

IPV6

Indice generale

La necessità di IPv6.....	2
La necessità di IPv6.....	2
Internet of Everything.....	2
Coesistenza di IPv4 e IPv6.....	2
Rappresentazione degli indirizzi IPv6.....	4
Formato preferito.....	4
Regola 1: Omettere gli zeri iniziali.....	6
Regola 2: Omettere i segmenti costituiti da tutti 0.....	6
Tipi di indirizzi IPv6.....	7
Lunghezza del prefisso IPv6.....	8
Indirizzi IPv6 unicast.....	8
Indirizzi IPv6 unicast link-local.....	9
Struttura di un indirizzo IPv6 unicast globale.....	11
Configurazione statica di un indirizzo unicast globale.....	13
Processo EUI-64 e numero generato in modo casuale.....	19
Processo EUI-64.....	19
ID interfaccia generato in modo casuale.....	20
Indirizzi link-local dinamici.....	22
Indirizzi link-local statici.....	24
Indirizzi IPv6 multicast assegnati.....	28
Indirizzi IPv6 multicast richiesti dal nodo.....	30
ICMPv4 e ICMPv6.....	30
Messaggi RS e RA ICMPv6.....	31
Ping: Verifica dello stack locale.....	33

La necessità di IPv6

IPv6 è stato progettato per essere il successore di IPv4. IPv6 prevede uno spazio degli indirizzi più ampio a 128 bit, in grado di generare 340 sistilioni di indirizzi (ossia il numero 340 seguito da 36 zeri). Tuttavia, IPv6 non si limita a un numero maggiore di indirizzi. Quando l'IETF ha iniziato a sviluppare un successore per IPv4, ha sfruttato questa opportunità per risolvere le limitazioni di IPv4 e includere ulteriori miglioramenti. Un esempio è il protocollo Internet Control Message Protocol versione 6 (ICMPv6), che include la risoluzione degli indirizzi e la configurazione automatica degli indirizzi, assenti in ICMP per IPv4 (ICMPv4).

La necessità di IPv6

L'esaurimento dello spazio degli indirizzi IPv4 è stato il fattore motivante per il passaggio a IPv6. Con l'aumento delle connessioni a Internet in Africa, Asia e in altre parti del mondo, non esistono indirizzi IPv4 sufficienti per supportare questa crescita.

In teoria, il numero massimo di indirizzi IPv4 è 4,3 miliardi. Gli indirizzi privati in combinazione con Network Address Translation (NAT) sono stati fondamentali per rallentare l'esaurimento dello spazio degli indirizzi IPv4. Tuttavia, NAT danneggia molte applicazioni e presenta limitazioni che ostacolano seriamente le comunicazioni peer-to-peer.

Internet of Everything

L'Internet di oggi è radicalmente diverso da quello degli scorsi decenni. L'Internet di oggi non è costituito soltanto da e-mail, pagine Web e trasferimento di file tra computer. Internet, con la sua evoluzione, sta diventando l'"Internet delle cose". L'accesso a Internet non avverrà più solo da dispositivi quali computer, tablet e smartphone. I dispositivi di domani, dotati di sensori e di connessione a Internet, comprenderanno tutto: dalle automobili ai dispositivi biomedici, dagli elettrodomestici agli ecosistemi naturali.

Con una popolazione Internet in aumento, uno spazio degli indirizzi IPv4 limitato, i problemi di NAT e lo sviluppo dell'Internet of Everything, è giunto il momento di iniziare la transizione verso IPv6.

Coesistenza di IPv4 e IPv6

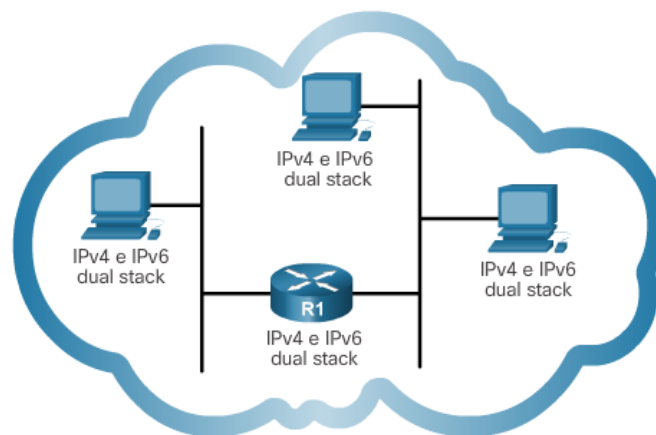
Non è stata stabilita una data per il passaggio a IPv6. Per il futuro prossimo, IPv4 e IPv6 coesisteranno. Si prevede che la transizione durerà anni. L'IETF ha creato vari protocolli e strumenti per aiutare gli amministratori di rete a migrare le proprie reti a IPv6. Le tecniche di migrazione possono essere suddivise in tre categorie:

- **Dual stack:** come mostrato nella Figura 1, dual stack consente la coesistenza di IPv4 e IPv6 nello stesso segmento di rete. I dispositivi dual stack eseguono contemporaneamente gli stack dei protocolli IPv4 e IPv6.

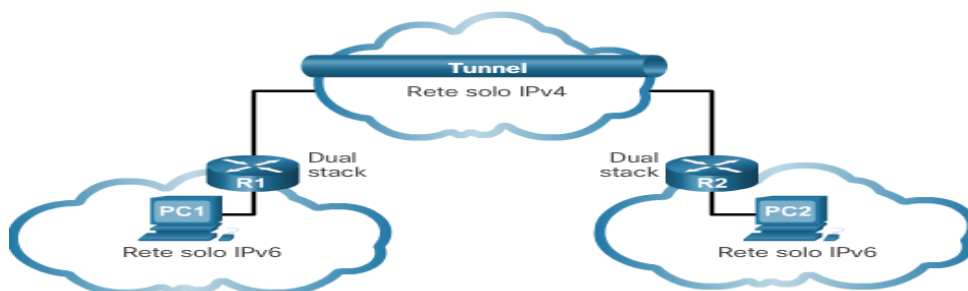
- **Tunneling:** come mostrato nella Figura 2, il tunneling è un metodo di trasporto di un pacchetto IPv6 su una rete IPv4. Il pacchetto IPv6 è incapsulato in un pacchetto IPv4, come avviene per altri tipi di dati.
- **Traduzione:** come mostrato nella Figura 3, Network Address Translation 64 (NAT64) consente ai dispositivi abilitati per IPv6 di comunicare con dispositivi abilitati per IPv4 utilizzando una tecnica di traduzione simile a NAT per IPv4. Un pacchetto IPv6 viene tradotto in un pacchetto IPv4 e viceversa.

Nota: il tunneling e la traduzione vengono utilizzati solo laddove necessario. L'obiettivo dovrebbe essere ottenere comunicazioni IPv6 native dall'origine alla destinazione.

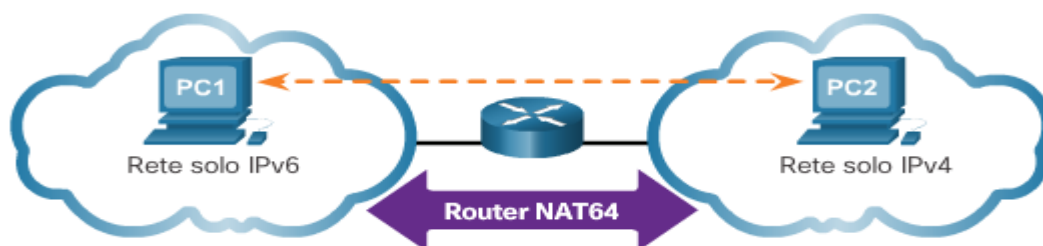
Dual stack



Tunneling



Traduzione



Rappresentazione degli indirizzi IPv6

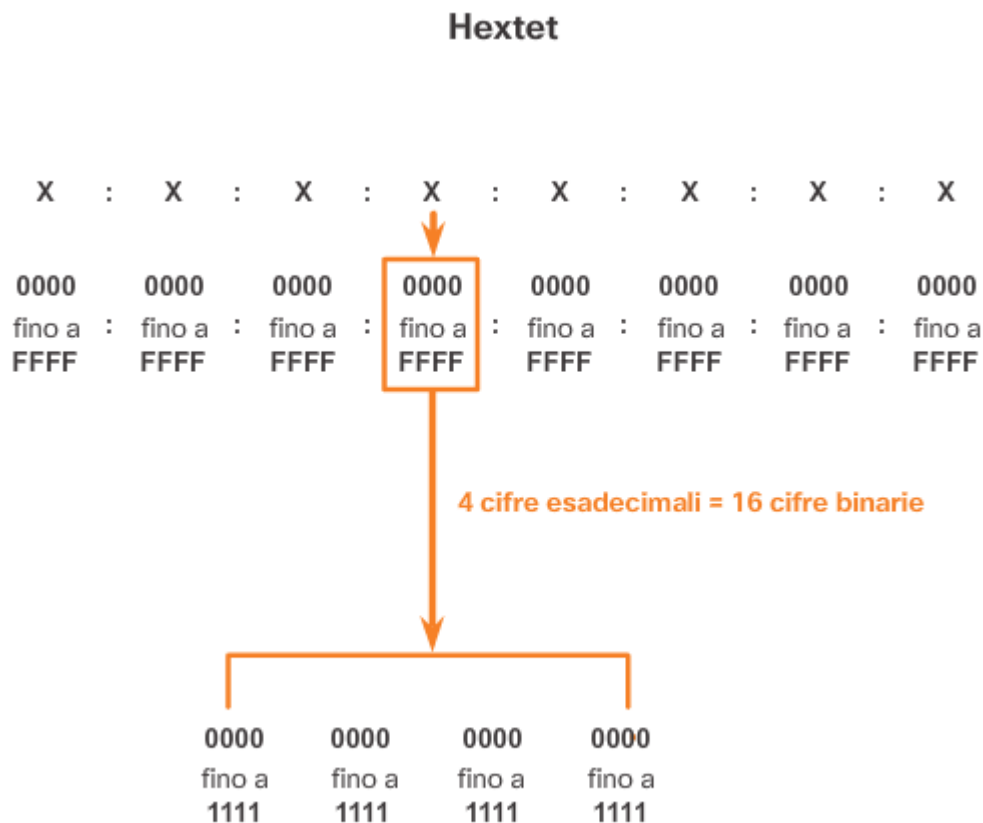
Gli indirizzi IPv6 hanno una lunghezza di 128 bit e sono scritti sotto forma di stringa di valori esadecimali. Ogni gruppo di 4 bit è rappresentato da una singola cifra esadecimale, per un totale di 32 valori esadecimali, come mostrato nella Figura 1. Agli indirizzi IPv6 non si applica la distinzione tra maiuscole e minuscole e possono essere scritti in lettere minuscole o maiuscole.

Formato preferito

Come mostrato nella Figura 1, il formato preferito per scrivere un indirizzo IPv6 è x:x:x:x:x:x:x, dove ogni "x" rappresenta quattro valori esadecimali. Quando ci si riferisce agli 8 bit di un indirizzo IPv4, si utilizza il termine otetto. In IPv6, "hextet" è il termine non ufficiale utilizzato per indicare un segmento di 16 bit o di quattro valori esadecimali. Ogni "x" corrisponde a un unico hextet, 16 bit o quattro cifre esadecimali.

Quando si parla di "formato preferito", si intende che l'indirizzo IPv6 è scritto utilizzando tutte le 32 cifre esadecimali. Non significa necessariamente che sia il metodo ideale per rappresentare gli indirizzi IPv6. Nelle seguenti pagine, verranno analizzate due regole che contribuiscono a ridurre il numero di cifre necessarie per rappresentare un indirizzo IPv6.

La Figura 2 è un riepilogo della relazione tra numerazione decimale, binaria ed esadecimale. La Figura 3 presenta esempi di indirizzi IPv6 nel formato preferito.



Numerazione esadecimale

Equivalenti decimali e binari dei valori esadecimali da 0 a F

Decimale	Binario	Esadecimale
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Esempi di formato preferito

```

2001 : 0DB8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
2001 : 0DB8 : 0000 : 00A3 : ABCD : 0000 : 0000 : 1234
2001 : 0DB8 : 000A : 0001 : 0000 : 0000 : 0000 : 0100
2001 : 0DB8 : AAAA : 0001 : 0000 : 0000 : 0000 : 0200
FE80 : 0000 : 0000 : 0000 : 0123 : 4567 : 89AB : CDEF
FE80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
FF02 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
FF02 : 0000 : 0000 : 0000 : 0000 : 0001 : FF00 : 0200
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0001
0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000

```

Regola 1: Omettere gli zeri iniziali

La prima regola per favorire la riduzione della notazione degli indirizzi IPv6 consiste nell'omettere tutti gli zeri iniziali in tutte le sezioni a 16 bit o hextet. Ad esempio:

- 01AB può essere rappresentato come 1AB
- 09F0 può essere rappresentato come 9F0
- 0A00 può essere rappresentato come A00
- 00AB può essere rappresentato come AB

Questa regola si applica solo agli zeri iniziali, NON agli zeri finali, altrimenti l'indirizzo sarebbe ambiguo. Ad esempio, l'hextet "ABC" potrebbe essere "0ABC" o "ABC0", ma questi non rappresentano lo stesso valore.

Preferito	2001:0DB8:0000:1111:0000:0000:0000:0200
Senza zeri iniziali	2001: DB8: 0:1111: 0: 0: 0: 200

Regola 2: Omettere i segmenti costituiti da tutti 0

La seconda regola per favorire la riduzione della notazione degli indirizzi IPv6 consiste nel fatto che i due punti doppi (::) possono sostituire qualunque stringa singola e contigua di uno o più segmenti a 16 bit (hextet) composti interamente da zeri.

I due punti doppi (::) possono essere utilizzati solo una volta all'interno di un indirizzo, altrimenti vi sarebbe più di un indirizzo risultante. Quando questa regola viene utilizzata con la tecnica dell'omissione degli zeri iniziali, la notazione degli indirizzi IPv6 spesso può essere notevolmente ridotta. Questo è comunemente noto come formato compresso.

