

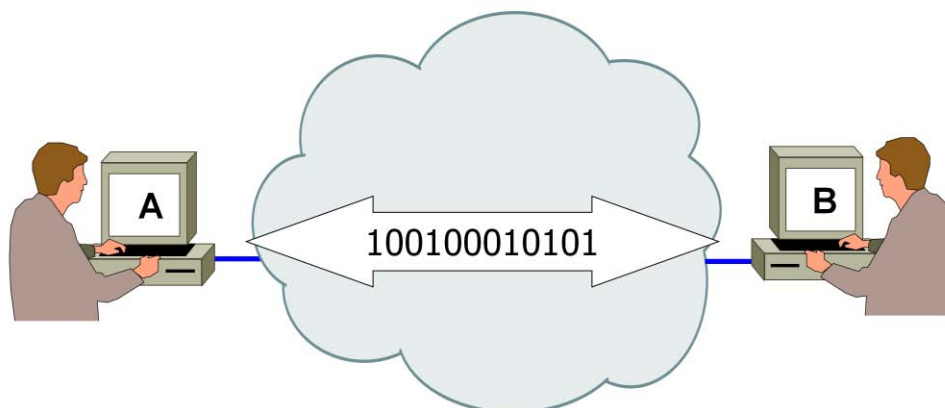
Le Reti IP per le infrastrutture  
critiche e la sicurezza fisica

# **CAPITOLO 1**

## **Il modello di riferimento ISO/OSI**



## Comunicare in rete



[www.ncp-italy.com](http://www.ncp-italy.com)

Il modello di riferimento ISO/OSI 1-2

Lo scambio di dati tra due o più computer non è un processo semplice, non basta spedire la stringa di bit che rappresenta il dato lungo la linea di trasmissione per far sì che la comunicazione possa ritenersi attivata con successo, ma è necessario mettere in piedi un processo molto più complesso per poter garantire un dialogo efficace tra le macchine. Per prima cosa occorre implementare dei protocolli di comunicazione. Per protocollo si intende la descrizione formale di un insieme di regole che governano lo scambio di informazione tra i dispositivi interconnessi. **L'applicazione** di un determinato protocollo garantisce, in altre parole, che le entità collegate parlino la stessa lingua, vengano evitate incomprensioni e quindi perdita di informazioni.



# Comunicare in rete



[www.ncp-italy.com](http://www.ncp-italy.com)

Il modello di riferimento ISO/OSI 1-3

Non tutti i protocolli sono così semplici e non tutte le transazioni si risolvono in cinque comandi, questo esempio però è abbastanza esemplificativo di come le cose vanno nella comunicazione tra applicazioni. Non dimentichiamo, inoltre, che la semplicità deriva anche **dall'aver** supposto che le applicazioni potessero parlare direttamente tra di loro attraverso un canale virtuale. Nella realtà le applicazioni sono residenti in stazioni collegate tra di loro condividendo un mezzo trasmissivo reale sul quale transitano i messaggi, e questo complica notevolmente le cose per almeno tre motivi:

- su di una stazione possono essere presenti più applicazioni.
- su di una rete possono essere presenti più stazioni.
- i messaggi inviati su un mezzo trasmissivo reale, come abbiamo già avuto modo di accennare nei capitoli precedenti, sono soggetti a disturbi e ad alterazioni di varia natura e, pertanto, possono arrivare a destinazione alterati.

Ecco che nasce **l'esigenza** di introdurre degli altri protocolli che permettano di risolvere le problematiche sopra descritte, più precisamente:

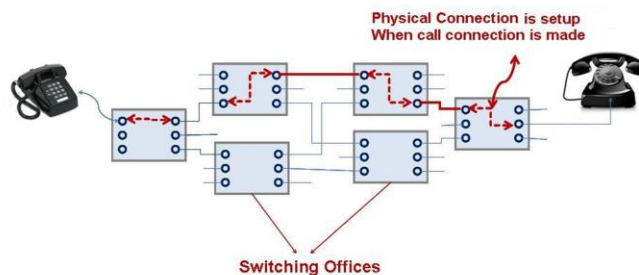
- distinguere le applicazioni tra di loro operando una corretta comunicazione tra applicazione sorgente e applicazione destinazione
- distinguere le stazioni tra di loro operando una corretta comunicazione tra la stazione sorgente e la stazione destinazione
- fare in modo che la comunicazione sia affidabile, cioè che i messaggi arrivino tutti, nella sequenza giusta e integri.

Questa schematizzazione tiene conto, come abbiamo già accennato, del fatto che gli enti coinvolti nella comunicazione sono diversi: **l'applicazione**, la macchina, e la rete fisica di collegamento.

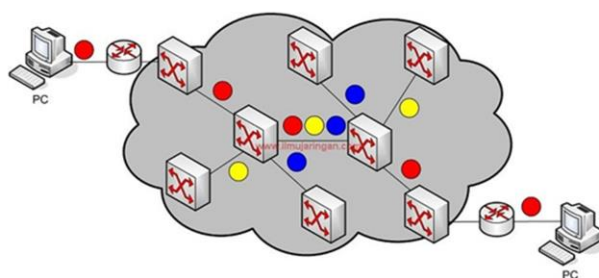




# Come fatta la rete ?



## Commutazione di circuito vs commutazione di pacchetto



[www.ncp-italy.com](http://www.ncp-italy.com)

Il modello di riferimento ISO/OSI 1-4



## Un modello a tre livelli



[www.ncp-italy.com](http://www.ncp-italy.com)

Il modello di riferimento ISO/OSI 1-5

Risulta abbastanza intuitivo suddividere le azioni che devono essere svolte per stabilire la comunicazione in tre livelli distinti che possiamo chiamare:

- Livello di accesso alla rete
- Livello di trasporto
- Livello applicativo

Il livello di accesso alla rete comprende il software residente nel calcolatore che gestisce le procedure per la consegna del messaggio alla rete di trasmissione, e quindi, per esempio, fornisce alla rete l'**indirizzo** del destinatario perché il messaggio venga consegnato alla stazione giusta, può fornire informazioni sulla priorità da assegnare al messaggio stesso, ecc, in generale, fornisce tutta una serie di dati che dipendono dalla specifica rete preposta al collegamento e ai servizi che questa rete offre.

Il livello di trasporto ha il compito di garantire l'**affidabilità** del collegamento, e quindi è preposto alla gestione di tutti quei meccanismi che fanno sì che i messaggi arrivino **all'applicazione** di destinazione integri e nello stesso ordine in cui sono partiti. Queste procedure sono indipendenti dalla particolare applicazione, e sono indipendenti anche dal particolare tipo di rete che viene adottata, quindi è ragionevole che vengano raggruppate in un livello indipendente e condiviso da tutte le particolari applicazioni presenti sul calcolatore.

Il Livello applicativo, infine, comprende il software di comunicazione presente sulle stazioni trasmittente e ricevente. I principali compiti svolti a questo livello sono: la composizione del messaggio applicativo da inviare, la sua corretta interpretazione in ricezione, l'**esecuzione** di azioni specifiche, sulla base del contenuto dei messaggi scambiati, e la produzione di responsi sul loro esito.



# Il modello ISO/OSI



- Riduce la complessità
- Standardizza le interfacce
- Facilita la modularità
- Assicura l'interoperabilità
- Accelera l'evoluzione
- Semplifica l'apprendimento

[www.ncp-italy.com](http://www.ncp-italy.com)

Il modello di riferimento ISO/OSI 1-6

Nel campo delle telecomunicazioni esistono vari organismi che hanno il compito di definire gli standard da utilizzare. Per standard **s'intende l'insieme** di regole o procedure che sono ampiamente utilizzate (standard de facto) o ufficialmente specificate (standard de jure).

ISO (International Standard Organization) è il principale ente di standardizzazione internazionale che si occupa anche di reti di calcolatori.

In questo paragrafo tratteremo in particolare gli sforzi fatti **dall'ISO**, per definire uno standard di riferimento per le reti di calcolatori. Il progetto partì negli anni '70, a fronte di una pressante esigenza derivante da un grande fermento nel settore delle reti che cominciava a svilupparsi in modo consistente. Per dare ordine agli enormi sforzi che i vari sviluppatori producevano, **l'ISO** propose un modello di riferimento oggi conosciuto come modello OSI (Open Systems Interconnections).

**Nell'affrontare** il problema cercando di definire funzionalità e terminologia di riferimento, ISO decise di adottare un approccio a livelli. **L'idea** era quella che abbiamo già descritto, cioè identificare e circoscrivere problematiche e funzioni per poi organizzarle in livelli separati ma interoperanti.

Tutti i problemi di comunicazione tra due applicazioni sono stati affrontati e razionalizzati dal comitato ISO in un unico schema concettuale di sette livelli (layers), ognuno dei quali esegue funzioni ben specifiche. Questo modello è oggi comunemente conosciuto come **"Pila OSI"**. Il modello OSI non ha lo scopo di definire protocolli specifici ma di fornire una base comune su cui sviluppare nuovi standard per **l'interconnessione** di apparati elettronici e un modello rispetto al quale confrontare eventuali soluzioni di rete proprietarie.

I vantaggi di un sistema a livelli sono molteplici:

dividere i complessi aspetti **dell'Internetworking**, cioè di strutture molto articolate composte da più reti interconnesse tra di loro, in elementi più semplici

- mettere in grado gli sviluppatori di concentrare i loro sforzi su specifiche funzioni
- definire delle interfacce standard per garantire **l'interoperabilità** tra livelli adiacenti
- prevenire che i cambiamenti su certe funzioni impattino su altre
- In dipendenza dei livelli così da favorire evoluzione e sviluppo
- dividere la complessità della materia in sottoinsiemi più facilmente comprensibili



## Livelli e funzioni



[www.ncp-italy.com](http://www.ncp-italy.com)

Il modello di riferimento ISO/OSI 1-7

Livello 1, o livello fisico.

Il livello fisico riguarda **l'interfaccia** fisica vera e propria e le regole che governano la trasmissione dei bit da un dispositivo **all'altro**. Il livello fisico comprende specifiche:

Meccaniche. Si riferiscono agli aspetti meccanici **dell'interfaccia**, tipicamente rappresentano le specifiche del connettore.

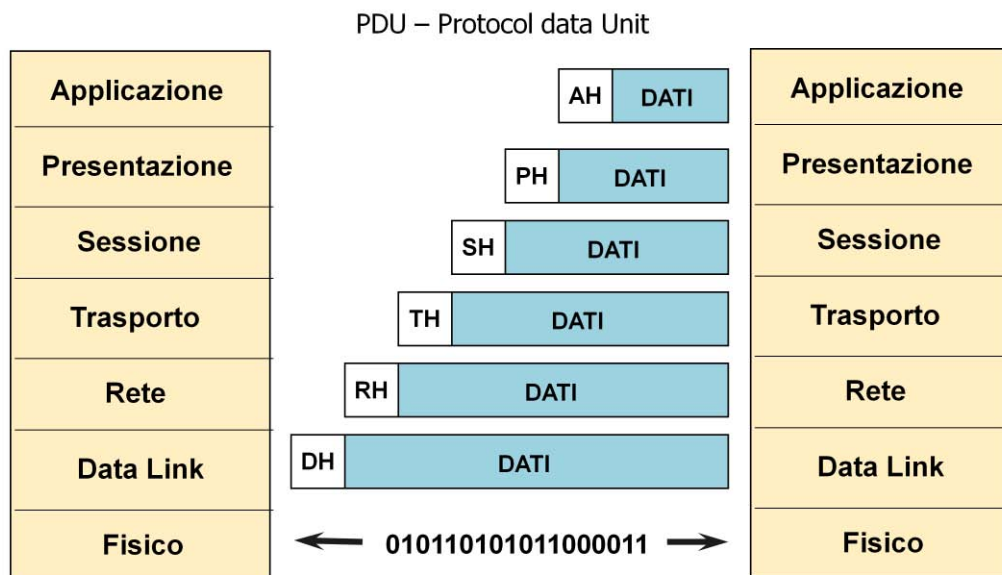
Elettriche. Comprendono le caratteristiche del segnale elettrico come i livelli di tensione e il bit rate.

Funzionali. Specificano le funzioni assegnate ad ogni singolo circuito di interfaccia.

Procedurali. Specificano le procedure che governano il flusso di bit lungo la linea.



# Processo di Imbustamento



[www.ncp-italy.com](http://www.ncp-italy.com)

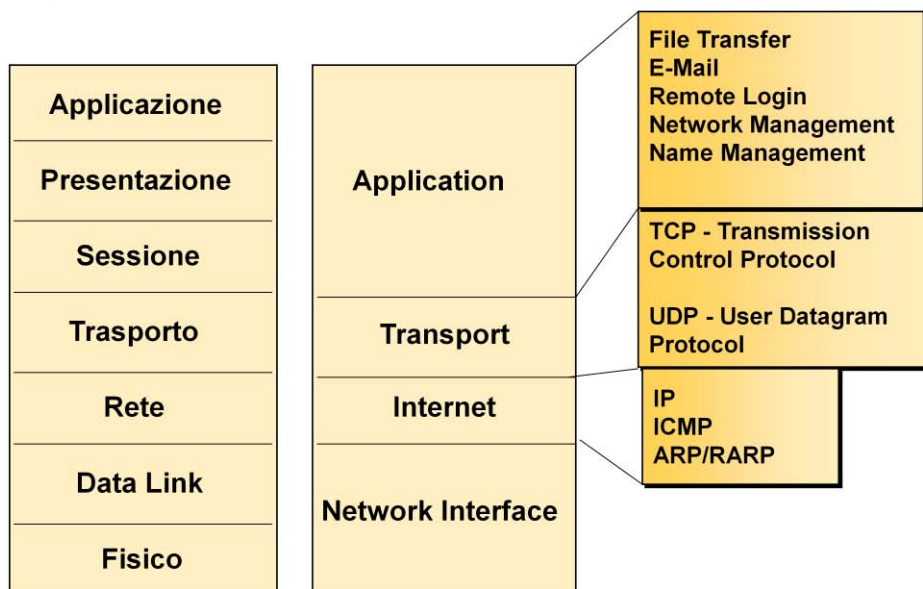
Il modello di riferimento ISO/OSI 1-8

Ogni livello offre dei servizi a quello superiore. Per poter far questo, ogni livello introduce dei parametri caratteristici di gestione. Per esempio, per controllare che i messaggi arrivino nella sequenza giusta **s'introduce** un numero progressivo con il quale marcare ogni messaggio, per crittografare un messaggio **s'inviano** le chiavi di cifratura, per raggiungere una stazione si indica **l'indirizzo** e così via. Si comprende da queste osservazioni che al contenuto informativo originario del messaggio, man mano che si procede verso il basso della pila OSI, si aggiungono delle informazioni extra. **L'insieme** di queste informazioni, introdotte da ogni singolo livello, si chiama testata o header del messaggio. I messaggi risultano quindi composti da una testata o **header** e da un contenuto informativo che si chiama anche "**carico pagante**" o pay-load o semplicemente "**dati**". Un messaggio siffatto prende il nome di PDU Protocol Data Unit.

Nel procedere **dall'alto** verso il basso della pila OSI, accade che ogni livello costruisce la propria PDU aggiungendo il suo header alla PDU che gli viene passata dal livello superiore. Questo processo è chiamato imbustamento o encapsulation, ricorda, infatti, il gesto **d'introduzione** di una lettera **all'interno** di una busta affrancata.



## OSI vs TCP/IP



[www.ncp-italy.com](http://www.ncp-italy.com)

Il modello di riferimento ISO/OSI 1-9

Se il modello OSI è diventato il modello standard per classificare le funzioni delle comunicazioni, la suite di protocolli TCP/IP è **l'architettura** più usata. Questa suite raccoglie tutta una serie di protocolli che sono stati pubblicati quali standard di Internet.

Pur non essendoci alcun modello architetturale ufficiale, in base agli standard protocollari che sono stati sviluppati, nel TCP/IP le funzioni relative alle comunicazione possono essere raggruppati in quattro livelli indipendenti:

Livello di applicazione (Application)

Livello di trasporto (Transport)

Livello di Internet

Livello di interfaccia con la rete (Network Interface)

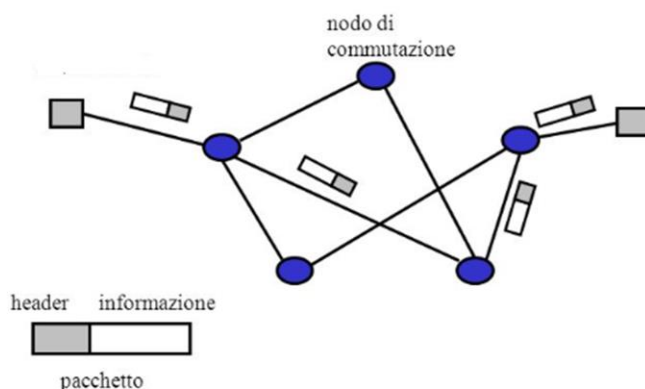
Il modello presenta **un'evidente** semplificazione con la mancanza completa dei livelli Sessione e Presentazione, le cui funzionalità sono completamente demandate al livello Applicativo.

Nel caso del TCP/IP si ha un livello 4 connection-oriented poggiato su livelli 3 e 2 connectionless. **L'affidabilità** della comunicazione è completamente demandata al livello di Trasporto. Tutto il resto si svolge in maniera best-effort.

Il livello 3 o livello Internet contiene protocolli come **l'IP** (Internet Protocol) che forniscono la capacità di instradamento del messaggio attraverso una molteplicità di reti.



## Pacchetti in movimento



[www.ncp-italy.com](http://www.ncp-italy.com)

Il modello di riferimento ISO/OSI 1-10

Le informazioni viaggiano da una stazione **all'altra** della rete sotto forma di pacchetti con un header che contiene le informazioni per **l'instradamento** (motrice) e un vano informazione (rimorchio) che contiene i dati da consegnare al mittente. I nodi di commutazione della rete inoltrano il pacchetto al prossimo nodo (next-hop) in base alle indicazioni contenute **nell'header** cercando di seguire il migliore percorso. In una rete IP **l'header** contiene **l'indirizzo** del destinatario.



# Tipologie di reti

## Types of Computer Networks



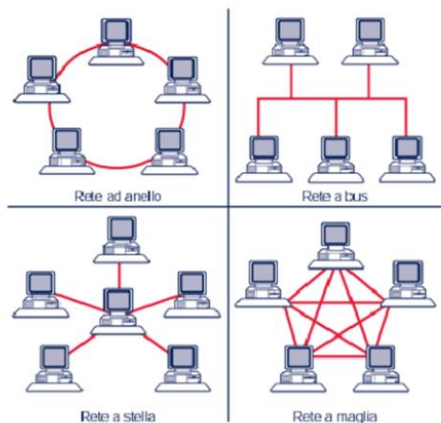
[www.ncp-italy.com](http://www.ncp-italy.com)

Il modello di riferimento ISO/OSI 1-11





# Topologie di reti



[www.ncp-italy.com](http://www.ncp-italy.com)

Il modello di riferimento ISO/OSI 1-12



# Wireless vs Wired



[www.ncp-italy.com](http://www.ncp-italy.com)

Il modello di riferimento ISO/OSI 1-13



## Infrastruttura - rete

Rete cablata a regola d'arte in grado di supportare le alte prestazioni richieste: Cat 6a per supportare i 10Gbps **UTP** 100 m, Cat 7a per i 40 **STP** Gbps.

Una rete LAN **Ethernet** di alte prestazioni, con supporto del PoE, del VLAN tagging, dei meccanismi di sicurezza 802.1x con multidomain, link aggregation 802.3ad, Rapid Spanning Tree, LLDP/CCDP per VLAN negotiation.

Una rete wireless di alte prestazione **802.11ac**, con supporto del roaming L2/L3, meccanismi di QoS e di segregazione del traffico, sicura con utilizzo dei meccanismi di cifratura WPA2 e di autenticazione 802.1x.

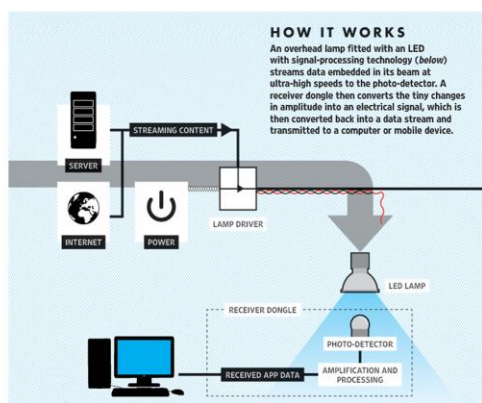


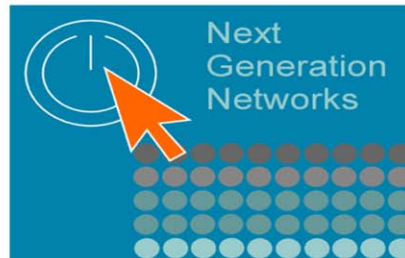




Un sistema Li-Fi è stato testato con successo a Tallin (capitale dell'Estonia), all'interno di un ambiente produttivo/industriale. A partire dalla prima metà del 2015 Velmenni, startup estone attiva nel settore dell'hi-tech, ha utilizzato un impianto Li-Fi per connettere a Internet computer, smartphone e altri dispositivi di rete. E i risultati, stando a quanto dichiarato dal CEO di Velmenni Deepak Solanki, sono molto incoraggianti: la rete Li-Fi estone ha raggiunto una velocità di connessione di **224 gigabit al secondo** (28 gigabyte al secondo), circa **100 volte più veloce della migliore tecnologia Wi-Fi** oggi disponibile sul mercato.

Negli esperimenti condotti sinora, gli scienziati hanno raggiunto una velocità di trasmissione dati di **3,5 gigabit al secondo** (poco più di 4 megabyte) modulando adeguatamente la luce emessa da un singolo LED di colore blu. Sfruttando LED a luce bianca, invece, la velocità di trasferimento è ridotta a 1,7 gigabit al secondo.





Una NGN è una rete a commutazione di pacchetto ***all-IP*** *in grado di fornire servizi di telecomunicazioni attraverso molteplici tecnologie di trasporto*, caratterizzate da differenti QoS, in cui le funzioni relative ai servizi sono indipendenti dalle sottostanti tecnologie relative al trasporto.

Le Reti WAN 4-17



## **Multimedialità, Interattività, Mobilità, Convergenza e integrazione**

TV broadcast

Pay Per View

Pay TV

Videotelefonia

Videoconferenza

Videoassistenza

Telelavoro

Gaming On-Line

Home-shopping

Home-banking

Telemedicina

e-learning

Accesso a banche dati

Web-TV

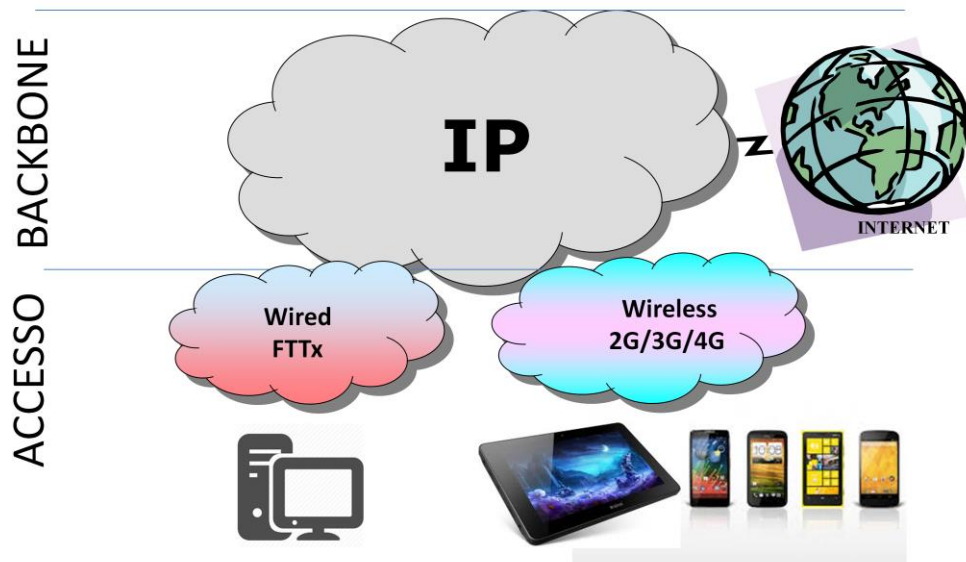
VoD

Web 2.0

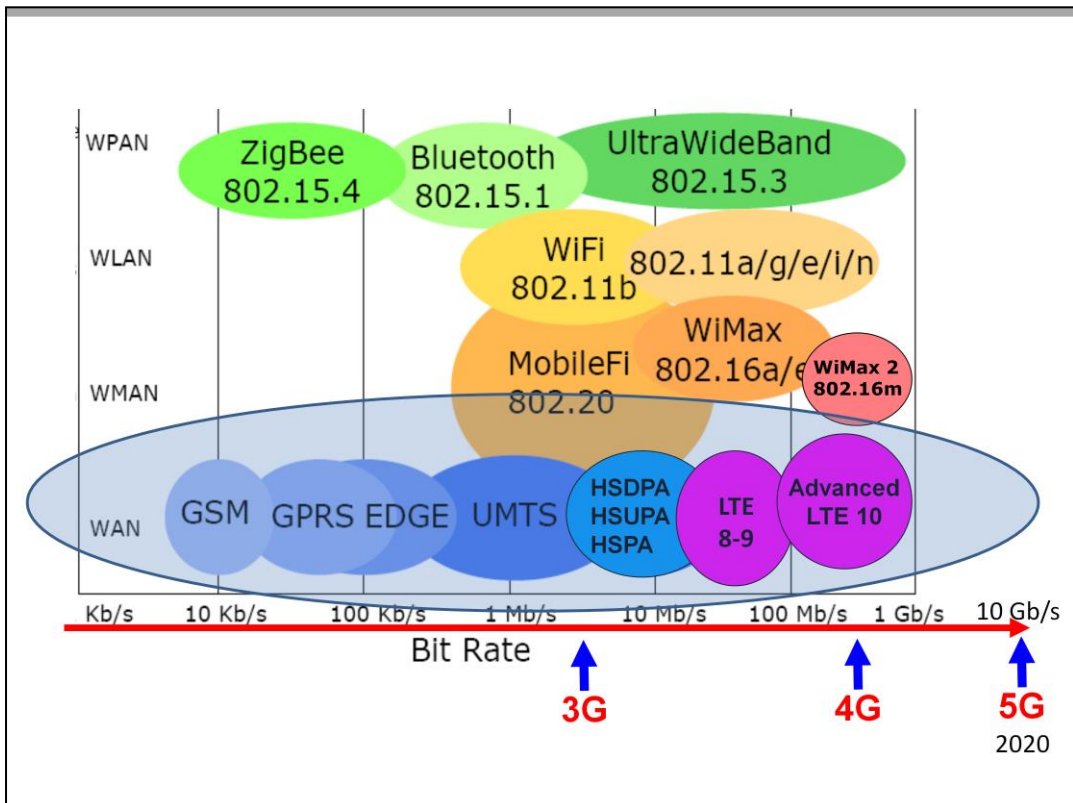
Le Reti WAN 4-18



## Connettività wireless vs wired









### Mobile networks download speed comparison



Produced by 4G.co.uk.

3G fino a 21 Megabit al secondo  
4G fino a 100 Megabit al secondo

**4GPLUS** è la nuova rete mobile che da oggi ti  
permette di raggiungere connessioni fino a  
**300 Megabit al secondo**



#### Navigazione internet

Con 4G Internet è veloce come sfogliare un giornale

Questi tempi sono indicativi e si basano sulle velocità di connessione massime teoricamente raggiungibili  
(21 Mbps per il 3G e 100 Mbps per il 4G e fino a 300 Mbps per il 4GPLUS)





4G

Navighi a tutta velocità



Internet Passport

Per i tuoi viaggi all'estero



Navighi alla velocità del 4G più veloce di sempre fino a 225 Mbps. Inclusa in tutti i piani per tablet, pc e chiavette.

Con il servizio 4G di Wind è possibile navigare in Internet, guardare video, caricare immagini su web e scaricare musica ad alta velocità fino a **150 Mbps.**



#### Cosa serve per navigare in 4G

- Smartphone\* o Tablet 4G
- SIM 4G
- Una qualsiasi offerta Ricaricabile o Abbonamento con Internet incluso



#### Attiva ora l'Opzione LTE !



Video in qualità HD



Download super veloce



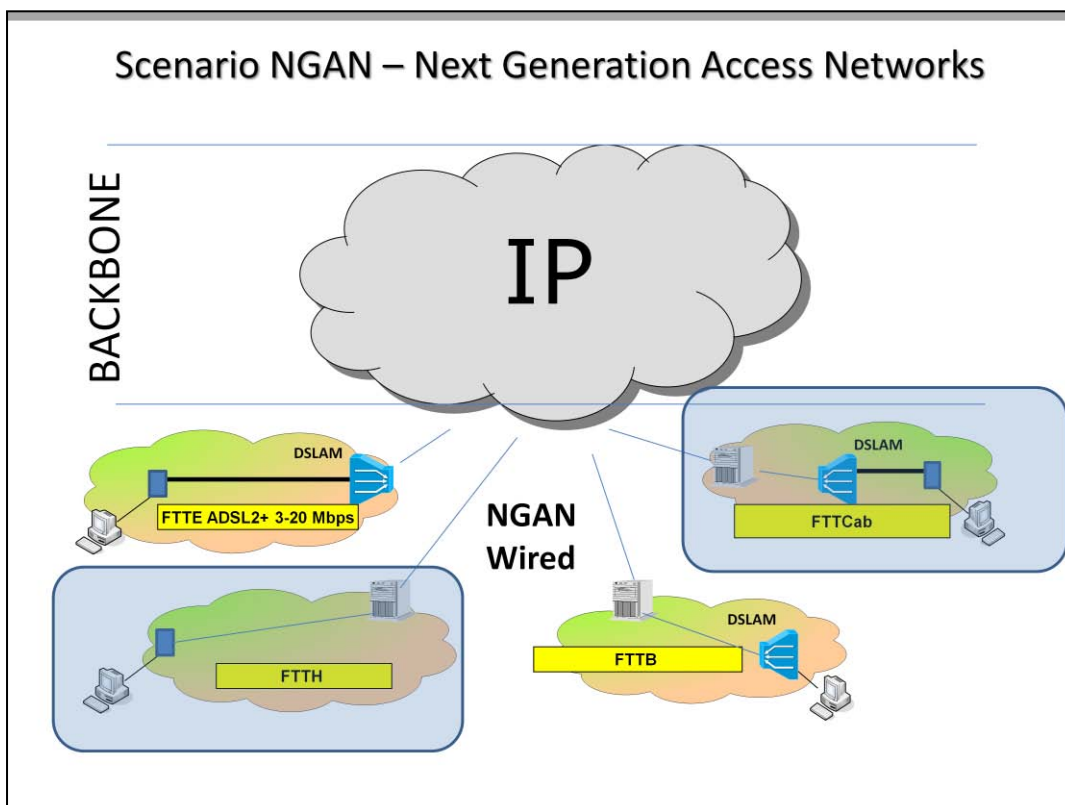
Altissime prestazioni

Navighi fino a 100 Mbps nei comuni coperti Smartphone, Tablet e Chiavette abilitate.

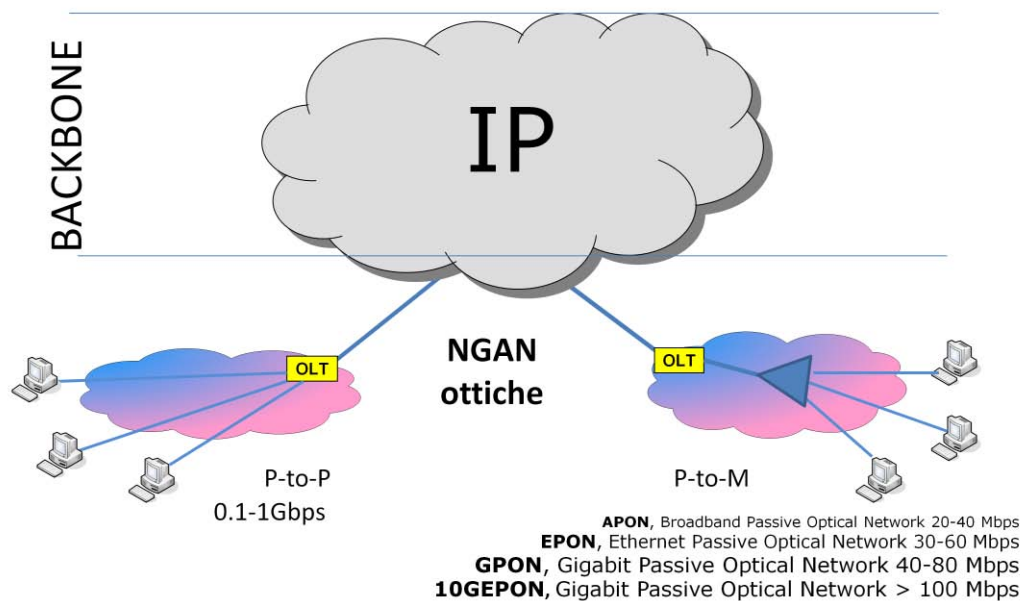


L'azienda americana lancia suo Snapdragon X16 Lte modem , è uno dei primi chip capaci di raggiungere il limite di **1 Gbps (LTE Category 16)**, in scaricamento da smartphone e tablet ed è certo il fiore all'occhiello dell'offerta. La velocità di upload è invece limitata a 150 Mbps.  
Ci si aspetta di vedere i primi prodotti con il «super» modem già dalla fine del 2016.

## Scenario NGAN – Next Generation Access Networks



## Scenario NGAN – Next Generation Access Networks







*una rete “unica” in architettura punto-punto per l’Italia rappresenta una **scelta troppo onerosa** che potrebbe determinare, a parità di capitale investibile, una copertura territoriale ristretta e, probabilmente, non in linea con gli **sfidanti obiettivi dell’Agenda Digitale Europea** (abbonamenti ad oltre 100 Mb/s per almeno il 50% delle famiglie al 2020);*

Francesco Vatalaro, Presidente “Comitato NGN Italia, Roma, 10 maggio 2012

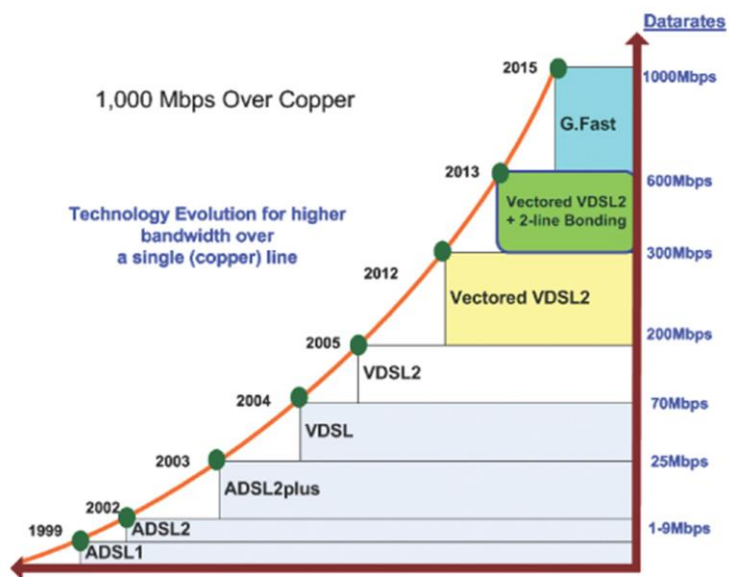
## FTTCab

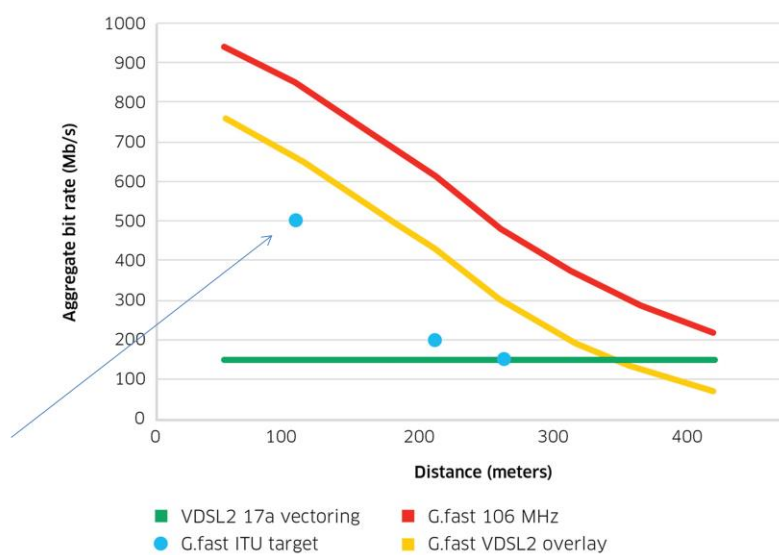
L'Italia è nella situazione ideale con distanza media fra Cabinet ed Edificio di **250 metri** ( Francia 750 metri)

Ci possono essere le condizioni per soddisfare l'agenda digitale europea. Rispetto a FTTH basterebbe arrivare a **150 mila armadi (5-6 anni)** anziché raggiungere 28 milioni di punti di accesso (15-20 anni).

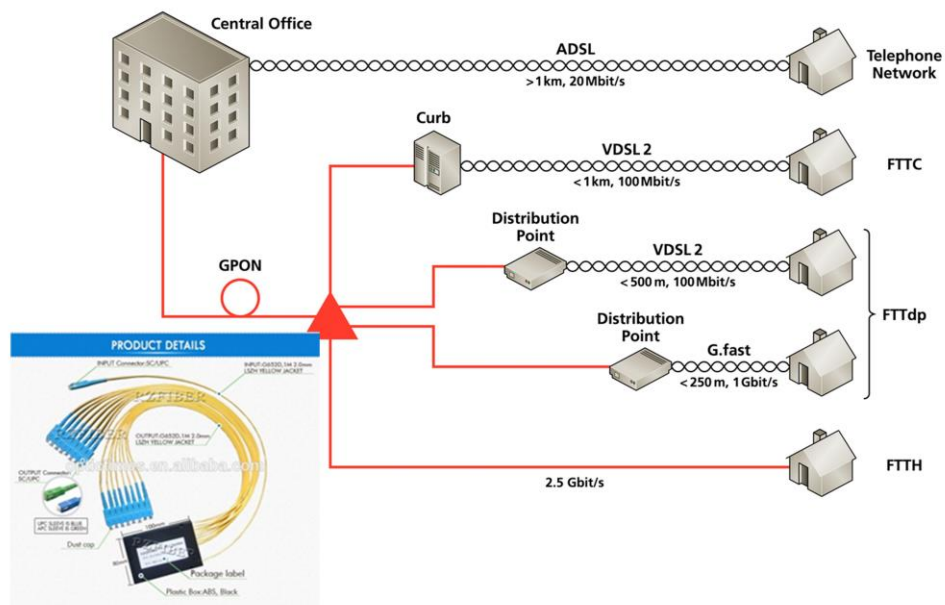
**VDSL2**: fino a 200 Mbps

**G. Fast**: da 200 Mbps a 1 Gbps

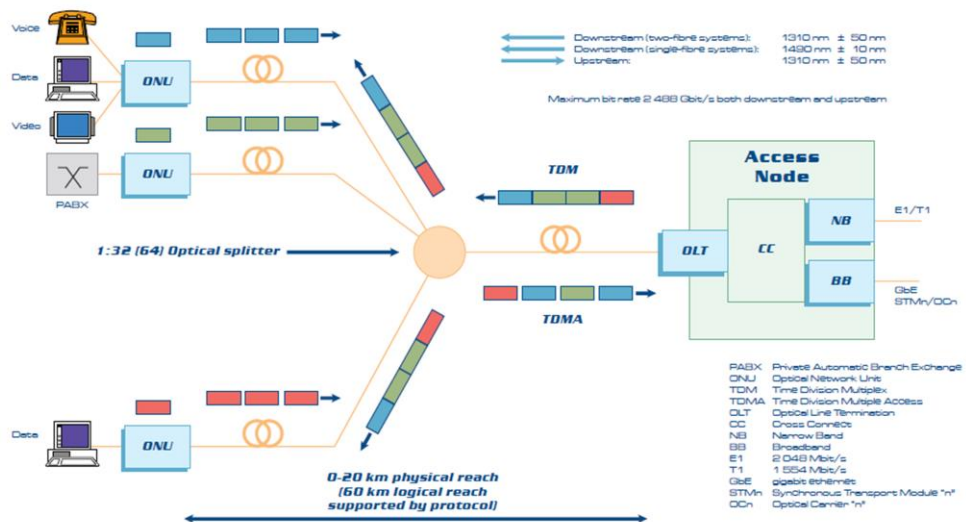




## FTTdp



# Architettura GPON



Il massimo fattore di splitting nelle GPON è 1:64 al livello fisico, ma la OLT è in grado di gestire 1:128 al livello MAC, in previsione dell'uso di amplificatori ottici in rete. Così pure la massima distanza tra OLT e ONU di 20 km è da intendere in modo differenziale, in quanto il livello MAC può gestire valori di *round trip delay* fino a 60 km (*Long-reach PON*).

## TIM SMART FIBRA

### FTTCab (VDSL2)

#### TIM SMART FIBRA

Velocità di trasmissione è fino a **50 Mbps** in download e fino a 10 Mbps in upload






#### TIM SMART SUPERFIBRA

fino a **100 Mbps** in download e fino a 20 Mbps in upload

### FTTH

fino a **300 Mps** in download e fino a 20 Mps in upload,  
Milano

# Offerta Fibra Ottica

FTTH		Absolute Fibra	100 Mbps
FTTC		Fibra Full	
FTTH/FTTC		Jet Fibra 100	
		Super Fibra	
		Naviga veloce e senza limiti fino a <b>300 Mega in download</b> e <b>100 Mega in upload.</b>	
FTTH		Roma	



Mondo Vodafone » Comunicati Stampa

## Vodafone lancia la prima offerta fibra a 500 Mbps

di Flaviolncarbone | 18/04/2016 16:45

*A Milano Bologna e Torino la rete più veloce d'Italia  
Vodafone-Netflix anche sulla fibra*



Milano, 18 aprile 2016 – Vodafone lancia la fibra a 500 Mbps con tecnologia Fiber to the Home (FTTH) nelle città di Milano, Bologna e Torino, diventando così il primo operatore a raggiungere questa velocità in Italia.

Con la connessione fino a 500 Mbps i clienti Vodafone potranno usufruire di servizi differenzianti, ottimizzare la qualità di streaming audio e video, accelerare il download di file e contenuti multimediali, diminuendo sensibilmente la latenza ed i tempi di attesa. Con la fibra a 500 Mbps si ottengono le migliori performance anche avendo più dispositivi connessi contemporaneamente alla propria rete domestica.

## Vodafone: per la prima volta in Italia raggiunti 1 Gbps su 4G e 10 Gbps su Fibra

di Flaviolncarbone | 02/03/2016 15:30

*Con il Piano Spring già coperto il 95% della popolazione in 4G, servizi in Fibra disponibili in oltre 200 città*



Milano, 2 marzo 2016 – Oggi a Milano **Vodafone** ha mostrato per la prima volta in Italia le potenzialità della rete mobile **4G** a **1,2 Gigabit al secondo** e della banda ultra larga su rete in **Fibra** d'accesso a **10 Gigabit al secondo**. Attraverso la prima applicazione su apparati commerciali, Vodafone ha illustrato le prospettive delle nuove reti ultraveloci fisse e mobili.

L'evoluzione della rete mobile è stata realizzata combinando tutte le frequenze radio oggi disponibili per realizzare la connessione mobile a 1,2 Gbps, mentre per la fibra l'utilizzo della tecnologia **10GPON** ha permesso di raggiungere in accesso i 10 Gbps. In

entrambi i casi è stata utilizzata tecnologia Huawei.



Rete globale

<http://www.geant.org/Networks>

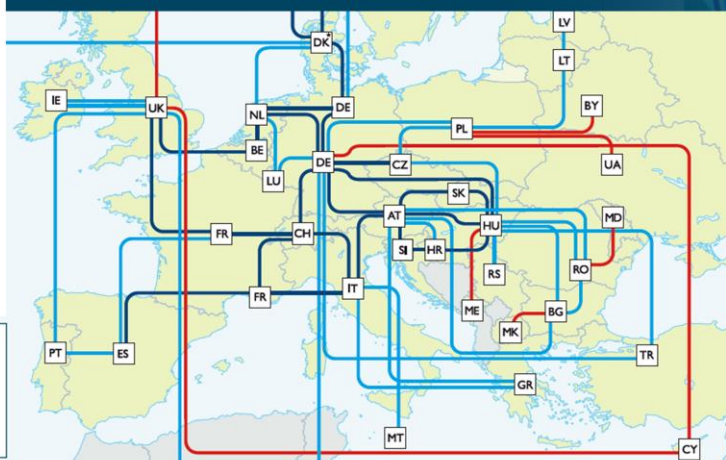


### GÉANT pan-European network

Europe's essential terabit-ready network is the most advanced and well-connected research and education network in the world.

