

## COMMUTAZIONE DI PACCHETTO - COMMUTAZIONE DI CIRCUITO

La commutazione di pacchetto è una tecnica di accesso multiplo a ripartizione nel tempo, utilizzata per condividere un canale di comunicazione tra più stazioni in modo non deterministico, utilizzata generalmente per realizzare reti di calcolatori. Si distingue dalla commutazione di circuito, che è tipicamente usata nelle comunicazioni telefoniche.

Tali tecniche non comportano l'attivazione di una linea di comunicazione dedicata fra un elaboratore ed un altro, ma consentono lo svolgimento simultaneo di più comunicazioni fra computer, massimizzando così l'utilizzazione dei mezzi trasmissivi impiegati.

In una rete a commutazione di pacchetto l'informazione da trasmettere viene suddivisa in pacchetti di dimensione abbastanza piccola; ad ognuno di essi viene aggiunta un'intestazione che contiene tutta l'informazione necessaria affinché il pacchetto possa venire inoltrato alla sua destinazione finale e sulla sua posizione all'interno dell'informazione che viene trasferita. I pacchetti vengono inviati individualmente attraverso la rete e vengono poi riassemblati nella loro forma originale quando arrivano sul computer di destinazione.

L'intera capacità trasmissiva disponibile viene impegnata per la trasmissione di ciascun pacchetto.

Se vi sono più pacchetti da trasmettere contemporaneamente, questi vengono memorizzati in una coda, subendo un ritardo di accodamento e rischiando di essere scartati in caso di esaurimento della memoria disponibile per la coda.

Mentre in una rete a commutazione di circuito la capacità del canale trasmissivo è interamente dedicata ad una specifica comunicazione, la commutazione di pacchetto si rivela molto più efficiente nonostante la maggior quantità di dati inviata, in quanto i canali fisici sono utilizzati solo per il tempo strettamente necessario. Inoltre, poiché ogni pacchetto porta con sé la sua identificazione, una rete può trasportare nello stesso tempo pacchetti provenienti da sorgenti differenti.

La commutazione di pacchetto permette quindi a più utenti di inviare informazioni attraverso la rete in modo efficiente e simultaneo, risparmiando tempo e costi mediante la condivisione di uno stesso canale trasmissivo (cavo elettrico, etere, fibra ottica, ecc.).

Storicamente la commutazione di pacchetto poneva qualche problema nel caso fosse necessaria una disponibilità garantita di banda o nelle trasmissioni real time: si pensi a una trasmissione video, dove le immagini arrivano con un flusso costante. Al giorno d'oggi è però possibile aggiungere una "priorità" ai pacchetti per garantire che un numero sufficiente di essi venga inviato, a scapito di altri pacchetti che non abbiano un'urgenza specifica - ad esempio, un file da trasferire.

La commutazione di pacchetto è uno dei possibili metodi di moltiplicazione, ovvero è una tecnica per suddividere la capacità trasmissiva di un canale tra diversi utilizzatori.

### LAN

LAN è l'acronimo per il termine inglese local area network, in italiano rete locale.

Identifica una rete costituita da computer collegati tra loro (comprese le interconnessioni e le periferiche condivise) all'interno di un ambito fisico delimitato (ad esempio in una stanza o in un edificio, o anche in più edifici vicini tra di loro) che non superi la distanza di qualche chilometro.

Le LAN hanno dimensioni contenute, il che favorisce il tempo di trasmissione, che è noto. Le LAN tradizionali lavorano tra 10 Mbps e 100 Mbps, hanno bassi ritardi e pochissimi errori. Le LAN recenti operano fino a 1 Gbps (ma sono utilizzate solo in ambienti server o storage di grosse dimensioni).

## PROTOCOLLO IPV4

**IPv4** è la versione di rappresentazione di indirizzi IP attualmente in uso dell'Internet Protocol. Esso è descritto nell'IETF RFC 791 pubblicato per la prima volta nel settembre 1981.

Il diagramma seguente mostra come è fatto l'header del protocollo IPv4:

00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
Versione		IHL		Servizio				Lunghezza totale																							
Identificazione										Flags		Offset frammentazione																			
TTL				Protocollo				Checksum																							
Indirizzo mittente																Indirizzo destinatario															
Opzioni												Padding																			

Notare che la larghezza della cella è proporzionale alla lunghezza del campo. In testa alla tabella sono numerati i bit. Di seguito riporto il sorgente contenuto nella libreria *ip.h* di Linux.

