

# Informazioni sul protocollo ARP (Proxy Address Resolution Protocol)

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Come funziona il proxy ARP?](#)

[Esempio di rete](#)

[Vantaggi del proxy ARP](#)

[Svantaggi del proxy ARP](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come il protocollo ARP proxy aiuti i computer di una subnet a raggiungere subnet remote senza dover configurare il routing o un gateway predefinito.

## Prerequisiti

### Requisiti

Questo documento richiede la comprensione dell'ambiente ARP (Proxy Address Resolution Protocol) e Ethernet.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS® Software Release 12.2 (10b)
- Cisco serie 2500 Router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

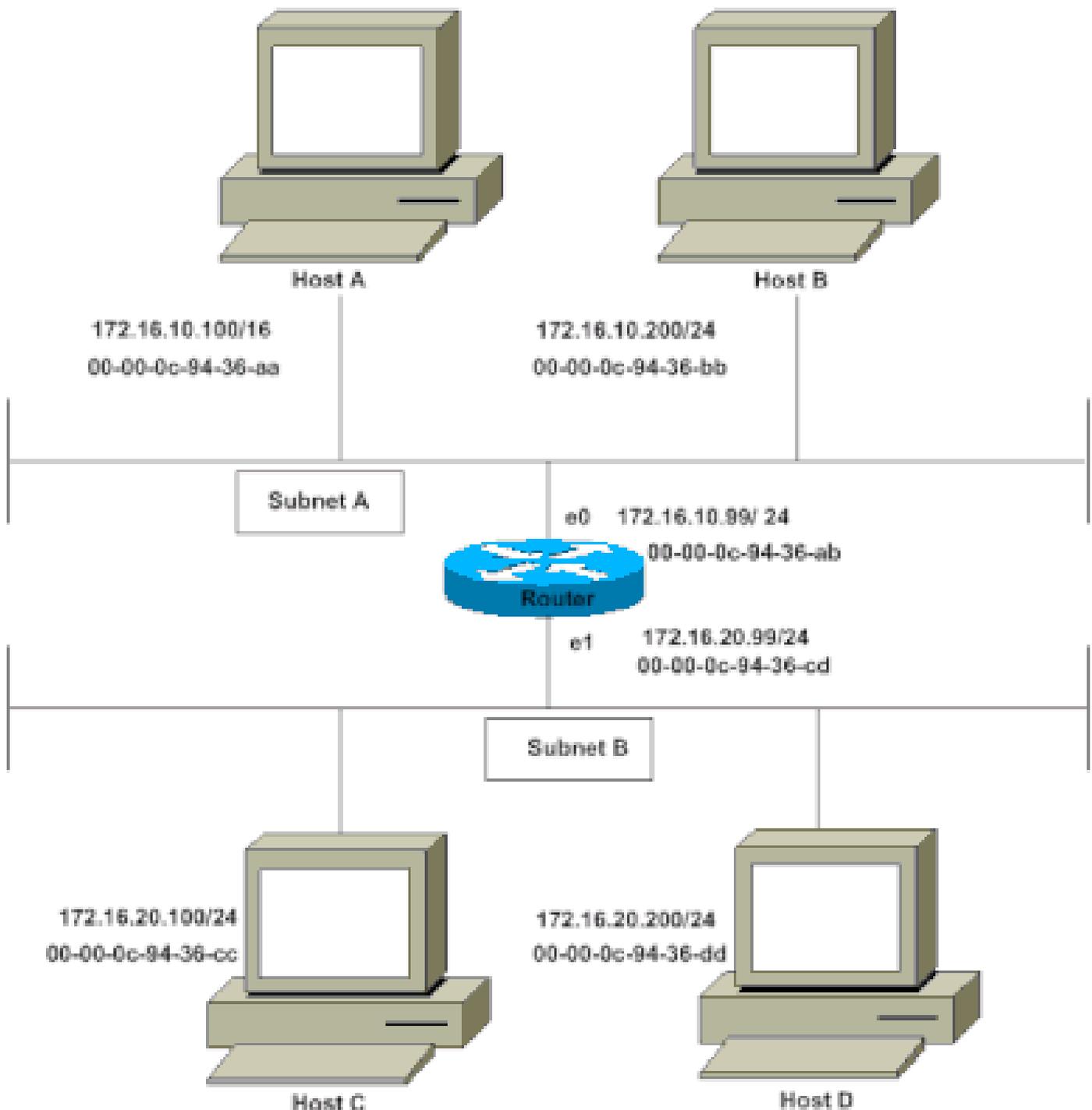
## Premesse

In questo documento viene spiegato il protocollo proxy Address Resolution Protocol (ARP). Nel protocollo proxy ARP, un host, in genere un router, risponde alle richieste ARP destinate a un'altra macchina. Se si falsifica la propria identità, il router accetta la responsabilità di inoltrare i pacchetti alla destinazione "reale". Il proxy ARP può aiutare le macchine di una subnet a raggiungere le subnet remote senza configurare il routing o un gateway predefinito. Il proxy ARP è definito nella RFC 1027.

## Come funziona il proxy ARP?

Questo è un esempio di come funziona il proxy ARP:

Esempio di rete



Esempio di rete

L'host A (172.16.10.100) sulla subnet A deve inviare i pacchetti all'host D (172.16.20.200) sulla subnet B. Come mostrato nel diagramma, l'host A ha una subnet mask /16. Ciò significa che l'host A ritiene di essere connesso direttamente a tutta la rete 172.16.0.0. Quando l'host A deve comunicare con uno dei dispositivi che ritiene siano collegati direttamente, invia una richiesta ARP alla destinazione. Riepilogando, quando l'host A deve inviare un pacchetto all'host D, suppone che quest'ultimo sia connesso direttamente e gli invia una richiesta ARP.

