

# 21

## INTERNETWORKING CON ATM\*

---

Abbiamo già visto come la tecnica ATM possa essere utilizzata su scala locale, metropolitana e geografica. Per poter sfruttare ATM congiuntamente alle architetture di rete (TCP/IP, SNA, DECnet, IPX, ecc.) occorre però che queste si adattino alla nuova tecnologia. Sono stati seguiti due approcci:

- realizzare uno strato software che, emulando su ATM le funzionalità delle reti locali, consenta di trasportare qualsiasi protocollo di rete (tale approccio, proposto dall'ATM Forum, è stato descritto nel capitolo 20);
- modificare le architetture di rete introducendo il supporto nativo per ATM.

Questo secondo approccio è stato usato, per esempio, da IBM nella sua architettura APPN (si veda il paragrafo 18.5) ed è oggetto di discussione da parte del gruppo di lavoro "IP over ATM" dell'IETF (Internet Engineering Task Force) con particolare riferimento all'architettura di rete TCP/IP. Tale gruppo di lavoro produce periodicamente un documento [1] che riassume lo stato dei lavori in questo settore e che è alla base di questo capitolo.

### 21.1 TERMINOLOGIA

Questo paragrafo fornisce la definizione di alcuni termini che verranno utilizzati nel seguito:

---

\* Alla stesura di questo capitolo ha fornito un valido contributo l'ing. Davide Bergamasco, che ha svolto la sua tesi di laurea su questo tema presso il Politecnico di Torino. A Davide vanno i più sentiti ringraziamenti degli autori per la preziosa collaborazione.

- rete *broadcast*: rete che può essere composta da un numero arbitrario di stazioni e fornisce la funzionalità di trasmettere con un'unica operazione un pacchetto a tutte le stazioni. Le LAN sono un esempio di reti di questo tipo.
- rete *Non Broadcast Multiple Access* (NBMA): rete simile ad una rete broadcast, ma non fornisce la possibilità di trasmettere un pacchetto a tutte le stazioni. Fanno parte di questa categoria le reti X.25.
- rete *multicast capable*: rete che fornisce delle primitive per trasmettere con un'unica operazione un pacchetto ad un sottoinsieme delle stazioni della rete.

## 21.2 APPROCCI POSSIBILI

Quando si utilizza la tecnologia ATM, l'internetworking di reti locali e geografiche si arricchisce di interessanti possibilità e di molte complicazioni.

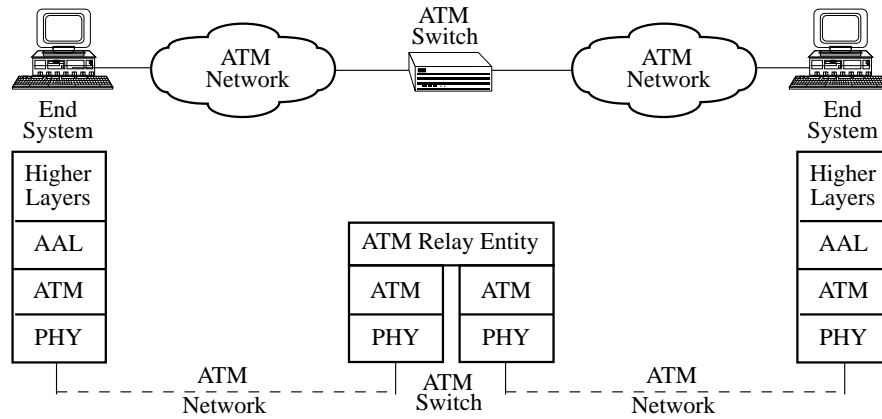
ATM può assumere il doppio ruolo di tecnologia con cui sono realizzate le reti da collegarsi (ad esempio LAN ATM), e di tecnologia con cui viene effettuato l'internetworking su base locale (dorsale di LAN in ATM) o su base geografica (servizio pubblico ATM).

Viste le molte combinazioni possibili, la trattazione che segue non è esaustiva, ma introduce comunque i tre livelli principali a cui può avvenire l'internetworking: livello 2 - sottolivello ATM, livello 2 - sottolivello 802.1D e livello 3.

### 21.2.1 Internetworking al sottolivello ATM

La prima soluzione è possibile solo se entrambe le reti da collegare sono in tecnologia ATM. Essa consiste nell'utilizzare uno switch che faccia transitare le celle ATM tra le due reti (figura 21.1).

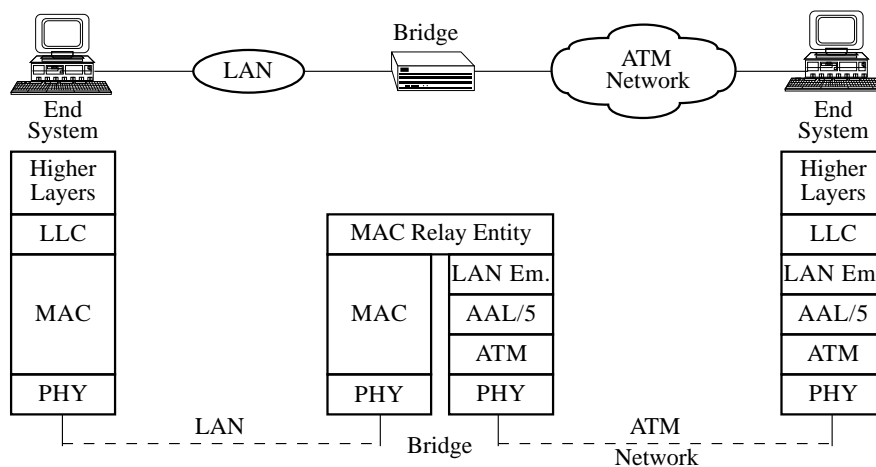
Un vantaggio di questo approccio è la totale trasparenza non solo ai protocolli di livello superiore (IP, OSI, IPX, ecc.), ma anche ai vari AAL e quindi ai vari tipi di applicazione (video, voce e dati). Inoltre, essendo l'internetworking effettuato dall'hardware degli switch, le prestazioni sono molto elevate. Per quanto concerne i limiti, oltre a quello già citato per cui le due reti da interconnettersi devono essere entrambe in tecnologia ATM, occorre evidenziare i potenziali problemi di sicurezza nel caso che una delle reti ATM sia un servizio pubblico che offre la possibilità di stabilire SVC.



**Fig. 21.1** - Internetworking mediante switch ATM.

### 21.2.2 Internetworking mediante bridge

Per interconnettere una rete locale con una rete ATM, il livello più basso a cui effettuare l'internetworking è quello dei bridge IEEE 802.1D (si veda il capitolo 11). Abbiamo già trattato questa soluzione nel capitolo 20, mostrando come, per colmare le differenze tra le due tecnologie, occorra far ricorso ad un servizio di "LAN Emulation". La figura 21.2 mostra un esempio di internetworking effettuato a tale livello e la stratificazione software corrispondente.



**Fig. 21.2** - Internetworking mediante bridge.

Le prestazioni di questa soluzione continuano a rimanere elevate (i bridge elaborano poco - e quindi velocemente - i pacchetti), è ovviamente possibile trasferire solo dati (non voce o video in tempo reale), ma viene mantenuta la trasparenza ai protocolli di livello superiore. Il livello di sicurezza offerto da questa soluzione non è significativamente maggiore di quello della soluzione precedente.

Inoltre questa soluzione, come la precedente, tende a creare delle LAN emulate di grandi dimensioni che spesso non possono essere usate in modo efficace dai protocolli di alto livello. Ad esempio, il protocollo IP ha la necessità di definire una corrispondenza tra le subnet IP e le LAN e spesso le network IP hanno una netmask 255.255.255.0 (si veda il paragrafo 16.5) che impone una dimensione massima della subnet IP, e quindi della LAN, pari a 256 indirizzi.

### 21.2.3 Internetworking mediante router

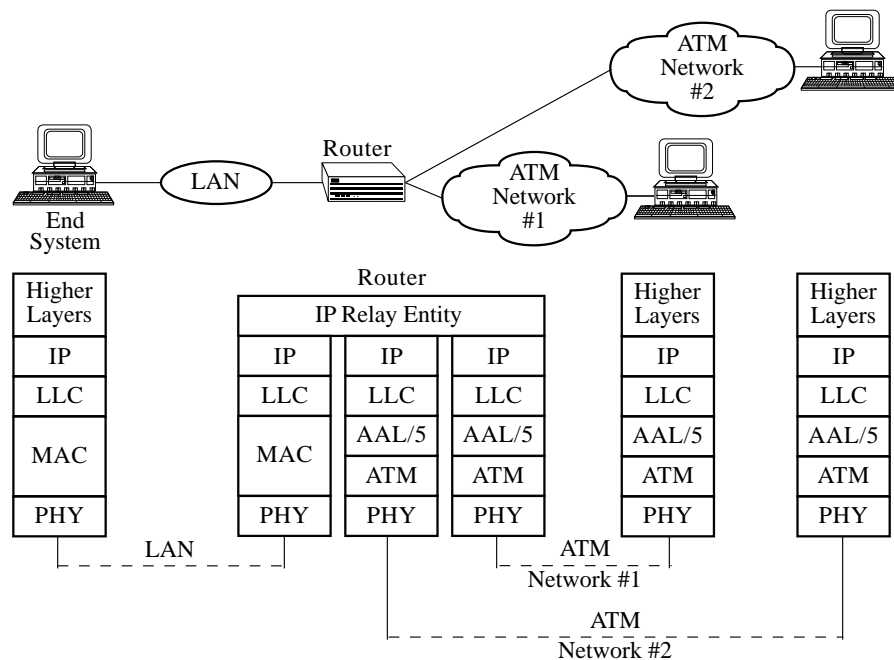
L'ultima possibilità è offerta dall'utilizzo dei router e risulta la più idonea quando si debbano affrontare topologie magliate complesse, in cui sono presenti mezzi trasmissivi differenziati. Inoltre, l'utilizzo di router permette di affrontare meglio i problemi della sicurezza, anche se in linea di principio tende a penalizzare le prestazioni. Infatti se si considera la stratificazione dei protocolli in figura 21.3 si vede che, nel caso un router interconnetta due reti ATM, esso deve ricostruire la trama IP partendo dalle celle ATM, determinarne l'instradamento e quindi riframmentare il pacchetto IP in celle ATM. Questo è costoso e non introduce alcun vantaggio se non quello di non modificare i protocolli esistenti.

### 21.2.4 Osservazioni

Guardando al futuro delle reti e dell'internetworking vedremo una sempre maggior quantità di reti ATM interconnesse tra di loro direttamente a livello ATM, cioè tramite switch. Questa struttura crea la possibilità di poter stabilire circuiti virtuali diretti tra coppie qualsiasi di nodi, i quali attraversano i confini delle subnet IP. In base a quanto discusso nel capitolo 16, questo è da considerarsi una violazione del Modello IP Classico in cui due subnet IP separate possono comunicare solo attraverso un router.

Per risolvere tale problema sono possibili due approcci. Il primo mira ad ammettere la connettività diretta, anche se questa supera i limiti delle subnet IP,

sfruttando le possibilità offerte da certe reti NBMA, tra cui ATM. In pratica, si tratta di estendere l'Address Resolution Protocol (ARP) oltre ai limiti della subnet IP.



**Fig. 21.3** - Internetworking mediante router.

Il secondo si basa su *IP routing* e *IP forwarding*, cioè sull'interconnessione tramite router modificati di subnet IP. Questo secondo approccio deve sempre essere scelto quando:

- le dimensioni dell'internetworking sono significative;
- si utilizzano mezzi trasmissivi differenziati, non essendo possibile utilizzare un'unica tecnologia di rete;
- ragioni di affidabilità non consentono di utilizzare una topologia stellare ed impongono una topologia magliata.

Questi due approcci richiedono comunque la risoluzione di un insieme di problemi comuni che verranno descritti nel prossimo paragrafo. In particolare occorre considerare che le stazioni ATM continueranno probabilmente ad essere multiprotocollo e quindi ad avere la necessità di trasmettere e ricevere, oltre ai pacchetti IP, anche quelli di altri protocolli, quali DECnet, IPX, OSI, ecc.

Occorre infine sottolineare che era stata tentata una classificazione degli approcci di IP su ATM differenziandoli per LAN, MAN, WAN. Tale classificazione è stata abbandonata in quanto impropria: la distanza nelle reti ATM incrementa il ritardo di propagazione e diminuisce le prestazioni, ma non cambia sostanzialmente l'organizzazione della rete stessa e le problematiche gestionali o di instradamento del traffico.

### 21.3 INCAPSULAMENTO ED IDENTIFICAZIONE DEI PROTOCOLLI

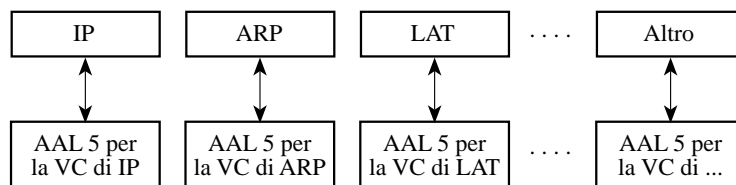
L'incapsulamento dei pacchetti e l'identificazione dei punti terminali dei circuiti virtuali sono due problematiche comuni a tutti gli approcci e indipendenti dalle considerazioni di topologia e di routing.

#### 21.3.1 VC multiplexing

Nello standard UNI [9] è previsto che il punto di terminazione di una VC sia stabilito durante la fase di call setup. Un approccio semplice è il *VC multiplexing* o *null encapsulation* che prevede di terminare una VC tramite una istanza di AAL5 direttamente su un protocollo di livello 3 (si veda la figura 21.4). Ad esempio, nel caso dell'architettura TCP/IP, la terminazione della VC è il protocollo IP, si pone cioè direttamente il pacchetto IP all'interno della AAL-SDU.

La realizzazione del VC multiplexing è trattata nello RFC 1483 [2] e nello RFC 1755 [14].

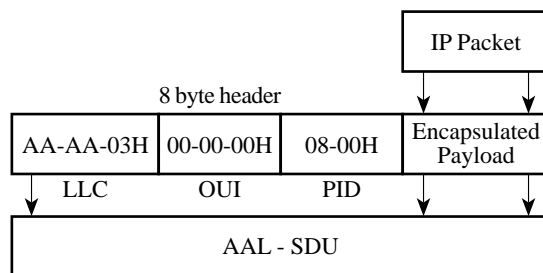
Questo approccio è limitativo in ambienti multiprotocollo dove ogni protocollo richiede la creazione di una VC separata e questo crea un carico di lavoro notevole sugli switch ATM per l'apertura e la chiusura delle VC.



**Fig. 21.4** - Reti multiprotocollo mediante VC multiplexing.

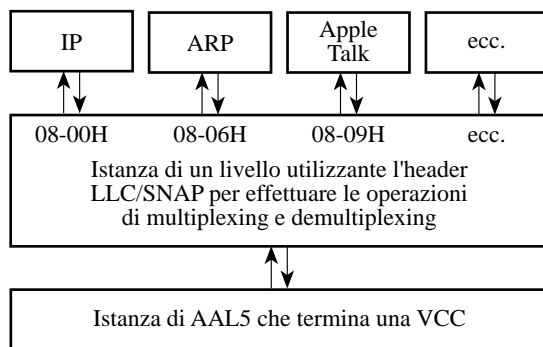
### 21.3.2 Incapsulamento LLC/SNAP

Lo RFC 1483 [2], pur ammettendo il VC multiplexing, propone un approccio alternativo definito *LLC/SNAP encapsulation*. Tale approccio è un adattamento ad ATM di quanto sviluppato nel progetto IEEE 802 e descritto nel paragrafo 5.7.4. Esso consente di trasportare un numero arbitrario di protocolli all'interno di una singola VC, differenziandoli tramite un header LLC/SNAP (la figura 21.5 mostra il trasporto di pacchetti IP su ATM e può essere paragonata con la figura 5.10 che mostra il trasporto di pacchetti IP su LAN IEEE 802).



**Fig. 21.5** - Incapsulamento LLC/SNAP.

La figura 21.6 mostra un esempio di più protocolli di derivazione Ethernet (OUI = 00-00-00H) che condividono la stessa VC e vengono differenziati in funzione del valore del campo PID (Protocol IDentifier).



**Fig. 21.6** - Condivisione di una VC tramite LLC/SNAP.

### 21.3.3 Altri metodi di incapsulamento

Il gruppo di lavoro "IP over ATM" ha discusso anche altri metodi di incapsulamento oltre a quelli definiti nello RFC 1483. Tali metodi hanno la caratteristica di eliminare, in larga parte o totalmente, l'overhead dovuto all'header dei pacchetti IP. Infatti, una volta stabilita la VC, gran parte dell'header IP diviene inutile: in particolare gli indirizzi del mittente e del destinatario, non sono più necessari ai fini dell'instradamento del pacchetto.

Sono stati proposti due approcci di incapsulamento che riducono o eliminano l'header IP:

- il primo è denominato TULIP (*TCP and UDP over Lightweight IP*);
- il secondo è noto come TUNIC (*TCP and UDP over Nonexistent IP Connection*).

#### TULIP

L'approccio TULIP prevede di conservare unicamente il campo indicante il tipo di protocollo di livello 4 trasportato dal pacchetto. Infatti, una volta stabilita una SVC tra due ES, viene a crearsi un collegamento implicito tra le loro entità IP (si veda la figura 21.7) e molti campi dell'header IP possono essere eliminati.

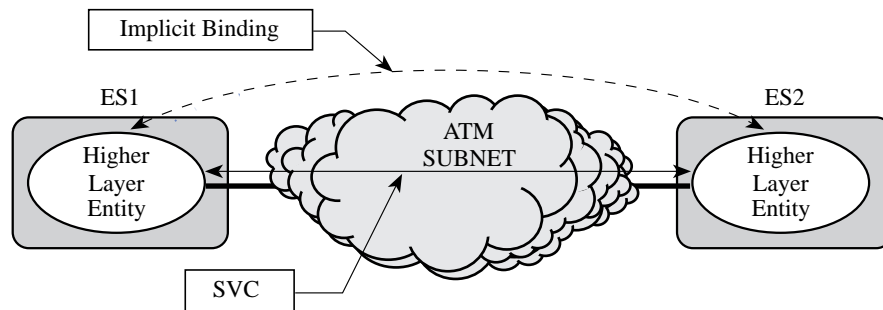


Fig. 21.7 - I modelli TULIP e TUNIC.

Infatti:

- non sussistono ulteriori problemi di instradamento, quindi gli indirizzi IP di mittente e destinatario non servono più;
- la lunghezza di ciascun pacchetto IP è indicata dal campo *length* della CPCS-PDU che lo contiene, quindi il campo corrispondente dell'header IP può essere eliminato;



- non avviene la frammentazione in quanto il campo *payload* della CPCS-PDU può contenere un pacchetto IP di dimensione massima (64 K ottetti);
- le condizioni eccezionali possono essere gestite mediante la segnalazione ATM.

TULIP non altera in alcun modo l'architettura di TCP/IP poiché ciascun ES continua a possedere il proprio indirizzo IP e le decisioni sull'instradamento continuano ad essere prese in funzione di tale indirizzo. Viene sfruttata unicamente la caratteristica di ATM di fornire canali di comunicazione end-to-end di tipo punto-punto al fine di eliminare gran parte dell'overhead associato a ciascun pacchetto IP.

## TUNIC

L'incapsulamento TUNIC prevede addirittura l'eliminazione dell'intero header IP da ogni pacchetto, assumendo che sussista tra le entità TCP o UDP il collegamento implicito tra due ES, dopo la creazione di una VC. In effetti si tratta di un approccio simile al VC multiplexing spinto ad un livello superiore, ovvero invece di dedicare una VC ad ogni protocollo di livello 3, nel caso di TUNIC viene dedicata una VC a ciascun protocollo di livello 4.

La tabella 21.1 riporta un confronto tra le varie metodologie di incapsulamento\*.

Incapsulamento	Informazioni "in banda"	Informazioni "fuori banda"
LLC/SNAP	Indirizzi sorgente e destinazione, famiglia di protocolli di livello 3, protocollo di livello 4, porte di accesso ai servizi	Nulla
VC multiplexing	Indirizzi sorgente e destinazione, protocollo di livello 4, porte di accesso ai servizi	Famiglia di protocolli di livello 3
TULIP	Protocollo di livello 4, porte di accesso ai servizi	Indirizzi sorgente e destinazione, famiglia di protocolli di livello 3
TUNIC	nulla	Indirizzi sorgente e destinazione, famiglia di protocolli di livello 3, protocollo di livello 4, porte di accesso ai servizi

**Tab. 21.1** - Metodi di incapsulamento.

\* Le espressioni "in banda" e "fuori banda" derivano del gergo in uso presso la telefonia classica e stanno ad indicare due tecniche di segnalazione. La segnalazione in banda è quella effettuata nella stessa banda di frequenze utilizzate per il segnale vocale (es. segnalazione a toni); nella segnalazione fuori banda, l'informazione di segnalazione è veicolata in una banda di frequenze disgiunta da quella destinata al segnale vocale (es. segnalazione ad impulsi in banda base).

## 21.4 IL MODELLO IP CLASSICO APPLICATO ALLE RETI ATM

L'adattamento del Modello IP Classico alle reti ATM è specificato nello RFC 1577 [12].

Il Modello IP Classico assume che a reti distinte a livello Data Link siano assegnate subnet IP differenti. In particolare si introduce il concetto di *Logical IP Subnetwork* (LIS), ovvero di un insieme di host e router che soddisfano i seguenti requisiti:

- tutti i membri di una LIS (host o router) sono posti sotto il controllo di una singola autorità amministrativa che provvede alla loro gestione e configurazione;
- tutti i membri di una LIS devono condividere la stessa subnet IP e la stessa netmask;
- tutti i membri di una LIS devono essere collegati direttamente alla stessa rete ATM affinché possano comunicare direttamente tra di loro per mezzo di SVC (topologia a maglia completa);
- in ogni LIS deve essere disponibile un meccanismo di risoluzione di indirizzi IP in indirizzi ATM e viceversa affinché sia possibile, all'occorrenza, creare le SVC tra i vari membri;
- tutti gli host di una LIS devono poter accedere ad un router di default che consenta loro di comunicare con destinazioni esterne alla LIS.

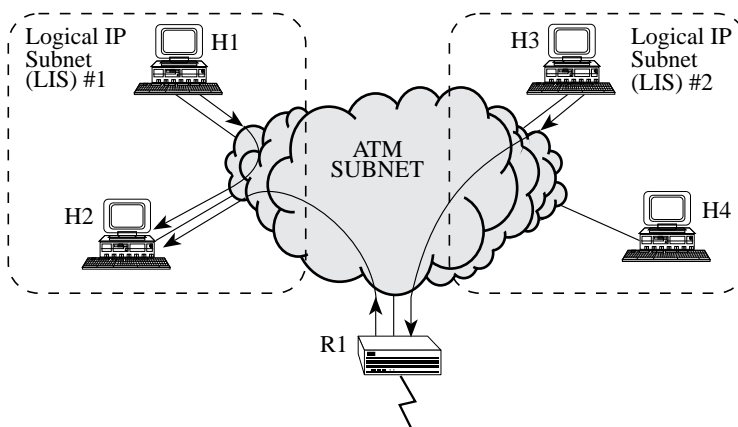
Le comunicazioni tra gli host avvengono in base alle seguenti regole (le esemplificazioni fanno riferimento alla figura 21.8):

- host facenti parte della stessa LIS (destinazione "locale") possono comunicare direttamente tra loro attraverso una apposita SVC (es. H1 ed H2);
- un host può comunicare con altri host all'esterno della propria LIS (destinazione "remota") unicamente rivolgendosi al proprio router di default affinché effettui l'instradamento dei pacchetti verso la destinazione finale, anche quando entrambi gli host sono collegati alla stessa rete ATM (es. H2 ed H3 che comunicano attraverso R1\*).

Esattamente come nelle subnet IP classiche, la decisione sul fatto che la destinazione sia "locale" o "remota" viene presa sulla base del confronto tra l'indirizzo IP del mittente e della destinazione (si veda il paragrafo 16.5).

---

\* Si noti che un router può configurare più interfacce "logiche" connesse a subnet IP diverse su un'unica interfaccia ATM.



**Fig. 21.8** - Modello IP Classico in ambiente ATM.

L'esempio riportato in figura 21.8 è concettualmente analogo a quello di figura 16.6 con la differenza che nel primo tutti gli host ed i router sono collegati alla medesima infrastruttura trasmissiva ATM; nonostante ciò, siccome gli host appartengono a subnet IP (o meglio LIS) differenti, le comunicazioni continuano ad avere luogo esattamente come in figura 16.6, ove le subnet IP sono invece fisicamente distinte.

L'adattamento del Modello IP Classico alle reti ATM dal punto di vista architetturale risulta essere una soluzione semplice in quanto introduce un numero limitato di modifiche, ma dal punto di vista delle prestazioni non sembra essere il più appropriato in quanto, come sarà evidenziato nei seguenti paragrafi, tende a sfruttare il substrato ATM in modo non ottimale.

Il Modello IP Classico, per essere realizzato su reti ATM, necessita di una definizione della Maximum Transmission Unit (MTU) (paragrafo 21.5), di un meccanismo per la risoluzione degli indirizzi IP in indirizzi ATM (paragrafo 21.6) e di opportune procedure di segnalazione (paragrafo 21.7).

## 21.5 DEFINIZIONE DELLA MTU DI IP SU RETI ATM

Lo RFC 1626 [8] fissa per la *Maximum Transmission Unit* (MTU) del protocollo IP su reti ATM un valore di default pari a 9180 ottetti. Tale valore è stato scelto in base alle seguenti argomentazioni:

- lo RFC 1209 definisce per la MTU di IP su SMDS un valore di default pari a 9180 ottetti; pertanto, ai fini dell'interoperabilità SMDS - ATM è opportuno che i pacchetti IP abbiano le stesse dimensioni;

- la maggior parte dei protocolli e degli applicativi che si appoggiano su TCP/IP, come ad esempio NFS (Network File System), generano PDU di notevoli dimensioni (tipicamente nell'ordine degli 8 KB). Affinché i pacchetti IP in cui esse sono incapsulate non vengano frammentati, è necessario che la MTU di IP su ATM abbia dimensioni non inferiori a quelle di dette PDU;
- i router IP offrono migliori prestazioni se operano su pacchetti di grosse dimensioni dal momento che l'overhead computazionale che essi introducono dipende in misura maggiore dal numero di pacchetti instradati piuttosto che dal numero di byte trasmessi.

Nelle reti ATM, aggiungendo alla dimensione di default della MTU di IP (9180 ottetti) gli otto ottetti dell'header LLC/SNAP si ottiene una dimensione della AAL-SDU (e quindi della CPCS-SDU) pari a 9188 ottetti. Quindi all'atto dell'attivazione di una SVC, se l'ES chiamante desidera utilizzare la dimensione di default della MTU, dovrà specificare nel messaggio di setup il valore 9188.

## 21.6 RISOLUZIONE DEGLI INDIRIZZI

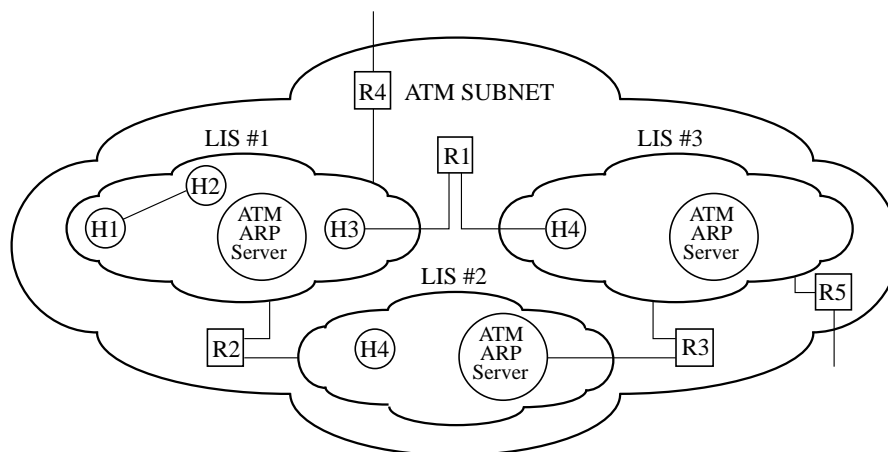
Lo RFC 1577 [14] stabilisce che la risoluzione degli indirizzi nell'ambito di una LIS realizzata tramite una rete ATM debba essere effettuata mediante i protocolli:

- *ATM Address Resolution Protocol* (ATMARP), per quanto concerne la risoluzione diretta (da indirizzi IP ad indirizzi ATM);
- *Inverse ATM Address Resolution Protocol* (InATMARP), per quanto concerne la risoluzione inversa (da indirizzi ATM ad indirizzi IP).

Tali protocolli, pur essendo funzionalmente identici alle versioni standard ARP ed InARP, dal punto di vista implementativo sono invece differenti poiché:

- ARP ed InARP basano il loro funzionamento sull'utilizzo di trasmissioni broadcast;
- ATMARP ed InATMARP devono necessariamente ricorrere ad un *ATMARP server* (figura 21.9), dal momento che si trovano ad operare in un ambiente caratterizzato da connessioni punto-punto quale quello ATM.

L'ATMARP server è la sede della tabella di corrispondenza tra indirizzi IP ed indirizzi ATM di tutti i membri della LIS (*ATMARP client*) in cui opera; esso, basandosi su detta tabella, ha la responsabilità di rispondere ad ogni richiesta di risoluzione di indirizzo proveniente da un qualunque client della LIS servita. Si noti che in una LIS può operare un solo ATMARP server, mentre quest'ultimo può servire contemporaneamente più LIS.



**Fig. 21.9** - Modello IP Classico in ambiente ATM.

L'implementazione di ATMARP ed InATMARP si differenzia a seconda del tipo di connessioni virtuali fornite dalla rete ATM.

Se la rete ATM fornisce unicamente connessioni virtuali permanenti, la risoluzione diretta degli indirizzi non è necessaria: esiste una corrispondenza biunivoca ed "immutabile" tra connessioni virtuali e indirizzi IP di destinazione. Ogni stazione crea e mantiene una tabella di corrispondenza tra indirizzi IP e identificatori di connessione virtuale (VCI/VPI) inviando richieste InATMARP su ciascuna delle connessioni virtuali. Dal momento che le entry di tale tabella devono essere sottoposte ad ageing al fine di garantirne un costante aggiornamento, la procedura sopra descritta si ripete periodicamente.

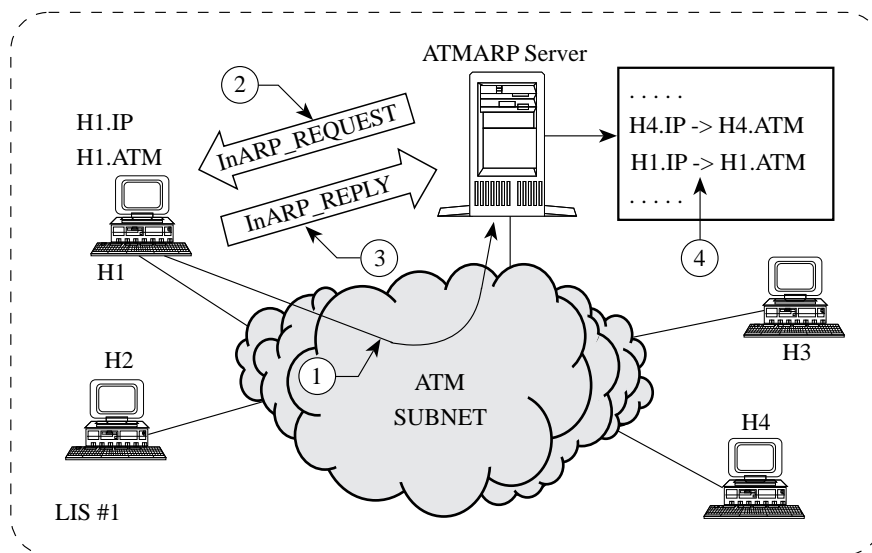
Se invece la rete ATM fornisce connessioni virtuali commutate, le procedure di risoluzione degli indirizzi, sia diretta, sia inversa, sono essenziali ai fini del routing nell'ambito della LIS.

### 21.6.1 Il server ATMARP

Un ATMARP server costruisce ed aggiorna dinamicamente la tabella di corrispondenza come segue:

- quando un client stabilisce una connessione con il server, il server invia subito al client una richiesta InATMARP (InARP\_REQUEST) in modo da determinarne l'indirizzo IP (figura 21.10);

- quando giunge la risposta dal client (InARP\_REPLY), il server, che era già a conoscenza dell'indirizzo ATM del client avendolo ricevuto durante la procedura di segnalazione, inserisce oppure aggiorna una entry del tipo <Client\_ATM\_Address, Client\_IP\_Address> nella tabella;
- alla entry è inoltre associato l'identificatore della connessione virtuale (VCI/VPI) dalla quale è pervenuta la richiesta, nonché un timestamp da utilizzarsi ai fini dell'ageing della stessa.

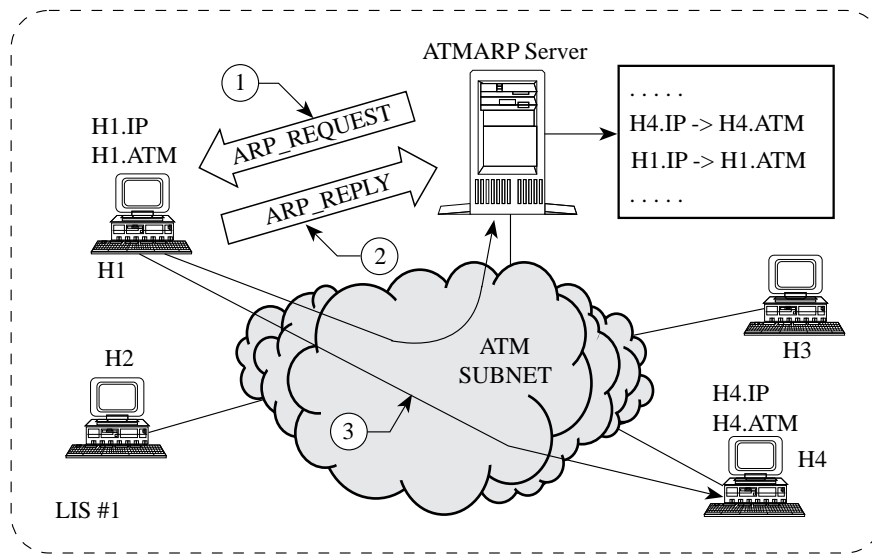


**Fig. 21.10** - Registrazione di ATMARP client.

Quando il server ATMARP (figura 21.11) riceve una richiesta di risoluzione di indirizzo diretta (ARP\_REQUEST), esso può generare due tipi di risposte:

- ARP\_REPLY: è la risposta positiva, contenente l'indirizzo ATM richiesto; essa viene restituita se nella tabella esiste una entry con l'indirizzo IP ricevuto nella richiesta;
- ARP\_NAK: è la risposta negativa nel caso contrario.

La risposta negativa, non prevista originariamente da ARP, consente al client di capire se il server è fuori servizio (nessuna risposta ricevuta), oppure se la destinazione non appartiene alla LIS o non ha ancora contattato il server (ARP\_NAK).



**Fig. 21.11** - ATMARP server: risoluzione indirizzo.

### 21.6.2 Il client ATMARP

Ogni client ATMARP mantiene una tabella locale (cache) contenente le ultime risposte ottenute dal server. Quando il client deve tradurre un indirizzo per prima cosa consulta la tabella locale: se non trova la risposta contatta l'ATMARP server e aggiorna la tabella locale con la risposta ottenuta.

### 21.6.3 Ageing delle tabelle ATMARP

Sia il server che i client devono tenere costantemente aggiornate le proprie tabelle ATMARP. Le entry della tabella del server sono valide per 20 minuti, mentre quelle delle tabelle dei client lo sono per 15 minuti.

Prima di eliminare una entry scaduta, il server deve generare una richiesta InARP\_REQUEST su ogni connessione virtuale associata a tale entry. Se giunge una risposta InARP\_REPLY, la entry viene ripristinata, in caso contrario, oppure se non vi sono connessioni associate alla entry, essa viene cancellata.

#### 21.6.4 Trasporto dei pacchetti ATMARP e InATMARP

I pacchetti generati dai protocolli ATMARP e InATMARP devono essere trasportati sulla rete ATM esattamente come i pacchetti IP, ossia mediante il metodo dell'incapsulamento LLC/SNAP (occorre utilizzare come EtherType il valore assegnato ad ARP: 08-06H).

#### 21.7 ASPETTI DI SEGNALAZIONE ATM

In un ambiente caratterizzato da connessioni virtuali commutate due stazioni devono poter stabilire e rilasciare connessioni in funzione del traffico. In ATM questo è possibile grazie al protocollo di segnalazione UNI [9] che dalla versione 3.0 in poi fornisce questa prestazione. Le procedure definite da tale protocollo consentono alla rete di localizzare un destinatario per mezzo del suo indirizzo ATM, di riservare le risorse da destinarsi alla connessione in via di apertura e di svolgere eventualmente negoziazione di parametri tra le stazioni.

Un end system IP connesso ad una rete ATM deve ricorrere alla segnalazione per l'apertura di una connessione virtuale qualora desideri inviare un pacchetto ad un altro end system IP e:

- non esista alcuna connessione stabilita in precedenza;
- esista una connessione aperta, ma questa non possa essere utilizzata (ad esempio perchè caratterizzata da una *Quality of Service* (QoS) non adatta al traffico IP).

Una connessione può invece essere abbattuta mediante segnalazione sia dalla stazione chiamante sia dalla chiamata. È importante che una connessione venga rilasciata dopo l'uso poiché nelle reti pubbliche esiste tipicamente un sistema di tariffazione in base al tempo di utilizzo delle connessioni. Per questo motivo ogni stazione che si interfaccia con reti pubbliche deve incorporare un meccanismo, basato su *inactivity timer*, che provochi la chiusura di quelle connessioni che sono rimaste inattive oltre il periodo di tempo prestabilito. Per le stazioni che operano su reti private il suddetto meccanismo di time-out è opzionale.

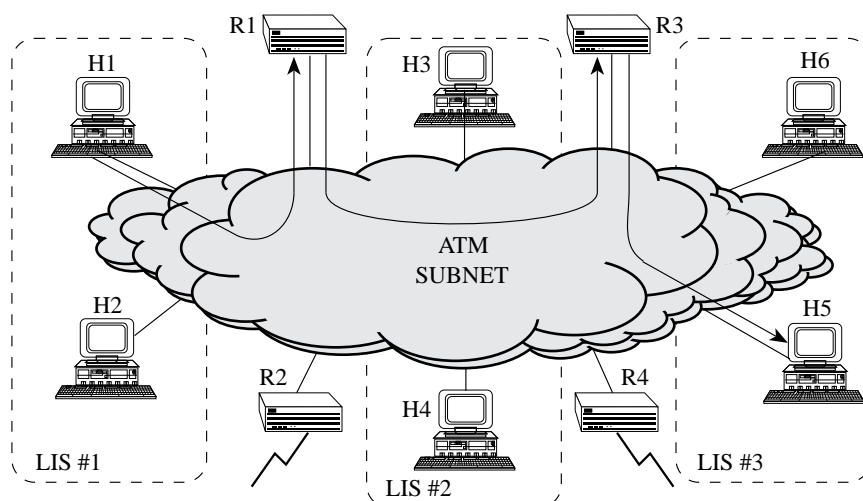
L'utilizzo del protocollo UNI da parte del protocollo IP è descritto nello RFC 1755 [14].



