

IPv6

Importanza di IP

Il protocollo IP è considerato un protocollo chiave nella pila OSI: se si guarda la pila OSI, si nota che essa è a clessidra, con al centro IP. Questa particolare forma è data dal fatto che a livelli più bassi i protocolli si diversificano a seconda della struttura fisica della rete (Wifi, cablata, ...) e a livelli più alti esistono protocolli diversi a seconda del tipo di informazione che si deve elaborare/trasportare (posta elettronica, audio/video, pagine web,...). IP è, invece, il più diffuso protocollo di trasmissione di livello 3. Al momento esistono due versioni di IP: v4 e v6.

All'interno di questo corso si analizzeranno le caratteristiche dell'IPv6, mentre per la descrizione approfondita dell'IPv4 è rimandata ad altri corsi.

Limiti di IPv4

L'IPv4 è la versione al momento più usata in tutto l'Occidente (Nord America, Europa), ma presenta diversi limiti, che porteranno, probabilmente, all'adozione della nuova versione (IPv6) in tempi relativamente brevi.

I limiti di IPv4 più evidenti sono:

-esaurimento dello spazio di indirizzamento (32bit). Questo fatto è causato da:

--**numero consistente di combinazioni riservate per indirizzi multicast**, per indirizzi privati, indirizzi indeterminati, indirizzi broadcast.

--**frammentazione degli indirizzi, data da un numero elevato di indirizzi assegnati**, ma non effettivamente utilizzati.

-scalabilità del routing: siccome tutte le reti IP per essere raggiunte devono essere annunciate, i pacchetti BGP, che si scambiano i vari Autonomous System (AS), man mano che aumenta la frammentazione e il numero degli indirizzi assegnati diventano sempre più grandi, generando tabelle di routing sempre più difficili da consultare (al momento sono di circa 320MB per gli ISP più grandi).

-richiesta di servizi nuovi o più efficienti, in modo da ottimizzare le funzioni di instradamento (ad esempio implementarle in HW). Alcuni nuovi servizi che negli ultimi anni sono diventati fondamentali:

--**mobilità**, nel senso che si abbia la possibilità di mantenere l'indirizzo IP anche nel caso in cui si cambi l'interfaccia fisica di rete.

--**sicurezza**.

--**plug & play** (autoconfigurazione).

--**qualità del servizio**, QoS (come la garanzia di un tempo massimo di attraversamento, ...).

--**multicast completamente automatico**.

Metodi di attribuzione indirizzi IPv4

All'inizio degli anni '90 gli indirizzi IPv4 stavano finendo a causa dell'apparizione del WEB. Per limitare la velocità di crescita delle richieste di indirizzi di IPv4 sono state usate due strategie:

-NAT, anche se vanno contro l'idea che i router non possano spaccettare i pacchetti ad un livello superiore al 4, con il quale è possibile attribuire indirizzi logici differenti a gruppi di host con lo stesso indirizzo IP, mediante l'uso di porte TCP/UDP.

-criteri di assegnazione degli indirizzi più attenti. La IANA (divisa in 5 agenzie regionali) ha cominciato ad assegnare le reti "/8" alle agenzie regionali. Ogni agenzia può chiedere un nuovo /8 quando non ha più di "/9" indirizzi disponibili da assegnare oppure quando non si hanno abbastanza indirizzi da coprire tutti gli indirizzi che verranno utilizzati nei 18 mesi successivi (velocità di consumo degli indirizzi). Al momento restano circa 20 "/8" da assegnare.

-riassegnando parte degli indirizzi non utilizzati (per il momento questa strada non è ancora stata intrapresa), verificando quali gruppi di indirizzi non sono annunciati nei pacchetti BGP tra gli AS più importanti.

Funzionalità di IPv6

IETF nel 1992 ha proposto una "call for proposals" per introdurre una nuova versione del protocollo IP. La proposta vincente fu quella di SIPP.

Secondo IPv6, gli header risultano essere a lunghezza fissa (40B):

-versione (4bit), nella realtà non è utilizzato, in quanto il protocollo di livello 3 si conosce già in un campo del protocollo di livello 2.

-traffic class (8bit) gestisce la qualità del servizio (QoS).

-flow label (20bit).

-payload length (16 bit) indica la lunghezza del carico dati del pacchetto (max 64Kb).

-**next header** (8bit) indica se i bit successivi si riferiscono ad un altro header IPv6 oppure ad un protocollo di livello superiore (es. TCP). In questo modo è possibile specificare le opzioni dentro agli header successivi. Questa tecnica rende più difficile stabilire la posizione delle intestazioni di livello superiore (in IPv4 bastava vedere i campi header length e protocol type). Esiste un ordine degli header consigliato (Hop by hop, routing, fragment, authentication, encrypted, destination option), ma non è detto che sia così (ad esempio il destination option può essere in seconda posizione). Tutte le opzioni specificate dal next header sono allineate a 32bit.

-**hop limit** (8bit) indica il numero massimo di router attraversabili prima che il pacchetto venga scartato. Questo campo è utile per evitare che i pacchetti IP continuino a girare nel caso di loop nella topologia della rete.

-**source IP address** (128bit).

-**destination IP address** (128bit).

Caratteristiche di IPv6

IPv6 non ammette la frammentazione a livello router, come invece era in IPv4; infatti, la frammentazione deve essere effettuata direttamente da chi invia il pacchetto. In più, in IPv6 non è più presente il checksum, in quanto si è capito che i controlli degli errori a livelli più bassi sono abbastanza accurati.

IPv6 introduce nuove caratteristiche interessanti ma, introduce alcune problematiche:

-**difficoltà nel localizzare le intestazioni di livello 4**, in quanto il numero degli header non è fisso, e il tipo di protocollo di livello superiore è indicato solo nell'ultimo header.

-**indirizzi molto grossi** (tabelle di lookup e (T)CAM molto grosse).

-**frammentazione affidata a chi invia il pacchetto**, che magari non conosce la lunghezza massima dei pacchetti trasportabili da alcuni rami della rete.

-**tabelle dei DNS non univoche**, siccome è possibile avere più indirizzi per una stessa interfaccia.

Alcune caratteristiche introdotte dall'IPv6 erano già state inserite in IPv4, mediante l'utilizzo di soluzioni tampone (ad esempio per l'autoconfigurazione era stata inserita grazie al DHCP). La differenza con il passato è che in IPv6 queste nuove funzionalità sono definite all'interno del protocollo stesso.

Le soluzioni tampone stanno ostacolando la migrazione allo standard IPv6, anche se a breve sarà necessario.

Architettura di indirizzamento di IPv6

Come in IPv4, anche in IPv6 esistono diversi tipi di indirizzamento, ma a differenza della versione precedente, IPv6 consente la coesistenza di indirizzi diversi sulla stessa interfaccia, in modo da permettere il collegamento con ISP diversi o a reti diverse di una stessa interfaccia contemporaneamente.

Esistono 3 tipi di indirizzamento:

-**unicast**: il pacchetto inviato deve raggiungere una sola destinazione. Si riconoscono due tipi di indirizzamento unicast:

--**link local**, che è l'indirizzo necessario per comunicare all'interno di una sottorete.

--**global**, che è l'indirizzo IP pubblico. Ci può essere più di un global address per interfaccia (in modo da favorire l'aggregazione e da permettere la connessione a ISP diversi su una stessa interfaccia).

--**site-local**, l'indirizzo privato all'interno di una sottorete (che può essere composta anche da più sottoreti).

-**multicast**: il pacchetto deve raggiungere tutte le interfacce di un gruppo multicast. Per individuare gli ascoltatori multicast presenti in una rete è presente un protocollo, che sostituisce l'IGMP di IPv4. L'indirizzo di un pacchetto multicast è dato da:

--**group ID**, gruppo multicast a cui si fa riferimento.

--**flag**, indica se è un indirizzo multicast transitorio o permanente.

--**scope**, che indica il livello del gruppo multicast (può essere a livello di nodo, link, sito, locale o globale).

-**anycast**: il pacchetto deve raggiungere almeno un'interfaccia di un gruppo anycast. È utile, ad esempio, se si necessita di un servizio, offerto da un gruppo di server uguali. È usato ad esempio per i DNS, per favorire l'autoconfigurazione.

Con IPv6, è stato tolto l'indirizzo di broadcast perché consuma troppe risorse di elaborazione e di banda. Esso è stato sostituito da gruppi multicast standard, che vengono attribuiti alle macchine nel momento in cui si connettono alla rete. Ad esempio per conoscere il un indirizzo di rete non viene più inviato un messaggio broadcast, ma un messaggio in multicast diretto a tutti i router della rete (utilizzando un gruppo multicast standard).

Rappresentazione degli indirizzi IPv6

Per rendere comprensibile la scrittura degli indirizzi IPv4 si ricorreva alla notazione decimale puntata (130.192.16.17).

In IPv6 si usa la base 16 in gruppi di 4 cifre divise da ":" (FEDC:BA98:876::7:AD:AL:3423).

I gruppi di zeri possono essere compattati con "::" (ovviamente solo una volta per indirizzo in modo da non creare

ambiguità).

L'indirizzo di loopback si scrive "::1".

L'indirizzo non specificato è "::".

Tutti gli indirizzi che iniziano per ::xxx.xxx.xxx.xxx sono utilizzati per gli indirizzi IPv4, usati per renderli interfacciabili con IPv6. Gli indirizzi di compatibilità di IPv4 si scrivono in decimale puntato.

Tutti gli indirizzi che iniziano per ::FFFF:xxx:xxx:xxx:xxx sono utilizzati per mappare un indirizzo IPv4 su macchine dual-stack, in modo da non dover duplicare i socket su cui è in ascolto una macchina (un socket IPv4 e uno IPv6).

Non si usano più le net mask, poiché il concetto è sostituito con il prefix di rete con notazione /n.

Tutti gli indirizzi che iniziano per 2o3 sono indirizzi unicast aggregabili.

Tutti gli indirizzi che iniziano per FE sono link local.

Tutti gli indirizzi che iniziano FD sono privati. Per evitare sovrapposizioni di indirizzi in caso si uniscano reti private differenti si estrae la base casualmente, in modo da rendere questo fatto improbabile. Altrimenti si possono usare due NAT in entrambe le direzioni.

Tutti gli indirizzi multicast iniziano per FF.

Tutti gli indirizzi che iniziano per 0000:010 sono per IPX

Tutti gli indirizzi 0000:001 sono per NSAP.

Molti range di indirizzi non sono utilizzabili come indirizzi IP ma gli verranno date funzioni specifiche.

Gerarchia di indirizzamento in IPv6

La struttura della rete web IPv6 è molto simile a quella di IPv4, in quanto anche essa è strutturata in livelli:

-**Top Level Authority** sono gli ISP di livello più alti.

-**Next Level Authority**

-**Provider**

-**Clienti**

Questa gerarchia non è obbligata in quanti alcuni clienti possono connettersi direttamente ai Top Level, oppure è possibile che due blocchi dello stesso livello siano collegati tra di loro. Questa gerarchia logica è però utile per dividere in parti gli indirizzi IP:

-48 bit per la **topologia di rete pubblica** (prefisso di rete):

--2o3.

--id di top level authority (circa 13).

--clienti e sottoclienti delle top level.

-16 bit per la **topologia di rete privata**.

-64bit per numerare le **interfacce**. Questo numero è diventato più grosso addirittura del MAC-address (48bit). E' quindi possibile utilizzare l'indirizzo fisico per costruire questa parte dell'indirizzo IP: la traduzione viene effettuata dividendo il MAC address in due blocchi da 24bit. I 24 bit più alti vengono messi nella parte alta dei 64 bit, poi viene messo un blocco FFFE ed infine la parte bassa del MAC address.

