

# 網際網路交換中心之路由安全相互協議規範(MANRS)

## MANRS IXP Programme

### 中文版

( 本文為 <https://www.manrs.org/ixps/> 之翻譯，

於 2019 年 9 月，由 TWNIC 提供此翻譯中文版供參考。 )

**MANRS** 是邁向全球強健及安全路由基礎設施的重要一步

**MANRS** 行動(MANRS Actions)最初是針對網路營運商而設計，但是，網際網路交換中心(IXP, Internet Exchange Point)在保護網際網路方面，亦應扮演積極的角色。IXP 代表具有共同經營目標的活躍社群，並已對更具韌性及更安全的網際網路基礎設施做出貢獻。

**MANRS** 可運用 IXP 的資訊安全基線，協助 IXP 打造安全的鄰域，同時展現出 IXP 對網際網路生態系統資訊安全及永續性的承諾，並致力於提供高品質的服務。

**IXP** 是 **MANRS** 社群內的重要夥伴

IXP 可以成為協同合作的焦點，負責討論與推廣路由安全的重要性。為了解決 IXP 獨特的需求和考量，社群已為 IXP 成員建立了一套相關，但是獨立的 **MANRS** 行動。

資格標準及實施證明

在加入時，**IXP** 必須實施大部分的 **IXP** 計畫行動（至少五分之三），以展現其決心。行動 1 和 2 為強制項目，且 **IXP** 至少必須實施一項額外行動。

應在相關文件（例如 **IXP** 政策、技術概要等）中反映出實施的具體行動，且本文件應可公開取得，或至少可提供給 **IXP** 成員。在加入 **MANRS** 時，會要求 **IXP** 提供該文件的連結。

本文件之用語

**IXP 成員(IXP member)** - 使用由一個 **IXP** 提供之互連服務的網路，視 **IXP** 的模式而定，可能是一個做為 **IXP** 客戶的 **IXP** 成員等。

**MANRS IXP 計畫(MANRS IXPP)參與者(MANRS IXP Programme (MANRS IXPP) participant)** - 參與 **MANRS IXPP** 的 **IXP**

**IXP** 計畫行動方案

行動 1、防止傳播錯誤的路由資訊。（強制）

**IXP** 在路由伺服器上，依據路由資訊資料（**IRR** 及 / 或 **RPKI**）過濾路由通知。

依據認證程序的結果，遵循 **IXP** 發布的政策，過濾無效的通知。

在利用路由伺服器促成多邊互連的 **IXP** 時，應使用該伺服器確認接收自對等方的路由通知，並在過濾後送至其他對等方。特殊用途，例如研究專案，已超出本要求之範圍。

認證方式通常是依據 **IRR** 資料（解析 **AS-SET** 物件）或 **RPKI** 資料（**ROA** 物件或有效的快取），檢查 **BGP** 通知。依據「bogons」或「martians」（**RFC1918**、**RFC5735** 及 **RFC6598** 定義之 **IP** 前綴、**RFC5398**、**RFC6793**、**RFC6996**、**RFC7300**、**RFC7607** 定義之 **AS-PATH** 中的 **ASN**）檢查通知，也是常見的做法。

行動 **2**、向 **IXP** 成員推廣 **MANRS**。（必須完成一項或多項）

**IXP** 鼓勵或協助成員實施 **MANRS** 行動。（針對不同的誘因等級，有 **4** 個獨立的核取方塊，且必須完成一項或多項。）

**IXP** 可藉由鼓勵其成員實施部分或完整的 **MANRS** 行動，以積極推廣 **MANRS**，且可採取不同的鼓勵形式：

行動 **2-1**：協助其成員在適當的儲存庫（**IRR** 及 / 或 **RPKI**）中，留存準確的路由資訊

例如採取訓練或教學的方式，做為加入流程的一部分

行動 **2-2**：在成員實施 **MANRS ISP** 行動時提供協助

例如採取訓練或教學的方式，做為加入流程的一部分

行動 **2-3**：在成員清單及網站上顯示其參與 **MANRS**

行動 **2-4**：提供與 **MANRS** 就緒有關的誘因

此可能為象徵性的降價或任何其他利益，原因在於符合 **MANRS** 的成員不太可能會對其他對等方及 **IXP** 運作造成困擾，且容易協調等，因此可降低提供 **IXP** 服務的成本。

行動 **3**、保護對等互連平台。

**IXP** 已發布對等互連架構不允許之流量的政策，並已針對此等流量進行過濾。

一般而言，過濾適用於：

- 不允許的乙太網框架格式
- 不允許的乙太類型(Ethertypes)
- 連結本地協定，例如 IRDP、ICMP 重新導向、發現協定(CDP, EDP)、VLAN / 中繼協定(VTP, DTP)、BOOTP/DHCP 等
- 受到 MAC 連接埠安全組態之限制

嚴格來說，雖然不算路由，但是保持第二層(Layer 2)的衛生(hygiene)，可確保平台平順運作，並有助於 **IXP** 基礎設施與路由的穩定性。

行動 4、促進網路營運商之間的全球運作溝通及協調。

**IXP** 是透過提供必要的郵件清單與成員目錄，促進成員之間的溝通。**IXP** 及其每一位成員皆至少擁有一個有效、使用中的電子信箱地址與電話號碼，可供其他成員在發生濫用、資訊安全及操作事件時使用。

**IXP** 成員之間的有效溝通，對於緩解錯誤配置、中斷或 DoS 攻擊等網路事件而言至關重要。郵件清單或其他通信方式，以及包含最新聯絡資訊之所有交換成員可取得的成員目錄，均扮演至關重要的角色。

行動 5、為成員提供監控及除錯工具。

**IXP** 提供窺鏡給其成員。

窺鏡(looking glass)是一項重要的設施，可協助排除路由事件或異常，並防止或縮短潛在的中斷。**IXP** 應將路由伺服器的窺鏡介面提供給其成員。