UNICAM
Università di Camerino

Laurea in INFORMATICA

INTERNET, RETI e SICUREZZA A.A. 2025/2026
Capitolo 4a – Protocolli di Rete ed Instradamento

Fausto Marcantoni
fausto.marcantoni@unicam.it

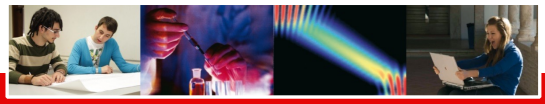
1

Dichiarazione di copyright

L'utilizzo dei contenuti della lezione sono riservati alla fruizione personale degli studenti iscritti ai corsi dell'Università di Camerino. ***Sono vietate*** *la diffusione intera o parziale di video o immagini della lezione, nonché la modifica dei contenuti senza il consenso, espresso per iscritto, del titolare o dei titolari dei diritti d'autore e di immagine.*

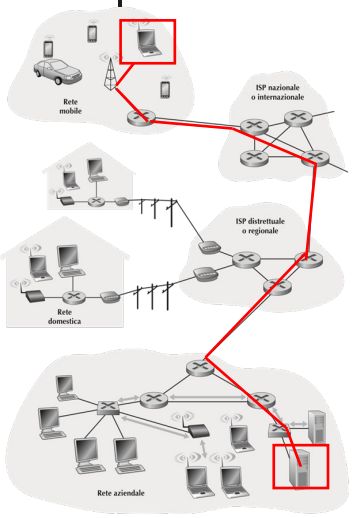
Copyright notice

The contents of this lesson are subject to copyright and intended only for personal use by students enrolled in courses offered by the University of Camerino. For this reason, any partial or total reproduction, adaptation, modification and/or transformation of the contents of this lesson, by any means, without the prior written authorization of the copyright owner, is strictly prohibited.



2

Livello di collegamento



Invio di un datagramma da uno degli host wireless a uno dei server

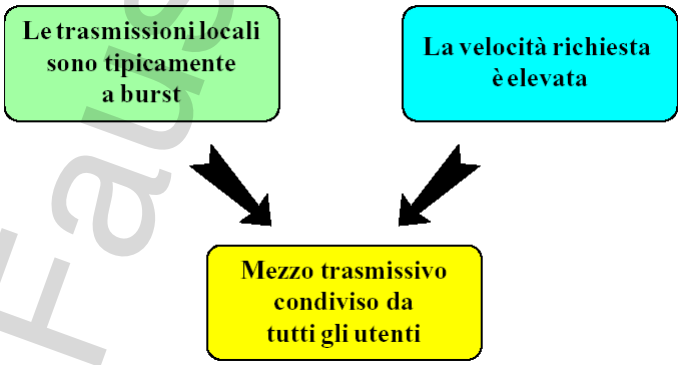
Il datagramma dovrà attraversare sei collegamenti:

1. collegamento WiFi tra l'host sorgente e l'access point WiFi
2. un collegamento Ethernet dall'access point allo switch a livello di collegamento
3. un collegamento tra lo switch a livello di collegamento e il router
4. un collegamento tra i due router
5. un collegamento Ethernet tra il router e lo switch a livello di collegamento
6. un collegamento Ethernet tra lo switch e il server

3

LOCAL AREA NETWORK (LAN)

È un sistema di comunicazione che permette ad apparecchiature indipendenti di comunicare tra di loro entro un'area delimitata utilizzando un canale fisico a velocità elevata e con basso tasso di errore. [*definizione IEEE*]



4

Protocolli e collegamenti ad accesso multiplo

2 tipi di collegamento

- **punto a punto**
- **broadcast**

Collegamento punto a punto → costituito da un trasmittente a un'estremità del collegamento e da un unico ricevente all'altra

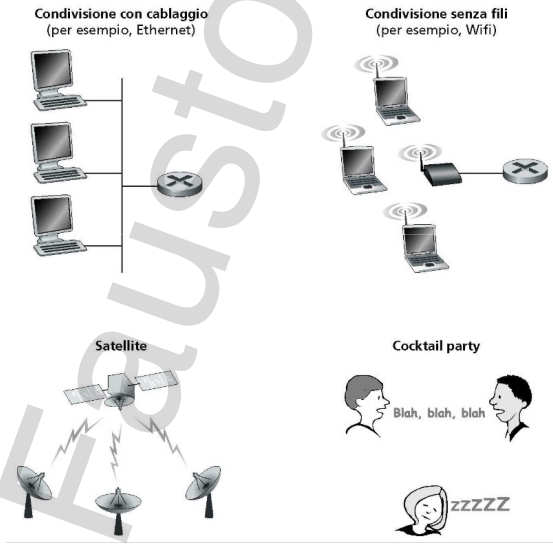
Collegamento broadcast → più nodi trasmittenti e riceventi connessi allo stesso canale broadcast condiviso

Problema dell'accesso multiplo → come coordinare l'accesso di più nodi trasmittenti e riceventi in un canale broadcast condiviso

Protocolli ad accesso multiplo → richiesti in un'ampia varietà di configurazioni di rete, comprese le *LAN cablate*, quelle *wireless* e le *reti satellitari*

5

Canali ad accesso multiplo



6

Collegamenti di accesso multiplo

Esistono due tipi di collegamenti di rete:

Collegamento punto-punto
- Impiegato per connessioni telefoniche.
- Collegamenti punto-punto tra Ethernet e host.

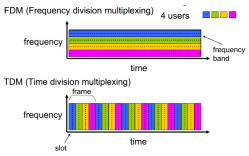
Collegamento broadcast
- Ethernet tradizionale
- HFC in upstream (sistemi Hybrid Fiber Coaxial che utilizzano il cavo coassiale per raggiungere l'utente finale)
- Wireless LAN 802.11

7

Protocolli e collegamenti ad accesso multiplo

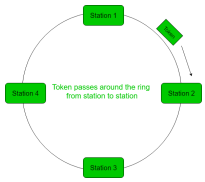
I protocolli ad accesso multiplo sono suddivisibili nelle seguenti categorie:

Protocolli a suddivisione del canale (channel partitioning protocol)



Protocolli ad accesso casuale (random access protocol)

Protocolli a rotazione (taking-turn protocol)



8

Protocolli di accesso multiplo

tre tipologie:

Protocolli a suddivisione del canale (*channel partitioning*)
Suddivide un canale in "parti più piccole" (slot di tempo, frequenza, codice).

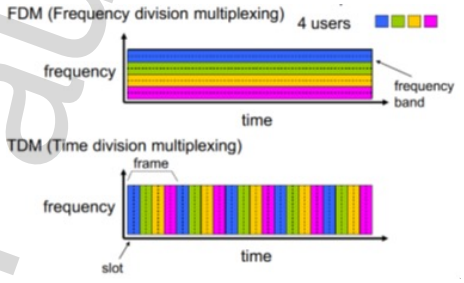
Protocolli ad accesso casuale (*random access*)
I canali non vengono divisi e si può verificare una collisione.
I nodi coinvolti ritrasmettono ripetutamente i pacchetti.

Protocolli a rotazione ("*taking-turn*")
Ciascun nodo ha il suo turno di trasmissione, ma i nodi che hanno molto da trasmettere possono avere turni più lunghi.

9

Protocolli a suddivisione del canale: TDMA-FDMA

TDMA: accesso multiplo a divisione di tempo.
Suddivide il canale condiviso in *intervalli di tempo.*
Gli slot non usati rimangono inattivi
FDMA: accesso multiplo a divisione di frequenza.
Suddivide il canale in bande di frequenza.
A ciascuna stazione è assegnata una banda di frequenza prefissata.



10

Protocolli ad accesso casuale

- Quando un nodo deve inviare un pacchetto:
  - trasmette sempre alla massima velocità consentita dal canale
  - non vi è coordinazione a priori tra i nodi
- Due o più nodi trasmittenti ➜ "collisione"
- Il protocollo ad accesso casuale definisce:
  - Come rilevare un'eventuale collisione.
  - Come ritrasmettere se si è verificata una collisione.
- Esempi di protocolli ad accesso casuale:
  - ✓ slotted ALOHA
  - ✓ ALOHA
  - ✓ CSMA, CSMA/CD, CSMA/CA

Protocolli a rotazione

Protocollo polling:
Un nodo principale sonda "a turno" gli altri.
In particolare:
elimina le collisioni
elimina gli slot vuoti
ritardo di polling

Protocollo token-passing:
Un messaggio di controllo circola fra i nodi seguendo un ordine prefissato.
Messaggio di controllo (*token*).
In particolare:
decentralizzato
altamente efficiente
il guasto di un nodo può mettere fuori uso l'intero canale

Reti di elaboratori

Caratteristiche delle LAN

- ✓ Basso costo
- ✓ Facile upgrading
- ✓ Versatili in termini di riconfigurabilità
- ✓ Flessibili in termini di manutenzione
- ✓ Capaci di sopportare carichi di lavoro elevati
- ✓ Stabili nel tempo
- ✓ Capaci di collegare centinaia di utenti
- ✓ Efficienti in termini di operazioni e accessi consentiti
- ✓ Capaci di coprire distanze anche fino a parecchi km
- ✓ Dotate di capacità di trasmissione anche fino a 1000Mbps

13

Reti di elaboratori

Caratteristiche di una LAN

- Hanno sempre un solo canale trasmissivo ad alta velocità condiviso nel tempo da tutti i sistemi collegati
- Quando un sistema trasmette diventa proprietario temporaneamente dell'intera capacità trasmissiva della rete
- La trasmissione è sempre di tipo "broadcast"
- Alcune complicazioni:
  - È necessaria la presenza di indirizzi
  - Occorre **arbitrare** l'accesso all'unico mezzo trasmissivo (protocolli di reti locali)

14

Attributi di una LAN

- **Affidabilità**: tecnologia consolidata
- **Flessibilità**:
  - LAN di soli PC o integrazione PC-Mainframe / PC-Server
  - supporto simultaneo di più architetture di rete tra di loro incompatibili ai livelli più alti
- **Modularità**: componenti standard di molti costruttori perfettamente interscambiabili
- **Espandibilità**:
  - secondo l'esigenze dell'utente
  - facilitata da una accurata progettazione a priori
- **Gestibilità**: tramite protocolli di management (SNMP)

Componenti di una LAN

- Un Sistema di Calcolo (PC, Workstation, mobile, … → **host**)
- Il Software di rete (S. O., applicativi, programmi, protocolli, …)
- Le NIC (Network Interface Card *[wired - wireless]*)
- Le API (Application Programming Interface)
- Concentratori o Hub: che fungono da nodi di accesso
- Cablaggio strutturato: l'insieme dei mezzi fisici di trasmissione, comprensivi di altri componenti quali connettori, adattatori, schede, antenne, ecc…

Classificazione delle LAN

Le Reti LAN vengono classificate sulla base dell'**hardware** e del **software**.

☑ Hardware:
il tipo di architettura con cui la rete LAN è realizzata

☑ Software:
il sistema operativo che definisce i protocolli di rete cioè gli standard di comunicazione

17

Classificazione delle LAN

Hardware:
il tipo di architettura con cui la rete LAN è realizzata

I quattro elementi base dalla cui combinazione nascono le diverse architetture impiegate nelle LAN sono:

- la topologia
- il mezzo trasmissivo
- le tecniche di trasmissione
- i metodi di accesso alla rete

18

Classificazione delle LAN

Software:
il sistema operativo che definisce i protocolli di rete cioè gli standard di comunicazione

Il supporto alle reti LAN è fornito da due componenti software :

- sw di rete di alto livello (sistemi operativi o protocolli);
- sw di interfaccia delle NIC (i driver di rete)

19

PROTOCOLLI delle LAN

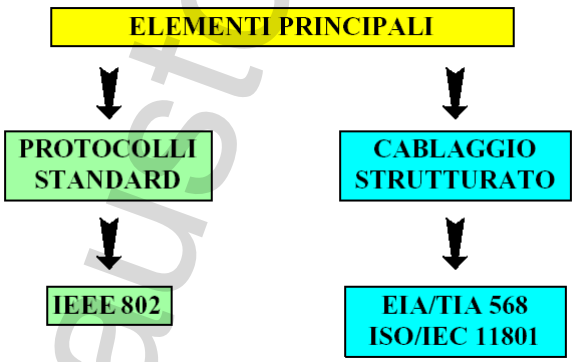
NET WARE
LAN MANAGER e LAN SERVER
VINES
TCP/IP
LANtastic
DECnet
PATHWORKS
SNA (System Network Architecture)
APPN (Advanced Peer-to-PeerNetworking)
APPLE TALK

20

PROTOCOLLI delle LAN

- **NET WARE** della Novell; realizza al suo interno un'architettura Client/Server con sw server e sw client.
- **LAN MANAGER e LAN SERVER** di Microsoft e IBM rispettivamente; anche qui sistemi Client accedono a funzioni del Server, come file e stampanti.
- **VINES** : caratteristiche simili a Netware, Lan Manager e Lan Server con in più prestazioni per reti WAN.
- **TCP/IP** del Dipartimento della difesa degli USA; ideato da Cerf e Khan nel 1974, si basa sul modello Client/Server Peer-to-Peer.
- **LAN tastic** di Artisoft; impiegato su reti di piccole dimensioni.
- **DEC** net è della DEC e funziona su architetture proprietarie (microcomputer e workstation DEC).
- **PATHWORKS** racchiude famiglie di protocolli DEC che possono essere impiegati anche su architetture non proprietarie.
- **SNA** : dell'IBM per i grossi mainframe.
- **APPN** : dell'IBM ma usati anche su piccoli sistemi
- **APPLE TALK** : integra sw di rete e sw d'utente.

Elementi Principali



Il progetto IEEE 802 definisce un insieme di standard per le LAN e le MAN, relativamente ai livelli data link e fisico.

Standards IEEE

Active Working Groups and Study Groups
- 802.1 Higher Layer LAN Protocols Working Group
- 802.3 Ethernet Working Group
- 802.11 Wireless LAN Working Group
- 802.15 Wireless Personal Area Network (WPAN) Working Group
- 802.16 Broadband Wireless Access Working Group
- 802.17 Resilient Packet Ring Working Group
- 802.18 Radio Regulatory TAG
- 802.19 Coexistence TAG
- 802.20 Mobile Broadband Wireless Access (MBWA) Working Group
- 802.21 Media Independent Handoff Working Group
- 802.22 Wireless Regional Area Networks

Inactive Working Groups and Study Groups
- 802.2 Logical Link Control Working Group
- 802.5 Token Ring Working Group
- 802.12 Demand Priority Working Group

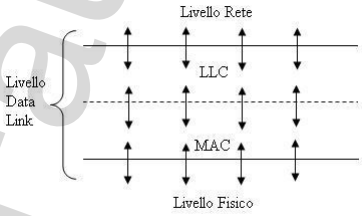
Disbanded Working Groups and Study Groups
- 802.4 Token Bus Working Group
- 802.6 Metropolitan Area Network Working Group
- 802.7 Broadband TAG
- 802.8 Fiber Optic TAG
- 802.9 Isochronous LAN Working Group
- 802.10 Security Working Group
- 802.14 Cable Modem Working Group

23

Livello Data Link

Data link control (***livello di protocollo di linea***): l'ultimo passo **prima della trasmissione** vera e propria, è quello di **strutturare il messaggio** secondo il formato previsto dal protocollo utilizzato sulla linea in uscita.

Vanno anche definite le funzioni di controllo della trasmissione.



24

Livello Data Link

Il livello di **LLC** (***Logical Link Control***) supporta servizi di livello più alto:

Gestione degli indirizzi: assegna alla frame l'indirizzo sorgente e destinazione.

Gestione degli errori: meccanismi di conferma (ack) e ritrasmissione (timeout).

Ordinamento: frammentazione di frame troppo lunghe ed ordinamento in ricezione.

Controllo di flusso: uso di numeri di sequenza e di meccanismi "sliding window".

Il **MAC** (***Medium Access Control***)
si occupa della gestione dell'accesso al mezzo fisico

25

Livello Data Link

Le operazioni compiute a questo livello si possono così riassumere:

- **In trasmissione:**
  - **riceve un flusso** di dati dal livello superiore, e se è il caso, li spezzetta in blocchi (detti **frame**) che non superino la lunghezza prestabilita
  - aggiunge eventuali delimitatori ai frame (intestazione/fine) ed esegue l'algoritmo previsto per il **controllo dell'errore**, calcolando ed aggiungendo il campo di controllo (check)
  - **invia i frame** in sequenza al livello fisico (cioè sul mezzo trasmissivo)

26

Livello Data Link

Le operazioni compiute a questo livello si possono così riassumere:

- **In ricezione:**
  - **riceve un flusso di bit** dal livello fisico sottostante
  - riconosce ed analizza **l'intestazione dai frame**
  - esegue l'algoritmo previsto per il **controllo dell'errore**, e verifica che il campo di controllo corrisponda a quanto previsto
  - elimina l'intestazione e l'end-frame, e ricompone il flusso di dati, che **consegna al livello superiore**

Livello Data Link

Obiettivo principale:

Fornire al livello di rete di due **macchine adiacenti** un ***canale di comunicazione*** il più possibile affidabile.

- macchine adiacenti: fisicamente connesse da un canale di comunicazione (es. un cavo coassiale, doppino telefonico)
- canale di comunicazione: "tubo digitale", ovvero i bit sono ricevuti nello stesso ordine in cui sono inviati

- Problematiche: **il canale fisico non è ideale**
  - errori di trasmissione tra sorgente e destinazione
  - necessità di dover gestire la velocità di trasmissione dei dati
  - ritardo di propagazione non nullo

Il sottolivello MAC

Bisogna considerare però che il livello Data Link ha a che fare con il livello 1, ovvero il livello fisico (direttamente collegato al mezzo fisico)

Il mezzo fisico (canale di comunicazione) può essere:

- **dedicato** (reti punto-punto)
- **condiviso** (reti broadcast)

Se il mezzo fisico è condiviso, nascono una serie di problematiche relative all'accesso a tale mezzo

- selezione dell'host che ha **il diritto di trasmettere** sul mezzo condiviso
- situazione di **competizione per la risorsa trasmissiva**

Viene introdotto un sotto-livello al livello 2 che gestisce queste problematiche

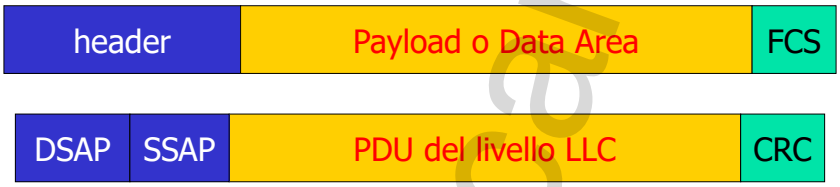
MAC (Medium Access Control)

COME SPECIFICARE IL DESTINATARIO ?

- Problema:
  - Mettere in comunicazione diretta due calcolatori senza disturbare gli altri che comunque ricevono copia di tutti i dati in transito (in teoria)
- Assegnare a ciascuna stazione un numero identificativo
  - INDIRIZZO DI ACCESSO AL MEZZO (Media ACcess address)
- Il **frame** deve dunque contenere **l'indirizzo del destinatario**, ma anche **l'indirizzo del mittente** per facilitare la risposta

MAC PDU – [protocol data unit] (FRAME)

- I campi principali di una MAC PDU sono:
  - Gli indirizzi (detti SAP: Service Access Point) univoci a livello mondiale: http://standards-oui.ieee.org/cid/cid.txt
    - DSAP: Destination SAP
    - SSAP: Source SAP
- La PDU contiene i dati
- La FCS (Frame Check Sequence): un CRC (Cyclic Redundancy Code) su 32 bit per il controllo dell'integrità della trama



31

Cyclic Redundancy Code

Cyclic Redundancy Check(CRC) Code

It's used to detect errors by adding some redundant bits along with data bits.

Algorithm : -

Lets consider data bits : 101101110

- In CRC code we select a polynomial or generator code of length 'r'.
- Then we append r-1 zeros to the data bit before any further computation.
- Lets say the polynomial is x^3+x^2+1, i.e 1101.
- Data bits after appending zeros : 101101110000
- Now we need to perform long division to compute redundant bits. Lets do it

http://www.online.scuola.zanichelli.it/addomineinformatica-files/approfondimenti/ZanichelliI_Addomine_A5_01.pdf

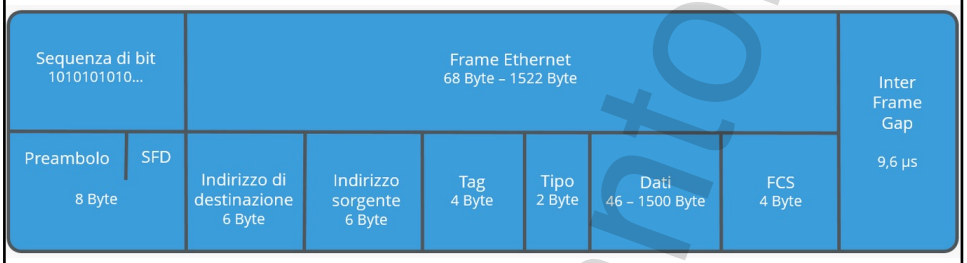
https://www.eee.hku.hk/~sdma/elec7073/Part2-2-Cyclic%20redundancy%20check%20(CRC).pdf

https://www.youtube.com/watch?v=WPkT-Uw5qX0

32

Reti di elaboratori

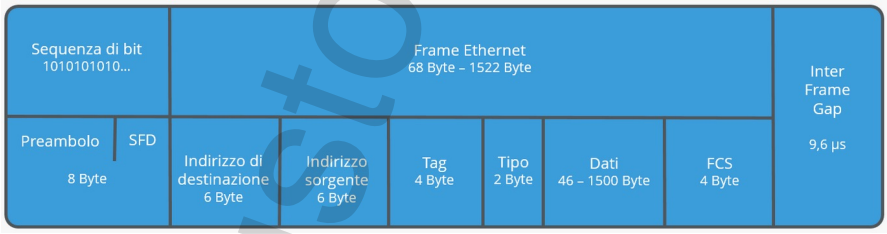
Frame Ethernet



33

Reti di elaboratori

Frame Ethernet



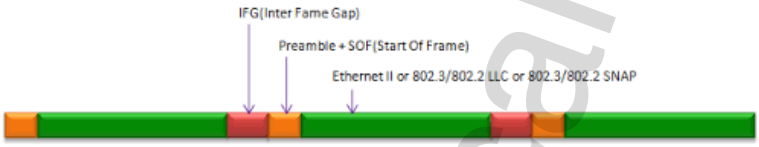
(PreamboloStart Frame Delimiter (SFD))	(8 byte)	Sincronizzazione dei riceventi Sequenza di bit che avvia il frame
Indirizzo di destinazione (MAC)	6 byte	Indirizzo hardware della scheda di rete di destinazione
Indirizzo sorgente (MAC)	6 byte	Indirizzo hardware della scheda di rete di origine
Tag	4 byte	Tag VLAN opzionale per l'integrazione in reti VLAN (IEEE 802.1q)
Tipo	2 byte	Ethernet II: etichettatura dei protocolli di livello 3
Dati	46-1522 byte	Payload Dati
Source Service Access Point (SSAP)	1 byte	Indirizzo sorgente del dispositivo di invio
Frame Check Sequence (FCS)	4 byte	Checksum che calcola l'intero frame
(Inter Frame Gap (IFS))	-	Interruzione di trasmissione di 9,6 µs

34

Inter Frame Gap(IPG)

spaziatura delle frame

il MAC garantisce che tra due pacchetti consecutivi intercorra un lasso di tempo minimo pari al parametro che viene identificato con il nome di **Inter Frame Gap(IPG)**.
Questo tempo serve a delimitare la fine di un pacchetto e a separarlo da quello successivo



https://en.wikipedia.org/wiki/Interpacket_gap

35

Tipi Frame Ethernet

A seconda dello standard Ethernet, i frame Ethernet sono strutturati in modo diverso e possono contenere più o meno campi di dati, in base al protocollo di rete.

