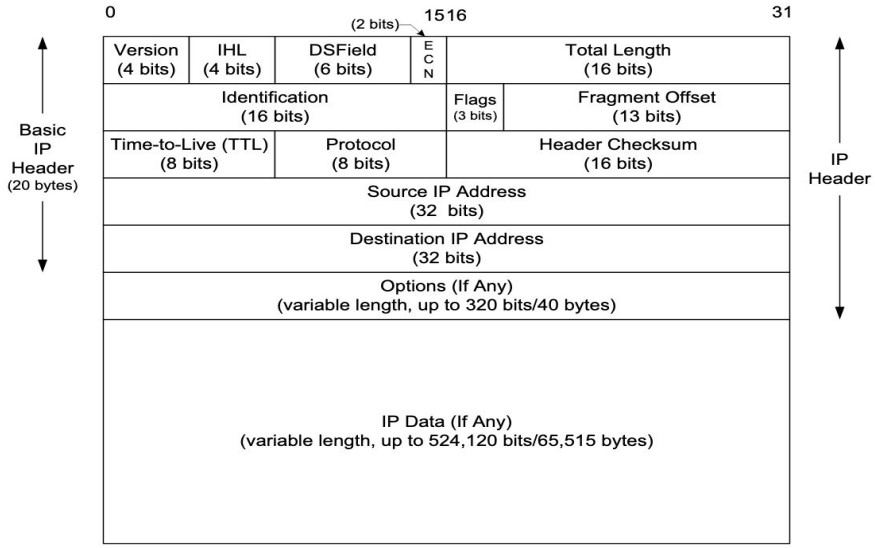
G. Papastergiou et al., "De-Ossifying the Internet Transport Layer: A Survey and Future Perspectives," IEEE Communications Surveys & Tutorials, Vol. 19, No. 1, pp. 619-639, 2017.

Arash Molavi Kakhki et al., “Taking a long look at QUIC: an approach for rigorous evaluation of rapidly evolving transport protocols”, Communications of the ACM, Vol. 62, No. 7, pp. 86-94, 2019.

TCP/IP: Il livello rete

- In TCP/IP il livello rete è implementato dallo Internet Protocol (IP)
- Due versioni di IP attualmente in uso su Internet:
  - IPv4: la versione attuale, che è quella di gran lunga più utilizzata
  - IPv6: la versione futura di IP, attualmente in fase di adozione iniziale
- Diversi strumenti di compatibilità tra IPv4 e IPv6 sono disponibili

IPv4 header



Courtesy: K. Fall, W. R. Stevens, G. Wright, "TCP/IP Illustrated Volume 1: The Protocols", 2nd Edition, Addison-Wesley Professional, Pearson, Year: 2012

Indirizzi IP (versione 4)

- Un indirizzo IPv4 è composto da 32 bit e suddiviso in una parte che identifica la Local Area Network (LAN) in cui esso si trova (network ID) e in una parte di host (host ID)
- La lunghezza del network ID è variabile
- Supporto al subnetting
- Rappresentazione di indirizzi IPv4 segue la cosiddetta “dotted notation”:
  - 192.168.0.1/24

Indirizzi IP (versione 4)

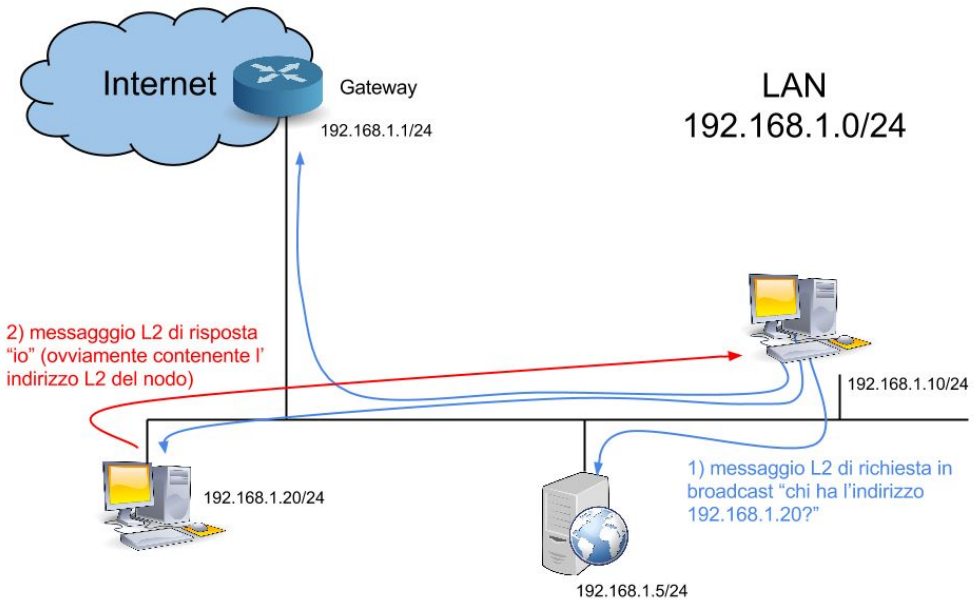
- Il numero massimo teorico possibile di indirizzi IPv4 è di circa 4 miliardi (2^32)
- In realtà non tutti gli indirizzi sono utilizzabili, visto che alcuni indirizzi (~18 milioni) sono riservati per l'uso in reti private:
  - 10.0.0.0/8 (255.0.0.0)
  - 172.16.0.0/12 (255.240.0.0)
  - 192.168.0.0/16 (255.255.0.0)
- In più altri indirizzi sono riservati per multicast
- Infine, limite minimo efficienza di assegnazione indirizzi:

A. Durand, C.Huitema, “The Host - Density Ratio for Address Assignment Efficiency: An update on the H ratio”, RFC 3194, November 2001.

