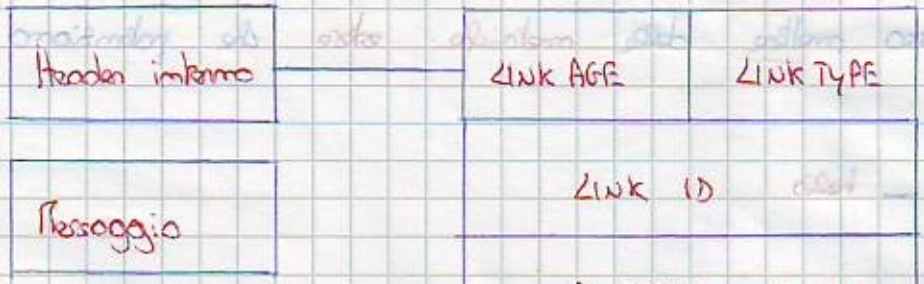
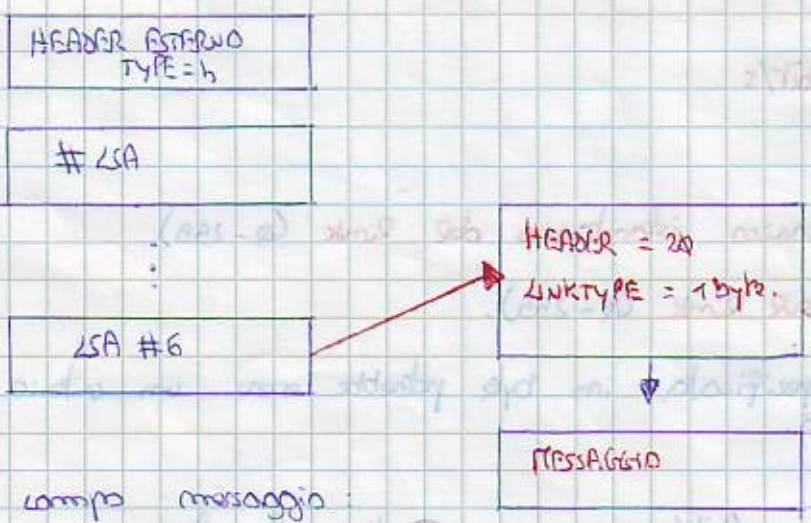


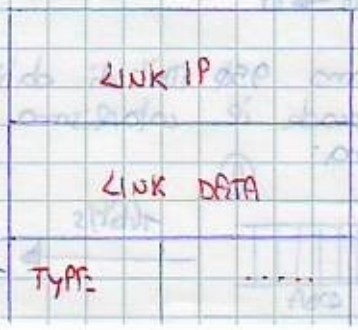
Il checksum protegge l'header interno da errori di trasmissione. Attraverso il campo linkage invece identifico il tempo passato da quando è stato generato il messaggio. Il campo link type invece specifica il tipo di link che viene pubblicizzato. Si noti che i tipi di link sono:

1) Routing link che sono anche quelli principali
2) Network link
3) Summary link to network
4) Summary link to AS BOUNDARY ROUTER.

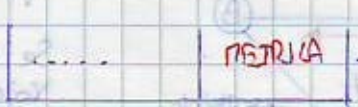
I router link vengono suddivisi poi in link PUNTO-PUNTO, link SALIENTI, link STUB, e link VIRTUALI. Il secondo e il terzo tipo di link pubblicizzano la direzione da prendere verso una data rete. Infine il secondo, il terzo e il quarto link sono link logici. Per pubblicizzare un routing link usiamo LSA UPDATE che è così fatto:



Zoomiamo il campo messaggio:



1, 2, 3, 4



→ numero che va da 0 a 65535

Link IP e link DATA hanno un significato diverso a seconda del link. Per esempio in un link punto-punto si pubblicizzano gli indirizzi IP delle interfacce dei router.

