網際網路交換中心路由安全實作探討
-以 FOX 交換中心為例

陳俊傑
財團法人國家實驗研究院國家高速網路與計算中心
jjchen@narlabs.org.tw

摘要

本文將說明網際網路交換中心IXP運作機制與路由安全防護的議題，包含交換中心路由監控與安全防護機制，說明 FOX 交換中心路由安全政策與開發建置的 IRR/RPKI 路由監控與過濾系統功能，利用 IRR 與 RPKI 路由資料來認證 IXP 成員宣告路由的正確性，避免 BGP 路由劫持(BGP Hijacking)與路由洩露(BGP Leak)的路由攻擊問題並提供 UI 介面連動 IXP Route Server 進行過濾與封鎖。

關鍵詞：網際網路交換中心 IXP、FOX、路由安全、BGP、網際網路路由註冊 IRR、資源公鑰基礎建設 RPKI。

1. 前言

隨著網際網路的技術進步與便利，網際網路的使用者也大幅增加，根據全球網路設備大廠思科(Cisco)網際網路年報[1]指出2023年全球有53億網際網路使用者，平均每個人有3.6台上網設備，寬頻速度平均達110Mbps，網際網路使用者數量趨勢如圖1。

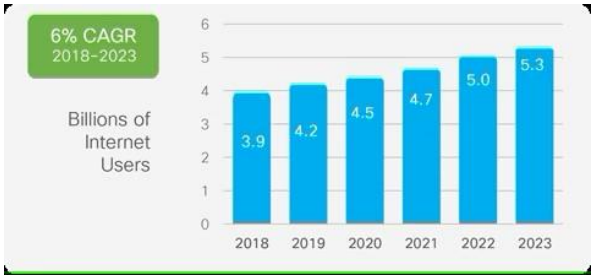

圖1 網際網路使用者數量趨勢
*Source: Cisco Annual Internet Report, 2018-2023

網際網路提供者(Internet Service Provider， ISP)頻寬大幅提升，ISP 間的路由交換也越來越多，國際網路學會(Internet Society)[2]舉出網際網路交換中心(Internet Exchange Point，IXP)為各區域 ISP 間創建更短的路由，與將本地 ISP 流量轉送到國外相比，這是一種更經濟實惠的替代方案。IXP 以更低的成本提供更好的彈性、穩定性、效率和質量改進。由於 ISP 在 IXP 進行路由交換，IXP 的路由安全相對重要，本文針對 IXP 路由安全進行探討，於第2章節陳述 IXP 路由安全議題，第3章節描述 FOX[3]交換中心路由政策，第4章節說明 FOX 交換中心路由監控與過濾系統開發緣由與功能，第5章節說明系統現況與結論。

2. IXP 路由安全議題

根據 Internet Society IXP 定義[4]，IXP 提供實體 Layer2網路交換環境，讓 ISP 接入 IXP 進行對等互連(Peering)，ISP 網路利用各自所擁有的自主系統碼(Autonomous System Number，ASN)與邊界閘道路由協定(Border Gateway Protocol ，BGP)來進行 Peering 以交換 ISP 下所屬的路由網段由交換，IXP 網路架構示意如圖2。

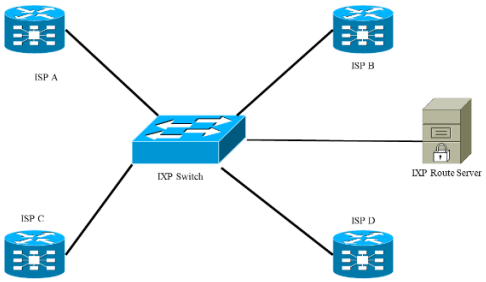

圖2 IXP 架構示意圖

ISP 經由 IXP 進行 Peering 有兩種方式[5]，一種為 MLPA (Multi-Lateral Peering Agreement)，ISP 只要通過 IXP Route Server 建立 BGP 連線來交換路由資訊，一種為 BLPA (Bi-Lateral Peering Agreement)，ISP 根據自己的需求與個別 ISP 進行 Peering，兩者的差異是經由 Route Server(RS)來收送路由，ISP 可以節省建立 BGP 連線與設定，如圖3所示。