Indirizzo errato:

- 2001:0DB8::ABCD::1234

Possibili espansioni degli indirizzi compressi ambigui:

- 2001:0DB8::ABCD:0000:0000:1234
- 2001:0DB8::ABCD:0000:0000:0000:1234
- 2001:0DB8:0000:ABCD::1234
- 2001:0DB8:0000:0000:ABCD::1234

Preferito	2001:0DB8:0000:1111:0000:0000:0000:0200
Senza zeri iniziali	2001: DB8: 0:1111: 0: 0: 0: 200
Compresso	2001:DB8:0:1111::200

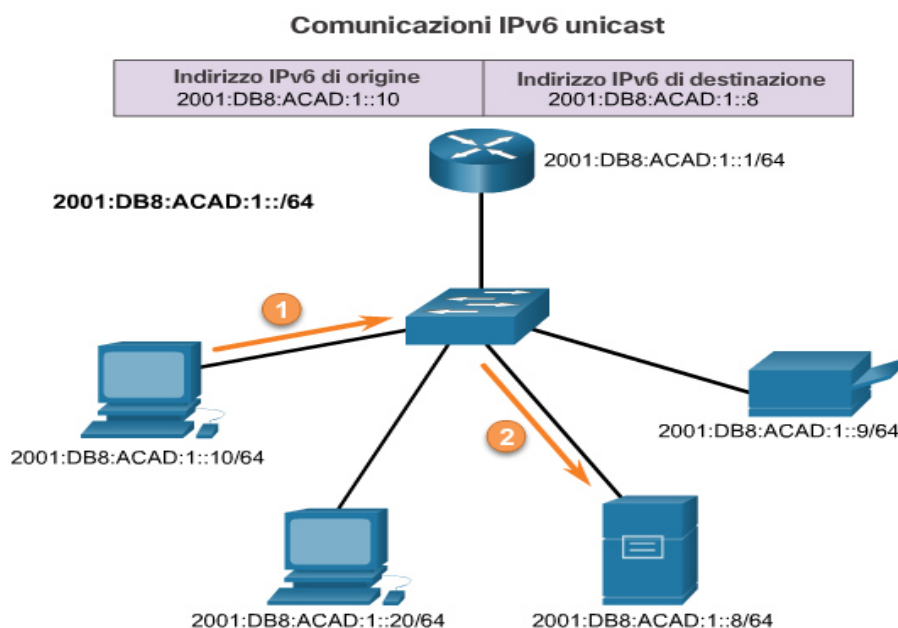
esempi di come l'utilizzo dei due punti doppi (::) e l'omissione degli zeri iniziali possano ridurre le dimensioni di un indirizzo IPv6.

Tipi di indirizzi IPv6

Esistono tre tipi di indirizzi IPv6:

- **Unicast:** un indirizzo IPv6 unicast identifica in modo univoco un'interfaccia su un dispositivo abilitato per IPv6. Come illustrato nella figura, un indirizzo IPv6 di origine deve essere un indirizzo unicast.
- **Multicast:** un indirizzo IPv6 multicast viene utilizzato per inviare un singolo pacchetto IPv6 a diverse destinazioni.
- **Anycast:** un indirizzo IPv6 anycast è un indirizzo IPv6 unicast che può essere assegnato a più dispositivi. Un pacchetto inviato a un indirizzo anycast viene instradato al dispositivo più vicino che presenta quell'indirizzo.

A differenza di IPv4, IPv6 non dispone di un indirizzo di broadcast. Tuttavia, esiste un indirizzo IPv6 multicast di tipo "tutti i nodi" che produce essenzialmente lo stesso risultato.

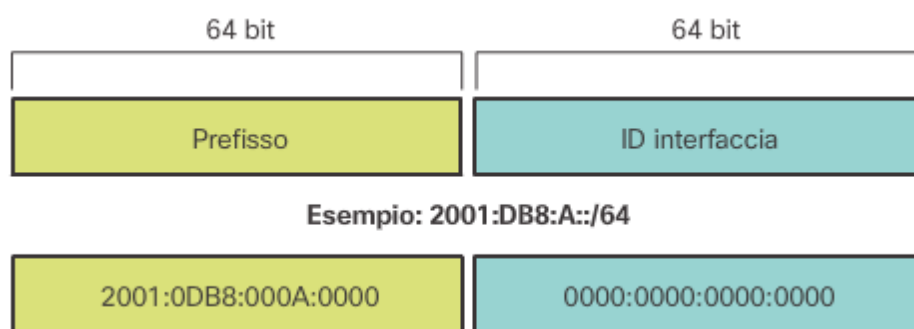


Lunghezza del prefisso IPv6

Occorre ricordare che il prefisso o la porzione rete di un indirizzo IPv4 può essere identificato da una subnet mask decimale puntata o dalla lunghezza del prefisso (notazione slash). Ad esempio, un indirizzo IPv4 192.168.1.10 con subnet mask decimale puntata 255.255.255.0 è equivalente a 192.168.1.10/24.

IPv6 utilizza la lunghezza del prefisso per rappresentare la porzione di prefisso dell'indirizzo. IPv6 non utilizza la notazione della subnet mask decimale puntata. La lunghezza del prefisso è utilizzata per indicare la porzione rete di un indirizzo IPv6 utilizzando indirizzo IPv6/lunghezza del prefisso.

La lunghezza del prefisso può variare da 0 a 128. Una lunghezza tipica del prefisso IPv6 per le LAN e la maggior parte degli altri tipi di reti è /64. Questo significa che il prefisso o la porzione rete dell'indirizzo hanno una lunghezza di 64 bit, mentre gli altri 64 bit vengono destinati all'ID interfaccia (porzione dell'host) dell'indirizzo.



Indirizzi IPv6 unicast

Un indirizzo IPv6 unicast identifica in modo univoco un'interfaccia su un dispositivo abilitato per IPv6. Un pacchetto inviato a un indirizzo unicast viene ricevuto dall'interfaccia a cui è assegnato a quell'indirizzo. In maniera simile a IPv4, un indirizzo IPv6 di origine deve essere un indirizzo unicast. L'indirizzo IPv6 di destinazione può essere un indirizzo unicast o multicast.

I tipi più comuni di indirizzi IPv6 unicast sono gli indirizzi unicast globali (GUA) e gli indirizzi unicast link-local.

Unicast globale

Un indirizzo unicast globale è simile a un indirizzo IPv4 pubblico. Si tratta di indirizzi univoci a livello globale, instradabili su Internet. Gli indirizzi unicast globali possono essere configurati in modo statico o assegnati in modo dinamico.

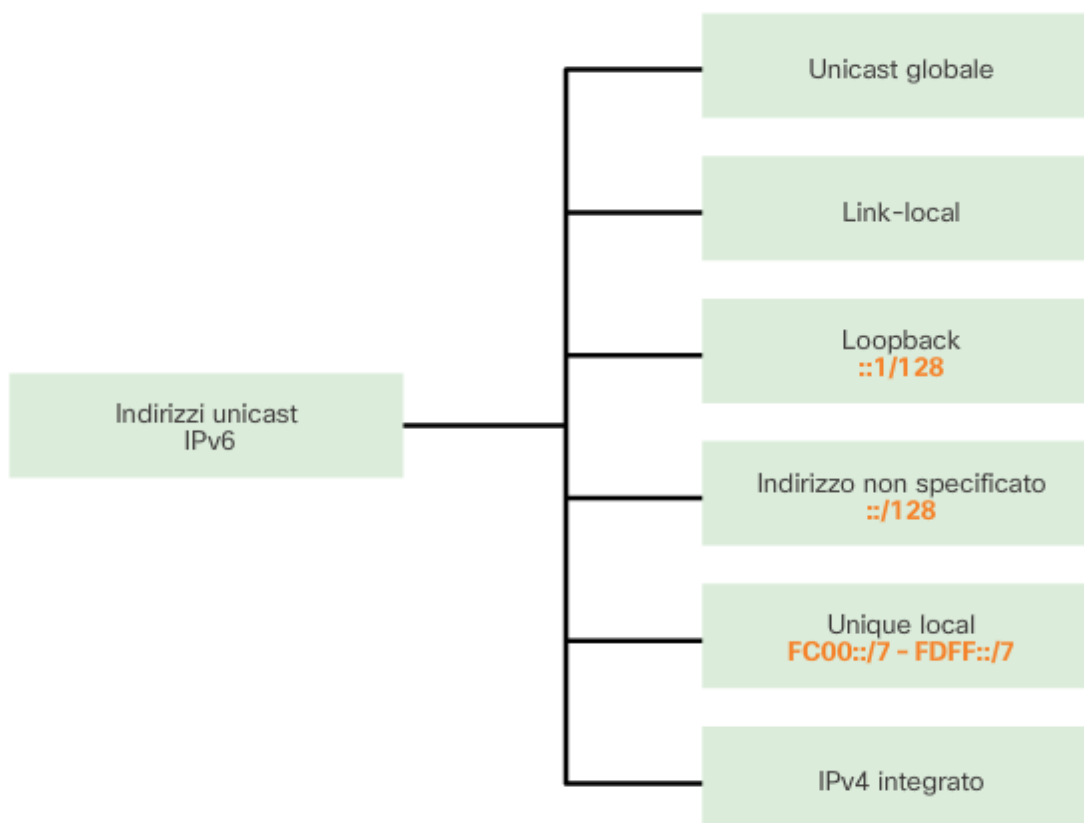
Link-local

Gli indirizzi link-local vengono utilizzati per comunicare con altri dispositivi nello stesso link locale. Con IPv6, il termine **link** si riferisce a una subnet. Gli indirizzi link-local sono associati a un singolo link. La loro unicità deve essere confermata solo in quel link, perché non sono instradabili oltre. In altre parole, i router non inoltrano pacchetti con un indirizzo link-local di origine o di destinazione.

Unique local

Un altro tipo di indirizzo unicast è l'indirizzo unicast unique local. Gli indirizzi IPv6 locali univoci mostrano alcune somiglianze con gli indirizzi RFC 1918 **privati per IPv4**, ma esistono differenze significative. Gli indirizzi locali univoci vengono utilizzati per l'indirizzamento locale all'interno di un sito o entro un numero limitato di siti. Questi indirizzi non devono essere instradabili a IPv6 globale e non devono essere tradotti in un indirizzo IPv6 globale. Gli indirizzi locali univoci rientrano nell'intervallo compreso tra **FC00::/7 e FDFF::/7**.

Con IPv4, gli indirizzi privati si combinano con NAT/PAT per fornire una traduzione molti-a-uno di indirizzi da privato a pubblico. Ciò avviene a causa della disponibilità limitata dello spazio degli indirizzi IPv4. Molti siti utilizzano anche la natura privata degli indirizzi RFC 1918 per aiutare a proteggere o nascondere la rete da potenziali rischi per la sicurezza. Tuttavia, questo non è l'uso che era stato previsto per queste tecnologie e l'IETF ha sempre consigliato ai siti di prendere le dovute precauzioni di sicurezza nel router rivolto verso Internet. **Gli indirizzi locali univoci possono essere utilizzati per i dispositivi che non avranno mai accesso da o necessità di accedere a un'altra rete.**



Indirizzi IPv6 unicast link-local

Un indirizzo IPv6 link-local consente a un dispositivo di comunicare con altri dispositivi abilitati per IPv6 nello stesso link e solo in quel link (subnet). I pacchetti con un indirizzo link-local di origine o di destinazione non possono essere instradati oltre il link da cui ha avuto origine il pacchetto.

L'indirizzo unicast globale non è un requisito. Tuttavia, ogni interfaccia di rete abilitata per IPv6 deve disporre di un indirizzo link-local.

Se su un'interfaccia non è configurato manualmente un indirizzo link-local, il dispositivo ne crea uno automaticamente senza comunicare con un server DHCP. Gli host abilitati per IPv6 creano un indirizzo IPv6 link-local anche se al dispositivo non veniva assegnato un indirizzo IPv6 unicast globale. Questo consente ai dispositivi abilitati per IPv6 di comunicare con altri dispositivi abilitati per IPv6 nella stessa subnet. Sono comprese le comunicazioni con il gateway predefinito (router).

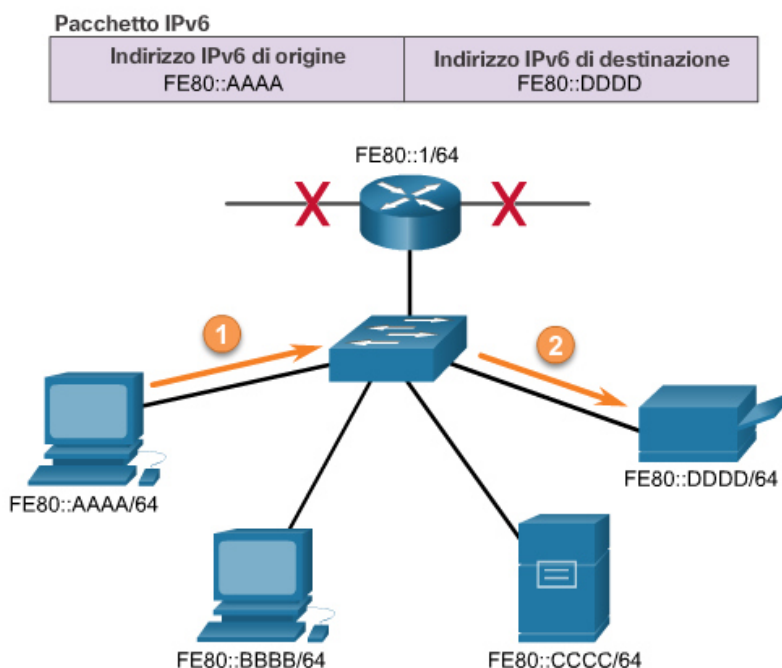
Gli indirizzi IPv6 link-local sono compresi nell'intervallo FE80::/10. /10 indica che i primi 10 bit sono 1111 1110 10xx xxxx. Il primo hextet ha un intervallo compreso tra 1111 1110 1000 0000 (FE80) e 1111 1110 1011 1111 (FEBF).

La Figura 1 mostra un esempio di comunicazione utilizzando indirizzi IPv6 link-local.

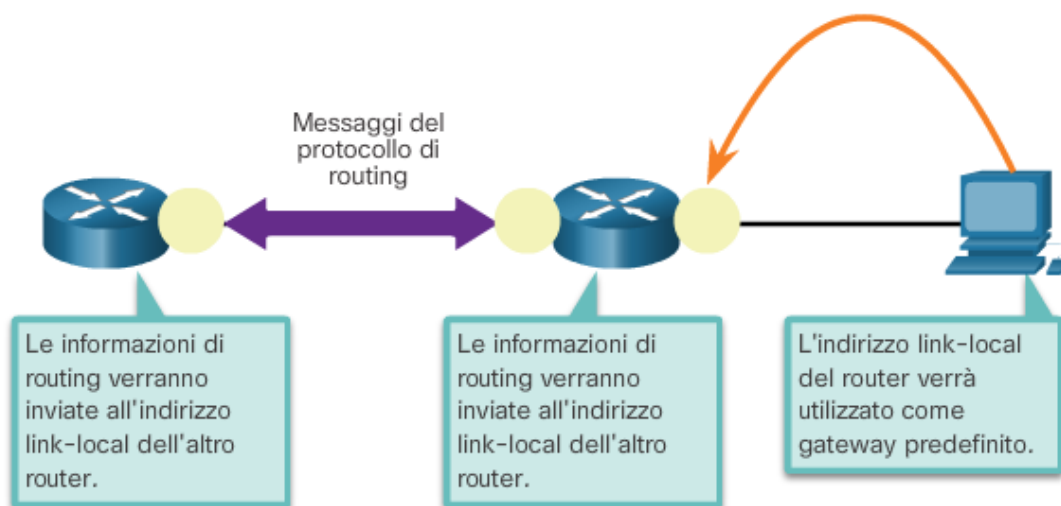
La Figura 2 mostra alcuni degli utilizzi degli indirizzi IPv6 link-local.

