

Informazioni su OSPF (Open Shortest Path First): guida alla progettazione

Sommario

[Introduzione](#)

[Premesse](#)

[OSPF e RIP](#)

[Cosa sono i link state \(stati del collegamento\)?](#)

[Algoritmo SPF \(Shortest Path First\)](#)

[Costo OSPF](#)

[Albero dei cammini minimi](#)

[Aree e router di confine](#)

[Pacchetti link state](#)

[Abilitare il protocollo OSPF sul router](#)

[Autenticazione OSPF](#)

[Autenticazione con password semplice](#)

[Autenticazione con digest del messaggio](#)

[Dorsale o area 0](#)

[Collegamenti virtuali](#)

[Aree non connesse fisicamente all'area 0](#)

[Dorsale](#)

[Router vicini](#)

[Adiacenze](#)

[Scelta del router designato \(DR\)](#)

[Creare l'adiacenza](#)

[Adiacenze sulle interfacce point-to-point](#)

[Adiacenze sulle reti NBMA \(Non-Broadcast Multi-Access\)](#)

[Evitare di creare router DR e configurare router vicini sulle reti NBMA](#)

[Sottointerfacce point-to-point](#)

[Selezionare i tipi di rete dell'interfaccia](#)

[OSPF e riepilogo delle route](#)

[Riepilogo delle route inter-area](#)

[Riepilogo delle route esterne](#)

[Aree stub](#)

[Ridistribuire le route nell'OSPF](#)

[Route esterne E1 ed E2](#)

[Ridistribuire l'OSPF negli altri protocolli](#)

[Uso di una metrica valida](#)

[VLSM](#)

[Ridistribuzione reciproca](#)

[Inserire route predefinite nell'OSPF](#)

[Suggerimenti per la progettazione del protocollo OSPF](#)

[Numero di router per area](#)

[Numero di router vicini](#)

[Numero di aree per ABR](#)

[Topologia magliata e parzialmente magliata](#)

[Problemi di memoria](#)

[Riepilogo](#)

[Appendice A: Sincronizzazione del database link state](#)

[Annunci LSA \(Link State Advertisement\)](#)

[Esempio di database OSPF](#)

[Appendice B: OSPF e indirizzamento IP multicast](#)

[Appendice C: Subnet mask a lunghezza variabile \(VLSM, Variable Length Subnet Mask\)](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come funziona il protocollo OSPF e come utilizzarlo per progettare e realizzare reti grandi e complesse.

Premesse

Il protocollo OSPF (Open Shortest Path First), definito nella RFC 2328, è un protocollo gateway interno utilizzato per distribuire le informazioni di routing in un sistema autonomo.

Il protocollo OSPF è nato dall'esigenza di avere un protocollo IGP (Internal Gateway Protocol) non proprietario efficiente per la famiglia di protocolli TCP/IP.

L'idea di un IGP interoperabile comune per Internet era sorta già nel 1988, ma non è stata formalizzata che nel 1991.

All'epoca, il team di lavoro OSPF ha chiesto che il protocollo venisse considerato come un miglioramento del Draft Internet Standard.

A differenza dei tradizionali protocolli di routing Internet, come il RIP, che utilizzano l'algoritmo Bellman-Ford basato sul vettore, il protocollo OSPF si basa sulla tecnologia link state.

OSPF ha introdotto nuovi concetti, tra cui l'autenticazione degli aggiornamenti di routing, le subnet mask a lunghezza variabile (VLSM) e il riepilogo delle route.

In questi capitoli viene descritta la terminologia OSPF, l'algoritmo, i vantaggi e i dettagli del protocollo nella progettazione di reti moderne, grandi e complesse.

OSPF e RIP

La rapida crescita e l'espansione delle reti moderne ha esaurito tutte le potenzialità del protocollo

RIP (Routing Information Protocol), i cui limiti possono causare problemi nelle reti di grande dimensioni:

- Il RIP ha un limite di 15 hop. Una rete con più di 15 hop (15 router) è considerata non raggiungibile.
- Il protocollo RIP non è in grado di gestire le subnet mask a lunghezza variabile (VLSM, Variable Length Subnet Mask). Data la carenza di indirizzi IP e la flessibilità delle VLSM per l'assegnazione efficiente degli indirizzi IP, questa è una limitazione considerevole.

Le trasmissioni periodiche dell'intera tabella di routing consumano molta larghezza di banda. Si tratta di un problema rilevante nelle reti di grandi dimensioni, in particolare quando i collegamenti sono lenti o si usano cloud WAN.

- Nel protocollo RIP, la convergenza è più lenta rispetto all'OSPF. Nelle reti di grandi dimensioni, la convergenza deve essere questione di minuti.
- Periodicamente i router RIP diventano inattivi e raccolgono dati inutili, mentre le informazioni meno recenti vengono scartate lentamente. In ambienti di grandi dimensioni, questo comportamento non è adeguato e potrebbe causare incoerenze nel routing.
- Il protocollo RIP non calcola i ritardi di rete e i costi del collegamento. Le decisioni di routing si basano sul numero di hop. Il percorso con il numero di hop più basso per raggiungere la destinazione è sempre preferito anche se il percorso più lungo ha una larghezza di banda aggregata migliore e meno ritardi.
- Le reti RIP sono reti flat e non prevedono la presenza di aree o confini. L'introduzione del routing senza classi e l'uso intelligente di aggregazione e riepilogo hanno reso le reti RIP obsolete.

Per questo motivo è stata introdotta una nuova versione del protocollo RIP, chiamata RIP2, con alcune migliorie. RIP2 risolve i problemi delle VLSM, l'autenticazione e gli aggiornamenti del routing multicast.

RIP2 non rappresenta un netto miglioramento rispetto al protocollo RIP (ora denominato RIP1) perché presenta ancora limiti nel numero di hop e tempi di convergenza lunghi, due ambiti che non possono essere trascurati nelle reti di grandi dimensioni.

Con il protocollo OSPF invece è possibile affrontare la maggior parte dei problemi di cui abbiamo parlato:

- Il protocollo OSPF non prevede limiti al numero di hop.
- L'uso intelligente della VLSM permette un'allocazione efficiente degli indirizzi IP.
- Il protocollo OSPF usa l'IP multicast per inviare gli aggiornamenti degli stati del collegamento (link state). Questo garantisce un minor consumo delle risorse di elaborazione sui router che non sono in ascolto dei pacchetti OSPF. Gli aggiornamenti non sono inviati a intervalli fissi, ma solo nel caso in cui siano state apportate modifiche al routing. Questo garantisce una larghezza di banda efficiente.
- Il protocollo OSPF ha tempi di convergenza migliori del protocollo RIP, in quanto le modifiche di routing vengono propagate all'istante e non a intervalli prestabiliti.
- Il protocollo OSPF consente un migliore bilanciamento del carico.
- Il protocollo OSPF consente una definizione logica delle reti in cui i router possono essere

suddivisi in aree. Ciò limita la distribuzione degli aggiornamenti link state all'intera rete. Inoltre, fornisce un meccanismo per aggregare le route e ridurre la propagazione non necessaria delle informazioni della subnet.

- Il protocollo OSPF permette di indirizzare l'autenticazione utilizzando diversi metodi di autenticazione delle password.
- Il protocollo OSPF permette di trasferire e contrassegnare con tag le route esterne inserite in un sistema autonomo. In questo modo si tiene traccia delle route esterne immesse da protocolli esterni come BGP.

Ciò comporta una maggiore complessità nella configurazione e nella risoluzione dei problemi delle reti OSPF.

Gli amministratori, abituati alla semplicità del protocollo RIP, devono confrontarsi con una mole di nuove informazioni da imparare per stare al passo con le reti OSPF.

Ciò aumenta il carico di lavoro per l'allocazione della memoria e l'utilizzo della CPU. Per gestire il sovraccarico causato dall'OSPF, potrebbe essere necessario eseguire l'upgrade di alcuni router con protocollo RIP.

Cosa sono i link state (stati del collegamento)?

OSPF è un protocollo link state, ossia raccoglie informazioni sugli stati del collegamento. Si potrebbe pensare al collegamento come a un'interfaccia del router. Lo stato del collegamento è una descrizione di tale interfaccia e del rapporto con i router vicini.

Una descrizione dell'interfaccia può essere, ad esempio, l'indirizzo IP dell'interfaccia, la maschera, il tipo di rete a cui è connessa, i router connessi a tale rete e così via.

Tutti gli stati del collegamento vengono raccolti in un database.

Algoritmo SPF (Shortest Path First)

Il protocollo OSPF usa un algoritmo SPF (Shortest Path First) per creare e calcolare il percorso più breve per tutte le destinazioni. Il percorso più breve viene calcolato con l'algoritmo Dijkstra.

L'algoritmo in sé è complicato, Cerchiamo quindi di descriverne i vari passaggi in modo semplice:

1. Al momento dell'inizializzazione o in seguito a una modifica delle informazioni di routing, un router genera un annuncio LSA (Link State Advertisement). L'annuncio riunisce tutti gli stati del collegamento sul router.
2. Tutti i router si scambiano gli stati del collegamento tramite flooding. Quando riceve un aggiornamento link state, ciascun router deve archivarne una copia nel suo database e trasmetterlo quindi agli altri router.
3. Una volta aggiornati tutti i database, il router calcola un albero dei cammini minimi per tutte le destinazioni. Il router usa l'algoritmo di Dijkstra per calcolare l'albero dei cammini minimi, le destinazioni, il costo associato e l'hop successivo per raggiungere tali destinazioni formano la tabella di routing IP.

4. Se non si verificano cambiamenti nella rete OSPF, ad esempio modifiche al costo di un collegamento oppure aggiunta o rimozione di una rete, il protocollo OSPF rimane silente. Le modifiche invece vengono comunicate tramite i pacchetti link state; l'algoritmo Dijkstra ricalcola quindi il percorso più breve.

L'algoritmo posiziona ogni router alla radice di un albero e calcola il percorso più breve per ciascuna destinazione in base al costo cumulativo richiesto per raggiungerla.

Anche se tutti i router creano un albero dei cammini minimi che usa lo stesso database link state, ciascuno di essi ha una propria visione della topologia. In queste sezioni vengono illustrati i fattori che determinano la creazione di un albero dei cammini minimi.

Costo OSPF

Nel protocollo OSPF, il costo, o metrica, di un'interfaccia identifica il sovraccarico necessario per inviare i pacchetti attraverso una determinata interfaccia.

Il costo di un'interfaccia è inversamente proporzionale alla larghezza di banda dell'interfaccia. Maggiore è la larghezza di banda, minore è il costo.

Attraversare una linea seriale a 56k comporta un maggiore sovraccarico, e quindi un costo più alto, e maggiori ritardi rispetto a una linea Ethernet da 10M.

La formula utilizzata per calcolare il costo è:

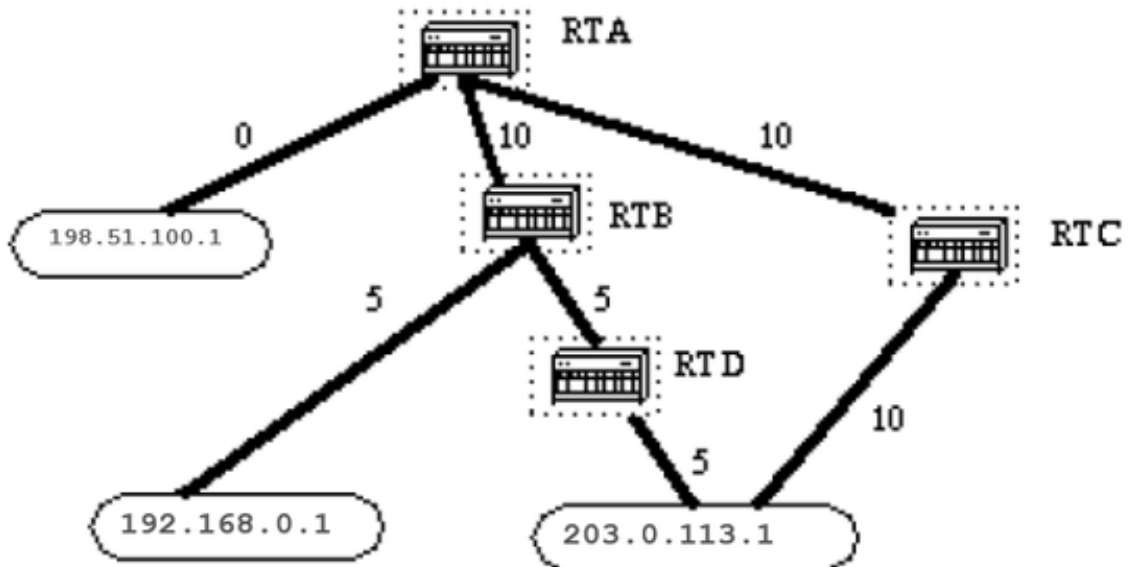
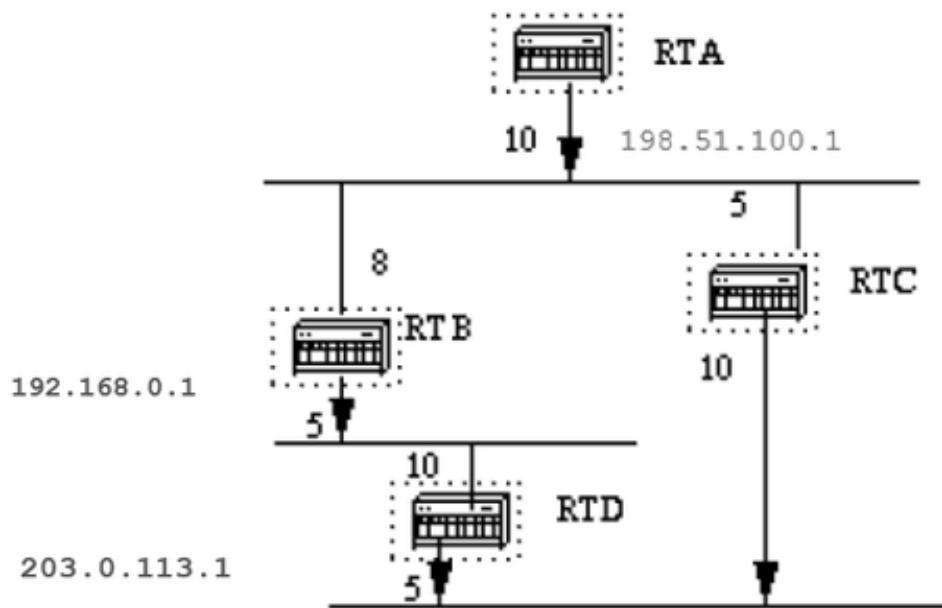
- $\text{costo} = 100000000 / \text{larghezza di banda in bps}$

Ad esempio, usare una linea Ethernet a 10M costa $10 \text{ EXP}8/10 \text{ EXP}7 = 10$; usare una linea T1 costa $10 \text{ EXP}8/1544000 = 64$.

ip ospf cost <value> Per impostazione predefinita, il costo di un'interfaccia viene calcolato in base alla larghezza di banda; è possibile forzare il costo di un'interfaccia con il comando `interface subconfiguration mode`.

Albero dei cammini minimi

Fare riferimento a questo diagramma di rete con i costi di interfaccia indicati. Per creare l'albero dei cammini minimi per RTA, dovremmo impostare RTA come radice della struttura ad albero e calcolare il costo minimo per ciascuna destinazione.



Ecco la topologia della rete dal punto di vista di RTA. Notare la direzione delle frecce nel calcolo del costo.

Il costo dell'interfaccia tra RTB e la rete 198.51.100.1 non è rilevante se il costo è calcolato per raggiungere la rete 192.168.0.1.

RTA può raggiungere la rete 192.168.0.1 tramite RTB con un costo pari a 15 (10+5).

Inoltre, RTA può raggiungere la rete 203.0.113.1 tramite RTC con un costo di 20 (10+10) oppure tramite RTB con un costo di 20 (10+5+5).

Nel caso esistano percorsi di uguale costo per la stessa destinazione, l'implementazione del protocollo OSPF tiene traccia di massimo sei (6) hop successivi per la stessa destinazione.

Dopo aver creato l'albero dei cammini minimi, il router crea la tabella di routing. Per le reti connesse direttamente, il costo, o metrica, è pari a 0; per le altre reti, il costo è calcolato in base alla struttura ad albero.

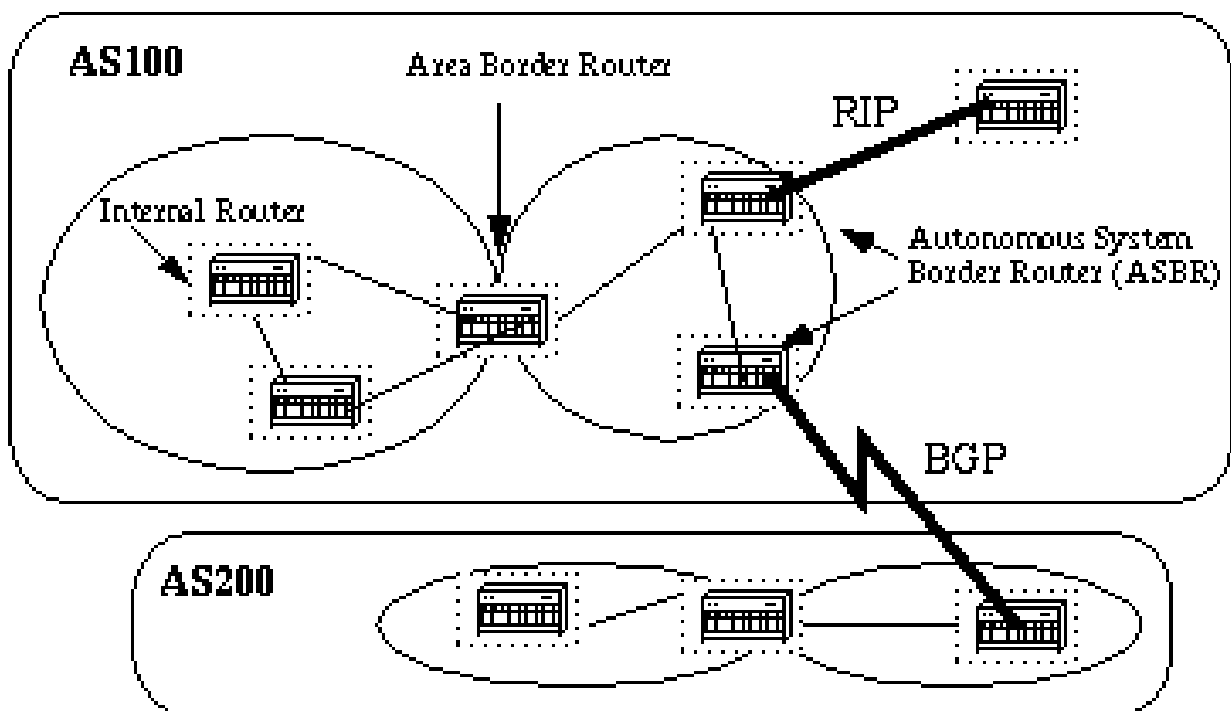
Area e router di confine

Come accennato in precedenza, OSPF utilizza il flooding per aggiornare i router sugli stati dei collegamenti. Qualsiasi modifica alle informazioni di routing viene trasmessa a tutti i router della rete.

Le aree sono introdotte per mettere un limite alla trasmissione di tali aggiornamenti. Il flooding e il calcolo dell'algoritmo Dijkstra su un router vengono quindi limitati alle modifiche verificatesi all'interno di un'area.

Tutti i router che appartengono alla stessa area usano lo stesso database link state. I router che appartengono a più aree e che connettono tali aree alla dorsale vengono chiamati router ABR (Area Border Router).

I router ABR devono pertanto conservare le informazioni che descrivono la dorsale e le altre aree connesse.



Area e interfaccia sono correlate. Un router le cui interfacce sono tutte all'interno della stessa area è detto router interno (IR, Internal Router).

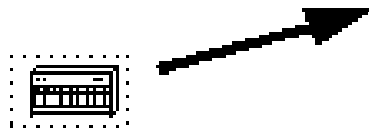
Un router le cui interfacce sono in più aree è detto router ABR (Area Border Router).

I router che fungono da gateway (ridistribuzione) tra OSPF e altri protocolli di routing (IGRP, EIGRP, IS-IS, RIP, BGP, Static) o altre istanze del processo di routing OSPF sono chiamati router ASBR (Autonomous System Boundary Router). Qualsiasi router può essere un router ABR o un router ASBR.