## 21.8 ROUTING E FORWARDING IP SU RETI ATM

Il Modello IP Classico su ATM, di cui si è discusso nel paragrafo 21.4, costituisce una soluzione valida solamente a breve termine in quanto, non comportando significative revisioni architetturali del TCP/IP, risulta essere di facile e rapida attuazione. In un'ottica di lungo periodo, tenendo conto che le esigenze delle applicazioni in termini di banda e di QoS sono in costante crescita, il paradigma di forwarding hop-by-hop\* caratteristico del Modello IP Classico risulta invece inadeguato. In particolare tale modello presenta limitazioni intrinseche che sono alla base di un utilizzo inefficiente dell'infrastruttura trasmissiva ATM, tra cui:

- forwarding dei pacchetti IP lungo cammini non ottimali (figura 21.12);
- banda limitata ed elevata latenza a causa dei ritardi introdotti dai router;
- incapacità di sfruttamento di caratteristiche quali banda garantita e QoS tipiche dell'ambiente connection oriented.



**Fig. 21.12** - Esempio di cammino end-to-end non ottimo.

Risulta quindi necessario individuare modelli architetturali caratterizzati da una maggiore flessibilità, capaci di sfruttare appieno le potenzialità intrinseche

\* Con il termine hop si indica una tratta trasmissiva tra due stazioni (si veda il paragrafo 14.6); con il termine single-hop un cammino end-to-end composto da una singola tratta trasmissiva; con il termine hop-by-hop un cammino composto da più tratte trasmissive collegate da router.

della tecnologia ATM. L'obiettivo fondamentale di tali modelli deve essere quello di permettere la comunicazione diretta a livello Data Link tra qualunque coppia di sistemi collegati ad una rete ATM, indipendentemente dalla LIS a cui appartengono. L'eliminazione degli hop ridondanti si traduce in un duplice vantaggio:

- miglioramento nelle prestazioni, dal momento che non si hanno più elaborazioni intermedie a livello IP;
- abbattimento dei costi, dovuto all'eliminazione di router non necessari.

Ai fini della sicurezza, tuttavia, la connettività diretta a livello Data Link non è sempre desiderabile: talvolta un hop aggiuntivo è necessario perché il router ad esso corrispondente opera come un firewall (barriera antintrusione).

In generale si possono individuare tre casi di ottimizzazione locale dei cammini. Qualunque siano gli host  $H$  e  $H'$  ed i *router di frontiera*\*  $R_f$  e  $R'_f$  collegati alla stessa rete ATM, deve essere possibile realizzare i seguenti cammini end-to-end con un singolo hop:

- $H - H'$ : comunicazione diretta tra host per il trasporto del traffico interno alla rete ATM;
- $H - R_f$ : comunicazione tra host e router di frontiera per il traffico in ingresso/uscita dalla rete ATM;
- $R_f - R'_f$ : comunicazione tra router di ingresso e router di uscita per il traffico in transito nella rete ATM.

Una soluzione architetturale in grado di supportare le suddette ottimizzazioni deve inoltre possedere i seguenti requisiti:

- *interoperabilità*: host e router modificati in base alla nuova architettura di routing devono essere compatibili con tutti i dispositivi ancora conformi al Modello IP Classico;
- *praticità*: le modifiche al software di bordo devono essere ridotte al minimo e concentrate soprattutto nei router, dal momento che questi sono in numero notevolmente inferiore e gestiti in modo più centralizzato rispetto agli host;
- *robustezza*: la nuova architettura di routing deve essere robusta nei confronti di errori software, hardware e di comunicazione almeno quanto quella tradizionale;
- *sicurezza*: la nuova architettura deve offrire almeno gli stessi standard di sicurezza presenti in quella tradizionale.

---

\* Un router che interconnette tra loro due o più reti IP è detto *router di frontiera*. Nell'esempio di figura 21.7 i router di frontiera sono  $R_2$  e  $R_4$ , mentre i router  $R_1$  ed  $R_3$  non lo sono in quanto interconnettono subnet IP nell'ambito della stessa rete IP.

## 21.9 ALCUNE SOLUZIONI ARCHITETTURALI

Sinora sono state identificate quattro possibili soluzioni architetturali alle problematiche di routing e forwarding IP su reti ATM discusse nel paragrafo precedente:

- *Hop-by-hop redirection*. Tale approccio estende il meccanismo di redirection classico in modo da far collassare i cammini multi-hop nell'ambito della rete ATM in un cammino single-hop (paragrafo 21.10).
- *Routing esteso*. Si propone di modificare i protocolli di routing per consentire ai router di frontiera collegati ad una rete ATM di scambiarsi i rispettivi indirizzi ATM affinché possano stabilire VC dirette (paragrafo 21.11).
- *Estensioni al protocollo ARP*. Questo approccio mira ad estendere la funzionalità del protocollo ATM ARP all'esterno delle singole LIS, al fine di offrire un servizio che copra l'intera rete ATM. Un esempio di tale approccio è rappresentato dal protocollo NHRP (paragrafo 21.12).
- *Router con capacità di commutazione di cella ATM*. Il quarto ed ultimo approccio propone una modifica all'hardware dei router in modo da consentire a tali dispositivi di "saldare" tra loro i segmenti dei cammini che li attraversano; ciò permette di realizzare cammini end-to-end filtrati a livello IP, ma unificati a livello ATM (paragrafo 21.13).

### 21.10 HOP-BY-HOP REDIRECTION

L'approccio hop-by-hop redirection tende ad eliminare tutti gli hop non necessari contenuti in un cammino end-to-end tra due sistemi collegati alla stessa rete ATM. Tale schema si basa sulla seguente idea: quando al primo router lungo il cammino giunge un pacchetto dal mittente, esso, dopo aver concluso che l'hop successivo si trova anch'esso all'interno della rete ATM, invia al mittente un messaggio XRedirect (*eXtended Redirect*, una estensione al protocollo ICMP\*). Il mittente può a questo punto inviare il pacchetto successivo all'indirizzo specificato

---

\* ICMP (*Internet Control Message Protocol*) è un protocollo che consente a router ed host di scambiarsi informazioni di servizio quali messaggi di errore, controllo e configurazione. Il messaggio redirect è uno dei più importanti in quanto è alla base del meccanismo di *redirection*. Tale messaggio consente infatti ad un router che riceve un pacchetto destinato ad un host collegato alla stessa subnet dell'host mittente, di segnalare a quest'ultimo che può raggiungere la destinazione desiderata direttamente.

nel messaggio XRedirect; se a tale indirizzo fa capo un altro router il cui attraversamento è inutile, anche questo router invierà al mittente un messaggio XRedirect. L'applicazione iterativa del suddetto procedimento presso tutti i router intermedi si conclude in un cammino single-hop tra mittente e destinazione.

Per realizzare lo schema hop-by-hop redirection occorre modificare il software di bordo dei router e degli host. La modifica principale deve essere apportata al protocollo ICMP affinché supporti il nuovo messaggio XRedirect. Non è possibile utilizzare il messaggio redirect convenzionale in quanto esso può trasportare unicamente gli indirizzi IP associati ai router, mentre lo schema hop-by-hop redirection necessita che i messaggi di redirezione contengano indirizzi IP ed ATM sia dei router sia degli host.

### 21.11 ROUTING ESTESO

Lo schema hop-by-hop redirection è applicabile solamente quando l'host mittente è membro della rete ATM in quanto è compito suo redirigere via via il proprio traffico, in base ai messaggi XRedirect, verso la destinazione finale. Dal momento che tali messaggi non vengono ricevuti dai router, si rende necessario estendere opportunamente i protocolli di routing con un meccanismo analogo. Solo in tal modo è possibile ottimizzare il forwarding del traffico di transito sulla rete ATM tra coppie di router di frontiera.

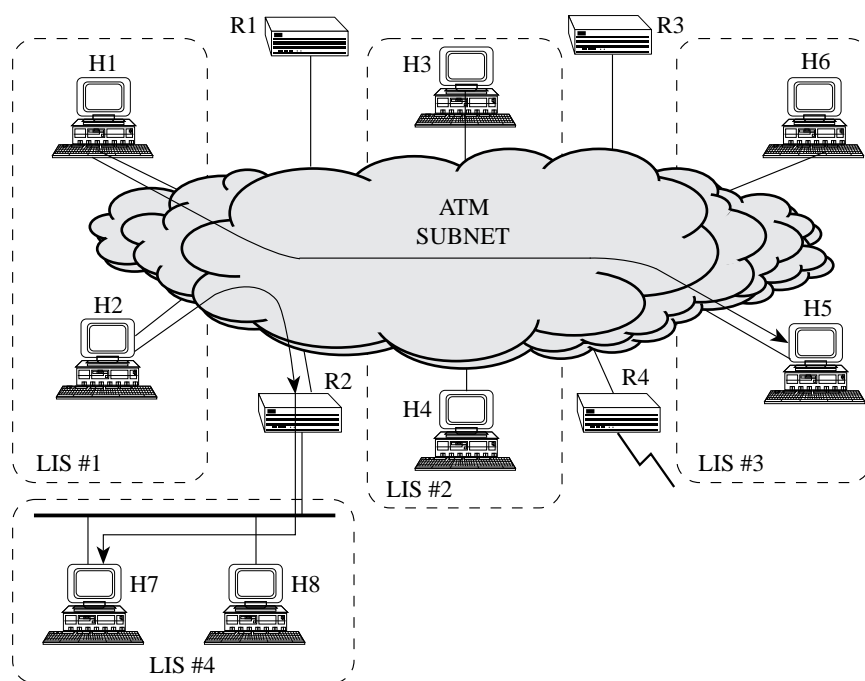
Facendo riferimento alla figura 21.12, supponiamo, ad esempio, che al router di frontiera R4 giunga dall'interfaccia non collegata alla rete ATM una serie di pacchetti destinati ad una rete facente capo all'altro router di frontiera R2. Supponiamo inoltre che la tabella di instradamento di R4 preveda che per raggiungere R2 esso debba fare riferimento ad R1. Sulla base di tale indicazione R4 invia il primo pacchetto a R1; quest'ultimo nota che il pacchetto è destinato ad R2 e che quest'ultimo è collegato alla stessa rete ATM di R4. Siccome il cammino R4 - R1 - R2 risulta non ottimale, R1 segnala ad R4, per mezzo di un opportuno messaggio del protocollo di routing esteso, di redirigere il proprio traffico verso R2 e fornisce contemporaneamente l'indirizzo ATM di quest'ultimo. In tal modo R4 può aggiornare la propria tabella di instradamento, cosicché tutti i pacchetti successivi siano inviati direttamente a R2.

### 21.12 NHRP: NEXT HOP RESOLUTION PROTOCOL

Una rete ATM di grandi dimensioni quale una SVC ATM WAN, è tipicamente ripartita in una pluralità di LIS indipendenti (si pensi ad esempio al caso di varie

ATM LAN, corrispondenti ciascuna ad una LIS, interconnesse mediante una SVC ATM WAN). Il protocollo ATMARP (paragrafo 21.6) consente di risolvere l'indirizzo IP di una destinazione (host o router) nel corrispondente indirizzo ATM solamente se questa appartiene alla LIS del mittente.

Ai fini del superamento della limitazione intrinseca al Modello IP Classico sopra evidenziata, il gruppo di lavoro ROLC (Routing Over Large Cloud) di IETF ha sviluppato il protocollo *NBMA Next Hop Resolution Protocol* (NBMA NHRP), un protocollo di routing e risoluzione degli indirizzi adatto a tutte le tecnologie di networking NBMA che, come ATM, non supportano trasmissioni broadcast [6], [11].



**Fig. 21.13** - Esempio di forwarding IP basato sul protocollo NHRP.

NBMA NHRP consente ad una stazione mittente (host o router) che deve comunicare attraverso una rete ATM di determinare gli indirizzi IP ed ATM del cosiddetto *next hop* verso la stazione di destinazione, noto l'indirizzo IP di quest'ultima. Se la destinazione fa parte della rete ATM del mittente, l'indirizzo del next hop restituito da NHRP sarà l'indirizzo ATM della destinazione stessa, altrimenti sarà quello del router di frontiera che si trova sul più breve cammino possibile (in termini di hop) tra mittente e destinazione. Una volta noto l'indirizzo ATM del next hop, la

stazione mittente può attivare una SVC con esso ed avviare la trasmissione di pacchetti IP. Ad esempio, facendo riferimento alla figura 21.13, per mezzo di NHRP, H1 è in grado di apprendere l'indirizzo ATM di H5 e quindi di stabilire una SVC con quest'ultimo invece di inviare i pacchetti lungo il cammino multi-hop H1 - R1 - R3 - H5 come accadeva in figura 21.7. Inoltre H2 viene informato che il "miglior" router di uscita per raggiungere H7 è R2 e non il router di default R1.

Il protocollo NHRP, eliminando dai cammini end-to-end tutti gli hop non necessari, permette di ottimizzare notevolmente il processo di forwarding di pacchetti IP nell'ambito di una rete ATM.

I paragrafi seguenti illustrano più in dettaglio le caratteristiche del protocollo NHRP.