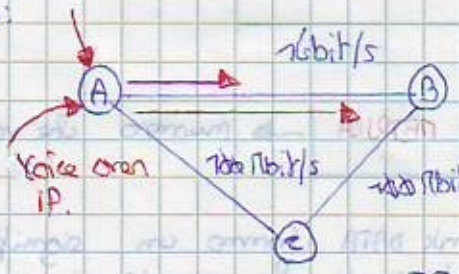
Nei campi visti posso mettere delle metriche extra che potenziano OSPF. Quindi riassumendo:

PACCHETTI OSPF:
- hello
- database description
- LSA REQUEST
- LSA UPDATE
  - 1) Router link
    - PUNTO-PUNTO
    - TRANSIGUITE
    - STUB
    - VIRTUALE.
  - 2) Network link
  - 3) Summary link to Network
  - 4) Summary link to AS Border
- LSA ACKNOWLEDGE

Parliamo ora di IGRP ed EGRP che ricordo sempre nella categoria IGP, ma che però sono proprietari, cioè sono di marca.
E-IGRP sta per Enhanced Interior Gateway Protocol ed è una versione migliorata di IGRP. È sostanzialmente un algoritmo DISTANCE VECTOR tipo il RIP ma più evoluto. Supporta completamente il subnetting come RIP2 ma ha metriche più evolute ed orientate alla qualità del servizio. Le metriche supportate da E-IGRP sono:

1) Banda Link : kbit/s
2) HopCount (0 - 255)
3) Valutazione del carico istantaneo del link (0 - 255).
4) Tasso di errore sul link (0 - 255).
5) MTU LINK che specificata in byte potrebbe essere un criterio di instradamento dei dati.

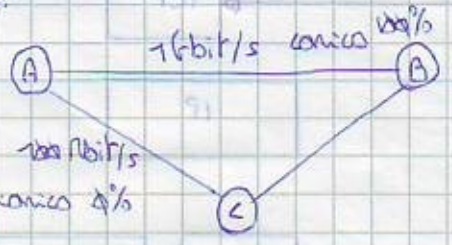
Per esempio:



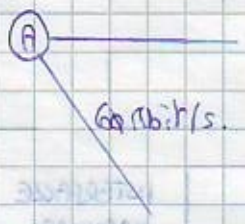
Ipotesi: A → B

Se abbiamo 950 Mbit di dati e 60 Mbit di voice accade il catalisma in quanto in A si ha:

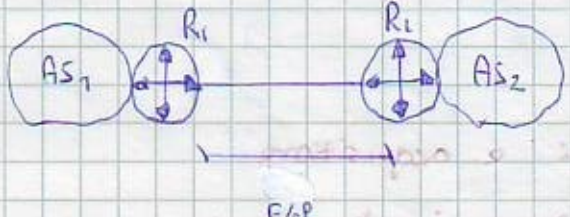
Il link va in sovraccarico la coda in A inizia a riempirsi, e questo mi "ammazza" la performance dei dati e mi degrada la prestazione della rete. In questa situazione OSPF è poco furbo. Invece E-IGRP può seguire lo stesso percorso. Immaginiamo si ricordi che un router non sa a priori la capacità per ogni flusso di informazioni. E-IGRP prende delle azioni non preventive ma reattive. Cioè i router misurano il carico dei link. Dopo di che si segue il confronto. Es:



Il carico si distribuisce lungo AB e AC. Quindi:

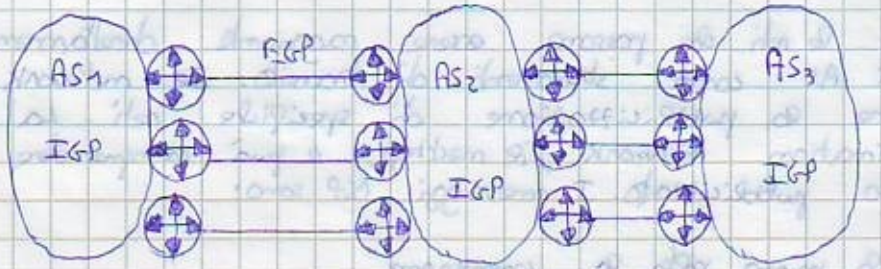


E-IGRP però soffre del problema della scalabilità perché si basa sul DISTANCE VECTOR. E-IGRP può anche controllare il rischio di errore. Quindi:



