

1° PARTE

La Storia di Internet

Anni 60'

- Internet è il risultato dell'evoluzione del concetto di Galactic Network discussa da J.C.R. Licklider nell'agosto 1962:
"Infrastruttura basata su un insieme di computer globalmente interconnessi"
- Licklider è stato il direttore del programma di ricerca in computer del progetto DARPA, iniziato nell'ottobre del 1962:
 - Egli convinse i suoi successori a DARPA dell'importanza del concetto di rete
 - Il nome cambia numerose volte da progetto ARPA (*Advanced Research Projects Agency*) a DARPA (*Defence Advanced Research Projects Agency*) e viceversa, ma attualmente è chiamato DARPA

-Nel 1962 viene completato il sistema SAGE:

- *Semi Automatic Ground Environment*
- Diventa il primo sistema di allarme in Nord America
- Basato sui sistemi di puntamento ottici in grado di identificare gli oggetti in movimento e mostrarli negli schermi radar
- Usato per dirigere la difesa aerea

-Nel 1961 Kleinrock pubblica il primo libro sulla teoria del "Packet Switching" (scambio di pacchetti dati)

→ Lo step successivo fu quello di far parlare due computer:

- Nel 1965, Roberts ha connesso The TX-2 computer in Massachusetts con il Q-32 in California con un collegamento dial-up a bassa velocità, creando la prima wide-area computer network
- Il risultato di questo esperimento confermò gli studi di Kleinrock e la necessità dell'introduzione del Packet Switching

-Nel 1969 prima connessione riuscita host-to-host dal primo nodo UCLA a Stanford al secondo nodo ARPANET

→ Al primo login IMP è andato in crash, ma al secondo è riuscito

→ Nell'aprile di quell'anno Steve Crocker invia un documento intitolato "Request for Comments", il primo che ha documentato l'architettura di ARPANET e di internet

ANNI 70'

- Nel 1972 L'ILLIAC IV, il più grande supercomputer di quei tempi viene collegato alla rete ARPANET per consentire a migliaia di scienziati l'accesso remoto alle sue uniche capacità di calcolo.
- Nel 1973 Vint Cerf e Bob Kahn a Stanford creano il TCP/IP: nasce la posta elettronica
- Sempre in quell'anno Bob Metcalfe inventa l'Ethernet

-Nel 1976 Seymour Cray dimostra il primo supercomputer basato su processore vettoriale: Il Cray-1

-Nel 1979 Vint Cerf, in DARPA, continua a perseguire la sua visione di Internet formando *L'International Cooperation Board* e un *Internet Configuration Control Board* al MIT.

- Sempre in quell'anno Landweber alla Wisconsin University disegna un network scientifico CSNET

Anni 80'

- Nel 1980 TCP viene adottato come protocollo standard dal DoD (dipartimento di difesa USA)
- Inizia l'attività di USENET e compaiono i primi gruppi di discussione delle NEWS (prima applicazione client-server)
- Agli inizi del 1981 oltre 200 computer connessi al CSNET
 - Sempre in quell'anno viene lanciato il primo computer portatile, Osborne, e il PC IBM, uno dei primi computer personali a essere ampiamente adottato sia nel settore commerciale che domestico.
- Nel 1983, Jon Postel con altri collaboratori sviluppano il Domain Name System (il DNS) e raccomandano l'uso della forma di indirizzamento “*user@host.domain*”
 - Il numero di host connessi cresce sempre più, anche grazie alla commercializzazione di Ethernet
 - ARPANET abbandona il protocollo di comunicazione tra mainframe NCP ed adotta TCP/IP
 - A causa dell'aumento numero di host in rete, vengono introdotte le reti IP di classe A,B e C.
- Nel 1984 vengono introdotti i nomi a dominio con i famosi Top Level Domain (TLD) .edu, .com, .net, .org, e la codifica ISO per i nomi delle nazioni del mondo (.it, .fr , .de)
 - In Inghilterra nasce la rete JANET, per connettere la comunità scientifica
 - In America invece la NSF (National Science Foundation) costituisce i supercomputer centers, per connettere anch'essa la comunità scientifica.
- Nel 1985 nasce NSFNET, acronimo di National Science Foundation Network, una rete di computer ad alta velocità finanziata dalla National Science Foundation (NSF) degli Stati Uniti. È stata un'iniziativa chiave per lo sviluppo delle infrastrutture di Internet.

-Altri importanti avvenimenti in questo decennio:

- Gli host internet passano da 2000 a 30000 in un anno
- Il TCP è disponibile nelle workstation e nei PC
- Ethernet è accettata come tecnologia di cablaggio di edifici e campus
- Compaiono le prime multinazionali operanti nel settore delle reti
- Il 30/04/1986 l'Italia si connette ad internet
- NFS intuisce la portata e il significato commerciale della velocità di crescita di Internet e la sua rete passa da linee T1 (1.55 Mbps) a linee T3 (45 Mbps)
- NFS fino alla fine del decennio connette tutti i paesi più potenti al mondo

-Tim Berners-Lee nel 1989 al CERN (Consiglio europeo per la ricerca nucleare) propone il concetto di ipertesto: NASCE IL WORLD WIDE WEB!

Anni 90'

- Nel 1990 ARPANET viene chiusa
- Nel 1991 nasce PGP, acronimo di "Pretty Good Privacy", un software di crittografia utilizzato per la protezione della privacy e la sicurezza delle comunicazioni digitali. È stato sviluppato da Phil Zimmermann ed è diventato uno dei programmi più diffusi per crittografare e decrittografare e-mail, file e altri dati digitali.

-Nel 1995 The Federal Networking Council (FNC) usa il termine “Internet” riferendosi al sistema globale di informazione che:

- è collegato insieme da un unico globale indirizzo basato sull'IP
- è capace di supportare le comunicazioni utilizzando il TCP (transmission Control Protocol)

Anni 2000

-Grazie alla diffusione massiva di dispositivi cellulari, l'incremento delle capacità computazionali sui dispositivi mobili e lo sviluppo di nuove tecnologie (Javascript e HTML), nascono i social network

-Nel 2002 viene fondata Linkedin, social orientato all'occupazione professionale

-Nel 2004 Mark Zuckerberg fonda Facebook, nel 2006 Twitter fondata da Jack Dorsey, Biz Stone e Evan Williams

-Nel 2005 tre ex dipendenti di paypal sviluppano e lanciano youtube, acquistata da google nel 2006 dopo il suo enorme successo

-Nel 2010 viene lanciata da Kevin Systrom e Mike Krieger Instagram, orientato allo scambio di immagini e video

2° PARTE

Internet

Definizione

Internet è una **rete globale di reti** che abilita sistemi informatici a **comunicare direttamente** ed in modo trasparente e a condividere servizi in ogni parte del mondo. Costituisce inoltre anche una **fonte condivisa e globale di informazioni**, conoscenza e senso di collaborazione e cooperazione tra diverse e innumerevoli comunità. È definita formalmente nell'RFC1122 (specificazione tecnica che stabilisce le linee guida per l'implementazione di IPv4 su reti locali).

L' **Internet Protocol** (IP) fornisce esclusivamente le funzioni necessarie per l'**invio** di un pacchetto di bit (**datagram**) da una **sorgente ad una destinazione** che sono due host (qualsiasi dispositivo collegato a una rete che partecipa alla comunicazione tramite il protocollo IP) identificati ciascuno da un indirizzo a lunghezza fissa, l'indirizzo IP.

L'**IP versione 4** fornisce anche i servizi di **frammentazione e riassemblaggio** di datagram, quando la trasmissione avviene attraverso reti con capacità di trasporto di pacchetti più piccola del pacchetto originale. **IP versione 6 abolisce** questo comportamento in quanto non più necessario.

L'IP è invocato dai protocolli host-to-host e invoca i protocolli di rete locali per trasportare l'internet datagram al successivo **gateway** (dispositivi o componenti di rete che sono responsabili della trasmissione dei datagram) o host di destinazione.

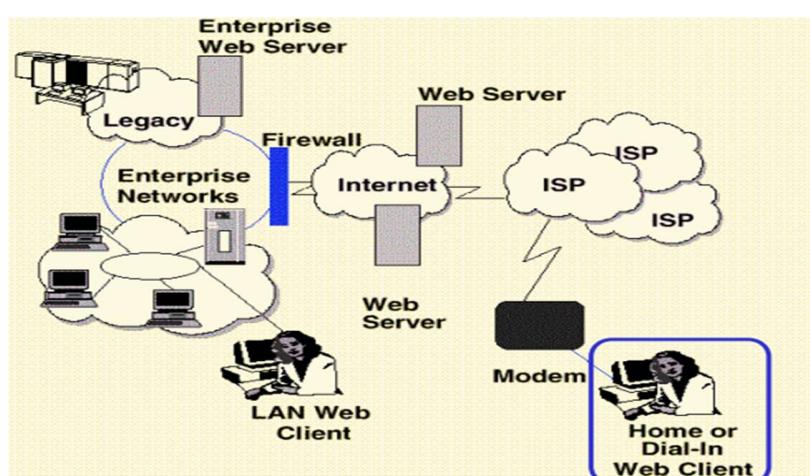
L'IP tratta ogni internet **datagram come entità completamente indipendente** dagli altri internet datagram. I vari **moduli internet** (dispositivi o componenti di rete che sono responsabili della trasmissione dei datagram, come router o switch) usano gli **indirizzi** presenti nell'**internet header** (parte fondamentale del pacchetto di dati IPv4 che contiene numerose informazioni) per **trasmettere i datagram** internet verso le loro destinazioni. La **selezione del cammino da seguire** per la trasmissione è chiamato **routing** e il modello operativo prevede che un modulo internet risieda in ogni host impegnato in comunicazioni internet e in ogni gateway che interconnette delle reti. Il routing è un **processo dinamico**, che tiene conto delle variazioni istantanee della rete, che viene eseguito avvalendosi dei protocolli di routing dinamici.

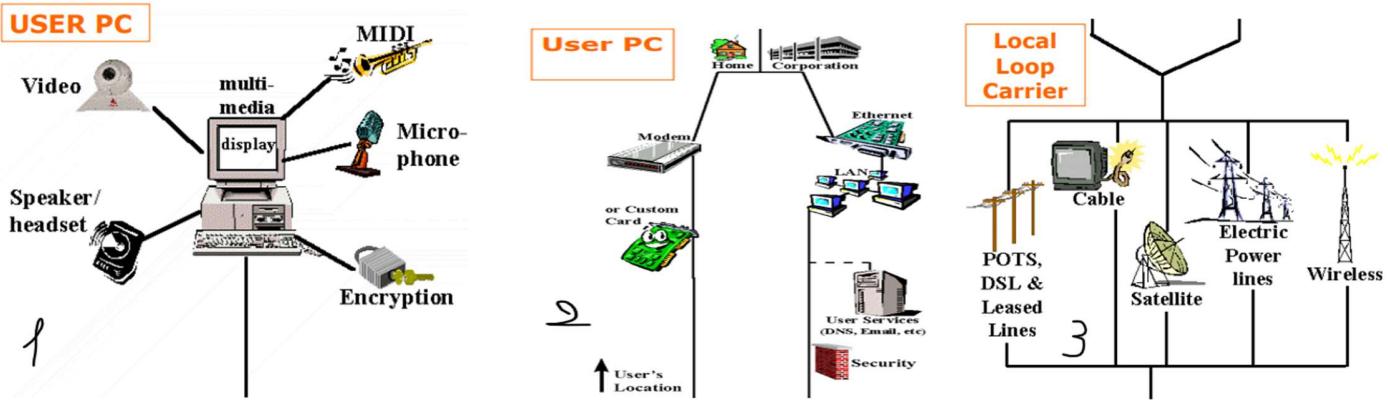
I **moduli** condividono delle **regole comuni** per interpretare i campi dell'indirizzo internet, per frammentare e riassemblare datagram. I **gateway**, possiedono procedure per effettuare anche scelte di routing.

Elementi dell'infrastruttura

Andremo ora ad
di elementi di una

analizzare i seguenti livelli
infrastruttura Internet





1) Home or Dial-In Web Client

Un qualsiasi dispositivo oggi è abilitato a ricevere e inviare messaggi di tipo audio e video.

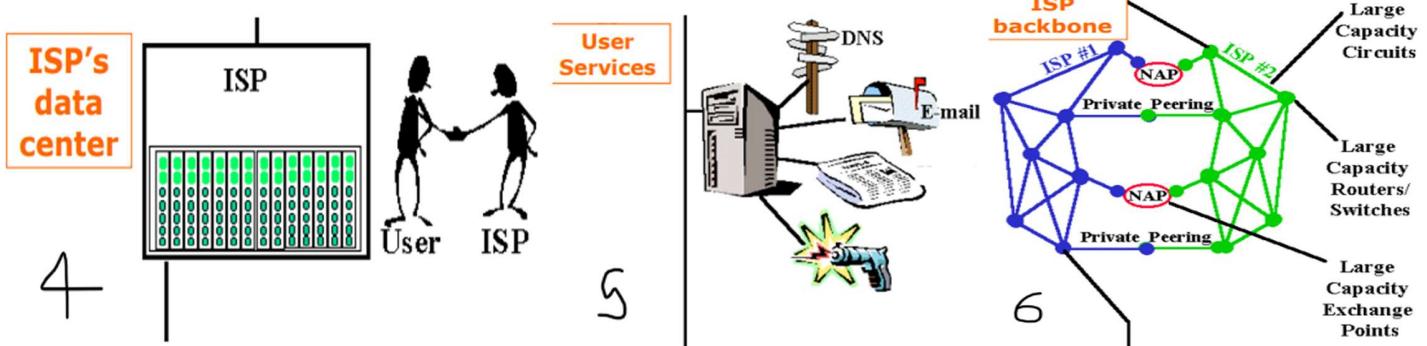
Questo è possibile grazie a componenti come: Scheda Audio, Microfono, Casse, Scheda Grafica, Webcam, Riconoscitori vocali

2) Modem

Sono gli apparati dell'utente per connettere il PC dell'utente al "Local Loop" (Customer Premise Equipment - CPE) come la linea telefonica, l'ADSL, FTTH, NAT, Firewall, LAN, WIFI

3) Communication Line

Connette l'utente all'ISP (Internet Service Provider, azienda servizi rete): come ADSL, Fibra Ottica, Wireless, Satellite, Cable network e Elettric Power Lines



4) ISP

Il punto di accesso all'ISP generalmente è il data center centrale. Le connessioni vengono veicolate dalle centrali del fornitore dei servizi di ultimo miglio della rete di accesso (Telecom) al fornitore di servizi che ha il diritto di vendita del servizio all'utente.

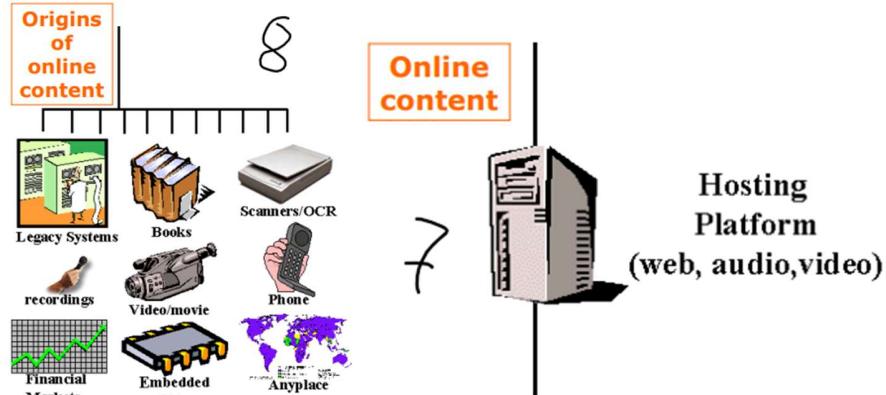
5) Internet-WebServer

Sono i servizi che gli utenti usano durante l'accesso ad Internet come Email, Domain Name Server, SSH, User Web Hosting. Questi server richiedono collegamenti veloci, processori potenti e grandi quantità di memoria quindi devono essere fault tolerant (continuare a lavorare anche se ci sono errori che vengono limitati) e load balanced (carico di lavoro di rete equidistribuito).

6) ISP backbone

Gli Internet Service Provider (ISP) utilizzano un'infrastruttura complessa per interconnettere i loro punti di presenza (POP), gli altri ISP e il contenuto online. Il nucleo di questa infrastruttura è costituito dal backbone dell'ISP, che collega i POP tra loro e con altre reti Internet. Il backbone utilizza tecnologie avanzate come la fibra ottica e dispositivi come router e switch per instradare il traffico dati in modo efficiente e affidabile. I backbone providers forniscono connettività ad alta velocità agli ISP, mentre i Network Access Points (NAP) sono punti di interconnessione tra ISP che ottimizzano il percorso del traffico. Inoltre, i Neutral Access Points (NAP) forniscono punti di interconnessione neutrali per facilitare lo scambio di traffico tra gli ISP. Questa complessa infrastruttura è progettata per garantire una

connettività Internet affidabile e di alta qualità per gli utenti finali.



7) Online content

Sono gli host con cui interagiscono gli utenti. – Web Server platforms – Hosting Farms I sistemi Cloud offrono soluzioni scalabili a costi sostenibili

8) Origins of online content

L'architettura dell'infrastruttura di Internet è il fondamento su cui si basa la connettività e lo scambio di informazioni nel mondo digitale. Essa comprende:

- La connessione delle sorgenti di informazioni del mondo reale, che possono essere sia risorse elettroniche esistenti sia legacy systems, ossia sistemi basati su tecnologie obsolete ma ancora utilizzati per le loro caratteristiche di affidabilità e sicurezza.
- L'integrazione delle risorse stampate attraverso scanner per convertirle in formato elettronico, consentendo così la digitalizzazione e l'accesso online a informazioni precedentemente disponibili solo in formato cartaceo.
- La trasmissione di una vasta gamma di contenuti audio e video in modalità broadcast su Internet, rendendo disponibili programmi televisivi, radiofonici e altri media digitali agli utenti online.
- L'implementazione della tecnologia Voice over IP (VOIP) che consente la trasmissione delle comunicazioni vocali attraverso Internet, offrendo un'alternativa economica e flessibile alle tradizionali linee telefoniche.

Architettura dell'infrastruttura di Internet

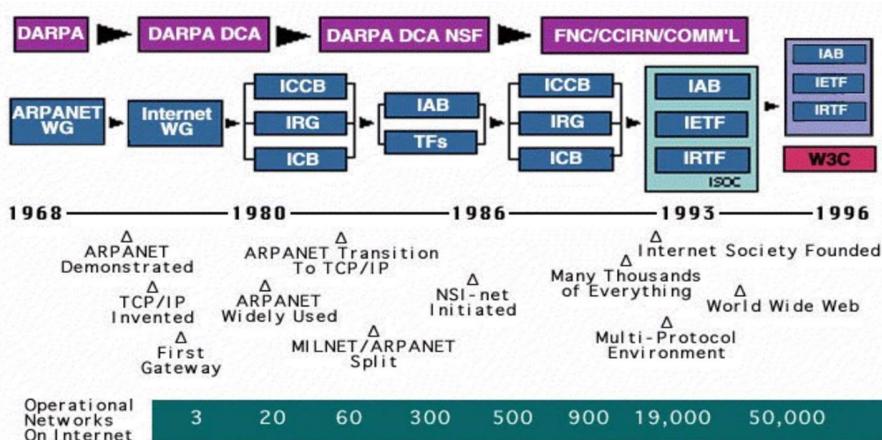
IIII!

Internet governance

L'**Internet governance** è una **struttura** complessa e meritocratica **organizzata** nel seguente modo:

- I leader storici, i quali coordinano i vari organismi di standardizzazione
- I rappresentanti dei governi
- Le aziende che hanno il core business in questo mondo
- I tecnici e gli sviluppatori che mantengono e sviluppano i principali software
- Gli utenti, che con i loro canoni pagano per usare la rete e portano denaro

Evoluzione del governo di Internet



Un ente storico: IANA

Alcuni Standard di Internet hanno bisogno di una **forma organizzativa** come la gestione dello spazio di indirizzamento IP o dei numeri protocollo IP

La responsabilità complessiva di ciò è **assegnata** all'Internet Assigned Numbers Authority (**IANA**)

Regional Internet Registries

IANA ha delegato ad alcune entità regionali la gestione locale:

- ARIN per le Americhe
- RIPE NCC per l'Europa
- Asia-Pacific-NIC (**APNIC**) per l'area Asia-Pacifico
- Latin America and Caribbean Network Information Centre (**LACNIC**)
- African Network Information Centre (**AFRINIC**) per l'Africa

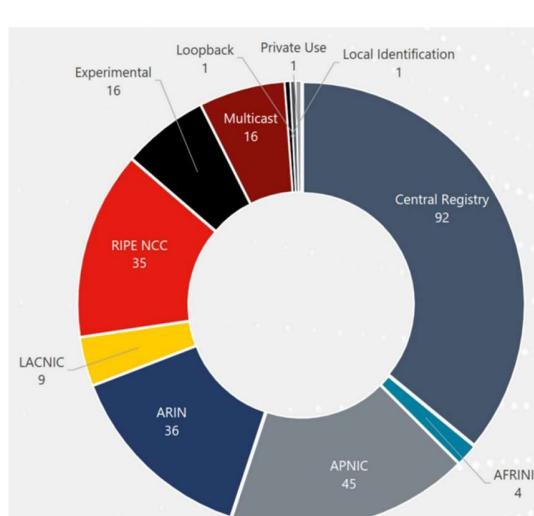
ICANN



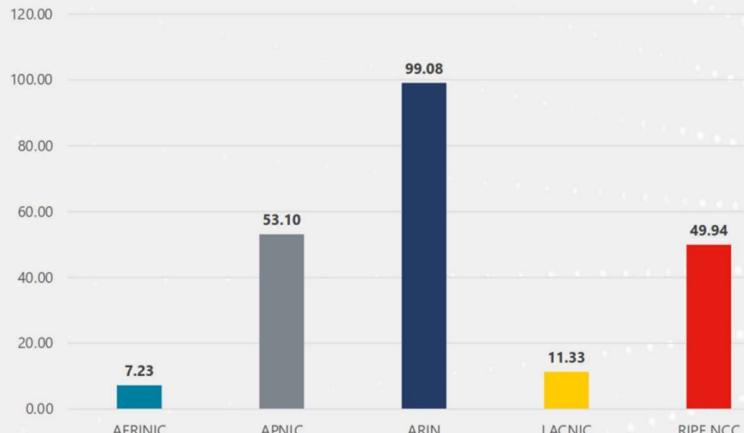
L'**ICANN** (Internet Corporation for Assigned Name and Numbers) è l'ente che coordina i Regional Internet Registries ed ha una **struttura più partecipata** e democratica rispetto a IANA.

Amministrazione di Internet e gestione degli spazi

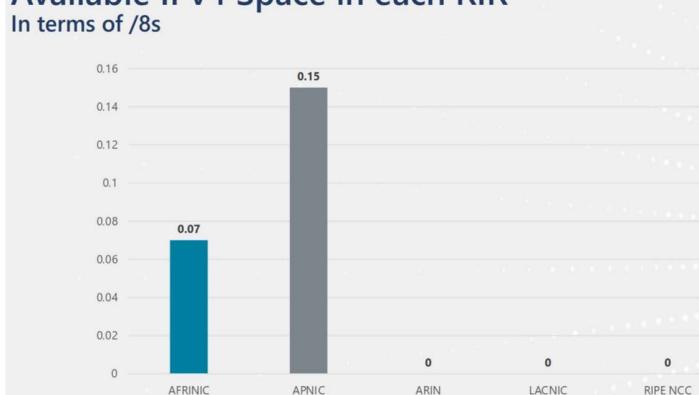
IPv4 address space



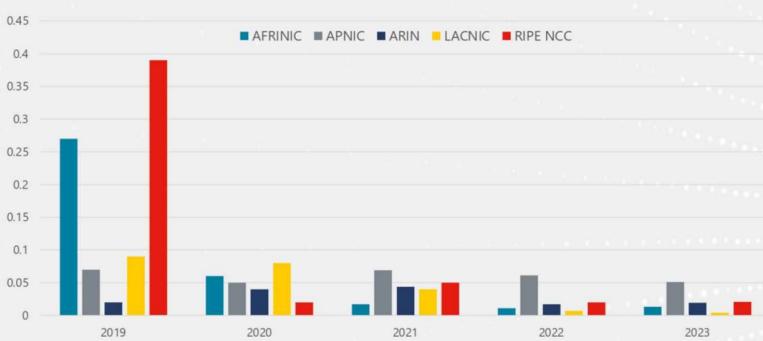
Total IPv4 Addresses Managed by each RIR In terms of /8s



Available IPv4 Space in each RIR In terms of /8s

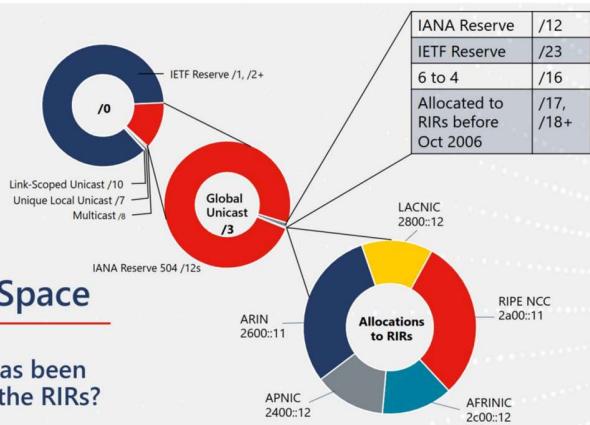


IPv4 Space Issued by RIRs per Year In terms of /8s

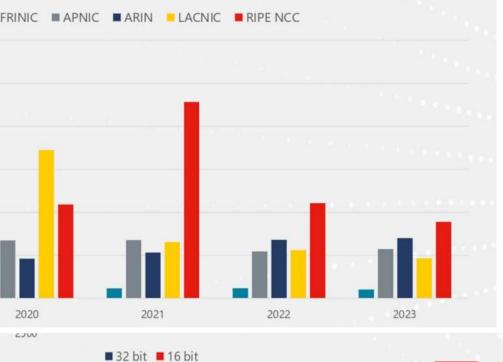


All IPv6 Address Space

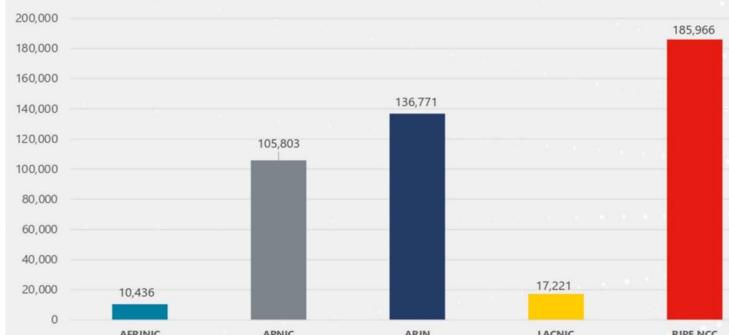
How much has been allocated to the RIRs?



IPv6 Allocations Issued by RIRs Prefixes allocated each year by RIR

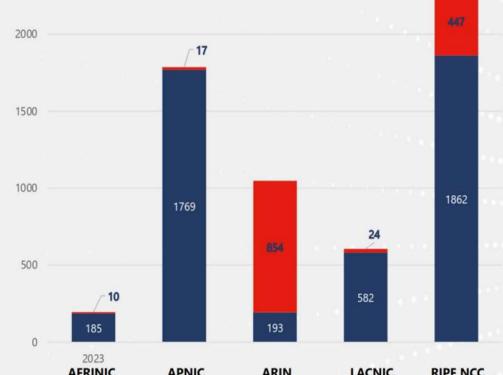


Total Allocated Space IPv6 space (in /32s) each RIR has allocated



ASN Assignments by RIRs

ASNs each RIR issued in 2023

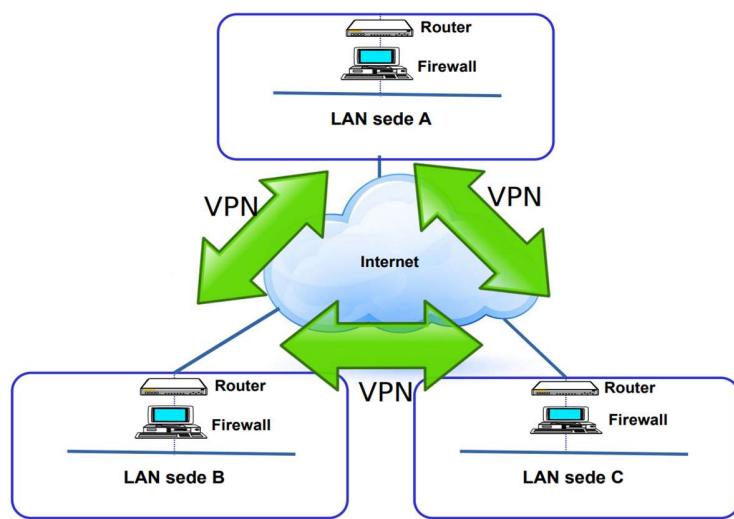


Standards di Internet

Internet esiste a livello tecnico e di sviluppo attraverso la creazione, la verifica e l'**implementazione di Standard Internet**. Questi sono **sviluppati** dall' Internet Engineering Task Force (**IETF**) e sono **esaminati** dall' Internet Engineering Steering Group (**IESG**) e poi **promulgati** dalla Internet Society (**ISOC**) come standard internazionali. L'**RFC Editor** è poi responsabile della **preparazione e organizzazione** dello standard nella forma finale.

Internet Research Task Force (IRTF) ha lo scopo di **promuovere la ricerca** e lo sviluppo di Internet coordinando le attività di diversi Gruppi di Ricerca e lavora sotto il controllo dell'Internet Research Steering Group. Il coordinatore di IRTF fa parte del comitato di gestione di IRSG ed è nominato dall'Internet Activity Board (IAB).

Intranet



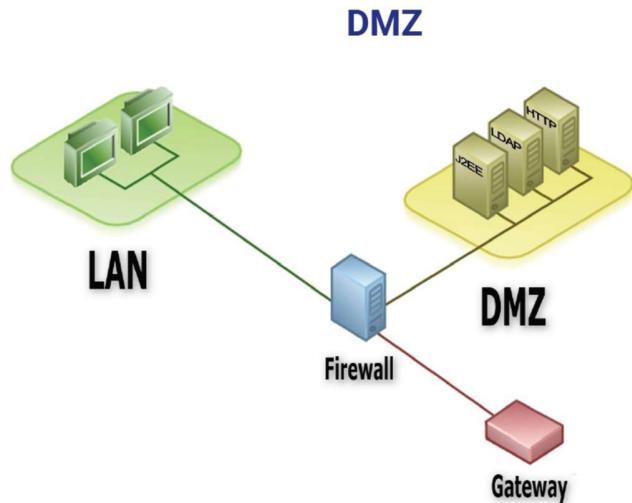
Intranet è il termine che descrive l'**uso delle tecnologie Internet all'interno di una organizzazione**. L'intranet ha come obiettivo quello di trasferire la mole di informazione aziendale ad ogni individuo con costi, tempo e sforzo minimi. I prerequisiti per l'attivazione di una Intranet aziendale sono una **rete locale** che interconnecta i computer e un'informatizzazione diffusa dei vari settori. Grazie all'Intranet le tecnologie telematiche ed i servizi di Internet si diffondono orizzontalmente e verticalmente nella struttura aziendale. L'Intranet ha come periferica un computer e da qui origina la sua straordinaria capacità e potenzialità di trasmettere, integrare, rappresentare qualsiasi tipo di informazione.

Il **router nell'intranet si occupa** di gestire i dati tra i **computer** della rete aziendale e Internet, consentire l'attivazione di una politica di controllo degli accessi alla rete locale, consentire l'accesso controllato e selettivo a computer e servizi. L'intranet è una tecnologia che porta alla ottimizzazione e riduzione dei costi di comunicazione e marketing.

Intranet aziendali

L'Intranet aziendale si riferisce all'utilizzo delle tecnologie Internet all'interno di un'organizzazione anziché per le connessioni esterne con l'Internet globale. Questo implica il **trasferimento efficiente delle informazioni aziendali** a ogni individuo con minimi costi, tempo e sforzo. L'**adozione di un'Intranet** ha un **impatto significativo** sulle operazioni aziendali, migliorando l'efficienza, facilitando la ricerca e lo sviluppo.

Extranet



Con extranet si identificano le risorse hardware e software che realizzano la presenza visibile in Internet di una organizzazione. Queste risorse sono ad esempio data mining, data warehouse, e-commerce e servizi Web. Questi sono servizi che vengono solitamente posti in una speciale area, in cui il controllo del firewall è più lasco: De-Militarized Zone (DMZ). I server in quest'area non sono ritenuti critici e per questo i servizi in genere vengono replicati da server protetti.