L'indirizzo IPv4 è formato da 32 bit, esso è univoco sulla rete di cui fa parte. Tale indirizzo, inoltre, non va assegnato all'host, ma alle connessioni fisiche alla rete che l'host possiede (nel caso di host multicollegati o di dispositivi di rete). Si è però verificato che i primi paesi in cui si è diffuso Internet e all'interno di essi i primi provider, si sono "accapparrati" un numero di Ip proporzionalmente sbilanciato. Gli ultimi provider hanno pertanto dovuto ricorrere ad un sistema per ovviare alla scarsità degli IP a loro attribuiti. Hanno pertanto considerato gli utenti a loro connessi di una intera città come un'unica LAN e pertanto tutti dotati dello stesso IP.

Concettualmente l'indirizzo IP si compone di due parti:

1. identificatore di rete e precisamente della sottorete
2. identificatore di host

Per semplificarne la lettura, ogni indirizzo IP viene descritto con 4 numeri in base decimale, in modo che ognuno rappresenti un byte (il valore di un byte varia da 0 a 255 quando lo consideriamo in base dieci), separati dal simbolo "punto"; un esempio di indirizzo IPv4 è 192.0.34.166.

Ogni indirizzo in cui l'identificativo host presenta tutti 0 ci si riferisce alla rete, mentre se tutti i bit di questo identificativo sono a 1 ci si riferisce ad una trasmissione broadcast diretta.

(broadcast: si intende la trasmissione di informazioni da un sistema trasmittente ad un insieme di sistemi riceventi non definito a priori. Esempio La Radio)

In pratica quando ad un router arriva un pacchetto con un indirizzo host con tutti bit a 1, questo esegue un broadcast a tutti gli host della sottorete.

Se un host deve comunicare con un altro host della stessa sottorete, userà il protocollo di livello 2 della rete a cui è collegato, altrimenti dovrà inviare i pacchetti ad un gateway o router, che sarà connesso ad altre reti e si occuperà di inoltrare i pacchetti ricevuti.

La comunicazione tra i router avviene mediante indirizzi IP utilizzando delle tecniche particolari di indirizzamento per individuare la sottorete e l'host.

Originariamente lo schema delle suddivisione delle due componenti era a classi per cui un indirizzo IP aveva una delle seguenti forme:

	8	16	24	31
CLASSE A	0   ident. rete		identificatore di host	
CLASSE B	1   0   identificatore di rete		identificatore di host	
CLASSE C	1   1   0   identificatore di rete			ident. di host
CLASSE D	1   1   1   0   indirizzo multicast			

Con questi schemi l'indirizzo è ad autoidentificazione perché il confine tra le due componenti si può determinare con i bit più significativi.

Vediamo come:

- *classe A*: il primo byte rappresenta la rete, gli altri l'host; [0-127].x.x.x. La maschera di sottorete è 255.0.0.0, o /8. Questi indirizzi iniziano tutti con un bit a 0.
- *classe B*: i primi due byte rappresentano la rete, gli altri l'host; [128-191].y.x.x (gli y sono parte dell'indirizzo di rete, gli x dell'indirizzo di host). La maschera di sottorete è 255.255.0.0, o /16. Questi indirizzi iniziano con la sequenza 10
- *classe C*: i primi 3 byte rappresentano la rete, gli altri l'host; [192-223].y.y.x. La maschera di sottorete è 255.255.255.0, o /24. Questi indirizzi iniziano con la sequenza 110
- *classe D*: riservata agli indirizzi multicast: [224-255].x.x.x

Limiti - Il numero di indirizzi univoci disponibili in IPv4 è

$$2^{32} = 256^4 = 4.294.967.296 \cong 4,3 \cdot 10^9$$

ma bisogna tener presente che non vengono usati tutti, perché alcuni sono riservati a un particolare utilizzo (ad esempio gli indirizzi 0.0.0.0, 255.255.255.255, 192.0.34.166 e la

classe 192.168.0.1/16) e perché certe classi non vengono sfruttate interamente per via della suddivisione interna in classi più piccole.

L'indirizzamento a classi, proprio per questo, presenta diversi limiti dovuti soprattutto al numero di host gestibili dalle diverse classi.

In pratica se si esauriscono gli indirizzi univoci resi disponibili da una classe, ad esempio la C connettendo più di 255 host, occorre fare ricorso ad un indirizzo di classe superiore.

Il cambiamento di indirizzo non è indolore con questa tecnica perché il software di rete va aggiornato con i nuovi indirizzi e non consente una transizione graduale.