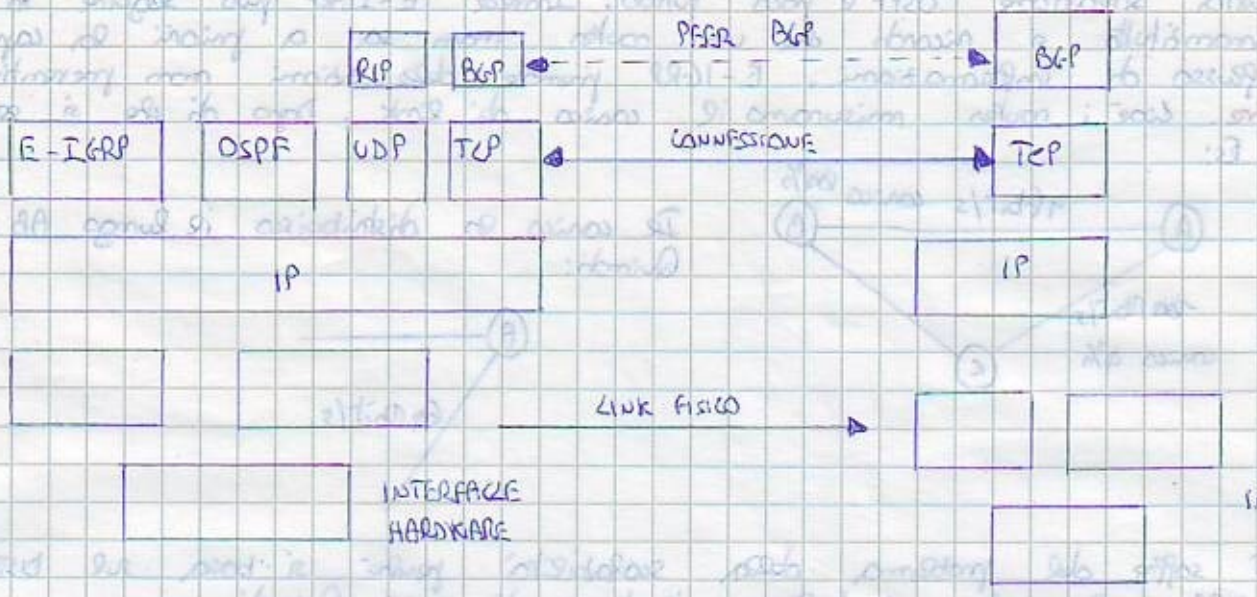
NB: Non esiste un solo router tra 2 AS.

Si noti inoltre che in R_1 e R_2 c'è un'istanza di IGP. Un EGP comune è il Border Gateway Protocol. Oggi si usa la versione 4 di questo protocollo. Vediamo un esempio:



Tutti i router devono avere sia IGP che EGP. In questo contesto non si usano le metriche che, perché la pubblicizzazione avviene tramite multicast. In particolare nascono problemi nella coerenza delle metriche negli AS, e bisogna prevenire i comportamenti scorretti. Quindi non si usano le metriche perché non si può garantire il successo. Il BGP (Border Gateway Protocol) è in grado di individuare due percorsi da AS_1 a AS_2. Ma come fa a scegliere il percorso? I criteri potrebbero essere commerciali, cioè faccio un accordo con gli AS che mi convengono. Si ricordi infatti che è possibile conoscere gli AS attraversati da ogni percorso. È importante anche il criterio di affidabilità degli AS. Un altro criterio è il numero di AS attraversati. Scelgo il percorso che attraversa meno AS. Questo criterio è un po' misto perché anche gli AS in questione possono essere poco affidabili. Ma il BGP usa pubblicizza? pubblicizza informazioni di raggiungibilità delle reti. Il BGP notifica solo le variazioni. È inutile avere ancora delle informazioni sulle stesse reti. Quindi compare per esempio notificata la rete non pubblicizzata prima, oppure la rete precedentemente pubblicizzata ma ora non più raggiungibile. Quindi si pubblicizzano solo le novità. Un router BGP supporta il submetting. Poi nei router ci sono delle procedure di autenticazione piuttosto stringenti. Queste procedure servono perché spesso gli hacker attaccano i router BGP.

