Problemi con IPv4 e IPv6

IPv4 presenta delle problematiche che verrano risolte con l'introduzione di IPv6 :

Tabelle di routing: Dentro i router sono presenti delle tabelle di instradamento che indicano le porte di uscita in base alla destinazione che il pacchetto in ingresso deve raggiungere. Le tabelle di routing iniziano a diventare parecchio complicate a causa del vecchio standard IP che assegnava in modo disordinato le locazioni geografiche .

Indirizzi : Dato che gli indirizzi IPv4 sono gerarchici, bisogna distribuirli secondo un certo criterio, ma purtroppo i gruppi di indirizzi sono stati assegnati in maniera disordinata (a casaccio).

In IPv4, gli indirizzi sono a 32 bit, scritti in formato decimale puntato e sono divisi in classi di indirizzi. Ciò significa che solo un numero limitato di indirizzi IPv4 sono disponibili per l'uso (circa 4 miliardi).

In IPv6, gli indirizzi sono a 128 bit e sono scritti in formato esadecimale. Questo sistema di indirizzamento offre un numero molto più grande di indirizzi rispetto ad IPv4, quasi illimitato.

Sicurezza : riguarda la mancanza di meccanismi di sicurezza adeguati a proteggere i dati trasmessi sulla rete. Il livello di sicurezza di IPv4, posto dopo il livello di trasporto, tiene in chiaro tutti i dati successivi, inclusi gli indirizzi IP e le porte. Questi dati sensibili vengono trasmessi in chiaro, rendendoli vulnerabili agli attacchi di spoofing degli indirizzi IP. IPv6 invece supporta la crittografia e la sicurezza dei pacchetti attraverso l'utilizzo di IPsec, un insieme di protocolli di sicurezza che forniscono autenticazione, integrità dei dati e crittografia per i pacchetti IP.

Autoconfigurazione (Plug & Play): in IPv4, la configurazione degli indirizzi IP e delle impostazioni di rete di un dispositivo deve essere effettuata manualmente o mediante l'utilizzo di protocolli come DHCP. L'autoconfigurazione plug and play è una funzionalità di IPv6 che consente ai dispositivi di configurare automaticamente la propria interfaccia di rete, senza la necessità di un amministratore di rete o di un server DHCP.

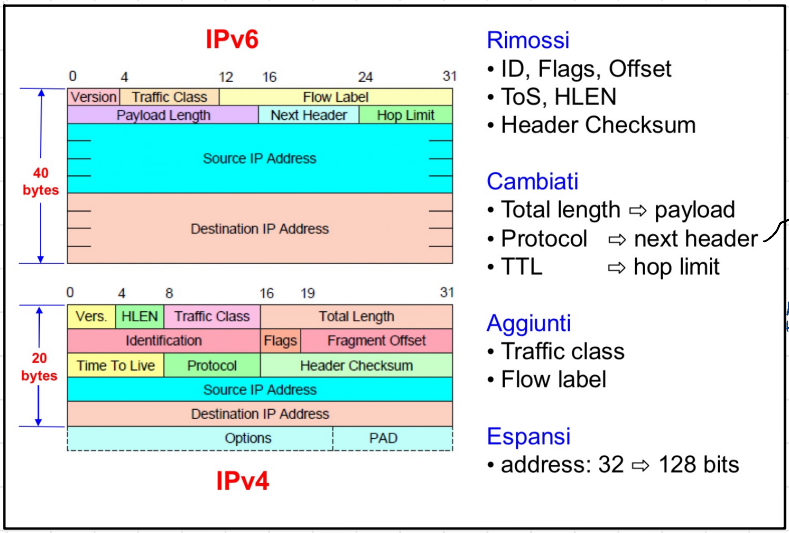
Rimane essenziale DHCPv6 perche plug&play non fornisce gateway predefinito e server DNS

Gestione della qualità del servizio (QoS): la gestione della QoS è un problema importante nella comunicazione di rete, poiché consente di garantire determinati livelli di servizio per le applicazioni. In IPv4, la QoS è gestita mediante il campo Type of Service (ToS) nell'intestazione IP ma non viene mai sfruttato. In IPv6 il bit Flow Label consente di fornire un livello di servizio differenziato per flussi di traffico specifici sulla rete.

Indirizzamento multicast: in IPv4, l'indirizzamento multicast è limitato ai soli indirizzi di classe D, che consentono la trasmissione di dati a un gruppo di destinatari. Lo spazio di indirizzamento multicast in IPv4 è limitato e non è sufficiente per supportare un gran numero di gruppi multicast. Gli indirizzi multicast IPv6 sono un sottoinsieme degli indirizzi IPv6 e hanno una struttura specifica per supportare l'invio di pacchetti a più host contemporaneamente. Gli indirizzi multicast IPv6 iniziano con il prefisso `**ff**`, seguito da altri campi che consentono una maggiore flessibilità nella definizione di gruppi multicast