In pratica l'indicatore di rete univoco non poteva adempiere alle esigenze della crescita che negli anni '80 ebbero le reti LAN. Quindi per risparmiare i prefissi di rete si dovettero escogitare altre tecniche come quella del mascheramento per continuare a fare in modo che IPv4 potesse adempiere al suo ruolo prima dell'entrata di IPv6

L'indirizzamento in classi è considerato obsoleto, e per permettere un migliore sfruttamento degli indirizzi IP disponibili, è stato introdotto l'indirizzamento senza classi, o CIDR.

La modifica introdotta dal CIDR consiste essenzialmente nell'utilizzare maschere di sottorete (subnet mask) di lunghezza arbitraria, mentre l'indirizzamento con classi ammetteva solo tre lunghezze della maschera di sottorete: /8, /16 e /24. La maschera della vecchia classe C (/24) è ancora popolare, ma si usano anche maschere più corte per reti grandi (/23 o /22) o più lunghe per reti piccole (/25, /26, fino a /30 per reti punto-punto). I bit che nella maschera di sottorete sono a 1 fanno parte dell'indirizzo della sottorete, gli altri sono l'indirizzo dell'host. Normalmente, la maschera di sottorete è costituita da N bit a 1 seguiti da (32-N) bit a 0, e può essere abbreviata nella forma /N.

In questo modo non si è vincolati a un numero fisso di bit per determinare l'indirizzo di rete, ma i bit utili a rappresentare la rete, piuttosto che l'host, sono fissati liberamente.

Con l'aumento del numero di dispositivi connessi ad Internet la capacità di indirizzamento della attuale versione IPv4 del protocollo TCP/IP si sta rapidamente consumando; questo problema viene generalmente chiamato saturazione degli indirizzi IPv4.

## **TCP - TRANSMISSION CONTROL PROTOCOL**

è uno dei principali protocolli della Suite di protocolli Internet. TCP è il protocollo di trasporto, definito nel RFC 793, su cui si appoggiano gran parte delle applicazioni Internet.

Il TCP è un protocollo corrispondente al livello 4 (trasporto) del modello di riferimento OSI, e di solito è usato in combinazione con il protocollo di livello 3 (rete) IP. La corrispondenza con il modello OSI non è perfetta, in quanto il TCP e l'IP nascono prima. La loro combinazione è indicata come TCP/IP ed è, alle volte, erroneamente considerata un unico protocollo.

Il TCP nacque nel 1970 come frutto del lavoro di un gruppo di ricerca del dipartimento di difesa statunitense. I suoi punti di forza sono l'alta affidabilità e robustezza. La sua

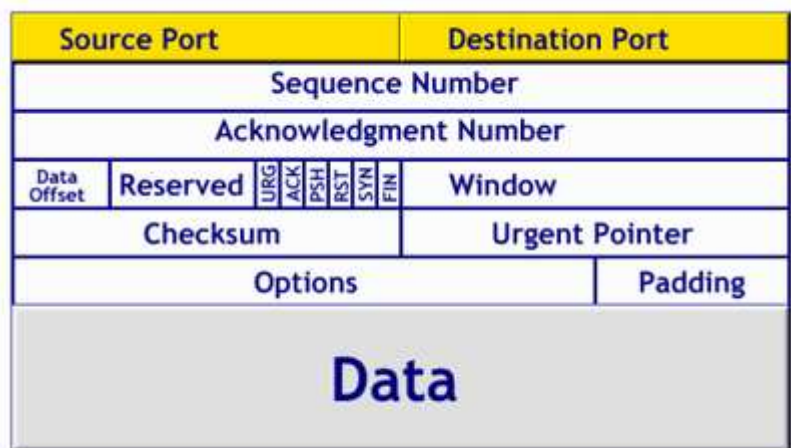
popolarità si deve anche grazie ad una sua implementazione diffusa dalla Università di Berkeley in California sotto forma di sorgenti.

Suite di protocolli Internet <a href="#">Modifica</a>	
Livello applicazioni	HTTP, HTTPS, SMTP, POP3, IMAP, FTP, DNS, SSH, IRC, SNMP, SIP, RTSP, Rsync, Telnet, HSRP, BitTorrent, RTP,...
Livello di trasporto	TCP, UDP, SCTP, DCCP ...
Livello di internetworking	IPv4, IPv6, DHCP, ICMP, BGP, OSPF, RIP, IGRP, IGMP, IPsec...
Livello di collegamento	Ethernet, WiFi, PPP, Token ring, ARP, ATM, FDDI, LLC, SLIP ...
Livello fisico	Doppino, Fibra ottica, Cavo coassiale, Codifica Manchester, Codifica 4B/5B, WiFi ...

