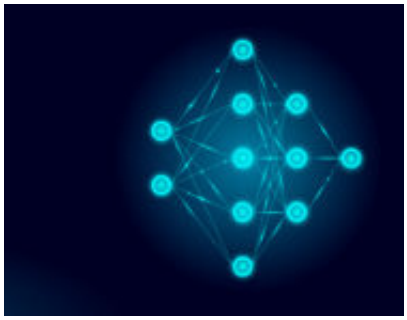
Aspetti di sicurezza di BGP e Routing in Internet - parte I

Author : Andrea Pasquinucci

Date : 16 Marzo 2020



Lo straordinario successo di Internet, ovvero della rete globale di comunicazione che ormai viene usata dalla maggioranza degli abitanti del nostro pianeta Terra, è dovuto ed è possibile fondamentalmente grazie a **due protocolli** che permettono all'infrastruttura di telecomunicazioni di funzionare egregiamente: il “Domain Name System (DNS)”, di cui abbiamo scritto nel maggio 2019, e il “Border Gateway Protocol (BGP)” ovvero il protocollo di Routing dei pacchetti IP.

Entrambi i protocolli risalgono agli anni '80 (Rif. 1), sono evoluti nel tempo e hanno dimostrato una incredibile resilienza, scalabilità e capacità di supportare la disponibilità del servizio. D'altra parte funzionalità specifiche per garantire l'**integrità** e l'**autenticità** dei dati[1] non sono state previste inizialmente e col tempo è risultato difficile includerle. Se per DNS è in corso l'implementazione di DNSSEC (si vedano gli articoli di maggio 2019), in questo articolo si considerano gli aspetti di sicurezza del Routing in Internet, ovvero del protocollo BGP-4 (Rif. 3) attualmente in uso.

Routing in Internet

Prima di descrivere minacce, vulnerabilità e rischi, è necessario un breve ripasso di cosa sia Routing IP in Internet. Il **protocollo IP** (Internet Protocol, Rif. 2) assegna a ogni dispositivo connesso alla rete Internet un indirizzo numerico IPv4[2], di 32 bit tipicamente scritto con 4 ottetti come 192.168.222.1, o IPv6, di 64 bit. Per semplicità in questo articolo si considerano solo gli indirizzi IPv4 ma quanto discusso si applica in generale anche agli indirizzi IPv6, seppur nel caso con qualche modifica.

Scopo primario del protocollo IP è di permettere a un pacchetto di dati inviato da un elaboratore di raggiungere un altro elaboratore di cui sia noto l'indirizzo IP. Visto che la rete IP si estende su tutta la superficie terreste[3], il problema che il Routing, in questo caso BGP-4, risolve è quello di individuare il percorso nelle reti di trasporto di dati digitali per raggiungere l'indirizzo di destinazione. Figuratamente la situazione è simile a quella di una rete autostradale (i cavi di trasporto dati) sulla quale transitano vetture (i pacchetti dati) e gli svincoli tra due o più

autostrade (i router). Come agli svincoli autostradali sono presenti i cartelli di segnalazione per indicare su quale autostrada proseguire per raggiungere una destinazione, nei router è presente una “tabella di Routing” che indica su quale cavo/rete inviare un pacchetto perché giunga a destinazione. Il protocollo BGP-4 ha come compito quello di gestire la “tabella di Routing” di ogni router IP in Internet[4].

Si incontrano immediatamente due difficoltà pratiche:

- il numero di *Prefissi*, ovvero di “cartelli stradali”, che ogni ruoter IP che ha una tabella di Routing completa deve mantenere, oggi supera 800.000;
- le tabelle di Routing sono molto dinamiche, gli aggiornamenti sono continui e molto frequenti, tipicamente nell'ordine dei minuti.

Questo si comprende facilmente visto che una tabella completa di Routing contiene le indicazioni su come raggiungere ogni indirizzo IP pubblico, in qualunque parte della Terra. Le modifiche della tabella sono dovute non solo all'attivazione o rimozione di indirizzi IP, ma anche al cambio di percorso per l'attivazione o spegnimento di percorsi dati, ad esempio cavi sottomarini, collegamenti satellitari o anche solo collegamenti tra due Internet Provider.

Indirizzi IP e Routing

È necessario approfondire un poco la gestione degli indirizzi IP e il funzionamento del Routing BGP-4 anche per quanto sarà discusso più avanti.