Pacchetti link state

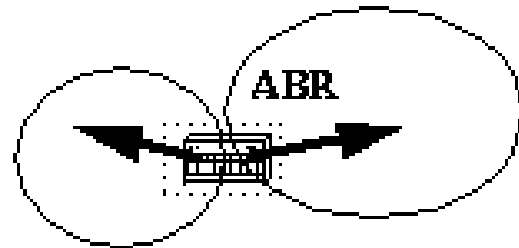
I pacchetti link state possono essere diversi, questi sono quelli normalmente usati in un database OSPF (Appendice A e illustrati qui).

Router Links



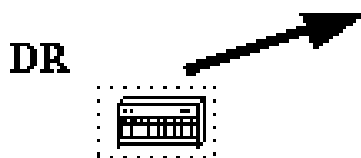
Describe the state and cost of the router's links (interfaces) to the area (Intra-area).

Summary Links



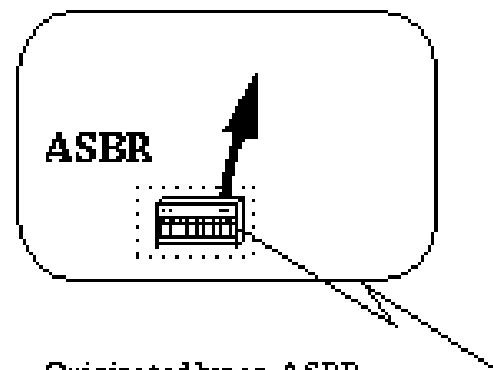
Originated by ABRs only. Describe networks in the AS but outside of an Area (Inter-area). Also describe the location of the ASBR.

Network Links



Originated for multi-access segments with more than one attached router. Describe all routers attached to the specific segment. Originated by a Designated Router (discussed later on).

External Links



Originated by an ASBR. Describe destinations external the autonomous system or a default route to the outside AS.

I collegamenti del router sono un'indicazione dello stato delle interfacce di un router in una determinata area designata. Ogni router genera un collegamento per tutte le sue interfacce.

I collegamenti di riepilogo sono generati dagli ABR; questo è il modo in cui vengono trasmesse a tutte le aree le informazioni sulla raggiungibilità della rete.

In genere, tutte le informazioni vengono trasmesse alla dorsale (area 0) e, dalla dorsale, alle altre aree.

Gli ABR trasmettono anche le informazioni sulla raggiungibilità dell'ASBR. In questo modo i router possono sapere come raggiungere le route esterne degli altri sistemi autonomi.

I collegamenti di rete sono generati da un router designato (DR, Designated Router) su un segmento (parleremo dei router DR più avanti).

Queste informazioni sono originate da tutti i router connessi a un particolare segmento con accessi multipli come Ethernet, **Token Ring** e FDDI (anche NBMA).

I collegamenti esterni sono originati dalle reti esterne al sistema autonomo. Queste reti vengono inserite nel protocollo OSPF tramite redistribuzione. Il router ASBR inserisce tali route in un sistema autonomo.

Abilitare il protocollo OSPF sul router

L'abilitazione del protocollo OSPF sul router comporta i due passaggi seguenti in modalità configurazione:

- Abilitare un processo OSPF con il **router ospf <process-id>** comando.
- Assegnazione dell'area alle interfacce con il **network <network or IP address> <mask> <area-id>** comando.

La variabile process-id dell'OSPF è un valore numerico specifico del router. Non deve corrispondere ai process-id degli altri router.

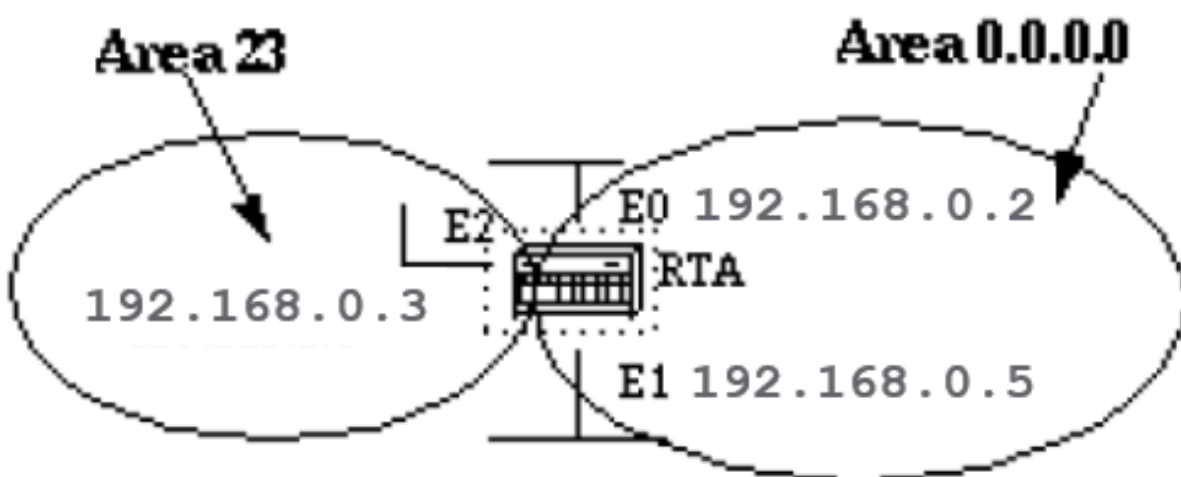
Anche se è possibile eseguire più processi OSPF sullo stesso router, non è consigliabile in quanto verrebbero create più istanze di database con conseguente sovraccarico.

Il **network** comando è un metodo di assegnazione di un'interfaccia a un'area specifica. La maschera viene utilizzata per inserire un elenco di interfacce nella stessa area con un'unica riga di configurazione.

La maschera contiene bit di caratteri jolly, dove 0 è una corrispondenza e 1 è un bit "do not care", ad esempio 0.0.255.255 indica una corrispondenza con i primi due byte del numero di rete.

La variabile **area-ID** è il numero dell'area in cui si desidera inserire l'interfaccia. La variabile **area-id** può essere un numero intero compreso tra 0 e 4294967295 o può assumere una forma simile a un indirizzo IP A.B.C.D.

Di seguito è riportato un esempio:



RTA# interface Ethernet0 ip address 192.168.0.2 255.255.255.0 interface Ethernet1 ip address 192.168.0.5 255.255.255.0 interface Ethernet2 ip address 192.168.0.8 255.255.255.0

La prima istruzione inserisce E0 ed E1 nella stessa area 0.0.0.0, la seconda istruzione inserisce E2 nell'area 23. Si noti la maschera 0.0.0.0, che indica una corrispondenza completa dell'indirizzo IP.

In caso sia difficile individuare la maschera, questo è un modo semplice per inserire un'interfaccia in una determinata area.

Autenticazione OSPF

È possibile autenticare i pacchetti OSPF in modo che i router possano partecipare ai domini di routing in base a password predefinite.

Per impostazione predefinita, un router utilizza un'autenticazione Null, ossia gli scambi di routing sulla rete non vengono autenticati. Esistono altri due metodi di autenticazione: autenticazione e **Message Digest** autenticazione con password semplici (MD-5).

Autenticazione con password semplice

L'autenticazione con password semplice consente di configurare una password (chiave) per ciascuna area. I router della stessa area che desiderano partecipare al dominio di routing devono essere configurati con la stessa chiave.

Lo svantaggio di questo metodo è che è vulnerabile agli attacchi passivi. Chiunque abbia un analizzatore di collegamenti potrebbe facilmente ottenere la password.

Per abilitare l'autenticazione con password, usare questi comandi:

- **ip ospf authentication-key key** (nell'interfaccia specifica)
- **area area-id authentication** (questo va sotto router ospf <process-id>)

Di seguito è riportato un esempio:

```
interface Ethernet0 ip address 10.0.0.1 255.255.255.0 ip ospf authentication-key mypassword router ospf 10 network 10.0.0.0 0.0.255.255 area 0 area 0 authentication-key mypassword
```

Autenticazione con digest del messaggio

L'autenticazione con digest del messaggio è un processo di autenticazione crittografica. Una chiave (password) e un ID chiave vengono configurati su ciascun router.

Il router utilizza un algoritmo basato sul pacchetto OSPF, sulla chiave e sull'ID chiave per generare un "digest del messaggio" che viene aggiunto al pacchetto.

A differenza dell'autenticazione con password semplice, la chiave non viene scambiata sulla rete cablata. In ogni pacchetto OSPF è incluso anche un numero di sequenza non decrescente per proteggersi dagli attacchi replay.

Questo metodo consente anche transizioni ininterrotte tra le chiavi. Ciò permette agli amministratori di modificare la password OSPF senza dover interrompere la comunicazione.

Se un'interfaccia è configurata con una nuova chiave, il router invia più copie dello stesso pacchetto, ciascuna autenticata con chiavi diverse.

Il router non invia pacchetti duplicati quando rileva che tutti i router vicini hanno adottato la nuova chiave.

Questi sono i comandi utilizzati nell'autenticazione con digest del messaggio:

- **ip ospf message-digest-key keyid md5 key** (utilizzato nell'interfaccia)
- **area area-id authentication message-digest** (utilizzato in router ospf <process-id>)

Di seguito è riportato un esempio:

```
interface Ethernet0 ip address 10.0.0.1 255.255.255.0 ip ospf message-digest-key 10 md5 mypassword router ospf 10 network 10.0.0.0 0.0.255.255 area 0
```

Dorsale o area 0

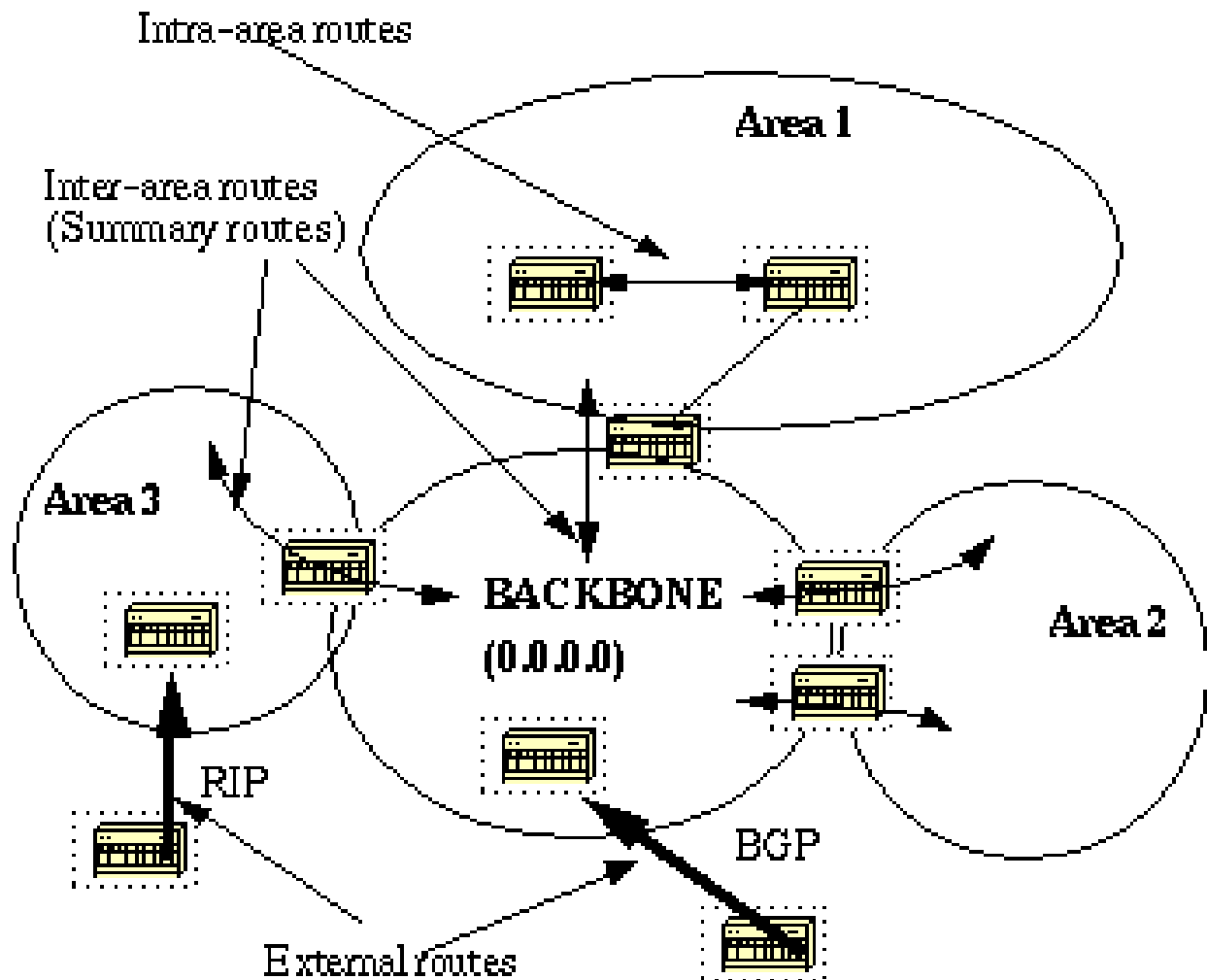
Negli scenari con più aree, alcune restrizioni limitano l'uso del protocollo OSPF. Se sono state configurate più aree, una di queste aree deve essere l'area 0, chiamata anche dorsale.

Nella progettazione delle reti, è buona prassi iniziare dall'area 0 per espanderla successivamente nelle altre aree.

La dorsale deve essere al centro di tutte le altre aree, ovvero tutte le aree devono essere fisicamente connesse alla dorsale.

Infatti, l'OSPF si aspetta che tutte le aree trasmettano informazioni di routing alla dorsale e che la dorsale, a sua volta, trasmetta tali informazioni alle altre aree.

In questo diagramma viene illustrato il flusso di informazioni in una rete OSPF:



In questo diagramma, tutte le aree sono connesse direttamente alla dorsale. Nelle rare situazioni in cui viene introdotta una nuova area che non ha un accesso fisico diretto alla dorsale, è necessario configurare un collegamento virtuale.

I collegamenti virtuali sono illustrati nella sezione successiva. Notare che le informazioni di routing possono essere di tipo diverso. Le route generate all'interno di un'area, ossia la cui destinazione appartenga alla stessa area, sono chiamate **route intra-area**.

Nella tabella di routing IP, tali route sono in genere contrassegnate dalla lettera **O**. Le route provenienti da altre aree vengono denominate **inter-area** o **Summary routes**.

Nella tabella di routing IP, queste route sono contrassegnate da **O IA**. Vengono chiamate le route che hanno origine da altri protocolli di routing (o processi OSPF diversi) e che vengono iniettate in OSPF tramite redistribuzione **external routes**.

Nella tabella di routing IP, queste route sono contrassegnate da **O E2** o **O E1**. Più route alla stessa destinazione sono preferite nell'ordine seguente: **intra-area, inter-area, external E1, external E2**. Le route esterne E1 ed E2 sono spiegate più avanti.

Collegamenti virtuali

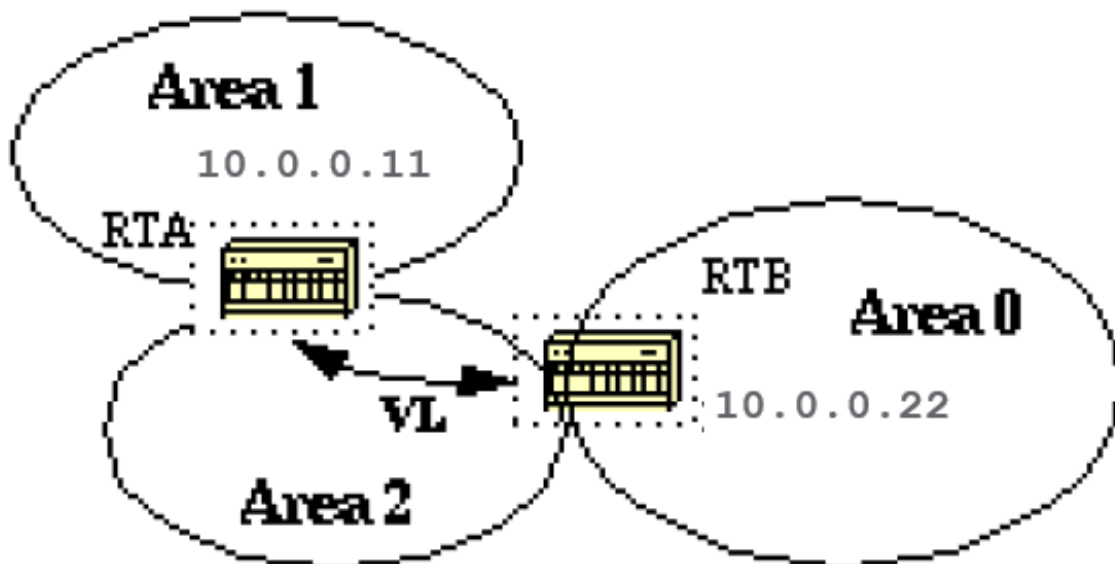
I collegamenti virtuali vengono utilizzati con due finalità:

- Per un'area che non ha una connessione fisica alla dorsale
- Per applicare le patch alla dorsale in caso di discontinuità dell'area 0.

Aree non connesse fisicamente all'area 0

Come accennato in precedenza, l'area 0 deve essere al centro di tutte le altre aree. In alcuni rari casi in cui è impossibile avere un'area fisicamente connessa alla dorsale, viene utilizzato un collegamento virtuale.

Il collegamento virtuale fornisce all'area disconnessa un percorso logico per raggiungere la dorsale. Il collegamento virtuale deve essere stabilito tra due ABR con un'area comune, con uno dei due router connesso alla dorsale,



In questo esempio, l'area 1 non ha una connessione fisica diretta con l'area 0. È necessario configurare un collegamento virtuale tra RTA e RTB. L'area 2 deve essere utilizzata come area di transito, RTB diventa il punto di ingresso nell'area 0.

In questo modo RTA e l'area 1 hanno una connessione logica alla dorsale. Per configurare un collegamento virtuale, utilizzare il sottocomando OSPF del **area <area-id> virtual-link <RID>** router sia su RTA che su RTB, dove area-id è l'area di transito.

Nel diagramma questa è l'area 2. RID è l'ID del router. L'ID del router OSPF è in genere l'indirizzo IP più alto presente sulla confezione ovvero l'indirizzo di loopback più alto, se presente.

L'ID del router viene calcolato solo al momento dell'avvio. Per trovare l'ID del router, usare il **show ip ospf interface** comando.

Supponendo che 10.0.0.11 e 10.0.0.22 siano i RID rispettivamente di RTA e RTB, la configurazione OSPF di entrambi i router sarebbe:

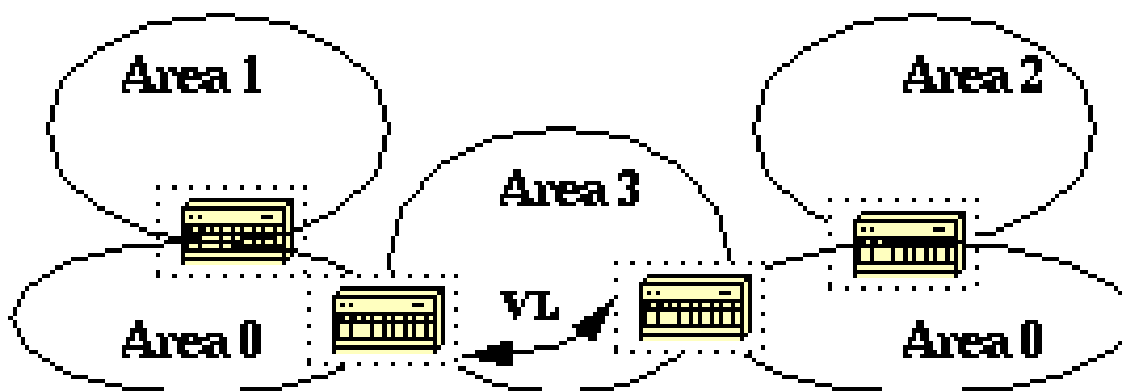
```
RTA# router ospf 10 area 2 virtual-link 10.0.0.22 RTB# router ospf 10 area 2 virtual-link 10.0.0.11
```

Dorsale

OSPF permette di collegare parti discontinue della dorsale utilizzando un collegamento virtuale. In alcuni casi, è necessario collegare tra loro diverse aree 0.

Ciò può verificarsi se, ad esempio, un'azienda desidera far convergere due reti OSPF distinte in un'unica rete con un'area 0 comune. In altri casi, i collegamenti virtuali vengono aggiunti per ridondanza nel caso in cui un errore del router causi la suddivisione della dorsale in due.

È possibile configurare un collegamento virtuale tra ABR separati che toccano l'area 0 su ciascun lato e che hanno un'area comune (illustrata qui).



In questo diagramma, due aree 0 sono collegate tra loro da un collegamento virtuale. Nel caso in cui non esista un'area comune, è possibile creare un'area aggiuntiva, ad esempio l'area 3, per trasformarla in area di transito.