Chiaramente il BGP si appoggia su TCP. Quindi:



STACK PROTOCOLLARE IN ROUTING

Perciò le fasi del BGP sono:

1) acquisizione dei router BGP vicini e acquisizione
2) apertura della connessione TCP con i router vicini
3) fase di scambio delle informazioni

Un router BGP pubblicizza le reti che possono essere raggiunte direttamente e le reti raggiungibili usando altri AS come strumenti di transito. Il network manager può abilitare e disabilitare la pubblicizzazione di specifiche reti. La pubblicizzazione comprende la destination network, il next hop, e può comprendere la serie di AS attraversati dal percorso pubblicizzato. I messaggi BGP sono:

1) OPEN che apre per la prima volta la connessione
2) UPDATE per inviare le variazioni
3) NOTIFICATION per inviare messaggi di incongruenze (esse stesse).
4) KEEP ALIVE che mantengono la connessione e vengono mandati periodicamente.

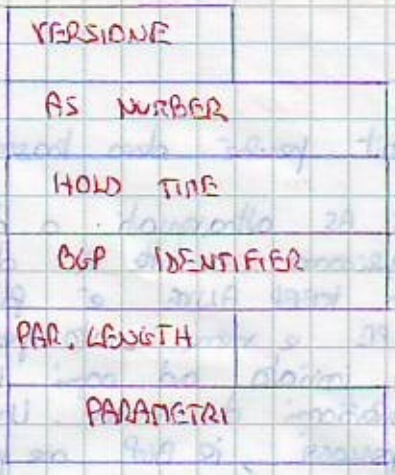
Vediamo ora la struttura dei messaggi BGP:

→ in cui è incluso il codice che mantiene viva l'autenticazione

NB: Un messaggio BGP può avere dimensioni arbitrarie.

Quindi la comunicazione si apre mediante il messaggio OPEN. Esso ha la

seguente struttura:

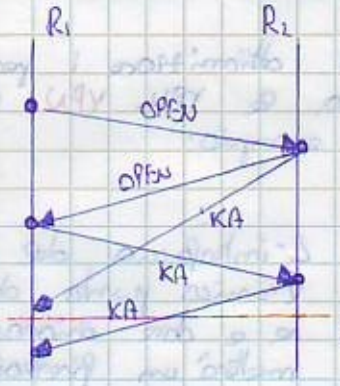


→ è il numero massimo di secondi che possono passare tra due messaggi consecutivi. Ogni HOLD TIME di tempo viene inviato un messaggio di tipo ALIVE. Questo serve perché se si hanno dei malfunzionamenti nel router, questo non invia più messaggi la connessione, dopo questo tempo, viene considerata morta.

Tra 2 AS si possono avere più router BGP.

parametri inerenti a procedure di identificazione.

Quindi si ha il seguente diagramma temporale:

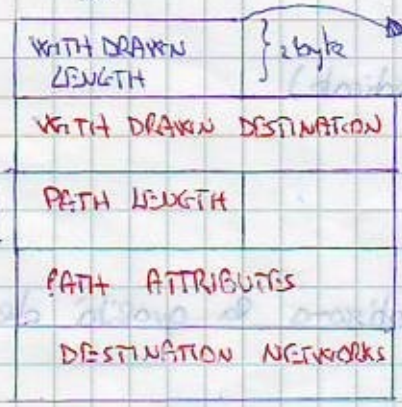


NB: KA = KEEP ALIVE e viene spedito dopo ogni HOLD TIME.