Nota: in genere, l'indirizzo link-local del router, e non l'indirizzo unicast globale, viene utilizzato come gateway predefinito dagli altri dispositivi sul link.

Comunicazioni link-local IPv6



Utilizzi di un indirizzo IPv6 link-local



Struttura di un indirizzo IPv6 unicast globale

Gli indirizzi IPv6 unicast globali (GUA) sono univoci a livello globale e instradabili su Internet IPv6. Questi indirizzi corrispondono agli indirizzi IPv4 pubblici. L'ICANN (Internet Committee for Assigned Names and Numbers), l'operatore di IANA, assegna blocchi di indirizzi IPv6 ai cinque RIR (**Regional Internet Registry** è un'organizzazione che sovrintende all'assegnamento e alla registrazione delle risorse numeriche di [Internet](#) in una specifica area geografica. In particolare ci si riferisce all'assegnazione degli [indirizzi IP](#), necessari per aggiungere nuovi [nodi](#) alla Rete e fondamentali per il funzionamento della stessa.). Attualmente, vengono assegnati solo indirizzi unicast globali con i primi tre bit corrispondenti a 001 o 2000::/3. In altre parole, la prima cifra esadecimale di un indirizzo GUA inizia con 2 o 3. Questo è solo 1/8 dello spazio totale disponibile per gli indirizzi IPv6, escludendo solo una porzione molto piccola per altri tipi di indirizzi unicast e multicast.

Nota: l'indirizzo 2001:0DB8::/32 è stato riservato a scopo di documentazione, compreso l'uso negli esempi.

La Figura 1 mostra la struttura e l'intervallo di un indirizzo unicast globale.

Un indirizzo unicast globale presenta tre parti:

- Prefisso di routing globale
- ID subnet
- ID interfaccia

Prefisso di routing globale

Il prefisso di routing globale è la porzione di prefisso o **di rete dell'indirizzo assegnato dal provider**, ad esempio un ISP, a un cliente o a un sito. In genere, i RIR **assegnano ai clienti un prefisso di**

routing globale /48. Questo può includere varie tipologie di utenti, da reti aziendali a singole abitazioni.

La Figura 2 mostra la struttura di un indirizzo unicast globale utilizzando un prefisso di routing globale /48. I prefissi /48 sono i prefissi di routing globale più comunemente assegnati e verranno utilizzati nella maggior parte degli esempi di questo corso.

Ad esempio, l'indirizzo IPv6 2001:0DB8:ACAD::/48 presenta un prefisso che indica che i primi 48 bit (3 hextet) (2001:0DB8:ACAD) rappresentano il prefisso o la porzione rete dell'indirizzo. I due punti doppi (::) prima della lunghezza del prefisso /48 indicano che il resto dell'indirizzo contiene tutti zeri.

La dimensione del prefisso di routing globale determina la dimensione dell'ID subnet.

ID subnet

L'ID subnet è utilizzato da un'azienda per identificare le subnet all'interno del proprio sito. Quanto più grande è l'ID subnet, tante più subnet sono disponibili.

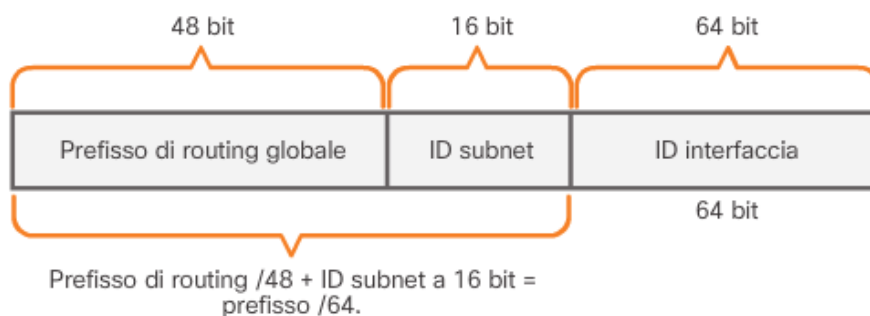
ID interfaccia

L'ID interfaccia IPv6 è equivalente alla porzione dell'host di un indirizzo IPv4. Si utilizza il termine ID interfaccia perché un singolo host può avere diverse interfacce, ciascuna con uno o più indirizzi IPv6. Si consiglia vivamente di utilizzare subnet /64 nella maggior parte dei casi, ovvero un ID interfaccia a 64 bit, come mostrato nella Figura 2.

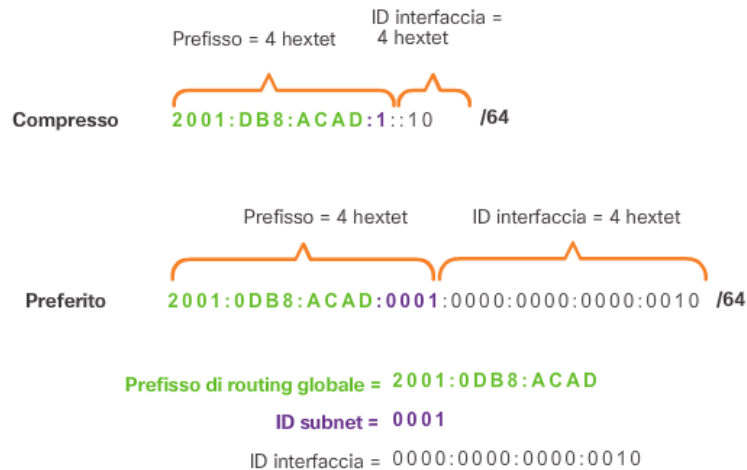
Nota: a differenza di IPv4, in IPv6 è possibile assegnare a un dispositivo indirizzi degli host composti solo da zeri o da 1. L'indirizzo di soli 1 può essere utilizzato in quanto gli indirizzi di broadcast non vengono impiegati all'interno di IPv6. Anche l'indirizzo di soli zeri può essere utilizzato, ma è riservato come indirizzo anycast subnet-router e deve essere assegnato solo a router.

Un modo semplice per leggere la maggior parte degli indirizzi IPv6 è calcolare il numero di hextet. Come mostrato nella Figura 3, in un indirizzo unicast globale /64 i primi quattro hextet sono riservati alla porzione rete dell'indirizzo, mentre il quarto hextet indica l'ID subnet. I quattro hextet rimanenti sono per l'ID interfaccia.

Prefisso di routing globale IPv6 /48



Lettura di un indirizzo unicast globale



Indirizzo IPv6 unicast globale



Configurazione statica di un indirizzo unicast globale

Configurazione del router

La maggior parte dei comandi di configurazione e verifica di IPv6 in Cisco IOS sono simili a quelli di IPv4. In molti casi, l'unica differenza è l'utilizzo di **ipv6** anziché **ip** all'interno dei comandi.

Il comando per configurare un indirizzo IPv6 unicast globale in un'interfaccia è **ipv6 address ipv6-address/prefix-length**.

Si noti che non vi sono spazi tra *ipv6-address* e *prefix-length*.

La configurazione di esempio utilizza la topologia mostrata nella Figura 1 e queste subnet IPv6:

- 2001:0DB8:ACAD:0001:/64 (o 2001:DB8:ACAD:1::/64)
- 2001:0DB8:ACAD:0002:/64 (o 2001:DB8:ACAD:2::/64)
- 2001:0DB8:ACAD:0003:/64 (o 2001:DB8:ACAD:3::/64)

La Figura 1 mostra anche i comandi necessari per configurare l'indirizzo IPv6 unicast globale sull'interfaccia GigabitEthernet 0/0, GigabitEthernet 0/1 e Serial 0/0/0 di R1.

Configurazione dell'host

La configurazione manuale dell'indirizzo IPv6 in un host è simile alla configurazione di un indirizzo IPv4.

Come mostrato nella Figura 1, l'indirizzo del gateway predefinito configurato per PC1 è 2001:DB8:ACAD:1::1. Questo è l'indirizzo unicast globale dell'interfaccia GigabitEthernet di R1 nella stessa rete. In alternativa, l'indirizzo del gateway predefinito può essere configurato in modo da corrispondere all'indirizzo link-local dell'interfaccia GigabitEthernet. Entrambe le configurazioni funzionano.

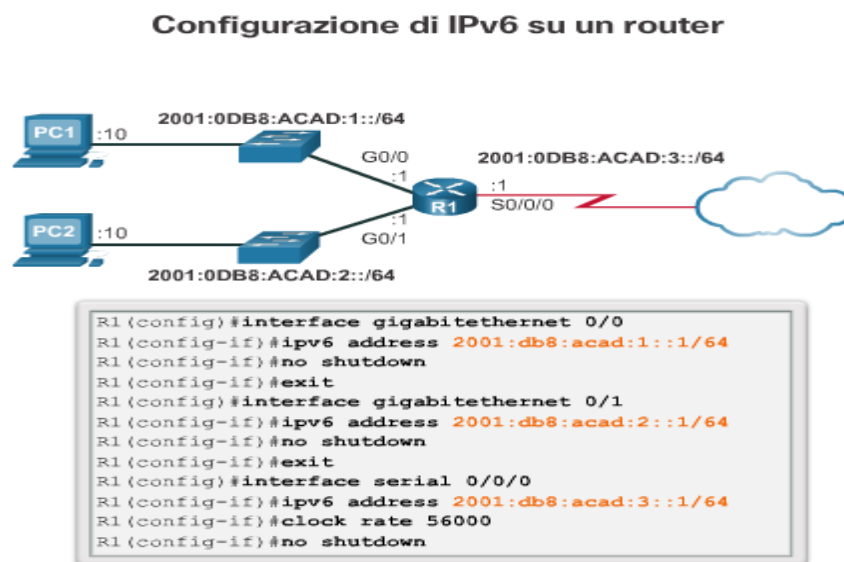
Utilizzare il controllore di sintassi nella Figura 3 per configurare l'indirizzo IPv6 unicast globale.

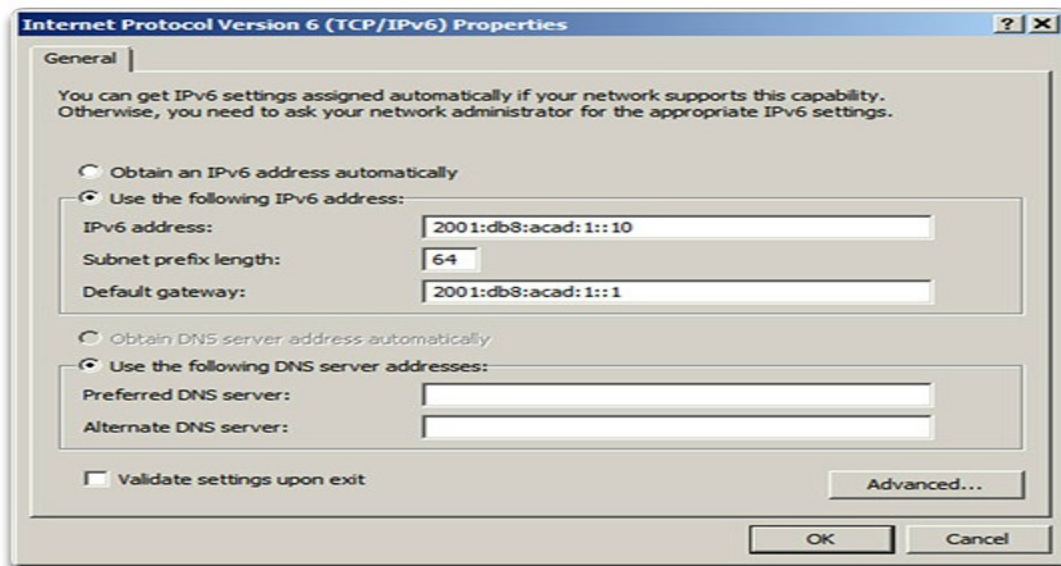
Come per IPv4, la configurazione degli indirizzi statici sui client non è scalabile in ambienti di grandi dimensioni. Per questo motivo, la maggior parte degli amministratori di rete in una rete IPv6 abiliterà l'assegnazione dinamica degli indirizzi IPv6.

Esistono due modi in cui un dispositivo può ottenere automaticamente un indirizzo IPv6 unicast globale:

- Stateless Address Autoconfiguration (SLAAC)
- DHCPv6 stateful

Nota: quando si utilizzano DHCPv6 o SLAAC, l'indirizzo link-local del router locale viene specificato automaticamente come l'indirizzo del gateway predefinito.





Configurazione dinamica: SLAAC Stateless Address Autoconfiguration (SLAAC) è un metodo che consente a un dispositivo di ottenere il prefisso, la lunghezza del prefisso, l'indirizzo del gateway predefinito e altre informazioni da un *router IPv6* senza l'utilizzo di un server DHCPv6. Con SLAAC, i dispositivi si affidano ai messaggi Router Advertisement (RA) ICMPv6 del router locale per ottenere le informazioni necessarie.

Ogni 200 secondi i router IPv6 inviano periodicamente messaggi RA ICMPv6 a tutti i dispositivi abilitati per IPv6 della rete. Un messaggio RA viene inviato anche in risposta a un host che invia un messaggio Router Solicitation (RS) ICMPv6.

Il routing IPv6 non è abilitato per impostazione predefinita. Per attivare un router come router IPv6, è necessario utilizzare il comando di configurazione globale **ipv6 unicast-routing**.

Nota: gli indirizzi IPv6 possono essere configurati in un router senza che si tratti di un router IPv6.

Il messaggio RA ICMPv6 è un suggerimento dato a un dispositivo su come ottenere un indirizzo IPv6 unicast globale. L'ultima decisione spetta al sistema operativo del dispositivo. Il messaggio RA ICMPv6 include:

- **Prefisso di rete e lunghezza del prefisso:** indica al dispositivo la rete a cui appartiene.
- **Indirizzo gateway predefinito:** è un indirizzo IPv6 link-local, l'indirizzo IPv6 di origine del messaggio RA.
- **Indirizzi DNS e nome del dominio:** indirizzi di server DNS e un nome del dominio.