3° PARTE

PILA ISO/OSI

Modello concettuale basato su livelli che definisce il modo in cui le reti inviano dati dal mittente al destinatario, viene utilizzato per descrivere ogni componente nell'ambito della comunicazione dei dati, in modo da permettere la definizione di regole e standards, è composto da 7 livelli dal basso verso l'alto:

1. **Physical**: Trasmette i bit -> Ethernet, fiber, wireless
2. **Data Link**: Organizza i bit in frame -> MAC Address
3. **Network**: Gestisce il routing dei pacchetti -> IP address
4. **Transport**: Assicura la consegna affidabile dei dati -> TCP/UDP
5. **Session**: Coordina le sessioni di comunicazione
6. **Presentation**: Gestisce la rappresentazione dei dati
7. **Application**: Fornisce l'interfaccia per le applicazioni di rete

OSI (Open System Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	Process
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	F I L T E R I N G TCP/SPX/UDP	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	Routers IP/IPX/ICMP	Internet Can be used on all layers
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Land Based Layers
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	Hub	Network

È uno strumento teorico per confrontare diverse implementazioni di protocolli di rete, con una scarsa implementazione nel mondo reale infatti viene usato solo per la posta elettronica e per servizi di directory

L'approccio di dividere in livelli, fa in modo che ogni livello sia dedicato ad un insieme specifico di servizi, ogni livello, ad eccezione dei livelli 1 e 7, è collegato al precedente e al successivo, e sfrutta i servizi del livello sotto di lui. Ogni livello è costituito da una o più entità, usano i servizi del livello inferiore e forniscono servizi al livello superiore tramite il loro **SaP(service access point)**. Le operazioni specifiche di un livello sono realizzate mediante un insieme di protocolli

Standard

Gli standard sono specifiche tecniche stabilite per garantire l'interoperabilità, l'efficienza e la sicurezza nei vari settori. Nei contesti tecnologici, gli standard definiscono protocolli, formati e procedure che consentono a dispositivi e sistemi di comunicare tra loro in modo coerente e affidabile.

IEEE 802

è una famiglia di standard di reti locali e metropolitane sviluppati dal **IEEE (Institute of Electrical and Electronics Engineers)**. Questi standard definiscono protocolli per la trasmissione dei dati su reti cablate e wireless. Ecco una panoramica dello standard **IEEE 802**:

è un insieme di standard definiti dall'IEEE per reti **locali (LAN)** e reti **metropolitane (MAN)**. Copre una vasta gamma di tecnologie di rete, tra cui Ethernet, Wi-Fi e Bluetooth. Ogni sottoinsieme della famiglia di standard 802 è identificato da un numero di protocollo univoco

Standard	Name	Topic
802.1	Internetworking	Routing,Bridging, and network-to-network Communications
802.2	Logical Link Control	Error and flow control over data frames
802.3	Ethernet LAN	All forms of Ethernet media and interfaces
802.4	Token BUS LAN	All forms of Token Bus media and interfaces
802.5	Token Ring LAN	All forms of Token Ring media and interfaces
802.6	Metropolitan Area Network	MAN technologies,Addressing, and Services
802.7	Broadband technical Advisory Group	Broadband network media,interfaces, adn other Equipments
802.8	Fiber Optic Technical Advisory Group	Fiber Optic media used in token-passing Networks like FDDI
802.9	Integrated Voice/ Data Network	Integration of voice and data traffic Over a single network medium
802.10	Netwok Security	Network access controls,encryption,Certification, and other Security topics
802.11	Wireless Networks	Standards for wireless networking for many different broadcast frquencies and usage techniques
802.12	High-Speed Networking	A variety of 100 Mbps-plus technologies,including 100 BASE-VG
802.14	Cable Broadband LANs and MANs	Standards for designing network over coaxial cable-based broadband connections.
802.15	Wireless Personal Area Networks	The coexistence of wireless personal area networks with Others wireless devices in unlicensed frequency bands.
802.16	Broadband Wireless Access	The atmospheric interface and related functions associated with Wireless Local Loop(WLL)

Lo standard IEEE 802 può essere collegato a diversi strati del modello OSI, a seconda del tipo di tecnologia di rete specifica che definisce.

1. IEEE 802.3 (Ethernet):

- Strato fisico (Physical Layer)
- Strato di collegamento dati (Data Link Layer)

2. IEEE 802.11 (Wi-Fi):

- Strato fisico (Physical Layer)
- Strato di collegamento dati (Data Link Layer)

3. IEEE 802.1Q (VLAN):

- Strato di collegamento dati (Data Link Layer)

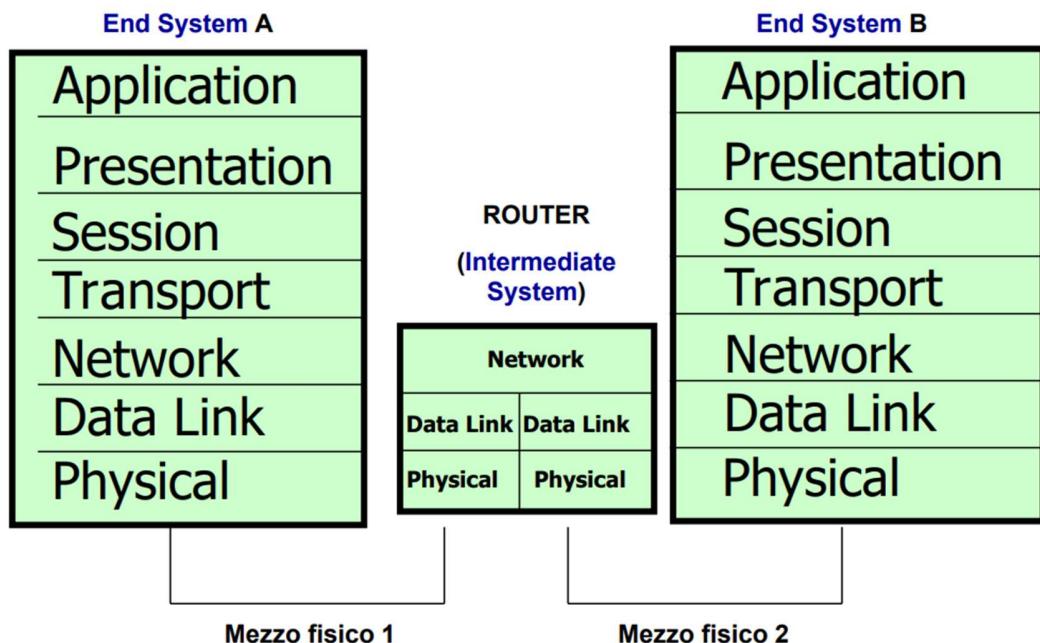
4. IEEE 802.15 (Bluetooth):

- Strato fisico (Physical Layer)
- Strato di collegamento dati (Data Link Layer)

Ogni standard all'interno della famiglia IEEE 802 ha il proprio insieme di specifiche e requisiti, ma tutti sono progettati per garantire l'interoperabilità e le prestazioni ottimali nei rispettivi ambiti di applicazione.

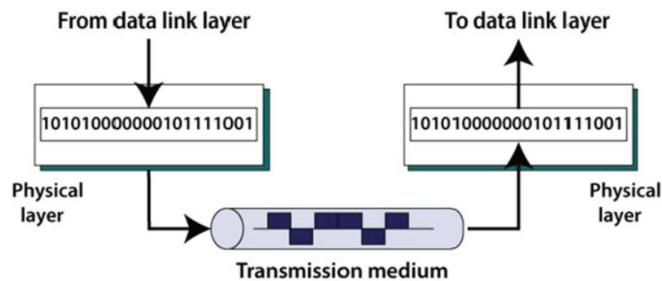
intermediate system (IS)

Il termine **Intermediate System (IS)** è un termine OSI che indica un nodo (tipicamente un router) che ha capacità di instradare messaggi a livello 3 verso altri nodi. Il termine **End System (ES)** è un termine OSI che indica un nodo che può agire solamente come sorgente o destinazione finale di dati dell'utente e che non effettua le funzioni di routing.



4° PARTE

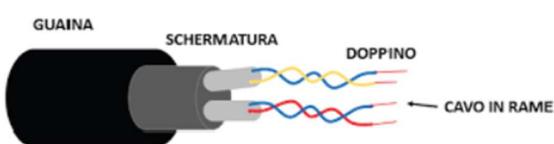
Physical Layer



Il **physical layer** è collocato al livello più basso, il livello fisico, ed è un **insieme di regole** che specificano le **connessioni elettriche e fisiche tra i dispositivi fisici**. Questo livello specifica le connessioni dei cavi e il tipo di segnale elettrico associato ai vari pin di connessione delle interfacce utilizzate per trasferire dati tra i diversi dispositivi di rete. Il **physical link corrisponde agli standard di interfaccia dei vari dispositivi**. Le regole del Physical Layer definiscono la trasmissione dati per i terminali, i modem, le schede di rete, etc.

Mezzi Trasmissivi

Doppino



Un **doppino ritorto** è un tipo di linea di trasmissione composto da una **coppia di conduttori in rame isolati**.

È un elemento essenziale nella telefonia ed ethernet.

Esistono **diversi tipi di doppino** a seconda della schermatura:

	Unshielded	Shielded
Unscreened	UTP 	STP
Screened	S/UTP - FTP - S/FTP 	S/STP



Doppino - UTP

L'Unshielded Twisted-Pair (**UTP**) è il mezzo **più economico e facile da installare** per il cablaggio strutturato degli edifici. Utilizza il connettore RJ45 per la connessione delle stazioni. Si tratta dell'**evoluzione del singolo doppino in rame**, dove più doppini vengono torti in maniera precisa per ridurre le interferenze elettromagnetiche, affiancati in una guaina. Tuttavia, è fortemente **soggetto a disturbi** da macchine elettriche e luci fluorescenti, in quanto agisce da antenna e più lungo è il segmento, maggiore è il disturbo. Per **ridurre i disturbi** si potrebbe utilizzare lo Shielded Twisted-Pair (**STP**), ma questo è considerato **tropo costoso** e difficile da stendere. I cavi **UTP** sono disponibili in **diverse categorie**, dove una categoria più alta indica un cavo più rigido e affidabile. I cavi UTP non sono schermati, ma per la certificazione di un

impianto è richiesto l'uso di cavi di Cat. 5/5e. Tuttavia, per supportare Gigabit Ethernet, sono necessari cavi di qualità superiore, schermati.

Cat 5	Velocità fino a 100Mbps (FastEthernet) larghezza di banda 100MHz	4/8
Cat 5e	Velocità fino a 1Gbps, larghezza di banda 100MHz	8
Cat 6/6A	Velocità fino a 10Gbps, larghezza di banda 250-500MHz	8
Cat 7/7A	Velocità fino a 10Gbps, larghezza di banda 600-1000MHz	8
Cat 8/Supra Cat 8	Velocità fino a 40Gbps, larghezza di banda fino a 1600-2000MHz	8

Cavo Coassiale

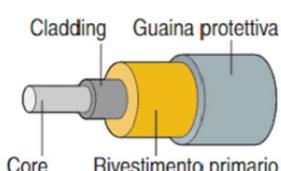
Il **cavo coassiale** è un cavo elettrico **utilizzato per trasmettere segnali informativi**. Viene prodotto in **diversi tipi** in base alla frequenza e alla potenza del segnale da trasportare, con due valori principali di impedenza: 50 ohm e 75 ohm. Il cavo coassiale è **originariamente utilizzato nelle reti Ethernet e ArcNet**.

È composto da un filo di **rame centrale**, ricoperto da un dielettrico, una calza in rame e una guaina in polietilene. Esistono due versioni di cavo coassiale per Ethernet, entrambe con impedenza di 50 ohm: il cavo thick (RG-8) e il cavo thin (RG-58). Nel caso del thick ethernet, si utilizza un transceiver collegato con un cavo a 9 fili ad un connettore AUI a 15 pin. Per il thin ethernet, si impiega un connettore a T con innesto a baionetta.

Fibre ottiche

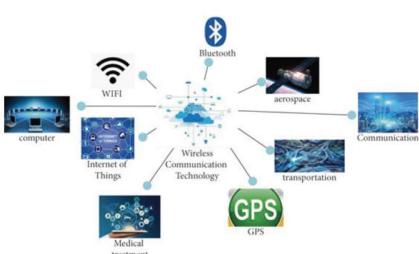


Le **fibre ottiche** sono filamenti flessibili e trasparenti realizzati tramite la trafilatura di vetro (silice) o plastica, con un diametro leggermente superiore a quello di un cappello umano. Sono principalmente utilizzate per **trasmettere la luce tra le estremità della fibra** e sono ampiamente impiegate nelle comunicazioni. Le fibre ottiche **consentono trasmissioni su distanze più lunghe** e con **larghezze di banda più elevate** rispetto ai cavi elettrici. Tuttavia, presentano alcuni **svantaggi**, come una **terminazione del cavo complessa** e la necessità di interventi altrettanto complessi in caso di interruzioni del cavo.



Un **cavo in fibra ottica** è composto da un nucleo centrale (**Core e Cladding**) attraverso il quale viaggiano i segnali ottici, circondato da un mantello (**Rivestimento primario**) che aiuta a mantenere la luce all'interno del nucleo grazie alla riflessione totale interna. Il tutto è protetto da un rivestimento esterno (**Guaina protettiva**) che fornisce protezione meccanica e ambientale. Il **funzionamento** si basa sulla **riflessione totale interna**, dove la luce rimbalza all'interno del nucleo grazie alla differenza di indice di rifrazione. Quando il **segnale raggiunge l'estremità della fibra**, può essere decodificato e trasmesso in informazioni utilizzabili attraverso dispositivi ottici come trasmettitori e ricevitori ottici.

Connessioni Wireless

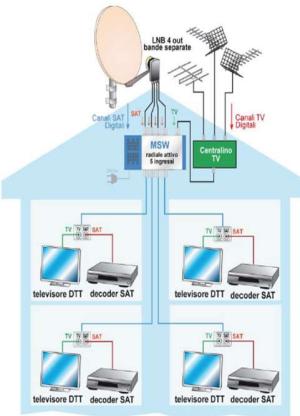


La **comunicazione wireless** implica trasmettere informazioni senza l'uso di fili o cavi. Questo metodo abbraccia **tutte le forme di connessione tra dispositivi che si avvalgono di segnali wireless**. Grazie alla mancanza di infrastruttura fisica, la comunicazione wireless offre **diversi vantaggi**:

- **Efficienza dei costi:** Elimina la necessità di costose infrastrutture fisiche e di pratiche di manutenzione, riducendo i costi.

- **Flessibilità:** Consente la comunicazione indipendentemente dalla posizione degli utenti.
- **Convenienza:** I dispositivi wireless, come i telefoni cellulari, sono facili da utilizzare e non richiedono collegamenti fisici per trasmettere o ricevere messaggi.
- **Velocità:** Migliora la connettività di rete e l'accesso ai dati in termini di velocità e precisione.
- **Accessibilità:** Le aree remote possono essere facilmente collegate alla rete grazie alla tecnologia wireless, senza la necessità di posare linee terrestri.
- **Connettività costante:** Offre una connettività continua e affidabile, indipendentemente dalle condizioni fisiche del terreno.

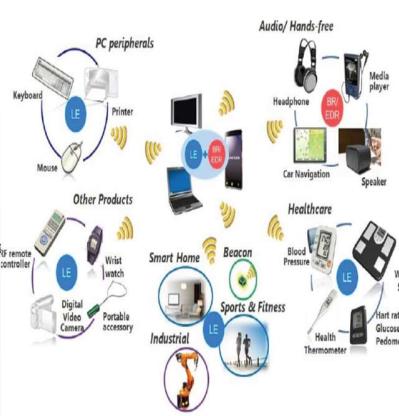
Tv analogica e Digitale



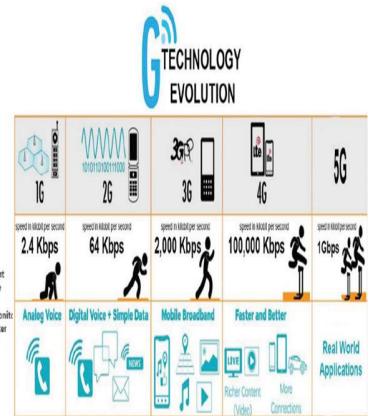
Reti domestiche WIFI



Bluetooth



Telefonia Mobile



5° PARTE

Data Link Layer

-Il secondo livello del modello OSI (Open System Interconnection) descrive come un dispositivo guadagna l'accesso al mezzo specificato nel physical layer e come realizza la comunicazione con un nodo adiacente

-Servizi del Data link layer:

1. Trasmissione affidabile del frame
2. Controllo del flusso
3. Rilevamento e correzione degli errori
4. Modalità half-duplex e full-duplex: la modalità "half duplex" permette la trasmissione o la ricezione di dati in momenti separati, mentre la modalità "full duplex" consente la trasmissione e la ricezione simultanea dei dati su canali separati.

-Fanno parte di questo livello le schede di rete (NIC), gli hub, i bridge e i dispositivi di switching che operano una divisione del dominio di collisione Ethernet

-Per problemi realizzativi, i primi due livelli di OSI vengono suddivisi dallo standard IEEE 802.3 in:

- Livello fisico: specifica caratteristiche elettriche e modalità di segnali per ogni standard utilizzato
- LLC (logical link control): livello di gestione logica del link.

-Realizza funzioni di gestione del link mediante un protocollo trasmissivo sostanzialmente comune alle diverse varianti a livello fisico.

-Per questo livello è stato sviluppato un unico standard: riceve dati dal livello superiore e li invia passandoli al MAC sotto forma di una o più trame.

-LLC prevede 3 varianti:

1. LLC1 servizio senza connessione e senza conferma:
-Permette l'invio di frame su base libera e non prevede nessuna conferma dei dati trasmessi e ricevuti
2. LLC2 servizio basato su una connessione logica:
-Richiede che prima della trasmissione venga stabilita una connessione logica tra i punti di accesso al servizio dell'utente chiamato e chiamante
3. LLC3 servizio senza connessione con conferma:
-Non richiede connessione logica e trasmette le singole trame richiedendo la conferma di ricezione prima di inviare la prossima trama.

-Esempio di trama Ethernet:

1. **PRE (preamble)**: sequenza binaria che permette la sincronizzazione della trasmissione
2. **SFD (Starting Frame Delimiter)**: sequenza binaria 10101011(in esa AB) da lì in poi inizia il frame vero e proprio
3. **DA (Destination Adress)**: indirizzo di destinazione MAC address composto da 6 byte (aa:bb:cc:dd: ff sempre esa) se il primo bit è 0 la destinazione è soltanto una altrimenti è più di una
4. **SA (Source Adress)**: struttura simile al Destination address il primo bit è sempre zero dato che l'invio è sempre da un singolo

5. **L/T(lenght/type)**: lunghezza e tipo del frame
 6. **Payload(dati)**: i dati veri e propri da 46 byte a 1500 byte, se sono meno di 46 dobbiamo mettere dei byte di riempimento, per motivi di controllo dell'errore
 7. **PAD**: campo di riempimento utilizzato per garantire la lunghezza minima di 64 byte
 8. **FCS (Frame Check Sequence)**: calcolato su tutto il frame usando un algoritmo chiamato **CRC (cyclic redundancy control)**, il ricevente farà lo stesso e lo confronterà con quello di questo campo
- MAC (media access control): gestione dell'accesso al mezzo trasmissivo. Funge da interfaccia tra livello fisico e LLC

-IEEE: L'Institute of Electrical and Electronic Engineers è molto attivo nello sviluppo di standard di comunicazione dati, il sottocomitato 802 ha iniziato prima che fosse stabilito un valido mercato per le reti locali, segnando comunque un avanzamento teorico fondamentale.

→L'802 si concentra sull'interfaccia fisica degli apparati e sulle procedure richieste per stabilire mantenere e terminare connessione tra dispositivi di rete:

- Definizione e formato dei dati
- Controllo dell'errore
- Attività per il controllo del flusso dell'informazione

IEEE 802.3 Connattività fisica:

→I primi standard ethernet ad essere stati definiti supportavano una velocità di trasmissione dati a 10mbps, al giorno d'oggi esistono molte varianti di 802.3:

- **3 - 10BASE5**: Cavo coassiale a filo spesso con una lunghezza massima di cablaggio di 500 metri. Si basa sul processo CSMA/CD.
- **3a - 10BASE2**: cavo coassiale a filo sottile che utilizza connettori Bayonet Neill-Concelman (BNC), con una lunghezza massima di cablaggio di 185 metri.
- **3i - 10BASE-F**: cavi Ethernet in fibra ottica.
- **3i - 10BASE-T**: Normale cavo telefonico a doppini intrecciati che utilizza cavi a doppini intrecciati non schermati (UTP) come strato fisico e cavi in fibra ottica come mezzo di trasmissione. Altre varianti includono IEEE 802.3u e 100BASE-TX.

- **3b - 10BROAD36:** Cavo coassiale multicanale a banda larga con una lunghezza massima del segmento di 3.600 metri.
- **3bt:** Power over Ethernet (POE) di terza generazione che utilizza quattro coppie di cavi twisted-pair per supportare le applicazioni IoT.
- **3x - Full-Duplex:** Fornisce il controllo di flusso e include il framing DIX.
- **10baseFOIRL:** Alternativamente al cavo Thick ethernet è possibile utilizzare fibra ottica ed un transceiver Fiber Optic MAU (**FOMAU**).
Il **FOMAU** è in grado di ricevere e trasmettere segnali ottici lungo un segmento di fibra ottica di lunghezza massima pari a 1000m
- **10baseF:** È la modalità che definisce l'uso di IEEE802.3 utilizzando come mezzo trasmissivo la fibra ottica.
Si suddivide in tre sotto-standard: **10baseFP**, **10baseFB**, **10baseFL**.

*Il 10 nella designazione del tipo indica la velocità di trasmissione (10 Mbps)

*BASE si riferisce alla segnalazione in banda base

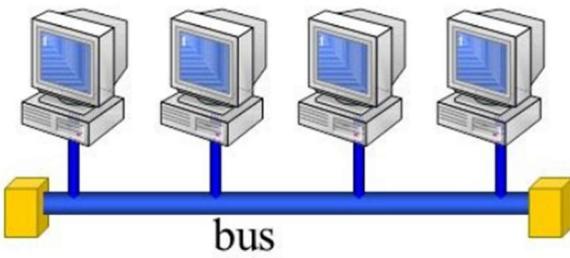
*La "T" rappresenta il doppino la "F" rappresenta il cavo in fibra

6° PARTE

Topologia delle reti

La disposizione degli elementi di una rete di comunicazione come nodi e collegamenti è detta **Topologia di rete**, può essere rappresentata fisicamente o in modo logico, la collocazione dei componenti della rete come la posizione dei dispositivi e l'installazione dei cavi, fa parte della topologia fisica, mentre la topologia logica descrive il flusso dei dati all'interno della rete.

Topologia a BUS



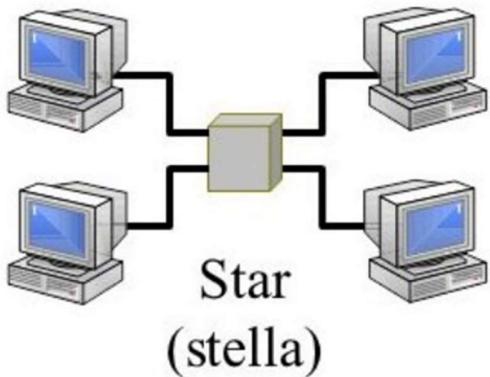
- un cavo fa da percorso principale, dove vengono connesse tutte le stazioni
- tutti i dati che vengono trasmessi vengono resi disponibili a tutte le stazioni

Contro:

- solo la stazione destinataria legge il messaggio
- il cavo deve essere terminato da entrambi i lati

- se il cavo viene interrotto l'intera rete va giù

Topologia a Stella

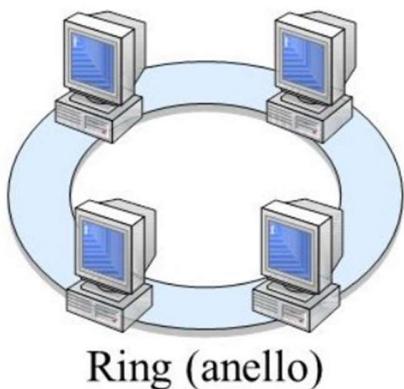


- ogni stazione è connessa ad un hub, quest'ultimo gestisce la comunicazione con ciascun nodo indipendentemente dagli altri nodi
- le ethernet recenti hanno una tipologia fisica a stella, ma logicamente si comportano come la topologia a BUS
- i guasti ad i cavi non mandano giù tutta la rete

Contro:

- cavi difettosi causano l'invio di pacchetti di lunghezza errata

Topologia ad anello



- un cavo che connette tutte le stazioni, logicamente simile ad un anello
- considerabile come una topologia a BUS chiusa
- il metodo di accesso ai dati richiede che i dati circolino ad anello, le reti moderne sono fisicamente a **stella** e logicamente ad **anello** (Token ring, FDDI)

Topologia ad Albero



albero

- ogni nodo fornisce accesso alla stazione a cui è collegato oppure instrada i dati verso un nodo a cui è a sua volta collegato
- comunicazione inefficiente tra nodi lontani

Tipi di rete

WAN (Wide Area Network)

Interconnette due o più reti disperse geograficamente, tramite fibra ottica(dedicata) viene usata per collegamenti Nazionali o Internazionali, connette host collegati a sottoreti, le WAN sono costituite da:

- Collegamenti (linee, circuiti, canali e dorsali)
- Elementi di commutazione (router)

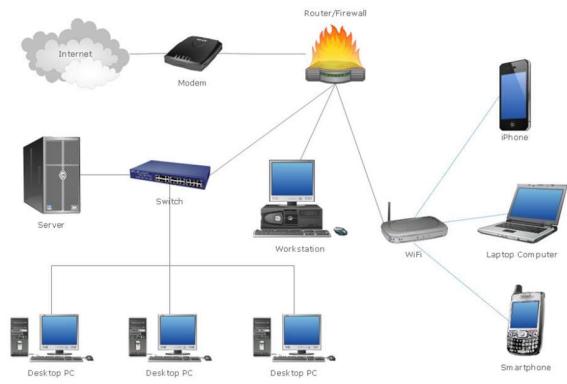
Inoltre, ci dà la possibilità di avere:

- Gestione del Routing complessa
- Possibilità di interconnettere reti eterogenee
- Uso di router multiprotocollo e adozione nella WAN della stessa politica di Routing

MAN (Metropolitan Area Network)

Un'area con esigenze ad alte prestazioni, sono reti dette a Banda larga (nome dato dai protocolli delle prime implementazioni), dall'esterno viene vista come un'unica entità, il gestore della rete ne regola l'accesso e ne definisce le politiche di Routing, collegano più reti LAN geograficamente vicine

LAN (Local Area Network)



Sono reti private come quella che abbiamo in casa, come quella di una scuola o università sono collegate tramite LAN, è regolata da politiche proprie di accesso e Routing, consente la condivisione di risorse hardware e software

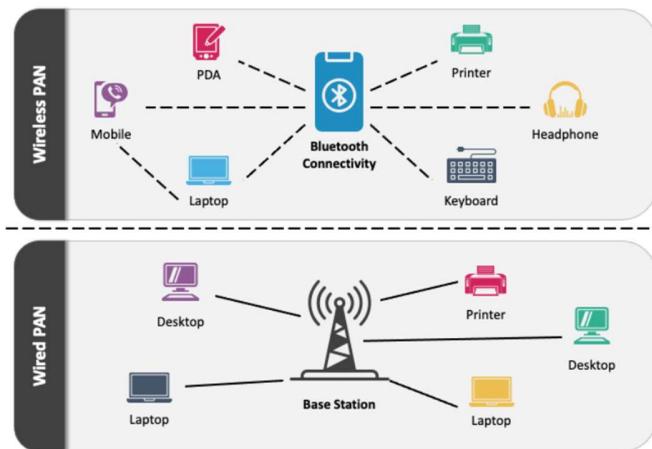
Banda base e Banda larga

Nelle LAN a livello fisico ci sono due tecniche trasmissive che vengono adottate per lo scambio dei dati, la **banda base** (la più comune) e la **banda larga** (o banda traslata)

La **Bandia base** è una tecnica trasmissiva dove il livello fisico del nodo LAN utilizza tutta la banda, dato che può trasmettere a velocità pari alla capacità di quest'ultima, viene usata nello standard 802.3 e nello standard Ethernet; tuttavia, non avviene la modulazione del segnale elettrico questo comporta distanze limitate ma semplifica l'hardware di interfaccia

La **Bandia Larga** invece modula la frequenza del segnale e divide in sotto canali indipendenti la banda disponibile, ciascun nodo di una rete può trasmettere su una o più sotto bande

PAN (Personal Area Network)



Rete utilizzate per far comunicare dispositivi molto vicini tra loro, ha un raggio di azione di pochi metri

- Bluetooth
- Passaggio di dati tramite USB o FireWire

Metodi di accesso LAN

Per far trasmettere due pc alla volta in rete ci sono 2 metodi di accesso

- **Deterministico:** ogni computer aspetta il suo turno
- **Non Deterministico:** ogni stazione trasmettere in qualunque momento

Token Passing: metodo deterministico usato nelle reti **token-ring, ARCNet e FFDI**

un anello dove circolano frame vuoti di informazione, quando un host deve inviare un messaggio prende un **token** e occupa uno dei frame vuoti, che poi viene esaminato da ogni nodo successivo fino a quando non arriva al nodo destinatario, che metterà **il bit di ricezione a 0** così quando il frame passerà di nuovo al mittente quest'ultimo avrà la conferma della ricezione

Carrier Sense Multiple Access CSMA/CD: con Collision Detection metodo di accesso random utilizzato nelle reti Ethernet, il nodo ascolta se il mezzo trasmisivo è libero prima di iniziare a trasmettere, se un nodo deve trasmettere un pacchetto dopo un tempo **T<t(tempo di propagazione del segnale)** vedrà il percorso libero e trasmettendo il proprio pacchetto si genererà una collisione, ed entrambi i pacchetti vengono cancellati, nel modello **CD(Collision detection)** le collisioni sono rilevate e vengono ritardate tramite l'algoritmo di **backoff** (usa il MAC address come dato univoco), l'unico modo per risolvere questo problema definitivamente è usare uno **switch**

7° PARTE

Ethernet

L'interfaccia **Ethernet** (Schede di rete) svolge le seguenti funzioni:

- Codifica e decodifica dei dati
- Link management
- Codifica e decodifica Manchester dei bit

è posta a metà del primo livello **ISO/OSI** ed il secondo, nello specifico nel sottolivello **MAC**

Identifica una rete locale operante con metodo di accesso **CSMA/CD** su un bus logico costituito da Hub e Switch (in origine era un cavo coassiale), lo standard **Ethernet e 802.3** posso interoperate tra di loro in quanto a livello fisico non ci sono differenze, ma a livello logico la trama del frame è diversa ed in questo caso è il livello applicativo che deve assicurare la lunghezza minima di 46 byte, ed il campo di tipo indica il protocollo di trasporto utilizzato dai livelli superiori

lo standard ethernet

Lo standard Ethernet ha subito evoluzioni significative nel corso del tempo. Originariamente, operava su un bus costituito da cavo coassiale e utilizzava il metodo di accesso **CSMA/CD**. Tuttavia, nelle moderne reti Ethernet, il bus è implementato logicamente dagli apparati attivi di rete come hub e switch. Nonostante queste differenze di

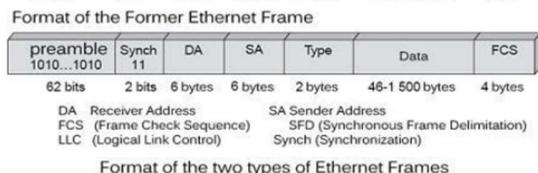
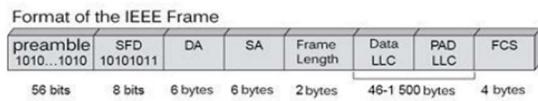
implementazione, gli apparati conformi agli standard possono comunque interoperare poiché non presentano differenze a livello fisico.

Le principali differenze tra lo standard Ethernet originale e le moderne implementazioni includono:

-**Formato della trama:** Le moderne reti Ethernet utilizzano un formato di trama diverso rispetto allo standard originale.

-**Lunghezza minima del messaggio:** Nel caso dello standard Ethernet originale, il livello applicativo deve assicurare una lunghezza minima di 46 byte per il messaggio.

