

Titolo nota

## FORMATO DEI DATAGRAMMI IP

Version (4 bit)	IHL (4 bit)	Type of Service (8 bit)	Total Length (16 bit)	
Identification (16 bit)		Flags (3 bit)	Fragment Offset (13 bit)	
Time To Live (8 bit)	Protocol (8 bit)	Header Checksum (16 bit)		
Source Address (32 bit)				
Destination Address (32 bit)				
Options ...			Padding	

Titolo nota

VERSIONE : INFORMAZIONE RIGUARDO LA VERSIONE DEL PROTOCOLO IP. SERVE PER ISTRUIRE TUTTI I DISPOSITIVI DELLA RETE AD INTERPRETARE CORRETTAMENTE I CAMPI DELL'INTESTAZIONE

IHL (INTERMEDIATE HEADER LENGTH) :

LUNGHEZZA DELL'INTESTAZIONE INTERMEDIA

SPECIFICA LA LUNGHEZZA EFFETTIVA DELLA INTESTAZIONE IN PAROLE DI 32 bit.

Titolo nota

LA LUNGHEZZA MINIMA È 5

LA LUNGHEZZA MASSIMA È 15 (-> 1111)

SE UNA PAROLA DI 32 BIT NON È COMPLETA SI  
USANO DEI VALORI DI RIEMPIIMENTO (PADDING)

TOS (TYPE OF SERVICE)

TIPO DI SERVIZIO

SERVE PER POTER CLASSIFICARE I DATAGRAMMI

Titolo nota

ESEMPIO: ASSEGNIARE PRIORITÀ DIFFERENTE

SERVE, QUANDO POSSIBILE, PER CREARE DEI  
PERCORSI CON ATTRIBUTI SPECIFICI

LUNGHEZZA TOTALE: SERVE A DICHIARARE

LA LUNGHEZZA DEL DATAGRAMMA INCLUDENDO

IL PAYLOAD (PARTE INFORMATIVA) E LA TESTATA

È UN CAMPO DI 16 BIT QUINDI LA LUNGHEZZA  
MASSIMA È  $2^{16}-1$  BIT.

Titolo nota

IDENTIFICAZIONE : È UN CAMPO UTILIZZATO PER IDENTIFICARE I DATAFRAME (FRAMMENTI) CON CUI È STATO SUDDIVISO IL DATAFRAME ORIGINARIO DI DIMENSIONE ECCEDENTE LA MASSIMA AMMESSA. QUESTA INFORMAZIONE SERVE PER RIPRISTINARE, UNA VOLTA RICEVUTO COMPLETAMENTE, IL DATAGRAMMA ORIGINALE NELLA SUA VERSIONE NATIVA.  
(ASSEMBLAGGIO)

Titolo nota

FLAG : SONO UTILIZZATI PER ANNUNCIARE E GESTIRE LA FRAMMENTAZIONE DI UN DATAGRAMMA. IL PRIMO BIT (DETTO BIT D) SE DI VALORE 1 INDICA CHE IL DATAGRAMMA DEVE ESSERE TRASFERITO SEMPRE FRAMMENTATO.

IL SECONDO BIT (DETTO BIT M) VIENE USATO PER RIPRISTINARE IL DATAGRAMMA NEL SUO FORMATO ORIGINALE. VALE 1 PER TUTTI I FRAMMENTI

TRAHNE L'ULTIMO PER IL QUALE VALE 0.

(DEI TRE BIT SE NE USANO SOLO 2)

### FRAGMENT OFFSET (SPIAZZAMENTO DEL FRAMMENTO)

VIENE USATO PER INDICARE LA POSIZIONE DEL PRIMO  
BYTE DEL FRAMMENTO RISPETTO ALLA STRUTTURA DEL  
DATAGRAMMA ORIGINALE.

È INDICATO COME MULTIPLO DI 8 BYTE.

### TTL (TIME TO LIVE) : TEMPO DI VITA

INDICA IL TEMPO MASSIMO CHE UN DATAGRAMMA  
PUÒ TRASCORRERE DENTRO UNA RETE.

QUESTO PARAMETRO VIENE DIMINUITO DI QUANTITÀ  
PREFISSATE QUANDO IL DATAGRAMMA ATTRAVERSA  
GLI APPARATI DI RETE. VIENE CONTROLLATO  
PRIMA DI PROCESSARE IL DATAGRAMMA.

SE IL VALORE DEL CAMPO VIENE TROVATO  
A ZERO IL DATAGRAMMA NON VIENE PIÙ

RIPETUTO.

IL DISPOSITIVO DI DESTINAZIONE CONOSCEMDA IL VALORE DEL CAMPO ATTEMDE L'ARRIVO DEL DATAGRAMMA ENTRO QUESTO TEMPO ALTRIMENTI LO CONSIDERA PERDUTO.

PROTOCOL : È UTILIZZATO DAL LIVELLO IP DI DESTINAZIONE PER PASSARE IL PAYLOAD AL LIVELLO TCP ED ASSOCIAVELO AL PROTOCOLLO

CORRISPONDENTE: TCP o UDP  
OPPURE IL PAYLOAD PUÒ ESSERE ASSOCIAVTO AD UN PROTOCOLLO DEL LIVELLO IP.

HEADER CHECKSUM : (SOMMA DI CONTROLLO DELLA INTESTAZIONE)

SERVE PER EVITARE DI INOLTRARE I DATAGRAMMI VERSO DESTINAZIONI ERRATE.

SOURCE ADDRESS : (INDIRIZZO MITTELENTE)

DESTINATION ADDRESS : (INDIRIZZO DESTINAZIONE)

OPTIONS :

• SICUREZZA : IL PAYLOAD PUÒ ESSERE CIFRATO  
CONTIENE LE INFORMAZIONI NECESSARIE PER  
LA SUA COMPRENSIONE

• INSTRADAMENTO DALLA SORGENTE  
CONTIENE, SE CONOSCIUTO, LE INFORMAZIONI  
(ELenco DI INDIRIZZI) DEI DISPOSITIVI CHE  
DEVONO ESSERE VISITATI DAL PERCORSO  
SORGENTE → DESTINAZIONE.