Come mostrato nella Figura 1, sono disponibili tre opzioni per i messaggi RA:

- Opzione 1: SLAAC
- Opzione 2: SLAAC con un server DHCPv6 stateless
- Opzione 3: DHCPv6 stateful (senza SLAAC)

Opzione 1 RA: SLAAC

Per impostazione predefinita, il messaggio RA suggerisce che il dispositivo ricevente utilizzi le informazioni contenute nel messaggio RA per creare il proprio indirizzo IPv6 unicast globale e per tutte le altre informazioni. I servizi di un server DHCPv6 non sono necessari.

SLAAC è stateless, il che significa che non è presente un server centrale (ad esempio, un server DHCPv6 stateful) che assegna indirizzi unicast globali e conserva un elenco dei dispositivi e dei relativi indirizzi. Con SLAAC, il dispositivo client utilizza le informazioni contenute nel messaggio RA per creare il proprio indirizzo unicast globale. Come mostrato nella Figura 2, le due parti dell'indirizzo vengono create nel seguente modo:

- **Prefisso:** ricevuto nel messaggio RA
- **ID interfaccia:** utilizza il processo EUI-64 o viene generato un numero casuale a 64 bit

Messaggi RS (Router Solicitation) e RA (Router Advertisement)



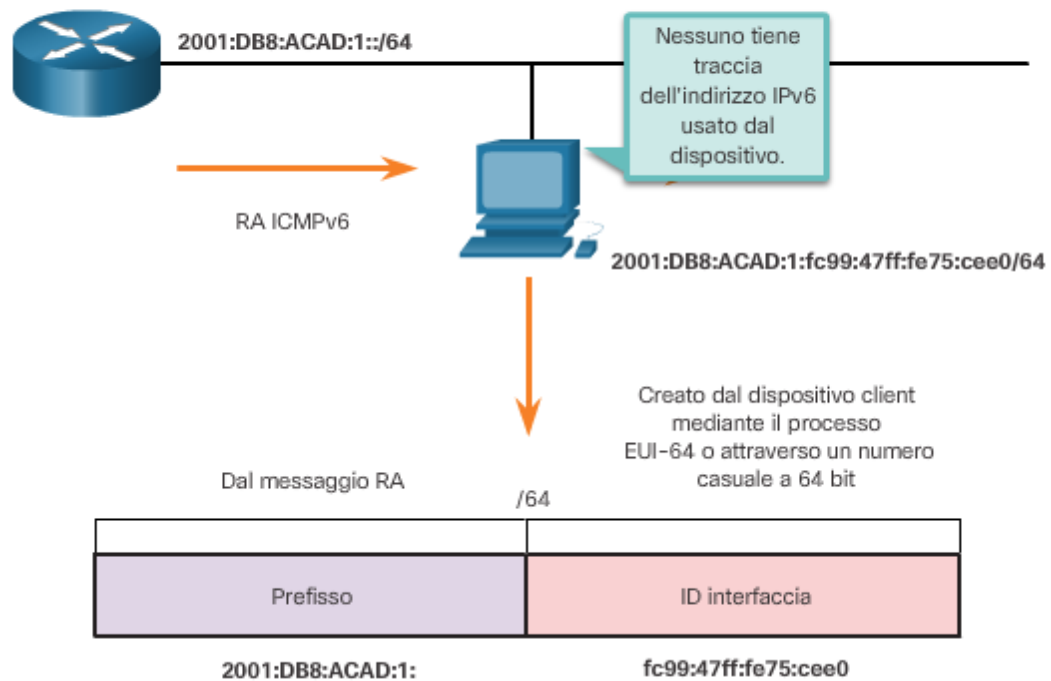
Opzioni RA

Opzione 1 (solo SLAAC): "Invio delle informazioni richieste: prefisso, lunghezza del prefisso, gateway predefinito."

Opzione 2 (SLAAC e DHCPv6): "Oltre ai dati forniti è necessario ottenere altre informazioni, come gli indirizzi DNS, da un server DHCPv6."

Opzione 3 (solo DHCPv6): "Non si dispone di queste informazioni. Richiedere tutte le informazioni necessarie a un server DHCPv6."

Indirizzo unicast globale e SLAAC



Configurazione dinamica: DHCPv6

Per impostazione predefinita, il messaggio RA corrisponde all'opzione 1, solo SLAAC. L'interfaccia del router può essere configurata in modo che invii un annuncio router utilizzando SLAAC e DHCPv6 stateless o solo DHCPv6 stateful.

Opzione 2 RA: SLAAC e DHCPv6 stateless

Con questa opzione, il messaggio RA suggerisce che i dispositivi utilizzino:

- SLAAC per creare il proprio indirizzo IPv6 unicast globale.
- L'indirizzo link-local del router, l'indirizzo IPv6 di origine RA per l'indirizzo del gateway predefinito.
- Un server DHCPv6 stateless per ottenere altre informazioni, ad esempio un indirizzo del server DNS e un nome del dominio.

Un server DHCPv6 stateless distribuisce indirizzi del server DNS e nomi di dominio. Non assegna indirizzi unicast globali.

Opzione 3 RA: DHCPv6 stateful

Il metodo DHCPv6 stateful è simile a DHCP per IPv4. Un dispositivo può ricevere automaticamente informazioni di indirizzamento, tra cui un indirizzo unicast globale, la lunghezza del prefisso e gli indirizzi dei server DNS utilizzando i servizi di un server DHCPv6 stateful.

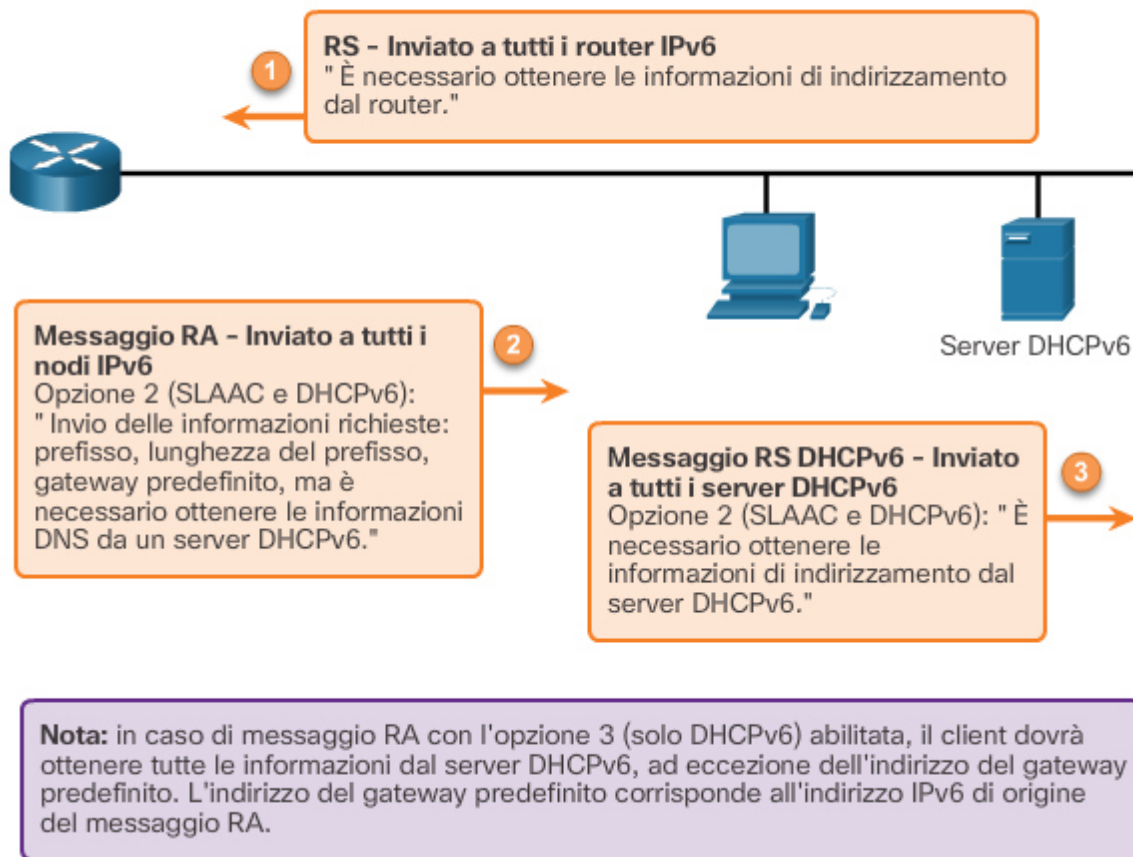
Con questa opzione, il messaggio RA suggerisce che i dispositivi utilizzino:

- L'indirizzo link-local del router, l'indirizzo IPv6 di origine RA per l'indirizzo del gateway predefinito.
- Un server DHCPv6 stateful per ottenere un indirizzo unicast globale, l'indirizzo del server DNS, il nome del dominio e tutte le altre informazioni.

Un server DHCPv6 stateful assegna e conserva un elenco che indica la corrispondenza tra i dispositivi e gli indirizzi IPv6 ricevuti. DHCP per IPv4 è stateful.

Nota: l'indirizzo del gateway predefinito può essere ottenuto solo dinamicamente dal messaggio RA. Il server DHCPv6 stateless o stateful non fornisce l'indirizzo del gateway predefinito.

Messaggi RS (Router Solicitation) e RA (Router Advertisement)



Processo EUI-64 e numero generato in modo casuale

Quando il messaggio RA è SLAAC o SLAAC con DHCPv6 stateless, il client deve generare il proprio ID interfaccia. Il client conosce la porzione di prefisso dell'indirizzo dal messaggio RA, ma deve creare il proprio ID interfaccia. L'ID interfaccia può essere creato utilizzando il processo EUI-64 o un numero a 64 bit generato in modo casuale, come mostrato nella Figura 1.

Processo EUI-64

L'IEEE ha definito l'EUI (Extended Unique Identifier) o processo EUI-64 modificato. Questo processo utilizza l'indirizzo MAC Ethernet a 48 bit di un client e inserisce altri 16 bit in mezzo all'indirizzo MAC a 48 bit per creare un ID interfaccia a 64 bit.

Gli indirizzi MAC Ethernet in genere sono rappresentati in numeri esadecimali e si compongono di due parti:

- **Organizationally Unique Identifier (OUI):** l'OUI è un codice produttore a 24 bit (6 cifre esadecimali) assegnato da IEEE.
- **Identificativo dispositivo:** l'identificativo dispositivo è un valore univoco a 24 bit (6 cifre esadecimali) all'interno di un OUI comune.

Un ID interfaccia EUI-64 è rappresentato tramite la numerazione binaria ed è composto da tre parti:

- OUI a 24 bit dell'indirizzo MAC del client, ma il settimo bit, ossia il bit Universally/Locally (U/L), è invertito. Questo significa che se il settimo bit è uno 0 diventa un 1 e viceversa.
- Il valore FFFE a 16 bit inserito (in numerazione esadecimale).
- L'identificativo del dispositivo a 24 bit, proveniente dall'indirizzo MAC del client.

Il processo EUI-64 è illustrato nella Figura 2, utilizzando l'indirizzo MAC GigabitEthernet di R1 FC99:4775:CEE0.

Fase 1: Dividere l'indirizzo MAC tra l'OUI e l'identificativo del dispositivo.

Fase 2: Inserire il valore esadecimale FFFE, che in numerazione binaria è: 1111 1111 1111 1110.

Fase 3: Convertire i primi 2 valori esadecimali dell'OUI in numerazione binaria e invertire il bit U/L (7° bit). In questo esempio, lo 0 nel 7° bit è diventato un 1.

Il risultato è un ID interfaccia EUI-64 generato FE99:47FF:FE75:CEE0.

Nota: l'utilizzo del bit U/L e i motivi per cui modificare il suo valore vengono illustrati nell'RFC 5342.

La Figura 3 mostra l'indirizzo IPv6 unicast globale del PCA creato dinamicamente utilizzando SLAAC e il processo EUI-64. Un modo semplice per capire che un indirizzo è stato probabilmente creato utilizzando il processo EUI-64 è il valore FFFE posizionato in mezzo all'ID interfaccia, come mostrato nella Figura 3.

Il vantaggio del metodo EUI-64 è che l'indirizzo MAC Ethernet può essere utilizzato per determinare l'ID interfaccia. Inoltre, questo metodo consente agli amministratori di rete di tenere facilmente traccia di un indirizzo IPv6 in un dispositivo terminale utilizzando l'indirizzo MAC univoco. Tuttavia, questo ha causato preoccupazioni relative alla privacy tra molti utenti, che temono che il percorso dei propri pacchetti possa essere tracciato fino al computer fisico effettivo. **A causa di queste preoccupazioni, è possibile utilizzare un ID interfaccia generato in modo casuale.**

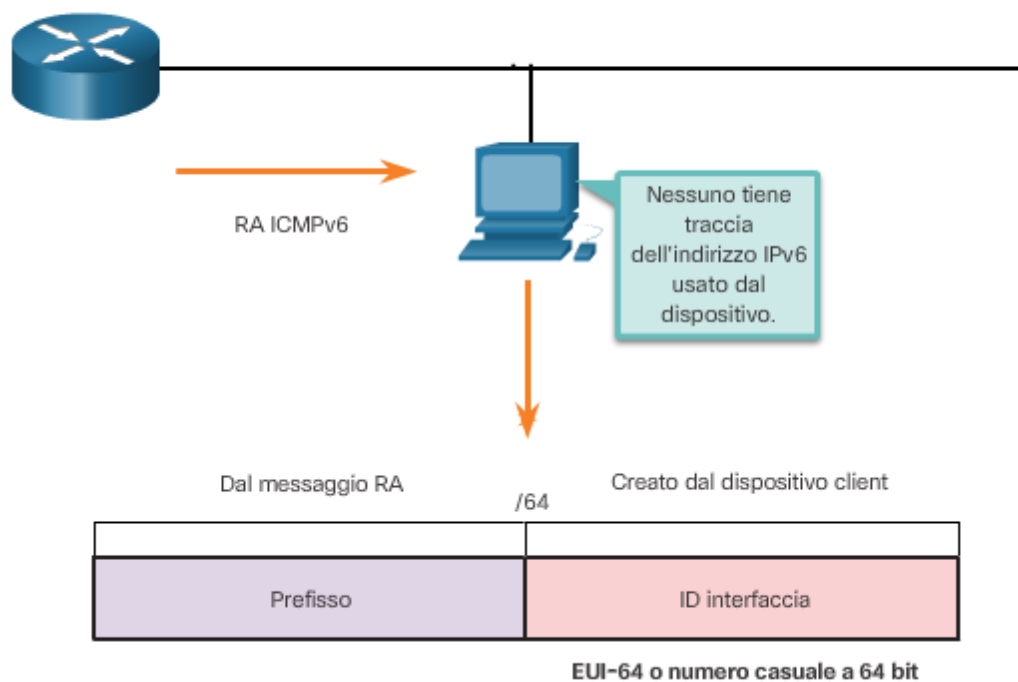
ID interfaccia generato in modo casuale

A seconda del sistema operativo, un dispositivo può utilizzare un ID interfaccia generato in modo casuale anziché l'indirizzo MAC e il processo EUI-64. Ad esempio, a partire da Windows Vista, Windows utilizza un ID interfaccia generato in modo casuale anziché uno creato con EUI-64. Windows XP e i sistemi operativi Windows precedenti utilizzavano EUI-64.