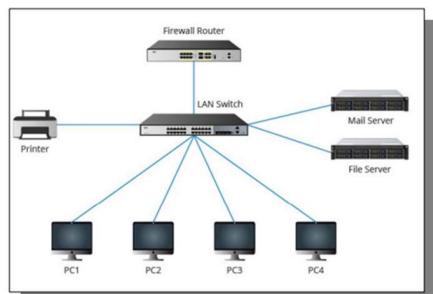
-**Campo tipo:** Una differenza fondamentale è rappresentata dal campo tipo, che indica il tipo di protocollo di trasporto utilizzato dai livelli superiori. Questo campo può variare tra le implementazioni e gli standard Ethernet.



Format of the two types of Ethernet Frames

switched lan

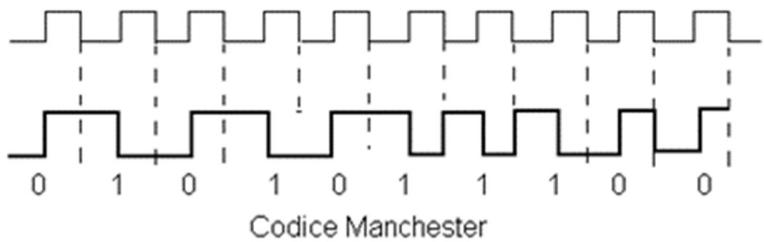
Le **switched lan** rappresentano una soluzione ottimale per migliorare le prestazioni di una rete Ethernet, poiché suddividono il dominio di collisione della rete stessa. Si basano sull'uso di apparati chiamati switch, i quali operano una selezione accurata dei dati trasmessi dagli host. Ogni switch mantiene un buffer locale degli indirizzi MAC degli host collegati alle sue porte, consentendo la trasmissione diretta dei pacchetti solo alla porta destinata all'host di destinazione. Questo rende il funzionamento degli switch trasparente per gli utenti.



La migrazione a una rete commutata risolve definitivamente i principali problemi del metodo di accesso **CSMA/CD**, minimizzando le collisioni. Questa tecnologia è caratterizzata da bassi costi implementativi e offre all'utente la possibilità di utilizzare tecnologie miste, garantendo una manutenzione semplificata e una grande flessibilità. Inoltre, la transizione a una rete commutata comporta semplicemente la sostituzione degli apparati attivi, mantenendo invariato il cablaggio esistente, se di tipo 10baseT.

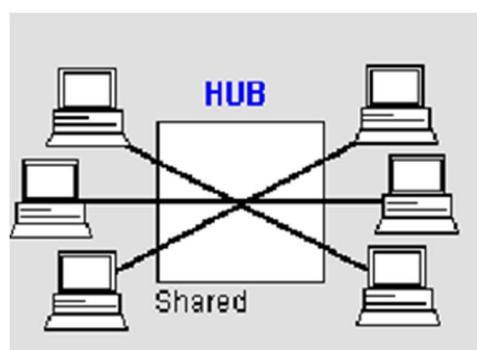
Codifica Manchester

Serve per sincronizzare i dati tra il mittente ed il destinatario, garantendo una transizione del segnale elettrico in ogni bit trasmesso, questo permette ad appositi circuiti di agganciare in fase il loro clock a quello del trasmettitore, durante la ricezione del preambolo, e quindi fa in modo che il pacchetto(frame) venga ricevuto con la giusta temporizzazione



HUB

Un **hub di rete** è un dispositivo passivo che funge da punto di connessione centrale per diversi dispositivi su una rete locale. Riceve segnali da un dispositivo e li ritrasmette a tutti gli altri dispositivi collegati, senza effettuare alcuna elaborazione sui dati. Si comporta in modo simile ad i **BUS**, quindi, c'è rischio di collisioni, i primi switch costavano molto quindi era comune avere uno switch e degli Hub, oppure solo un hub



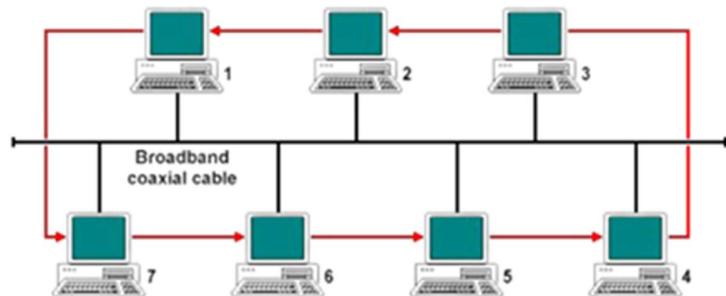
8° PARTE

IEEE 802.4 Token bus

-Obiettivo: formare una rete a bus con modalità trasmissiva broadband

-Basato sul Manufacturing Automation Protocol (MAP): protocollo di comunicazione sviluppato per facilitare lo scambio di dati tra dispositivi di automazione industriale

-Non ebbe molto successo a causa dei costi implementativi

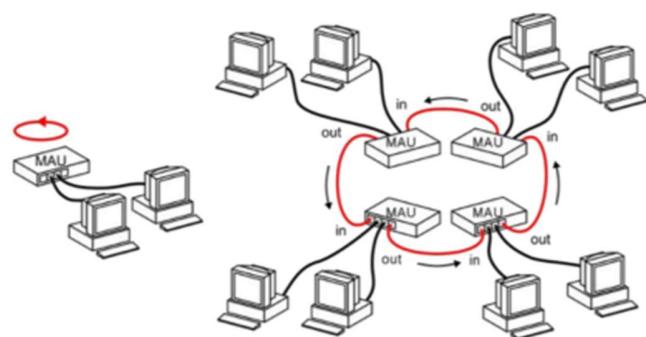


IEEE 802.5 Token Ring

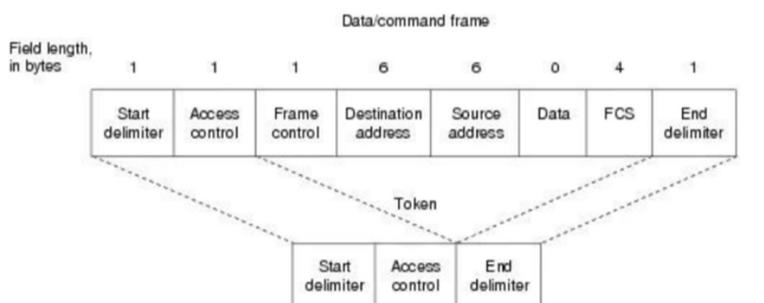
-Describe una modalità trasmissiva a token, in cui la connessione delle stazioni avviene con dei collegamenti punto-punto tra le stazioni formando un anello chiuso

→Presso ogni nodo viene rigenerato il segnale elettrico ed esaminato il contenuto della trama

→Per evitare che un nodo guasto blocchi l'intera connessione, l'interconnessione tra le stazioni avviene mediante un Medium Access Unit (MAU)



-Trama:



- **Delimitatore di inizio** (1 byte): ha la stessa funzione di base del preambolo in un frame Ethernet.
- **Controllo di accesso** (1 byte): contiene il bit di token, il bit di monitoraggio e i bit di priorità.
- **Frame Control** (1 byte): contiene informazioni sul controllo di accesso.
- **Indirizzo di destinazione** (6 byte)
- **Indirizzo sorgente** (6 byte)
- **Dati** (nessun limite di dimensione specificato): sono i dati effettivamente inviati. Dato che il THT = 10 msecondi, il limite pratico di dimensione del frame è di 4500 byte.
- **Sequenza di controllo del frame** (4 byte): bit di controllo degli errori CRC
- **Delimitatore di fine** (1 byte): indica la fine del frame.
- **Frame Status Field** (1 byte): serve come ACK e indica se l'indirizzo è stato riconosciuto e il frame copiato dal computer ricevente prima di essere rimandato indietro sull'anello.

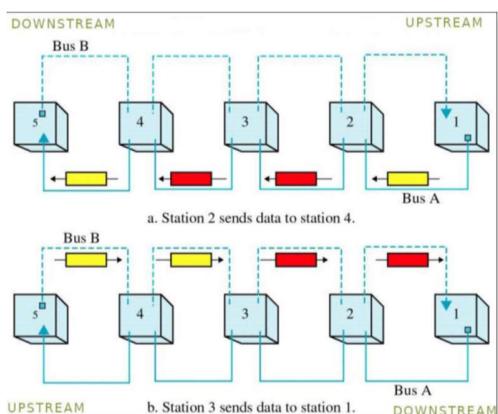
IEEE 802.6 MAN

-Nasce dall'esigenza di estendere i servizi della local Area Network in un'estensione metropolitana
 →Dopo vari tipi di interconnessioni, il Distributed Queue Dual Bus (DQDS) è divenuto lo standard dell'IEEE 802.6
 →La MAN di base è costituita da 512 nodi, 160 km, 150 Mbps dual bus network, ma ciascuno di questi parametri può essere considerevolmente esteso
 →Questo standard può essere utilizzato come rete privata o pubblica, le compagnie telefoniche hanno partecipato attivamente allo sviluppo di questo standard

-Metodo di accesso alla rete attraverso il protocollo DQDS:

→Il metodo di accesso alla rete mediante DQDB coinvolge due bus separati, noti come bus primario e bus secondario. Gli utenti accedono alla rete inserendo i propri dati in un'apposita coda (queue). Quando è il turno di un utente di trasmettere, il protocollo DQDB assegna un intervallo di tempo durante il quale l'utente può trasmettere i propri dati sul bus primario.

Il protocollo DQDB implementa anche un meccanismo di priorità per garantire che i pacchetti più urgenti vengano trasmessi prima. Inoltre, il protocollo gestisce automaticamente i conflitti e le collisioni che possono verificarsi durante la trasmissione dei dati.



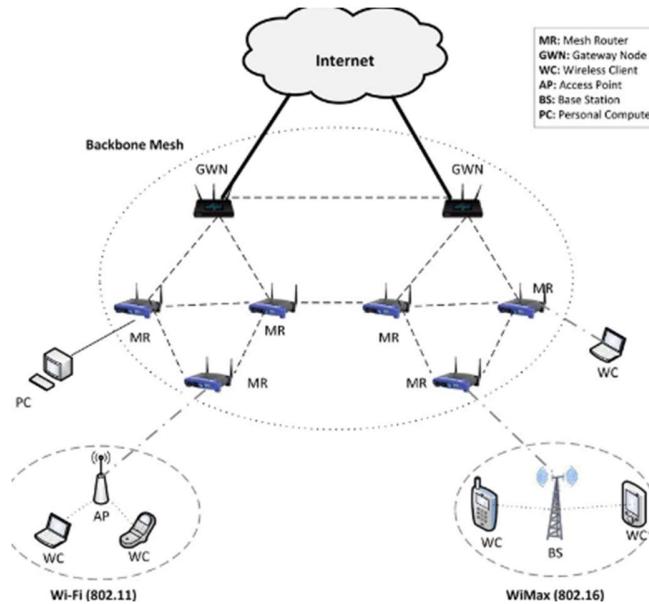
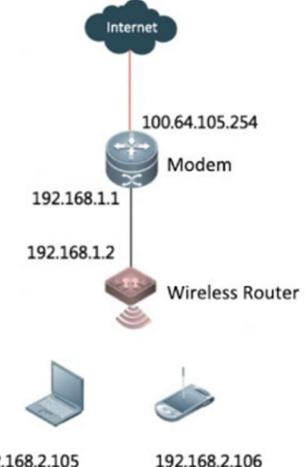
9° PARTE

Reti wireless

Il forte **sviluppo delle reti Wireless** negli ultimi anni è dovuto agli enormi vantaggi che porta:

- non sono necessari lavori di cablaggio e ciò preserva gli edifici storici
- gli utenti possono muoversi e accedere ai servizi di rete ovunque
- si possono creare reti temporanee
- è possibile il roaming, spostarsi fisicamente rimanendo connessi alla rete
- scalabilità: adattarsi dinamicamente senza causare problematiche avvertibili, condizionare gli altri servizi o interromperli
- gestire numero di utenze variabili
- fungere da estensione di LAN cablate
- implementare la sicurezza a livelli molto elevati (certificati X.509)
- la maggioranza dei dispositivi mobili è in grado di connettersi wireless

Home broadband architecture



Reti wireless: dispositivi

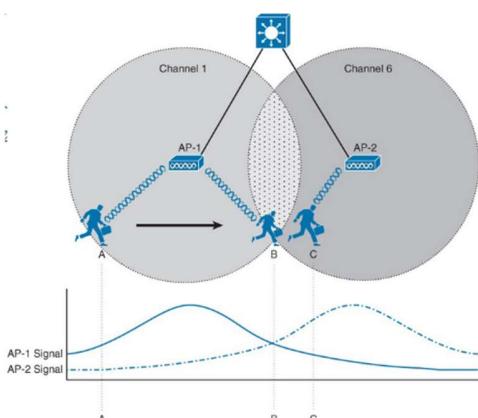
Access Point (AP)

- sono antenne che comunicano con i client e tra di loro. La base delle reti wireless
- Gli AP sono collegati a uno switch mediante un cavo UTP per ottimizzare le prestazioni
- A seconda delle caratteristiche dell'AP e dell'ambiente la potenza va dai 20m ai 300m
- Il posizionamento degli AP è strategico per ricoprire al meglio la zona wireless LAN. La sovrapposizione con l'AP adiacente deve essere del 10-15%
- Con lo spostamento del client la connessione viene mantenuta passando da un AP all'altro

Network Interface Card (NIC)

- un client della rete wireless deve possedere un dispositivo in grado di trasmettere e ricevere segnali con l'AP
- i NIC possono essere schede PCMCIA, PCI-E o dispositivi usb

Sovrapposizione di due celle e roaming



Se l'AP-1 ha ancora dei frame wireless destinati al client dopo il roaming (spostamento del client che entra nella cella di un diverso AP), li inoltra all'AP-2 attraverso l'infrastruttura cablata, semplicemente perché è lì che risiede l'indirizzo MAC del client

Lo standard IEEE 802.11

Il gruppo di lavoro dell'IEEE 802.11 si occupa della standardizzazione di sottolivello MAC e fisico delle reti wireless.

Tre componenti fondamentali che lavorano insieme per gestire la comunicazione wireless sono

- **LLC** (Logical Link Control)
- **MAC** (Media Access Control)
- **PHY** (Physical Layer)

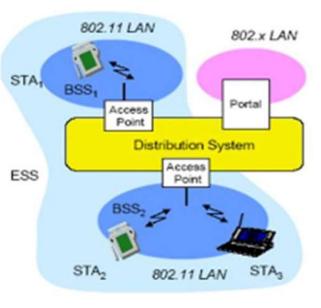
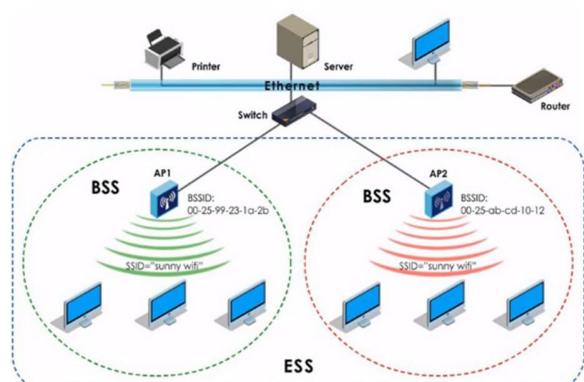
Un unico MAC supporta diverse varianti o tecnologie di livello fisico (PHY). Il MAC fornisce un'interfaccia comune per l'accesso al mezzo trasmittivo, consentendo ai dispositivi di comunicare tra loro indipendentemente dalla tecnologia PHY utilizzata

L'entità fondamentale di una rete wireless è chiamata **Basic Service Set**

(BSS). E' costituito da una o più stazioni wireless (pc, smartphone) e dall'AP a cui le stazioni sono associate, le stazioni si trovano geograficamente all'interno della cella dell'AP.

Un BSS può operare in due modi:

- BSS indipendente (**Independent BSS**): In questa modalità, le stazioni comunicano direttamente tra loro senza l'uso di un access point centrale
- BSS infrastrutturato (**Infrastructure Network BSS**): In questa modalità, le stazioni comunicano tramite un access point (AP). L'AP può fungere da ponte tra le stazioni wireless e la rete cablata (modalità più comune nelle reti Wi-Fi domestiche e aziendali)



Normalmente una WLAN è costituita da più celle.
L'infrastruttura di interconnessione tra i diversi BSS
è denominata **Distribution System** (DS)

Il wireless MAC supporta sia servizi connectionless da 1 a 54Mbps, sia servizi di tipo sincrono (per controllo di voce, video)

Le interfacce fisiche possono essere a infrarossi o a radiofrequenze (frequenze 2,4 GHz – 5 GHz – 18 GHz).

Il metodo di accesso è il CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) [le collisioni vengono evitate invece che rilevate(IEEE 802.3)]

WLAN a infrarossi

La luce infrarossa non può passare attraverso le pareti, una cella della WLAN a infrarossi quindi è limitata a una singola stanza dell'edificio. Esistono due tipi di WLAN IR: a infrarossi **diffusi** e a infrarossi **diretti**.

Queste WLAN lavorano su lunghezze d'onda di 800 - 900 nm. Gli IR diretti hanno una velocità di trasmissione più alta e un raggio di copertura più basso (1-10 Mbps, 25m) rispetto agli IR diffusi (1-4 Mbps, 60m). Gli IR diffusi supportano client sia stazionari che mobili e come metodo di accesso usano il CSMA.

Gli IR diretti non permettono la connessione a client mobili e come metodo d'accesso usano il Token ring e il CSMA.

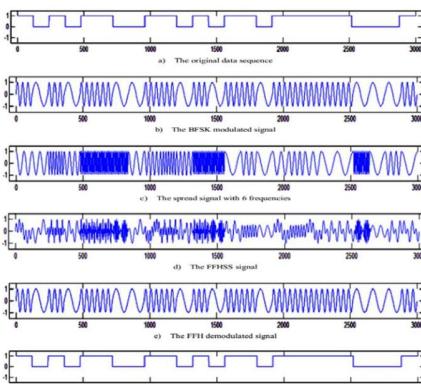
WLAN a spettro diffuso SS [Spread Spectrum]

Questo tipo di WLAN opera nelle bande di frequenza ISM [(Industrial, Scientific, and Medical) sono parti dello spettro elettromagnetico riservate per l'uso industriale, scientifico e medico senza necessità di licenza].

Nelle WLAN SS si distinguono due tipologie:

- IR a spettro diffuso a **salto di frequenza** (Frequency-Hopping Spread Spectrum, **FHSS**)
 - velocità 1-3 Mbps | mobilità completa | copertura 30-100m | tipo di modulazione FSK (**collare the gang fsk 4L**)
- IR a spettro diffuso a **sequenza diretta** (Direct Sequence Spread Spectrum, **DSSS**)
 - velocità 2-20Mbps | mobilità stazionaria/mobile | copertura 30-250m | tipo di modulazione QPSK

per entrambe metodo di accesso CSMA



FHSS (Frequency-Hopping Spread Spectrum)

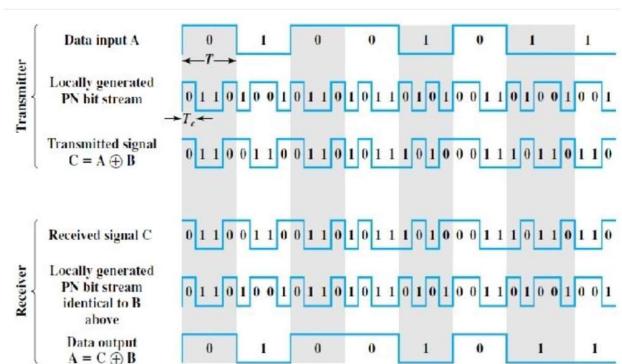
In questo tipo di trasmissione la **frequenza portante viene modificata** in base al rumore o a una **sequenza pseudocasuale** iniettata. Questa sequenza pseudocasuale è nota solamente al trasmettitore (che la inietta) e al ricevitore (che la rimuove per recuperare le informazioni originali).

Questa tecnica impedisce la perdita di dati, limita il rumore ,la diafonia (interferenze causate da un'altro canale di trasmissione adiacente) e le interferenze elettromagnetiche, preservando l'integrità del segnale e l'affidabilità delle comunicazioni

DSSS (Direct Sequence Spread Spectrum)

Il segnale trasmesso viene diviso e iniettato con più frequenze all'interno di una particolare banda di frequenza. **I dati originali vengono mescolati con bit di dati o codici ridondanti, chiamati chip o codice di sparpagliamento.**

Il DSSS permette una trasmissione sicura e il recupero di dati originali in caso di perdite parziali o dati danneggiati. È più veloce del FHSS ma è vulnerabile alle interferenze elettromagnetiche e al rumore causato da altri dispositivi che operano nella stessa banda di frequenza.



WLAN a radiofrequenza a microonde

Una WLAN a radiofrequenza opera in bande con e senza licenza. Le caratteristiche della WLAN RF sono le seguenti:

- Velocità di trasmissione dati: 10-20 Mbps
- Mobilità: supporta sia la modalità fissa che quella mobile
- Copertura: 10-40 metri
- Tipo di modulazione: FSK/QPSK
- Metodo di accesso: Reservation ALOHA e CSMA

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

E' un protocollo di accesso al mezzo utilizzato nelle reti wireless progettato per regolare l'accesso concorrente al canale di trasmissione, garantisce che i dispositivi trasmettano in modo ordinato riducendo al minimo le collisioni di dati.

Nelle reti cablate Ethernet se si verifica una collisione lo sbalzo dell'energia di un segnale è notevole (raddoppia) e quindi facilmente identificabile per questo si usa adotta il protocollo CSMA/CD (Collision Detection). Nelle reti wireless invece una collisione non è facilmente rilevabile in quanto il segnale aumenta solo del 5-10%, risulta impensabile per ciò appoggiarsi a un protocollo del tipo Collision Detection, risulta più pratico un protocollo che **evita le collisioni**. Per questo motivo **CSMA/CA è stato progettato appositamente per le reti wireless**.

Il CSMA/CA per regolare l'accesso al canale si basa su questi tre concetti:

- **Spazio InterFrame (DIFS - Distributed Inter-Frame Space):** Il DIFS è un intervallo di tempo che deve trascorrere tra il completamento di una trasmissione e l'inizio di un'altra, per garantire che il canale sia libero da altre trasmissioni. Il DIFS è utilizzato per evitare collisioni tra i pacchetti e può essere utilizzato anche per definire la priorità di una stazione o di un frame. Più alto è DIFS, più bassa è la priorità.
- **Contention Window:** La finestra di contesa è un intervallo di tempo casuale diviso in "slot" durante il quale un dispositivo attende prima di tentare di trasmettere dati dopo aver rilevato che il canale è libero.
- **Acknowledgments (ACK):** Dopo aver ricevuto un pacchetto di dati, il dispositivo destinatario invia un segnale di risposta noto come acknowledgment (ACK) al dispositivo mittente per confermare la ricezione corretta dei dati. Se il mittente non riceve l'ACK entro un certo periodo di tempo timer di time-out, assume che il pacchetto sia stato perso o danneggiato e ritenta di inviarlo.

varianti della famiglia di standard 802.11

IEEE 802.11b

Noto come **High Rate Wireless Ethernet** o **Wi-Fi**, prestazioni analoghe alla Ethernet (11Mbs), usa frequenze di 2.4GHz. E' lo standard wireless più popolare per la facile configurazione, la flessibilità e la possibilità di assimilare la WLAN a una rete Ethernet.

Retrocompatibile con i dispositivi che usano lo standard IEEE 802.11 tradizionale (interoperabilità garantita dalla WECA)

IEEE 802.11a

Velocità fino ai 54Mbs, la sua scarsa diffusione è dovuta alla incompatibilità con i dispositivi IEEE802.11b

IEEE 802.11d (IEEE 802.11c)

L'obiettivo principale di IEEE 802.11d è di permettere ai dispositivi Wi-Fi di adattarsi alle normative locali sulle frequenze e potenze di trasmissione nei vari paesi. Questo è particolarmente importante in ambienti internazionali, dove le regole per l'uso delle frequenze radio possono variare significativamente. (l'802.11c è stato sospeso ed è confluito nel IEEE 802.11 d)

IEEE 802.11e

Progettata per migliorare la qualità del servizio (QoS, Quality of Service) nelle reti Wi-Fi in ambienti IEEE 802.11. Questo standard modifica il sottolivello MAC e introduce meccanismi che consentono di gestire in modo più efficiente il traffico di rete, garantendo priorità ai dati sensibili al ritardo, come voce, video e altre applicazioni multimediali

IEEE 802.11g

E' lo standard che sancisce la nuova generazione del wireless, garantendo piena interoperabilità con lo standard IEEE 802.11b. Offre una banda trasmisiva di 54Mbps usando una frequenza di 2.4GHz. La sua portata in condizioni ideali è di 300 m

IEEE 802.11be

Extremely High Throughput o **EHT** potenzialmente il prossimo emendamento dello standard IEEE 802.11 a cui sarà designato Wi-Fi 7.

Si baserà su 802.11ax, concentrando sul funzionamento WLAN in ambienti interni ed esterni con velocità stazionarie e pedonali nelle bande di frequenza a 2,4, 5 e 6 GHz. • Si prevede che le velocità raggiungano i **40 Gbps**, pari a Thunderbolt 3.

Lo standard IEEE 802.15

E' un gruppo di lavoro del comitato per gli standard IEEE 802 dell'Institute of Electrical and Electronics Engineers (IEEE) che specifica gli standard delle reti personali wireless (WPAN).

Esistono 10 aree di sviluppo principali di questo gruppo.

10° PARTE

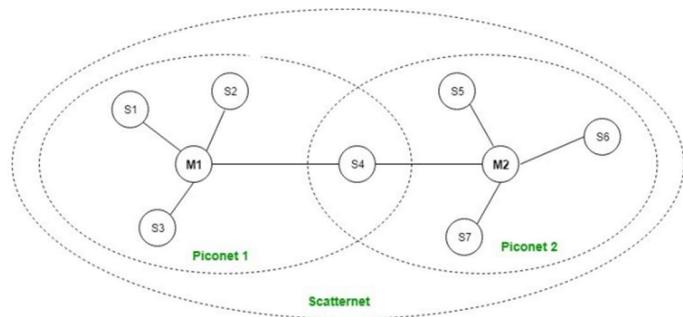
Bluetooth

Bluetooth è gestito dal Bluetooth Special Interest Group (**SIG**) che conta numerosissime aziende associate nei settori informatici. L'**IEEE** ha inizialmente standardizzato il **bluetooth** ma ora non lo gestisce più infatti il Bluetooth **SIG** supervisiona lo sviluppo delle specifiche, gestisce il programma di qualificazione e protegge i marchi.

Topologia

Il Bluetooth è uno standard tecnologico wireless che **facilita lo scambio di dati tra dispositivi mobili e fissi su brevi distanze**, nonché la creazione di reti personali (PAN). La sua **architettura** definisce due tipi principali di reti: le **piconet** e gli **scatternet**.

Una **piconet** è una rete Bluetooth che comprende un nodo primario, chiamato nodo master, e fino a sette nodi



secondari attivi, noti come nodi slave, per un totale di otto nodi attivi entro un raggio di 10 metri. La **comunicazione avviene tra master e slave**, con possibilità di comunicazione uno-a-uno o uno-a-molti. Non è possibile la comunicazione diretta tra nodi slave. Inoltre, possono esserci fino a 255 nodi inattivi in attesa di essere attivati.

Gli **scatternet** si formano tramite l'interconnessione di diverse piconet. Uno slave di una piconet può agire come master o primario in un'altra piconet, fungendo da ponte tra le due reti. Una stazione non può essere il master in due piconet contemporaneamente.

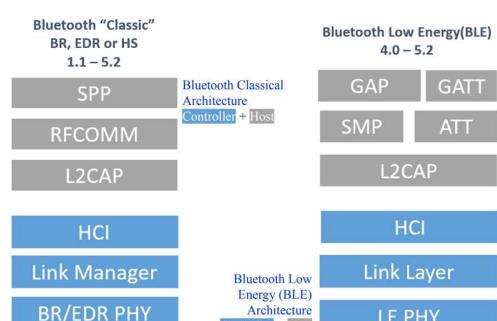
Caratteristiche

Il **Bluetooth utilizza onde radio UHF** nelle bande ISM, da 2,402 GHz a 2,48 GHz. È comunemente impiegato come alternativa senza fili alle connessioni via cavo, per lo scambio di file tra dispositivi portatili vicini e per collegare telefoni cellulari e lettori musicali con cuffie. La potenza di trasmissione è limitata a 2,5 mW, con una portata massima di circa 10 metri.

Utilizza la tecnologia radio frequency-hopping spread spectrum (**FHSS**), suddividendo i dati in pacchetti e trasmettendoli su uno dei 79 canali Bluetooth designati, con una larghezza di banda di 1 MHz ciascuno. Con l'abilitazione dell'Adaptive Frequency-Hopping (AFH), esegue di solito 1600 salti al secondo.

Il **Bluetooth Low Energy** utilizza una spaziatura di 2 MHz, consentendo l'uso di 40 canali.

Bluetooth e SIG



Un dispositivo può essere compatibile con uno o **entrambi i tipi di Bluetooth** illustrati qui a sinistra (**Classic e Low**). Nel caso in cui supporti entrambi, è **definito** come "**Smart Ready**" e include sia l'hardware per la modalità Classica che per il BLE (Bluetooth Low Energy). La **maggior parte** degli smartphone, workstation e computer portatili moderni è **dotata di chip** Bluetooth che supportano entrambe le modalità di connessione. Questi chip sono comunemente **chiamati chip Bluetooth Dual-Mode**.

BLE - Controller

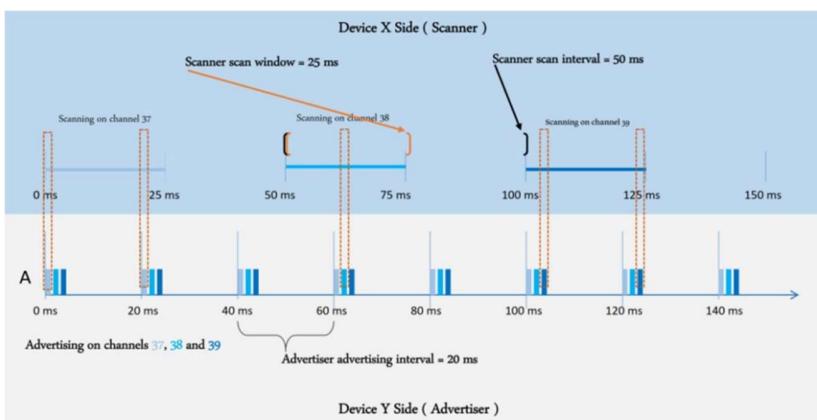
Il **BLE Controller** gestisce diverse funzioni essenziali. Il **livello fisico (PHY)** si occupa della **modulazione e demodulazione RF**, operando nella banda ISM a 2,4 GHz, condivisa con altri protocolli wireless come il Wi-Fi e il Bluetooth classico. La comunicazione avviene attraverso 40 canali RF suddivisi con spaziatura di 2 MHz. I canali 37, 38 e 39, noti come **advertisement channels**, sono utilizzati per la ricerca e la creazione di connessioni, mentre i restanti canali sono canali dati per la comunicazione bidirezionale. Per ridurre le interferenze, **BLE utilizza uno schema di salto di frequenza (FHSS)** che determina quale canale utilizzare per il prossimo evento di connessione.

BLE - Link Layer

Il **Bluetooth Link Layer** è il livello che si **interfaccia direttamente con il livello fisico**, spesso implementato tramite hardware per soddisfare i requisiti in tempo reale del BLE. Gestisce segnalazione, scansione e connessioni, incapsula

dati dai livelli superiori in pacchetti BLE, gestisce errori dei pacchetti e può cifrare la comunicazione con AES-CCM a 128 bit. Definisce i ruoli e gli stati dei dispositivi come Advertiser, Scanner, Master e Slave. Durante le fasi di ricerca/connessione, il ruolo del Link Layer può cambiare, ad esempio, un dispositivo può passare da Scanner a Master durante l'handshake per una connessione.

Il **funzionamento della BLE Discovery Phase** è illustrato nell'immagine a sinistra



Durante la **fase di ricerca di una connessione BLE**, un dispositivo trasmette lo stesso pacchetto di advertising su ciascuno dei tre canali di avviso (37, 38 e 39) a intervalli fissi, chiamati Advertiser Advertising Interval. Dal lato dello scanner, che di solito è un dispositivo mobile o un computer host, la scansione non è continua ma avviene a intervalli prefissati, chiamati Scanner Scan Interval. Durante questo intervallo, la scansione è attiva solo in una parte di esso, chiamata Scanner Scan Window. Lo scanner e l'advertiser non sono sincronizzati, ma per aumentare la probabilità di rilevamento del segnale, l'intervallo di scansione dello scanner deve essere almeno il doppio dell'intervallo di avviso dell'advertiser.