Le caratteristiche principali del TCP sono:

- La creazione di una connessione (protocollo orientato alla connessione)
- La gestione di connessioni punto-punto
- La garanzia che i dati trasmessi giungano a destinazione in ordine e senza perdita di informazione (tramite il meccanismo di acknowledgment e ritrasmissione)
- Attraverso il meccanismo della finestra scorrevole, offre funzionalità di controllo di flusso e controllo della congestione, vitali per il buon utilizzo della rete IP, che non offre alcuna garanzia in ordine alla consegna dei pacchetti, al ritardo, alla congestione.
- Una funzione di moltiplicazione delle connessioni ottenuta attraverso il meccanismo delle porte.

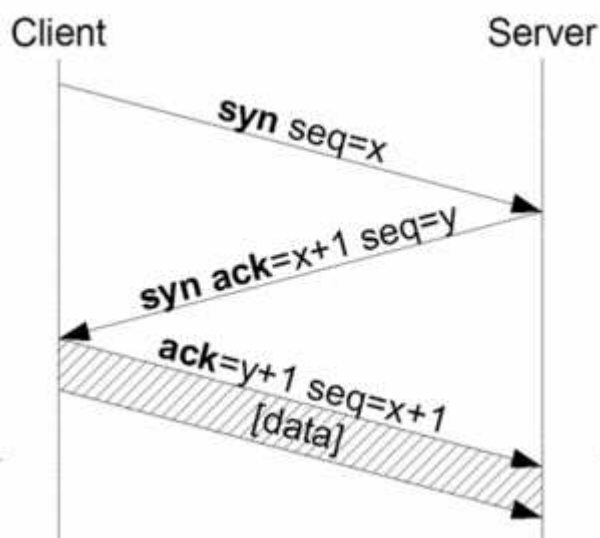
L'header di un segmento TCP è così strutturato:



- Porta sorgente (*Source port*) [16 bit]
- Porta di destinazione (*Destination port*) [16 bit]

- Numero di sequenza (*Sequence number*) [32 bit], indica la posizione del primo byte di dati del segmento TCP all'interno del flusso completo; se il flag SYN è impostato, il valore del sequence number corrisponde all'Initial Sequence Number (ISN);
- Numero di acknowledgment (*Acknowledgment number*) [32 bit], contiene il valore del prossimo sequence number che la sorgente del segmento TCP è in attesa di ricevere ed è utilizzato congiuntamente al flag ACK;
- Data offset [4 bit], indica la lunghezza (in word da 32 bit) dell'header del segmento TCP;
- 6 bit riservati (*Reserved*), non utilizzati e predisposti per sviluppi futuri del protocollo;
- Bit di controllo (*Control bits*) [6 bit], possono essere impostati ad 1 o 0 e indicano:
  - URG: il valore dell'urgent pointer è valido;
  - ACK: il valore dell'acknowledgment number è valido;
  - PSH: l'host che riceve il segmento TCP deve provvedere a trasferire i dati al Livello applicazioni il più velocemente possibile;
  - RST: reset della connessione;
  - SYN: se impostato, indica che si tratta del primo segmento della connessione;
  - FIN: se impostato, indica che si tratta dell'ultimo segmento della connessione;
- Finestra (*Window*) [16 bit], indica il numero di byte che il mittente è in grado di accettare a partire dal byte indicato dall'acknowledgment number;
- Checksum [16 bit], utilizzato per il controllo della validità del segmento;
- Urgent pointer [16 bit], puntatore al sequence number di dati con priorità di trasferimento;
- Opzioni (facoltative)
- Padding, utilizzato per completare i bit non utilizzati dalle opzioni

La procedura utilizzata per instaurare in modo affidabile una connessione TCP tra due host è chiamata *three-way handshake* (triplice stretta di mano), ad indicare la necessità di scambiare tre messaggi per garantire la corretta creazione della connessione.



Supponiamo, per esemplificare, che l'host A (il client) intenda instaurare una comunicazione TCP con l'host B (il server); i passi indicati dalla tecnica three-way handshake sono:

1. A invia un segmento SYN a B, contenente il suo sequence number  $x$ ;
2. B invia un segmento SYN/ACK ad A, contenente il suo sequence number  $y$  e l'acknowledgment del sequence number  $x$  di A;
3. A invia un segmento ACK a B con l'acknowledgement del sequence number  $y$  di B.