#### 21.12.1 Descrizione del protocollo NBMA NHRP

Il protocollo NBMA NHRP necessita dell'installazione nell'ambito di una rete ATM di una o più entità note come *Next Hop Server* (NHS). Ciascun NHS serve un determinato insieme di host e router (*client*). Gli NHS, oltre a collaborare tra loro per la risoluzione di un next hop nell'ambito della loro rete ATM, possono partecipare a protocolli di routing per apprendere la topologia delle interconnessioni. Infine, gli NHS possono anche affiancarsi agli ARP server, condividendo eventualmente lo stesso hardware, in modo da realizzare una architettura di routing eterogenea in grado di supportare sia host NHRP-capable sia host che operano unicamente in base al Modello IP Classico.

Ciascun NHS gestisce una tabella di corrispondenza tra indirizzi IP ed indirizzi ATM dei client che serve, denominata *next hop resolution cache*, del tutto analoga a quella degli ARP server. Detta tabella può essere configurata manualmente oppure costruita ed aggiornata dinamicamente nei seguenti modi:

- mediante un processo di registrazione attuato dai client mediante l'invio al proprio NHS di un messaggio NHRP\_Register;
- estraendo le informazioni dalle richieste di risoluzione ricevute dai client attraverso il messaggio NHRP\_Request;
- estraendo le informazioni dalle risposte provenienti dagli altri NHS della rete tramite il messaggio NHRP\_Reply.

Si supponga ora che una stazione S debba determinare l'indirizzo ATM del next hop verso D. S si rivolge al proprio NHS inviandogli un messaggio NHRP\_Request. Il messaggio NHRP\_Request è incapsulato in un pacchetto IP e

trasmesso al NHS attraverso una VC creata all'atto della registrazione, oppure creata ad hoc per la trasmissione della richiesta.

Nel frattempo, in attesa della risposta da parte del NHS, S può procedere come segue:

- a) scartare il pacchetto che deve trasmettere a D;
- b) trattenere il pacchetto fino a quando non giunge la risposta del NHS;
- c) inviare il pacchetto al proprio router di default.

La scelta attuata dipende dalle politiche locali alla LIS cui S appartiene, anche se viene raccomandata la soluzione c) come scelta di default, in quanto consente che il pacchetto giunga comunque a D senza costringere S ad inutili attese. Ovviamente il processo di risoluzione non è attuato per ogni pacchetto trasmesso ad una data destinazione in quanto i client dispongono di una cache locale.

Quando il NHS riceve il messaggio NHRP\_Request proveniente da S verifica se nella propria cache è presente una entry contenente l'indirizzo ATM del next hop verso D. Se così non è, il NHS inoltra la stessa richiesta ad un altro NHS. La richiesta passa di NHS in NHS fino a quando non si verifica una delle seguenti condizioni:

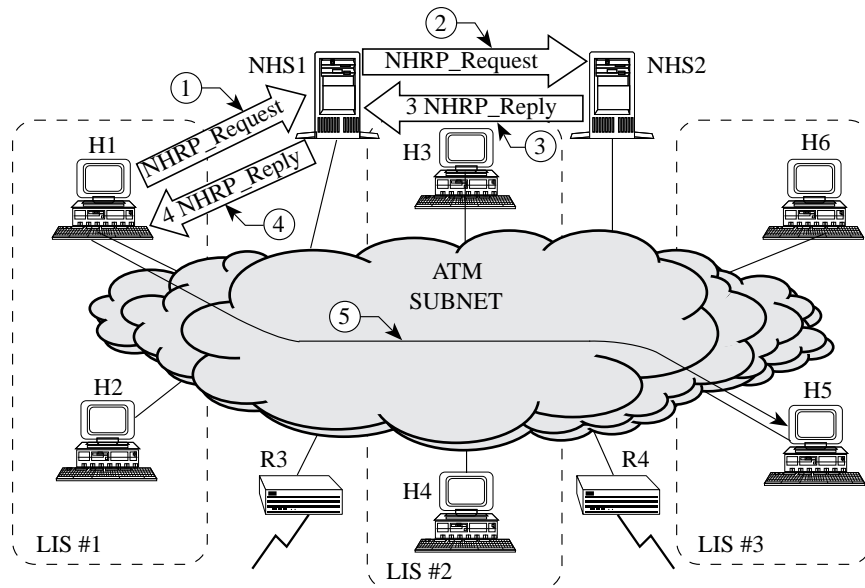
- la richiesta giunge al NHS che serve D. Quest'ultimo è in grado di evadere la richiesta generando un messaggio NHRP\_Reply contenente gli indirizzi IP ed ATM del next hop verso D. Ovviamente, se D non è collegato alla rete ATM, tale next hop D è l'indirizzo ATM del router di frontiera verso la rete su cui D risiede.
- nessun NHS è in grado di risolvere il next hop verso D. In tal caso l'ultimo NHS visitato genera un messaggio NHRP\_Reply di tipo negativo.

In entrambi i casi, il messaggio NHRP\_Reply viene inoltrato ad S lungo lo stesso cammino compiuto da NHRP\_Request affinché tutti gli NHS attraversati dalla risposta possano inserire nelle loro cache le informazioni in esso contenute. Questo fatto consente agli NHS di rispondere a richieste successive per lo stesso next hop mediante le cosiddette "risposte non autorevoli", ossia risposte che non provengono dal NHS presso cui il client si è registrato. Se un tentativo di comunicazione basato su una risposta non autorevole fallisce (probabilmente perché si sono verificate delle variazioni nella rete), la stazione mittente può inviare una nuova NHRP\_Request, richiedendo una risposta autorevole.

In figura 21.14 è rappresentata una situazione esemplificativa di quanto sopra descritto. L'host H1 intende trasmettere un pacchetto all'host H5, ma non ne conosce l'indirizzo ATM. Invia pertanto una NHRP\_Request a NHS1 il quale, tuttavia, non dispone di tale informazione. La richiesta viene inoltrata a NHS2 il

quale, essendo il NHS che serve H5, è in grado di generare una NHRP\_Reply con l'indirizzo ATM richiesto. Tale risposta, ritornando verso H1, attraversa NHS1 consentendo a quest'ultimo di copiare detto indirizzo nella propria cache per un futuro utilizzo come risposta non autorevole. La risposta giunge infine ad H1, il quale è ora in grado di stabilire una VC con H5 ed inviargli il pacchetto che aveva trattenuto in attesa della risposta.

NHRP consente inoltre di associare l'indirizzo ATM di un next hop ad una intera subnet IP. Ad esempio, se il router X è il next hop tra la stazione S e la stazione D, significa che X è il router di uscita da utilizzare per raggiungere tutte le altre stazioni che condividono lo stesso prefisso di subnet IP di D.



**Fig. 21.14** - Esempio di risoluzione dell'indirizzo ATM mediante NHRP.

### 21.12.2 Modalità di installazione

NHRP prevede due differenti modalità di installazione note come *fabric mode* e *server mode*. Le due modalità si distinguono unicamente nel modo di propagazione dei messaggi NHRP tra gli NHS. È opportuno che i client collegati alla rete ATM non siano a conoscenza del modo in cui NHRP opera, cosicché una variazione nella strategia di installazione possa avvenire in modo del tutto trasparente rispetto agli host.



## Server mode

L'installazione di NHRP in server mode presuppone che nell'ambito della rete ATM operi un numero non elevato di NHS e che l'accoppiamento tra NHRP ed il processo di forwarding IP sia molto debole; in particolare in questa modalità non sussiste alcun legame tra i cammini intrapresi dalle richieste attraverso gli NHS ed i cammini seguiti dai pacchetti IP verso destinazioni da questi servite.

Se la rete ATM supporta VC punto-multipunto, ciascun client potrebbe stabilire una VC avente come leaf node tutti gli NHS. In tal modo, una NHRP\_Request proveniente da un client solleciterebbe una o più NHRP\_Reply dai NHS, in funzione del tipo di risposta che il client si aspetta (autorevole o non autorevole). Tale approccio presenta il vantaggio di ridurre il numero di NHS attraversati da ogni richiesta ad uno solo, ma può risultare oneroso in termini di consumo di risorse della rete qualora i client siano numerosi.

L'inconveniente suddetto può essere eliminato connettendo ogni NHS a tutti gli altri tramite una VC punto-multipunto che l'NHS utilizza per effettuare il forwarding delle richieste che non è in grado di risolvere. Nuovamente, ad ogni NHRP\_Request inoltrata sulla VC punto-multipunto possono corrispondere una o più NHRP\_Reply in funzione del tipo di risposta che il richiedente si aspetta. Un simile approccio consente di ridurre il numero di NHS attraversati dalle richieste a due solamente e, siccome gli NHS sono pochi, non introduce sulla rete un eccessivo overhead dovuto alla gestione delle VC punto-multipunto.

## Fabric mode

L'installazione di NHRP in fabric mode prevede che gli NHS siano localizzati in tutti i router che collegano la rete ATM con il mondo esterno. Questo fatto implica che vi sia un forte accoppiamento tra NHRP ed il processo di forwarding IP, in particolare i cammini intrapresi dai messaggi NHRP\_Request verso gli NHS coincidono con i cammini dei pacchetti IP instradati secondo il Modello IP Classico.

Le richieste vengono esaminate da vari NHS/router attraversati sino a quando si verifica una delle seguenti situazioni:

- la NHRP\_Request giunge al NHS/router che serve la destinazione indicata: il NHS/router genera una NHRP\_Reply positiva;
- la NHRP\_Request giunge ad un NHS/router che non è in grado di inoltrarla ulteriormente poiché non conosce alcun cammino di instradamento verso la destinazione finale: il NHS/router genera una NHRP\_Reply negativa;

- la NHRP\_Request giunge ad un NHS/router che non è in grado di inoltrarla verso il NHS che serve la destinazione a causa dell'assenza di connettività con quest'ultimo: anche in questo caso il NHS/router genera una NHRP\_Reply negativa;

In ogni caso la NHRP\_Reply viene trasmessa al richiedente esattamente come è stato descritto per il server mode.

### 21.12.3 Configurazione di NHRP

Alla luce di quanto discusso nei paragrafi precedenti, emergono i seguenti requisiti di configurazione per NHRP:

- ciascun client, indipendentemente dal fatto che si tratti di un host o un router, deve essere configurato con gli indirizzi IP ed ATM di almeno un NHS;
- ogni NHS deve essere configurato con la propria identità e l'insieme di subnet IP servite;
- se NHRP opera in server mode, ciascun NHS deve essere anche configurato con gli indirizzi ATM ed IP di tutti gli altri NHS operanti all'interno della rete ATM;
- se NHRP opera in fabric mode, ciascun NHS che funge anche da router di frontiera per la rete ATM deve essere configurato in modo da poter partecipare ai protocolli di routing intra- ed inter-domain;
- gli NHS possono essere configurati con gli indirizzi ATM dei client da loro serviti sia staticamente (server mode), sia dinamicamente osservando i messaggi NHRP\_Request (fabric mode); un'ulteriore modalità di configurazione è basata sulla registrazione esplicita dei client attraverso i messaggi NHRP\_Register.

#### I client NHRP

I client devono ovviamente inserire nelle cache tutte le risposte che ricevono dai server. Devono essere inserite anche entry incomplete, ossia quelle corrispondenti a richieste non ancora evase. Ciò è necessario poiché le stazioni non devono effettuare ulteriori richieste per una data destinazione qualora ve ne sia già una pendente. Inoltre, le stazioni sono tenute a eliminare sia le entry per le quali è scaduto l'holding time, sia quelle indicate nei messaggi NHRP\_Purge ricevuti dagli NHS.

#### Gli NHS finali

Gli NHS che servono una destinazione devono inserire una entry nella propria

cache per tutte le risposte che hanno evaso con informazioni che potrebbero variare nel tempo. Ciò consente agli NHS di inviare un messaggio NHRP\_Purge alle stazioni nel momento in cui le suddette informazioni variano. Inoltre, gli NHS sono tenuti ad inserire una entry nella propria cache relativamente a ciascuna stazione dalla quale hanno ricevuto richieste di risoluzione. Tale entry deve essere eliminata allo scadere dell'holding time ad essa associato.

### Gli NHS di transito

Un NHS può inserire nella propria cache le informazioni relative alle richieste che instrada verso altri NHS e alle relative risposte. Gli NHS di transito possono rispondere direttamente a richieste non autorevoli, con informazioni tratte dalle proprie cache. Infine essi, come tutti gli altri sistemi NHRP, devono rimuovere tutte le entry per cui sia scaduto l'Holding Time.

### Dinamica delle cache

Lo scopo fondamentale di NHRP è quello di risolvere gli indirizzi IP delle stazioni direttamente connesse ad una rete ATM nei corrispondenti indirizzi ATM. Essendo tali associazioni tipicamente piuttosto statiche, una appropriata scelta degli holding time delle entry nelle varie cache tende a minimizzare sia il traffico di richieste e risposte, sia i problemi derivanti dalle variazioni di indirizzo.

Tuttavia, nel caso in cui una destinazione non sia collegata direttamente alla rete ATM, l'associazione tra l'indirizzo IP di quest'ultima e l'indirizzo ATM di un router di uscita verso la rete cui essa appartiene può anche essere molto più dinamica. Ciò provoca un aumento della probabilità che l'informazione presente in qualche cache sia inattendibile. In questo caso, però, la conseguenza di una entry non più valida non è la perdita di connettività con la destinazione, ma semplicemente un cammino di instradamento non ottimale.

È pertanto necessario che un router/NHS, accortosi di una variazione nel percorso di instradamento verso una certa destinazione, invii un messaggio NHRP\_Purge al mittente affinché elimini dalla propria cache la entry obsoleta ed effettui una richiesta autorevole per trovare un nuovo router di uscita.