- Ethernet II
- Ethernet 802.3raw
- Ethernet IEEE 802.3
- Ethernet IEEE 802.3 SNAP
- VLAN 802.1q – Ethernet II Tagged e IEEE 802.3 Tagged

36

Indirizzi MAC

- Sono standardizzati dalla IEEE
- sono lunghi 6 byte, cioè 48 bit
- si scrivono come 6 coppie di cifre esadecimali

00001000000000000010101100111100000011111001 1010

0	8	0	0	2	b	3	c	0	7	9	a

08-00-2b-3c-07-9a
08:00:2b:3c:07:9a
08-00-2B-3C-07-9A

37

Struttura Indirizzi MAC

- Si compongono di due parti grandi 3 Byte ciascuna:
- I tre byte più significativi indicano il lotto di indirizzi acquistato dal costruttore della scheda, detto anche *vendor code o OUI (Organization Unique Identifier).*
- I tre meno significativi sono una numerazione progressiva decisa dal costruttore

0	8	0	0	2	b	3	c	0	7	9	a

OUI assegnato dall'IEEE Assegnato dal costruttore

38

ALCUNI OUI

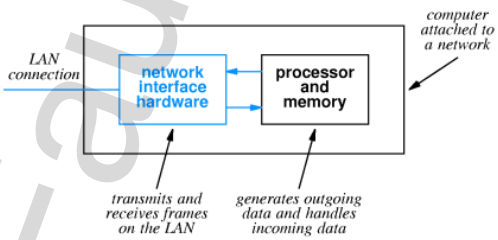
Organization	Address Block
Cisco	00000Ch
DEC	08002B (et. al.)
IBM	08005A (et. al)
Sun	080020h
Proteon	000093h
Bay-Networks	0000A2h

http://standards.ieee.org/develop/regauth/oui/oui.txt

39

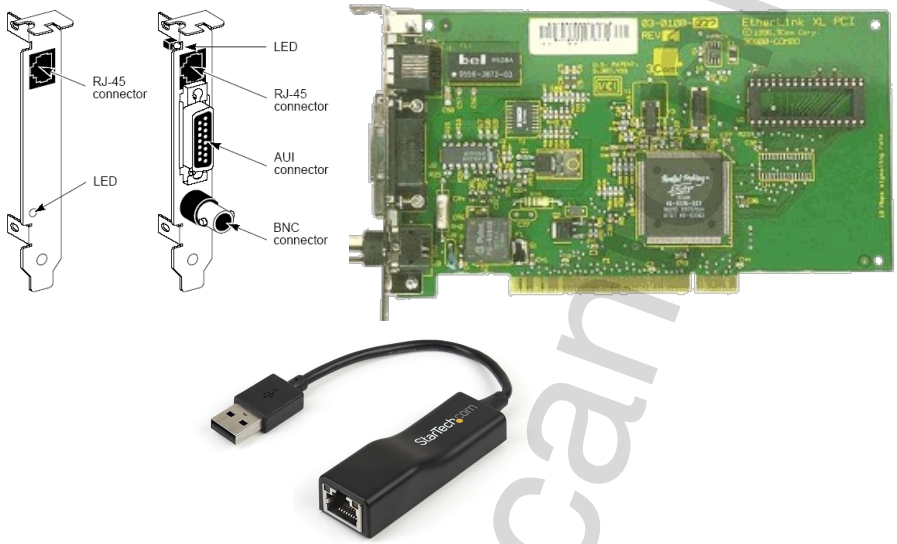
La scheda di rete

- Si occupa dei dettagli di **trasmissione e ricezione**
- Lavora in maniera **indipendente dal computer**
- Sfrutta l'indirizzo fisico per **cestinare** il frame oppure per **trasferirlo** al computer



40

La scheda di rete (wired)



41

La scheda di rete (wireless)

42

Indirizzo fisico

- Deve essere **unico** in una LAN (no su internet)
- Come si **assegna un indirizzo** alla stazione e chi è responsabile dell'unicità ?
- Indirizzi statici
  - Assegnati dai costruttori e non cambia se non si cambia la scheda di rete
- Indirizzi configurabili
  - I costruttori mettono a disposizione dip switch o software per determinare l'indirizzo da parte dei clienti
- Indirizzi dinamici
  - Sono assegnati automaticamente alla stazione ad ogni riavvio

Indirizzi MAC

- Sono di tre tipi:
  - **Unicast:** di una singola stazione
  - **Multicast:** di un gruppo di stazioni
  - **Broadcast:** di tutte le stazioni (ff-ff-ff-ff-ff-ff)
- Ogni scheda di rete quando riceve un pacchetto lo passa ai livelli superiori nei seguenti casi:
  - Broadcast: sempre
  - Multicast: se ne è stata abilitata la ricezione via software
  - Unicast: se il DSAP è uguale a quello hardware della scheda (scritto in una ROM) o a quello caricato da software in un apposito buffer

Indirizzi di gruppo

- Servono tipicamente per scoprire i nodi adiacenti
- Esistono due modi diversi di impiego:
  - Solicitation:
    - la stazione che è interessata a scoprire chi offre un dato servizio invia un pacchetto di multicast con l'indirizzo di quel servizio
    - Le stazioni che offrono tale servizio rispondono alla solicitation.
  - Advertisement:
    - le stazioni che offrono un servizio periodicamente trasmettono un pacchetto di multicast per informare di tale offerta tutte le altre stazioni

Neighbor Discovery

45

Powershell - Get-Neighbor

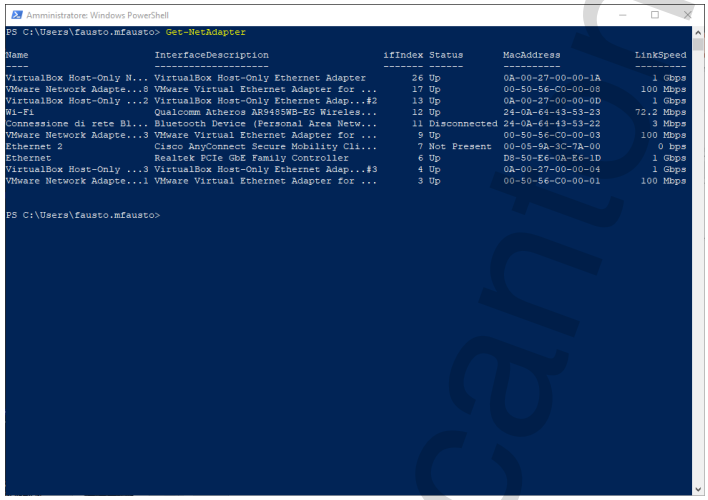
```
Get-NetNeighbor
  [[-IPAddress] <String[]>]
  [-InterfaceIndex <UInt32[]>]
  [-InterfaceAlias <String[]>]
  [-LinkLayerAddress <String[]>]
  [-State <State[]>]
  [-AddressFamily <AddressFamily[]>]
  [-AssociatedIPInterface <CimInstance>]
  [-PolicyStore <String>]
  [-IncludeAllCompartments]
  [-CimSession <CimSession[]>]
  [-ThrottleLimit <Int32>]
  [-AsJob]
  [<CommonParameters>]
```

https://docs.microsoft.com/en-us/powershell/module/nettcpip/get-netneighbor?view=windowsserver2019-ps

46

Powershell - Get-Neighbor

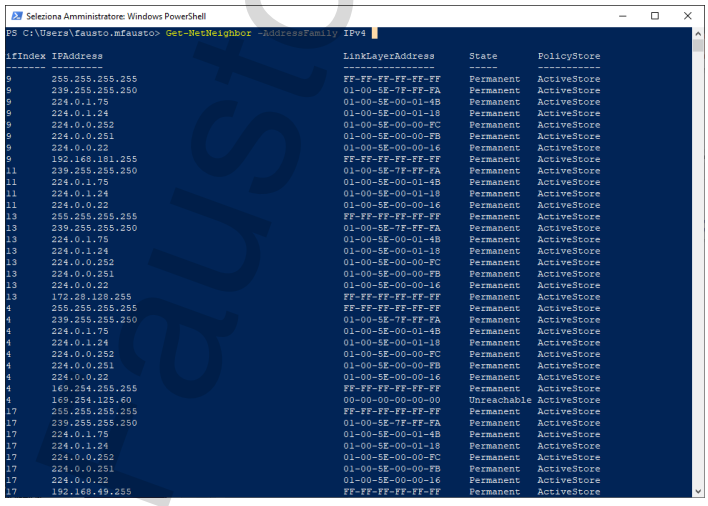
```
Get-NetAdapter
```



47

Powershell - Get-Neighbor

```
Get-NetNeighbor -AddressFamily IPv4
```



48

ip neigh show

```
studente@studente-VirtualBox: ~
studente@studente-VirtualBox:~$ ip neigh show
192.168.1.13 dev wlx5cd9980cc870 lladdr 24:0a:64:43:53:23 STALE
192.168.1.10 dev wlx5cd9980cc870 lladdr 9c:32:ce:97:ea:cb STALE
192.168.1.7 dev wlx5cd9980cc870 lladdr 1a:37:9a:c8:b8:37 STALE
192.168.1.17 dev wlx5cd9980cc870  FAILED
192.168.1.1 dev wlx5cd9980cc870 lladdr 14:14:59:2d:eb:20 STALE
192.168.1.3 dev wlx5cd9980cc870 lladdr e8:b2:fe:20:01:94 REACHABLE
fe80::411:973f:2a48:3aee dev wlx5cd9980cc870 lladdr 1a:37:9a:c8:b8:37 REACHABLE
studente@studente-VirtualBox:~$
```


49

arp-scan

sudo arp-scan -I en9 --localnet

```
faustomarcantoni — -zsh — 80×24
faustomarcantoni@MacBook-Pro-di-Fausto ~ % sudo arp-scan -I en9 --localnet
Interface: en9, type: EN10MB, MAC: a0:ce:c8:ac:dc:ee, IPv4: 193.205.92.119
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
193.205.92.2    10:b3:d5:e2:b4:5f       Cisco Systems, Inc
193.205.92.27   00:50:56:a4:41:ab       VMware, Inc.
193.205.92.61   3c:ec:ef:04:b7:30       Super Micro Computer, Inc.
193.205.92.62   3c:ec:ef:04:b7:30       Super Micro Computer, Inc.
193.205.92.63   3c:ec:ef:04:b7:30       Super Micro Computer, Inc.
193.205.92.64   3c:ec:ef:04:b7:30       Super Micro Computer, Inc.
193.205.92.65   3c:ec:ef:04:b7:30       Super Micro Computer, Inc.
193.205.92.66   00:50:56:a4:eb:78       VMware, Inc.
193.205.92.74   00:50:56:9a:54:a4       VMware, Inc.
193.205.92.81   00:50:56:a4:a4:62       VMware, Inc.
193.205.92.75   00:50:56:b9:05:0c       VMware, Inc.
193.205.92.84   24:5e:be:30:e4:1f       QNAP Systems, Inc.
193.205.92.79   00:0c:29:4f:ca:68       VMware, Inc.
193.205.92.86   00:0c:29:fb:58:62       VMware, Inc.
193.205.92.97   00:50:56:a4:24:fd       VMware, Inc.
193.205.92.98   4c:d7:17:9a:de:b1       (Unknown)
193.205.92.100  00:50:56:a4:34:a7       VMware, Inc.
193.205.92.102  00:50:56:b9:7f:89       VMware, Inc.
193.205.92.106  00:50:56:a4:ae:74       VMware, Inc.
193.205.92.108  00:50:56:a4:50:c3       VMware, Inc.
193.205.92.113  9c:7b:ef:4e:86:61       Hewlett Packard
```


50

Neighbor Discovery Protocol

Il **Neighbor Discovery Protocol** (**NDP**) è un protocollo nella suite di protocolli Internet utilizzato da IPv6. Opera a livello di accesso alla rete ed è impiegato per:

- **autoconfigurare gli indirizzi dei nodi**
- **individuare altri nodi sulla rete**
- **recuperare l'indirizzo di accesso alla rete (es. indirizzo MAC) degli altri nodi**
- **rilevare un conflitto di indirizzi**
- **trovare router disponibili sulla rete**
- **trovare DNS operativi sulla rete**

Indirizzi di gruppo

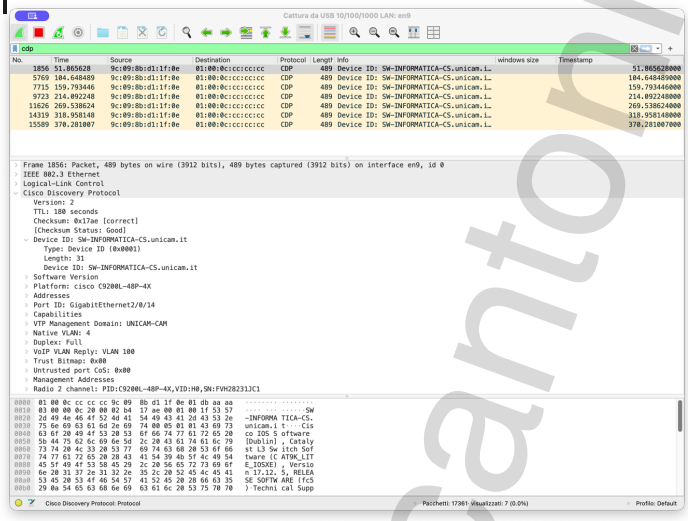
Neighbor Discovery

- **Cisco Discovery Protocol** (CDP) è un protocollo proprietario di livello 2 sviluppato da Cisco ed è supportato da quasi tutti i dispositivi Cisco.
- Il suo scopo è quella di condividere informazioni con i dispositivi adiacenti, come il sistema operativo e l'indirizzo IP, …
- I dispositivi Cisco trasmettono annunci CDP all'indirizzo di destinazione multicast 01-00-0c-cc-cc-cc,

https://learningnetwork.cisco.com/docs/DOC-26872

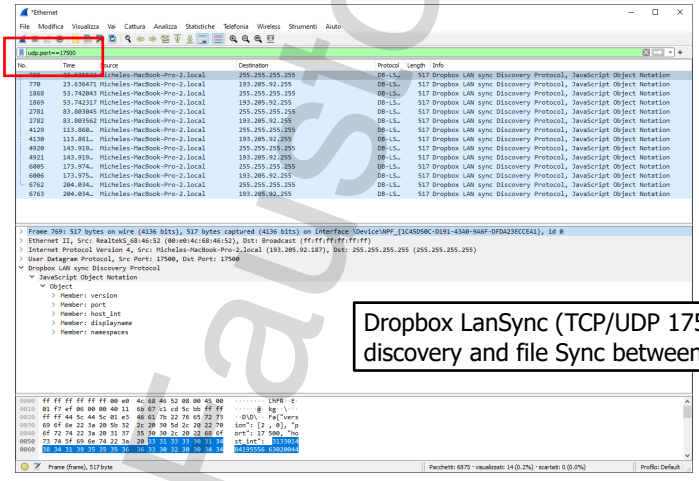
Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
20b3992aab54	Gig 3/8	122	T S	SecureSta	ge.1.47
20b399627b06	Fas 6/1	130	R T S	SecureSta	ge.1.48
20b399b31f2a	Gig 3/11	178	R T S	SecureSta	ge.1.24
20b3992ad09e	Gig 4/2	179	T S	SecureSta	ge.1.47
20b3993e7196	Fas 6/1	129	R T S	SecureSta	ge.1.48
20b39961779a	Gig 3/14	169	R T S	SecureSta	ge.1.24
UBNT	Fas 6/1	110	T	NVSN	
UBNT_A	Gig 5/4	98	T	R5N	br0
UBNT_A	Gig 5/12	98	T	R5N	br0
farmacologia	Gig 4/15	132	S I	WS-C2950S	Gig 0/1
A4S01	Gig 5/1	116	S I	WS-C3560C	Gig 0/1
Router	Gig 5/4	136	R S I	3745	Fas 1/0
Router	Gig 5/12	136	R S I	3745	Fas 1/0
Switch	Gig 3/6	152	S I	WS-C2960S	Gig 0/49
Switch	Gig 7/4	165	S I	WS-C2950G	Gig 0/2
Switch	Fas 6/1	122	S I	WS-C2950G	Fas 0/20
Switch	Gig 3/7	172	S I	WS-C2950G	Gig 0/1
2-Sabbieti	Gig 3/12	115	R	Mikrotik	bridge1

Cisco Discovery Protocol



53

Dropbox discovery

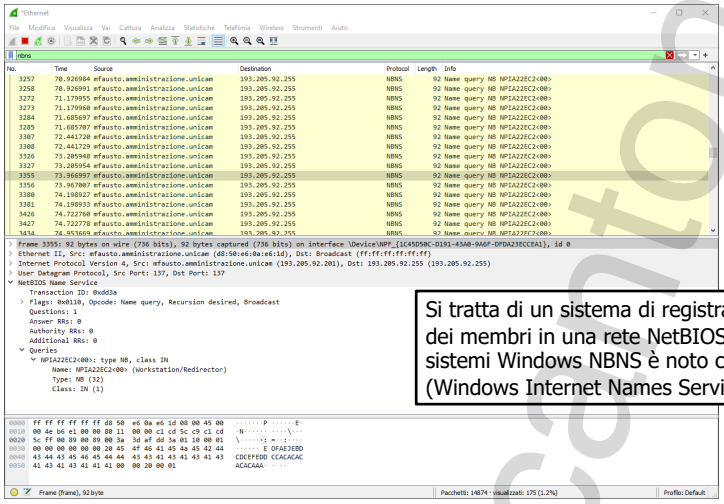


Dropbox LanSync (TCP/UDP 17500), used for LAN discovery and file Sync between Dropbox Clients.

54

Reti di elaboratori

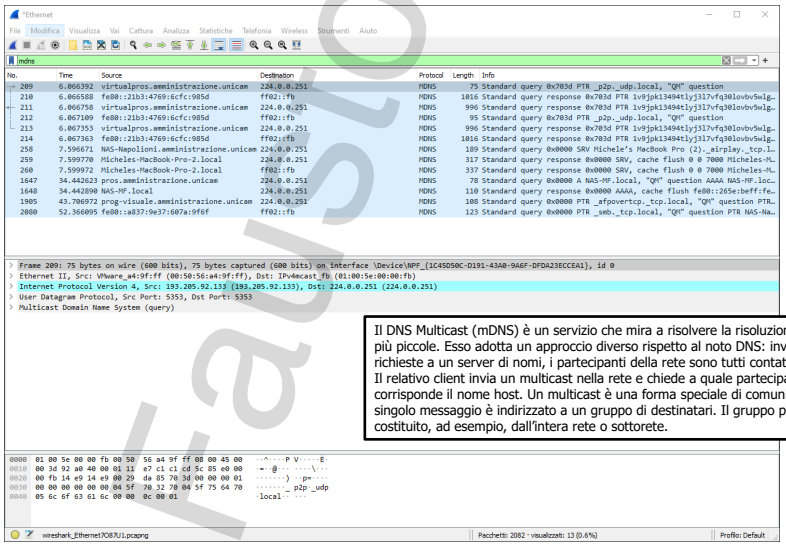
nbns -NetBIOS Name Service



Si tratta di un sistema di registrazione dei nomi dei membri in una rete NetBIOS su TCP . Sui sistemi Windows NBNS è noto come WINS (Windows Internet Names Service)

Reti di elaboratori

mDNS - DNS Multicast



Il DNS Multicast (mDNS) è un servizio che mira a risolvere la risoluzione dei nomi in reti più piccole. Esso adotta un approccio diverso rispetto al noto DNS: invece di inviare richieste a un server di nomi, i partecipanti della rete sono tutti contattati direttamente. Il relativo client invia un multicast nella rete e chiede a quale partecipante della rete corrisponde il nome host. Un multicast è una forma speciale di comunicazione in cui un singolo messaggio è indirizzato a un gruppo di destinatari. Il gruppo può essere costituito, ad esempio, dall'intera rete o sottorete.

Problema della risoluzione degli indirizzi

57

Problema della risoluzione degli indirizzi

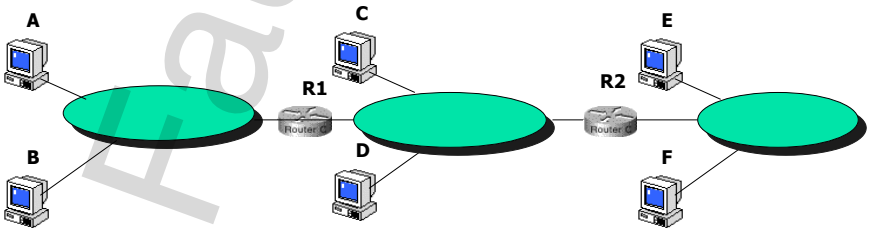
- Gli indirizzi IP sono compresi/gestiti dal software (stack TCP/IP), ma non dai dispositivi delle reti fisiche
- La traduzione dal formato protocollo al formato fisico si chiama RISOLUZIONE DELL'INDIRIZZO (ARP=Address Resolution Protocol)
- Un calcolatore può risolvere l'indirizzo solo se appartiene alla stessa rete fisica.