Avendo chiamate SYN poi insieme SYN + ACK e infine ACK se si cercano solo i segmenti di tipo ACK si ottengono tutte le nuove connessioni instaurate.

## Protocollo di routing OSPF – Open Shortest Path First

Open Shortest Path First o OSPF è uno dei protocolli di instradamento più diffusi che utilizza l'instradamento a stato del collegamento. Questo standard è *open* (aperto) nel senso che è un protocollo non proprietario. Il protocollo utilizza un metodo di instradamento che non si differenzia sostanzialmente da quello a stato delle linee, ma aggiunge delle altre proprietà:

- Autenticazione dei messaggi
- Bilanciamento del carico
- Aggiunta di un ulteriore grado di gerarchia nei domini

Una situazione di questo tipo porta ad una condizione in cui il nodo pubblicizzante tale possibilità riceve una quantità di pacchetti non gestibile. In questo caso l'instradamento fallisce dato che molti pacchetti vengono persi, soprattutto in caso di grosso carico di dati. Una forma di autenticazione come quella realizzata dal protocollo OSPF è in grado di garantire un buon grado di sicurezza anche contro utenti esterni malintenzionati. Tale caratteristica è stata introdotta anche in altri protocolli di instradamento importanti e diffusi come ad esempio RIP.

Suite di protocolli Internet <a href="#">Modifica</a>	
Livello applicazioni	HTTP, HTTPS, SMTP, POP3, IMAP, FTP, DNS, SSH, IRC, SNMP, SIP, RTSP, Rsync, Telnet, HSRP, BitTorrent, RTP,...
Livello di trasporto	TCP, UDP, SCTP, DCCP ...
Livello di internetworking	IPv4, IPv6, DHCP, ICMP, BGP, <b>OSPF</b> , RIP, IGRP, IGMP, IPsec...
Livello di collegamento	Ethernet, WiFi, PPP, Token ring, ARP, ATM, FDDI, LLC, SLIP ...
Livello fisico	Doppino, Fibra ottica, Cavo coassiale, Codifica Manchester, Codifica 4B/5B, WiFi ...

Il protocollo è in grado anche di gestire casi in cui percorsi diretti verso la stessa destinazione abbiano costi differenti.

Una rete OSPF è divisa in *aree*. Esse sono gruppi logici di router le cui informazioni possono essere sommarizzate rispetto al resto della rete. Diversi tipi di aree "speciali" sono definite:

### Area Backbone

L'area backbone (conosciuta anche come area zero) rappresenta il cuore di una rete OSPF. Tutte le altre aree sono collegate ad essa e il routing inter-area passa tramite un router di questa rete.

### Stub area

Per Stub Area si intendono quei tipi di area che non ricevono route esterne. Le route esterne saranno poi definite e distribuite da un altro protocollo di Routing. Quindi, le stub area necessitano di relegare ad una route di default lo scambio per il traffico con quelle esterne al dominio di appartenenza

### Totally stubby area

Una totally stubby area è simile ad una stub area, however this area does not allow summary routes in addition to the external routes, i.e., inter-area (IA) routes are not summarized into totally stubby areas. L'unico modo in cui il traffico esce dall'area è una route di default che è l'unica di Tipo-3 LSA pubblicata nell'area. Quando c'è solo una route per uscire dall'area, devono essere effettuate meno decisioni di routing dal processore di route, con minore utilizzo di risorse di sistema. Questa è la versione Cisco della NSSA.

### Not-so-stubby area

Identificata anche come NSSA, una not-so-stubby area è un tipo di stub area che può importare route esterne di AS e mandarle al backbone, ma non può ricevere tali route esterne di AS dal backbone o da altre aree. Cisco implementa anche una versione proprietaria di NSSA chiamata NSSA Totally Stubby area. Si prende la responsabilità di una Totally Stubby area, col significato che route riassuntive di tipo 3 e 4 non vanno ad inondare questo tipo di area.

## Protocollo di routing RIP – Routing Information Protocol

Il Routing Information Protocol (RIP) è uno dei protocolli di routing più usati su reti locali ed aiuta i router ad adattarsi dinamicamente ai cambiamenti dei collegamenti di rete, scambiandosi informazioni riguardo a quali reti ogni router può raggiungere e quanto lontano siano. Anche se il RIP è ancora attivamente usato, è generalmente sostituito da protocolli di routing link-state come OSPF e EIGRP.