## 21.13 CELL SWITCHING ROUTER

Un *Cell Switching Router* (CSR) è un apparato di internetworking che integra al suo interno le funzionalità di routing e forwarding IP e di commutatore di celle

ATM [5]. Grazie a dette capacità, un CSR è in grado, in funzione delle informazioni di routing IP, di concatenare una VC in ingresso con una VC in uscita, fornendo quindi connettività a livello ATM anche tra coppie di host che appartengono a LIS differenti, senza violare il Modello IP Classico.

### 21.13.1 Motivazioni

Le soluzioni architetturali illustrate nei paragrafi precedenti mirano ad eliminare dai cammini end-to-end tutti i router non indispensabili. Non è detto che tale scelta sia sempre la migliore; ad esempio, le funzionalità di forwarding IP tra LIS distinte continuano ad essere richieste nei seguenti casi:

- quando una stazione H1 intende comunque trasmettere pacchetti IP ad una destinazione H2 mentre è in corso la segnalazione per creare una VC diretta H1 - H2; ad esempio, H1 ha inviato una richiesta di risoluzione NHRP dell'indirizzo IP di H2 e, in attesa della risposta, inizia a spedire i pacchetti a H2 tramite un cammino multi-hop;
- quando le esigenze di banda e QoS di talune applicazioni non giustificano lo sforzo di creare una VC tra mittente e destinazione (paragrafo 21.14);
- quando la connettività diretta a livello ATM non è consentita esplicitamente da politiche inerenti la sicurezza.

Inoltre occorre tenere in seria considerazione l'interoperabilità con le tecniche di "*resource reservation*" (RSVP\* e STII\*\*) ed il concetto di "*flusso IP*" (IPv6\*\*\*). RSVP, STII e IPv6 mirano a fornire a livello IP banda e QoS garantite, in modo indipendente dalle reti fisiche sottostanti.

L'introduzione dei CSR è una soluzione diametralmente opposta a quelle viste in precedenza e consiste nell'adeguare il substrato trasmissivo ATM alle preroga-

---

\* RSVP (*Resource reSerVation Protocol*) è un protocollo che consente ad un host destinatario di "prenotare" l'utilizzo di risorse, in termini di banda dedicata priorità di servizio, presso i router attraversati dal traffico di pacchetti IP proveniente da un certo mittente.

\*\* STII (*STream protocol version II*) può essere considerato come una versione connection oriented di IP che necessita di una fase di creazione di una connessione tra un mittente ed una destinazione prima della trasmissione dei pacchetti. I router STII-compatibili dislocati lungo il cammino di tale connessione riservano quindi una quota delle loro risorse in accordo alle indicazioni fornite dal mittente.

\*\*\* IPv6 (*Internet Protocol version 6*), noto anche come IPng (*IP next generation*), è una evoluzione di IP che prevede nell'header un campo denominato *FlowID*. Come lascia intuire il nome stesso, tale campo indica la presenza di un flusso attivo di pacchetti e viene utilizzato dai router IPv6-compatibili per allocare le proprie risorse in funzione delle caratteristiche di detto flusso.

tive del Modello IP Classico. I CSR si fanno carico di fornire canali di comunicazione end-to-end a livello ATM anche tra host che non condividono la stessa subnet IP. Tale soluzione presenta i seguenti vantaggi:

- miglioramento delle prestazioni nel forwarding dei pacchetti IP in ambienti multi-LIS dovuto all'eliminazione della latenza introdotta dalle elaborazioni a livello IP presso i router;
- possibilità di fornire livelli di banda e QoS adeguati alle applicazioni odierne;
- supporto delle tecniche di resource reservation (RSVP e STII) e dei flussi IP (IPv6);
- conformità all'architettura originaria di TCP/IP che prevede un modello di internetworking imperniato sui router.

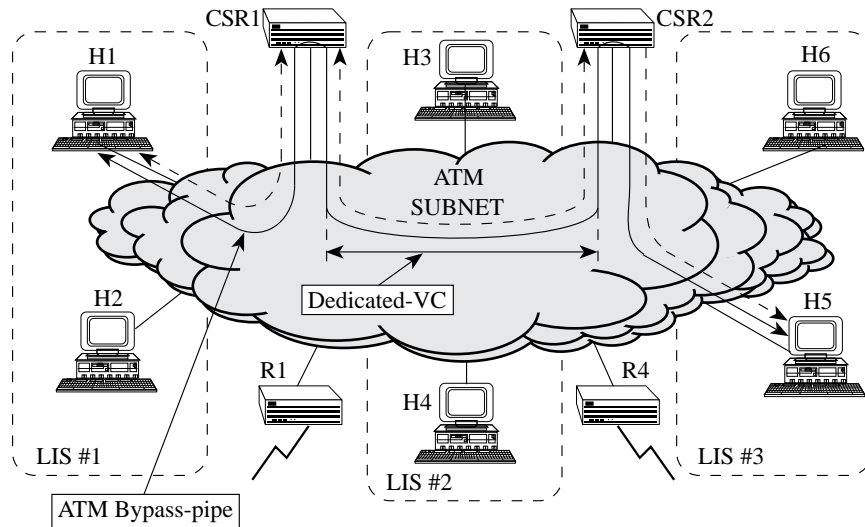
### 21.13.2 Architettura di internetworking basata su CSR

Dal punto di vista architetturale un CSR è simile ad uno switch ATM in quanto è in grado di commutare un flusso di celle proveniente da una VC di ingresso, a cui corrisponde un host mittente, in un flusso di celle su una VC di uscita, associata ad un host di destinazione. A differenza degli switch ATM, nei CSR la concatenazione dei flussi è sotto il controllo dell'entità che effettua il forwarding IP, ossia essa ha luogo solo qualora esista un flusso attivo di pacchetti IP tra mittente e destinazione. Se tale concatenazione avviene presso tutti i CSR attraversati da un cammino end-to-end che unisce mittente e destinazione, si realizza una cosiddetta *ATM bypass-pipe*, ovvero una successione di VC che connettono tra loro CSR adiacenti (nonché mittente e destinazione con i CSR più "vicini"). Il termine ATM bypass-pipe è stato coniato appositamente per distinguere il concetto ad esso sotteso da quello rappresentato dalla convenzionale VC ATM.

In figura 21.15 è mostrata una configurazione di networking basata su CSR. È possibile notare un cammino end-to-end tra gli host H1 e H5 che attraversa le LIS #1, #2 e #3, passando per due CSR. Tale cammino può essere supportato sia tramite una ATM bypass-pipe, sia mediante il convenzionale forwarding hop-by-hop, a seconda delle esigenze delle applicazioni. Infatti tra ciascuna coppia di nodi sono attive due classi di VC:

- *Default-VC*: sono VC utilizzate e condivise tra tutte le applicazioni per le quali il convenzionale forwarding IP hop-by-hop risulta adeguato. Tutti i pacchetti che giungono ai CSR attraverso tali VC sono elaborati a livello IP esattamente come avviene nel Modello IP Classico.

- *Dedicated-VC*: sono particolari VC che vengono concatenate tra loro presso i CSR al fine di costruire una ATM bypass-pipe dedicata ad una particolare applicazione.



**Fig. 21.15** - Esempio di internetworking basato su CSR.

Il cammino seguito da una ATM bypass-pipe dipende dalle tabelle di instradamento dei CSR, e quindi i pacchetti compiono lo stesso percorso dei pacchetti instradati hop-by-hop. Nel caso di figura 21.15, i pacchetti trasmessi dall'host H1 e destinati all'host H2 sono trasferiti lungo il cammino H1 - CSR1 - CSR2 - H2 indipendentemente dal fatto che la comunicazione avvenga hop-by-hop o attraverso una ATM bypass-pipe.

#### Gestione delle dedicated-VC

Vi sono tre possibili alternative per quanto concerne la gestione delle dedicated-VC:

- Creazione di una SVC on-demand.* Ogni volta che deve essere stabilita una ATM bypass-pipe, le dedicated-VC che la compongono vengono create sul momento mediante la normale procedura di segnalazione ATM. Quando la ATM bypass-pipe non serve più, le corrispondenti dedicated-VC vengono rilasciate.
- Uso di PVC.* Tra ogni coppia di CSR e tra questi ultimi e gli host, l'amministratore della rete preconfigura un certo numero di PVC. Quando occorre creare una ATM bypass-pipe, le dedicated-VC che costituiscono quest'ultima vengono scelte tra le PVC che in quel momento sono inutilizzate.

- c) *Uso di VCI liberi nell'ambito di PVP/SVP.* Tra ogni coppia di CSR e tra questi ultimi e gli host, vengono stabiliti un certo numero di PVP (*Permanent Virtual Path*) o SVP (*Switched Virtual Path*). I PVP possono essere configurati dall'amministratore della rete, mentre gli SVP vengono creati la prima volta che una VC (*dedicated-VC* o *default-VC*) deve essere creata tra due nodi. Quando occorre creare una ATM bypass-pipe, le *dedicated-VC* vengono create all'interno del PVP/SVP.

La scelta del metodo di gestione delle *dedicated-VC* dipende dal tipo di ottimizzazione che si desidera ottenere.

Nel caso a) viene ottimizzato l'uso delle risorse di rete in quanto le *dedicated-VC* sono create solo quando servono effettivamente. Tuttavia si ha una elevata latenza nella costruzione della ATM bypass-pipe in quanto per ciascuna delle sue componenti occorre prima effettuare una risoluzione di indirizzo mediante ATM ARP e poi avviare la procedura di segnalazione.

Nei casi b) e c) la latenza è notevolmente inferiore rispetto al caso a) in quanto viene saltata la fase di creazione delle singole *dedicated-VC*. Tuttavia si manifesta uno spreco di risorse in quanto una quota di banda è staticamente allocata alle PVC o ai PVP, anche se attraverso questi ultimi non transita traffico. Il caso c) risulta comunque preferibile rispetto al caso b) in quanto le risorse di rete e le funzionalità di controllo sono allocate all'intero gruppo di VC rappresentato dalla PVP piuttosto che alla singola PVC.

### Creazione e rilascio di ATM bypass-pipe

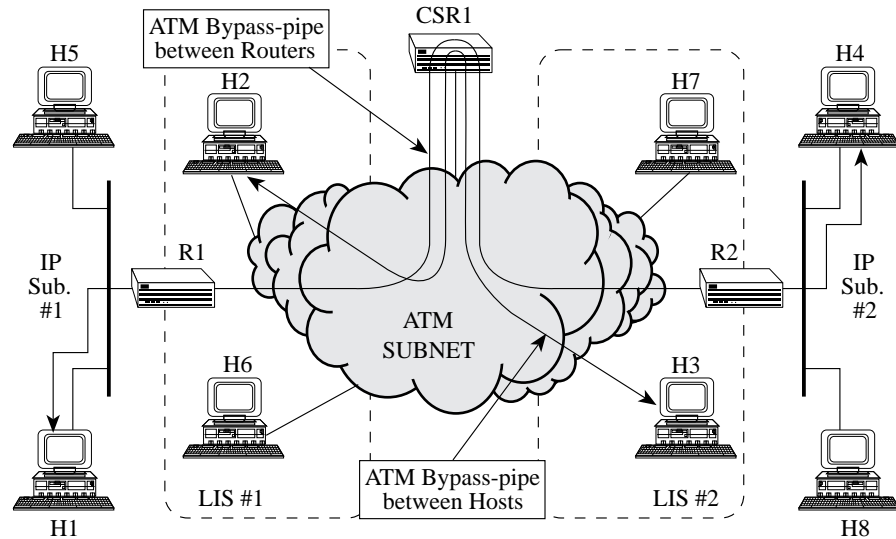
Le ATM bypass-pipe possono essere create in base al verificarsi di due eventi:

- 1) esplicita richiesta del livello IP o dei livelli superiori di un host;
- 2) decisione autonoma di un CSR presa in base a misurazioni condotte sul traffico IP che lo attraversa.

Il caso 1) può essere ulteriormente classificato in base al fatto che il richiedente sia o meno in grado di supportare direttamente una ATM bypass-pipe. Facendo riferimento alla figura 21.16, gli host H2 ed H3 forniscono detto supporto in quanto sono direttamente collegati alla rete ATM. Invece gli host H1 ed H4, pur non facendo parte di quest'ultima, potrebbero comunque trarre vantaggio dalla ATM bypass-pipe R1 - CSR1 - R3; è quindi opportuno che anche ad essi sia consentito partecipare, sebbene per via indiretta, al protocollo di controllo delle ATM bypass-pipe.

Nel primo caso (H2 - H3), l'host mittente ospita un'apposita entità di gestione delle ATM bypass-pipe alla quale il livello IP o i livelli superiori inviano le

richieste. Tale entità comunica con le corrispondenti entità a bordo dei CSR e dell'host di destinazione al fine di stabilire una ATM bypass-pipe tra i due host coinvolti dalla comunicazione.