Il **funzionamento di un BLE Connection Phase** illustrato nell'immagine a sinistra

Una volta che uno scanner, identificato come dispositivo X, ha raccolto le informazioni necessarie su un advertiser di interesse, avvia un processo di connessione Bluetooth Low Energy (BLE). Durante questa connessione, lo scanner funge da Master (Link Layer Master), mentre l'advertiser assume il ruolo di Slave (Link Layer Slave). Il processo di negoziazione tra Master e Slave riguarda diversi parametri fondamentali per la connessione BLE. Tra questi, l'Intervallo di connessione, che determina il tempo tra due eventi di connessione consecutivi, e il Numero di pacchetti BLE per evento di connessione, che dipende principalmente dalla libreria/OS utilizzata e dall'hardware BLE. Inoltre, viene negoziata anche la **Slave Latency**, che permette allo Slave di saltare eventi di connessione inattivi per risparmiare energia, mantenendo comunque una latenza inferiore al **Supervision Timeout**, il quale indica la durata massima di attesa del Master per una risposta dello Slave prima di contrassegnare la connessione come terminata.

Un altro parametro negoziabile è la **Data-Packet Length**, che varia in base alla versione di BLE utilizzata. Il Preamble

viene utilizzato per allineare le finestre di trasmissione e ricezione dei due dispositivi collegati, mentre l'Access Address, generato casualmente per ogni connessione BLE, minimizza le collisioni sui canali di dati. Nei pacchetti di avviso, l'indirizzo di accesso assume un valore fisso. Infine, il CRC (Cyclic Redundancy Check) viene impiegato per rilevare

eventuali errori nei pacchetti ricevuti, fornendo un controllo dell'integrità dei dati nel livello di collegamento. Questi parametri e procedure sono fondamentali per garantire una connessione BLE stabile e efficiente tra dispositivi.

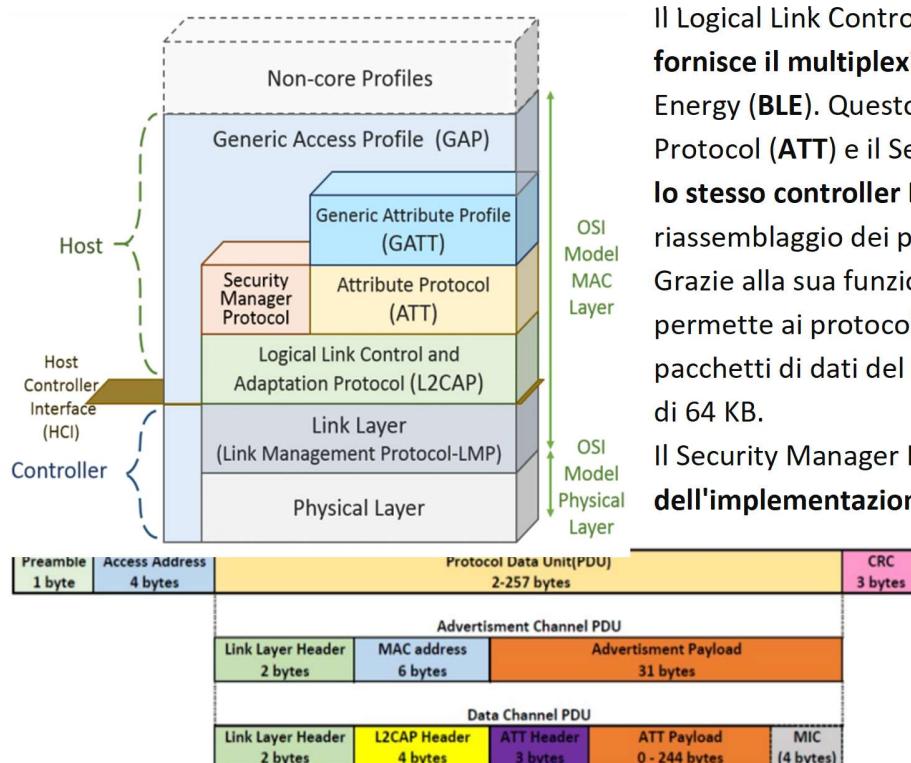
Frame del protocollo di comunicazione:

Il **Preamble** è utilizzato per sincronizzare le finestre di trasmissione e ricezione dei dispositivi collegati.

L'**Access Address**, generato casualmente per ogni connessione BLE, riduce la probabilità di collisioni sui canali di dati. Nei pacchetti di avviso, l'indirizzo di accesso è impostato su un valore fisso per un'identificazione chiara.

Il **CRC** consente al ricevitore di rilevare errori nei pacchetti, garantendo l'integrità dei dati nel livello di collegamento Bluetooth.

BLE – Host



Advertisement packets size:

- For BLE 4.0: 31 byte payload plus optional additional 31 bytes in scan response.
- For BLE 5.0 and above: 255 byte payload through advertisement extension.

Data packets size:

- For BLE 4.0: 27 byte payload. Only 20 available for the user data.
- For BLE 4.2 and above: 251 byte payload. Only 244 available for the user data.

Il **Logical Link Control and Adaptation Layer Protocol (L2CAP)** fornisce il **multiplexing** per i **livelli superiori** nel **Bluetooth Low Energy (BLE)**. Questo permette a protocolli come l'**Attribute Protocol (ATT)** e il **Security Manager Protocol (SMP)** di **condividere lo stesso controller BLE**, gestendo la segmentazione e il riassemblaggio dei pacchetti tra i livelli superiori e il controller BLE. Grazie alla sua funzione di segmentazione/riassemblaggio, L2CAP permette ai protocolli e alle applicazioni di trasmettere e ricevere pacchetti di dati del livello superiore con una lunghezza massima di 64 KB.

Il **Security Manager Protocol (SMP)** è **responsabile dell'implementazione della sicurezza per le applicazioni BLE**, offrendo servizi come l'autenticazione del dispositivo, l'autorizzazione del dispositivo, la privacy del dispositivo e l'integrità, la confidenzialità e la privacy dei dati.

ATTRIBUTE

Handle

UUID

Permissions

Value

L'Attribute Protocol (**ATT**) è un **protocollo client/server** che **gestisce gli attributi presentati da un dispositivo BLE**. Gli attributi sono coppie chiave-valore e l'attributo è l'unità base dei dati in ATT e in GATT (Generic Attribute Profile). Questo protocollo definisce la trasmissione delle unità di dati, dove il client richiede i dati al server che li invia al client. Ogni server ATT contiene dati organizzati in una tabella piatta di attributi, ognuno con un handle (chiave dell'attributo), un UUID (identificatore univoco universale), permessi di accesso (livello di sicurezza dell'attributo) e il valore effettivo dei dati dell'attributo (contenuto effettivo)

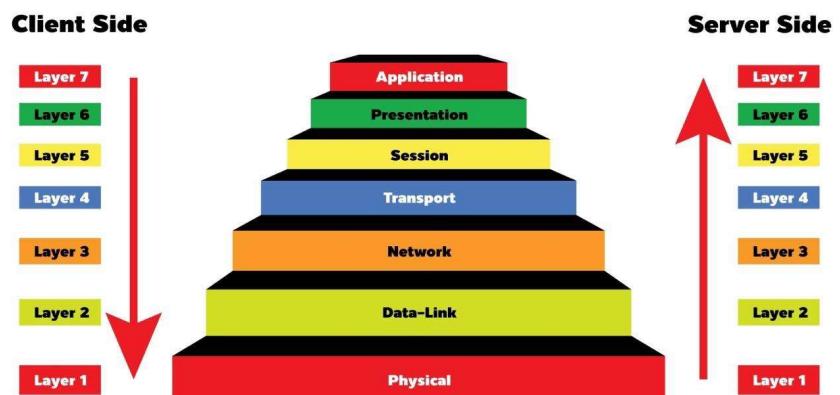
I **livelli successivi** nel BLE sono il Generic Attribute Profile (**GATT**) e il Generic Access Profile (**GAP**). Il GATT dettaglia lo scambio di tutti i dati del profilo e dell'utente in una connessione BLE, mentre il GAP definisce le interazioni di basso livello con i dispositivi. Questi due livelli forniscono un'astrazione completa per i livelli sottostanti, rendendo più agevole l'interazione con i dispositivi BLE e la gestione dei dati.

11° PARTE

-#| Layers dal 3 al 7 |#-

Network layer - (router, switch liv. 3)

È responsabile della **realizzazione di una connessione tra due nodi della rete**: il nodo sorgente e quello destinatario, inclusa la **scelta e la gestione del routing** (cioè le regole che permettono l'instradamento delle informazioni in base all'indirizzo della rete di destinazione) e lo scambio di informazioni tra i due nodi. Appartengono a questo livello i **router** e gli apparati di commutazione (**switch**) abilitati a funzioni di routing. I servizi di questo livello sono associati al movimento dei dati nella rete, inclusi l'**indirizzamento, il routing e le procedure di controllo dei flussi**. Il protocollo IP si occupa di questo livello.



Transport layer - (switch liv. 4)

E' il livello che **garantisce che il trasferimento delle informazioni avvenga correttamente**.

Analizza la comunicazione tra due nodi, assumendo che il network layer è in grado di stabilire il cammino ottimale tra i due nodi, quindi si occupa di:

- controllare l'errore
- verificare la sequenza delle informazioni
- analizzare i fattori di affidabilità dello scambio di dati tra i due nodi

Appartengono a questo livello i dispositivi di commutazione che operano a livello 4, quali ad esempio i **proxies(intermediario tra gli utenti ed internet)**

È il primo livello end-to-end (ovvero il controllo avviene alle estremità: origine e destinazione)

Appartengono a questo livello i **protocolli TCP e UDP**

Session layer

Gestisce le sessioni: fornisce le regole per attivare e terminare le **connessioni tra nodi della rete**.

Questo livello è responsabile di stabilire, mantenere e terminare le sessioni di comunicazione tra applicazioni.

Il session layer inoltre controlla il flusso di messaggi tra nodi, **controlla il dialogo** (determinando quale dispositivo può trasmettere dati in un dato momento), controllo dei dati da ambo i nodi, **sincronizzazione e gestione delle interruzioni**.

Presentation layer

I servizi di questo livello sono relativi alla **trasformazione dei dati**, alla loro formattazione e alla sintassi (trasformazione dei dati tra il formato utilizzato dall'applicazione e il formato di rete), in modo da essere **rappresentati opportunamente nel dispositivo di ricezione**.

Sono previste 3 rappresentazioni dell'informazione che si vuole comunicare:

- Rappresentazione Astratta:** Una rappresentazione neutra dei dati, indipendente dalla piattaforma e dal formato locale specifico, che definisce i dati in un formato comune.
- Rappresentazione Locale:** La rappresentazione dei dati specifica per il sistema locale dell'applicazione mittente o ricevente.
- Rappresentazione per il Trasferimento:** La rappresentazione dei dati usata durante il trasferimento attraverso la rete

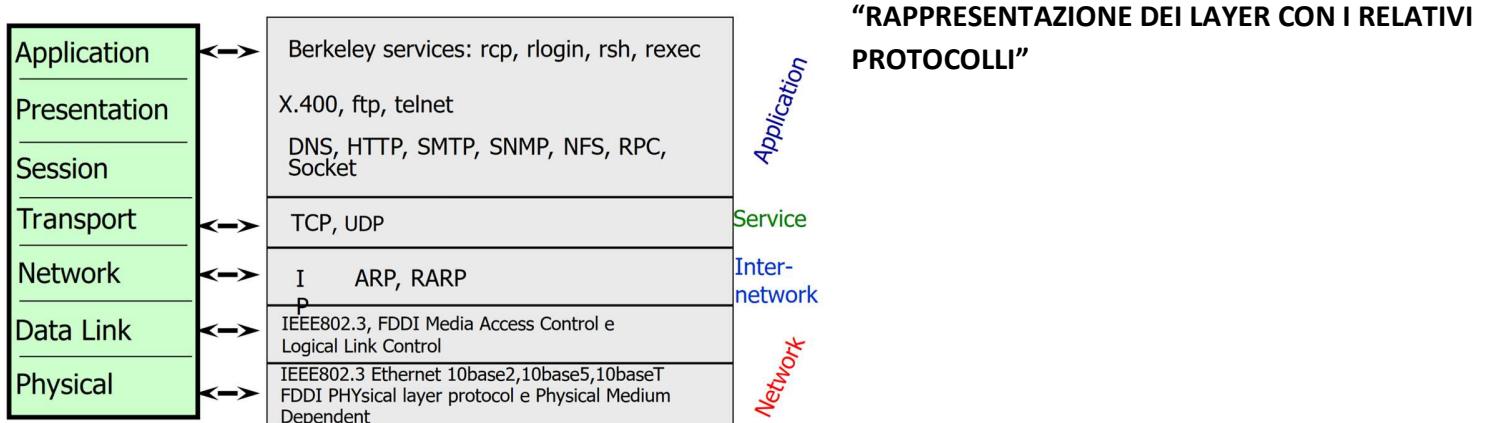
Esempi di trasformazioni: crittografia/crittografiazione, compressione/decompressione

Application layer

Questo livello fornisce servizi e **interfacce dirette agli utenti finali** e alle applicazioni per facilitare la comunicazione attraverso la rete. Funziona come un intermediario tra le applicazioni software e i livelli inferiori del modello OSI, gestendo vari protocolli e processi che supportano le attività di rete, è una **finestra** attraverso la quale è possibile accedere a tutti i servizi messi a disposizione dal modello OSI.

Esempi di funzioni svolte da questo livello:

- terminale virtuale (VT)
- file transfer access management (FTAM)
- Posta elettronica, X.400
- condivisione di risorse
- accesso a database (X.500, servizio di Directory)



Famiglia di protocolli TCP/IP

La famiglia dei protocolli TCP/IP è un insieme di protocolli di comunicazione utilizzati per la trasmissione di dati su reti di computer, tra cui Internet. TCP/IP sta per Transmission Control Protocol/Internet Protocol, i due protocolli principali della suite.

Internet Protocol, IP

La sua funzione primaria è di instradare i pacchetti di dati attraverso le reti fino a raggiungere la destinazione finale, internet viene visto come una singola rete virtuale che interconnette tutti gli host a cui è possibile comunicare.

Il software di Internet è costruito attorno alla gerarchia di questi tre concetti:

- Servizio di consegna del pacchetto senza connessione**: ogni pacchetto viene consegnato indipendentemente,

ogni pacchetto può fare strade diverse dagli altri per giungere a destinazione

2. **Servizio di trasporto inaffidabile**: i pacchetti possono andare persi o fuori sequenza

3. **Servizi di applicazione**: sono protocolli e software che forniscono funzionalità di rete direttamente utilizzabili dagli utenti finali. Operano al livello più alto del modello OSI e si interfacciano con applicazioni utente per offrire vari servizi, come navigazione web HTTPS, email SMTP, trasferimento di file FTP

Consegna best-effort: si fa di tutto per consegnare i pacchetti: l'inaffidabilità si verifica solo per malfunzionamenti hardware. E' compito dei servizi di più alto livello provvedere a garantire l'affidabilità della trasmissione re-inviano i pacchetti persi e ristabilendo la giusta sequenza tra i pacchetti.

IP è responsabile **dell'instradamento** dei pacchetti di dati da un dispositivo sorgente a un dispositivo di destinazione attraverso una rete interconnessa (**routing**), ma non specifica la struttura interna dei dati stessi. Questo è compito dei protocolli di livello superiore, come il Transmission Control Protocol (TCP) o il User Datagram Protocol (UDP), che operano sopra IP nel modello TCP/IP.

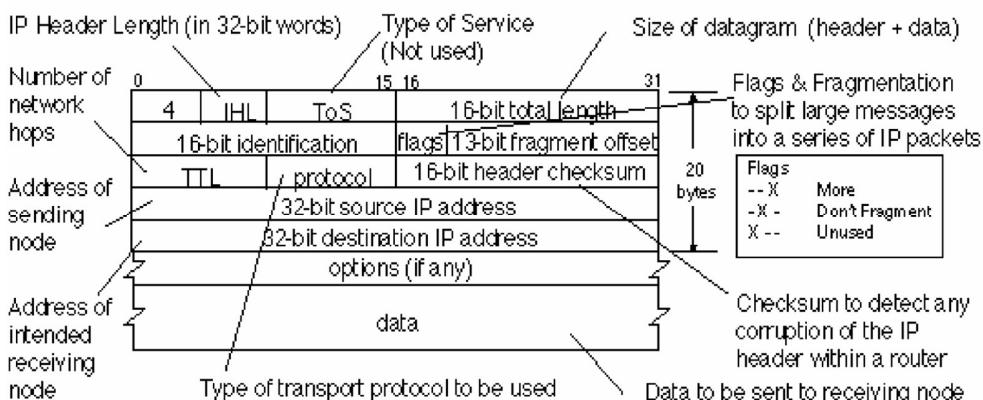
Le regole dell'IP inglobano i concetti di

- consegna non affidabile dei pacchetti
- elaborazione dei pacchetti da parte di host e gateway
- generazione dei messaggi di errore (ICMP)
- determinazione delle condizioni in cui occorre scartare i pacchetti

Datagram IP

Un datagram IP è l'**unità fondamentale di trasmissione di dati** nel protocollo Internet (IP). È costituito da due parti principali: **l'header** e il **payload** (il contenuto del pacchetto). L'header contiene informazioni di controllo necessarie per instradare il datagramma attraverso la rete fino alla destinazione, mentre il payload contiene i dati effettivi trasportati.

Header del datagram ip



Nell'header del datagram IP sono presenti i seguenti campi:

- **VERS** un campo di 4 bit che indica la versione IP del datagram. La Versione attualmente in uso è la 4 (IPv4), si sta introducendo la 6 (IPv6) che potenzia l'indirizzo IP a 64 bit e ne potenzia i servizi e le potenzialità
- **HLEN** un campo di 4 bit che indica la lunghezza dell'header del datagram in parole da 32 bit
- **LUNGHEZZA TOTALE** campo

lungo 16 bit che indica la lunghezza totale del datagram in ottetti, compresa l'area dati. La massima dimensione possibile per un datagram è $2^{16} = 65535$ ottetti

- **TIPO DI SERVIZIO** un campo di 8 bit che indica come deve essere gestito il datagram. E' diviso in:

- 3 bit di PRECEDENZA che consentono al trasmettitore di specificare l'importanza del datagram (valori da 0 a 7)
- 3 bit suddivisi in campi D T e R specifica il tipo di trasporto desiderato per il datagram. Se attivi, il bit D chiede un basso ritardo, il bit T richiede un alto throughput, il bit R alta affidabilità.
- gli altri 2 bit BO non ci sono nelle slide

- **IDENTIFICAZIONE, FLAG e OFFSET DEL FRAMMENTO** sono campi che controllano la frammentazione e il riassembaggio dei datagram a seguito dell'incapsulamento dei datagram nelle trame a livello fisico. Frammentazione e riassemblaggio dei datagram sono funzioni svolte dai protocolli a livello fisico della rete in cui si opera
- **TTL** indica la durata in secondi concessa al datagram per restare nel sistema internet
- **PROTOCOL** indica quale protocollo di più alto livello ha generato la porzione DATI trasportata dal datagram (es: 1=ICMP, 2=IGMP, 16=TCP, 17=UDP)
- **CHECKSUM** garantisce il controllo dell'integrità dell'header del datagram, mediante calcolo di un algoritmo Cyclic Redundancy Check (CRC) sui bit dell'header
- **IP ADDRESS DI PROVENIENZA** indirizzo IP a 32 bit dell'host che ha generato l'informazione contenuta nel datagram
- **IP ADDRESS DI DESTINAZIONE** indirizzo IP a 32 bit dell'host al quale è destinata l'informazione contenuta nel datagram. Anche se il datagram è instradato attraverso diversi gateway questi campi non cambiano mai
- **DATI** contiene i dati trasportati dal datagram
- **OPZIONI IP** un campo opzionale usato per funzioni di test e debugging della rete.
- **RIEMPIMENTO** un'area che viene riempita di bit a 0 per garantire che la lunghezza del datagram sia multipla di 32 bit

Elaborazione dell'Header IP (dopo un hop(?))

- Calcolo del checksum e verifica della sua validità, verifica che i campi dell'header contengano valori validi.
- Analisi della routing table per calcolare il next hop.
- Modifica dei campi che richiedono aggiornamento (TTL, header checksum).

Indirizzo IPv4

Un indirizzo IP su 32 bit (4 byte) permette di **identificare univocamente una rete ed uno specifico host appartenente alla rete:**

x.y.z.w (Es: 141.250.1.7)

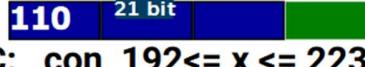
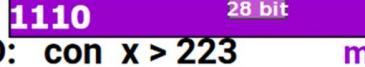
L'indirizzo si divide in due parti:

1. rete
2. host

Esistono 5 tipi di classi di indirizzi IP vedi 12° parte .

12° PARTE

Classi di indirizzi IP

- 126 reti da 16 milioni di host
subnet mask associata:
255.0.0.0
- Classe A: con $x < 128$ rete host **255.0.0.0**
- 16382 reti da 64000 host
- Classe B: con $128 \leq x \leq 191$ **255.255.0.0**
- 2 milioni di reti da 254 host
- Classe C: con $192 \leq x \leq 223$ **255.255.255.0**
- multicast addresses
- Classe D: con $x > 223$ **11110**
- Classe E con $x > 240$ (riservata)

X . Y . Z . W

Connessione alla rete

Dato che le tre classi primarie (A, B, C) sono identificabili in base ai primi due bit, è molto agevole per i router estrarre la parte rete e la parte host di un indirizzo IP. L'indirizzo IP identifica la **connessione di un host alla rete** (non l'host in sé). Macchine come i **router** che presentano più connessioni alla rete **hanno più indirizzi IP**: uno per ogni connessione alla rete.

Indirizzi di rete e broadcast

Gli indirizzi IP possono far riferimento a **rete** o ad **host**.

Un indirizzo IP dove i bit che indicano la parte host (la w sulla foto sopra) sono pari a **0** indica la rete stessa ed è chiamato **indirizzo di rete** (per questo motivo è convenzione non assegnare l'hostid 0 ad un singolo host).

Gli indirizzi IP possono essere utilizzati per specificare **indirizzi broadcast** (cioè indirizzi riservati a tutti gli host della rete) ponendo i bit della parte dell'host dell'indirizzo IP a **1**.

Indirizzi speciali

Default route

0.0.0.0 (in IPv4)

In italiano “percorso predefinito”, è una configurazione del protocollo internet (IP) che stabilisce una regola per l’ingresso dei pacchetti quando non è disponibile un indirizzo specifico di un host da qualsiasi meccanismo di routing.

Il percorso predefinito è generalmente l’indirizzo di un altro router che tratta il pacchetto allo stesso modo:

- Se un percorso corrisponde
 - il pacchetto viene inoltrato di conseguenza
- Altrimenti
 - il pacchetto viene inoltrato al percorso predefinito di quel router.
- Se un router NON dispone di un default route
 - il pacchetto viene cancellato

Loopback Address

127.0.0.1 (in IPv4)

L’indirizzo di loopback, chiamato anche localhost, si tratta di un indirizzo interno che rimanda al sistema locale e che permette la comunicazione tra processi, ma esclusivamente tra processi che sono eseguiti nella stessa macchina.

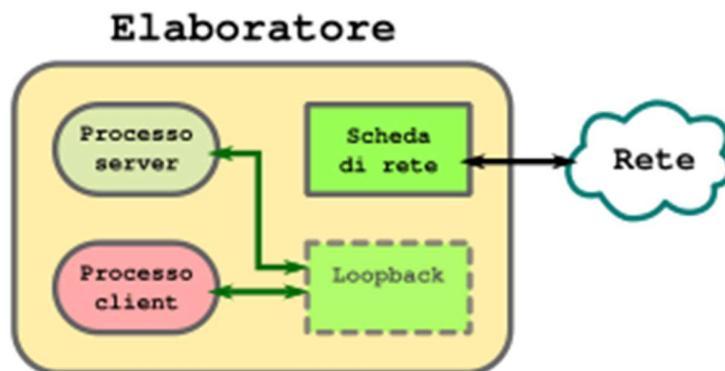
A grandi linee, è una scheda di rete virtuale gestita dal protocollo TCP/IP. I dati inviati all’IP di loopback (127.0.0.1) non vengono instradati attraverso la scheda di rete, ma attraverso l’interfaccia di loopback.

Grazie ai loopback i dati vengono gestiti localmente, senza l’ausilio della scheda di rete (da qui il termine *localhost*)

Scopo di questa interfaccia → Testare il funzionamento di un sistema

Ma possono essere utilizzate anche in contesti diversi dalle reti di computer

L’interfaccia di loopback non è hardware, ma è realizzata virtualmente nel sistema operativo



Indirizzi di rete e indirizzi di broadcast

- Broadcast locale
 - 255.255.255.255
- Per una rete di classe A
 - x.0.0.0 e x.255.255.255
- Per una rete di classe B
 - x.y.0.0 e x.y.255.255
- Per una rete di classe C
 - x.y.z.0 e x.y.z.255

Indirizzi privati

10.0.0.0/8

172.16.0.0/12

192.168.0.0/16

Questi indirizzi identificano **reti private** (definite così dall' RFC 1918), **non instradabili dai router** (tali indirizzi sono gestiti e amministrati dai **NAT server (Network Address Translation)** che gestiscono la conversione indirizzo pubblico-privato)

Indirizzi link local

169.254.0.0/16

Questo indirizzo è definito come **link local** (RFC 3927). Tali indirizzi vengono assegnati ad un'interfaccia dal sistema operativo quando ci sono problemi con l'assegnazione di indirizzi da parte di un **server DHCP**.

Questo indirizzo di rete è **valido solo per la comunicazione all'interno di un segmento di rete (link) o per il dominio di broadcast al quale l'host è connesso**.

Non vi è garanzia che un indirizzo link local sia **univoco**.

I router **non instradano pacchetti** con indirizzi link local.

Il protocollo ethernet utilizza solo indirizzi link local ed in questo caso sono i produttori hardware ad assicurare che gli indirizzi fisici non siano univoci.

Server DHCP

DHCP (Dynamic Host Configuration Protocol, in italiano "Protocollo di configurazione IP dinamica") indica un **protocollo ausiliario che permette ai dispositivi o ai terminali di una certa rete locale di ricevere automaticamente ad ogni richiesta di accesso**, da una rete IP, **la configurazione IP necessaria per stabilire una connessione e operare su una rete più ampia basata su internet protocol**.

Configurazione IP

Per configurare un host IP occorre specificare le seguenti entità:

- **Indirizzo IP**
- **Subnet mask**
- **Default gateway**
- **Indirizzo IP del nameserver**

La **possibilità alternativa** è quella di utilizzare il **protocollo DHCP** e lasciare gestire la definizione di queste informazioni a tale protocollo. Questa è una soluzione che, oltre a **semplificare la fase di configurazione permette di gestire facilmente la gestione della rete** (posso cambiare gli indirizzi IP e/o i parametri di configurazione senza intervenire sul client, cosa molto importante nel caso di grandi organizzazioni)

Un errore in fase di configurazione dei parametri IP genera malfunzionamenti:

- **Se si sbaglia la definizione di default gateway** le applicazioni locali funzionano, mentre quelle che richiedono connessioni all'esterno della rete locale no, poiché non si è in grado di raggiungere il giusto gateway
- **Un errore nella subnet mask può generare errori di connettività.** E' possibile, anche se altamente sconsigliabile, che la definizione di subnet mask differisca tra gli host della rete. L'effetto risultante può essere quello di comportamenti non prevedibili.

Indirizzamento con Subnet

L'indirizzamento con Subnet introduce un nuovo livello gerarchico negli indirizzi IP.

E' una tecnica trasparente per le reti ed i router remoti.

Semplifica la gestione delle varie LAN di un'organizzazione.

Viene definita la subnet mask per trovare il numero associato alla rete

10	Net ID	Host ID	Indirizzo originale	
10	Net ID	Subnet ID	Host ID	Indirizzo subnetted

Schema per Subnetting

Consideriamo l'indirizzo di classe B di cui dispone l'Università di Perugia:

141.250.0.0

Nello schema generale di subnet che viene utilizzato oggi, in genere ad ogni Università viene assegnato un indirizzo IP di classe C, con una subnet mask di 255.255.255.0

Vediamo come si calcola l'indirizzo della subnet per l'indirizzo: **141.250.5.25**

IP: **141** **250** **5** **25**
10001101|11111010|00000101|00011001

Mask: **255** **255** **255** **0**
11111111|11111111|11111111|00000000

AND:

10001101|11111010|00000101|00000000

Sotto ogni numero è presente la sua rappresentazione in codice binario

es: 141 → 10001101 → 128 + 0 + 0 + 0 + 8 + 4 + 0 + 1

La riga mask ci fa capire in che classe siamo. In questo caso, dato che riempie i primi 3 "slot" di bit, capiamo che ci troviamo in una classe C e che quindi 141.250.5.0 sarà l'indirizzo di rete e 25 l'host.

Se volessimo subnet mask più piccole (con circa 100 host) dovremmo adottare una **subnet mask più restrittiva**, 255.255.255.128 o /25.

Avremmo due reti: 141.250.5.0 e 141.250.5.128

L'intervallo degli indirizzi host in questo caso andrebbe da:

141 250 5 129
10001101|11111010|00000101|10000001

141 250 5 254
10001101|11111010|00000101|11111110

Questi sono il primo e l'ultimo indirizzo, l'indirizzo di broadcast è → 141.250.5.255

Subnetting

Un indirizzo IP di una rete può essere gestito come un insieme di sottoreti introducendo una **subnet mask più restrittiva** che assegna i bit più significativi della parte host alla parte di network, ottenendo da un indirizzo di una certa classe, un insieme di sottoreti di classe inferiore e conseguentemente di dimensioni inferiori.

Es: Rete di classe C 194.143.128

n. bit	rete	ind. Rete	num. Host
25	194.143.128.	{0, 128}	128
26	194.143.128.	{0,64,128,192}	64
27	194.143.128.	{0,32,64,96,128,160,192,224}	32
28	194.143.128 .	{0,16,32,48,64,80,96,112,128,144,160,176,192,208,224,240}	16
29	194.143.128.{0,8,16,24,32,40,48,56,64,72,80,86,96,104,112,120,128,136,144,150,160,168,176,184,192,200,208,216,224,232,240,248}	8	

Spiegazione esempio

Nella classe C l'indirizzo di rete occupa i primi 3 slot (255.255.255.0), in questo caso l'indirizzo di rete è 194.143.128.0. e quindi sarebbe
11000010. 10001111. 10000000.
in questo caso sono 24 bit

Nel momento in cui l'esempio ci dice che il numero di bit è 25 capiamo subito che possono esserci 2 reti

- 1) 194.143.128.0 (num host 0)
- 2) 194.143.128.1 (num host 128)

Se il numero di bit fosse stato 26 le possibilità aumentano:

- 1) 194.143.128.00 (num host 0)
- 2) 194.143.128.01 (num host 64)
- 3) 194.143.128.10 (num host 128)
- 4) 194.143.128.11 (num host 192)

E così via

Subnet mask

La subnet mask deve avere per la parte rete tutti i bit a 1 (senza 0 nella sequenza della parte di rete). Questo implica che i possibili indirizzi di una rete di classe C, ad esempio 194.143.128.0 sono:

- 11111111 11111111 11111111 11 (Subnet mask:255.255.255.192)
 - 11000010 10001111 10000000 00 0 (Rete 194.143.128.0)
 - 000000 0 ind. rete 1
 - 111111 63 ind. broadcast 1
 - 11000010 10001111 10000000 01 64 (Rete 194.143.128.64)
 - 000000 64 ind. rete 2
 - 111111 127 ind. broadcast 2
 - 11000010 10001111 10000000 10 128 (Rete 194.143.128.128)
 - 000000 128 ind. rete 3
 - 111111 191 ind. broadcast 3
 - 11000010 10001111 10000000 11 192 (Rete 194.143.128.192)
 - 000000 192 ind. rete 4
 - 111111 255 ind. broadcast 4

Subnets

La realizzazione di subnet comporta l'alterazione del comportamento standard della classe primaria IP mediante introduzione di una **subnet mask** che alteri il significato (va applicata all'indirizzo IP e ne modifica il significato primario) La subnet mask **altera le informazioni standard** relative alla **rete** ed all'**host** presente nell'indirizzo primario.