Una volta che il router ha ricevuto i messaggi OPEN e KEEP ALIVE può iniziare la connessione TCP.

2) Apertura della connessione TCP.

Vediamo ora il messaggio BGP UPDATE:

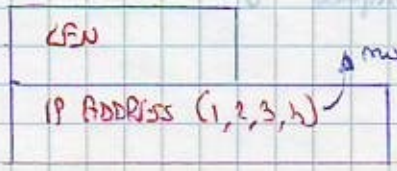


→ specifica la lunghezza della sezione successiva del messaggio BGP. Se è maggiore di 0, inizia una nuova sezione

→ pubblicizza reti non più raggiungibili.

→ sequenza degli AS attraversati

I path attributes hanno il problema che si riferiscono a tutte le destination network. Gli indirizzi IP in BGP vengono trasmessi in modo compresso per risparmiare il più possibile. Ma come comprimo il più possibile gli indirizzi IP? Trasmetto solo il network prefix.



Con LEN si specifica la lunghezza della subnet mask misurata in bit.

(56)

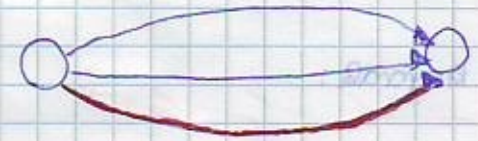
Per esempio: /9 ⇒ LEN = 9
IP ADDRESS = 2 byte

Quindi:

1 1 1 1 1 1 1 1 . 1 0 0 0 . . .

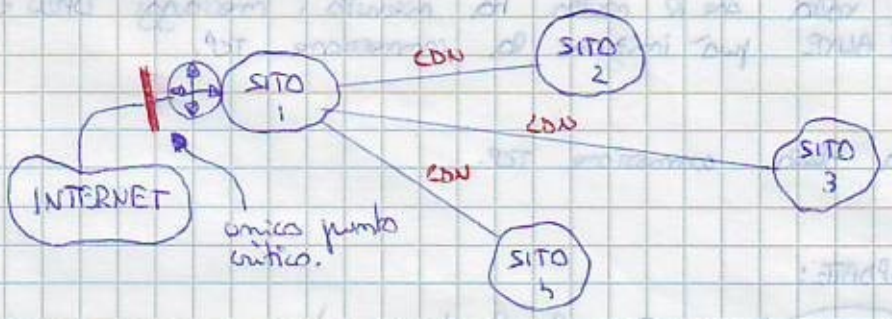
↳ trasmetto solo questo + 7 bit perché devo trasmettere 2 byte.

I PATH ATTRIBUTES contengono una lista degli AS attraversati o da che AS ho "imparato" questa informazione. Tali path si applicano a tutte le destination network pubblicizzate nel messaggio. Il messaggio KEEP ALIVE è fatto dal solo header di 19 byte cioè il MARKER + LENGTH + TYPE e viene usato per mantenere viva la connessione TCP tra due router, è viene inviato ad ogni HOLD TIME di tempo. NOTIFICATION infine si usa per le segnalazioni di errore. Una caratteristica negativa di BGP è che se ci sono più percorsi, il BGP ne può usare solo uno.



Quindi BGP non ha la caratteristica del LOAD SHARING.

Questa era prevedibile in quanto il BGP non tende ad ottimizzare i percorsi ed inoltre consente una connettività globale. Vediamo ora le VPN. VPN sta per Virtual Private Network. Consideriamo il seguente esempio:



L'interfaccia del router è l'unico punto da sorvegliare e dove chiaramente metterò un firewall.

CDN = circuiti diretti numerici (linee dedicate).