A deve mandare un messaggio a B

A risolve l'indirizzo di B

A deve mandare un messaggio a F

R2 risolve l'indirizzo di F



58

Tecniche di risoluzione: risoluzione statica

A. Si ha la possibilità di scegliere l'indirizzo fisico quando si installa la scheda di rete

1. Fare in modo che gli uni siano uguali a parte degli altri **IP = 192.5.48.3 Indir.Fisico = 3**
2. Determinare una **funzione f** molto semplice in modo tale che **Ind.Fis. = f(IP)**

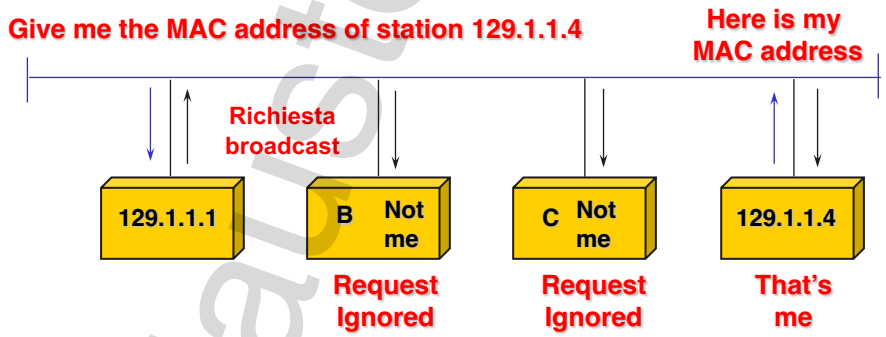
B. Non si ha la possibilità di scegliere l'indirizzo fisico

1. Uno o più computer della medesima rete (server) memorizzano **coppie di indirizzi**
2. Ricerca vettoriale sulla **tabella delle coppie**

TABELLA DI RISOLUZIONE	
Indirizzo IP	Indirizzo fisico
197.15.3.2	0A:07:4B:12.32.36
197.15.3.3	0A:9C:28:71:32:8D
197.15.3.4	0A:11:C3:68:01:99
197.15.3.5	0A:74:59:32:CC:1F
197.15.3.6	0A:04:BC:00:03:28
197.15.3.7	0A:77:81:0E:52:FA

59

Tecniche di risoluzione: risoluzione dinamica

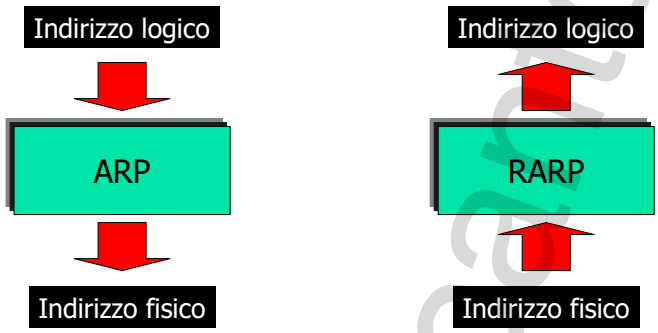


60

Il protocollo ARP

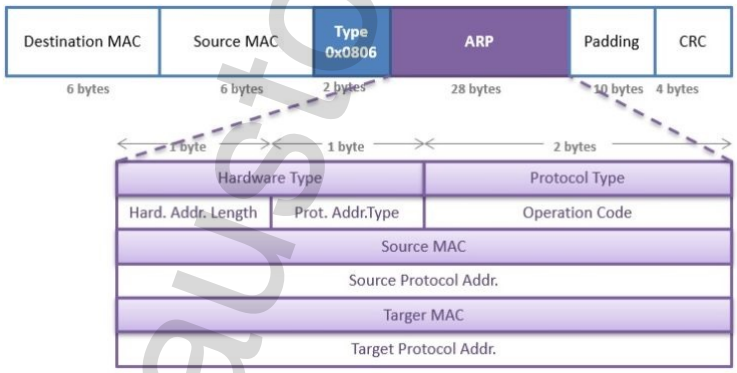
La famiglia TCP/IP incorpora due protocolli :

- ARP per la risoluzione degli indirizzi
- RARP per la risoluzione inversa degli indirizzi



61

Header ARP



https://datatracker.ietf.org/doc/html/rfc826

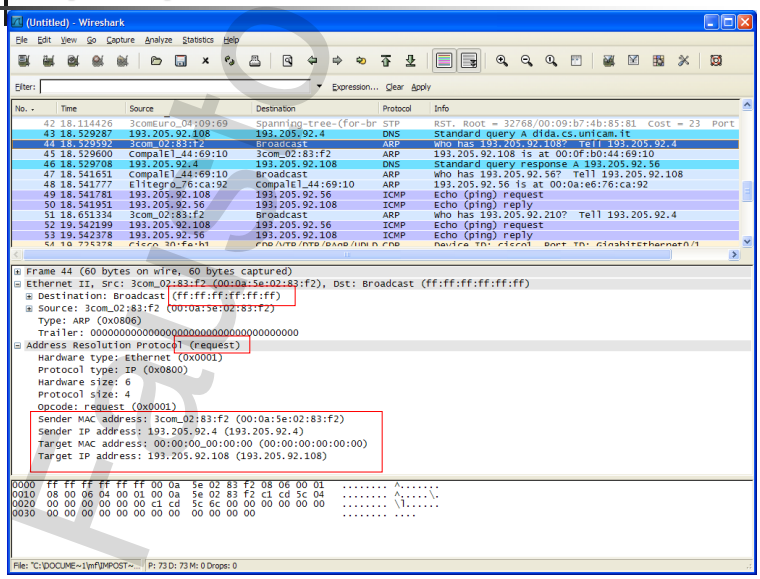
62

Header ARP

- **Hardware Address Space**: in questi 2 byte viene specificato il tipo di indirizzo hardware.
- **Protocol Address Space**: questo campo di 2 byte indica il tipo di protocollo di rete.
- **Hardware Address Length**: questi 8 bit definiscono la lunghezza ***n*** dell'indirizzo hardware.
- **Protocol Address Length**: questo campo determina la lunghezza ***m*** dell'indirizzo di rete.
- **Opcode**: il campo di 2 byte indica di che tipo di operazione si tratta. Una richiesta RARP ha il valore 3 e la risposta corrispondente ha il valore 4.
- **Source Hardware Address**: qui viene memorizzato l'indirizzo MAC del mittente. La lunghezza effettiva di questo campo è ***n*** e viene specificata dall'informazione data nell'Hardware Adress Length. In una rete Ethernet classica è di 6 byte.
- **Source Protocol Adress**: in questo campo in teoria dovrebbe essere indicato l'indirizzo IP del mittente, ma se questo non è noto al momento della richiesta, il campo non viene definito. La risposta, invece, contiene l'indirizzo IP del server. La lunghezza di questo campo è ***m*** e dipende dalla lunghezza dell'indirizzo del protocollo. In genere il campo ha la lunghezza di un indirizzo IPv4, ovvero 4 byte.
- **Target Hardware Address**: questo campo contiene l'indirizzo MAC di destinazione. Poiché nella richiesta RARP non esiste una destinazione specifica, qui viene visualizzato anche l'indirizzo del mittente. Nella risposta il server inserisce anche l'indirizzo del client richiedente. Questo campo ha la lunghezza ***n*** e nel caso di una rete Ethernet ha una dimensione di 6 byte.
- **Target Protocol Adress**: l'ultimo campo non viene definito durante una richiesta per contenere poi, alla risposta del server, l'informazione ricercata: l'indirizzo IP dell'utente di rete. Questo campo ha la lunghezza ***m***, di solito 4 bytes.

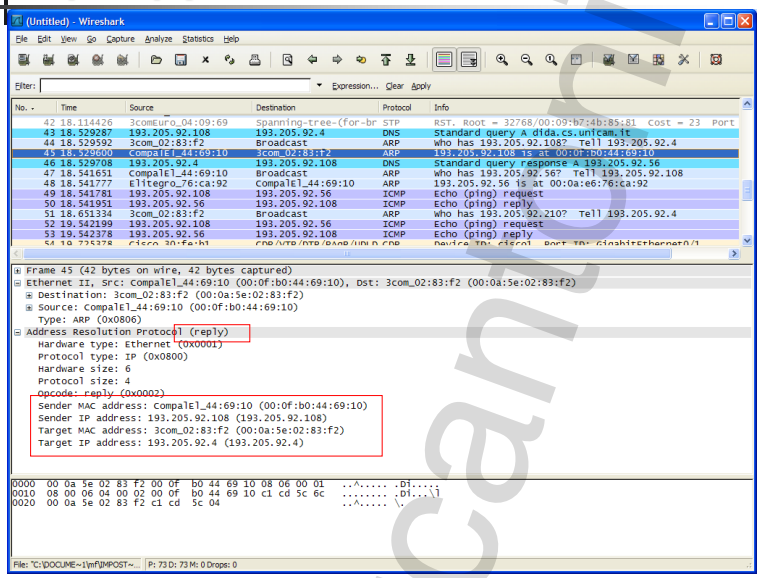
63

Arp - request



64

Arp - reply



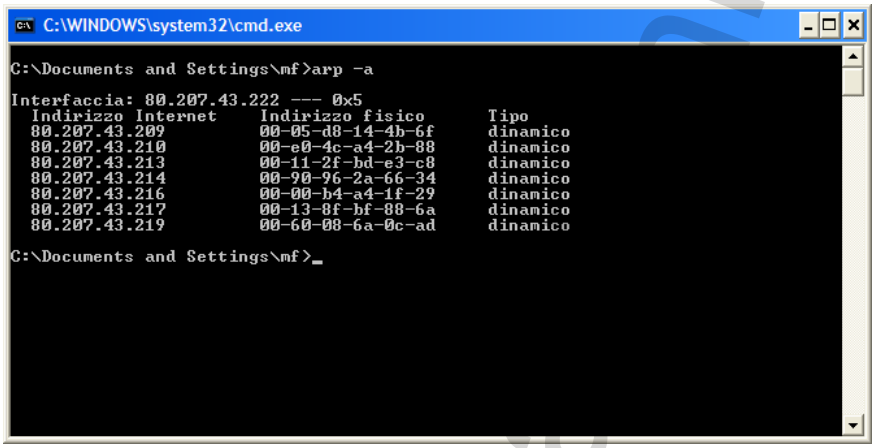
65

I miglioramenti apportati nel tempo ad ARP

- Per ridurre i costi di comunicazione i computer hanno una cache delle corrispondenze recentemente acquisite tra indirizzi IP e quelli fisici
- Per evitare l'obsolescenza dell'informazione (es: un computer si blocca) il protocollo richiede che venga impostato un temporizzatore (cache timeout di ARP)
- Quando si sostituisce la scheda di rete, in fase di inizializzazione il computer può avvisare tutti gli altri inviando un broadcast ARP
- **ARP è un protocollo di basso livello che nasconde l'indirizzo fisico di rete sottostante, permettendo di assegnare un indirizzo IP arbitrario ad ogni macchina**

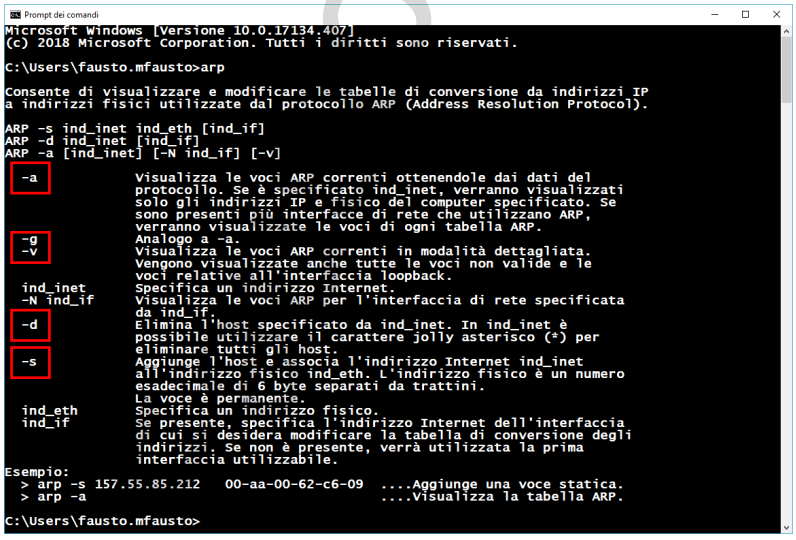
66

Esempio comando arp



67

Comando arp



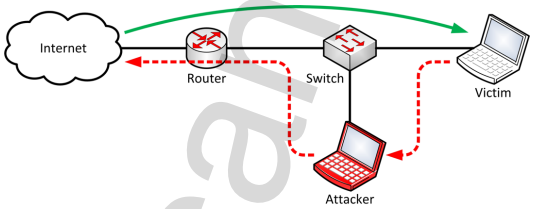
68

ARP poisoning

Le tabelle ARP si possono manipolare facilmente tramite pacchetti falsificati.
In questo caso si parla di **ARP poisoning** (dall'inglese "to poison" = avvelenare) o **ARP spoofing**, cioè di un attacco ***man in the middle*** che consente agli hacker di inserirsi senza farsi notare tra due sistemi comunicanti.

possibili contromisure:

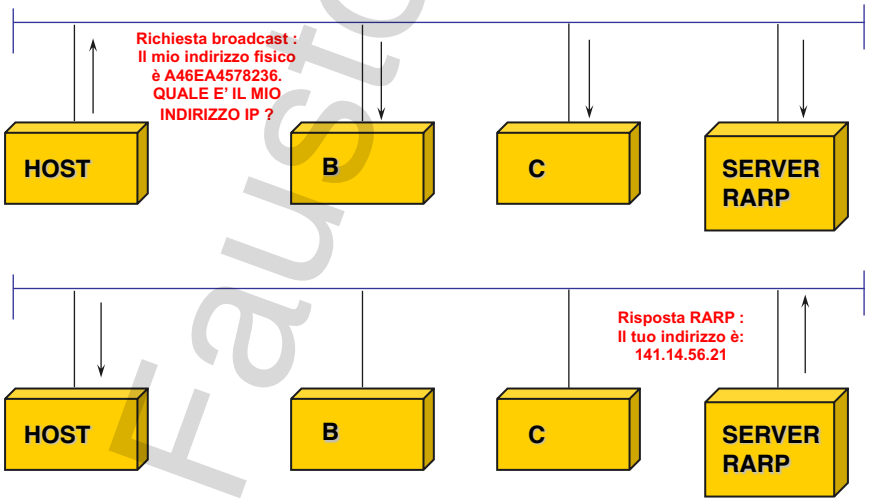
Arpwatch
XArp
ArpGuard



https://github.com/alandau/arpspoof
https://linuxsecurity.expert/security-tools/arp-poisoning-tools

69

Il protocollo RARP



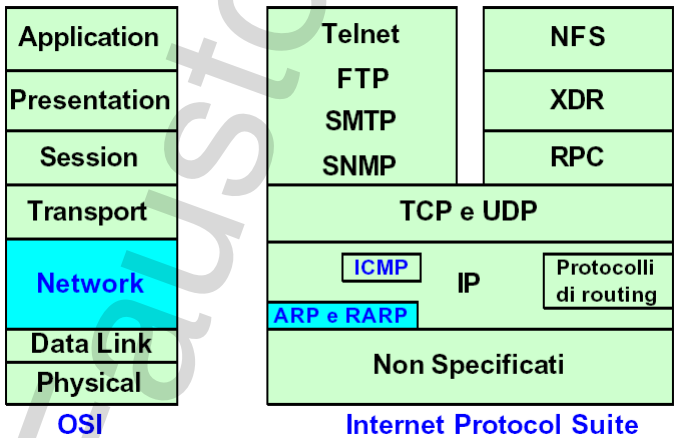
70

Operazioni del protocollo RARP

1. All'avvio del sistema un computer che non ha memoria permanente deve contattare un server per determinare il suo indirizzo IP
2. Si ricorre all'indirizzo fisico della macchina per individuarla univocamente
3. I server RARP della rete ricevono il messaggio
4. Cercano la corrispondenza in una tabella e rispondono al mittente
5. La macchina una volta ottenuto l'indirizzo IP non usa più RARP fino alla reinizializzazione

71

ARP & RARP



72

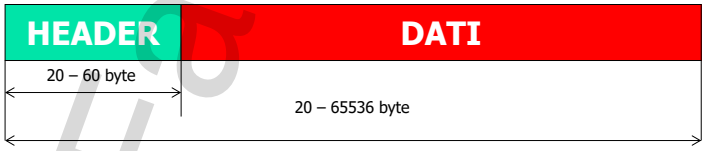
Il protocollo IP: funzionalità

Funzionalità del protocollo IP

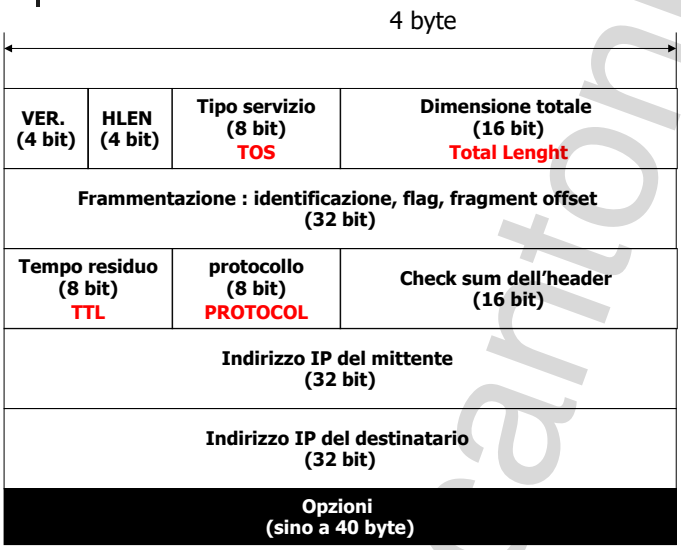
- Gestione indirizzi a 32 bit a livello di rete e di host
- Algoritmo di Forwarding
  - Routing: implementato in protocolli ad hoc
- Configurazione di classi di servizio
- Frammentazione e riassemblaggio dei pacchetti
- Funzionalità accessorie
  - Monitoring della comunicazione (ICMP Internet Control Message Protocol)
  - Interfaccia verso reti broadcast (ARP, RARP)
  - Gestione del traffico multicast (IGMP Internet Group Management Protocol)

Il protocollo IP: modello di trasporto

- Meccanismo di trasmissione di pacchetti (**datagrammi**) utilizzato dallo stack TCP/IP
  - Non affidabile
  - Best efforts
  - Senza connessioni (packet switching)



Protocollo IP - header



75

Protocollo IP - header

VER. (4 bit)	HLEN (4 bit)	Tipologia servizio (8 bit)	Dimensione totale (16 bit)

- VER Versione - Indica la versione del datagramma IP: per IPv4, ha valore 4.
- HLEN lunghezza dell'header
  - Espressa in **numero di parole** di 4 byte (0000=0 fino a 1111=15)
  - Varia a seconda delle opzioni da 5 (0101) (20 bytes) a 15 (1111) (60 bytes)
- Tipo di servizio: stabilisce come i router dovranno trattare il datagramma indicando una eventuale differenziazione del traffico
- Dimensione di header + dati
  - Risulta importante quando bisogna fare delle operazioni sul datagram
    - In ethernet i dati possono andare da 46 a 1500; se il datagram è < di 46 byte è necessario riempire la trama con informazioni di riempimento e quindi l'applicativo deve conoscere quanto sono grandi i dati

76

Reti di elaboratori

Protocollo IP - header

Tempo residuo (8 bit)	protocollo (8 bit)	Checksum dell'header (16 bit)

- Tempo residuo (Time To Live) → conta il numero di router attraversati dal datagramma
  - Per evitare che un pacchetto rimanga nella rete per sempre
  - Ogni router diminuisce di uno
  - Quando si arriva a zero il router rigetta il datagramma
- Protocollo → stabilisce a quale protocollo va consegnato il pacchetto (6 →TCP, 17 →UDP, ICMP, IGMP, OSPF etc..)
- Checksum → verifica che le informazioni dell'header non siano danneggiate durante il percorso

Reti di elaboratori

Protocollo IP – header - type of protocol

http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Decimal	Keyword	Protocol	IPv6 Extension Header	
0	HOPOPT	IPv6 Hop-by-Hop Option	Y	[RFC2460]
1	ICMP	Internet Control Message		[RFC792]
2	IGMP	Internet Group Management		[RFC1112]
3	GGP	Gateway-to-Gateway		[RFC823]
4	IPv4	IPv4 encapsulation		[RFC2003]
5	ST	Stream		[RFC1190][RFC1819]
6	TCP	Transmission Control		[RFC793]
7	CBT	CBT		[Tony_Ballardie]
8	EGP	Exterior Gateway Protocol		[RFC888][David_Mills]
9	IGP	any private interior gateway (used by Cisco for their IGRP)		[Internet_Assigned_Numbers_Authority]
10	BBN-RCC-MON	BBN RCC Monitoring		[Steve_Chipman]
11	NVP-II	Network Voice Protocol		[RFC741][Steve_Casner]
12	PUP	PUP		[Boggs, D., J. Shoch, E. Taft, and R. Metcalfe, "PUP: An Int also in IEEE Transactions on Communication, Volume COM-
13	ARGUS	ARGUS		[Robert_W_Scheifler]
14	EMCON	EMCON		[<mystery contact>]
15	XNET	Cross Net Debugger		[Haverty, J., "XNET Formats for Internet Protocol Version 4",
16	CHAOS	Chaos		[J_Noel_Chiappa]
17	UDP	User Datagram		[RFC768][Jon_Postel]
18	MUX	Multiplexing		[Cohen, D. and J. Postel, "Multiplexing Protocol", IEN 90, US
19	DCN-MEAS	DCN Measurement Subsystems		[David_Mills]
20	HMP	Host Monitoring		[RFC869][Bob_Hinden]
21	PRM	Packet Radio Measurement		[Zaw_Sing_Su]

Header Cecksum

- Questo campo controlla solamente la presenza di un errore nell'intestazione e non viene fatto alcun controllo sull'area dati, che è invece di pertinenza del protocollo di trasporto.
- Il controllo viene effettuato considerando **ogni due byte dell'header come un numero, sommando tutti i numeri** e ponendo il complemento a 1 della somma nel campo checksum (CRC).
- Questo meccanismo di calcolo facilita il controllo di integrità dal parte del ricevente del pacchetto in quanto basta sommare tutti i blocchi da 16 bits di cui è composto l'header IP (compresa la checksum):
  - se il risultato è composto da tutti 1, il pacchetto è stato ricevuto correttamente,
  - altrimenti c'è stato un errore.
- Questo controllo di parità permette solo di scoprire un errore, ma non di correggerlo.
- La scelta di un codice semplice (di tipo **parity check**) è dettata dal fatto che si cerca di mantenere la complessità ai bordi della rete, mentre controlli più sofisticati vengono fatti dagli end system attraverso i protocolli di livello superiore.
- **Questo campo viene ricalcolato ad ogni hop**

79

Frammentazione (1)

- Un datagramma può viaggiare su reti diverse
- Un router
  1. Estrae il datagramma dalla trama che dipende dalla rete dove ha viaggiato
  2. Legge il datagramma
  3. Lo inserisce nella nuova trama che dipende dalla rete fisica su cui sarà inviato

80

MTU per alcuni tipi di protocolli

Tipo di rete	MTU (byte)
Hyperchannel/link	65535
Token ring IBM (16mbps)	17914
Token ring IEEE 802.5 (4mbps)	4464
FDDI	4352
Ethernet	1500
X.25	576
Point to point (low delay)	296

81

Migliore MTU

Miglior MTU per Giocare Online
(PS4, PS5, Xbox One/X, Switch, Wii, 3DS)