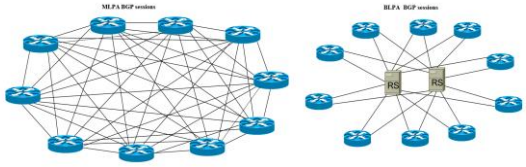

圖3 IXP BGP sessions

又依據亞太網路資訊中心(Asia-Pacific Network Information Centre，APNIC))路由統計[5]，目前網路網路的路由筆數達932962筆，ASN 數量達74517個，網際網路路由筆數逐年增加如圖4[5]，BGP 路由協定作為 IXP 主要的路由交換協定，在 IXP 的

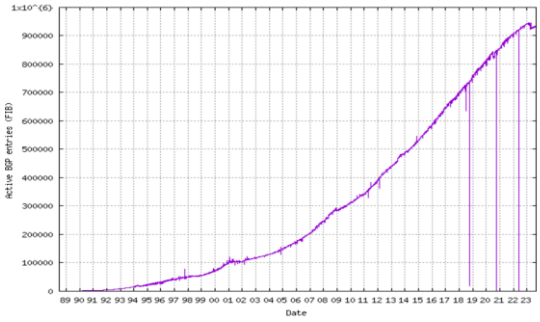

圖4 Internet BGP 路由筆數

的安全考量方面是需要特別去強調與施作，BGP 的運作與安全性在 RFC 7454[6]中有全面性的建議與討論，另外 IXP 中的經由 RS 來控制 BGP 路由收送，在 RFC 7948[7]有提及網際網路 BGP Route Server 的安全性考量，綜合兩份 RFC，在 IXP 的路由安全考量有幾方面，2.1 IXP peering subnet 不屬於任何 ISP，只是利用此網段的一個 peer IP 來進行 BGP 路由交換，且當作 BGP 路由的下一跳(Next-hop)，ISP 須禁止將 IXP peering subnet 在轉宣告出其他網路，避免 IXP peeing subnet 受到 DDoS 攻擊; 2.2 路由數量限制，由於 IXP 不提供轉訊服務(Transit)，ISP 所交換的路由須設定上限，避免大量的路由轉發造成其他 ISP 的路由爆量; 2.3路由過濾機制，避免 ISP 宣告錯誤路由與 ASN 訊息，須進行路由過濾機制，防止錯誤的路由散發;2.4路由驗證，由於 IXP RS 收取 ISP 路由並進行轉發，須針對 ISP 送過來的路由進行路由的正確性驗證與過濾，避免發生 BGP 劫持(BGP Hijacking)與路由洩露(BGP Leak)的路由攻擊問題。後續第3個章節將說明 FOX RS 路由政策與相對應的 RS 路由安全防護設定，第4章節將說明 FOX 開發的路由驗證與過濾系統。

3. FOX 交換中心路由政策

FOX 參考[6][7]訂定 RS 路由政策[8]，針對各項路由政策相對應的 RS 路由設定[9]，建立 RS 路由過濾設定樣板，將該樣本套用在每個成員的 BGP 路由基本設定上，樣板各路由設定詳細說明如下，

3.1 預設過濾的路由網段

過濾 Bogon 網段(prefixes)，私人及保留的網段及預設路由(Default route)，RS 設定樣板如下。

```
#----------------------------------------------------
Bogon prefixes filtering(IPv4)
#----------------------------------------------------
policy-options
        begin
         prefix-list "BOGONS_V4"
            prefix 0.0.0.0/0 exact
            prefix 0.0.0.0/0 through 6
            prefix 10.0.0.0/8 longer
prefix 100.64.0.0/10 longer
            prefix 127.0.0.0/8 longer
            prefix 128.0.0.0/16 longer
            prefix 169.254.0.0/16 longer
            prefix 172.16.0.0/12 longer
            prefix 191.255.0.0/16 longer
            prefix 192.0.0.0/24 longer
            prefix 192.0.2.0/24 longer
            prefix 198.18.0.0/15 longer
prefix 192.88.99.0/24 longer
prefix 192.168.0.0/16 longer
prefix 198.51.100.0/24 longer
            prefix 203.0.133.0/24 longer
            prefix 224.0.0.0/3 longer
            prefix 240.0.0.0/4 longer
           prefix 255.255.255.255/32 longer
          exit
 policy-statement BGP_FILTER_IN"
            entry 20
               from
                  prefix-list "BOGONS_V4"
               action drop
              exit
            exit
             default-action accept
          exit
         commit
       exit
#----------------------------------------------------
Bogon prefixes filtering(IPv6)
#----------------------------------------------------
policy-options
         begin
         prefix-list "BOGONS_V6"
            prefix ::/8 longer
            prefix 100::/64 longer
            prefix 2001:2::/48 longer
            prefix 2001:10::/28 longer
            prefix 2001:db8::/32 longer
            prefix 2002::/16 longer
            prefix 3ffe::/16 longer
            prefix fc00::/7 longer
            prefix fe80::/10 longer
            prefix fec0::/10 longer
            prefix ff00::/8 longer
          exit
 policy-statement "BGP_FILTER_IN"
            entry 30
               from
                  prefix-list "BOGONS_V6"
               exit
               action drop
               exit
            exit
            default-action accept
          exit
         commit
exit
```