Nel caso in cui un'area diversa dalla dorsale venga partizionata, la dorsale si occupa del partizionamento senza utilizzare alcun collegamento virtuale.

Una delle parti suddivise viene resa nota all'altra tramite route inter-area anziché tramite route intra-area.

Router vicini

I router che condividono un segmento comune diventano vicini su tale segmento. I router vicini vengono scelti tramite il protocollo **Hello**. I **pacchetti Hello** vengono inviati periodicamente da ogni interfaccia utilizzando l'IP multicast (Appendice B).

I router diventano vicini non appena si vedono elencati nel pacchetto Hello del router vicino. In questo modo è garantita una comunicazione bidirezionale. La negoziazione tra router vicini verte solo sull'indirizzo principale.

È possibile configurare indirizzi secondari su un'interfaccia, a condizione che appartengano alla stessa area dell'indirizzo principale.

Due router diventano vicini solo se soddisfano questo criterio.

- **Area-id:** Due router con un segmento comune; le loro interfacce devono appartenere alla stessa area su quel segmento. Le interfacce devono appartenere alla stessa subnet e avere una maschera simile.
- **Authentication:** Il protocollo OSPF consente di configurare una password per un'area specifica. I router che vogliono diventare vicini devono scambiarsi la stessa password su uno specifico segmento.
- **Hello and Dead Intervals:** Il protocollo OSPF scambia **Hello** pacchetti su ciascun segmento. Questa è una forma di keepalive utilizzata dai router per confermare la propria esistenza su un segmento e per scegliere un router designato (DR) sui segmenti con accessi multipli.

L' **Hello** intervallo specifica l'intervallo di tempo, in secondi, tra i **Hello** pacchetti inviati da un router su un'interfaccia OSPF.

L'intervallo di inattività è il numero di secondi che un **Hello** pacchetto di router non è stato rilevato prima che i relativi vicini dichiarino inattivo il router OSPF.

- OSPF richiede che tali intervalli siano esattamente gli stessi nei due router vicini. In caso di differenze, i router non saranno vicini su quel segmento. I comandi dell'interfaccia del router usati per impostare questi timer sono: **ip ospf hello-interval seconds** e **ip ospf dead-interval seconds**.
- **Stub area flag:** Due router devono anche accordarsi sull'indicatore dell'area dello stub nei **Hello** pacchetti per diventare vicini. Le aree stub sono discusse in una sezione successiva. Tenere presente che la definizione delle aree stub influisce sul processo di scelta dei router vicini.

Adiacenze

Dopo essere diventati router vicini, il passo successivo è diventare adiacenti. I router adiacenti sono router che vanno oltre il semplice **Hello** scambio e procedono al processo di scambio del database.

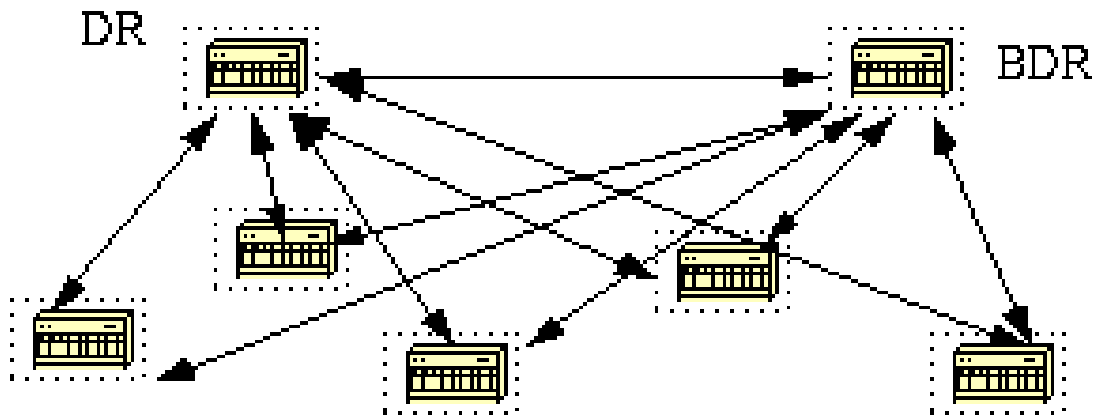
Al fine di ridurre al minimo la quantità di informazioni scambiate su un determinato segmento, OSPF sceglie un router designato (DR, Designated Router) e un router designato di backup (BDR, Backup Designated Router) su ogni segmento con accessi multipli.

Il BDR viene scelto come meccanismo di backup in caso il router designato diventasse inattivo. La logica di questo meccanismo è che i router abbiano un punto di contatto centrale per lo scambio delle informazioni.

Invece di scambiarsi gli aggiornamenti con gli altri router del segmento, ogni router scambia informazioni con il DR e il BDR.

Il DR e il BDR inoltrano le informazioni a tutti gli altri router. In termini matematici, questo riduce lo scambio di informazioni da $O(n*n)$ a $O(n)$ dove n è il numero di router su un segmento con accessi multipli.

In questo diagramma è raffigurato un modello di router con DR e BDR:



In questo diagramma, tutti i router condividono un segmento comune con accessi multipli. A causa dello scambio di **Hello** pacchetti, un router viene scelto per il DR e un altro per il BDR.

Ogni router sul segmento (che è già un router vicino) prova a stabilire una adiacenza con il DR e con il BDR.

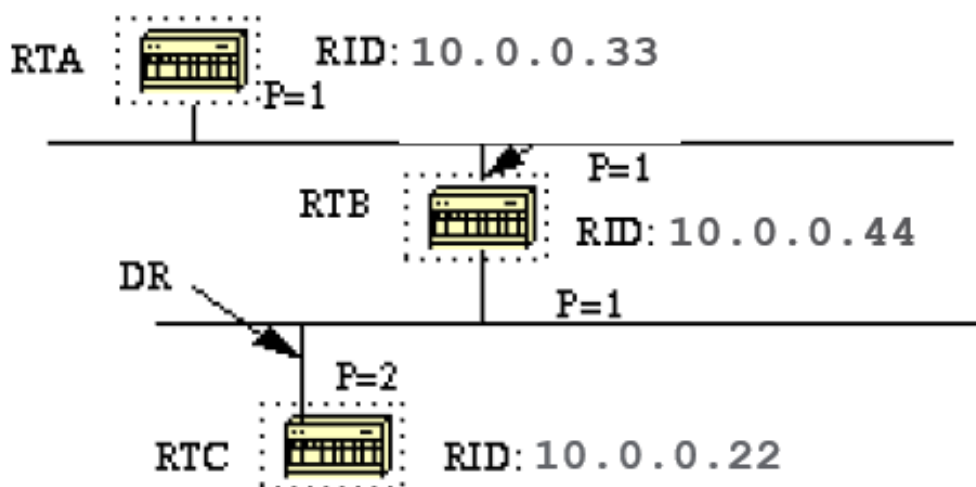
Scelta del router designato (DR)

La scelta di DR e BDR viene effettuata tramite il **Hello** protocollo. I **Hello** pacchetti vengono scambiati tramite pacchetti IP multicast (Appendice B) su ciascun segmento.

Il router con la massima priorità OSPF su un segmento diventa il DR di quel segmento. Lo stesso processo viene ripetuto per il BDR. In caso di parità, viene scelto il router con il RID più alto.

L'impostazione predefinita per la priorità dell'interfaccia OSPF è 1. Tenere presente che i concetti di DR e BDR si riferiscono a segmenti con accessi multipli. Il valore di priorità OSPF su un'interfaccia viene specificato con il comando `ip ospf priority <value>` interface.

Un valore di priorità pari a zero indica un'interfaccia che non deve essere scelta come DR o BDR. Lo stato dell'interfaccia con priorità zero è **DROTHER**. Di seguito è illustrato il processo di scelta del router DR:



In questo diagramma, RTA e RTB hanno un'interfaccia con medesima priorità, ma RTB ha un RID più alto, quindi RTB diventa il router DR su quel segmento. RTC ha una priorità superiore rispetto a RTB, quindi su quel segmento RTC diventa il router DR.

Creare l'adiacenza

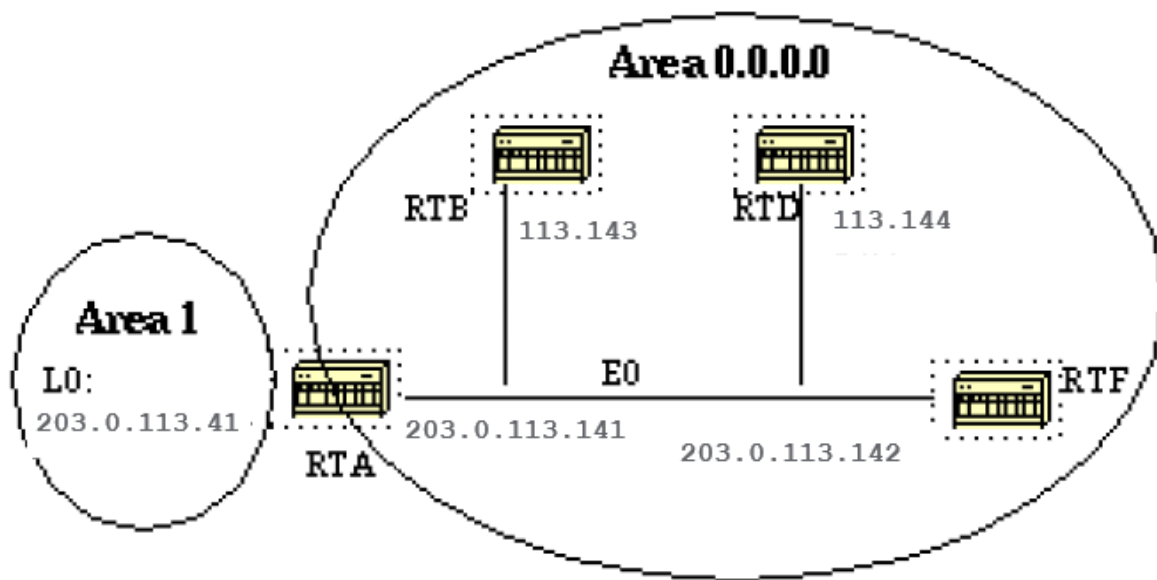
Il processo di creazione dell'adiacenza è composto da diverse fasi. I router che sono diventati adiacenti hanno lo stesso database link state.

Di seguito è riportato un riepilogo degli stati che un'interfaccia attraversa prima di diventare adiacente a un altro router:

- **Non attiva:** nessuna informazione ricevuta da nessun router sul segmento.
- **Tentativo:** sui cloud NBMA (Non Broadcast Multi Access) come **Frame Relay** e X.25, questo stato indica che non sono state ricevute informazioni recenti dal router vicino. Per contattare il router vicino, inviare pacchetti **Hello** alla velocità Poll Interval ridotta.
- **Inizializzazione:** l'interfaccia ha rilevato un pacchetto **Hello** proveniente da un router vicino, ma la comunicazione bidirezionale non è stata ancora stabilita.
- **Bidirezionale:** è in corso una comunicazione bidirezionale con un router vicino. Il router si è visto nei pacchetti **Hello** provenienti da un router vicino. Al termine di questa fase, vengono scelti i router DR e BDR. Al termine della fase Bidirezionale, i router decidono se procedere alla creazione di un'adiacenza. La decisione si basa sul fatto che uno dei router sia un DR o BDR o che il collegamento sia un collegamento point-to-point o virtuale.
- **Exstart:** i router cercano di stabilire il numero di sequenza iniziale da utilizzare nei pacchetti di scambio delle informazioni. Il numero di sequenza assicura che i router ottengano sempre le informazioni più aggiornate. Un router diventa il router principale e l'altro il router secondario. Il router principale esegue il polling del router secondario in cerca di informazioni.
- **Scambio:** i router descrivono l'intero database link state attraverso l'invio di pacchetti di descrizione del database. In questo stato, i pacchetti potrebbero essere trasmessi alle altre interfacce sul router in modalità flooding.

- **Caricamento:** in questo stato, i router finalizzano lo scambio delle informazioni. Sono già stati creati un elenco di richieste e un elenco di ritrasmissione degli stati dei collegamenti. Tutte le informazioni che sembrano incomplete o obsolete vengono inserite nell'elenco di richieste. Gli aggiornamenti vengono inseriti nell'elenco di ritrasmissione finché non vengono confermati.
- **Completa:** in questo stato, l'adiacenza è completa. I router vicini sono completamente adiacenti. I router adiacenti hanno un database link state simile.

Di seguito è riportato un esempio:



RTA, RTB, RTD e RTF condividono un segmento comune (E0) nell'area 0.0.0.0. Queste sono le configurazioni di RTA e RTF. RTB e RTD devono avere una configurazione simile a RTF e non sono inclusi.

```
RTA# hostname RTA interface Loopback0 ip address 203.0.113.41 255.255.255.0 interface Ethernet0 ip address 203.0.113.141 255.255.255.0 router ospf
```

È un semplice esempio che mostra un paio di comandi molto utili per il debug delle reti OSPF.

- **show ip ospf interface <interface>**

Questo comando permette di stabilire rapidamente se tutte le interfacce appartengono alle aree in cui dovrebbero trovarsi. La sequenza con cui sono elencati i comandi di rete OSPF è molto importante.

Nella configurazione di RTA, se l'istruzione "network 203.0.113.100 0.0.255.255 area 0.0.0.0" è stata inserita prima dell'istruzione "network 203.0.113.41 0.0.0.0 area 1", tutte le interfacce si troverebbero nell'area 0, il che è errato perché il loopback si trova nell'area 1.

Questo è l'output del comando su RTA, RTF, RTB e RTD:

```
<#root>
```

```
RTA#
```

```
show ip ospf interface e0
```

```
Ethernet0 is up, line protocol is up Internet Address 203.0.113.141 255.255.255.0,
```

```
Area 0.0.0.0 Process ID 10, Router ID 203.0.113.41, Network Type BROADCAST
```

```
, Cost: 10 Transmit Delay is 1 sec,
```

```
State BDR, Priority 1 Designated Router (ID) 203.0.113.151
```

```
, Interface address 203.0.113.142
```

```
Backup Designated router (ID) 203.0.113.41
```

```
, Interface address 203.0.113.141 Timer intervals configured,
```

```
Hello 10, Dead 40
```

```
, Wait 40, Retransmit 5 Hello due in 0:00:02
```

```
Neighbor Count is 3, Adjacent neighbor count is 3
```

```
Adjacent with neighbor 203.0.113.151 (Designated Router) Loopback0 is up, line protocol is up Internet
```

```
show ip ospf interface e0
```

```
Ethernet0 is up, line protocol is up Internet Address 203.0.113.142 255.255.255.0,
```

```
Area 0.0.0.0 Process ID 10, Router ID 203.0.113.151, Network Type BROADCAST
```

```
, Cost: 10 Transmit Delay is 1 sec,
```

```
State DR, Priority 1
```

```
Designated Router (ID) 203.0.113.151
```

```
, Interface address 203.0.113.142
```

```
Backup Designated router (ID) 203.0.113.41
```

```
, Interface address 203.0.113.141 Timer intervals configured,
```

```
Hello 10, Dead 40
```

```
, Wait 40, Retransmit 5 Hello due in 0:00:08
```

```
Neighbor Count is 3, Adjacent neighbor count is 3
```

```
Adjacent with neighbor 203.0.113.41 (Backup Designated Router) RTD#
```

```
show ip ospf interface e0
```

```
Ethernet0 is up, line protocol is up Internet Address 203.0.113.144 255.255.255.0,
```

```
Area 0.0.0.0 Process ID 10, Router ID 192.0.2.174, Network Type BROADCAST
```

```

, Cost: 10 Transmit Delay is 1 sec,
State DROTHER
, Priority 1
Designated Router (ID) 203.0.113.151
, Interface address 203.0.113.142
Backup Designated router (ID) 203.0.113.41
, Interface address 203.0.113.141 Timer intervals configured,
Hello 10, Dead 40
, Wait 40, Retransmit 5 Hello due in 0:00:03
Neighbor Count is 3, Adjacent neighbor count is 2
Adjacent with neighbor 203.0.113.151 (Designated Router) Adjacent with neighbor 203.0.113.41 (Backup D
show ip ospf interface e0
Ethernet0 is up, line protocol is up Internet Address 203.0.113.143 255.255.255.0,
Area 0.0.0.0 Process ID 10, Router ID 203.0.113.121, Network Type BROADCAST
, Cost: 10 Transmit Delay is 1 sec,
State DROTHER
, Priority 1
Designated Router (ID) 203.0.113.151
, Interface address 203.0.113.142
Backup Designated router (ID) 203.0.113.41
, Interface address 203.0.113.141 Timer intervals configured,
Hello 10, Dead 40
, Wait 40, Retransmit 5 Hello due in 0:00:03
Neighbor Count is 3, Adjacent neighbor count is 2
Adjacent with neighbor 203.0.113.151 (Designated Router) Adjacent with neighbor 203.0.113.41 (Backup D

```

Questo output mostra informazioni molto importanti. Per l'output su RTA, Ethernet0 si trova nell'area 0.0.0.0. L'ID processo è 10 (router ospf 10) e l'ID router è 203.0.113.41.

Tenere presente che il RID è l'indirizzo IP più alto presente sulla confezione o nell'interfaccia di loopback, calcolato all'avvio o ogni volta che il processo OSPF viene riavviato.

Lo stato dell'interfaccia è BDR. Poiché tutti i router hanno la stessa priorità OSPF su Ethernet 0 (valore predefinito pari a 1), l'interfaccia di RTF è stata scelta come DR perché ha il RID più alto.

Allo stesso modo, RTA è stato scelto come router BDR. RTD e RTB non sono né DR né BDR e il loro stato è DROTHER.

Notare il numero di router vicini e il numero di router adiacenti. RTD ha tre router vicini ed è adiacente a due di essi, il DR e il BDR. RTF ha tre router vicini ed è adiacente a tutti perché è il router designato (DR).

Le informazioni sul tipo di rete sono importanti e determinano lo stato dell'interfaccia. Sulle reti broadcast come Ethernet, la scelta dei router DR e BDR è irrilevante

per l'utente finale. In altri scenari, ad esempio nelle reti NBMA come Frame Relay e X.25, la scelta è invece molto importante affinché OSPF funzioni correttamente.

Con l'introduzione delle sottointerfacce point-to-point e point-to-multipoint, la scelta del DR non è più un problema. Il funzionamento del protocollo OSPF su NBMA viene illustrato nella sezione successiva.

Un altro comando da considerare è:

- **show ip ospf neighbor**

Esaminiamo l'output di RTD:

```
<#root>
```

```
RTD#
```

```
show ip ospf neighbor
```

```
Neighbor ID Pri State Dead Time Address Interface 203.0.113.121 1 2WAY/DROTHER 0:00:37 203.0.113.143 E
```

Il **show ip ospf neighbor** comando mostra lo stato di tutti i vicini su un particolare segmento. Non preoccuparsi se l'**ID del router vicino** non appartiene al segmento che si sta visualizzando.

Nel nostro caso 203.0.113.121 e 203.0.113.151 non sono su Ethernet0. L'**ID del router vicino** è in effetti il RID di qualsiasi indirizzo IP sulla confezione.

RTD e RTB sono solo vicini, ecco perché lo stato è 2WAY/DROTHER. RTD è adiacente a RTA e RTF e il suo stato è FULL/DR e FULL/BDR.

Adiacenze sulle interfacce point-to-point

OSPF forma sempre un'adiacenza con il router vicino sull'altro lato di un'interfaccia point-to-point come nelle linee seriali point-to-point. I router DR o BDR non sono previsti e lo stato delle interfacce seriali è point-to-point.

Adiacenze sulle reti NBMA (Non-Broadcast Multi-Access)

Prestare particolare attenzione nella configurazione di OSPF sulle reti NBMA come Frame Relay, X.25, ATM. Il protocollo considera tali reti come un qualsiasi altro supporto di trasmissione come Ethernet.

I cloud NBMA sono generalmente integrati in una topologia a stella. I PVC o gli SVC sono organizzati in una topologia parzialmente magliata e la topologia fisica non fornisce gli accessi multipli che il protocollo OSPF è in grado di rilevare.