"*Esistono video e articoli online che sostengono che abbassando manualmente il valore MTU ad un* ***valore specifico come 1473 o 1475 si può ridurre la latenza o il ping****. Alcune persone hanno anche affermato che l'abbassamento del valore MTU li ha aiutati ad* ***aggirare un'interruzione del Playsation Network alla fine del 2014****, consentendo loro di accedere alla Playstation Network laddove gli altri non potevano.*

L'idea alla base di tutto ciò è che i pacchetti più piccoli possono essere inviati più rapidamente a destinazione, il che significa una latenza potenzialmente inferiore. Purtroppo molti post e video del forum su questo argomento dipingono un quadro molto semplicistico, il che implica che se si modifica il valore MTU in un valore magico come 1473, la latenza si abbassa automaticamente per tutti coloro che lo provano. In realtà non è così semplice, come spiegheremo di seguito."

https://weakwifisolutions.com/miglior-mtu-per-giocare-online/

82

Verificare la propria MTU - Windows

netsh interface ipv4 show interfaces

```
C:\Users\fausto.mfausto>netsh interface ipv4  show inte

Idx     Met.         MTU          Stato                Nome
---  ----------  ----------  ------------  ---------------------------
  8           5        1500  disconnected  Ethernet
 26          55        1500  connected     Wi-Fi
 31          35        1500  connected     VMware Network Adapter VMnet1
  3          35        1500  connected     VMware Network Adapter VMnet8
  1          75  4294967295  connected     Loopback Pseudo-Interface 1
 21          25        1500  connected     Npcap Loopback Adapter
 12          25        1500  disconnected  Connessione alla rete locale (LAN)* 4
```


Verificare la propria MTU - Linux

ifconfig

```
root@pen-test:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 193.204.15.114  netmask 255.255.255.0  broadcast 193.204.15.255
        inet6 fe80::20c:29ff:fe69:46ac  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:69:46:ac  txqueuelen 1000  (Ethernet)
        RX packets 238  bytes 21620 (21.1 KiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 26  bytes 2880 (2.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 1022  bytes 61298 (59.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1022  bytes 61298 (59.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@pen-test:~#
```

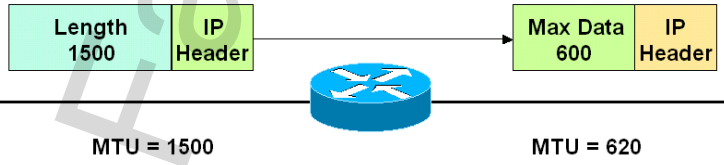
Frammentazione (2)

- Per rendere IP indipendente dalle reti fisiche il datagramma ha dimensione 65535 bytes pari al massimo MTU utilizzato
- Se il protocollo di collegamento ha MTU più piccolo si deve procedere alla frammentazione (suddivisione in unità più piccole)
- Il datagramma può essere frammentato dall'host mittente oppure da un router incontrato lungo il cammino
- Il riassemblaggio viene fatto sempre e soltanto dall'host destinatario
- I campi che vengono modificati sono la dimensione totale, flag ed offset di frammentazione

85

Frammentazione : schema riassuntivo

- **Tecnologie di rete di livello 1-2**
  - **Definiscono normalmente un pacchetto massimo trasportabile (Maximum Trasport Unit)**
    - **Ethernet v.2.0: 1500 bytes**
  - **Solitamente non supportano la frammentazione**
    - **Ethernet non prevede campi per questo scopo**
- **Frammentazione**
  - **Può essere necessaria quando un pacchetto deve venire inoltrato su una rete con MTU inferiore**



86

Campi di frammentazione

Identificazione	16 bit	Individua univocamente il frammento Tutti i frammenti hanno lo stesso ID number
Flag	3 bit	Primo bit riservato Secondo bit = 1 non si può frammentare (messaggio di errore ICMP) Terzo bit = 0 frammento è l'ultimo del datagramma o il solo
Offset di frammentazione	13 bit	Fornisce la posizione del frammento nel datagramma originario **misurata in unità di 8 byte**. (La dimensione del payload di ogni frammento è un multiplo di 8 byte)

87

13 bit di offset della frammentazione in wireshark

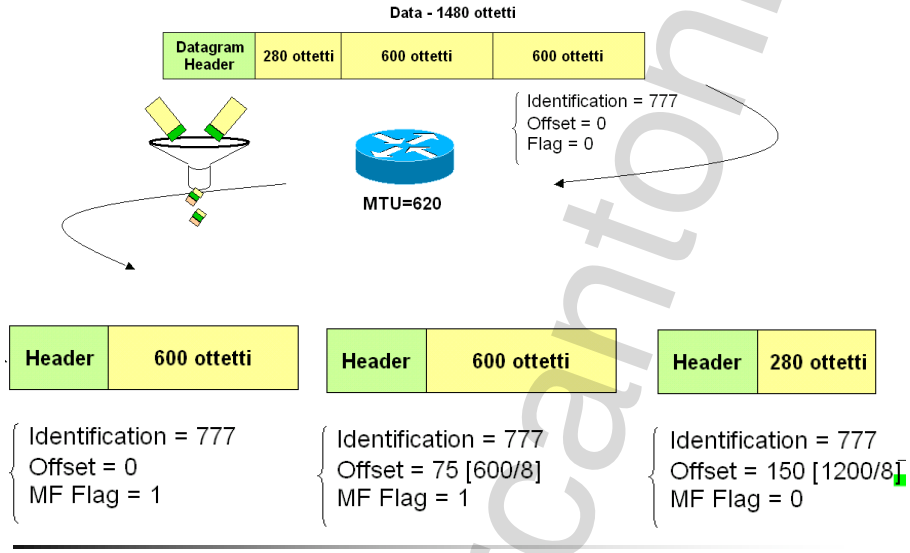
```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1500
  Identification: 0x622b (25131)
v 001. .... = Flags: 0x1, More fragments
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
  ...0 0000 1011 1001 = Fragment Offset: 1480
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0x0a20 [validation disabled]
```

0 0000 1011 10001 = 185 → 185*8=1480

13 bit offset

88

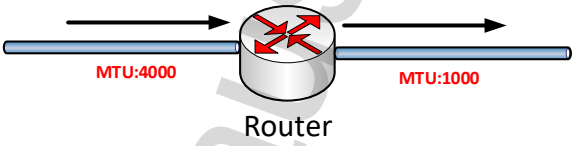
Esempio frammentazione



89

Esempio frammentazione

Un datagramma da 2600 byte deve essere instradato
da una rete con MTU 4000 su una rete con MTU 1000



Header length = 20 Totale length = 2600 ID=0x1c24 DF flag = 0 MF flag = 0 Fragment offset = 0	Header length = 20 Totale length = 628 ID=0x1c24 DF flag = 0 MF flag = 0 Fragment offset = 224	Header length = 20 Totale length = 976 ID=0x1c24 DF flag = 0 MF flag = 1 Fragment offset = 122	Header length = 20 Totale length = 976 ID=0x1c24 DF flag = 0 MF flag = 1 Fragment offset = 0

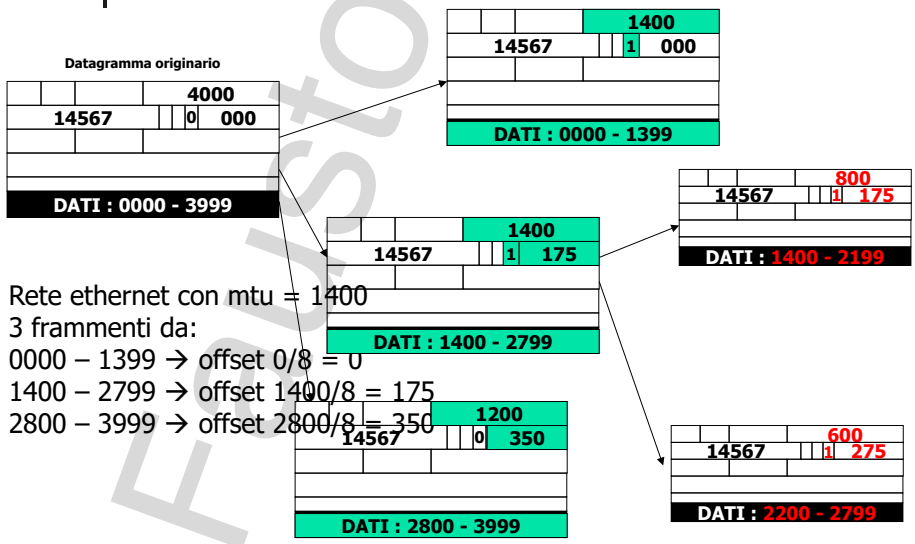
90

Frammentazione

- Tutti i frammenti (tranne l'ultimo) hanno un payload di **dimensione multipla di 8 byte**
- Essendo la dimensione massima di un datagramma 65535 byte, ci possono essere al massimo 65536/8 cioè 8192 frammenti per ogni datagramma
- La posizione del payload di un frammento rispetto al payload del pacchetto originario è espressa mediante un **offset** (spiazzamento) di **13 bit**

91

Esempio di frammentazione



Rete ethernet con mtu = 1400
3 frammenti da:
0000 – 1399 → offset 0/8 = 0
1400 – 2799 → offset 1400/8 = 175
2800 – 3999 → offset 2800/8 = 350

92

Esercizio

Un pacchetto IP di 5265 byte deve attraversare un link avente MaximumTransfer Unit (MTU) pari a 1500 bytes. Come verrà frammentato?

Sequence	Identifier	Total Length	DF May/Don't	MF Last/More	Fragment Offset
0	126	5265	0	0	0

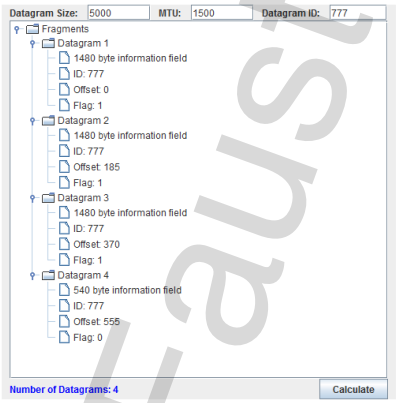
Sequence	Identifier	Payload Length	DF May/Don't	MF Last/More	Fragment Offset
0	126	1480	0	1	0
1	126	1480	0	1	185
2	126	1480	0	1	370
3	126	805	0	0	555

93

Frammentazione

IP Fragmentation

Note: Datagram size includes an IP header of 20 bytes.
MTU and Datagram size must be greater than 30, and all values must be less than 2^16 - 1 (65535).



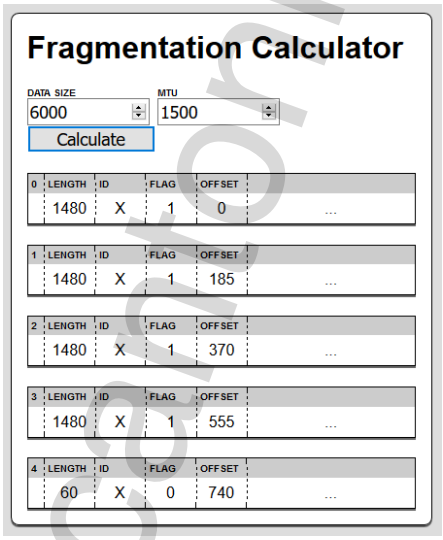
Non funziona più

http://wps.pearsoned.it/ema_it_aw_kurose_network_3/39/9996/2559052.cw/content/index.html

94

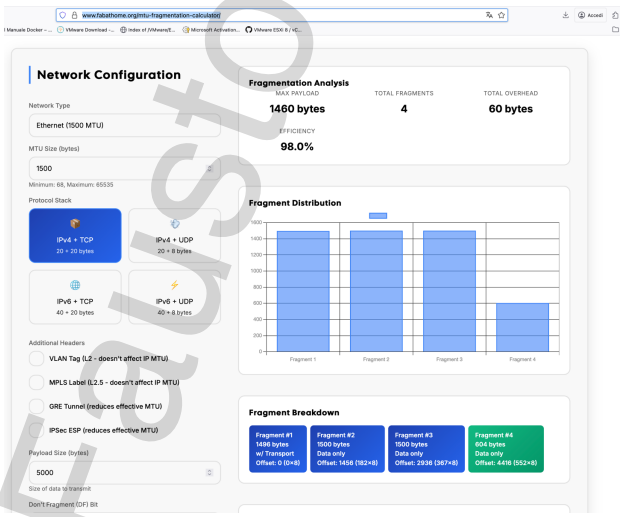
Frammentazione

http://fixmycode.github.io/IPFCalc/



95

Frammentazione



https://www.fabathome.org/mtu-fragmentation-calculator/

96

Frammentazione: problematiche

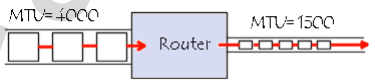
- In generale sconsigliata
  - Maggiore overhead di trasmissione
    - La perdita di un frammento invalida tutto il pacchetto
    - Maggior numero di bytes per gli headers
  - Impegna risorse (timer, buffer) nell'host ricevente
  - Possibili attacchi di tipo denial of service
    - Invio di molti frammenti "singoli": il TCP/IP alloca risorse aspettando l'arrivo dei frammenti rimanenti
- Soluzioni
  - Esistono metodi per determinare la MTU più piccola esistente sul percorso (ping -f -l 1472 193.205.92.2) verificare con wireshark
  - Ormai quasi tutti supportano MTU pari a 1500 bytes
- Funzionalità tolta in IPv6

97

Frammentazione: problematiche

NEXT HOP ROUTER ?

- Il pacchetto può percorrere delle reti che supportano MTU più grandi
  - La frammentazione non sarebbe più necessaria
- Minore overhead:
  - Banda (headers)
  - CPU (numero di pacchetti inoltrati)
- Si evita la perdita di singoli frammenti
  - Singoli frammenti persi invalidano comunque tutto il pacchetto



98

Frammentazione: problematiche

Host di destinazione ?

- **Complessità ai bordi**
  - **Non è necessario complicare i router per fargli gestire il riassemblaggio**
- **È semplice gestire il fatto per cui pacchetti diversi fanno percorsi diversi**

99

Ricostruzione datagramma

- Il primo frammento ha offset = 0
- Il secondo frammento ha offset = alla dimensione del primo / 8
- Il terzo frammento ha offset uguale alla dimensione complessiva del primo + il secondo / 8
- Si prosegue in questo modo sino ad incontrare il frammento con flag = 0

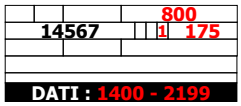
Ordine di arrivo dei frammenti:

1 - 2 - 3 - 4

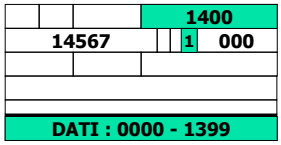
Ordine di riassemblaggio

2 - 1 - 4 -3

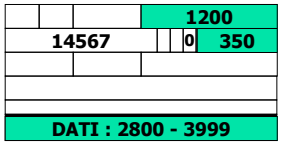
1



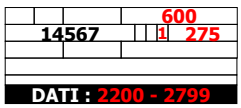
2



3



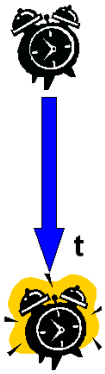
4



100

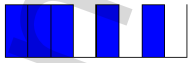
Riassemblaggio

- TCP/IP: deframmentazione riservata al nodo destinatario del pacchetto (end node)



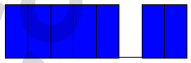
alla ricezione del primo frammento l'end node fa partire un reassembly timer

memorizza tutti i frammenti in un buffer



t

se allo scadere del timer il pacchetto non è completo segnala un errore



101

Campi modificabili al transito:

- TTL
- Header Checksum
- Flags (nel caso di frammentazione)
- Fragment Offset (nel caso di frammentazione)
- Total Length
- Options

102

Frammentazione: esercizio

Utilizzando l'analizzatore di rete, verificare:

Windows

ping -l 2000 193.205.92.2

-l 2000 pacchetto grande 2000 byte

ping -f -l 2000 193.205.92.2

-f NON frammentare

ping -l 4433 193.205.92.2

quanti frammenti ???

MasOs

ping -s 2000 193.205.92.2

ping -D -s 2000 193.205.92.2

-D NON frammentare

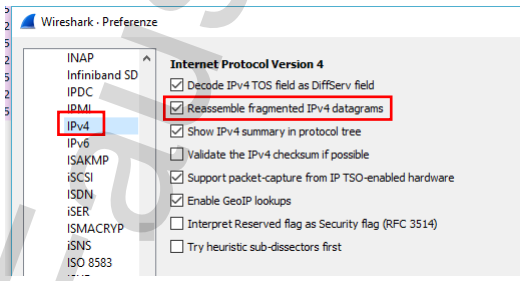
103

Wireshark → frammentazione

One Answer: oldest newest most voted

1 That happens because your Wireshark is doing IPv4 datagram reassembly, which means that it gathers all datagrams and displays them in a reassembled order.

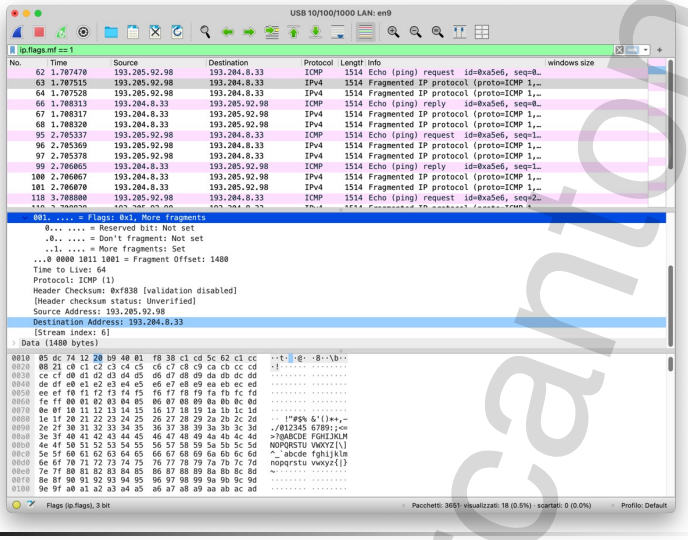
To see the "real" packets you can turn that feature off. Go to Edit -> Preferences -> Protocols -> IPv4 and deselect "Reassemble fragmented IPv4 datagrams" (or something similar; these captions change sometimes depending on your version of Wireshark).



104

Frammentazione: esercizio

ip.flags.mf == 1 or ip.frag_offset > 0



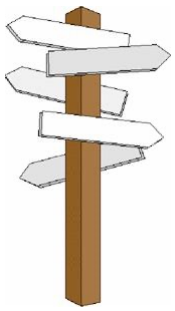
105

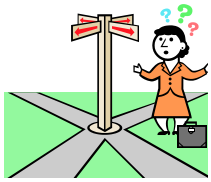
IP: Internet Protocol

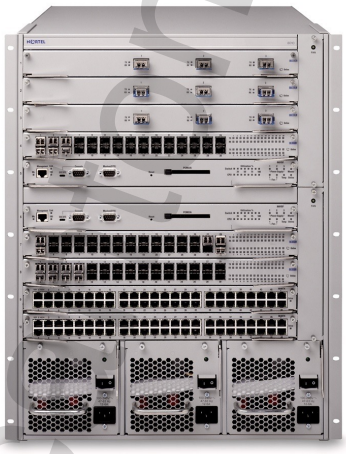
- È il livello Network di TCP/IP
- Offre un servizio non connesso
- Semplice protocollo di tipo Datagram
- Un protocollo datato … …
- ma non obsoleto
- *Oggi: IPv4*
- *Domani: IPv6*

106

Instradamento







107

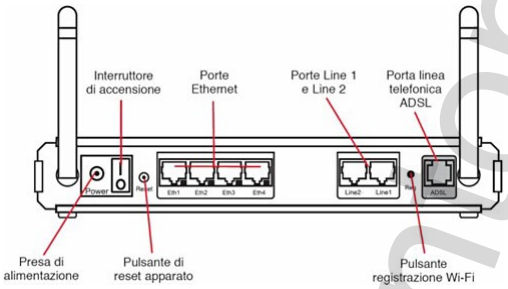
Il router

Nella tecnologia delle reti informatiche un router, in inglese letteralmente instradatore, ***è un dispositivo di rete che si occupa di instradare pacchetti tra reti diverse ed eterogenee***.

Un Router lavora al livello 3 (rete) del modello OSI, ed è quindi in grado di interconnettere reti di livello 2 eterogenee, come ad esempio una LAN ethernet con un collegamento geografico in tecnologia frame relay, CDM, ATM, ADSL, …

108

Il router "casalingo"



Quante reti ????