Gli indirizzi IP sono gestiti a livello globale dalla **IANA** (Internet Assigned Numbers Authority) che assegna blocchi di indirizzi IP alle cinque **RIR** (Regional Internet Registries): APNIC, LACNIC, ARIN, AFRINIC, RIPE. Ognuna delle cinque RIR ha competenza solo su di una zona geografica (Rif. 4), ad esempio il RIPE su Europa e Asia del Nord e Ovest. Le RIR a loro volta assegnano blocchi di indirizzi IP ai **LIR** (Local Internet Register) che tipicamente sono Internet Provider, Carrier ma anche grandi organizzazioni e università. A loro volta le LIR allocano blocchi di indirizzi IP ai propri clienti finali. Un'organizzazione che vuole connettersi a Internet con indirizzi IP esplicitamente a lei assegnati, deve per prima cosa ottenere dalla propria LIR uno (o più per organizzazioni molto grandi o distribuite a livello mondiale) numero di **AS** (Autonomous System). Gli indirizzi IP possono essere assegnati solo ad un AS che è stato assegnato a sua volta a un'organizzazione.

Gli indirizzi IP sono assegnati in blocchi ed ogni blocco è descritto dal proprio **Prefisso**. Il Prefisso sono le cifre più significative (a sinistra) comuni a tutti gli indirizzi IP del blocco. Ogni Prefisso ha una lunghezza indicata con */nn* ove nn è la lunghezza in bit del Prefisso. Ad esempio il blocco di indirizzi IP con inizio [5] 10.10.0.0 e fine 10.10.255.255 ha Prefisso 10.10.0.0/16.

Visto che gli indirizzi IP sono assegnati solo a AS e solo in blocchi identificati da Prefissi, è logico che una tabella BGP contenga Prefissi e AS.

BGP-4 prevede la presenza, almeno logica, di tre tipi di tabelle: per comodità in questo articolo

sarà chiamata “tabella BGP” (o “Adj-RIB-In”) una tabella logica in cui un router raccoglie tutti i dati di Routing BGP che ha ricevuto e che possono essere utili; con “tabella di Routing” (o Loc-RIB, Local-Routing-Information-Base) è indicata la tabella con solo le informazioni utilizzate dal router stesso per il Routing dei pachetti IP in ogni istante; e infine con tabella “Update BGP” (o “Adj-RIB-Out”) una tabella logica con le informazioni di routing da inviare ai propri Peer.
La procedura di compilazione di queste tabelle è in linea di principio non troppo difficile anche se richiede alcuni passaggi.

1. Accordi tra organizzazioni

Potrà sembrare strano, ma il primo passo è un accordo, tipicamente commerciale, tra organizzazioni che intendono scambiarsi traffico dati su Internet tramite il protocollo IP. Questo accordo disciplina eventuali costi, tipo e quantità di traffico e anche quali router BGP dell'AS di una organizzazione scambiano “annunci”, ovvero i dati necessari a compilare le tabelle BGP, di Routing e di Update, con quali router BGP dell'altra organizzazione.

2. “Peering” BGP

Una volta definito l'accordo tra le organizzazioni, è possibile configurare un collegamento dati detto “Peering” tra i router BPG delle due AS allo scopo di scambiare “annunci” BGP ed i loro aggiornamenti (modifiche, cancellazioni ecc.). Un annuncio BGP contiene molte informazioni, ma per gli scopi di questo articolo ci limitiamo solo a quelle principali descritte in Fig. 1.