Mediante subnetting si

- **suddivide** una rete primaria in **più sottoreti differenti** che diventano **entità autonome** dal punto di vista del **routing** e del **TCP/IP**
- **accorpano** più reti fisiche primarie diverse in un'unica rete per semplificare le informazioni di routing da trasmettere ai router

La decisione di creare una sottorete dipende da aspetti topologici, organizzativi e tecnici:

- **Ragioni topologiche**

- Superamento limiti di distanza
 - a seconda del tipo di rete considerata occorre considerarne le caratteristiche fisiche e le specifiche di interfaccia. Ad esempio ogni segmento UTP deve essere al massimo lungo 100m. Da notare che la lunghezza dei cavi della rete è data dalla somma di tutti i segmenti, include le bretelle di giunzione negli armadi e i segmenti che vanno dalla presa di rete all'interfaccia di rete dei singoli host.
- Connessione di reti fisiche diverse
 - router IP possono essere usati per collegare reti che hanno una diversa tecnologia o un diverso mezzo trasmittivo (da token ring a ethernet o tra ethernet con diverso mezzo trasmittivo, es : fibra cavo coassiale).
- Filtro del traffico fra reti
 - il traffico locale rimane nella sottorete locale, solo il traffico verso altre reti è inviato al gateway

- **Ragioni organizzative**

- Amministrazione
 - le sottoreti possono essere usate per delegare la gestione degli indirizzi, il controllo e la diagnostica a piccole entità
- Visibilità di strutture
 - singole strutture (es. dipartimenti universitari) necessitano di realizzare la propria autonomia al fine di meglio organizzare i servizi
- Isolamento del traffico
 - per motivi di sicurezza è preferibile isolare il traffico locale in modo tale da renderlo inaccessibile all'esterno

- **Ragioni tecniche**

- Ottimizzazione dell'uso dello spazio di indirizzamento IP
- Limitazione del dominio di broadcast IP
- Limitazione degli effetti di eventuali malfunzionamenti

Piano di indirizzamento IP

E' il documento che il network administrator deve scrivere e tenere aggiornato per descrivere l'utilizzo del proprio spazio di indirizzamento IP

Es:

194.143.128.0 /26	255.255.255.192	rete internal1
194.143.128.64 /26	255.255.255.192	rete interna2
194.143.128.128/25	255.255.255.128	rete interna3
194.143.129.0 /30	255.255.255.252	punto-punto1
194.143.129.4 /30	255.255.255.252	punto-punto2
194.143.129.8 /29	255.255.255.248	rete lab1
194.143.129.16 /28	255.255.255.240	rete lab2
194.143.129.32 /27	255.255.255.224	rete lab3
194.143.129.64 /26	255.255.255.192	rete lab3
194.143.129.128/25	255.255.255.128	rete amml

13° PARTE

ARP: Address Resolution Protocol

Serve a mappare(associare) gli indirizzi IP agli indirizzi MAC(Media Access Control) anche detto indirizzo fisico, le applicazioni di solito conoscono solo il nome del host o/e il suo indirizzo IP, viene usato quando si deve encapsulare un pacchetto di Livello 3(Network) al Livello inferiore ovvero 2(Data Link).

Ad esempio supponiamo di avere 2 host “A” e “B”, dove “A” ha bisogno di conoscere l’indirizzo fisico del Host “B”

- B invia un pacchetto broadcast contenente un indirizzo IP e chiede all’host che ha quell’indirizzo IP di rispondere con il proprio indirizzo MAC, inoltre in questo pacchetto mette anche il proprio MAC così che possa essere noto agli altri host
- A gli risponde con il proprio MAC address
- B mette in una cache(locale) il MAC address e lo associa a l’indirizzo ip

La cache di ARP può diventare inaffidabile in qualsiasi momento senza preavviso, dato che alla combinazione IP-MAC piace cambiare, ma comunque utile in quanto ci permette di aumentare l’efficienza

Funzioni e problemi di ARP

il protocolla ARP svolge principalmente due funzioni:

- Determinare gli indirizzi fisici quando si trasmette un pacchetto da un host ad un altro
- Rispondere a richieste ARP di altre macchine

e possono esserci le seguenti problematiche dato che usa il meccanismo di richiesta via broadcast può generare problemi

- se si aggiornano i dati nella cache ARP allo scadere esatto del timer può portare a ritardi, per questo si effettua una “rivalutazione anticipata” prima dello scadere del timer
- se ci sono richieste ARP pendenti potrebbero avere un impatto negativo sugli altri protocolli

RARP: Reverse Address Resolution Protocol

Ha un funzionamento simile al ARP ma in questo caso abbiamo noto il MAC address ma non l’indirizzo IP quindi prendendendo sempre come esempio Host “A” e “B”:

- B invia un pacchetto broadcast contenente un indirizzo MAC e chiede alla macchina che ha quell’indirizzo MAC di rispondere con il proprio indirizzo IP
- A gli risponde con il proprio IP
- B mette in una cache(locale) l’IP e lo associa a l’indirizzo MAC

Protocollo ICMP

L'internet control message protocol, è stato **progettato per riportare le anomalie che potrebbero accadere nel routing di pacchetti**, ci da la possibilità di controllare lo stato della rete, alcuni dei messaggi del ICMP sono:

Codice	Messaggio	Codice	Messaggio
0	Echo Reply	13	Timestamp Request
3	Destination Unreachable	14	Timestamp Replay
4	Source Quence	15	Information Request
5	Redirect	16	Information Replay
8	Echo Request	17	Address Mask Request
11	Time Exceeded for a Datagram	18	Address Mask Replay
12	Parameter Problem on a Datagram		

messaggi che riportano anomalie

messaggi di verifica della raggiungibilità di un nodo

Redirect

il messaggio di reindirizzamento ICMP informa l'host che c'è una via di routing più efficiente, attraverso una rete

Mask request e Replay

viene mandato da un host al router, sono stati introdotti per permettere di scoprire automaticamente la netmask usata nella rete dove è situato l'host

IP Multicasting

Serve a mandare un pacchetto o datagram ad un gruppo di host identificato da un indirizzo ip, gli host appartenenti ad un gruppo possono cambiare, un gruppo di Host può essere permanente(ha un indirizzo ip assegnato) o transitorio, è responsabilità dei **multicast agents** creare e mantenere informazioni sui gruppi transitori

IGMP (Internet Group Management Protocol)

Supporta le funzioni di **IP multicasting**, consentendo ad un host di creare, unirsi o abbandonare un **gruppo multicast**, inoltre implementa anche la possibilità di inviare un **datagram IP**(pacchetto) ad un gruppo di host

UDP: User Datagram Protocol

L'UDP è un protocollo di trasporto molto semplice, infatti è connectionless e senza handshaking, offre due servizi all'IP:

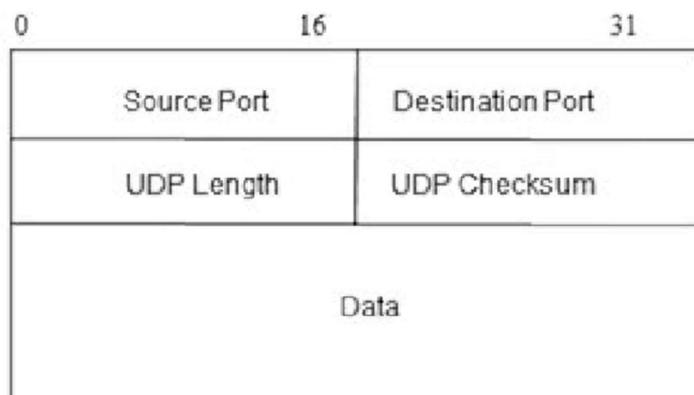
- **Multiplexing e De-Multiplexing:** permette a più applicazioni su un host di inviare e ricevere dati allo stesso tempo, ogni processo viene identificato da un **port number**
- Controllo del errore sui dati

il **port number** o **numero di porta** serve per identificare un'applicazione, il SO deve fornire i meccanismi alle applicazioni per accedere alle porte e specificarle, l'ente [IANA](#) ha assegnato determinati servizi a determinate porte:

- **Well known:** dalla porta 0 alla 1023 servizi come **DNS** e **HTTP**
- **Porte utente:** 1024 alla 49151
- **Assegnate dinamicamente** dalla 49152 a 65535

Un protocollo applicativo che usa UDP si fa carico di gestire l'intero problema dell'affidabilità come l'invio duplicato di messaggi, consegna in ritardo, consegna fuori ordine, è un protocollo posto sopra il **livello IP** ma sotto i **protocolli applicativi**, UDP funziona molto bene in ambiti locali ma non su una rete di dimensioni maggiori

Datagram UDP



contiene la porta mittente quella di arrivo, la lunghezza del datagram e il checksum non sempre presente in quanto opzionale l'host ricevente calcola il checksum se il risultato è errato cancella il pacchetto

TCP: Transmission Control Protocol

Fornisce un **servizio di consegna affidabile delle informazioni con connessione**, ci fornisce un metodo per l'invio e la ricezione dei dati suddivisi in pacchetti, garantendo una consegna affidabile nel ordine corretto e senza errori.

Anche questo protocollo usa i port number per identificare i flussi dati tra le varie applicazioni di un host, ma in modo più complesso rispetto al **UDP** gli oggetti da identificare sono connessioni virtuali di circuiti e non singole porte, per fare ciò usa i **Socket** ovvero la combinazione di **indirizzo IP(host)** e **numero di porta**, questo permette la condivisione di un port number tra più host aumentando di molto l'efficienza di internet

Caratteristiche TCP/IP

- **orientamento dello stream:** Quando due applicativi trasferiscono dati, questi vengono memorizzati come sequenze di bit, anche chiamate "**stream**", suddivise in byte. Il servizio di consegna dello **stream** passa gli stessi bit nella stessa sequenza dal mittente al destinatario
- **Connessione di circuito virtuale:** il trasferimento degli stream funziona in modo simile ad una chiamata telefonica, solo quando mittente e destinatario hanno verificato l'esistenza delle condizioni necessarie inizia lo scambio di informazioni
- **Trasferimento Bufferizzato:** A seconda della quantità di dati generati da un applicazione, il protocollo decide se attendere la generazione di più byte da accoppare e inviare, oppure inviare blocchi di dati più piccoli man mano che vengono generati
- **stream non strutturata:** il **TCP** non rispetta eventuali strutture, presenti nei dati, è compito degli applicativi che usano questo protocollo comprendere la struttura dei dati trasmessi
- **connessione full duplex:** le connessioni fornite dal servizio di stream consentono il trasferimento simultaneo in entrambe le direzioni

Affidabilità del trasporto di stream

Un complesso meccanismo di trasmissione tra mittente e destinatario basato su:

- controllo dell'errore, del flusso e della congestione
- connessione: attivazione, controllo e chiusura
- protocollo orientato alla connessione, con connessione unicast tra server e client

ha un overhead maggiore rispetto all **UDP**, ma ha un affidabilità molto alta infatti molti protocolli usano **TCP** per la sua affidabilità alcuni esempi sono **HTTP, SMTP, SSH, POP, IMAP**

[[Gervasi qua approfondisce alcune cose già dette Slide 346 a 351 pacco 1]]

14° PARTE

Routing

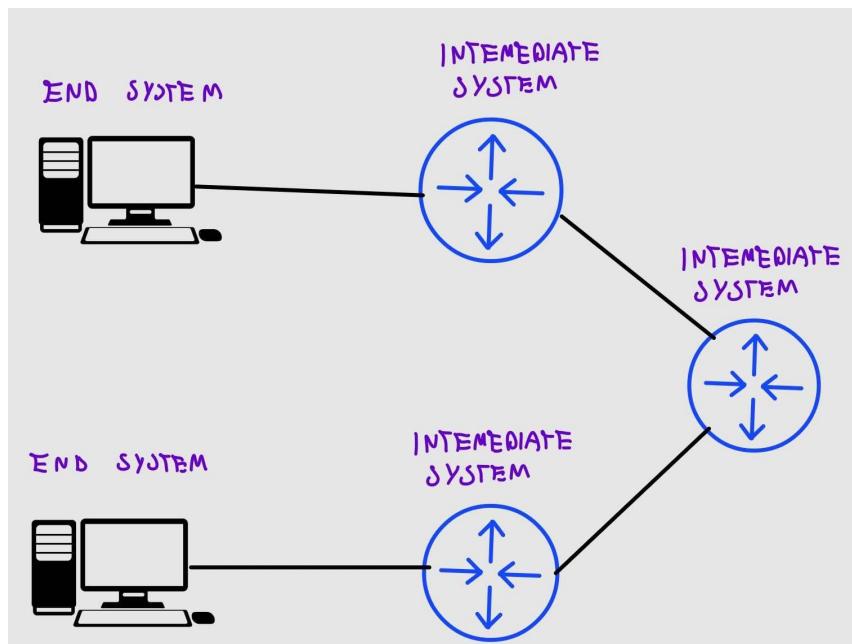
Il **Routing**(Instradamento) consiste nello scambiare informazioni in una rete da una sorgente ad una destinazione, incontrando almeno un nodo intermedio, fa parte del **livello 3 del modello ISO/OSI(Network layer)** il **routing** svolge due attività di base:

- determinare il percorso ottimale di routing
- trasportare pacchetti attraverso una rete

introduciamo il concetto di **Metric** ovvero la lunghezza di un percorso in termini di gateway traversati, utile a stabilire un percorso ottimale da calcolare da parte di un protocollo di routing, e l'associazione di **destination/next hop** per calcolare quale nodo intermedio rappresenta il miglior percorso per avvicinarcisi alla destinazione del pacchetto.

i router comunicano tra di loro e mantengono aggiornate le **tabelle di routing**, tramite la trasmissione di vari messaggi:

- **routing update**: contiene una **tabella di routing** o una parte, un router analizzando questo messaggio è capace di comprendere la topologia della rete
- **link- state advertisement**: è un messaggio usato dai i router che usano il protocollo **OSPF(Open Shortest Path First)** lo vedremo in seguito, informano i router lo stato del link del mittente e consentono a loro stessi di calcolare il percorso migliore da seguire per arrivare a destinazione



i router sono gli **intermediate system(next hop)** mentre i pc o meglio gli host sono gli **end point** ovvero le **destinazioni**

Algoritmi di Routing

Gli algoritmi di routing devono avere almeno uno o più dei seguenti requisiti:

- ottimale: deve scegliere la migliore strada
- efficienza: devono essere il più semplici possibile e tenere l'overhead altrettanto basso consumando meno risorse possibili
- robustezza e stabilità: devono comportarsi bene e correttamente in condizioni non previste
- rapidità: la scelta del percorso deve avvenire subito e con il minor sforzo possibile
- flessibilità: devono riuscire ad adattarsi facilmente alle situazioni

NB: come abbiamo visto con betti ad algoritmi non possiamo avere tutto dalla vita, quindi anche un'opportuna scelta di un algoritmo piuttosto che un altro è importante

Classificazione Algoritmi di routing

- Statici o dinamici
- Single path o Multi path
- Lineari o Gerarchici
- Host Intelligent o Router intelligent
- Intradomain o Interdomain
- Link state o distance vector

Metriche Algoritmi di Routing

Gli algoritmi usano una o più delle seguenti metriche per determinare il percorso migliore:

- Path length
- Reliability
- Delay
- Bandwidth
- Load
- Communication cost

Routing Table

i **gateway**(ora la maggior parte dei router fungono da gateway non è stato sempre così , ma a quanto pare per gervasi Gateway=Router ma sono due cose diverse che ora vengono accorpate nel router) instradano i pacchetti tra reti diverse

Un host prende decisioni di routing in base a dove si trova il destinatario:

- se è sulla rete locale vengono spediti direttamente all'host di destinazione
- se è una rete remota i dati vengono mandati al gateway locale

il **protocollo IP** basa le sue decisioni di routing sulla parte RETE dell'indirizzo IP e analizza quest'ultimo nel modo seguente:

- determina la **classe del IP**
- controlla la rete di destinazione, **se è una sottorete** applica all'indirizzo di destinazione la **subnet mask** per determinare se può essere inviata direttamente al destinatario oppure se deve essere instradata tramite un gateway
- cerca la rete di destinazione nella **routing table**
- esegue il routing dei pacchetti seguendo il percorso indicato nella **tabella di routing**(lato host di solito)

Esempio tabella di routing, per visualizzarla fare netstat - nr su un terminale unix based(Linux, Mac OS X, Powershell di Windows)

IPv4 Route Table						
=====						
Active Routes:						
Network Destination	Netmask	Gateway	Interface	Metric		
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.237	25		
0.0.0.0	0.0.0.0	26.0.0.1	26.4.199.111	9257		
26.0.0.0	255.0.0.0	On-link	26.4.199.111	257		
26.4.199.111	255.255.255.255	On-link	26.4.199.111	257		
26.255.255.255	255.255.255.255	On-link	26.4.199.111	257		
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331		
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331		
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331		
192.168.1.0	255.255.255.0	On-link	192.168.1.237	281		
192.168.1.237	255.255.255.255	On-link	192.168.1.237	281		
192.168.1.255	255.255.255.255	On-link	192.168.1.237	281		
224.0.0.0	240.0.0.0	On-link	127.0.0.1	331		
224.0.0.0	240.0.0.0	On-link	192.168.1.237	281		
224.0.0.0	240.0.0.0	On-link	26.4.199.111	257		
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331		
255.255.255.255	255.255.255.255	On-link	192.168.1.237	281		
255.255.255.255	255.255.255.255	On-link	26.4.199.111	257		
=====						
Persistent Routes:						
Network Address	Netmask	Gateway	Address	Metric		
0.0.0.0	0.0.0.0	26.0.0.1		9256		

In sostanza le routing table permettono ad un router di fare le scelte corrette per indirizzare i pacchetti, e prendono informazioni da due sorgenti:

- File di configurazione creato dall'amministratore di rete e salvato sul dispositivo
- dai protocolli dinamici di aggiornamento

Gli host non eseguono tipicamente protocolli di routing dinamici e tendono a tenere “congelata” la tabella di routing al contrario dei router

Tipi di routing

ci sono 3 tipi di routing:

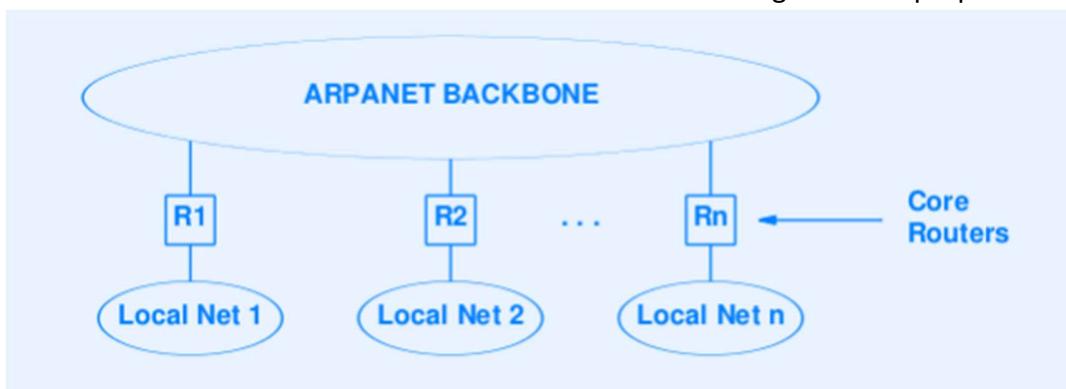
1. **Minimale**: operazione di base di aggiornamento di una tabella di routing effettuate al momento della definizione di un interfaccia
2. **Statico**: routing gestito da informazioni predefinite e costanti, utile in topologie di rete molto semplici come una rete connessa in un solo modo al backbone(rete che interconnette reti più piccole)
3. **Dinamico**: routing gestito via software da protocolli di routing che si adattano a tutti i cambiamenti della rete. questi ultimi utilizzano dei pacchetti per scambiarsi informazioni di aggiornamento per le routing table

Routing con informazioni parziali

Per i router all'interno di un **Autonomous system**(usa protocolli di tipo IGP) le informazioni possedute da un singolo router sono parziali, conoscono solo le reti collegate a loro stessi, e si affida ad un default router per tutte le reti che non conosce, inoltre permette a livello locale ad i router di modificare in modo autonomo alcune **istruzione di routing** e creano il rischio di avere inconsistenze e di rendere inaccessibili delle reti

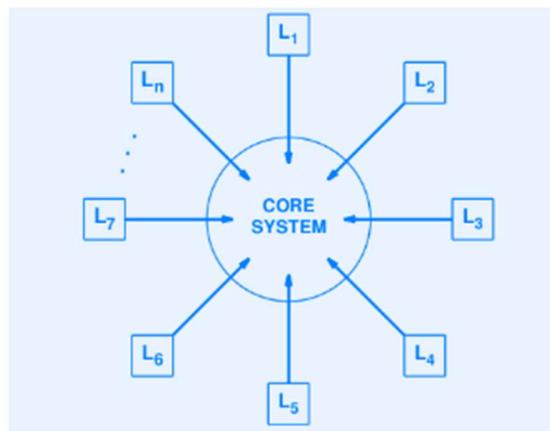
Routing originale di internet (Storia) ?

Era costituito da una backbone centrale e una serie di router che connettono ognuno una propria rete



prevedeva un insieme di router centrali che conoscevano completamente le destinazioni di tutte le reti e gli altri router conoscevano le informazioni locali, questo a costo di:

- Colli di bottiglia
- scorciatoie non possibili
- soluzione non scalabile



In poche parole era un sistema gerarchico gestito da una sola organizzazione, e non scalabile in quanto complesso farlo e comunque ci sarebbe troppo overhead, inoltre era impossibile pensare di collegare tutte le reti fisiche alla backbone(perchè era solo una)

Core routing

La soluzione adottata oggi un insieme di **router centralizzati**(router molto potenti usati nelle backbone) hanno le informazioni su tutte le possibili destinazioni di internet, funzionano bene per delle reti che hanno **un solo backbone**, se viene estesa ad altre backbone il routing diventa complesso, rischio di **routing loop** se tutti i router usano una **default route**(pacchetti che vanno in loop nella rete fino a che non scade il loro **TTL time to live**)

Architettura moderna

Nel approccio moderno i router del core system conoscono le destinazioni di tutte le reti, dove un meccanismo consente di contattare i **core router** per conoscere le informazioni di routing, inoltre c'è un modo che consente ad i router di ricevere aggiornamenti in **modo automatico**, gli algoritmi usati per distribuire gli aggiornamenti in modo automatico sono i seguenti:

- Distance-vector
 - Link-state

Algoritmo Distance-vector

la **routing table** viene inizializzata con tutte le reti direttamente connesse, con una cadenza periodica viene eseguito l’algoritmo per scambiare informazioni con i router raggiungibili attraverso le reti connesse, un router invia una lista di tuple che contengono **L’IP di Destinazione e la distanza**, il router che riceve le informazioni le confronta con quelle in suo possesso, sostituendo con le nuove istruzioni se sono migliori di quelle in suo possesso

Destination	Distance	Route	Destination	Distance
Net 1	0	direct	Net 1	2
Net 2	0	direct	→ Net 4	3
Net 4	8	Router L	→ Net 17	6
Net 17	5	Router M	→ Net 21	4
Net 24	6	Router J	Net 24	5
Net 30	2	Router Q	Net 30	10
Net 42	2	Router J	→ Net 42	3

Link-state update

Ogni **nodo(router)** costruisce una mappa delle connettività di rete, nella forma di un grafo, che mostra quali nodi sono connessi ad altri nodi, una volta fatto ciò ogni nodo in modo indipendente calcola, il prossimo percorso migliore, e lo fa per ogni destinazione nella rete, ogni lista di percorsi migliori formerà la routing table di ogni nodo

Autonomous System

Per **Dominio di routing** si intende l'insieme delle reti, amministrate e controllate dalla stessa organizzazione, una rete o un **IS(intermediate system)** può essere:

- interno ad un dominio di routing
- esterno ad un dominio di routing

Un **ISP** può gestire più autonomous system, la politica di routing di un **AS** viene identificata dal **ASN(autonomous system number)** che vengono assegnati per l'appunto agli AS per fare in modo che possano effettuare routing **BGP**(Border Gateway Protocol)

I router che instradano messaggi all'interno dello stesso **AS** sono detti **interior router** e usano un protocollo **IGP**(Interior Gateway Protocol), mentre quelli che instradano messaggi tra **AS** diversi sono chiamati **exterior router** e usano un protocollo **EGP**(Exterior Gateway Protocol)

ASN (Autonomous System Number)

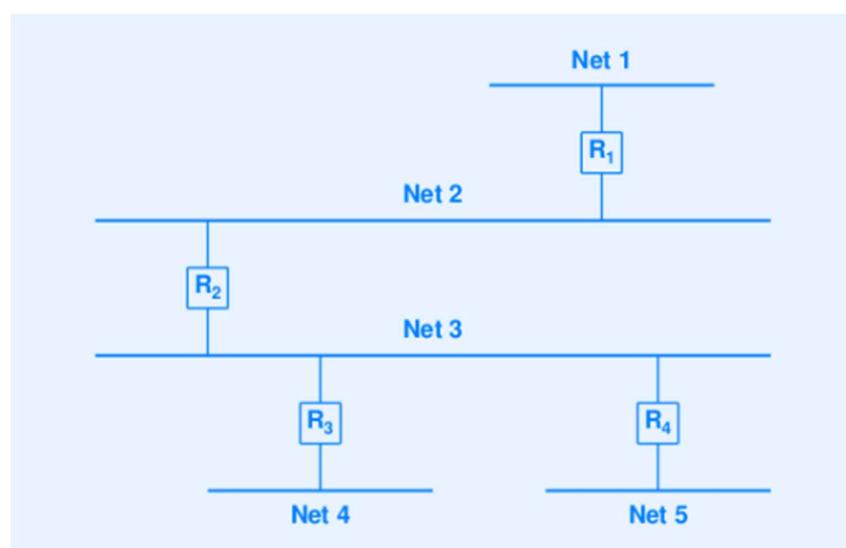
Gli ASN in passato erano assegnati da **IANA**, ora vengono assegnati da **ICANN** ai **Regional Internet Registries** e si suddividono in:

- **Multihomed Autonomous System**: mantiene connessione con più **AS**, questo gli consente di rimanere connesso alla rete internet anche se una delle connessioni ha un malfunzionamento
- **Stub Autonomous System**: è un **AS** connesso solamente ad un altro **AS**, questo tipo di **AS** consente forme di peering privato(interconnessione tra due reti di 2 ISP diversi, utile a ridurre i costi) con altri **AS**
- **Transit Autonomous System**: è un **AS** che fornisce connessioni con altre reti, Una rete "A" può usare una rete "B"(**Transit AS**) per comunicare con la rete "C"

Per ottenere il rilascio di un **ASN** l'**AS** deve essere collegato a internet da almeno 2 punti e con diversi **ISP**

Routing statico

Usate tipicamente dagli **host** e qualche volta dai **router**, sono **Routing table** che vengono inizializzate all'avvio del dispositivo, e non cambiano mai, possiamo configurare piccole reti in questo modo, ma nulla di più sotto l'aspetto reti

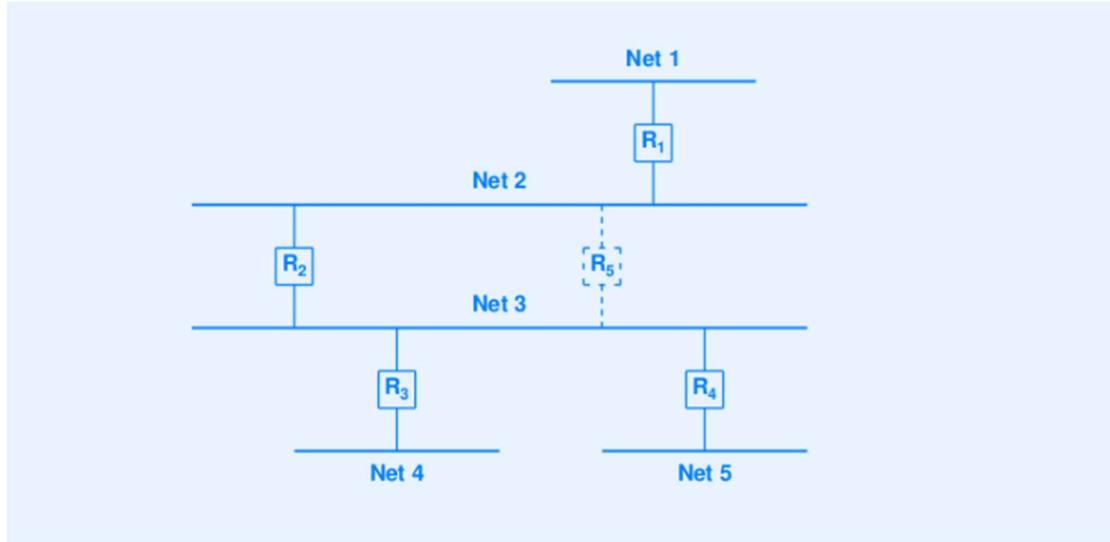


Come possiamo vedere **ogni rete ha un solo cammino possibile**

Routing Dinamico

anche questo tipo di **routing** viene inizializzato all'avvio del dispositivo dove va a prendere alcune route dal file di configurazione, ma poi si aggiorna da solo usando i **protocolli di routing**, questo metodo è difficilmente usato negli host, ma **comune nei Router**

Esempio in cui è necessario avere routing dinamico:



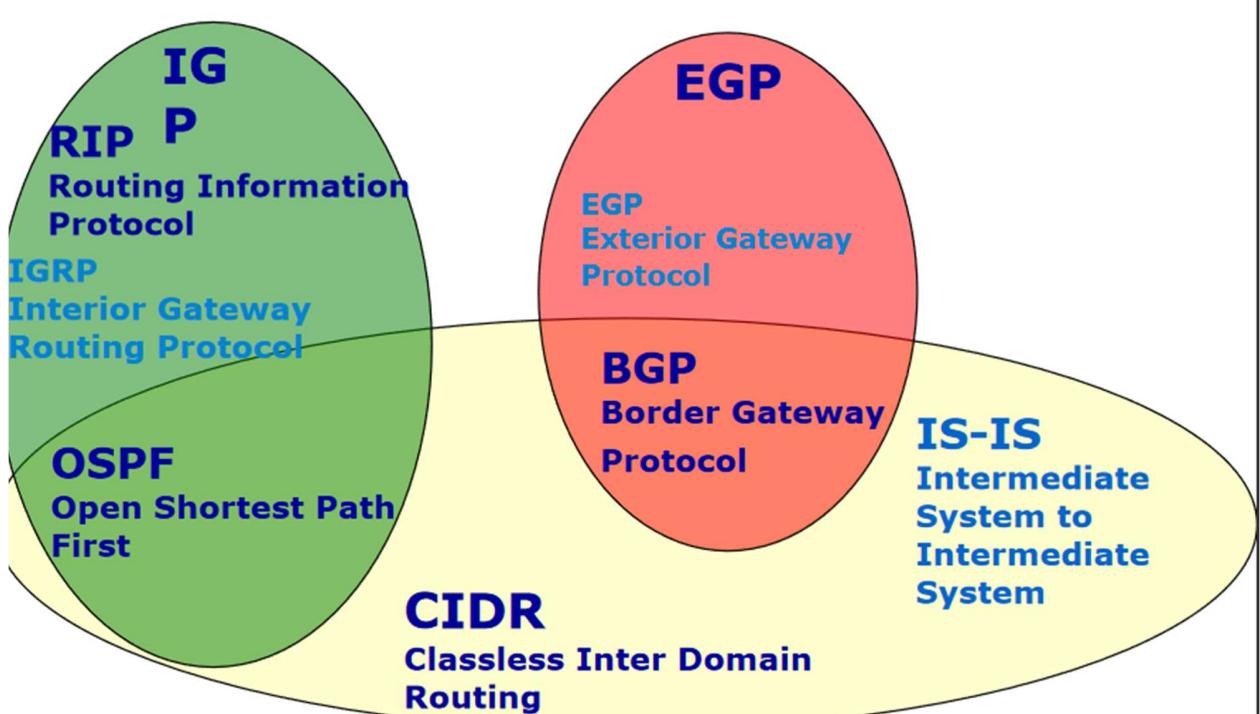
Ci sono più percorsi possibili per raggiungere una rete

Scambio di informazioni di routing all'interno di un AS

Viene effettuato tramite gli **IGP**(Interior Gateway Protocols), le scelte dei protocolli **IGP** sono effettuate dagli **AS**, mentre se un **AS** si connette al resto del mondo deve usare un protocollo **EGP**(exterior gateway protocol) per annunciare la propria raggiungibilità

15° PARTE

Protocolli di routing



OSPF (Open Shortest Path First)

OSPF è un protocollo **IGP**(Interior Gateway Protocol) Open source, è un **link-state routing protocol**, perché invia LSA(link-state advertisements) comunica la topologia di un router a tutti gli altri router nella stessa area, è una procedura computazionalmente pesante, OSPF ha le seguenti caratteristiche:

- è Open Source
- Basato sul l'algoritmo Short Path First(di Dijkstra)
- supporta subnet variabili
- implementa il routing dinamico
- esegue il bilanciamento del carico
- supporta l'autenticazione dei messaggi
- supporta sistemi gerarchici

Nel **LSA** invia informazioni relative alle interfacce attive ed altre metriche, router all'interno della stessa area condividono lo stesso **DB topologico**, questo genera due tipi di traffico routing;