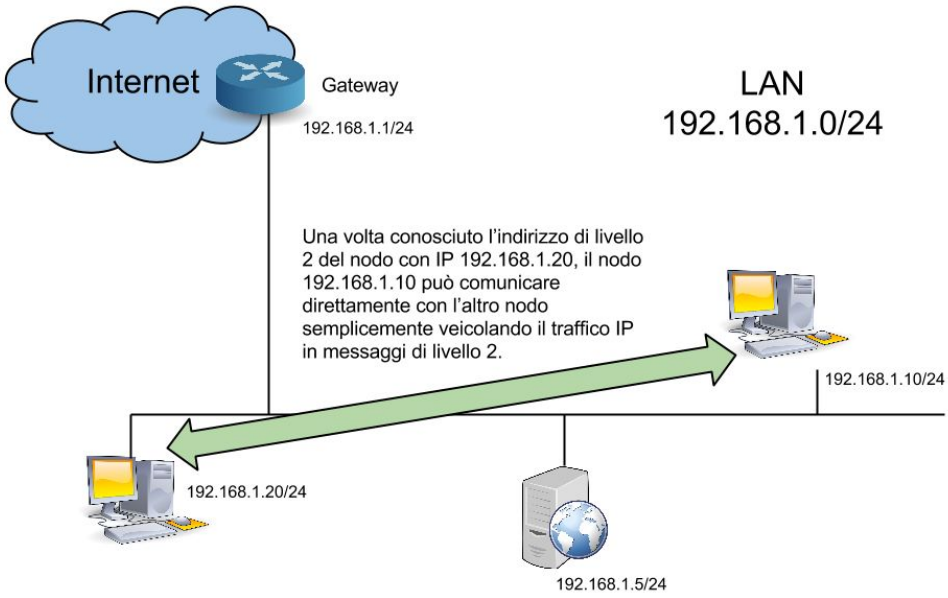
Routing in una LAN

- All'interno di una LAN i dispositivi IP possono comunicare direttamente tra loro semplicemente usando le funzioni offerte dal protocollo di livello 2
- Uso di Address Resolution Prototol (ARP) per scoprire quale indirizzo di livello 2 (link) corrisponda a un dato indirizzo di livello 3 (IP)

Routing in una LAN



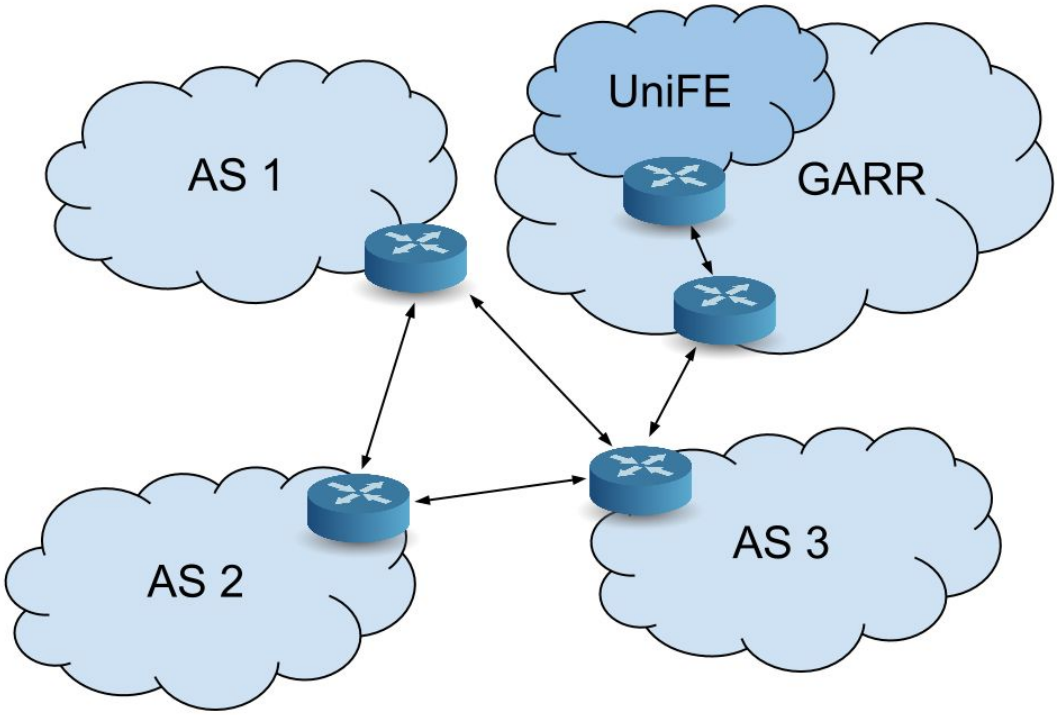
Routing in una LAN



Oltre una LAN: Internet e AS

- Internet è un insieme di Autonomous System, ovverosia reti di primo livello, interconnesse
  - UniFE è nell'AS del GARR, la rete italiana dell'università e della ricerca: http://www.garr.it
- Al loro interno gli AS hanno molte altre sottoreti
  - Ad esempio, al GARR sono collegate molte organizzazioni: http://www.garr.it/a/utenti/organizzazione-collegate

Internet e AS



Routing al di fuori di una LAN

- Per comunicare con nodi al di fuori di una LAN si usa il meccanismo di IP routing
- Speciali dispositivi, detti *router*, si occupano dell'instradamento dei pacchetti
- Ciascun router ha una *tabella di routing*, che contiene le informazioni di instradamento dei pacchetti
- L'instradamento viene fatto a seconda dell'IP di destinazione di un pacchetto, seguendo la regola del *longest matching prefix*

Protocolli di Routing

- La dimensione spesso enorme delle reti impedisce di configurare le informazioni di instradamento manualmente sui router
- Necessità di protocolli che gestiscano automaticamente le tabelle di routing
  - BGP per routing inter-AS
  - OSPF e RIP per routing intra-AS

Problemi di IPv4

- IPv4 ha un numero molto limitato di indirizzi
- Gli indirizzi IPv4 sono praticamente esauriti
  - Quelli a disposizione di Europa e Asia sono esauriti rispettivamente nel 2012 e nel 2011
  - Solo l'Africa si stima avrà sufficienti indirizzi IPv4 fino al 2022
  - Gli altri continenti si stima esauriranno gli indirizzi IPv4 nel 2015
- Necessità di meccanismi per sopperire a questa mancanza:
  - NAT
  - Migrazione a IPv6

Network Address Translation (NAT)

- NAT è una soluzione che trasforma automaticamente indirizzi privati in indirizzi globali
  - All'attraversamento di un dispositivo NAT (tipicamente un router di confine), i pacchetti IP in uscita vengono modificati sostituendo all'indirizzo privato mittente X un indirizzo pubblico Y
  - I pacchetti IP in ingresso per l'indirizzo Y saranno manipolati in modo inverso. Ovverosia, all'indirizzo Y pubblico sarà sostituito l'indirizzo privato X.
- Possibilità di connettere a Internet reti con un numero elevato di indirizzi privati utilizzando un numero relativamente basso di indirizzi pubblici
- NAT è uno strumento molto utilizzato (praticamente ubiquo)

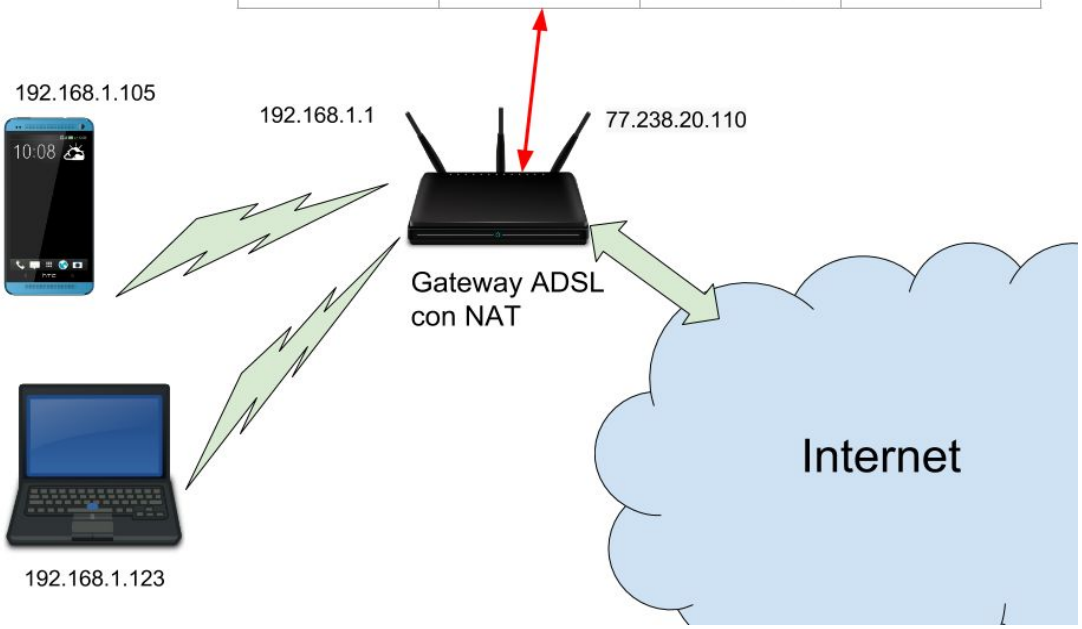
Network Address Translation (NAT)

- Sfortunatamente, il NAT è un approccio che presenta anche numerosi svantaggi
- Problemi nel caso si voglia rendere accessibili all'esterno servizi che girano nella rete con indirizzi privati
  - Necessità di configurazioni ad hoc per server
  - Uso di protocolli per consentire al traffico esterno di passare attraverso il NAT (STUN, TURN, ICE, ecc.)
- Problemi con alcuni tipi di servizi
  - Ad esempio, per abilitare FTP attivo è necessario un NAT steteful con uno specifico modulo di protocol translation
- **Nella Internet moderna, esistono molti strumenti, denominati “middleboxes”, che, come NAT, manipolano il traffico per vari motivi e possono rappresentare un problema per le applicazioni**

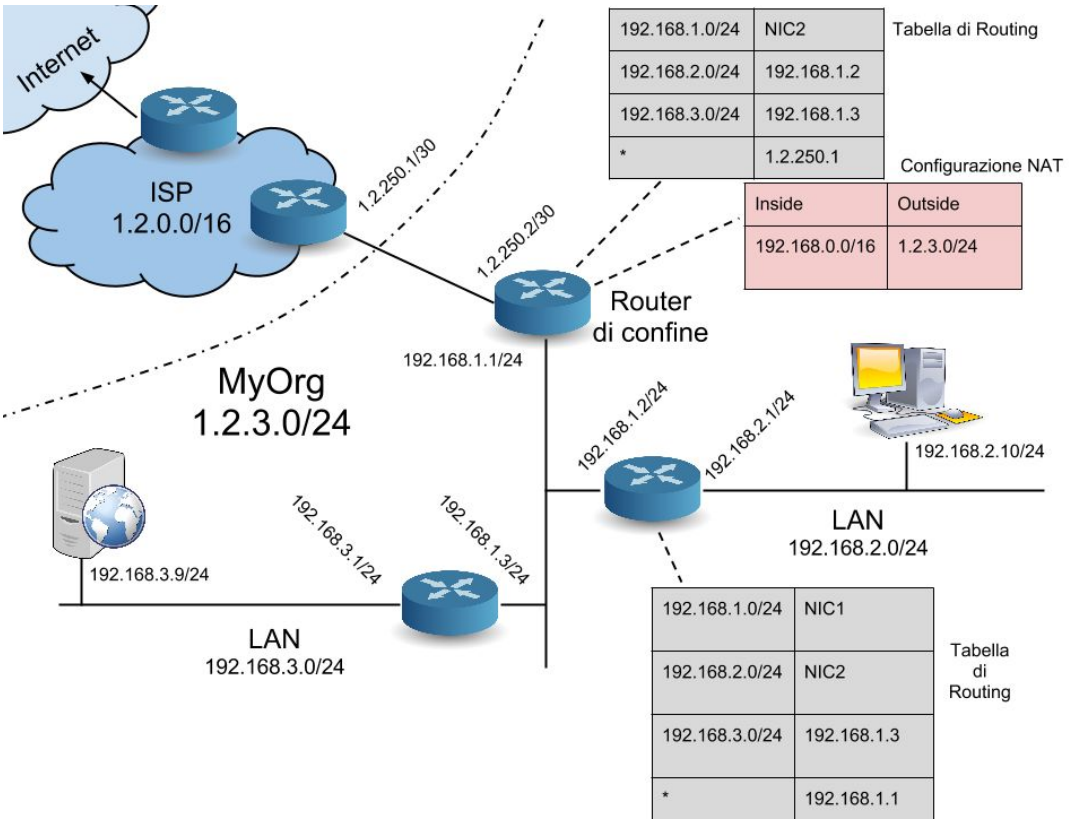
Esempio: NAT in ambienti SOHO

Tabella delle corrispondenze

Indirizzo interno	Porta interna	Indirizzo esterno	Porta esterna
192.168.1.105	50120	77.238.20.110	49123
192.168.1.105	51278	77.238.20.110	65321
192.168.1.123	50328	77.238.20.110	37852