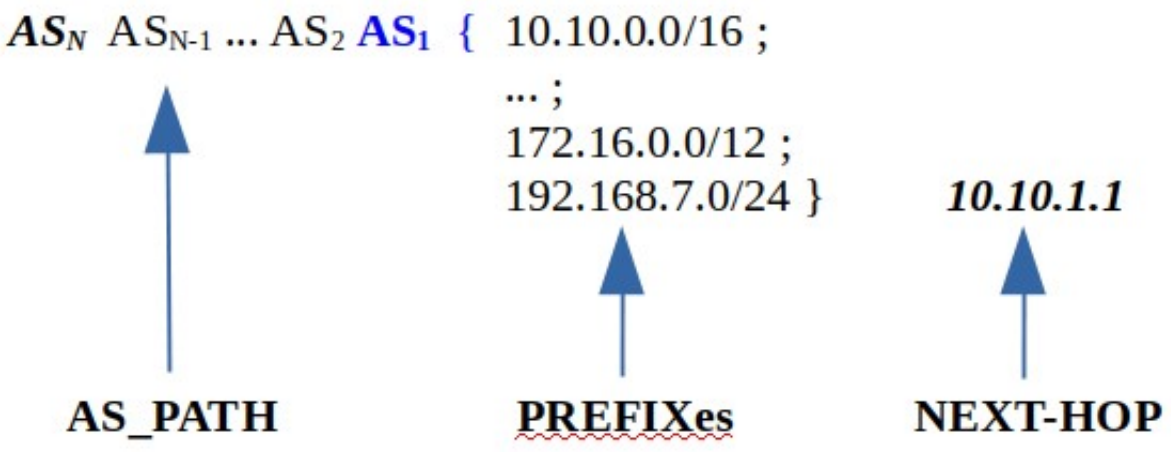


Fig. 1. Principali informazioni presenti in un annuncio BGP

Quando un AS (AS_1) invia i **propri** indirizzi IP ad un'altra AS con cui ha un *peering* BGP, invia i Prefissi (vedi Fig.1), prepende (anche più di una volta) il proprio numero di AS (AS_1) e postpone l'indirizzo IP (Next-Hop) verso il quale il Peer deve inviare il traffico per raggiungere i Prefissi. Il router BGP dell'AS ricevente deve validare il numero di AS da cui ha ricevuto i dati e la raggiungibilità del Netx-Hop. In generale ogni volta che un router BGP riceve un annuncio da un'altra AS, verifica che all'annuncio sia stato preposto il numero dell'AS da cui lo ha ricevuto. In

questo modo, mentre l'annuncio transita da AS ad AS, si forma la AS_PATH, ovvero il cammino tra le AS che l'annuncio ha fatto per arrivare al router BGP in cui è presente. Si noti che i Prefissi appartengono alla prima AS in AS_PATH (AS_1 nel caso di Fig.1).

L'indirizzo IP del Next-Hop, ovvero del primo router a cui inviare i dati per raggiungere quei Prefissi, è invece un'informazione locale, può essere l'indirizzo del router BGP che gli ha inviato l'annuncio od un altro indirizzo IP dell'AS (AS_N) da cui è arrivato l'annuncio e concordato tra le due AS in *Peering*.

Tutti gli annunci ricevuti da un router BGP dai propri *Peer* vengono inseriti e tenuti aggiornati nella “tabella BGP”. Si noti come i dati contenuti nella “tabella BGP” sono sempre una vista locale condivisa con i propri Peer.

3. La “tabella di Routing”

È importante notare che nella “tabella BGP” lo stesso Prefisso può essere presente più volte, annunciato da AS diverse con AS_PATH diverse ma sempre terminanti in AS_1 (ma nel caso di grandi organizzazioni con più AS, lo stesso prefisso può anche essere annunciato inizialmente da AS diverse, come sarà discusso più avanti). Un router BGP deve quindi decidere a quale dei propri Peer inviare il traffico per ognuno dei Prefissi conosciuti. I criteri di scelta sono molti, a partire dai requisiti stipulati negli accordi con i propri Peer: alcune rotte devono essere escluse (filtrate), altre privilegiate ecc. In generale ogni AS deve decidere la propria “Politica di Routing” ed in base a questa vengono configurati i router BGP in modo da selezionare le rotte appropriate. La rotta scelta, viene quindi inserita nella “tabella di Routing” (o Loc-RIB, Local-Routing-Information-Base) ove le uniche informazioni necessarie sono il Prefisso di destinazione del pacchetto e l'indirizzo IP a cui inviarlo, ovvero il Next-Hop.

La “tabella di Routing” è però molto dinamica, si consideri il seguente esempio: il router BGP di una AS in mezzo all'AS_PATH scelta si guasta ed un aggiornamento dell'annuncio pertanto cancella la rotta dalle tabelle. Il router BGP che utilizzava quella rotta, deve scegliere una rotta alternativa per raggiungere quel Prefisso. Alla riattivazione del router BGP guasto, viene re-inserita la rotta precedente, e così via.

4. La “tabella di Update”

Infine il router BGP invia ai propri Peer gli annunci BGP che contengono solo rotte (Prefissi) presenti nella “tabella di Routing” (altrimenti i Prefissi non sarebbero raggiungibili tramite il router BGP che invia l'annuncio) con l'AS_PATH e gli altri dati BGP presenti nella “tabella di Update”. Si noti che un router BGP non è obbligato ad inviare la propria intera “tabella di Routing” ma solo quei Prefissi concordati con il Peer negli accordi formali.