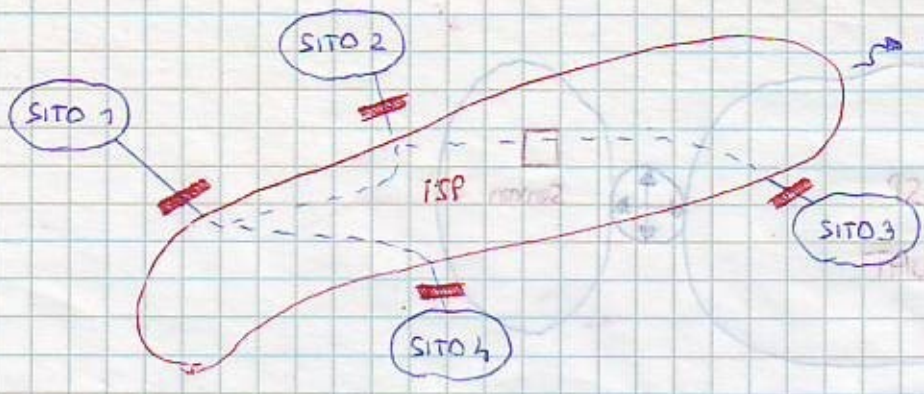
I punti positivi del CDN sono:

1) Banda garantita
2) Implementare tecniche che mi garantiscono la qualità del servizio.
3) Sicurezza

I punti negativi sono:

1) costo elevato. Solo le grandi imprese possono permetterselo.

Un'altra soluzione per le piccole - medie imprese è:



→ servizio BEST-EFFORT

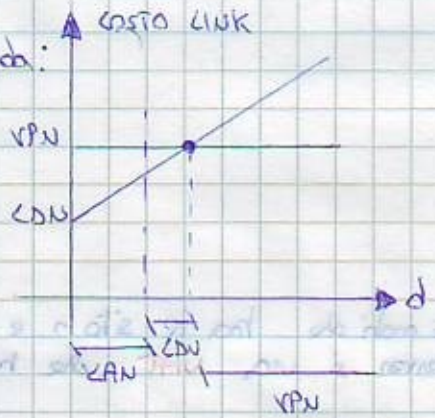
Uso coi dei collegamenti virtuali tra i vari siti.

Il collegamento è di tipo virtuale perché non ha una propria infrastruttura. Uso quella del gestore (ISP). Ha la garanzia così di avere la connettività ad ogni sito. Vediamo i punti positivi del VPN:

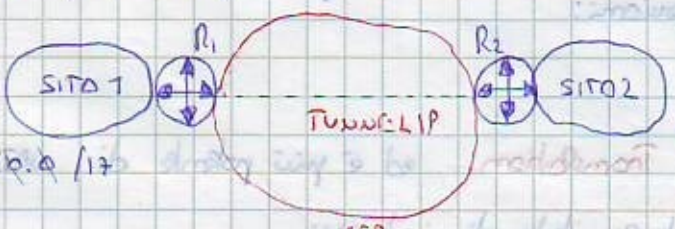
1) Ha un costo relativamente basso rispetto a CDN. Non sempre però accade ciò.

I punti negativi sono:

1) Ha banda non garantita. Solo che l'accesso conosca la banda.
2) Non implementa una tecnica di qualità
3) Sicurezza

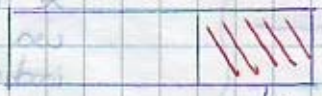


Vediamo ora come si gestisce la sicurezza tramite VPN. Prendiamo per esempio:



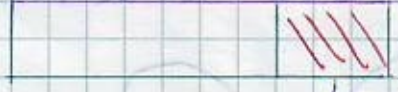
R_1:	D.N	N.H
	199.11	TUNNEL verso R_2

Si prende il pacchetto IP con:



↳ 199.11.9.4 per esempio

Questo pacchetto viene criptato e impacchettato in un altro pacchetto IP. Quindi si avrà:



↳ SA: R_1
DA: R_2
PROTOCOL: TUNNEL (numero)

} sono le uniche cose che vengono pubblicizzate in rete.

Abbiamo così ottenuto una forma di Privacy. I pacchetti sono criptati. Un altro problema legato alla VPN ma non solo è quello degli indirizzi IP. Consideriamo: