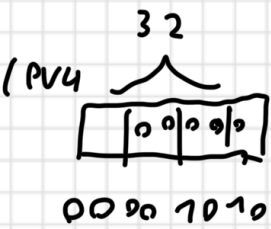


IPV4 RPL 78

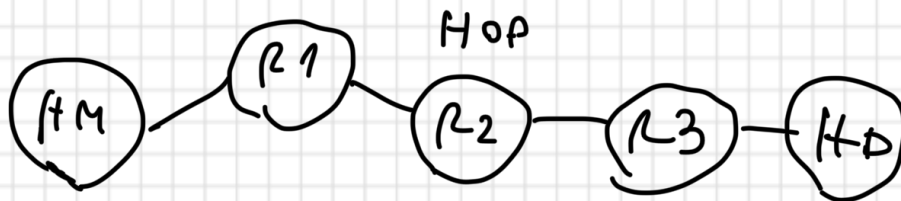
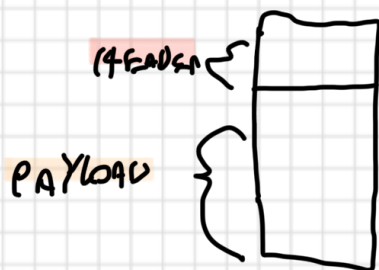
$2^{24}$  (15M128)  
10.0.0.0 - 10.255.255.255



172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

DATA GRAM



UNA DELLE AFFIDABILITÀ DEL DATA GRAM È QUELLA DI CERCARE LA  
VIA PIÙ COME PER RAGGIUNGERE IL RECEIVER.

QUALITÀ DI SERVIZIO (QoS) = È UN INSIEME DI

TECNOLOGIE E MECCANISMI CHE PERMETTONO DI GESTIRE

E OTTIMIZZARE LE RISORSE DI RETE PER GARANTIRE  
SPECIFICI LIVELLI DI PERFORMANCE.

QD) NEL CASO IPV4 MA ANCHE IPV6 N/A NE CHIAMATO BEST EFFORT.

NO- ABBIAMO NESSUNA GARANZIA CHE VADA A DESTINAZIONE SE MANDO 8 DATACRAMMI, ALLO STESSO RICEVUTA.

SE LI RICEVE, NON E' DETTO CHE LI RICEVE IN ORDINE IN CUI ESSI SONO STATI MANDATI.

I PROGETTISTI HANNO DECISO DI USARE LA QD) RELATIVAMENTE BASSA PER CENLANDO DI SEMPLIFICARE IL PENCONO.

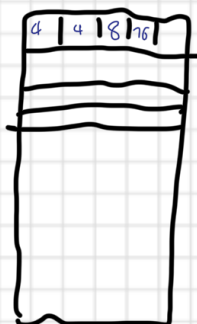
UDP = PROTOCOLLO QUASI VUOTO, MA HA PERO' LA POSSIBILITA' DI USARE IPV4 COSI' COM'E'.

INTESTAZIONE (HEADER):

SI USANO DIVERSE CONVENZIONI OVVERO PENSANO CON PIANO A 32 BIT.

LA PRIMA PIANO E' SUDDIVISA IN 4 PARTI.

HEADER



I PRIMI 4 BIT SONO INTERPRETATI COME UN NUMERO  
INTERO TRA 0 E 15  $\Rightarrow$  NUMERO DI VERSIONI OTTO  
NEL PRV 1 PRIMI 4 BIT ASSUMONO VERSIONE OTTO

IN BASE AL TIPO DI PV (4 BIT) I COMPONENTI  
IN MANIERA DIVERSA.

LA MANIERA STANDARD PER CONTROLLARE PROBLEMI/ERRORI  
E' QUELLO DI ELENCHARE IL DATA CREAMMA.

LA CATTURA DEL SECONDO 4 BIT MI PERMETTONO  
DI CAPIRE LA LUNGHEZZA DELL'INTERSTAGIONE PERO'  
ALLORA INFORMAZIONI POSSONO ANCHE ESSERE OMESSE  
E MI DICE SE CI SONO O PERO.

PRV 4 NON HA OPZIONI.