Minacce, rischi e attacchi al Routing BGP

La principale minaccia al Routing BGP è usualmente chiamata “BGP Hijacking” e consiste nella manipolazione (modifica, cancellazione, inserimento ecc.) delle informazioni (annunci) utilizzate per costruire le tabelle BGP e di Routing, o la modifica diretta delle tabelle.

Le possibili conseguenze di un attacco di BGP Hijacking possono essere raggruppate in due classi:

Denial of Service: se un Prefisso è rimosso dalla tabella di Routing od il traffico è inviato su di una rotta che non è in grado di consegnarlo al destinatario (fenomeno anche chiamato “blackholing”), effettivamente viene rimosso da Internet qualunque sistema e servizio che utilizza gli indirizzi IP in quel Prefisso. Questo è spesso accaduto per errore, ma vi sono stati alcuni casi di attacchi volontari. Tra gli episodi più famosi di questo tipo si possono citare:

- 24 dicembre 2004: l'Internet Provider TTNet in Turchia per errore fa convergere tutto il traffico Internet verso la propria rete;
- 7 maggio 2005: per un errore di configurazione di un Internet Provider, Google scompare da Internet per poco meno di 1 ora;
- 24 febbraio 2008: nel tentativo di bloccare l'accesso a YouTube, il Pakistan lo rimuove completamente da Internet;
- 5 gennaio 2017: nel tentativo di bloccare l'accesso ad alcuni siti solo per adulti, l'Iran blocca l'accesso a questi siti in tutto Internet;
- 12 novembre 2018: per un errore di configurazione di un Internet Provider, Google scompare da Internet per poco meno di un'ora.

Ovviamente per un sito web commerciale di grande traffico lo scomparire da Internet anche per poco tempo può provocare dei danni economici ingenti.

Man in the Middle: in questo caso la manipolazione delle tabelle di Routing ha lo scopo di deviare il traffico e farlo passare attraverso reti anche nemiche. Il traffico può essere solamente letto oppure indirizzato verso siti o servizi civetta che imitano il servizio originale. Molti di questi attacchi sono stati perpetrati allo scopo di rubare monete digitali (ad esempio Bitcoin) o di attaccare siti di banche e istituti finanziari, tra questi si possono citare:

- febbraio 2013: il traffico diretto ad alcuni siti di banche e grandi aziende di diverse nazioni è stato instradato per piccoli periodi di tempo, una vittima alla volta, attraverso una rete in Bielorussa;
- agosto 2013: il traffico verso alcuni Prefissi principalmente americani è diretto attraverso un Internet Provider Islandese;
- 24 aprile 2018: diversione del traffico diretto ad alcune reti Amazon allo scopo di rubare monete digitali da alcuni servizi su AWS;
- 30 luglio 2018: il traffico mondiale dell'App Telegram viene fatto transitare attraverso l'Iran;
- 2016-2017: forse il più famoso caso di ridirezione del traffico Internet è quello relativo al dirottamento del traffico attraverso la Cina, per lunghi periodi di tempo, anche mesi, tra gli Stati Uniti ed alcuni Prefissi in altre nazioni tra cui Italia, Canada, Corea, Giappone, Scandinavia ecc. (Rif. 5).

Se un attaccante riesce a dirottare il traffico di suo interesse attraverso una rete che controlla, oltre a leggere il contenuto dei dati scambiati (se non cifrati), può modificarli o impersonare il destinatario

Un altro interessante esempio di BGP Hijacking è stata la frode “3ve” (Rif. 6) che nel 2017 arrivò a controllare 1,5 milioni di indirizzi IP e defraudò alcune aziende di pubblicità online di circa 29 milioni di US dollari. Fornendo spesso documenti falsi, questa organizzazione criminale riuscì a far assegnare a proprie società di comodo, alcuni AS in realtà assegnati ad aziende chiuse o fallite, e Prefissi assegnati ad altre organizzazioni ma non utilizzati, ovvero non “annunciati”. Sfruttando la mancanza di controlli e di interesse dei veri assegnatari delle AS e dei Prefissi, “3ve” utilizzò questi indirizzi IP per creare traffico realistico ma falso[6] su propri siti web nei quali erano presenti le pubblicità delle aziende da frodare. Nell'arco di circa un anno, vi fu un enorme numero di visualizzazioni delle pubblicità su questi siti web che da una parte fruttò all'organizzazione criminale lauti guadagni, ma al contempo suscitò l'interesse delle aziende di pubblicità online che avviarono una investigazione che portò all'individuazione ed all'arresto di alcuni dei criminali.