• INSTRADAMENTO APPROSSIMATO DALLA SORGENTE  
ELenco DEGLI INDIRIZZI DEI DISPOSITIVI  
PREFERITI PER DEFINIRE IL PERCORSO  
SORGENTE → DESTINAZIONE

### REGISTRAZIONE DEL PERCORSO

VIENE UTILIZZATO DAI DISPOSITIVI VISITATI DAL DATAGRAMMA DURANTE IL SUO TRASFERIMENTO DALLA SORGENTE → DESTINAZIONE PER INDICARE IL PROPRIO INDIRIZZO IP.

L'ELenco finale formato può costituire LA ROTTA DA SEGUIRE PER I DATAGRAMMI SUCCESSIVI

### IDENTIFICAZIONE DEL FLUSSO

CONSENTE DI NOTIFICARE AI DISPOSITIVI VISITATI DAL DATAGRAMMA IL TIPO DI FLUSSO DI APPARTENENZA E QUINDI RENDERE POSSIBILI POLITICHE DI GESTIONE A PRIORITA.

### TIME-STAMP :

SERVE PER I DISPOSITIVI PER REGISTRARE IL TEMPO DI ELABORAZIONE DEL DATAGRAMMA.

## FRAMMENTAZIONE E RICOMBINAZIONE

MTU = MAXIMUM TRANSMISSION UNIT

VALORE MASSIMO IN BYTE DI UN DATAGRAMMA

GENERALMENTE CONDIZIONATO DAL VALORE MASSIMO

ACCETTATO DAL LIVELLO COLLEGAMENTO SU CUI

SI Poggia lo STRATO IP.

PER ILLUSTRARE COME L'OPERAZIONE DI FRAMMENTAZIONE  
Venga IMPLEMENTATA RIFERIAMOCI AD UN ESEMPIO.

UN HOST VOGLIE TRASFERIRE SU UNA RETE TCP/IP

UN BLOCCO DI 4000 BYTES INCLUSA L'INTESTAZIONE  
DEL LIVELLO TRASPORTO. UTILIZZANDO UNA

RETE IL CUI LIVELLO COLLEGAMENTO ACCETTA

PACCHETTI DI 1500 BYTES.

SI DEVE PROCEDERE ALLA FRAMMENTAZIONE  
DEL DATAGRAMMA ORIGINALE IN DATAGRAMMI PIÙ  
PICCOLI

VIENGOLO TUTTI I FRAMMENTI DI DATI TRAMME  
L'ULTIMO DOVRA ESSERE MULTIPLI DI 8 byte.

L'INTESTAZIONE DEVE ESSERE CONSIDERATA  
PER OGNI FRAMMENTO

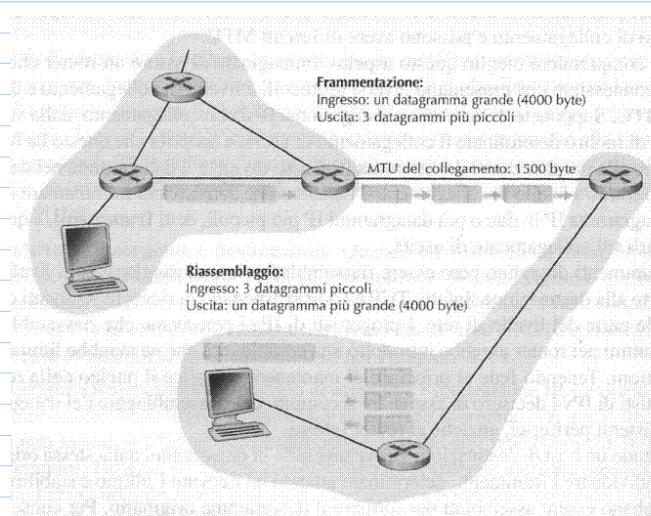
### CONSEGUENZA

SE LA MTU ACCETZATA DAL LIVELLO COLLEGAMENTO  
E 1500 Byte il payload dovrà essere  
 $1500 - 20 = 1480$

CHE FORTUNATAMENTE È UN MULTIPLO DI  
8. QUINDI PUÒ ESSERE UTILIZZATO  
QUESTO VALORE.

L'IMPLEMENTAZIONE DELLA FRAMMENTAZIONE VIENE  
GESTITA OPERANDO SUI CAMPI:

- IDENTIFICATION
- FLAG
- FRAGMENT OFFSET



Frammento	Byte	ID	Spiazzamento	Flag
1° frammento	1480 byte nel campo dati del datagramma	Identificatore = 777	Spiazzamento = 0 (i dati saranno inseriti a partire dal byte 0)	Flag = 1 (segue altro frammento)
2° frammento	1480 byte di dati	Identificatore = 777	Spiazzamento = 185 (i dati saranno inseriti a partire dal byte 1480. (Nota: $1480 = 185 \times 8$ )	Flag = 1 (segue altro frammento)
3° frammento	1020 byte di dati (Nota: $1020 = 3980 - 1480 - 1480$ )	Identificatore = 777	Spiazzamento = 370 (i dati saranno inseriti a partire dal byte 2960. $2960 = 370 \times 8$ )	Flag = 0 (ultimo frammento)

### NOTE

- SE QUALCHE FRAMMENTO NON ARRIVA A DESTINAZIONE, L'INTERO DATAGRAMMA (INCOMPLETO) VIENE ELIMINATO

SE IL LIVELLO TRASPORTO UTILIZZA TCP ALLORA SI POTRÀ RECUPERARE LA PERDITA RICHIEDENDO ALLA SORGENTE UNA NUOVA TRASMISSIONE

- Si aumenta la complessità degli apparati di rete in quanto devono gestire le operazioni di frammentazione e riassemblaggio
- Maggiore vulnerabilità ad attacchi esterni

### ESEMPIO

Un attaccante invia al dispositivo destinazione un flusso di piccoli frammenti nessuno con spiazzamento nullo.

Il dispositivo può collassare cercando di processare i datagrammi degeneri.

## ALTRA POSSIBILITÀ

FRAMMENTI CON SPIAZZAMENTI CHE SI SOVRAPPONGANO

LA VERSIONE IPv6 NON UTILIZZINA LA FRAMMENTAZIONE.

Titolo nota

## INDIRIZZI IP

OGNI DISPOSITIVO DI RETE HA UN INDIRIZZO UNICO CHE CONTIENE UN **NETID** E UN **HOSTID**.