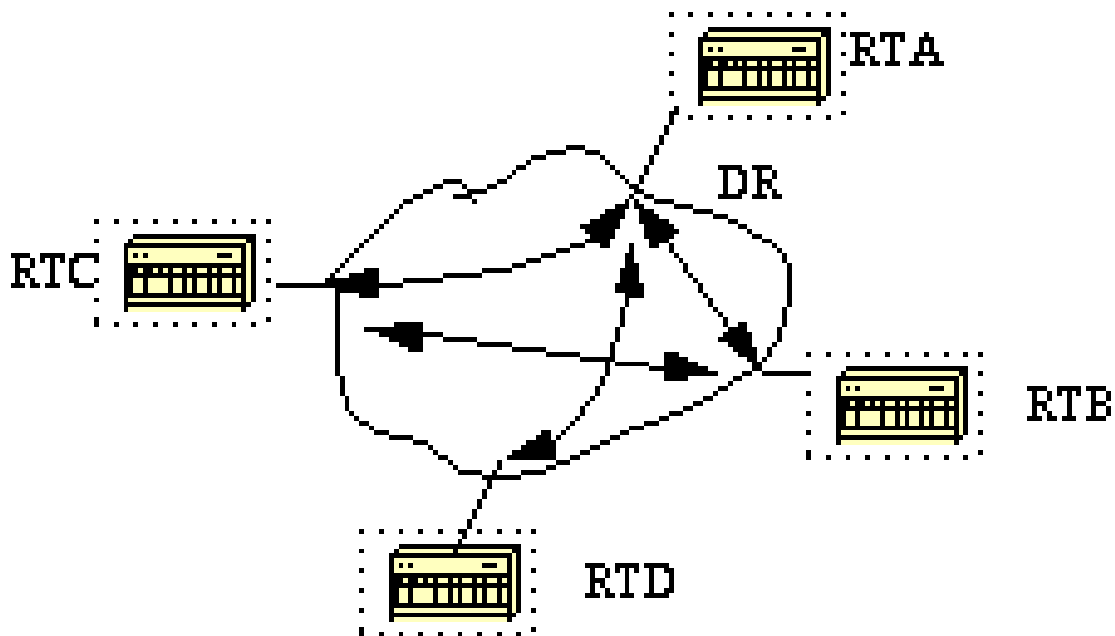
La scelta del DR è un'operazione importante perché il DR e il BDR devono avere una connettività fisica completa con tutti i router esistenti sul cloud.

A causa della mancanza di funzionalità di trasmissione, il DR e il BDR devono disporre di un elenco statico di tutti gli altri router collegati al cloud.

A tale scopo, il **neighbor ip-address [priority number] [poll-interval seconds]** comando, dove "ip-address" e "priority" sono l'indirizzo IP e la priorità OSPF assegnata al router adiacente.

Un router vicino con priorità 0 non può diventare router DR. L'intervallo di polling (poll-interval) è il tempo durante cui l'interfaccia NBMA rimane in attesa prima del polling (un pacchetto **Hello** inviato) a un router vicino che si presume inattivo.

Il **neighbor** comando si applica ai router con potenziale DR o BDR (priorità dell'interfaccia diversa da 0). Questo diagramma mostra una rete in cui il processo di scelta del DR è molto importante:



In questo diagramma, è essenziale che l'interfaccia tra RTA e il cloud sia scelta come DR, in quanto RTA è l'unico router che ha una connettività completa con tutti gli altri router.

La scelta del DR potrebbe essere influenzata dal parametro della priorità OSPF sulle interfacce. I router che non devono diventare DR o BDR hanno una priorità pari a 0, gli altri router potrebbero avere una priorità inferiore.

Il **neighbor** comando non viene descritto in dettaglio in questo documento e diventa obsoleto tramite la nuova interfaccia Tipo di rete, a prescindere dal supporto fisico sottostante. L'argomento è trattato nella sezione successiva.

Evitare di creare router DR e configurare router vicini sulle reti NBMA

Per evitare le complicazioni della configurazione di router vicini di tipo statico e router specifici che diventano DR o BDR sul cloud non broadcast, è possibile usare metodi diversi.

Il metodo da utilizzare dipende dal progetto di rete a cui si sta lavorando, ossia se si sta creando una nuova rete o modificando una rete esistente.

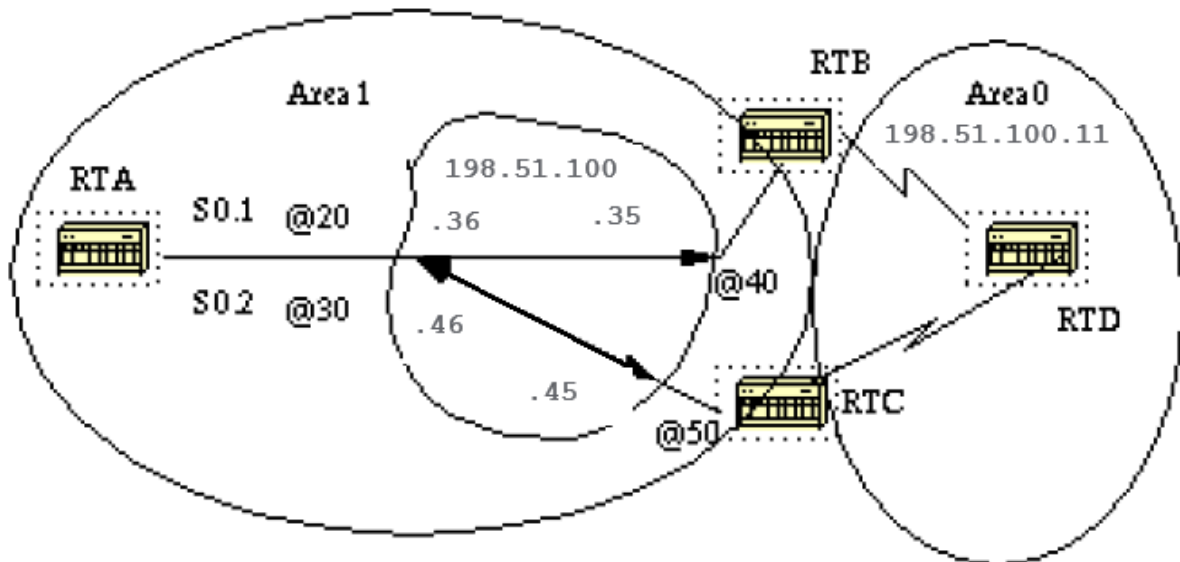
Sottointerfacce point-to-point

Una sottointerfaccia è un modo logico per definire un'interfaccia. La stessa interfaccia fisica può essere suddivisa in più interfacce logiche, con ogni sottointerfaccia definita come point-to-point.

L'obiettivo di questa progettazione è migliorare la gestione dei problemi causati dallo split horizon su NBMA e dai protocolli di routing basati sul vettore.

Una sottointerfaccia point-to-point ha le proprietà di qualsiasi interfaccia point-to-point fisica. Per quanto riguarda il protocollo OSPF, si forma sempre una adiacenza su una sottointerfaccia point-to-point senza scelta di DR o BDR.

Questo diagramma raffigura le sottointerfacce point-to-point:



In questo diagramma, su RTA, possiamo dividere Serial 0 in due sottointerfacce point-to-point, S0.1 e S0.2. In questo modo, OSPF considera il cloud come una serie di collegamenti point-to-point anziché una rete con accessi multipli.

L'unico svantaggio del point-to-point è che ogni segmento appartiene a una subnet diversa. Questa è una condizione inaccettabile, perché alcuni amministratori hanno già assegnato una subnet IP all'intero cloud.

Un'altra soluzione consiste nell'utilizzare interfacce IP non numerate sul cloud. Tuttavia, anche questa soluzione non è soddisfacente, ad esempio se la WAN viene gestita in base agli indirizzi IP delle linee seriali. Questa è una configurazione tipica per RTA e RTB:

```
RTA# interface Serial 0 no ip address encapsulation frame-relay interface Serial0.1 point-to-point ip address 198.51.100.36 255.255.252.0 frame-relay int
```

Selezionare i tipi di rete dell'interfaccia

Il comando utilizzato per impostare il tipo di rete di un'interfaccia OSPF è:

```
<#root>
```

```
ip ospf network {broadcast | non-broadcast | point-to-multipoint}
```

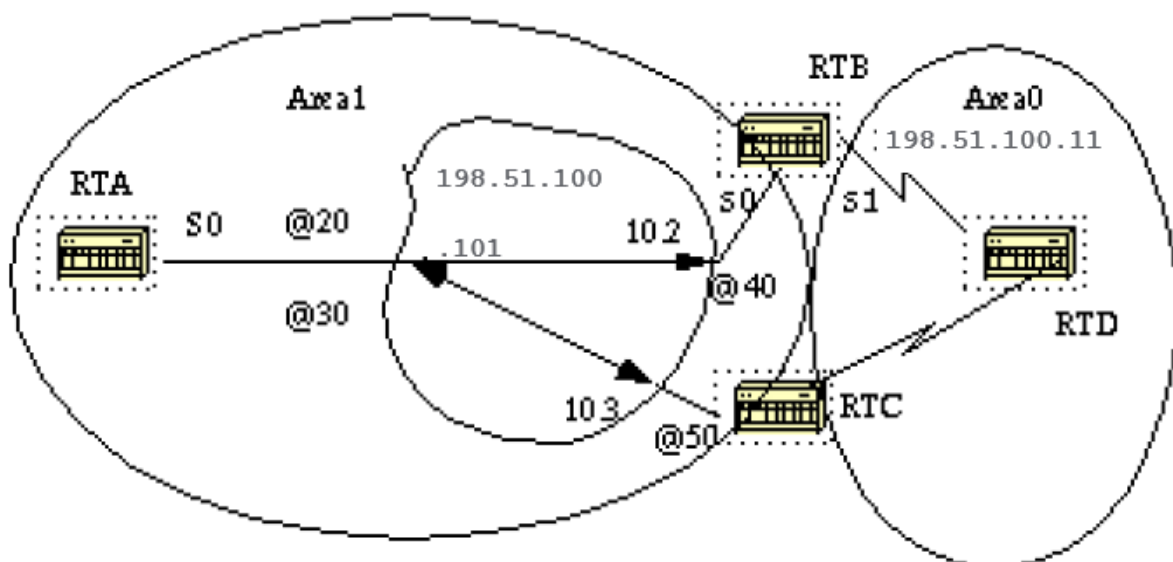
Interfacce point-to-multipoint

Un'interfaccia point-to-multipoint OSPF è un'interfaccia point-to-point numerata con uno o più router vicini e rappresenta un miglioramento dell'interfaccia point-to-point già illustrata.

Non occorre preoccuparsi di avere più subnet per ciascun collegamento point-to-point, in quanto il cloud è configurato come un'unica subnet.

Ciò si adatta bene in caso di migrazione verso un modello point-to-point senza cambiare l'indirizzo IP sul cloud. Inoltre, si possono ignorare i DR e le istruzioni dei router adiacenti.

Il protocollo OSPF point-to-multipoint funziona attraverso lo scambio di ulteriori aggiornamenti link state con una serie di informazioni sulla connettività ai router vicini.



```
RTA# interface Loopback0 ip address 203.0.113.101 255.255.255.0 interface Serial0 ip address 198.51.100.101 255.255.255.0 encapsulation frame-relay i
```


Tenere presente che non sono state configurate istruzioni di mappatura statica del frame relay, in quanto è l'ARP inverso a occuparsi della mappatura tra DLCI e indirizzi IP. Esaminiamo alcuni aspetti **show ip ospf interface** e **show ip ospf route** risultati:

```
<#root>
```

```
RTA#
```

```
show ip ospf interface s0
```

```
Serial0 is up, line protocol is up Internet Address 198.51.100.101 255.255.255.0, Area 0 Process ID 10
```

```
show ip ospf neighbor
```

```
Neighbor ID Pri State Dead Time Address Interface 198.51.100.103 1 FULL/ - 0:01:35 198.51.100.103 Serial0
```

```
show ip ospf interface s0
```

```
Serial0 is up, line protocol is up Internet Address 198.51.100.102 255.255.255.0, Area 0 Process ID 10
```

```
show ip ospf neighbor
```

```
Neighbor ID Pri State Dead Time Address Interface 203.0.113.101 1 FULL/ - 0:01:52 198.51.100.101 Serial0
```

L'unico svantaggio del modello point-to-multipoint è che genera route Host multiple (route con maschera 255.255.255.255) per tutti i router vicini. Prendere nota delle route Host nella tabella di routing IP per RTB:

```
<#root>
```

```
RTB#
```

```
show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external
```

```
198.51.100.103 255.255.255.255
```

```
[110/128] via 198.51.100.101, 00:00:00, Serial0 O
```

```
198.51.100.101 255.255.255.255
```

```
[110/64] via 198.51.100.101, 00:00:00, Serial0 C 198.51.100.100 255.255.255.0 is directly connected, S
```

```
show ip route
```

```
203.0.113.210 255.255.255.255 is subnetted, 1 subnets O 203.0.113.101 [110/65] via 198.51.100.101, Serial0
```

```
O 198.51.100.102 255.255.255.255 [110/128] via 198.51.100.101, Serial1 O 198.51.100.101 255.255.255.255 [
```

```
C 198.51.100.100 255.255.255.0 is directly connected, Serial1 172.16.0.0 255.255.255.0 is subnetted, 1
```

```
O 172.16.0.1 [110/192] via 198.51.100.101, 00:14:29, Serial1
```

Si noti che nella tabella di routing IP di RTC, la rete 172.16.0.1 è raggiungibile tramite l'hop successivo 198.51.100.101 e non tramite 198.51.100.102, come accadrebbe normalmente nei cloud Frame Relay che condividono la stessa subnet.

Questo è un vantaggio della configurazione point-to-multipoint perché non è necessaria la mappatura statica su RTC per raggiungere l'hop successivo 198.51.100.102.

Interfacce di trasmissione

Questo approccio rappresenta una soluzione alternativa per il **neighbor** comando che elenca in modo statico tutti i vicini correnti. L'interfaccia viene impostata in modo logico per la trasmissione e si comporta come se il router fosse connesso a una LAN.

La scelta dei router DR e BDR viene eseguita comunque, pertanto garantire una topologia a maglia completa o una selezione statica del DR in base alla priorità dell'interfaccia. Il comando che permette di impostare l'interfaccia di trasmissione è:

```
<#root>
```

```
ip ospf network broadcast
```

OSPF e riepilogo delle route

Il riepilogo è il consolidamento di più route in un unico annuncio. Ciò avviene normalmente ai confini dei router **ABR (Area Border Router)**.

Sebbene il riepilogo sia configurato tra due aree qualsiasi, è meglio eseguire il riepilogo nella direzione della dorsale. In questo modo la dorsale riceve tutti gli indirizzi aggregati e a sua volta li inserisce, già riepilogati, in altre aree.

Esistono due tipi di riepilogo:

- Riepilogo delle route inter-area
- Riepilogo delle route esterne

Riepilogo delle route inter-area

Il riepilogo delle route inter-area viene eseguito sugli ABR e si applica alle route all'interno del sistema autonomo. Non si applica alle route esterne immesse nel protocollo OSPF tramite redistribuzione.

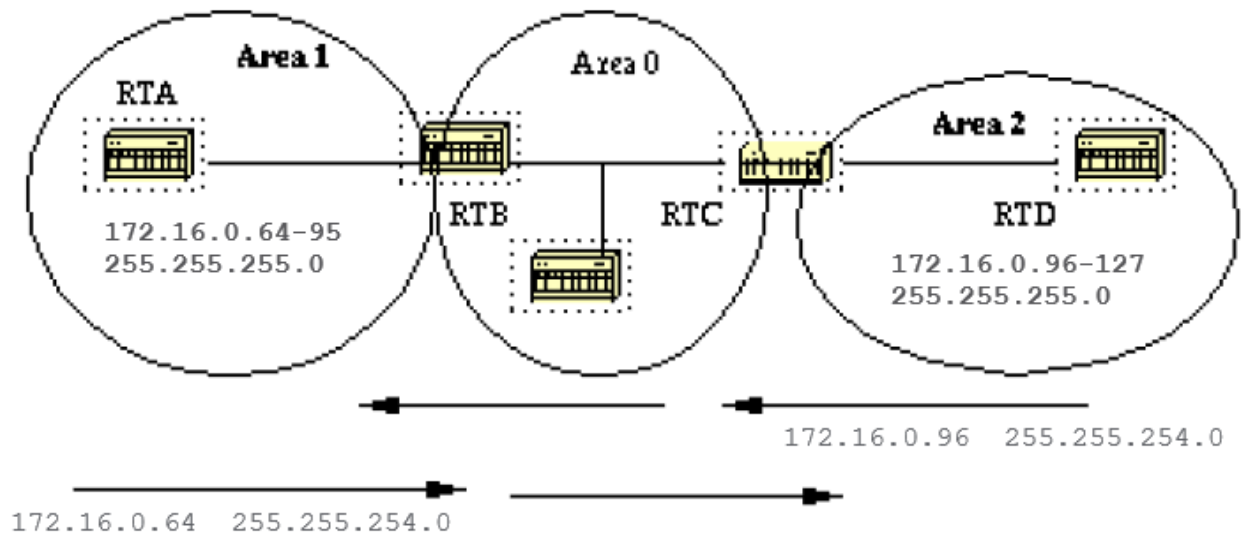
Per sfruttare il vantaggio del riepilogo, i numeri di rete nelle aree devono essere assegnati in modo contiguo in modo che questi indirizzi siano raggruppati in un intervallo.

Per specificare un intervallo di indirizzi, effettuare questa attività in modalità di configurazione del router:

```
<#root>
```

```
area area-id range address mask
```

Dove **area-id** è l'area contenente le reti da riepilogare. "address" e "mask" specificano l'intervallo degli indirizzi che devono essere inclusi in un intervallo. Questo è un esempio di riepilogo:



In questo diagramma, RTB riassume l'intervallo di subnet da 172.16.0.64 a 172.16.0.95 in un solo intervallo: 172.16.0.64 255.255.224.0. Per ottenere questo risultato, mascherare i primi tre bit più a sinistra di 64 con la maschera 255.255.224.0.

Analogamente, RTC genera l'indirizzo di riepilogo 172.16.0.96.255.255.224.0 nella dorsale. Notare che il riepilogo ha esito positivo perché i due intervalli di subnet sono distinti, 64-95 e 96-127.

Il riepilogo è più difficile se le subnet tra l'area 1 e l'area 2 sono sovrapposte. Gli intervalli di riepilogo che si sovrappongono verrebbero ricevuti sulla dorsale e i router al centro non saprebbero dove inviare il traffico in base all'indirizzo di riepilogo.

Questa è la configurazione relativa di RTB:

```
RTB# router ospf 100 area 1 range 172.16.0.64 255.255.224.0
```

Prima di Cisco IOS® Software Release 12.1(6), si consigliava di configurare manualmente, sull'ABR, una route statica di eliminazione per l'indirizzo di riepilogo per evitare possibili loop di routing. Per la route di riepilogo mostrata, utilizzare questo comando:


```
<#root>
```

```
ip route 172.16.0.64 255.255.224.0 null0
```

In Cisco IOS® 12.1(6) e versioni successive, la route di eliminazione viene generata automaticamente per impostazione predefinita. Per eliminare la route, configurare i comandi in **router ospf**:

- Entrambi **[no] discard-route internal**
- O **[no] discard-route external**

Nota sul calcolo della metrica dell'indirizzo di riepilogo: in base alla RFC 1583, la metrica delle route di riepilogo viene calcolata in base alla metrica minima dei percorsi disponibili.

[La RFC 2178 \(ora sostituita dalla RFC 2328\) ha modificato il metodo specificato per il calcolo delle metriche delle route di riepilogo: ora è il percorso con il costo massimo \(o più elevato\) a determinare il costo del riepilogo.](#) 

Nelle versioni Cisco IOS® precedenti alla 12.0, lo standard implementato era RFC 1583. A partire da Cisco IOS® 12.0, Cisco ha modificato il comportamento del protocollo OSPF per renderlo conforme alla nuova RFC 2328.

Il routing potrebbe quindi non essere ottimale, ad esempio se tutti gli ABR di un'area non sono stati aggiornati contemporaneamente con il nuovo codice.

Per risolvere questo potenziale problema, è stato aggiunto un comando alla configurazione OSPF di Cisco IOS® che permette di disabilitare in modo selettivo la compatibilità con la RFC 2328.