- Inter-area routing
- Intra-area routing

Il **backbone del OSPF** si occupa di distribuire le informazioni di routing tra le aree, inoltre è fatto ad per operare all'interno di un **AS** infatti è un **intra-AS(IGP)** anche se può inviare e ricevere verso altri **AS**, questi ultimi possono essere divisi in aree, **OSPF distingue tra 4 tipi di router:**

- **Internal router:** router che operano all'interno di un area
- **Area Border router:** router che connettono due o più aree(Approfondimento qua sotto)
- **Backbone router:** router che appartengono alla dorsale(Ovvero l'area 0)
- **Border AS Router:** router posti al confine tra **AS**

ABR(Area Border Router)

Router con più interfacce possono appartenere a più aree allo stesso tempo e prendono il nome **ABR(Area Border Router)** mantengono diversi DB topologici per ogni area

OSPF Virtual Link

In alcuni casi potrebbe essere necessario stabilire una connessione tra due aree OSPF che non possono essere collegate fisicamente, qui entrano in gioco i **Virtual-Links**, vengono stabiliti tra router di backbone che condividono link con aree **non-backbone**

OSPF Packets

Hello Packet

Viene usato per scoprire i **Neighbors(Vicini)**



Usato da **2 router OSPF** vicini per controllare reciprocamente la loro raggiungibilità, se un router non dovesse rispondere, c'è un intervallo chiamato **Router Dead Interval**, dopo il quale se il router contattato non risponde viene considerato inattivo, mentre l'**Hello Interval** è il tempo che passa tra i messaggi di **HELLO**, di solito è di 10 secondi quando un router viene avviato tramite messaggi di tipo HELLO si costruisce la mappa topologica e si definiscono:

- I router adiacenti
- Il **Designed Router (DR)**
- Il **Designed Router di backup (BDR)**

Database Description

Dopo essersi scambiati il messaggio di **HELLO**, questo lo step successivo è lo scambio dei messaggi di **descrizione di un DB**, nello scambio un router fa da **Master** e L'altro da **Slave** e conferma la ricezione di ogni messaggio con una risposta

Link State Request- Link-State Update

Dopo lo scambio dei messaggi di **descrizione dei database** il router invia un messaggio di richiesta dello stato dei collegamenti, ed il vicino gli risponde con le informazioni aggiornate che ha tramite un messaggio di **Link-State Update** una volta ricevuto dall'altro router lo confermerà con **Link State ack**

[[Per la composizione dei pacchetti che molto probabilmente non chiederà andare a slide 399-405]]

Funzionamento OSPF(Opzionale non c'è sulle slide)

Fonte: [OSPF Explained | Step by Step](#)

1. 2 router che usano **OSPF** sulle stesse **link(inteso come collegamento fisico o logico)**, decidono di formare una **Neighbour relationship**
 - 1.1. Ogni router deve scegliere un **RID(router ID)**, riconosce univocamente il router espresso sotto forma di **IPv4**, può essere scelto manualmente o automaticamente(sceglie l'ip di loopback più alto o oppure non di loopback più alto) dal router
 - 1.2. una volta configurati i **RID**, 2 router(**R1 e R2**) **R1** manda un messaggio di **HELLO** ad **R2**, **R2** una volta ricevuto il messaggio da **R1**, controlla che ci siano i requisiti necessari per diventare Neighbors, come l'**id dell'area** che deve essere lo stesso ed altri requisiti
 - 1.3. se i requisiti sono soddisfatti **R2** manda un messaggio di **HELLO** ad **R1** con il proprio **RID** e quello del **R1**, **R1** vedrà se stesso come Neighbor conosciuto
 - 1.4. **R1** allora manderà un altro **HELLO** con **R2** riconosciuto come vicino, ed a questo punto i 2 router sono **ufficialmente Neighbors!**
2. i router che hanno formato una **relazione Neighbour**, scambiano tra di loro le informazioni **LSDB(Link State Database)** usate per calcolare i percorsi di routing, contiene lo stato dei collegamenti di rete, ed in base alle informazioni apprese in seguito allo scambio dei **LSDB**, ogni router deciderà quali informazioni aggiungere al proprio **LSDB**
 - 2.1. presupponendo che la nostra rete OSPF abbia più di due router, presupponiamo 6, vengono eletti un **DR** e **BDR(Presidente e vicepresidente per essere volgari)**, questo per evitare che ci sia uno sciame di pacchetti, infatti tutti i router saranno Full Neighbors solo con il DR se diventa inattivo il BDR
 - 2.1.1. quando viene mandato un aggiornamento da un router ad esempio se una connessione diventa inattiva, lo inoltra a tutti, e viene "ignorato" poi il **DR** lo rimanda e i router ora lo ricevono e aggiornano i loro **LSDB**
 - 2.2. ora torniamo al caso di prima ovvero 2 router, a questo punto uno dei due diventerà **Master** e L'altro **Slave(in base al RID)** **R1** il master controlla lo scambio delle informazioni, ora i router si scambiano tra di loro i **DBD(Database Description)**, se uno dei due router necessita di un'informazione la richiede
 - 2.2.1. ad esempio **R1** nota che c'è un'informazione che gli serve nella **DBD** ricevuta da **R2**, allora la richiedera ad **R2** tramite **un Link state Request**, che gli risponde mandando un **Link State Update**, **R1** confermerà di aver ricevuto le informazioni tramite un **LSAck(Link State Acknowledgment)**

RIP

Si basa sull'algoritmo di **Bellman-Ford**, chiamato anche **Distance-Vector**, ha un limite di **15 hops**, oltre il quale una destinazione è **irraggiungibile(da 16 in poi vede ∞)**, un router che usa **RIP** invia tutta la routing table o una parte di essa(**Triggered Update**) ad i vicini(router distanti 1 hop) ogni 30 secondi è un algoritmo più leggero e semplice da implementare rispetto ad **OSPF** esistono **3 versioni di RIP**

- **RIPv1:** Non supporta le **SubNet mask** vede solo quella predefinita, e non ha autenticazione quindi malintenzionati potrebbero collegare un router ed iniettare route fittizie
- **RIPv2:** Supporta le **SubNet mask**, ed è stata introdotta l'autenticazione
- **RIPng:** supporta indirizzi IPv6

RIP distingue tra interfacce Attive i **router(sono attivi e passivi)** e **Passive gli host**

- **Attive:** inviano istruzioni di routing
- **Passive:** ricevono le informazioni e aggiornano le loro routing table

RIP usa il protocollo [UDP](#) ed usa due meccanismi per ottimizzare l'efficienza e la stabilità di una rete che usa **RIP**:

- **Triggered Update:** obbliga i router a propagare gli aggiornamenti subito senza attendere che i timer si azzerino
- **Split Horizon:** previene l'inoltro di un pacchetto alla stessa interfaccia che lo ha inviato
- **Poison Reverse:** serve ad informare i router di una rottura che non è più disponibile, al posto di cancellare la route dalla propria **routing table** e attendere che venga eliminata tramite il processo di aggiornamento periodico, imposta la distanza di quella route a **16** e la propaga velocizzando il processo di eliminazione questo metodo è anche chiamato **Poison Update**

[Networking Basics - How RIP Works](#) ← se vi interessa, plus per gli esempi che non capirete di gervasi ed altre cose che ho già scritto andare a slide 425 a 427

16° PARTE

-Exterior Gateway Protocol (EGP) dynamic routing protocol -

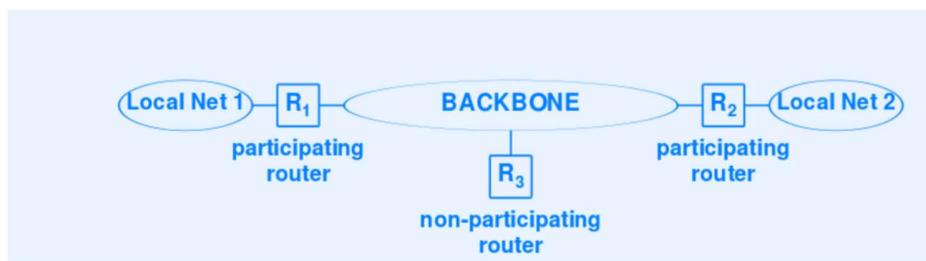
I router di Internet devono essere divisi in gruppi (AS (autonomous system)) per 3 motivi:

- Se ogni organizzazione fosse costituita da una singola rete, non esisterebbe un protocollo di routing in grado di scambiare informazioni di routing in modo efficiente: se il numero di router è grande il traffico diventa insostenibile.
- Poiché non condividono una rete comune, i router di Internet non possono comunicare direttamente
- In una grande rete Internet, le reti e i router non possono essere gestiti tutti da una singola entità e non sono sempre scelti i percorsi più brevi. Poiché le reti sono possedute e gestite da organizzazioni commerciali indipendenti, queste devono poter scegliere politiche differenti.

Ogni gruppo deve poter controllare indipendentemente l'instradamento e l'accesso.

Due sono i problemi che impattano sulla capacità dei router di scambiarsi efficientemente le informazioni di routing:

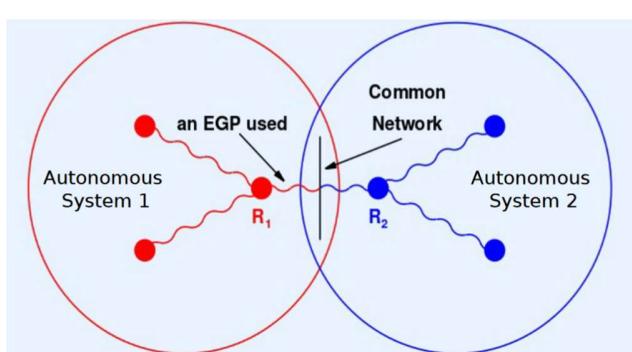
- Il **ritardo**: il tempo che occorre affinché le informazioni aggiornate si propaghino dipende dal numero di router coinvolti, N. Per questo N deve essere mantenuto piccolo.
- L'**overhead**: poiché ogni router deve inviare messaggi per aggiornare le informazioni, maggiore è il numero di router coinvolti, maggiore è il traffico. Siccome i messaggi contengono l'elenco delle possibili destinazioni, anche le dimensioni aumentano al crescere del numero di router.



Se un router esterno ad un gruppo (R3) sceglie un router partecipante ad un gruppo (R1) come default router si generano inefficienze: R3 invierà a R1 anche il traffico destinato alla rete 2 invece che inviare i pacchetti direttamente a R2 (problema del salto extra). Il protocollo ICMP non può risolvere questo problema in quanto esso manda messaggi di diagnostica o errore solamente alla sorgente [immagine sopra]

Ci può servire un protocollo utile per comunicare tra due AS , il:

Border gateway Protocol (BGP)



- I router R1 e R2 sono **peer BGP** uno dell'altro e sono detti **router di confine dei rispettivi Autonomous System**
- I router R1 e R2, attraverso BGP, **annunciano la raggiungibilità** delle reti dei propri AS all'esterno

Caratteristiche di BGP:

- Comunicazione tra AS
- Coordinamento tra più router BGP (iBGP)
- Diffusione delle informazioni di raggiungibilità
- Paradigma del salto successivo
- Supporto delle politiche di routing
- Trasporto affidabile
- Informazioni d'instradamento
- Aggiornamenti incrementali
- Supporto per l'indirizzamento senza classi
- Aggregazione di routes
- Autenticazione

Funzioni di base del BGP

I peer che eseguono il protocollo BGP eseguono **tre funzioni di base**:

- Innanzitutto **i peer si autenticano l'un l'altro** e si scambiano un insieme di messaggi per stabilire la correttezza delle operazioni e se entrambi sono disponibili a comunicare
- Successivamente avviene la fase principale del BGP: ciascuno **invia all'altro le informazioni relative alle reti raggiungibili, fornendo i dati del salto successivo.**
- La terza funzione permette di **verificare** che i peer e la connessione di rete **stanno funzionando correttamente.**

Per eseguire queste tre funzioni, il protocollo BGP definisce un insieme di 5 messaggi:

- Open
- Update
- Notification
- Keepalive
- Refresh

Documentazione del BGP

Diversi sono i **documenti RFC** relativi a BGP, tra i quali:

- RFC 1771—Describe BGP4, la versione corrente di BGP
- RFC 1654—Describe la prima specifica di BGP4
- RFC 1105, RFC 1163, e RFC 1267—Descrivono le versioni precedenti di BGP rispetto a BGP4

I documenti RFC (Request for Comments) sono pubblicazioni ufficiali dell'Internet Engineering Task Force (IETF) e dell'Internet Society (ISOC) che descrivono metodi, comportamenti, ricerche o innovazioni applicabili all'infrastruttura di Internet e alle reti di computer connesse

BGP

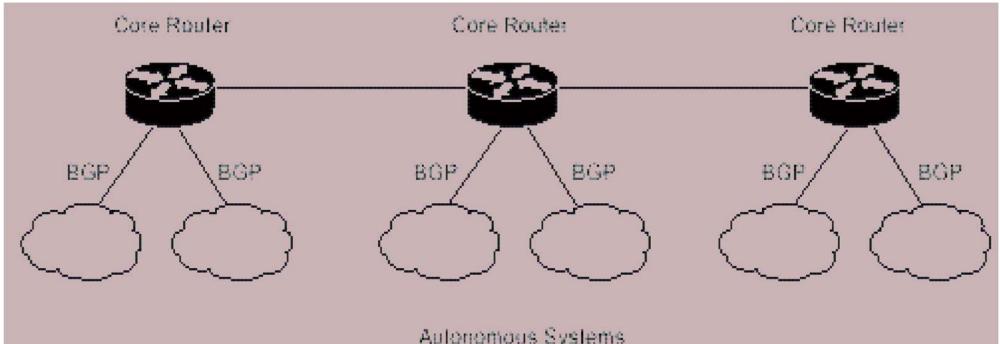
BGP effettua **interdomain routing** in reti TCP/IP.

E' un Exterior Gateway Protocol (EGP) usato per la **comunicazione tra AS**

Si basa su un algoritmo vettore-distanza evoluto

Si occupa del transito di dati di terze parti su una certa rete.

Le reti vengono suddivise in:



- reti **stub**: è una rete che è connessa a un solo sistema autonomo (AS) e non fornisce percorsi di transito verso altre reti
- reti **multi connesse(multihomiging)**: è una rete che è collegata a più di un sistema autonomo (AS). Questa configurazione offre maggiore ridondanza e affidabilità, poiché la rete ha più percorsi alternativi per raggiungere altre destinazioni su Internet
- reti di **transito**: è una rete che non solo è connessa a più AS, ma fornisce anche servizi di transito, permettendo il passaggio del traffico tra diversi AS. Le reti di transito giocano un ruolo cruciale nell'infrastruttura di Internet, facilitando la connessione tra vari segmenti della rete globale. Sono spesso reti di tipo **backbone**

INTER-autonomous system routing:

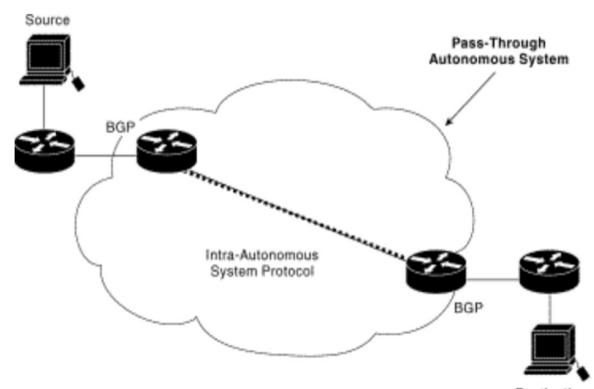
- avviene tra due o più **router BGP appartenenti ad AS diversi**.
- Router vicini (**peers**, o neighbors) usano BGP per mantenere una vista omogenea della topologia della rete.
- Internet usa questo tipo di routing, essendo costituita da entità che appartengono a diversi AS
- BGP è utilizzato in questi casi **per calcolare il percorso che fornisca il routing migliore** attraverso Internet

INTRA-autonomous system routing:

- avviene tra due o più **router BGP appartenenti allo stesso AS (iBGP)**.
- Router vicini usano BGP per mantenere una vista omogenea della topologia del sistema.
- BGP **identifica quale router serve da punto di connessione ottimale per l'interconnessione con specifici AS esterni**.
- Internet usa questo tipo di routing per consentire ad **un'organizzazione** di usare BGP per fornire il **routing ottimale tra i suoi AS**.
- BGP può fornire servizi di routing sia inter- che intra-autonomous system

pass-through autonomous system routing:

- si riferisce alla capacità di un sistema autonomo (AS) di **intradare traffico non destinato a esso, ma che deve attraversarlo per raggiungere la sua destinazione finale**.
Quindi avviene tra due o più router BGP che scambiano traffico attraverso un AS che non esegue BGP



Funzionamento BGP

- BGP usa la porta **TCP 179**

- Due router BGP formano tra loro una connessione TCP (**peer o neighbor routers**), si **autenticano** reciprocamente e scambiano messaggi per aprire e confermare i parametri di connessione.
- I due neighbor all'inizio si **scambiano tutta la loro routing table**, comunicando per ciascuna rete (in formato Classless Inter Domain Routing (CIDR), cioè indirizzo IP/bit subnet mask) il prossimo hop
- Successivamente vengono scambiati **messaggi contenenti gli aggiornamenti sui percorsi modificati**
- BGP verifica continuamente che i partner e le reti stiano funzionando correttamente.
- BGP mantiene le routing tables, trasmette routing update e basa le decisioni di routing sulla base delle routing metric
- Le funzioni primarie sono lo **scambio di informazioni network reachability**, inclusa la lista dei percorsi per gli AS con altri sistemi BGP
- Ogni router BGP **mantiene una lista di tutti i percorsi fattibili verso una particolare rete**. Il router non aggiorna le tabelle fino a che non riceve un aggiornamento incrementale.
- I dispositivi BGP scambiano informazioni di routing sulla base di uno scambio iniziale e successivi aggiornamenti.
- Quando un router si **collega per la prima volta riceve l'intera tabella di routing**. Similmente quando le informazioni cambiano, vengono spedite in forma di insieme di aggiornamenti periodici.
- L'aggiornamento propaga solo il routing ottimale per una certa rete
- BGP **mantiene un numero di versione** della routing table che deve essere lo stesso per il rispettivo peer BGP
- Il numero di versione cambia ogni volta che BGP aggiorna la routing table attraverso aggiornamenti
- pacchetti di tipo keepalive sono inviati per verificare l'integrità della sessione BGP tra i peers
- pacchetti di tipo notification sono inviati in risposta a condizioni di errore o in situazioni speciali
- BGP usa una **routing metric singola**, che consiste in un numero in unità arbitrarie che **specifica il grado di preferenza per quel dato link**. Viene assegnato dal Network Administrator ad ogni link. Il numero assegnato può basarsi su ogni tipo di criterio possibile, incluso il numero di AS che devono essere attraversati, la scalabilità, la velocità, il ritardo della comunicazione, il costo.

messaggi

Il BGP-4 definisce 5 tipi di messaggio:

open message: apre una sessione BGP tra peers ed è il primo messaggio inviato da ciascuna parte dopo l'attivazione della sessione TCP. Questo messaggio è confermato da un messaggio keep-alive del peer e deve essere confermato prima che abbia luogo lo scambio di messaggi ordinario.

keep-alive message: informa ogni sistema peer BGP che un dispositivo è attivo. I messaggi keep-alive sono inviati con una frequenza tale da prevenire che la sessione BGP si esaurisca.

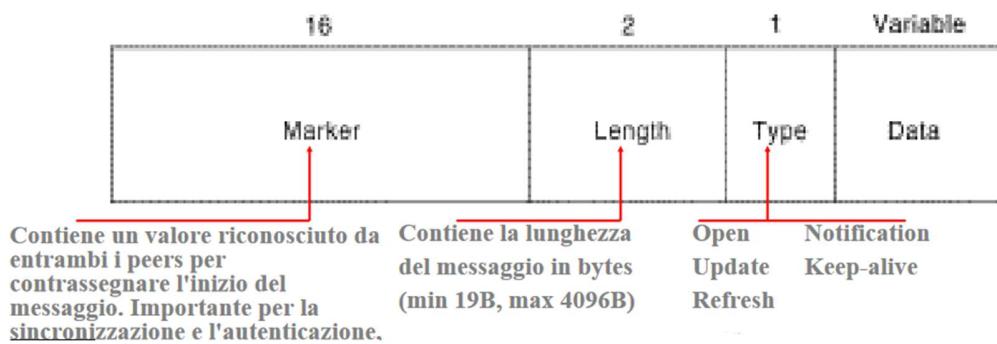
update message: è usato per effettuare l'aggiornamento del routing ad ogni sistema BGP, consentendo ai router di effettuare un disegno consistente della topologia di rete. Gli aggiornamenti sono inviati usando TCP per ragioni di affidabilità. Il messaggio di update può cancellare routes irraggiungibili dalla routing table.

notification message: è inviato quando si evidenzia una condizione di errore. Il messaggio notification è utilizzato per chiudere una sessione attiva e per avvisare i router connessi del perché la sessione viene chiusa

refresh message: richiede il reinvio delle informazioni di routing per una rete da parte di un peer

Header di un pacchetto BGP

Ciascun pacchetto BGP contiene un header la cui funzione principale è quella di **identificare lo scopo del pacchetto** in questione



struttura di un OPEN MESSAGE

Un Open message è costituito da **header + questo blocco** —>

1	2	2	4	1	4
Version	Autonomous System	Hold-Time	BGP Identifier	Optional Parameters Length	Optional Parameters
BGP version number	AS number del mittente	Numero max di secondi di attesa senza ricevimento di messaggi dal trasmettitore	identificativo BGP del mittente (IP address), identico per tutti i peer BGP	Lunghezza del campo parametri opzionali. (se presente)	Lista dei parametri opzionali.

struttura di un UPDATE

MESSAGE

Un Update message è costituito da **header + questo blocco** —>

2	Variable	2	Variable	Variable
Unfeasible Routes Length	Withdrawn Routes	Total Path Attribute Length	Path Attributes	Network Layer Reachability Information
Indica la lunghezza del campo withdrawn routes	Lista di IP riferiti a route irraggiungibili	Lunghezza del campo Path Attribute	Describe le caratteristiche del percorso annunciato: <i>Origin AS path Next Hop Multi Exit Disc Local Pref Atomic aggregate Aggregator</i>	Contiene la lista di prefissi IP riferiti alle route annunciate

struttura di un NOTIFICATION MESSAGE

Un Update message è costituito da **header** + questo blocco →

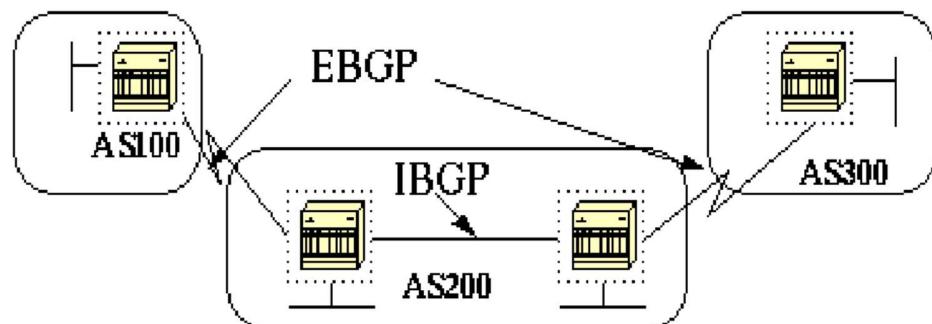
1	1	Variable
Error Code	Error Subcode	Error Data

Indica il tipo di errore:

*Message Header Error,
Open Message Error,
Update Message Error,
Hold Time Expired,
Finite State Machine Error,
Cease*

Fornisce ulteriori informazioni sulla natura dell'errore riportato

Contiene dati relativi all'errore e ai sottocodici di errore. E' un campo usato per diagnosticare la ragione del messaggio



eBGP e iBGP

Si può distinguere tra **eBGP** (peers appartenenti ad AS diversi) e **iBGP** (peers appartenenti allo **stesso AS**):

17° PARTE

(IPv6) Perché un nuovo protocollo IP?

Lo spazio di indirizzamento IPv4 è **prossimo all'esaurimento**, anche se le problematiche relative sono state mitigate dall'adozione delle reti private e dalla combinazione dei protocolli DHCP e NAT.

Un nuovo protocollo IP porterebbe anche a una **migliore gestione del traffico IP e possibilità di gestire QoS** (Quality of Service) e a **uno spazio di indirizzamento più grande** (da 32 bit a 128 bit) con le seguenti caratteristiche:

- Permette una **reale connettività globale**
- **Non più reti o host nascosti**
- **Tutti gli host possono essere raggiungibili** e quindi essere "server"
- E' possibile **usare sistemi di sicurezza Punto-Punto**
- **Autoconfigurazione**
 - Possibilità di usare 64 bits per l'host con la garanzia di unicità
 - Plug and play
 - Possibilità di gestire in modo più semplice il Multihoming
 - Facilità nel Renumbering (rinominazione della rete ?)

Multihoming

Connettere un host o una rete di computer a più di una rete per **aumentare affidabilità** (se un singolo pacchetto fallisce, i pacchetti possono comunque essere instradati attraverso le restanti reti) e **prestazioni** (a seconda della destinazione, potrebbe essere più efficiente instradare attraverso una rete o l'altra)

- **Intestazione del pacchetto IP efficiente ed estendibile**
 - Numero minore di campi nell'header principale
 - efficienza di routing
 - migliori prestazioni
 - Estendibilità dell'header
 - Miglior gestione delle opzioni
 - Eliminata la possibilità di frammentare un pacchetto in transito
- **Caratteristiche intrinseche**
 - Sicurezza
 - Mobilità
 - Maggior utilizzo del Multicast
 - sostituisce il broadcast
 - Uso più efficiente della rete

Header IPv4

Allineamento a 32 bit, i campi in giallo spariscono in IPv6

Ver	I. H. L.	Type Of Ser.	total length			
		Identification	Flag	Fragment offset		
TTL		Protocol	Checksum			
32 bits Source Address						
32 bits Destination Address						
IP Options			Padding			

Header IPv6

Allineato a 64 bit, 40 byte senza le Header Extension

Ver	Traffic Class	Flow Label		
		Payload Length		Next Header
128 bits Source Address		Hop Limit		
128 bits Destination Address				

Principali differenze tra Header IPv4 e Header IPv6

- **Definizione datagramma**

- Pacchetto di dimensioni limitate che contiene gli indirizzi di provenienza e di destinazione del pacchetto e l'indicazione delle risorse e servizi utilizzati. La spedizione del pacchetto non richiede quindi scambi preventivi di messaggi tra i data terminal della sorgente e della destinazione del pacchetto

- **Struttura del datagramma**

- Lunghezza Header

- IPv6

- dimensioni header: 40 byte

- Overhead maggiore

- potenziale riduzione dei dati trasmessi su reti Ethernet

- Forwarding ottimizzato

- IPv4

- dimensioni header: 20 byte

- Indirizzi IP

- IPv6

- Indirizzi composti da 128 bit

- incremento che ha portato a semplificare la parte restante dell'header eliminando alcuni campi e funzionalità del livello di rete

- occupa l'80% dell'header

- indirizzo ip composto da 32 cifre divise da i : in 8 campi da 4

- ogni campo è composto da 16 bit in notazione esadecimale

- il valore è indipendente dalla notazione maiuscola o minuscola delle lettere

- gli zero a sinistra di ogni campo sono opzionali

- campi successivi di zero sono rappresentati da ::, ma solo **una volta in un indirizzo**
[Esempi di indirizzi IPv6 nelle slide 474 e 475]

- In una URL devono essere scritti fra parentesi quadre

- Programmi che usano URL sono stati modificati allo scopo

- scomodo per gli utenti

- prevalentemente usato per scopi diagnostici

- più comodo usare una notazione per nome a dominio

- IPv4

- indirizzi composti da 32 bit

- **Eliminazione del campo lunghezza header**

- IPv6

- non è presente il campo che specifica la lunghezza dell'header

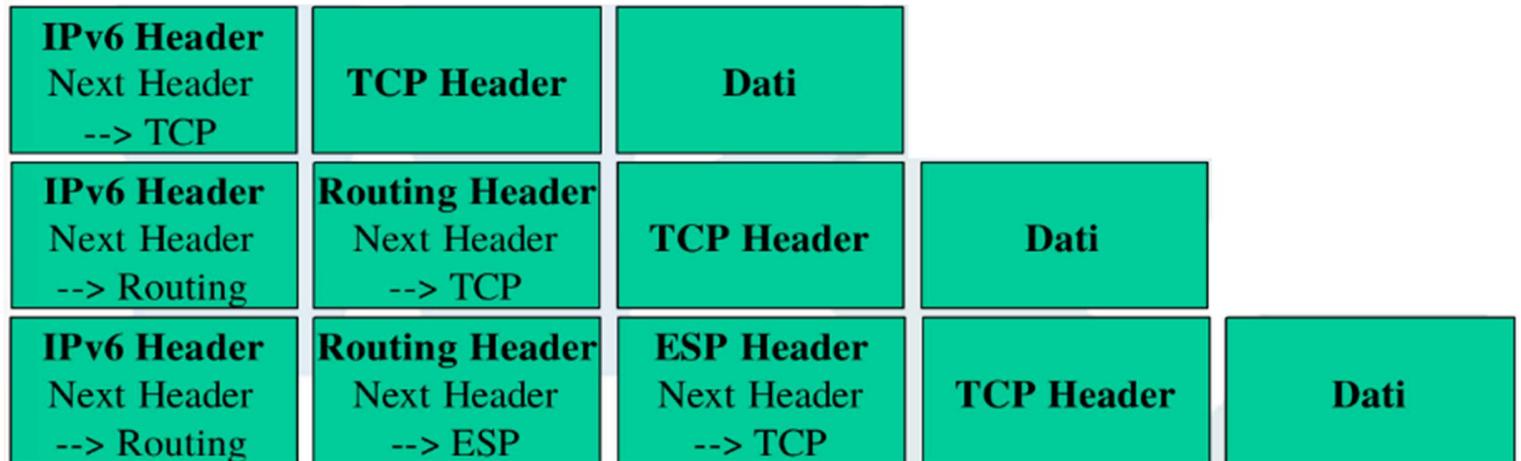
- lunghezza minima fissa

- meccanismo di estensione header modificato

- elaborazione dei pacchetti da parte dei router semplificata

- **Eliminazione della frammentazione**
 - IPv6
 - funzione eliminata
 - nodi finali responsabili della frammentazione
 - migliori tempi di elaborazione dei pacchetti
 - IPv4
 - possibilità di frammentare i pacchetti più grandi per adattarli
- **Estensione Header**
 - IPv6
 - può aggiungere funzionalità opzionali ai datagrammi
 - routing più efficiente
- **In sintesi**
 - IPv6
 - maggiore spazio di indirizzi
 - la struttura semplificata e l'eliminazione della frammentazione migliorano le prestazioni di routing
 - le estensioni header forniscono maggiore flessibilità per future implementazioni di nuove funzionalità

Extension header



Tipi di header

- **Hop-by-hop option (00)**
 - Queste informazioni devono essere esaminate da ogni nodo lungo il percorso del pacchetto
 - Usato per i router alert ed i Jumbogram (pacchetto a livello internet che supera l'unità di trasmissione massima standard)
- **Routing (43)**
 - Simile all'opzione IPv4 loose source route (traduzione degli indirizzi (?)
 - Indica una lista di router da attraversare
 - Usato per il mobile IPv6

- **Fragment (44)**
 - Usato soltanto dall'host mittente per l'host destinatario
- **Destination option (60)**
 - Usato per trasportare informazioni opzionali che saranno valutate soltanto dall'host destinatario
 - Usato per il mobile IPv6
- **Authentication Header (51)**
 - Fornisce l'autenticazione; un modo per verificare che l'indirizzo del mittente sia autentico e che il pacchetto non sia stato alterato durante il percorso
- **Encapsulating Security Payload (50)**
 - Garantisce che solo il destinatario autorizzato sarà in grado di leggere il pacchetto
- **Ordine header:**
 - IPv6 header
 - Hop-by-Hop Options header
 - Destination Options header (quando è presente un routing header)
 - Routing header
 - Fragment header
 - Authentication header
 - Encapsulating Security Payload header
 - Destination Options header
 - Upper-layer header

Tipi di indirizzi

- **Unicast**
 - Unspecified
 - Loopback
 - Indirizzi Scoped
 - Link local
 - Site local
- **Aggregatable Global**
- **Multicast**
 - Broadcast non esiste in IPv6
- **Anycast**

Subnet Prefix e Host identifier

L'indirizzo IPv6 unicast è diviso in **2 parti**:

- Primi 64 bit identificano il prefisso di rete
- Ultimi 64 bit identificano l'host
- 0:0:0:0 : 0:0:0:0 (prima parte rete, seconda parte host)
- L'host può essere identificato:
 - manualmente 0,1,2,3 etc.
 - Usando l'identificativo di interfaccia MAC o EUI 48. Viene ricalcolato per essere usato come parte host dell'indirizzo IPv6 - EUI 64

Indirizzo Unspecified

- Indica l'assenza di indirizzo
- Può essere usato nella richiesta iniziale DHCP per ottenere un indirizzo

Indirizzo di Loopback

- Identifica l'host stesso
- è il localhost
 - 127.0.0.1 (IPv4)
 - 0:0:0:0:0:0:1 o ::1 (IPv6)

Indirizzo Link local

- E' uno scoped address (novità di IPv6) (? fai approfondimento)
- Scope (ambito) = local link (i.e. LAN,VLAN)
 - può essere usato solo fra nodi dello stesso link
 - non può essere instradato dai router
- Automaticamente configurato su ogni interfaccia
 - Usa l'interface identifier (approfondisci)
- Formato
 - FE80:0:0:<interface identifier>
- Fornisce ad ogni nodo un indirizzo IPv6 per iniziare le comunicazioni

Indirizzo Site local

- E' uno scoped address
- Scope = site (una rete di link)
 - può essere usato soltanto fra nodi dello stesso site
 - Non può essere usato fuori dal site (es.Internet)
 - Molto simile agli indirizzi privati IPv4
- Non configurato di default
- Formato:
 - FEC0:0:0:<subnet id>:<interface id>
 - Permette un piano di indirizzamento per un intero sito
- Esempi d'uso:
 - Numerare un site prima di connetterlo a internet
 - Indirizzamento privato (es. stampanti locali)

Aggregatable Global

La politica dell'assegnazione di indirizzi IPv6 deve essere profondamente diversa da quella di IPv4 considerata l'abbondanza di indirizzi IPv6

Come best practice si adotta la seguente strategia:

- /23 → regional register
- /35 → Local internet register
- /48 → organizzazioni (utenti finali)
- /64 → sottoreti degli utenti

Multicast

- Uno a tanti
- Non esiste il broadcast in IPv6. Multicast è usato al suo posto, soprattutto nei link locali
- Scoped address:
 - Node, link, site, organization, global
 - sostituisce il TTL dell'IPv4
- Formato:
 - FF<flags><scope>>::<multicast group>
 - Flag = 0 permanente / 1 temporaneo (non so cosa significa)

Indirizzi multicast riservati

Address	Scope	Use
FF01::1	Interface-local	All Nodes
FF02::1	Link-local	All Nodes
FF01::2	Interface-local	All Routers
FF02::2	Link-local	All Routers
FF05::2	Site-local	All Routers
FF02::1:FFXX:XXXX	Link-local	Solicited-Node

Anycast

- Uno al più vicino: serve per le funzioni di discovery
- Gli indirizzi Anycast non sono distinguibili dagli indirizzi Unicast
 - allocati dallo stesso spazio di indirizzamento unicast
 - ultimi 64 bit formati da serie di 1 e ultimi 7 bit dell'indirizzo (diversi se EUI64 o non EUI 64)
- Alcuni indirizzi anycast sono riservati per usi specifici:
 - Router subnet
 - Mobile IPv6 home agent discovery

Indirizzi per ogni host

Ogni host IPv6 dovrebbe riconoscere i seguenti indirizzi come identificanti se stesso:

- Indirizzo Link - local per ogni interfaccia
- Indirizzi unicast/anycast assegnati (manualmente o automaticamente)
- Indirizzo di Loopback
- Indirizzo del gruppo all-nodes multicast
- Indirizzi SOlicited-node multicast per ogni indirizzo unicast e anycast assegnato
- Indirizzi Multicast di tutti gli altri gruppi di cui l'host faccia parte

Come l'host seleziona un indirizzo

Un nodo ha molti indirizzi IPv6 e, per scegliere quale sarà usato come sorgente e destinazione per ogni flusso, si seguono queste regole:

- Usare il giusto scope (ambito) in base alla destinazione (global, site, local)
- Usare l'indirizzo più simile alla destinazione (IPv4, IPv6)

L'algoritmo di scelta può essere sovrascritto dall'applicazione o dai protocolli dello Stack TCP/IP

18° PARTE

Telnet

Telnet è un servizio di rete che emula un terminale a carattere (ASCII). È definito dalle specifiche RFC854 e RFC855. Ecco alcuni punti chiave:

1. Funzione di Telnet:

- Telnet consente l'accesso remoto a un sistema tramite la rete.
- Si basa sul protocollo TCP per garantire una connessione affidabile.