**NETID**: NEL CASO DI UN HOST IDENTIFICA LA RETE A CUI È COLLEGATO.

**HOSTID**: IDENTIFICA IL DISPOSITIVO host

IL CONFINE TRA HOST E COLLEGAMENTO  
FISICO VIENE INDICATO COME

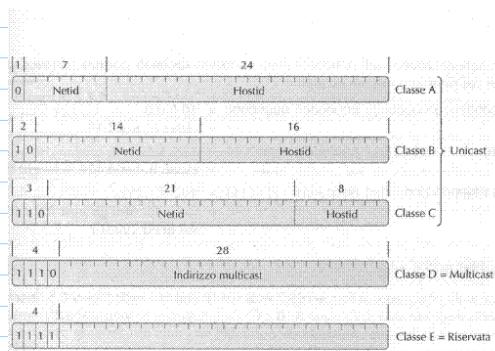
## INTERFACCIA

DALLA SUA NASCITA SONO STATI UTILIZZATI CINQUE  
SCHEMI DIVERSI PER ASSEGNARE GLI INDIRIZZI IP.

L'OBBIETTIVO RICORRENTE E' QUELLO DI AUMENTARE  
IL NUMERO DI UTENTI ED UTILIZZARE IN MODO  
MIGLIORE IL CAMPO DI INDIRIZZO DI 32 bit.

## INDIRIZZI BASATI SULLE CLASSI

### PRIMO METODO PROPOSTO



## SOTTORETI (SUBNETTING)

PRIMO TENTATIVO PER MIGLIORARE L'USO DEL CAMPO INDIRIZZO.

QUANDO SI DEVONO INTERCONNETTARE RETI DIFFERENTI IN GENERE LO SI DEVE FARE CON DISPOSITIVI (ROUTER) ED ASSEGNAENDO AD OGNI RETE UN NETID AUMENTANDO QUINDI LA RICHIESTA DI INDIRIZZI PER UNO STESSO SITO.

QUESTO PROBLEMA È STATO RISOLTO  
INTRODUCENDO IL NUOVO PARADIGMA DI  
**SOTTORETE.**

### INDIRIZZI SENZA CLASSI

PERMETTE DI UTILIZZARE TUTTO IL CAMPO  
DI INDIRIZZO IN MODO PIÙ EFFICIENTE.

NON SI HANNO SOTTOCAMPI DI DIMENSIONI  
FISSE COME NELLA METODOLOGIA A CLASSI

### TRADIZIONE DEGLI INDIRIZZI DI RETE

#### NAT : NETWORK ADDRESS TRANSLATION

DI CONCEZIONE PIÙ RECENTE DEI PRECEDENTI.

AD OGNI RETE DI ACCESSO VIENE ASSEGNAUTO  
UN SOLO INDIRIZZO IP.

QUESTO VIENE UTILIZZATO PER COLLEGAMENTI  
DEI DISPOSITIVI DI RETE VERSO L'ESTERNO.

PER LE COMUNICAZIONI INTERNE ALLA RETE  
SI UTILIZZA UN INDIRIZZO PRIVATO.

### IPv6

UTILIZZA UN CAMPO DI INDIRIZZO PIÙ ESTESO.

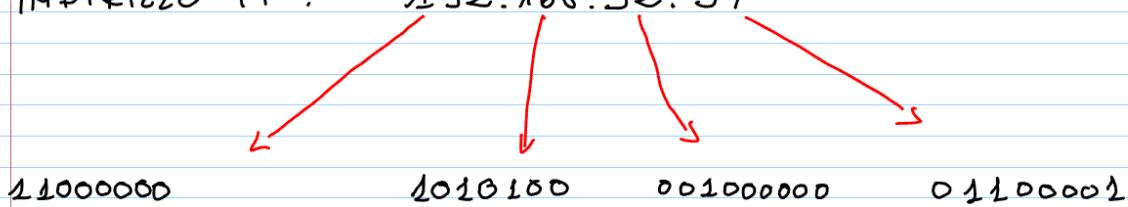
### NOTAZIONE IPv4

GLI INDIRIZZI IP VENGONO FORNITI SECONDO  
UNA NOTAZIONE DECIMALE PUNTATA.

SI HANNO 4 NUMERI SEPARATI DA UN PUNTO  
CIASCONO RIFERITO AL VALORE BINARIO DEL  
BYTE DI INDIRIZZO CORRISPONDENTE.

## ESEMPIO

INDIRIZZO IP : 192.168.32.97



## SOTTORETE

QUANDO SI DEVONO INTERCONNETTERE RETI DIFFERENTI  
(FORMATO FRAME) SI DEVONO UTILIZZARE DISPOSITIVI  
(ROUTER) IN GRADO DI GESTIRE LA FRAMMENTAZIONE

QUESTO IMPLICA CHE IL DISPOSITIVO DEVE  
AVERE UN INDIRIZZO IP PER OGNI RETE  
CHE GESTISCE

PROBLEMA CON SITI CON MOLTE RETI

IL CONCETTO DI SOTTORETE E' STATO INTRODOTTO PER SVINCOLARE LE RICHIESTE DI INTERCONNESSIONI LOCALI DA QUELLE VERSO IL MONDO INTERNET ESTERNO

TUTTO QUESTO SI TRADUCE NELL'ASSOCIARE IL NETID AL SITO E NON ALLE SINGOLE RETI

Ogni rete locale (del sito) detta SOTTORETE viene identificata mediante il campo HOSTID della metodologia a classi.

Il campo HOSTID e' quindi diviso in due sottocampi

SUBNETID : IDENTIFICATORE DELLA SOTTORETE

HOSTID : IDENTIFICATORE DEL DISPOSITIVO DELLA SOTTORETE

LA PARTE SUBNETID E HOSTID HANNO  
QUINDI UN SIGNIFICATO LOCALE ED È PER  
QUESTO INDICATA COME PARTE LOCALE

MASCHERA DI RETE (ADDRESS MASK)

SERVE PER DEFINIRE I CONFINI DEI  
SOTTOINDIRIZZI DI UNA PARTICOLARE  
RETE (NETID)

### REGOLA

HA SIMBOLI BINARI 1 NELLE POSIZIONI DEI  
BIT RIFERITI AL NETID E SUBNETID E  
SIMBOLI BINARI 0 NELLE POSIZIONI DEL  
CAMPO HOSTID

### ESEMPIO

11111111. 11111111. 11111111. 00000000

255 . 255 . 255 . 0

QUESTO SIGNIFICA CHE IL CAMPO INDIRIZZO  
RIPORTERÀ NEI PRIMI 3 BYTE LE  
INDICAZIONI NETID SUBNETID METRE IL  
QUARTO BYTE SARÀ DEDICATO AL CAMPO  
HOSTID.