ICMPv6

Questa nuova versione di ICMP ha principalmente lo scopo di accostarsi ad IPv6 per svolgere alcune funzioni fondamentali:

-**error reporting** (contenuto in ICMPv4).

-**neighbor discovery**, eliminando ARP (mediante i messaggi 135, 136).

-**multicast group**, eliminando IGMPv4 (mediante i messaggi 130, 131 e 132). Questa parte è detta Multicast Listener Discovery.

-**autoconfigurazione** (mediante 133 e 134).

Il formato del pacchetto ICMPv6 è simile ad ICMPv4: tipo, codice, checksum (debole) e contenuto. Il tipo può essere, ad esempio:

-**1** destinazione non raggiungibile

-**2** pacchetto troppo grosso, che permette la frammentazione a livello client.

-**3** TTL esaurito

-**4** problemi di protocollo

-**128** echo request

-**129** echo reply

-**130** Group Membership Query

-**131** Group Membership Report

-132 Group Membership Termination

-133 Router Solicitation, mediante il quale un client sollecita il default gateway (di cui non conosce l'indirizzo) a inviare un messaggio ICMPv6 134.

-134 Router Advertisement, mediante il quale un router informa tutti gli host il prefisso di rete.

-135 Neighbor Solicitation.

-136 Neighbor Advertisement.

-137 Redirect.

DHCPv6

Grazie all'autoconfigurazione DHCP è diventato inutile, ma è stato ugualmente mantenuto, per inviare informazioni specifiche di configurazione. E' ad esempio utile nell'uso dei token, necessari per mantenere le impostazioni predefinite per un certo host. I messaggi disponibili sono:

-solicit.

-advertise.

-request.

-reply.

-release.

-reconfigure.

Autoconfigurazione

Siccome il prefisso di una rete dipende dal provider che si usa, con IPv6 è più probabile che esso cambi. Sono necessari dei meccanismi per rendere la rinumerazione automatica e quindi evitare la configurazione manuale. E' inoltre importante pensare di non utilizzare router specifici con la sola funzione di autoconfigurare gli host.

L'autoconfigurazione avviene per parti:

-**autoconfigurazione degli host stateless**, mediante la generazione di un indirizzo link-local e la verifica che esso sia univoco all'interno della sottorete. La traduzione viene effettuata dividendo il MAC address in due blocchi da 24bit. I 24 bit più alti vengono messi nella parte alta dei 64 bit di indirizzo host, poi viene messo un blocco FFFE e poi la parte bassa del MAC address. Per costruire la parte alta dell'indirizzo globale si usa l'indirizzo contenuto nei pacchetti ICMPv6 di tipo "router advertisement", che vengono inviati dal gateway periodicamente. I prefissi devono essere aggiornati periodicamente in quanto hanno un tempo di vita dopo il quale diventano non validi. E' presente anche un metodo di rilevazione di unicità del proprio indirizzo IP all'interno di una sottorete, detto duplicate address detection (si invia una neighbor solicitation in multicast a tutti i vicini che hanno come indirizzo MAC le ultime 24 cifre del mio MAC. Se risponde qualcuno non va bene, altrimenti significa che il mio indirizzo è univoco (maggioranza dei casi). A questo punto si annuncia il proprio indirizzo IP, in modo da evitare errori nel caso in cui due host stiano cercando di prendere lo stesso IP.). L'autoconfigurazione basata su MAC crea problemi di privacy, poiché ogni interfaccia diventa tracciabile. E' possibile utilizzare un algoritmo non deterministico (indirizzo stateless + numero casuale su 64 bit -> MD5 -> selezione dei 64bit più significativi -> settare il bit 6 a 0). E' possibile utilizzare entrambi gli algoritmi a seconda dell'applicazione (indirizzo "default", indirizzo "privacy").

-**autoconfigurazione dei router**, che permette la configurazione della parte alta degli indirizzi, nel caso in cui esso venga cambiato. Essa avviene mediante il protocollo PCOs (Prefix Control Operations), che permette di propagare le nuove informazioni sui prefissi inserite in un router a tutti i router.

DNS

Il protocollo DNS non subisce modifiche con l'avvento di IPv6 e quindi il suo scopo rimane quello di costruire un database distribuito in modo da associare a nomi logici indirizzi IP. Esso subisce comunque qualche piccola correzione:

-**aggiunta di indirizzi più lunghi** nelle righe di indirizzi (tipo AAAA).

-**risoluzione dei conflitti tra indirizzi IPv4/IPv6**, introducendo il tipo della risposta (A/AAAA). E' possibile specificare il tipo ANY, in modo da ricevere sia i record A (IPv4), sia quelli di tipo AAAA (IPv6).

ARP

Il protocollo ARP non viene mantenuto con l'introduzione dell'IPv6, ma viene, come detto, inglobato in ICMPv6. Il meccanismo logico su cui si basava ARP, viene modificato in quanto:

-**scopre gli indirizzi dei routers** della rete.

-**scopre i prefissi di rete** a cui un host è connesso.

Per conoscere il MAC address associato ad un host che si trova nella stessa sottorete è sufficiente inviare un pacchetto IPv6 con indirizzo MAC un indirizzo multicast così costruito:

-FF

-uno speciale gruppo di bit (**3333**)

-gli ultimi 32 bit dell'indirizzo IPv6.

In questo modo è possibile disturbare poco la rete, grazie all'uso degli indirizzi multicast.

L'inoltro del pacchetto vero e proprio avviene come in IPv4. Se bisogna inviare un pacchetto ad un indirizzo locale, l'inoltro avviene a livello 2 (dopo aver eseguito una Neighbor Solicitation, per conoscere l'indirizzo MAC del destinatario), altrimenti si inoltra mediante longest prefix match (dopo aver capito quale sia la destinazione con un router advertisement). Le risposte vengono memorizzate in cache, in modo da velocizzare il procedimento.

Sicurezza in IPv6

IPv6 utilizza come autenticazione MD5 e come cifratura DES-CBC. Sono le stesse di IPsec, protocollo aggiunto in IPv4 per garantire la sicurezza. La sicurezza si ottiene:

-crittografando il contenuto dei messaggi.

-crittografando l'indirizzo del destinatario e del mittente.

-garantendo l'**integrità** dei messaggi inviati/ricevuti.

Alcuni problemi non possono essere risolti mediante la cifratura, come ad esempio gli attacchi DDos (richieste fittizie per intasare i server, in modo da non consentire il normale soddisfacimento delle richieste). Molto spesso questi attacchi sono distribuiti in modo da non rendere possibile il blocco selettivo degli IP che stanno effettuando l'attacco. Il network scanning è la tecnica usata per iniziare questi attacchi (che prevede di cercare una porta libera per installare software maligno). Aumentando lo spazio di indirizzamento, IPv6 dovrebbe rendere più difficoltoso il network scanning, ma non è sempre così (indirizzo stateless basati su 48bit, indirizzi sequenziali, indirizzi MAC con parte alta spesso simile poiché comune ai costruttori, probabilità di avere indirizzi simili).

Protocolli di routing

Il protocollo RIPng rimane utilizzabile, nonostante sia ormai abbastanza datato.

E' stata, invece, implementata una nuova versione di OSPF (OSPFv3), che non introduce modifiche rilevanti a parte la sostituzione degli indirizzi IPv4 con gli indirizzi IPv6.

Transizione a IPv6

Analizzando la situazione attuale si nota che gran parte del traffico internet è ancora basato su IPv4, ma a breve la migrazione a IPv6 risulterà necessaria. I motivi di questo ritardo sono da attribuire a diversi fattori:

-aggiornamento dei router (che ormai è avvenuto). Gli apparati interessati non sono solo i router, ma anche quegli switch, che svolgono funzioni speciali (ad es: IGMP snooping). Al momento, per rendere possibile la coesistenza di IPv4 e IPv6 si separano gli stack di rete (dual stack con approccio ships in the night, che prevede la duplicazione delle tabelle di routing, delle regole dei firewall, dei protocolli di routing,...).

-aggiornamento delle macchine utente (tutti gli OS ormai supportano sia IPv4, che IPv6). Anche qui la soluzione si basa su dual stack (ogni host ha il supporto completo per entrambi i protocolli, e quindi necessita sia di indirizzi IPv4 e di IPv6). Si sta passando ad una soluzione di tipo dual layer, che prevede di utilizzare la maggior parte degli indirizzi IPv4 in formato IPv6, utilizzando i protocolli di livello superiore solo con indirizzi di tipo IPv6.

-aggiornamento delle applicazioni (la situazione è problematica).

Data la situazione attuale sono necessari alcuni meccanismi di comunicazione tra IPv4 e IPv6. Essi si ottengono con la tecnica del tunneling, che prevede l'installazione di un'applicazione specifica sui router, che permette l'impaccamento e lo spaccamento di pacchetti IPv6 in pacchetti IPv4 (protocollo GRE + si cambia l'intestazione del protocol type).

Automatic Tunnel e IPv4 compatibile

Per trasportare indirizzi IPv6 su infrastrutture IPv4 è possibile usare l'automatic tunnel. Questa tecnica prevede che nel momento in cui un pacchetto IPv6 raggiunge una rete IPv4, esso viene impacchettato in un pacchetto IPv4. A questo punto viene aperto un tunnel mettendo nell'indirizzo del destinatario l'indirizzo dell'uscita del tunnel.

Se avviene, invece, che un pacchetto IPv4 raggiunga un'area IPv6 vengono messi a 0 tutti i 96 bit a sinistra dell'indirizzo IPv4, in modo da renderlo compatibile con l'IPv6. Sui vari sistemi operativi ci sono diversi comandi per abilitare l'automatic tunnel (in alcuni è attivo di default). Se il destinatario è all'interno di una rete IPv4, ma il mittente no, il pacchetto parte in IPv6 e poi viene impacchettato in un pacchetto IPv4 solo nel momento in cui esso arriva nella sottorete IPv4. Questa tecnica funziona sia se il destinatario si trova in una rete IPv6 o IPv4.

Altre tecniche

Per trasportare pacchetti IP in reti IP di versioni differenti, esistono anche altre tecniche:

-**6over4** serve per trasportare pacchetti IPv6 su infrastrutture IPv4. La tecnica è in disuso, in quanto prevede l'esistenza di reti IPv4 multicast spesso non disponibili. In più il multicast spreca molta banda.

-**6to4** si basa su una traduzione degli indirizzi delle interfacce dei router IPv4 in IPv6. Con questo metodo è possibile indirizzare all'interno di reti IPv4 intere reti IPv6. Questo approccio non è compatibile con i NAT ed è normalmente utilizzabile in modalità host->6to4 area. Ogni numero decimale dell'indirizzo IPv4 (quelli divisi da ".") viene convertito in esadecimale e vengono messi:

--prefisso 6to4 (**2002**)

--**indirizzo IP convertito** (48bit)

--**address space** (80bit), utile a numerare gli host nelle sottoreti interne.

-**ISATAP** è un meccanismo usato per propagare le informazioni di routing interne a reti 6to4, non collegate direttamente. Questa funzione non sarebbe possibile senza ISATAP, che ottiene questo risultato usando i server DNS per questo scopo. Ogni router può scoprire queste informazioni andando a consultare i domini ISATAP, contenuti nei server DNS.

-**Teredo**, che permette di imbustare i pacchetti IPv6 in IPv4/UDP, in modo da superare i NAT. Questo meccanismo richiede un server esterno, in grado di associare gli indirizzi privati in indirizzi pubblici.

-**Tunnel Broker**, che cerca di risolvere i problemi causati dai NAT in modo diverso rispetto a Teredo: esso usa script locali che permettono i tunnel IPv6.