Suite di protocolli Internet <a href="#">Modifica</a>	
Livello applicazioni	HTTP, HTTPS, SMTP, POP3, IMAP, FTP, DNS, SSH, IRC, SNMP, SIP, RTSP, Rsync, Telnet, HSRP, BitTorrent, RTP, ...
Livello di trasporto	TCP, UDP, SCTP, DCCP ...
Livello di internetworking	IPv4, IPv6, DHCP, ICMP, BGP, OSPF, RIP, IGRP, IGMP, IPsec...
Livello di collegamento	Ethernet, WiFi, PPP, Token ring, ARP, ATM, FDDI, LLC, SLIP ...
Livello fisico	Doppino, Fibra ottica, Cavo coassiale, Codifica Manchester, Codifica 4B/5B, WiFi ...

RIP è stato sviluppato nel 1969 come parte di ARPANET e usa l'algoritmo Bellman-Ford. RIP è un protocollo di routing distance-vector che impiega il conteggio dei numeri di salti (hop count) come metrica di routing. Il massimo numero di hop permessi è 15. Ogni router RIP trasmette di default, ogni 30 secondi, la propria tabella completa di routing a tutti i vicini direttamente collegati, generando grandi quantità di traffico di rete su reti a bassa capacità trasmissiva. Lavora *sopra* il livello di rete della suite Internet Protocol, usando User Datagram Protocol sulla Porta 520 per trasportare i relativi dati. Un meccanismo denominato split horizon è usato per evitare gli anelli (loop) nel percorso di inoltro dei pacchetti.

In molti ambienti di rete RIP non è la prima scelta tra i protocolli di routing poiché il tempo di convergenza e scalabilità della rete sono scarsi se confrontati con OSPF o IS-IS, inoltre il basso numero di hop supportati limita severamente la grandezza della rete. D'altra parte, è molto facile da configurare ed è implementato anche nei router di fascia bassa.

Ci sono 3 versioni di RIP: *RIPv1*, *RIPv2*, e *RIPng*.

- RIPv1, definito da (RFC 1058), usa il routing "classful". Gli aggiornamenti delle tabelle di routing non contengono la maschera di sottorete rendendo impossibile la creazione di sottoreti di dimensione diversa all'interno della stessa rete. Non viene supportata nessuna forma di autenticazione, lasciando RIPv1 vulnerabile ad attacchi.
- RIPv2, è stato sviluppato nel 1994 e definito da (RFC 2453), include il trasporto delle informazioni sulla maschera di sottorete, supportando così il Classless Inter-Domain Routing, CIDR. Per garantire la sicurezza degli aggiornamenti sono disponibili 2 metodi: autenticazione semplice con testo in chiaro e MD5, (RFC 2082). Per mantenere la compatibilità all'indietro il limite di hop count rimane a 15.
- RIPng, (RFC 2080), è una estensione del protocollo originale RIPv1 per supportare IPv6.

## **Protocollo di Routing BGP – Border Gateway Protocol**

Il Border Gateway Protocol (BGP) è un protocollo di rete usato per connettere tra loro più router che appartengono a sistemi autonomi distinti e che vengono chiamati gateway.

Il Border Gateway Protocol è un protocollo di instradamento (*routing*) che agisce nel 'cuore' di Internet. Il BGP funziona attraverso la gestione di una tabella di reti IP, o prefissi, che forniscono informazioni sulla raggiungibilità delle diverse reti tra più sistemi autonomi (Autonomous System, AS). Si tratta di un protocollo di routing a indicazione di percorso (*path vector*), che non usa metriche di carattere tecnico ma prende le decisioni di instradamento basandosi su politiche (regole) determinate da ciascuna rete. La versione corrente, BGP-4, è definita nella specifica RFC 1771.

Il BGP supporta il routing indipendente dalle classi (Classless InterDomain Routing) e usa un meccanismo di aggregazione degli instradamenti per diminuire le dimensioni delle relative tabelle. Nella rete Internet viene usata la versione 4 del protocollo a partire dal 1994; tutte le versioni precedenti sono considerate obsolete.

Il protocollo BGP è stato creato per sostituire il protocollo di routing EGP e consentire un instradamento completamente decentralizzato, eliminando così gli ostacoli che impedivano la soppressione della dorsale Internet NSFNET. In tal modo Internet è divenuta un sistema pienamente decentralizzato.