Esempio completo di routing



192.168.1.0/24	NIC2
192.168.2.0/24	192.168.1.2
192.168.3.0/24	192.168.1.3
*	1.2.250.1

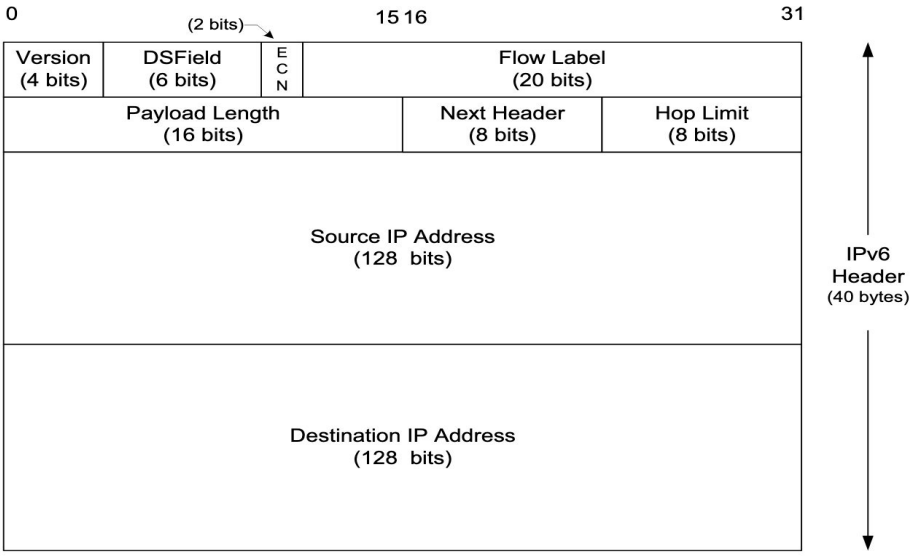
Inside	Outside
192.168.0.0/16	1.2.3.0/24

192.168.1.0/24	NIC1
192.168.2.0/24	NIC2
192.168.3.0/24	192.168.1.3
*	192.168.1.1

IPv6

- IPv6 è la nuova versione di IP, specificatamente progettata per superare i limiti di scalabilità di IPv4
- IPv6 adotta indirizzi di 128 bit
  - Questo consente di allocare (in teoria) $3{,}4 * 10^{38}$ indirizzi (un numero di indirizzi per metro quadro di superficie della Terra maggiore del numero di Avogadro)
- Numerosi vantaggi rispetto a IPv4
  - Adozione di un formato di frame più semplice (e quindi veloce da processare per i router)
  - Indirizzi con diversi scope: link-local, site-local (deprecato) e global
  - Ripensamento di alcuni protocolli in favore di soluzioni più robuste (es. da ARP a Neighbor Discovery)
  - Estensioni per connettere dispositivi low-power

IPv6 header



Courtesy: K. Fall, W. R. Stevens, G. Wright, “TCP/IP Illustrated Volume 1: The Protocols”, 2nd Edition, Addison-Wesley Professional, Pearson, Year: 2012

Indirizzi IPv6

- Rappresentazione esadecimale
  - FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
- Sequenze di zeri sono abbreviate con “::”
  - 1080:0:0:0:0:0:200C:417A = 1080::200C:417A
- Tre tipologie di indirizzo:
- Unicast
- Anycast
- Multicast

Indirizzi IPv6

- Vari scope di indirizzamento
  - Link local (FE80::/10)
  - Site local (FEC0::/10) (deprecato)
  - Global (2000::/3)
  - Multicast (FF00::/8)
- Indirizzi di tipo speciale:
- IPv4-mapped (::FFFF:0:0/96)
- IPv4-compatible (::/96)
- 6to4

Adozione di IPv6

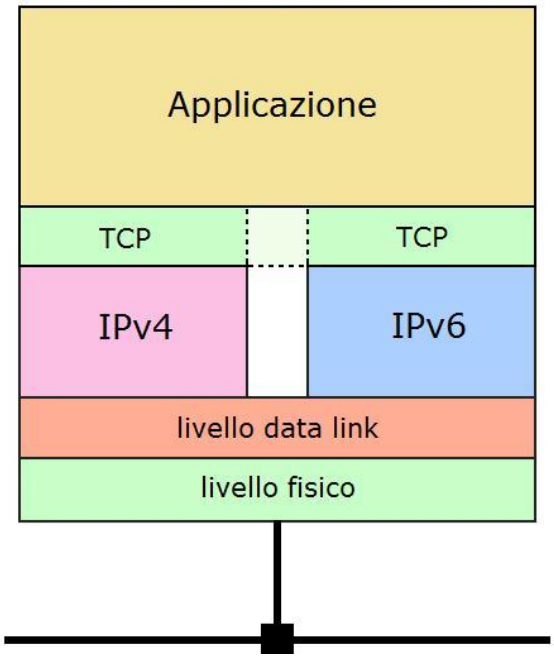
- Per supportare IPv6 c'è la necessità di modificare tutto il software (applicazioni e sistemi operativi) e il firmware (che gira in router, switch, gateway, ecc.) di rete
  - Talvolta questo comporta notevoli problemi (es. FTP, gateway DSL)
- La maggior parte di sistemi operativi, applicazioni e router supporta già IPv6

Compatibilità IPv4 e IPv6

- Al momento esistono fondamentalmente 3 situazioni per quanto riguarda la connettività IP:
  - reti con sola connettività IPv4 (es. WiFi UniFE)
  - reti con sola connettività IPv6
  - reti sia con connettività IPv4 che con connettività IPv6 (es. rete fissa UniFE)
- **Bisogna progettare applicazioni in grado di funzionare in tutte e tre le condizioni summenzionate**
- Servono soluzioni per far parlare le reti del primo tipo con quelle del secondo