Migrazione delle applicazioni

La conversione delle applicazioni da IPv4 a IPv6 è uno dei problemi più difficili da risolvere.

Per ottenere il passaggio a IPv6, è necessario che le interfacce socket (a livello server) vengano modificate, in quanto è necessario specificare in fase di programmazione la famiglia del protocollo da usare. Con le nuove librerie dei socket è possibile utilizzare strutture compatibili sia per IPv6 e IPv4.

Le nuove librerie creano problemi di timeout lato client, in quanto nel caso in cui una macchina non risponda all'indirizzo IPv6, bisogna ripetere la richiesta in formato IPv4. Questa duplicazione delle richieste crea un tempo di attesa maggiore, causando lo scatto dei timeout nell'applicazione.

Le nuove librerie lato server devono essere in grado di ricevere richieste di connessione sia IPv4, che IPv6. Per ottenere questo risultato è necessario duplicare il codice, in modo da creare dei socket doppi.

Il codice da modificare nelle applicazioni, in realtà, non è molto, ma difficilmente individuabile, e causa la ricompilazione del codice.

E' necessario modificare sia lato client, che lato server anche le parti di codice relative agli URL, in quanto in IPv4 il separatore degli indirizzi IPv6 (":") indica il numero di porta e questo crea non pochi problemi (per specificare un numero di porta in IPv6 bisogna racchiudere l'indirizzo numerico tra "[]").

Esistono anche protocolli di livello applicazione, che hanno al loro interno indirizzi IP, che in questo caso devono essere aggiornati. Un esempio è dato dalle applicazioni peer to peer.

Al momento non è conveniente creare applicazioni solo IPv6, in quanto le reti esistenti sono per lo più IPv4.

VPN

Generalità

Esistono diverse interpretazioni del termine "VPN". VPN è l'acronimo di rete privata virtuale e richiama quindi una connettività su un'infrastruttura condivisa in modo da trattare la rete (virtuale e distribuita) come una rete privata. In questo modo è possibile adottare le politiche (di indirizzamento, della gestione della qualità, della sicurezza, dell'affidabilità, ...) di tipo privato. Una rete privata è una rete in cui esistono dei canali usati solo per quella determinata rete: non ci sono quindi canali condivisi tra più reti. Le VPN creano canali virtuali diretti tra destinazioni che non si trovano fisicamente nella stessa rete privata. Grazie alle VPN è possibile avere garanzie (di banda, di affidabilità, ...) anche su reti non private. Le VPN esistono in quanto i costi di gestione di una rete privata vera e propria tra host distanti fisicamente risultano essere troppo alti.

Normalmente le VPN sono utilizzate sulla rete internet, in modo tale che gli host vedano alcuni destinatari come diretti, anche se in realtà non si trovano realmente nella stessa rete.

Per gestire le VPN sono necessari apparati supplementari, ma in genere portano ad un notevole risparmio in termini economici. Molto spesso i router (di categoria medio-alta) permettono di gestire autonomamente le reti VPN e i firewall necessari.

Problematiche

Creare una rete VPN non è un problema di semplice soluzione, in quanto si possono avere numerose complicazioni. Ad esempio è possibile che sia necessario consentire la connessione ad una VPN anche di utenti mobili o di utenti remoti che non hanno router VPN, oppure di uffici remoti molto distanti.

Tutti gli utenti, nel momento in cui si vogliono connettere alla rete VPN fanno richiesta di accesso ad un firewall, che, dopo aver consultato un server AAA (Authentication, Authorization, Accounting) esegue diverse operazioni:

- permette o nega l'**accesso** alla VPN.

- definisce i servizi** a cui l'utente è autorizzato.

- misura** il consumo di risorse degli utenti.

I meccanismi di autenticazione devono essere sicuri e variano a seconda del tipo di utente. Ad esempio gli utenti mobili avranno un metodo di autenticazione più veloce e semplice rispetto agli uffici distaccati, che non subiranno quasi mai disconnessioni.

Tipi di VPN

Esistono diverse tipologie di reti VPN. Molto spesso questi tipi coesistono su una struttura VPN comune:

- VPN di accesso**, consentono il collegamento di singoli apparecchi. Virtualizzano quindi le reti dial-up. Esistono diversi protocolli di gestione PPTP, L2TP. E' possibile usare infrastrutture condivise (reti di service provider, internet) mediante reti condivise (ADSL, ISDN, Wireless, DSL, ...). Normalmente è necessario configurare in modo apposito le macchine per l'accesso alla VPN.

- VPN site to site**, che consentono la virtualizzazione di canali dedicati. Protocolli IPsec, GRE, MPLS. E' possibile usare infrastrutture condivise (reti di service provider, internet) mediante reti condivise (ADSL, Fibra, Ethernet, ...).

Funzionalità VPN

E' possibile usare le reti VPN in diversi modi, a seconda dello scopo per cui esse sono progettata:

- VPN Intranet** permette il collegamento di tutte le risorse all'interno della rete VPN. (Site to Site). Si esige connessione sicura (cifatura), priorità del traffico (ad esempio priorità diverse a seconda dei dati che passano), scalabilità. E' necessario un firewall che permette l'accesso a determinate risorse a seconda del tipo di utente.

- VPN Extranet** permette la condivisione di alcune funzionalità tra più aziende. (Site to Site). E' necessario un firewall all'ingresso della rete VPN (in modo da separare il traffico proveniente da una rete o da un'altra). Bisogna gestire il conflitto di indirizzi tra le reti (NAT, oppure è necessario rendere univoci gli spazi di indirizzamento, ...).

- VPN ad accesso remoto** permette l'accesso a utenti remoti. (VPN di accesso).

- VPN con accesso a internet** permette la connessione di una VPN ad una rete esterna. Il collegamento può essere di due tipi:

- accesso a internet centralizzato**, in cui l'accesso a internet della rete avviene attraverso un server centrale per tutta la rete. In questo modo è possibile filtrare il traffico in modo molto accurato e evitare accessi indesiderati alla rete.

- accesso a internet volontario**, in cui l'accesso è distribuito tra gli utenti della rete. Questo evita di dover utilizzare sempre lo stesso apparecchio per uscire dalla rete, ma crea problemi di sicurezza e di gestione, in quanto è sufficiente che un utente non sia sufficientemente protetto da permettere l'accesso ad un estraneo ad alcune risorse della VPN. In più le regole di filtraggio del traffico sono difficilmente aggiornabili.

Modelli di VPN

Dal punto di vista organizzativo le VPN possono essere gestite in due modi:

- modello overlay** consiste nella sovrapposizione della rete virtuale sulla rete fisica. In questo modo l'ISP non sa dell'esistenza della VPN (a meno che non snidi i pacchetti). In questo modo però bisogna usare alcuni apparecchi (VPN gateway) che si conoscono tra loro. In più il routing all'interno della VPN è a carico di chi crea la VPN. Alcuni esempi sono L2TP, PPTP (VPN ad accesso), IPsec, GRE (VPN site to site).

- modello peer** lascia l'incarico di gestire la VPN all'ISP, che quindi gestisce anche l'instradamento. Non si possono fare reti di accesso peer pure, in quanto gli utenti non possono connettersi in modo dinamico. Un esempio di VPN peer è dato da MPLS (VPN Site to site). Nel modello peer esistono due entità: Il Provider Edge (PE), primo dispositivo della rete del provider, e il Customer Edge (CE), l'ultimo router prima della rete utente.

Altre differenziazioni

Si possono individuare reti VPN differenti a seconda del protocollo che emulano. Si possono avere VPN che emulano le funzionalità di livello 2 (i router virtuali sono bridge), oppure emulano reti IP, oppure VPN che emulano canali diretti, oppure VPN che lavorano a livello 3/4...

Modelli VPN

Esistono diverse tipologie di reti VPN, ecco un breve riassunto:

-Overlay Model

--**Layer 2**, emula un protocollo di livello 2 (linea dedicata o rete locale)

---**Frame Relay** (Provider Provisioned)

---**ATM**

---**MPLS**

--**Layer 3** (Customer Based / Provider Provisioned)

---**IPsec+GRE**

---**PPTP**

--**Layer 4** (Customer Based)

---**SSL**

-**Peer Model**, che prevedono l'esistenza di host, che si connettono a Edge Router, che hanno lo scopo di creare dei tunnel tra di loro.

--**Dedicated Router** (Provider Provisioned), non più usato. Esistevano degli Edge Router dedicati per creare tunnel e per instradare i pacchetti. Questo metodo è molto oneroso e necessita di un lungo tempo di installazione, in quanto necessita l'installazione di un nuovo router apposito per ogni postazione che si vuole connettere alla VPN.

--**MPLS** (Provider Provisioned)

---**BGP**

---**VR**

--**Shared Router** (Provider Provisioned), in cui esistono router con installate più macchine virtuali, ognuna dedicata allo smistamento dei pacchetti, la gestione dell'instradamento dei pacchetti,

Topologie di VPN

La scelta di una topologia dipende dal traffico della rete (a seconda se il traffico avviene soprattutto tra host o tra host e server centrale). Alcune topologie tipiche sono:

-**Hub and spole** prevede l'implementazione di una topologia a stella, in cui gli host si connettono ad un insieme di server in una sede centrale. L'instradamento è sub-ottimo (ogni pacchetto è sempre consegnato in due passi), ma non sempre risulta essere veloce. C'è un numero minimo di tunnel, ma il gateway della sede centrale può essere spesso intasato.

-**Mesh** non prevede una topologia particolare: tutti gli host si possono collegare con gli altri host. In questo modo si può ottimizzare il routing (anche se risulta oneroso calcolare le tabelle di routing), ma si può avere un numero molto alto di tunnel.

Componenti necessari per la realizzazione della VPN

Abbiamo necessità di avere meccanismi e protocolli per separare il traffico della rete e quello della VPN. Questa funzione è data dai protocolli di tunneling.

Bisogna avere dei meccanismi di cifratura, che non permettano a chi sniffa i pacchetti del tunnel di capirne il significato. In più sono necessarie alcune tecniche per garantire l'integrità dei dati trasferiti, in modo da permettere il riconoscimento delle modifiche. Infine sono necessari dei meccanismi di autenticazione.

Meccanismi di Tunneling

I meccanismi di tunneling consistono nell'incapsulare un pacchetto destinato ad un host in un altro pacchetto. E' possibile effettuare il tunneling a livello IP (GRE e IPsec), che consiste nell'incapsulare pacchetti IP in pacchetti IP, oppure a livello 2 (PPTP, L2TP), che consiste nell'incapsulare pacchetti di livello 2 in pacchetti IP.

L'ordine delle intestazioni all'interno dei pacchetti non segue più il modello OSI in quanto dopo un'intestazione di livello 3 può esserci un'intestazione di livello 2 o un'altra di livello 3.

GRE (Generic Routing Encapsulation)

Per utilizzare GRE è necessario inserire nel campo protocol di IPv4 il valore 47. Un pacchetto GRE è formato da righe da 32bit.

All'interno dell'intestazione GRE sono presenti diversi campi:

-**obbligatori**:

--**protocol** indica il tipo della trama contenuta (un protocollo di livello 2/3).

--**recur** indica il numero massimo di incapsulamenti (deve essere 0, in pratica non può essere usato).

--**flag** indicano l'esistenza dei campi opzionali.

--**version** indica la versione

-**opzionali**:

--**checksum** controlla gli errori.

--**offset**.

--**routing** permette di effettuare il routing step by step.

--**key** indica la dimensione del pacchetto e il numero del tunnel

--**sequence number e ack number** necessary per scartare i pacchetti fuori ordini e per controller il flusso e la congestione. Questi campi non permettono il recupero di messaggi danneggiati, in quanto a queste operazioni (se richieste) sono gestite dal PPP o da un protocollo di livello superiore.