Suite di protocolli Internet <a href="#">Modifica</a>	
Livello applicazioni	HTTP, HTTPS, SMTP, POP3, IMAP, FTP, DNS, SSH, IRC, SNMP, SIP, RTSP, Rsync, Telnet, HSRP, BitTorrent, RTP,...
Livello di trasporto	TCP, UDP, SCTP, DCCP ...
Livello di internetworking	IPv4, IPv6, DHCP, ICMP, <b>BGP</b> , OSPF, RIP, IGRP, IGMP, IPsec...
Livello di collegamento	Ethernet, WiFi, PPP, Token ring, ARP, ATM, FDDI, LLC, SLIP ...
Livello fisico	Doppino, Fibra ottica, Cavo coassiale, Codifica Manchester, Codifica 4B/5B, WiFi ...

Anche le reti IP private di maggiori dimensioni possono trovare benefici dall'uso del BGP, ad esempio nel caso del collegamento di un gran numero di reti OSPF, una situazione in cui il protocollo OSPF non è in grado di scalare in modo efficiente. Un altro motivo che può spingere all'uso del BGP è la configurazione di una rete in *multihoming* per offrire una maggiore ridondanza.

Gli utenti di Internet, nella maggior parte dei casi, non utilizzano il protocollo BGP direttamente. Tuttavia, poiché quasi tutti i provider Internet (ISP) sono obbligati a usarlo per stabilire i criteri di routing reciproci, si tratta di uno dei protocolli più importanti di Internet. Come utile confronto si possono valutare analogie e differenze con il Sistema di Segnalazione n. 7, che costituisce il protocollo cardine per l'attivazione di una chiamata tra operatori della rete telefonica pubblica (PSTN).

Nel protocollo BGP le coppie di sistemi adiacenti, detti **peer**, vengono stabilite mediante configurazione manuale dei router stabilendo una sessione TCP sulla porta 179. L'iniziatore della sessione BGP (*speaker*) invia periodicamente (per default ogni 60 secondi) dei messaggi *keepalive* da 19 byte per mantenere attiva la connessione. Tra i protocolli di routing, il BGP è l'unico a utilizzare il TCP come protocollo di trasporto.

Quando viene usato all'interno di uno stesso AS il protocollo BGP viene chiamato **BGP Interno** (IBGP, *Interior Border Gateway Protocol*); nell'uso tra AS distinti viene chiamato **BGP Esterno** (EBGP, *Exterior Border Gateway Protocol*). I router che svolgono compiti di instradamento del traffico IBGP vengono chiamati **router di transito**; quelli che si trovano sul margine esterno di un AS e utilizzano il protocollo EBGP per scambiare informazioni con il proprio ISP vengono chiamati **router di bordo** o **di confine**.

Tutti i router all'interno di un dato AS che partecipano all'instradamento via BGP devono essere configurati secondo una topologia a maglie completamente connesse: ciascun router deve essere configurato come *peer* di tutti gli altri. Naturalmente ciò pone seri problemi di scalabilità, poiché il numero di connessioni necessarie cresce con il quadrato

del numero dei router coinvolti. Per ovviare a questo problema il protocollo BGP prevede due soluzioni: i **route reflector** (RFC 2796) e le **confederazioni** (RFC 3065).

I *route reflector* riducono il numero di connessioni necessarie nell'ambito di un AS. È possibile designare in tal modo un solo router (o due, per ridondanza) e configurare gli altri router appartenenti all'AS come *peer* soltanto di quest'ultimo.

Le confederazioni vengono usate nel caso di reti particolarmente estese, nelle quali un AS di grandi dimensioni può essere configurato in modo da comprendere vari AS interni di più facile gestione. È possibile usare le confederazioni anche contemporaneamente ai *route reflector*.

I *peer* BGP usano un semplice automa a stati finiti per prendere le decisioni che riguardano l'interazione con altri *peer* BGP. L'automa è composto da sei stati - Idle (Inattiva), Connect (Connetti), Active (Attivo), OpenSent (Apertura Inviata), OpenConfirm (Apertura Confermata) ed Established (Stabilito). Ciascun *peer* BGP attraversa gli stati descritti quando cerca di stabilire e mantenere in vita una sessione con un altro *peer*.

Il BGP prevede una procedura di **smorzamento** (*damping*) per ridurre gli effetti della volatilità degli instradamenti. Tale fenomeno può essere causato dalla interruzione e dal successivo ripristino dei collegamenti a livello di WAN / WLAN oppure da errori di configurazione o gestione dei router. In assenza di *damping* può accadere che gli instradamenti vengano inseriti ed eliminati dalle tabelle di routing con grande rapidità, il che può avere un impatto rilevante sul carico di lavoro dei router e di conseguenza sulla stabilità complessiva delle procedure di instradamento.