**Fig. 21.16** - Esempio di internetworking con CSR e Router convenzionali.

Nel secondo caso (H1 e H4), né il mittente né la destinazione dispongono della suddetta entità. Il livello IP o i livelli superiori possono tuttavia effettuare una richiesta di prenotazione delle risorse tramite STII o RSVP. Tale richiesta si propaga lungo il cammino verso la destinazione (STII) oppure verso il mittente (RSVP) e quando raggiunge il CSR questi la traduce in una corrispondente richiesta di creazione di una ATM bypass-pipe. Il risultato finale è che una richiesta di prenotazione di risorse, effettuata da un host che non partecipa direttamente alla gestione delle ATM bypass-pipe, avvia un processo che si conclude con la creazione di una ATM bypass-pipe tra i CSR della rete ATM attraversati dal traffico.

Per quanto concerne il caso 2), un CSR può iniziare la procedura di creazione di una ATM bypass-pipe sulla base di misurazioni da esso effettuate sul traffico diretto verso una certa destinazione. Ad esempio, facendo sempre riferimento alla figura 21.16, quando CSR1 si accorge che esiste un elevato volume di traffico proveniente dalla subnet IP #1 e diretto verso l'host H3, può richiedere la creazione della ATM bypass-pipe R1 - CSR1 - H3.



Il rilascio delle ATM bypass-pipe è provocato da eventi analoghi a quelli visti sopra. Nel caso 1) il rilascio è causato da esplicite richieste da parte degli host, sia tramite il protocollo di controllo sia attraverso i meccanismi di prenotazione delle risorse. Nel caso 2), invece, un CSR richiede la chiusura di una ATM bypass-pipe qualora noti che il volume di traffico per la quale essa era stata creata scenda al di sotto di un determinato livello.

Da quanto sopra emerge che le richieste per la creazione di una ATM bypass-pipe possono provenire sia dal mittente (ad esempio nel caso STII), sia dalla destinazione (ad esempio nel caso RSVP). Il protocollo deve pertanto supportare entrambi i tipi di richieste.

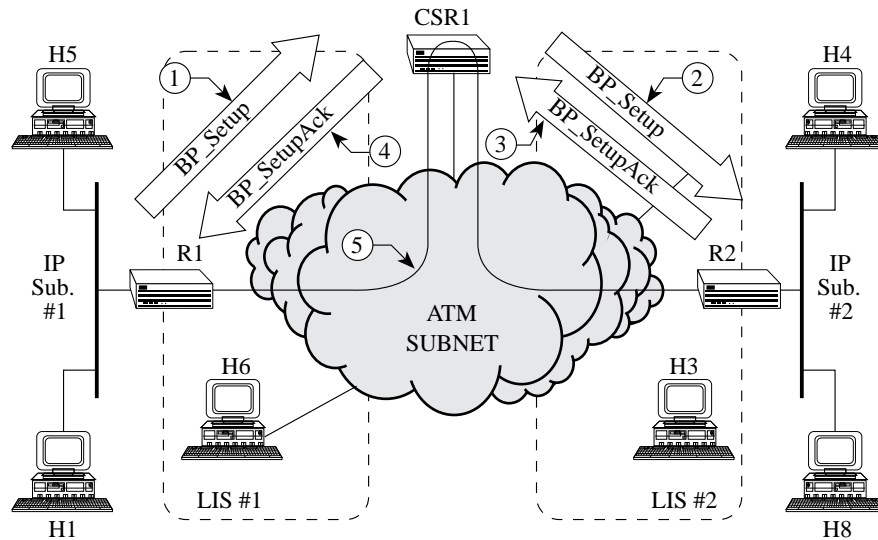
### Richieste provenienti dal mittente

Un mittente, per richiedere la creazione di una ATM bypass-pipe, deve utilizzare il messaggio BP\_Setup mediante il quale specifica:

- l'indirizzo IP della destinazione finale;
- l'identificatore della ATM bypass-pipe in fase di creazione;
- l'identificatore della dedicated-VC che intende utilizzare come componente della ATM bypass-pipe;
- la quantità di banda da allocare alla ATM bypass-pipe.

Tale messaggio deve essere trasmesso al primo CSR che si trova sul cammino verso la destinazione finale (figura 21.17). Quando un CSR riceve il messaggio BP\_Setup dal nodo che lo precede, determina il next-hop in base alla propria tabella di instradamento e, qualora la banda richiesta sia disponibile, sceglie o crea una dedicated-VC verso il next-hop da usare come componente della costruenda ATM bypass-pipe. Infine invia un analogo messaggio BP\_Setup al prossimo nodo. Questa procedura è ripetuta fino a quando il messaggio BP\_Setup giunge alla destinazione finale oppure fino a quando un CSR intermedio non constata che la ATM bypass-pipe non può essere estesa ulteriormente, ad esempio a causa di scarsità di banda.

L'ultimo nodo raggiunto dal messaggio BP\_Setup risponde con un messaggio BP\_SetupAck, il quale compie a ritroso il cammino verso il mittente. Quando tale messaggio giunge al mittente la procedura per la creazione della ATM bypass-pipe può considerarsi conclusa. In figura 21.17 è mostrato un esempio di creazione di ATM bypass-pipe tra i router R1, R2 e CSR1 secondo la procedura sopra descritta.

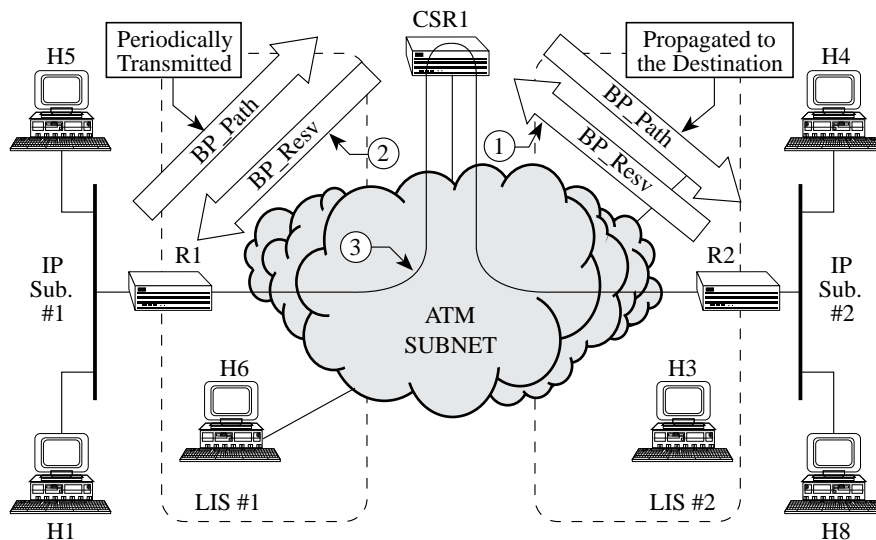


**Fig. 21.17** - Esempio di creazione di una ATM bypass-pipe iniziata dal mittente.

#### Richieste provenienti dalla destinazione

In questo caso, il mittente trasmette periodicamente un messaggio BP\_Path verso la destinazione utilizzando il cammino indicato dalla tabella di instradamento (figura 21.18). Tali messaggi sono necessari affinché la destinazione possa inviare i messaggi per la prenotazione delle risorse BP\_Resv verso il mittente lungo lo stesso cammino seguito dai messaggi BP\_Path. I messaggi BP\_Resv sono trasmessi dai nodi (CSR o host) o quando ricevono un messaggio analogo da un nodo più a valle, oppure quando un'entità RSVP al loro interno genera una richiesta di prenotazione.

Il contenuto dei messaggi BP\_Resv è lo stesso dei messaggi Resv del protocollo RSVP, con l'aggiunta di informazioni specifiche per la creazione della ATM bypass-pipe come l'identificatore della dedicated-VC da utilizzare come una sua componente e la banda da dedicare ad essa. Quando un nodo riceve un messaggio BP\_Resv, determina l'hop precedente mediante le informazioni ricavate dai messaggi BP\_Path; se dispone di banda sufficiente ad accogliere la richiesta, seleziona o crea una dedicated-VC verso tale nodo ed infine invia a quest'ultimo un messaggio BP\_Resv. Questa procedura viene ripetuta fino a quando il messaggio BP\_Resv raggiunge il mittente oppure un CSR intermedio non è in grado di propagare ulteriormente detto messaggio. In quest'ultimo frangente il CSR viene assunto come punto di ingresso della ATM bypass-pipe.



**Fig. 21.18** - Esempio di creazione di una ATM bypass-pipe iniziata dalla destinazione.

Dopo la creazione della ATM bypass-pipe, il mittente continua a trasmettere periodicamente messaggi BP\_Path così come la destinazione continua l'invio di messaggi BP\_Resv. Ciò avviene al fine di mantenere attiva la ATM bypass-pipe: infatti, se anche uno solo dei CSR da questa attraversati non riceve per un certo periodo di tempo un messaggio BP\_Resv, provvede automaticamente al suo rilascio.

Qualora si verificasse una variazione nel forwarding IP dovuta a mutamenti topologici durante il periodo di vita di una ATM bypass-pipe, i messaggi BP\_Path seguirebbero un nuovo percorso. Automaticamente i corrispondenti messaggi BP\_Resv percorrerebbero a ritroso il nuovo cammino, provocando il rilascio della ATM bypass-pipe che seguiva il vecchio percorso e la creazione di una nuova ATM bypass-pipe.

#### 21.14 SUPPORTO DI SERVIZI CONNECTION ORIENTED E QOS

Uno dei motivi per cui il Modello IP Classico tende ad utilizzare l'infrastruttura trasmissiva ATM in modo non ottimale risiede nell'impossibilità di sfruttamento della QoS e delle capacità di gestione del traffico tipiche di un ambiente connection oriented quale ATM. Ciò risulta particolarmente svantaggioso se si pensa alla natura estrema-

mente diversificata del traffico IP in funzione del tipo di applicazioni che lo produce.

Vi sono, ad esempio, applicazioni caratterizzate da una durata molto breve e da uno scambio di pacchetti decisamente contenuto, come ping o le query di DNS (*Domain Name Server*). Altre applicazioni, pur avendo una durata relativamente limitata, generano notevoli moli di traffico come, ad esempio, FTP (*File Transfer Protocol*). Altre ancora sono caratterizzate da una durata piuttosto lunga, ma da un numero di pacchetti scambiati molto contenuto (ad esempio le sessioni telnet). Infine vi sono applicazioni (al momento attuale relativamente poche, ma si prevede un forte sviluppo per il futuro) che hanno sia una durata sia un volume di traffico prodotto decisamente elevati (applicazioni multimediali come la videoconferenza).

Le esigenze in termini di tipo di servizio e di QoS manifestate da applicazioni come quelle sopracitate sono estremamente diversificate. Ad esempio, per una applicazione di videoconferenza sarebbe adeguato un servizio connection oriented basato su una SVC punto-multipunto a larga banda caratterizzata da ritardo basso e costante e da un tasso di perdita relativamente elevato; d'altra parte, per effettuare una query di un DNS risulterebbe appropriato un servizio connectionless basato su router e realizzato con una SVC avente banda trascurabile, ritardo elevato ed un tasso di perdita il più contenuto possibile.

Nell'ottica della QoS, il Modello IP Classico non è in grado di utilizzare in modo flessibile ed adattativo l'infrastruttura trasmissiva ATM. Infatti l'intero traffico in transito tra due host nella stessa LIS deve essere multiplato, mediante incapsulamento LLC/SNAP, su una singola VC caratterizzata da un servizio di tipo "best effort". Ciò implica che tipi di traffico con esigenze estremamente differenti come quelli sopra descritti devono condividere uno canale di comunicazione di qualità non garantita.

Per considerare correttamente la QoS occorre modificare il Modello IP Classico mediante opportune estensioni architetturali che consentano di:

- stabilire tra gli host più VC da destinare al trasporto di traffici di differente natura;
- svincolare la gestione di dette VC dal processo decisionale sulla "localizzazione" delle destinazioni.

Tale approccio è illustrato nei dettagli nel paragrafo seguente.

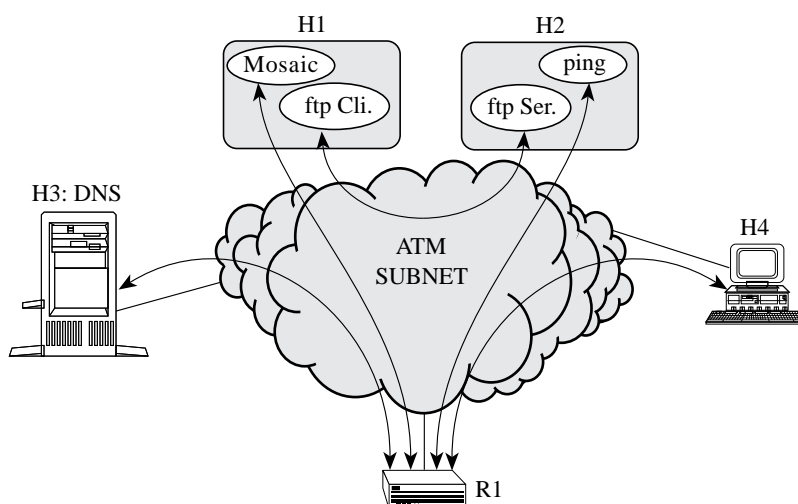
#### 21.14.1 Gestione delle VC in funzione della QoS

Per offrire servizi di trasporto adeguati a ciascun tipo di traffico, sarebbe opportuno demandare la gestione delle VC direttamente alle applicazioni o, in modo più appropriato, gestire le VC in funzione dei requisiti di QoS richiesti dalle

applicazioni [4]. Risulta infatti evidente che esistono due classi di applicazioni:

- applicazioni le cui esigenze giustificano ampiamente un servizio connection oriented basato su SVC interamente dedicate (videoconferenza, sessioni interattive, file transfer);
- applicazioni per le quali risulterebbe più appropriato un servizio connectionless realizzato con una PVC condivisa verso il router di default. Per questo secondo tipo di applicazioni, infatti, l'overhead associato alla gestione delle SVC risulta eccessivamente penalizzante, soprattutto qualora la durata delle attività sia breve. Sarebbe assurdo, ad esempio, stabilire una SVC per effettuare una query al DNS ed abbatterla subito dopo; risulta invece più economico inviare il pacchetto con la richiesta per il DNS al router e lasciare che questi si occupi di inoltrarla al destinatario.