3.2 ASN 過濾

過濾 BGP 路由中的 AS 路徑包含 Bogon ASNs、私人及保留的 ASNs，不允許成員宣告包含私人與保留的 ASNs 路徑的 BGP 路由。

```
policy-options
begin
as-path-group "BOGONS_ASN"
   entry 10 expression ".* 23456 .*"
   entry 15 expression ".* [64496-64511] .*"
   entry 20 expression ".* [65536-65551] .*"
   entry 25 expression ".* [64512-65534] .*"
   entry 30 expression ".* [4200000000-
```

```
    4294967294] .*"
    entry 35 expression ".* 65535 .*"
    entry 40 expression ".* 4294967295 .*"
    entry 45 expression ".* [65552-131071] .*"
  exit
  policy-statement "BGP_FILTER_IN"
    entry 10
      from
        as-path-group "BOGONS_ASN"
      exit
      action drop
    exit
      default-action accept
      exit
  commit
exit
```

3.3 路由網段長度過濾

過濾長度大於/24(IPv4)、/48(IPv6)的網段，避免成員宣告路由網段過長造成路由過於分散與造成路由表過大。

```
policy-options
  begin
  prefix-list "TOO_SMALL_PREFIXES"
    prefix 0.0.0.0/0 prefix-length-range 25-32
    prefix ::/0 prefix-length-range 49-128
              exit
   policy-statement "BGP_FILTER_IN"
     entry 40
      from
      prefix-list "TOO_SMALL_PREFIXES"
       exit
       action drop
       exit
       exit
       default-action accept
       exit
       commit
     exit
```

3.4 AS 路徑長度過濾

過濾過長的 AS Paths，過濾成員宣告過長 AS 路徑的路由，避免中間轉訊的 ISP 過多，容易造成路由迴圈與路由洩漏。

```
policy-options
       begin
       policy-statement "BGP_FILTER_IN"
          entry 50
             from
                as-path-length 10 or-higher
             exit
             action drop
             exit
          exit
                default-action accept
             exit
```

3.5 路由筆數上限

設定路由筆數上限(預設為100筆，可依需求調整)，避免路由風暴產生，造成 RS 與成員的路由處理資源耗盡。

```
bgp
       graceful-restart
       exit
       local-as 9681
       bfd-enable
       best-path-selection
          compare-origin-validation-state
         origin-invalid-unusable
       exit
      group "IX_eBGP"
      prefix-limit ipv4 200 threshold 95 idle-
      timeout 30
      prefix-limit ipv6 200 threshold 95 idle-
      timeout 30
      remove-private
       local-address 211.73.85.x
       third-party-nexthop
        monitor
            station all
             route-monitoring post-policy
             no shutdown
             exit
        exit
       exit
```

3.6 IRR 過濾

網際網路路由註冊(Internet Routing Registry，IRR)[10]是一個全域的分散式路由資訊資料庫，在1995年開始建立，目的為確保網際網路的路由穩定與一致性，IRR 資料庫包含 ISP 的路由政策與宣告，以確保其他 ISP 可以查詢並利用此資料庫來進行網路除錯與規劃。FOX 建置路由監控與 IRR 路由比對系統，用來確認 FOX IXP 成員的路由正確性來避免 BGP Hijacking/BGP Leaking 問題發生。