Il comando new configuration si trova in **router ospf** e ha la sintassi seguente:

<#root>

[no] compatible rfc1583

Il parametro predefinito è compatibile con la RFC 1583. Questo comando è disponibile in queste versioni di Cisco IOS®:

- 12.1(03)DC
- 12.1(03)DB
- 12.001(001.003) - 12.1 Mainline
- 12.1(01.03)T - 12.1 T-Train
- 12.000(010.004) - 12.0 Mainline

- 12.1(01.03)E - 12.1 E-Train
- 12.1(01.03)EC
- 12.0(10.05)W05(18.00.10)
- 12.0(10.05)SC

Riepilogo delle route esterne

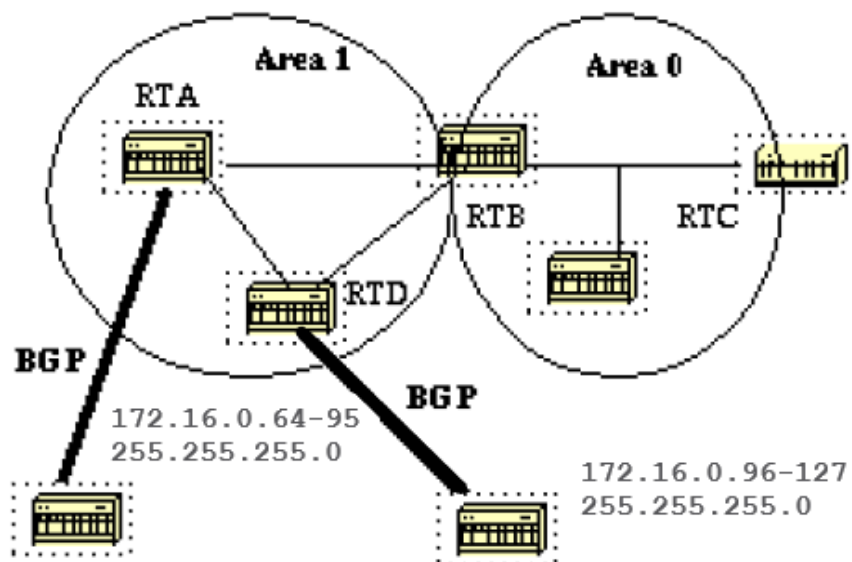
Il riepilogo delle route esterne riguarda esclusivamente le route esterne che sono state inserite nell'OSPF tramite redistribuzione. Inoltre, gli intervalli esterni che vengono riepilogati devono essere contigui.

Il riepilogo degli intervalli sovrapposti di due router diversi potrebbe causare l'invio dei pacchetti alla destinazione errata. Il riepilogo viene eseguito tramite il **router ospf** sottocomando:

```
<#root>
```

```
summary-address ip-address mask
```

Il comando è valido solo per gli ASBR che eseguono la redistribuzione nell'OSPF.



In questo diagramma, RTA e RTD inseriscono le route esterne nell'OSPF mediante redistribuzione. RTA inserisce le subnet nell'intervallo 128.213.64-95 e RTD nell'intervallo 128.213.96-127. Per riassumere le subnet in un intervallo su ciascun router:

```
RTA# router ospf 100 summary-address 172.16.0.64 255.255.224.0 redistribute bgp 50 metric 1000 subnets RTD# router ospf 100 summary-address 172.1
```

In questo modo RTA genera una route esterna 172.16.0.64 255.255.224.0 e RTD genera 172.16.0.96 255.255.224.0.

Si noti che il **summary-address** comando non ha alcun effetto se utilizzato in RTB, in quanto RTB non esegue la redistribuzione in OSPF.

Aree stub

OSPF consente di configurare alcune aree come aree stub. Le reti esterne, ad esempio quelle ridistribuite da altri protocolli nell'OSPF, non possono essere inviate in un'area stub.

Per raggiungere le destinazioni esterne, queste aree usano una route predefinita. La configurazione di un'area stub riduce le dimensioni del database topologico di un'area e i requisiti di memoria dei router presenti.

Per essere configurata come area stub, un'area deve avere un unico punto di uscita oppure il routing alle destinazioni esterne non deve seguire un percorso ottimale.

In altre parole, un'area stub che ha più punti di uscita, ha anche uno o più ABR che inseriscono una route predefinita nell'area.

Le destinazioni esterne possono essere raggiunte con un percorso non ottimale uscendo dall'area tramite un punto che è più lontano rispetto agli altri punti di uscita.

Un'altra limitazione impedisce che l'area stub venga utilizzata come area di transito per i collegamenti virtuali. Inoltre, un ASBR non può essere interno all'area stub.

Queste limitazioni vengono applicate perché un'area stub è configurata principalmente per non trasportare route esterne e una qualsiasi di queste situazioni provoca l'inserimento di collegamenti esterni nell'area. La dorsale non può essere configurata come area stub.

Tutti i router OSPF all'interno di un'area stub devono essere configurati come router stub. Quando un'area è configurata come stub, tutte le interfacce di quell'area si scambiano pacchetti **Hello** con un flag per segnalare che l'interfaccia è stub.

In realtà si tratta semplicemente di un bit del pacchetto **Hello** (bit E) che viene impostato a 0. Tutti i router che hanno un segmento comune devono concordare su tale flag. In caso contrario, non possono diventare vicini e il routing non viene effettuato.

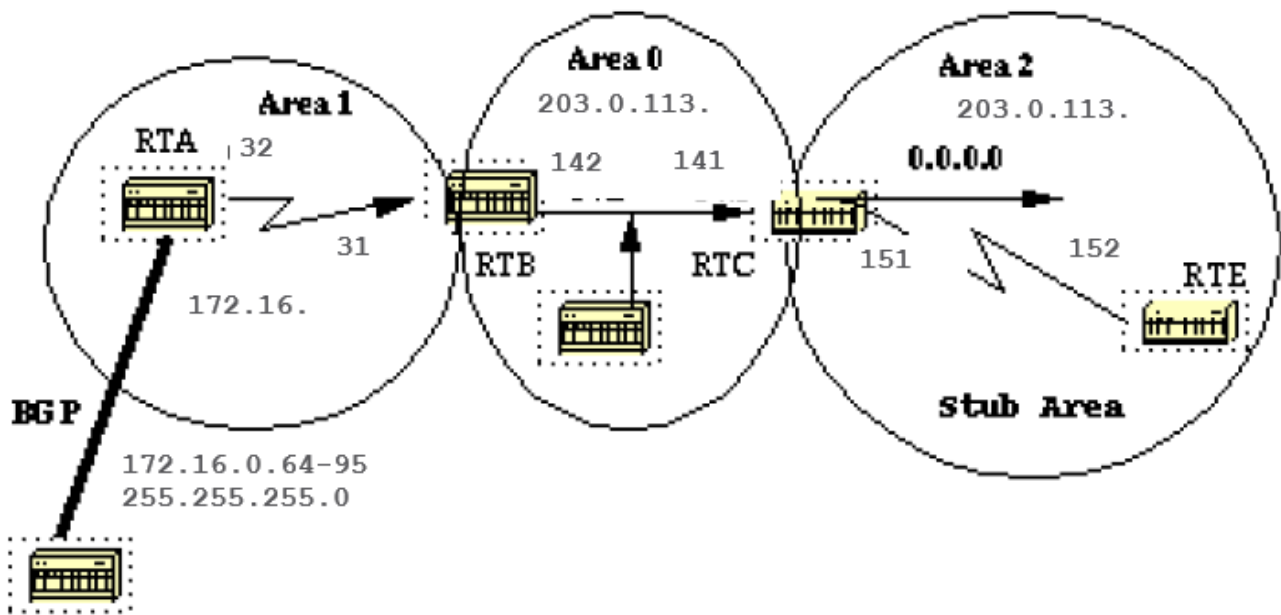
Un'estensione delle aree stub viene definita **TSA (Totally Stubby Area)**. Cisco lo indica con l'aggiunta di una parola **no-summary** chiave alla configurazione dell'area di stub.

Un'area **TSA** impedisce alle route esterne e alle route di riepilogo (route inter-area) di entrare nell'area.

In questo modo, le uniche route che possono entrare nell'area sono le route intra-area e la route predefinita 0.0.0.0.

- Il comando che configura un'area come stub è: **area <area-id> stub [no-summary]**
- Di seguito è riportato il comando che consente di configurare un costo predefinito in un'area: **area area-id default-cost cost**

Se il costo non viene impostato con tale comando, l'ABR annuncia un costo pari a 1.



Si supponga che l'area 2 debba essere configurata come area stub. Questo esempio la tabella di routing di RTE prima e dopo la configurazione dell'area 2 come area stub.

<#root>

```
RTC# interface Ethernet 0 ip address 203.0.113.141 255.255.255.0 interface Serial1 ip address 203.0.113.151 255.255.255.252 router ospf 10 network 203
```

```
show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa

RTE ha appreso le route inter-area (O IA) 203.0.113.140 e 172.16.0.63, la route intra-area (O) 172.16.0.208 e la route esterna (O E2) 172.16.0.64.

Per configurare l'area 2 come stub:

```
RTC# interface Ethernet 0 ip address 203.0.113.141 255.255.255.0 interface Serial1 ip address 203.0.113.151 255.255.255.252 router ospf 10 network 203
```

Si noti che il **stub** comando è configurato anche su RTE, altrimenti RTE non diventa mai un router adiacente a RTC. Il costo predefinito non è stato impostato, quindi RTC annuncia 0.0.0.0 a RTE con una metrica pari a 1.

<#root>

RTE#

```
show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa

Tenere presente che vengono visualizzate tutte le route tranne le route esterne che sono state sostituite dalla route predefinita 0.0.0.0. Il costo della route è 65 (64 per una linea T1 + 1 annunciato da RTC).

Ora configuriamo l'area 2 come area TSA e cambieremo il costo predefinito da 0.0.0.0 a 10.

<#root>

```
RTC# interface Ethernet 0 ip address 203.0.113.141 255.255.255.0 interface Serial1 ip address 203.0.113.151 255.255.255.252 router ospf 10 network 203
```

```
show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa

Tenere presente che le uniche route visualizzate sono le route intra-area (O) e la route predefinita 0.0.0.0. Le route esterne e le route inter-area sono state bloccate.

Il costo della route predefinita è ora 74 (64 per una linea T1 + 10 annunciato da RTC). In questo caso non è necessaria alcuna configurazione su RTE.

L'area è già stub e il **no-summary** comando non influisce sul pacchetto Hello come il **stub** comando.

Ridistribuire le route nell'OSPF

Ridistribuendo le route nell'OSPF da altri protocolli di routing o da routing statici, queste route diventano route esterne OSPF. Per ridistribuire le route in OSPF, immettere questo comando in modalità di configurazione router:

<#root>

```
redistribute protocol [process-id] [metric value] [metric-type value] [route-map map-tag] [subnets]
```



Nota: questo comando deve trovarsi su un'unica riga.

Le variabili **protocol** e **process-id** definiscono il protocollo che inseriamo nell'OSPF e, se presente, l'ID del processo. La metrica è il costo che assegniamo alla route esterna.

Se non viene specificata alcuna metrica, OSPF inserisce un valore predefinito di 20 quando vengono ridistribuite le route da tutti i protocolli, a eccezione delle route BGP che hanno una metrica pari a 1. Il valore metric-type viene descritto nel paragrafo successivo.

La route map è un metodo utilizzato per controllare la redistribuzione delle route tra i domini di routing. Il formato di una route map è:

<#root>

```
route-map map-tag [[permit | deny] | [sequence-number]]
```

Con la redistribuzione delle route in OSPF, vengono ridistribuite solo le route che non dispongono di subnet se la parola **subnets** chiave non è specificata.

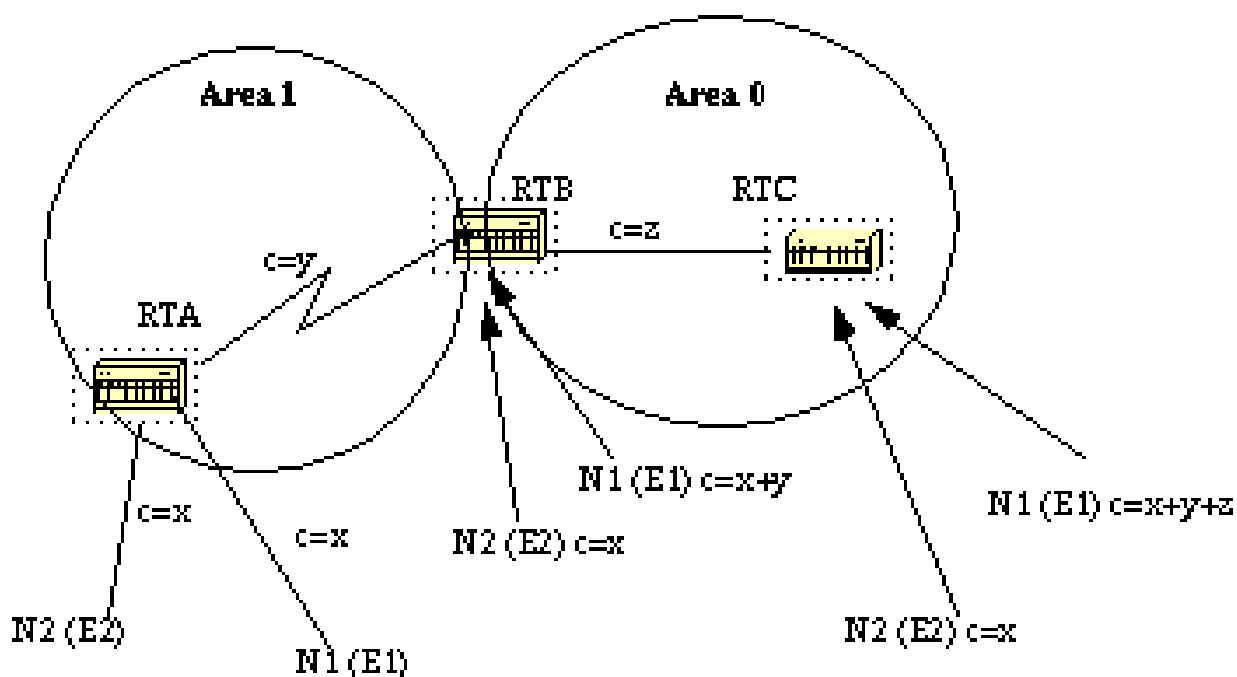
Route esterne E1 ed E2

Le route esterne possono essere di due tipi, tipo 1 e tipo 2. La differenza tra i due tipi sta nel modo in cui viene calcolato il costo (metrica) della route.

Il costo di una route di tipo 2 è sempre il costo esterno, indipendentemente da quanto è costato raggiungere la route (costo interno).

Un costo di tipo 1 equivale alla somma del costo esterno e del costo interno necessario per raggiungere la route.

Se indirizzate alla medesima destinazione, una route di tipo 1 è sempre preferita a una route di tipo 2,

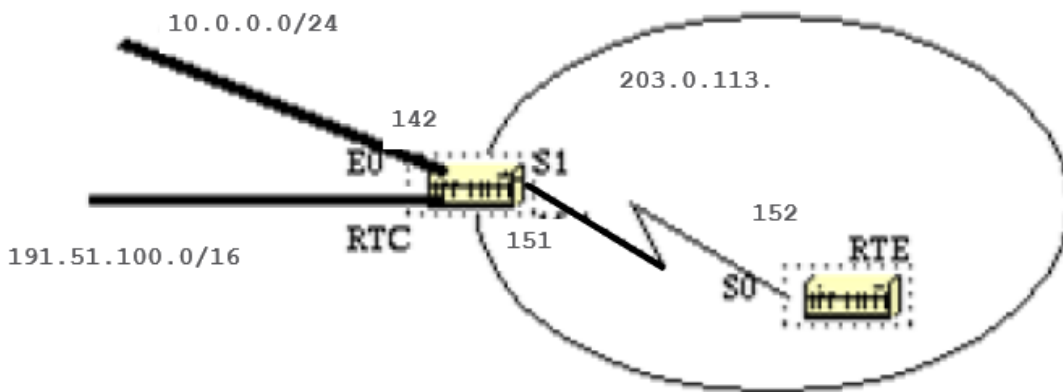


Come si evince da questo diagramma, RTA redistribuisce due route esterne nell'OSPF. N1 e N2 hanno entrambi un costo esterno di x . L'unica differenza è che N1 viene redistribuito nell'OSPF con una metrica di tipo 1 e N2 viene redistribuito con una metrica di tipo 2.

Se tracciamo le route che vanno dall'area 1 all'area 0, il costo per raggiungere N2 visto da RTB o RTC è sempre x . Il costo interno lungo il percorso non viene preso in considerazione. D'altro canto, il costo per raggiungere N1 è maggiore per via del costo interno. Il costo è $x+y$ visto da RTB e $x+y+z$ visto da RTC.

Se le route esterne sono entrambe di tipo 2 e i costi esterni per la rete di destinazione sono uguali, viene scelto come percorso migliore quello con il costo più basso per l'ASBR.

Se non viene specificato diversamente, il tipo esterno predefinito assegnato alle route esterne è 2.



Supponiamo di aver aggiunto due route statiche dirette a E0 su RTC: 10.0.0.16 255.255.255.0 (la notazione /24 indica una maschera a 24 bit a partire dall'estrema sinistra) e 198.51.100.1 255.255.0.0.

In questo esempio vengono mostrati i diversi comportamenti quando vengono utilizzati parametri diversi nel **redistribute** comando di RTC:

```
<#root>
```

```
RTC# interface Ethernet0 ip address 203.0.113.142 255.255.255.0 interface Serial1 ip address 203.0.113.151 255.255.255.252 router ospf 10
```

```
redistribute static
```

```
network 203.0.113.150 0.0.0.255 area 2 network 203.0.113.140 0.0.0.255 area 0 ip route 10.0.0.16 255.2
```

L'output di **show ip route** su RTE:

```
<#root>
```

```
RTE#
```

```
show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa

Si noti che l'unica route esterna visualizzata è 198.51.100.1, in quanto non è stata utilizzata la parola **subnet** chiave. Tenere presente che se la parola **subnet** chiave non viene utilizzata, verranno ridistribuite solo le route che non dispongono di subnet. Nel nostro caso 10.0.0.16 è una route di classe A con subnet e non viene ridistribuita. Poiché la parola **metric** chiave non è stata utilizzata (o un' **default-metric** istruzione sotto il router OSPF), il costo allocato alla route esterna è 20 (il valore predefinito è 1 per BGP).

```
<#root>
```

```
redistribute static metric 50 subnets
```

```
RTE#
```

```
show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa
```

```
50
```

```
] via 203.0.113.151, 00:00:02, Serial0 203.0.113.150 255.255.255.252 is subnetted, 1 subnets C 203.0.11
```

```
50
```

```
] via 203.0.113.151, 00:00:02, Serial0
```

Notare che 10.0.0.16 viene ora visualizzato e il costo delle route esterne è diventato 50. Poiché le route esterne sono di tipo 2 (E2), il costo interno non è stato aggiunto. Supponiamo ora di cambiare il tipo in E1:

```
<#root>
```

```
redistribute static metric 50 metric-type 1 subnets
```

```
RTE#
```

```
show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa
```

```
114
```

```
] via 203.0.113.151, 00:04:20, Serial0 203.0.113.150 255.255.255.252 is subnetted, 1 subnets C 203.0.11
```

```
114
```

```
] via 203.0.113.151, 00:04:21, Serial0
```

Il tipo è cambiato in E1 e al costo è stato aggiunto il costo interno di S0 pari a 64 per un totale di 64+50=114.

Supponiamo di aggiungere una route map alla configurazione di RTC:

<#root>

```
RTC# interface Ethernet0 ip address 203.0.113.142 255.255.255.0 interface Serial1 ip address 203.0.113.151 255.255.255.252 router ospf 10
redistribute static metric 50 metric-type 1 subnets route-map STOPUPDATE
network 203.0.113.150 0.0.0.255 area 2 network 203.0.113.140 0.0.0.255 area 0 ip route 10.0.0.16 255.2
```

La route map consente di ridistribuire solo 198.51.100.1 nell'OSPF; tutte le altre route vengono rifiutate. Ecco perché 10.0.0.16 non compare più nella tabella di routing di RTE.

<#root>

RTE#

```
show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa
```

Ridistribuire l'OSPF negli altri protocolli

Uso di una metrica valida

Ogni volta che si ridistribuisce OSPF in altri protocolli, occorre rispettare anche le regole degli altri protocolli. In particolare, la metrica applicata deve corrispondere alla metrica del protocollo in cui viene ridistribuito l'OSPF.