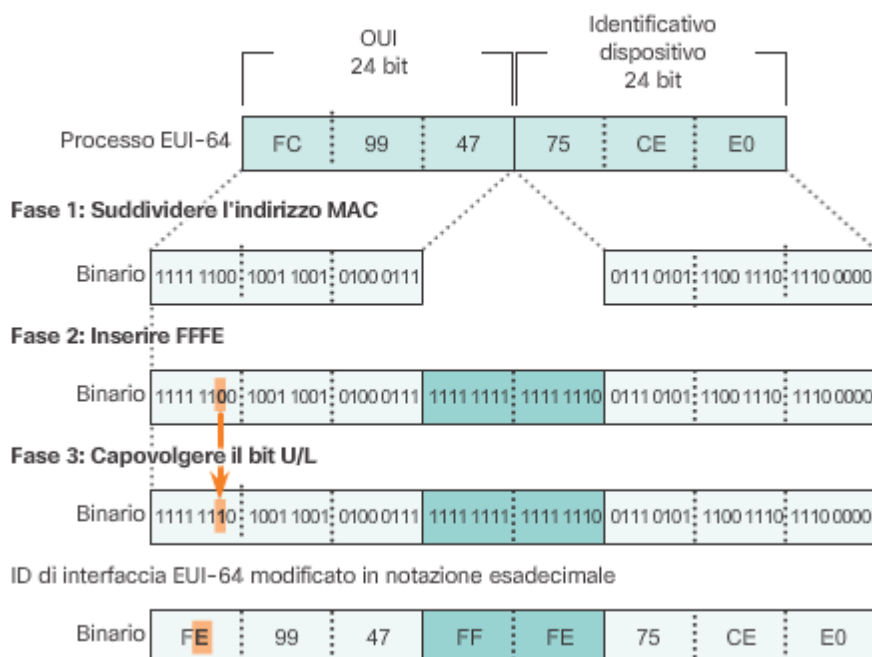
Dopo aver stabilito l'ID interfaccia, tramite processo EUI-64 o generazione casuale, è possibile combinarlo con un prefisso IPv6 nel messaggio RA per creare un indirizzo unicast globale, come mostrato nella Figura 4.

Nota: per garantire l'univocità degli indirizzi IPv6 unicast, il client può utilizzare un processo noto come rilevamento degli indirizzi duplicati (DAD). Questo assomiglia a una richiesta ARP del proprio indirizzo. Se non arriva una risposta, l'indirizzo è univoco.

Processo EUI-64



Processo EUI-64



```

PCA> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  : 
    IPv6 Address. . . . . : 2001:db8:acad:1:fc99:47ff:FE75:cee0
    Link-local IPv6 Address . . . . : fe80::fc99:47FF:FE75:CEE0
    Default Gateway . . . . . : fe80::1

```

```

PCB> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  : 
    IPv6 Address. . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
    Link-local IPv6 Address . . . . : fe80::50a5:8a35:a5bb:66e1
    Default Gateway . . . . . : fe80::1

```

Indirizzi link-local dinamici

Tutti i dispositivi IPv6 devono avere un indirizzo IPv6 link-local. Un indirizzo link-local può essere definito dinamicamente o configurato manualmente come indirizzo link-local statico.

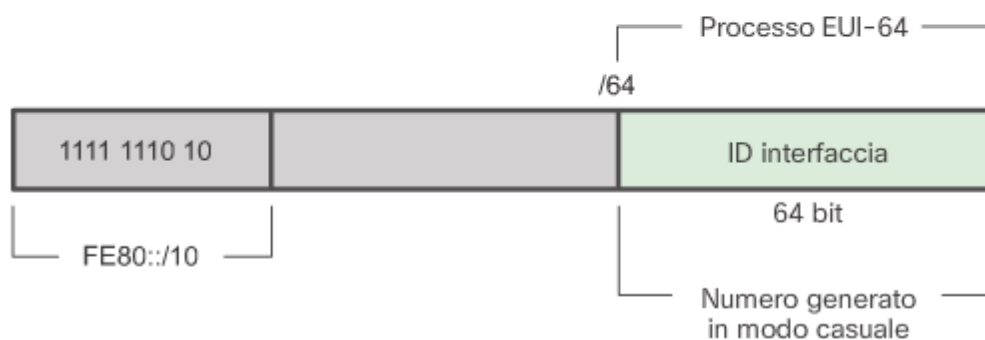
La Figura 1 mostra che l'indirizzo link-local viene creato in modo dinamico utilizzando il prefisso FE80::10 e l'ID interfaccia utilizzando il processo EUI-64 o un numero a 64 bit generato in modo casuale. I sistemi operativi utilizzano solitamente lo stesso metodo per un indirizzo unicast globale creato con SLAAC e un indirizzo link-local assegnato dinamicamente, come mostrato nella Figura 2.

I router Cisco creano automaticamente un indirizzo IPv6 link-local ogni volta che un indirizzo unicast globale viene assegnato all'interfaccia. Per impostazione predefinita, i router Cisco IOS utilizzano EUI-64 per generare l'ID interfaccia per tutti gli indirizzi link-local nelle interfacce IPv6. Per le interfacce seriali, il router utilizza l'indirizzo MAC di un'interfaccia Ethernet. Occorre ricordare che un indirizzo link-local deve essere univoco solo in tale link o rete. Tuttavia, uno svantaggio dell'utilizzo dell'indirizzo link-local assegnato dinamicamente è la lunghezza dell'ID interfaccia, che rende difficile individuare e ricordare gli indirizzi assegnati. La Figura 3 mostra

l'indirizzo MAC nell'interfaccia GigabitEthernet 0/0 del router R1. Questo indirizzo viene utilizzato per creare dinamicamente l'indirizzo link-local nella stessa interfaccia.

Per facilitare il riconoscimento e la memorizzazione di questi indirizzi nei router, è pratica comune configurare staticamente gli indirizzi IPv6 link-local nei router.

Indirizzo link-local IPv6



Indirizzi link-local creati in modo dinamico

ID interfaccia generato dal processo EUI-64

```
PCA> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  :
    IPv6 Address. . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
    Link-local IPv6 Address . . . . : fe80::fc99:47ff:fe75:cee0
    Default Gateway . . . . . : fe80::1
```

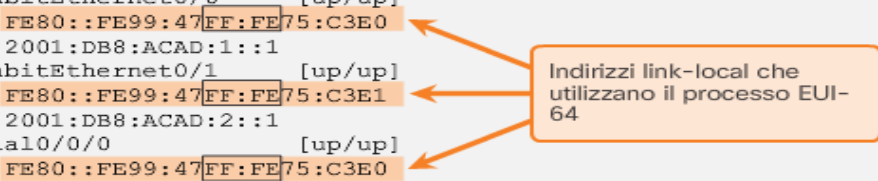
ID interfaccia generato da un numero casuale a 64 bit

```
PCE> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  :
    IPv6 Address. . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
    Link-local IPv6 Address . . . . : fe80::50a5:8a35:a5bb:66e1
    Default Gateway . . . . . : fe80::1
```

Indirizzo link-local generato dal processo EUI-64 del router

```
R1# show interface gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
  (bia fc99.4775.c3e0)
<Output omissa>

R1# show ipv6 interface brief
GigabitEthernet0/0 [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:1::1
GigabitEthernet0/1 [up/up]
  FE80::FE99:47FF:FE75:C3E1
  2001:DB8:ACAD:2::1
Serial0/0/0 [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:ACAD:3::1
Serial0/0/1 [administratively down/down]
  unassigned
R1#
```



Indirizzi link-local statici

La configurazione manuale degli indirizzi link-local offre la possibilità di creare un indirizzo riconoscibile e semplice da ricordare. In genere, è necessario solo creare indirizzi link-local riconoscibili nei router. Questo è utile perché gli indirizzi link-local del router sono utilizzati come indirizzi del gateway predefinito e per i messaggi di annuncio di routing.

Gli indirizzi link-local possono essere configurati manualmente utilizzando lo stesso comando di interfaccia impiegato per creare indirizzi IPv6 unicast globali, ma con l'aggiunta del parametro **link-local**. Quando un indirizzo inizia con questo hextet entro l'intervallo da FE80 a FEBF, il parametro link-local deve seguire l'indirizzo.

La figura mostra la configurazione di un indirizzo link-local utilizzando il comando di interfaccia **ipv6 address**. L'indirizzo link-local FE80::1 viene utilizzato per semplificare il riconoscimento dell'appartenenza al router R1. Lo stesso indirizzo IPv6 link-local è configurato in tutte le interfacce di R1. FE80::1 può essere configurato in ogni link perché deve essere univoco solo in quel link.

Analogamente a R1, il router R2 verrebbe configurato con FE80::2 come indirizzo IPv6 link-local in tutte le relative interfacce.

Configurazione degli indirizzi link-local su R1

Router(config-if) #

```
ipv6 address link-local-address link-local
```

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
    link-local    Use link-local address

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#
```

Verifica della configurazione degli indirizzi IPv6

Come mostrato nella Figura 1, il comando per verificare la configurazione dell'interfaccia IPv6 è simile al comando utilizzato per IPv4.

Il comando **show interface** mostra l'indirizzo MAC delle interfacce Ethernet. EUI-64 utilizza questo indirizzo MAC per generare l'ID interfaccia per l'indirizzo link-local. Inoltre, il comando **show ipv6 interface brief** mostra l'output abbreviato per ciascuna delle interfacce. L'output **[up/up]** viene prodotto sulla stessa riga dell'interfaccia e indica lo stato dell'interfaccia a livello 1/livello 2. Questo corrisponde alle colonne **Status** (Stato) e **Protocol** (Protocollo) nel comando IPv4 equivalente.

Si noti che ogni interfaccia presenta due indirizzi IPv6. Il secondo indirizzo di ogni interfaccia è l'indirizzo unicast globale configurato. Il primo indirizzo, quello che inizia con FE80, è l'indirizzo unicast link-local per l'interfaccia. **Ricordare che l'indirizzo link-local viene aggiunto automaticamente all'interfaccia quando viene assegnato un indirizzo unicast globale.**

Inoltre, si noti che l'indirizzo link-local Serial 0/0/0 di R1 è uguale a quello relativo all'interfaccia GigabitEthernet 0/0. Le interfacce seriali non hanno indirizzi MAC Ethernet, quindi Cisco IOS utilizza l'indirizzo MAC della prima interfaccia Ethernet disponibile. Questo è possibile perché le interfacce link-local devono essere univoche solo su quel link.

L'indirizzo link-local dell'interfaccia del router è solitamente l'indirizzo del gateway predefinito per i dispositivi che si trovano in tale link o rete.

Come mostrato nella Figura 2, il comando **show ipv6 route** può essere utilizzato per verificare che le reti IPv6 e gli indirizzi di interfaccia IPv6 specifici siano stati installati nella tabella di routing IPv6. Il comando **show ipv6 route** visualizza solo le reti IPv6, non le reti IPv4.

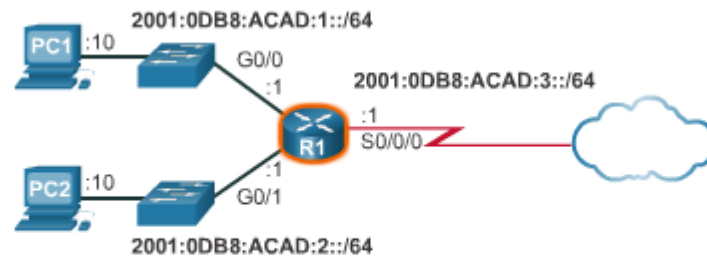
All'interno della tabella di routing, una **C** accanto a una route indica che questa è una rete connessa direttamente. Quando l'interfaccia del router è configurata con un indirizzo unicast globale e si trova in stato "up/up", il prefisso IPv6 e la lunghezza del prefisso vengono aggiunti alla tabella di routing IPv6 come una route connessa.

Nota: la **L** indica una route locale, l'indirizzo IPv6 specifico assegnato all'interfaccia. Non si tratta di un indirizzo link-local. Gli indirizzi link-local non sono inclusi nella tabella di routing del router perché non sono indirizzi instradabili.

L'indirizzo IPv6 unicast globale configurato nell'interfaccia è installato anche nella tabella di routing come route locale. La route locale ha un prefisso /128. Le route locali vengono utilizzate dalla tabella di routing per elaborare in modo efficace pacchetti con l'indirizzo dell'interfaccia del router come indirizzo di destinazione.

Il comando **ping** per IPv6 è identico al comando utilizzato con IPv4, tranne che viene utilizzato un indirizzo IPv6. Come mostrato nella Figura 3, il comando viene utilizzato per verificare la connettività di livello 3 tra R1 e PC1. Quando si esegue il ping di un indirizzo link-local da un router, Cisco IOS chiede all'utente di indicare l'interfaccia di uscita. Poiché l'indirizzo link-local di destinazione può trovarsi su uno o più link o reti, il router deve sapere a quale interfaccia inviare il ping.

Utilizzare il controllore di sintassi nella Figura 4 per verificare la configurazione dell'indirizzo IPv6.