3.7 RPKI 過濾

資源公鑰基礎建設 Resource Public Key Infrastructure，RPKI)[11]用於保護網際網路路由基礎建設，特別是在邊界閘道器協定 BGP 上。RPKI 利用路由起源授權 ROA (Route Origin Authorization)的格式，將 IP 位址與自治系統編號 ASN 進行連結，ISP 可利用簽署過的 IP 位址終端憑證以及 ASN 終端憑證建立 ROA，使 IP 位址與 ASN 關聯起來。 FOX 建置 RPKI 路由比對過濾系統同以同步 ROA 資料。當 FOX 成員發送路由給 Fox Route server 時，FOX 使用 RPKI 驗證合法性，每筆路由比對來源宣告後有以下三種結果： 有效(Valid)、無效(Invalid)、未知(Unknown)。FOX 預設會對 Invalid 路由進行阻擋，特殊情

況可申請暫時允許，在 Unknown 的部分則會通知成員說明該筆路由合法性。IRR 與 RPKI 過濾系統詳細的系統功能說明將在下個章節陳述。

4. FOX 交換中心路由監控與過濾系統

由於 IRR 與 RPKI 的資料來源與使用目的不一樣，所以會產生路由一致性的問題，如圖5顯示同一筆路由會有不一致的比對結果。

Prefix	in BGP (RIS)	IRRs	RPKI ROV	VRPs
120.107.0.0/16	✓		☺	maxLength: 16
120.96.0.0/11	✓		☺	maxLength: 11
134.208.0.0/16	✓	NTTCOM RADB	👁	
140.110.0.0/15	✓	NTTCOM RADB APNIC	☺	maxLength: 15
140.112.0.0/12	✓	NTTCOM RADB	☺	maxLength: 12
140.128.0.0/13	✓	NTTCOM RADB	☺	maxLength: 13
140.128.0.0/16				maxLength: 16
140.136.0.0/15	✓	NTTCOM RADB	☺	maxLength: 15
140.138.0.0/16	✓	NTTCOM RADB	☺	maxLength: 16
140.138.0.0/24		RADB		
140.92.0.0/16	✓	NTTCOM RADB	👁	
140.92.0.0/17	✓		👁	
140.92.128.0/17	✓		👁	
163.13.0.0/16	✓	NTTCOM RADB	☺	maxLength: 16

圖5 IRR 與 RPKI 路由比對差異

另外，根據 CAIDA (UC San Diego)研究顯示目前最大的 IRR 資料庫 RADB 覆蓋了將近60%網際網路路由表[12]，但 RPKI 的資料也不斷增加中，如圖6。

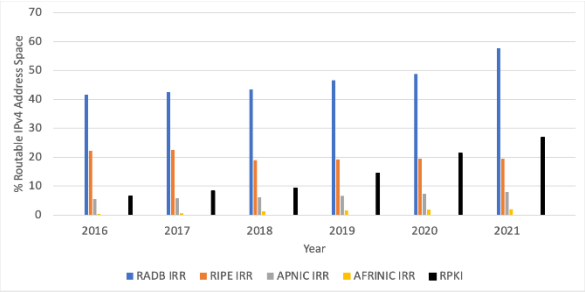

圖6 IRR 與 RPKI IPv4路由數目佔比

FOX 為了解決 IRR 與 RPKI 路由過濾資料不一致問題，在 FOX CBM 網管系統的路由監控模組新開發建置了 IRR/RPKI 路由監控與過濾系統，系統架構如圖7。

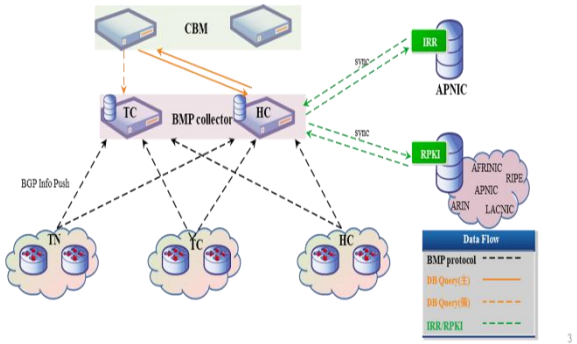

圖7 FOX IRR/RPKI 路由監控與過濾系統架構圖

CBM 網管系統利用 HC、TC BMP[13] Collector 收取 RS 路由資訊並存入 DB 資料庫進行後續的監控與比對，BMP 為一種 BGP 路由監控協定，可由 RS 主動提供 BGP 路由串流資訊給 BGP Collector 收集 RS 路由資訊。在 IRR 資料的同步與比對方面，BMP Server 透過 FTP 方式將 IRR 資料拉回並寫入 DB， BMP Server 從資料庫取出 BGP Prefix、AS 資料與 IRR table 比對，產出比對結果顯示於 CBM，資料流如圖8。