Ad esempio, la metrica RIP conta gli hop da un minimo di 1 a un massimo di 16, dove 1 indica che una rete è a un hop di distanza e 16 indica che la rete è irraggiungibile. I protocolli IGRP ed EIGRP richiedono invece una metrica del tipo:

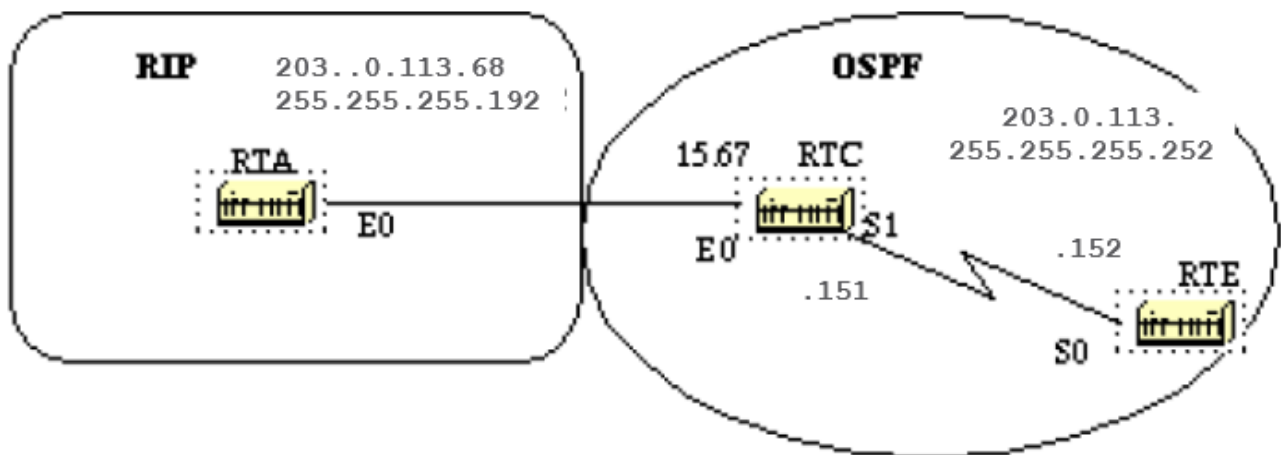
<#root>

```
default-metric bandwidth delay reliability loading mtu
```

VLSM

Un altro aspetto da tenere in considerazione è la subnet mask a lunghezza variabile, o VLSM (Variable Length Subnet Mask) (Appendice C). OSPF può trasportare le informazioni di più subnet per la stessa rete principale, a differenza di altri protocolli come RIP e IGRP (il protocollo EIGRP supporta la VLSM).

Se la stessa rete principale supera i confini di un dominio OSPF e RIP, le informazioni VLSM ridistribuite nei protocolli RIP o IGRP vanno perse ed è necessario configurare le route statiche nei domini RIP o IGRP. Questo esempio illustra il problema.



In questo diagramma, RTE esegue il protocollo OSPF e RTA esegue il protocollo RIP. RTC esegue la redistribuzione tra i due protocolli. Il problema è che la rete di classe C 203.0.113.150 ha una subnet variabile e due maschere diverse 255.255.255.252 e 255.255.255.192.

Di seguito la configurazione e le tabelle di routing di RTE e RTA:

<#root>

RTA# interface Ethernet0 ip address 203.0.113.68 255.255.255.192 router rip network 203.0.113.150 RTC# interface Ethernet0 ip address 203.0.113.67 255.255.255.192

show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external

show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external

RTE ha riconosciuto che la route 203.0.113.150 ha due subnet, mentre RTA ritiene che abbia una sola subnet (quella configurata sull'interfaccia).

Le informazioni sulla subnet 203.0.113.150 255.255.255.252 vengono perse nel dominio RIP. Per raggiungere tale subnet, è necessario configurare una route statica su RTA:

<#root>

RTA# interface Ethernet0 ip address 203.0.113.68 255.255.255.192 router rip network 203.0.113.150

ip route 203.0.113.150 255.255.255.0 203.0.113.67

In questo modo RTA è in grado di raggiungere le altre subnet.

Ridistribuzione reciproca

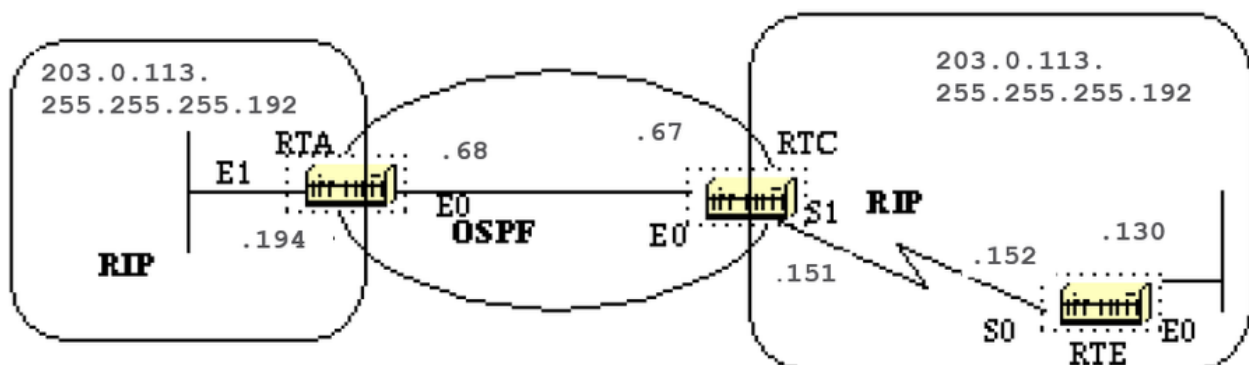
La ridistribuzione reciproca tra i protocolli deve essere effettuata con molta attenzione e in modo controllato. Una configurazione errata può causare il loop delle informazioni di routing.

Una buona prassi è impedire l'inserimento di informazioni apprese da un protocollo nello stesso protocollo.

Le interfacce passive e gli elenchi di distribuzione devono essere applicati sui router di redistribuzione. Filtrare le informazioni con i protocolli link-state come OSPF è un'operazione complessa.


Distribute-list out funziona sull'ASBR per filtrare le route redistribute in altri protocolli. **Distribute-list in** funziona su qualsiasi router per impedire le route dalla tabella di routing, ma non impedisce la propagazione dei pacchetti allo stato del collegamento; i router a valle disporrebbero comunque delle route.

Per evitare loop, si consiglia di non usare i filtri sul protocollo OSPF e di applicarli invece agli altri protocolli.



Per illustrare questa situazione, supponiamo che su RTA, RTC e RTE venga eseguito il protocollo RIP. RTC e RTA usano anche il protocollo OSPF. Sia RTC che RTA effettuano la redistribuzione tra RIP e OSPF.

Se non si desidera che il RIP proveniente da RTE venga inserito nel dominio OSPF, impostare un'interfaccia passiva su E0 per il RIP di RTC. Tuttavia, è stato consentito l'inserimento del RIP proveniente da RTA nell'OSPF. Ecco il risultato:

 **Nota:** non utilizzare questa configurazione.

<#root>

```
RTE# interface Ethernet0 ip address 203.0.113.151 255.255.255.192 interface Serial0 ip address 203.0.113.152 255.255.255.192 router rip network 203.0.
```

```
show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external  
R 203.0.113.151 [120/1] via 203.0.113.68, 00:01:08, Ethernet0 [120/1] via 203.0.113.152, 00:00:11, Serial0
```

0 203.0.113.151 [110/20] via 203.0.113.68, 00:21:41, Ethernet0

Tenere presente che RTC può raggiungere la subnet 203.0.113.151 usando due percorsi: Serial 1 ed Ethernet 0 (E0 è ovviamente il percorso sbagliato). Ciò si è verificato perché RTC ha fornito questa voce a RTA tramite OSPF e RTA l'ha restituita tramite RIP in quanto non acquisita tramite lo stesso protocollo RIP.

Questo è un esempio su scala ridotta dei loop che possono verificarsi a causa di una configurazione errata. Nelle reti di grandi dimensioni la situazione è persino più complessa.

Per risolvere il problema nel nostro esempio, non inviare **RIP** sulla subnet Ethernet 0 di RTA tramite un'interfaccia passiva. Questa operazione non è idonea nel caso in cui alcuni router su Ethernet utilizzino esclusivamente il protocollo RIP.

In questo caso, è possibile consentire a RTC di inviare il protocollo RIP su Ethernet; in questo modo RTA non lo restituisce a causa dello split horizon (non funziona sulle reti NBMA se lo split horizon è disattivato).

Lo split horizon non consente l'invio di aggiornamenti sulla stessa interfaccia da cui sono stati acquisiti (ossia tramite lo stesso protocollo).

Un altro metodo valido è applicare i comandi distribute-list su RTA per impedire che le subnet apprese tramite OSPF vengano reinserite nel protocollo RIP su Ethernet. Quest'ultimo viene utilizzato:

<#root>

```
RTA# interface Ethernet0 ip address 203.0.113.68 255.255.255.192 router ospf 10 redistribute rip metric 10 subnets network 203.0.113.150 0.0.0.255 area  
distribute-list 1 out ospf 10
```

L'output della tabella di routing di RTC sarà:

<#root>

```
RTF#  
show ip route  
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external  
R 203.0.113.151 [120/1] via 203.0.113.152, 00:00:19, Serial1  
O 203.0.113.151 [110/20] via 203.0.113.68, 00:21:41, Ethernet0
```

Inserire route predefinite nell'OSPF

Il router di confine di un sistema autonomo, o ASBR (Autonomous System Boundary Router), può essere configurato in modo che generi una route predefinita nel dominio OSPF. Un router diventa un ASBR ogni volta che le route vengono ridistribuite in un dominio OSPF.

Tuttavia, un ASBR non genera automaticamente una route predefinita nel dominio di routing OSPF.

Per fare in modo che OSPF generi una route predefinita, procedere come segue:

<#root>

```
default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]
```

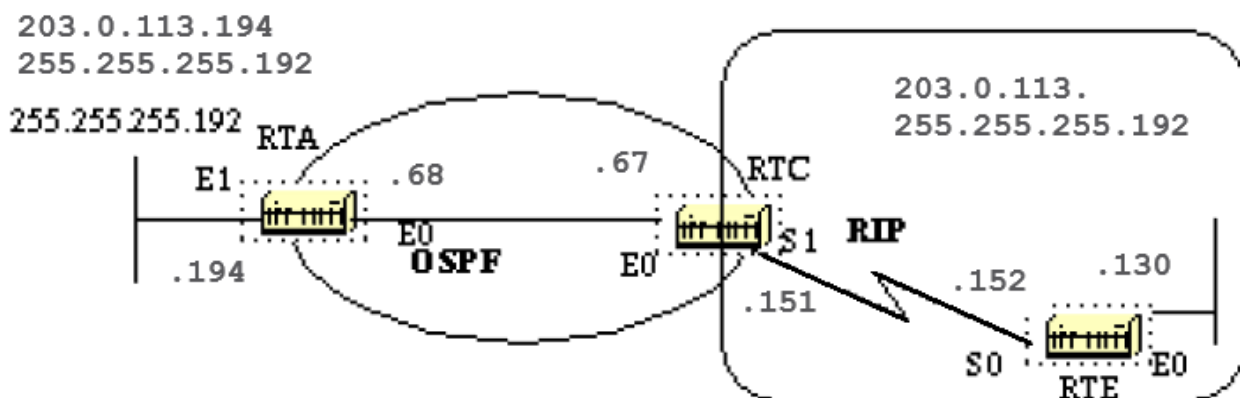


Nota: questo comando deve trovarsi su un'unica riga.

Per generare una route predefinita, è possibile seguire due metodi. Il primo è annunciare la route 0.0.0.0 all'interno del dominio, ma solo se l'ASBR stesso ha già una route predefinita. Il secondo è annunciare la route 0.0.0.0 indipendentemente dal fatto che l'ASBR abbia una route predefinita. Quest'ultima può essere impostata con la parola chiave **always**.

Prestare attenzione quando si utilizza la parola **always** chiave. Se il router annuncia una route predefinita (0.0.0.0) all'interno del dominio e non ha una route predefinita o un percorso per raggiungere le destinazioni, il routing viene interrotto.

La metrica e il tipo di metrica sono il costo e il tipo (E1 o E2) assegnati alla route predefinita. La route map specifica l'insieme di condizioni che devono essere soddisfatte per generare la route predefinita.



Supponiamo che RTE inserisca una route predefinita 0.0.0.0 nel protocollo RIP. RTC ha un gateway di ultima istanza di 203.0.113.152. RTC non propaga l'impostazione predefinita a RTA finché non viene configurato RTC con un **default-information originate** comando.

<#root>

RTC#

```
show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa

```
default-information originate metric 10
```

```
router rip redistribute ospf 10 metric 2 passive-interface Ethernet0 network 203.0.113.150 RTA#
```

```
show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa

Tenere presente che RTA ha appreso 0.0.0.0 come route esterna con metrica 10. Il gateway di ultima istanza è impostato su 203.0.113.67 come previsto.

Suggerimenti per la progettazione del protocollo OSPF

La RFC (1583) OSPF non offre alcuna indicazione sul numero di router di un'area o sul numero di router vicini per segmento né suggerisce il modo migliore per creare la rete.

Esistono diversi approcci alla progettazione della rete OSPF. la cosa importante da ricordare è però che qualsiasi protocollo, portato ai suoi limiti, può non funzionare correttamente.

Cercare di non complicare troppo il protocollo, ma usarlo in modo da valorizzarne le funzionalità.

Numero di router per area

Il numero massimo di router per area dipende da diversi fattori:

- Qual è il tipo di area?
- Quale tipo di potenza della CPU è disponibile in quell'area?
- Quale tipo di supporto?
- OSPF funziona in modalità NBMA?
- La rete NBMA è magliata?
- Sono presenti molti LSA esterni nella rete?
- Le altre aree sono riassunte in modo efficiente?

Per questi motivi, è difficile individuare un numero massimo di router per area. Rivolgersi al rivenditore locale o al tecnico di sistema per consigli esperti sul progetto della rete.

Numero di router vicini

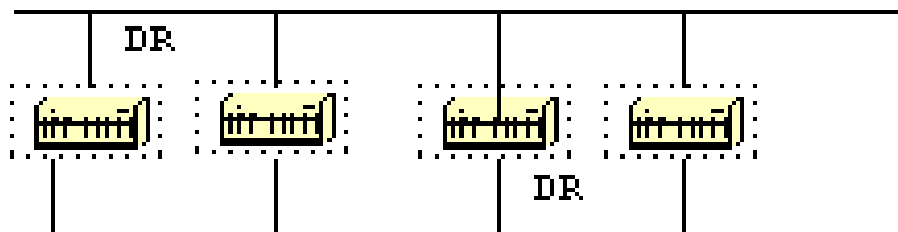
Anche il numero di router connessi alla stessa LAN è importante. Ogni LAN ha un DR e un BDR che creano adiacenze con tutti gli altri router.

Minore è il numero di router vicini sulla LAN, minore è il numero di adiacenze che un DR o un BDR deve creare. Ciò dipende dalla potenza del router.

È sempre possibile modificare la priorità OSPF in modo che venga selezionato un DR. Evitare che lo stesso router sia dichiarato DR su più di un segmento.

Se la scelta del DR si basa sul RID più alto, un router potrebbe accidentalmente diventare un DR su tutti i segmenti a cui è connesso. Il router viene sottoposto a un carico di lavoro eccessivo, mentre gli altri router rimangono inattivi.

`More neighbors = more work for DR/BDR`



Numero di aree per ABR

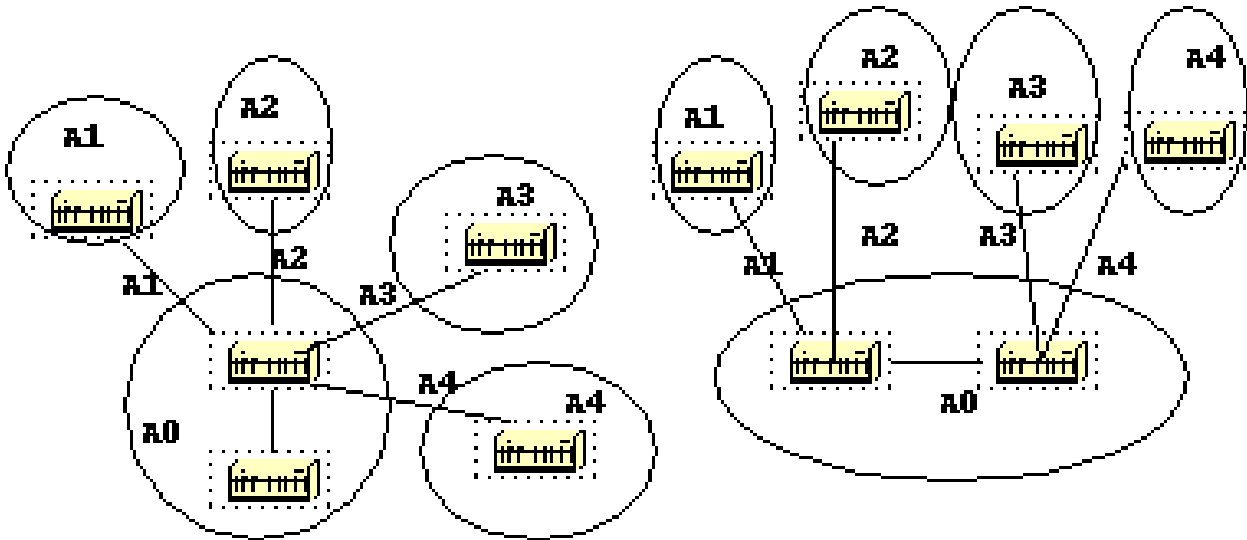
Gli ABR conservano una copia del database di tutte le aree in cui operano. Se, ad esempio, un router è connesso a cinque aree, conserva un elenco di cinque database diversi.

Il numero di aree per ABR dipende da molti fattori, tra cui il tipo di area (normale, stub, NSSA), la potenza della CPU dell'ABR, il numero di route per area e il numero di route esterne per area.

Per questo motivo, non è possibile consigliare un numero specifico. È preferibile non sovraccaricare un ABR quando è sempre possibile distribuire le aree su altri router.

Questo diagramma mostra la differenza tra un ABR che contiene cinque database diversi (compresa l'area 0) e due ABR che contengono tre database ciascuno.

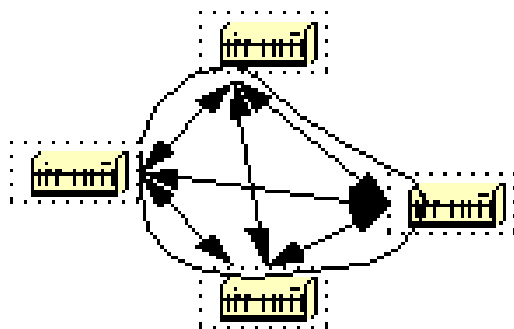
Queste sono solo linee guida. Un numero maggiore di aree configurate per ABR riduce le prestazioni. In alcuni casi, prestazioni inferiori potrebbero essere tollerate.



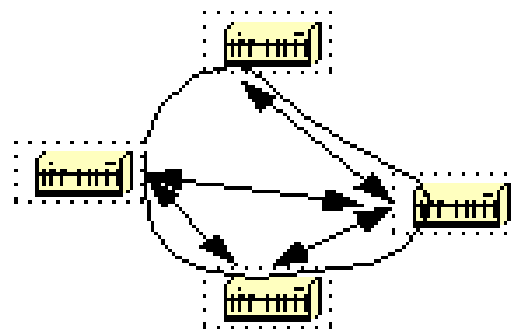
Topologia magliata e parzialmente magliata

La combinazione di bassa larghezza di banda e numero elevato di link state (associati ai cloud NBMA (Non Broadcast Multi-Access) come **Frame Relay** o **X.25**) comporta sempre dei problemi.

Una topologia parzialmente magliata ha mostrato prestazioni migliori di una topologia a maglia completa. Una rete point-to-point o point-to-multipoint ben progettata funziona molto meglio delle reti multipunto che devono affrontare i problemi del router DR.



Full Mesh
(not recommended)



Partial Mesh
(Works better)

Problemi di memoria

Non è facile capire quanta memoria dedicare a una configurazione OSPF. I problemi di memoria si verificano in genere quando vengono inserite troppe route esterne nel dominio OSPF.

Un'area dorsale con 40 router e una route predefinita per le destinazioni esterne avrebbe meno problemi di memoria rispetto a un'area dorsale con 4 router e 33.000 route esterne inserite nell'OSPF.

Una buona progettazione OSPF risolve anche i problemi di memoria. Il riepilogo dei router ABR e l'uso di aree stub potrebbero ridurre ulteriormente il numero di route scambiate.

La memoria totale utilizzata da OSPF è la somma della memoria utilizzata nella tabella di routing (**show ip route summary**) e della memoria utilizzata nel database dello stato del collegamento.

I numeri sono il risultato di una stima. Ogni voce nella tabella di routing utilizza tra 200 e 280 byte circa, più 44 byte per ogni percorso aggiuntivo.

Ogni LSA utilizza un sovraccarico di 100 byte oltre le dimensioni dell'LSA effettivo, a cui potrebbero aggiungersi 60–100 byte (per i collegamenti del router, a seconda del numero di interfacce sul router).

Questo valore deve essere aggiunto alla memoria utilizzata da altri processi e dallo stesso Cisco IOS®. Per conoscere il numero esatto, eseguire **show memory** con e senza OSPF attivato.

e calcolare la differenza di memoria del processore utilizzata (conservare una copia di backup delle configurazioni).