```
R1# show ipv6 interface brief
GigabitEthernet0/0    [up/up]
FE80::FE99:47FF:FE75:C3E0
2001:DB8:ACAD:1::1
GigabitEthernet0/1    [up/up]
FE80::FE99:47FF:FE75:C3E1
2001:DB8:ACAD:2::1
Serial0/0/0           [up/up]
FE80::FE99:47FF:FE75:C3E0
2001:DB8:ACAD:3::1
Serial0/0/1           [administratively down/down]
unassigned
R1#
```

```
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static

<Output omissa>

C   2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
    via GigabitEthernet0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
    via Serial0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
    via Serial0/0/0, receive
L   FF00::/8 [0/0]
    via Null0, receive
R1#
```

```
R1# ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout
is 2 seconds:
!!!!
Success rate is 100 percent (5/5)
R1#
```

Indirizzi IPv6 multicast assegnati

Gli indirizzi IPv6 multicast sono simili agli indirizzi IPv4 multicast. Come illustrato in precedenza, un indirizzo multicast viene utilizzato per inviare un singolo pacchetto a una o più destinazioni (gruppo multicast). Gli indirizzi IPv6 multicast hanno il prefisso FF00::/8.

Nota: gli indirizzi multicast possono essere solo indirizzi di destinazione e non indirizzi di origine.

Esistono due tipi di indirizzi IPv6 multicast:

- Multicast assegnato
- Multicast richiesto dal nodo

Multicast assegnato

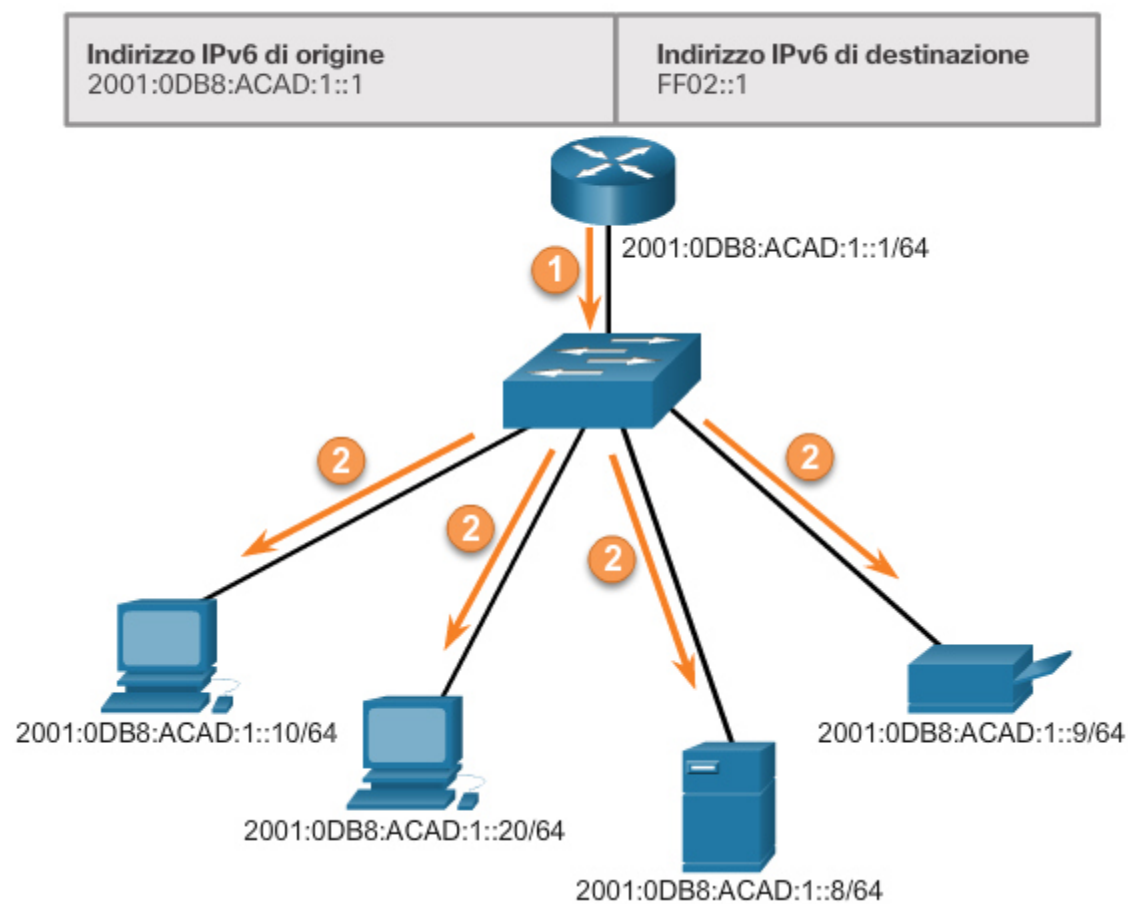
Gli indirizzi multicast assegnati sono indirizzi multicast riservati a gruppi predefiniti di dispositivi. Un indirizzo multicast assegnato è un singolo indirizzo utilizzato per raggiungere un gruppo di dispositivi che esegue un protocollo o un servizio comune. Gli indirizzi multicast assegnati vengono utilizzati nel contesto di protocolli specifici, come DHCPv6.

Due gruppi IPv6 multicast assegnati comuni includono:

- **Gruppo multicast di tipo "tutti i nodi" FF02::1:** si tratta di un gruppo multicast al quale si uniscono tutti i dispositivi abilitati per IPv6. Un pacchetto inviato a questo gruppo viene ricevuto ed elaborato da tutte le interfacce IPv6 nel link o nella rete. Questo ha lo stesso effetto dell'indirizzo di broadcast in IPv4. La figura mostra un esempio di comunicazione utilizzando l'indirizzo multicast di tipo "tutti i nodi". Un router IPv6 invia messaggi RA Internet Control Message Protocol versione 6 (ICMPv6) al gruppo multicast "tutti i nodi". Il messaggio RA comunica a tutti i dispositivi abilitati per IPv6 che si trovano nella rete le informazioni di indirizzamento, ad esempio prefisso, lunghezza del prefisso e gateway predefinito.
- **Gruppo multicast di tipo "tutti i router" FF02::2:** si tratta di un gruppo multicast al quale si uniscono tutti i router IPv6. Un router diventa un membro di questo gruppo quando è abilitato come router IPv6 con il comando di configurazione globale **ipv6 unicast-routing**. Un pacchetto inviato a questo gruppo viene ricevuto ed elaborato da tutti i router IPv6 nel link o nella rete.

I dispositivi abilitati per IPv6 inviano messaggi RS ICMPv6 all'indirizzo multicast di tipo "tutti i router". Il messaggio RS richiede al router IPv6 di emettere un messaggio RA per assistere il dispositivo nella configurazione del proprio indirizzo.

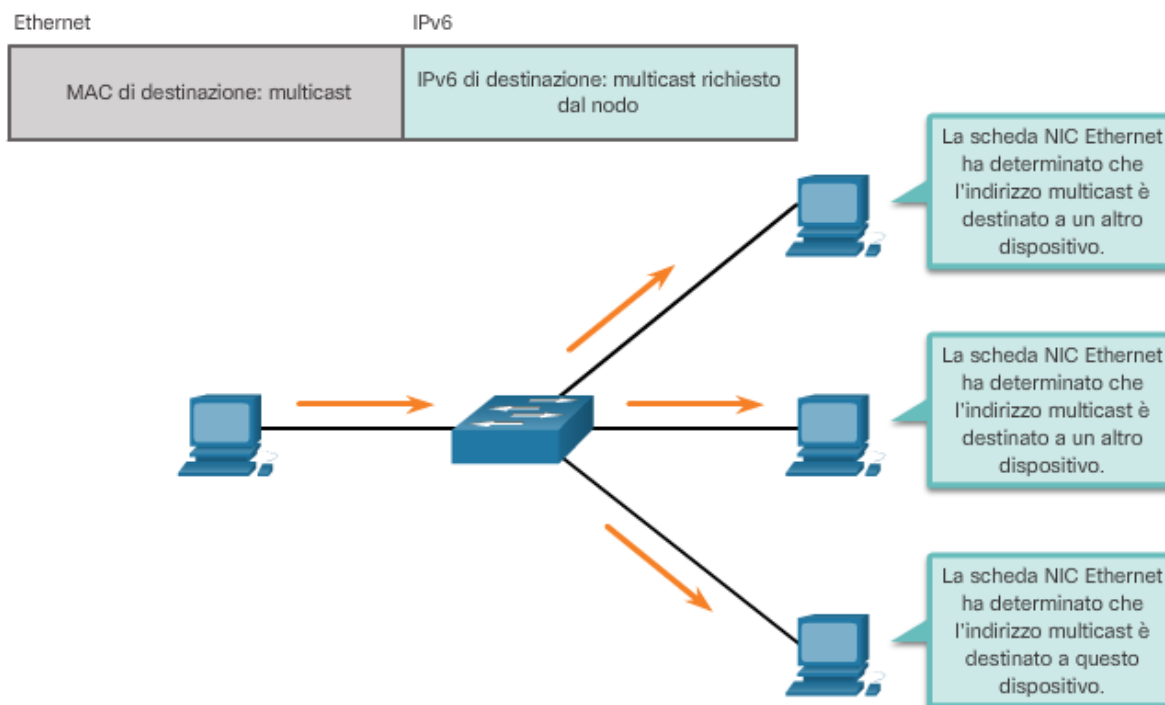
Comunicazioni multicast con tutti i nodi IPv6



Indirizzi IPv6 multicast richiesti dal nodo

Un indirizzo multicast richiesto dal nodo è simile all'indirizzo multicast di tipo "tutti i nodi". Il vantaggio di un indirizzo multicast richiesto dal nodo è dato dal fatto che è associato a un indirizzo multicast Ethernet speciale. Ciò consente alla NIC Ethernet di filtrare il frame esaminando l'indirizzo MAC di destinazione senza inviarlo al processo IPv6 per verificare se il dispositivo è la destinazione prevista del pacchetto IPv6.

Indirizzo multicast richiesto dal nodo IPv6



ICMPv4 e ICMPv6

Sebbene IP sia solo un protocollo best effort (non si garantisce la consegna), la suite TCP/IP prevede l'invio di messaggi nel caso in cui si verifichino determinati errori. Questi messaggi vengono inviati utilizzando i servizi di ICMP. Lo scopo di questi messaggi non è rendere affidabile il protocollo IP, ma fornire feedback sui problemi relativi all'elaborazione di pacchetti IP in determinate condizioni. I messaggi ICMP non sono obbligatori e spesso non sono consentiti all'interno di una rete, per motivi di sicurezza.

ICMP è disponibile sia per IPv4 che per IPv6. ICMPv4 è il protocollo di messaggistica per IPv4. ICMPv6 offre gli stessi servizi per IPv6, ma include ulteriori funzionalità. In questo corso, il termine ICMP verrà utilizzato quando ci si riferisce sia a ICMPv4 che a ICMPv6.

I tipi di messaggi ICMP e i motivi del loro invio sono vari. Di seguito verranno illustrati alcuni dei messaggi più comuni.

I messaggi ICMP condivisi da ICMPv4 e ICMPv6 includono:

- Host confirmation (Conferma dell'host)
- Destination or Service Unreachable (Destinazione o servizio irraggiungibile)
- Time exceeded (Tempo scaduto)
- Route redirection (Reindirizzamento di route)

Host Confirmation

È possibile utilizzare un messaggio echo ICMP per stabilire se un host è operativo. L'host locale invia una richiesta echo ICMP a un host. Se l'host è disponibile, l'host di destinazione risponde inviando una risposta echo. Nella figura, fare clic sul pulsante Riproduci per visualizzare un'animazione della richiesta/risposta echo ICMP. Questo utilizzo dei messaggi echo ICMP è alla base dell'utilità ping.

Destination or Service Unreachable

Quando un host o un gateway ricevono un pacchetto che non possono consegnare, possono utilizzare un messaggio ICMP Destination Unreachable (Destinazione non raggiungibile) per informare l'origine che la destinazione o il servizio non sono raggiungibili. Il messaggio include un codice che indica il motivo per cui non è stato possibile consegnare il pacchetto.

Alcuni dei codici di destinazione non raggiungibile per ICMPv4 sono:

- 0 - Net unreachable (Rete non raggiungibile)
- 1 - Host unreachable (Host non raggiungibile)
- 2 - Protocol unreachable (Protocollo non raggiungibile)
- 3 - Port unreachable (Porta non raggiungibile)

Nota: in ICMPv6, i codici per i messaggi di destinazione non raggiungibile sono simili, ma leggermente diversi.

Time Exceeded

Il messaggio di tempo scaduto ICMPv4 viene usato dal router per indicare che un pacchetto non può essere inoltrato perché il campo Time to Live (TTL) (Durata) del pacchetto è stato ridotto a 0. Se un router riceve un pacchetto e riduce il campo TTL nel pacchetto IPv4 a zero, elimina il pacchetto e invia un messaggio Time Exceeded all'host di origine.

ICMPv6 invia anche un messaggio Time Exceeded se il router non è in grado di inoltrare un pacchetto IPv6 perché il pacchetto è scaduto. IPv6 non contiene un campo TTL, ma utilizza il campo del limite di hop per stabilire se il pacchetto è scaduto.

Messaggi RS e RA ICMPv6

I messaggi informativi e di errore di ICMPv6 sono molto simili ai messaggi di controllo e di errore implementati da ICMPv4. Tuttavia, ICMPv6 presenta nuove funzioni e funzionalità migliorate non disponibili in ICMPv4. I messaggi ICMPv6 sono incapsulati in IPv6.

ICMPv6 include quattro nuovi protocolli come parte del protocollo Neighbor Discovery (ND o NDP).

Scambio di messaggi tra un router IPv6 e un dispositivo IPv6:

- Messaggio Router Solicitation (RS)
- Messaggio Router Advertisement (RA)

Scambio di messaggi tra dispositivi IPv6:

- Messaggio Neighbor Solicitation (NS)
- Messaggio Neighbor Advertisement (NA)

Nota: ICMPv6 ND include anche il messaggio di reindirizzamento, che ha una funzione simile al messaggio di reindirizzamento utilizzato in ICMPv4.

I messaggi NS e NA vengono utilizzati per la risoluzione degli indirizzi e il rilevamento degli indirizzi duplicati (DAD).

Risoluzione degli indirizzi

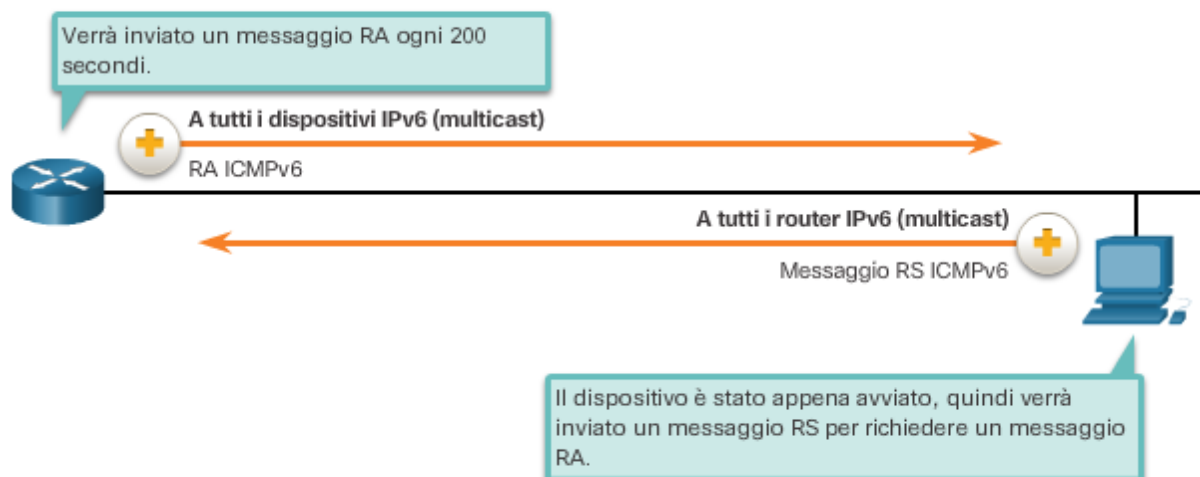
La risoluzione degli indirizzi viene utilizzata quando un dispositivo nella LAN conosce l'indirizzo IPv6 unicast di una destinazione, ma non il relativo indirizzo MAC Ethernet. Per stabilire l'indirizzo MAC per la destinazione, il dispositivo invia un messaggio NS all'indirizzo del nodo richiesto. Il messaggio include l'indirizzo IPv6 noto (di destinazione). Il dispositivo con l'indirizzo IPv6 di destinazione risponde con un messaggio NA contenente il proprio indirizzo MAC Ethernet. La Figura 2 mostra due computer che si scambiano messaggi NS e NA. Fare clic su ogni messaggio per ulteriori informazioni.

Rilevamento degli indirizzi duplicati (DAD)

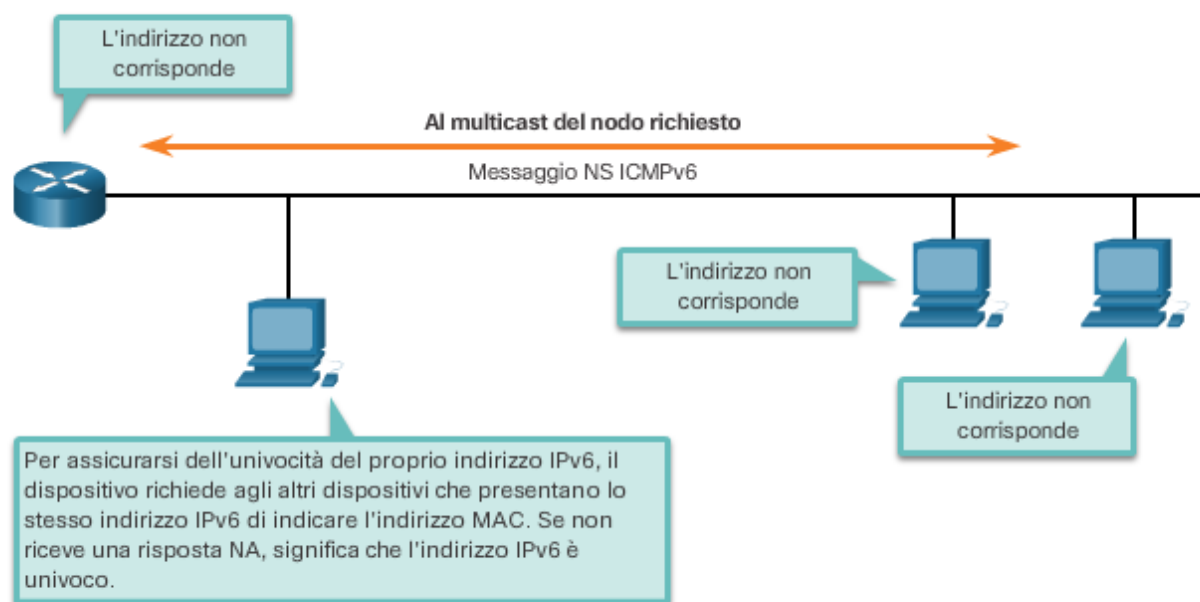
Quando a un dispositivo viene assegnato un indirizzo unicast globale o un indirizzo unicast link-local, si consiglia di eseguire il DAD sull'indirizzo in modo da garantire che sia univoco. Per verificare l'univocità di un indirizzo, il dispositivo invia un messaggio NS con il proprio indirizzo IPv6 come indirizzo IPv6 di destinazione, come mostrato nella Figura 3. Se un altro dispositivo nella rete dispone di questo indirizzo, risponde con un messaggio NA. Questo messaggio NA comunica al dispositivo di invio che l'indirizzo è in uso. Se un messaggio NA corrispondente non viene restituito entro un determinato periodo di tempo, l'indirizzo unicast è univoco e può essere utilizzato.