**GÉANT provided the fast and convenient 500G bandwidth Network in the world**

- 1–9 Gbps
- multiples of 10 Gbps
- multiples of 100 Gbps



## **CAPITOLO 2**

### **Le reti LAN: Ethernet e sue evoluzioni Wireless LAN**

#### **Sommario**

- Il livello fisico e il livello Data-Link
- Definizione di LAN
- Soluzioni topologiche
- Il progetto IEEE 802
- La tecnologia CSMA/CD
- Ethernet e sue evoluzioni
- Wireless LAN



## LAN (*Local Area Network*)

- La disponibilità di un **unico canale fisico a velocità elevata e con basso tasso di errore**, condiviso nel tempo da tutte le stazioni, ha come conseguenza che:
  - Quando un sistema trasmette diventa temporaneamente proprietario del mezzo di comunicazione e dell'intera capacità trasmissiva
  - Quando un sistema trasmette tutti gli altri ricevono, la trasmissione è sempre di tipo broadcast
  - E' necessaria la presenza di indirizzi per stabilire mittente e destinatario
  - Occorre un meccanismo per arbitrare l'accesso al mezzo trasmissivo
- Il tipo di comunicazione è tipicamente **connectionless** e **best-effort** grazie al basso tasso di errore. La trasmissione è sempre sincrona e bilanciata, può essere **half-duplex** e **full-duplex**

[www.ncp-italy.com](http://www.ncp-italy.com)

Le reti LAN: Ethernet e sue evoluzioni 2-2

Una LAN è un sistema di comunicazione che permette a stazioni indipendenti di comunicare tra di loro utilizzando un unico canale fisico a velocità elevata e con basso tasso di errore.

Essi sono progettate per:

- **Operare entro un'area limitata**
- Permettere un accesso multiplo al mezzo a larga banda
- Controllare la rete privatamente attraverso una amministrazione locale
- Fornire una connettività a tempo pieno
- Connettere fisicamente dispositivi adiacenti.

La disponibilità di un solo canale trasmissivo condiviso nel tempo da tutte le stazioni ha come conseguenza che:

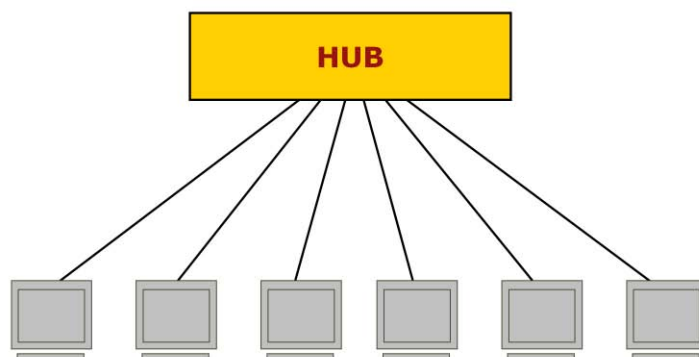
- Quando un sistema trasmette diventa temporaneamente proprietario **del mezzo di comunicazione e dell'intera capacità trasmissiva**
- Quando un sistema trasmette tutti gli altri ricevono, la trasmissione è sempre di tipo broadcast
- **E' necessaria la presenza di indirizzi per stabilire mittente e destinatario**
- **Occorre un meccanismo per arbitrare l'accesso al mezzo trasmissivo**

Il tipo di comunicazione è tipicamente **connectionless** e **best-effort** grazie al basso tasso di errore. La trasmissione è sempre sincrona e bilanciata, può essere half-duplex e full-duplex a seconda dei dispositivi di concentrazione utilizzati, hub nel primo caso, switch nel secondo.

Vedremo più avanti come queste problematiche sono state affrontate e risolte nelle tecnologie più utilizzate: Ethernet, Token Ring e FDDI.



## Cablaggio a stella



La topologia a stella implica la presenza di un **punto di concentrazione** al quale devono essere connessi tutte le stazioni. Questo approccio permette la realizzazione di un sistema di **cablaggio strutturato** semplificando molto la gestione e la manutenzione della rete.

[www.ncp-italy.com](http://www.ncp-italy.com)

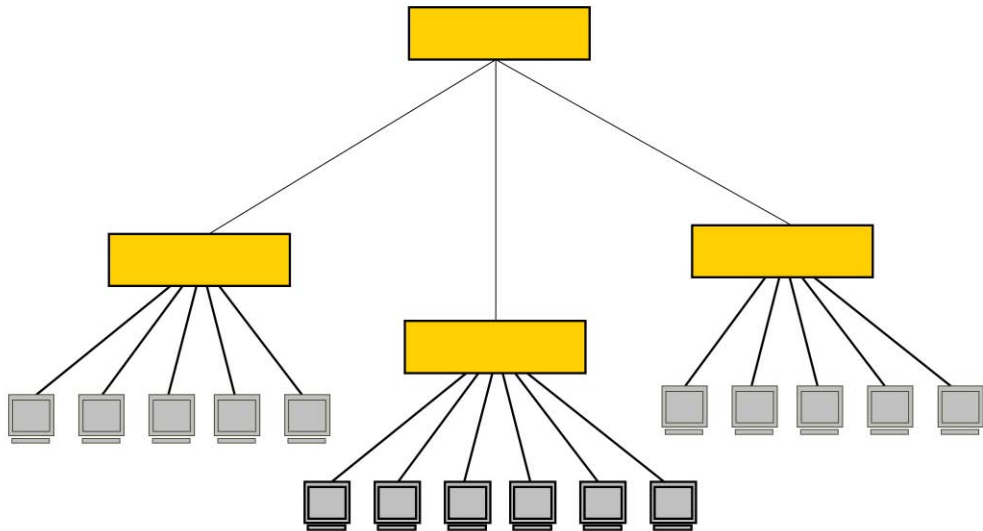
Le reti LAN: Ethernet e sue evoluzioni 2-3

La topologia a stella implica la presenza di un centro stella, un nodo che, per assicurare una trasmissione di tipo broadcast, si limita a ripetere il **segnale che riceve da un'interfaccia su tutte le altre, e non fa quindi una commutazione.**

La stella si realizza collegando ogni macchina al centro stella attraverso un doppio collegamento, uno per ogni direzione, utilizzando tipicamente Twisted Pair o fibra ottica.



## Struttura logica ad albero

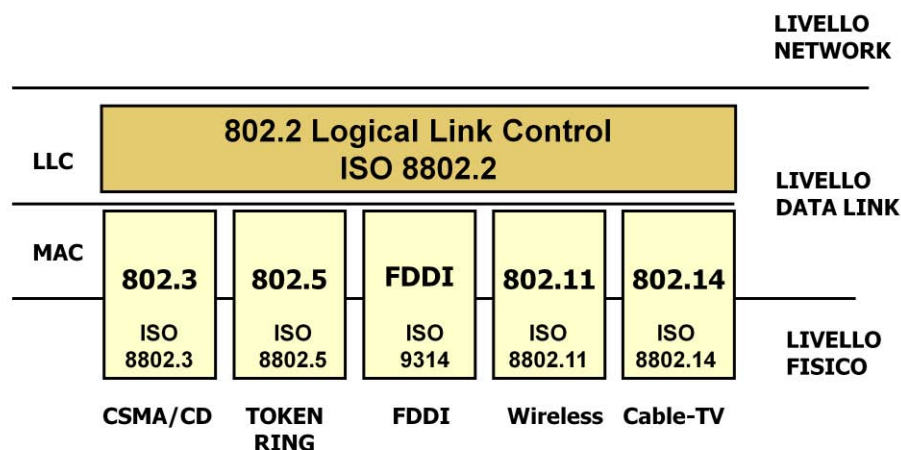


Le reti LAN: Ethernet e sue evoluzioni 2-4

In un sistema a stella è possibile isolare porzioni della rete mal funzionanti senza inficiare sulla operatività del sistema. D'altro canto ogni centro stella rappresenta un punto critico per l'affidabilità della rete, poiché un suo guasto significherebbe l'interruzione del collegamento di tutti i sistemi ad esso attestati. In genere la stella si trasforma in una **gerarchia logica ad albero** favorendo la scalabilità del sistema.



## Il progetto IEEE 802



[www.ncp-italy.com](http://www.ncp-italy.com)

Le reti LAN: Ethernet e sue evoluzioni 2-5

Quando, all'inizio degli anni '80, cominciarono a diffondersi le prime reti locali (ARC, Token Ring, Ethernet), IEEE decise di avviare un progetto per la standardizzazione delle LAN e delle MAN (Metropolitan Area Network). Furono così, costituiti sei comitati raccolti nel progetto IEEE 802 (il numero **802** fu scelto proprio per ricordare il mese di Febbraio dell'80 in cui furono definiti gli standard per i primi due livelli della pila OSI). Questi comitati sono:

- 802.1 Internetworking;
- 802.2 Logical Link Control;
- 802.3 Ethernet;
- 802.4 Token Bus;
- 802.5 Token Ring;
- 802.6 MAN.

A questi comitati, si aggiunsero in seguito altri quali, citando solo i più noti:

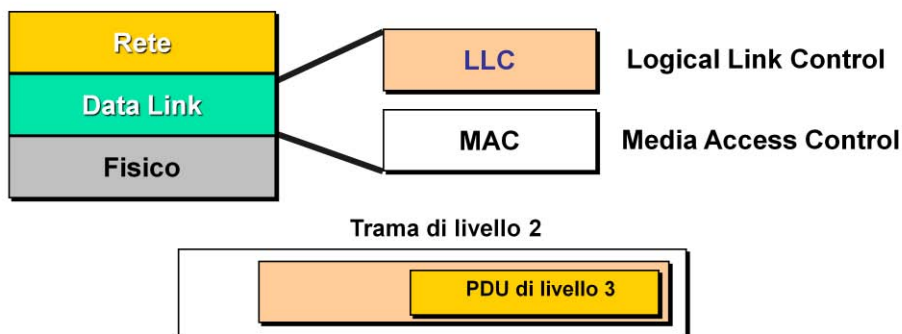
- 802.8 Fiber-Optics Technical Advisory Group;
- 802.9 Integrated Services Data Networks (ISDN);
- 802.10 Network Security;
- 802.11 Wireless Networks;
- 802.14 Cable Modem.

**IEEE 802 introduce l'idea che le LAN devono fornire un'interfaccia unificata verso il livello Rete (Network), pur utilizzando tecnologie trasmissive diverse. Per raggiungere questo scopo il livello di Linea (Data Link) è stato scisso in due sottolivelli, quello che interfaccia la parte superiore della pila OSI, quella logica, e quello che interfaccia la parte inferiore, quella fisica.**





# Trame e Sottolivelli



- **LLC si interfaccia con il livello logico superiore**  
Recupero errori, controllo di flusso, sequenzializzazione e conferma
- **MAC si interfaccia con il livello fisico inferiore**  
Controllo di accesso, indirizzamento, 'framing', controllo di errore

[www.ncp-italy.com](http://www.ncp-italy.com)

Le reti LAN: Ethernet e sue evoluzioni 2-6

I sottolivelli o sublayers sono:

- LLC (Logical Link Control)
- MAC (Media Access Control)

**Il livello MAC si occupa di gestire l'accesso al mezzo fisico, di conseguenza risulta fortemente influenzato dalla soluzione tecnologica adottata a livello 1 (Ethernet, Token Ring, FDDI).**

Il livello LLC ha invece lo scopo di gestire lo scambio delle informazioni con i livelli logici superiori e il compito di introdurre eventuali servizi di livello 2. Questo sottolivello è comune a tutte le tecnologie di LAN, quindi è indipendente dalla struttura e dalla topologia della rete, dal mezzo di **trasmissione utilizzato e dal MAC, ed è descritto nell'apposito standard IEEE 802.2.**

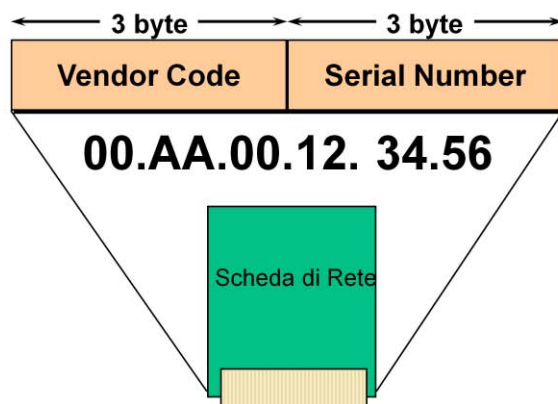
In particolare LLC offre 3 possibili servizi:

1. Il servizio LLC1, di tipo non connesso senza acknowledgement
2. Il servizio LLC2, di tipo connesso con acknowledgement
3. Il servizio LLC3, di tipo non connesso con acknowledgement

**Per esempio, nelle reti LAN l'utilizzo della tecnologia Ethernet prevede un servizio tipo LLC1, mentre nelle trasmissioni che richiedono sempre una modalità connessa e con meccanismi di ack e ritrasmissione, si utilizza un servizio tipo LLC2.**



## Gli indirizzi MAC



- **L'indirizzo MAC è integrato nella scheda di rete**

L'indirizzo MAC, conosciuto anche come indirizzo fisico, o indirizzo hardware, rappresenta il codice che univocamente identifica la scheda di rete. Il MAC è integrato nella scheda stessa, direttamente dal costruttore, nel momento della produzione. Dovunque la scheda vada, porterà con sé questo indirizzo. L'utente può definire l'indirizzo logico di una stazione, quello di livello 3, ma non l'indirizzo fisico (con delle eccezioni che qui non tratteremo).

L'indirizzo MAC è composto da sei byte ed è diviso in due parti: 3 byte rappresentano l'OUI (Organizational Uniform Identifier) che identifica il costruttore, e tre byte un numero seriale univoco (Serial Number) stabilito dal costruttore stesso. Gli OUI detti anche "Vendor Code" (Codice del venditore) sono assegnati da IEEE.



## Codici OUI

OUI	Costruttore
00-00-0C	Cisco
00-00-AA	Xerox
00-AA-00	Intel
08-00-5A	IBM
02-60-8C	3Com
08-00-07	Apple
00-00-C6	HP

Le reti LAN: Ethernet e sue evoluzioni 2-8



# Ethernet (1)

- Xerox Digital Equipment e Intel nel 1982 rilascia **Ethernet versione II**,
- **IEEE 802.3**, sulla base delle specifiche di Ethernet II, sviluppa il proprio standard
- Le due specifiche Etrhernet II e 802.3 sono in grado di convivere
- **Tecnologia CSMA/CD**: *Carrier Sense Multiple Access with Collision Detection*.
  - **Carrier Sense** (rilevazione della trasmissione) è il principio secondo il quale ogni stazione, prima di trasmettere, deve verificare se il mezzo trasmissivo è libero, si parla in questo caso di *listen before talking*.
  - **Multiple access** esprime la condizione per cui due o più stazioni, sentendo il mezzo libero, decidono di trasmettere contemporaneamente entrando quindi in conflitto tra loro.
  - **Collision Detection** è la fase di rilevazione di un evento di sovrapposizione tra due o più trasmissioni, cioè, di una cosiddetta "collisione". Per accorgersi di una collisione le stazioni devono poter ascoltare il mezzo trasmissivo mentre trasmettono, si parla in questo caso di *listen while talking*.
- Tecnologia **"indeterministica"**
  - non esiste un tempo massimo di attesa prima di poter trasmettere; in linea di principio una stazione potrebbe sempre trovare il mezzo occupato o incappare in una collisione.

I primi lavori di sviluppo di Ethernet furono eseguiti da Xerox a cui si unirono in seguito Digital Equipment e Intel. Insieme definirono la prima specifica nel 1980. Successivamente lo stesso gruppo nel 1982 rilasciò la versione definitiva conosciuta come Ethernet versione II, a volte chiamato anche DIX Ethernet dalle iniziali dei costruttori. In seguito la commissione IEEE 802.3, sulla base delle specifiche di Ethernet II, sviluppò il proprio standard che ricalca l'approccio di Xerox, Intel e Digital per il modo in cui è realizzato l'accesso al mezzo introducendo al contempo delle differenze nella descrizione complessiva del livello Data Link che analizzeremo più avanti. Oggi le due specifiche Etrhernet II e 802.3 sono in grado di convivere grazie a delle opportune convenzioni che permettono ai software delle schede di rete di riconoscere e quindi utilizzare le due differenti versioni.

Il tipo di tecnologia utilizzata da Ethernet si chiama CSMA/CD che significa **Carrier Sense Multiple Access with Collision Detection**. La sigla sintetizza i tre principi fondamentali operativi di Ethernet.

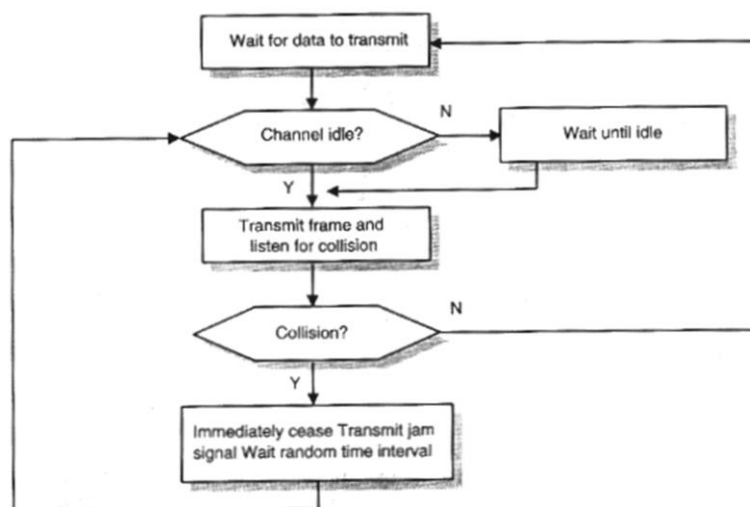
**Carrier Sense**(*rilevazione della trasmissione*) è il principio secondo il quale ogni stazione, prima di trasmettere, deve verificare se il mezzo trasmissivo è libero, si parla in questo caso di *listen beifore talking*.

**Multiple access** esprime la condizione per cui due o più stazioni, sentendo il mezzo libero, decidono di trasmettere contemporaneamente entrando quindi in conflitto tra loro.

**Collision Detection** è la fase di rilevazione di un evento di sovrapposizione tra due o più trasmissioni, cioè, di una cosiddetta "collisione". Per accorgersi di una collisione le stazioni devono poter ascoltare il mezzo trasmissivo mentre trasmettono, si parla in questo caso di *listen while talking*. Il meccanismo delle collisioni è un modo per arbitrare il canale che può produrre una limitazione di banda disponibile qualora se ne generassero in numero elevato.



## Ethernet (2)



www.ncp-italy.com

Le reti LAN: Ethernet e sue evoluzioni 2-10

Le topologie di cablaggio previste per Ethernet sono 3: bus, stella e punto-punto.

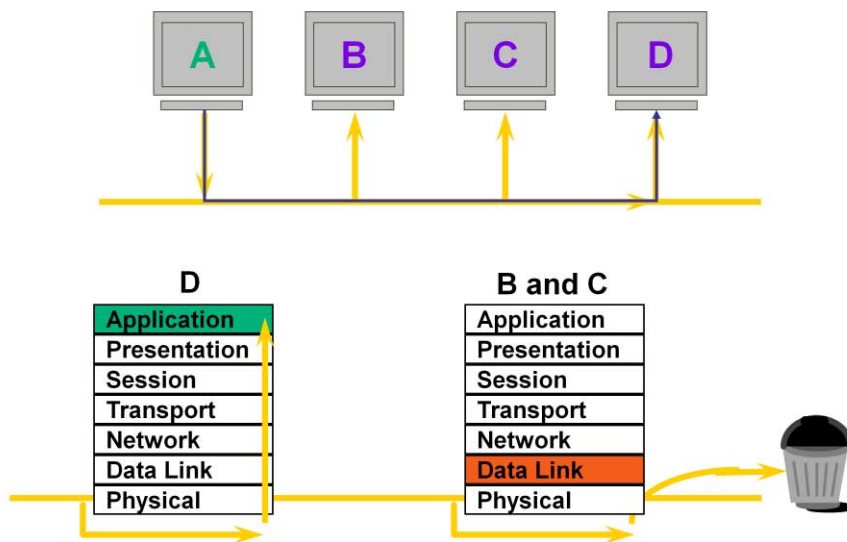
I mezzi trasmissivi ammessi sono: cavo coassiale (tipo thick e tipo thin), doppini (Twisted-Pair), fibre ottiche, CATV.

Per indicare le diverse soluzioni, a livello fisico, si utilizza una convenzione particolare composta da due numeri che precedono e succedono le parole "base" e "broad". La parola "base" sta per *baseband* e indica una trasmissione in banda base, mentre, la parola "broad" sta per *broadband* e indica una trasmissione multiplata su vari canali. Il numero che precede indica la velocità di trasmissione, mentre, il numero che succede indica le caratteristiche del mezzo. Ognuna delle soluzioni illustrate in tabella ha proprie caratteristiche e proprie limitazioni imposte dal mezzo trasmissivo utilizzato, tutte devono però rispettare, a livello fisico, i seguenti due parametri:

- il numero massimo delle stazioni collegabili è 1024
- la distanza massima ammessa tra due stazioni è 4 km



## Ethernet/802.3: operazioni



www.ncp-italy.com

Le reti LAN: Ethernet e sue evoluzioni 2-11

In fase di ricezione sono eseguiti sulla trama i seguenti controlli:

- **controllo della lunghezza della trama**, che deve essere compresa tra una dimensione minima e una massima (per Ethernet LEN MIN = 64 byte, LEN MAX=1518 byte);

- **controllo dell'integrità della trama**, viene ricalcolato il CRC e confrontato con il valore del campo FCS della trama ricevuta

- **controllo dell'indirizzo MAC destinazione**, che deve corrispondere a quello della stazione ricevente;

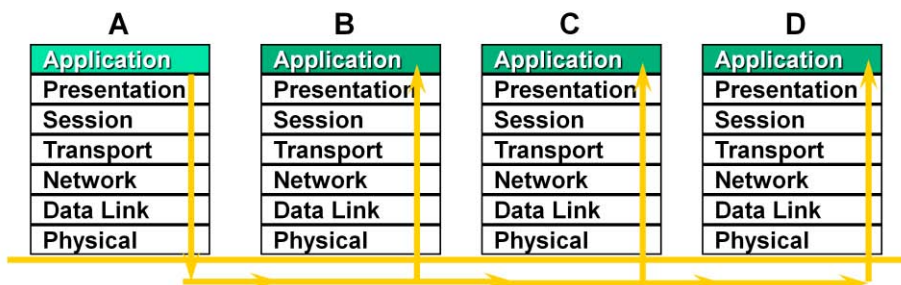
E' sufficiente che, solo una di queste verifiche fallisca, per far sì che la trama sia scartata.

Nel caso di successo, viene estratto il contenuto informativo della trama e passato alla CPU dell'elaboratore

Queste funzioni sono implementate nella scheda di rete.



## Ethernet/802.3 Broadcast



MAC Destinazione = FFFF.FFFF.FFFF

Esistono tre tipologie di indirizzi:

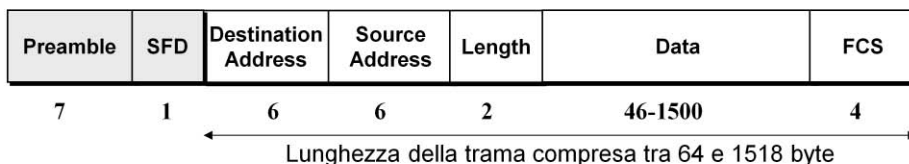
- Indirizzi Unicast: identificano in modo univoco una sola stazione
- Indirizzi Multicast: identificano un gruppo di stazioni
- Indirizzi Broadcast: identificano tutte le stazioni presenti su una rete

A livello MAC è definita una convenzione per distinguere le tre tipologie appena descritte. Se il primo bit trasmesso **dell'indirizzo** MAC di destinazione è uguale a zero si ha un indirizzo unicast, altrimenti un multicast. Se anche tutti i bit che seguono sono pari a 1 allora si ha un broadcast, in notazione esadecimale si ha FF.FF.FF.FF.FF.FF. Ogni stazione che riceve una trama di tipo broadcast deve accettarla, se ovviamente i controlli di integrità e lunghezza vanno a buon fine. Questo implica che la CPU **dell'elaboratore** deve necessariamente fermarsi per processare il pacchetto generando così un **interrupt**. Quando il tipo di protocolli utilizzati fa un largo uso di broadcast, si possono sperimentare delle degradazioni nelle prestazioni delle stazioni in rete. Nel caso del multicast la stazione per accettare la trama e processarla deve far parte di un cosiddetto **"gruppo di multicast"** al quale corrisponde uno specifico indirizzo. Per applicazioni multicast sono riservati gli indirizzi da 01.00.5E.00.00.00.00 a 01.00.5E.7F.FF.FF.



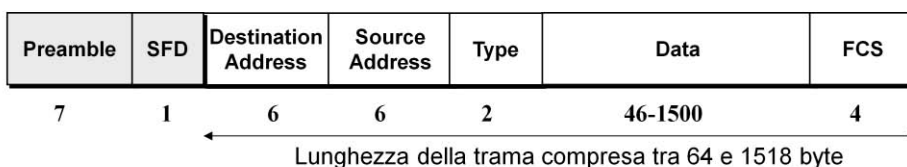
# Struttura delle trame Ethernet

## Ethernet IEEE 802.3



Preamble e SFD (Start Frame Delimiter) sono utilizzati per la sincronizzazione delle stazioni

## Ethernet II



Type = 0800 (IP), Type = 0806 (ARP), Type = 0000÷05DC (Length)

[www.ncp-italy.com](http://www.ncp-italy.com)

Le reti LAN: Ethernet e sue evoluzioni 2-13

La frame definita da Ethernet 802.3 differisce da Ethernet II per la quale non è previsto un livello LLC. La differenza sta nella diversa funzione dei campi TYPE e Length. Nel caso di 802.3 Length rappresenta la lunghezza del campo Data espressa in ottetti. Nel caso di Ethernet II, non essendo previsto un livello LLC, il campo TYPE rappresenta il tipo di protocollo di livello 3 incapsulato direttamente nel campo Data (p.e.: se TYPE = 0x0800 il livello 3 è costituito da IP). Le due versioni sono comunque interoperabili grazie ad una convenzione che permette ai driver di comprendere e quindi gestire il tipo di frame ricevuta. Se nel campo Length è presente un valore minore uguale di 1500 (0x05DC) i driver interpreteranno la frame come IEEE 802.3 altrimenti come Ethernet II. Infatti, lo standard prevede una lunghezza della trama, escluso il preambolo, compresa tra 64 e 1518 byte. Poiché la somma dei campi è uguale a 18 byte ne consegue che il campo Data non può essere maggiore di 1500 byte, quindi il campo Length non può assumere mai valori maggiori di 1500.

In testa ad ogni trama c'è un preambolo costituito da 7 ottetti che serve alla stazioni ricevente per sincronizzarsi con la trasmittente. Il preambolo è seguito da un campo chiamato SFD (**Start Frame Delimiter**) costituito da una sequenza di bit pari a 11010101; esso indica la fine del preambolo e l'inizio della trama.

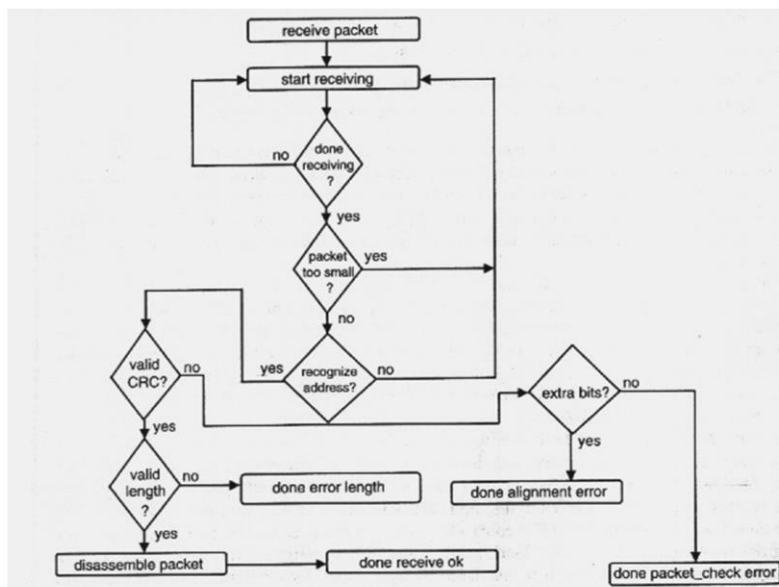
Il campo **Destination Address** è costituito dall'indirizzo MAC della stazione destinataria, mentre, nel campo **Source Address** è presente l'indirizzo della stazione sorgente. Il campo FCS (**Frame Check Sequence**) contiene il valore di CRC calcolato dalla stazione mittente sulla base dei campi che lo precedono.

Non esiste un segnalatore di fine trama, le trame si distinguono tra loro attraverso un intervallo di tempo che le separa temporalmente. La durata di questo intervallo non può scendere al disotto di un valore minimo fissato di 9,6 µs.





## Gestione della trama in ricezione



www.ncp-italy.com

Le reti LAN: Ethernet e sue evoluzioni 2-14

In fase di ricezione sono eseguiti sulla trama i seguenti controlli:

- **controllo della lunghezza della trama**, che deve essere compresa tra una dimensione minima e una massima (per Ethernet LEN MIN = 64 byte, LEN MAX=1518 byte);
- **controllo dell'integrità della trama**, viene ricalcolato il CRC e confrontato con il valore del campo FCS della trama ricevuta
- **controllo dell'indirizzo MAC destinazione**, che deve corrispondere a quello della stazione ricevente;

E' sufficiente che, solo una di queste verifiche fallisca, per far sì che la trama sia scartata.

Nel caso di successo, viene estratto il contenuto informativo della trama e passato alla CPU dell'elaboratore

Queste funzioni sono implementate nella scheda di rete.



## Sviluppi di Ethernet

- **Fast Ethernet** (progetto IEEE 802.3u ) 100Mbps
  - 100BaseTX: definisce le specifiche per l'utilizzo di cavi di categoria 5 UTP con due coppie per la trasmissione e la ricezione.
  - 100Base T4 : prevede l'utilizzo anche di cavi di categoria 3,4 UTP con 3 coppie per la trasmissione e ricezione e una per la rilevazione delle collisioni.
  - 100BaseFX: definisce le specifiche per la trasmissione su fibra ottica multimodale 62.5/125 microm..
- **Gigabit Ethernet** (progetto IEEE 802.3uz) 1 Gbps.
  - 1000BaseLX: definisce le specifiche per trasmissioni di tipo *long-wave laser* su fibra mono e multimodale.
  - 1000BaseSX: definisce le specifiche per trasmissioni di tipo *short-wave laser* su fibra multimodale.
  - 1000BaseCX: definisce le specifiche per trasmissioni su cavi in rame bilanciati e schermati a 150 ohm.
  - **1000BASE-T** (progetto 802.3ab) per un livello fisico in grado di utilizzare il classico doppino, per distanze massime di 100 metri.
- **10 Gigabit** (progetto IEEE 802.3ae)
  - Eliminato il meccanismo di CSMA/CD
  - solo tipo di trasmissione full duplex su fibra ottica mono-multimodale
  - Fino a 40 Km con **10GBASE-ER** (80 Km 10GBASE-ZR fuori standard)
  - **10GBase-T progetto IEEE 802.3an-2006** per un livello fisico in grado di utilizzare il classico doppino, per distanze massime di 100 metri.

[www.ncp-italy.com](http://www.ncp-italy.com)

Le reti LAN: Ethernet e sue evoluzioni 2-15

Ethernet si è ormai imposta come unica soluzione LAN. Questo processo che era già in atto alcuni anni fa, grazie alla sua facilità di installazione e manutenzione, ha subito una fortissima accelerazione. Due nuove tecnologie si sono rese con gli anni disponibili: la tecnologia Fast Ethernet (progetto IEEE 802.3u ) che ha portato la velocità di trasmissione a 100Mbps e Gigabit Ethernet (progetto IEEE 802.3uz) con la quale si è raggiunto 1 Gbps. **Esiste inoltre un'altra specifica sviluppata all'interno di IEEE 802.3 Working Group, nota come 1000BASE-T, che è stata sviluppata per un livello fisico in grado di utilizzare quattro coppie in rame non schermate di categoria 5, per distanze massime di 100 metri. Questo progetto è anche noto come 802.3ab.**

La tecnologia Ethernet non conosce sosta, i nuovi sviluppi prevedono già uno standard a 10 Gigabit. Alcuni apparati in commercio già supportano interfacce a questa velocità. Lo standard in ambito IEEE si chiama 802.3ae. Le novità rispetto alle versioni precedenti consistono **nell'eliminare il meccanismo di CSMA/CD prevedendo il solo tipo di trasmissione full duplex esclusivamente su fibra ottica mono-multimodale.** Rimane invariata, invece, la frame con le sue specifiche di lunghezza **massima e minima. L'altra importante novità è l'ampliamento dell'ambito di applicazione che investirà anche le WAN.** Infatti la distanza massima raggiungibile con fibra monomodale è stata elevata a 40 Km. Per maggiori informazioni consultate il sito di Gigabit Ethernet Alliance <http://www.gea.org>.



## Standard P802.3ba

- 40 Gigabit Ethernet, o **40GbE**, e 100 Gigabit Ethernet o **100GbE**
- Progetto partito nel 2007 e ratificato a maggio 2010
- Lo standard supporta solo il full duplex.
- Conserva la struttura della frame 802.3
- Mantiene minimum e maximum FrameSize di 802.3
- Supporta un bit error ratio (BER) migliore o uguale a  $10^{-12}$
- Supporta MAC data rates di 40 e 100 Gbit/s
- Fornisce specifiche a Physical Layer (PHY) per operazioni su single-mode optical fiber (SMF), OM3 multi-mode optical fiber (MMF), copper cable assembly, and backplane.

	40 Gigabit Ethernet	100 Gigabit Ethernet
At least 1m backplane	40GBASE-KR4	
At least 10m copper cable	40GBASE-CR4	100GBASE-CR10
At least 100m OM3 MMF	40GBASE-SR4	100GBASE-SR10
At least 10km SMF	40GBASE-LR4	100GBASE-LR4
At least 40km SMF		100GBASE-ER4

[www.ncp-italy.com](http://www.ncp-italy.com)

Le reti LAN: Ethernet e sue evoluzioni 2-16



## Power over Ethernet

- I vantaggi derivanti dall'applicazione della tecnologia PoE ai sistemi di sorveglianza IP sono molteplici:
  - PoE è una fonte di alimentazione intelligente
  - PoE rende più semplice e più economico consolidare l'erogazione di energia per sistemi VoIP e "IP Surveillance"
  - Lo standard di base è denominato **802.3af** e supporta l'erogazione di 12,95 W
  - Per andare incontro alle maggiori esigenze energia (p.e.: brandeggio delle videocamere) è stato ideato lo standard **802.3at** (denominato *PoE Plus*) che consente l'erogazione di 30 W.

**Power over Ethernet:** un altro ottimo motivo per migrare alla sorveglianza IP. Da sempre l'installazione di cavi per i sistemi di sicurezza è un processo dispendioso. I costi però possono lievitare ulteriormente se è necessario collegare in rete anche gli impianti di controllo degli accessi e antincendio. Senza dimenticare l'alimentazione. Le telecamere CCTV analogiche e altri dispositivi, come i multiplexer e i DVR richiedono un'alimentazione (cavi, uscite CA e prese) indipendente, che implica necessariamente doversi rivolgere ad elettricisti per ogni installazione. Infine, in molti casi è necessario predisporre gruppi di continuità (UPS) distinti per tutti i dispositivi dei sistemi "mission critical" per far fronte ad eventuali interruzioni dell'alimentazione. Elementi che hanno un grosso impatto sui costi.

Trasmissione sicura dell'energia elettrica ai dispositivi in rete senza alcuna riduzione delle prestazioni della rete

**Power over Ethernet (PoE)**, noto anche come Power over LAN, permette di ridurre i costi di utilizzo dei sistemi di sorveglianza basati su IP fino all'80% rispetto alle installazioni analogiche tradizionali. PoE è una tecnologia rivoluzionaria che integra dati, voce e alimentazione in un'infrastruttura LAN standard, utilizza cavi di rete Ethernet standard (CAT-5) ed alimenta i dispositivi di rete direttamente dalle porte a cui sono collegati. I cavi Ethernet CAT-5 standard sono costituiti da quattro coppie di doppi intrecciati, di cui solo due utilizzati per la trasmissione dei dati su reti 10BASE-T e 100Base-T. Gli altri due possono essere impiegati per alimentare dispositivi in rete.

## Quali vantaggi offre la nuova tecnologia?

I vantaggi derivanti dall'applicazione della tecnologia PoE ai sistemi di sorveglianza IP sono molteplici e vanno ben oltre i risparmi sui costi di installazione.

- **PoE è una fonte di alimentazione intelligente**

Le apparecchiature di alimentazione rese disponibili dalla tecnologia PoE consentono una gestione ottimale del sistema poiché utilizzano i protocolli esistenti come il Simple Network Management Protocol (SNMP). Ciò consente di scollegare la rete dall'alimentazione centralmente, ad esempio per effettuare interventi di manutenzione.

- **PoE rende più semplice e più economico consolidare l'erogazione di energia ai sistemi di sorveglianza IP**

La centralizzazione dell'alimentazione attraverso gli hub PoE (chiamati mid-span) permette di collegare i sistemi basati su PoE al gruppo di continuità (UPS) centrale che supporta generalmente la maggior parte della rete costituita da uno o due PC. Questa configurazione evita che eventuali interruzioni nell'alimentazione si ripercuotano sull'integrità del sistema di sorveglianza IP.

- **Gli hub PoE consentono ai responsabili della sicurezza di disattivare e reimpostare i dispositivi remotamente**

I sistemi PoE sono in grado di individuare con precisione i dispositivi in rete difettosi e di consentire ai responsabili di ripristinarli mediante la semplice pressione di un tasto. Questi dispositivi possono essere isolati dall'alimentazione, sostituiti da dispositivi nuovi e quindi riattivati.

- **La centralizzazione del controllo dell'alimentazione garantisce una maggiore sicurezza** limitando i problemi di vulnerabilità che possono verificarsi nel caso in cui il personale addetto alle pulizie o ai lavori edili abbia bisogno di utilizzare un punto di alimentazione di una videocamera.

- **PoE inoltre consente di massimizzare la copertura grazie ad un'installazione ottimale delle telecamere**

La nuova tecnologia permette agli installatori di installare le telecamere di rete in qualunque posizione, indipendentemente dalle fonti di alimentazione esistenti, che troppo spesso si trovano in prossimità dei battiscopa, ossia in posizione diametralmente opposta rispetto ai siti ottimali per le telecamere di sorveglianza.

## **Introduzione ai Protocolli e Standard 802.11**



## Propagazione del segnale radio

**Il segnale viene trasmesso radialmente dalla sorgente in tutte le direzioni.**

**La potenza del segnale trasmesso diminuisce in relazione alla distanza dalla sorgente:**

**Attraverso lo spazio libero la perdita della potenza di segnale è proporzionale al quadrato della distanza dalla sorgente.**

**In presenza di ostacoli (segnale riflesso), la perdita è proporzionale alla quarta potenza della distanza.**

### **PROPAGAZIONE DEL SEGNALE RADIO**

**Il segnale viene trasmesso radialmente dalla sorgente in tutte le direzioni.**

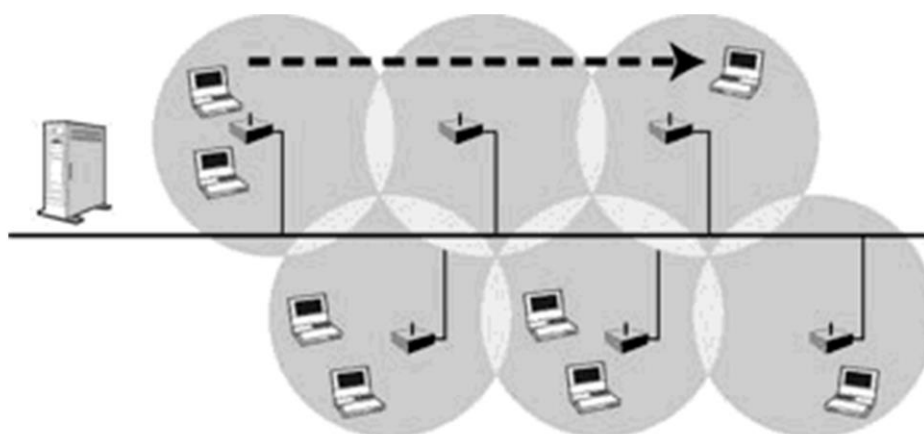
**La potenza del segnale trasmesso diminuisce in relazione alla distanza dalla sorgente:**

**☐Attraverso lo spazio libero la perdita della potenza di segnale è proporzionale al quadrato della distanza dalla sorgente.**

**☐In presenza di ostacoli (segnale riflesso), la perdita è proporzionale alla quarta potenza della distanza.**



## Infrastructure WLAN



[www.ncp-italy.com](http://www.ncp-italy.com)

Le reti LAN: Ethernet e sue evoluzioni 2-21

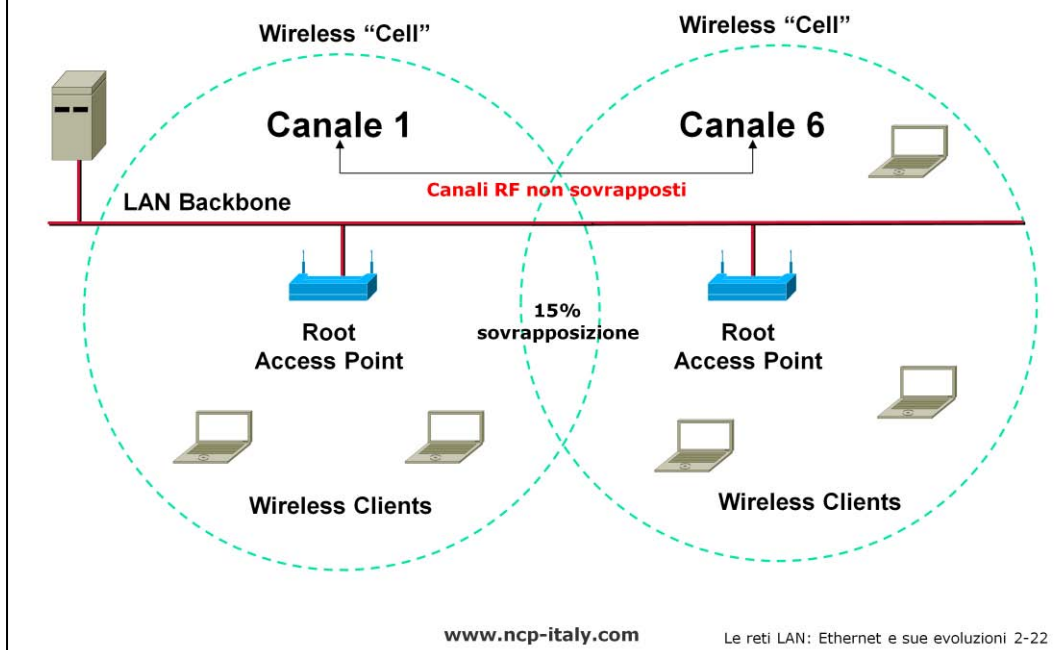
### Infrastructure WLAN

Nelle WLAN di tipo Infrastructure ***access point*** multipli collegano la rete wireless ad una rete cablata permettendo così la condivisione delle risorse tra le due diverse tipologie. In questo scenario gli ***access point***, oltre a mettere in comunicazione rete senza fili e rete con fili, svolgono una importante azione nella regolazione del traffico delle stazioni wireless **presenti nel proprio raggio d'azione**. Utilizzando **access points multipli** è possibile coprire un intero edificio o addirittura un campus.





## Access Point in topologia Root

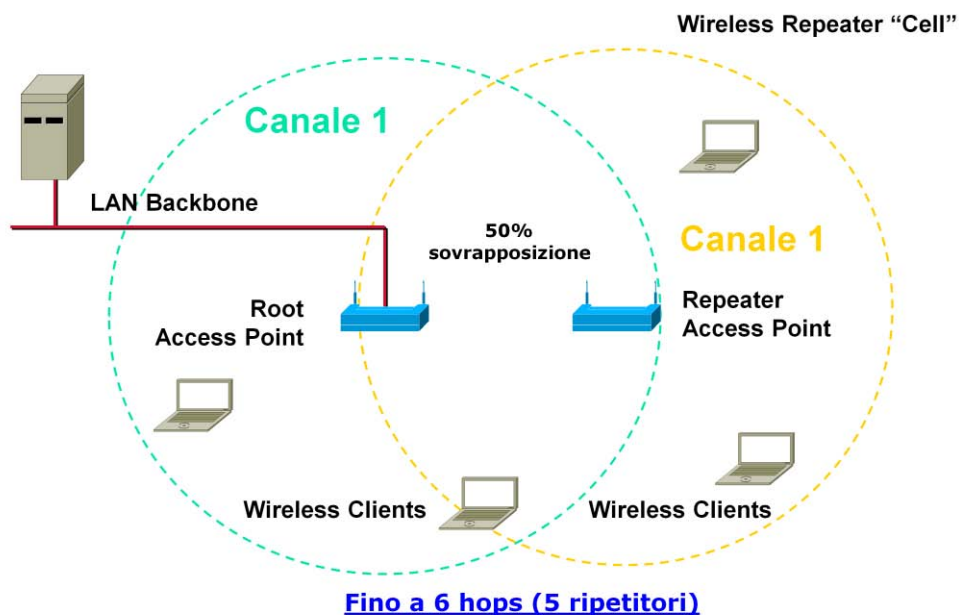


### Root (Access Point)

- Accetta associazioni e comunica soltanto con stazioni clients e repeaters.
- Non comunicherà con altri dispositivi Root.
- Qualunque numero di Root APs per sistema RF.



## Access Point in topologia Repeater



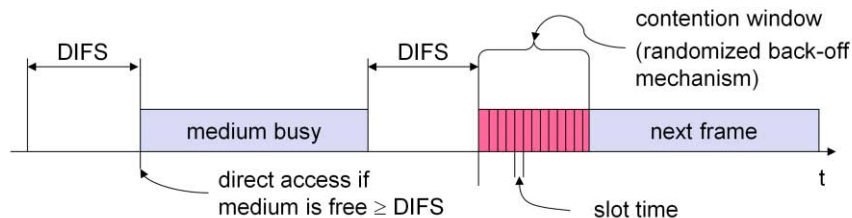
Le reti LAN: Ethernet e sue evoluzioni 2-23

### Non Root (Ripetitore)

- E' associato e comunica con un dispositivo Root=ON o un altro dispositivo Root=OFF che tuttavia è associato ad un Root=ON.
- Accetta associazioni e comunica soltanto con clients e ripetitori, finchè è registrato ad un dispositivo con Root=ON.



## CSMA/CA



- La stazione che ha dati da inviare inizia a sentire la presenza di segnale (Carrier Sense based on CCA-Clear Channel Assessment)
- Se il mezzo è libero per una durata pari ad IFS Inter-Frame Space, la stazione può iniziare ad inviare la frame di dati (IFS dipende dal servizio)
- Se il mezzo è occupato, la stazione deve attendere fino alla scadenza dell'IFS più un tempo addizionale Random Back-off (tempo multiplo di uno slot-time)
- Se un'altra stazione occupa il mezzo durante il tempo di back-off della stazione, il back-off timer si ferma (fairness).

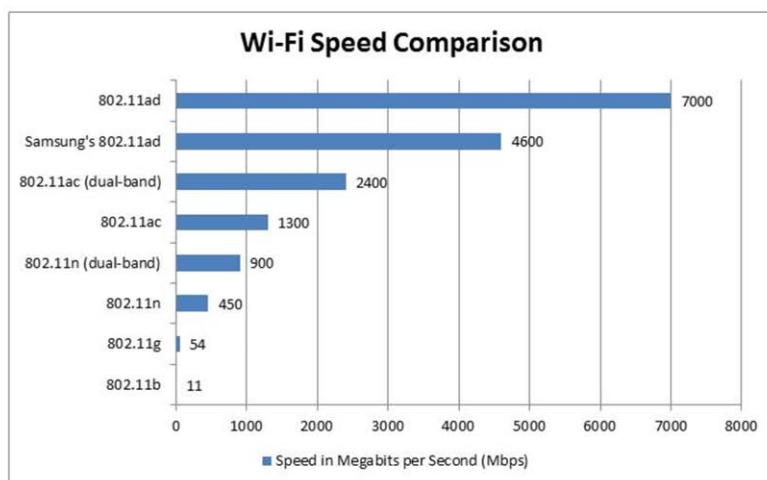
Le reti LAN: Ethernet e sue evoluzioni 2-24

La tecnologia di arbitraggio del mezzo utilizzata dalle reti wireless è conosciuta come CSMA/CA: *Carrier Sense Multiple Access with Collision Avoidance*. E' una tecnologia che al contrario di Ethernet gestisce l'arbitraggio del mezzo non attraverso il controllo delle collisioni ma attraverso la prevenzione di esse. Infatti, poiché nell'etere la rilevazione delle collisioni può facilmente non andare a buon fine, è preferibile evitare che si generino collisioni piuttosto che gestirle. Anche se in linea di principio la tecnologia CSMA/CA non può impedire la generazione di una collisione, di fatto la probabilità che l'evento si verifichi rimane molto bassa.

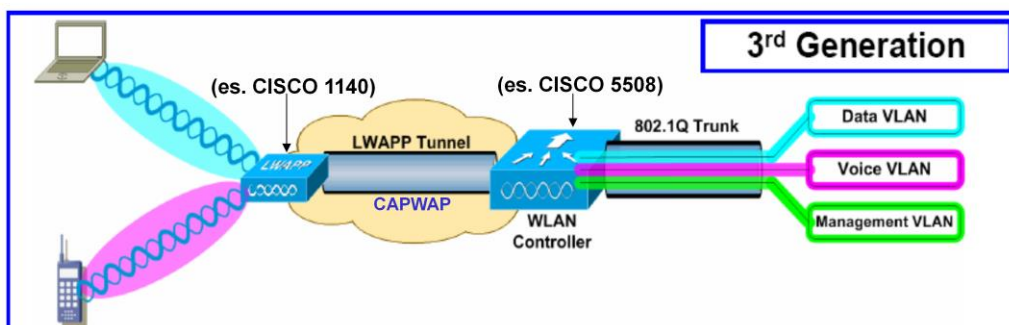
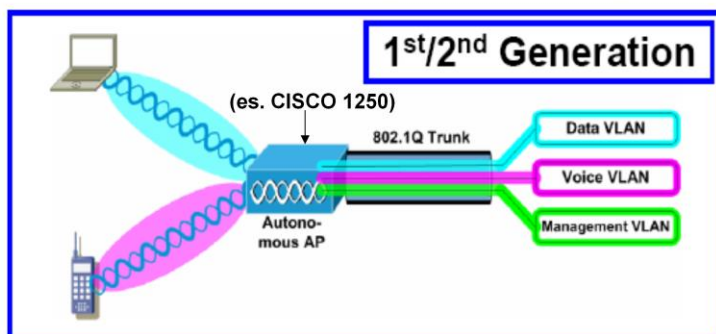
Come per Ethernet le stazioni verificano la disponibilità del mezzo mettendosi in stato di attesa se una trasmissione è già in atto. Al contrario di Ethernet, dove in caso di mezzo libero una stazione può liberamente iniziare la trasmissione, nelle reti wireless è, invece, prevista una fase di contesa molto articolata con lo scopo di evitare la generazione di collisioni.



## Evoluzione Wifi

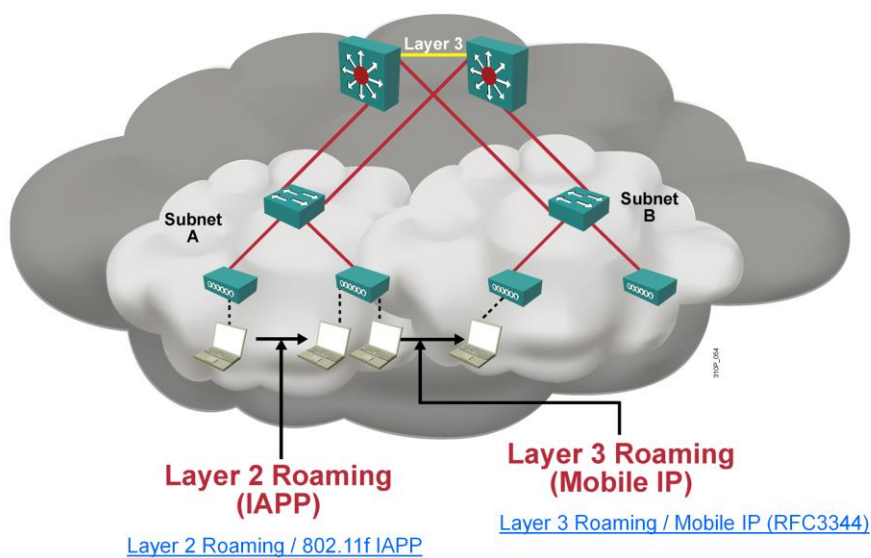


## EVOLUZIONE MODELLO WIRELESS AP DA UNO A DUE LIVELLI E SUPPORTO VLAN (MULTIPLE SSID)





## Layer 2 vs. Layer 3 Roaming



Le reti LAN: Ethernet e sue evoluzioni 2-27



## Reti Wireless e Sicurezza

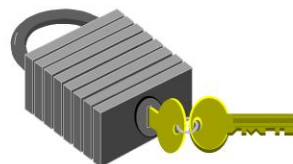
### ■ **WEP (Wired Equivalency Privacy)**

- Chiave a 40 bit e 128 bit WEP usa il protocollo cifrato RC4 della RSA Data Security, Inc. (RSADSI) per la cifratura.

### ■ **802.11i**

- Noto anche come WPA2, fornisce i migliori livelli di sicurezza
- Utilizza 802.11x per l'autenticazione e AES per la cifratura.

### ■ **VPN (virtual private network )**



[www.ncp-italy.com](http://www.ncp-italy.com)

Le reti LAN: Ethernet e sue evoluzioni 2-28

### **WEP**

Wired Equivalent Privacy (WEP) è un protocollo di sicurezza, definito seguendo lo standard IEEE Wireless Fidelity (Wi-Fi) , 802.11b, e creato per offrire una wireless local area network (WLAN) con un altissimo livello di sicurezza e privacy comparabile alle performance garantite da una wired LAN. Una wired local area network (LAN) è solitamente protetta da un sistema fisico di sicurezza (per sempio accessi controllati e sorvegliati all'edificio) che permette alti livelli di protezione nel caso si tratti di strutture fisiche da proteggere ,ma che al contrario può non risultare efficace nel caso di WLANs in quanto le onde radio non sono necessariamente contenute dalle pareti che limitano la rete aziendale. WEP offre un sistema di protezione simile a quello garantito dalle misure di protezione fisica della rete con l'aggiunta di un sistema di cifratura dei dati trasmessi nella WLAN.

### **VPN**

Una virtual private network (VPN) è uno strumento per utilizzare un'infrastruttura pubblica di telecomunicazione, come per esempio Internet, garantendo ai singoli utenti un accesso sicuro (sia da canale remoto che in azienda) alla rete aziendale. Una virtual private network è la soluzione alternativa ai sistemi molto costosi caratterizzati da linee dedicate (ossia di esclusivo utilizzo di un'unica azienda) .

### **802.11i**

802.11i è uno standard per la wireless local area networks (WLANs) in grado di fornire un sistema di crittografia per le reti che usano il diffuso 802.11a/b/g/n . Lo standard 802.11i il nuovo protocollo chiave di crittografia, chiamato Temporal Key Integrity Protocol (TKIP) e Advanced Encryption Standard (AES). Lo standard 802.11i è stato ufficialmente ratificato dallo IEEE nel giugno del 2004, diventando parte della famiglia 802.11 ossia acquisendo le specifiche delle reti wireless network. Le specifiche garantite dallo standard 802.11i offrono un livello di sicurezza sufficiente a soddisfare la maggior parte delle agenzie governative.



## Link utili

- <http://www.ciscopress.com>
- <http://www.ieee.org>
- <http://www.tiaonline.org>
- <http://www.eia.org>
- <http://www.gigabit-ethernet.org>
- <http://www.10gea.org>
- <http://www.bluetooth.com>
- <http://www.tuttoreti.com>
- <http://www.networkingitalia.it>

Bibliografia e link utili:

*CCNA INTRO Exam Certification Guide – Cisco Press*

*RETI LOCALI - Dal cablaggio all'internetworking - Gai, Montessoro, Nicoletti*

*Introduzione alle reti – Mondadori*

*Sistemi di comunicazione e Reti – Apogeo*

*Le Reti, guida di Peter Norton - Apogeo*

*W. Willinger, M. S. Taqqu, R. Sherman and D. V. Wilson, "Self-similarity Through High-Variability: Statistical Analysis of Ethernet LAN Traffic at the Source Level (Extended Version)", in Proc. ACM SIGComm'95, Cambridge, MA, 1995.*

*W. E. Leland, M. S. Taqqu, W. Willinger and D. V. Wilson, "On Self-Similar Nature of Ethernet Traffic", In Proc. ACM SIGComm. pp 183-193, San Francisco, Calif., September 1993.*

<http://www.ciscopress.com>

<http://www.ieee.org>

<http://www.tiaonline.org>

<http://www.eia.org>

<http://www.gigabit-ethernet.org>

<http://www.10gea.org>

<http://www.bluetooth.com>

<http://www.tuttoreti.com>

<http://www.networkingitalia.it>



## **CAPITOLO 3**

### **Principi di cablaggio strutturato**



## **IL CABLAGGIO STRUTTURATO**



### **Parte teorica**

- Cos'è il cablaggio strutturato
- Normative internazionali esistenti
- Cablaggio strutturato: cosa possiamo connettere ?
- Tipologie di mezzi trasmissivi

### **Parte pratica**

- Realizzazione di cavi in rame
- Tecniche di connettorizzazione di fibre ottiche
- Strumentazione: uso del certificatore
- Analisi della certifica

Principi di Cablaggio Strutturato 3-2



## Cos'è il cablaggio strutturato

Insieme di componenti passivi che permettono la trasmissione dei segnali da un'apparecchiatura ad un'altra e che devono sottintendere a degli standard comuni

I componenti sono cavi, connettori, prese, permutatori, armadi, etc

L'insieme dei componenti permette di interconnettere svariate apparecchiature elettriche quali: computer, telefoni, apparati di sicurezza, di monitoraggio, etc.

Principi di Cablaggio Strutturato 3-3



## Cos'è il cablaggio strutturato

Le specifiche comuni dei componenti passivi possono essere di tipo proprietario (IBM Cabling system, Digital Decnet...)

Conformi a standard nazionali o internazionali: TIA/EIA 568A, ISO/IEC 11801, prEN 50173, e futuri

Principi di Cablaggio Strutturato 3-2



## Cos'è il cablaggio strutturato

Progettare il cablaggio strutturato  
contestualmente alla costruzione degli edifici o  
in caso di ristrutturazione

Necessità di avere un cablaggio standard per  
gli edifici commerciali e residenziali

Principi di Cablaggio Strutturato 3-5



## Cos'è il cablaggio strutturato

Componenti passivi:

Mezzi trasmissivi quali rame e fibre ottiche

Strutture di permutazione

Connettori, spine o prese

Adattatori

Cassetti, supporti, canaline, armadi

Principi di Cablaggio Strutturato 3-6



## Normative internazionali esistenti

**TIA/EIA 568B**, (*Telecommunication Industry Association/Electronic Industries Alliance*) standard americano per i cablaggi di tipo office, approvato nel 2001 (sostituisce il 568A del 1995)

**ISO/IEC 11801**, (*International Organization for Standardization /International Electrotechnical Commission*) standard internazionale per i cablaggi di tipo office, approvato nel 1995

Principi di Cablaggio Strutturato 3-7



## Categorie e Classi di connessione

### Categorie

- definiscono le caratteristiche di ogni singolo componente

### Classi di connessione

- definiscono le caratteristiche che deve avere un collegamento (insieme dei componenti installati)

Per ottenere una determinata classe di connessione (es. classe D) è necessario usare componenti della corrispondente categoria (es. categoria 5E)

Principi di Cablaggio Strutturato 3-8



## Normative internazionali esistenti

### Tabella comparativa delle normative vigenti

VELOCITÀ DI TRASMISSIONE	CATEGORIA	CLASSE	ISO/IEC 11801	EIA/TIA 568A	EN 50173
fino a 100 KHz	1 <sup>(1)</sup>	A	• <sup>(2)</sup>	•	• <sup>(2)</sup>
fino a 1 MHz	2 <sup>(1)</sup>	B	• <sup>(2)</sup>	•	• <sup>(2)</sup>
fino a 16 MHz	3 <sup>(1)</sup>	C	•	•	•
fino a 20 MHz	4		•	•	
fino a 100 MHz	5	D	•	•	•
	5e	D 2000	•	•	•
fino a 250 MHz	6	E		•	
fino a 600 MHz	7*	F*		•	
2 GHz	Fibra ottica	Ottica	•	•	•

\* Classificazioni contenute in proposte normative non ancora approvate.

Principi di Cablaggio Strutturato 3-9



## Utilizzo del doppino in rame

- **Cat 1:** Currently unrecognized by TIA/EIA. Previously used for POTS telephone communications, ISDN and doorbell wiring.
- **Cat 2:** Currently unrecognized by TIA/EIA. Previously was frequently used on 4 Mbit/s token ring networks.
- **Cat 3:** Currently defined in TIA/EIA-568-B, used for data networks using frequencies up to 16 MHz. Historically popular for 10 Mbit/s Ethernet networks.
- **Cat 4:** Currently unrecognized by TIA/EIA. Defined up to 20 MHz, and was frequently used on 16 Mbit/s token ring networks.
- **Cat 5:** Currently unrecognized by TIA/EIA. Defined up to 100 MHz, and was frequently used on 100 Mbit/s Ethernet networks.
- **Cat 5e:** Currently defined in TIA/EIA-568-B. Defined up to 100 MHz, and is frequently used for both 100 Mbit/s, support 1000BASE-T (10-15m).
- **Cat 6:** Currently defined in TIA/EIA-568-B. Defined up to 250 MHz, 1000BASE-T and 10GBASE-T (37-55m).
- **Cat 6a:** Currently defined in ANSI/TIA/EIA-568-B.20. Defined up to 500 MHz, nearly double that of category 6. Suitable for 10GBASE-T.
- **Cat 7:** Currently defined in ISO/IEC 11801 Class F cabling. Defined up to 600 MHz. This standard specifies four individually-shielded pairs (S/FTP) inside an overall shield. Suitable for 10GBASE-T.
- **Cat 7a:** Currently defined in Amendment 1 and 2 of ISO/IEC 11801 Class FA cabling. Defined up to 1,000 MHz. Cable constructions is S/FTP. Suitable for 40GBASE-T (50m) e 100GBASE-T (15m).

[www.ncp-italy.com](http://www.ncp-italy.com)

Principi di Cablaggio Strutturato 3-10



## Normative internazionali esistenti

Ad ogni categoria è associato un insieme di tabelle con i valori richiesti per le varie caratteristiche del cavo:

- **attenuazione**
- **diafonia:** **NEXT** (paradiafonia), **FEXT** (telediafonia)  
e varie misure di power sum
- **rapporto segnale/rumore (ACR, ELFEXT, ecc.)**
- **velocità di propagazione**
- **resistenza**
- **impedenza**
- **ecc.**

Principi di Cablaggio Strutturato 3-11



## Normative internazionali esistenti

- **Curvatura cavo**
- Tutti i cavi ottici/rame possono supportare un raggio di curvatura minimo pari a 10 volte il diametro esterno del cavo stesso quando non sono soggetti a trazione, e 20 volte il diametro esterno quando sono soggetti a forza di trazione fino al valore massimo specificato per quel cavo

[www.ncp-italy.com](http://www.ncp-italy.com)

Principi di Cablaggio Strutturato 3-6



## Cosa posso connettere?

Gruppo di edifici appartenenti ad un unico comprensorio o campus

Estensione massima 4000 metri

Sia EIA/TIA che ISO/IEC 11801 stabiliscono una gerarchia stellare a 3 livelli

Centro stella di comprensorio

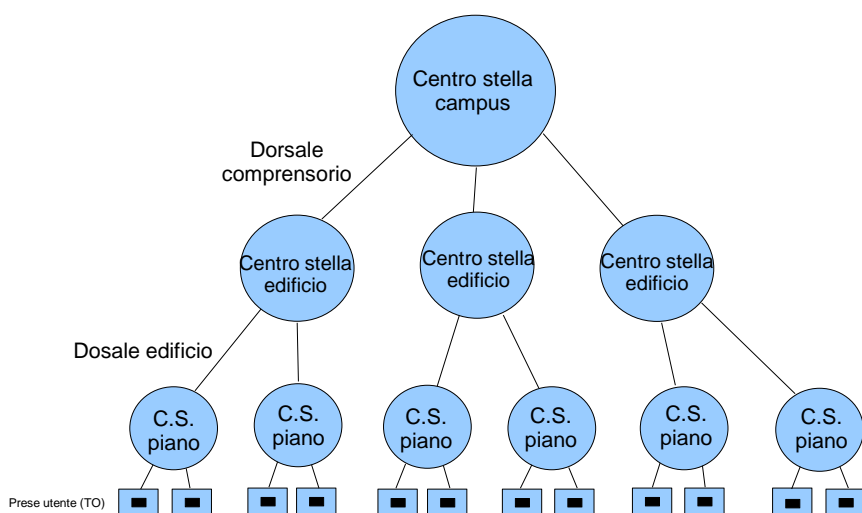
Centro stella di edificio

Centro stella di piano

Principi di Cablaggio Strutturato 3-13



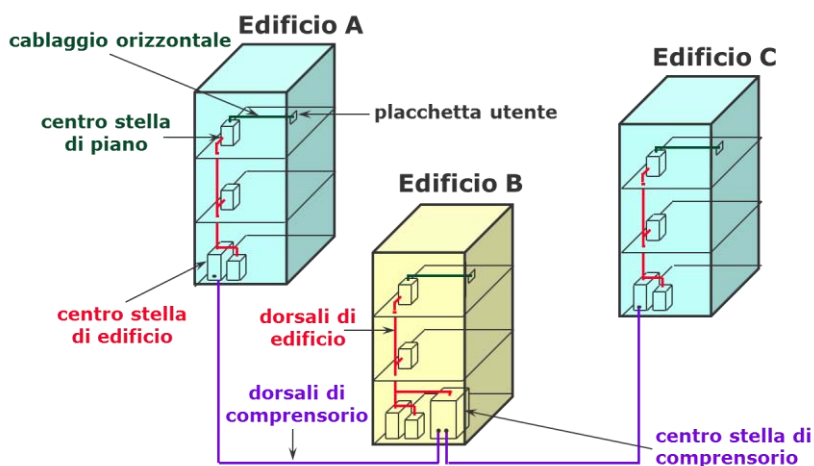
## Cosa posso connettere?



Principi di Cablaggio Strutturato 3-14



## Gli elementi del cablaggio



www.ncp-italy.com

Principi di Cablaggio Strutturato 3-15



## Gli elementi del cablaggio

- Gli elementi che costituiscono il cablaggio in EIA/TIA 568 sono:
  - **un armadio di distribuzione situato nell'edificio** centro stella di un compressorio, da cui vengono distribuiti i cavi di dorsale agli altri edifici;
  - per ogni edificio, un armadio di distribuzione da cui partono i cavi di dorsale di edificio verso i vari piani (**cablaggio verticale**);
  - per ogni piano, un armadio di piano da cui vengono distribuiti i cavi che raggiungono l'utente (**cablaggio orizzontale**).

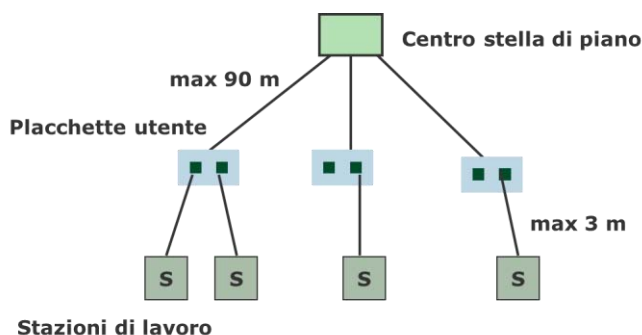
www.ncp-italy.com

Principi di Cablaggio Strutturato 3-16





## Cablaggio orizzontale



[www.ncp-italy.com](http://www.ncp-italy.com)

Principi di Cablaggio Strutturato 3-17



## Il cablaggio orizzontale

- Il cablaggio orizzontale consente di collegare i vari posti di lavoro all'armadio di piano; la topologia è di tipo stellare a partire dall'armadio di distribuzione.
- Ci sono distanze massime per i cavi di distribuzione e i cavi di utente.
- I cavi ammessi sono coppie UTP, coppie STP, thin ethernet e fibra multimodale.
- Ogni placchetta di utente o presa a muro contiene l'interfaccia per due cavi, di cui almeno uno deve essere UTP, con presa RJ45, e il secondo uno degli altri cavi ammessi; attualmente la soluzione più adottata è con due cavi UTP.

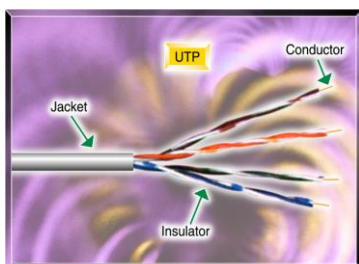
[www.ncp-italy.com](http://www.ncp-italy.com)

Principi di Cablaggio Strutturato 3-18



## Tipologie di mezzi trasmissivi

### Unshielded Twisted Pair



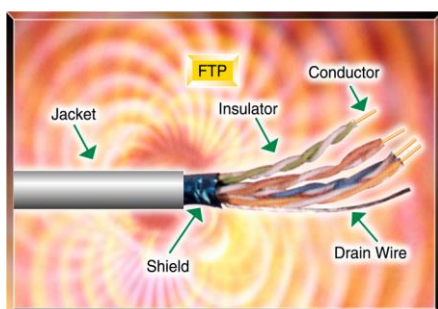
- 4 coppie binate o twisted
- rivestimento dielettrico che racchiude i cavi
- diverso spessore del cavo elettrico
- cavo non schermato
- tutt'ora il più diffuso al mondo

Principi di Cablaggio Strutturato 3-19



## Tipologie di mezzi trasmissivi

### Shielded Twisted Pair (FTP)

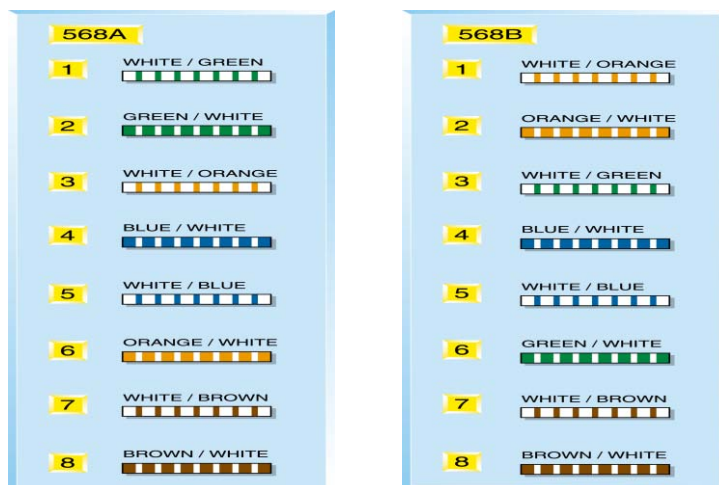


- Schermatura a foglio di alluminio
- riduzione degli effetti di interferenza

Principi di Cablaggio Strutturato 3-20



## Tipologia di cavo



Principi di Cablaggio Strutturato 3-21



## Cavo dritto (Straight-Through)



Hub/Switch

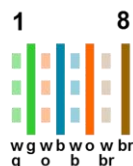
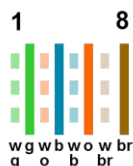


Server/Router

### Straight-Through Cable



Pin Label	Pin Label
1 TX+ ↔ 1	TX+
2 TX- ↔ 2	TX-
3 RX+ ↔ 3	RX+
4 NC 4	NC
5 NC 5	NC
6 RX- ↔ 6	RX-
7 NC 7	NC
8 NC 8	NC



Principi di Cablaggio Strutturato 3-22



## Cavo incrociato (Crossover)



Hub/Switch



Server/Router



### Pin Label

1 TX+  
2 TX-  
3 RX+  
4 NC  
5 NC  
6 RX-  
7 NC  
8 NC

### Pin Label

1 TX+  
2 TX-  
3 RX+  
4 NC  
5 NC  
6 RX-  
7 NC  
8 NC

### EIA/TIA T568A



### EIA/TIA T568B

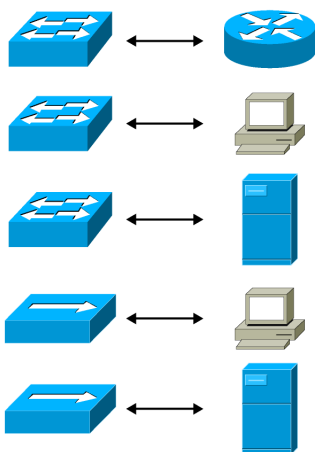


Principi di Cablaggio Strutturato 3-23

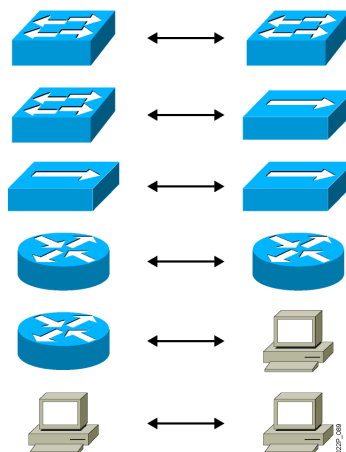


## Straight-Through vs. Crossover

### Straight-Through Cable



### Crossover Cable

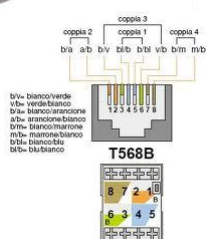


Principi di Cablaggio Strutturato 3-24



## Tipologie di mezzi trasmissivi

### rame



Mini-Com Jack Backshell



ORANGE Module



Red



Blue



BLUE Module



GREEN Module



YELLOW Module

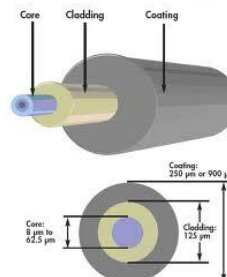


Principi di Cablaggio Strutturato 3-25



## Tipologie di mezzi trasmissivi

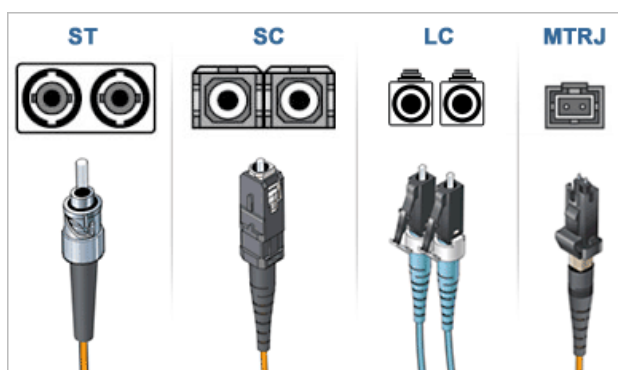
### Fibre ottiche LS0H



Principi di Cablaggio Strutturato 3-26



## Tipologie di connettori



Principi di Cablaggio Strutturato 3-27



## Tipologie di mezzi trasmissivi

Velocità e distanza:

100Base-tx-rame		100mt
100Base-fx-fibra	mm	2km
100Base-lx-fibra	mm	60km
100Base-sx-fibra	mm	300mt
1000BaseT/TX-rame		100mt
1000Base-sx-fibra	mm	275/550mt
1000Base-lx-fibra	sm	5Km(standard)/10km(produttori)
10GBase-s	mm	65mt,
10GBaseLx4	mm	300mt, sm 10km

mm= single mode, mm= multi mode

Principi di Cablaggio Strutturato 3-28



## Tipologie di mezzi trasmissivi

**"prima finestra":** 850 nm (nel campo del visibile), usata soprattutto con economici laser a diodo con luce multimodale. Permette di realizzare collegamenti di 275 m su fibre 62.5/125 e di 550 m su fibre 50/125.

**"seconda finestra":** 1310 nm, usata con laser multimodali o monomodali. Permette di realizzare collegamenti di 5 – 10 km su fibre monomodali.

**"terza finestra":** 1550 nm, usata con laser monomodali. Questa finestra permette di realizzare le distanze maggiori, compresi collegamenti di 100 km con apparati relativamente economici. Sfruttando questa lunghezza d'onda, una buona fibra monomodale raggiunge una attenuazione dell'ordine degli 0,2-0,25km

Principi di Cablaggio Strutturato 3-29



## Link utili

- <http://www.ciscopress.com>
- <http://www.ieee.org>
- <http://www.tiaonline.org>
- <http://www.eia.org>
- <http://www.gigabit-ethernet.org>
- <http://www.10gea.org>
- <http://www.tuttoreti.com>

[www.ncp-italy.com](http://www.ncp-italy.com)

Principi di Cablaggio Strutturato 3-30

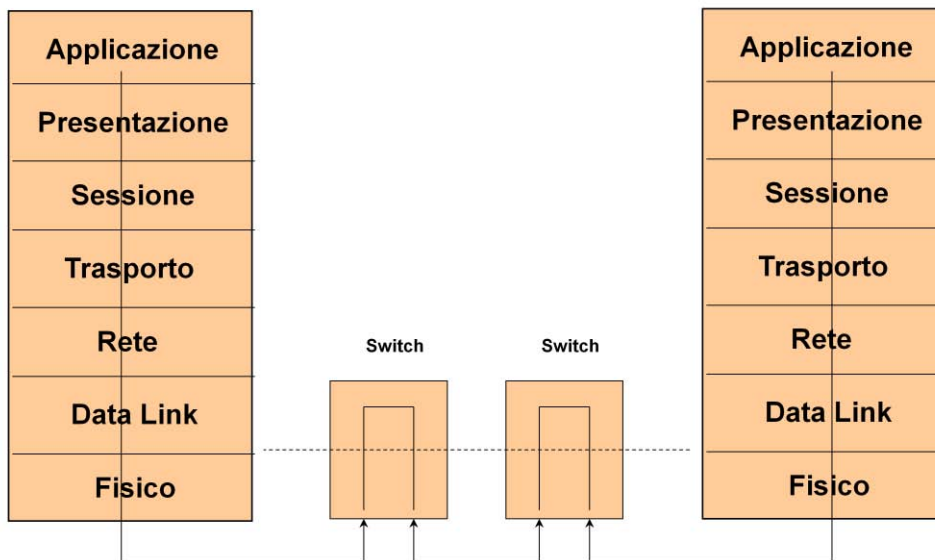
## **CAPITOLO 4**

### **La commutazione di livello 2**





## Lo Switch e la pila OSI



www.ncp-italy.com

La commutazione di livello 2 4-2

Gli switch operano a Livello 2 della pila OSI, si limitano ad analizzare le trame di livello 2 e ad eseguire una commutazione sulla base dei MAC Address.

Questo vuol dire che le operazioni di commutazione a questo livello sono completamente trasparenti ai protocolli di livello superiore come per esempio TCP/IP. In ambiente LAN un dispositivo che opera a Livello 2 è chiamato in modo più generale Bridge (in italiano ponte) per la sua funzione di mettere in comunicazione due segmenti di rete diversi. A questo tipo di apparato non è richiesta nessuna caratteristica di multiporta e di commutazione in hardware, funzionalità che invece sono proprie di uno switch.



## Gli Switch

- **Operano a Livello 2 della pila OSI.** questo vuol dire che le operazioni di commutazione a questo livello sono completamente trasparenti ai protocolli di livello superiore come per esempio TCP/IP. In ambiente LAN un dispositivo che opera a Livello 2 è chiamato in modo più generale *Bridge* (in italiano *ponte*) per la sua funzione di mettere in comunicazione due segmenti di rete diversi. A questo tipo di apparato non è richiesta nessuna caratteristica di multiporta e di commutazione in hardware, funzionalità che invece sono proprie di uno switch.
- **Realizzano le operazioni di commutazione in hardware.** Gli switch muovono i dati ricevuti su una porta di entrata sulla relativa porta di uscita, direttamente, senza consultare un processore separato. Realizzare questa funzione in hardware comporta prestazioni migliori, bassa latenza, minore complessità generale e, quindi, costi più accessibili. E' opportuno sottolineare che le operazioni logiche realizzate da un bridge e da uno switch sono le stesse, la differenza risiede proprio nelle diverse prestazioni, notevolmente migliori nel caso dello switch e pertanto si può affermare che dal punto di vista funzionale parlare di bridging o di switching è la stessa cosa, dal punto di vista delle prestazioni, invece, le differenze possono essere profonde.
- **Permettono una migliore gestione delle porte.** Uno switch di buona qualità è generalmente in grado di supportare meccanismi di *autosensing* per la rilevazione della velocità di trasmissione ed è in grado di lavorare sia in modalità half-duplex che full-duplex, al contrario degli hub per i quali è prevista la sola modalità half-duplex.
- **Sono in grado di realizzare VLAN.** Attraverso meccanismi di separazione dei domini di broadcast e l'utilizzo di protocolli di trunking sono in grado di eseguire una separazione logica delle LAN.

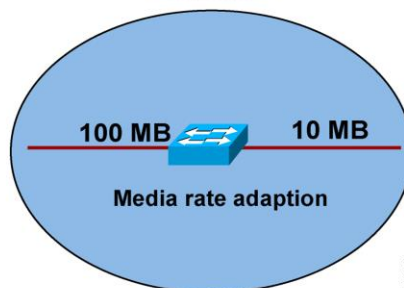
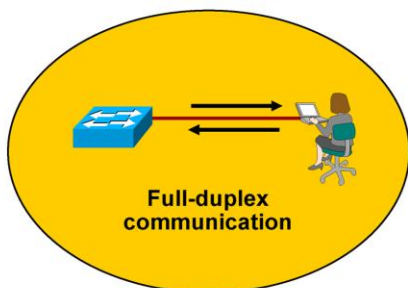
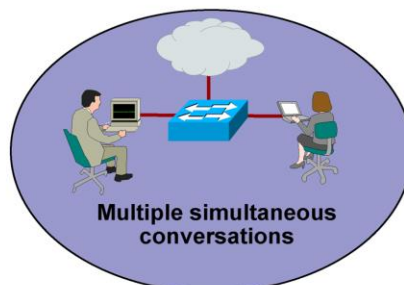
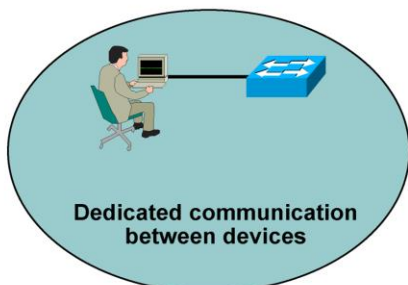
**Nell'ambito** delle reti, la parola Switch e il termine switching sono diventati molto popolari, anzi, qualsiasi applicazione tecnologica arricchita da questi termini istantaneamente si rinvigorisce con un'aura di alte prestazioni, basso costo e complessità ridotta.

Ma che cosa si intende esattamente per switching e perché questa parola è diventata così popolare? La risposta alla seconda domanda è semplice: prezzo e prestazioni. Le tecnologie di switching ed in particolare quelle associate con LAN e WAN offrono maggiori prestazioni e maggiori funzionalità a prezzi più bassi se paragonati alle tradizionali tecnologie che fanno utilizzo di hub. Le evoluzioni nella tecnologia del silicio riescono ormai ad integrare sempre maggiori capacità di elaborazione su chips sempre meno costosi dando così la possibilità ai costruttori di produrre apparati di alte prestazioni a prezzi ragionevoli. La popolarità dello switching risiede quindi nel fatto che è economico e altamente performante.

Per quanto riguarda poi che cosa si intende esattamente con la parola switching nel mondo del Networking, si possono formulare varie risposte. Il LAN switching è usato per gestire i flussi trasmissivi tra stazioni su differenti segmenti di rete generalmente in modalità broadcast multi accesso, in modo non connesso. Il WAN switching prende invece la forma di connessioni virtuali, composti da una serie di tratte successive, in grado di connettere tra loro più apparati remoti in modalità connessa, non broadcast con topologie punto-punto e/o multi accesso.



# LAN Switch

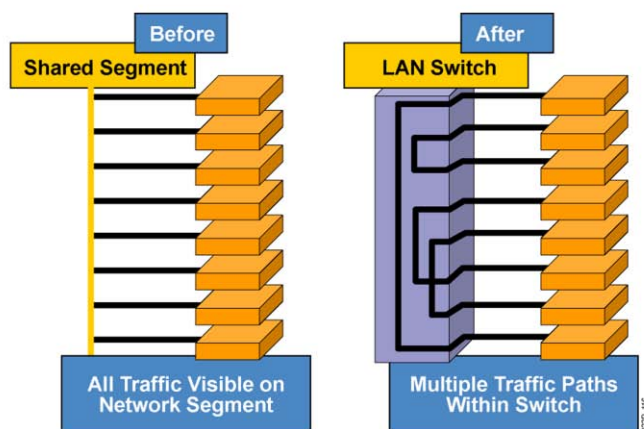


0229-108

La commutazione di livello 2 4-4



# Microsegmentation



Dedicated paths between sender and receiver hosts

La commutazione di livello 2 4-5



## Half Duplex vs. Full Duplex



**Half Duplex**



**Full Duplex**

La commutazione di livello 2 4-6

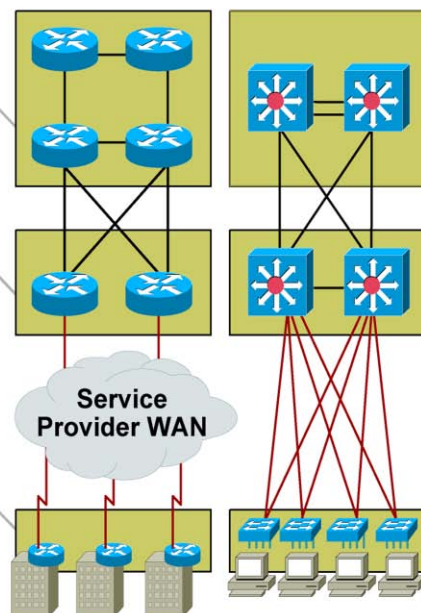


## Modello gerarchico

**Core layer:** Provides optimal transport between core routers and distribution sites

**Distribution layer:** Provides policy-based connectivity, peer reduction, and aggregation

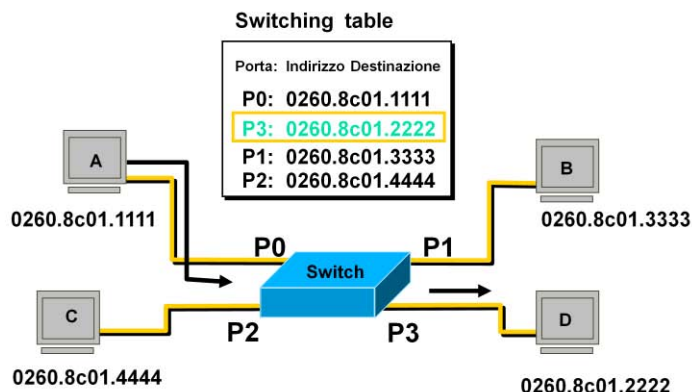
**Access layer** Provides common group access to the internetworking environment



La commutazione di livello 2 4-7



# Dinamica di commutazione



www.ncp-italy.com

La commutazione di livello 2 4-8

Il lavoro di uno switch è quello di inoltrare le trame di ingresso sulla corretta porta di uscita. La porta di uscita è determinata sulla base del MAC address di destinazione.

A differenza **dell'hub**, lo switch non diffonde direttamente il messaggio su tutte le porte, quindi a tutti gli utenti, ma indirizza il pacchetto ricevuto alla stazione (o alle stazioni) a cui il messaggio è effettivamente diretto. Per poter operare il corretto inoltramento dei pacchetti ricevuti, lo switch deve costruirsi una tabella, chiamata **switching table** che gli permetta di sapere su quale porta deve inoltrare il pacchetto perché arrivi al destinatario indicato, questa tabella consiste, quindi, in una serie di associazioni del tipo: indirizzo destinazione → porta di uscita. Quando una trama arriva, lo switch legge l'indirizzo di destinazione e controlla se esiste una corrispondenza nella **switching table**. In caso positivo procede con l'inoltramento sulla porta di uscita indicata nella associazione trovata, se nessuna corrispondenza è trovata, lo switch non può procedere e, pertanto procede con l'inoltramento su tutte le porte tranne quella di arrivo (quest'ultimo processo si chiama **flooding**).

I momenti fondamentali che impegnano uno switch sono:

- Learning
- Flooding
- Forwarding
- Loop avoidance

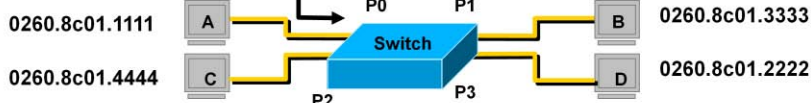
Nella fase di **learning** lo switch apprende le informazioni necessarie per creare la **switching table**. La fase di **forwarding** è quella di inoltramento delle trame sulla base delle informazioni contenute nella switching table, mentre il **flooding** è utilizzato in mancanza di informazioni nella switching table. La fase di **loop avoidance** consente allo switch di non introdurre eventuali circuiti chiusi nei quali le trame potrebbero girare **all'infinito** saturando la banda disponibile.



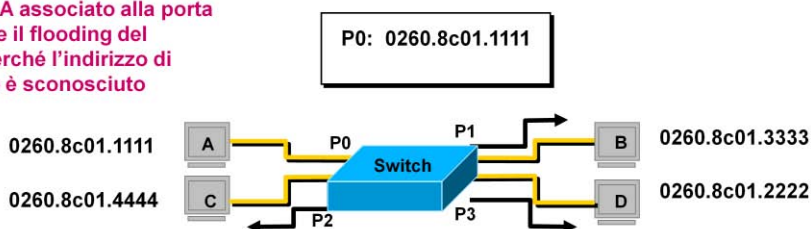
# Dinamica di commutazione

0. La switching table è vuota

1. A invia un pacchetto a B



2. Lo switch inserisce nella tabella l'indirizzo di A associato alla porta P0 ed esegue il flooding del pacchetto perché l'indirizzo di destinazione è sconosciuto



www.ncp-italy.com

La commutazione di livello 2 4-9

La fase di Learning (apprendimento) è una tecnica di auto apprendimento realizzato sulla base del traffico rilevato sulle porte dello switch stesso. Attraverso l'analisi di questo traffico è possibile costruire la tabella di coppie: indirizzo destinazione → porta d'uscita. Il processo è molto semplice: lo switch legge l'indirizzo sorgente di tutti i pacchetti che si presentano sulle sue porte e li associa alle porte stesse. È un processo dinamico sulla base del quale lo switch costruisce la sua tabella di commutazione. Quando un pacchetto si presenta su una porta di ingresso, lo switch esamina l'indirizzo di destinazione operando poi una ricerca dello stesso all'interno della sua tabella per scoprire su quale porta inoltrarlo, se la ricerca ha successo (cioè se l'indirizzo di destinazione è già contenuto nella tabella) commuta il pacchetto sulla porta indicata. Se, al contrario, quel destinatario non è ancora presente in tabella, allora si procede con una operazione di flooding (cioè si manda il messaggio a tutti). In ogni caso lo switch legge sempre (oltre che l'indirizzo del destinatario), anche l'indirizzo del mittente e lo associa alla porta su cui ha ricevuto il messaggio, così, un po' alla volta, costruisce la sua tabella. Un caso particolare è quando l'indirizzo destinazione è associato alla stessa porta su cui è stato ricevuto il pacchetto, in questo caso il pacchetto viene scartato. Le informazioni all'interno della tabella sono dinamiche e vengono mantenute aggiornate sulla base del traffico rilevato. Se dopo un certo periodo di tempo non viene rilevato più nessun pacchetto il cui indirizzo sorgente era già presente nella tabella, si procede con un aggiornamento della tabella rimuovendo tutte le informazioni contenenti l'indirizzo in questione. Questo tipo di tecnologia è principalmente utilizzata in Ethernet ed è conosciuta come Transparent Bridging.

Questa tecnologia è semplice da implementare e non richiede cambiamenti o elaborazioni sulle stazioni finali. Gli aspetti negativi di questa tecnologia sono legati principalmente al fatto che potrebbe richiedere la memorizzazione di un numero molto grande di indirizzi nella tabella di switching e al fatto che si possono creare dei loop qualora siano presenti due o più percorsi tra la stazione sorgente e la stazione di destinazione. La tecnica di Learning è generalmente affiancata da una tecnica di Spanning Tree.

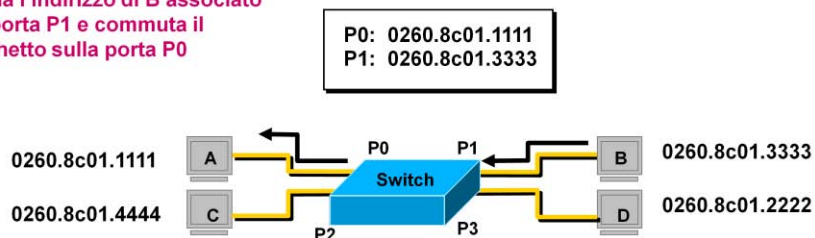




## Dinamica di commutazione

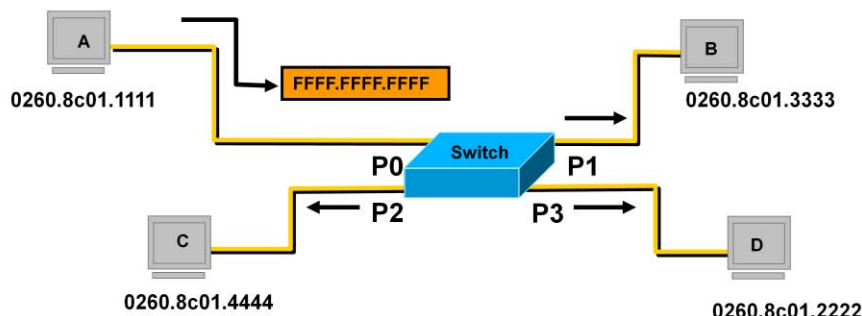
3. B risponde ad A

4. Lo switch inserisce nella tabella l'indirizzo di B associato alla porta P1 e commuta il pacchetto sulla porta P0





## Flooding dell'indirizzo broadcast



- Il processo di flooding è applicato alle trame:
  - Broadcast
  - Multicast
  - Unknown Unicast

www.ncp-italy.com

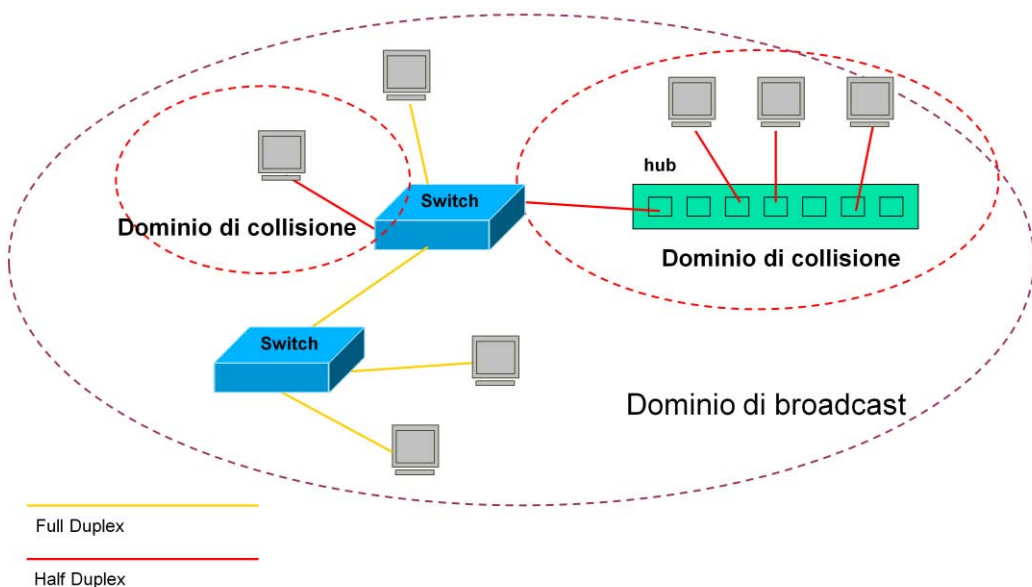
La commutazione di livello 2 4-11

Tra tutte le possibili combinazioni dei 48 bit che costituiscono il MAC ne esiste una che assume un significato particolare, è l'**indirizzo** MAC di broadcast costituito da tutti i bit posti a uno (in formato esadecimale, che risulta molto più sintetico da scrivere, questo indirizzo è: FFFF.FFFF.FFFF). La caratteristica peculiare di un broadcast è quella di essere esplicitamente diretta a tutti per cui tutte le stazioni che lo ricevono devono obbligatoriamente procedere con l'**elaborazione dell'informazione** ricevuta. Come abbiamo avuto già modo di sottolineare, questo implica un interrupt nella CPU della stazione ricevente, e quindi, la proliferazione dei broadcast **all'interno** di una LAN produce inevitabilmente una degradazione delle prestazioni **dell'intero** ambiente. Generalmente il numero dei broadcast aumenta con l'**aumentare** delle stazioni presenti sulla rete. Può essere utile quindi inserire un dispositivo che realizzi una segmentazione della rete in modo da separare le sorgenti di broadcast. Un dispositivo di commutazione a Livello 2 prevede la trasmissione di un pacchetto broadcast utilizzando la modalità del flooding in modo tale da far sì che possa raggiungere tutte le stazioni connesse.

Si dice per questo che un dispositivo di Livello 2 realizza un dominio di broadcast. Ad ogni porta è invece associato un dominio di collisione



## Segmentazione di uno switch



www.ncp-italy.com

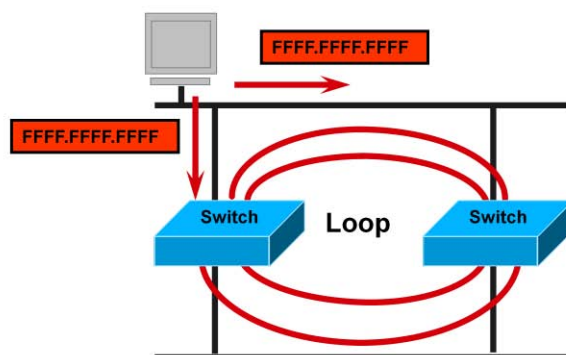
La commutazione di livello 2 4-12

Una rete Ethernet rappresenta al proprio interno un singolo dominio di collisione, cioè qualsiasi pacchetto trasmesso viene ricevuto da tutti e chiunque trasmetta in contemporanea a un altro genera una collisione che viene propagata a tutti i nodi del segmento. L'uso di ripetitori (hub) consente di ampliare le dimensioni fisiche della rete, aggiungendo altri segmenti che tuttavia rimangono un singolo dominio di collisione e perciò arrivano rapidamente a saturare la propria capacità trasmissiva.

L'inserimento di un bridge o di uno switch tra due segmenti permette di creare diversi domini di collisione, riducendo il traffico spurio e aumentando l'efficienza dell'impianto nel suo complesso. Un ulteriore aumento di efficienza è possibile suddividendo i domini di broadcasting.



## Generazione di un Loop



www.ncp-italy.com

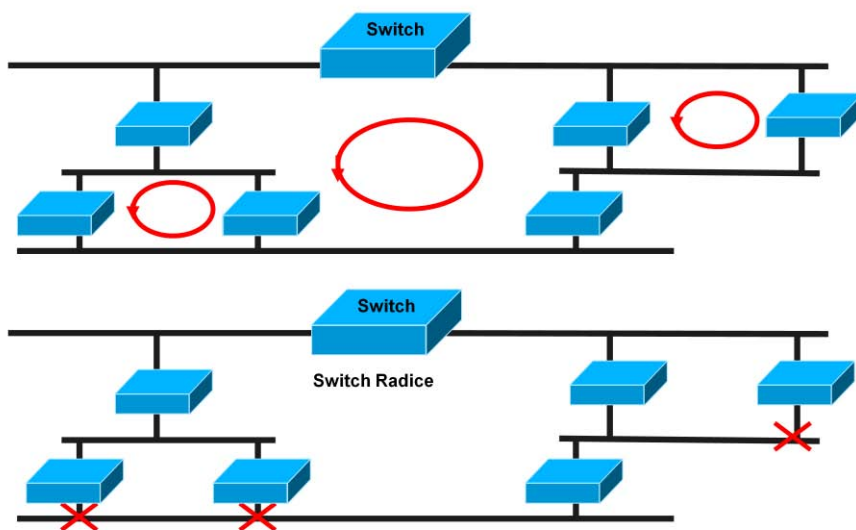
La commutazione di livello 2 4-13

La fase di Loop avoidance (evitare i loop, i percorsi chiusi) costituisce un processo costantemente attivo che interferisce con la commutazione delle trame perché può forzare una porta in uno stato di blocco per evitare la formazione di possibili loop.

Ma come si può formare un loop? Esaminiamo la situazione illustrata in figura e ipotizziamo che la stazione A emetta un broadcast. Poiché ogni switch procede con una operazione di flooding, accade che il pacchetto emesso continuerà a girare sulla rete indefinitamente, e quindi, dopo un **po'** di tempo la rete sarà completamente congestionata da soli pacchetti di broadcast. Per spezzare un simile loop non rimane altro da fare che bloccare una delle porte degli switch presenti. Ovviamente questo processo di blocco non può essere sotto la responsabilità **dell'amministratore** di rete ma deve essere un processo dinamico realizzato dagli stessi switch. Il protocollo predisposto ad eseguire tali operazioni si chiama, come già anticipato nelle sezioni precedenti, Spanning Tree Protocol (STP). STP è un protocollo molto complesso che ha come compito quello di prevenire la formazione di qualsiasi loop all'interno della rete realizzando un sistema di percorsi con struttura ad albero. Il protocollo è anche progettato in modo tale da poter reagire in tempi brevi a possibili cambiamenti topologici della rete. Il modo di operare di Spanning Tree si può sintetizzare in due macro processi: l'elezione dello switch radice, la determinazione dei percorsi verso tutti gli altri switch della rete a partire dallo switch radice. Durante quest'ultima fase il protocollo provvederà a mettere in stato di blocco tutte quelle porte che possono causare possibili loop, e non impediscono, comunque, di raggiungere tutte le stazioni della rete. Ogni qual volta dovessero intervenire cambiamenti nella struttura della rete, il protocollo riparte con il processo a cominciare dall'elezione dello switch radice. L'amministratore può solo intervenire cambiando i parametri di funzionamento di default del protocollo per meglio adattarlo alle caratteristiche della propria realtà. Questa ed altre configurazioni più complesse si possono operare sugli switch di nuova generazione



## Spanning Tree in azione



www.ncp-italy.com

La commutazione di livello 2 4-14

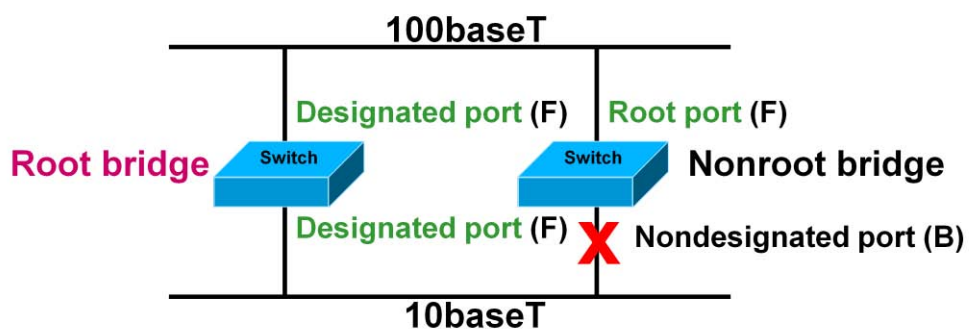
**L'applicazione dell'algoritmo** Spanning Tree ha la funzione di creare percorsi che non presentino nessun tipo di loop. Spanning Tree Protocol (STP) è definito da IEEE 802.1d e rappresenta un protocollo dinamico che prevede uno scambio continuo di pacchetti informativi tra tutti gli switch che compongono la rete. Per questo motivo la presenza di STP comporta un maggiore impegno delle risorse di elaborazione ed un maggiore impiego di banda.

Allo stato attuale è stato standardizzato il cosiddetto **Rapid Spanning Tree Protocol** (802.1w), che permette di avere tempi di convergenza molto più rapidi rispetto ai tradizionali 50 secondi di STP.



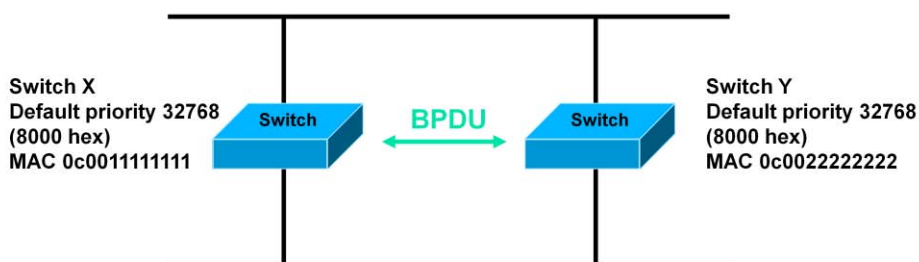
## Spanning-Tree: operazioni

- Un “**root bridge**” per rete
- Una “**root port**” per nonroot bridge
- Una “**designated port**” per segmento





## Spanning-Tree: selezione del Root Bridge



**BPDU = Bridge Protocol Data Unit** (default = inviata ogni 2 secondi)

**Root bridge = Bridge con il più basso Bridge ID**

**Bridge ID = Bridge priority + bridge MAC address**

Una trama BPDU contiene I seguenti campi:

- Protocol ID version
- Message type
- Flags
- Root ID
- Cost of path
- Bridge ID
- Port ID
- Message age
- Max age
- Hello time
- Forward delay

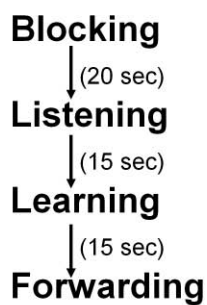
Il costo assegnato alle singole porte è il seguente:

Link Speed	Cost (nuova ratifica IEEE)	Cost (precedente IEEE)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	10



## Spanning-Tree: stati e convergenza

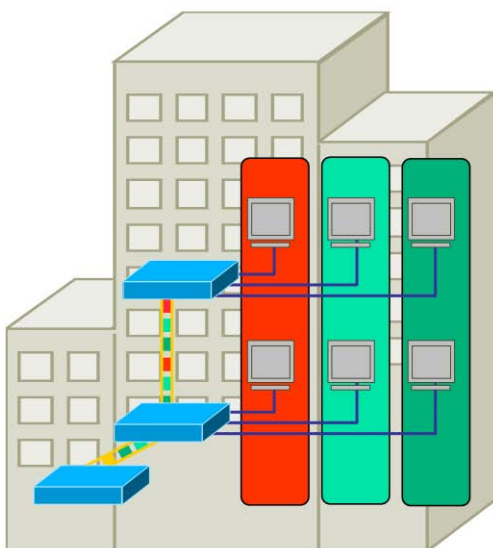
**Ogni porta per entrare nello stato forwarding deve attraversare degli stati intermedi ognuno caratterizzato da propri tempi di transito:**







## Introduzione alle VLAN



- Un gruppo di porte/utenti appartenenti allo stesso dominio di broadcast
- Gli utenti possono essere delocalizzati a piacere senza vincoli di posizione
- La divisione delle VLAN è un processo logico
- Il risultato è equivalente ad una vera e propria separazione fisica

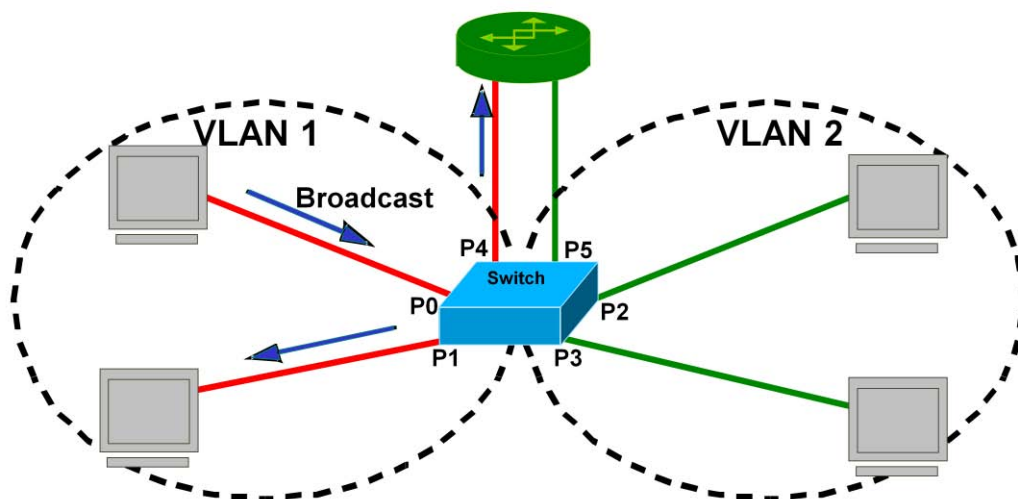
[www.ncp-italy.com](http://www.ncp-italy.com)

La commutazione di livello 2 4-18

Molti switch moderni riescono a costruire lan virtuali (vlan), cioè insiemi di macchine che si comportano come se fossero reti separate (quindi non condividono i broadcast) e che possono essere composte da macchine collegate a uno o più switch, comunque distribuite all'interno dell'azienda. Riunire questi utenti in gruppi di lavoro presenta il vantaggio di confinare il flusso dei dati così che non esca dalla cerchia di coloro che ne hanno effettivamente bisogno, facilita la gestione del traffico e della rete, e permette in ogni caso di avere risorse condivise tra due o più vlan, evitando gli inconvenienti di un'effettiva separazione fisica tra le lan: rigidità di riconfigurazione e difficoltà a condividere risorse comuni. Poiché non è ancora stato raggiunto un alto grado di standardizzazione in questo ambito, la definizione di vlan cambia da fornitore a fornitore, tuttavia nella sua essenza può essere riassunta nel concetto di **dominio di broadcast**.



## Comunicazione tra VLAN



Stazioni appartenenti a VLAN differenti possono comunicare soltanto a livello 3 attraverso un router

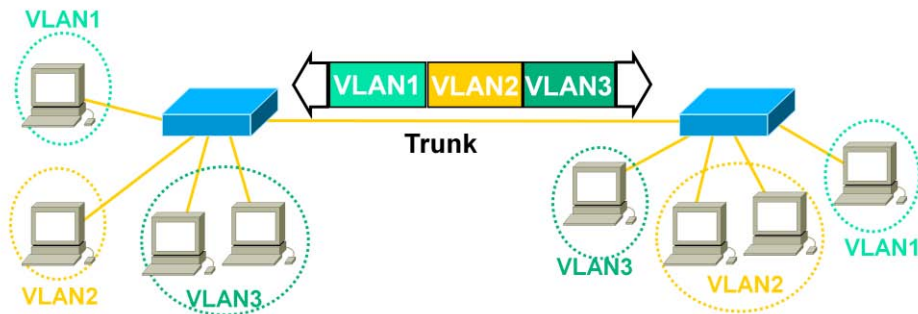
[www.ncp-italy.com](http://www.ncp-italy.com)

La commutazione di livello 2 4-19

Due o più virtual LAN, rappresentando dei domini di broadcast separati, non possono comunicare a livello due. Il traffico rimane rigorosamente separato realizzando una comunicazione intra-group, ma non inter-group. Nessun messaggio può attraversare lo switch per giungere ad una VLAN diversa da quella di provenienza. Al livello 2 della pila OSI, questo schema di comunicazione, equivale ad un insieme di LAN fisicamente isolate, mentre a livello 3, ad un insieme di subnet IP disconnesse una **dall'altra**. Generalmente ad ogni VLAN è associata una subnet IP. Non essendo permessa commutazione tra due VLAN, **l'unica** possibilità di interconnessione possibile è attraverso un router, a livello 3 della pila OSI. Lo schema di interconnessione prevede generalmente una interfaccia del router collegata ad una singola VLAN. **L'interfaccia** del router sarà utilizzata dagli utenti della VLAN come default gateway per comunicare con le altre VLAN o con **l'esterno**.



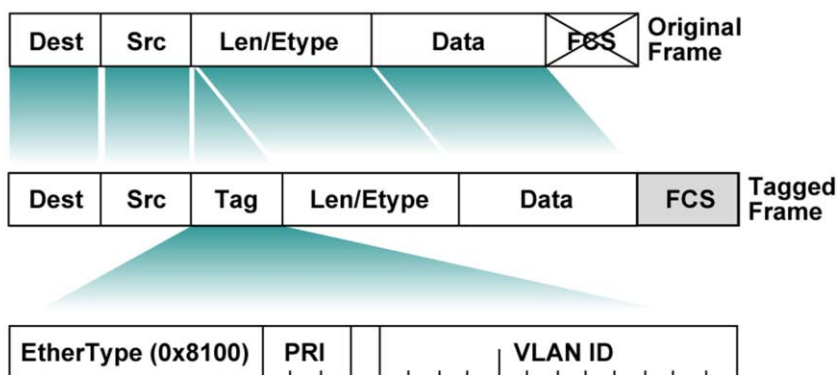
## Etichettatura delle trame



La separazione logica delle trame **all'interno** dello stesso Switch è un processo interno allo switch stesso. Le trame di entrata e di uscita sono rigorosamente conformi allo standard 802.3. Nella comunicazione tra Switch è necessario etichettare le trame per mantenere traccia della VLAN di appartenenza attraverso un identificativo univoco denominato VLAN\_ID. I link di connessione Switch-to-Switch si chiamano Trunk. Gli Switch rimuovono le etichette con il VLAN\_ID quando inoltrano una frame su un link non-trunk.



## IEEE 802.1Q

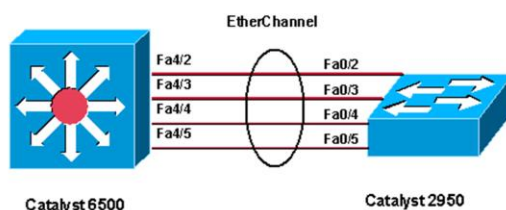


- Le frame sono etichettate con l'identificativo numerico della VLAN di appartenenza.

A livello 2 è possibile realizzare i cosiddetti Trunk per il trasporto delle VLAN attraverso l'utilizzo di opportuni protocolli detti di Tagging (perché aggiungono delle etichette per il trasporto dell'identificativo delle VLAN), uno di essi è definito dallo standard IEEE 802.1Q. All'interno del TAG introdotto nella frame ethernet tradizionale è presente un campo di 3 bit (PRI) attraverso il quale è possibile assegnare alla frame una priorità in una scala da 0 a 7 (802.1p). Più è alto il valore meno la frame sarà influenzata dalla presenza di eventuali congestioni.



## Aggregazione

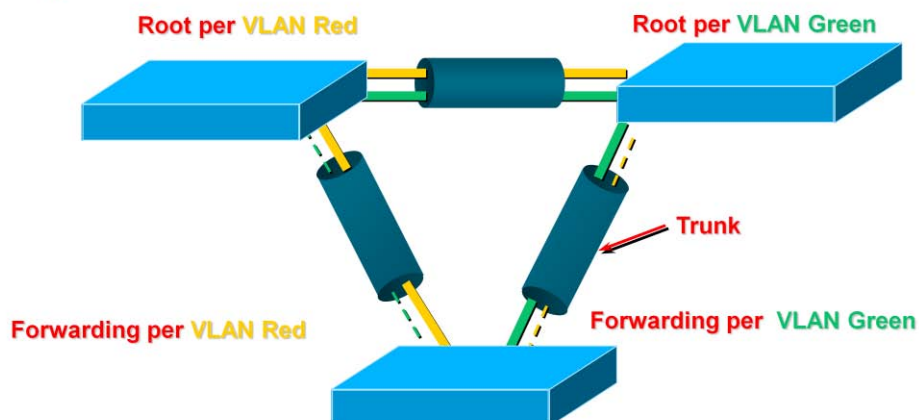


- PAgP (*Port Aggregation Protocol*)
  - Cisco proprietario
- LACP (*Link Aggregation Control Protocol*)
  - IEEE 802.3ad standard

Un elemento di sicuro spicco, **nell'ottica** di avere maggiore banda disponibile, è la tecnologia di aggregazione dei canali conosciuta come IEEE 802.3ad, che permette di superare i limiti di STP e utilizzare link multipli nei collegamenti switch-to-switch.



## Spanning Tree per VLAN



- Consente di avere una istanza di STP per VLAN definita
- Semplice metodo per la ridondanza a Livello 2.
- Fornisce un efficace meccanismo per la gestione dei flussi di traffico e della banda.



## Protocolli per STP

- 802.1d -> Spanning tree tradizionale (CST Common ST)
- 802.1w -> RSTP (Rapid Spanning Tree)
- 802.1s -> MSTP (Multiple Instance STP)



## Power over Ethernet

- I vantaggi derivanti dall'applicazione della tecnologia PoE ai sistemi di sorveglianza IP sono molteplici:
  - PoE è una fonte di alimentazione intelligente
  - PoE rende più semplice e più economico consolidare l'erogazione di energia per sistemi VoIP e "IP Surveillance"
  - Lo standard di base è denominato **802.3af** e supporta l'erogazione di 12,95 W
  - Per andare incontro alle maggiori esigenze energia (p.e.: brandeggio delle videocamere) è stato ideato lo standard **802.3at** (denominato *PoE Plus*) che consente l'erogazione di 30 W.

[www.ncp-italy.com](http://www.ncp-italy.com)

La commutazione di livello 2 4-25

**Power over Ethernet:** un altro ottimo motivo per migrare alla sorveglianza IP. Da sempre l'installazione di cavi per i sistemi di sicurezza è un processo dispendioso. I costi però possono lievitare ulteriormente se è necessario collegare in rete anche gli impianti di controllo degli accessi e antincendio. Senza dimenticare l'alimentazione. Le telecamere CCTV analogiche e altri dispositivi, come i multiplexer e i DVR richiedono un'alimentazione (cavi, uscite CA e prese) indipendente, che implica necessariamente doversi rivolgere ad elettricisti per ogni installazione. Infine, in molti casi è necessario predisporre gruppi di continuità (UPS) distinti per tutti i dispositivi dei sistemi "mission critical" per far fronte ad eventuali interruzioni dell'alimentazione. Elementi che hanno un grosso impatto sui costi.

Trasmissione sicura dell'energia elettrica ai dispositivi in rete senza alcuna riduzione delle prestazioni della rete

**Power over Ethernet (PoE)**, noto anche come Power over LAN, permette di ridurre i costi di utilizzo dei sistemi di sorveglianza basati su IP fino all'80% rispetto alle installazioni analogiche tradizionali. PoE è una tecnologia rivoluzionaria che integra dati, voce e alimentazione in un'infrastruttura LAN standard, utilizza cavi di rete Ethernet standard (CAT-5) ed alimenta i dispositivi di rete direttamente dalle porte a cui sono collegati. I cavi Ethernet CAT-5 standard sono costituiti da quattro coppie di doppiini intrecciati, di cui solo due utilizzati per la trasmissione dei dati su reti 10BASE-T e 100Base-T. Gli altri due possono essere impiegati per alimentare dispositivi in rete.



## **Quali vantaggi offre la nuova tecnologia?**

I vantaggi derivanti dall'applicazione della tecnologia PoE ai sistemi di sorveglianza IP sono molteplici e vanno ben oltre i risparmi sui costi di installazione.

- **PoE è una fonte di alimentazione intelligente**

Le apparecchiature di alimentazione rese disponibili dalla tecnologia PoE consentono una gestione ottimale del sistema poiché utilizzano i protocolli esistenti come il Simple Network Management Protocol (SNMP). Ciò consente di scollegare la rete dall'alimentazione centralmente, ad esempio per effettuare interventi di manutenzione.

- **PoE rende più semplice e più economico consolidare l'erogazione di energia ai sistemi di sorveglianza IP**

La centralizzazione dell'alimentazione attraverso gli hub PoE (chiamati mid-span) permette di collegare i sistemi basati su PoE al gruppo di continuità (UPS) centrale che supporta generalmente la maggior parte della rete costituita da uno o due PC. Questa configurazione evita che eventuali interruzioni nell'alimentazione si ripercuotano sull'integrità del sistema di sorveglianza IP.

- **Gli hub PoE consentono ai responsabili della sicurezza di disattivare e reimpostare i dispositivi remotamente**

I sistemi PoE sono in grado di individuare con precisione i dispositivi in rete difettosi e di consentire ai responsabili di ripristinarli mediante la semplice pressione di un tasto. Questi dispositivi possono essere isolati dall'alimentazione, sostituiti da dispositivi nuovi e quindi riattivati.

- **La centralizzazione del controllo dell'alimentazione garantisce una maggiore sicurezza** limitando i problemi di vulnerabilità che possono verificarsi nel caso in cui il personale addetto alle pulizie o ai lavori edili abbia bisogno di utilizzare un punto di alimentazione di una videocamera.

- **PoE inoltre consente di massimizzare la copertura grazie ad un'installazione ottimale delle telecamere**

La nuova tecnologia permette agli installatori di installare le telecamere di rete in qualunque posizione, indipendentemente dalle fonti di alimentazione esistenti, che troppo spesso si trovano in prossimità dei battiscopa, ossia in posizione diametralmente opposta rispetto ai siti ottimali per le telecamere di sorveglianza.



# Green Ethernet



- ❑ Invece del carico dei collegamenti, questa tecnologia monitora lo stato di attività delle porte anche quando sono collegate a un dispositivo (per esempio un PC) e pone la porta in uno stato di *stand-by*, ossia di basso consumo, quando non viene registrata alcuna attività.
- ❑ In aggiunta, la tecnologia è in grado di auto-adattare il consumo energetico rilevando anche la lunghezza fisica del cavo di collegamento tra il dispositivo di rete e il dispositivo esterno, diminuendo la potenza utilizzata al diminuire della lunghezza del cavo stesso, invece di alimentare la porta a un valore costante, pari a quello necessario per un cavo della lunghezza massima prevista dallo standard.

[www.ncp-italy.com](http://www.ncp-italy.com)

La commutazione di livello 2 4-27

La tecnologia si ispira a una proposta di standardizzazione attualmente al vaglio dell'IEEE (*Institute of Electrical and Electronics Engineers*) ma non ancora approvata. La proposta, identificata come 802.3az ha come obiettivo l'ottimizzazione dell'efficienza energetica dei dispositivi di rete ed è il risultato di un'attività di *task-force* promossa dall'IEEE stesso. L'idea di base della proposta consiste nell'inserire nei dispositivi di rete dei meccanismi per monitorare il carico dei collegamenti sulle porte Ethernet fisiche e adattare di conseguenza i propri consumi energetici al livello strettamente necessario.

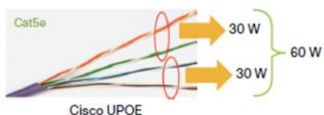


## Soluzione PoE

### Cisco EnergyWise



#### Cisco Universal Power Over Ethernet:



```
Layer3-Switch#show power inline
Available:370.0(w)  Used:30.9(w)  Remaining:339.1(w)
```

Interface	Admin	Oper	Power (Watts)	Device	Class	Max
Fa0/1	auto	off	0.0	n/a	n/a	15.4
Fa0/2	auto	off	0.0	n/a	n/a	15.4
Fa0/3	auto	off	0.0	n/a	n/a	15.4
Fa0/4	auto	off	0.0	n/a	n/a	15.4
Fa0/5	auto	off	0.0	n/a	n/a	15.4
Fa0/6	auto	on	6.3	IP Phone 7960	n/a	15.4
Fa0/7	auto	off	0.0	n/a	n/a	15.4
Fa0/8	auto	off	0.0	n/a	n/a	15.4
Fa0/9	auto	off	0.0	n/a	n/a	15.4
Fa0/35	auto	off	0.0	n/a	n/a	15.4
Fa0/36	auto	off	0.0	n/a	n/a	15.4
Fa0/37	auto	off	0.0	n/a	n/a	15.4
Fa0/38	auto	on	12.0	IP Phone 7975	3	15.4
Fa0/39	auto	off	0.0	n/a	n/a	15.4
Fa0/40	auto	off	0.0	n/a	n/a	15.4
Fa0/41	auto	off	0.0	n/a	n/a	15.4
Fa0/42	auto	on	6.3	IP Phone 7912	n/a	15.4
Fa0/43	auto	off	0.0	n/a	n/a	15.4
Fa0/44	auto	off	0.0	n/a	n/a	15.4
Fa0/45	auto	off	0.0	n/a	n/a	15.4
Fa0/46	auto	off	0.0	n/a	n/a	15.4
Fa0/47	auto	off	0.0	n/a	n/a	15.4
Fa0/48	auto	on	6.3	IP Phone 7940	n/a	15.4

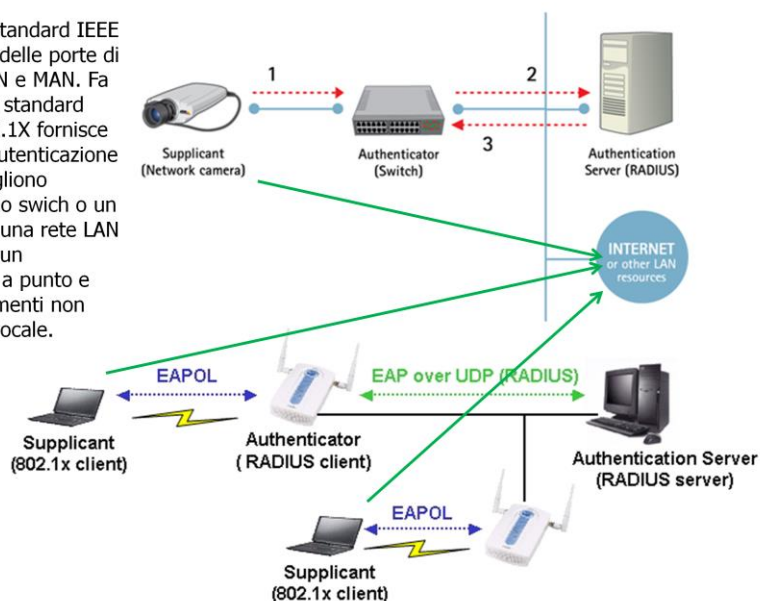
[www.ncp-italy.com](http://www.ncp-italy.com)

La commutazione di livello 2 4-28



## Autenticazione 802.1x

IEEE 802.1x è uno standard IEEE basato sul controllo delle porte di accesso alla rete LAN e MAN. Fa parte dell'insieme di standard IEEE 802. L'IEEE 802.1X fornisce un meccanismo di autenticazione ai dispositivi che vogliono collegarsi tramite uno switch o un access point wifi ad una rete LAN o WLAN, stabilendo un collegamento punto a punto e prevenendo collegamenti non autorizzati alla rete locale.

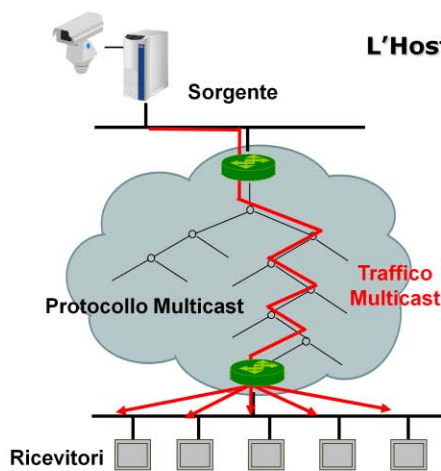


[www.ncp-italy.com](http://www.ncp-italy.com)

La commutazione di livello 2 4-29



# I benefici del Multicasting



L'Host sorgente **NON** utilizza alcun protocollo.

I router creano l'**ALBERO di distribuzione** attraverso il quale fluisce il traffico Multicast.

- DVMRP
- MOSPF
- PIM

Il PIM costruisce l'albero con l'aiuto di un protocollo di routing interno (OSPF, EIGRP, ....)

[www.ncp-italy.com](http://www.ncp-italy.com)

La commutazione di livello 2 4-30

Nella trasmissione multicast, i router costruiscono un albero che connette tutti i membri di un gruppo. Siffatto albero prende il nome di "**albero di distribuzione**", esso specifica un percorso unico tra la subnet delle sorgente e ogni altra subnet contenente un membro del gruppo. Ogni router conosce quali delle sue tratte appartiene **all'albero** così da poter duplicare il pacchetto multicast solo sulle interfacce interessate. Questa azione è realizzata generando il numero minimo di copie del messaggio sorgente per trasmetterlo a tutte le stazioni richiedenti. L'albero di distribuzione è dinamicamente aggiornato sulla base delle JOIN e delle LEAVE generate. Ci sono due tipologie di alberi di distribuzione: Source-specific Tree e Center-specific Tree denominati anche Shrttest-path Tree e Shared Tree.

I protocolli di routing multicast hanno la funzione di costruire gli alberi di distribuzione. I protocolli in questione sono:

DVRMP – Distance Vector Multicast Routing Protocol

MOSPF – Multicast OSPF

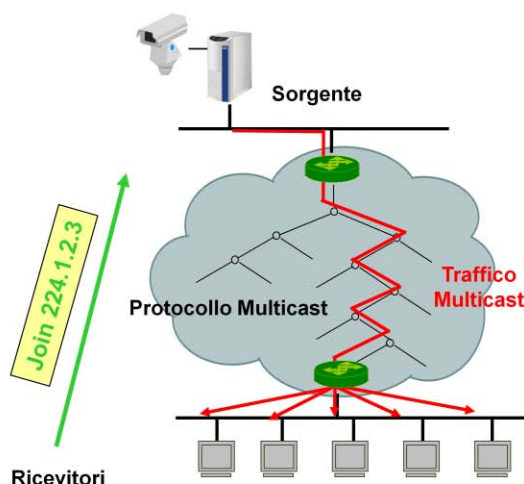
PIM – Protocol Independent Multicast



## IGMP – Internet Group Management Protocol

Il ricevitore invia un messaggio di **Join** IGMP esplicito che dichiara il suo interesse ad un determinato gruppo di Multicast (es. 224.1.2.3).

Attraverso l'intercettazione di questi messaggi i router della rete costruiscono l'albero di raggiungibilità dalla sorgente ai ricevitori.



[www.ncp-italy.com](http://www.ncp-italy.com)

La commutazione di livello 2 4-31

Le stazioni riceventi non hanno bisogno di ricevere una query per unirsi ad un gruppo di multicast, esse hanno la possibilità di inviare un messaggio di JOIN in qualsiasi momento, il messaggio di JOIN è semplicemente un report non richiesto (unsolicited).

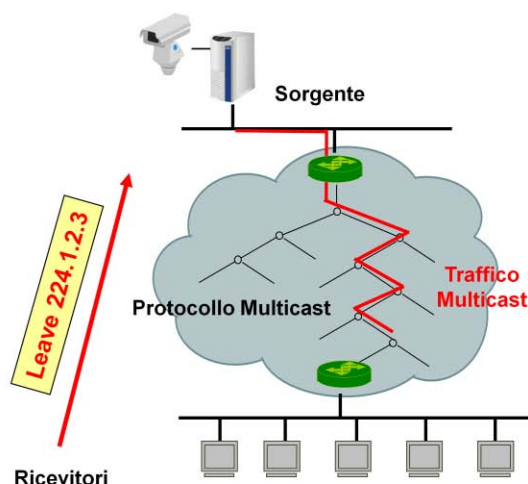
Nella versione 1 di IGMP non ci sono meccanismi di Leaving di abbandono del gruppo di multicast. Semplicemente un router se non riceve nessun Report dopo un certo numero di query assume che nessun membro (di un gruppo di multicast) è più presente e quindi modificherà l'albero delle raggiungibilità di conseguenza.



## IGMP – Internet Group Management Protocol

Il ricevitore invia un messaggio di **Leave** IGMP che dichiara la sua uscita dal gruppo di Multicast al quale si era unito.

Attraverso l'intercettazione di questi messaggi i router della rete ricalcolano l'albero di raggiungibilità dalla sorgente ai ricevitori.



[www.ncp-italy.com](http://www.ncp-italy.com)

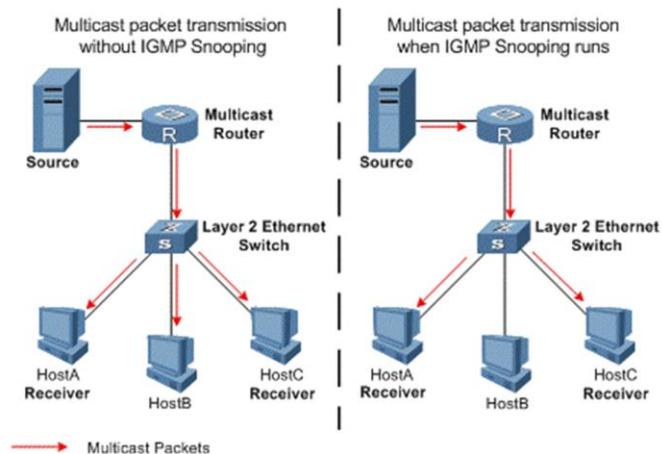
La commutazione di livello 2 4-32

Le stazioni riceventi non hanno bisogno di ricevere una query per unirsi ad un gruppo di multicast, esse hanno la possibilità di inviare un messaggio di JOIN in qualsiasi momento, il messaggio di JOIN è semplicemente un report non richiesto (unsolicited).

Nella versione 1 di IGMP non ci sono meccanismi di Leaving di abbandono del gruppo di multicast. Semplicemente un router se non riceve nessun Report dopo un certo numero di query assume che nessun membro (di un gruppo di multicast) è più presente e quindi modificherà l'albero delle raggiungibilità di conseguenza.



# IGMP Snooping

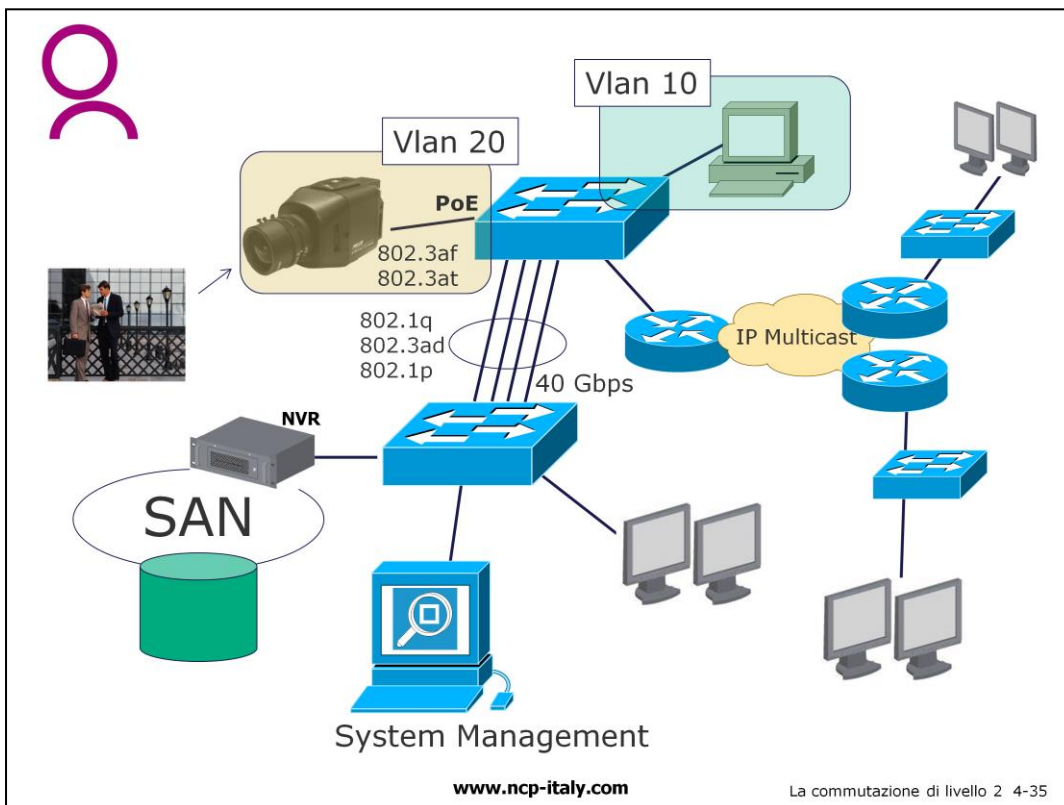


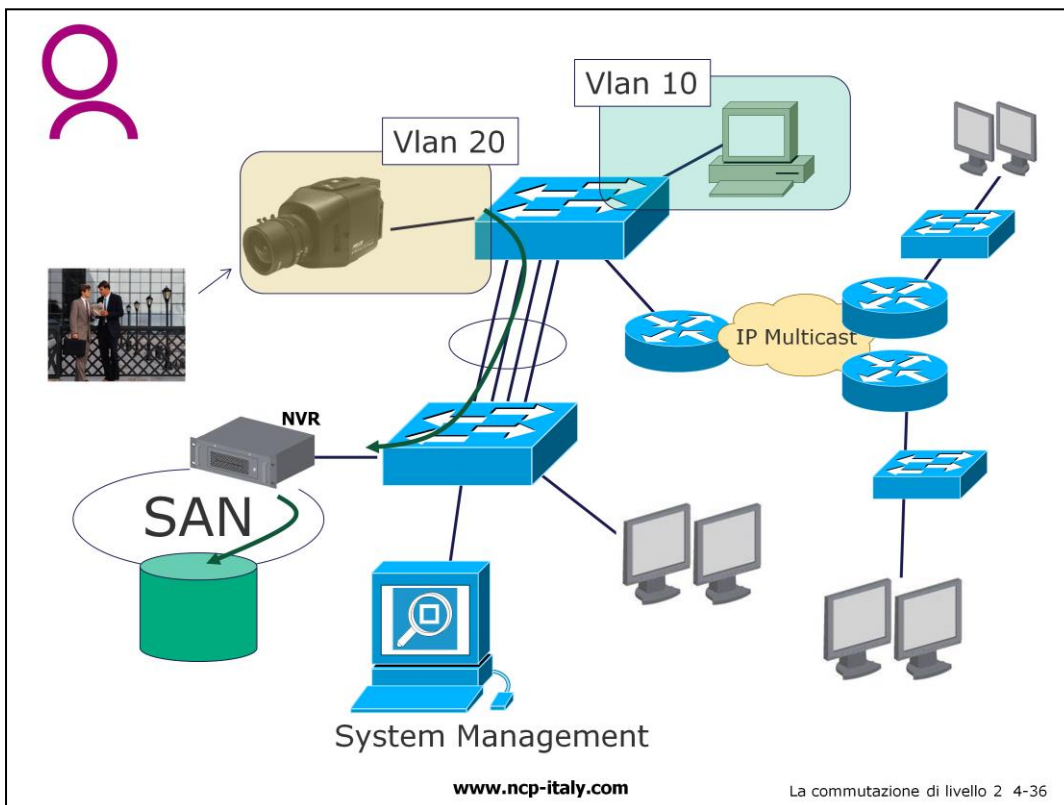


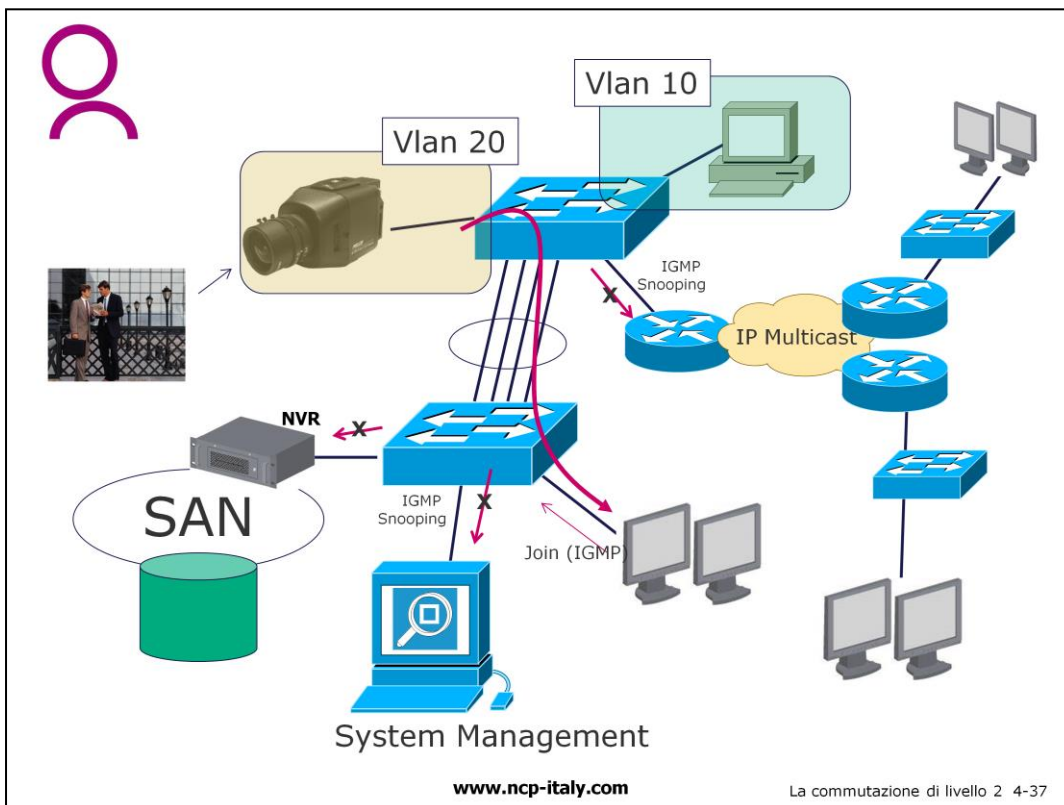


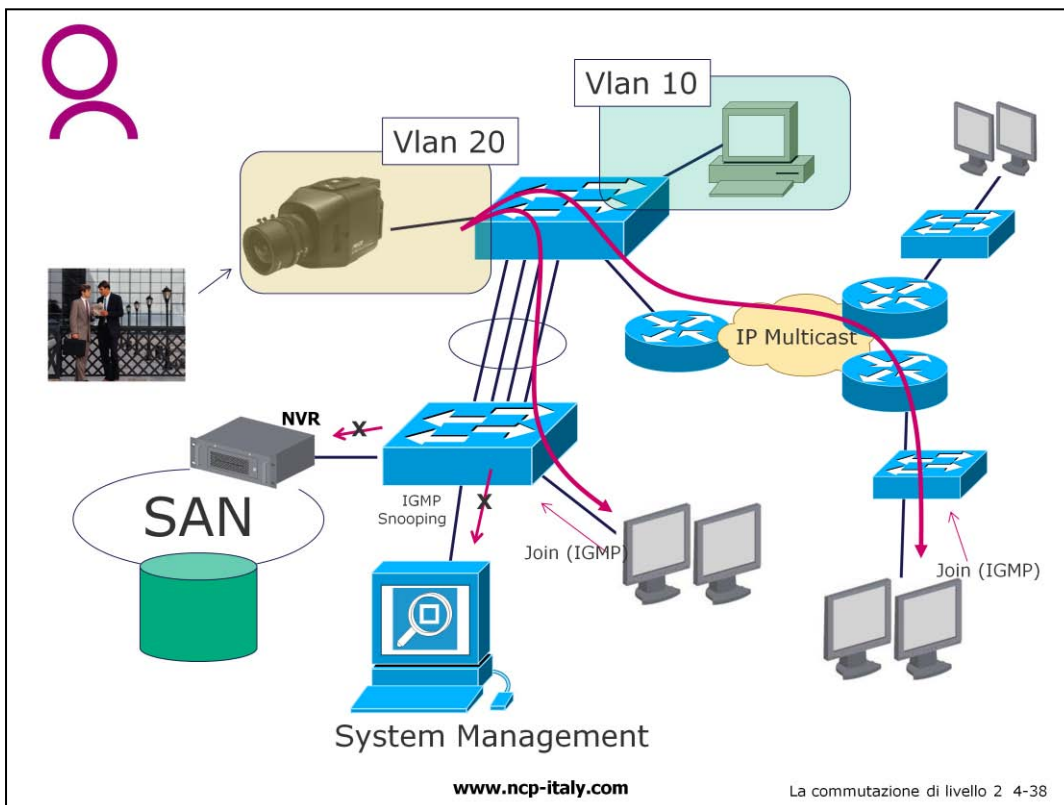
## Fattori chiave

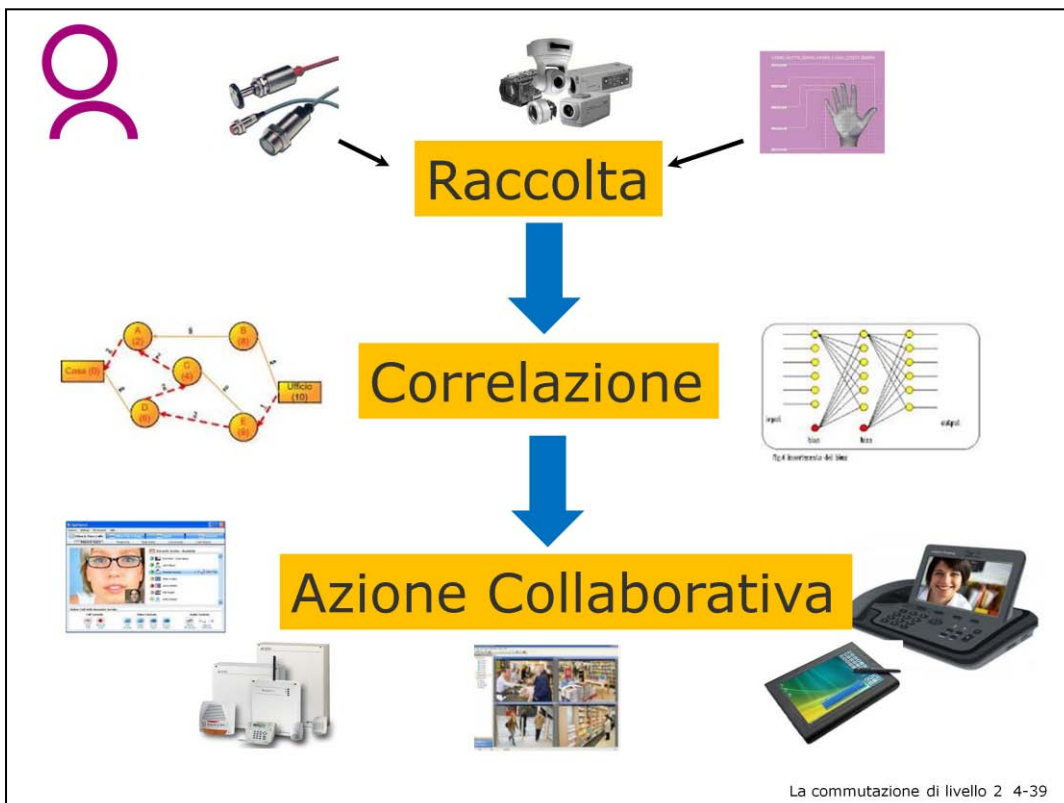
- **Acquisizione delle immagini**
  - Qualità delle immagini
- **Invio delle immagini**
  - Predisposizione della rete dati "*Video enabled*"
  - Gestione della banda
  - Compressione
- **Archiviazione** delle immagini
  - Sistemi di Storage
- **Elaborazione delle immagini**
  - Potenza di calcolo
  - Algoritmi di nuova generazione
- **Gestione dei sistemi**
  - IP Surveillance management













## Collaborative Total Control System



La commutazione di livello 2 4-40

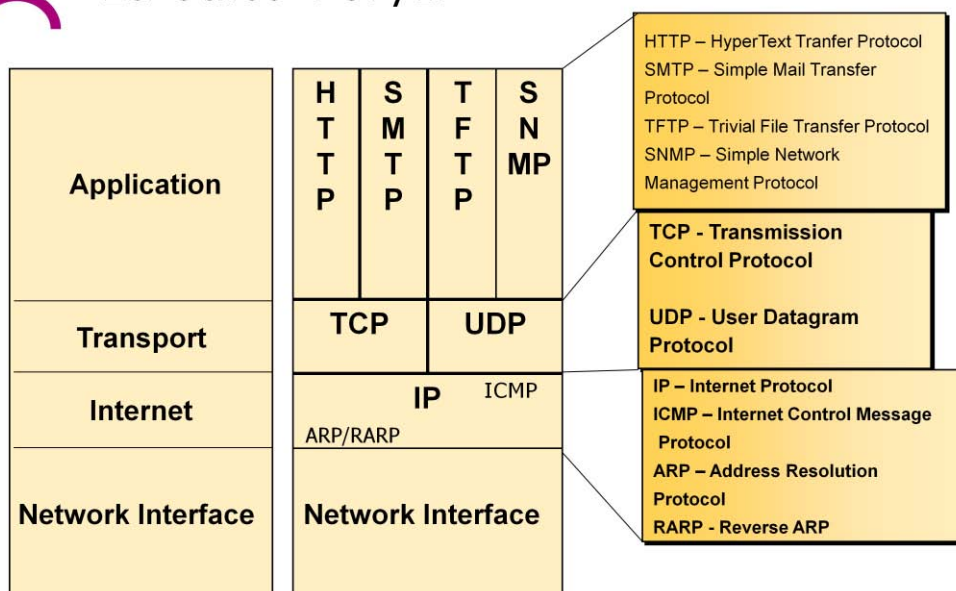
## **CAPITOLO 5**

### **La suite TCP/IP**





## La suite TCP/IP



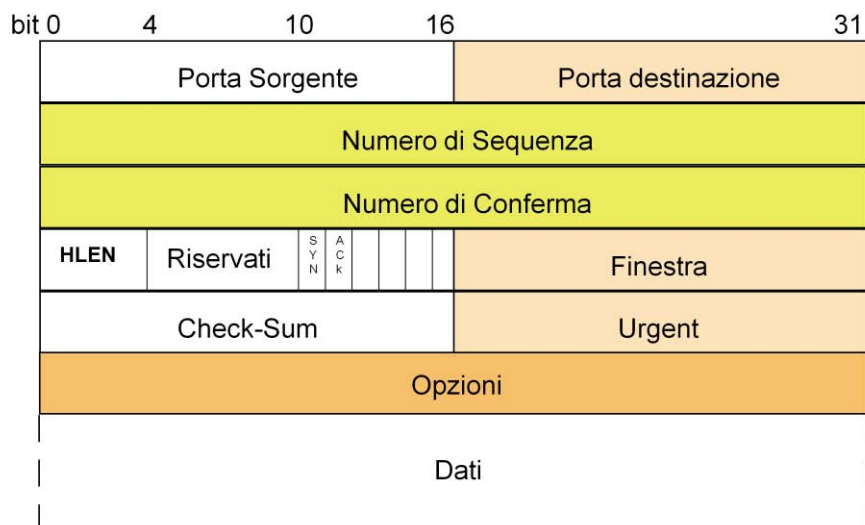
[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-2

Una delle ragioni principali del successo di Internet risiede senza dubbio nell'efficienza, semplicità di uso e convenienza delle sue basi tecnologiche. **L'intera** movimentazione dei flussi di traffico avviene sulla base di una famiglia di protocolli oggi diffusamente conosciuti come TCP/IP. Il TCP/IP non è infatti formato dai soli protocolli TCP e IP ma da una serie di altri protocolli ai vari livelli della pila protocollare tipica di Internet. TCP e IP rappresentano i protocolli fondamentali al corretto funzionamento di Internet, attraverso i quali si indica **l'intera** famiglia di tutti gli altri protocolli utilizzati.



## Formato di TCP



[www.ncp-italy.com](http://www.ncp-italy.com)

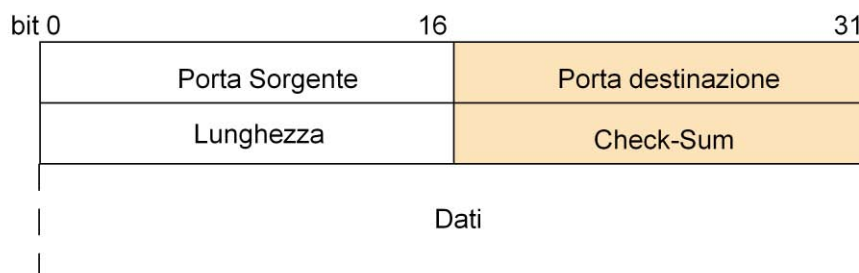
La suite TCP/IP 5-3

Il protocollo TCP (RFC 793) porta con se tutte quelle caratteristiche di affidabilità e robustezza che IP non possiede. Nel caso di TCP si parla infatti di comunicazione **"reliable"** (affidabile) mentre per IP di comunicazione **"consistant"** (consistente). Il compito di IP e dei suoi protocolli di routing è infatti quello di fornire dei percorsi consistenti con la struttura topologica della rete, mentre è completamente demandata al TCP la responsabilità di realizzare una comunicazione tra sistemi. Le principali caratteristiche di TCP sono:

- Application Multiplexing
- Three Way Handshake
- Windowing
- Sequencing
- Error Control



## Formato di UDP



UDP è un protocollo di trasporto di tipo non connesso.

Aggiunge due funzionalità a quelle di IP:

- multiplexing delle informazioni tra le varie applicazioni tramite il concetto di porta
- checksum (opzionale) per verificare l'integrità dei dati

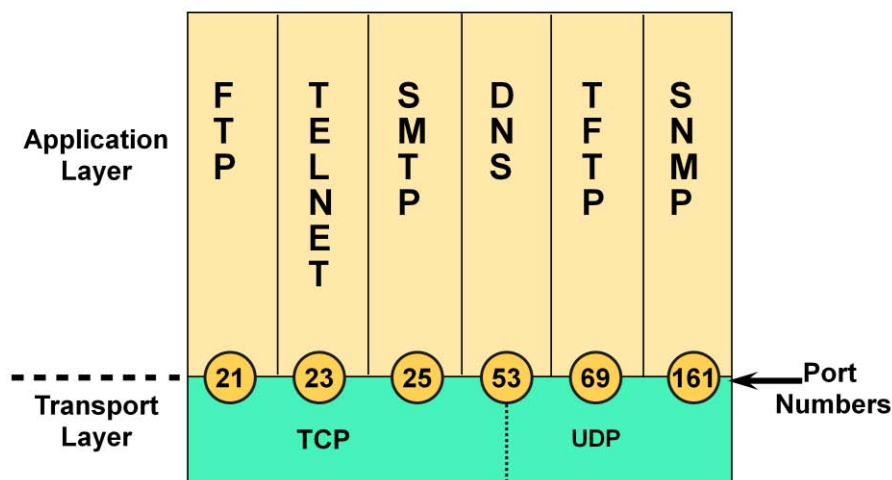
Non prevede un controllo di flusso. Non è in grado di adattarsi autonomamente a variazioni di traffico.

Non prevede meccanismi di ritrasmissione in caso di errori/perdite; eventuali meccanismi di ritrasmissione (se necessari) vengono gestiti direttamente **dall'applicazione**.

UDP è utilizzato per le applicazioni che non richiedono uno stretto controllo del flusso a livello di trasporto, alcune di queste applicazioni sono SNMP (Simple Network Management Protocol), TFTP (Trivial FTP) e DNS (Domain Name System), **quest'ultimo** in grado **all'occorrenza** di utilizzare anche TCP.



## Associazione porta/applicazione



www.ncp-italy.com

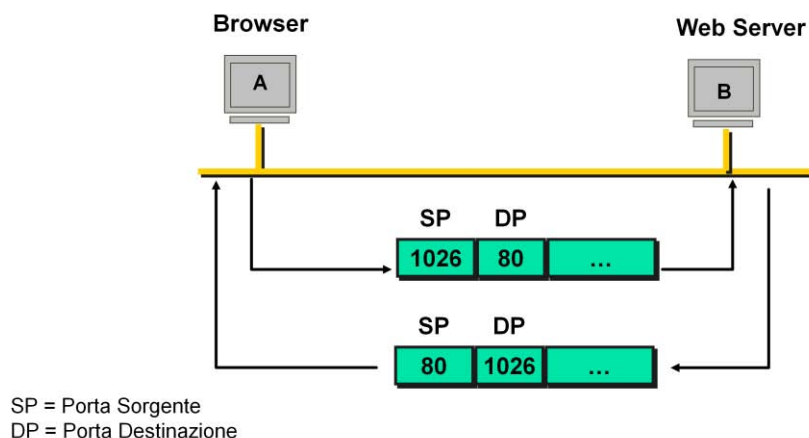
La suite TCP/IP 5-5

La discriminazione delle applicazioni avviene attraverso un numero di 16 bit che le identifica univocamente chiamato "port number" o semplicemente "porta". In figura sono mostrate alcune delle cosiddette "well-known port" assegnate alle relative applicazioni ormai famose e diffuse. **L'assegnazione** dei numeri delle porte è fondamentale per permettere una corretta comunicazione.

Si ricorre infatti ad un organismo internazionale per gestire **l'attribuzione** delle porte TCP: lo IANA che controlla e assegna le well-known port che sono assegnate **nell'intervallo** 0-1023. Le rimanenti porte (da 1024 a 65535), denominate Registered Ports, sono libere e lo IANA esercita solo **un'azione** di registrazione come servizio per la comunità. In particolare sono stati ratificati due appositi RFC che regolano **l'assegnazione** dei port number : RFC 1340 e 1700. Lo IANA **L'utilizzo** delle porte realizza la funzione di Application Multiplexing prima caratteristica di TCP e di UDP.



## Schema di comunicazione TCP



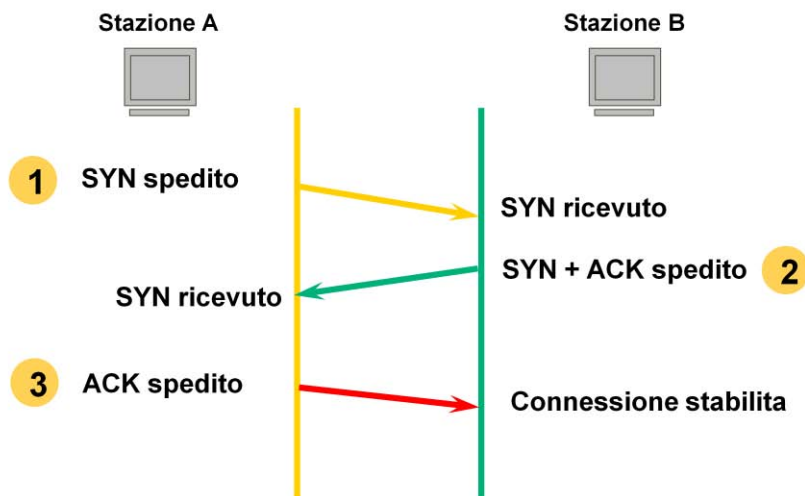
[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-6

Si distinguono in particolare due porte: la porta sorgente e la porta destinazione. La porta sorgente è la porta che identifica **l'applicazione** mittente, mentre, la porta destinazione identifica **l'applicazione** ricevente. Considerando la struttura Client-Server di Internet, **un'applicazione** Client cercherà di stabilire una connessione con **un'applicazione** Server indicando nei propri pacchetti la porta esatta associata **all'applicazione** Server e la porta che invece identifica se stessa per permettere al Server di risponderle correttamente. Ogni **"connection"** TCP (è così che si chiama in gergo tecnico una comunicazione TCP) presenta sempre una doppia porta: sorgente e destinazione. La porta sorgente è generalmente stabilita dal Client a partire dalla 1024 in poi.



# Three Way Handshake



www.ncp-italy.com

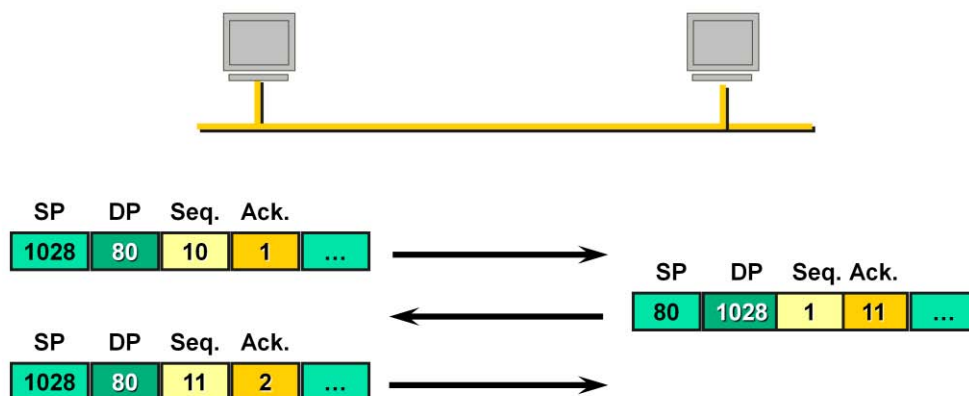
La suite TCP/IP 5-7

La funzione di Three Way Handshake opera fornendo al TCP la sua tipica caratteristica di protocollo connesso, il trasmittente infatti verifica la disponibilità del ricevente, dopo la quale avviene lo scambio delle informazioni, e al termine segue la fase di chiusura della comunicazione.

La fase di apertura della comunicazione avviene in tre passi successivi, potremmo dire con **"una stretta di mano tripla"** per rifarci al termine americano qui utilizzato (Three Way Handshake). Il mittente invia un primo pacchetto, detto di sincronismo o SYN, al destinatario (prima fase), il destinatario risponde con il proprio SYN e conferma (acknowledgement) anche la ricezione (seconda fase), il sorgente conferma la ricezione del SYN del destinatario (terza fase).



## Numerazione dei pacchetti



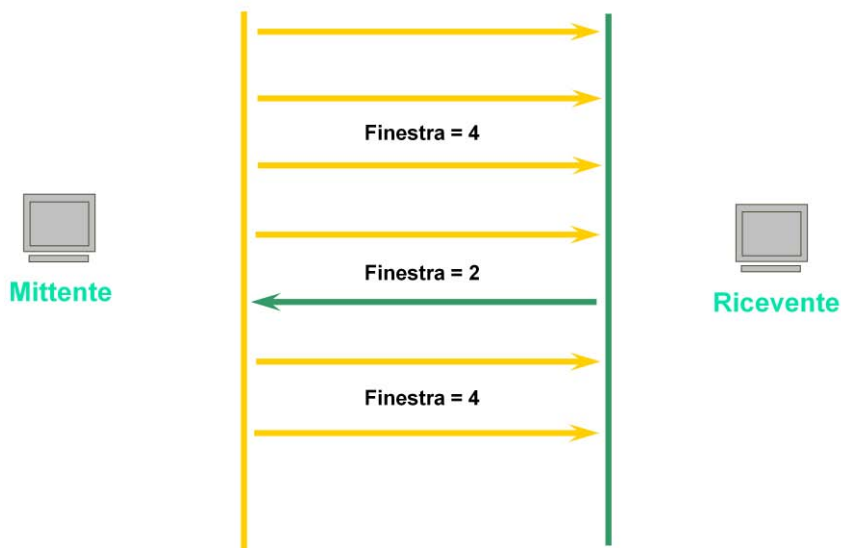
[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-8

La funzione di Sequencing fornisce al TCP la numerazione dei pacchetti per implementare i meccanismi per evitare la duplicazione e la dispersione dei pacchetti e garantire il corretto riassettaggio. In particolare TCP prevede un sequence number per numerare i pacchetti emessi e un ack number per numerare le conferme.



## Controllo del flusso con *Windowing*



[www.ncp-italy.com](http://www.ncp-italy.com)

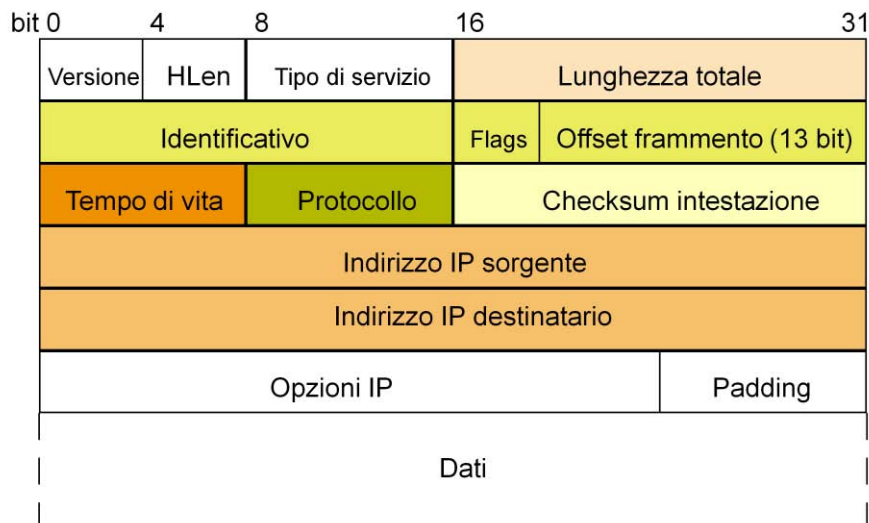
La suite TCP/IP 5-9

Il Windowing è invece un meccanismo molto sofisticato che permette al TCP di controllare il flusso modulando la velocità di trasmissione dei pacchetti. La modalità di trasmissione utilizzata da TCP prevede un invio dei pacchetti per gruppi. Il numero di pacchetti contenuti in un gruppo prende il nome di window (finestra). La stazione mittente invia un gruppo di pacchetti con finestra iniziale fissata a piacere, tipicamente bassa per poi aumentarla progressivamente, che viene in seguito continuamente negoziata con il destinatario.





## Formato IP



[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-10

Con riferimento alla pila protocollare e partendo dal livello più basso cominciano col notare che Internet è formata da una grande varietà di tecnologie di trasporto a livello locale (LAN) che a livello geografico (WAN). Tutte queste tecnologie, eterogenee tra loro, trovano integrazione a livello 3 attraverso il protocollo IP che è completamente svincolato dal mezzo trasmissivo. IP è lo strato logico che permette la comunicazione tra stazioni presenti su mezzi trasmissivi diversi. Attraverso di esso le comunicazioni si estendono oltre i limitati confini delle tecnologie di trasporto adottate sulle tratte WAN e sulle reti LAN. La condizione per comunicare in Internet è di possedere un indirizzo IP pubblico univoco. Se una stazione è accesa e presente in Internet con un proprio indirizzo IP allora è raggiungibile da tutte le altre stazioni che si trovano sulla rete. La comunicazione è resa possibile dai router che si occupano di connettere le varie reti individuando i percorsi migliori.

IP è un protocollo di livello network connectionless, che consente lo scambio di dati tra due computer (host) senza alcuna impostazione preliminare della chiamata (i due computer possono tuttavia condividere un protocollo di trasporto comune orientato alla connessione). Poiché IP è un protocollo non connesso, è possibile che i datagrammi vadano persi prima di arrivare a destinazione.

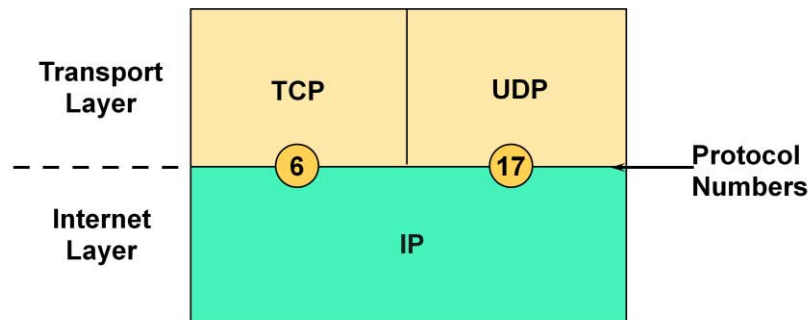
IP nasconde essendo un protocollo inaffidabile, non è munito di meccanismi di sicurezza: non prevede per esempio la correzioni degli errori, né possiede meccanismi di controllo di flusso. Il protocollo IP tratta ogni datagram come un'entità di trasmissione indipendente e scorrelata dalle altre. Il pacchetto IP ha una lunghezza variabile: 20 - 64byte

La somma dati + header deve essere minore dell' MTU (Maximum Transmission Unit), altrimenti si ha frammentazione.

- Source address: indirizzo IP mittente
- Destination address: indirizzo IP destinatario
- Protocol: protocollo di trasporto
- Fragment offset: offset del frammento nell'ambito del totale dei dati da trasmettere
- Identification: identificativo del datagram
- Flag: indica se il datagram rappresenta un frammento
- Time-To-Live (TTL): numero di router che un datagram può attraversare
- Header checksum: controllo errore sull'header
- HLen: lunghezza dell'header
- Total length: lunghezza totale



## Interfaccia tra livello 4 e IP



Il campo "Protocol" nell'header IP ha la funzione di interfaccia con i livelli superiori. Esso determina il contenuto del campo dati. Per esempio se Protocol = 6 il pacchetto IP trasporta TCP, se invece Protocol = 17 trasporta UDP.



## Messaggi ICMP

<b>administratively-prohibited</b>	<b>information reply</b>	<b>port unreachable</b>
<b>alternate-address</b>	<b>mask-reply</b>	<b>reassembly-timeout</b>
<b>conversion-error</b>	<b>mask-request</b>	<b>redirect</b>
<b>dod-host-prohibited</b>	<b>mobile-redirect</b>	<b>router-advertisement</b>
<b>dod-net-prohibited</b>	<b>net-redirect</b>	<b>router-solicitation</b>
<b>echo</b>	<b>net-tos-redirect</b>	<b>source-quench</b>
<b>echo-reply</b>	<b>net-tos-unreachable</b>	<b>source-route-failed</b>
<b>general-parameter-problem</b>	<b>net-unreachable</b>	<b>time-exceeded</b>
<b>host-isolated</b>	<b>network-unknown</b>	<b>traceroute</b>
<b>host-tos-redirect</b>	<b>no-room-for-option</b>	<b>ttl-exceeded</b>
<b>host-tos-unreachable</b>	<b>option-missing</b>	<b>unreachable</b>
<b>host-unknown</b>	<b>packet-too-big</b>	
<b>host-unreachable</b>	<b>parameter-problem</b>	

[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-12

Il protocollo ICMP è descritto in RFC 792. Incluso in tutte le implementazioni IP, è un protocollo di basso livello che si appoggia direttamente su IP.

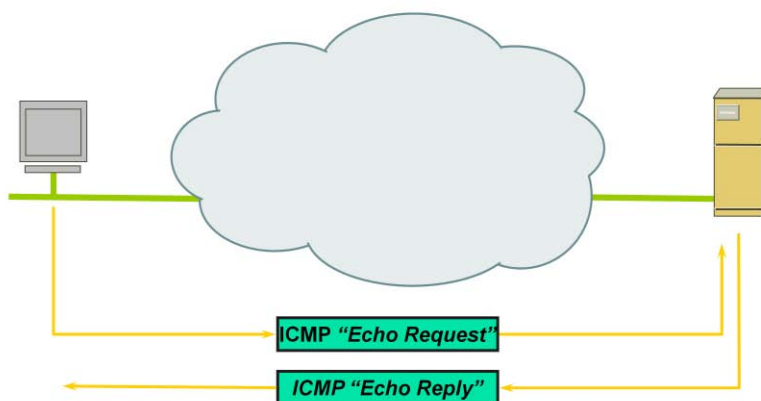
Utilizzato per la trasmissione dei messaggi di errore, di messaggi di controllo e misure di prestazioni.

I messaggi viaggiano nel campo dati del datagram IP. I messaggi vengono manipolati dal software IP, non dagli applicativi utente.

Gli amministratori sulla base del contenuto di questi messaggi sono in grado di valutare se la rete sta funzionando correttamente e in caso contrario di fare delle diagnosi di malfunzionamento.



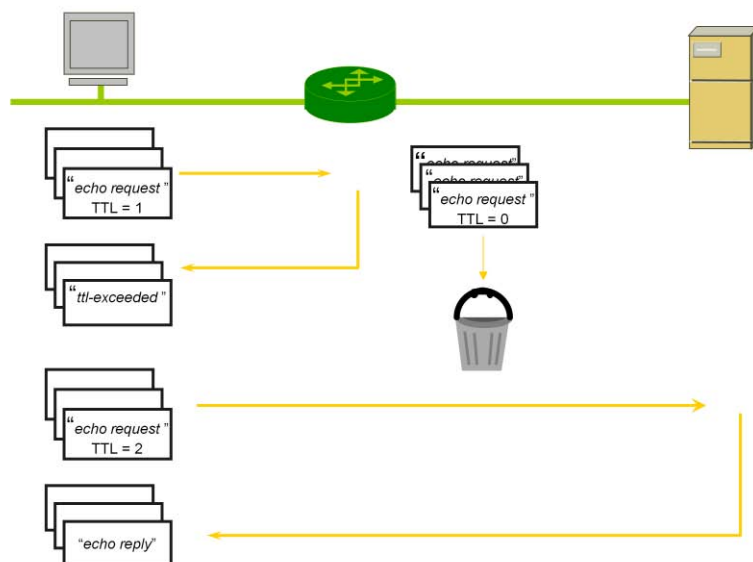
## Il Ping



La applicazione più utilizzata dagli amministratori è indubbiamente il cosiddetto PING. Attraverso il PING è possibile inviare ad una macchina in rete un messaggio di **"echo request"** al quale segue un messaggio di **"echo reply"**. Questa operazione, se arriva a buon fine, indica la raggiungibilità della stazione destinazione e assicura il corretto funzionamento degli strati protocollari dal livello 3 in sotto.



## II TRACEROUTE



www.ncp-italy.com

La suite TCP/IP 5-14

In caso di mancata raggiungibilità, è possibile utilizzare l'applicazione TRACEROUTE per procedere ad una verifica del percorso per evidenziarne i punti di interruzione. Il TRACEROUTE, infatti, invia una successione di messaggi di "echo request" a gruppi di tre incrementando il TTL a partire da 1. In questo modo i pacchetti IP raggiungono progressivamente i router presenti sul percorso verso la stazione destinazione, ricordiamo infatti che una delle operazioni che i router compiono sull'intestazione IP è decrementare il TTL di una unità, se il risultato è zero il pacchetto viene scartato. Ogni router, a fronte della ricezione del messaggio di "echo request", risponde con un "echo reply" se nella propria tabella di routing è presente una rotta verso la destinazione, altrimenti, risponde con un messaggio di errore adeguato che offre all'amministratore la possibilità di formulare delle diagnosi di "prima mano". Il TRACEROUTE mette in evidenza il numero di salti e i relativi ritardi introdotti per arrivare a destinazione offrendo generalmente anche delle statistiche sui tempi minimi, massimi e medi. Nella sua scansione dei percorsi mostra i nomi logici, se esistenti, dei vari router che attraversa permettendo una prima rozza mappa topologica.



## Esempio di Ping e Traceroute

### **Router#ping 192.168.1.254**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.254, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/13/44 ms

### **Router#ping**

Protocol [ip]:

Target IP address: 192.168.1.254

Repeat count [5]: 10

Datagram size [100]: 200

Timeout in seconds [2]: 4

Extended commands [n]: y

Source address or interface: 192.168.1.250

Type of service [0]: 5

Type escape sequence to abort.

Sending 10, 200-byte ICMP Echos to 192.168.1.254, timeout is 4 seconds:

!!!!!!!!

Success rate is 100 percent (10/10), round-trip min/avg/max = 4/16/52 ms

### **Router#traceroute 87.248.113.14**

Type escape sequence to abort.

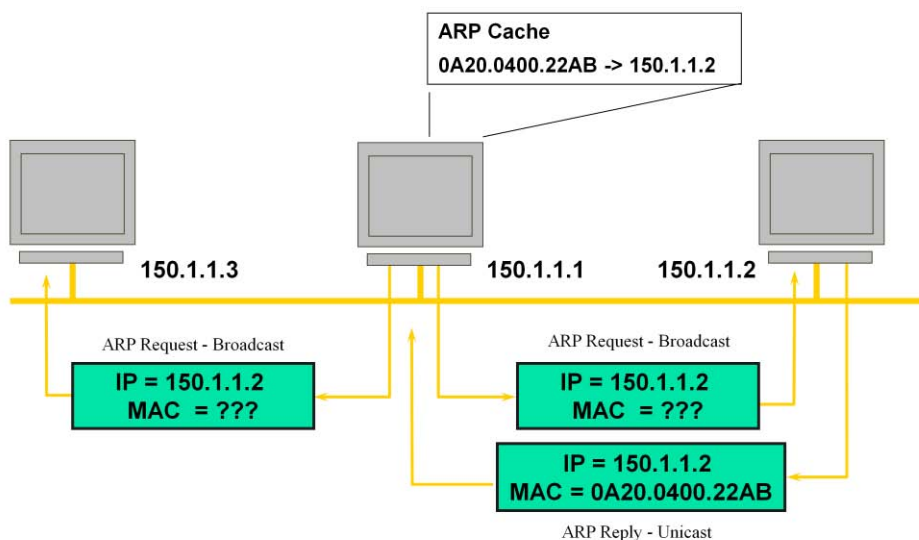
Tracing the route to 87.248.113.14

1 80.20.4.39 60 msec

2 151.99.98.158 48 msec



## ARP – Address Resolution Protocol



[Link to Trace ARP](#)

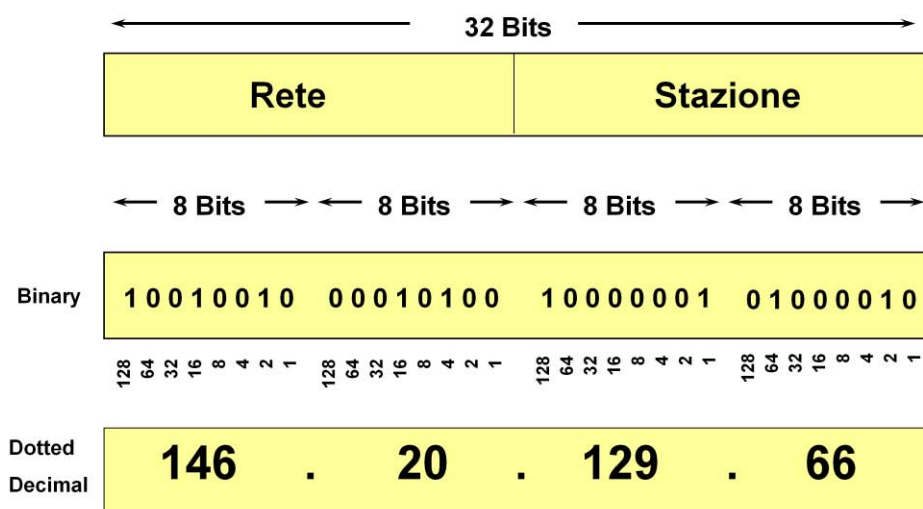
www.ncp-italy.com

La suite TCP/IP 5-16

Per le LAN l'**interfacciamento** tra livello 3 e livello 2 è realizzato da un particolare protocollo denominato ARP – Address resolution Protocol, posizionato a cavallo tra i due livelli. La funzione di ARP è di associare ad un indirizzo IP il rispettivo indirizzo MAC. Prima di iniziare una comunicazione, ogni stazione esegue una richiesta di risoluzione **dell'indirizzo** IP del destinatario nel rispettivo MAC address. Questa richiesta è eseguita in modalità broadcast in modo da pervenire a tutti, risponderà la sola stazione che possiede l'**indirizzo** IP che si vuol risolvere. Generalmente il risultato di questa operazione viene memorizzato in una cache temporanea per evitarne la ripetizione nelle comunicazioni successive.



## Struttura di un indirizzo IP



www.ncp-italy.com

La suite TCP/IP 5-17

L'indirizzo IP è composto da 32 bit ed è rappresentato in formato cosiddetto "dotted-decimal". In fatti i 32 bit sono strutturati in 4 ottetti (8bits) separati da un punto e rappresentati in formato decimale. L'indirizzo IP, come tutti gli indirizzi di livello 3, è un indirizzo logico strutturato.

Si parla di indirizzi logici strutturati quando è possibile identificare in un indirizzo due componenti distinte, che individuino la stazione e la rete di appartenenza. Ogni stazione appartenente ad un sistema di reti interconnesse, per essere individuata in modo univoco, deve possedere un indirizzo logico strutturato di livello 3. Si parla di indirizzo di rete (*network*) quando ci si riferisce alla componente che identifica la rete, mentre, si parla di indirizzo stazione (*host*) in riferimento alla componente che identifica la stazione. Tutte le stazioni appartenenti alla stessa rete devono condividere lo stesso identificativo di rete. Gli indirizzi logici strutturati ricoprono una particolare importanza nei processi d'instradamento dei pacchetti. I dispositivi che si occupano di eseguire l'instradamento dei pacchetti si chiamano *router*. Un *router* è in grado di scegliere il miglior percorso per raggiungere la rete dove si trova la stazione ricevente. Per far questo, si base sull'informazione contenuta nella porzione *network* dell'indirizzo logico di destinazione.





## Indirizzi IP: le classi

- Classe A: 

← 8 Bits →	← 8 Bits →	← 8 Bits →	← 8 Bits →
R	S	S	S
- Classe B: 

R	R	S	S
---	---	---	---
- Classe C: 

R	R	R	S
---	---	---	---
- Classe D: riservata al multicast
- Classe E: riservata a scopi di ricerca

**R = Rete**  
**S = Stazione**

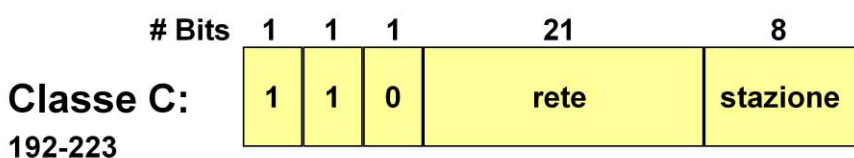
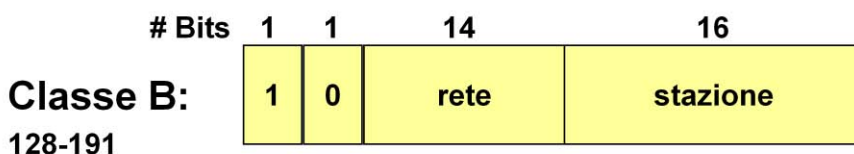
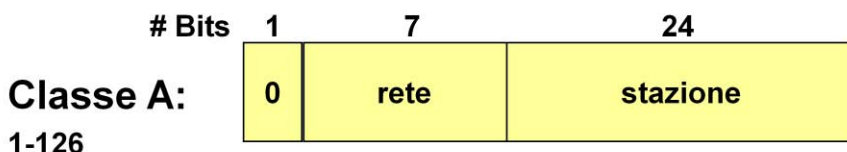
In Internet sono definite cinque classi di indirizzi designate con le lettere latine A, B, C, D, E; di queste solo le prime tre sono utilizzate effettivamente su Internet.

Le prime tre classi sono utilizzate per l'**assegnazione** degli indirizzi alle singole stazioni per la comunicazione unicast, mentre la classe D è riservata alla comunicazione multicast e possono essere utilizzati solo come indirizzi destinazione. La classe E è riservata a scopi di ricerca.

Ogni classe (A,B,C) presenta una propria struttura di indirizzi imponendo un ben definito numero di bit riservato alla porzione Rete. Una rete di classe A, ad esempio, è identificata dal primo byte con i restanti tre byte ad indicare i singoli nodi; una rete di classe B invece utilizza i primi 2 ottetti; mentre una rete di classe C è individuata dai prime tre lasciando solo l'ultimo per designare le stazioni.



## Definizione delle classi



Il riconoscimento del tipo di indirizzo viene eseguito sul primo byte sulla base della seguente regola: se il primo bit è uguale a zero si identifica un indirizzo di classe A, se il primo bit è uguale a 1 e il secondo è uguale a zero si determina un indirizzo di classe B, infine, se il terzo bit a essere uguale a 0 con i primi due posti a 1 si ha un indirizzo di classe C.

Sulla base di questa regola e utilizzando la notazione decimale ad ottetti per rappresentare gli indirizzi IP si perviene alla seguente distinzione: per le reti di classe A i valori del primo byte variano da 1 a 127 (127 riservato per gli indirizzi di loopback), per quelle di classe B da 128 a 191, per quelle di classe C da 192 a 223. Ne risulta che gli indirizzi di classe A sono limitati a 126. La loro caratteristica è di identificare un numero limitato di reti in grado di ospitare ciascuna un numero molto alto di stazioni, precisamente  $2^{24} - 2$  (16.777.214) essendo 24 il numero di bit riservato alla porzione Stazione e scartando il primo e ultimo indirizzo perché sempre riservati alla rete e al broadcast. Tali reti sono assegnate a grandi aziende e a ISP i quali estrarranno da queste "mega" reti altre sottoreti più piccole per indirizzare meglio le loro realtà tipicamente molto variegata e complesse. Esempi di reti di classe A assegnate a note aziende sono riportate in figura 16. Le reti di classe B (due byte per l'indirizzo) possono essere 16.384 ( $64 \times 256$ ), ognuna delle quali può ospitare fino a 65.534 host. Infine le reti di classe C potranno essere 2.097.152 ( $32 \times 256 \times 256$ ), composte da un massimo di 254 host.



## Alcune classi A assegnate

Rete	Azienda	Data
-----	-----	-----
003	General Electric Company	May 94
004	Bolt Beranek and Newman Inc.	Dec 92
009	IBM	Aug 92
012	AT&T Bell Laboratories	Jun 95
013	Xerox Corporation	Sep 91
015	Hewlett-Packard Company	Jul 94
016	Digital Equipment Corporation	Nov 94
017	Apple Computer Inc.	Jul 92
018	MIT	Jan 94
019	Ford Motor Company	May 95
047	Bell-Northern Research	Jan 91
055	Boeing Computer Services	Apr 95
056	U.S. Postal Service	Jun 94

[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-20



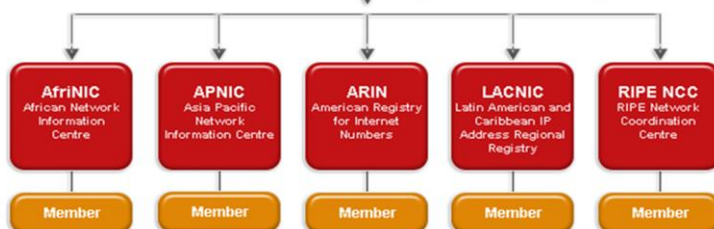
# La gerarchia delle Authority

Coordinates the allocation and assignment of :

- ✓ Domain names (forming a system referred to as "**DNS**");
- ✓ Internet protocol ("**IP**") addresses and autonomous system ("**AS**") numbers; and
- ✓ Protocol port and parameter numbers



**Regional Internet Registries (RIRs)**



**Local Internet Registries (LIRs)**

[Link to RIPE e LIR Registry](#)

[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-21

L'assegnazione effettiva degli indirizzi di rete viene curata da un organismo internazionale, l'Internet Assigned Number Authority (IANA), il quale a sua volta delega a 5 enti territoriali la gestione degli indirizzi di rete nei vari paesi:

- APNIC (Asia Pacific Network Information Centre) - Asia/Regioni del Pacifico
- ARIN (American Registry for Internet Numbers) - America e Africa sub-sahariana
- RIPE NCC (Réseaux IP Européens) - Europa e Regioni limitrofe
- AfriNIC (Africa Network Information Center)
- LACNIC (Latin American and Caribbean Network Information Center)

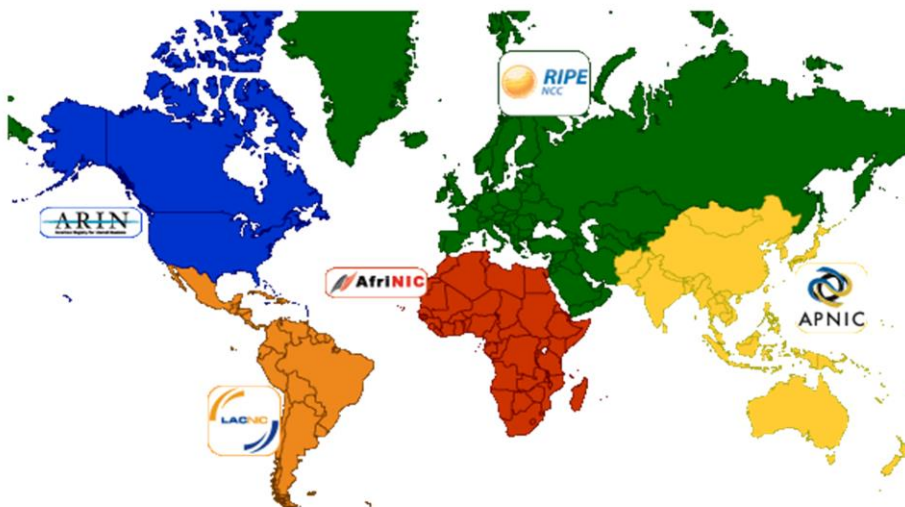
Ognuno di questi enti a sua volta assegna a delle entità locali chiamate LIR (Local Internet Registries) dei blocchi di indirizzi su base richiesta. Da questi ultimi si riforniscono aziende istituzioni pubbliche e piccoli ISP. Tra i LIR troviamo anche il GARR che storicamente si è dedicato alla gestione della Registration Authority italiana, ma l'espansione commerciale della rete Internet anche in Italia ha progressivamente portato allo svincolamento delle procedure centrali di gestione dal solo mondo della ricerca universitaria.

In ultima istanza la cura degli indirizzi di ogni singola stazione è affidata agli amministratori di rete in relazione alle proprie politiche aziendali in rispetto degli standard.

Una conseguenza del complicato (ma efficiente) schema di indirizzamento di Internet è che gli indirizzi sono limitati. Lo scorso febbraio 2011 IANA ha dato l'**annuncio** di aver esaurito le corti di indirizzi IP da assegnare ai Registry. Viviamo oggi una fase di transizione il nuovo protocollo IP, denominata 'IP Next Generation' o 'IP 6', basata su un sistema di indirizzamento a 128 bit. Le possibili combinazioni sono decisamente al di là del numero di abitanti del pianeta.



## Regional Internet Registries (RIRs)

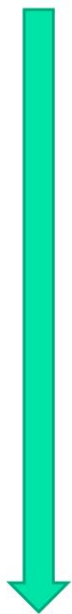


[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-22



## IPv4 vs IPv6



*IPv4 (32 bit)*

*192.0.2.53*

7 indirizzi IPv4 ogni  
milione di metri quadrati.

*IPv6 (128 bit)*

*2001:0db8:582:ae33::29*

Per ogni metro quadrato di superficie terrestre, ci sono  
666.000.000.000.000.000.000.000 indirizzi IPv6 unici, cioè  
**666 mila miliardi di miliardi.**





## Formato indirizzi IPv6

- Indirizzi di **128 bit** espressi in **esadecimale**, es.:  
**ABCD:EF01:2345:6789:ABCD:EF01:2345:6789**
- Si possono omettere gli zero iniziali e usare **::** al posto di una serie di zeri:  
**A:B:C:D:E:F:12:3456::194:221:3:122**
- Non si utilizza la Mask, ma la lunghezza del Prefisso espressa come **/N**:  
**172:16:34::/48** indica il Prefisso **172:0016:0034**

Per quanto riguarda gli indirizzi, in IPv6 la dimensione è stata estesa da 32 a 128 bit con l'utilizzo di un nuovo formato di rappresentazione. L'indirizzo è suddiviso in 8 blocchi da 16 bit ciascuno, separati dal carattere ":" (due punti) ed espresse in esadecimale. Questo nuovo formato e soprattutto la più grande lunghezza li rende difficili da ricordare e quindi di farne lo stesso utilizzo disinvolto degli indirizzi IPv4. Questo spingerà gli utenti ad utilizzare sempre più nomi simbolici e meccanismi di auto configurazione (DHCP). Esistono anche delle forme abbreviate per semplificarne la rappresentazione: si possono tralasciare gli zeri non significativi e sostituire una serie di zeri con il simbolo "::". La dimensione degli indirizzi IPv6 è stata studiata nell'ottica di rimandare il più a lungo possibile nuovi problemi di esaurimento, possibilmente per sempre. Per questo è stata scelta la lunghezza di 128 bit. Il numero di combinazioni generate da un simile valore è enorme e persino difficile da percepire, visto che si tratta di un numero composto da 38 zeri (in forma esponenziale circa  $3,4 \times 10^{38}$ ). Anche ipotizzando un futuro in cui tutto sarà connesso in rete, dai cellulari agli elettrodomestici, è difficile immaginare di esaurire una simile quantità di indirizzi. Per dare un'idea delle grandezze in gioco, riportiamo un calcolo eseguito sulla base delle ricerche di Huitema, per cui, ipotizzando una popolazione mondiale di 10 miliardi, e un numero di indirizzi IP per persona uguale a 100.000, sarebbero sufficienti 68 bit.

In IPv6 scompare completamente la vecchia suddivisione in classi, insieme al concetto di Netmask che viene sostituito da quello di "Prefix" (Prefisso). Il prefisso è indicato definendone la lunghezza utilizzando la notazione "/n" alla fine dell'indirizzo (dove "n" rappresenta appunto la lunghezza del prefisso espressa in bit). Un'altra novità di IPv6 è che non si fa più uso degli indirizzi di broadcast; sono previsti solo indirizzi unicast, multicast e introdotti i nuovi indirizzi di anycast, quest'ultimi per schematizzare un insieme di interfacce appartenenti ad uno stesso nodo; un pacchetto inviato ad un indirizzo anycast raggiunge l'interfaccia disponibile più vicina sulla base delle metriche dei protocolli di routing presenti.



## La subnet Mask

	Rete/Network				Stazione/Host			
IP	146	.	20	.	129	.	66	
Mask	1	1	1	1	1	1	1	1
Mask	255	.	255	.	0	.	0	
Rete	146	.	20	.	0	.	0	
Host	0	.	0	.	129	.	66	

[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-25

L'utilizzo della Mask ha come obiettivo quello di strutturare un indirizzo IP a piacere facendo variare a piacere la porzione dedicata alla rete e di conseguenza quella dedicata alla stazione. Il meccanismo è molto semplice, è sufficiente aggiungere all'indirizzo IP una sequenza di 32 bit, anch'essi espressi in formato dotted-decimal, che presenti 1 in corrispondenza della porzione rete e 0 in corrispondenza della porzione host. Definita una Mask rimangono automaticamente individuato l'indirizzo di rete e l'indirizzo stazione. Utilizzando la Mask è possibile creare delle reti di dimensioni variabili rispettando comunque lo schema delle classi.





## Maschere naturali

	8	16	24	
■ Classe A:	255	0	0	/8
■ Classe B:	255	255	0	/16
■ Classe C:	255	255	255	/24

Le reti relative ad ogni classe prendono il nome di  
**MAJOR NETWORKS**

Per ogni classe rimane individuata una maschera naturale ottenuta ponendo ad uno i bit della Mask relativi alle porzioni rete assegnate ad ogni classe. Oltre alla rappresentazione decimale, è possibile utilizzare anche una rappresentazione semplificata facendo seguire **all'indirizzo** IP, separato da uno **"/**", il numero di bit riservato alla rete.

Le reti relative ad ogni classe prendono il nome di Major Networks.

Esempi di Major Networks sono:

12.0.0.0 (classe A)

156.23.0.0 (classe B)

195.201.23.0 (classe C)

Non sono Major Networks:

12.123.0.0

24.189.67.0

167.24.192.0

195.98.0.0



## Combinazioni per Subnet mask

128	64	32	16	8	4	2	1	
↓	↓	↓	↓	↓	↓	↓	↓	
1	0	0	0	0	0	0	0	= 128
1	1	0	0	0	0	0	0	= 192
1	1	1	0	0	0	0	0	= 224
1	1	1	1	0	0	0	0	= 240
1	1	1	1	1	0	0	0	= 248
1	1	1	1	1	1	0	0	= 252
1	1	1	1	1	1	1	0	= 254
1	1	1	1	1	1	1	1	= 255



## AND Logico

X	Y	X(AND)Y
0	0	0
0	1	0
1	0	0
1	1	1



## Le sottoreti o *subnets*

	Rete		Sottorete	Stazione
IP 146.20.129.66	10010010	00010100	10000001	01000100
Mask 255.255.255.0	11111111	11111111	11111111	00000000
	10010010	00010100	10000001	00000000
Sottorete	146	20	129	0

www.ncp-italy.com

La suite TCP/IP 5-29

Nel 1985, l'**RFC 950** ha definito una procedura standard per supportare il subnetting, ovvero la divisione, di una singola rete di classe A, B o C in sottoreti di dimensioni minori. Il subnetting è stato introdotto per superare alcuni dei problemi che Internet cominciava ad avere con la gerarchia di indirizzamento a due livelli (network + host):

La continua crescita delle tabelle di routing.

Le organizzazioni dovevano richiedere un indirizzo di rete prima di poter installare una nuova LAN nella propria rete privata.

Entrambi questi problemi sono stati affrontati aggiungendo un terzo livello gerarchico (network + subnet + host) allo schema di indirizzamento iniziale.

Il subnetting ha risolto il problema della crescita delle tabelle di routing facendo in modo che le sottoreti di una rete non siano visibili **all'esterno** della rete stessa. Il percorso da Internet a qualsiasi sottorete di una certa rete IP è lo stesso, in quanto tutte le sottoreti condividono lo stesso indirizzo di rete (pur avendo differenti subnetid). Quindi, mentre i router **all'interno** della rete devono distinguere le singole sottoreti, i router di Internet hanno **un'unica** entry nella tabella di routing che individua tutte le sottoreti. Ciò consente **all'amministratore** di rete di introdurre una complessità arbitraria alla rete senza accrescere le dimensioni delle tabelle di routing di Internet.

Il subnetting ha risolto il problema della continua richiesta di indirizzi IP, assegnando ad ogni organizzazione uno (o al più alcuni) indirizzi di rete. **L'organizzazione** è poi libera di assegnare un differente numero di sottorete per ognuna delle sue reti interne. Ciò consente ad **un'organizzazione** di usufruire di sottoreti aggiuntive senza la necessità di ottenere un nuovo indirizzo di rete.

L'ampiezza dei campi subnet e host viene definita tramite un parametro detto netmask. La netmask contiene bit a uno in corrispondenza dei campi network e subnet, e a zero in corrispondenza del campo host.

Per determinare la subnet di appartenenza di un host a partire dal suo indirizzo IP, basta mettere in AND bit a bit la netmask con l'indirizzo IP. L'importanza di comprendere se due indirizzi appartengono o no alla stessa subnet è di fondamentale importanza in quanto il primo livello di routing è implicito nella corrispondenza fissata in TCP/IP tra reti fisiche e subnet IP: una rete fisica deve coincidere con una subnet IP.



## Esempio (1)

Assegnata la Major Network 146.20.0.0 realizzare delle subnet in grado di ospitare non più di 60 stazione ognuna

10010010	00010100	00000000	00	000000	146.20.0.0
11111111	11111111	11111111	11	000000	255.255.255.192
		00000000	00		146.20.0.0
		00000000	01		146.20.0.64
		00000000	10		146.20.0.128
10010010	00010100	.	.	000000	
		.	.		
		11111111	11		146.20.255.192



## Esempio (2)

Ad ogni subnet appartengono  $2^6$  indirizzi di cui il primo e l'ultimo sono riservati rispettivamente alla subnet e al broadcast -> indirizzi disponibili da assegnare alle stazioni  $2^6 - 2 = 62$ .

146.20.0.0          Major Network

255.255.255.192   Mask

146.20.0.0      Subnet-zero Not Recommended

146.20.0.64

146.20.0.128

•  
•  
•

146.20.0.128 Subnet

146.20.0.129

146.20.0.130

•

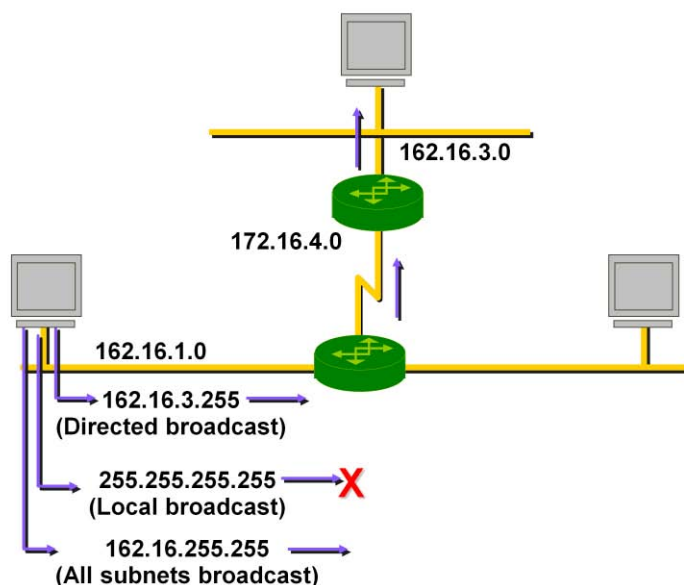
146.20.0.190

146.20.0.191 Broadcast

Stazioni



## Tipologie di Broadcast



www.ncp-italy.com

La suite TCP/IP 5-32

Esistono fondamentalmente due tipologie di broadcast:

- *Directed Broadcast*
- *Local Broadcast*

Il **Local Broadcast** è rappresentato dall'indirizzo 255.255.255.255, il quale indica che è diretto a tutti, e per questo motivo i router non lo inoltrano MAI confinandolo appunto "localmente".

Il **Directed Broadcast** è invece diretto alle stazioni di una particolare rete e, se il router possiede una rotta valida specifica, procede con l'instradamento.

Gli RFC che forniscono approfondimenti sul tema sono:

- RFC 919, Broadcasting Internet Datagrams
- RFC 922, Broadcasting IP Datagrams in the Presence of Subnets



# Inoltro dei pacchetti IP

## Inoltro diretto

- La trasmissione di un IP datagram tra due host connessi su una stessa rete IP (stesso prefisso) non coinvolge i router
- Il trasmettitore incapsula il datagram nel frame fisico e lo invia **direttamente all'host destinatario**

## Inoltro indiretto

- La trasmissione di un IP datagram tra due host connessi su differenti reti IP (diverso prefisso) coinvolge i router
- Il trasmettitore incapsula il datagram nel frame fisico e lo invia al **default gateway**
- I datagram passano da un router all'altro finchè non raggiungono un router che può trasmetterli direttamente

Si parla di rete fisica indicando le macchine, o meglio le interfacce, che sono attestate su una stessa sottorete dove una particolare tecnologia di trasporto assicura la connessione.

Una rete logica è **l'insieme** delle interfacce a cui è stato assegnato lo stesso indirizzo di subnet e in cui il routing è implicito: due macchine **all'interno** della stessa rete logica possono comunicare senza dover passare attraverso un router.

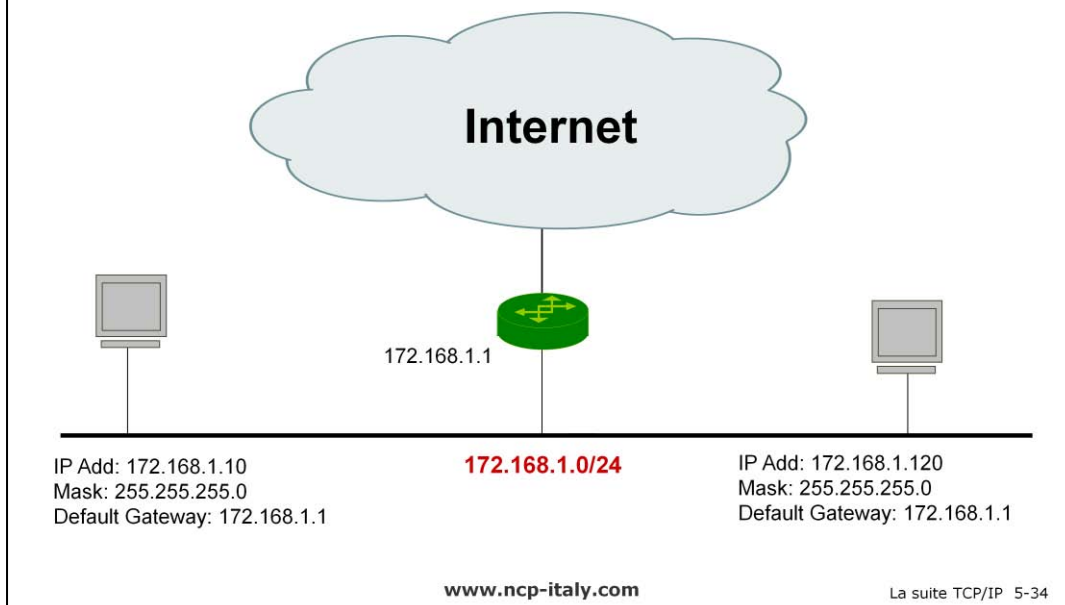
Come detto, IP assumeva originariamente una corrispondenza biunivoca tra reti fisiche e logiche; realizzazioni più moderne ammettono anche più reti logiche nella stessa rete fisica. Il routing tra reti logiche diverse è esplicito ed è gestito dai router tramite tabelle di instradamento.

IP adotta i concetti di destinazioni dirette e indirette nella sua logica di routing. Un host diretto è una stazione collegata direttamente alla rete ed al router della rete, mentre un host indiretto è un host di destinazione situato su una rete diversa da quella **dell'host** di origine; questo significa che il datagramma deve essere inviato ad un router intermedio prima di essere consegnato **all'host** di destinazione. Il modo in cui IP gestisce gli indirizzi e decide i percorsi di routing, richiede che una macchina esamini solo la parte contenente il prefisso **dell'indirizzo** di destinazione, per determinare se **l'host** di destinazione è collegato direttamente o indirettamente alla rete **dell'host** di origine: in altri termini, la macchina verifica la corrispondenza della parte **'network + subnet'** **dell'indirizzo** di destinazione e sceglie se effettuare un forwarding diretto o indiretto.





## Inoltro indiretto



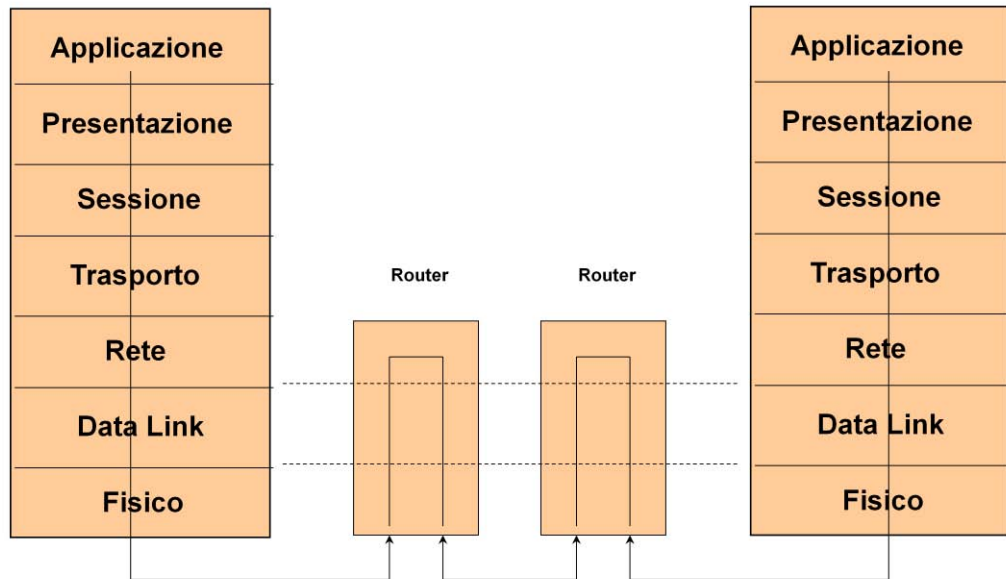
**Nell'inoltro** indiretto le stazioni fanno utilizzo di un Default Gateway, un dispositivo in grado di inoltrare i pacchetti verso altre reti, tipicamente un router.

Ogni stazione deve quindi conoscere **l'indirizzo** IP del router al quale far riferimento per **l'inoltro** dei pacchetti. La stazione capisce che deve utilizzare un Default Gateway guardando **l'indirizzo** IP della stazione di destinazione e confrontandolo con la subnet di appartenenza. Se la stazione verifica che la condizione di appartenenza è soddisfatta allora fa utilizzo del Default Gateway, altrimenti cercherà di raggiungere il destinatario direttamente sulla propria LAN utilizzandone **l'indirizzo** MAC presente in Arp Cache o risolto con **un'ARP** Request

## **Il routing dei pacchetti**



# Il Routing e la pila OSI



[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-36

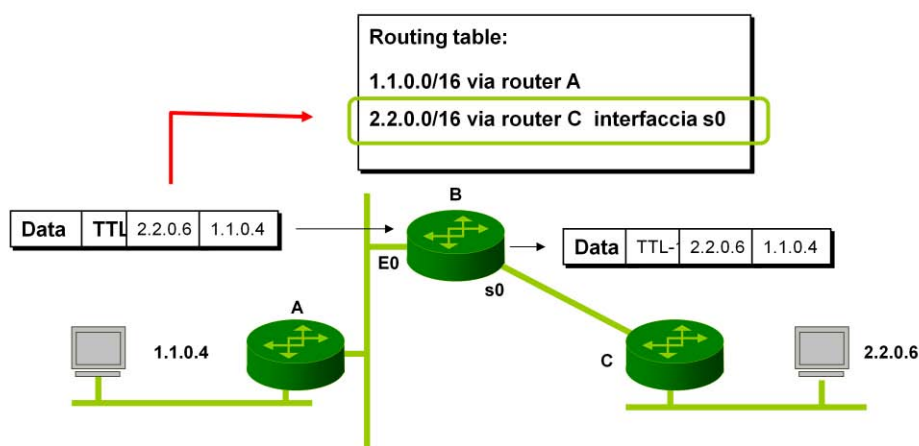


## Funzioni del router

- **Commutazione dei pacchetti**
  - Il router muove i pacchetti dall'interfaccia di entrata a quella di uscita sulla base delle informazioni contenute nella routing table
- **Determinazione del miglior percorso**
  - I router comunicando tra di loro o con l'intervento dell'amministratore determinano il miglior percorso verso le reti di destinazione
- **Integrazione dei mezzi trasmissivi**
  - Il router modifica il formato delle trame di livello 2 coerentemente con i mezzi trasmissivi delle interfacce impegnate nel processo di commutazione



# Commutazione dei pacchetti



www.ncp-italy.com

La suite TCP/IP 5-38

La principale funzionalità di un router è **l'instradamento** dei pacchetti (packet forwarding): un router riceve su **un'interfaccia** di entrata un pacchetto, controlla **l'indirizzo** IP di destinazione e decide su quale interfaccia inoltrare il pacchetto. Per prendere questa decisione il router deve mantenere in memoria delle informazioni che gli permettano di saper, in funzione della rete di destinazione, su quale interfaccia eseguire **l'inoltro**. Lo strumento che realizza questo processo si tabella di routing. Il processo decisionale di consultazione della tabella prende il nome di routing table lookup.

Ogni inserzione nella tabella è in genere composta da:

- la rete di destinazione seguita dalla Mask associata
- il costo del percorso verso la destinazione
- **l'indirizzo** del Next-Hop e/o **l'interfaccia** su cui inoltrare il pacchetto.

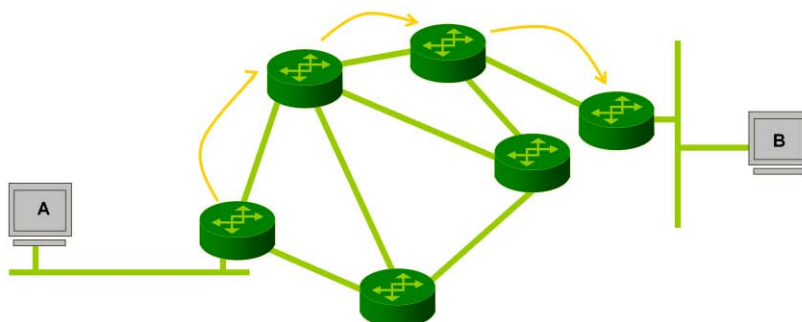
**L'insieme** di queste informazioni prende il nome di rotta (route)

Per Next-Hop si intende il router adiacente a cui affidare il pacchetto per i successivi inoltri per il raggiungimento della rete destinazione.

Nell'instradamento dei pacchetti si possono verificare due casi: il router è in grado di raggiungere direttamente la rete di destinazione ovvero il router non è in grado di raggiungere direttamente la rete di destinazione e deve fare affidamento ad un altro router al quale consegnare il pacchetto. Il router al quale viene consegnato il pacchetto prende il nome di next hop router o semplicemente next hop . Questo processo è anche noto con il nome di hop-by-hop routing, ed esprime come la consegna a destinazione del pacchetto avvenga attraverso un processo a salti successivi: come per attraversare un torrente si salta di sasso in sasso, così, per attraversare una rete complessa si salta di router in router.



## Determinazione del miglior percorso



- Rotte connesse
- Rotte statiche
- Rotte dinamiche

[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-39

Le rotte presenti **all'interno** della tabella di routing possono essere di tre tipologie

- rotte connesse: rotte corrispondenti alle interfacce del router.
- rotte statiche: rotte configurate staticamente dal gestore.
- rotte dinamiche: rotte apprese in modo dinamico attraverso l'utilizzo di un cosiddetto '**protocollo di routing**'

Nel caso che una stessa rotta venisse appresa da diverse fonti, deve essere specificato quale fonte deve essere preferita.

L'**amministratore** può scegliere se adottare una soluzione statica, dinamica o mista. Esaminiamone vantaggi e svantaggi prendendo in considerazione due aspetti fondamentali:

- adattamento ai cambiamenti topologici
- impegno di banda

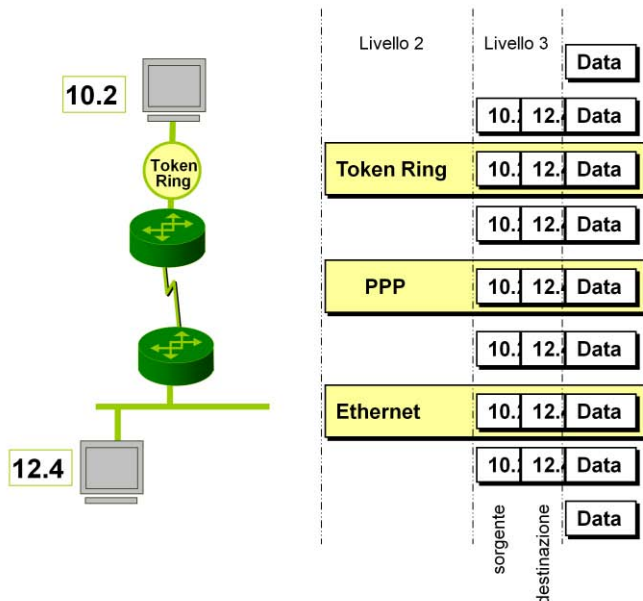
In un approccio statico i router ricevono le rotte direttamente **dall'amministratore** e non devono quindi scambiare informazioni fra di loro per costruirle, di conseguenza non generano traffico che può impegnare la rete. **D'altro** canto a fronte di un cambiamento topologico i router non sono in grado di adattarsi ad una nuova situazione, a meno che l'**amministratore** non intervenga di nuovo a modificare le rotte presenti in tabella con, ovviamente, lunghi tempi di reazione.

Il routing dinamico permette invece un adattamento molto veloce rispetto a possibili variazioni topologiche con un ricalcolo repentino della tabella di routing. Il tempo che il protocollo di routing impiega nel ricalcolo di tutte le tabelle di routing prende il nome di "**tempo di convergenza**", mentre si parla di "**convergenza**" in riferimento alla situazione di ristabilizzazione della rete dopo un processo di ricalcolo avvenuto a fronte di un cambiamento topologico.

I tempi di convergenza variano da protocollo a protocollo e possono andare da valori **dell'ordine** dei 2 secondi fino a qualche decina di minuti in casi di situazioni particolarmente sfavorevoli



## Integrazione dei mezzi trasmissivi



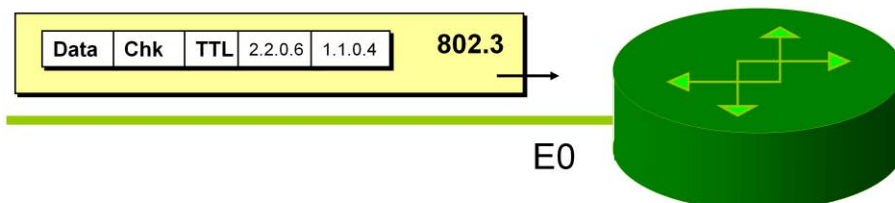
www.ncp-italy.com

La suite TCP/IP 5-40

È interessante notare che ad ogni salto tra un router e il successivo, si possono attraversare differenti tipi di tecnologie di trasporto Livello 2, questo implica che nel muovere un pacchetto **dall'interfaccia** di entrata a quella di uscita, il router può dover incapsulare il pacchetto in una trama di Livello 2 diversa. Nell'attraversare una serie di router, le informazioni di Livello 2 vengono continuamente rimaneggiate sia nei contenuti che nei formati.



## Operazioni elementari del Router



**IP Destinazione 2.2.0.6**

**IP Sorgente 1.1.0.4**

**TTL = 255**

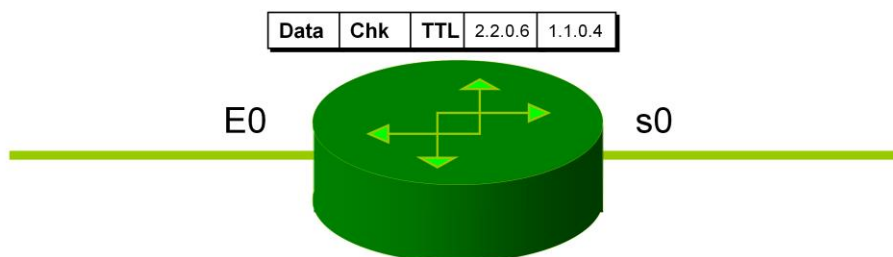
**Check-Sum = 85E2**





## Operazioni elementari del Router

Estrae il pacchetto IP dalla trama di Livello 2



**IP Destinazione 2.2.0.6**

**IP Sorgente 1.1.0.4**

**TTL = 255**

**Check-Sum = 85E2**

[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-42



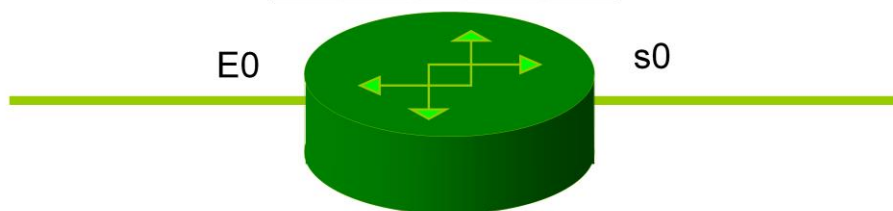
## Operazioni elementari del Router

Confronta l'indirizzo IP destinazione  
con la tabella di routing per verificare  
l'esistenza di una rotta

Routing table:

1.1.0.0/16 via router A  
2.2.0.0/16 via router C interfaccia s0

Data	Chk	TTL	2.2.0.6	1.1.0.4
------	-----	-----	---------	---------



IP Destinazione 2.2.0.6

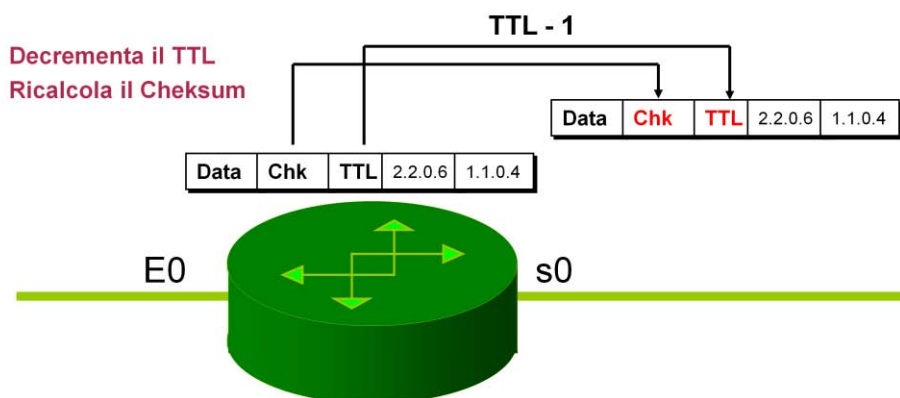
IP Sorgente 1.1.0.4

TTL = 255

Check-Sum = 85E2



## Operazioni elementari del Router



IP Destinazione 2.2.0.6

IP Sorgente 1.1.0.4

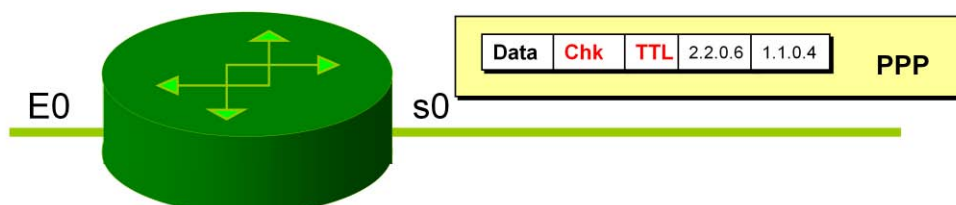
TTL = 254

Check-Sum = FF05



## Operazioni elementari del Router

Inoltra il pacchetto sulla relativa interfaccia  
di uscita imbustandolo con la trama giusta



**IP Destinazione 2.2.0.6**

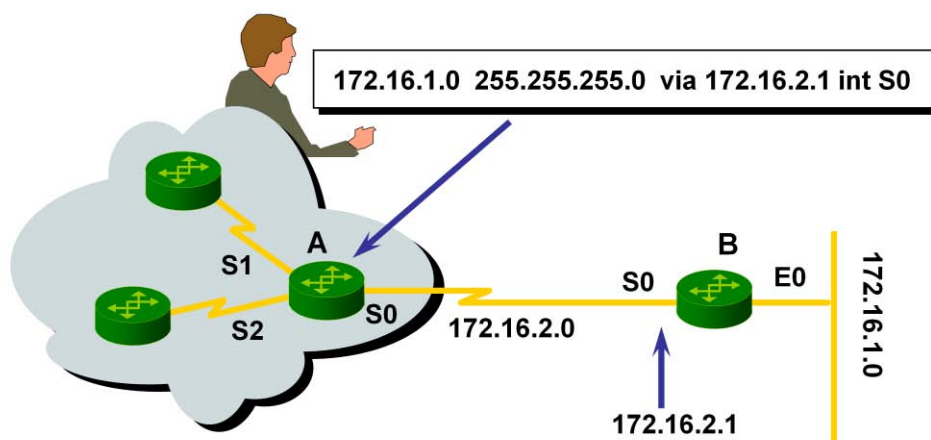
**IP Sorgente 1.1.0.4**

**TTL = 254**

**Check-Sum = FF05**

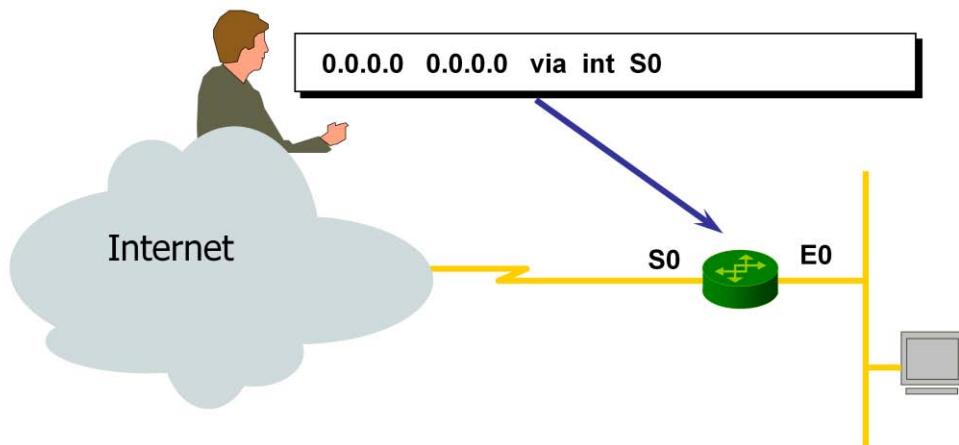


## Routing statico





## Default Route





## Il protocollo DHCP

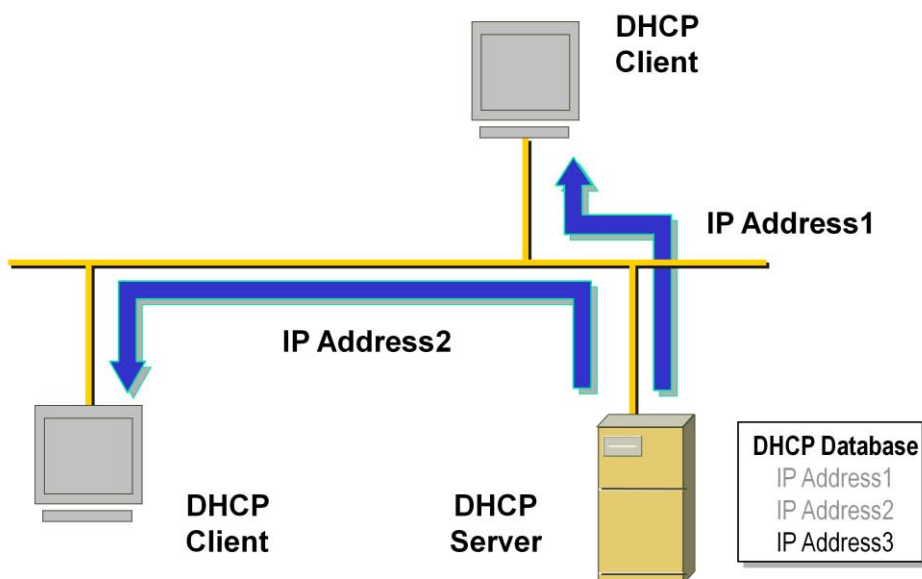
- Il protocollo DHCP (**Dynamic Host Configuration Protocol**) assegna automaticamente indirizzi IP ai computer superando le limitazioni imposte dalla configurazione manuale
- DHCP è un'estensione del protocollo **BOOTP** (RFC 1532), che consente a client BOOTP diskless di avviare e configurare automaticamente lo stack TCP/IP
- Il protocollo DHCP è definito negli **RFC 1533, 1534, 1541 e 1542**

Il protocollo DHCP (Dynamic Host Configuration Protocol) è utilizzato generalmente in ambito LAN per assegnare alle singole stazioni, in modo automatico e dinamico, un indirizzo IP pescato **all'interno** di un opportuno intervallo di indirizzi. Questo meccanismo introduce due considerevoli vantaggi:

- La possibilità di gestire **l'assegnazione** degli indirizzi IP in modo centralizzato, attraverso la gestione di un singolo server DHCP che dinamicamente soddisfa le richieste di indirizzi da parte dei client; **l'amministratore** di rete non deve più passare in rassegna ogni PC per configurare i corretti parametri di configurazione della scheda di rete.
- La possibilità di utilizzare un numero di indirizzi più basso delle reali postazioni presenti **all'interno dell'azienda**, saranno utilizzati solo gli indirizzi assegnati alle reali stazioni accese e collegate in rete.



## DHCP: client e server



[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-49

Il paradigma di comunicazione del protocollo DHCP è Client-Server. Il Server è in ascolto su una determinata porta UDP delle richieste che i Client, **all'atto dell'accensione**, eseguiranno lanciando in rete un broadcast. Il server DHCP intercetta il broadcast e inizia le procedure di assegnazione **dell'indirizzo** estraendolo dal suo database interno.





## Il protocollo DHCP

- DHCP utilizza un processo in **quattro fasi** per configurare un client DHCP
- L'intero processo di comunicazione DHCP avviene tramite le porte UDP 67 (server) e 68 (client)

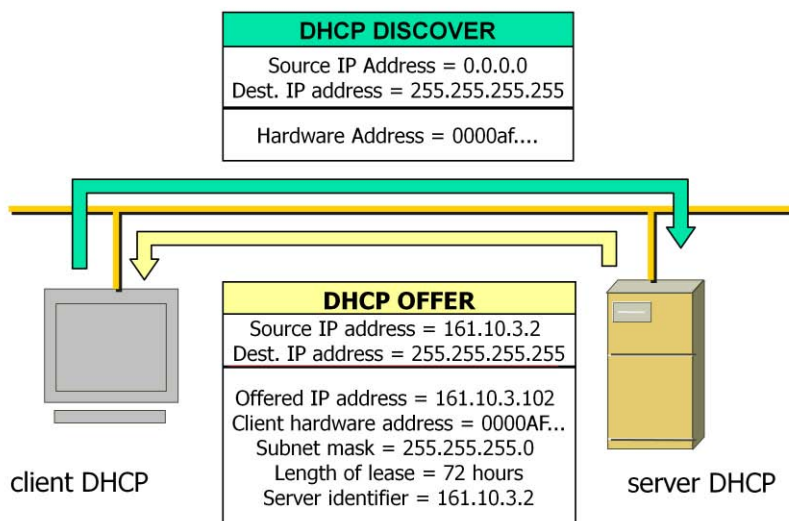


[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-50



## DHCP: Discover e Offer



www.ncp-italy.com

La suite TCP/IP 5-51

Quando un client viene inizializzato per la prima volta, richiede il lease di un indirizzo IP trasmettendo una richiesta tramite broadcast a tutti i server DHCP.

Non avendo un indirizzo IP e non conoscendo **l'indirizzo** IP di un server DHCP, il client utilizza 0.0.0.0 come indirizzo IP di origine e 255.255.255.255 come indirizzo IP di destinazione.

La richiesta di lease viene inviata in un messaggio DHCPDISCOVER, che contiene anche **l'indirizzo** MAC e il nome del client.

Tutti i server DHCP che ricevono la richiesta e dispongono di una configurazione valida per il client inviano tramite broadcast **un'offerta** che include le seguenti informazioni:

- **l'indirizzo** MAC del client, **un'offerta** di indirizzo IP, la subnet mask, durata del lease
- viene inviato inoltre un identificatore del server (indirizzo IP del server che ha inviato **l'offerta**)

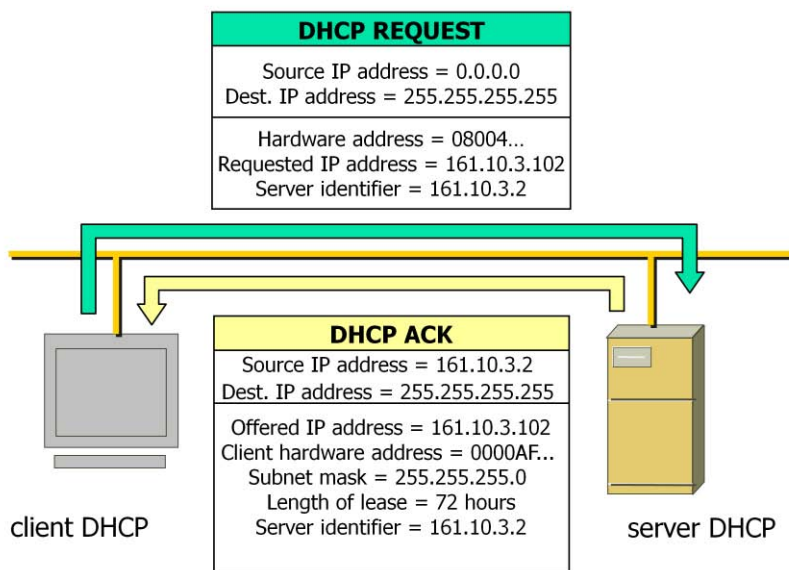
La trasmissione avviene tramite broadcast perchè il client non ha ancora un indirizzo IP. **L'offerta** viene inviata come messaggio DHCP OFFER.

Il client DHCP seleziona **l'indirizzo** IP dalla prima offerta ricevuta.

Il client DHCP attende **un'offerta** per un secondo. Se non riceve offerte, il client non potrà essere inizializzato e ritrasmetterà la richiesta tramite broadcast per tre volte. Se non riceve alcuna offerta dopo quattro richieste, il client riproverà ogni cinque minuti.



## DHCP: Request e Ack



www.ncp-italy.com

La suite TCP/IP 5-52

Dopo aver ricevuto **un'offerta** da almeno un server DHCP, il client comunica tramite broadcast a tutti i server DHCP che ha eseguito una selezione accettando **l'offerta**.

La selezione del lease viene inviata come messaggio DHCPREQUEST e include **l'indirizzo** IP del server di cui è stata accettata **l'offerta**.

A questo punto, tutti gli altri server DHCP ritirano le rispettive offerte in modo che gli indirizzi IP corrispondenti siano disponibili per la successiva richiesta di lease IP.

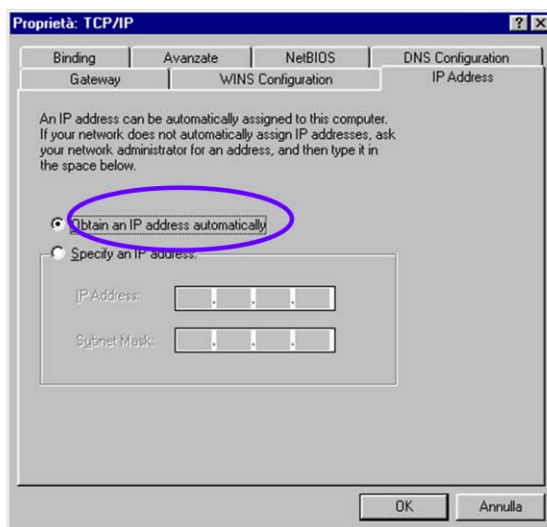
Il server DHCP di cui è stata accettata **l'offerta** invia al client tramite broadcast un riconoscimento di operazione riuscita sotto forma di messaggio DHCPACK.

Se il client cerca di ottenere il lease **dell'indirizzo** IP precedente e questo non è più disponibile, viene inviato tramite broadcast un riconoscimento di operazione non riuscita mediante il messaggio DHCPNACK.

Un messaggio DHCPNACK viene inviato anche se **l'indirizzo** IP richiesto non è più valido perchè il client è stato spostato in una diversa sottorete.



## Configurazione client DHCP



**Router(config-if)# ip address dhcp**

[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-53

- Quando un client DHCP effettua il reboot, se ha un indirizzo IP già precedentemente assegnatogli, invia un messaggio DHCPREQUEST tramite broadcast per verificare che il suo indirizzo IP sia ancora valido
- Se il client viene spostato in una subnet differente (durante il periodo in cui è spento), il server DHCP locale ricevendo un richiesta di rinnovo per un indirizzo IP non assegnato da lui, risponderà con un messaggio DHCPNACK. Il client inizierà quindi il processo di leasing in modo da ottenere un indirizzo IP valido sulla nuova subnet
- I client DHCP non rilasciano l'**indirizzo** IP quando vengono spenti
- **E'** possibile forzare un client a rilasciare il proprio indirizzo IP (il client invia un messaggio **DHCPRELEASE** al server DHCP per rinunciare al lease)
- Ciò risulta utile quando il client deve essere rimosso dalla rete oppure spostato in **un'altra** subnet



# Configurazione Server DHCP

**Attivazione del Server DHCP  
(abilitato di default)**

**Database remoto contenente  
associazioni statiche IP<->MAC  
(opzionale)**

**Indirizzi esclusi dall'assegnazione  
dinamica del DHCP**

```
service dhcp
!
ip dhcp database ftp://user:password@172.16.4.253/router-dhcp
ip dhcp excluded-address 172.16.1.1
!
ip dhcp pool 1
network 172.16.0.0 /16
domain-name cisco.com
dns-server 172.16.1.102 172.16.2.102
default-router 172.16.1.1
!
ip dhcp pool Mars
host 172.16.2.254
hardware-address 02c7.f800.0422 ieee802
client-name Mars
!
interface ethernet 0/0
ip address 172.16.1.1 255.255.255.0
```

**Intervallo di indirizzi e maschera**

**associazioni statiche IP<->MAC  
definite localmente  
(opzionale)**

[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-54



## DHCP in presenza di router

- Il caso in cui client e server sono nella stessa subnet è quello più semplice per le operazioni del protocollo DHCP
- DHCP diventa più complesso in presenza di router. Il problema nasce dal fatto che molti messaggi DHCP sono trasmessi in broadcast ed i router non inoltrano i broadcast
- Sarebbe necessario un server DHCP per ogni subnet
- Per evitare ciò, è stata adottata una soluzione (RFC 1542) che implica la possibilità per un router di inoltrare i messaggi DHCP broadcast

[www.ncp-italy.com](http://www.ncp-italy.com)

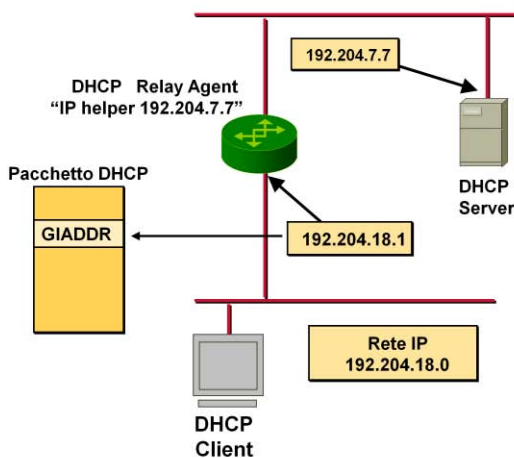
La suite TCP/IP 5-55

- Se non è presente un server DHCP in ogni subnet, i router della rete devono essere configurati per lasciar passare i messaggi DHCP broadcast
- Un router può essere configurato come **DHCP Relay Agent**
  - i messaggi DHCP utilizzano le porte UDP 67 e 68, quindi il router lascerà passare i messaggi inviati come broadcast IP su queste porte
- Un **DHCP Relay Agent** deve essere configurato con l'**indirizzo** IP del server DHCP al quale inviare i messaggi DHCP (broadcast) provenienti dal client



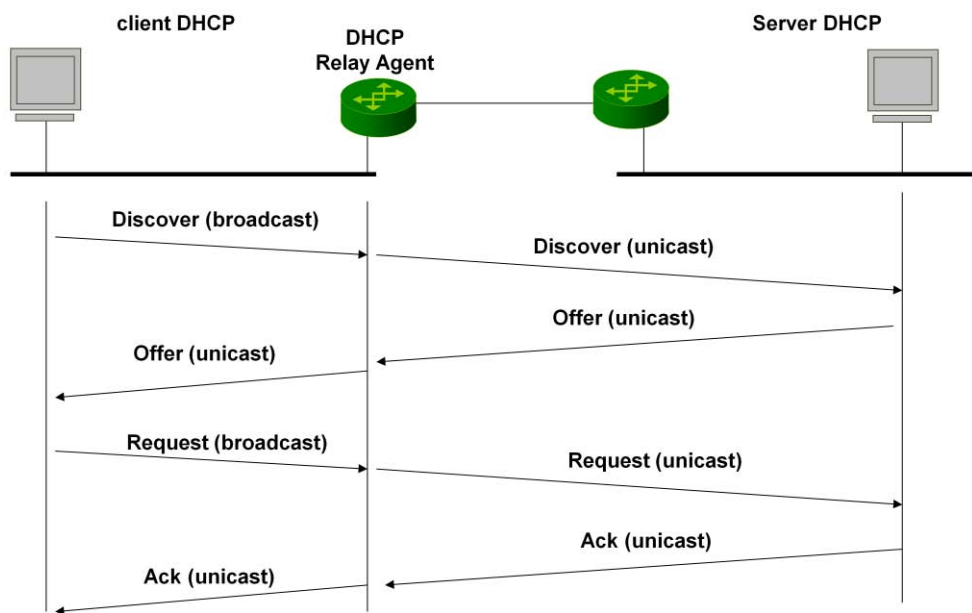
## DHCP Relay Agent: esempio

- Il client DHCP invia in broadcast un pacchetto DHCP di Discover
- Il router configurato come Relay Agent invia (in unicast) il pacchetto al DHCP server
- Il Relay Agent inserisce nel campo **GIADDR** l'indirizzo IP dell'interfaccia del router dalla quale ha ricevuto il pacchetto
- Il Relay agent può essere configurato con indirizzi di più server DHCP
- Il server DHCP utilizza il campo GIADDR del pacchetto di Discover per determinare il pool di indirizzi dal quale prelevare l'indirizzo da assegnare al client.





# DHCP Relay Agent



[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-57





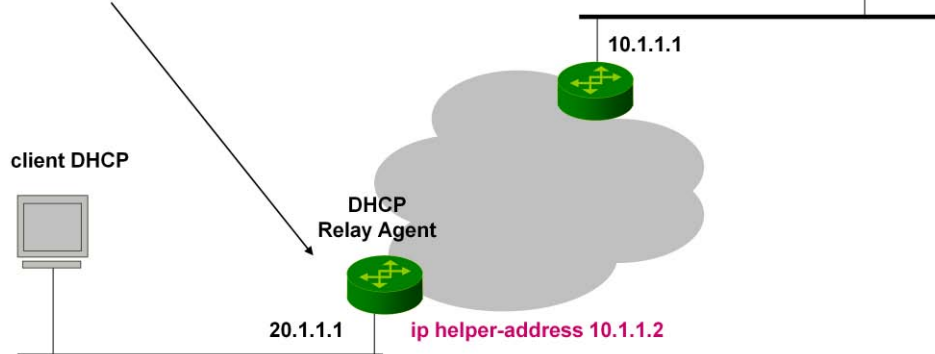
## Router Cisco come DHCP Relay Agent

```
interface ethernet 0
```

```
ip address 20.1.1.1 255.255.255.0
```

```
ip helper-address 10.1.1.2
```

```
ip forward-protocol udp 69
```



www.ncp-italy.com

La suite TCP/IP 5-58

Per utilizzare un router Cisco come DHCP relay agent, deve essere configurato il comando `ip helper-address` **sull'interfaccia** del router appartenente alla stessa subnet del client DHCP

L'indirizzo usato nel comando `ip helper-address` può essere l'indirizzo specifico di un server DHCP oppure l'indirizzo di una subnet, nel caso in cui siano presenti più server DHCP nello stesso segmento di rete



# Indirizzi IP privati

## **IANA-Allocated, Non-Internet Routable, IP Address Schemes**

<b>Class</b>	<b>Network Address Range</b>
A	10.0.0.0-10.255.255.255
B	172.16.0.0-172.31.255.255
C	192.168.0.0-192.168.255.255

[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-59

Lo IANA ha definito una serie di indirizzi, descritti nel RFC 1918, il cui utilizzo è raccomandato nelle reti private. Per rete privata si intende qui una rete connessa ad Internet in modo tale da poter individuare esattamente un confine che separi gli utenti di Internet da quelli interni appartenenti alla rete privata. Se gli utenti interni non debbono avere visibilità esterna, sono dei fruitori di Internet e non viceversa, allora è possibile assegnare ad essi degli indirizzi a piacere purché scelti **nell'ambito** del RFC 1918.



## NAT: benefici

- Accedere ad Internet senza richiedere indirizzi IP pubblici multipli
- Interconnettere reti IP con spazi di indirizzamento sovrapposti
- Migliorare la sicurezza della rete mascherando gli indirizzi reali degli host
- Mantenere il proprio schema di indirizzamento anche nel caso di un cambiamento di ISP



## NAT: caratteristiche

- Descritto in RFC 1631
- Modifica gli indirizzi IP nell'header IP (e, se serve, nel campo applicativo)
- La traduzione può essere:
  - Statica
    - mappatura statica uno-a-uno tra indirizzi interni ed esterni
  - Dinamica
    - la corrispondenza tra indirizzo interno ed indirizzo esterno è stabilita all'occorrenza e rilasciata in seguito

[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-61

Oltre a modificare l'indirizzo IP nell'intestazione del pacchetto devono essere effettuate anche altre operazioni:

- ricalcolo della checksum IP
- ricalcolo della checksum TCP
- modifica del campo dati se questo contiene riferimenti all'indirizzo IP da tradurre. Quest'ultima affermazione implica che le applicazioni utilizzate devono essere compatibili con il NAT. Per esempio l'FTP utilizza l'indirizzo sorgente nei suoi messaggi, il che costringe ad analizzare anche il livello applicativo. Nello specifico, il comando PORT di FTP contiene un riferimento all'indirizzo IP, sebbene in formato ASCII, che deve essere tradotto. Questa operazione può causare una modifica della lunghezza del pacchetto IP. Se la nuova dimensione del pacchetto è inferiore a quella originale, nel pacchetto vengono inseriti dei bit di riempimento per ricondurre la dimensione del pacchetto a quella originaria. Se il pacchetto diventa più grande di quello originale, il numero di sequenza (TCP) può essere modificato, una tabella speciale viene utilizzata per garantire la corretta traduzione dei numeri di ACK e SEQ.



## NAT: tipi di traduzione

- Network Address Translation (NAT)
  - Traduce solo gli indirizzi IP
  - Traduzione uno-a-uno, statica o dinamica
  - Funzione in ambedue i versi (interno, esterno)
  
- Port Address Translation (PAT)
  - Traduce le coppie Indirizzo/Porta
  - Traduzione uno-a-N
  - Riduce il consumo di indirizzi IP registrati
  - Funziona in un solo verso (interno->esterno)

[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-62

Gli applicativi supportati dal NAT sono:

- HTTP, TFTP, Telnet, NFS
- ICMP\*, FTP\*, DNS\*

Gli applicativi non supportati:

- DHCP
- SNMP
- DNS zone transfers
- IP multicast
- Routing table updates

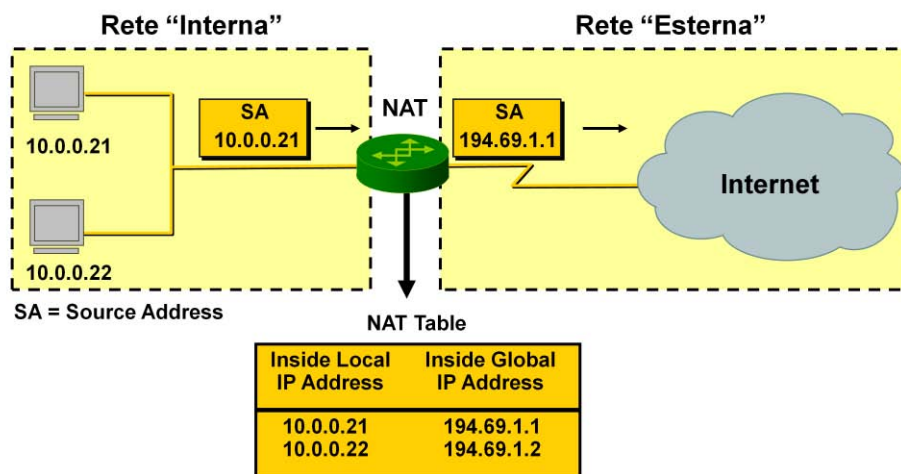
\* non supportato da tutte le implementazioni

Se i dati presenti nel pacchetto IP sono cifrati non è possibile per il NAT effettuare le operazioni di traduzione **all'interno** del pacchetto.

In particolare, le checksum IP e TCP devono essere accessibili, e quindi le corrispondenti intestazioni non possono essere cifrate.



## NAT: esempio



www.ncp-italy.com

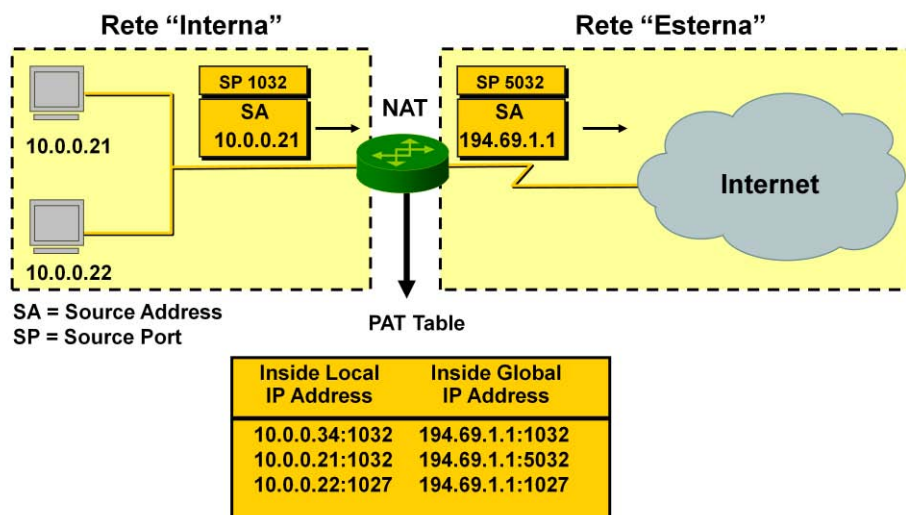
La suite TCP/IP 5-63

Il numero massimo di sessioni concorrenti dipende dalla quantità di memoria disponibile **sull'apparato**.

E' possibile utilizzare contemporaneamente sia traduzioni statiche che dinamiche, facendo attenzione che gli indirizzi statici siano esclusi dai pool di indirizzi dinamici. E' anche possibile fare in modo che soltanto una parte degli indirizzi della rete siano tradotti attraverso il NAT configurando delle opportune liste di accesso.



## PAT: esempio



[www.ncp-italy.com](http://www.ncp-italy.com)

La suite TCP/IP 5-64

L'utilizzo del PAT permette di utilizzare un unico indirizzo pubblico moltiplicando le sessioni concorrenti sulla base delle porte sorgenti TCP. In questo modo si possono mappare su un unico indirizzo pubblico fino a 65535 indirizzi (molte implementazioni allocano soltanto le porte non privilegiate da 1024 a 65535) in quanto il campo port è di 16 bit,



## NAT: considerazioni

- Oltre a modificare l'indirizzo IP nell'intestazione del pacchetto devono essere effettuate anche altre operazioni:
  - ricalcolo della checksum IP
  - ricalcolo della checksum TCP
  - modifica del campo dati se questo contiene riferimenti all'indirizzo IP da tradurre
  - In alcuni casi il NAT deve spiongersi nella traduzione fino al livello applicativo, si parla di ALG (Application Level Gateway).
    - Oltre ad applicazioni tradizionali come FTP, ci sono da considerare tutti i nuovi protocolli di comunicazione vocale (VoIP).





## Bibliografia e Link utili

- <http://www.ietf.org>
- <http://www.polito.it>
- <http://www.networkingitalia.it>
- <http://www.ciscopress.com>
- <http://www.protocols.com/>
- <http://www.netacad.it/new/default.asp>

*TANENBAUM, A. S. Computer Networks. Fourth Edition. Prentice Hall, 2002.*

*KUROSE, J. F. et al. Computer Networking: A Top-Down Approach Featuring the Internet. Second Edition, Pearson Addison Wesley, 2002.*

*COMER, D. Internetworking with TCP/IP: Principles, Protocols and Architecture. Fourth Edition, Prentice Hall, 2000.*

*STEVENS, W. R. The Protocols: TCP/IP Illustrated, Volume 1. First Edition, Addison-Wesley, 1994.*

*KESHAV, S. An Engineering Approach to Computer Networking. First Edition, Addison-Wesley, 1997.*

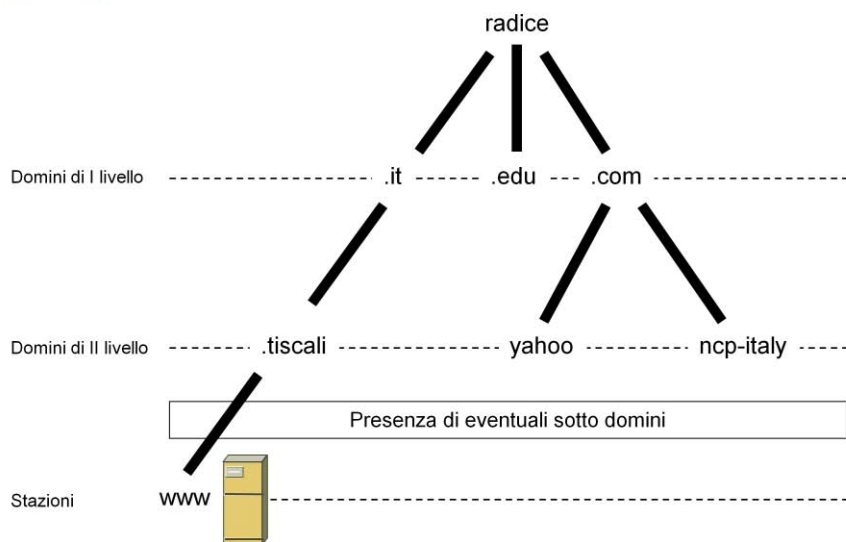
*STEINMETZ, R. et al. Multimedia: Computing, Communications and Applications. First Edition, Prentice Hall, 1995*

## **CAPITOLO 6**

### **DNS e Applicazioni**



## Nomi logici e DNS (1)



[www.ncp-italy.com](http://www.ncp-italy.com)

DNS e Applicazioni 6-2

Attraverso l'utilizzo del DNS è possibile associare ad ogni stazione di Internet un proprio nome, composto da stringhe di caratteri alfanumerici di lunghezza variabile. L'utilizzo di nomi simbolici è molto più semplice e intuitivo da maneggiare rispetto a inespressive sequenze di numeri. Ad esempio, all'indirizzo IP 195.130.225.72 corrisponde il nome logico **www.tiscali.it** che oltre ad essere più intelligibile fornisce anche delle informazioni aggiuntive di facile interpretazione: nel caso del nostro esempio si può facilmente capire che si tratta di un server web (www), del provider Tiscali (.tiscali), della nazione Italia (.it).

Come si può notare, i nomi si presentano come sequenze di caratteri separati da un punto. Essi sono inoltre strutturati secondo una linea gerarchica che suddivide l'intera rete in domini e sottodomini, formando un albero logico le cui terminazioni rappresentano le singole stazioni. Leggendo i nomi da sinistra a destra si risale la gerarchia partendo dalle stazioni. Nel caso del nostro esempio, è scritto prima il nome del server web, poi quello del provider e infine la nazione. Leggendola da destra verso sinistra invece si discende a partire dal livello più alto fino ad arrivare alle singole stazioni. Seguendo quest'ultimo percorso, si incontrano i domini di livello più alto (top level domain). In genere, il livello più alto identifica il paese o, per gli Stati Uniti, la tipologia del dominio: .EDU: università ed enti di ricerca, .COM: organizzazioni commerciali, .GOV: enti governativi, .MIL: enti militari, .NET: organizzazioni commerciali o di supporto e gestione della rete, .ORG: enti e organizzazioni non commerciali, .INT: organizzazioni internazionali, codice paese di due caratteri per indicare una nazione. Queste sei tipologie di domini sono state create quando Internet era diffusa, salvo rare eccezioni, solo negli Stati Uniti. Per questa ragione la rete venne suddivisa in domini, le cui sigle caratterizzavano direttamente il tipo di ente o organizzazione.

Continuando la lettura dei nomi da destra a sinistra, si scende verso i cosiddetti "domini di secondo livello", che invece rappresentano organizzazioni, aziende e singoli individui senza nessuna particolare restrizione. Anche se ogni nazione tende a introdurre delle proprie regolamentazioni è in genere possibile a chiunque lo voglia di registrare un proprio dominio di secondo livello. Grazie alla natura gerarchica del DNS è possibile creare dei sottodomini subordinati ad uno specifico dominio creando così un partizionamento gerarchicamente ordinato. Questo è molto utile per gestire organizzazioni di grandi dimensioni. Il numero dei sottodomini può variare in base alle esigenze specifiche senza particolari limitazioni. Per creare un nuovo dominio di secondo livello è necessaria l'autorizzazione dell'ente predisposto, mentre la definizione di eventuali sottodomini aggiuntivi non implica generalmente nessuna autorizzazione ed è a completo carico e discrezione del possessore del dominio di secondo livello, anche se ogni autorità nazionale di gestione del DNS può imporre delle regole particolari.



## DNS

### Top level domains

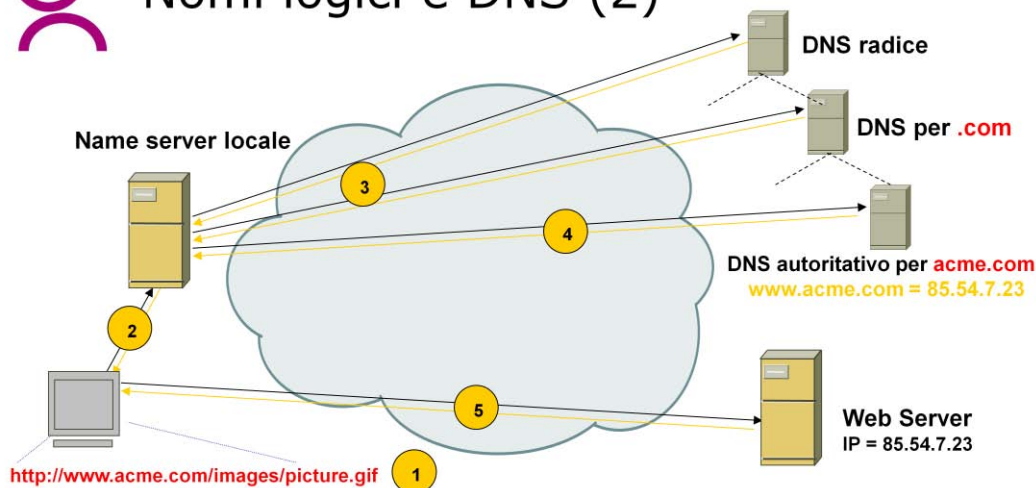
com	Organizzazioni commerciali (hp.com, sun.com ...)
edu	Organizzazioni educative (berkeley.edu, purdue.edu ...)
gov	Organizzazioni governative (nasa.gov, nsf.gov ...)
mil	Organizzazioni militari (army.mil, navy.mil ...)
net	Organizzazione di gestione reti (nsf.net ...)
org	Organizzazioni non commerciali (eff.org ...)
int	Organizzazioni internazionali (nato.int ...)
<i>country-code</i>	Codice di due caratteri per indicare una nazione (p.e. it)

Continuando la lettura dei nomi da destra a sinistra, si scende verso i cosiddetti “**domini di secondo livello**”, che invece rappresentano organizzazioni, aziende e singoli individui senza nessuna particolare restrizione. Anche se ogni nazione tende a introdurre delle proprie regolamentazioni è in genere possibile a chiunque lo voglia di registrare un proprio dominio di secondo livello. Grazie alla natura gerarchica del DNS è possibile creare dei sottodomini subordinati ad uno specifico dominio creando così un partizionamento gerarchicamente ordinato. Questo è molto utile per gestire organizzazioni di grandi dimensioni. Il numero dei sottodomini può variare in base alle esigenze specifiche senza particolari limitazioni. Per creare un nuovo dominio di secondo livello è necessaria **l'autorizzazione dell'ente** predisposto, mentre la definizione di eventuali sottodomini aggiuntivi non implica generalmente nessuna autorizzazione ed è a completo carico e discrezione del possessore del dominio di secondo livello, anche se ogni autorità nazionale di gestione del DNS può imporre delle regole particolari.

Internet è divisa in diversi domini di massimo livello (top-level domains). I domini di massimo livello sono di due specie: generici (generic domains) e geografici (country domains).



## Nomi logici e DNS (2)



1. L'utente inserisce la URL nel browser
2. Il resolver invia una richiesta DNS per risolvere `www.acme.com`
3. Il name server locale inizia l'iterazione delle richieste
4. Il name server locale risponde con l'indirizzo IP di `www.acme.com`
5. Il browser compone una richiesta HTTP verso 85.54.7.23 per ottenere "picture.gif"

www.ncp-italy.com

DNS e Applicazioni 6-4

Dal punto di vista tecnico il Domain Name Service è costituito da un sistema di database distribuiti nella rete chiamati name server, che colloquiano tra loro secondo la gerarchia in figura. Ogni azienda o associazione che gestisce un proprio dominio ha un server DNS di riferimento, chiamato authoritative name server, nel quale sono definite le coppie [indirizzo IP -> nome logico] di ogni singola macchina che si vuol rendere pubblica. Il name server ha la funzione di rispondere a delle interrogazioni che richiedono la risoluzione di un nome logico nell'indirizzo IP ad esso associato. Ogni Client è infatti dotato di uno specifico programma, denominato Resolver, che a fronte di una richiesta di connessione verso una risorsa della rete, invia una interrogazione al proprio Name Server di riferimento locale (authoritative name server) per avere in risposta l'indirizzo IP associato al nome simbolico della risorsa desiderata.

Se il name server locale non possiede l'informazione richiesta inizia un processo iterativo di richieste fino ad arrivare eventualmente all'autoritative name server del dominio al quale appartiene il nome che si sta tentando di risolvere. Nel fare questo lavoro di interrogazione ogni name server si annota gli indirizzi che ha conosciuto, in modo che le future richieste possano essere risolte immediatamente.

Grazie a questo meccanismo il DNS è sempre aggiornato: infatti la responsabilità di aggiornare i singoli name server è decentralizzata ai vari domini di secondo livello e non richiede una autorità centrale che tenga traccia di tutti i milioni di computer collegati a Internet.

Il cuore del DNS è formato da 13 speciali computer chiamati Root server. Essi sono gestiti da uno speciale ente denominato ICANN (The Internet Corporation for Assigned Names and Numbers) e sono distribuiti su tutto il mondo. Ognuno dei 13 Root Server contiene le stesse vitali informazioni per bilanciare il carico e fungere da back-up uno dell'altro.

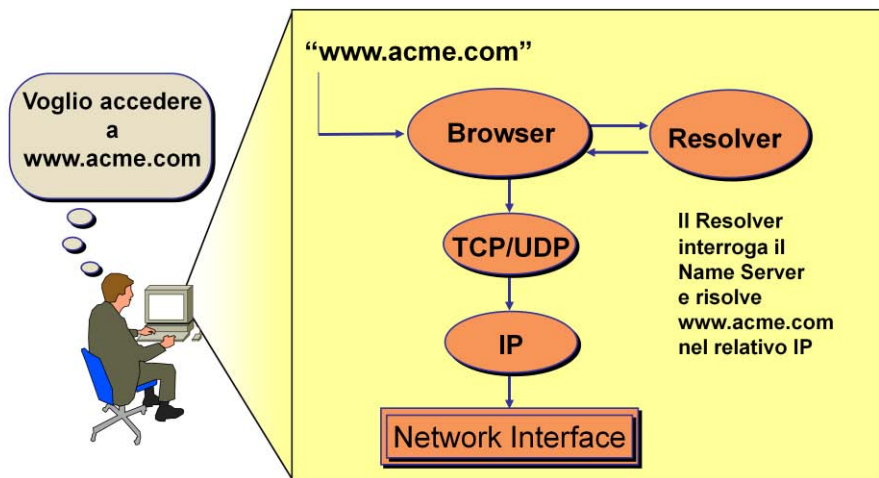
La loro importanza risiede nel fatto che contengono gli indirizzi IP di tutti i registri dei domini di livello più alto – sia i registri globali come .com, .org, etc. sia i 244 codici nazione come .fr (Francia), .cn (Cina), etc. Questa è chiaramente un'informazione critica che deve essere opportunamente gestita e salvaguardata. SE l'informazione non dovesse risultare precisa o incompleta alcune risorse della rete potrebbero non essere raggiungibili. In gergo DNS si dice che "l'informazione deve essere unica e autentica".

A seguire in ordine di importanza ci sono poi i Server che gestiscono i domini di primo livello (top level domain) i quali a loro volta devono mantenere l'informazione dei domini di secondo livello a loro subordinati. Il dominio .it per l'Italia è attualmente gestito dal GARR.

ICANN ha recentemente dato l'approvazione per definire un nuovo dominio di primo livello per l'Unione Europea (.EU). Si aspetta il suo lancio definitivo agli inizi del 2003.



## Il Resolver



www.ncp-italy.com

DNS e Applicazioni 6-5

Per associare i nomi agli indirizzi IP, un'applicazione utilizza un programma client, denominato **resolver**. Il **resolver** invia un pacchetto UDP, contenente il nome da risolvere, ad un DNS server locale, quest'ultimo determina l'indirizzo IP corrispondente e lo comunica al **resolver** che a sua volta lo fornisce all'applicazione da cui ha ricevuto la richiesta.

Almeno in teoria, un unico **name server** potrebbe contenere l'intero DNS database e rispondere a tutte le interrogazioni che lo riguardano. In realtà, questo server sarebbe così sovraccarico da essere inutilizzabile. Inoltre, se per qualsiasi motivo questo andasse down, l'intera Internet si fermerebbe.

Per evitare tali inconvenienti, lo spazio dei nomi DNS è suddiviso in zone non sovrapposte, costituite da una parte dell'albero dello spazio di dominio. Ogni zona contiene un **name server** responsabile della gestione della zona stessa.

Un **name server** viene classificato come primario o secondario. Come indicano queste definizioni, le funzioni del server primario sono duplicate in altre macchine, denominate appunto **name server** secondari.



## Tabelle DNS

```
;*****
;* Start of Authority Records *
;*****

@ IN SOA gw-mycompany.mycompany.net. admin.gw-mycompany.mycompany.net. (
1997112801 ; Serial number for this data (yyymmdd##)
86400 ; Refresh value for secondary name servers (8 ore )
7200 ; Retry value for secondary name servers (2 ore )
604800 ; Expire value for secondary name servers (1 settimana )
86400) ; Minimum TTL value (8 ore )

;NAME SERVER
mycompany.net. IN NS dns1.mycompany.net.
mycompany.net. IN NS dns2.mycompany.net.
;
;POSTA ELETTRONICA
mycompany.net. IN MX 50 mail.mycompany.net.
;
;SERVER
as5200-RM IN A 194.128.74.3
mail.mycompany.net. IN A 194.128.74.30
tacacs.mycompany.net. IN A 194.128.74.9
bind.mycompany.net. IN A 194.128.74.31
proxy.mycompany.net. IN A 194.128.74.5
;
; STAZIONI
zeus IN A 194.128.74.11
leonardo IN A 194.128.74.12
minos IN A 194.128.74.13
ares IN A 194.128.74.14
```



## Comandi DNS nel mio PC

Azzeramento cache DNS

```
C:\Users\DIRAMA>ipconfig /flushdns
```

Disabilitare e abilitare il servizio di Cache DNS

```
net stop dnscache
```

```
net start dnscache
```

Microsoft Windows [Versione 10.0.14393]

(c) 2016 Microsoft Corporation. Tutti i diritti sono riservati.

```
C:\Users\DIRAMA>nslookup
```

```
Server predefinito: dsldevice.lan
```

```
Address: 192.168.1.254
```

```
> www.google.com
```

```
Server: dsldevice.lan
```

```
Address: 192.168.1.254
```

Risposta da un server non autorevole:

```
Nome: www.google.com
```

```
Addresses: 2a00:1450:4002:802::2004
```

```
216.58.198.36
```





## Comandi DNS nel mio PC

```
> www.inps.it
Server: dsldevice.lan
Address: 192.168.1.254

Risposta da un server non autorevole:
Nome: www.inps.it
Address: 93.63.43.48

> www.ncp-italy.com
Server: dsldevice.lan
Address: 192.168.1.254

Risposta da un server non autorevole:
Nome: www.ncp-italy.com
Address: 195.110.136.138

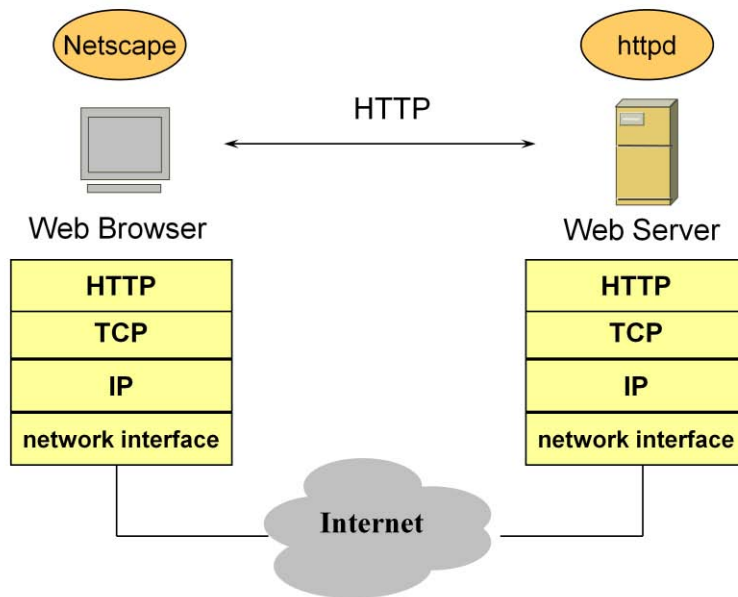
> set q=any
> www.libero.it
Server: dsldevice.lan
Address: 192.168.1.254

Risposta da un server non autorevole:
www.libero.it internet address = 37.9.239.32

libero.it nameserver = n1.libero.it
libero.it nameserver = n2.libero.it
n1.libero.it internet address = 156.154.66.47
n2.libero.it internet address = 156.154.67.47
```



# World Wide Web: il protocollo HTTP



www.ncp-italy.com

DNS e Applicazioni 6-9

Il protocollo Hypertext Transfer Protocol (HTTP) è la base del World Wide Web (WWW). Un Web client, chiamato comunemente browser, comunica con un Web server usando una o più connessioni TCP. La well-known port per indirizzare sul server il servizio è la port 80.

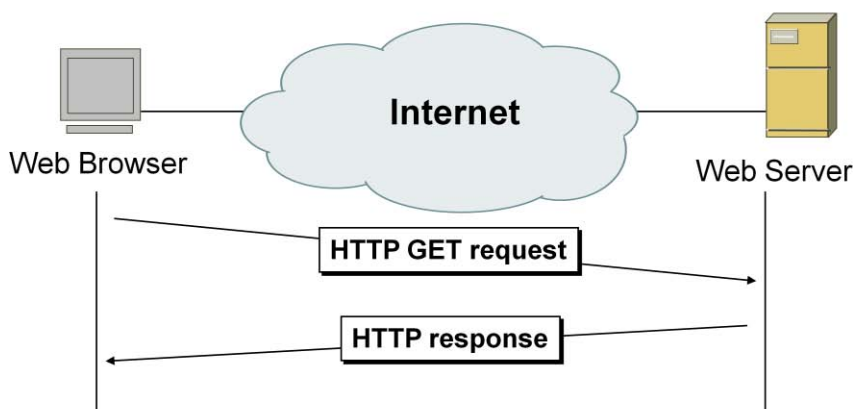
HTTP è il protocollo usato dal client e dal server per comunicare al di sopra delle connessioni TCP. I documenti che il server invia al client sono immagini, file di testo o documenti di tipo HTML (Hypertext Markup Language). HTTP è un protocollo semplice: il client stabilisce una connessione TCP con il server sulla porta 80, fa una richiesta e aspetta il documento di risposta, che in genere contiene puntatori (hypertext link) ad altri file, che possono risiedere anche su altri server. Il server indica la fine del documento chiudendo la connessione.

I file scambiati tra client e server Web sono in formato HTML. I file HTML sono file di testo (stampabili) contenenti speciali sequenze di caratteri (tag). Il client, interpretando i tag, definisce il formato della pagina (es.: dimensione dei caratteri, posizione del testo, ...). Per la visualizzazioni di particolari informazioni (campo Content-type) il client può utilizzare applicazioni esterne (viewer)



# Protocollo HTTP

- Il WWW è basato sul protocollo HTTP (HyperText Transfer Protocol)
- HTTP utilizza principalmente due tipi di messaggio:
  - una richiesta inviata dal client al server (**GET**)
  - la risposta del server



www.ncp-italy.com

DNS e Applicazioni 6-10

Il protocollo HTTP utilizza principalmente due tipi di messaggi, uno di richiesta inoltrato dal client, l'altro di risposta da parte del server.

Il client invia al server un comando GET request seguito dall'URL richiesto. All'interno di questo comando viene inserita anche la versione di HTTP, la 1.0 ad esempio. Il server risponde inizialmente con la status line, in cui comunica al client la versione di HTTP usata e in più lo informa, tramite un codice, sullo stato della sua richiesta, che può essere stata accettata oppure ha dato luogo ad un errore, ad esempio perché il documento individuato da URL non esiste. Se la richiesta è andata a buon fine, in response il server invia al client il documento, che può essere la home page di un sito in formato HTML. Sta al browser client analizzare i tag del documento per poi ricostruire e visualizzare correttamente la pagina.



## HTTP: esempio (1)

- Un utente normalmente scrive l'URL del sito Web al quale vuole collegarsi
  - Ad esempio, <http://www.olimpo.org/docs/zeus.html>
- Il browser traduce tale URL in un messaggio HTTP:
  - **GET** <http://www.olimpo.org/docs/zeus.html> **HTTP/1.0**
- Questo messaggio può essere suddiviso in tre parti:

Protocollo: HTTP Server: www.olimpo.org Request: GET /docs/zeus.html HTTP/1.0
---



## HTTP: esempio (2)

- Il browser effettua le seguenti operazioni:
  - risolve il nome *www.olimpo.org* in indirizzo IP (194.16.2.3)
  - instaura una connessione TCP (port destinazione 80) con 194.16.12.3
  - invia il messaggio HTTP: GET /docs/zeus.html HTTP/1.0
  - riceve la risposta dal server, che gli invia il file HTML
  - processa il file HTML e visualizza la pagina Web



# Il protocollo SNMP e il Network Management

- Il Network Management realizza 5 principali funzioni:
  - Fault management
  - Configuration management
  - Accounting management
  - Performance management
  - Security management
- Permette di ridurre:
  - I costi amministrativi interni
  - I tempi di inattività della rete
  - I costi apparati



Il network management permette il monitoraggio continuo dei componenti della rete, riducendo eventuali tempi di inattività, diminuendo i costi della mancata produzione e incrementando la sicurezza e stabilità della rete stessa.

E' possibile ricavare informazioni circa le caratteristiche del traffico di rete ed è così possibile pianificare strategie per interventi mirati al miglioramento delle performance come l'aggiunta di filtri, la riallocazione di server o implementazioni di VLAN.

La sicurezza nel management indica la possibilità di controllare gli accessi sui devices interconnessi, su servers e altre piattaforme. Inoltre permette di effettuare procedure automatiche per il frequente cambio delle password.

Il network management fornisce strumenti per:

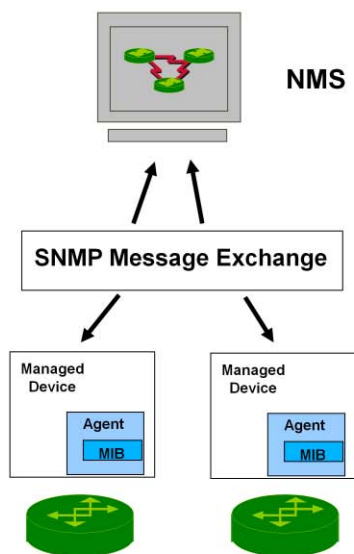
- semplificare i cambiamenti e monitorare le connessioni nella rete
- tracciare i cambiamenti e mantenere aggiornate le informazioni
- Implementare cambiamenti globali velocemente e trasferire informazioni.

I componenti principali del Network Management sono:

- Management Information Base (MIB)
- Simple Network Management Protocol (SNMP)



## Come lavora SNMP



- Utilizza il protocollo SNMP – *Simple Network Management protocol*
- Centralizza l'organizzazione, l'intervento e la risoluzione di problematiche della rete
- Crea un modello della rete

- NMS - *Network Management Service*
- SNMP
- Agents
- MIBs

[www.ncp-italy.com](http://www.ncp-italy.com)

DNS e Applicazioni 6-14

NMS: effettua il polling degli Agent sulla rete. Correla e visualizza le informazioni. Uno o più NMS devono essere presenti in una rete.

SNMP: è il protocollo utilizzato per lo scambio dei messaggi. **E'** posizionato nella pila ISO/OSI sopra UDP. Usa gli Agenti per trasferire le informazioni delle MIB tra NMS e apparati.

Managed Device: è un nodo di rete che contiene un SNMP Agent. Sono rappresentati dai comuni componenti di rete (Hub, Router, Host, Stampanti etc.)

Agent: è un modulo software per la gestione di rete che risiede in un Managed Device. Conosce le informazioni locali e le traduce in una forma compatibile con SNMP.

Il MIB è un insieme di variabili utilizzate per determinare lo stato **dell'** apparato. Ogni MIB è identificato tramite un '**object identifier**' univoco che è **un'** annotazione di numeri e punti basata su di una struttura ad albero (SMI tree). Le MIB sono depositarie delle informazioni di un apparato; esistono diversi standard di MIB ai quali vengono aggiunte MIB proprietarie per la gestione di profili legati al Produttore.



## Comandi Basi SNMP

SNMP utilizza UDP, porte 161 e 162 (traps)



Il monitoraggio e controllo di un apparato avviene tramite i comandi:

- Read (get): per richiedere informazioni al dispositivo
- Write (set): per modificare le informazioni contenute nel dispositivo
- Trap: sono usati per evitare di fare polling continuo e sono configurabili



# **CAPITOLO 7**

## **Sicurezza delle reti**

### **Sommario**

- I termini della sicurezza
- Tipologie di attacchi
- Autenticazione, Autorizzazione e Accounting
- Sicurezza perimetrale
- Sicurezza dei dati in transito



## I termini della Sicurezza

- **Autenticazione:** è una funzione che fornisce il controllo e la garanzia dell'identità di chi trasmette e di chi riceve i dati
- **Riservatezza:** impedisce la lettura non autorizzata dei messaggi
- **Integrità:** permette di controllare che i dati non subiscano modifiche
- **non Ripudio:** impedisce che le parti neghino di aver trasmesso o ricevuto messaggi, se lo hanno veramente fatto
- **Disponibilità:** garantisce l'accesso e la continuità nel tempo del servizio a tutti gli utenti autorizzati.

Internet rappresenta oggi un mezzo strategico indispensabile a qualsiasi azienda. La capillarità raggiunta e la diffusione della larga banda ne fanno una struttura in grado di supportare nuovi servizi come il collegamento e lo scambio dei dati tra reti private distribuite geograficamente. L'interesse per la possibilità di collegare reti remote, si scontra, però, con la necessità di salvaguardare opportunamente i dati che escono dai protetti confini aziendali.

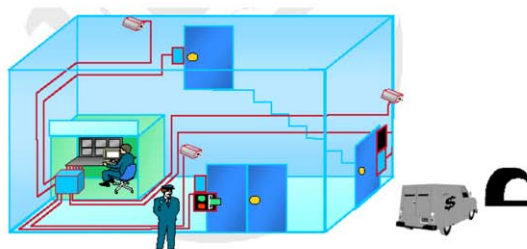
Queste nuove esigenze di sicurezza hanno portato gli addetti ai lavori alla ideazione di un sistema di comunicazione in grado di offrire tutta una serie di servizi specifici per coprire le funzioni di Autenticazione, Riservatezza, Integrità, non Ripudio e Disponibilità.

L'Autenticazione è una funzione che fornisce il controllo e la garanzia dell'identità di chi trasmette e di chi riceve i dati; la Riservatezza impedisce la lettura non autorizzata dei messaggi; l'Integrità permette di controllare che i dati non subiscano modifiche; il non Ripudio impedisce che le parti neghino di aver trasmesso o ricevuto messaggi, se lo hanno veramente fatto, infine, la Disponibilità garantisce l'accesso e la continuità nel tempo del servizio a tutti gli utenti autorizzati.



## La rete "sicura"

- Non esiste un sistema I.T. sicuro al 100%
- L'uso di un insieme di regole comportamentali di "buon senso" contribuisce al generale aumento della sicurezza della rete aziendale.
- Tali regole insieme ad una architettura tecnologica appropriata costituiscono il migliore approccio esistente per tutti i problemi riguardanti l'e-security.



www.ncp-italy.com

Sicurezza delle reti 7-3

Un insieme di regole per minimizzare il rischio di contagio da virus informatici è il seguente:

### **DECALOGO COMPORTAMENTALE PER LA SICUREZZA DAI VIRUS INFORMATICI**

Questo breve scritto vuole essere un promemoria delle azioni da tenere per ridurre il rischio di essere attaccati dai virus informatici. Data l'enorme differenza tra i virus e , soprattutto, la velocità di evoluzione di nuovi ceppi, il decalogo che segue è volutamente generico e volto a dare dei principi di "buon senso comportamentale". Si rimanda alle documentazioni pubblicate ad esempio sul sito: [www.symantec.com](http://www.symantec.com) per le istruzioni relative alla rimozione di virus noti.

1. evitare di introdurre nel computer dischetti floppy usati o di dubbia provenienza
2. se avete un antivirus installato fate l'aggiornamento settimanalmente
3. se avete il dubbio che il malfunzionamento del vostro computer sia dovuto ad un virus informatico seguite la seguente procedura:
  - a. scollegare il pc dalla rete dati
  - b. spegnete il computer
  - c. segnalate il malfunzionamento al C.E.D.
4. inserite una password all'avvio della macchina e custoditela in un luogo sicuro; le password devono essere di tipo alfanumerico e di almeno 6 caratteri (es. 123abc456) devono essere personali o conosciute esclusivamente dai colleghi di uno stesso ufficio e dall'amministratore del sistema
5. se il computer emette un messaggio di errore, annotate il messaggio di errore su un pezzo di carta, annotate le azioni che hanno condotto al malfunzionamento o al messaggio di errore e segnalate tempestivamente il guasto al C.E.D.
6. si raccomanda di eseguire sempre copie di sicurezza di documenti importanti; le copie vanno effettuate sempre su dischetti nuovi
7. se siete collegati ad Internet non fate mai il download di files con estensioni :  
.exe, .dll, .eml, .bin, .doc, .xls
8. se siete possessori di un indirizzo di posta elettronica disattivate l'anteprima di visualizzazione dal vostro programma di posta elettronica (Outlook, Eudora, Netscape)
9. non aprite allegati di posta elettronica se non siete certi sul mittente del messaggio e comunque seguite le raccomandazioni di cui al punto 2
10. ricordate che i virus informatici possono causare danni irreparabili alle banche dati

elettroniche si raccomanda quindi di avere comportamenti volti a diminuire il rischio di contagio informatico.



## Approccio sistematico alla Network Security

Le attività relative alla Network Security,  
possono essere distinte in 5 livelli:



- Autenticazione AAA (Authentication, Authorization, Accounting)
- Sicurezza perimetrale (Firewall, Proxy-firewall)
- Connessioni sicure (Virtual Private Network)
- Monitoraggio delle attività di sicurezza (Intrusion Detection Systems)
- Security Management

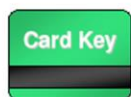
**Ad ogni livello logico corrisponde una appropriata tecnologia**

Il messaggio che dovrebbe , al giorno **d'oggi**, essere un dovere per un amministratore di rete è il seguente: **"Ogni rete informatica deve essere protetta"**.

Il **"sistema"** di protezione varia in genere da rete a rete. **L'analisi** e lo studio sistematico della topologia della rete e del contenuto dei servizi che essa trasporta, è fondamentale per capire quale debba essere la strategia di sicurezza da adottare. La rete protetta può contenere uno o più livelli difensivi integrati tra loro in modo tale da formare una griglia di sbarramento diversa per ogni tipologia di attacco.



## Autenticazione-Autorizzazione-Accounting



- **Autenticazione:**
  - il processo di verifica delle credenziali d'accesso dell'utente remoto
- **Autorizzazione:** concerne la possibilità di:
  - determinare quali servizi di rete ciascun utente sarà abilitato ad utilizzare
- **Accounting:** è la possibilità di tenere traccia dell'uso della rete da parte degli utenti. Ha il duplice obiettivo di:
  - monitorare l'uso della rete
  - addebitarne le relative spese agli utenti (es.:ISP)

### CASE STUDY:

Un'azienda che gestisce servizi di home-banking, desidera fornire ai suoi clienti informazioni on-line relative alla propria situazione finanziaria. Affinchè le operazioni di accesso on-line a queste informazioni da parte dei clienti avvengano in modalità protetta, ovvero le informazioni non siano utilizzabili da utenti non autorizzati, è necessario cifrare le informazioni durante il trasferimento sulle reti pubbliche. Queste modalità vengono solitamente implementate mediante procedure di autenticazione, autorizzazione e accounting (AAA) per l'identificazione dei mittenti e dei destinatari e protocollo IPSEC (in seguito introdotto per le VPN) per la cifratura dei dati. Tale tipo di scenario si può ovviamente generalizzare in tutti i casi in cui è richiesto un accesso autorizzato e sicuro alla propria rete aziendale.



## Sicurezza perimetrale



### Il firewall

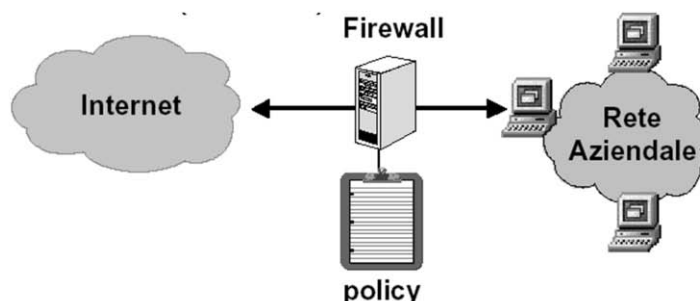
- E' una risposta metodologica ai problemi di Network Security
- L'approccio è:  
invece di (o meglio, oltre a...!!!) difendere  
tutti gli host esposti ad Internet, si  
convoglia il traffico di rete verso un unico  
punto di accesso alla rete aziendale (*choke  
point*, strozzatura)
- Su questo sistema viene implementata la politica di sicurezza  
della rete aziendale

Nella accezione più generale del termine, Il firewall è un meccanismo hardware e/o software che permette d'impostare restrizioni sull'accesso a uno o più computer collegati a Internet, normalmente per motivi di sicurezza.



## Firewall: una definizione

- Se volessimo dare una definizione di firewall, diremmo che:  
è un sistema (o un gruppo di sistemi) che applica una *Security Policy* tra una rete "sicura" (rete interna) e una rete "insicura" (Internet?)



Un firewall può essere un PC, un router, una workstation o una combinazione di questi elementi

[www.ncp-italy.com](http://www.ncp-italy.com)

Sicurezza delle reti 7-7

Un *firewall* è un sistema connesso alla rete con lo scopo di filtrare i pacchetti in transito. Tipicamente viene posto a bordo della rete con lo scopo di creare una barriera difensiva che aumenti il grado di sicurezza perimetrale, ovvero renda più difficile gli attacchi dall'esterno all'interno del sistema.

Un *firewall* può essere realizzato sia come infrastruttura *hardware* dedicata che utilizzando un *computer* e un opportuno insieme di *software*. Deve essere posto sul bordo (logico) della LAN se si desidera far passare per il *firewall* tutti i pacchetti in entrata e in uscita dalla rete locale. Il *firewall* controlla il flusso dei pacchetti, ovvero decide se consentire o negare l'accesso, implementando delle specifiche politiche di filtraggio del traffico.

Utilizzare un *firewall* significa dunque decidere e implementare delle politiche di sicurezza (*security policy*) che definiscono i criteri di protezione, ad esempio decidendo che è ammesso solo il traffico generato da alcuni servizi (la posta o il *Web*) e non traffico derivante da servizi non standard (che potrebbero rendere possibile o nascondere un attacco).

Si possono distinguere diverse tipologie di *firewall* che utilizzano meccanismi di verifica con differenti livelli di sofisticazione. In particolare i *firewall* più semplici filtrano i pacchetti esaminando le informazioni contenute nell'intestazione e, confrontandole con le *security policy*, decidono se autorizzare o no il transito. Offrono invece una protezione più completa i *firewall* che esaminano anche il contenuto dei pacchetti in transito, con lo scopo di assicurarsi che il sistema di destinazione dei messaggi sia realmente in attesa, ad esempio che lo scaricamento di una *mail* sia stato richiesto dal *client*.





## Proxy Firewall

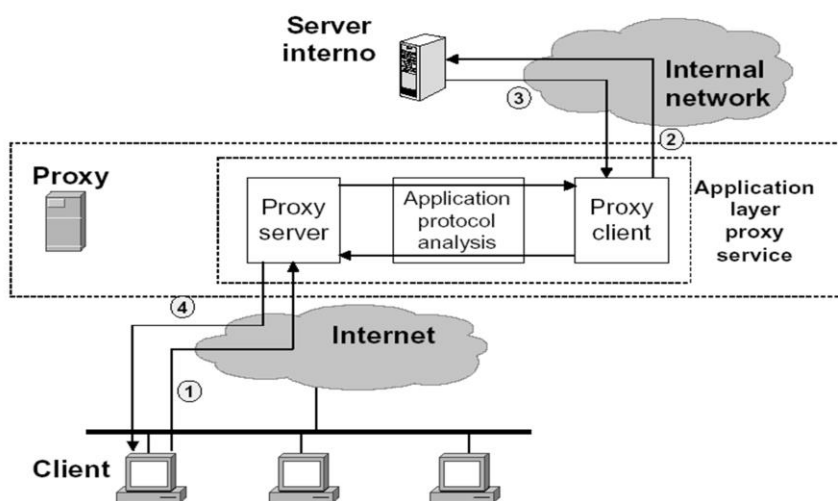
- I firewall che agiscono come **Application level Gateways**, sono spesso chiamati anche Proxy Firewall, per ciascuno dei servizi che devono essere acceduti sulla rete protetta un Proxy si comporta:
  - come un server per il client che vuole accedere ad un servizio residente su una macchina della rete protetta
  - come un client verso l'effettivo server di destinazione
- *In nessun caso il client remoto può connettersi direttamente con il server di destinazione*

Un Proxy è un oggetto che esegue delle azioni al posto di un altro oggetto. Si tratta di applicazioni specializzate che ricevono richieste di servizi Internet da parte degli utenti e le inviano ai server reali. I sistemi Proxy possono essere utilizzati sia per ragioni di sicurezza, sia per ragioni di performance, sia per motivi di necessità.

Il Proxy opera funzioni di filtraggio; non inoltra cioè sempre le richieste all'esterno, soprattutto se la politica di sicurezza dell'organizzazione a cui appartiene prevede l'inibizione di alcuni siti Web o altro.



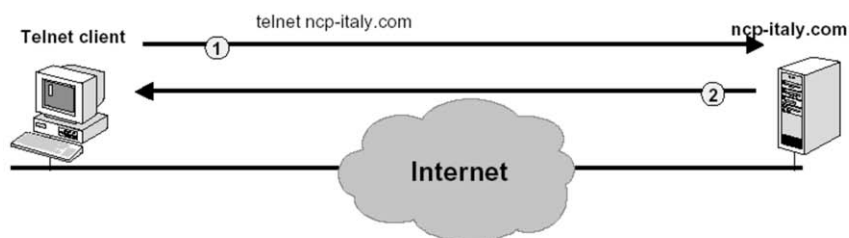
## Proxy Firewall: schema di funzionamento





## Esempio: servizio telnet (1)

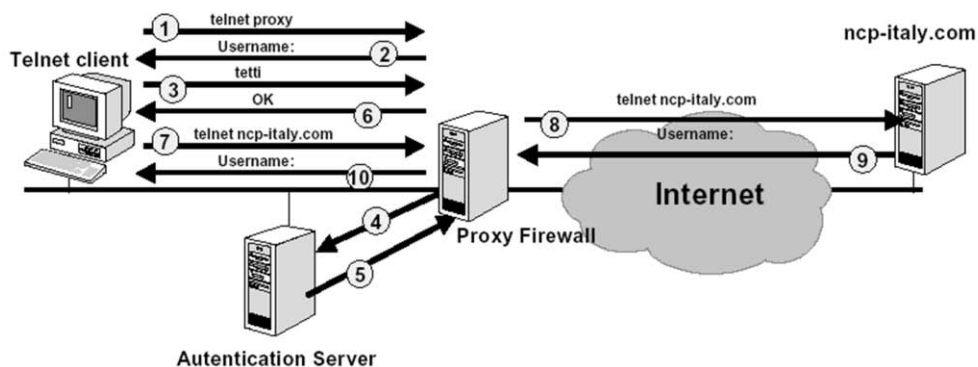
senza Proxy Firewall





## Esempio: servizio telnet (2)

Con Proxy Firewall



[www.ncp-italy.com](http://www.ncp-italy.com)

Sicurezza delle reti 7-11



## Stateful Inspection Firewall

- Questo tipo di firewall cerca di mescolare i vantaggi delle funzionalità di Packet Filtering e di Application Gateway
- L'analisi dell'intestazione del pacchetto che attraversa il firewall viene effettuata in modo centralizzato.
- Se il motore di analisi, in seguito all'ispezione del pacchetto, rileva, in base alla security policy da implementare, la necessità di autenticazione dell'utente, il controllo viene trasferito ad un motore di autenticazione.
- Una volta effettuata l'autenticazione, i successivi pacchetti facenti parte della medesima sessione vengono considerati come "autenticati", senza dover ulteriormente chiamare in causa il SW di autenticazione (approccio *stateful*).

*Il firewall fornisce due vantaggi fondamentali:*

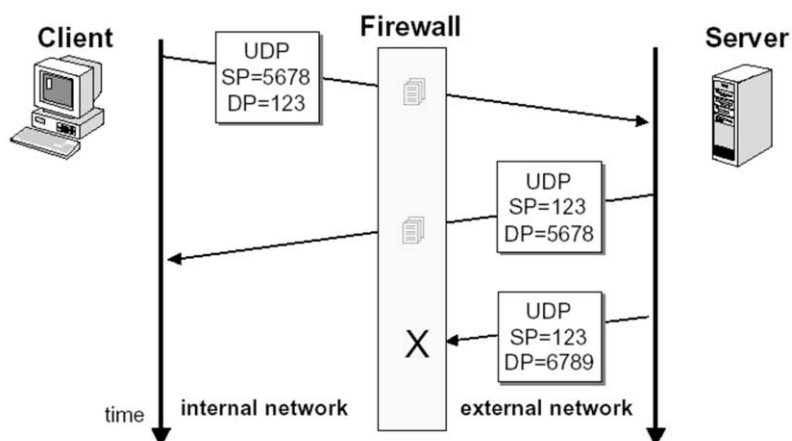
- TRASPARENZA (come packet filter) e
- MEMORIA DI SESSIONE (come proxy)

Questa tecnica di sicurezza usata nei firewall che tiene traccia dello stato di ciascuna connessione, opera sulla base di una serie di regole che governano i parametri da abbinare a ciascuno dei servizi erogati sulla rete. Verifica il traffico entrante e uscente a tutti i livelli, dalla connessione fisica, al protocollo, all'applicazione, e registra i modelli di comportamento dell'utente e usa tale registrazione per autenticare la connessione corrente e quelle future. Un punto debole di tale approccio è che, al rovinarsi della tabella che contiene regole e servizi, la rete può diventare vulnerabile. Il termine : "**stateful inspection**" fu coniato dalla Check Point Software Technologies LTD nel 1993-94; la tecnica fu usata per la prima volta nel prodotto Fire Wall-1.



## Stateful Inspection(2)

- Un firewall con funzionalità di *stateful inspection* ricorda lo 'stato' dei pacchetti che appaiono alle sue interfacce





## Connessioni sicure



- L'interesse per la possibilità di collegare reti remote, sfruttando la rete Internet si scontra, con la necessità di salvaguardare opportunamente i dati che escono dai protetti confini aziendali.

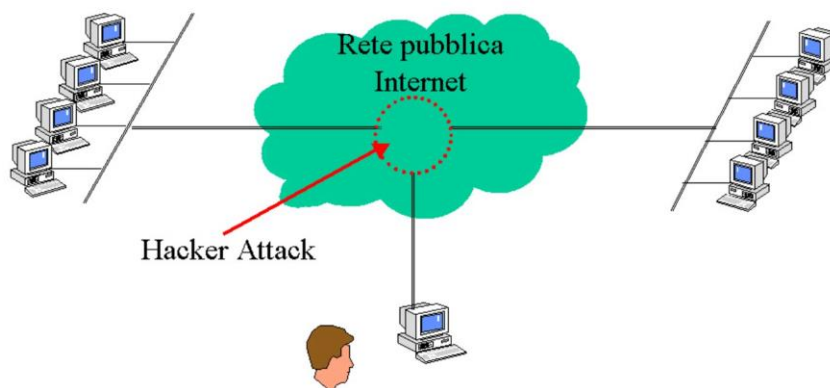
Internet rappresenta oggi un mezzo strategico indispensabile a qualsiasi azienda. La capillarità raggiunta e la diffusione della larga banda ne fanno una struttura in grado di supportare nuovi servizi come il collegamento e lo scambio dei dati tra reti private distribuite geograficamente. **L'interesse** per la possibilità di collegare reti remote, si scontra, però, con la necessità di salvaguardare opportunamente i dati che escono dai protetti confini aziendali.

Queste nuove esigenze di sicurezza hanno portato gli addetti ai lavori alla ideazione di un sistema di comunicazione in grado di offrire tutta una serie di servizi specifici per coprire le funzioni di Autenticazione, Riservatezza, Integrità, non Ripudio e Disponibilità.



## Sicurezza sui dati in transito

### Scenario MITM (Man In The Middle)



[www.ncp-italy.com](http://www.ncp-italy.com)

Sicurezza delle reti 7-15

I tentativi di accesso a dati riservati in transito su una rete possono verificarsi secondo diverse modalità e con impatti su uno o più dei servizi sopradescritti.

I messaggi, ad esempio, possono essere intercettati e i dati contenuti nella comunicazione possono essere modificati violandone così **l'integrità**. Un tipico scenario che si può verificare nel caso di comunicazioni tra reti private è il cosiddetto "**Man In The Middle**" (uomo in mezzo).

Nello scenario MITM si possono verificare attacchi che violano contemporaneamente uno o più servizi. **L'intruso** che si inserisce nella comunicazione può impersonare, ad esempio, gli interlocutori (Autenticazione), può leggere i dati (Riservatezza), modificarli (Integrità), oppure può mettere in atto azioni di disturbo (Disponibilità).





## Crittografia

- Esempio: Cifrario di Cesare  
 $chiave = 3$   
 $messaggio = \text{hello}$   
 $messaggio\ cifrato = (h+3, e+3, l+3, l+3, o+3) = \text{khoor}$
- La chiave utilizzata può essere estesa per rendere più difficile da intercettare la codifica  
 $chiave = 3,5$   
 $messaggio = \text{hello}$   
 $messaggio\ cifrato = (h+3, e+5, l+3, l+5, o+3) = \text{kloqr}$



La crittografia è un procedimento di codifica e decodifica dei messaggi basata su funzioni parametriche, la cui computazione dipende da un parametro detto chiave. Un messaggio crittografato non è direttamente leggibile se non si possiedono una funzione e una chiave per decriptarlo.

I meccanismi, anche molto evoluti, utilizzati nella crittografia classica, sono in realtà poco adatti ai sistemi basati su **computer** e reti. Una prima differenza sostanziale rispetto al passato risiede nella capacità di calcolo: molti meccanismi indecifrabili dall'uomo in tempi ragionevoli sono in realtà interpretabili velocemente da un attuale calcolatore che è in grado di compiere milioni di operazioni elementari al secondo. Occorre quindi progettare sistemi crittografici con algoritmi così complessi che un intruso, entrato in possesso anche di una grande quantità di testo criptato, non riesca a ricostruire il testo in chiaro corrispondente. Un altro problema deriva dal fatto che nella crittografia classica gli alleati nascondevano ai nemici sia il metodo per crittografare sia la chiave. Sulla rete utilizzare un algoritmo privato di crittografia può significare limitare il numero dei potenziali destinatari dei messaggi, per cui tipicamente la segretezza è riposta esclusivamente nella chiave.

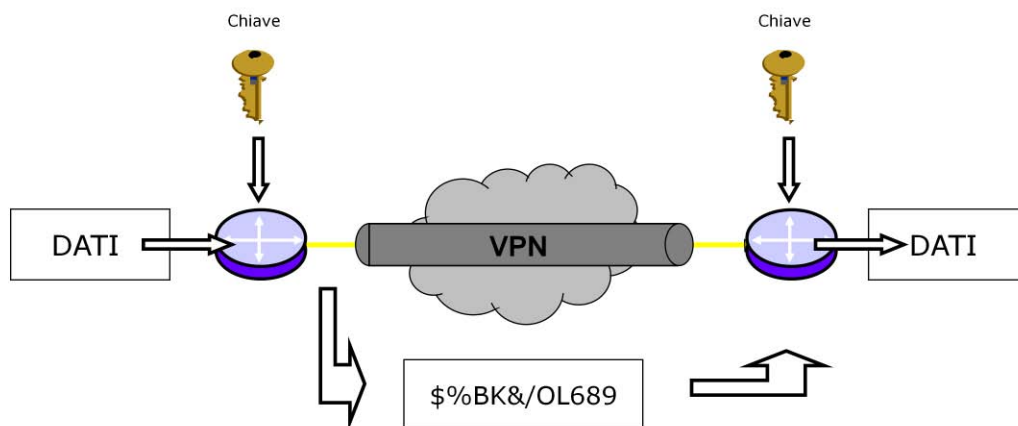
I metodi crittografici possono essere a chiave simmetrica o asimmetrica. **L'utilizzo** di algoritmi di crittografia simmetrica pone, però, il problema della distribuzione delle chiavi. Affinché la cifratura funzioni, i due interlocutori devono in qualche modo scambiarsi la chiave segreta e non possono farlo attraverso il canale di comunicazione che è supposto insicuro.

La soluzione ai problemi della crittografia simmetrica è stata trovata introducendo il concetto di chiave pubblica e chiave privata. In questo genere di algoritmi ogni interlocutore possiede due chiavi, una pubblica da

distribuire a tutti quelli con cui intende comunicare e una privata da tenere segreta. Per comunicare in sicurezza basta cifrare il messaggio con la chiave pubblica del destinatario. In questo modo il messaggio potrà essere decifrato soltanto dal destinatario con la propria chiave privata. Un algoritmo crittografico di questo tipo è detto a chiave asimmetrica. Un esempio molto noto è **l'algoritmo RSA** dalle iniziali di Rivest, Shamir e Adleman che per primi lo proposero. **L'uso** degli algoritmi asimmetrici poiché richiede **l'esecuzione** di molti calcoli matematici complessi viene spesso adottato soltanto nella fase iniziale della comunicazione per concordare una chiave segreta di crittografia simmetrica da utilizzare per il resto della trasmissione. In questo modo **l'uso** del pesante algoritmo della chiave pubblica viene usato per la trasmissione/ricezione di pochi dati (la chiave segreta).



## Cifratura a Chiave Simmetrica



- La chiave di cifratura è identica a quella di decifratura

[www.ncp-italy.com](http://www.ncp-italy.com)

Sicurezza delle reti 7-17

La cifratura a chiave simmetrica è un processo matematico reversibile imposta ad una stringa di dati di modo da alterarla e renderla non comprensibile.

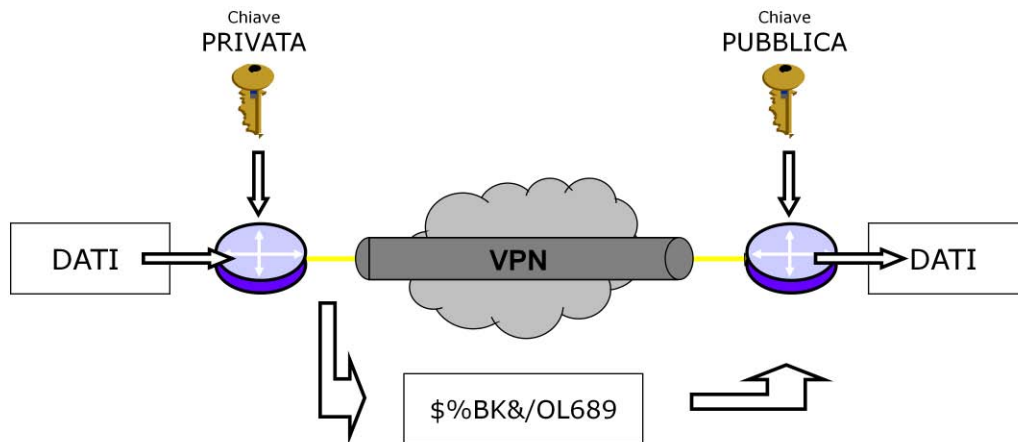
Solo chi possiede la chiave di cifratura sarà in grado di decifrare i dati.

La chiave di cifratura quindi è la stessa che viene utilizzata per decifrare i dati.

Come già affermato in precedenza, i metodi di cifratura a Chiave Simmetrica sono meno sicuri di quelli a Chiave Pubblica e Privata, ma sono notevolmente meno costosi dal punto di vista computazionale, vengono pertanto preferiti per la protezione dei pacchetti utente nello scambio di messaggi.



## Cifratura a Chiave Pubblica e Privata



- I dati cifrati con la chiave privata possono essere decifrati solo con la chiave pubblica e viceversa

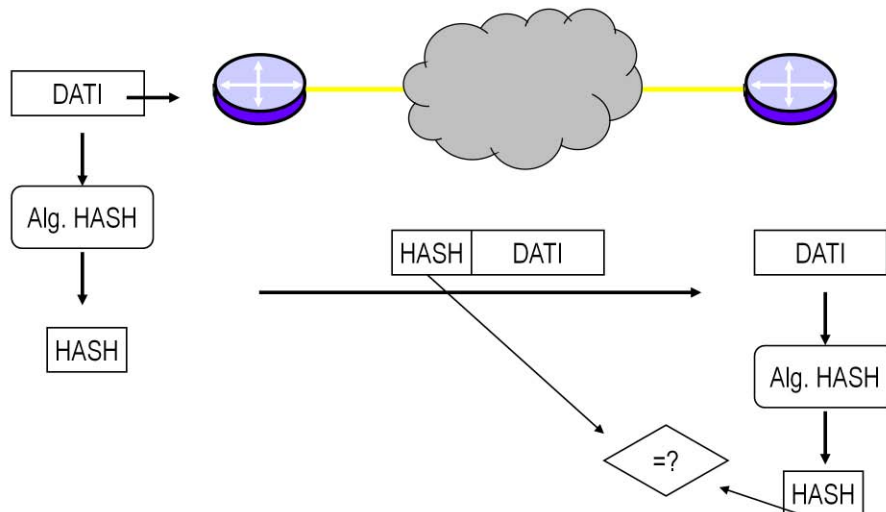
Nel caso della cifratura a chiave pubblica e privata i peer generano una coppia di chiavi legate da una relazione matematica. Una delle due chiavi (privata) viene tenuta segreta e **l'altra** (pubblica) viene inviata al peer. I dati cifrati con la chiave privata possono essere decodificati solo con quella pubblica e viceversa. Essere in grado di decifrare i dati con una delle due chiavi significa che sono stati cifrati con **l'altra**.

Il cardine di questo metodo è **l'identità** del possessore della chiave privata. E' fondamentale accertare **l'identità** del possessore della chiave privata nel momento in cui da **quest'ultimo** si riceve la chiave pubblica: infatti a questo scopo si utilizzano delle procedure fuori rete.

Successivamente, per ogni pacchetto ricevuto sarà facile accertare **l'identità** del mittente: **quest'ultimo** avrà cura di cifrare con la chiave privata una parte dei dati, se sarà possibile decifrarli con la chiave pubblica corrispondente, in questo modo viene accertato che il mittente è il solo possessore della chiave privata.



## Verifica della Integrità dei dati



- Il mittente aggiunge ai dati inviati un Hash dei dati stessi
- Il ricevente ricalcola l'Hash dei dati e lo confronta con l'Hash ricevuto
- La procedura serve anche ad autenticare il mittente

www.ncp-italy.com

Sicurezza delle reti 7-19

**L'algoritmo** HMAC (Hashed Message Authentication Codes) viene utilizzato per verificare se i dati ricevuti sono stati modificati nel transito e per autenticare il mittente.

Per grandi linee **l'algoritmo** funziona così:

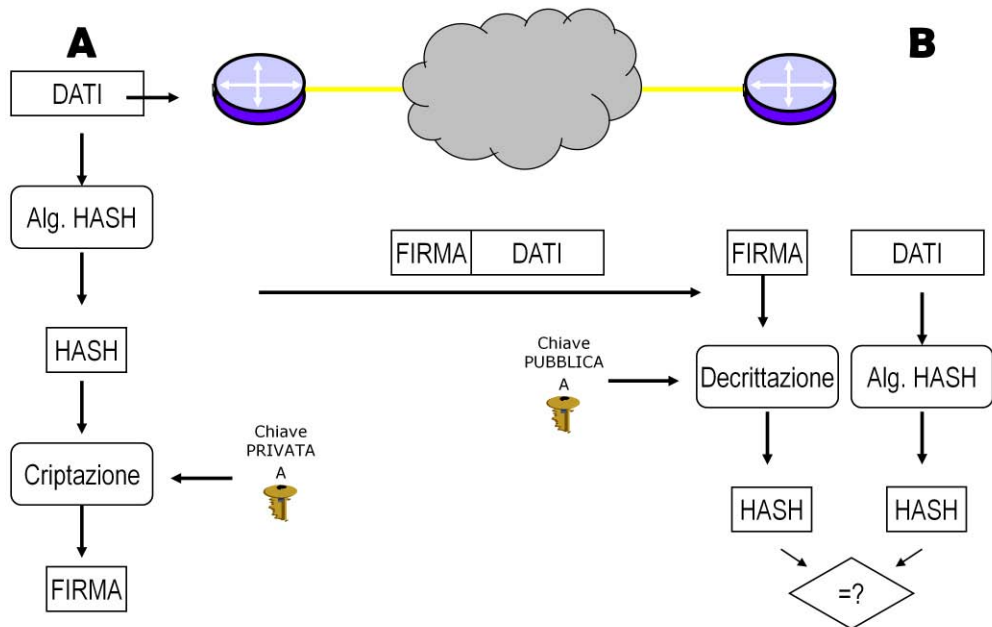
- il mittente dei dati, dopo aver generato il pacchetto, ne produce un Hash in base ad una determinata chiave;
- l'Hash dei dati viene aggiunto al pacchetto stesso;
- il destinatario del pacchetto (che possiede la stessa chiave del mittente) ricalcola l'Hash;
- l'Hash calcolato viene confrontato con quello ricevuto: se corrisponde, il pacchetto è considerato valido, altrimenti viene scartato. Una terza parte ostile che volesse catturare i dati spediti, modificarli e poi inviarli al destinatario non potrebbe, senza la chiave opportuna, generare un campo Hash valido.

**L'algoritmo** HMAC può essere basato sia sull'algoritmo MD5 che su SHA-1 (che è leggermente più sicuro).

Si noti che in realtà l'Hash indicato in figura non si ottiene con una semplice applicazione dell'algoritmo MD5 o di SHA-1: in genere l'algoritmo viene applicato ai dati almeno due volte.



# Firma Digitale



www.ncp-italy.com

Sicurezza delle reti 7-20

La Firma Digitale è una modalità molto robusta di autenticazione del mittente.

**L'algoritmo** prevede che il destinatario dei dati possieda la chiave pubblica del mittente.

La procedura è la seguente:

- il mittente genera l'**Hash** dei dati;
- l'**Hash** dei dati viene cifrato con la chiave privata del mittente producendo la firma che viene aggiunta ai dati stessi;
- il destinatario decifra la firma con la chiave pubblica del mittente, ottenendo l'**Hash**;
- con i dati ricevuti, l'**Hash** viene ricalcolato;
- l'**Hash** ricevuto ed l'**Hash** calcolato vengono confrontati.



## Confronto

Algoritmi	Descrizione
DES	Cifratura a blocco, cripta blocchi di dati a 64-bit. Lunghezza fissa della chiave a 64-bit (vengono utilizzati solamente 56 bit per la crittografia).
3DES	Applica il DES tre volte di seguito utilizzando tre chiavi differenti. Dimensione delle chiavi di 168 e 112 bit.
AES	Cifratura a blocco reiterata con lunghezza delle chiavi variabile. 128-, 192-, o 256-bit .
Rivest Ciphers	Famiglia di algoritmi ampiamente implementata. Blocchi variabili e dimensione delle chiavi.

Lucifer è ritenuto generalmente il primo algoritmo moderno a blocchi. Sviluppato dall'IBM negli anni settanta era basato sul lavoro di Horst Feistel. Una versione migliorata venne utilizzata dal governo degli Stati Uniti d'America per realizzare lo standard FIPS Data Encryption Standard (DES). Venne scelto dall'US National Bureau of Standards (NBS) dopo la pubblicazione del bando che invita a sottoporre all'attenzione del NSA i propri algoritmi di cifratura. Lo standard del DES venne pubblicato nel 1976 e da allora venne utilizzato fino alla fine del 2000.

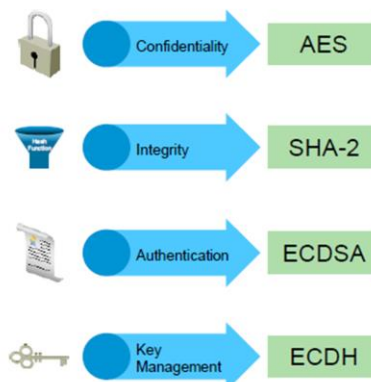
DES era progettato per resistere a una categoria di attacchi conosciuti dalla NSA e in seguito scoperti anche dall'IBM. Il principale limite del DES è la sua chiave di soli 56 bit. La dimostrazione definitiva dell'inadeguatezza del DES la si ebbe nel 1998 quando la Electronic Frontier Foundation riuscì a forzare la codifica DES con una macchina specializzata nel giro di tre giorni. Vennero sviluppate delle varianti del DES come il Triple DES, che offre una maggiore sicurezza ma risulta più lento per via della triplice esecuzione della cifratura DES.

Il DES è stato sostituito dal nuovo standard federale, Advanced Encryption Standard (AES), scelto dal National Institute of Standards and Technology (NIST) nel 2001 dopo 5 anni di standardizzazione. Il nuovo standard deriva da un algoritmo sviluppato da Joan Daemen e Vincent Rijmen e il suo nome è Rijndael. AES gestisce blocchi di 128 bit e chiavi di lunghezza 128, 192, 256 bit.



## Il meglio della sicurezza

- Migliora l'intera suite di crittografia
- Efficiente ad alti livelli di sicurezza e alte velocità
- Algoritmi di crittografia raccomandati dal governo U.S.
  - Subset di FIPS-140
  - Selezionato da U.S. National Security Agency (NSA)
- Introdotto in molti standard
  - RFC 4869 "Suite B Cryptographic Suites for IPsec"
- Approvato per dati classificati secret e top secret



[www.ncp-italy.com](http://www.ncp-italy.com)

Sicurezza delle reti 7-22

NSA Suite B Cryptography is a set of cryptographic algorithms promulgated by the National Security Agency as part of its Cryptographic Modernization Program. It is to serve as an interoperable cryptographic base for both unclassified information and most classified information.

Suite B was announced on 16 February 2005. A corresponding set of unpublished algorithms, Suite A, is "used in applications where Suite B may not be appropriate. Both Suite A and Suite B can be used to protect foreign releasable information, US-Only information, and Sensitive Compartmented Information (SCI)."

Suite B's components are:

Advanced Encryption Standard (AES) with key sizes of 128 and 256 bits. For traffic flow, AES should be used with either the Counter Mode (CTR) for low bandwidth traffic or the Galois/Counter Mode (GCM) mode of operation for high bandwidth traffic (see Block cipher modes of operation) – symmetric encryption

Elliptic Curve Digital Signature Algorithm (ECDSA) – digital signatures

Elliptic Curve Diffie-Hellman (ECDH) – key agreement

Secure Hash Algorithm 2 (SHA-256 and SHA-384) – message digest

As of October 2012, CNSSP-15 stated that the 256-bit elliptic curve (specified in FIPS 186-2), SHA-256, and AES with 128-bit keys are sufficient for protecting classified information up to the **Secret level**, while the 384-bit elliptic curve (specified in FIPS 186-2), SHA-384, and



AES with 256-bit keys are necessary for the protection of **Top Secret information**. As of August 2015, NSA indicated that only the Top Secret algorithm strengths should be used to protect all levels of classified information.



## Bibliografia e link utili

- William Stallings; *Sicurezza delle reti: Applicazioni e standard* -Addison Wesley
- Dieter Gollman; *Computer Security* - John Wiley & Sons
- *Guida alla sicurezza dei PC*; Stefano Bendandi;  
[http://www.html.it/sicurezza\\_pc/index.html](http://www.html.it/sicurezza_pc/index.html)
- *Sicurezza nelle reti locali*; OTE Osservatorio Tecnologico;  
<http://www.osservatoriotecnologico.net/RETI/sicurezza.htm>

*Dispense del corso di Sicurezza su Reti*; Alfredo De Santis;

<http://www.dia.unisa.it/ads.dir/corso-security/www/CORSO-0102/>

*The Probert E-Text Encyclopaedia*;

<http://www.sneaker.net.au/docs/encyclo/GIL1.HTM>

*Proteggi il tuo PC: I Portatili*.

[http://education.mondadori.it/libri/Download/Capitoli/334\\_cap04.pdf](http://education.mondadori.it/libri/Download/Capitoli/334_cap04.pdf)

*Virus Enciclopedia*; Trendmicro; <http://www.trendmicro.com/vinfo/virusencyclo/>

*Wild List*; <http://www.wildlist.org>

*La firma digitale*; Ministero per l'innovazione tecnologica;

[http://www.innovazione.gov.it/ita/egovernment/infrastrutture/firma\\_digitale.shtml](http://www.innovazione.gov.it/ita/egovernment/infrastrutture/firma_digitale.shtml)

William Stallings; *Sicurezza delle reti: Applicazioni e standard*; Addison Wesley

*Introduzione alla crittografia*; Pierre Loidreau;

<http://www.linuxfocus.org/Italiano/May2002/article243.shtml>

Dieter Gollman; *Computer Security*; John Wiley & Sons

*Crittografia e PGP*; Matteo Zinato; <http://www.html.it/crittografia/index.html>

*Dispense del corso di Sicurezza su Reti*; Alfredo De Santis;

<http://www.dia.unisa.it/ads.dir/corso-security/www/CORSO-0102/>

*Introduzione ai problemi legati alla crittografia e alla firma elettronica*; Daniele Giacomini;

<http://lagash.dft.unipa.it/AL/al287.htm>

*The International PGP Home Page*; <http://www.serve.com/nimrod/pgp.html>

*Introduzione alla firma digitale*; Interlex;

<http://www.interlex.it/docdigit/intro/indice.htm>