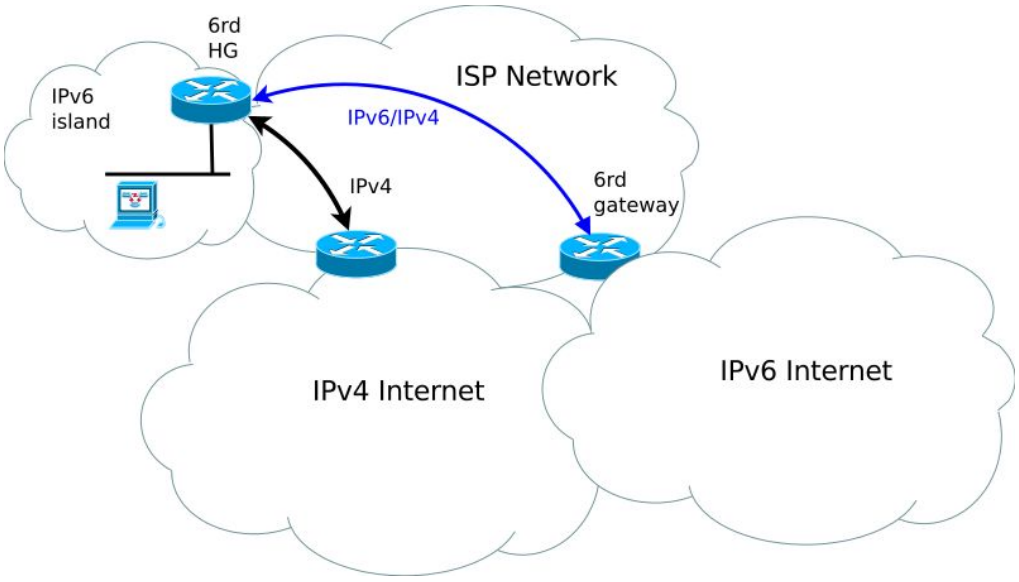
Applicazioni

- **Le applicazioni di rete moderne devono essere esplicitamente sviluppate per supportare sia IPv4 che IPv6 e adattarsi alle situazioni in cui un protocollo di rete sia non disponibile o privo di connettività** (vedremo come)



Courtesy: Wikipedia

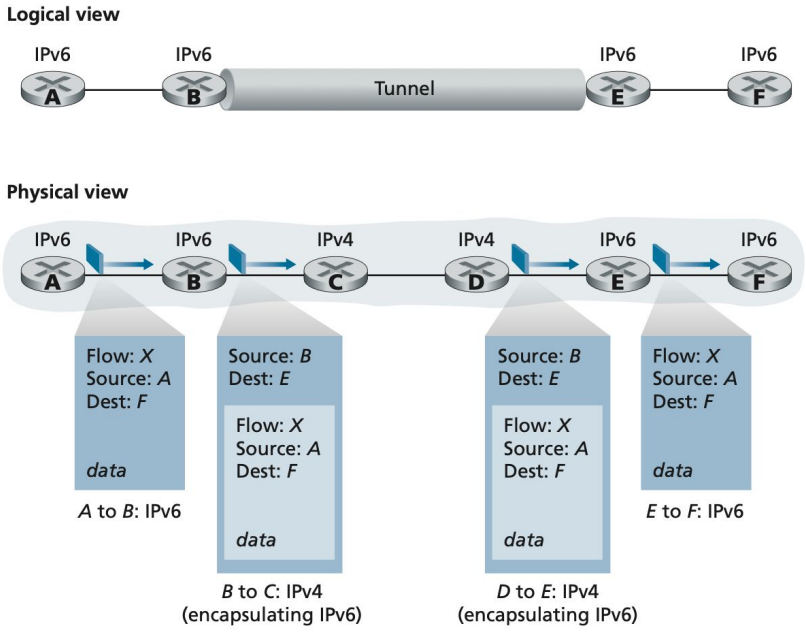
Strumenti di Retrocompatibilità



Courtesy: Wikipedia

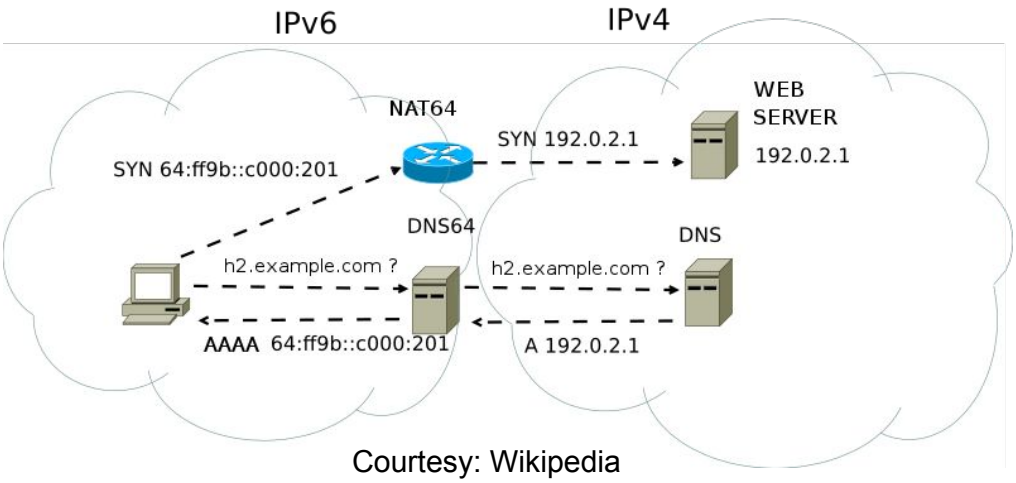
Strumenti di Retrocompatibilità

Veicolare traffico su tunnel (IPv6-in-IPv4 o IPv4-in-IPv6) rappresenta il meccanismo fondamentale