Indirizzamento host mobili: consente a un dispositivo di mantenere la stessa configurazione di rete IPv6 mentre si sposta da una rete a un'altra. Un dispositivo mobile possiede un indirizzo IPv6 permanente, noto come "indirizzo di casa", che è associato alla sua interfaccia di rete. Quando il dispositivo si sposta in una nuova rete, ottiene un nuovo indirizzo IPv6 temporaneo, noto come "indirizzo di cura", sulla nuova rete. Il dispositivo continua a utilizzare l'indirizzo di casa come il suo indirizzo permanente, ma utilizza l'indirizzo di cura come l'indirizzo sorgente per tutte le comunicazioni in uscita sulla nuova rete. In questo modo, le comunicazioni in uscita sembrano provenire dalla nuova rete, anche se il dispositivo conserva il suo indirizzo permanente

Datagramma IPv6



liste linkate dove ogni nodo è un header opzionale che viene aggiunto
NB vi è un CAMPO Total Length Header che è dice la lunghezza

La dimensione del datagramma IPv4 è variabile a seguito di campi opzionali che fanno passare la dimensione dell'header da 20 fino a 60 byte, questo rende complicata la ricerca attraverso le memorie associative. L'header in IPv6 ha infatti una lunghezza fissa di 40 byte, il che permette di rimuovere il campo che specifica la lunghezza dell'header.

In quanto non veniva utilizzato è stato rimosso anche il controllo dell'integrità dell'header tramite l'header checksum.

Il campo TTL non rappresentava un tempo ma un numero di nodi nel caso di IPv4, con IPv6 questo campo identifica invece un tempo reale massimo, entro il quale il pacchetto deve arrivare a destinazione o viene scartato.

In IPv6 viene meno il campo **protocol** e viene sostituito con **next header** , ovvero delle liste linkate nelle quali ogni nodo è un servizio o header opzionale che viene aggiunto al servizio già esistente. Un header opzionale contiene come primo campo un parametro "next header" che contiene il link al prossimo campo, messo all'inizio in quanto più veloce da trovare perchè ogni campo ha lunghezza variabile. Un secondo campo specifica appunto la lunghezza dell'header opzionale. Sono stati tolti i vari flag, offset ecc e sono stati inseriti tutti come header opzionali.

Non è possibile riassemblare la lista linkata inserendo dei nodi in mezzo e quindi il solo router mittente può eseguire la frammentazione del pacchetto ed è stato inoltre specificato un MTU minimo di 1280 byte per supportare un trasferimento tramite IPv6. In IPv4 se si perde un frammento si necessita di ritrasmettere l'intero pacchetto, IPv6 quindi obbliga a non poter frammentare. Viene previsto un header anche per la sicurezza "authentication header" che codifica tutto il resto del pacchetto.

In pratica con IPv6, il campo di offset del frammento è stato rimosso dall'intestazione del pacchetto, e quindi i router intermedi non possono frammentare il pacchetto. Invece, la frammentazione deve essere gestita dai dispositivi sorgente, che devono suddividere i dati in pacchetti con una dimensione inferiore al payload massimo definito da IPv6.

Struttura indirizzo IPv6

Un indirizzo IPv6 ha una struttura di 16 byte, ovvero128 bit, divisi in 8 gruppi di 16 bit (ovvero da 4 nibble) ciascuno, separati da due punti (:) .

Un indirizzo IPv6 è scritto in notazione esadecimale, che rappresenta ogni gruppo di 16 bit con un numero esadecimale da 0 a F. Per facilitare la scrittura degli indirizzi IPv6, è possibile omettere gli zeri iniziali di ogni gruppo di 16 bit e comprimere i gruppi di zeri consecutivi in un singolo gruppo di zeri, indicato con i due punti (::). Tuttavia, questa compressione può essere utilizzata solo una volta in ogni indirizzo IPv6.

Un esempio di indirizzo IPv6 scritto in notazione esadecimale è:

2001 : 0db8 : 85a3 : 0000 : 0000 : 8a2e : 0370 : 7334

Questo stesso indirizzo potrebbe essere scritto con la compressione dei gruppi di zeri consecutivi:

2001 : db8 : 85a3 :: 8a2e : 370 : 7334

L'indirizzo IPv6 può anche includere una prefisso di rete, che specifica la porzione dell'indirizzo che identifica la rete, e una porzione di interfaccia, che identifica il singolo host all'interno della rete. Il prefisso di rete è solitamente specificato con una lunghezza di prefisso, indicando il numero di bit che compongono la parte di rete (solitamente i primi 2 o 3 blocchi di 4 nibble) dell'indirizzo IPv6.

Ad esempio, un prefisso di rete di 64 bit indica che i primi 64 bit dell'indirizzo IPv6 sono riservati alla rete, mentre gli ultimi 64 bit sono utilizzati per identificare l'interfaccia host all'interno di quella rete.

Subnet mask in IPv6

La subnetting in IPv6 è analoga a quella in IPv4, ma con l'utilizzo di indirizzi a 128 bit anziché a 32 bit. Ciò significa che il numero di subnet disponibili è molto più elevato rispetto ad IPv4.
Per indicare la maschera di sottorete in IPv6, si utilizza il prefisso di sottorete, che specifica quanti bit dell'indirizzo IPv6 sono riservati alla sottorete. Il prefisso di sottorete viene solitamente specificato come un multiplo di 16 bit, ovvero un blocco di 4 nibble. Ad esempio, se si utilizza un prefisso di sottorete di /64, i primi 64 bit dell'indirizzo IPv6 sono riservati alla sottorete, mentre i restanti 64 bit sono riservati all'identificatore dell'interfaccia.