2. Client Telnet:

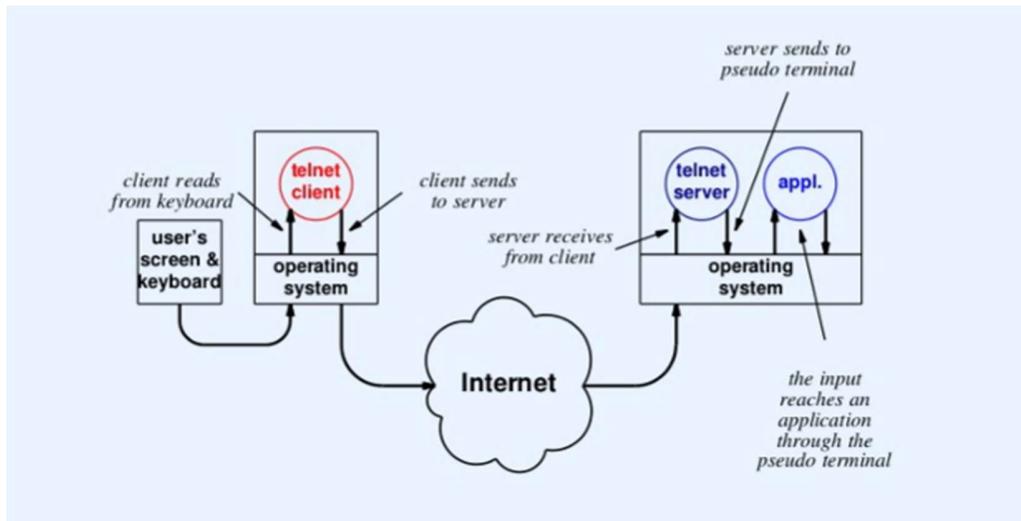
- Il client Telnet viene invocato dall'utente.
- Si connette a un server Telnet in esecuzione su un altro host tramite la porta 23.
- Trasmette i caratteri digitati dall'utente al server e visualizza l'output del comando eseguito dal server sulla finestra dell'utente.

3. Server Telnet:

- Accetta connessioni di rete dai client Telnet.
- Trasmette i caratteri digitati dall'utente al sistema operativo come se fossero digitati localmente.
- Invia l'output della sessione sulla connessione del client.

4. Questo servizio si basa su 3 aspetti:

- **Network Virtual Terminal (NVT)**: Un terminale virtuale con caratteristiche generali. Server e client traducono i controlli nativi in quelli del NVT, consentendo l'uso di Telnet senza strumenti specifici.
- **Opzioni negoziate**: Client e server negoziano opzioni per migliorare le funzionalità della sessione Telnet.
- **Viste simmetriche**: Consentono l'interazione tramite programmi anziché tastiera e monitor fisici.
- **Attenzione**: La negoziazione delle opzioni può generare cicli infiniti (errata interpretazione).



Rlogin

Rlogin è un protocollo di rete utilizzato principalmente nei sistemi BSD Unix. Ecco una breve sintesi:

1. **Scopo di rlogin:**

- Inventato per i sistemi BSD Unix.
- Include facilitazioni specifiche per l'ambiente Unix.

2. **Funzionalità chiave:**

- **Accesso senza password:** Permette all'amministratore di configurare più macchine in modo che se un utente ha lo stesso identificativo su queste macchine, l'accesso avvenga senza digitare la password.
- Questa soluzione semplifica la configurazione di ambienti distribuiti, ma comporta gravi problematiche di sicurezza.
- **Altre forme di autenticazione:** rlogin supporta anche altre modalità di autenticazione.

Remote shell

Remote shell (rsh) è simile a **rlogin** ed è anch'esso parte dei sistemi BSD Unix. Ecco una breve sintesi:

1. **Funzionalità di rsh:**

- Permette l'esecuzione remota di un singolo comando.
- L'esito del comando viene visualizzato nella finestra dell'utente nel sistema locale.
- È necessaria un'applicazione che consenta l'accesso da terminale a carattere per utilizzare rsh.

Port forwarding

E' una nuova funzionalità implementata da ssh (secure shell) simile al Network Address Translation (NAT), Permette di instradare connessioni TCP in un canale cifrato.

Il Remote Desktop

Il **Remote Desktop** è una tecnologia che consente agli utenti remoti di accedere a un computer e visualizzare la sua interfaccia grafica (GUI) su un altro dispositivo. Ecco alcuni punti chiave:

- **Accesso Grafico:** A differenza delle connessioni testuali o della riga di comando, il Remote Desktop offre un'esperienza grafica completa. Gli utenti possono vedere il desktop, le finestre e utilizzare mouse e tastiera come se fossero fisicamente presenti davanti al computer remoto.
- **Esempi di Protocolli:** Ci sono diversi protocolli utilizzati per implementare il Remote Desktop:
 - **Virtual Network Computing (VNC):** VNC è un protocollo open-source che consente di visualizzare e controllare il desktop di un computer remoto. È ampiamente utilizzato per l'accesso a distanza su diverse piattaforme.
 - **Remote Desktop Protocol (RDP):** RDP è un protocollo sviluppato da Microsoft per il suo sistema operativo Windows. Consente agli utenti di accedere a un computer Windows da un altro dispositivo Windows o anche da dispositivi non Windows utilizzando client RDP compatibili.

L'obsolescenza di Telnet

L'**obsolescenza di Telnet** è dovuta principalmente alla sua mancanza di sicurezza. Telnet trasmette i dati in chiaro, il che significa che le informazioni, inclusi nomi utente e password, possono essere intercettate da chiunque "sniffi" la rete. Questo rende Telnet vulnerabile agli attacchi di tipo "man-in-the-middle".

In molti sistemi moderni, Telnet è stato disabilitato o bloccato. Se si tenta di eseguire il comando Telnet, si otterrà un messaggio di errore simile a quello che hai mostrato.

Al posto di Telnet, si utilizza **SSH (Secure Shell)**. SSH cifra le informazioni trasmesse, garantendo una comunicazione sicura tra client e server. È ampiamente utilizzato per l'accesso remoto e la gestione di server.

Per gli utenti Windows, una soluzione comune è **PuTTY**, un client SSH gratuito e facile da usare. In ambiente Unix e Linux, si dispone di **OpenSSH**, che è incluso di default e offre funzionalità avanzate per l'accesso remoto sicuro.

FTP (File Transfer Protocol)

Protocollo per il trasferimento di file tra host in una rete TCP/IP (RFC 959)

Essendo basato sul protocollo di trasporto TCP è orientato alla connessione ed è affidabile

In ogni trasferimento dati intervengono 2 processi:

- Il Data Transfer Process (DTP) che si occupa del trasferimento vero e proprio tra un client e un server FTP
- Il Protocol Interpreter che si occupa di trasmettere comandi fra il client e il server FTP (dà inizio al processo FTP)

Sessione FTP:

- Una sessione FTP si compone di **due connessioni** bidirezionali:
 - La **prima** è la **sessione di controllo**, creata tra il server e il client. Il client stabilisce una connessione verso il server tramite la **porta 21**.
 - Alla richiesta di trasferimento dati, il **server DTP** (Data Transfer Process) apre una connessione apposita sulla **porta 20** con il **client DTP**. Durante questa fase, la sessione di controllo rimane attiva.

Sessione anonima:

- In una sessione anonima, l'account utilizzato è “**anonymous**”, e la password di solito corrisponde all'indirizzo email.
- I client hanno **solo diritto di lettura**, impedendo l'upload non autorizzato di dati sul server.

funzionamento:

il client contatta il server specificando i file e la direzione del trasferimento (scaricare/caricare). Il server mantiene i file localmente, accetta connessioni e soddisfa le richieste dei client. Le caratteristiche includono accesso interattivo, specifica del formato dei file (ASCII o EBCDIC) e controllo dell'autenticazione tramite login e password.

data transfer

Per il Data Transfer il client diventa server ed il server diventa client:

Il Client: Crea il processo per gestire il trasferimento dati, alloca la porta e invia il numero al server attraverso la connessione di controllo, Il processo nel frattempo attende richieste.

Il Server: Riceve le richieste, crea il processo per gestire il trasferimento dati ed infine il processo contatta il lato client.

All'inizio il protocollo FTP era usato da linea di comando.

Oggi: Gran parte delle richieste FTP originano da browser.

Comandi importanti FTP

I **comandi** FTP sono utilizzati per controllare l'accesso, configurare i parametri del trasferimento e gestire directory e file. Per stabilire e terminare una sessione FTP, si usano i comandi **OPEN** per connettersi al server, **USER** per specificare l'utente, **PASS** per la password e **QUIT** per terminare la sessione. Per configurare i parametri del trasferimento, si utilizzano i comandi **PORT** per specificare l'indirizzo IP e la porta e **PASV** per attivare la modalità passiva. Per il trasferimento dei file, si usa il comando **TYPE** per specificare il tipo di file (ascii o binario), **RECV** o **GET** per scaricare un file dal server e **SEND** o **PUT** per caricare un file sul server.

Per la gestione di directory e file, si utilizzano comandi come **DELETE** per eliminare un file remoto, **CD** per cambiare la directory corrente, **MKDIR** e **RMDIR** per creare o eliminare directory e **LS** o **DIR** per elencare i file nella directory corrente. Ad ogni comando inviato dal client FTP, il server risponde con appositi codici di risposta.

Per quanto riguarda la sicurezza, nelle versioni iniziali di FTP le password venivano trasferite in chiaro. Con l'introduzione di RFC 2228, sono stati introdotti nuovi comandi per aumentare la sicurezza, come **AUTH**, che consente al client di specificare il meccanismo per il trasferimento protetto delle informazioni.

Sicurezza di telnet e FTP

Telnet e **FTP** presentano il rischio di trasmettere dati sensibili in chiaro attraverso la rete, esponendo le informazioni come login, password e altri dati a possibili violazioni. È preferibile utilizzare versioni che utilizzano protocolli di

crittografia come SSH (Secure Shell) e SCP (Secure Copy) per scambiare dati in modo cifrato, offrendo maggiore sicurezza. Tuttavia, l'uso di SSH e SCP comporta un aumento del carico computazionale sia sul server che sul client. Molte implementazioni di client software per questi servizi consentono di utilizzare le versioni sicure. Inoltre, i socket SSH e SCP spesso vengono lasciati aperti sui firewall per consentire il passaggio sicuro dei dati.

Trivial File Transfer Protocol (TFTP)

Trivial File Transfer Protocol (TFTP) è un'alternativa più semplice a FTP, utilizzata principalmente per la copia di file interi con minori funzionalità rispetto a FTP. Il codice di TFTP è più leggero ed è pensato per essere utilizzato principalmente in reti locali (LAN). Funziona tramite UDP (User Datagram Protocol) e viene spesso utilizzato da macchine Diskless per ottenere l'immagine di avvio (bootstrap).

Crittografia

La tecnologia di crittografia si divide principalmente in due categorie: simmetrica e asimmetrica.

1. Crittografia Simmetrica (o Private Key Encryption):

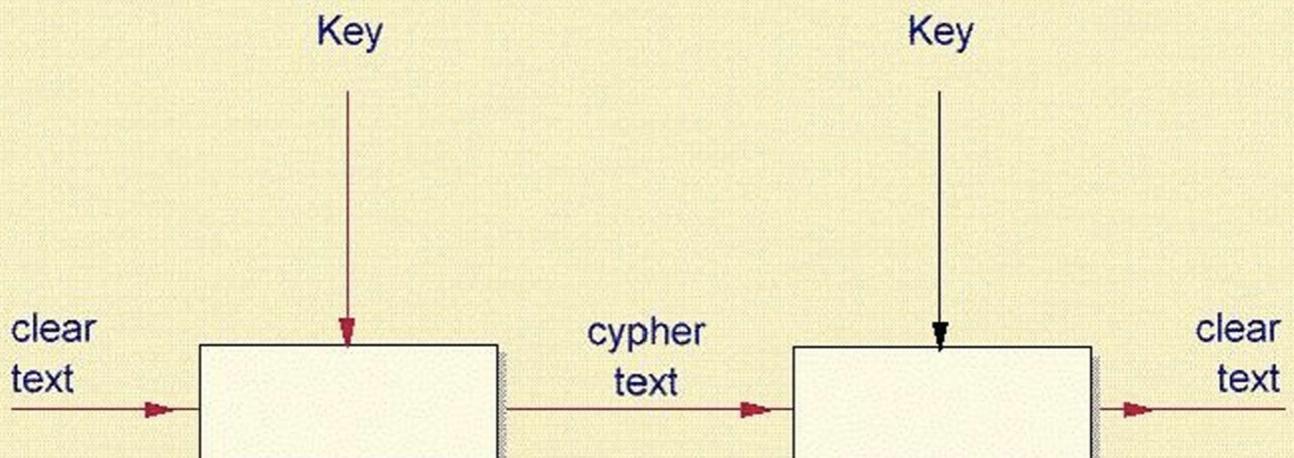
- Utilizza la stessa chiave per cifrare e decifrare i dati.
- Entrambi i partner devono condividere la stessa chiave segreta.
- Esempi includono il Data Encryption Standard (DES), l'Advanced Encryption Standard (AES) e Blowfish.

2. Crittografia Asimmetrica (o Public Key Encryption):

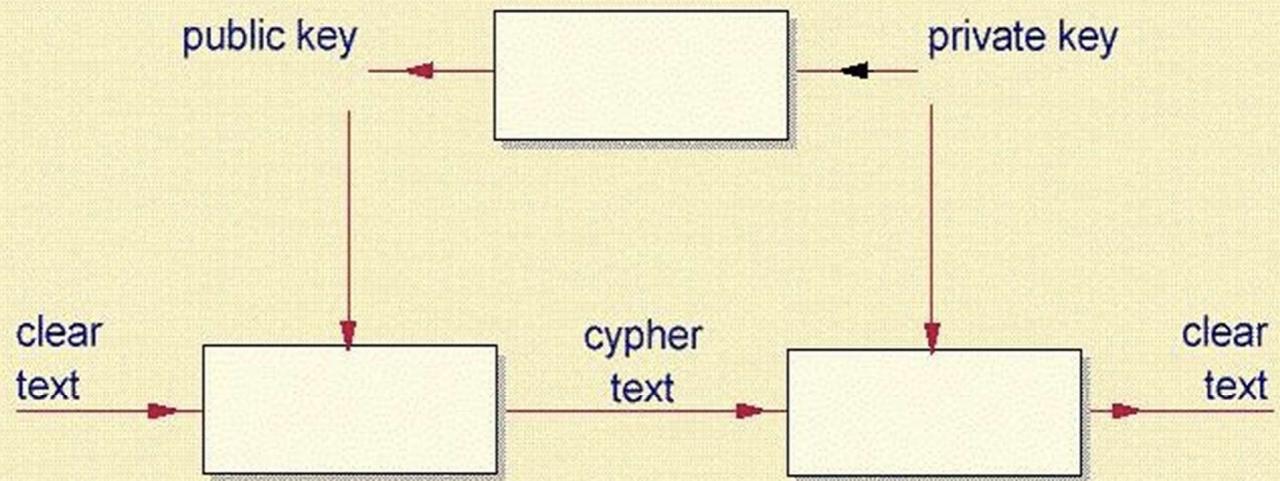
- Coinvolge una coppia di chiavi uniche per ogni utente: una chiave pubblica e una chiave privata.
- La chiave pubblica viene distribuita liberamente, mentre la chiave privata è mantenuta segreta dall'utente.
- La chiave pubblica viene utilizzata per cifrare i dati e la chiave privata corrispondente viene utilizzata per decifrarli.
- Un esempio comune è l'algoritmo RSA.

La **crittografia simmetrica** è efficace per la trasmissione di grandi quantità di dati, mentre la **crittografia asimmetrica** è utile per garantire la sicurezza delle comunicazioni senza richiedere la condivisione diretta delle chiavi segrete.

esempio **crittografia simmetrica**:



esempio di crittografia asimmetrica:



crittografia asimmetrica:

Riservatezza: Sì

Autenticazione: Sì

Non ripudio: No

Crittografia asimmetrica (firme digitali):

Riservatezza: No

Autenticazione: No

Non ripudio: Sì

Crittografia asimmetrica (firme digitali e riservatezza):

Riservatezza: sì

Autenticazione: sì

Non ripudio: sì

OPEN SSH

Questo software supporta i protocolli SSH1 e SSH2. Si tratta di una versione gratuita sviluppata nell'ambito del **progetto OpenBSD**, basata sulla libreria crittografica OpenSSL. Questo significa che molte delle sue funzionalità crittografiche dipendono dalla libreria OpenSSL, che non è regolata dalla licenza GNU Public License (GPL) e pertanto non è considerata software libero. Il protocollo SSH è disponibile in due versioni, SSH1 e SSH2, che sono incompatibili tra loro.

comando per la generazione della chiave: ssh-keygen

OpenSSH è una implementazione open source del protocollo SSH. Supporta entrambe le varianti principali della versione 1 di SSH: la 1.3 e la 1.5. Queste versioni utilizzano l'algoritmo di crittografia asimmetrica RSA per la negoziazione delle chiavi, insieme agli algoritmi simmetrici 3DES, AES e Blowfish per crittografare i dati. Tuttavia, non supporta l'algoritmo simmetrico IDEA a causa dei brevetti in alcuni stati. Per verificare l'integrità dei dati, OpenSSH utilizza un semplice algoritmo di Controllo di Ridondanza Ciclica (CRC).

SSH 2 è stata introdotta come una soluzione per superare le limitazioni dei brevetti legati a RSA e per risolvere problemi associati all'algoritmo CRC utilizzato in SSH1. Utilizza gli algoritmi asimmetrici Digital Signature Algorithm (DSA) e Diffie-Hellman (DH), entrambi privi di brevetti. In SSH2, al posto dell'algoritmo CRC, si utilizza l'algoritmo di autenticazione dei messaggi HMAC (Keyed-Hash Message Authentication Code). Inoltre, molte delle funzionalità di SSH2 si basano sulla libreria crittografica OpenSSL.

Gestione delle chiavi

La gestione delle chiavi in SSH avviene nel seguente modo:

- Le chiavi pubbliche e private sono memorizzate in file ASCII nella directory \$HOME/.ssh, con permessi di accesso 700.
- Nella stessa directory viene salvato il file known_hosts, contenente le chiavi pubbliche dei server ai quali ci si è collegati.
- Per gli host i cui chiavi pubbliche sono salvate nel file authorized_keys, non viene richiesta la password al momento del login.
- Alcuni software SSH permettono di gestire le chiavi pubbliche e private attraverso un certificato X.509.

OpenSSH è una suite di programmi che include:

- **ssh**: Sostituisce rlogin e telnet, consentendo connessioni sicure tramite SSH.
- **scp**: Sostituisce rcp per il trasferimento sicuro di file tramite tunnel SSH.
- **sftp**: Sostituisce ftp per il trasferimento sicuro di file tramite tunnel SSH.
- **sshd**: Il programma sshd è il demone che funziona sul server per gestire le richieste SSH dei client
- **ssh-add, ssh-agent, ssh-keygen**: Programmi di utilità per la gestione delle chiavi SSH.
- **sftp-server**: Daemon per il server SFTP, che consente il trasferimento di file in modo sicuro.

19° PARTE

DNS (Domain Name System)

Tendiamo a preferire i nomi agli indirizzi numerici e si deve garantire che ogni nome mnemonico identifichi univocamente un host, per cui si fissa una politica di gestione dello spazio dei nomi con un'autorità che garantisce l'applicazione della politica.

Ci sono due possibilità:

- Spazio dei nomi **piatto**
 - sequenza di caratteri senza alcuna ulteriore struttura
 - Il Network Information Center amministra lo spazio di denominazione e stabiliva se un nuovo nome era appropriato (proibiva nomi osceni o nomi in conflitto con quelli esistenti)
 - Vantaggio
 - nomi brevi
 - Svantaggi
 - non si può generalizzare questo schema a molte macchine per motivi sia tecnici che amministrativi
 - costo elevato per mantenere copie corrette dell'intero elenco di ciascun sito (e cresce se aumenta il numero di siti)
 - difficile da gestire e da consultare quando la rete è grande
- Spazio dei nomi **gerarchico**
 - spazio dei nomi diviso in zone (detto domini)
 - Per ogni dominio viene definita un'autorità di dominio per consentire la decentralizzazione della tabella
 - Migliore gestione
 - 2 possibili soluzioni:
 - Suddivisione in base alla topologia della rete
 - Suddivisione per organizzazione, pertanto indipendente dalle interconnessioni fisiche delle reti

Internet usa una sua suddivisione per organizzazione

- è utilizzato da tutti (è uno schema universale di denominazione)
- Ogni organizzazione definisce liberamente la struttura interna

- Si usa un insieme di parole separate da un campo delimitatore, **il punto**
 - dmi.unipg.it
 - unipg.it (è a sua volta un dominio)

Il top level domain è .it

TLD (Top level domain)

I domini di primo livello arrivano alla fine dei nomi di dominio e sono importanti per la classificazione dei nomi di dominio, **essenziali per le ricerche DNS**

L'RFC 2606 definisce alcuni domini riservati per evidente significato intrinseco:

- **.example**
- **.invalid**
- **.localhost**
- **.test**

ICANN (Internet Corporation for Assigned Names and Numbers)

E' un ente di gestione internazionale per proseguire i numerosi incarichi di gestione relativi alla rete Internet che in precedenza erano demandati ad altri organismi

Ha l'incarico di assegnare gli indirizzo IP e come identificatore di protocollo e di gestione del sistema dei nomi a dominio di primo livello

IANA (Internet Assigned Numbers Authority)

Organismo dell'ICANN

Ha la responsabilità nell'assegnazione degli indirizzi IP

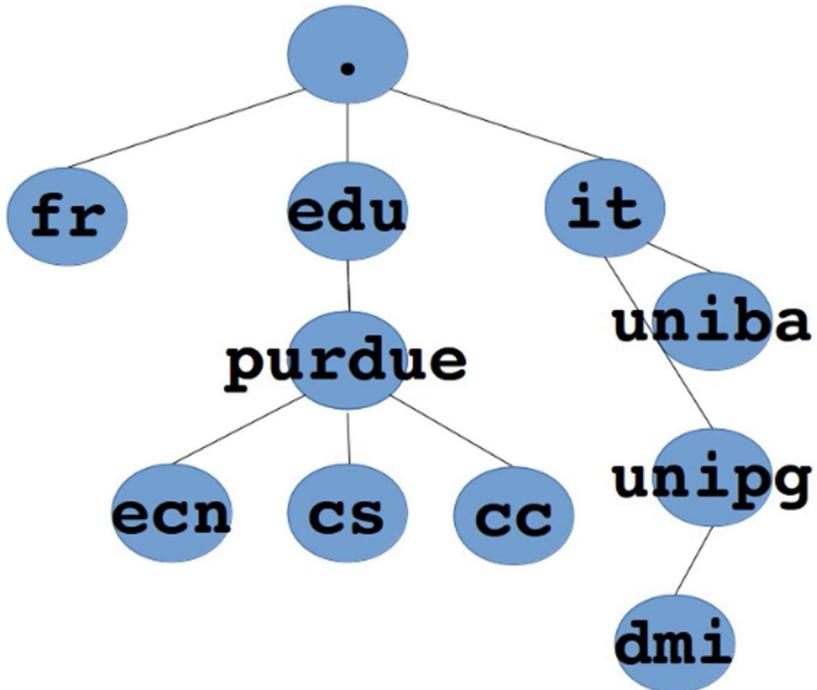
Mantiene un registro dei protocolli utilizzati su Internet

IANA ha suddiviso i TLD in **3 categorie**:

- **ccTLD**
 - lista dei paesi del mondo
- **gTLD**
 - generic TLD, usati da particolari organizzazioni (.com .mil .edu .gov)
- **Infrastrutturali**
 - l'unico è .arpa usato nella risoluzione inversa dei nomi

Si pensava che senza l'aggiunta di nuovi nomi, il DNS sarebbe collassato. Ora il proliferare dei nomi sta creando grossi problemi legali. Diventa impossibile proteggere un brand in questo modo.

TLDS



Autorità responsabili dei nomi

es.

UNIPG si registra presso un ente preposto e diventa responsabile del nome **.unipg.it**

DMI chiede all'università la registrazione del dominio **.dmi.unipg.it** e diventa responsabile di tale dominio ottenendo così la **delega amministrativa e tecnica**. L'amministratore di rete è responsabile dell'assegnazione dei nomi e degli indirizzi e della loro memorizzazione

I singoli soggetti che hanno bisogno di un nome a dominio (es. per un server) contattano l'amministratore di rete del dip perché gli assegna un indirizzo IP ed un nome e di gestire la registrazione del nuovo nome e indirizzo mediante il DNS.

Database DNS

Il database mantenuto dal DNS è costituito da:

- record
- nomi
- classi

Un nome può essere associato a diverse classi (host, mail, exchange, server DNS etc) dal database DNS

Pertanto è possibile associare ad ogni interfaccia di rete (su reti di tipo TCP/IP, ad ogni IP address) un nome (**hostname**). Si fa questo poiché i nomi sono più facili da ricordare e da scrivere correttamente rispetto agli indirizzi numerici.

Es: 141.250.1.7. oppure teseo.unipg.it

Quasi sempre gli indirizzi numerici e i nomi sono intercambiabili, ma in tutti i casi prima di effettuare una connessione il sistema **converte l'hostname in un IP address**.

La traduzione di nomi in indirizzi deve essere nota a tutti gli host della rete.

Risoluzione nome-indirizzo IP statica

Attraverso una **host table** (memorizzata su un semplice file ASCII) viene stabilito **una volta per tutte** l'associazione (mapping) tra indirizzo IP e hostname.

Indirizzo IP	Hostname	Alias
192.168.130.1	moe.unipg.it	moe
192.168.132.2	larry.unipg.it	Larry
192.168.130.40	omniw.unipg.it	omniw
192.168.132.20	pserver.unipg.it	pserver
192.168.132.45	powerbook.unipg.it	powerbook

Risoluzione nome-indirizzo IP dinamica

L'associazione (mapping) tra indirizzo IP e hostname viene stabilito dinamicamente.

Ogni host all'avvio **richiede ai server DNS le informazioni sui nomi da assegnare alle proprie interfacce** e attraverso appositi file di configurazione **ogni host sa quali server interrogare e i server quali nomi assegnare**.

Esempio UNIX

In ambiente UNIX esiste una implementazione dei protocolli del DNS: **Berkeley Internet Name Domain (BIND)**

BIND è un package di software comprendente:

- **i principali componenti del DNS** tra cui
 - un server DNS (named)
 - BIND SERVER, processo demone (programma eseguito in background) in grado di servire le richieste del resolver, il quale deve essere in esecuzione sull'host locale
 - una libreria di risoluzione di DNS (resolver)
 - BIND CLIENT, libreria di funzioni che permette di generare e inviare al server le richieste di informazioni sui nomi dei domini
- **Strumenti per la verifica del corretto funzionamento del server DNS** (dig o nslookup)

La configurazione del BIND (sia lato client che server) avviene **tramiti specifici file di testo** che ne descrivono il tipo di servizio fornito.

Configurazione del resolver (BIND client)

- Le funzioni del resolver sono configurate nel file **/etc/resolv.conf**
- Contiene una serie di istruzione per l'esecuzione delle richieste e viene letto all'avvio del processo che usa il resolver

Voci da inserire nel file:

- **nameserver address**
 - le richieste vengono inviate all'indirizzo IP *address* specificato. Si possono specificare più *nameserver* fino ad un max di 3, se il primo non risponde entro un tempo prestabilito, la richiesta viene passata al secondo e così via.
- **domain name**
 - definisce il nome di dominio di default. Il resolver aggiunge *name* a qualsiasi nome host che non contiene il carattere punto.
 - es:
 - dominio: dipmat.unipg.it
 - host: cartesio.dipmat.unipg.it
 - per accedere a questo servizio basta specificare il nome cartesio, il resolver aggiungerà il resto.
- **search domain1, domain2, ... domain**
 - ha la stessa funzione di *domain* con la possibilità di avere più domini da provare ad aggiungere al nome dell'host. La **differenza** con *domain* è che **viene aggiunto solo l'intero nome dei domini indicati**

Esempio del file di configurazione del resolver

```
# cat /etc/resolv.conf
search dmi.unipg.it unipg.it
nameserver 141.250.1.7
nameserver 141.250.1.6
```

Per verificare il corretto funzionamento:

```
# host teseo
teseo.unipg.it is 141.250.1.7
```

Zone files

E' un file ASCII che descrive una zona DNS. **Una zona DNS** è un sottoinsieme, spesso un singolo dominio, della struttura dei nomi di dominio gerarchici del DNS. Lo zone file contiene mappature tra nomi di dominio e indirizzi IP e altre risorse, organizzate sotto forma di rappresentazione testuale dei **record di risorse (RR)**. Uno zone file può essere un file master DNS, che descriva in modo autorevole una zone o può essere utilizzato per elencare il contenuto di una cache DNS. Hanno un formato fisso ed uno stesso metodo per definire i record di un dominio.