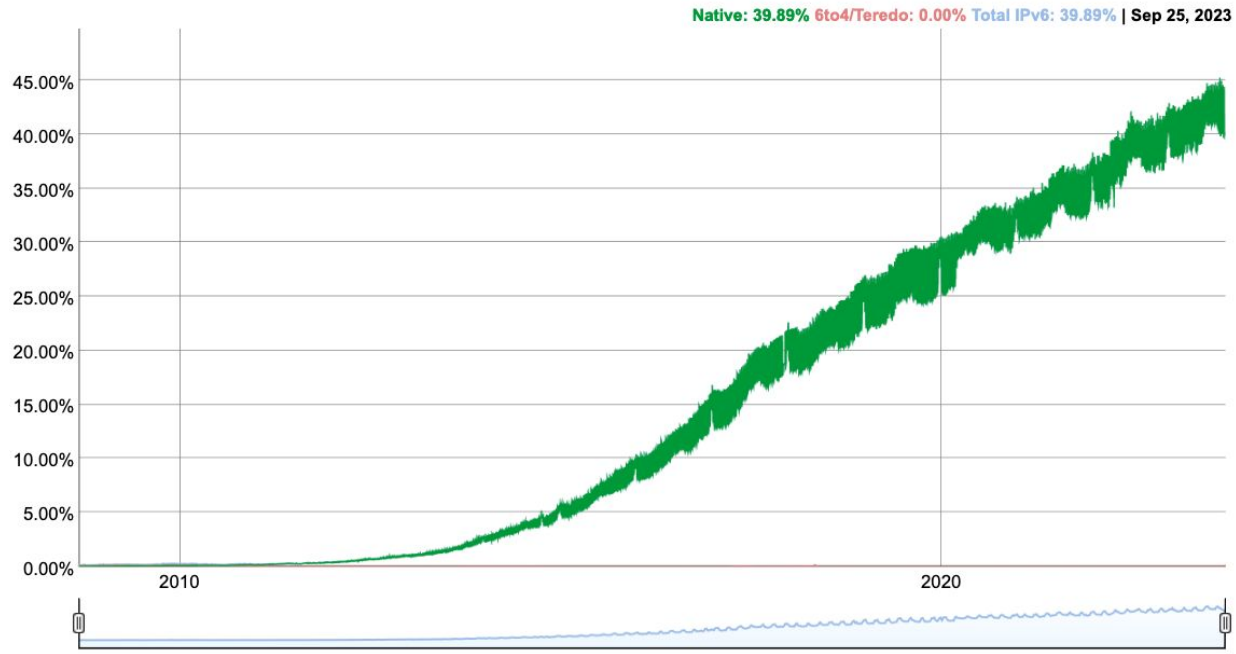
Strumenti di retrocompatibilità

Numerosi strumenti per facilitare la migrazione a IPv6 pur preservando la possibilità di comunicare con la vecchia rete IPv4 (NAT64 / DNS64, SIIT, 464XLAT, ecc.)



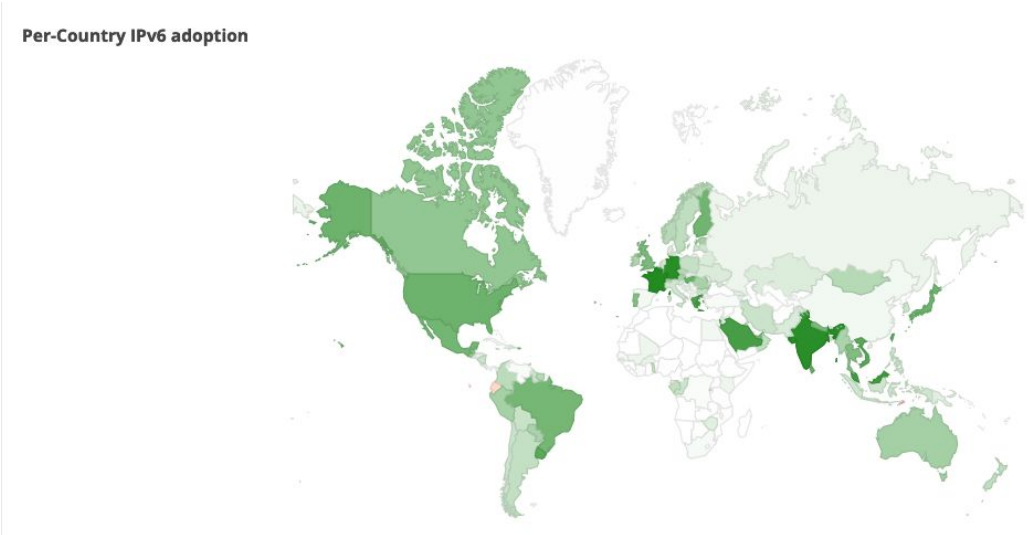
Courtesy: Wikipedia

Diffusione di IPv6 - globale



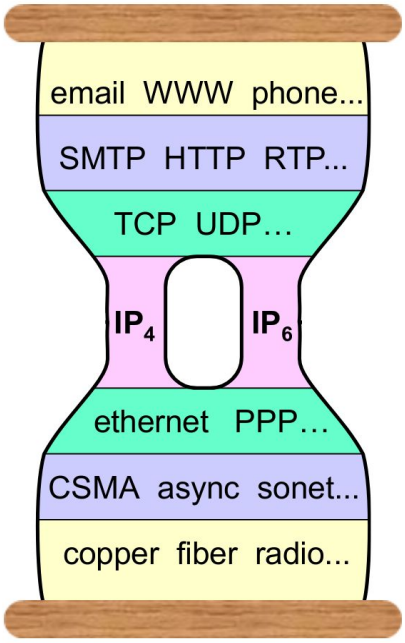
Secondo l'osservatorio di Google (https://www.google.com/intl/en/ipv6/statistics.html), più del 40% del traffico Internet al mondo viene veicolato su IPv6. (In Italia, molto meno: solo il 15%. Ma la situazione sta apparentemente migliorando: a settembre 2022 eravamo al 7.15%.)

Diffusione di IPv6 - per nazione



Secondo l'osservatorio di Google (https://www.google.com/intl/en/ipv6/statistics.html), più del 40% del traffico Internet al mondo viene veicolato su IPv6. (In Italia, molto meno: solo il 15%. Ma la situazione sta apparentemente migliorando: a settembre 2022 eravamo al 7.15%.)