### CASO PARTICOLARE

SE L'INDIRIZZO APPARTIENE ALLA CLASSE B

⇒ È PRESENTE UN BIT 0 NELLA SECONDA

POSIZIONE DEL CAMPO INDIRIZZO.

SI PUÒ CAPIRE CHE:

- I PRIMI DUE BYTE SONO IL NETID
- IL TERZO BYTE È IL SUBNETID
- IL QUARTO BYTE È IL CAMPO HOSTID

### ESEMPIO

AD UN CAMPUS È STATO ATTRIBUITO UN INDIRIZZO  
IP DI CLASSE B : 150.10.0.0

SUPPONEMMO CHE IL CAMPUS ABbia 160 SOTTORETI  
Ciascuna con non più di 70 DISPOSITIVI  
COME PUÓ ESSERE DEFINITA LA MASCHERA  
DI SOTTORETE?

### SOLUZIONE

SAPERE CHE L'INDIRIZZO È DI CLASSE B  
VUOL DIRE CHE LA PARTE NETID È LOCALE  
SOTTO DI 2 BYTE CIASCUNA.

### QUINDI:

SI SUDDIVIDE LA PARTE LOCALE ASSEGANDO  
IL PRIMO BYTE ALLA SUBNETID ED IL  
RESTANTE AL CAMPO HOSTID

## RISULTATO

255.255.255.0

## INDIRIZZI SENZA CLASSI

PROPOSTA A METÀ DEGLI ANNI '90,

PREVEDE CHE LA PARTE DI INDIRIZZO DI RETE IP  
POSSA ESSERE FORMATA DA UN NUMERO QUALSIASI  
DI bit.

UN INDIRIZZO SENZA CLASSE È

w.x.y.z/n

DOVE n INDICA IL NUMERO DI BIT DEDICATO AL

CAMPO NETIDESEMPIO

SI HA UNA RICHIESTA PER UN BLOCCO DI  
1000 ID DI HOST.

SI DEVE PREVERE 1024 HOSTID

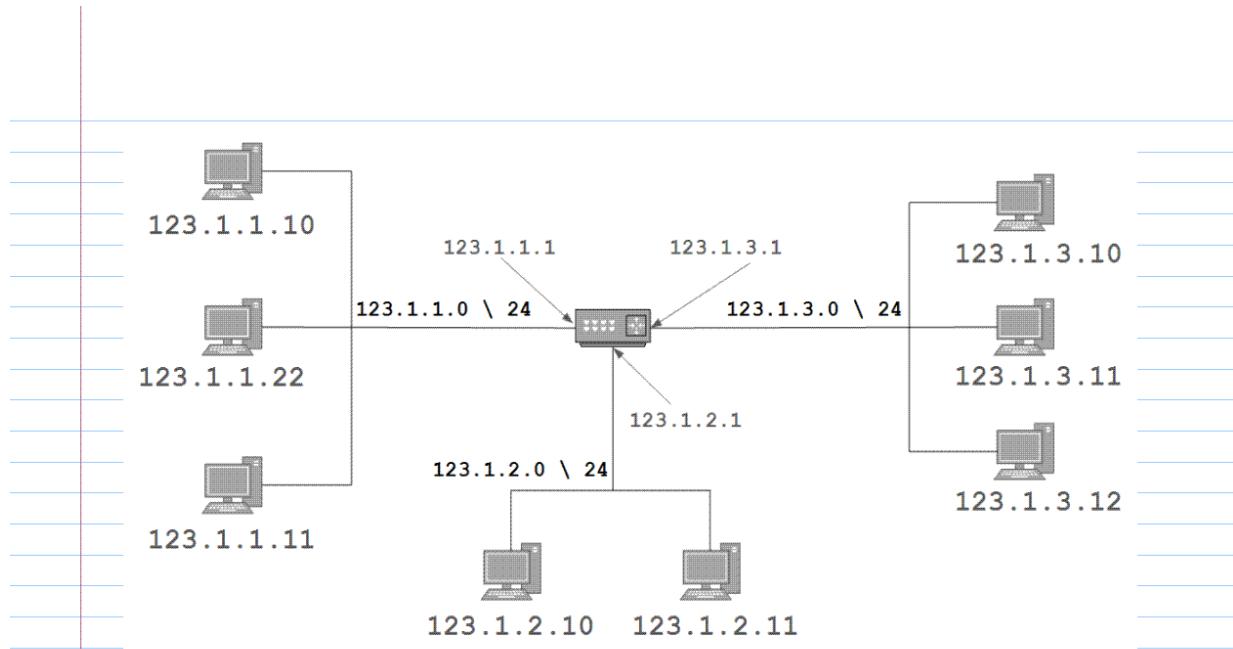
QUINDI DEI 32 bit CHE FORMANO L'INDIRIZZO  
NO DOVRANNO ESSERE RISERVATI ALLA  
SPECIFICA DEL CAMPO HOSTID

RISULTATO

w.x.y.z/22

CONSIDERAZIONE

QUESTA METODOLOGIA CONSENTE UN MIGLIORE  
UTILIZZO DEL CAMPO INDIRIZZO MA COMPLICA  
L'OPERAZIONE DI INSTRADAMENTO CHE VIENE  
REALIZZATA CON LA TECNICA CIDR



## CIDR : CLASS INTER-DOMAIN ROUTING.

ANCHE IN QUESTO CASO SI RICORRE ALLA  
DEFINIZIONE DI UNA MASCHERA

ESEMPIO :

AD UNA RETE, PARTE DI RETE PIÙ ESTESA, E'  
STATO ALLOCATO UN BLOCCO DI 1024 INDIRIZZI

Da 200.30.0.0 A 200.30.3.255

LA MASCHERA DEGLI INDIRIZZI SI OTTIENE  
IN QUESTO MODO:

200.30.0.0  $\Rightarrow$  11001000.00011110.00000000.00000000

200.30.3.255  $\Rightarrow$  11001000.00011110.00000011.111111

LA MASCHERA SARÀ:

255.255.252.0  $\Rightarrow$  11111111.11111111.11111100.00000000

IL CAMPO NETID È

200.30.0.0.