Nel processo di *damping* la volatilità di un instradamento subisce una diminuzione esponenziale. La prima volta che un instradamento va e viene in breve tempo per la prima volta, per qualsiasi ragione, il *damping* non interviene; vengono così conservati i tempi di risposta consueti del BGP. Quando l'evento si presenta una seconda volta, il BGP ignora il prefisso per un certo tempo, e le occorrenze successive vengono ritardate secondo una progressione esponenziale. Quando le anomalie sull'instradamento in questione sono cessate ed è trascorso un opportuno lasso di tempo, i prefissi possono essere ripristinati partendo da zero. Il *damping* può anche ridurre gli effetti degli attacchi ostili di tipo denial of service, in quanto gli intervalli temporali previsti dal meccanismo sono ampiamente personalizzabili.

A causa della maggiore velocità dei collegamenti delle dorsali e dei processori dei router, alcuni architetti di rete hanno suggerito che il *damping* non sia più importante come una volta, in quanto i router sono in grado di assorbire molto più rapidamente le modifiche alla tabella di routing. Alcuni hanno persino suggerito che il *damping* in queste condizioni possa peggiorare la situazione invece di migliorarla. Questo argomento è ancora controverso e oggetto di numerose ricerche.

Uno dei problemi più gravi del protocollo BGP, ma in realtà dell'intera infrastruttura di Internet, deriva dalla crescita della tabella di routing della stessa Internet. Se la tabella di routing globale crescesse fino al punto in cui la sua gestione dovesse superare le capacità di memoria e di potenza di calcolo dei router meno recenti, questi non sarebbero più in grado di agire adeguatamente da gateway per le parti di Internet collegate ad essi. Inoltre, cosa forse ancor più importante, le tabelle di routing più grandi richiedono tempi più lunghi

per stabilizzarsi (vedi sopra) dopo una modifica sostanziale nella connettività, garantendo nel frattempo solo una connettività ridotta, o talvolta assente.

Fino al 2001 la tabella di routing globale era in crescita esponenziale e minacciava di dare luogo, col tempo, a una interruzione generalizzata della connettività. Nel tentativo di contrastare questa eventualità, è in corso uno sforzo congiunto degli ISP per mantenere al minimo le dimensioni della tabella di routing globale, attraverso il ricorso ai meccanismi di Classless InterDomain Routing e aggregazione degli instradamenti. Questi sforzi hanno rallentato la crescita della tabella di routing sino a riportarla a un andamento lineare, allontanando in modo significativo il momento in cui sarà necessario sostituire i router più datati.

## TEORIA DELLE CODE

La teoria delle code è lo studio matematico delle linee di attesa (o code) e di vari processi correlati, come l'arrivo alla fine di una coda, l'attesa (essenzialmente un processo di immagazzinamento) e l'essere servito all'inizio della coda. Può essere applicata nei trasporti e nelle telecomunicazioni; occasionalmente è collegata alla Ride theory.

La prima pubblicazione sulla teoria delle code è del 1909 dell'ingegnere danese Agner Krarup Erlang.

Nel 1953, Kendall introdusse la notazione  $A/B/C$ , successivamente estesa come  $1/2/3/(4/5/6)$  nella quale i numeri sono sostituiti con quanto segue.

1. Un codice che descrive il processo di arrivo; i codici usati sono:
  - o M per "di Markov", implicante una distribuzione esponenziale negativa unilatera per i tempi di servizio o tra gli arrivi: ciò implica l'assenza di memoria di questi ultimi;
  - o D per distribuzione "degenere" o "deterministica" dei tempi di servizio;
  - o Ek per una distribuzione di Erlang con k come parametro di forma;
  - o G per una distribuzione "Generale".
2. Un codice simile che rappresenta il processo di servizio, usando gli stessi simboli.
3. Il numero di canali di servizio.
4. Le dimensioni massime del sistema: il massimo numero di clienti permessi nel sistema compresi coloro che vengono serviti attualmente; quando questo massimo viene raggiunto ulteriori arrivi vengono rifiutati.
5. Le dimensioni della fonte di arrivi: le dimensioni della popolazione da cui possono arrivare i clienti; questo limita il ritmo di arrivi, tanti più *jobs* sono presenti nella coda tanti meno ne sono disponibili per entrare nel sistema.
6. L'ordine di priorità nel quale sono serviti i *jobs* nella coda:
  - o First Come First Served (FCFS) (o First In First Out - FIFO) (il primo che arriva viene servito per primo);
  - o Last Come First Served (LCFS) (o Last In First Out - LIFO) (l'ultimo che arriva viene servito per primo);
  - o Service In Random Order (SIRO) (servizio in ordine casuale).