Modello a doppia clessidra



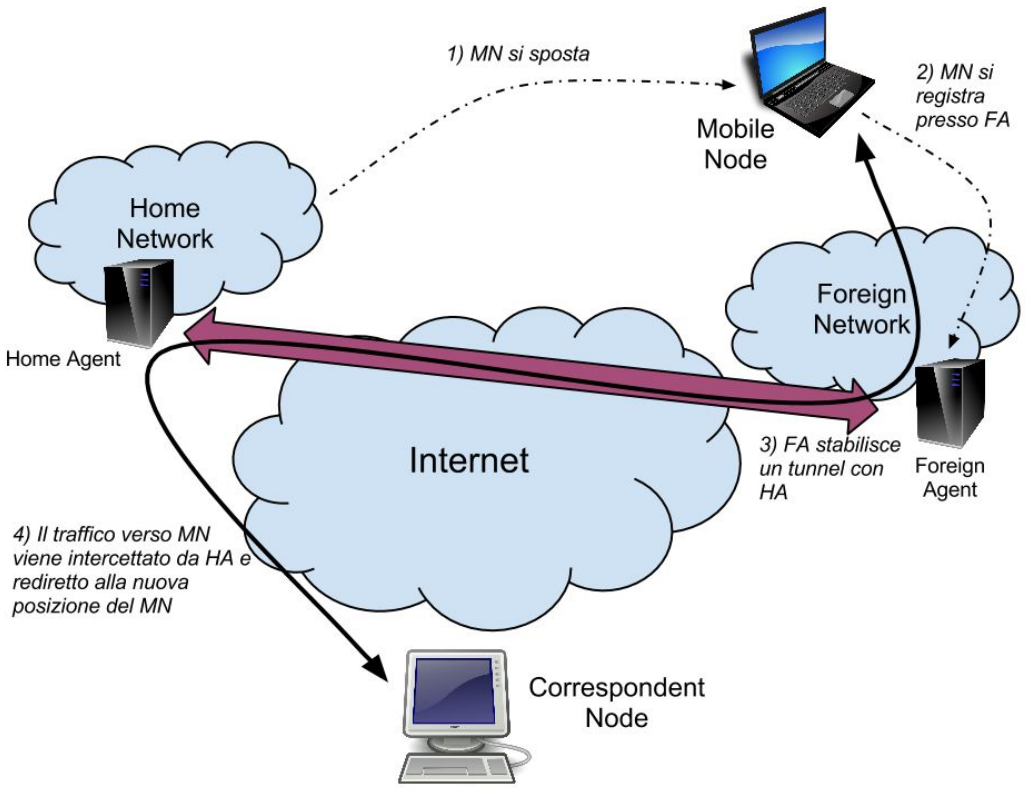
TCP/IP e mobilità

- Purtroppo TCP/IP è stato progettato per una rete fissa e non offre un buon supporto per i terminali mobili
  - La causa fondamentale è la duplice natura di ID e di "locator" degli indirizzi IP
- Adozione di diversi meccanismi per fornire il supporto alla mobilità dei nodi
  - DHCP
  - Mobile IP

Dynamic Host Configuration Protocol (DHCP)

- DHCP è il protocollo di autoconfigurazione attualmente più usato
- DHCP assegna dinamicamente un indirizzo IP a un nodo
  - Time-based leasing per riuso indirizzi
  - Riassegnazione dello stesso indirizzo allo stesso host se possibile
- Inoltre, DHCP configura anche gateway e DNS
- In IPv6 il ruolo del DHCP viene tipicamente svolto dallo Stateless Address Autoconfiguration (esiste pure DHCPv6, ma è quasi inutilizzato)

Mobile IP (MIPv4)



Mobile IPv6 (MIPv6)

- Più performante di MIPv4
  - Route optimization incluso nel protocollo
  - Uso di Routing Header vs. incapsulazione
  - Dynamic Home Address Discovery usa anycast e ritorna una singola risposta al nodo mobile
  - Largo uso di piggybacking grazie alle Dest. Opt.
- Più sicuro di MIPv4
  - Uso obbligatorio di IPSEC
  - Facilitato l'uso di packet filtering

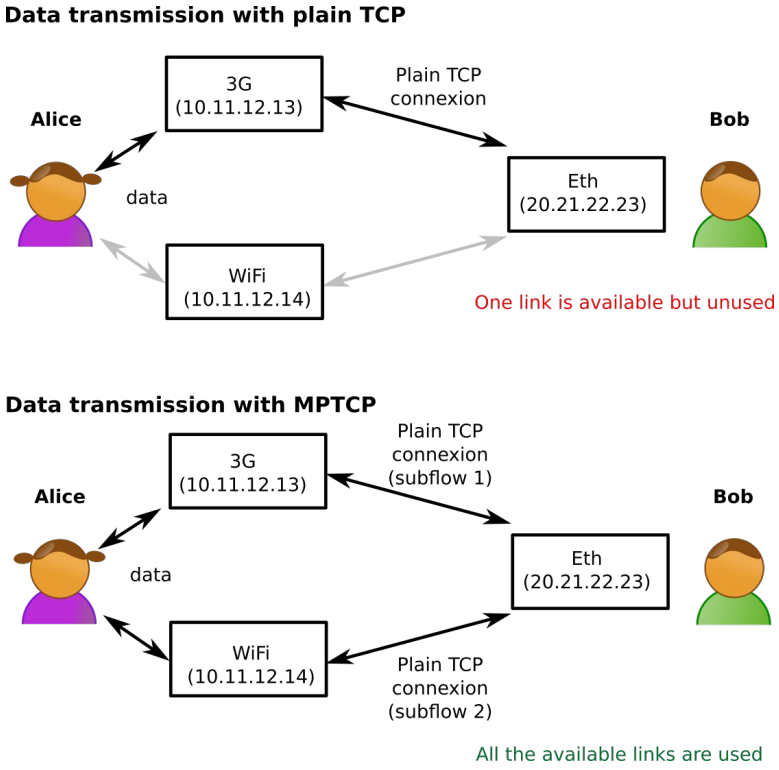
Mobile IPv6 (MIPv6)

- Più robusto e flessibile di MIPv4:
  - Uso di Neighbor Discovery al posto di ARP
  - Facilitato il routing di traffico multicast
  - Non sono più necessari Foreign Agent
  - Meccanismo di movement detection bidirezionale
  - Nuova opzione “Advertisement Interval” sul Router Advertisement
- Ciò nonostante, nemmeno MIPv6 è in grado di risolvere completamente i problemi di mobilità di IP
  - Network mobility
  - Administrative burden
  - Always best connected