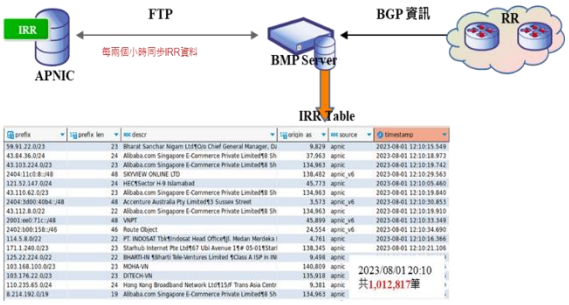

圖8 IRR 資料同步與比對

在 RPKI 資料同步與比對方面，BMP Server 透過 API 方式，將 RPKI 資料拉回並寫入 DB，RR 如啟用自身的 RPKI 比對機制，會透過 RTR 協定從 BMP 獲取 RPKI 資料，進行 BGP 資訊比對，BMP Server 從資料庫取出 BGP Prefix、AS 資料與 RPKI table 比對，產出比對結果顯示於 CBM，資料流如圖9。

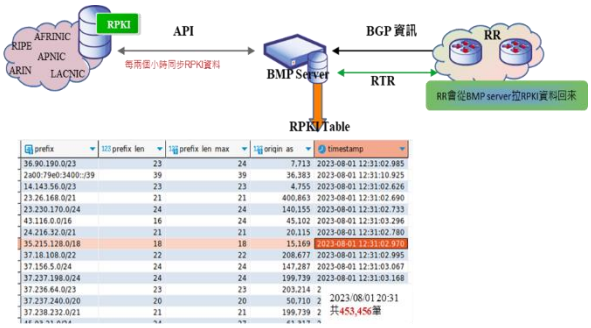

圖9 RPKI 資料同步與比對

從 DB 發現 IRR 與 RPKI 的資料筆數不一樣如表

1。

表1 IRR/RPKI 資料筆數

IRR DB	資料筆數	RPKI DB	資料筆數
APNIC	685,642	AFRINIC	7,532
APNIC_v6	327,175	APNIC	113,352
		AMIC	80,277
		LACNIC	31,878
		RIPE	220,417

當路由比對出現 Invalid 或 Unknown，系統會出現告警，如圖10，後續網路管理者可以使用系統 UI 與路由過濾腳本，針對 Invalid/Unknown 路由進行過濾封鎖與解鎖。

圖10 路由監控與比對結果

5. 結論

IRR/RPKI 路由監控與過濾系統在路由過濾功能牽涉到與 RR 路由設備的連線與設定，效能要求極高，須能盡快完成設備連線與封鎖腳本供裝，我們測試系統過濾效能，在封鎖/解鎖1筆路由時間如表2。因應未來可能須封鎖多筆路，我們測試了封鎖/解鎖1筆、10筆、100筆路由，結果如表3，發現封鎖時間不隨路由筆數增加而大幅增加，系統執行效能約可在30秒內完成。

表2 封鎖/解鎖 1筆路由時間

No.	封鎖執行時間			解鎖執行時間		
	開始	結束	耗時(秒)	開始	結束	耗時(秒)
1	2023/7/26 10:56:53	2023/7/26 10:57:15	22	2023/7/26 11:00:08	2023/7/26 11:00:33	25
2	2023/7/26 11:16:10	2023/7/26 11:16:33	23	2023/7/26 11:17:21	2023/7/26 11:17:46	25
3	2023/7/26 11:22:57	2023/7/26 11:23:19	22	2023/7/26 11:25:59	2023/7/26 11:26:23	24
4	2023/7/26 11:37:33	2023/7/26 11:37:57	24	2023/7/26 11:43:10	2023/7/26 11:43:35	25
5	2023/7/26 11:47:27	2023/7/26 11:47:50	23	2023/7/26 13:42:04	2023/7/26 13:42:29	25
6	2023/7/26 13:59:08	2023/7/26 13:59:31	23	2023/7/26 14:00:11	2023/7/26 14:00:36	25
7	2023/7/26 14:29:49	2023/7/26 14:30:12	23	2023/7/26 14:37:33	2023/7/26 14:37:58	25
8	2023/7/26 14:41:29	2023/7/26 14:41:52	23	2023/7/26 14:42:21	2023/7/26 14:42:46	25
9	2023/7/26 14:45:15	2023/7/26 14:45:39	24	2023/7/26 14:47:17	2023/7/26 14:47:45	28
10	2023/8/2 10:17:08	2023/8/2 10:17:32	24	2023/8/2 10:19:42	2023/8/2 10:20:09	27

表3 封鎖/解鎖多筆路由時間

路由筆數	封鎖執行時間			解鎖執行時間		
	開始	結束	耗時(秒)	開始	結束	耗時(秒)
1	2023/7/26 10:56:53	2023/7/26 10:57:15	22	2023/7/26 11:00:08	2023/7/26 11:00:33	25
10	2023/8/16 17:51:09	2023/8/16 17:51:30	21	2023/8/16 17:52:08	2023/7/26 17:52:34	26
100	2023/8/16 17:45:09	2023/8/16 17:45:40	31	2023/8/16 17:47:05	2023/8/16 17:47:43	38

在 RPKI 推廣尚不全面完整[14]，MANRS 統計 RPKI 驗證 Unknown Routes 尚有54.53%，如圖11

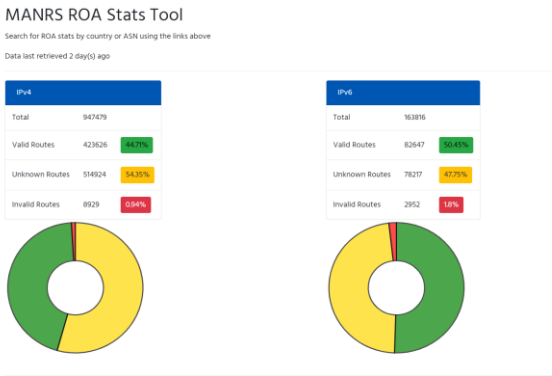

圖11 MANRS RPKI ROA 資料統計

且 IRR 資料正確性待考量[12]之際，不用強制性過濾機制並持續監控 IXP 成員路由正確性，主動通報並保留過濾機制的方式為現階段保護 IXP 路由安全的方法之一，FOX 交換中心已取得 MANRS IXP 成員認證[15]，將持續持續同步更多 IRR 資料來源並推廣 MANRS 認證，優化系統介面與統計報表，提供 IXP 更好的路由安全防護。

參考文獻

[1] Cisco Annual Internet Report，https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html

[2] https://www.internetsociety.org/issues/ixps/

[3] 張聖翊、李慧蘭、古立其5]、李柏毅、陳敏，“公共服務網路交換中心規劃與建置”，TANET2021 臺灣網際網路研討會，台中，2021

[4] https://www.internetsociety.org/resources/doc/2020/explainer-what-is-an-internet-exchange-point-ixp/

[5] APNIC IPV4 BGP Reports，https://bgp.potaroo.net/as2.0/bgp-active.html

[6] RFC7454 BGP Operations and Security，https://datatracker.ietf.org/doc/html/rfc7454

[7] RFC 7948 Internet Exchange BGP Route Server Operations， https://datatracker.ietf.org/doc/html/rfc7948

[8] FOX RS 連線路由政策，https://www.fox.net.tw/linked.html

[9] Nokia Configuration for MANRS Actions，https://www.manrs.org/participant/89/

[10] APNIC IRR service，https://www.apnic.net/manage-ip/apnic-services/routing-registry/

[11] TWNIC RPKI 服務，https://rpki.tw/RPKI_service.html

[12] IRR Hygiene in the RPKI Era，Du, B. et al. (2022). IRR Hygiene in the RPKI Era. In: Hohlfeld, O., Moura, G., Pelsser, C. (eds) Passive and Active Measurement. PAM 2022. Lecture Notes in Computer Science, vol 13210. Springer, Cham. https://doi.org/10.1007/978-3-030-98785-5_14

[13] RFC 7854 BGP Monitoring Protocol (BMP)，https://datatracker.ietf.org/doc/html/rfc7854

[14] MANRS RPKI ROA 統計報表，https://roa-stats.manrs.org/

[15] MANRS IXP Participant，https://www.manrs.org/participant/4090/