A seconda dei campi opzionali esistono altri campi aggiuntivi come la lista degli indirizzi IP, che elenca gli AS o dei router da attraversare nel caso in cui il routing step by step sia attivato.

L2TP (Layer 2 Tunneling Protocol)

E' protocollo per reti VPN dial-up, cioè una rete in cui gli host si possono connettere da postazioni diverse. L2TP è un protocollo che non è stato creato per essere installato direttamente sui terminali, ma è stato modificato solo in un momento successivo. In principio era necessario avere un collegamento diretto (punto a punto) tra l'host e una speciale macchina dell'ISP, con il compito di creare il tunnel.

E' un protocollo indipendente di livello 2, che non può fornire sistemi di autenticazione. Per questo motivo è stato introdotto il protocollo IPsec.

La creazione del tunnel avviene tra due apparecchi (il collegamento dei dispositivi con queste due macchine deve essere sicuro):

-**LAC** è installato sulla macchina utente o dal service provider.

-**LNS** ha lo scopo di tunnel end point, sistemato all'ingresso della VPN.

Esistono due tipi di messaggi:

-messaggi di **dato** sono composti da frame PPP all'interno di un pacchetto L2TP.

-messaggi di **controllo** sono composti da un'intestazione L2TP.

I pacchetti L2TP possono viaggiare all'interno di pacchetti UDP (porta 1701), FR, ATM (livello 2)...

Il pacchetto L2TP è composto dall'indirizzo di livello 2, dall'indirizzo di destinazione, dall'indirizzo IP, dall'UDP, dall'header L2TP e dai dati.

L'intestazione L2TP ha:

-**flag** per identificare se si tratta di un pacchetto dati o di controllo

-la **lunghezza** del pacchetto

-**session ID** e tunnel id consentono a più host, che lavorano con lo stesso LAC, di lavorare contemporaneamente, oppure di aprire più sessioni per lo stesso host. I messaggi di controllo provenienti dall'LNS al LAC viaggiano sullo stesso canale per tutte le sessioni, non hanno quindi bisogno di essere identificati.

-**offset size** indica la posizione dei dati all'interno del pacchetto.

-**versione** (l'attuale versione è 2).

-**NR** numero di sequenza dei messaggi di controllo, con la funzione di ACK.

-**NS** numero di sequenza per i messaggi dati (i pacchetti fuori ordine vengono scartati).

Per aprire una connessione L2TP è necessario creare una connessione di controllo tra il LAC e LNS e poi aprire la sessione dati.

I meccanismi di autenticazione si basano su un segreto comune tra LAC e LNS, basato su CHAP (il LAC invia una chiave di cifratura all'LNS, il quale risponde con la password codificata con la chiave). A questo punto LAC e LNS si scambiano dei local ID per aprire delle sessioni.

Le sessioni possono essere aperte dal LAC (in ingresso) oppure dall'LNS (in uscita).

L'autenticazione è fatta solo nelle fasi di inizializzazione; questo crea problemi di affidabilità dei canali aperti, in quanto è possibile iniettare pacchetti conoscendo il numero di sessione. La cifratura dei messaggi deve essere fatta con altri meccanismi.

PPTP (Point-to-point Tunneling Protocol)

PPTP è una proposta di Microsoft, Apple e altre aziende, per costruire tunnel direttamente dalla macchina utente. Successivamente esso è stato standardizzato.

All'inizio non possedeva un metodo di autenticazione molto forte, ma con l'introduzione di IPsec le cose sono migliorate.

L'inizio del tunnel avviene direttamente sulla macchina utente, mentre il termine del tunnel è dato dal PNS. L'apertura di un tunnel PPTP, come in L2TP, prevede l'apertura di un canale di controllo. I frame PPP viaggiano all'interno di pacchetti di altri protocolli.

Esistono meccanismi di autenticazione (MS CHAP) e di cifratura (MPPE). Esiste anche una versione che necessita di una struttura apposita da installare sugli ISP (PAC).

Come in L2TP, in PPTP esistono diversi tipi di messaggi:

- i **dati** viaggiano all'interno di pacchetti composti da intestazione di livello 2+IP+GRE+PPP+dati cifrati (datagram IP o NetBUEI)+coda (CRC)

- messaggi di **controllo** sono composti da un'intestazione di livello 2+IP+TCP (porta 1723)+messaggi di controllo PPTP+coda (CRC). Essi sono necessari per creare il tunnel. Hanno diverse funzioni come ECHO, chiudere/aprire la connessione, notifica di errori.

IPsec

IPsec è un'estensione di IPv4 ed è stato poi inglobato nell'IPv6. Esistono due formati:

- Autentication header protocol (**AH**) fornisce autenticazione, integrità dei dati ma non segretezza (messaggio non cifrato). Grazie all'intestazione AH è possibile rilevare se ci sono state manomissioni del messaggio.

- ESP** fornisce segretezza, autorizzazione e integrità dei dati. L'header ESP, il segmento TCP/UDP e la coda ESP vengono autenticati (è possibile individuare eventuali manomissioni), mentre solo il segmento TCP/UDP e la coda ESP vengono anche cifrati. Protocol number = 50.

IPsec può essere usato nei tunnel delle VPN in modo da garantire la cifratura, l'autenticazione e l'incapsulamento dei dati. IPsec può operare in due modi:

- transport mode** permette di mettere in pacchetti IPsec i dati di livello trasporto (TCP/UDP), il tutto poi incapsulato in un pacchetto IP.

- tunnel mode** permette di incapsulare in un pacchetto IPsec un pacchetto IP, tutto poi impacchettato in un altro pacchetto IP. In questo modo l'intestazione IP viene cifrata (non si riesce più a capire chi è il destinatario e il mittente reali).

Le Security Association sono associazioni monodirezionali, che definiscono i protocolli di autenticazione e crittografia (tipo/chiavi) per un determinato destinatario.

Per definire le security association si usa il protocollo Internet Key Exchange (IKE), che prevede che una volta che è stata definita una security association si generino delle altre security association.

VPN Gateway e Firewall

A seconda di dove si posiziona il firewall rispetto al VPN gateway all'interno della rete si possono avere diversi livelli di sicurezza:

- se il **firewall è posizionato davanti al VPN Gateway**, nel caso in cui i tunnel siano cifrati, il firewall non riesce più a gestire il traffico in ingresso nella VPN. Con questa configurazione, però, il VPN Gateway viene protetto da attacchi esterni, in quanto il firewall può bloccare il traffico verso il gateway.

- se il **firewall e il gateway sono posizionati in parallelo** il traffico in ingresso al gateway non è filtrato (può essere attaccato con attacchi ECHO), in più il traffico in uscita non è controllato.

- se il **VPN gateway è posizionato davanti al firewall** il VPN gateway non è protetto dal firewall. Il firewall però può filtrare il traffico in ingresso/uscita non cifrato.

- se il **firewall è integrato nel VPN Gateway** è garantita la massima flessibilità, in quanto è possibile filtrare sia il traffico in ingresso al gateway e il traffico prima di essere cifrato.

IPsec, VPN Gateway e NAT

I NAT non sono compatibili con la versione di IPsec di tipo AH, in quanto l'indirizzo IP del destinatario risulta essere cifrato e non è quindi modificabile dal NAT.

I NAT non sono compatibili con IPsec Transport Mode in quanto parte dell'indirizzo viene modificato.

Non è possibile usare NAT o PAT perché la porta è in entrambi i casi cifrata.

I NAT sono compatibili con il Tunnel Mode se i pacchetti sono modificati prima di entrare nel gateway, anche se questa condizione non si verifica molto spesso.

Intrusion Detection System (IDS)

Sono delle "sonde" virtuali che hanno lo scopo di analizzare il traffico, in modo da vedere se sono presenti dei pacchetti anomali. Gli IDS sono posizionati tra il router e il firewall e dentro la rete privata.

VPN SSL

Le SSL sono "tunnel" di livello 4. Grazie a questo modello è possibile cifrare e autenticare il tunnel.

Le SSL possono essere usate sia per VPN site-to-site, sia per accesso remoto ed anche per accedere ad un particolare servizio (pseudo-VPN).

Questo meccanismo è più semplice rispetto a IPsec (in principio IPsec poteva essere implementato solo in kernel mode e quindi alcuni errori potevano portare al crash del sistema). Le SSL possono superare facilmente i NAT, in quanto sono di livello superiore.

Un difetto di SSL è che i pacchetti vengono scartati ad un livello molto alto (tempo di elaborazione richiesto maggiore), rendendo vulnerabili i sistemi che utilizzano questo metodo ad attacchi DOS.

SSL, rispetto a PPT, ha introdotto fin dalle prime versioni un sistema di sicurezza migliore e risulta essere facilmente utilizzabile anche su piattaforme non Microsoft. In più PPT utilizza GRE e questo può rappresentare un problema in quanto alcuni ISP bloccano il traffico GRE.

Altri utilizzi di SSL

E' possibile usare SSL anche per altri scopi:

-**Proxying.** Il client usa HTTPS fino alla VPN Gateway (con funzione di proxy). Il Gateway usa HTTP per collegarsi al server.

-Traduzione di applicazione (**Application Translation**). E' possibile usare SSL anche su protocolli nati senza autenticazione (FTP, SMTP, POP, IMAP). E' possibile utilizzare HTTPS fino al VPN Gateway, che poi provvede alla traduzione del pacchetto nel protocollo corretto.

-**Port Forwarding.** Grazie a SSL è anche possibile ricevere dati su una porta e inoltrarli su un'altra. E' possibile usare una porta per contattare il VPN Gateway, che poi invia la richiesta su una porta specifica del server. Il port forwarding può avvenire sia sul VPN gateway, sia sulla macchina utente. Questo meccanismo funziona solo con i protocolli che usano solo porte fisse.

-**Newtork extension.** Questa tecnica permette di creare dei tunnel sicuri per accedere a protocolli non sicuri, mediante l'uso di VPN Gateway.

TRAFFICO AUDIO/VIDEO

Rete telefonica

Quando si parla di trasporto audio/video ci sono essenzialmente due tipi di problemi:

-la **segnalazione** indica come iniziare e mantenere il collegamento.

-la **codifica** indica il modo in cui trasmettere i dati.

In questo corso si studierà solo la segnalazione, a parte qualche piccolo accenno sulla fase di codifica, per avere un'idea di cosa si sta trasmettendo.

Attualmente la rete telefonica, almeno nella parte più interna, è diventata una rete IP, basata su backbone. La parte più periferica è invece ancora in forma analogica.

La rete telefonica è ancora a commutazione di circuito. L'allocazione del circuito è statica ed è costituita da un canale a 64Kbps (640000) full duplex. Ogni campione è di 8bit.

Nella rete telefonica non c'è compressione, nè è prevista la comunicazione ad alta qualità (stereo, codec migliori, ...), se non mediante l'utilizzo di canali a multipli di 64Kbps. Non viene effettuata la soppressione dei silenzi, nè la moltiplicazione statica (non è possibile variare la banda).

Prima dell'inizio della telefonata è necessaria una fase di segnalazione (call step).

Rete dati (VoIP)

Nella parte centrale anche la rete telefonica è composta da una rete a commutazione di pacchetto, in modo da avere moltiplicazione statica, che rende utile la soppressione dei silenzi (si risparmia banda). Si può avere anche compressione (anche se in realtà non si è ancora riusciti a metterla in pratica, in quanto essa porta la perdita di dati, che per le telefonate non risulta importante, ma provoca danni irreversibili nel caso in cui si utilizzino modem o fax). E' possibile trasmettere ad alta qualità.