109

Inoltro - Instradamento

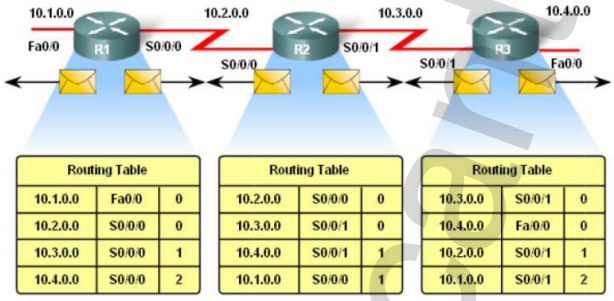
inoltro (forwarding) e **instradamento** (routing)

- ✓ Tecnica di inoltro:
  - definisce le regole con le quali un pacchetto viene inoltrato verso l'uscita (normalmente sulla base della lettura di una tabella di instradamento)
- ✓ Algoritmo di instradamento:
  - definisce le regole con le quali viene scelto un percorso in rete tra sorgente e destinazione (sulla base delle quali vengono scritte le tabelle di instradamento)
- ✓ Protocollo di instradamento:
  - definisce i messaggi che si scambiano i nodi di rete per implementare l'algoritmo di instradamento

110

tabella di routing - tabella di instradamento

tabella di routing - **tabella di instradamento**
è un database, memorizzato in un router o in un host, che elenca le **rotte di destinazione** di una data rete e in molti casi **una metrica** di tale rotta



metrica

Una metrica è un valore assegnato a una route IP per una determinata interfaccia di rete.
Identifica il **costo associato all'utilizzo di tale route**.
Ad esempio, la metrica può essere calcolata in termini di

- **velocità del collegamento**
- **numero di hop**
- **ritardo temporale**

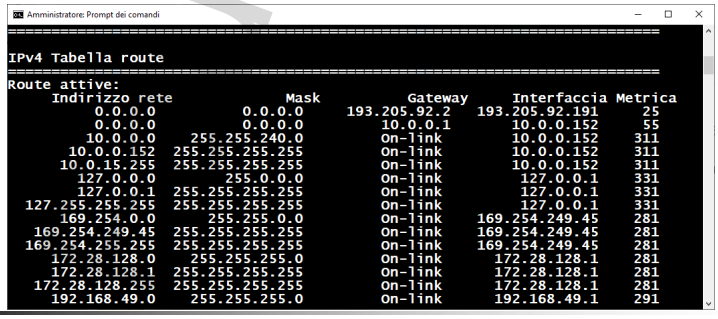


Tabella di instradamento

Nelle **tabelle di instradamento** è elencato per ciascuna sottorete
- **il relativo netID**
- **l'indirizzo del router di inoltro**

Una tabella di instradamento **è un insieme di righe** che contiene i seguenti quattro indirizzi:
- ✓ **Indirizzo della rete di destinazione**
- ✓ **Maschera di rete**
- ✓ **Interfaccia su cui inoltrare**
- ✓ **Indirizzo del next hop**

Ad ogni percorso è associato il **costo/metrica** per raggiungere la destinazione

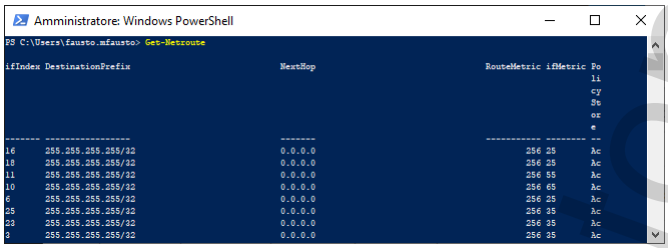
route print

```
Amministratore: Prompt dei comandi
Microsoft Windows [Versione 10.0.19043.1348]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\fausto.mfausto>route print
===========================================================================
Elenco interfacce
 26...0a 00 27 00 00 1a ......VirtualBox Host-Only Ethernet Adapter
  6...d8 50 e6 0a e6 1d ......Realtek PCIe GbE Family Controller
  4...0a 00 27 00 00 04 ......VirtualBox Host-Only Ethernet Adapter #3
 12...0a 00 27 00 00 0c ......VirtualBox Host-Only Ethernet Adapter #2
 18...16 0a 64 43 53 23 ......Microsoft Wi-Fi Direct Virtual Adapter
 16...26 0a 64 43 53 23 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  3...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 23...00 50 56 c0 00 03 ......VMware Virtual Ethernet Adapter for VMnet3
 25...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 11...24 0a 64 43 53 23 ......Qualcomm Atheros AR9485WB-EG Wireless Network Adapter
 10...24 0a 64 43 53 22 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete          Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0    193.205.92.2   193.205.92.191     25
          0.0.0.0          0.0.0.0       10.0.0.1        10.0.0.83     55
         10.0.0.0    255.255.240.0         On-link        10.0.0.83    311
        10.0.0.83  255.255.255.255         On-link        10.0.0.83    311
     10.0.15.255  255.255.255.255         On-link        10.0.0.83    311
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      169.254.0.0        255.255.0.0         On-link    169.254.249.45    281
    169.254.249.45  255.255.255.255         On-link    169.254.249.45    281
  169.254.255.255  255.255.255.255         On-link    169.254.249.45    281
      172.28.128.0    255.255.255.0         On-link      172.28.128.1    281
      172.28.128.1  255.255.255.255         On-link      172.28.128.1    281
    172.28.128.255  255.255.255.255         On-link      172.28.128.1    281
      192.168.49.0    255.255.255.0         On-link      192.168.49.1    291
      192.168.49.1  255.255.255.255         On-link      192.168.49.1    291
    192.168.49.255  255.255.255.255         On-link      192.168.49.1    291
      192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
      192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
    192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
```

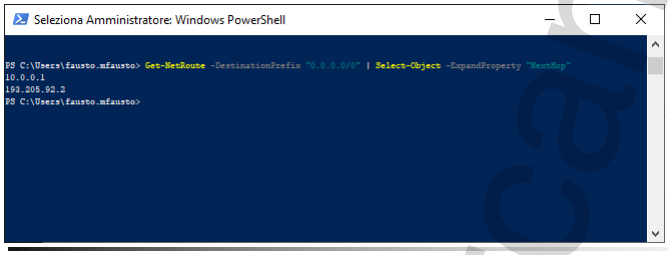
Indirizzo della rete di destinazione
Maschera di rete
Indirizzo del next hop
Interfaccia su cui inoltrare

Powershell - Get-NetRoute

```
Get-NetRoute
```




```
Get-NetRoute -DestinationPrefix "0.0.0.0/0" | Select-Object -ExpandProperty "NextHop"
```



115

Instradamento (Forwarding)

Instradamento (Forwarding)

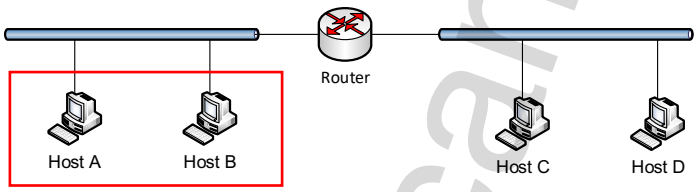
- Operazione comune a tutte le macchine con stack TCP/IP
  - router
  - end systems
- Il procedimento si applica:
  - se l'host in esame è il mittente del pacchetto
  - router intermedio sul percorso verso la destinazione

116

Reti di elaboratori

Instradamento diretto o indiretto

- DIRETTO
  - **Tra hosts nella stessa net**
  - **L'instradamento coinvolge solo i livelli 1 e 2 (a parte eventuali ARP request)**
  - **Hosts identificati tramite l'HW address**
    - **Indirizzi MAC sulle LAN**
    - **Indirizzi di DTE in X.25**
    - **Identificatori DLCI in Frame Relay**
    - **……**

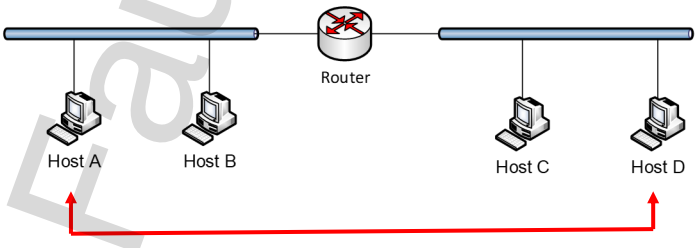


117

Reti di elaboratori

Instradamento diretto o indiretto

- INDIRETTO
  - **Tra hosts in net diverse**
  - **L'instradamento coinvolge i livelli 1 , 2 e 3**
  - **Hosts identificati tramite l'IP address**
  - **Gli host devono conoscere almeno un router presente sulla loro rete fisica**



118

Instradamento diretto o indiretto

Domanda fondamentale:

la destinazione appartiene alla mia stessa rete IP?

119

Network Prefix Match

```
10.1.1.1          00001010.00000001.00000001.00000001
                                                    AND
255.255.255.0     11111111.11111111.11111111.00000000
-------------------------------------------------------
10.1.1.0          00001010.00000001.00000001.00000000 network
```

IP host con pacchetto da inoltrare

Destinatario 1

```
10.1.1.2          00001010.00000001.00000001.00000010
                                                    AND
255.255.255.0     11111111.11111111.11111111.00000000
-------------------------------------------------------
10.1.1.0          00001010.00000001.00000001.00000000 network
```

Appartiene alla stessa rete instradamento diretto

Destinatario 2

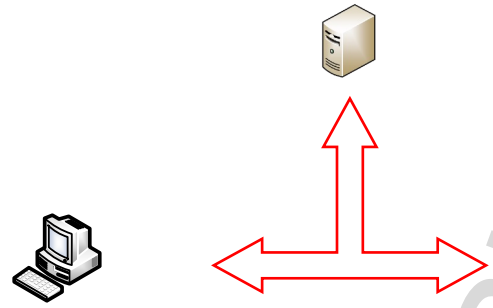
```
10.2.1.4          00001010.00000010.00000001.00000100
                                                    AND
255.255.255.0     11111111.11111111.11111111.00000000
-------------------------------------------------------
10.2.1.0          00001010.00000010.00000001.00000000 network
```

Appartiene alla stessa rete instradamento indiretto

120

Network Prefix Match

```
Address:   10.1.1.1          00001010.00000001.0000 0001.00000001
Netmask:   255.255.240.0     11111111.11111111.1111 0000.00000000
Network:   10.1.0.0/20       00001010.00000001.0000 0000.00000000
```



10.1.12.36
255.255.240.0

10.1.17.42
255.255.240.0

121

Network Prefix Match

```
Address:   10.1.1.1          00001010.00000001.0000 0001.00000001
Netmask:   255.255.240.0     11111111.11111111.1111 0000.00000000
Network:   10.1.0.0/20       00001010.00000001.0000 0000.00000000
```

Indirizzamento diretto

```
Address:   10.1.12.36        00001010.00000001.0000 1100.00100100
Netmask:   255.255.240.0 = 20 11111111.11111111.1111 0000.00000000
Network:   10.1.0.0/20       00001010.00000001.0000 0000.00000000
```


122

Reti di elaboratori

Network Prefix Match

```
Address:   10.1.1.1          00001010.00000001.0000 0001.00000001
Netmask:   255.255.240.0     11111111.11111111.1111 0000.00000000
Network:   10.1.0.0/20       00001010.00000001.0000 0000.00000000
```

Indirizzamento indiretto

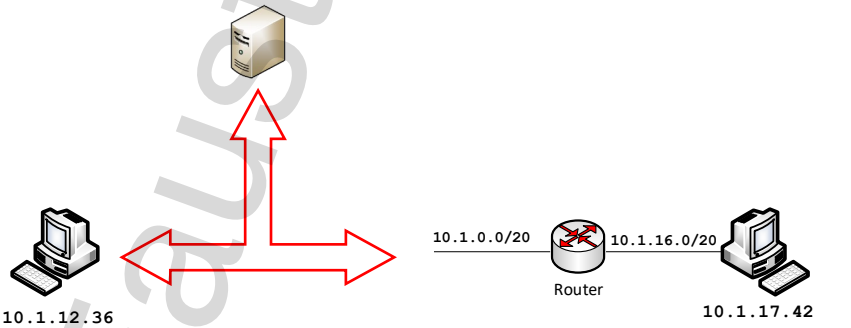
```
Address:   10.1.17.42        00001010.00000001.0001 0001.00101010
Netmask:   255.255.240.0 = 20 11111111.11111111.1111 0000.00000000
Network:   10.1.16.0/20      00001010.00000001.0001 0000.00000000
```


123

Reti di elaboratori

Network Prefix Match

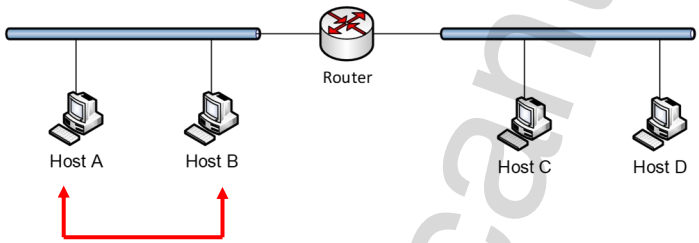
```
Address:   10.1.1.1          00001010.00000001.0000 0001.00000001
Netmask:   255.255.240.0     11111111.11111111.1111 0000.00000000
Network:   10.1.0.0/20       00001010.00000001.0000 0000.00000000
```



124

Instradamento diretto

MAC_source	MAC address "A"
MAC_destination	MAC address "B"
IP_source	IP address "A"
IP_destination	IP address "B"
DATI	

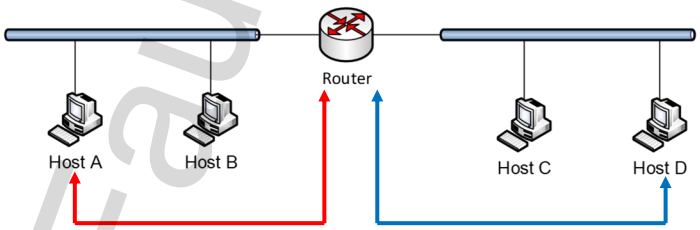


125

Instradamento indiretto

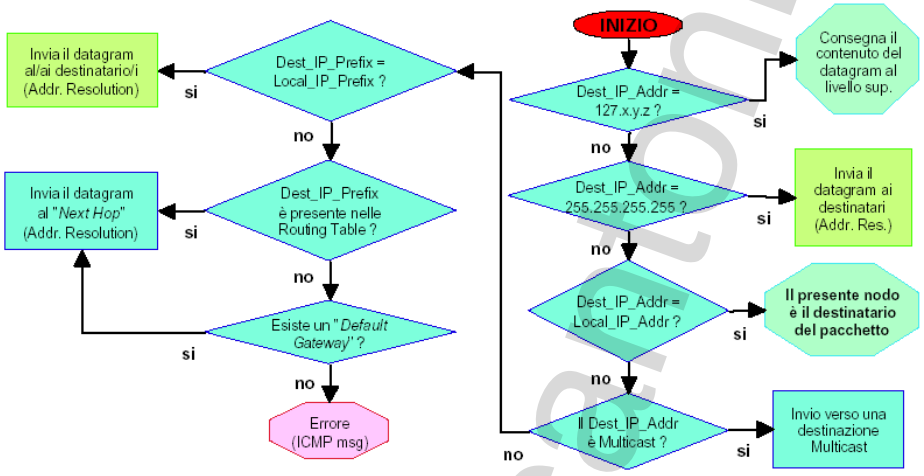
MAC_source	MAC address "A"
MAC_destination	MAC address "R"
IP_source	IP address "A"
IP_destination	IP address "R"
DATI	

MAC_source	MAC address "R"
MAC_destination	MAC address "D"
IP_source	IP address "R"
IP_destination	IP address "D"
DATI	



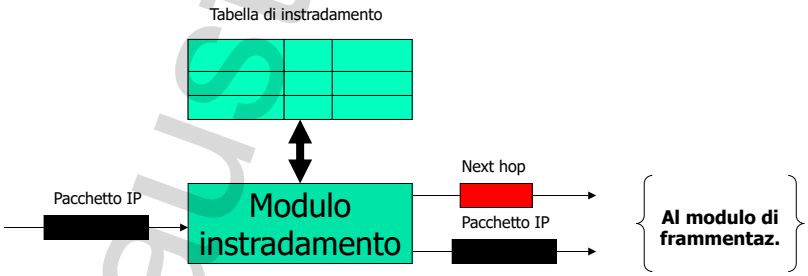
126

Algoritmo di instradamento



127

Modulo di instradamento



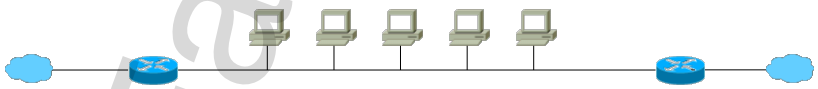
128

Tabella di instradamento

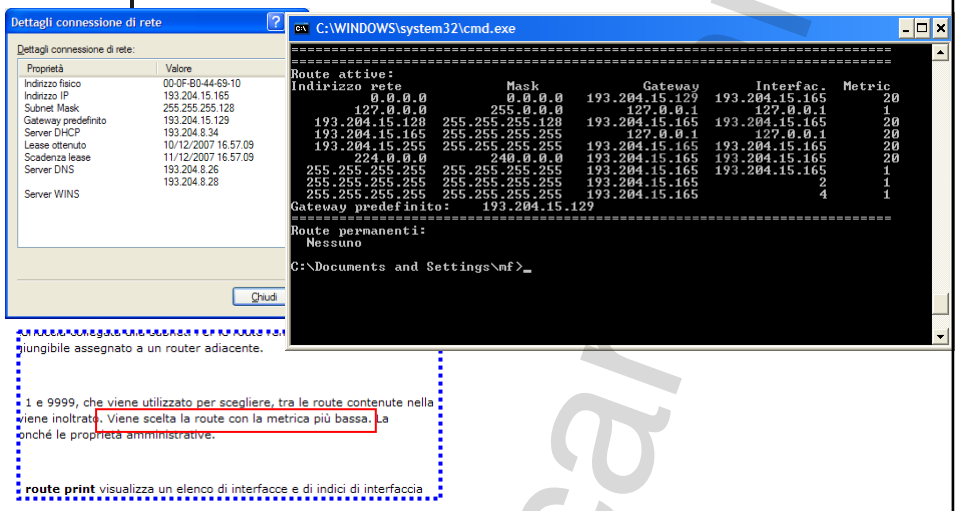
- Presente (obbligatoria) in tutti gli host IP
  - Più sviluppata sui routers
- Elenco di coppie:
  - Destinazioni raggiungibili dall'host
  - Next hop router "migliore"
  - Es: *da Torino a Napoli è necessario passare per Roma*
- Informazione aggiuntiva: costo
  - Discrimina tra percorsi alternativi verso una stessa destinazione

Next Hop

- Deve essere obbligatoriamente un indirizzo direttamente raggiungibile
- Percorsi asimmetrici
  - Normali nel mondo TCP/IP
  - Il next hop è configurato in una sola direzione
  - la direzione opposta può scegliere un altro percorso



Il comando "route"



https://technet.microsoft.com/it-it/windows-server-docs/management/windows-commands/route_ws2008

131

Il comando "route" – 2 reti → eth - eth

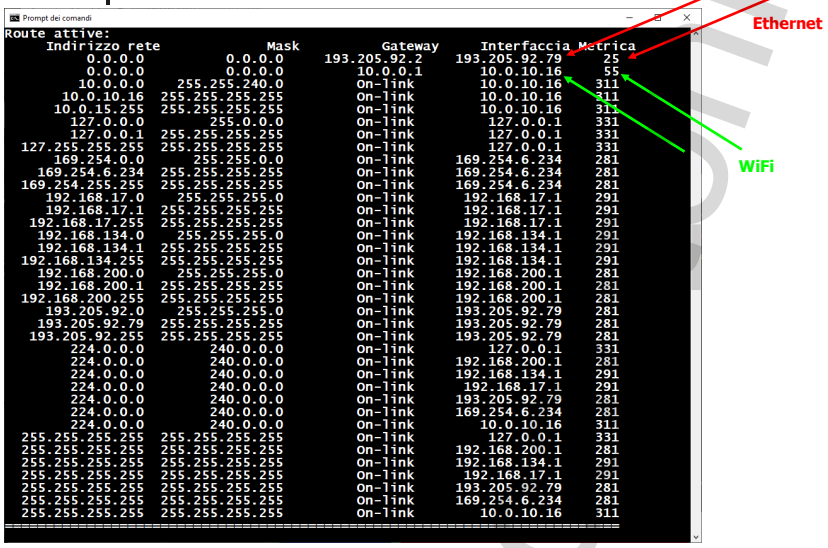
```
IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete            Mask          Gateway       Interfaccia Metrica
          0.0.0.0          0.0.0.0    193.205.92.2   193.205.92.113     20
          0.0.0.0          0.0.0.0     90.147.12.2     90.147.12.92     25
       90.147.12.0    255.255.254.0         On-link     90.147.12.92    281
     90.147.12.92  255.255.255.255         On-link     90.147.12.92    281
     90.147.13.255  255.255.255.255         On-link     90.147.12.92    281
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    306
      169.254.0.0      255.255.0.0         On-link    169.254.144.31    276
      169.254.0.0      255.255.0.0         On-link    169.254.51.123    276
  169.254.51.123  255.255.255.255         On-link    169.254.51.123    276
  169.254.144.31  255.255.255.255         On-link    169.254.144.31    276
  169.254.255.255  255.255.255.255         On-link    169.254.144.31    276
  169.254.255.255  255.255.255.255         On-link    169.254.51.123    276
     193.205.92.0    255.255.255.0         On-link    193.205.92.113    276
   193.205.92.113  255.255.255.255         On-link    193.205.92.113    276
   193.205.92.255  255.255.255.255         On-link    193.205.92.113    276
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    193.205.92.113    276
        224.0.0.0        240.0.0.0         On-link    169.254.51.123    276
        224.0.0.0        240.0.0.0         On-link    169.254.144.31    276
        224.0.0.0        240.0.0.0         On-link     90.147.12.92     281
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    193.205.92.113    276
  255.255.255.255  255.255.255.255         On-link    169.254.51.123    276
  255.255.255.255  255.255.255.255         On-link    169.254.144.31    276
  255.255.255.255  255.255.255.255         On-link     90.147.12.92     281
===========================================================================
Route permanenti:
  Nessuna
```

Ethernet

Ethernet

132

Il comando "route" – 2 reti → eth - wifi



133

ip route show

```
faustomarcantoni@MacBook-Pro-di-Fausto ~ % ip route show
default via 193.205.92.2 dev en9
127.0.0.0/8 via 127.0.0.1 dev lo0
127.0.0.1/32 via 127.0.0.1 dev lo0
169.254.0.0/16 dev en9 scope link
193.205.92.0/24 dev en9 scope link
193.205.92.2/32 dev en9 scope link
193.205.92.79/32 dev en9 scope link
224.0.0.0/4 dev en9 scope link
255.255.255.255/32 dev en9 scope link
faustomarcantoni@MacBook-Pro-di-Fausto ~ %
```

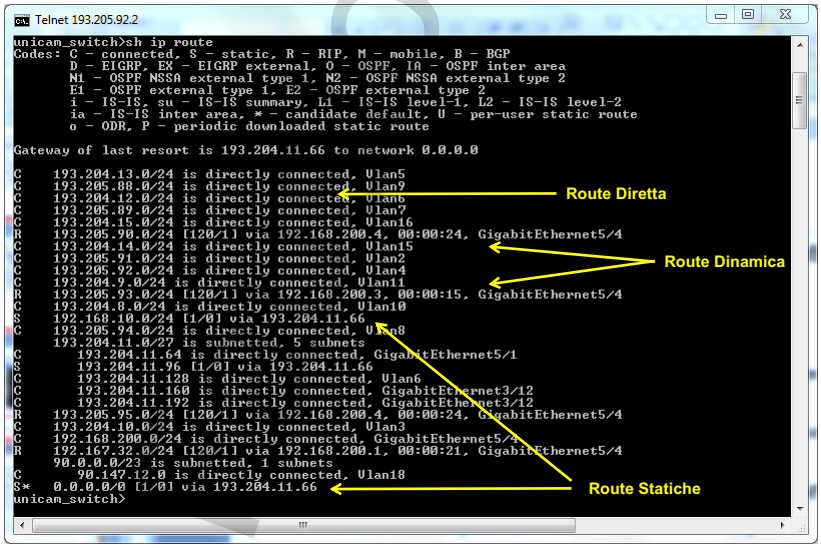

134

Tipologie di informazioni

- Informazioni nella tabella di instradamento
  - Route Diretta
    - address range corrispondenti alle interfacce del router
  - Route Statiche
    - route configurate staticamente dal gestore/amministratore
  - Route Dinamica
    - address range appresi attraverso un 'protocollo di routing'
    - route apprese attraverso ICMP redirect
- Route per uno stesso address range appresa da diverse fonti (es. Dinamica + Statica)
  - Deve essere specificato quale deve essere preferita
- Default route presente sugli end-systems e gran parte dei routers

135

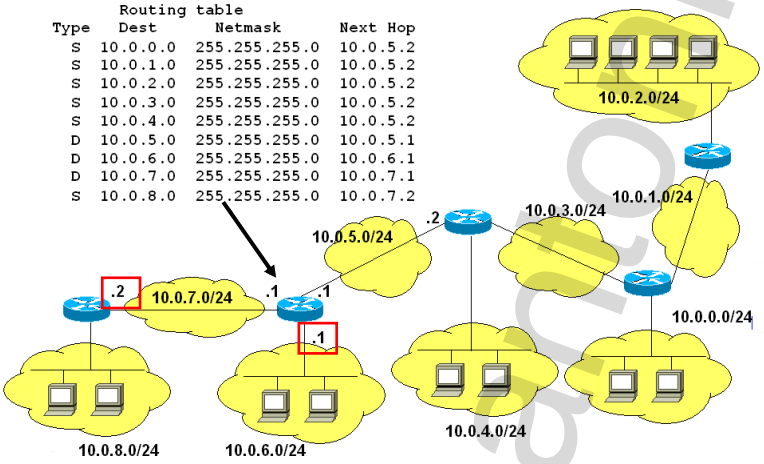
Tabella di routing



136

Tabella di instradamento di un router

```
Routing table
Type   Dest        Netmask         Next Hop
  S  10.0.0.0   255.255.255.0   10.0.5.2
  S  10.0.1.0   255.255.255.0   10.0.5.2
  S  10.0.2.0   255.255.255.0   10.0.5.2
  S  10.0.3.0   255.255.255.0   10.0.5.2
  S  10.0.4.0   255.255.255.0   10.0.5.2
  D  10.0.5.0   255.255.255.0   10.0.5.1
  D  10.0.6.0   255.255.255.0   10.0.6.1
  D  10.0.7.0   255.255.255.0   10.0.7.1
  S  10.0.8.0   255.255.255.0   10.0.7.2
```



Le interfacce dei router appartengono alla rete

137

Composizione della tabella di instradamento

Mask	Indirizzo destinatario	Indirizzo next-hop	Flag	Reference count	Uso	Interfaccia
255.0.0.0	124.0.0.0	145.6.7.23	UG	4	20	M2
.....	.....	.....	.....	.....	.....	.....