Nota: il DAD non è obbligatorio, ma l'RFC 4861 consiglia di eseguirlo sugli indirizzi unicast.

Messaggi tra un router IPv6 e un dispositivo IPv6



Rilevamento degli indirizzi duplicati (DAD)



Ping: Verifica dello stack locale

Il ping è un'utilità di test che utilizza messaggi di richiesta e di risposta echo ICMP per verificare la connettività tra host. Il ping funziona sia con gli host IPv4 che IPv6.

Per verificare la connettività con un altro host in una rete, viene inviata una richiesta echo all'indirizzo dell'host utilizzando il comando ping. Se l'host all'indirizzo specificato riceve la richiesta echo, risponde con una risposta echo. Alla ricezione della risposta echo, il ping fornisce feedback sul tempo intercorso tra l'invio della richiesta e la ricezione della risposta. Questo può rappresentare un'indicazione delle prestazioni di rete.

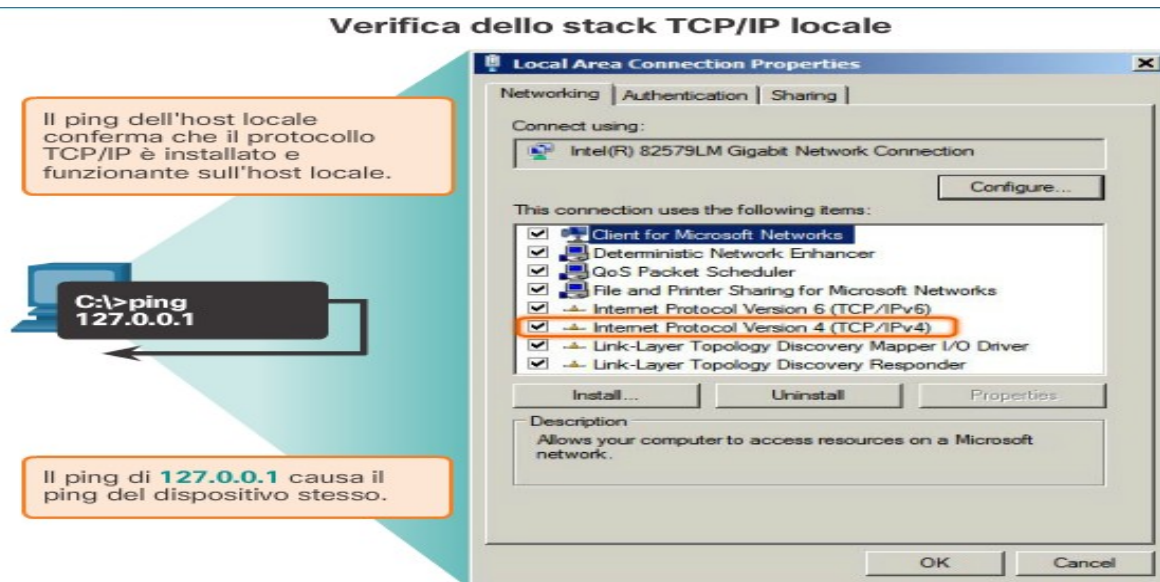
Il ping ha un valore di timeout per la risposta. Se una risposta non viene ricevuta entro il tempo di timeout, il ping restituisce un messaggio che indica che non è stata ricevuta alcuna risposta. Questo di norma indica la presenza di un problema, ma potrebbe indicare anche che nella rete sono state abilitate le funzioni di sicurezza che bloccano i messaggi ping.

Dopo che tutte le richieste sono state inviate, l'utilità ping fornisce un riepilogo che include la percentuale di successo e il tempo medio di round trip alla destinazione.

Ping del loopback locale

Esistono alcuni casi speciali di test e verifica per i quali è possibile utilizzare il ping. Un caso è quello della verifica della configurazione interna di IPv4 o IPv6 sull'host locale. Per eseguire questo test, inviare un ping all'indirizzo di loopback locale 127.0.0.1 per IPv4 (::1 per IPv6). La verifica del loopback IPv4 viene illustrata nella figura.

Una risposta da 127.0.0.1 per IPv4 o ::1 per IPv6 indica che IP è installato correttamente sull'host. La risposta proviene dal livello rete. Tuttavia, la risposta non rappresenta un'indicazione della corretta configurazione di indirizzi, subnet mask o gateway, né fornisce alcuna indicazione relativa allo stato dei livelli inferiori dello stack di rete. Esegue semplicemente il test di IP fino al livello rete. Un messaggio di errore indica che TCP/IP non è operativo nell'host.



12.17 Indirizzi IPv6 allocati da IANA

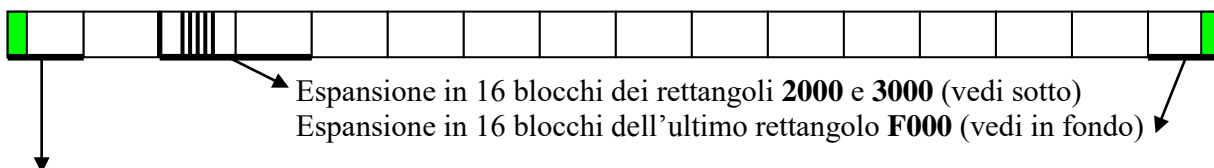
Vedi url: <http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml>
 Inoltre: Per gli **indirizzi Speciali** → RFC 4773 e 6890 + url:
<http://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml>
 Per gli **indirizzi Global Unicast** (=instradabili sul web), **già allocati ai RIRs o liberi**:
<http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xhtml>
 Per gli **indirizzi Multicast**, **allocati o liberi**:
<http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml>

Range o singolo IPv6	Nome	Scopo	(in giallo, gli indirizzi principali)
::/128	Unspecified	Nessun IPv6 assegnato, RFC 4291	
::1/128	Loopback	Se stessi , come IPv4 127.0.0.1, RFC 4291	
::2/128 - 03FF::/16 (::10 - 00000011 11111111:...)	(Global Un. riserv.)	Contiene vari sub-range assegnati o deprecati , ad es. per gli IPv4-embedded o IPv4-mapped	
0400::/6 - 1FFF::/16 (00000100 - 00011111 11111111:...)	(Global Un. riserv.)	per espandibilità futura, per ora sono di IANA; coprono, con gli altri, oltre il 95% degli IPv6	
2000::/3 (0010...)	Global Unicast	IPv6 Globali assegnati ai 5 RIRs, e Speciali : cfr RFC 2928	
- 2001::/23	IETF Protocol	Per interoperabilità IPv4 – IPv6, RFC 4380	
- 2001::/32	TEREDO	cfr RFC 5180	
- 2001:2::/48	Benchmarking	cfr RFC 4843	
- 2001:10::/28	ORCHID		
- 2001:0200::/23 - 2001:B000/20	Global Unicast	Assegnati ai 5 RIRs; (libero da 2001:C000/18)	
- 2001:DB8::/32	Documentation	cfr RFC 3849 (“sottratto” ad APNIC !)	
- 2002::/16	6to4	Per interoperabilità IPv4 – IPv6, RFC 3056	
- 2003::/18	Global Unicast	Assegnato al RIPE NCC	
- 2400::/12 - 2C00::/12	Global Unicast	Assegnati variamente, in piccola parte , ai 5 RIRs	
- 2C10::/12 - 3FFF::/16	(Global Un. riserv.)	per espandibilità futura, come 0400:: ... (vedi)	
4000::/2 - FBFF::/6 (0100 - ...)	(Global Un. riserv.)	per espandibilità futura, come 0400:: ... (vedi)	
FC00::/7 - FFFF::/16 (11111100:: - 11111101 11111111:...)	Unique-local (ULA)	Simili agli IPv4 Privati della RFC 1918 (10..., 172.16-31..., 192.168...) nelle LAN; RFC 4193	
FE00::/9 (11111110:0::)	(Global Un. riserv.)	per espandibilità futura, come 0400:: ... (vedi)	
FE80::/9 (11111110:1::)	(indirizzi privati)	cfr RFC 4291, che li presenta in due gruppi :	
- FE80::/10 (11111110:10::)	Link-local, o Link-Scoped	Indirizzi Unicast non instradabili su Internet, da usare solo nelle LAN, tipo APIPA 169.254.x.y, e	
- FEC0::/10 (11111110:11::)	Site-local Scoped	cfr RFC 3513; prima versione con funzione degli Unique-local FC00::/7 (vedi sopra), oggi deprecata	
FF00::/8 (11111111::)	Multicast	Pacchetti destinati a tutti i nodi associati :	
- FF01::1 o ::2 o ::FB/128	Node-local Scope	cfr RFC 3307, 4291 e 6762 (::FB → DNS)	
- FF02::1/128	Link-local Scope	è il simil-broadcast : a tutti i nodi del link	
- FF02::2/128	idem	è il router-multicast : a tutti i Router del link	
- FF02::5 o ::6 o ::9 o ::A/128	(routing protocols)	a tutti i Router OSPFv3, RIPng ed EIGRP del link	
- FF02::x/128	(altri 30 Link-local Sc.)	tra cui FF02::1:2 = All DHCPv6 Agents & Servers e FF02::1:3 = Link-local Multicast Name Resolution, tipo DNS (RFC 4795)	
- FF05::x/128	Site-local Scope	cfr RFC 3307, 3315, 4291, 6762 e 6621, tra cui FF05::1:3 = All DHCPv6 Servers (RFC 3315, come anche FF02:1::2)	
- FF0x::x/128	Variable Scope	cfr RFC 3307, 4291 e altre (sono circa 80)	
- FF3x::x/128	Source-Specific	cfr RFC 3307 e 4607	
- altri FF00::/8	(Multicast riservati)	da definire	

Graficamente

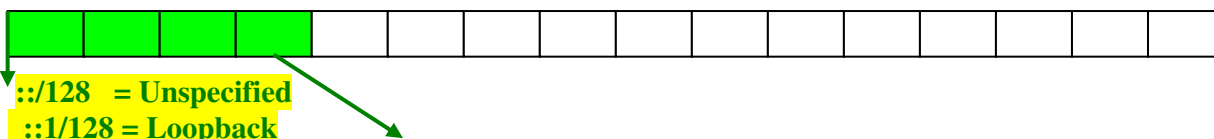
Spazio di indirizzamento IPv6 – ogni rettangolo indica la prima cifra hex dell'IPv6:

0000 1000 2000 3000 4000 5000 6000 7000 8000 9000 A000 B000 C000 D000 E000 F000



(Blocco 0) Espansione in 16 blocchi del primo rettangolo 0000:

0000 0100 0200 0300 0400 0500 0600 0700 0800 0900 0A00 0B00 0C00 0D00 0E00 0F00

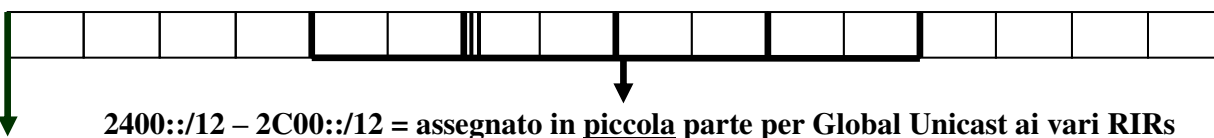


Nel range colorato **::2/128 - 03FF::/16**, poche assegnazioni (IPv4-mapped addr., Discard Only, ecc.)

Tutto il resto del blocco 0000::/4 (i 3/4 finali, da 0400::/6) è ancora da assegnare.

(Blocchi 2-3) Espansione in 16 blocchi dei rettangoli 2000 e 3000:

2000 2100 2200 2300 2400 2500 2600 2700 2800 2900 2A00 2B00 2C00 2D00 2E00 2F00



2001::/16 = assegnato in buona parte per Global Unicast ai vari RIRs (con 2001:DB8::/32 x Doc.) fino a 2001:B000::/20, mentre 2001:C000::/18 resta da assegnare. NB: dal solo blocco 2001::/16 si possono assegnare blocchi /23 a 128 richieste dei RIRs; finora circa 80.

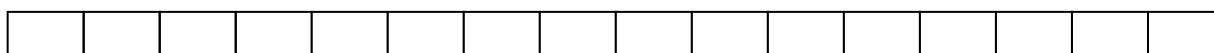
Da un blocco /23, un RIR assegna blocchi /32 a 512 richieste degli ISP → 65536 utenti.

2002::/16 = assegnato per 6to4 (interoperabilità IPv4 – IPv6)

2003::/18 = assegnato al RIR RIPE NCC

Tutto il resto del blocco 2000::/4 (frammentato) è da assegnare.

3000 3100 3200 3300 3400 3500 3600 3700 3800 3900 3A00 3B00 3C00 3D00 3E00 3F00

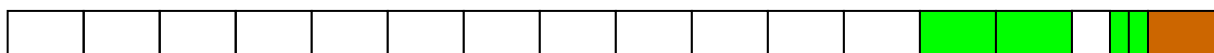


Preallocato per Global Unicast nel blocco 2000::/3, ma TUTTO ancora da assegnare

Conteneva pochi range obsoleti e ora deprecati, per **Teredo** e **6bone**, che sono stati **restituiti** a IANA.

(Blocco F) Espansione in 16 blocchi dell'ultimo rettangolo F000:

F000 F100 F200 F300 F400 F500 F600 F700 F800 F900 FA00 FB00 FC00 FD00 FE00 FF00



FC00::/7 = Unique-local

FE00::/9 = Global Unicast da assegnare

FE80::9 = IPv6 privati, divisi in: FE80::/10 = Link-local, e FEC0::/10 = Site-local, deprecati

FF00::/8 = Multicast, con 5 sottogruppi: Node-local, **Link-local**, **Site-local**, Variable Scope e S.S.

Tutto il resto del blocco F000::/4 (i 3/4 iniziali, fino a FC00::/6 escluso) è da assegnare.

Tutti i rettangoli bianchi  sono ancora riservati a IANA, **da assegnare** (oltre il 95%).

IPv4 vs. IPv6 **parallel slalom**

By: Marco Paganini – eForHum Milan – May 2015

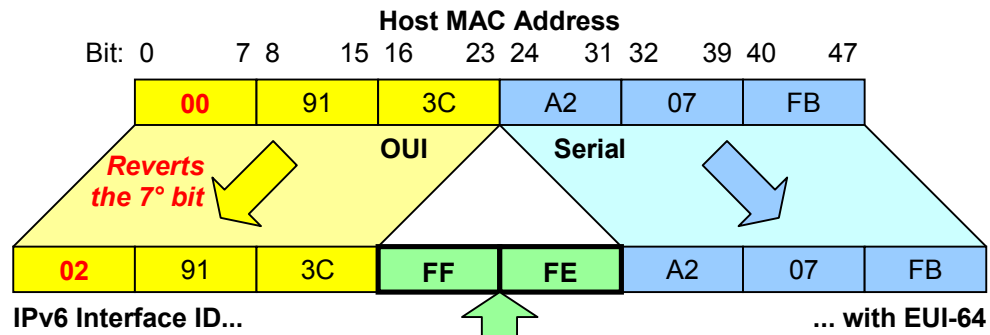
N.	Feature	IPv4	START	IPv6
1	N. of address bits	32	●	128
2	N. of addresses	4.3 billions = 2^{32}	●	340 undecillions, i.e. billions of billions of billions of billions = 2^{128}
3	Representation	Dotted Decimal Notation	●	8 groups of 4 hex digits/each; a group is also called an hextet
4	Typical address	192.168.0.1	●	2001:0db8:acad:0001:0000:0000:0000:1234 or 2001:db8:acad:1:0:0:0:1234 or 2001:db8:acad:1::1234