### PROCEDURA

OGNI ROUTER DI UNA GRANDE RETE CONTIENE  
UNA COPIA DELLA MASCHERA DEGLI INDIRIZZI  
DELLE RETI CHE NE FAHNO PARTE INSIEME  
AL NETID DELLA CORRISPONDENTE RETE

- IL ROUTER LEGGE L'INDIRIZZO IP DI DESTINAZIONE

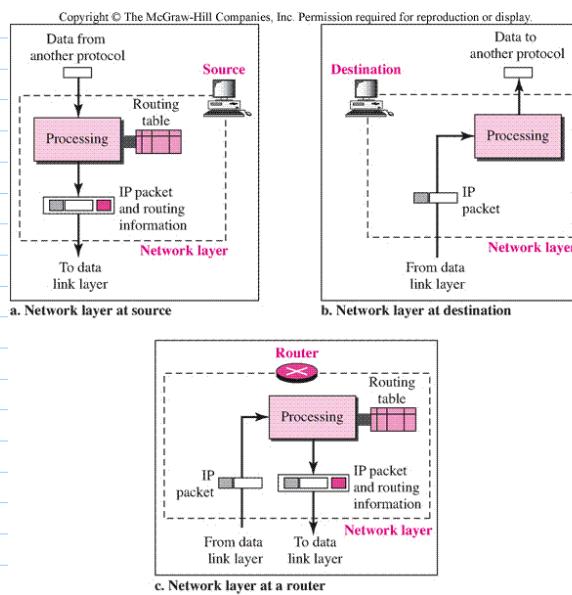
- SI ESEGUE L'OPERAZIONE AND LOGICA  
SU DI ESSO E SU LE MASCHERE  
PRESENTI IN MEMORIA

SE VIENE TROVATA UNA CORRISPONDENZA



NETID TROVATO UGUALE A QUELLO ASSOCIAZIO  
ALLA MASCHERA

IL ROUTER IDENTIFICA LA PORTA DI USCITA  
VERSO LA QUALE INDIRIZZARE IL DATAGRAMMA  
PRECEDENTEMENTE DEFINITA IN ACCORDO CON  
L'ALGORITMO DI ROUTING UTILIZZATO.



### NOTA

POÓ ACCADERE CHE UN CERTO NUMERO DI HOST ASSOCIATI AD UNA RETE A CUI È STATO ASSEGNAZIONATO UN BLOCCO CONSISTENTE DI INDIRIZZI DIA LUOGO A PIÙ DI UNA CORRISPONDENZA.

IN QUESTO CASO SI PRIVILEGIÀ LA MASCHERA  
COH IL MAGGIORE NUMERO DI 1



NUMERO MINORE DI POSSIBILI INDIRIZZI DI  
HOST.

### UN ESEMPIO PRATICO

IL PROTOCOLLO IP DEL NOSTRO DISPOSITIVO È

INDIRIZZO IP 192.168.32.97

SUBMASK 255.255.255.224

SI RICHI EDE UNA CONMESSIOME AL  
DISPOSITIVO COH INDIRIZZO IP:

192.168.32.130

PRIMO PASSOTRASDUZIONE IN BINARIO

SOURCE IP : 11000000 10101000 00100000 01100001

DESTINATION IP : 11000000 10101000 00100000 10000010

SUBNET MASK : 11111111 11111111 11111111 11100000

IL LIVELLO IP EFFETUERÀ L'OPERAZIONE DI  
AND LOGICO. SI AURÀ QUINDI:

IP DI SORGENTE

11000000 10101000 00100000 01100001 AND

11111111 11111111 11111111 11100000 =

11000000 10101000 00100000 01100000

192 . 168 . 032 . 096

ANALOGA MENTE PER L' IP DI DESTINAZIONE

11000000 101010000 00100000 10000010 AND

11111111 11111111 11111111 11000000 =

11000000 101010000 00100000 10000000

192 . 168 . 032 . 128

### DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

QUESTO PROTOCOLLO CONSENTE DI DEFINIRE

UNA PROCEDURA PER ASSEGNARE AD UN HOST

DI UNA RETE UN INDIRIZZO IP GENERALMENTE

IN MODALITÀ DINAMICA (CIOÈ NON SEMPRE

GLI VIENE ASSEGNAZIO LO STESSO IP) E SU

BASE TEMPORALE DEFINITA (NON PERMANENTE).

OLTRE A QUESTO DHCP TRASFERISCE LE SEGUENTI INFORMAZIONI:

- MASCHERA DI SOTTORETE
- INDIRIZZO DEL ROUTER PER USCIRE DALLA RETE.

DHCP E' DETTO PLUG-AND-PLAY PER LA SUA CAPACITÀ DI RENDERE AUTOMATICO IL PROCESSO DI ASSEGNAZIONE.