Multipath TCP

- Versione di TCP con supporto multipath (ovverosia a connessioni che usano N>1 endpoint e N subflow) pensata per dispositivi mobile
- Supportato da tutti i principali sistemi operativi, soprattutto in ambito mobile
- Soluzione (relativamente) semplice ma molto efficace

Multipath TCP



Courtesy: Wikipedia

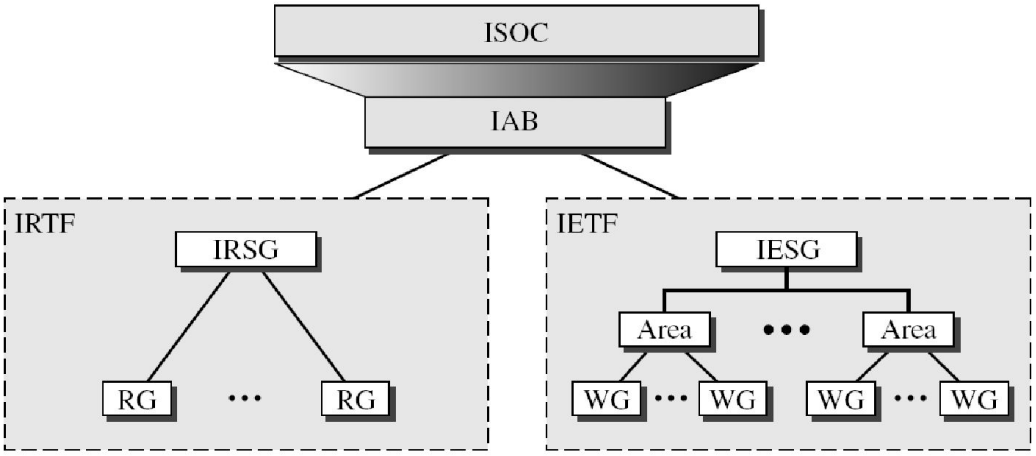
TCP/IP: sotto il livello rete

- L'ubiquità di IP permette all'ingegnere informatico, che si occupa di sviluppare applicazioni di rete, di non curarsi dei protocolli di livello 1 e 2
  - Ragioniamo sempre in termini di scambio di messaggi su TCP o UDP
  - In larga misura, si può anche ignorare la tecnologia di comunicazione sottostante
- Tuttavia, si deve fare sempre molta attenzione ad alcuni aspetti molto importanti:
  - Performance
  - Middleboxes
  - Supporto a IPv6

Internet - Organi di Controllo

- Il principale organo di controllo di Internet è la Internet Society (ISOC)
- ISOC è un'organizzazione internazionale (con sedi a Washington e Ginevra) non governativa per la promozione dell'utilizzo e dell'accesso a Internet
- La Internet Architecture Board (IAB) è l'organo tecnico di ISOC
- IAB ha diverse sottoorganizzazioni, la più importante delle quali è certamente IETF

ISOC



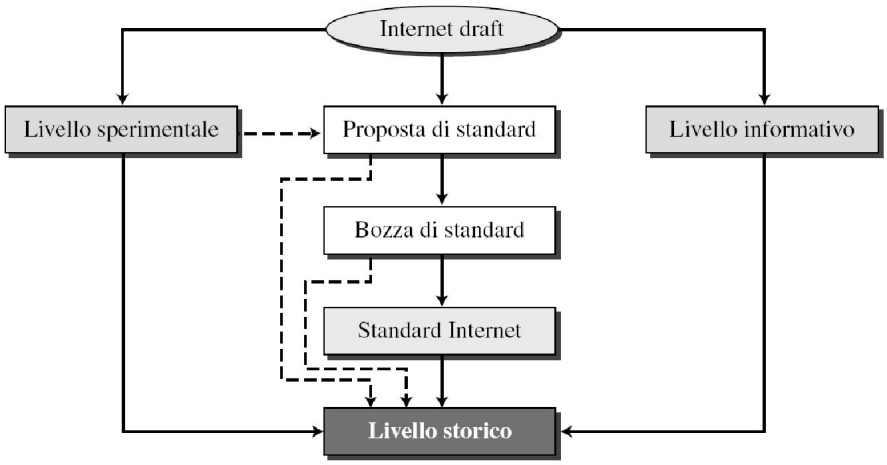
Internet Engineering Task Force (IETF)

- IETF è l'organo che ha il compito di definire le specifiche dei protocolli di rete usati su Internet
  - http://www.ietf.org
- Composta da ingegneri e ricercatori che contribuiscono gratuitamente con il proprio lavoro
- Diversi comitati (working group) che lavorano su un tema specifico
  - http://datatracker.ietf.org/wg/
- Organizzazione molto democratica
  - Working group decidono “a consenso”
  - Tutti possono partecipare

RFC

- I Request For Comments (RFC) sono i documenti fondamentali che definiscono gli standard di Internet
- Accessibili liberamente sul Web all'indirizzo http://www.rfc-editor.org

RFC: Processo di Pubblicazione



Per ulteriori informazioni visitate il sito Web
http://www.rfc-editor.org/pubprocess.html

Internet Assigned Numbers Authority (IANA)

- IANA è un dipartimento di ICANN con il compito di coordinare alcuni degli elementi chiave che permettono a Internet di continuare a funzionare senza intoppi
- In particolare, IANA gestisce:
  - Assegnazione corrispondenze tra servizi e numeri di porta
  - Allocazione indirizzi IP agli Internet Registry
  - Root DNS

Internet Registry

- Gli indirizzi IP (sia IPv4 che IPv6) vengono generalmente assegnati in modo gerarchico
- Gli utenti ottengono gli indirizzi IP dal proprio Internet Service Provider (ISP)
- Gli ISP ottengono l'assegnazione di indirizzi IP da un Local Internet Registry (LIR), da un National Internet Registry (NIR), o dal corrispondente Regional Internet Registry (RIR)

Regional Internet Registry

- Esistono 5 Regional Internet Registry
  - AfriNIC Africa Region
  - APNIC Asia/Pacific Region
  - ARIN North America Region
  - LACNIC Latin America and some Caribbean Islands
  - RIPE NCC Europe, Middle East, and Central Asia
- Il nostro RIR di riferimento è ovviamente RIPE
  - http://www.ripe.net/