Route flapping e BGP route flap damping

Uno dei problemi che può creare gravi difficoltà alla gestione delle rotte BGP, è quello dell'instabilità negli annunci. Vi possono essere molti motivi, dalla non convergenza dell'algoritmo di scelta del miglior annuncio per un certo Prefisso, al troppo traffico sul canale di comunicazione con un Peer (si ricordi che il traffico BGP è *inline*, non utilizza connessioni dedicate), per i quali un annuncio può essere inserito nella Tabella di Routing e poco dopo rimosso. L'alternarsi, o “flapping”, dell'annuncio di alcune rotte può rallentare il router BGP impiegando troppe risorse nel calcolo del miglior annuncio, nella modifica delle rotte, e nell'invio delle modifiche ai Peer. E la distribuzione di un “flapping” può causare nei Peer ulteriori “flapping” in una reazione a catena.

La soluzione prevista da BGP-4 è quella del “route flap damping” (Rif. 7): nel caso in cui un annuncio vari troppo frequentemente, il router deve sospenderlo (quindi non inserirlo nella propria tabella di Routing ne inviarlo ai Peer) per un certo periodo di tempo in attesa che l'instabilità si risolva. Più è instabile la rotta e più il periodo di sospensione è lungo, sino ad un massimo di tempo dopo il quale il router prova comunque a ri-annunciare la rotta. Ma l'utilizzo stesso del “route flap damping” può in alcune situazioni causare più danni di quanti ne risolva (si vedano ad esempio le due posizioni del RIPE riportate in Rif. 8) e va quindi adottato con cautela.

Nella seconda parte di questo articolo saranno descritte in maggior dettaglio le problematiche di sicurezza di BGP-4 e le misure di sicurezza adottate e in corso di valutazione.

Note

[1] Essendo tutti dati pubblici, non si pongono problemi riguardo la riservatezza dei dati se non per quanto riguarda eventuali aspetti di Privacy, che però non sono considerati in questo articolo.

[2] Si noti che tra il 2011 e il 2019 si è esaurita l'assegnazione di indirizzi IPv4, oggi si possono richiedere nuovi indirizzi IPv6 o attendere che vengano resi liberi degli indirizzi IPv4 in uso.

[3] In realtà dal 2010 anche gli astronauti sulla Stazione Spaziale possono accedere a Internet ma indirettamente, tramite un elaboratore a terra.

[4] Questo è tecnicamente indicato con E-BGP, External BGP, mentre I-BGP, Internal BGP, descrive l'applicazione del protocollo a reti interne a un'organizzazione, o più precisamente a una AS, come viene descritto di seguito.

[5] Gli indirizzi IP mostrati in questo articolo sono del tutto casuali e tipicamente non validi in Internet ma solo come indirizzi privati locali.

[6] Gli indirizzi IP erano assegnati a server sui quali erano eseguiti dei Bot che visitavano i siti web e cliccavano sulle pubblicità.

Riferimenti bibliografici

Rif. 1: i protocolli originali sono specificati in RFC-882 e RFC-883 per DNS e RFC-1105 per BGP.

Rif. 2: RFC-791 “Internet Protocol”.

Rif. 3: RFC-4271 “A Border Gateway Protocol 4 (BGP-4)"

Rif. 4: si veda ad esempio https://en.wikipedia.org/wiki/Regional_Internet_registry per cartine e maggiori dettagli.

Rif. 5: C.C. Demchak, Y. Shavitt “China’s Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom’s BGP Hijacking”, Military Cyber Affairs: Vol. 3, Iss. 1, Article 7, https://scholarcommons.usf.edu/mca/vol3/iss1/7/

Rif 6: Google and White Ops “The Hunt for 3ve”, https://services.google.com/fh/files/blogs/3ve_google_whiteops_whitepaper_final_nov_2018.pdf , si veda anche A. Pasquinucci “Like a Movie Plot: the 3ve Defrauding Scheme”, https://blog.ucci.it/2019/01/02/like-a-movie-plot-the-3ve-defrauding-scheme/ , e ArsTechnica “How 3ve’s BGP hijackers eluded the Internet—and made $29M”, https://arstechnica.com/information-technology/2018/12/how-3ves-bgp-hijackers-eluded-the-internet-and-made-29m/

Rif. 7: RFC-2439 “BGP Route Flap Damping”

Rif. 8: “RIPE Routing Working Group Recommendations On Route-flap Damping” https://www.ripe.net/publications/docs/ripe-378 e https://www.ripe.net/publications/docs/ripe-580

Articolo a cura di **Andrea Pasquinucci**