### ESEMPIO

IL PORTATILE O SMARTPHONE DI UNA PERSONA CHE SI SPOSTA DALLA PROPRIA RETE DOMESTICA A QUELLA DEL LUOGO DI LAVORO

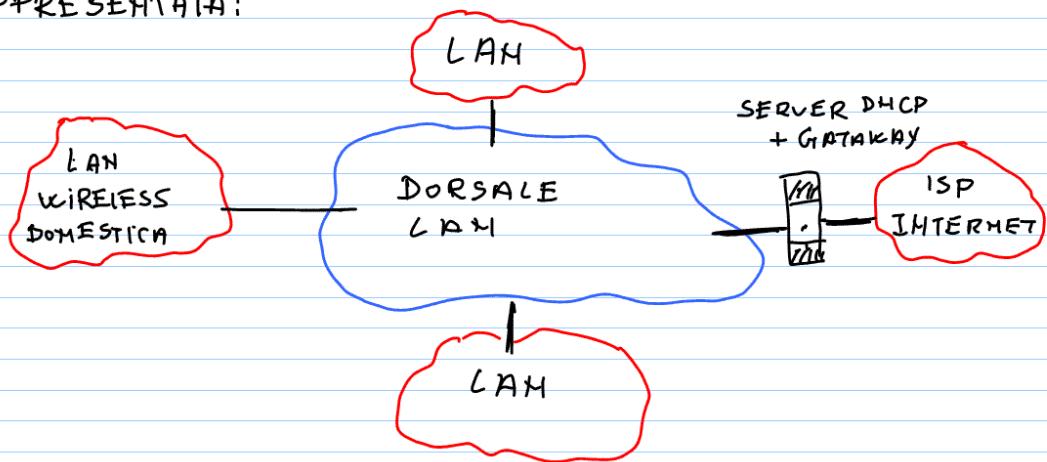
QUESTO PROTOCOLLO PERMETTE ALI ISP DI RIDURRE IL NUMERO DI INDIRIZZI IP RISPETTO AI POTENZIALI DISPOSITIVI DI UTENTE CHE SI POSSANO CONNETTERE ALLA RETE.

DHCP È DETTO PROTOCOLLO CLIENT-SERVER

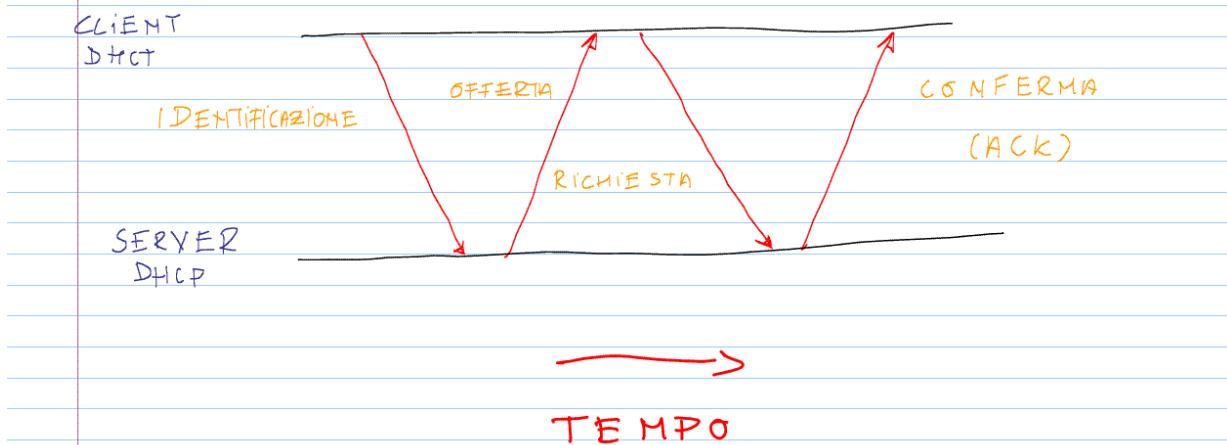
IL CLIENT È DI SOLITO UN HOST APPENA CONNESSO  
CHE DESIDERÀ INFORMAZIONI SULLA RETE DAL  
SERVER DHCP.

COME ESEMPIO SPECIFICO POSSIAMO PENSARE  
AD UN UTENTE CHE DALLA PROPRIA ABITAZIONE  
CON IL PROPRIO LAPTOP ACCEDÈ ALLA RETE INTERNET  
PER SCARICARE LA PROPRIA POSTA ELETTRONICA.

LA SITUAZIONE PRECEDENTE PUÒ ESSERE COSÌ  
RAPPRESENTATA:



LA SEQUENZA DEI MESSAGGI SCAMBIAZI E' :



### DESCRIZIONE

MESSAGGIO DI IDENTIFICAZIONE : DHCP DISCOVER

E' INVIATO DAL CLIENT DHCP (HOST CORRENTE)

A TUTTI GLI HOST UTILIZZANDO L'INDIRIZZO

BROADCAST 255.255.255.255. DI DESTINAZIONE

E COME IP SORGENTE 0.0.0.0

IL MESSAGGIO CONTIENE UN IDENTIFICATORE IN MODO

CHE IL CLIENT POSSA METTERE IN RELAZIONE LA

RISPOSTA DEL SERVER CON LA SUA RICHIESTA

QUESTO MESSAGGIO VIENE INSERITO IN UN DATAGRAMMA UDP CON PORTA SORGENTE 68 E PORTA DESTINAZIONE 67.

PER IDENTIFICARE LA RICHIESTA E' PRESENTE UN CAMPO DEFINITO TRANSACTION ID DI 32 bit CHE VIENE GENERATO CASUALMENTE.

### MESSAGGIO DI OFFERTA (DHCP OFFER)

E' LA RISPOSTA DEL SERVER CHE, OLTRE AL FLAG DI IDENTIFICAZIONE, CONTIENE LE INFORMAZIONI RIGUARDO:

- INDIRIZZO IP PROPOSTO
- MASCHERA DI RETE
- VALIDITÀ TEMPORALE DELL'ASSEGNAZIONE

NOTA: E' POSSIBILE RIMORARE LA DURATA DELL'INDIRIZZO

QUESTO MESSAGGIO VIENE INCAPSULATO IN UN DATAGRAMMA UDP CON I NUMERI DI PORTA INVERTITI.

IL DATAGRAMMA IP HA L'INDIRIZZO SORGENTE DEL SERVER DHCP CHE PROPONE L'OFFERTA E COME CAMPO DESTINATION ADDRESS ANCORA L'INDIRIZZO BROADCAST.

IL MESSAGGIO VIENE RICEVUTO DA TUTTI QUINDI ANCHE DAI SERVER DHCP.

### MESSAGGIO DI RICHIESTA (DHCP REQUEST)

L'OFFERTA PUÓ ARRIVARE DA PIÚ SERVER.

IL CLIENT SELEZIONA LA PIÚ CONVENIENTE E LA INVIA IN RETE SOTTO FORMA DI RISPOSTA SPECIFICANDO I PARAMETRI SELEZIONATI

### MESSAGGIO DI CONFERMA (DHCP ACK)

E' RESTITUITO DAL SERVER CON LA SPECIFICA DEI PARAMETRI DICHIARATI CON DHCP REQUEST IN MODO DA NOTIFICARME LA CONFERMA.