5	CIDR – Classless Inter-Domain Routing, or prefix length	From /8 to /30 for nets and subnets but also < /8 for supernets; Cisco also accepts /31 subnets, and the /32 “host mask” (an IP alone)	●	/48 for nets and /64 for subnets, but also < /48 for supernets, and /49 - /63 for subnet aggregation; subnets may have prefix > /64, at the nibble boundary (/68, /72...)
6	Subnet Mask	Dotted Decimal Notation, with all “1” on the left, i.e. 255.255.255.0	●	Not used: network portion is the “prefix length” only, i.e. /64
7	Classes	Class A: 1 st byte 0-127 (255.0.0.0) Class B: 128-191 (255.255.0.0) Class C: 192-223 (255.255.255.0) (A, B & C are for Unicast traffic) Class D: 224-239 (Multicast) Class E: 240-255 (IANA reserved)	●	No Classes at all (so, no automatic summarization applies for IPv6 networks / addresses)
8	N. of subnets	It depends on the bits borrowed from the Host portion of the Major net; i.e. 172.16.3.0 255.255.255.0 has 8 bits borrowed from a Class B net, so it's one of $2^8 = 256$ subnets	●	Subnets are normally 2^{16} (65.536) for each net, or Site prefix (/48); all the fourth hextet is dedicated to the subnets definition, by default
9	What ISPs allocate / sell to their customers	Small number of public addresses (no longer available) i.e. /32 for 1 address, /31 for 2 addresses, /30 for 4, /29 for 8, /28 for 16... Small/residential users very often only receive one dynamic public address on their WAN link interf.	●	Normally, ISPs allocate /48 site prefixes to their customers, regardless of their “importance”. Each customer has then up to 65.536 subnets “for free”; if no subnets are used, set fourth hextet to 0, or to 1, or to ffff, or to any!
10	N. of addresses per interface	Normally only one (but secondary addresses can seldom be used)	●	Normally, IPv6 interfaces have: - a Link-local address alone, for local comm. only (i.e. FE80::1/64) - a Global-unicast address, with a Link-local mate, for global comm. Global-unicast addresses can be more than one; Link-local is one
11	Size of the subnets	It depends on the bits leaved in the Host portion of the address, after subnetting was possibly done. Major Class A nets have $2^{24} = 16,7$ millions IPs; /30 only have 4 IPs	●	Normally, subnets have 64 bits in the IID-Interface ID portion of the address, the rightmost half of it. Thus, IPv6 subnets allow for $2^{64} = 18.5$ billions of billions of IPs

12	Scopes of addresses	Unicast (Classes A, B & C) Multicast (Class D) Broadcast (directed 192.168.0.255 or limited 255.255.255.255)	Unicast (different types → see) Multicast (FF00::/8); includes the ● “broadcast concept” (= FF02::1) Anycast (these are Global-unicast assigned to different devices)
13	Special and public addresses	0.0.0.0/32 = unspecified IPv4 0.0.0.0/8 = reserved ● 127.0.0.0/8 = loopback / local host (16 million addresses... wasted) 10.0.0.0/8 = private Class A netw. 172.16.0.0/12 = private Class B n. 192.168.0.0/16 = private Class C 169.254.0.0/16 = APIPA-Autom. Private IP Addressing / Link-local All other A-B-C Class are public	::/128 = unspecified IPv6 ::1/128 = loopback / local host (only 1 address of the... infinite) FC00::/7 = Unique-local (ULA), routable only within their Site FE80::/10 (RFC 4291: FE80::/64) = Link-local, non routable, only for local communication on a link FF00::/8 = Multicast, of 5 scopes 2000::/3 = public Global-unicast (small parts of 2000::/4 assigned, mostly from 2001::/16)
14	Documentation addresses	192.0.2.0/24 209.165.200.0/24 ... 201.0 ... 202.0 and few others (seldom used)	● 2001:db8::/32, supplied by APNIC; third hexet is typically “acad”, “beef”, “cafe”, “feed”...
15	NAT	Different uses of NAT allow: - Client with private addresses to access the Web (dynamic + PAT) - DMZ Servers to be reachable from the Web on public addresses ● - merging of two networks with similar private addressing, etc.	No NAT is used for IPv6: Global-unicast addresses are public. NAT64 is used for IPv4 – IPv6 coexistence in the short term, by replacement of Packet headers
16	Layer 3 to Layer 2 address resolution protocol	ARP – A special Packet (Ethernet code 0x806) is sent to L2 broadcast (ff-ff-ff-ff-ff-ff), requesting the MAC address of the local node with a given IP	● ND – Neighbor Discovery: a NS-Neighbor Solicitation ICMPv6 message (code 135) is sent to the target node, requesting a NA-Neighbor Advertisement (code 136) from it, with its MAC addr.
17	ICMP and PING	The ICMPv4-Internet Control Message Protocol v4 includes up to 15 different message types (from 0 to 18, with holes); the most used types are: 0=Echo Reply, 3=Destination unreachable (with subcodes), 8=Echo Request and 11=Time Exceeded. PING = 8 → 0 ●	The ICMPv6 protocol includes many messages for functions similar to the ICMPv4 ones, plus the ND-Neighbor Discovery suite described above, including also the RS-Router Solicitation (code 133), RA-Router Advertisement (code 134) and Redirect (c. 137). PING = 135 → 136
18	Static address configuration methods	Only one method is available: just configure the address and its Subnet Mask: that’s all, folks!	● Three static methods are available to setup a Global-unicast address: - fully static: assign all 128 bits - EUI-64: assign the /64 prefix and add eui-64 : the IID is derived from a local MAC (see A1) or from the fully static Link-local - random: only on Windows PCs

19	How to enable the routing globally on Cisco IOS	IPv4 is already enabled by default on Cisco Routers and Multilayer Switches ●	To turn a Router or a Multilayer Switch into a dual-stack device, use the command: D(config)# ipv6 unicast-routing
20	How to enable an interface on the protocol on Cisco IOS	IPv4 is always enabled by default on Cisco Routers and Multilayer Switches routed interfaces; just add an IP and no shut to the interface ●	By adding the command: D(config)# ipv6 enable to an interface, it generates its EUI-64 Link-local address
21	Dynamic address configuration methods	After ICMP, RARP and BOOTP made the history, today only the DHCP-Dynamic Host Configuration Protocol is available (RFC 2131 & 2132 for optional fields): Cl. → Se. DHCP Discover (L2 bro) Se. → Cl. DHCP Offer (L2 unicast) Cl. → Se. DHCP Request (L2 bro) Se. → Cl. DHCP Ack (L2 unicast). Other messages are defined, i.e. Nak, Decline, Release and Inform. DHCP can supply > 30 parameters ●	Again, three dynamic methods: - SLAAC-StateLess Address AutoConfiguration: the node finds a Router on its link (→ FF02::2) and receives the prefix and D.G. (Router's Link-local) + EUI-64 - Stateless DHCPv6: the same as above, but a DHCPv6 Server can add DNS, domain name, NTP, etc - Stateful DHCPv6: the Router delegates the duty to a DHCPv6 Server (sometimes... to itself!)
22	How to get a dynamic address under Cisco IOS	D(config-if)# ip address dhcp ●	Referring to the three methods: - D(config-if)# ipv6 address autoconfig for methods 1 & 2 - D(config-if)# ipv6 address dhcp for Stateful DHCPv6 method
23	How to route DHCP requests to a remote (helper) Server	D(config-if)# ip helper-address ipv4-address-of-Server on the interface receiving the DHCP Discover messages ●	D(config-if)# ipv6 relay destination ipv6-address-of-Server on the interface receiving the DHCPv6 Solicit messages
24	D.V. routing protocols	RIPv1, RIPv2, IGRP, EIGRP ●	RIPng, EIGRP for IPv6 EIGRP is activated by no shut . Networks are supplied to protocol in the D(config-if)# mode
25	L.S. routing protocols	OSPFv2, IS-IS ●	OSPFv3 Networks are supplied to protocol in the D(config-if)# mode
26	Packet Header	It is normally a 20 bytes header, with 12 fields (see A2), namely: Vers.=4, IHL=5, ToS, Pkt length, Identif + Flags + Pkt offset (for Packet fragmentation), TTL, Protocol (i.e. 1=ICMP, 6=TCP, 17=UDP, 41=IPv6), Header checksum, Source address, Destination addr. ●	It is normally a 40 bytes header with 8 fields (see A3), namely: Vers.=6, Traffic class, Flow label, Payload length, Next header, Hop limit, Source address, Destination address. Additional Extension Headers can follow, for fragmentation, VPN...
27	Ethertype	The 16 bits code used by Layer 2 protocols to identify IPv4 is 0x800 = 0000 1000 0000 0000 ●	The 16 bits code used by Layer 2 protocols to identify IPv6 is 0x86DD = 1000 0110 1101 1101
28			
29			
30			

Annexes

A1 – EUI-64 method to generate a unique IID for IPv6 addresses



A2 – IPv4 Packet Header

Byte 1		Byte 2		Byte 3		Byte 4	
Vers = 4	IHL = 5	Type of Service	Packet Length				
Identification			Flags	Fragment Offset			
TTL-Time To Live		Protocol	Header Checksum				
Source Address							
Destination Address							
Options					Padding...		
Data / Payload (L4 Segment)							
...							

A3 – IPv6 Packet Header

Byte 1		Byte 2		Byte 3		Byte 4	
Vers. = 6	Traffic Class (8 bit)		Flow Label (20 bit)				
Payload Length			Next Header		Hop Limit		
Source Address (128 bit)							
.							
.							
.							
Destination Address (128 bit)							
.							
.							
.							
Data / Payload (or Next Header)							
...							