Per il processo di messa in AND
Nell'instradamento di default ed in quello di host specifico il mask è 255.255.255.255

Numero utenti che stanno usando il percorso

Contiene cinque switch on/off
U → router attivo
G → destinatario su altra rete
H→ Host specifico
.....

Numero pacchetti trasmessi al destinatario

Nome dell'interfaccia

138

tabella di instradamento

La tabella di instradamento è composta da almeno tre campi di informazioni:

identificatore di rete: la sottorete di destinazione e la maschera di rete
metrica: la metrica di instradamento del percorso attraverso il quale deve essere inviato il pacchetto. Il percorso andrà in direzione del gateway con la metrica più bassa.
hop successivo: il prossimo hop, o gateway, è l'indirizzo della stazione successiva a cui il pacchetto deve essere inviato sulla strada per la sua destinazione finale

A seconda dell'applicazione e dell'implementazione, può anche contenere valori aggiuntivi che perfezionano la selezione del percorso:

qualità del servizio: associato al percorso. Ad esempio, il flag U indica che una route IP è attiva.
criteri di filtraggio: elenchi di controllo di accesso elenchi associati al percorso
interfaccia: come eth0 per la prima scheda Ethernet, eth1 per la seconda scheda Ethernet, ecc.

tabella di instradamento

Campo	Descrizione
Destination	Rete o host di destinazione (es. 192.168.1.0/24 o default)
Gateway	Indirizzo IP del router o gateway da usare per raggiungere la destinazione
Genmask / Netmask	Maschera di sottorete che definisce la dimensione della rete
Flags	Indicatori sul tipo di rotta (es. U = Up, G = Gateway, H = Host, S = Static)
Refs	Numero di riferimenti (quante volte la rotta è stata usata)
Use	Numero di pacchetti inviati tramite questa rotta
Iface / Netif	Interfaccia di rete utilizzata (es. en0, en1)
Metric	Priorità della rotta (valore più basso = rotta preferita)

Flags della tabella di instradamento

Flag	Significato	Descrizione
U	*Up*	La rotta è attiva e utilizzabile.
G	*Gateway*	La rotta passa attraverso un gateway (non è direttamente connessa).
H	*Host*	La rotta è verso un singolo host, non verso una rete.
S	*Static*	La rotta è stata aggiunta manualmente e non è dinamica.
C	*Cloning*	Indica che la rotta può generare voci derivate (tipico dell'ARP).
L	*Link-local*	Rotta verso un indirizzo link-local (es. 169.254.x.x).
W	*WasCloned*	La rotta è stata clonata dinamicamente.
R	*Reject*	I pacchetti per questa rotta vengono scartati.
B	*Broadcast*	Rotta verso un indirizzo broadcast.
D	*Dynamic*	Rotta appresa dinamicamente (es. da un protocollo di routing).
M	*Modified*	Rotta modificata da un redirect ICMP.
X	*Blackhole*	I pacchetti vengono scartati senza inviare messaggi di errore.

141

Metriche

Due parametri (**metriche**) universalmente accettati sono:

Hops: numero di salti effettuati, cioè il numero di router attraversati lungo il cammino

Costo: somma dei costi di tutte le linee attraversate; il costo di una linea è inversamente proporzionale alla sua velocità (banda trasmissiva, tipo e affidabilità del mezzo trasmissivo, lunghezza del percorso, traffico di rete,....)

142

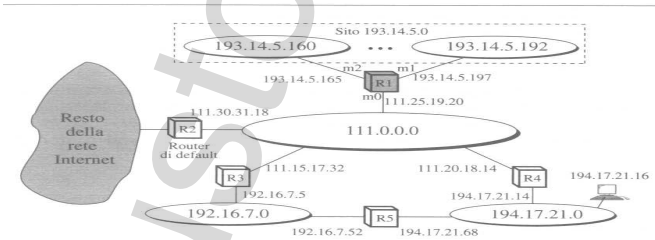
ricerca nella tabella

La ricerca nella tabella avviene utilizzando:
- l'indirizzo IP di destinazione del datagramma
- l'indirizzo IP di destinazione e la netmask specificati in ciascuna riga della tabella

Procedura:
- il controllo viene effettuato a partire dalla riga che presenta **una netmask con un numero maggiore di bit a uno**: priorità alle route più specifiche (prima host, poi reti piccole, poi reti grandi: ***longest-prefix match***)
- si esegue un'operazione di AND bit per bit tra l'indirizzo di destinazione del datagramma e **la netmask** di ciascuna riga.
- il risultato viene confrontato con la destinazione specificata nella riga stessa:
  - ✓ se coincidono, la riga è quella giusta
  - ✓ altrimenti continuo con la successiva
- una volta trovata la riga corrispondente, il lookup si ferma e il datagramma viene instradato secondo la modalità specificata
- se nessuna riga corrisponde, si usa il **gateway di default**

143

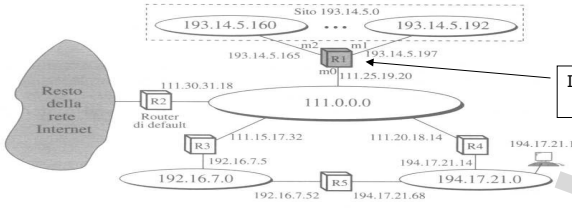
Modulo di instradamento per il router R1



	Mask	Destinatario	Next Hop	F.	R.C.	U.	I.
Consegna diretta	255.0.0.0	111.0.0.0	—	U	0	0	m0
	255.255.255.224	193.14.5.160	—	U	0	0	m2
	255.255.255.224	193.14.5.192	—	U	0	0	m1
	.....	.....	....	....	....	....	....
	.....	.....	....	....	....	....	....
	.....	.....	....	....	....	....	....
Host specifico	255.255.255.255	194.17.21.16	111.20.18.14	UGH	0	0	m0
Rete specifica	255.255.255.0	192.16.7.0	111.15.17.32	UG	0	0	m0
	255.255.255.0	194.17.21.0	111.20.18.14	UG	0	0	m0
Default routing	0.0.0.0	0.0.0.0	111.30.31.18	UG	0	0	m0

144

Esempio 1



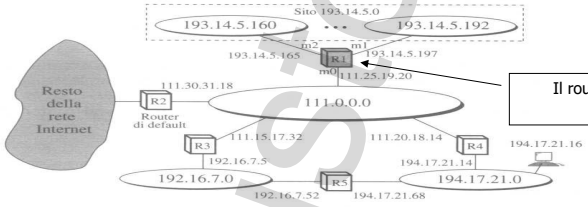
Il router R1 riceve 500 pacchetti con indirizzo destinatario 192.16.7.14

si esegue un'operazione di AND bit per bit tra l'indirizzo di destinazione del datagramma e la netmask di ciascuna riga.
il risultato viene confrontato con la destinazione specificata nella riga stessa:
se coincidono, la riga è quella giusta
altrimenti continuo con la successiva

tipo	Destinazione	Mask	AND	Destinatario	Esito	Next hop	R	U	I
Consegna diretta	192.16.7.14	255.0.0.0	192.0.0.0	111.0.0.0	NO				
Consegna diretta	192.16.7.14	255.255.255.224	192.16.7.0	193.14.5.160	NO				
Consegna diretta	192.16.7.14	255.255.255.224	192.16.7.0	193.14.15.192	NO				
Host specifico	192.16.7.14	255.255.255.255	192.16.7.14	194.17.21.16	NO				
Rete specifica	192.16.7.14	255.255.255.0	192.16.7.0	192.16.7.0	SI	111.15.17.32	1	500	m0
Rete specifica	192.16.7.14	255.255.255.0		194.17.21.0					
Default	192.16.7.14	0.0.0.0		0.0.0.0					

145

Esempio 2



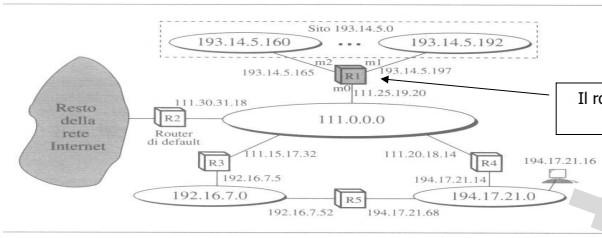
Il router R1 riceve 100 pacchetti con indirizzo destinatario 193.14.5.176

si esegue un'operazione di AND bit per bit tra l'indirizzo di destinazione del datagramma e la netmask di ciascuna riga.
il risultato viene confrontato con la destinazione specificata nella riga stessa:
se coincidono, la riga è quella giusta
altrimenti continuo con la successiva

tipo	Destinazione	Mask	AND	Destinatario	Esito	Next hop	R	U	I
Consegna diretta	193.14.5.176	255.0.0.0	193.0.0.0	111.0.0.0	NO				
Consegna diretta	193.14.5.176	255.255.255.224	193.14.5.160	193.14.5.160	SI	193.14.5.165	1	100	m2
Consegna diretta	193.14.5.176	255.255.255.224		193.14.15.192					
Host specifico	193.14.5.176	255.255.255.255		194.17.21.16					
Rete specifica	193.14.5.176	255.255.255.0		192.16.7.0					
Rete specifica	193.14.5.176	255.255.255.0		194.17.21.0					
Default	193.14.5.176	0.0.0.0		0.0.0.0					

146

Esempio 3



Il router R1 riceve 20 pacchetti con indirizzo destinatario 200.34.12.34

si esegue un'operazione di AND bit per bit tra l'indirizzo di destinazione del datagramma e la netmask di ciascuna riga.
il risultato viene confrontato con la destinazione specificata nella riga stessa:
se coincidono, la riga è quella giusta
altrimenti continuo con la successiva

tipo	Destinazione	Mask	AND	Destinatario	Esito	Next hop	R	U	I
Consegna diretta	200.34.12.34	255.0.0.0	200.0.0.0	111.0.0.0	NO				
Consegna diretta	200.34.12.34	255.255.255.224	200.34.12.32	193.14.5.160	NO				
Consegna diretta	200.34.12.34	255.255.255.224	200.34.12.32	193.14.15.192	NO				
Host specifico	200.34.12.34	255.255.255.255	200.34.12.34	194.17.21.16	NO				
Rete specifica	200.34.12.34	255.255.255.0	200.34.12.0	192.16.7.0	NO				
Rete specifica	200.34.12.34	255.255.255.0	200.34.12.0	194.17.21.0	NO				
Default	200.34.12.34	0.0.0.0	0.0.0.0	0.0.0.0	SI	111.30.31.18	1	20	m0

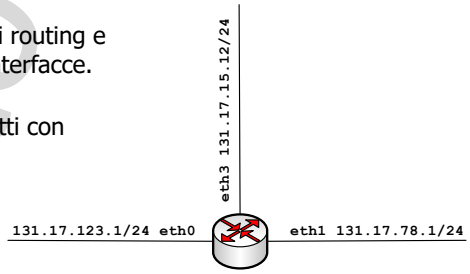
147

Esercizio 1

Un router ha la seguente tabella di routing e la seguente configurazione delle interfacce.

come avviene l'inoltro per pacchetti con indirizzo di destinazione:

- 131.17.123.88
- 131.56.78.4
- 190.78.90.2



network	netmask	next hop
131.175.21.0	255.255.255.0	131.17.123.254
131.175.16.0	255.255.255.0	131.17.78.254
131.56.0.0	255.255.0.0	131.17.15.254
131.155.0.0	255.255.0.0	131.17.15.254
0.0.0.0	0.0.0.0	131.17.123.254

148

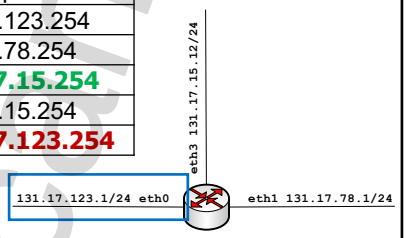
Reti di elaboratori

Soluzione

indirizzo di destinazione:

- **131.17.123.88** → viene inoltrato sull'interfaccia eth0 con l'indirizzo MAC
- **131.56.78.4** → viene inoltrato al gateway 131.17.15.254
- **190.78.90.2** → viene inoltrato al gateway 131.17.123.254

network	netmask	next hop
131.175.21.0	255.255.255.0	131.17.123.254
131.175.16.0	255.255.255.0	131.17.78.254
131.56.0.0	**255.255.0.0**	**131.17.15.254**
131.155.0.0	255.255.0.0	131.17.15.254
0.0.0.0	**0.0.0.0**	**131.17.123.254**



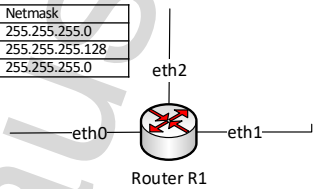
149

Reti di elaboratori

Esercizio 2

Un router ha la seguente configurazione delle interfacce e la seguente tabella di routing.
Il router riceve gli 8 pacchetti riportati di seguito, per ciascuno dei quali vengono riportati l'indirizzo IP di destinazione e l'interfaccia attraverso cui il router riceve il pacchetto.
Si chiede di indicare il comportamento del router per ciascuno dei pacchetti specificando se il router scarta o inoltra il pacchetto.
Nel caso in cui il router decida di inoltrare il pacchetto, specificare l'indirizzo IP del next hop e se l'inoltro è di tipo diretto o indiretto.

Interface	IP Address	Netmask
eth0	131.175.124.235	255.255.255.0
eth1	131.175.123.129	255.255.255.128
eth2	131.175.122.1	255.255.255.0



Network	Netmask	Next Hop
130.170.0.0	255.255.0.0	131.175.124.1
130.171.0.0	255.255.0.0	131.175.123.132
130.171.4.0	255.255.252.0	131.175.122.2
130.170.10.0	255.255.254.0	131.175.122.3
0.0.0.0	0.0.0.0	131.175.123.3

PACCHETTI RICEVUTI

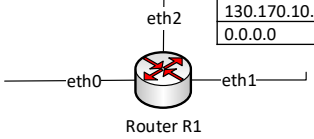
```
A) 131.175.124.64 da eth2
B) 131.175.124.255 da eth0
C) 131.175.123.132 da eth2
D) 130.170.132.240 da eth1
E) 130.170.11.64 da eth1
F) 130.171.5.125 da eth1
G) 156.198.34.14 da eth0
H) 0.0.0.132 da eth1
```


150

Soluzione

Interface	IP Address	Netmask
eth0	131.175.124.235	255.255.255.0
eth1	131.175.123.129	255.255.255.128
eth2	131.175.122.1	255.255.255.0

Network	Netmask	Next Hop
130.170.0.0	255.255.0.0	131.175.124.1
130.171.0.0	255.255.0.0	131.175.123.132
130.171.4.0	255.255.252.0	131.175.122.2
130.170.10.0	255.255.254.0	131.175.122.3
0.0.0.0	0.0.0.0	131.175.123.3



A) 131.175.124.64 da eth2

```
131.175.124.64 10000011.10101111.0111110 101000000
255.255.255.0  11111111.11111111.1111111 000000000
131.175.124.0  10000001.10101111.0111110 000000000
```

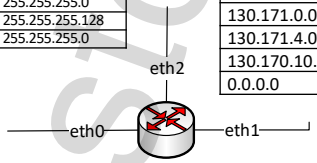
Inoltro diretto attraverso eth0

151

Soluzione

Interface	IP Address	Netmask
eth0	131.175.124.235	255.255.255.0
eth1	131.175.123.129	255.255.255.128
eth2	131.175.122.1	255.255.255.0

Network	Netmask	Next Hop
130.170.0.0	255.255.0.0	131.175.124.1
130.171.0.0	255.255.0.0	131.175.123.132
130.171.4.0	255.255.252.0	131.175.122.2
130.170.10.0	255.255.254.0	131.175.122.3
0.0.0.0	0.0.0.0	131.175.123.3



B) 131.175.124.255 da eth0

```
131.175.124.255    10000011.10101111.01111011.11111111
```

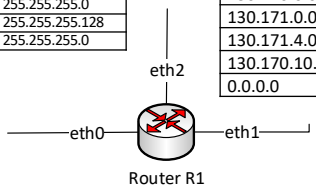
L'indirizzo destinazione è l'indirizzo di broadcast di eth0
Pacchetto giunto a destinazione

152

Soluzione

Interface	IP Address	Netmask
eth0	131.175.124.235	255.255.255.0
eth1	131.175.123.129	255.255.255.128
eth2	131.175.122.1	255.255.255.0

Network	Netmask	Next Hop
130.170.0.0	255.255.0.0	131.175.124.1
130.171.0.0	255.255.0.0	131.175.123.132
130.171.4.0	255.255.252.0	131.175.122.2
130.170.10.0	255.255.254.0	131.175.122.3
0.0.0.0	0.0.0.0	131.175.123.3



C) 131.175.123.132 da eth2

```
          131.175.123.132   10000011.10101111.01111011.1 0000100
          255.255.255.128   11111111.11111111.11111111.1 0000000

HostMin: 131.175.123.129   10000011.10101111.01111011.1 0000001
HostMax: 131.175.123.254   10000011.10101111.01111011.1 1111110
```

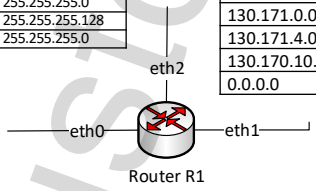
Inoltro diretto attraverso eth1

153

Soluzione

Interface	IP Address	Netmask
eth0	131.175.124.235	255.255.255.0
eth1	131.175.123.129	255.255.255.128
eth2	131.175.122.1	255.255.255.0

Network	Netmask	Next Hop
130.170.0.0	255.255.0.0	131.175.124.1
130.171.0.0	255.255.0.0	131.175.123.132
130.171.4.0	255.255.252.0	131.175.122.2
130.170.10.0	255.255.254.0	131.175.122.3
0.0.0.0	0.0.0.0	131.175.123.3



D) 130.170.132.240 da eth1

```
Address:   130.170.0.0          10000010.10101010 .00000000.00000000
Netmask:   255.255.0.0 = 16     11111111.11111111 .00000000.00000000
Network:   130.170.0.0/16       10000010.10101010 .00000000.00000000
Broadcast: 130.170.255.255      10000010.10101010 .11111111.11111111
HostMin:   130.170.0.1          10000010.10101010 .00000000.00000001
HostMax:   130.170.255.254      10000010.10101010 .11111111.11111110
```

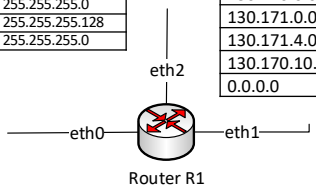
Inoltro indiretto
Prima riga della tabella di routing, NH: 131.175.124.1

154

Soluzione

Interface	IP Address	Netmask
eth0	131.175.124.235	255.255.255.0
eth1	131.175.123.129	255.255.255.128
eth2	131.175.122.1	255.255.255.0

Network	Netmask	Next Hop
130.170.0.0	255.255.0.0	131.175.124.1
130.171.0.0	255.255.0.0	131.175.123.132
130.171.4.0	255.255.252.0	131.175.122.2
130.170.10.0	255.255.254.0	131.175.122.3
0.0.0.0	0.0.0.0	131.175.123.3



E) 130.170.11.64 da eth1

```
Address:   130.170.10.0          10000010.10101010.0000101 0.00000000
Netmask:   255.255.254.0 = 23    11111111.11111111.1111111 0.00000000
Network:   130.170.10.0/23       10000010.10101010.0000101 0.00000000
Broadcast: 130.170.11.255        10000010.10101010.0000101 1.11111111
HostMin:   130.170.10.1          10000010.10101010.0000101 0.00000001
HostMax:   130.170.11.254        10000010.10101010.0000101 1.11111110
```

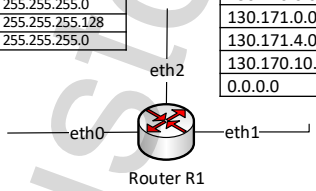
Inoltro indiretto
Quarta riga della tabella di routing, NH: 131.175.122.3

155

Soluzione

Interface	IP Address	Netmask
eth0	131.175.124.235	255.255.255.0
eth1	131.175.123.129	255.255.255.128
eth2	131.175.122.1	255.255.255.0

Network	Netmask	Next Hop
130.170.0.0	255.255.0.0	131.175.124.1
130.171.0.0	255.255.0.0	131.175.123.132
130.171.4.0	255.255.252.0	131.175.122.2
130.170.10.0	255.255.254.0	131.175.122.3
0.0.0.0	0.0.0.0	131.175.123.3



F) 130.171.5.125 da eth1

```
Address:   130.171.4.0           10000010.10101011.000001 00.00000000
Netmask:   255.255.252.0 = 22    11111111.11111111.111111 00.00000000
Network:   130.171.4.0/22        10000010.10101011.000001 00.00000000
Broadcast: 130.171.7.255         10000010.10101011.000001 11.11111111
HostMin:   130.171.4.1           10000010.10101011.000001 00.00000001
HostMax:   130.171.7.254         10000010.10101011.000001 11.11111110
```