La rete dati introduce il problema della gestione della qualità della chiamata, in quanto la banda non è prenotata e quindi non garantita; inoltre i tempi di attraversamento e di interarrivo (jitter) sono aleatori e non garantiti a priori.

Vantaggi del VoIP

Diversi soggetti hanno visto diversi miglioramenti con l'arrivo del VoIP:

-**consumer** non ha costi aggiuntivi oltre alla connessione a internet.

-**telecom** può trasmettere più dati con minor banda, grazie alla commutazione di pacchetto.

-**enterprise** (utente aziendale) non ha costi aggiuntivi, può personalizzare il servizio (inoltre delle chiamate a seconda di vari parametri, informazioni sul traffico, sulle chiamate, e-presence, instant messaging, videochiamata, condivisione di applicazioni, trasferimento files).

ToIP

ToIP è una via di mezzo tra VoIP e rete telefonica, che permette di continuare ad utilizzare i terminali normalmente utilizzati per la telefonia, ma che in verità trasporta i dati via IP. In questo modo non è necessario cambiare i terminali di rete, ma solo le centraline telefoniche. Il ToIP non offre servizi aggiuntivi/innovativi, ma è solo una tecnica diversa del trasferimento del traffico voce. Con ToIP è possibile anche collegare dei PC, alcuni collegati direttamente alla rete IP del gestore, altri nella rete internet.

Flusso VoIP

Esso è schematizzabile in fasi:

-**campionamento** trasforma il segnale da analogico in digitale. E' importante la frequenza di campionamento e la sensibilità, che determina l'errore di quantizzazione. Questi due fattori influiscono sul bit rate teorico.

-**codifica** comprime i dati. La codifica influisce sul bit rate effettivo, in quanto è dato dal bit rate teorico/fattore di compressione. In questa fase è prevista la soppressione del silenzio (con inserimento di rumore bianco) e la cancellazione dell'eco. La codifica necessita del tempo e quindi introduce un certo ritardo (in più alcune codifiche, ad esempio MPEG, necessitano dei frame successivi per essere calcolati). La codifica può essere:

--codifica **per differenze** (senza perdita). Esso può essere predittiva o statica.

--codifica **pesata**.

--codifica **a perdita**.

-**pacchettizzazione** è una funzione necessaria per abbassare l'overhead degli header, anche se introduce molto ritardo. Essa migliora l'efficienza. I pacchetti normalmente contengono circa 20/40ms di informazione.

-**accodamento** mentre si attende che il pacchetto venga effettivamente inviato. Alcuni router cercano di avere un accodamento a priorità, in modo da far passare prima i pacchetti audio/video rispetto al resto del traffico. Il problema è che il compito di marcare il traffico è spesso lasciato all'utente, che quindi può marcare anche pacchetti che in realtà non sono A/V.

-**trasferimento** è la fase più delicata del flusso VoIP. Il tempo necessario a trasmettere completamente il pacchetto è limitato superiormente dal tempo di trasmissione del pacchetto stesso. Avere MTU troppo elevate dà problemi.

-**de-jitter** serve ad annullare i tempi di interarrivo. I pacchetti che arrivano troppo tardi vengono considerati persi.

-**riordinamento**

-**decodifica** decompone i dati. Questa fase è messa in atto dal riproduttore.

-**controllo dell'errore**, basata su bit di parità (ridondanza). La ritrasmissione non può essere effettuata, in quanto richiederebbe troppo tempo.

Protocollo di trasmissione RTP (Real-Time Protocol)

RTP è un protocollo pensato per trasportare pacchetti audio/video. RTP non gestisce la frammentazione e il riassettaggio dei pacchetti, poiché i pacchetti sono normalmente molto piccoli (per evitare problemi di attesa).

Esso non gestisce gli errori di trasmissione, poiché spesso la ritrasmissione non è necessaria. Non specifica il formato dei dati, in modo da permettere un buon numero di codifiche.

RTP completa il livello 4 insieme a UDP e non necessita in modo restrittivo di reti IP, anche se in realtà viene usato soprattutto su di esse. RTP è usato solo dalle macchine che sono alle estremità della comunicazione, non è quindi necessario che i router intermedi comprendano i pacchetti RTP.

L'RTCP è il protocollo associato all'RTP per il monitoraggio e il controllo della comunicazione.

I campi più importanti dell'header RTP sono:

-**payload** type indica il tipo di dato che viene trasportato. Le codifiche sono standard. Il payload type è indicato in ogni pacchetto, in modo da lasciare la possibilità all'utente di modificare la codifica al volo. In questo modo è anche possibile adattare la codifica, grazie alle informazioni raccolte dall'RTCP.

-Synchronization source identifier (**SSRC**) serve ad identificare la sorgente del messaggio, in modo da poter sincronizzare microfono/webcam e altri dispositivi.

-**numero di sequenza** serve a verificare la presenza di pacchetti persi.

-**timestamp** ha un significato diverso a seconda del payload. Serve per l'ordinamento e insieme al numero di sequenza

serve a riconoscere quali siano i pacchetti persi e quali siano i momenti di silenzio.

-n contributing source identifier (**CSRC**) serve nel caso in cui ci siano dei mixer (dispositivi che servono ad capire la provenienza dei flussi nel caso in cui essi vengano uniti in un'unica sorgente). I campi CSRC sono facoltativi e il loro numero è contenuto in un campo CC. Il mixer è utile per risparmiare banda.

Non è possibile stabilire a priori porte standard per l'RTP, in quanto i flussi RTP possono essere molteplici in parallelo su porte diverse.

Gateway tra reti telefoniche e IP

Il gateway che collega una rete telefonica alla rete IP privata e poi al nuovo gateway è formato da diversi gateway:

-**gateway per i campioni audio** ad alta velocità.

-**gateway per la segnalazione** gestisce dei toni. La frequenza dei dati è molto più bassa, ma i dati sono molto più complessi. In più esso deve riprodurre dei suoni, introducendo dei pacchetti gestiti dal media gateway.

-**gateway per il controllo**.

Protocolli di segnalazione

Gli scopi della segnalazione sono:

-l'**indirizzamento**.

-il **trasporto dei dati**.

-la **sicurezza** della comunicazione (cifatura, autenticazione, ...).

-supporto a **servizi aggiuntivi**.

-**semplicità**.

I principali standard sono H.323 ITU (è un gruppo di protocollo più vecchio e più complesso) e SIP (è HTTP like e molto semplice).

H.323

E' ancora molto usato, ma in futuro dovrebbe finire in disuso, a causa della sua complessità. Esso è stato pensato per funzionare su reti locali (in quanto un tempo non c'era abbastanza banda sulle reti geografiche per gestire il traffico A/V). Esso supporta audio/video e lavagna distribuita.

Prevede la presenza di un gatekeeper, con la funzione di gestire la comunicazione tra due o più client.

La multipoint control unit (MCU) ha lo scopo di negoziare i metodi di comunicazione tra i due interlocutori e di fungere da mixer/switch dei flussi. L'MCU è utilizzata in caso di conferenza tra 3 o più terminali.

Una zona è definita come un insieme di elementi H.323 gestiti da un solo gatekeeper.

I dati A/V viaggiano su RTP affiancati dall'RTCP. In più, per il controllo della segnalazione vera e propria, esistono diversi tipi di protocolli, che funzionano direttamente su TCP/UDP:

-**RAS control**.

-**call control**.

-**control**.

-**dati**.

SIP

SIP (Session Initiation Protocol)

E' un protocollo di livello applicativo, definito dall'IETF. SIP è stato costruito ex-novo senza usare standard precedenti, in modo da sfruttare le caratteristiche della rete IP.

Ha scopi limitati:

-**protocollo di controllo** (segnalazione).

--non si specifica il tipo di trasmissione (audio/video).

--non si prenotano risorse sulla rete.

-**semplicità**.

-**segnalazione di tipo end-to-end** (trasparente ai router che attraversa).

-**sfrutta protocolli esistenti** come RTP/RTCP, SDP (descrive le caratteristiche della comunicazione), RSVP, SAP, ...

-possibilità di **riconoscimento** di un utente indipendente dall'indirizzo IP, attraverso il name mapping.

-**personal mobility** consente l'inoltro in caso di mancata risposta.

Il formato è HTTP-like (stringhe ASCII) e prevede un'interazione di tipo client-server.

SIP può funzionare su TCP (utile per aggirare i firewall), UDP (molto semplice da usare) e SSL (TLS, che consente la cifatura).

Non è prevista la frammentazione (quindi i pacchetti sono al massimo di 1500B) in quanto i messaggi non sono molto grossi.

SIP consente:

- chiamate vocali** (conferenza multipla non ancora implementata).
- e-presence** (per vedere lo stato di un utente).
- instant messaging**.
- lavagna condivisa** (non sempre supportata).
- file transfer**/giochi interattivi (non molto supportata).
- VoIP**, per motivi economici è la cosa meglio supportata.

SIP e VoIP

SIP svolge alcune funzioni necessarie per la gestione di una trasmissione VoIP:

- localizza** l'utente, associando lo username di un utente con l'indirizzo IP usato in quel momento.
- definisce i mezzi** che ha a disposizione un utente e quali codec supporta
- informa la rete dello stato** in cui si trova l'utente
- stabilisce i **parametri** della comunicazione
- gestisce i **servizi supplementari**, come l'aggiunta di più utenti ad una conversazione, il trasferimento delle chiamate,

Protocolli usati da SIP

La gestione di una chiamata avviene con la creazione di un flusso audio/video accanto ad un flusso di controllo, come l'RTCP. Per rendere più semplice il protocollo di comunicazione si utilizzano altri protocolli:

- RTSP** (usa IP) serve per controllare (avanti/indietro...) le trasmissioni in streaming. Non è detto che sia utile.
- SDP** è contenuto dei messaggi SIP.
- SIP** usa TCP/UDP e Definisce i parametri della connessione.
- T.120** serve per mandare dati.

SDP (Session Description Protocol)

SDP ha il compito di definire i parametri delle sessioni multimediali SIP. Grazie a SDP i partecipanti alla conversazione SIP capiscono quali siano:

- il numero dei **flussi dati/controllo**.
- il **tipo** dei dati.
- codec** di comunicazione.
- il **protocollo di trasporto**.
- la **banda** da utilizzare.
- gli **indirizzi** e le **porte** coinvolte.
- il **tempo di inizio e di fine** del flusso (per lo streaming).
- informazioni** sulla sorgente.

SDP esisteva già prima dell'introduzione di SIP e quindi alcune sue parti non sono più utilizzate da SIP. I messaggi SDP sono in formato testuale e possono essere inclusi in pacchetti SIP, mentre le informazioni di controllo viaggiano a parte.

Alcuni attributi di SDP sono:

- v**, versione.
- o**, chi ha creato la sessione.
- s**, il nome della sessione.
- u**, URI della sessione.
- m**, numero del media e indirizzo di trasporto.

Componenti SIP

Per gestire SIP sono necessari alcuni server accessori:

- User Agent** (Client-Server). La parte client serve per inviare una richiesta di chiamata, al contrario il server serve per rispondere ad una richiesta. Questa parte può essere svolta da un software oppure da un terminale utente con l'aspetto di telefono.
- Registrar** Server serve a raccogliere tutte le informazioni sugli utenti connessi. Associa ad un cliente un indirizzo IP. Serve inoltre a gestire dei meccanismi di autenticazione, consultando un AAA Server.

-**AAA** Server contiene le informazioni di autorizzazione, accounting e autenticazione necessarie alla gestione della rete. Questo server è normalmente già presente sulla rete per altri scopi.

-**Location** Server serve per cercare e localizzare un utente, siccome gli user possono cambiare IP.

-**Proxy** Server (Outbound/inbound) serve per connettersi verso domini esterni, in quanto SIP è basato su domini. Risolve anche problemi di NAT, in quanto può svolgere funzioni di relay (un client può chiamare il proxy server al posto che un altro client direttamente).

-**Redirect** Server serve per redirigere il traffico a seconda di alcune condizioni (tenta, ad esempio, di "inseguire" l'utente in base ad indirizzi IP noti).

-**Media** Server serve per contenere le caselle vocali (segreterie telefoniche), in modo da essere raggiungibili in ogni momento, anche quando il client è spento. Può contenere anche dei messaggi preregistrati per svolgere funzioni.

-**Media Proxy** serve per filtrare il traffico A/V o effettuare transcodifiche. Viene usato per semplificare i client.

-**MCU** serve per svolgere funzioni di mixer (per trasmissioni multicast). Viene usato per semplificare i client (il client non deve gestire chi entra/esce dalle conversazioni).

-**Gateway** serve per gestire i collegamenti con la rete telefonica.

Molto spesso i server sono raccolti su un'unica macchina (registrar, SIP proxy e Redirect, Media Proxy vanno a formare il SIP server).

Caratteristiche SIP

Gli indirizzi hanno la stessa forma della posta elettronica (nome@dominio). Anche il meccanismo di traduzione di alias->IP avviene in modo simile alla posta elettronica. La differenza è che nel DNS server non è presente l'indirizzo IP del destinatario, ma l'indirizzo IP del dominio del SIP server. In questo modo si consulta poi il Registrar server (che può essere collocato nel SIP server stesso), che associa l'indirizzo IP corretto. Nella fase di connessione (login) è necessario che il client si vada a registrare dal proprio SIP server.

L'indirizzamento tra domini segue la filosofia standard internet:

- **nomeutente@dominio.com**

- **num_telefono@gateway**, in cui il numero di telefono è un numero di rete telefonica.

E' possibile personalizzare il protocollo di trasporto, l'indirizzo multicast e il time to live.

Per la gestione dei domini SIP vengono usati due record DNS:

-record **SRV** dà le informazioni sul server e sulle priorità. Il formato è **_servizio._protocollo.nomedominio TTL Classe**(IN per reti ip, ...) tipo(SRV) Priorità(per gestire più server in un determinato ordine, priorità più alta associata a numeri più bassi) peso(per gestire il bilanciamento del carico, ad esempio si può dare ad un server il doppio del traffico rispetto ad un altro) porta (associata al protocollo) target.

-record **NAPTR** dà le informazioni su un servizio il formato è **dominio-name classe NAPTR order** (definisce le precedenze) **preference** (bilancia le richieste) **flag service regexp** (permette di definire gruppi di utenti) **target** (nome del servizio).

Conversione dei numeri di telefono

I numeri di telefono classici seguono lo standard E.164, mentre gli indirizzi SIP utilizzano un altro formato.

Per effettuare le chiamate da un terminale classico alla rete SIP è necessario avere dei meccanismi di conversione per rendere i numeri SIP compatibili.

In un certo senso, anche i numeri E.164, per mezzo dei prefissi, usano criteri gerarchici.

Al momento non ci sono standard, che permettano le chiamate da SIP verso la rete telefonica, mentre ENUM risolve il problema contrario.

Standard ENUM

Occorre disporre di un'applicazione (ENUM) con lo scopo di tradurre un numero in un dominio ed effettuare la richiesta al DNS. La procedura è riassumibile nei seguenti passi:

-si **eliminano i caratteri** che non sono cifre all'interno del numero di telefono (ad esempio il "+").

-si **inverte** il numero di telefono.

-si mettono dei **punti** tra una cifra e l'altra.

-il risultato è un nome DNS a cui **si aggiunge e164.arpa**.

-il **DNS risponde** con una lista di NAPTR, che contiene una regexp, che indica l'operazione da fare.

I casi possibili sono:

-**chiamata da gateway VoIP verso SIP**, il gateway traduce l'indirizzo e fa una richiesta al DNS. Il DNS restituisce l'IP del SIP server. A questo punto viene contattato il server SIP, che inoltra la chiamata all'utente (poiché il client potrebbe

essere sotto NAT).

-**chiamata da SIP a SIP**, il DNS restituisce l'indirizzo del SIP server, che inoltra la chiamata.

Per realizzare una struttura SIP completamente funzionante è necessaria un'infrastruttura di scala mondiale. Al momento questa infrastruttura è difficile da realizzare, in quanto gli stati hanno visioni differenti sull'ente a cui affidare il controllo. In Germania, ad esempio, il controllo è stato affidato ad un'organizzazione neutra, in Cina e in Francia, invece, l'assegnazione del dominio è affidata all'ITU (dell'ONU).

Il problema si è risolto, facendo in modo che ogni nazione gestisca a modo proprio i numeri con il proprio prefisso nazionale.

I meccanismi di ENUM possono essere usati all'interno di reti più piccole. In questo caso si utilizzano numerazioni distinte a seconda se si vuole contattare un numero interno all'infrastruttura oppure un esterno.

Messaggi SIP

Essi sono composti da stringhe ASCII con il seguente formato:

- tipo** del messaggio
- una serie di **header** SIP
- una **linea vuota** (CRLF)
- il **Payload** (SDP), che è opzionale.

I messaggi tipici sono:

- REGISTER** serve per registrare un indirizzo SIP all'interno di un server. Il server è ricavato dal dominio. Le richieste di registrazione possono essere fatte a più server contemporaneamente.
- INVITE** è la richiesta di comunicazione. Il messaggio viene mandato verso un server e può essere inviato anche durante una conversazione. Esso contiene una descrizione SDP, che indica i parametri di comunicazione.
- ACK** indica una conclusione positiva alla richiesta di chiamata (viene generato dal chiamante) e viene inviata per iniziare la comunicazione vera e propria. Può contenere una descrizione SDP, che descrive i parametri di comunicazione (opzioni, protocolli, ...).
- BYE** indica la chiusura A/V.
- CANCEL** cancella una richiesta di connessione ancora pendente. Può anche essere usato per chiudere le fork(), nel caso in cui uno stesso utente abbia registrazioni multiple su indirizzi IP diversi, nel momento in cui la chiamata abbia esito positivo su uno degli indirizzi.
- OPTIONS** dichiara le capacità dello user agent.
- SUBSCRIBE** segnala la richiesta di voler conoscere lo stato di uno user agent.
- NOTIFY** informa dello stato di un UA
- MESSAGE** inoltra un messaggio (testo/XML) usato per l'istant messaging.

Le intestazioni degli header più importanti sono:

- From** identifica il chiamante (in ogni fase della comunicazione)
- To** indica il chiamato.
- Contact** è l'indirizzo IP del chiamato.
- Via** traccia i server SIP attraversati da un messaggio.
- Record Routing** impone che tutti i pacchetti debbano attraversare i proxy server, al posto che raggiungere direttamente il destinatario (necessario in caso di NAT).
- Call-ID** identifica la chiamata.
- Cseq** indica la sequenza dei messaggi, in quanto è possibile il trasporto UDP, il quale non garantisce l'arrivo in ordine dei messaggi.
- Subject** è il soggetto della chiamata.
- Content-type** indica il tipo e il sottotipo del contenuto del pacchetto SIP (MIME).
- Content length** indica la lunghezza del payload.
- Content encoding** indica le elaborazioni sui messaggi (UTF-8, aschi, 7bit, ...).

Le risposte possono essere composti da codici numerici. I principali sono:

- 1xx** indica risposte provvisorie:
- 100** indica che si sta cercando il destinatario.
- 180** indica che il destinatario è stato trovato e che il suo telefono SIP sta suonando.
- 182** indica che la propria richiesta è in coda.
- 2xx** indica le risposte positive:
- 200** OK.
- 3xx** indica la redirectione.

-**4xx** indica errori nel client (errore di sintassi o richiesta non eseguibile):

--**404** indica che il destinatario non è stato trovato.

--**407** indica un errore di autenticazione nel proxy.

-**5xx** indica errori nel server.

-**6xx** indica errori generici:

--**600** indica che il destinatario è risultato occupato ovunque su tutti gli indirizzi.

--**603** indica che la chiamata è stata rifiutata.

Nello standard le comunicazioni vengono distinte in:

-**transazione** sono i messaggi tra una richiesta e una risposta. In questa fase rimangono invariati From, to, call-ID e Cseq.

-**dialogo** è una relazione tra User Agent che inizia quando viene ricevuta una risposta positiva. Il destinatario è all'interno del campo contact.

Risoluzione di un indirizzo SIP

La risoluzione di un indirizzo SIP in un indirizzo IP è una fase necessaria, sia

per cercare un determinato utente per un messaggio INVITE, sia per effettuare una REGISTER. La procedura è:

-contattare un server DNS per una **query NAPTR** (si scoprono i nomi dei servizi)

-contattare il server DNS per una **query SRV** (si scoprono i server che svolgono quei servizi).

-contattare il server A/AAAA per gestire l'**autenticazione**.

Nel caso in cui ci siano risposte da parte del DNS alle richieste NAPTR e SRV (magari perché filtrate da un firewall), si usano nomi standard. In questo caso viene fatta direttamente la richiesta A/AAAA.

Solitamente le risposte del server DNS ad una richiesta NAPTR includono anche tutte le risposte SRV possibili.

Sicurezza e SIP

La sicurezza in SIP si ottiene nei seguenti modi:

-**autenticando** ogni utente, mediante l'AAA Server.

-**cifrando il corpo dei messaggi** SIP (non della telefonata) e dell'elenco dei nodi intermedi su cui è transitato il messaggio (è possibile che si creino dei loop).

-gestendo dei meccanismi per risolvere i problemi di **spam** e di **Denial of Service**.

Generalità

Skype è un protocollo VoIP proprietario, in continua evoluzione e non conosciuto completamente. Skype usa molti concetti delle reti PeerToPeer, in quanto gli sviluppatori sono gli stessi di Kazaa.

Caratteristiche di Skype

Skype risulta avere numerosi punti di forza a SIP, ma anche alcuni punti deboli che lo rendono poco utilizzato a livello aziendale:

-**Non è necessario avere indirizzi pubblici** per il VoIP (i NAT non sono un problema).

-**La qualità del servizio non è un prerequisito necessario** per Skype (in quanto la rete al momento è abbastanza libera).

-**Non sono necessarie infrastrutture costose** per utilizzarlo.

-Ha dimostrato che **una rete P2P può essere utile** anche per altri scopi oltre alla condivisione di file.

-La voce può essere trasmessa anche su **TCP** (nonostante TCP preveda la ritrasmissione e alcuni sistemi di controllo della congestione).

-**buca i firewall**. Questo è possibile grazie a TCP e a diverse tecniche:

--la **chiamata** è spesso **diretta**.

--**triangolazione** attraverso relay (senza perdita della qualità).

-**soppressione di pause ed eco**.

-ottima **gestione della voce**.

-è **free**, ma con codice criptato. La struttura del programma non è convenzionale e quindi è probabile che sia compilato in modo custom. E' presente un meccanismo di offuscazione del codice. E' impossibile il debugging (in quanto sono previsti dei meccanismi che controllano la velocità di esecuzione).

Struttura logica dell'overlay

Skype si basa su client e supernodi (che non sono altro che nodi client promossi a supernodi). E' presente un bootstrap server, utile per le prime connessioni (quando un client non ha l'indice dei supernodi in cache).

I supernodi contengono l'indice dei nodi vicini, cercano i supernodi vicini e si scambiano informazioni. I supernodi devono quindi gestire traffico aggiuntivo (circa 5Kbps). E' possibile disabilitare la possibilità di diventare supernodo (non ufficialmente). In alcune versioni è anche possibile forzare la scelta di un supernodo attraverso l'editing di un file di configurazione.

Skype ha inoltre numerosi gateway in molti paesi, in modo da consentire costi di chiamata ridotti anche a numeri fissi.

Fase di Boot

Il client si collega ad uno o più supernodi, salvati in un file locale. In mancanza di una lista o in caso di connessione fallita ci si collega ad un insieme di nodi predefiniti, detti bootstrap servers.

Il protocollo preferito è UDP, anche se in caso di fallback è TCP (nel caso in cui ci si trovi in una rete con firewall). Le porte cambiano spesso (per evitare che si venga scoperti dai firewall).

Fase di Login

Per iniziare la comunicazione è necessaria una fase di login presso un server specifico.

Un primo tentativo è fatto contattando direttamente il server, mentre, in caso di fallimento, la richiesta di login viene inoltrata attraverso i supernodi.

Viene controllata se la versione usata è l'ultima disponibile.

Viene usato un protocollo STUN-like per capire se si è dietro un NAT.

Ricerca di un utente

La ricerca viene fatta attraverso il supernodo al quale ci si è collegati. Per questa fase non si usa mai il login server per evitare che Skype venga bloccato. La ricerca non è chiara, ma comunque avviene mediante la replicazione dell'indice tra i supernodi. Un utente è sempre localizzabile se si è collegato nelle ultime 72 ore.

E' possibile la ricerca mediante wildcard (è quindi possibile ricercare un utente mediante parte del nome). In questo caso la ricerca è più onerosa.

Scambio dei dati (VoIP)

Normalmente il collegamento è diretto (nel caso in cui gli host siano pubblici o uno solo sia dietro NAT). Nel caso in cui questo non sia possibile la fase di collegamento si ottiene mediante la triangolazione grazie ai supernodi. In questo caso il traffico è criptato.

E' inoltre possibile lo scambio file, che si ottiene nello stesso modo del VoIP (è abbastanza lento nel caso di triangolazione).

Trasmissione della voce

I codec utilizzati sono standard ed occupano una banda 3-16 Kbps. Non c'è soppressione dei silenzi ed un'ottima gestione del ritardo.

Rispetto agli altri meccanismi VoIP, Skype permette, come detto, la comunicazione TCP.

Altre funzionalità

Oltre al VoIP, Skype permette:

- conferenza multipla**, mediante l'utilizzo di un client HUB. Non è quindi richiesto il set-up di nodi aggiuntivi.
- instant messaging**, non interoperabile con altre reti.
- e-presence**.
- file transfer**, anche se con scarse prestazioni.

Bloccare Skype

E' difficile bloccare Skype in ogni fase della sua esecuzione:

- durante la **comunicazione** è molto difficile in quanto usa indifferentemente TCP e UDP di qualunque porta (ogni tanto usa addirittura la porta 80).
- durante la **fase di autenticazione** è difficile perché dovrebbero essere bloccati tutti i collegamenti con i supernodi e tutti i pacchetti diretti ai Bootstrap Servers.
- durante la **fase di login** è impossibile perché dovrebbero essere bloccate le richieste inoltrate all'overlay.
- durante lo **scambio di dati** è difficile perché è cifrato e spesso diretto.

Problematiche di Skype

Skype è un protocollo molto utilizzato in ambito privato, ma usato raramente in ambito aziendale, in quanto:

- Skype non può garantire una certa **qualità del servizio**, in quanto è fuori dalla pila dei protocolli di rete. L'infrastruttura P2P è robusta, ma il singolo nodo può essere inaffidabile.
- Il **codice è chiuso** e i protocolli proprietari (impossibile sapere come vengono trattati i dati).
- Problemi di **intercettazione** (legali).
- L'**overlay** non è influenzabile dall'utente (impossibile il controllo da parte dell'utente sul destinatario delle proprie informazioni).

RETI GEOGRAFICHE

Collegamenti

Per rete geografica si intende un insieme di collegamenti che utilizza protocolli di livello 2 o 3, in grado di interconnettere reti più piccole, che si trovano fisicamente lontane. Un tempo le reti geografiche erano di tipo analogico o digitale, anche se ormai la maggior parte delle reti analogiche (CDA e X.25) sono state abbandonate. Prevalentemente all'estero, negli anni '90 sono state sviluppate le reti metropolitane (DQDB e SMDS), che avevano lo scopo di interconnettere ad alta velocità le città. Con l'avanzare della tecnologia e con la possibilità di cablare ad alta velocità lunghe distanze, le reti metropolitane sono state ormai accantonate.

I collegamenti geografici usano diverse tecnologie:

- CDN** (collegamenti diretti numerici), mediante TDM, frame relay, MPLS, ATM, ...
- telefonia digitale**, mediante ISDN, ATM, ...

ISDN

ISDN non ha avuto un grande successo in Italia, in quanto la tecnologia è arrivata un po' troppo tardi. Essa prevede un unico collegamento a velocità fissa, che permette la Fonia e il trasporto dei dati. Anche il terminale telefonico deve essere digitale. ISDN esisteva (anche se è ancora usata in alcune località) in due versioni:

- 2B+D** prevede 2 canali dati a 64Kbps e 1 canale di segnalazione a 16Kbps.
- 30B+D** prevede 30 canali a 64Kbps e 1 canale di segnalazione a 16Kbps.

TDM (Time Division Multiplexing)

TDM è un protocollo, che permette l'esistenza di più flussi di dati all'interno di un unico canale. Tutta la banda disponibile viene data ad ogni flusso ad intervalli regolari. Se ad un flusso di dati sono assegnati più slot di tempo del canale la banda assegnata al flusso aumenterà. Al momento questa tecnologia è usata solo per i collegamenti punto a punto.

SDH (Gerarchia sincrona digitale)

SDH è stato implementato in diverse versioni, che permettono ai flussi di dati di viaggiare a velocità standard (a partire da 1.5Mbps a 2.4 Gbps e oltre). SDH prevede l'esistenza di un multiplexer (MUX) a divisione di tempo, che svolge funzioni simili ai MUX del TDM, anche se prevede intervalli di tempo uguali per ogni canale. I MUX e i DEMUX devono essere sincronizzati tra loro e molto veloci (soprattutto per funzionare con le versioni più spinte).

Spesso all'interno delle linee che usano MUX-DEMUX sono inseriti dei ripetitori, che permettono di evitare problemi di attenuazione. Sono presenti anche degli Add/Drop MUX che permettono l'uscita di un canale oppure l'inserimento in uno slot libero.

La nomenclatura risulta essere:

- sezione**, collegamento tra un MUX e un ripetitore.
- linea**, collegamento tra un MUX e un Add/Drop MUX.
- percorso**, collegamento tra due MUX.

Formato delle trame SDH

In questo paragrafo si prende in considerazione la versione STS-1.

Il frame SDH è una matrice composta da 9 colonne e da 125 righe. Ciascuna cella è da 1B. Questa trama si ripete ogni 125 micro secondi (8Ktrame/secondo). Il carico utile (payload) è meno dello spazio totale disponibile, in quanto per ogni frame sono inserite informazioni aggiuntive necessarie per il collegamento.

Per aumentare la banda nelle versioni successive si è aumentato il numero di byte per ogni cella, mentre il tempo di trama non è stato modificato, in quanto è comune a tutte le linee e permette la loro interoperabilità. PDH è una variante di SDH.

X.25

X.25 è un protocollo che usa il livello 2-3 a circuito virtuale. Ciascun circuito virtuale è impostato manualmente (i pacchetti non sono instradati dinamicamente come con il protocollo IP).

X.25 è stato concepito per reti molto rumorose e poco affidabili e per questo prevede la presenza di ACK. Questa scelta ha implicato che con la crescita della velocità del canale si dovessero avere finestre di trasmissione sempre più grosse, con la conseguente crescita della dimensione dei pacchetti da memorizzare in attesa di conferma. Per questo motivo non è più molto usato.

Frame Relay

E' simile all'X.25 ma è solo di livello 2. Non è più presente l'ACK e quindi non si va incontro ai problemi di X.25.

CIR=Bc/Tc indica il numero massimo di bit nell'unità di tempo che possono essere inseriti nella rete (a seconda di un accordo).

Il ritardo introdotto dal Frame Relay è minore rispetto a X.25 e le prestazioni sono complessivamente migliori.

ATM (Asynchronous Transfer Mode)

ATM è un protocollo di comunicazione che si basa sul multiplexing statistico, che permette il multiplexing di linee non allineate temporalmente. ATM è nato per rimpiazzare Ethernet e spopolare nelle reti geografiche. Questi obiettivi non sono stati raggiunti, in quanto al momento ATM è usato solo nelle reti ADSL, per collegare il DSLAM alla rete dell'operatore che offre il servizio.

Le caratteristiche principali sono:

- segnalazione sofisticata.**
- meccanismi di controllo** di flusso molto avanzati.
- allocazione dinamica** della banda.
- granulosità fine** nell'assegnazione della banda.
- supporto al **traffico bursty** (a blocchi).
- adattabilità** sia ad applicazioni sensibili al ritardo, sia a quelle sensibili alla perdita.
- commutazione di cella di dimensione fissa.** Ogni cella è di 53 ottetti, di cui 5 di intestazione e 48 di dato. La dimensione fissa semplifica la commutazione. La dimensione piccola evita problemi di frammentazione e consente trasmissione A/V.
- inserimento di **priorità.**
- metodi per **dividere/assemblare segmenti.**

MPLS

Struttura fisica delle reti geografiche

La struttura delle telecomunicazione può essere rappresentata con un diagramma a cipolla. A partire dall'interno:

-**WDW** (wide length mux). Per ciascuna fibra ottica ci sono più segnali su lunghezze d'onda (frequenza) diverse.

Esistono dei metodi per mettere IP su DWDM, grazie all'estrazione/immissione dei canali. E' difficile però perché la commutazione è troppo rapida e per questo si fanno principalmente canali punto a punto.

-**SONET/SDH.** Viene fatto il time divisioning mux su ogni canale WDW.

-**ATM** oppure Frame Relay.

-**IP.**

Questa struttura è troppo complessa, in quanto ci sono troppe tecnologie e quindi risulta essere molto costosa da mantenere.

MPLS

Per cercare di risolvere i problemi portati dalla struttura a cipolla prevede di inserire sopra allo switching in frequenza una struttura basata su IP/MPLS. In questo modo si possono risolvere molti problemi di costi.

In più IP ha il problema della convergenza delle ruote verso un'unica zona della rete verso la stessa destinazione, anche se si parte da mittenti diversi. Questo porta a un sovraccarico di alcune aree della rete.

L'idea su cui si basa MPLS è quella di instradare i pacchetti IP in base ad un label, che rappresenta il nome di un circuito virtuale (commutazione di circuito).

La commutazione di circuito risulta essere molto più veloce della commutazione di pacchetto basata sul longest prefix match dell'IP (può essere gestita in hardware).

Grazie alla commutazione di circuito è anche possibile instradare il pacchetto secondo la politica preferita, in quanto è possibile imporre il percorso.

Per realizzare questa tecnologia sono necessari diversi dispositivi:

- LSR** (Label switch router) non hanno collegamenti con dispositivi esterni alla rete MPLS. Essi hanno una tabella (per ogni porta) che indica l'instradamento (data una label x su una porta x1, viene indicato la porta x2 dove smistare il pacchetto e la nuova label y).

- Label edge router**, che hanno lo scopo di aggiungere/togliere le label ai pacchetti IP entranti in base a una tabella (per una destinazione d devo mettere una label x).