NOTA

IL MESSAGGIO DHCP\_REQUEST HA LA TESTATA IP COMPLETATA CON TUTTE LE INFORMAZIONI ACQUISITE.

IL CAMPO INDIRIZZO DESTINAZIONE È ANCORA IMPOSTATO SULLA MODALITÀ BROADCAST

SERVE PER INFORMARE GLI ALTRI SERVER DHCP CHE LA LORO OFFERTA È STATA SCARTATA

IL MESSAGGIO DI RISPOSTA / CONFIRMA DHCP ACK È INVIATO DAL SERVER PREFERITO PER CONFIRMARE LA PROPOSTA  $\Rightarrow$  POTREBBE ACCADERE CHE NEL TEMPO INTERCORSO TRA C'OFFERTA E LA RICHIESTA IL SERVER DHCP HA OFFERTO L'INDIRIZZO AD UN ALTRO RICHIEDENTE.  
IN QUESTO CASO SI INVIA DHCP\_NACK.  
LA RISPOSTA È INVIATA IN BROADCAST PER NOTIFICARE A TUTTI I SERVER L'ACCETTAZIONE O RIFIUTO DELLA RICHIESTA.

## TRADUZIONE DEGLI INDIRIZZI DI RETE

IN GENERE AD UN ISP VENGONO ASSEGNAI  
BLOCCHI DI INDIRIZZI INFERIORI AL NUMERO DI  
UTENTI.

PER SUPERARE QUESTO PROBLEMA SI ASSEGNAIO  
DINAMICAMENTE GLI INDIRIZZI SU BASE TEMPORANEA  
MEDIANTE UNA PROCEDURA DENOMINATA  
NAT : NETWORK ADDRESS TRANSLATION

LO SCOPO DELLO SCHEMA DI TRADUZIONE DEGLI INDIRIZZI DI  
RETE (NAT) E' ASSEGNARE AD OGNI RETE  
DI ACCESSO UN SOLO INDIRIZZO IP

QUESTO INDIRIZZO VIENE UTILIZZATO DA TUTTI GLI  
HOST PER COMUNICARE ALL'ESTERNO DELLA  
LORO RETE DI ACCESSO.

PER COMUNICAZIONI INTERNE ALLA RETE SI  
USA UN INDIRIZZO PRIVATO.

PER QUESTO SCOPO SONO STATI INDIVIDUATI  
TRE BLOCCHI DI INDIRIZZI PRIVATI

10.0.0.0 10.255.255.255/8

172.16.0.0 172.31.255.255/12

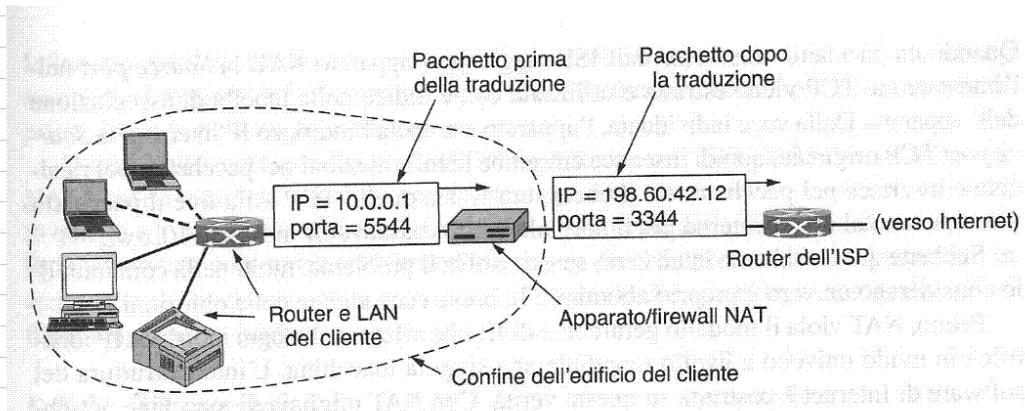
192.168.0.0 192.168.255.255/16

DI SOLITO LA SCELTA E' SUL PRIMO GRUPPO

QUANDO UN DATAGRAMMA DEVE LASCIARE LA  
RETE PRIVATA PER DIRIGERSI VERSO L'ISP  
DEVE ESSERE ESEGUITA UNA TRADUZIONE  
DI INDIRIZZO DA QUELLO PRIVATO ALL'UNICO  
INDIRIZZO ESTERNO DISPONIBILE (CONDIVISO)

QUESTA OPERAZIONE E' GESTITA DALL'APPARATO  
NAT

## FUNZIONAMENTO NAT



## DISCUSSIONE

Ogni dispositivo della rete privata ha un IP del tipo : 10.x.y.z  
 NEL NOSTRO ESEMPIO : 10.0.0.1  
 QUANDO IL DATAGRAMMA DEVE LASCIARE LA RETE PRIVATA ESSO DEVE PASSARE DAL DISPOSITIVO NAT CHE ASSOCIERÀ L'IP PRIVATO ALL'EFFETTIVO INDIRIZZO IP ASSEGNATO AL SITO.

NEL NOSTRO ESEMPIO : 192.60.42.12

### PROBLEMA

IL MECCANISMO FUNZIONA IN USCITA MA QUANDO DALL'ESTERNO SI DEVONO INVIARE DATAGRAMMI A DISPOSITIVI (HOST) DELLA RETE PRIVATA QUESTI VENGONO INDIRIZZATI A 192.60.42.12

COME RIESCE L'APPARATO NAT A CAPIRE QUALE HOST DELLA RETE PRIVATA NE È EFFETTIVAMENTE IL DESTINATARIO ?

### SOLUZIONI

- SPECIFICARE L'IP PRIVATO DEL MITTENTE DELLA TRASMISSIONE INIZIALE (E QUINDI DELLA CONSEGUENTE RISPOSTA) ➡ NON ATTUABILE PER MANCANZA NELLA TESTATA IP4 DI UN CAMPO ADEGUATO
- SFRUTTARE L'ESPERIENZA : QUESTA METODOLOGIA SI BASA SULLA COSTATAZIONE PRATICA CHE LA MAGGIOR PARTE DEI DATAGRAMMI IP È LEGATA A SERVIZI TCP O UDP.