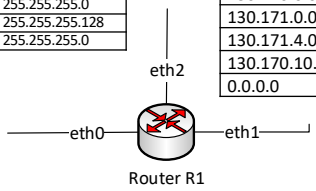
Inoltro indiretto
Terza riga della tabella di routing, NH: 131.175.122.2

156

Soluzione

Interface	IP Address	Netmask
eth0	131.175.124.235	255.255.255.0
eth1	131.175.123.129	255.255.255.128
eth2	131.175.122.1	255.255.255.0

Network	Netmask	Next Hop
130.170.0.0	255.255.0.0	131.175.124.1
130.171.0.0	255.255.0.0	131.175.123.132
130.171.4.0	255.255.252.0	131.175.122.2
130.170.10.0	255.255.254.0	131.175.122.3
0.0.0.0	0.0.0.0	131.175.123.3



G) 156.198.34.14 da eth0

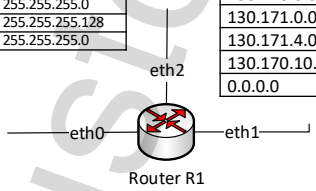
Inoltro indiretto
Ultima riga della tabella di routing, NH: 131.175.123.3
Default Gateway del router

157

Soluzione

Interface	IP Address	Netmask
eth0	131.175.124.235	255.255.255.0
eth1	131.175.123.129	255.255.255.128
eth2	131.175.122.1	255.255.255.0

Network	Netmask	Next Hop
130.170.0.0	255.255.0.0	131.175.124.1
130.171.0.0	255.255.0.0	131.175.123.132
130.171.4.0	255.255.252.0	131.175.122.2
130.170.10.0	255.255.254.0	131.175.122.3
0.0.0.0	0.0.0.0	131.175.123.3



H) 0.0.0.132 da eth1

Scartato
Indirizzo speciale valido solo come sorgente
indica l'host all'interno della rete

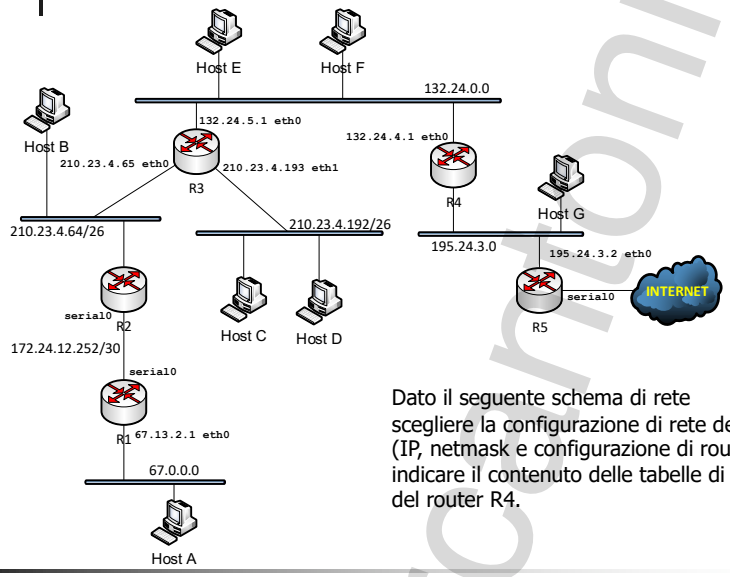
https://tools.ietf.org/html/rfc3330

2. Global and Other Specialized Address Blocks

0.0.0.0/8 - Addresses in this block refer to source hosts on "this" network. Address 0.0.0.0/32 may be used as a source address for this host on this network; other addresses within 0.0.0.0/8 may be used to refer to specified hosts on this network [RFC1700, page 4].

158

Esercizio 3



Dato il seguente schema di rete scegliere la configurazione di rete dell'Host C (IP, netmask e configurazione di routing) e indicare il contenuto delle tabelle di routing del router R4.

159

Osservazioni

La rete in figura è costituita dalle 6 sottoreti seguenti (internet esclusa)

1. **67.0.0.0 è una rete di classe A (netmask 255.0.0.0).**
2. **172.24.12.252/30 è una sottorete di una rete di classe B privata (172.24.0.0). Il numero 30 finale indica i bit corrispondenti alla parte di indirizzo che specifica la sottorete. Di conseguenza rispetto alla netmask della rete di classe B originaria si devono considerare ulteriori 14 bit che corrispondono a tutti i bit del terzo byte e a 6 bit del quarto. In questo modo i 216 indirizzi per gli host della classe B originaria (compresi l'indirizzo di rete e il broadcast) vengono divisi in 214 sottoreti, in ciascuna delle quali sono disponibili 4 indirizzi (i 2 bit rimanenti sui 32 dell'indirizzo completo), ovvero escludendo l'indirizzo di rete e il broadcast sono assegnabili 2 indirizzi (172.24.12.253 e 172.24.12.254) che corrisponderanno ai due router R1 e R2 sulla linea seriale (non è indicata l'assegnazione per questione di leggibilità, si può scegliere una delle soluzioni possibili). La netmask della rete sarà 255.255.255.252 (si veda la sezione "calcolo netmask" alla fine del documento).**
3. **210.23.4.64/26 è una sottorete di una rete di classe C (210.23.4.0). In questo caso la parte di indirizzo riservata alla rete comprende 26 bit ovvero 2 bit aggiuntivi rispetto a quanto previsto per le reti di classe C. In questo modo lo spazio di indirizzi viene suddiviso in 4 sottoreti (22) che sono in ordine 210.23.4.0 (byte finale 00-000000), 210.23.4.64 (byte finale 01-000000), 210.23.4.128 (byte finale 10-000000) e 210.23.4.192 (byte finale 11-000000). La netmask corrispondente è 255.255.255.192. In questa sottorete possono essere assegnati gli indirizzi da 210.23.4.65 a 210.23.4.126 (lasciando 210.23.4.64 per la rete – tutti i bit dell'host a 0 – e 210.23.4.127 per il broadcast – tutti i bit dell'host a 1).**
4. **210.23.4.192/26 è una sottorete di una rete di classe C (210.23.4.0) analogamente al caso precedente. Anche in questo caso la netmask corrispondente è 255.255.255.192. In questa sottorete possono essere assegnati gli indirizzi da 210.23.4.193 a 210.23.4.254 (lasciando 210.23.4.192 per la rete – tutti i bit dell'host a 0 – e 210.23.4.255 per il broadcast – tutti i bit dell'host a 1).**
5. **132.24.0.0 è una rete di classe B (netmask 255.255.0.0).**
6. **195.24.3.0 è una rete di classe C (netmask 255.255.255.0).**

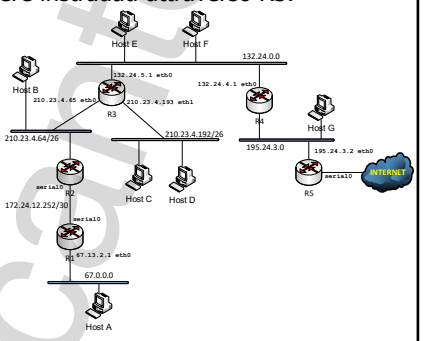
160

Soluzione

Configurazione dell'Host C

L'Host C è nella rete 210.23.4.192/26 per cui gli può essere assegnato un indirizzo IP nell'intervallo 210.23.4.193 a 210.23.4.254 purché non già in uso (210.23.4.193).
La netmask è 255.255.255.192.
Il default gateway è il router R3 (210.23.4.193), ovvero tutti i datagram non diretti alla sottorete 210.23.4.192 devono essere instradati attraverso R3.
Riassumendo la soluzione è

- IP: 210.23.4.194/26
- Netmask: 255.255.255.192 /26
- Default gateway: 210.23.4.193



161

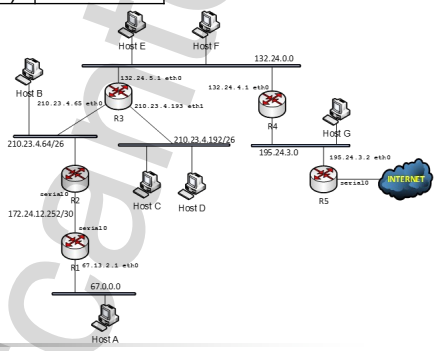
Soluzione: nota

Per configurare il default gateway è sufficiente indicare l'indirizzo IP del router che permette di instradare i pacchetti verso le altre reti (si usa l'indirizzo IP dell'interfaccia che è collegata alla sottorete in cui si trova l'host). Nel caso di reti "***transienti***" (*solo per breve tempo; temporaneo o transitorio)* ovvero con più di un router collegato, come ad esempio la rete 132.24.0.0 dell'esercizio, la definizione del default gateway è più delicata.
Infatti dovendo indicare un solo default gateway occorre fare una scelta fra quelli disponibili (R3 – 132.24.5.1 – e R4 – 132.24.4.1 nel caso di figura). Il criterio di scelta dovrebbe basarsi sulla "***direzione principale***" del traffico a partire dall'host considerato. Ad esempio se l'Host F scambia dati prevalentemente con gli host delle sottoreti alla destra (210.23.4.64/26, 210.23.4.192/26, 172.24.12.252/30, 67.0.0.0) conviene indicare R3 come default gateway; se invece il traffico prevalente è verso le reti a sinistra (195.24.3.0 e Internet) allora conviene indicare R4. Questa soluzione permette di evitare che la maggior parte dei datagram inviati dall'Host F transitino per due volte sulla rete 132.24.0.0 raddoppiando di fatto il traffico generato dal'HostF . Infatti se il default gateway è R4 e l'Host F invia un pacchetto ad un host sulla rete 67.0.0.0, il pacchetto viene prima indirizzato a R4 che poi provvede a inoltrarlo a R3 che è sul tragitto necessario a recapitarlo al destinatario finale. Come conseguenza la trasmissione del datagram impegna due volte la rete ethernet (Host F->R4 e R4->R3) per lo stesso datagram. La soluzione sarebbe quella di configurare in modo completo le tabelle di routing di tutti gli host della rete transiente indicando per ogni rete nota il router da usare. Questa soluzione è più laboriosa ma ottimizza il traffico. In ogni caso appare chiaro che avere molti host su una rete transiente non è una soluzione ottimale.

162

Soluzione

Destinazione	Netmask	Next-hop	Interfaccia
67.0.0.0	255.0.0.0	132.24.5.1 (R3)	eth0
172.24.12.252	255.255.255.252	132.24.5.1 (R3)	eth0
210.23.4.64	255.255.255.192	132.24.5.1 (R3)	eth0
210.23.4.192	255.255.255.192	132.24.5.1 (R3)	eth0
132.24.0.0	255.255.0.0	Diretta (MAC)	eth0
195.24.3.0	255.255.255.0	Diretta (MAC)	eth1
0.0.0.0	0.0.0.0	195.24.3.2 (R5)	eth1



Configurazione del router R4

Le tabelle di routine del router R4 devono contenere le indicazioni per consegnare i datagram a tutte le sottoreti presenti, oltre a indicare l'instradamento di default per tutte le altre reti (Internet).

La soluzione è la tabella seguente.

163

Internet Control Message Protocol (ICMP)

La suite TCP/IP include un protocollo che IP utilizza per inviare messaggi di errore:

Internet Control Message Protocol (ICMP)

Tale protocollo è richiesto per un'implementazione standard di IP.

I due protocolli sono **interdipendenti**:

- IP utilizza ICMP per mandare un messaggio di errore
- ICMP utilizza IP per trasportare i suoi messaggi

164

Internet Control Message Protocol

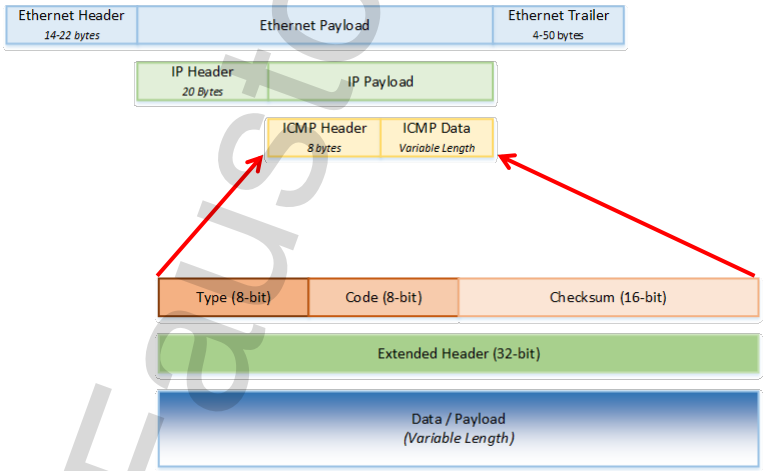
IP definisce un servizio di comunicazione **best-effort** in cui i datagrams possono essere persi, duplicati, ritardati, o consegnati in disordine.

Può sembrare che un servizio di tipo best-effort non richieda alcuna protezione di errore, ma è necessario sottolineare che ***un servizio best-effort non è senza controllo***.

IP tenta di evitare errori e di riportare eventuali problemi quando essi accadono.

165

Header ICMP



166

Header ICMP

MAC header | IP header | ICMP header | Data :::

ICMP header:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Type								Code								ICMP header checksum															
Data :::																															

Type. ***8 bits***. *Specifies the format of the ICMP message.*

Code. ***8 bits***. *Further qualifies the ICMP message.*

ICMP Header Checksum. ***16 bits***. *Checksum that covers the ICMP message. This is the 16-bit one's complement of the one's complement sum of the ICMP message starting with the Type field. The checksum field should be cleared to zero before generating the checksum.*

Data. ***Variable length***. *Contains the data specific to the message type indicated by the Type and Code fields.*

Formato ICMP Message

Type. ***8 bits***. *Specifies the format of the ICMP message.*

Type	Description	References
0	Echo reply.	
1	Reserved.	
2	Reserved.	
3	Destination unreachable.	
4	Source quench.	
5	Redirect.	
6	Alternate Host Address.	
7		
8	Echo request.	
9	Router advertisement.	
10	Router solicitation.	
11	Time exceeded.	
12	Parameter problem.	
13	Timestamp request.	
14	Timestamp reply.	
15	Information request.	
16	Information reply.	
17	Address mask request.	
18	Address mask reply.	
19	Reserved (for security).	

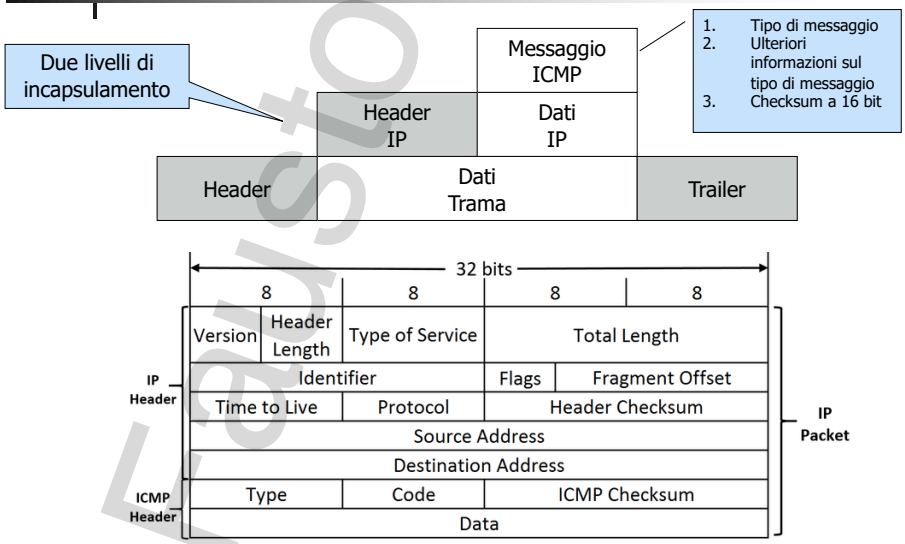
Type	Description	References
20 - 29	Reserved (for robustness experiment).	
30	Traceroute.	
31	Conversion error.	
32	Mobile Host Redirect.	
33	IPv6 Where-Are-You.	
34	IPv6 I-Am-Here.	
35	Mobile Registration Request.	
36	Mobile Registration Reply.	
37	Domain Name request.	
38	Domain Name reply.	
39	SKIP Algorithm Discovery Protocol.	
40	Photuris, Security failures.	
41	Experimental mobility protocols.	RFC 4065
42 - 255	Reserved.	

https://datatracker.ietf.org/doc/html/rfc6918

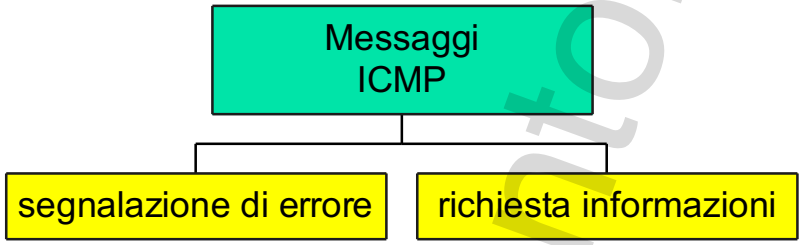
Trasporto dei Messaggi ICMP

- **ICMP utilizza IP** per trasportare ogni messaggio di errore.
- Quando un router e/o un host ha un messaggio ICMP da inviare, crea un datagram IP ed **incapsula** il messaggio ICMP in tale datagram.
- Il messaggio ICMP viene posizionato **nell'area dati** del datagram IP.
- Il datagram viene quindi spedito normalmente, incapsulando il datagram completo all'interno di una frame di livello 2.

Incapsulamento e messaggi ICMP

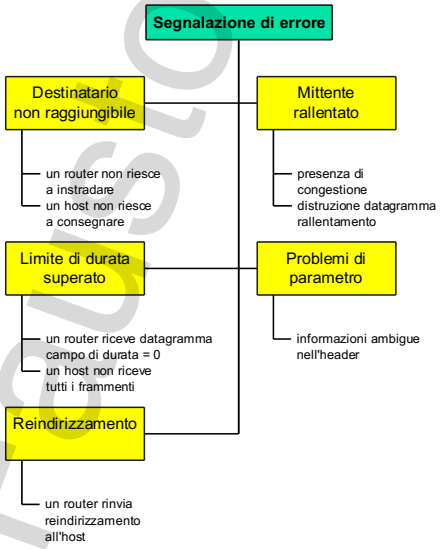


Messaggi ICMP



171

ICMP: segnalazione di errore



172

Destinazione irraggiungibile

0	8	16	31
TYPE → 3	CODE → 0 – 15	CHECKSUM	
UNUSED			
Internet header + first 64 bits of datagram			
.....			

- Rete irraggiungibile → errore di instradamento
- Host irraggiungibile → fallimenti di consegna
- Ogni volta che si verifica questo errore il router
  - Scarta il datagram ed invia un messaggio ICMP alla sorgente
  - La sorgente saprà quale indirizzo è irraggiungibile

Destinazione irraggiungibile

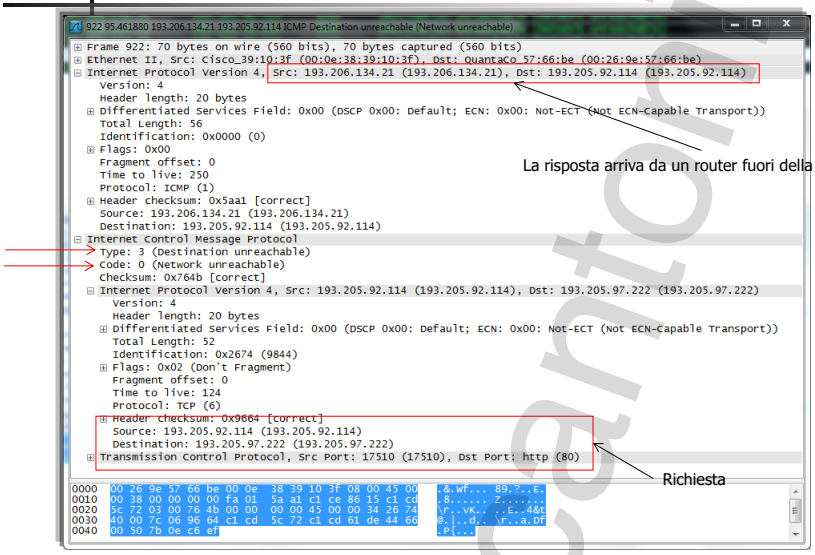
Packet format:

Type. 8 bits. **Set to 3.**
Code. 8 bits. **Specifies the reason for the error.**

00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Type	Code	ICMP header checksum
Unused		Next-Hop MTU.
IP header + the first 8 bytes of the original datagram's data.		

Code	Description
0	Network unreachable error.
1	Host unreachable error.
2	Protocol unreachable error. When the designated transport protocol is not supported.
3	Port unreachable error. When the designated transport protocol (e.g., UDP) is unable to demultiplex the datagram but has no protocol mechanism to inform the sender.
4	The datagram is too big. Packet fragmentation is required but the DF bit in the IP header is set.
5	Source route failed error.
6	Destination network unknown error.
7	Destination host unknown error.
8	Source host isolated error. Obsolete.
9	The destination network is administratively prohibited.
10	The destination host is administratively prohibited.
11	The network is unreachable for Type Of Service.
12	The host is unreachable for Type Of Service.
13	Communication Administratively Prohibited. This is generated if a router cannot forward a packet due to administrative filtering.
14	Host precedence violation. Sent by the first hop router to a host to indicate that a requested precedence is not permitted for the particular combination of source/destination host or network, upper layer protocol, and source/destination port.
15	Precedence cutoff in effect. The network operators have imposed a minimum level of precedence required for operation, the datagram was sent with a precedence below this level.

Esempio ICMP



175

Rilevazione di percorsi circolari o eccessivamente lunghi (messaggio di tempo scaduto)

0	8	16	31
TYPE → 11	CODE → 0 – 1	CHECKSUM	
UNUSED			
Internet header + first 64 bits of datagram			
.....			

- Code = 0 → tempo di vita scaduto
- Code = 1 → tempo di riassemblaggio dei **frammenti** scaduto

176

Reti di elaboratori

Richiesta di modifica di percorso da parte del router (messaggio di reindirizzamento)

0	8	16	31
TYPE → 5	CODE → 0 – 3	CHECKSUM	
ROUTER INTERNET ADDRESS			
Internet header + first 64 bits of datagram			
.....			

- La configurazione iniziale di un host contiene le informazioni minime di instradamento
- Quando un router rileva che un host sta usando un percorso non ottimale
  - Gli invia un messaggio ICMP
  - Inoltra comunque il pacchetto
- Il campo ROUTER INTERNET ADDRESS contiene l'indirizzo del router che l'host deve usare per raggiungere la destinazione menzionata nell'intestazione del datagram

177

Reti di elaboratori

Controllo del flusso del datagram e della congestione (messaggio di blocco della sorgente)

0	8	16	31
TYPE → 4	CODE → 0	CHECKSUM	
UNUSED			
Internet header + first 64 bits of datagram			
.....			