Un oculato utilizzo delle SVC dedicate e dei router tende sia a ridurre il carico che grava sulla rete ATM a causa delle frequenti attività di segnalazione per la creazione e l'abbattimento di SVC, sia ad eliminare i ritardi dovuti allo stesso motivo; tale politica produce quindi benefici sia per la rete che per le applicazioni. Una situazione simile allo scenario sopra delineato è rappresentata in figura 21.19. Si può notare che un'operazione di file transfer in corso tra gli host H1 e H2 avviene attraverso una SVC dedicata, mentre una interrogazione al DNS (H3) effettuata da un'altra applicazione in esecuzione su H1 viene fatta transitare attraverso il router R1, esattamente come il ping effettuato da H2 nei confronti di H4.



**Fig. 21.19** - Esempio di gestione delle VC in funzione della QoS.

In base alla precedente classificazione, ciascun host dovrebbe pertanto stabilire se la destinazione sono "locali" o "remote" indipendentemente dagli indirizzi IP, ma in funzione delle esigenze di QoS manifestate dalle applicazioni che sta eseguendo. Quindi tale decisione non è più invariante nel tempo. Ad esempio, se l'host H1 esegue ping per verificare se H2 è operativo, la comunicazione passa attraverso il router R1 e la destinazione risulta pertanto "remota". Se, immediatamente dopo aver appurato che H2 è attivo, H1 stabilisce una SVC con H2 per la sessione FTP, la destinazione risulta ora "locale". Inoltre una destinazione può risultare contemporaneamente "locale" e "remota": ad esempio un host che funge da DNS potrebbe operare anche come file server e nessuno impedisce che un altro host possa simultaneamente interrogare il database dei nomi ed effettuare una operazione di file transfer.

#### 21.14.2 Ridefinizione del concetto di LIS

Per permettere che gli host prendano la decisione "destinazione locale/remota" non in base agli indirizzi IP, ma a seconda del tipo di applicazioni che stanno eseguendo, si deve ridefinire il concetto di LIS. Una LIS diviene una associazione tra un insieme di host ed uno o più router che gli host possono utilizzare per raggiungere:

1. destinazioni che non condividono lo stesso Data Link ATM;
2. destinazioni che condividono lo stesso Data Link ATM, ma per le quali non si desidera creare apposite SVC in quanto la comunicazione ha luogo tra applicazioni che non giustificano un tale sforzo.

Dato quindi un insieme di host, una LIS identifica l'insieme di router che gli host possono usare come primo hop (*first-hop router*) verso una delle suddette destinazioni. Dualmente, dato un insieme di router, una LIS identifica l'insieme di host per i quali i router fungono da ultimo hop (*last-hop router*). Tale definizione risulta compatibile con quella del Modello IP Classico su ATM raccomandato dalla RFC 1577, rendendo possibile un percorso di migrazione verso il nuovo modello architetturale assolutamente trasparente. Tale migrazione è realizzabile mediante opportune modifiche agli host ed ai router.

#### Modifiche agli host

La principale modifica da apportare agli host concerne ovviamente il meccanismo di gestione delle stesse SVC, il quale deve essere posto sotto il controllo

delle applicazioni o, in modo più appropriato, controllato dai requisiti di QoS richiesti dalle applicazioni.

Per ogni applicazione che trarrebbe vantaggi consistenti dall'impiego di una SVC diretta con la controparte, l'host deve tentare di stabilire tale SVC con la destinazione indipendentemente dagli indirizzi IP del mittente e della destinazione. Se non risulta possibile stabilire tale SVC, l'host deve inviare i pacchetti ad un router della LIS (ad esempio il router di default con il quale è tipicamente collegato mediante una PVC o una VC semi-permanente). Per quanto concerne le applicazioni che non traggono benefici dalla connettività diretta, l'host deve rivolgersi in ogni caso ad uno dei router della LIS.

### Modifiche ai router

La principale modifica da apportare ai router concerne l'inibizione del meccanismo di redirezione. Quando un router associato ad una LIS riceve un pacchetto da un host appartenente alla LIS e destinato ad un altro host della stessa LIS, esso deve effettuare il forwarding del pacchetto verso l'host di destinazione astenendosi dall'inviare un messaggio ICMP di redirect all'host mittente. Questo in quanto i router di una LIS vengono utilizzati anche per mantenere la connettività nell'ambito della LIS stessa tra host le cui applicazioni non necessitano di SVC dirette.

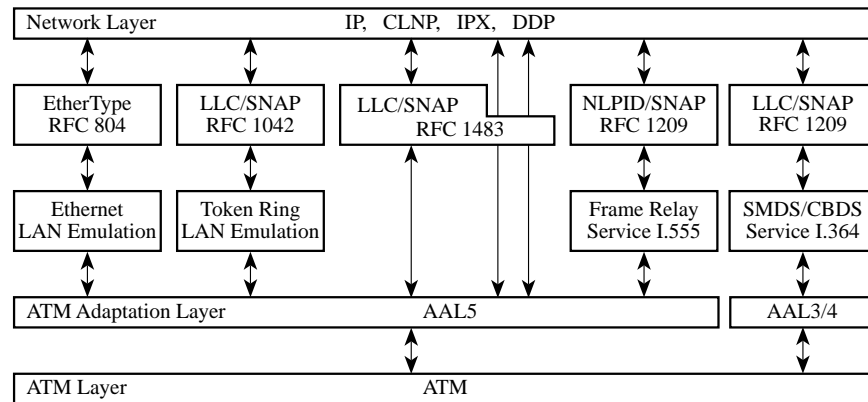
## 21.15 ESEMPIO DI INTERFACCIA ATM

Per cercare di fornire un'idea di come possa essere realizzato in pratica quanto sino a qui descritto, questo paragrafo illustra l'organizzazione interna della scheda ATM AIP che è utilizzabile sui router Cisco della famiglia 7000.

La figura 21.20 mostra lo schema a blocchi di tale scheda dove è possibile vedere che sul livello ATM si appoggiano due possibili ALL: l'AAL3/4 e l'AAL5.

Il primo è utilizzato per fornire servizi di tipo SMDS/CBDS quali quelli descritti nel paragrafo 13.6. Lo standard SMDS/CBDS prevede infatti una trasmissione di celle compatibili con quelle ATM; il supporto di più protocolli di livello superiore (in figura 21.20 sono indicati IP, OSI-CLNP, IPX e DDP, ma la lista è incompleta) è fornito tramite un header LLC/SNAP, in accordo allo RFC 1209.

L'AAL5 è invece utilizzato per il Modello IP Classico, per l'emulazione del servizio Frame Relay (si veda il paragrafo 13.5) e per l'emulazione di LAN (si veda il capitolo 20) sia Ethernet sia Token Ring.



**Fig. 21.20** - Schema a blocchi della scheda Cisco AIP.

Il supporto di più protocolli di alto livello può avvenire sia tramite LLC/SNAP, sia tramite null encapsulation e naturalmente tramite LAN Emulation.

La scheda AIP offre sia le funzionalità di LAN Emulation Client sia quelle di LAN Emulation Service; è in grado di operare come ATMARP client e server e gestisce il protocollo NBMA - NHRP sia in versione client sia in versione server.

I livelli fisici supportati dalla scheda sono vari e la scheda è quindi resa disponibile con connettori di interfaccia alternativi. La figura 21.21 dettaglia ulteriormente l'organizzazione di tale scheda con particolare riferimento ai livelli fisici e ATM.

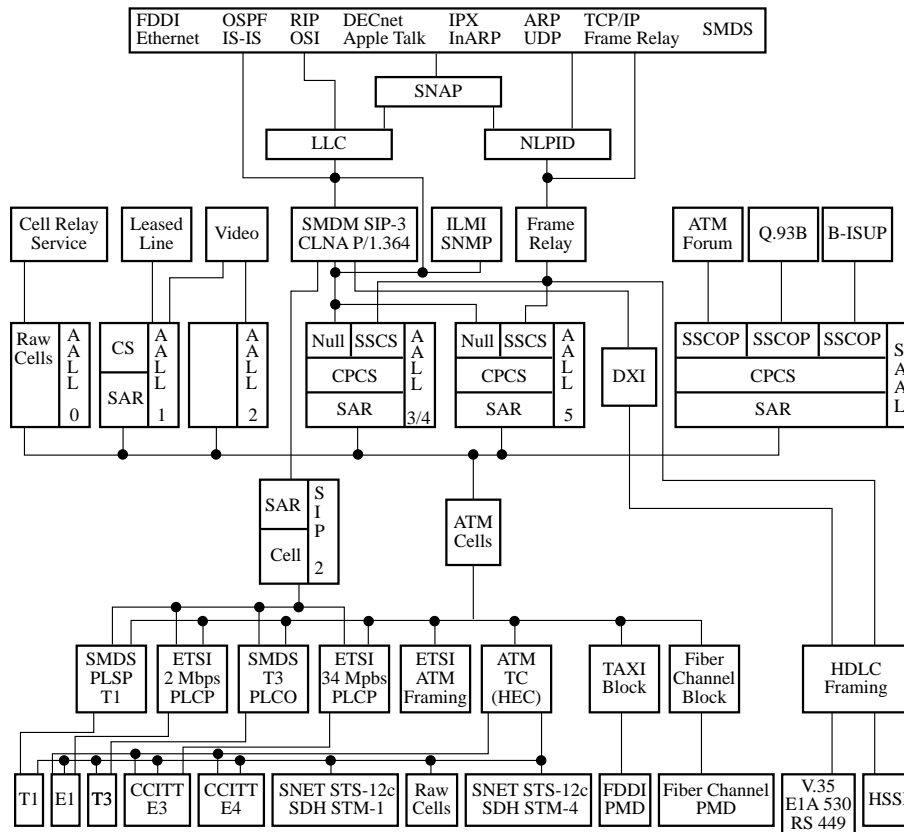
In particolare si può osservare che i livelli fisici sono suddivisi in due gruppi: a trama HDLC e a cella.

Nel caso di interfacce a trama (V.35, HSSI, ...) il protocollo utilizzato è il DXI (si veda il paragrafo 13.6) ed è richiesta una unità di frammentazione in celle (CSU/DSU) esterna.

Nel caso di interfacce a cella sono forniti i seguenti standard:

- plesiocroni in conformità alle gerarchie europee E1, E3 ed E4 ed americane T1 e T3 (si veda il paragrafo 12.5);
- sincroni in conformità alle gerarchie SONET/SDH alle velocità di 155 e 622 Mb/s (si veda il paragrafo 12.6);
- TAXI e ATM nativo su fibra ottica.





**Fig. 21.21** - Schema dettagliato della scheda Cisco AIP.

## BIBLIOGRAFIA

- [1] R.G Cole, D.H.Shur, C.Villamizar, "IP over ATM: A Framework Document," Internet Draft, draft-ietf-ipatm-framework-doc-02, April 1995.
- [2] J. Heinanen, "RFC 1483: Multiprotocol Encapsulation over ATM adaptation layer 5," July 1993.
- [3] R. Braden, J. Postel and Y. Rekhter, "RFC 1620: Internet Architecture Extensions for Shared Media," May 1994.
- [4] Y. Rekhter, D. Kandlur, "IP Architecture Extensions for ATM," Internet Draft draft-rekhter-ip-atm-architecture.txt, January 1995.

- [5] Y. Katsube, K. Nagami and H. Esaki, "Router Architecture Extensions for ATM: Overview," Internet Draft draft-katsube-router-atm-overview-00.txt, March 1995.
- [6] D. Katz, D. Piscitello, "NBMA Next Hop Resolution Protocol," Internet Draft draft-ietf-rolc-nhrp-04.txt, May 1995.
- [7] G. Armitage, "Support for multicast over UNI 3.1 based ATM networks," Internet Draft draft-ietf-ipatm-ipmc-04.txt, February 1995.
- [8] R. Atkinson, "RFC 1626: Default IP MTU for use over ATM AAL5," May 1994.
- [9] ATM Forum, "ATM User-Network Interface Specification," Prentice Hall, September 1993.
- [10] J. Garrett, J. Hagan, and J. Wong, "RFC 1433: Directed ARP," March 1993.
- [11] J. Heinanen and R. Govindan, "RFC 1735: NBMA address resolution protocol (NARP)," December 1994.
- [12] M. Laubach, "RFC 1577: Classical IP and ARP over ATM," January 1994.
- [13] J. Mogul and S. Deering. "RFC 1191: Path MTU discovery," November 1990.
- [14] M. Perez, F. Liaw, D. Grossman, A. Mankin, and A. Hoffman, "RFC 1755: ATM signalling support for IPover ATM," January 1995.
- [15] M. Ohta et al., "Connection Oriented and Connectionless IP Forwarding over ATM networks", Internet Draft, October 1994