I principali componenti di un zone file sono detti **standard resource record (RR)**:

- **SOA**
- **NS**
- **A (AAAA per IPv6)**
- **PTR**
- **MX**
- **CNAME**

Formato Resource Record RR

[name] [ttl] in **type data**

- **name**
 - nome di uno *specifico host* op di un *dominio* a cui il RR si riferisce; generalmente si utilizza il carattere @ per riferirlo al dominio che viene definito dallo zone file stesso.
- **ttl**
 - time to live, definisce il tempo massimo (in secondi) oltre cui l'informazione nel RR non può essere considerata valida in una cache di un sistema remoto
- **in**
 - indica che il record successivo è un internet DNS RR
- **type**
 - identifica il tipo del RR
- **data**
 - informazione specifica del tipo RR

SOA (Start Of Authority)

Segna l'inizio di un zone file e generalmente è anche il primo record ad essere utilizzato. Esiste un solo SOA associato ad ogni zone file

Si presenta nel seguente formato:

```
[name] [ttl] IN SOA origin contact (
    serial
    refresh
    retry
    expire
    minimum
)
```

- **origin**
 - indica il primary master server per questo dominio
- **contact**
 - email address dell'amministratore del dominio. A differenza di un indirizzo email non compare il carattere @, che viene sostituito dal punto. Se postmaster@unipg.it è l'amministratore del dominio apparirà *postmaster..unipg.it*
- **serial**
 - indica la versione dello zone file. E' conveniente esprimere nella forma yyymmddnn. E' estremamente importante in quanto permette ai secondary server di stabilire se lo zone file in loro possesso è stato modificato: confrontando questo campo con quello nello zone file nel primary server
- **refresh**
 - esprime il tempo che deve aspettare il secondary server prima di controllare il SOA sul primary server. Generalmente un giorno (86400 secondi)
- **retry**
 - indica il tempo che dovrà aspettare il secondary server prima di effettuare una nuova richiesta se la prima fallisce. Generalmente un'ora (3600 secondi)
- **expire**
 - indica il tempo dopo il quale il secondary server dovrà riprendere lo zone file. Generalmente 604800 secondi pari a 7 giorni
- **minimum**
 - è il valore di default del Time To Leave (TTL) per tutti i record del dominio dove non è espresso

NS (Name Server)

Identifica il nome del server che ha l'autorità per il dominio

Si presenta nel seguente formato:

```
[domain] [ttl] IN NS server
```

Le estensioni permettono di indicare i server autorizzati a rispondere per il sottodominio

es: dominio **unipg.it**, sottodominio **plant.unipg.it** (in named.hosts)

```
plant 432000 in ns pack.plant.unipg.it
```

A (Address record)

Utilizzato per associare un hostname ad un indirizzo IP

Si presenta nel seguente formato:

[hostname] [ttl] IN A address

- **hostname**
 - nome che si vuol assegnare all'indirizzo IP address
- **address**
 - l'indirizzo IP corrispondente

Utilizzo di @ come estensione per indicare come name il dominio corrente

AAAA (Address record)

Utilizzate per associare un hostname ad un indirizzo IPv6

Si presenta con il seguente formato:

[hostname] [ttl] IN AAAA address

- **hostname**
 - nome che si vuol assegnare all'indirizzo IP address
- **address**
 - l'indirizzo IP corrispondente

Come estensioni troviamo l'utilizzo di @ come name per indicare il dominio corrente

Con BIND:

```
$ORIGIN 6net.garr.it
www in aaaa 3ffe:b00:c18:1:290:27ff:fe17:fc1d
```

MX (MAIL eXchanger)

Definisce il server che gestisce la posta per un singolo host o un intero dominio; tutta la posta viene rediretta sul server specificato

Si presenta nel seguente formato:

[name] [ttl] IN MX preference host

- **name**
 - di host o dominio a cui le email verranno indirizzate
- **preference**
 - permette di stabilire un ordine di preferenza se sono presenti più mail server; più è basso, maggiore sarà la priorità. I valori partono da 0 e sono multipli di 5
- **host**
 - nome del mail server

Come estensioni troviamo l'utilizzo di @ come name per indicare il dominio corrente

CNAME (Canonical NAME)

Definisce un alias per il nome di un host

Si presenta nel seguente formato:

nickname [ttl] IN CNAME host

PTR (domain name PoinTR)

Permette di associare indirizzi IP ad un nome di host

Si presenta nel seguente formato:

[name] [ttl] IN PTR host

- **name**
 - numero che identifica n-esimo indirizzo IP nella rete
- **host**
 - nome completo dell'host

IPv6 PTR record (ip6.arpa):

\$ORIGIN 1.0.0.0.8.1.c.0.0.0.b.0.e.f.f.3.ip6.arpa.d.1.c.f.7.1.e.f.f.f.7.2.0.9.2.0. in ptr www.6net.garr.it

Configurazione di named

Comando utilizzato per avviare il servizio DNS

- **Sintassi**

```
named [-c configfile
```

```
    -d level
```

```
    -p port
```

```
    -n ncpus
```

```
    -t directory
```

```
    -u user
```

```
]
```

- **-c**
 - utilizzato per specificare la posizione del file **named.conf** se diversa da **/etc/named.conf**
- **-d**
 - utilizzato per attivare il debug (maggiore level, maggiore il dettaglio) salvando le informazioni nel file **\$dir/named.run**
- **-p**
 - per default il servizio risponde alla porta 53 (TCP/UDP), con questa opzione si può specificare una porta diversa
- **-n**
 - il kernel instanzia ncpus thread per sfruttare i sistemi multiprocessore
- **-t**
 - Il processo esegue un cambio di directory appena letto il file di configurazione
- **-u**
 - il processo named viene eseguito dall'utente specificato, invece che da root

Rispetto al resolver, per la configurazione di named vengono utilizzati più file:

- **named.conf**
 - contiene i parametri generali di configurazione del *named* ed i puntatori ai file contenenti le informazioni dei domini gestiti dal server (**zone files**)
- **named.ca**
 - puntatori ai root domains server
- **named.local**
 - reverse per l'indirizzo loopback
- **named.host**
 - zone file per la risoluzione diretta
- **named.rev**
 - zone file per la risoluzione inversa

N.B.: i nomi utilizzati sono del tutto **generici ed arbitrari**

Configurazione del BIND

Il BIND può essere configurato in 3 diversi modi:

- **caching-only**
 - il processo è in esecuzione ma non esiste nessun nameserver database file. Ogni richiesta (dal resolver) viene rediretta su altri server ed il risultato memorizzato in un cache locale per servire future richieste (necessari solo *named.conf* e *named.ca*)
- **primary**
 - è il gestore (authoritative server) di informazioni riguardanti specifici domini. Legge le informazioni da appositi file (configurati dall'amministratore) detti **zone files**
- **secondary**
 - scarica gli zone file dal primary server e li memorizza localmente in appositi file detti **zone file transfer**: copia completa di tutte le informazioni sui domini

named.conf

Consente a *named* di puntare ai file contenenti le informazioni sui domini, sia locali che remoti. Ci sono appositi comandi per configurare questo file tipo:

Caching-only

vengono omessi i comandi di configurazione del primary e del secondary ad eccezione per il dominio di loopback

primary	0.0.127.IN-ADDR.ARPA	/etc/named.local
----------------	-----------------------------	-------------------------

Indica a *named* che il server locale è **primary server** per il proprio dominio di loopback e che le relative informazioni sono contenute in **/etc/named.local**

cache	.	/etc/named.ca
--------------	---	----------------------

indica a *named* di memorizzare in una cache locale le risposte ottenute dal nameserver (a cui redirige le richieste dai resolver) e di inizializzare la cache con la lista dei root server contenuta nel file **/etc/named.ca**

primary server

directory		/etc
primary	unipg.it	named.hosts
primary	250.141.IN-ADDR.ARPA	named.rev
primary	0.0.127.IN-ADDR.ARPA	named.local
cache	.	named.ca

primary unipg.it named.hosts

Dichiara che il server locale è il primary server per *unipg.it* e il relativo zone file è *named.hosts*

primary 250.141.IN-ADDR.ARPA named.rev

Puntatore al file *named.rev* in cui c'è l'associazione tra gli indirizzi IP, nel *192.168.0.0*, con i relativi *hostnames*

Indica inoltre che il server locale è il primary server per il **reverse domain** *250.141.IN-ADDR.ARPA*, con le informazioni relative nel file *named.rev*

secondary server

directory		/etc
secondary	unipg.it	141.250.1.1 unipg.it.hosts
secondary	250.141.IN-ADDR.ARPA	141.250.1.1 250.141.rev
primary	0.0.127.IN-ADDR.ARPA	named.local
cache	.	named.ca

secondary unipg.it 141.250.1.1 unipg.it.hosts

Dichiara che il server locale deve scaricare le info sul dominio *unipg.it* del server con indirizzo IP *141.250.1.1* e memorizzarle nel file **/etc/unipg.it.hosts**

secondary	250.141.IN-ADDR.ARPA	141.250.1.1	250.141.rev
------------------	-----------------------------	--------------------	--------------------

Indica inoltre che il server locale è il secondary server per il **reverse domain** 250.141.IN-ADDR.ARPA e che i relativi dati vanno scaricati dal server con IP 141.250.1.1 e memorizzati nel file /etc/250.141.rev

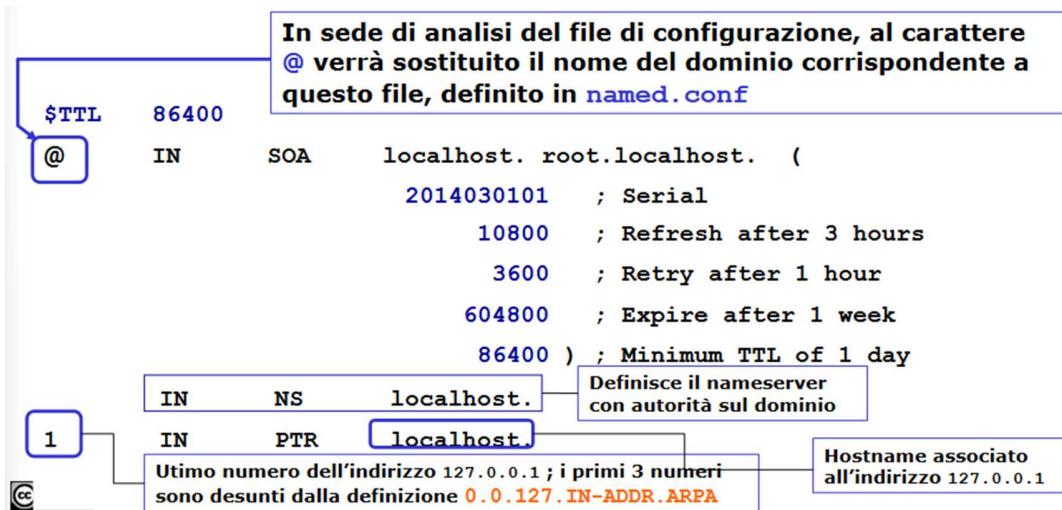
named.ca

Puntatori ai root domains server (pag.550)

named.local

E' lo **zone file** per la traduzione del reverse domain 0.0.127.IN-ADDR.ARPA

Il suo scopo è quello di **permettere la conversazione dell'indirizzo IP 127.0.0.1** (detto loopback address) **nell'hostname localhost**

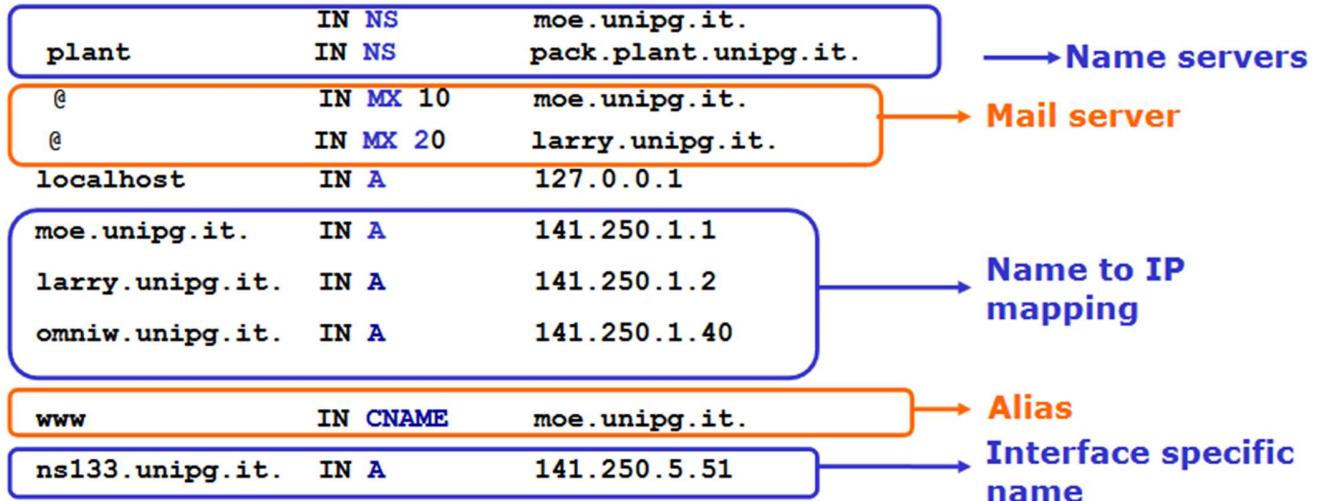


named.hosts

E' lo zone file per la conversione diretta

Il suo scopo è quello di permettere la conversione di hostname in indirizzi IP. Contiene la maggior parte delle informazioni sui domini

```
@ IN SOA moe.unipg.it. root.moe.unipg.it. (
                                2014030101 ; Serial
                                10800      ; Refresh
                                3600       ; Retry
                                604800    ; Expire
                                86400     ; Minimum
```



named.rev

E' lo zone file per la traduzione dei reverse domain inseriti nel named.conf

Il suo scopo è quello di permettere la conversione di indirizzi IP in hostname

dig

Tool di debugging che consente di interrogare direttamente un nameserver per ottenere informazioni e verificarne la configurazione (guarda pag.569)

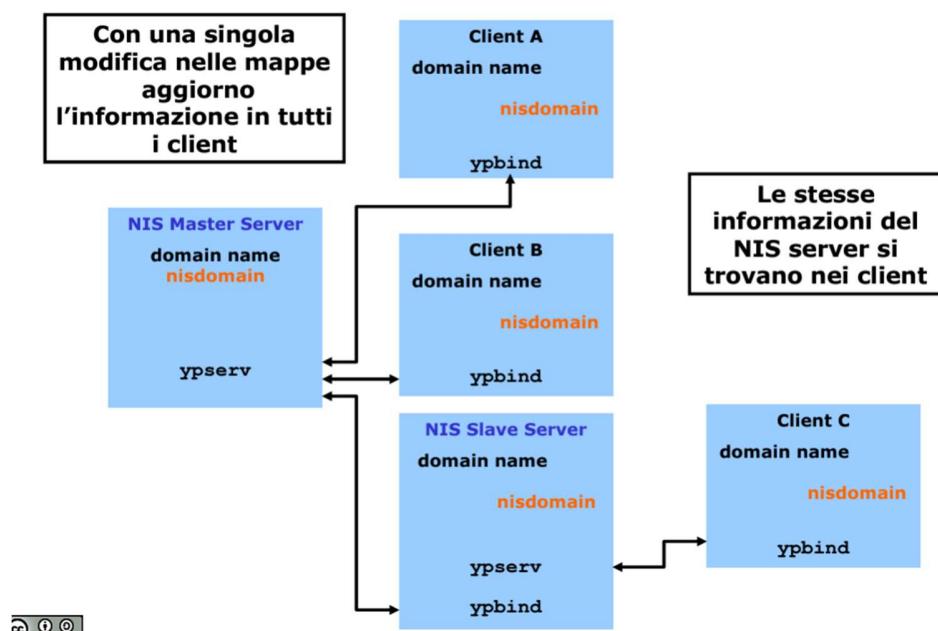
ESEMPI DELL'USO DEL NAMED A PAG. 567 E 568!!!

20° PARTE

NIS (Network Information Service)

NIS (Network Information Service) è un servizio che centralizza la gestione delle risorse amministrative su un insieme di host, permettendo agli utenti di mantenere login, password, home directory e autorizzazioni spostandosi tra diversi host. Questo sistema realizza un database centralizzato che facilita il controllo e la condivisione automatica delle risorse. È fondamentale per applicazioni parallele e distribuite e per la creazione di cluster di computer, poiché semplifica l'accesso a file e risorse indipendentemente dal nodo di elaborazione.

il **NIS** converte i principali file UNIX in un formato database chiamato NIS map, rendendo le informazioni accessibili attraverso la rete. Il vantaggio principale è il controllo centralizzato dei file amministrativi su un singolo server, accessibile da ogni host in rete. L'utilizzo di NIS è completamente trasparente per l'utente finale.



Il Network File System (NFS)

Il **Network File System (NFS)** permette di condividere directory e file su una rete, consentendo a utenti e programmi di accedere a file memorizzati su sistemi remoti come se fossero locali.

Vantaggi di NFS:

- **Riduzione spazio disco locale:** Una singola copia per directory condivisa.
- **Semplificazione dei task di supporto:** Aggiornamento centralizzato dei file, accessibili da tutta la rete.
- **Manipolazione dei file remoti:** Utilizzo di comandi UNIX locali, come `cp`, per gestire file remoti.

Componenti fondamentali di NFS:

- **Client:** Utilizza le directory remote come se fossero parte del filesystem locale.
- **Server:** Mette a disposizione le proprie directory per l'uso da parte dei client.

Gli sviluppatori hanno implementato NFS creando tre parti indipendenti: NFS stesso, Remote Procedure Call (RPC), e eXternal Data Representation (XDR). RPC e XDR sono stati sviluppati anche per essere utilizzati da altri protocolli e programmi applicativi.

Usando NFS, i programmi accedono ai file remoti con le stesse procedure utilizzate per i file locali grazie all'uso di RPC e XDR. Ad esempio, un programmatore può suddividere un'applicazione in una parte client e una parte server, che comunicano tramite RPC.

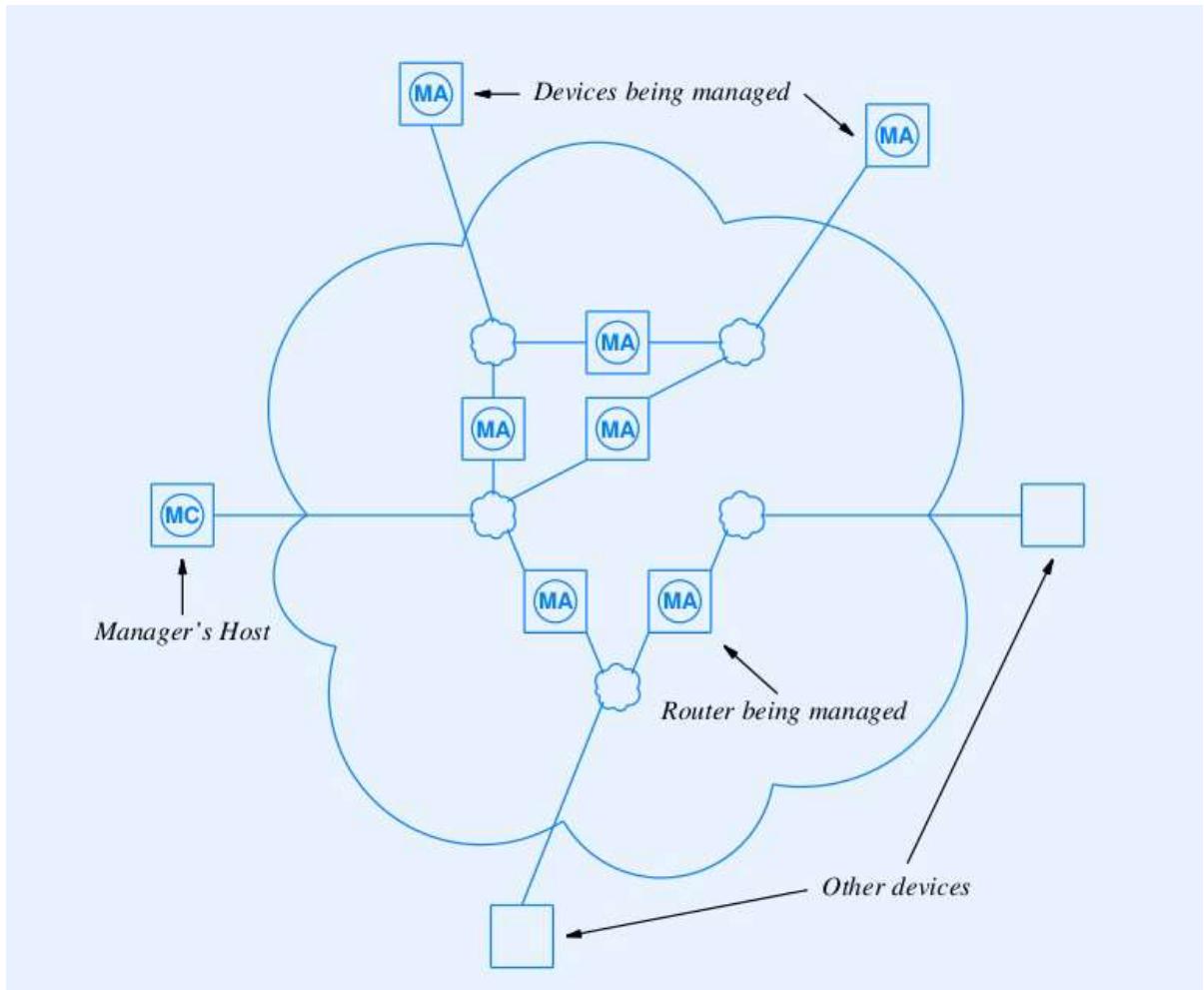
SNMP Simple Network Management Protocol :

La gestione delle reti è cruciale e in continua evoluzione, dato il ruolo vitale delle reti e dei servizi per aziende, individui e istituzioni. L'interruzione della rete può significare un blocco parziale o totale delle attività.

Il **Simple Network Management Protocol (SNMP)** è il protocollo più potente e diffuso per la gestione di reti, sistemi e applicazioni. Gli amministratori di sistema usano SNMP per **inviare richieste e comandi ai nodi della rete, monitorando lo stato delle risorse e delle applicazioni**. In una rete Internet, un host con funzioni di manager controlla lo stato dei router e degli altri dispositivi di rete.

SNMP opera a livello applicazione e comunica con i dispositivi utilizzando i servizi di trasporto del **TCP/IP**, permettendo il controllo di qualsiasi dispositivo connesso a Internet, non limitandosi ai dispositivi di rete locale.

Schema:



Componenti SNMP

- **Nodi gestiti o Agent:** Dispositivi che raccolgono dati SNMP e rispondono alle richieste del Manager (**host, stampanti, router, switch, hub, ecc.**).
- **Stazione di gestione o Manager:** Programma che interroga e invia comandi agli agenti, permettendo la gestione intelligente degli eventi.
- **Informazioni di gestione o Management Information Base (MIB):** Archivio di informazioni di gestione fornito dagli agenti, chiamati oggetti.
- **Protocollo di gestione (SNMP):** Definisce le modalità di interazione tra il Manager e gli Agenti.
- **Struttura dell'informazione di gestione (SMI):** Definisce la struttura delle informazioni da gestire.

SNMP v3

Ultima versione SNMP(**SNMP v3**) migliora il servizio in vari campi tra cui:

- Authentication: per proteggere contro modifiche delle informazioni, il mascheramento e la modifica della sequenza dei messaggi;
- Privacy: per garantire la riservatezza delle informazioni;
- Nuovi strumenti di controllo, inclusi strumenti grafici per la definizione delle regole di accesso
- Configurazione remota di sistemi gestibili, mediante un insieme di operazioni sicure

SNMP v3

21° PARTE

MIB

La collezione di tutti i possibili oggetti in una rete è chiamata **Management Information Base (MIB)**.

- Ogni oggetto mantiene una serie di variabili SNMP che descrivono il suo stato.
- Il Manager comunica con gli Agent tramite il protocollo SNMP, che permette di conoscere e modificare lo stato delle variabili MIB.

In caso di eventi imprevisti, viene generato un SNMP trap, la stazione di gestione (Manager) può richiedere informazioni sullo stato delle variabili mediante messaggi, Quando si verificano dei trap, i messaggi si intensificano, un approccio denominato polling orientato ai trap.

Structure of Management Information (SMI)

La **Structure of Management Information (SMI)** è l'insieme delle regole che definiscono i nomi delle variabili MIB. Include definizioni di base come l'indirizzo (valori costituiti da 4 byte) e il contatore (intero da 0 a $2^{32} - 1$). È specificata con l'**Abstract Syntax Notation 1 (ASN.1)**, uno **standard ISO**. ASN.1 specifica la sintassi dei nomi (in formato leggibile dall'utente) e la codifica binaria (nel formato usato nei messaggi). Lo spazio dei nomi è assoluto e gerarchico.

ASN.1

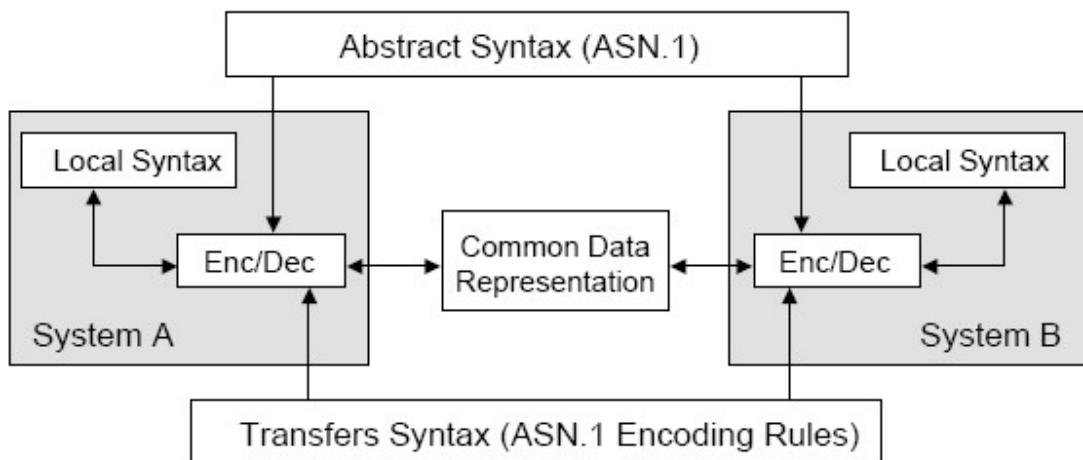
Abstract Syntax Notation One (da non confondere con l'ASN): notazione internazionalmente standardizzata indipendente dall'implementazione, dalla piattaforma e dal linguaggio, volta a specificare strutture dati ad alto livello di astrazione

L'Object Identifier

L'**Object Identifier** contiene i criteri per definire un oggetto seguendo una struttura ad albero di standard, posizionando ogni oggetto o standard in una regione specifica dell'albero. La porzione usata da SNMP ha come radici gli organismi di standardizzazione **ISO e CCITT (ora ITU)**. Da queste radici si dipartono degli archi che definiscono sotto-organizzazioni, ciascuna associata a un'etichetta e un numero.

ASN . 1

ASN.1 definisce il metodo univoco per convertire i valori dei tipi ASN.1 in una sequenza di byte, nota come Basic Encoding Rules (BER), senza ambiguità. La codifica è ricorsiva, quindi la codifica di un oggetto composto è la concatenazione delle codifiche dei suoi componenti. Ogni valore trasmesso deve includere tre campi: l'identificatore (tipo o estensione), la lunghezza del campo dati in byte e il campo dati stesso. Dopo l'adozione dell'ASN.1 per SNMP, sono state definite 4 macro e 8 tipi di dati molto utilizzati in SNMP, descritti da Structure of Management Informations (SMI).



(Riferimento al MIB)

Il Management Information Base (MIB) definisce la collezione degli oggetti gestiti da SNMP. Questi oggetti sono raggruppati in 12 categorie, corrispondenti a 12 nodi al di sotto del nodo mib-2 nella struttura ad albero ASN.1. Le categorie servono per definire le basi di ciò che deve essere compreso dal Manager.

Categorie MIB

MIB category	Includes Information About
system	The host or router operating system
interfaces	Individual network interfaces
at	Address translation (e.g., ARP mappings)
ip	Internet Protocol software
icmp	Internet Control Message Protocol software
tcp	Transmission Control Protocol software
udp	User Datagram Protocol software
ospf	Open Shortest Path First software
bgp	Border Gateway Protocol software
rmon	Remote network monitoring
rip-2	Routing Information Protocol software
dns	Domain Name System software

Categorie più importanti:

Il gruppo "**system**" fornisce informazioni sul tipo di dispositivo, chi lo ha chiamato, l'hardware e il software contenuti, e la persona da contattare in caso di guasti o malfunzionamenti. Questo è cruciale se la gestione viene appaltata ad altri, poiché i gestori sapranno chi contattare in caso di problemi.

Il gruppo "**interfaces**" contiene i Network Interface Controller (NIC), ovvero le schede di rete, che tengono traccia dei pacchetti e byte inviati e ricevuti, del numero di quelli rifiutati, dei broadcast e della dimensione della coda di uscita.

Il gruppo "**AT**" precedentemente teneva traccia delle conversioni tra indirizzi Ethernet e indirizzi Internet, ma ora è vuoto poiché questi oggetti sono stati spostati negli specifici protocolli in SNMPv2.

Il gruppo "**IP**" si occupa del traffico a livello di rete, gestendo l'Internet Protocol (IP) dal nodo al nodo. È ricco di contatori che monitorano i pacchetti persi per vari motivi e tiene traccia del riassemblaggio e della frammentazione dei pacchetti IP.

Il gruppo "**ICMP**" è dedicato ai messaggi di errore IP, poiché l'Internet Control Message Protocol (ICMP) è un protocollo di gestione dell'IP. Aggiorna i contatori per i vari tipi di messaggi ICMP, registrandone il numero.

Il gruppo "TCP" si occupa del traffico a livello di trasporto, relativo al Transmission Control Protocol (TCP). Aggiorna i contatori riguardanti le connessioni aperte, sia totali che attuali, i segmenti inviati e ricevuti e altre statistiche relative al TCP.

Il gruppo "EGP" monitora il traffico relativo all'Exterior Gateway Protocol (EGP), che sono protocolli di routing esterni agli Autonomous System (AS). Questo gruppo tiene traccia di quanti pacchetti sono stati inviati e ricevuti e rileva eventuali anomalie.

Il gruppo "Trasmission" contiene MIB specifici del dispositivo, mantenendo ad esempio statistiche specifiche per il protocollo Ethernet.

Il gruppo "SNMP" raccoglie statistiche sul protocollo Simple Network Management Protocol (SNMP) stesso, come il numero e il tipo di messaggi inviati.

Variabili MIB

MIB Variable	Category	Meaning
sysUpTime	system	Time since last reboot
ifNumber	interfaces	Number of network interfaces
ifMtu	interfaces	MTU for a particular interface
ipDefaultTTL	ip	Value IP uses in time-to-live field
iplnReceives	ip	Number of datagrams received
ipForwDatagrams	ip	Number of datagrams forwarded
ipOutNoRoutes	ip	Number of routing failures
ipReasmOKs	ip	Number of datagrams reassembled
ipFragOKs	ip	Number of datagrams fragmented
ipRoutingTable	ip	IP Routing table
icmplnEchos	icmp	Number of ICMP Echo Requests received
tcpRtoMin	tcp	Minimum retransmission time TCP allows
tcpMaxConn	tcp	Maximum TCP connections allowed
tcplnSegs	tcp	Number of segments TCP has received
udplnDatagrams	udp	Number of UDP datagrams received

Nagios

Nagios è uno dei software Open Source più popolari per la gestione delle reti utilizzando SNMP.

Con Nagios, gli utenti possono configurare regole di monitoraggio per controllare costantemente i servizi e i dispositivi di rete. Quando viene rilevato un problema o un'anomalia, Nagios può notificare gli amministratori tramite email, messaggi di testo o altri metodi di notifica, consentendo loro di intervenire prontamente per risolvere il problema e mantenere l'affidabilità e le prestazioni della rete.