- Quando i datagram **arrivano troppo rapidamente** i router li accodano in memoria
- Quando la memoria è esaurita
  - Si devono scartare gli ulteriori datagram in arrivo
  - Si invia un messaggio di blocco della sorgente
- Si tratta di una richiesta di riduzione di velocità

178

ICMP Parameters

Internet Control Message Protocol (ICMP) Parameters

Last Updated
2018-06-15
Available Formats
XML HTML Plain text

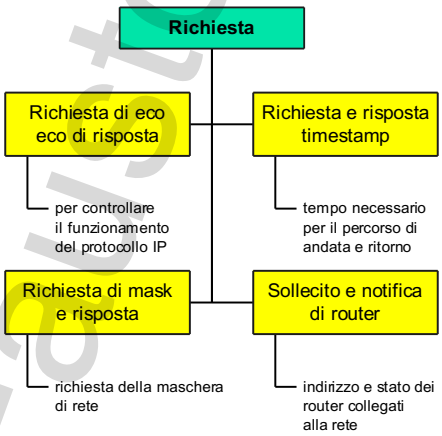
Registries included below

- ICMP Type Numbers
- Code Fields
  - Type 0 — Echo Reply
  - Type 1 — Unassigned
  - Type 2 — Unassigned
  - Type 3 — Destination Unreachable
  - Type 4 — Source Quench (Deprecated)
  - Type 5 — Redirect
  - Type 6 — Alternate Host Address (Deprecated)
  - Type 7 — Unassigned
  - Type 8 — Echo
  - Type 9 — Router Advertisement
  - Type 10 — Router Selection
  - Type 11 — Time Exceeded
  - Type 12 — Parameter Problem
  - Type 13 — Timestamp
  - Type 14 — Timestamp Reply
  - Type 15 — Information Request (Deprecated)
  - Type 16 — Information Reply (Deprecated)
  - Type 17 — Address Mask Request (Deprecated)
  - Type 18 — Address Mask Reply (Deprecated)
  - Type 19 — Reserved (for Security)
  - Types 20-29 — Reserved (for Robustness Experiment)
  - Type 30 — Traceroute (Deprecated)
  - Type 31 — Datagram Conversion Error (Deprecated)

https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

179

ICMP: messaggi di richiesta



180

Verifica di raggiungibilità e dello stato di destinazione

0	8	16	31
TYPE → 8 o 0	CODE → 0	CHECKSUM	
IDENTIFIER		SEQUENCE NUMBER	
OPTIONAL DATA			
.....			

- Il campo OPTIONAL DATA contiene i dati che debbono essere restituiti al mittente
- TYPE = 8 → richiesta
- TYPE = 0 → risposta
- Identifier e Sequence Number sono usati dal mittente per far corrispondere le risposte alle richieste
- Su molti sistemi il comando usato dagli utenti per inviare le richieste ICMP di eco è denominato **ping**

ICMP per verifica connettività

```
C:\>ping

Sintassi: ping [-t] [-a] [-n conteggio] [-l dimensione] [-f] [-i durata]
               [-v tipo servizio] [-r conteggio] [-s conteggio]
               [[-j elenco host] | [-k elenco host]]
               [-w timeout] elenco di destinazioni

Opzioni:
    -t                Effettua un ping sull'host specificato finché non viene
                      interrotto.
                      Per visualizzare le statistiche e continuare - digitare
                      Ctrl-Inter;
                      Per interrompere - digitare Ctrl-C.
    -a                Risolve gli indirizzi in nomi host.
    -n conteggio      Numero di richieste di eco da inviare.
    -l dimensione     Invia dimensioni buffer.
    -f                Imposta il flag per la disattivazione della
                      frammentazione nel pacchetto.
    -i durata         Durata.
    -v tipo servizio  Tipologia di servizio.
    -r conteggio      Registra route per il conteggio dei punti di passaggio.
    -s conteggio      Timestamp per il conteggio dei punti di passaggio.
    -j elenco host    Instradamento libero lungo l'elenco host.
    -k elenco host    Instradamento vincolato lungo l'elenco host.
    -w timeout        Timeout in millisecondi per ogni risposta.
```

Default TTL

Default TTL (Time To Live) Values of Different OS

TTL (Time To Live) è un "valore del timer" incluso nei pacchetti inviati sulle reti che indica al destinatario per quanto tempo conservare o utilizzare il pacchetto prima di scartare e far scadere i dati (pacchetto).
I valori TTL sono diversi per i diversi sistemi operativi. Quindi, puoi determinare il sistema operativo in base al valore TTL.

http://www.binbert.com/blog/2009/12/default-time-to-live-ttl-values/

http://subinsb.com/default-device-ttl-values

Linux: Use the sysctl command to view and set the default TTL:

```
sysctl net.ipv4.ip_default_ttl
sysctl -w net.ipv4.ip_default_ttl=64
```

Windows: The registry key that controls the default TTL is:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DefaultTTL
```


La sincronizzazione degli orologi ed il calcolo del tempo di transito (risposta di timestamp)

0	8	16	31
TYPE → 13 o 14	CODE → 0	CHECKSUM	
IDENTIFIER		SEQUENCE NUMBER	
ORIGINATE TIMESTAMP			
RECEIVE TIMESTAMP			
TRANSMIT TIMESTAMP			

- I campi timestamp specificano il tempo in millisecondi a partire dalla mezzanotte ora universale :
  - ORIGINATE TIMESTAMP → compilato dal mittente prima che il pacchetto sia trasmesso
  - RECEIVE TIMESTAMP → compilato al ricevimento della richiesta
  - TRANSMIT TIMESTAMP → subito prima che la risposta sia trasmessa
- Gli host usano i tre campi per sincronizzare gli orologi
- L'host può calcolare il tempo totale di transito in rete
- **Sostituito da NTP**

NTP: Network Time Protocol

Il *Network Time Protocol* (NTP) è un sistema per la sincronizzazione del tempo di orologio dei calcolatori attraverso la rete Internet.

Sviluppato principalmente presso l'università del Delaware negli Stati Uniti.

Ne sono state definite 3 versioni: la 1 nel 1988, la 2 nel 1989 e la 3 nel 1992. la versione corrente è la versione 3, compatibile con le precedenti.

Per facilitare l'uso dell'NTP sui personal computer è stata definita la versione semplificata *Simplified NTP* (SNTP 1995).

Le principali caratteristiche dell'NTP sono le seguenti

- È **completamente automatico** e mantiene la **sincronizzazione in modo continuativo**;
- È adatto alla sincronizzazione sia di un solo calcolatore, sia di intere reti di calcolatori;
- Si può utilizzare con quasi tutti i tipi di calcolatori;
- È resistente ai guasti e dinamicamente auto configurante;
- Diffonde il tempo **UTC**, quindi è indipendente dai fusi orari e dalle ore legali;
- La **precisione** di sincronizzazione arriva fino ad 1 millisecondo;

185

Porte di rete utilizzata dal servizio ora di Windows

Il servizio ora di Windows comunica in una rete per identificare le origini di ora affidabile, ottenere informazioni sull'ora e fornire le informazioni ad altri computer. Questa comunicazione viene eseguita come definito dal NTP e SNTP (Simple Network Time Protocol).

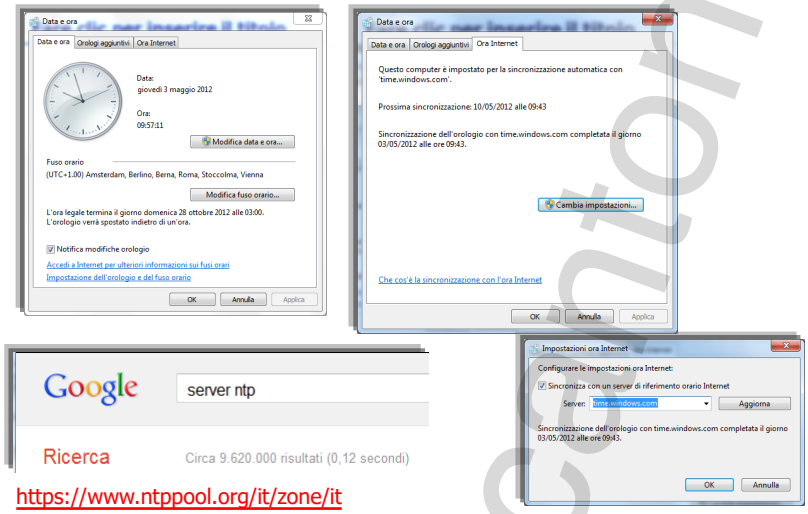
Assegnazioni delle porte per il servizio Ora di Windows
Porte di rete utilizzata dal servizio ora di Windows

Nome del servizio	UDP	TCP
NTP	123	N/D
SNTP	123	N/D

186

set ntp server windows 10

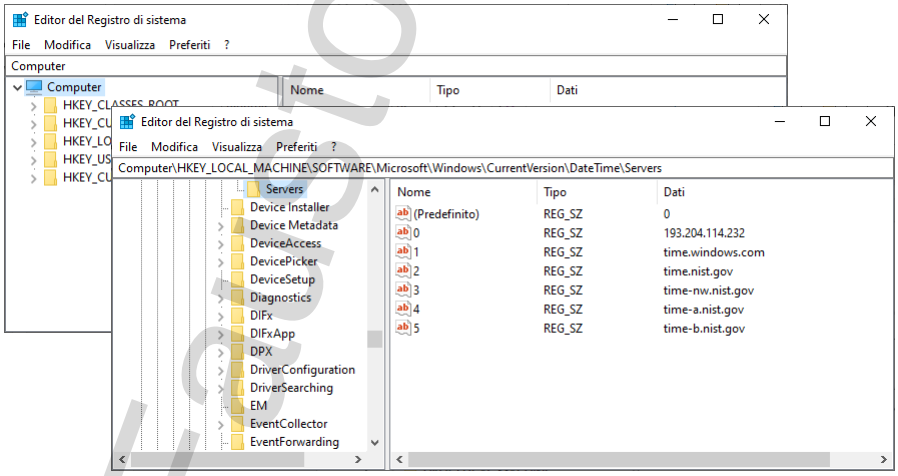
To configure NTP, you still need to use the classic Control Panel applet.



https://www.ntppool.org/it/zone/it

187

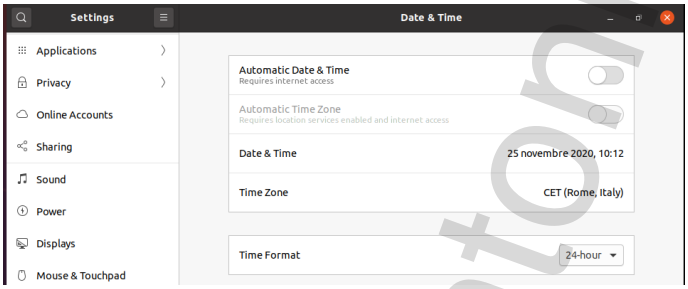
set ntp server windows 10 - regedit



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\Servers

188

NTP: esempio Linux

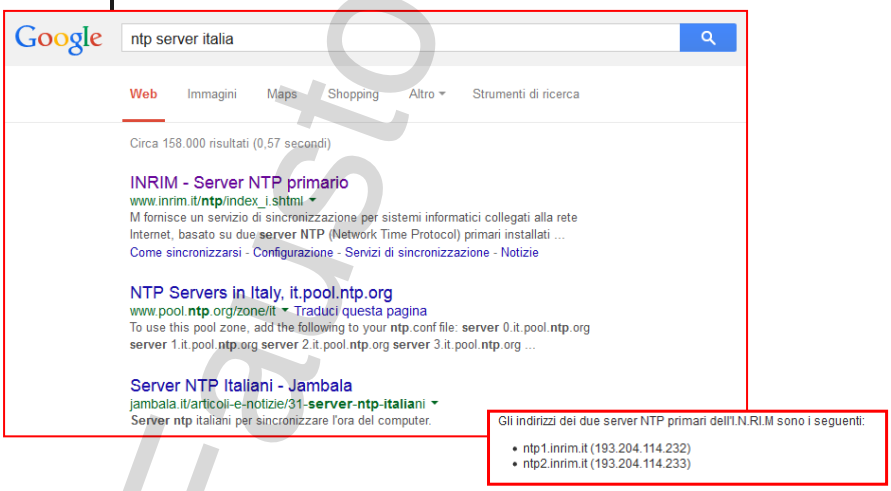



```
# sudo apt install sntp
# sudo sntp it.pool.ntp.org
# sudo apt install ntp
```

Il pacchetto installerà un demone che resterà in funzione e si occuperà di sincronizzare l'orologio del server con un server NTP mondiale.
Il file di configurazione del demone è /etc/ntp.conf. In questo file vanno specificati i server NTP da contattare per la sincronizzazione, ad esempio ntp1.ien.it o ntp2.ien.it.

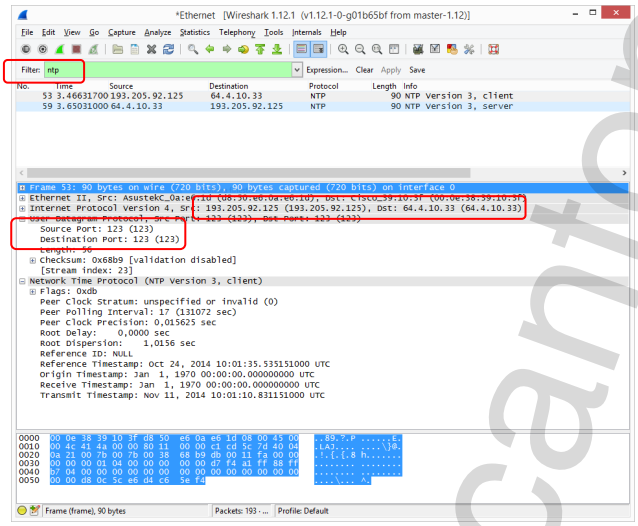
189

NTP: Network Time Protocol - Italia



190

NTP: Network Time Protocol



191

Usare ICMP per Tracciare un Percorso (1/3)

- *Traceroute* invia una serie di datagram ed attende una risposta a ciascuno di essi.
- *traceroute*, prima di spedire il primo datagram, setta ad "1" il valore del campo *TIME TO LIVE*.
- Il primo router che riceve il datagram decrementa tale contatore, scarta il datagram ed invia in risposta un messaggio **ICMP di *time exceeded***.
- Dal momento che il messaggio ICMP viaggia all'interno di un datagram IP, *traceroute* può estrarre l'indirizzo IP della sorgente ed annunciare l'indirizzo IP del primo router lungo il percorso verso la destinazione.

192

Usare ICMP per Tracciare un Percorso (2/3)

- Dopo aver scoperto l'indirizzo del primo router, traceroute invia un datagram con TIME TO LIVE settato a "2".
- Il primo router decrementa il contatore e forwarda il datagram;
- il secondo router scarta il datagram ed invia un messaggio **ICMP di *time exceeded*** di errore.

Usare ICMP per Tracciare un Percorso (3/3)

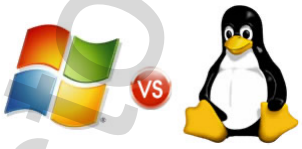
- Analogamente, una volta ricevuto un messaggio di errore da un router a distanza 2, traceroute invia un datagram con TIME TO LIVE settato a "3", poi a "4", etc.
- traceroute continua ad incrementare il TIME TO LIVE fino a quando il valore è abbastanza elevato da permettere al datagram di raggiungere la sua destinazione.

Usare ICMP per Tracciare un Percorso (3/3)

- Cosa succede quando il TTL permette al datagram di raggiungere la destinazione?
- Per assicurarsi di ricevere una risposta, traceroute invia un datagram a cui l'host di destinazione sia "***obbligato***" a rispondere.

- Esistono due possibilità:
  - Inviare un messaggio **ICMP di echo request**; l'host di destinazione genererà **un echo reply**
  - Inviare un datagram ad **un'applicazione non-esistente**; l'host di destinazione genererà un messaggio **ICMP di destination unreachable**

Usare ICMP per Tracciare un Percorso (Microsoft vs Linux)



- L'implementazione Microsoft di *traceroute* (*tracert*) implementa il primo approccio; quindi ogni volta che invia un datagram, *tracert* riceve un messaggio ICMP *time exceeded* da un router lungo il percorso oppure l'*echo reply* dal computer destinazione.

- La maggior parte dei sistemi Unix, invece, utilizza il secondo metodo; traceroute invia un messaggio UDP ad un programma non esistente sull'host di destinazione. Ogni volta che invia un datagram, traceroute riceve quindi un messaggio ICMP *time exceeded* da un router lungo il percorso oppure un messaggio ICMP *destination unreachable* dal computer destinazione.

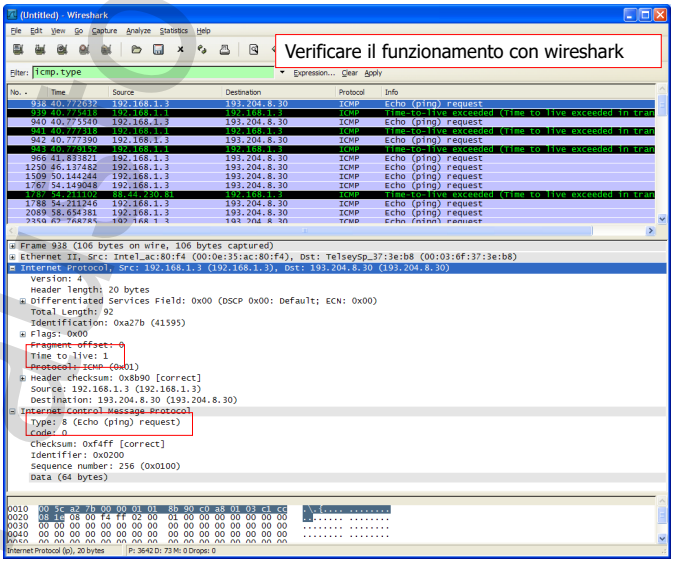
Usare ICMP per Tracciare un Percorso (Microsoft vs Linux)

Le due implementazioni di *traceroute* possono produrre **risultati differenti** quando la **destinazione è *un router* oppure *un host* con interfacce di rete multiple.**

Per capire il perché è necessario chiarire che:

- Quando un *echo request* arriva al computer di destinazione, ICMP genera un *echo reply* con indirizzo di sorgente uguale all'indirizzo IP a cui la richiesta è stata inviata
- Quando un datagram arriva e nessun programma è in attesa, ICMP utilizza l'indirizzo dell'interfaccia tramite la quale viene spedito il messaggio di errore

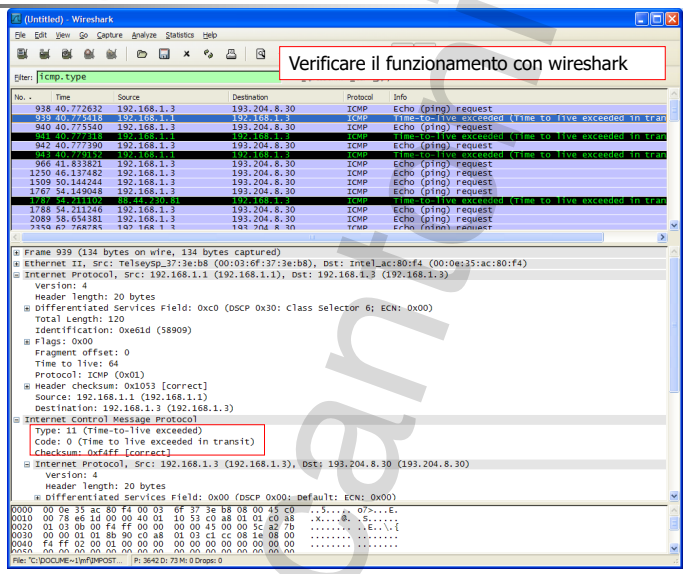
Usare ICMP per Tracciare un Percorso (esercizio)



Usare ICMP per Tracciare un Percorso (esercizio)

"E:\Google Drive\corsi\reti\Reti di Elaboratori\tools\traceroute.pcap"

Verificare il funzionamento con wireshark



199

Come viene utilizzato l'ICMP negli attacchi DDoS?

In un attacco DDoS (Distributed Denial of Service) l'ICMP viene utilizzato in diversi modi:

- un attacco di flooding ICMP
- un attacco PoD - Ping of Death
- un attacco smurf

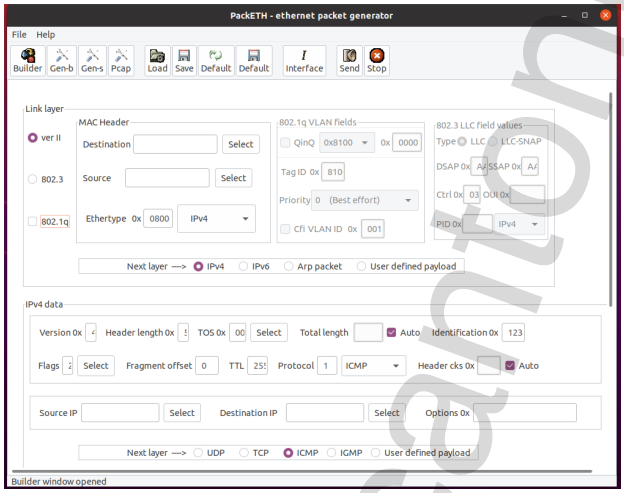
In un attacco di flooding ICMP, l'aggressore cerca di inviare così tanti ping che il dispositivo bersagliato non è in grado di gestire tutti i pacchetti di richiesta eco ICMP. Poiché ogni pacchetto richiede un'elaborazione e una risposta, tutte le risorse del dispositivo sono assorbite in queste operazioni e il dispositivo non potrà servire gli utenti legittimi.

Un attacco PoD prevede che un aggressore invii un ping estremamente grande a un dispositivo che non è in grado di gestire ping di quella dimensione. La macchina potrebbe arrestarsi in modo anomalo o bloccarsi. Il pacchetto di dati viene frammentato mentre si dirige verso l'obiettivo, ma durante il processo di riassemblaggio viene rimesso insieme. Quando raggiunge l'obiettivo, sovraccarica il buffer e causa il malfunzionamento del dispositivo. Gli attacchi PoD sono più pericolosi per le macchine meno recenti.

In un attacco smurf, l'aggressore trasmette un pacchetto ICMP che ha un indirizzo IP contraffatto o falso. Quando l'apparecchio in rete risponde, ogni risposta viene inviata all'indirizzo IP sottoposto a spoofing e la destinazione viene inondata di una quantità infinita di pacchetti ICMP. Solitamente questo tipo di attacco è un problema solo per le apparecchiature più vecchie.

200

Packet Generator



http://packeth.sourceforge.net/packeth/Home.html

201

Packet Generator

TRex Realistic Traffic Generator https://trex-tgn.cisco.com/

Packet Sender https://packetsender.com/

202