3

NELLE INTESTAZIONI TCP E UDP E' PRESENTE  
UN CAMPO CHE IDENTIFICA IL SERVIZIO SPECIFICHO  
ID DELLA PORTA SORGENTE E DELLA  
PORTA DESTINAZIONE DELLA MACCHINA  
CHE DEVE RICEVERE IL DATAGRAMMA.

QUESTO CAMPO COMPRENDE 2 BYTES, ED  
INDICA SU BASE E2E DOVE INIZIA E TERMINA  
UN COLLEGAMENTO TRA LAYER TCP.

QUANDO UN PROCESSO DESIDERÀ STABILIRE UNA CONNESSIONE  
TCP CON UN PROCESSO REMOTO SELEZIONA UNA  
PORTA DISPONIBILE CHE DIVENTERÀ LA **PORTA  
SORGENTE**.

QUESTA SERVIRÀ PER RICONOSCERE I  
DATAGRAMMI ARRIVATI AL LIVELLO TCP E  
RELATIVI ALLA PARTICOLARE CONNESSIONE.

IL PROCESSO IDENTIFICA CON ADEGUATA PROCEDURA  
LA PORTA CON CUI IL FLUSSO DEI DATAGRAMMI  
SARÀ RICONOSCIBILE ALLA DESTINAZIONE

### PORTA DI DESTINAZIONE

COME VEDREMO LE PORTE DA 0 A 1023  
SONO PREASSEGNAME A SERVIZI NOTI.

### RICAPITOLANDO:

OGNI MESSAGGIO TCP IN USCITA CONTIENE  
L'INFORMAZIONE DELLA PORTA SORGENTE E DESTINAZIONE.  
INSIEME PERMETTONO DI IDENTIFICARE LA  
CONNESSIONE.

## PROCEDURA

LA CONOSCENZA DEL CAMPO PORTA SORGENTE  
(SOURCE PORT) OFFRE LA SOLUZIONE AL  
NOSTRO PROBLEMA.

- PER OGNI DATAGRAMMA SI SOSTITUISCE L'IP PRIVATO  
CON QUELLO PUBBLICO
- IL CAMPO SOURCE PORT È SOSTITUITO DA  
UN INDICE CHE PUNTA ALLA TABELLA INTERNA  
DEL NAT IN CORRISPONDENZA DELLA VOCE

CHE CONTIENE LA SPECIFICA SIA DELLA SOURCE Port  
SIA DELL'INDIRIZZO IP PRIVATO DELLA MACCHINA  
SORGENTE ( E QUINDI DESTINAZIONE PER I  
DATAGRAMMI IN INGRESSO).

NOTA : SI DEVONO RIDEFINIRE i CAMPI  
DI CONTROLLO DELLE TESTATE TCP E IP.

### OSSERVAZIONE

E' NECESSARIA QUESTA PROCEDURA POICHÉ IL SOLO CAMPO SOURCE PORT NON SAREBBE SUFFICIENTE.

POTREBBE ACCADERE CHE PROCESSI DI MACCHINE DIFFERENTI DECIDANO DI UTILIZZARE UNA STESSA PORTA.

### GIVUSTO PER CONCLUDERE:

QUANDO ARRIVA UN DATAGRAMMA DALL'ESTERNO LA LETTURA DEL CAMPO SOURCE Port (RIDEFINITO IN USCITA) VIENE UTILIZZATO COME INDICE NELLA TABELLA DI ASSOCIAZIONE PER RECUPERARE LE INFORMAZIONI RELATIVE ALLA EFFETTUA SPECIFICA DI SOURCE Port E DELL'INDIRIZZO IP PRIVATO DELLA MACCHINA DI DESTINAZIONE

SUCCESSIVAMENTE VENGONO RIDEFINITI I CAMPI DI CONTROLLO DELLE TESTATE TCP E IP ED INFINE IL DATAGRAMMA È INVIATO AL ROUTER INTERNO PER L'INSTRADAMENTO.

QUESTA SOLUZIONE DETTATA DALLA PRATICA NON È ACCETTATA DA TUTTI.

### CRITICITÀ

- OGNI MACCHINA NON È PIÙ ASSOCIASTA UNIVOCAMENTE AD UN INDIRIZZO IP.
- NON VALE PIÙ IL PARADIGMA DI CONNETTIVITÀ EZE. SECONDO IL QUALE UN HOST PUÒ INVIARE DATAGRAMMI AD UN ALTRO HOST IN QUALSIASI MOMENTO.  
CON L'USO DEL NAT QUESTO NON È POSSIBILE:  
UN HOST DELLA RETE PRIVATA PUÒ ESSERE RAGGIUNTO DA UN HOST ESTERNO.

I DATAGRAMMI IN INGRESSO POSSONO ESSERE CORRETTAMENTE ACCETTATI SOLO DOPO QUELLI IN USCITA.

E' POSSIBILE RISOLVERE QUESTA CRITICITÀ ADOTTANDO PROCEDURE SPECIFICHE (NAT TRAVERSAL)

- INTERNET DIVIENE CONNECTION ORIENTED.

QUESTO INFILISCE ANCHE SULLA RESILIENZA DELLA

RÈTE → SE IL NAT SI GUASTA TUTTE

LE CONNESSIONI MEMORIZZATE SI PERDONO.

- SI VIOLA IL PRINCIPIO BASE DELLA STRATIFICAZIONE DEI PROTOCOLLI:

SE IL LIVELLO TCP FOSSE RIDISSEGNATO PREVEDENDO

INTESTAZIONI DIFFERENTI (ES. SOURCE PORT A

32 bit) IL NAT NON FUNZIONEREbbe.

- ALCHE APPLICAZIONI USANO PIÙ PORTE.

- NUMERO DI ASSOCIAZIONI POSSIBILE ALTO

MA LIMITATO

## CONCLUSIONE

NONO STANTE LE PRECEDENTI CRITICITÀ IL  
MECCANISMO NAT È RELATIVAMENTE  
SEMPLICE ED HA INDUBBIAMENTE UN EFFETTO  
BENEFICO NEI RIGUARDI DEL PROBLEMA DELLA  
LIMITAZIONE DEGLI INDIRIZZI IP DISPONIBILI  
PER QUESTO, AD OGGI, È DIFFICILE PREDIRE  
CHE VENGÀ ABBANDONATO.