Gli ALTRI 8 BIT SI CHIAMANO TYPE DI SERVIZIO

16 BIT: MI DICONO LA LUNGHEZZA DEL DATA  
GRAMMA, LUNGHEZZA IN BYTE.

I SUCCESSIVI 32 BIT SONO DIVISI IN 3 PARTI:

1) IDENTIFICATORE: RAPPRESENTA SU 16 BIT

2) SERVE PER CRESTARE LA FRAMMENTAZIONE DEL  
DATA CREAMMA: 16 BIT DIVISI IN 3 BIT

CHIAMATI FLAG

3) SUDDIVISA ARCHITETTURA IN 3 PARTI:

1 BYTE HA 8 BIT, SECONDO HA 8 BIT E  
ULTIMO 16 BIT.

1 BYTE: SI CHIAMA TTL (TIME TO LIVE)

2 BYTE: NEXT LEVEL PROTOCOL

16 BIT RIMANGONO: SI CHIAMANO CHECK SUM

SE DATACAM FASSE DISPARI POTREBBE ESSERE UNA  
DIFFERENZA DI PRESSIONE.

TRACE ROUT = MI SERVE PER IDENTIFICARE I PERSONI  
DEI DATACAM

ICMP = PROTOCOLLO AUSILIARIO SEMPRE AL LIVELLO  
3 E MI SERVE PER MANDARE MESSAGGI DI  
ERRORE.

SE FALLISSE L'INVIO PUO' NOTIFICARMI L'ERRORE.

CONTINGE L'INDIRIZZO IP CHE SANDEBBE QUELLO DEL  
PRIMO ROUTER QUINDI POSSO DIRE

L'IP DE ROUTER 1 ( $IP_{n1}$ ), ROUTER 2 ( $IP_{n2}$ ) ECC.

QUANDO ARRIVA ALL'HOST SI DESTINGUE:

NUOVA TUTTE LE DISTANZE DO CIGRUE ROUTER

E POSSO FARE TUTTO QUELLO GRAZIE ALLA

"LIBERTÀ" DI SEMPLIFICARE IL TIME TO LEAVE.

L'HEADER SI CORRIGE CON UN INDIZIO MENTRE È  
ACCIDENTE.

GLI INDIZI PERMAN, NON VERGON "STANDARD" OVVERO RAN  
POSSO INDICARE, SOLO GLI INDIZI PUBBLICI POSSO  
ESSERE INVIATI.

NEXT LEVEL PROTOCOL = INDICA SE UTILIZZIAMO IL  
PROTOCOLLO TCP O UDP

CHI PUÒ USARE IL LIVELLO 3? IL LIVELLO 4 QUINDI  
ALL'INTERNO DEL PIAVIOLO POSSO QUINDI TRAVARE  
ANCHE PROTOCOLLI DEL LIVELLO 3

HEADER QUINDI INCAPUBA VARE INFORMAZIONI, PER QUESTO  
MOTIVO POSSO TRAVARE IPV6 ALL'INTERNO DI UN IPV4  
O VICEVERSA (CONTROLLARE PER SICUREZZA)



ENTRANCE: PROTOCOLLO 2 MA ANCHE L'ALTRA 1  
IN QUANTO LA VOLTA SIA IN REGISTRO FUOCO CUG  
VIRIVALE.

CHECKSUM = CONTROLLO DI INTEGRITÀ.  
CI SONO DIVERSI ALGORITMI PER VERIFICARE  
L'INTEGRITÀ.

CHECKSUM USA UN ALGORITMO A 16 BIT

VANTAGGIO: SEMPLICE DA CALCOLARE

CONTRO: NON TUTTI GLI ERRORI POSSONO ESSERE  
RICOROSIVITI.

CI SONO ALTRI ALGORITMI PIU' AFFIDABILI:  
COME AD ESEMPIO CRC 32

CHECKSUM A 16 BIT E' LA VERSIONE PIU'  
USATA MA SERVE PER VERIFICARE L'INTEGRITA'  
DI INTEGRITA' VIENE USATO SOLO NEI HEADER  
SE FALLISSE IL CHECKSUM SULL'HEADER IL DATACAM  
VIENE PERDUTO.

CHECKSUM E' MILIA DI PROTEZIONE SOLO A LIVELLO 3

IL ROUTER VA A MODIFICARE IL TTL,

MA SE CAMBIA IL TTL DEVO RICALCOLARE IL  
CHECKSUM

LE COSE CHE CAMBIANO SONO TTL E CHECKSUM