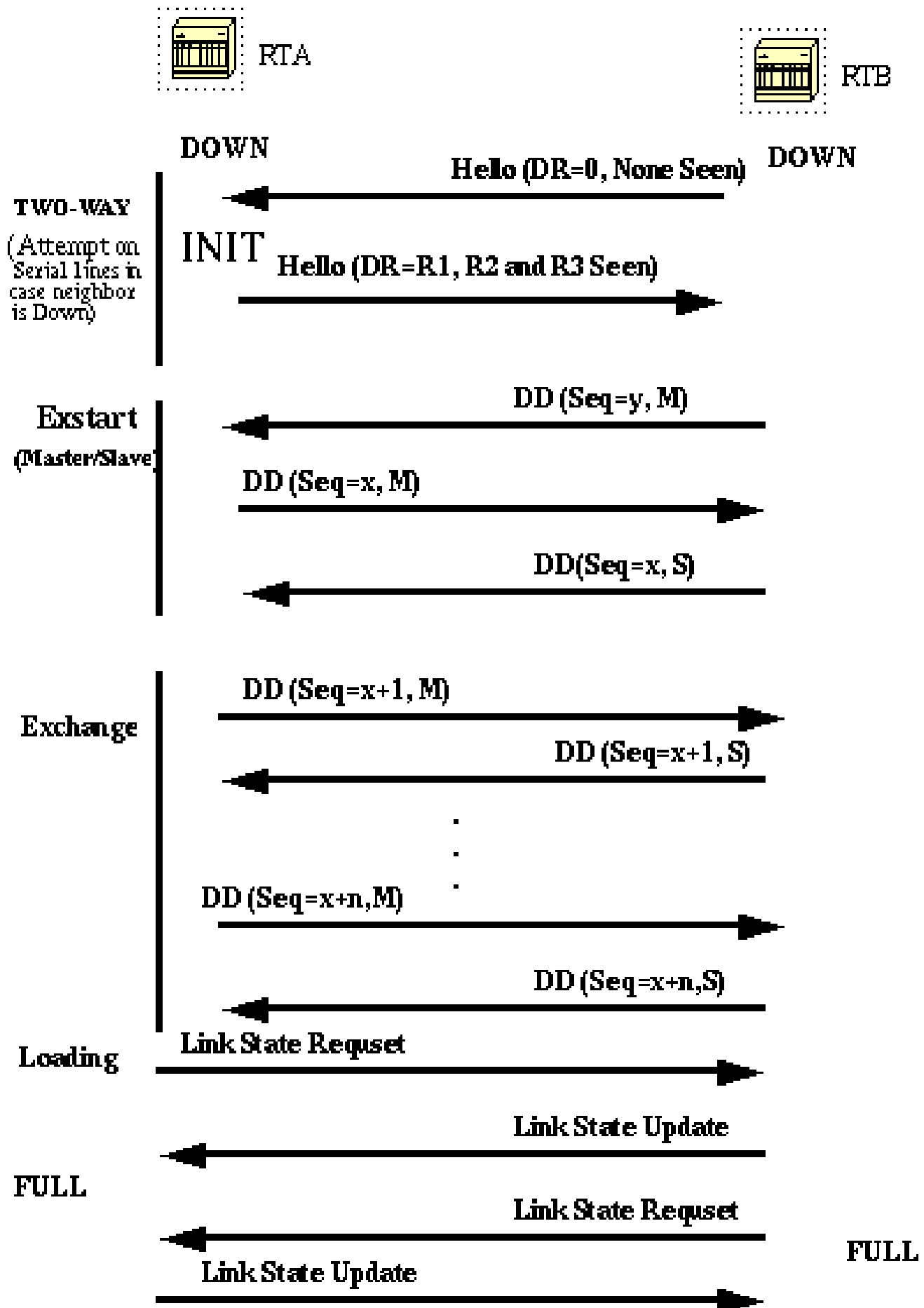
In genere una tabella di routing con meno di 500 kB può contenere da 2 a 4 MB di RAM. Le reti con dimensioni superiori a 500 kB richiedono da 8 a 16 MB o da 32 a 64 MB con route complete inserite da Internet.

Riepilogo

Il protocollo OSPF definito nella RFC 1583 fornisce un protocollo aperto ed efficiente che consente alle reti di più fornitori di comunicare utilizzando la famiglia di protocolli TCP/IP.

Alcuni dei vantaggi dell'OSPF sono: convergenza rapida, VLSM, autenticazione, segmentazione gerarchica, riepilogo delle route e aggregazione necessarie per gestire reti grandi e complesse.

Appendice A: Sincronizzazione del database link state



). Si tratta di annunci LSA abbreviati sotto forma di intestazioni. L'intestazione fornisce informazioni sufficienti per identificare un collegamento.

Il nodo primario invia pacchetti DD che vengono confermati da pacchetti DD inviati dal nodo secondario. Tutte le adiacenze nello stato Scambio o in uno stato successivo vengono utilizzate dalla procedura di flooding.

Tali adiacenze possono trasmettere e ricevere tutti i tipi di pacchetti del protocollo di routing OSPF.

Nello stato **Caricamento**, vengono inviati ai router vicini pacchetti link state che chiedono gli annunci più recenti, già rilevati ma non ancora ricevuti. Ogni router crea un elenco di LSA necessari per aggiornare la propria adiacenza.

Per garantire la conferma di ogni LSA, viene gestito un elenco di **ritrasmissione**. Per specificare il numero di secondi tra una ritrasmissione e l'altra degli annunci LSA dell'adiacenza, è possibile usare:

```
<#root>
```

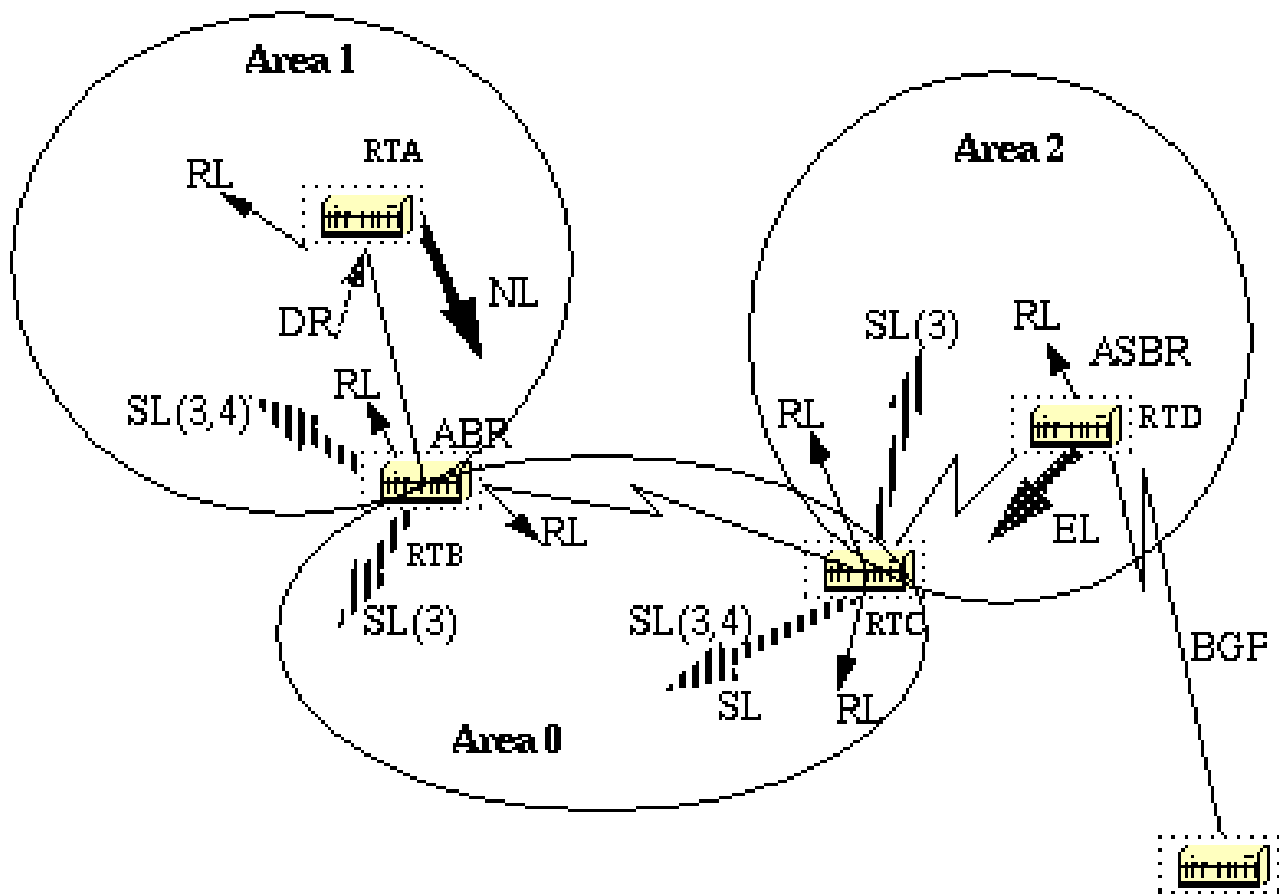
```
ip ospf retransmit-interval seconds
```

I pacchetti di aggiornamento link state vengono inviati in risposta ai pacchetti di richiesta. I pacchetti di aggiornamento link state vengono trasmessi in modalità flooding a tutte le adiacenze.

Nello stato **Completa**, i router vicini sono anche completamente adiacenti. I database di un'area comune sono una corrispondenza esatta tra router adiacenti.

Ogni LSA ha un campo **age** relativo alla durata che viene periodicamente incrementato mentre si trova nel database o quando viene trasmesso a tutti i dispositivi dell'area (modalità flooding). Quando un LSA raggiunge la durata massima (**Maxage**) e non è inserito in nessun elenco di ritrasmissione dei router vicini, viene eliminato dal database.

Annunci LSA (Link State Advertisement)



Gli annunci LSA possono essere di cinque tipi. I collegamenti del router (RL, Router Link) sono generati da tutti i router e descrivono lo stato delle interfacce del router all'interno di un'area specifica.

Vengono trasmessi a tutti i dispositivi presenti nell'area del router (modalità flooding). I collegamenti di rete (NL, Network Link) sono generati da un DR di un particolare segmento e segnalano quali router sono connessi.

I collegamenti di riepilogo (SL, Summary Link) sono collegamenti inter-area (tipo 3) ed elencano le reti interne ad altre aree, ma ancora appartenenti al sistema autonomo.

I collegamenti di riepilogo vengono inseriti dall'ABR dalla dorsale ad altre aree e da altre aree alla dorsale. Questi collegamenti vengono usati per l'aggregazione tra le aree.

Altri tipi di collegamenti di riepilogo sono i collegamenti asbr-summary. Si tratta di collegamenti di tipo 4 indirizzati all'ASBR. Ciò garantisce che tutti i router conoscano il modo per uscire dal sistema autonomo.

L'ultimo tipo è il tipo 5, i collegamenti esterni (EL, External Link), che vengono inseriti nel dominio dal router ASBR.

Il diagramma che precede illustra i diversi tipi di collegamento. RTA genera un collegamento del router (RL) nell'area 1 ed essendo il DR di quel segmento genera anche un collegamento di rete (NL).

RTB è un ABR e genera un collegamento RL nell'area 1 e nell'area 0. Inoltre, RTB genera collegamenti di riepilogo nell'area 1 e nell'area 0.

Questi collegamenti sono l'elenco delle reti scambiate tra le due aree.

Un collegamento di riepilogo ASBR viene inserito da RTB nell'area 1. In questo modo viene segnalata l'esistenza di RTD, il router di confine del sistema autonomo (ASBR).

Analogamente, RTC, che è un altro ABR, genera il collegamento RL per l'area 0 e l'area 2 e un collegamento SL (3) nell'area 2 (poiché non annuncia alcun ASBR) e un collegamento SL (3,4) nell'area 0 annunciando RTD.

RTD genera un collegamento RL per l'area 2 e un collegamento EL per le route esterne apprese tramite BGP. I router esterni vengono trasmessi a tutti i dispositivi del dominio (modalità flooding).

In questa tabella è riportato un riepilogo degli annunci LSA.

Tipo LS	Descrizione dell'annuncio
1	Annunci dei collegamenti del router. Generati da ciascun router per ogni area di cui fanno parte. Descrivono gli stati del collegamento del router all'area. Gli stati vengono trasmessi a tutti i dispositivi di una determinata area (modalità flooding).
2	Annunci dei collegamenti di rete. Generati dai router designati (DR). Descrivono l'insieme di router collegati a una particolare rete. Vengono trasmessi a tutti i dispositivi dell'area che contiene la rete (modalità flooding).
3 o 4	Annunci dei collegamenti di riepilogo. Generati dai router ABR. Descrivono le route inter-area (tra aree diverse). Il tipo 3 descrive le route indirizzate alle reti, utilizzato anche a scopo di aggregazione. Il tipo 4 descrive le route indirizzate all'ASBR.
5	Annunci dei collegamenti esterni al sistema autonomo. Originati dal router ASBR. Descrivono le route indirizzate alle destinazioni esterne al sistema autonomo. Vengono trasmesse in tutta la rete ad eccezione delle aree stub.

Se si esamina il database OSPF in dettaglio, con `show ip ospf database detail`, sono disponibili parole chiave diverse, ad esempio **Link-Data**, **Link-ID**, e **Link-state ID**. Sono termini non uniformi, in quanto il loro valore dipende dal tipo di link state e dal tipo di collegamento.

Rivediamo questa terminologia e forniamo un esempio dettagliato sul database OSPF visto dal router.

Il Link-State ID definisce fondamentalmente l'identità del link state a seconda del tipo.

I collegamenti del router sono identificati dall'ID del router (RID) da cui è stato originato l'annuncio.

I collegamenti di rete sono identificati dall'indirizzo IP relativo del DR. Ciò ha senso perché i collegamenti di rete sono originati dal router designato.

I collegamenti di riepilogo (tipo 3) sono identificati dai numeri della rete IP delle destinazioni a cui sono indirizzati.

I collegamenti di riepilogo dell'ASBR (collegamenti di riepilogo di tipo 4) sono identificati dal RID dell'ASBR.

I collegamenti esterni sono identificati dai numeri di rete IP delle destinazioni esterne a cui sono indirizzati. Queste informazioni sono riepilogate in questa tabella:

Tipo LS	Link State ID (nella vista di livello superiore del database quando si fa riferimento a un router, questo viene chiamato Link ID)
---------	---

1	L'ID del router (RID) di origine.
2	L'indirizzo dell'interfaccia IP del router designato della rete.
3	Il numero della rete di destinazione.
4	L'ID del router ASBR descritto.
5	Il numero della rete esterna.

I diversi collegamenti disponibili:

Collegamenti della rete stub: questo termine non ha nulla a che fare con le aree stub. Un segmento stub è un segmento a cui è collegato un solo router.

Un segmento Ethernet o Token Ring con un router collegato è considerato un collegamento a una rete stub. Un'interfaccia di loopback è considerata anche un collegamento alla rete stub con una maschera 255.255.255.255 (route host).

Collegamenti point-to-point: questi collegamenti possono essere connessioni seriali point-to-point fisiche o logiche (sottointerfacce). Possono essere numerati (indirizzo IP configurato sul collegamento) o non numerati.

Collegamenti di transito: si tratta di interfacce connesse alle reti a cui è collegato più di un router, da cui il nome transito.

Collegamenti virtuali: si tratta di collegamenti logici che collegano le aree senza connessioni fisiche alla dorsale. I collegamenti virtuali sono trattati come collegamenti point-to-point numerati.

Il valore **Link-ID** è un identificativo del collegamento ed è diverso per ciascun tipo di collegamento.

Un **collegamento di transito** è identificato dall'indirizzo IP del DR su quel collegamento.

Un **collegamento point-to-point numerato** viene identificato dal RID del router vicino sul collegamento point-to-point.

I collegamenti virtuali sono identici ai **collegamenti point-to-point**.

I collegamenti alle reti stub sono identificati dall'indirizzo IP dell'interfaccia alla rete stub. Queste informazioni sono riepilogate in questa tabella:

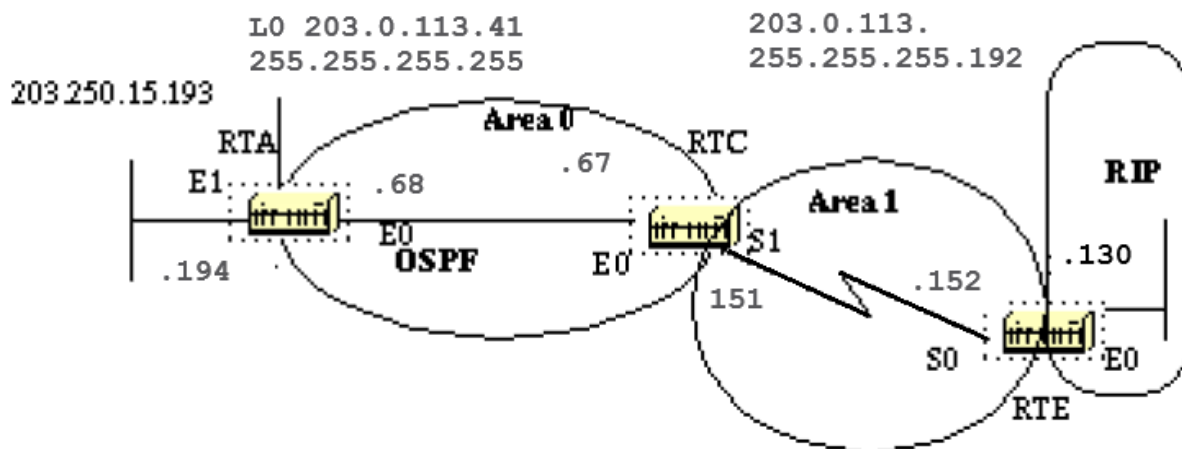
Tipo di collegamento	Link ID (applicabile ai singoli collegamenti)
Point-to-point	ID router vicino
Collegamento alla rete di transito	Indirizzo dell'interfaccia del DR
Collegamento alla rete stub (la maschera di loopback, eventualmente, è 255.255.255.255)	Numero di rete/subnet
Collegamento virtuale	ID router vicino

Il **Link Data** è l'indirizzo IP del collegamento, ad eccezione della rete stub dove corrispondono alla maschera di rete.

Tipo di collegamento	Link Data
Rete stub	Maschera di rete
Altre reti (solo per i collegamenti del router)	Indirizzo dell'interfaccia IP associato del router

Infine, un **router di annuncio** è il RID del router che ha inviato l'annuncio LSA.

Esempio di database OSPF



Dato questo diagramma di rete, le configurazioni e le tabelle di routing IP, ecco vari modi in cui il database OSPF può essere interpretato.

```
<#root>
```

```
RTA# interface Loopback0 ip address 203.0.113.41 255.255.255.255 interface Ethernet0 ip address 203.0.113.68 255.255.255.192 interface Ethernet1 ip a
```

```
show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa
```

```
show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa
```

```
show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP externa
```

Vista generale del database

```
<#root>
```

```
RTC#
```

```
show ip ospf database
```

```
OSPF Router with ID (203.0.113.67) (Process ID 10) Router Link States (Area 1) Link ID ADV Router Age
```

Questa è una panoramica generale dell'intero database OSPF. Il database viene elencato in base alle aree. In questo caso, esaminiamo il database di RTC che è un ABR. Vengono elencati sia i database dell'area 1 che quelli dell'area 0.

L'area 1 è composta da collegamenti del router e collegamenti di riepilogo. Non è presente alcun collegamento di rete in quanto non esiste alcun DR sui segmenti dell'area 1. Non è presente nessun collegamento ASBR di riepilogo nell'area 1 perché l'unico ASBR si trova nell'area 0.

I collegamenti esterni non appartengono a un'area particolare e vengono trasmessi a tutti i dispositivi (modalità flooding). Tenere presente che tutti i collegamenti sono i collegamenti cumulativi raccolti da tutti i router di un'area.

Concentriamoci in particolare il database dell'area 0. Il Link-ID qui indicato è in realtà un Link-State ID e rappresenta l'intero router, non un singolo collegamento. Può sembrare ambiguo.

Tenere presente che questo Link-ID di alto livello (in realtà un Link-State ID) rappresenta l'intero router e non solo un collegamento.

Collegamenti del router

```
<#root>
```

```
Router Link States (Area 0) Link ID ADV Router Age Seq# Checksum
```

```
Link count
```

```
203.0.113.41 203.0.113.41 179 0x80000029 0x9ADA
```

```
3
```

```
203.0.113.67 203.0.113.67 675 0x800001E2 0xDD23
```

```
1
```

Iniziamo dai collegamenti del router. Sono elencate due voci per 203.0.113.41 e 203.0.113.67, ovvero i RID dei due router dell'area 0. Inoltre, viene indicato il numero di collegamenti nell'area 0 per ogni router. RTA ha tre collegamenti all'area 0 e RTC ha un collegamento. Una panoramica dettagliata dei collegamenti del router RTC:

```
<#root>
```

```
RTC#
```

```
show ip ospf database router 203.0.113.67
```

```
OSPF Router with ID (203.0.113.67) (Process ID 10) Router Link States (Area 1) LS age: 1169 Options: (
```

```
Link connected to: a Stub Network (Link ID) Network/subnet number: 203.0.113.150 (Link Data) Network Mas
```

In questo caso OSPF genera un collegamento stub aggiuntivo per ogni interfaccia point-to-point. Non deve stupire che il numero dei collegamenti superi il numero delle interfacce fisiche.