- Label switched Path** (LSP) sono i percorsi virtuali (tunnel) che partono dall'Ingress router verso l'Egress router.

Esistono diverse versioni:

- MPLambdaS** permette di mettere label in grado di instradare i pacchetti su percorsi a commutazione d'onda.

- G-MPLS** permette il packet/cell/circuit/lambda switching. Queste funzionalità aggiuntive sono realizzate configurando i commutatori manualmente.

Funzionalità MPLS

Le principali funzionalità di MPLS sono:

- possibilità di gestire **flussi a differenti livelli di granularità** (a livello di macchina/sottoreti o di applicazione). Questo significa che si possono prendere percorsi diversi a seconda del tipo di pacchetto (WEB/VOIP) oppure a seconda della destinazione.

- indipendenza dal livello 2/3. Anche se normalmente è usato con IP.

- si **interfaccia con protocolli esistenti** (RSVP e OSPF).

- è **impacchettabile** in altri pacchetti MPLS, in modo da garantire circuiti virtuali tra operatori differenti.

- se si usa ATM o frame relay in coppia con MPLS il **label è derivato** dall'ATM o dal Frame Relay.

Pacchetti MPLS

Ogni pacchetto è formato da:

- 20bit di **label**.

- 3bit di **classe** del servizio (priorità).

- 1bit **flag** indica se è l'ultima intestazione MPLS.

- 8 bit **TTL** indica il time to live.

Funzioni dei router

Le funzioni possibili sono:

- PUSH** aggiunge un label (ingress router).

- POP** elimina il label più esterna (egress router).

- SWAP** cambia un label con un'altra (switch).

FEC (forwarding equivalence class)

I criteri per scegliere un LSP o un altro sono basati sulla scelta della classe. I possibili criteri per attribuire una classe:

- stessa destinazione unicast**.

- stessa destinazione multicast**.

- ottimizzazione** di alcune tipologie di pacchetti (traffic engineering).

- qualità del servizio o **classe di servizio** (VoIP/Web).

- stesso tunnel VPN**.

Il LSP è scelto in base alla label scelta dall'ingress router.

La costruzione delle tabelle è data da messaggi inviati dai router che si trovano più vicini alla destinazione, anche se è possibile stabilire i label staticamente (non scalabile, difficile da implementare, non interoperabile).

Protocolli alternativi e potenzialità di MPLS

Esistono diversi protocolli per mappare le label:

- LDP** permette di convertire IP unicast su labels.

- SRVP** e **CR-LDP** permettono di ottimizzare il traffic engineering.

- PIM** permette di mappare indirizzi IP multicast su labels.

- BGP** è utile per le VPN.

I protocolli di routing utilizzati possono essere:

- OSPF**.

- IS-IS** adattabile ad esigenze specifiche.

- BGP-4**.

-**RIP** non è più usato a causa di problemi.

-**IGRP** è un protocollo di proprietà di CISCO.

-versioni dei protocolli precedenti con in aggiunta della desinenza **TE** (traffic engineering)

Grazie all'MPLS, è anche possibile definire percorsi alternativi in base a dei vincoli (in modo da usare percorsi alternativi senza avere link e router in comune, in modo da garantire il funzionamento anche in casi estremi). Queste informazioni aggiuntive possono essere:

-**capacità** del canale.

-**utilizzo** del canale.

-**dipendenze** dei link.

MPLS e VPN

Grazie a MPLS è possibile effettuare collegamenti virtuali punto a punto di livello 2 (PWE3). E' anche possibile creare collegamenti virtuali di tipo peer.

Pseudo wire emulation end to end (PWE3) prevede che diversi dispositivi customer edge (CE) si colleghino a degli edge router. I vari edge router sono collegati attraverso LSP virtuali tra di loro. I vari LSP sono contrassegnati con gruppi di label differenti. In partenza ad ogni pacchetto IP vengono assegnati due label:

-quello più esterno serve per l'**instradamento nella rete MPLS** (verrà modificato da ogni edge router che incontra).

-quello più interno permette di capire ad ogni **edge router** verso quale CE inoltrare i pacchetti.

Questo tipo di collegamenti virtuali sono principalmente gestiti in modo manuale (ci sono dei tool che permettono la semplificazione di questa procedura). Nel modello peer, invece, è possibile associare reti private tra di loro (ci può essere sovrapposizione parziale degli spazi di indirizzamento). Gli edge router usano una VPN routing and forwarding table (VRF), che associa per ogni rete privata dove si trovano gli indirizzi privati relativi. Per costruire queste tabelle l'edge router guarda i label switch path virtuali che ci sono aperti tra le varie reti. Per comunicare tra loro i vari router usano il BGP, che permette la comunicazione a router non collegati direttamente. Anche in questo caso gli edge router inseriscono due label MPLS (uno per individuare la VPN e l'altro per il percorso). Grazie a questo meccanismo non sono necessari altri dispositivi (VPN gateway, ...). E' possibile anche avere VPN che usano edge router virtuali.

Vantaggi delle VPN basate su MPLS

Usare MPLS porta numerosi vantaggi:

-l'utente ha libertà di scegliere il proprio **piano di indirizzamento** (a meno che in futuro non si voglia collegare la VPN a internet o ad altre VPN).

-i router CE **non scambiano informazioni** addizionali (se non quelle che sarebbero necessarie se i router fossero collegati direttamente) tra di loro.

-l'utente non deve gestire la rete MPLS (**provider provisioned**).

-i provider **non devono avere apparecchi specifici** per ogni utente.

-le VPN **possono estendersi su più provider** (se essi si mettono d'accordo sui collegamenti MPLS).

-**isolamento del traffico**, ma non si ha la cifratura su MPLS (anche se si possono trasmettere pacchetti cifrati di più alto livello).

-è supportata la **qualità del servizio** (anche se in realtà è poco usata).

QoS su IP

Qualità del servizio su reti IP (QOS)

Le reti a commutazione di pacchetto sono nate seguendo la filosofia best-effort, senza quindi garantire tempi di consegna o senza differenziare il traffico. Per ottenere questi risultati si devono usare altri protocolli:

-**RSVP** permette di prenotare alcune risorse

-**servizi differenziati** permettono di classificare il traffico (non si garantisce nulla, ma si garantisce che alcune classi abbiano priorità su altre classi).

-**servizi integrati** permettono di garantire risorse (molto difficile da implementare).

Meccanismi per garantire QOS

Alcuni meccanismi usati sono:

-**politiche di scheduling nelle code** dei router:

--coda standard a **FIFO** non consente la QOS.

--coda a **priorità** (senza diritto di prelazione) invia i pacchetti a seconda della classe di traffico. Esistono quindi code FIFO differenti a seconda della priorità (le code a priorità maggiore vengono svuotate prima di trasmettere i pacchetti

delle code a priorità minore).

--**round robin** cicla a turno tutte le code.

--**weighted fair queuing** permette di gestire pesi differenti per le diverse code, che comunque vengono ciclata.

-**politiche di scarto delle code** dei router:

--**tail drop** elimina il pacchetto che arriva.

--**priority** elimina il pacchetto a priorità più bassa.

--**random** elimina un pacchetto a caso.

--**RED** elimina dei pacchetti con probabilità maggiore al crescere della lunghezza della coda.

-meccanismi di **policing** (permettono di verificare se ognuno rispetta il proprio limite di traffico) si basano sul traffico medio sul lungo periodo e sulla massima dimensione dei burst (scarica di pacchetti massimo), che viene chiamata dimensione del picco. Il meccanismo più usato è il modello a token (token bucket), che prevede di garantire le risorse in base a dei "gettoni". Se non sono ancora stati usati tutti i gettoni, la risorsa richiesta viene esaudita immediatamente, altrimenti è messa in attesa di un gettone oppure marcata come non garantita. Il numero massimo di pacchetti immessi nella rete è $rt+b$ con r uguale alla velocità di immissione dei token e b uguale al numero massimo di token; b indica anche la dimensione massima del burst.

Con la combinazione delle tecniche precedenti è possibile garantire la QOS. Ad esempio se si utilizza il modello a token unito con un sistema a code di priorità i pacchetti a priorità più alta avremo un tempo di attraversamento garantito di $t=b*L/r$, mentre la banda garantita è data dalla banda minima della rete.

IntServ

Su IP non ci sono problemi di segnalazione in quanto c'è instradamento connection less e in più IP è best-effort.

I problemi di segnalazione su IP nascono quando si vuole una certa QOS. Per questo motivo sono stati introdotti due approcci al problema:

-**Intserv** prevede di trattare il traffico in base al flusso di appartenenza dei pacchetti.

-**DiffServ** prevede di trattare il traffico in base al tipo.

IntServ

IntServ è uno standard, che specifica i descrittori dei flussi. Essi sono basati su:

-**filterspec**, dato dalla destinazione/sorgente.

-**flowspec**, dato dalle caratteristiche del traffico e dai servizi che si vogliono garantire.

Per controllare i flussi, i router sono muniti di un classificatore dei pacchetti, uno schedatore dei pacchetti e un gestore dei buffer. In più è necessario un controllo di immissione per i pacchetti in ingresso, in modo da garantire la prenotazione delle risorse.

Protocollo RSVP

RSVP prevede una serie di messaggi tra i router in modo da dare la possibilità di prenotare risorse per flussi. Il problema principale è che utilizzare i flussi a priorità differenziata è molto complesso da gestire per i router molto trafficati. Un altro problema è la bassa scalabilità del protocollo, in quanto al crescere del numero di flussi, le difficoltà aumentano.

Lo standard è stato completato nel 1994. La maggior parte dei router è in grado di gestire i messaggi RSVP ma, in realtà, solo pochi filtrano realmente il traffico grazie a questo protocollo. RSVP garantisce:

-**perdite**.

-**ritardo**.

-**banda**.

RSVP controlla l'accesso e le tecniche di accodamento di ogni flusso all'interno dei router che lo usano. RSVP è pensato per ricevitori e flussi eterogenei. Il ricevitore chiede alla rete che gli venga attribuito un flusso, in modo che gli venga garantita una certa QoS. Le risorse vengono prenotate in base alle possibilità dei router e non in base all'RSVP.

DiffServ

DiffServ permette di classificare il traffico in diversi tipi indipendenti dai flussi di dati. In questo modo viene semplificato il lavoro dei router. Tutti i pacchetti di una classe vengono trattati allo stesso modo. Nel momento in cui un pacchetto entra in una rete viene classificato e non sono necessarie ulteriori classificazioni (a meno che non si esca da una rete). Questo meccanismo è molto più semplice e scalabile rispetto a IntServ. La classificazione può essere gestita direttamente dall'utente, nel caso in cui si facciano pagare di più i servizi a priorità più alta. SLA indica il tipo di contratto sulla vendita dei servizi (tra clienti e ISP oppure tra ISP), mentre SLS indica le caratteristiche garantite a

seconda del tipo di traffico (burst size). Un DiffServ necessita di un classificatore, uno scheduler delle code e un riclassificatore.

Il campo ToS dell'IP indica la classe di appartenenza del pacchetto. All'interno del DiffServ è stato definito anche il comportamento della classe all'interno di ogni hop (PHB), in quanto essa può variare in ogni router. I parametri di variazione sono impostati dal gestore del router. Gli standard sono:

- expedite forwarding garantisce un rate di servizio maggiore o uguale al valore specificato.

- assured forwarding assegna diverse priorità di scarto a seconda della classe.

E' possibile definire il per domain behavior (PDB), che informa su quale comportamento e quali garanzie si avranno all'interno di un intero dominio. Vengono definiti:

- i **classificatori**.

- i **condizionatori**.

- la **concatenazione** dei PHB previsti.