Indirizzi riservati

Gli indirizzi IPv6 riservati sono indirizzi che non sono assegnati ad alcuna interfaccia di rete e sono stati riservati per scopi speciali. Questi indirizzi non sono utilizzabili per la comunicazione su Internet e non possono essere assegnati a nessun host.

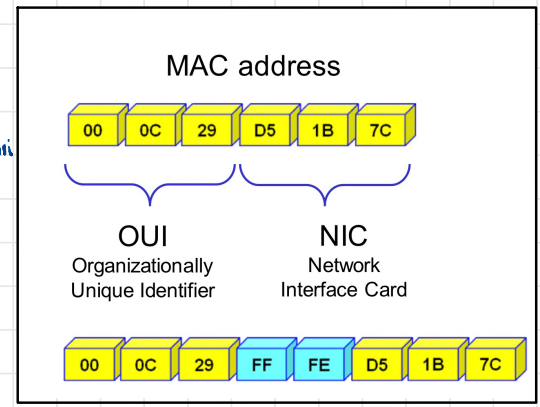
- Gli indirizzi **FEC0::/48** sono stati originariamente riservati per l'indirizzamento di sito locale, ovvero per la comunicazione tra nodi all'interno di un sito

- Gli indirizzi **FE80::/64** sono utilizzati per gli indirizzi di **local-link**, ovvero indirizzi che possono essere utilizzati solo all'interno di una rete locale e che non sono instradati su Internet. Questi indirizzi vengono utilizzati per la comunicazione tra nodi della **stessa rete locale**, ad esempio tra due computer collegati alla stessa LAN e non possono essere assegnati a dispositivi su reti differenti.
  Gli indirizzi local link IPv6 sono simili agli indirizzi privati IPv4 in quanto entrambi sono utilizzati all'interno di una rete privata e non sono accessibili direttamente dall'esterno della rete.

EUI-64 (extended unique identifier-64) + 64 dal prefisso di rete

Gli indirizzi IPv6 globali, ovvero quelli che è possibile utilizzare per navigare in rete, vengono autogenerati a partire dal MAC address della scheda di rete del dispositivo stesso.
L'EUI-64 è un metodo di generazione degli identificatori per le interfacce di rete in IPv6. EUI-64 usa l'indirizzo MAC della scheda di rete, composto da 6 byte (48 bit) e lo modifica inserendo un blocco **FF:FE** da 2 byte (16 bit) in mezzo tra i primi e gli ultimi tre byte del MAC, ottenendo i 64 bit che identificano l'interfaccia di rete.

Indirizzi Globali AUTOGENERATI A PARTIRE DAL MAC della schede di Rete
EUI-64 = genera gli identificatori per le interfaccie di rete.
inserisce due Blocchi FF::FE da 2 byte così diventa 64 bit



Questo metodo semplifica la configurazione automatica degli indirizzi IPv6 per le interfacce di rete, garantendo anche l'unicità degli identificatori.

Comunicazione tra reti con IPv6

Gli indirizzi IPv6 sono suddivisi in quattro tipi principali:

- **Unicast** : identificano in modo univoco un'interfaccia di rete su una singola macchina. Sono utilizzati per la comunicazione diretta tra due host.
- **Broadcast** : in IPv6 non esiste più il concetto di indirizzo broadcast. Viene invece utilizzato il concetto di indirizzo multicast per la comunicazione a tutti i nodi di una rete.
- **Multicast** : identificano un gruppo di interfacce di rete che hanno una qualifica specifica e vengono utilizzati per la comunicazione di gruppo. Sono identificati da un prefisso iniziale "FF" seguito da un numero identificativo che specifica il gruppo di destinazione.
- **Anycast** : novità di IPv6, identificano un insieme di interfacce di rete, ma solo una di queste viene selezionata come destinazione del pacchetto. Viene utilizzato il concetto di anycast per identificare il nodo più vicino in una rete che condivide lo stesso indirizzo anycast.

Comunicazione tra reti con IPv6

Quando un dispositivo IPv6 ha bisogno di comunicare con un altro dispositivo **sulla stessa rete**, utilizza NDP (ARP) per determinare il suo indirizzo MAC. In questo modo, il dispositivo che ha iniziato la comunicazione può mappare l'indirizzo IPv6 del destinatario con il suo indirizzo MAC e inviare i pacchetti direttamente a livello di link layer.

Per quanto riguarda la comunicazione **tra LAN differenti**, viene utilizzato il protocollo DHCPv6 per assegnare gli indirizzi IPv6 ai client e per fornire altre informazioni di configurazione come il gateway predefinito e i server DNS (cose che non da l'autoconfigurazione Plug&Play). Non ha più senso utilizzare NAT in IPv6 poiché lo spazio degli indirizzi è molto ampio e non esiste più il problema di esaurimento degli indirizzi come in IPv4.