<#root>

Router Link States (Area 0) LS age: 1227 Options: (No TOS-capability)

LS Type: Router Links Link State ID: 203.0.113.67 Advertising Router: 203.0.113.67

LS Seq Number: 80000003 Checksum: 0xA041 Length: 36 Area Border Router

Number of Links: 1 Link connected to: a Transit Network (Link ID) Designated Router address: 203.0.113.68

Number of TOS metrics: 0 TOS 0 Metrics: 10

Infatti, il Link ID equivale all'indirizzo IP (non al RID) del DR collegato; in questo caso è 203.0.113.68. Il Link Data è l'indirizzo IP di RTC.

Collegamenti di rete

Net Link States (Area 0) Link ID ADV Router Age Seq# Checksum 203.0.113.68 203.0.113.41 334 0x80000001 0xB6B5

Viene elencato un solo collegamento di rete, indicato dall'indirizzo IP dell'interfaccia (non dal RID) del DR, in questo caso 203.0.113.68. Una vista dettagliata di questa voce:

<#root>

RTC#

show ip ospf database network

OSPF Router with ID (203.0.113.67) (Process ID 10) Net Link States (Area 0) Routing Bit Set on this LS

Link State ID: 203.0.113.68 (address of Designated Router) Advertising Router: 203.0.113.41

LS Seq Number: 80000002 Checksum: 0xB4B6 Length: 32 Network Mask: 255.255.255.192

Attached Router: 203.0.113.41 Attached Router: 203.0.113.67

Tenere presente che i collegamenti di rete elencano i RID dei router collegati alla rete di transito; in questo caso i RID elencati sono di RTA e RTC.

Collegamenti di riepilogo

<#root>

Summary Net Link States (Area 0) Link ID ADV Router Age Seq# Checksum 203.0.113.150 203.0.113.67 792 0x80000002 0xAEBC Area 0 has one summary

show ip ospf database summary (area 1 is not listed)

Summary Net Link States (Area 0) LS age: 615 Options: (No TOS-capability) LS Type: Summary Links(Netwo

Link State ID: 203.0.113.150 (summary Network Number)

Advertising Router: 203.0.113.67 LS Seq Number: 80000003 Checksum: 0xACBE Length: 28 Network Mask: 255

Collegamenti ASBR di riepilogo

```
Summary ASB Link States (Area 0) Link ID ADV Router Age Seq# Checksum 203.0.113.16 203.0.113.67 579 0x80000001 0xF9AF
```

Un'indicazione per individuare qual è il router ASBR. In questo caso, l'ASBR è RTE ed è rappresentato dal suo RID 203.0.113.16. Il router di annuncio di questa voce nell'area 0 è RTC con RID 203.0.113.67. Una vista dettagliata della voce ASBR di riepilogo:

```
<#root>
```

```
RTC#
```

```
show ip ospf database asbr-summary
```

```
OSPF Router with ID (203.0.113.67) (Process ID 10) Summary ASB Link States (Area 0) LS age: 802 Option
LS Type: Summary Links(AS Boundary Router) Link State ID: 203.0.113.16 (AS Boundary Router address) Adve
LS Seq Number: 80000003 Checksum: 0xF5B1 Length: 28 Network Mask: 0.0.0.0 TOS: 0 Metric: 64
```

Collegamenti esterni

```
AS External Link States Link ID ADV Router Age Seq# Checksum Tag 0.0.0.0 203.0.113.16 1787 0x80000001 0x98CE 10 203.0.113.1288 203.0.113.16
```

Sono presenti due collegamenti esterni, il primo è lo 0.0.0.0 iniettato in OSPF tramite il **default-information originate** comando.

L'altra voce è la rete 203.0.113.128 8, inserita nell'OSPF tramite redistribuzione.

Il router che annuncia queste reti è 203.0.113.16, il RID di RTE.

Questa è la vista dettagliata delle route esterne:

```
<#root>
```

```
RTC#
```

```
show ip ospf database external
```

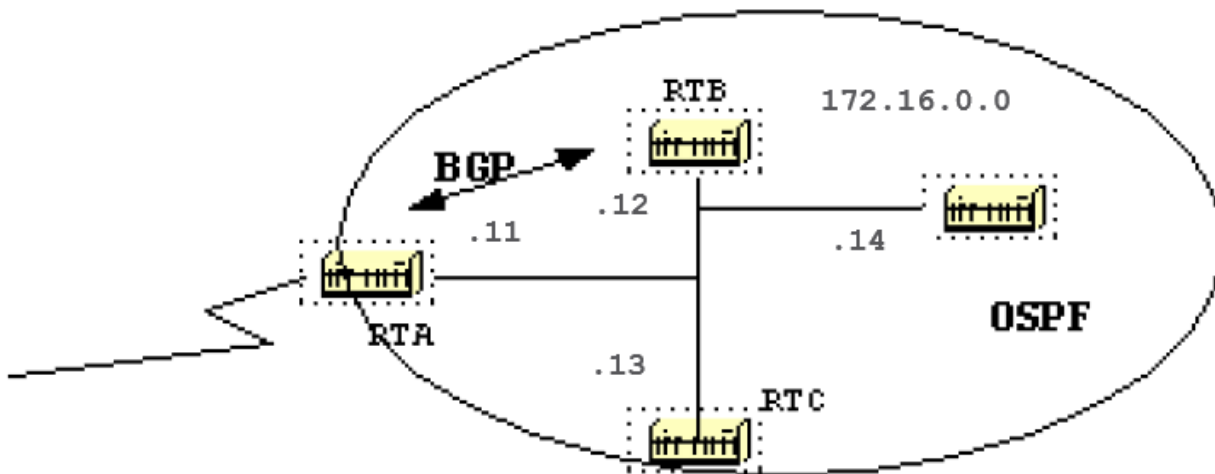
```
OSPF Router with ID (203.0.113.67) (Process ID 10) AS External Link States Routing Bit Set on this LSA
LS Type: AS External Link Link State ID: 0.0.0.0 (External Network Number ) Advertising Router: 203.0.11
LS Seq Number: 80000002 Checksum: 0x96CF Length: 36 Network Mask: 0.0.0.0 Metric Type: 2 (Larger than
Forward Address: 0.0.0.0
External Route Tag: 10 Routing Bit Set on this LSA LS age: 226 Options: (No TOS-capability)
```

LS Type: AS External Link Link State ID: 203.0.113.1288 (External Network Number) Advertising Router: 203.0.113.1288
LS Seq Number: 80000002 Checksum: 0x93C4 Length: 36 Network Mask: 255.255.255.192 Metric Type: 2 (Large Metric)
Forward Address: 0.0.0.0
External Route Tag: 0

Notare l'indirizzo di inoltro. Ogni volta che questo indirizzo è 0.0.0.0, indica che le route esterne sono raggiungibili tramite il router di annuncio, in questo caso 203.250.16.130.

Per questo motivo, l'identità dell'ASBR viene inserita dagli ABR in altre aree che utilizzano i collegamenti di riepilogo ASBR.

L'indirizzo di inoltro non è sempre 0.0.0.0. In alcuni casi, potrebbe trattarsi dell'indirizzo IP di un altro router sullo stesso segmento. Questo diagramma illustra questa situazione:



In questo esempio, RTB usa il protocollo BGP su RTA e il protocollo OSPF sul resto del dominio. RTA non esegue il protocollo OSPF. RTB ridistribuisce le route BGP nell'OSPF.

In base all'OSPF, RTB è un ASBR che annuncia le route esterne. L'indirizzo di inoltro in questo caso è impostato su 172.16.0.11 e non sul router di annuncio (0.0.0.0) RTB.

Non è necessario effettuare l'hop aggiuntivo. I router all'interno del dominio OSPF devono raggiungere l'indirizzo di inoltro tramite OSPF affinché le route esterne vengano inserite nella tabella di routing IP.

Se l'indirizzo di inoltro viene raggiunto tramite un altro protocollo o non è accessibile, le voci esterne saranno nel database ma non nella tabella di routing IP.

Un'altra situazione potrebbe verificarsi se sia RTB che RTC sono ASBR (RTC esegue anche BGP con RTA). In questa situazione, per evitare carichi di lavoro eccessivi, uno dei due router non annuncia (e quindi elimina) le route esterne. Il router con il RID più alto ha la priorità.

Il database completo

Ecco un esempio di database. Ora è possibile rivedere e spiegare ogni singola voce:

<#root>

RTC#

show ip ospf database router

OSPF Router with ID (203.0.113.67) (Process ID 10) Router Link States (Area 1) LS age: 926 Options: (N

show ip ospf database network

OSPF Router with ID (203.0.113.67) (Process ID 10) Net Link States (Area 0) Routing Bit Set on this LS

show ip ospf database summary

OSPF Router with ID (203.0.113.67) (Process ID 10) Summary Net Link States (Area 1) LS age: 8 Options:

show ip ospf asbr-summary

OSPF Router with ID (203.0.113.67) (Process ID 10) Summary ASB Link States (Area 0) LS age: 576 Option

show ip ospf database external

OSPF Router with ID (203.0.113.67) (Process ID 10) AS External Link States Routing Bit Set on this LSA

Appendice B: OSPF e indirizzamento IP multicast

OSPF ha utilizzato indirizzi IP multicast per scambiare i pacchetti Hello e gli aggiornamenti link state. Un indirizzo IP multicast viene implementato con indirizzi di classe D. L'indirizzo di classe D è compreso tra 224.0.0.0 e 239.255.255.255.

Class D addressing

0

31



Alcuni indirizzi IP multicast speciali sono riservati per OSPF:

- 224.0.0.5: Tutti i router OSPF devono essere in grado di trasmettere e restare in ascolto su questo indirizzo.
- 224.0.0.6: Tutti i router DR e BDR devono essere in grado di trasmettere e restare in ascolto su questo indirizzo.

La mappatura tra indirizzi IP multicast e indirizzi MAC prevede la regola:

Per le reti con accessi multipli che supportano il multicast, i 23 bit di ordine inferiore dell'indirizzo IP vengono utilizzati come bit di ordine inferiore dell'indirizzo MAC multicast 01-005E-00-00-00. Ad esempio:

- 224.0.0.5 verrebbe associato a 01-00-5E-00-00-05
- 224.0.0.6 verrebbe associato a 01-00-5E-00-00-06

OSPF utilizza la trasmissione su reti Token Ring.

Appendice C: Subnet mask a lunghezza variabile (VLSM, Variable Length Subnet Mask)

Ecco un grafico di conversione binario/decimale:

	0000		0001		0010		0011		0100		0101		0110		0111
0	0000	16	0000	32	0000	48	0000	64	0000	80	0000	96	0000	112	0000
1	0001	17	0001	33	0001	49	0001	65	0001	81	0001	97	0001	113	0001
2	0010	18	0010	34	0010	50	0010	66	0010	82	0010	98	0010	114	0010
3	0011	19	0011	35	0011	51	0011	67	0011	83	0011	99	0011	115	0011
4	0100	20	0100	36	0100	52	0100	68	0100	84	0100	100	0100	116	0100
5	0101	21	0101	37	0101	53	0101	69	0101	85	0101	101	0101	117	0101
6	0110	22	0110	38	0110	54	0110	70	0110	86	0110	102	0110	118	0110
7	0111	23	0111	39	0111	55	0111	71	0111	87	0111	103	0111	119	0111
8	1000	24	1000	40	1000	56	1000	72	1000	88	1000	104	1000	120	1000
9	1001	25	1001	41	1001	57	1001	73	1001	89	1001	105	1001	121	1001
10	1010	26	1010	42	1010	58	1010	74	1010	90	1010	106	1010	122	1010
11	1011	27	1011	43	1011	59	1011	75	1011	91	1011	107	1011	123	1011
12	1100	28	1100	44	1100	60	1100	76	1100	92	1100	108	1100	124	1100
13	1101	29	1101	45	1101	61	1101	77	1101	93	1101	109	1101	125	1101
14	1110	30	1110	46	1110	62	1110	78	1110	94	1110	110	1110	126	1110
15	1111	31	1111	47	1111	63	1111	79	1111	95	1111	111	1111	127	1111
	1000		1001		1010		1011		1100		1101		1110		1111
128	0000	144	0000	160	0000	176	0000	192	0000	208	0000	224	0000	240	0000
129	0001	145	0001	161	0001	177	0001	193	0001	209	0001	225	0001	241	0001
130	0010	146	0010	162	0010	178	0010	194	0010	210	0010	226	0010	242	0010
131	0011	147	0011	163	0011	179	0011	195	0011	211	0011	227	0011	243	0011
132	0100	148	0100	164	0100	180	0100	196	0100	212	0100	228	0100	244	0100
133	0101	149	0101	165	0101	181	0101	197	0101	213	0101	229	0101	245	0101
134	0110	150	0110	166	0110	182	0110	198	0110	214	0110	230	0110	246	0110
135	0111	151	0111	167	0111	183	0111	199	0111	215	0111	231	0111	247	0111
136	1000	152	1000	168	1000	184	1000	200	1000	216	1000	232	1000	248	1000
137	1001	153	1001	169	1001	185	1001	201	1001	217	1001	233	1001	249	1001
138	1010	154	1010	170	1010	186	1010	202	1010	218	1010	234	1010	250	1010
139	1011	155	1011	171	1011	187	1011	203	1011	219	1011	235	1011	251	1011
140	1100	156	1100	172	1100	188	1100	204	1100	220	1100	236	1100	252	1100

141	1101	157	1101	173	1101	189	1101	205	1101	221	1101	237	1101	253	1101
142	1110	158	1110	174	1110	190	1110	206	1110	222	1110	238	1110	254	1110
143	1111	159	1111	175	1111	191	1111	207	1111	223	1111	239	1111	255	1111

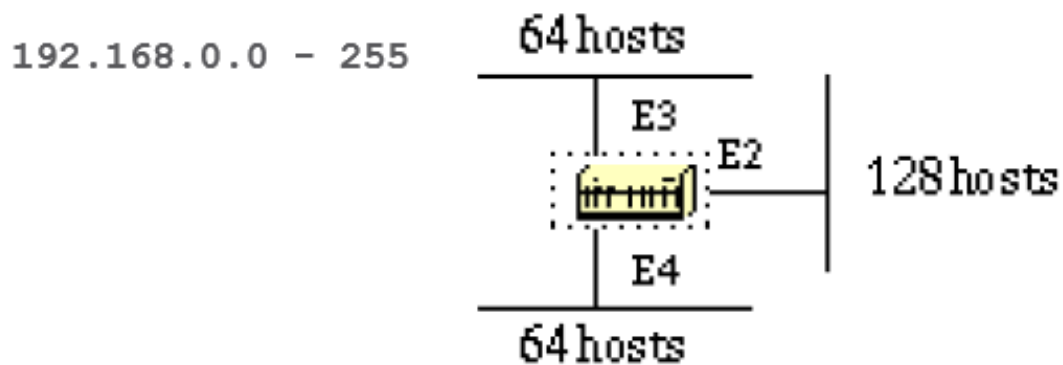
L'idea alla base delle subnet mask a lunghezza variabile (VLSM) è quella di offrire una maggiore flessibilità nella suddivisione di una rete principale in più subnet e mantenere un numero adeguato di host in ciascuna subnet.

Senza VLSM è possibile applicare una sola subnet mask a una rete principale. Ciò limita il numero di host dato il numero di subnet richieste.

Se si sceglie la maschera in modo da avere un numero sufficiente di subnet, non è possibile assegnare abbastanza host a ciascuna subnet. Lo stesso ragionamento si applica agli host; una maschera che permette di avere un numero sufficiente di host non fornisce spazio sufficiente per le subnet.

Ad esempio, supponiamo che sia stata assegnata una rete di classe C 192.168.0.0 e che sia necessario suddividere tale rete in tre subnet con 100 host in una subnet e 50 host nelle rimanenti.

Ignorando i due limiti 0 e 255, in teoria sarebbero disponibili 256 indirizzi (192.168.0.0 - 192.168.0.255). Questo risultato non può essere ottenuto senza VLSM.



È possibile utilizzare alcune subnet mask; tenere presente che una maschera deve avere un numero di uno contigui a partire da sinistra; i bit restanti devono essere tutti 0.

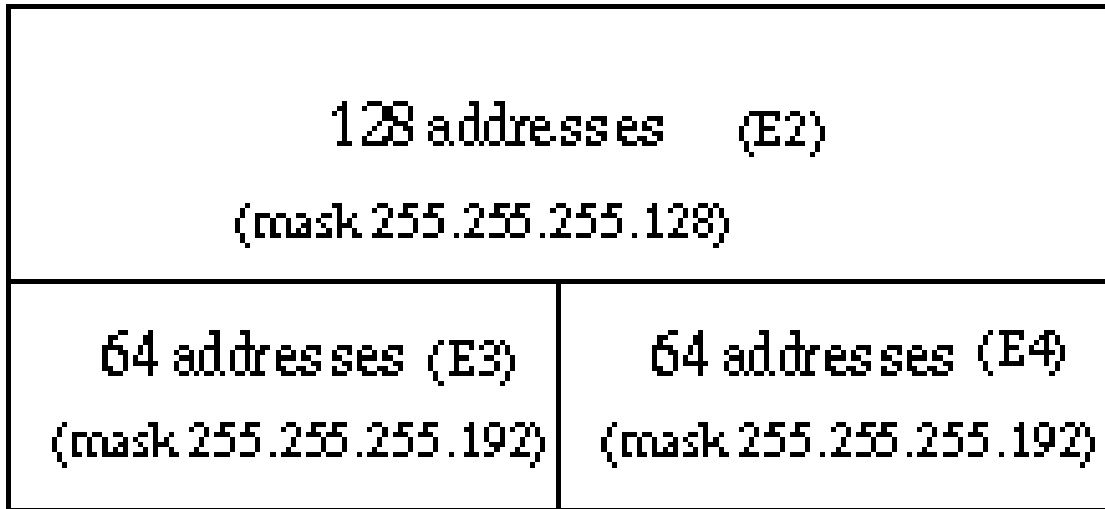
-252 (1111 1100) The address space is divided into 64. -248 (1111 1000) The address space is divided into 32. -240 (1111 0000) The address space is divided into 16.

Senza VLSM è possibile utilizzare la maschera 255.255.255.128 e dividere gli indirizzi in 2 subnet con 128 host ciascuna oppure utilizzare 255.255.255.192 e dividere lo spazio in 4 subnet con 64 host ciascuna.

Ciò non soddisfa però il requisito. Se si utilizzano più maschere, è possibile utilizzare la maschera 128 e creare un'altra subnet per il secondo blocco di indirizzi con la maschera 192.

In questa tabella viene mostrato come è stato suddiviso lo spazio degli indirizzi.

VLSM



Prestare attenzione nell'assegnazione degli indirizzi IP per ciascuna maschera. L'assegnazione di un indirizzo IP al router o a un host utilizza l'intera subnet per quel segmento.

Ad esempio, se si assegna 192.168.0.10 255.255.255.128 a E2, l'intero intervallo di indirizzi compreso tra 192.168.0.0 e 192.168.0.127 viene utilizzato da E2.

Allo stesso modo, se si assegna 192.168.0.160 255.255.255.128 a E2, l'intero intervallo di indirizzi compreso tra 192.168.0.128 e 192.168.0.255 viene utilizzato dal segmento E2.

Questa è un'illustrazione di come il router interpreta questi indirizzi. Tenere presente che ogni volta che si utilizza una maschera diversa dalla maschera naturale, ad esempio per creare una subnet, il router non accetterà una subnet pari a zero come risultato della combinazione di indirizzo IP e maschera.

Per risolvere il problema, usare il **ip subnet-zero** comando sul router.

```
<#root>
```

```
RTA# ip subnet-zero interface Ethernet2 ip address 192.168.0.10 255.255.255.128 interface Ethernet3 ip address 192.168.0.160 255.255.255.192 interface
```

```
show ip route connected
```

```
192.168.0.0 is variably subnetted, 3 subnets, 2 masks C 192.168.0.0 255.255.255.128 is directly connect
```

Informazioni correlate

- [Routing di Cisco IOS® IP: Guida di riferimento OSPF](#)
- [OSPF e MTU](#)
- [I router vicini OSPF sono bloccati nello stato Exstart e Scambio a causa di una mancata corrispondenza delle MTU](#)
- [Pagina di supporto del protocollo OSPF](#)
- [OSPF: Domande frequenti](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

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).