Per raggiungere l'host D (172.16.20.200), l'host A deve conoscere l'indirizzo MAC dell'host D.

Quindi, l'host A trasmette una richiesta ARP sulla subnet A, come mostrato:

Indirizzo MAC mittente	Indirizzo IP mittente	Indirizzo MAC di destinazione	Target IP address
------------------------	-----------------------	-------------------------------	-------------------

00-00-0c-94-36-aa	172.16.10.100	00-00-00-00-00-00	172.16.20.200
-------------------	---------------	-------------------	---------------

In questa richiesta ARP, l'host A (172.16.10.100) chiede che l'host D (172.16.20.200) gli invii l'indirizzo MAC. Il pacchetto della richiesta ARP viene quindi incapsulato in un frame Ethernet con l'indirizzo MAC dell'host A come indirizzo di origine e l'indirizzo di broadcast (FFFF.FFFF.FFFF) come indirizzo di destinazione. Poiché la richiesta ARP è una richiesta di broadcast, raggiunge tutti i nodi della subnet A, inclusa l'interfaccia e0 del router, ma non raggiunge l'host D. La richiesta di broadcast non raggiunge l'host D perché i router, per impostazione predefinita, non inoltrano pacchetti di broadcast.

Poiché il router sa che l'indirizzo di destinazione (172.16.20.200) si trova su un'altra subnet e può raggiungere l'host D, risponde con il proprio indirizzo MAC all'host A.

Indirizzo MAC mittente	Indirizzo IP mittente	Indirizzo MAC di destinazione	Target IP address
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

Questa è la risposta proxy ARP che il router invia all'host A. Il pacchetto di risposta proxy ARP è incapsulato in un frame Ethernet il cui indirizzo di origine è l'indirizzo MAC del router e il cui indirizzo di destinazione è l'indirizzo MAC dell'host A. Le risposte ARP sono sempre unicast rispetto al richiedente originale.

Alla ricezione di questa risposta ARP, l'host A aggiorna la tabella ARP, come mostrato:

Indirizzo IP	Indirizzo MAC
172.16.20.200	00-00-0c-94-36-ab

Da questo momento in poi, l'host A inoltra tutti gli altri pacchetti che devono raggiungere 172.16.20.200 (host D) all'indirizzo MAC 00-00-0c-94-36-ab (router). Poiché il router sa come raggiungere l'host D, inoltra il pacchetto all'host D. La cache ARP sugli host nella subnet A viene popolata con l'indirizzo MAC del router per tutti gli host della subnet B. Quindi, tutti i pacchetti destinati alla subnet B vengono inviati al router. Il router inoltra tali pacchetti agli host della subnet B.

Nella tabella viene mostrata la cache ARP dell'host A:

Indirizzo IP	Indirizzo MAC
172.16.20.200	00-00-0c-94-36-ab
172.16.20.100	00-00-0c-94-36-ab
172.16.10.99	00-00-0c-94-36-ab
172.16.10.200	00-00-0c-94-36-bb



Nota: più indirizzi IP sono associati a un unico indirizzo MAC, l'indirizzo MAC di questo router, a indicare che il proxy ARP è in uso.

---

L'interfaccia di Cisco deve essere configurata in modo da accettare e rispondere al proxy ARP. L'opzione è abilitata per impostazione predefinita. Il **no ip proxy-arp** comando deve essere configurato sull'interfaccia del router collegato al router ISP. Il ARP proxy può essere disabilitato su ciascuna interfaccia singolarmente con il comando di configurazione interfacciano **ip proxy-arp** , come mostrato:

```
<#root>
```

```
Router#
```

```
configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#

```
interface ethernet 0
```

Router(config-if)#

```
no ip proxy-arp
```

Router(config-if)#

^Z

Router#

Per abilitare il protocollo ARP proxy su un'interfaccia, usare il comando di configurazione dell'**ip proxy-arp** interfaccia.

---

---



Il vantaggio principale del proxy ARP è che può essere aggiunto a un singolo router sulla rete senza interferire con le tabelle di routing degli altri router.

Il proxy ARP deve essere utilizzato sulla rete in cui gli host IP non sono configurati con un gateway predefinito o non hanno funzionalità di routing.

## **Svantaggi del proxy ARP**

Gli host non hanno alcuna idea dei dettagli fisici della propria rete e presumono che si tratti di una rete piatta in cui possono raggiungere qualsiasi destinazione se inviano una richiesta ARP. Quando si utilizza ARP per tutti gli elementi, gli svantaggi sono evidenti. tra cui:

- La quantità di traffico ARP sul segmento aumenta.
- Gli host hanno bisogno di tabelle ARP più grandi per gestire la mappatura tra indirizzi IP e indirizzi MAC.
- La sicurezza può essere compromessa. Una macchina può affermare di essere un'altra per intercettare i pacchetti, una tecnica chiamata "spoofing".
- Non funziona per le reti che non utilizzano il protocollo APR per la risoluzione degli indirizzi.
- Non si applica a tutte le topologie di rete. Ad esempio, se sono presenti più router che si connettono alle due reti fisiche.

## Informazioni correlate

- [Risorse di supporto IP](#)
- [Pagina di supporto NAT](#)
- [Strumenti e risorse](#)
- [Supporto tecnico Cisco e download](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).