本文档旨在规范化 IPv4 数据包的 MPLS 封装处理，以减轻针对 MPLS 基础设施的基于 IPv4 选项的安全攻击的现有风险。在 RFC791 规定中，典型的 IPv4 数据包首部可选字段包括时间戳、安全性和特殊路由的规定。在实际应用中，典型的例子包括严格和松散的源路由选项、记录路由选项和路由器警报选项。

多协议标签交换（MPLS）将基于前缀的转发等价类（FEC）相关联的数据包被封装成一个标签堆栈，然后通过标签交换路由器（LSRs）序列沿着标签交换路径（LSP）进行切换。但当时尚未形成有关 MPLS 的正式标准，这可能会导致下游 LSR 可能没有足够的 IPv4 路由信息来转发包，从而导致包丢失。其次，下游 lsr 必须应用 IPv4 转发规则，这可能会使它们受到 IPv4 安全攻击。

于是，在本文档，提出了以下要求：

1. 入口标签路由器的要求

1.1 必须实行的策略：

• 在确定是否对 IPv4 数据包推送 MPLS 标签堆栈时，或在确定标签堆栈中出现的标签值时，应**忽略 IPv4 数据数据包首部中其他可选选项**。【可在入口 LER 上配置，但默认情况下应启用】

• 在启用具有更具体转发规则的信令消息或处理数据包时，不应更改此处理规则。

• **适用范围**：资源预留协议（RSVP）、源路由[RFC791]、未来定义的其他 FEC 规范。

1.2 该策略的作用

• 防止属于基于前缀的 FEC 的 IPv4 数据包因为首部选项而绕过 MPLS 封装。

• 防止特定选项类型（如路由器警）在入口 LER 时强制 MPLS 实施路由器警告标签（标签值 1）。

2. 安全考虑

如果不采取以上措施，可能会产生以下安全问题，对 MPLS 基础设施产生影响：

1) 绕过 MPLS 封装的攻击：

攻击者可能通过绕过在入口 LER 处的 MPLS 封装，并强制在入口 LER 处对 MPLS 打 Router Alert 标签，从而在下游 LSR 上触发 DoS 条件，这可能对控制和管理协议产生不利影响，从而影响 LSR 的可用性。

2) 绕过 MPLS 核心隐藏的攻击：

攻击者在入口 LER 处绕过 MPLS 封装，使这些数据包在 MPLS 核心网络下游不进行标签交换，而绕过 MPLS 核心隐藏，从而暴露了网络拓扑结构。

3) 绕过 MPLS 网络转发的攻击：

攻击者在入口 LER 处绕过 MPLS 封装，使这些数据包在 MPLS 核心网络下游不携带 IPv4 路由信息，可能阻止带有合法选项的 IPv4 数据包通过 MPLS 网络传输，引发 ICMP 终点不可达消息。

4) 绕过 LSP Diffserv 隧道的攻击：

攻击者在入口 LER 处绕过 MPLS 封装，绕过 LSP Diffserv 隧道和入口 LER 处的 MPLS 服务类（CoS）字段标记策略,这可能导致未经授权的各方窃取高优先级服务。

5) 绕过 MPLS 封装的 RSVP 软状态攻击：

攻击者在入口 LER 处绕过 MPLS 封装，在下游 LSR 上构建 RSVP 软状态。这可能导致未经授权的各方窃取服务或由于锁定 LSR 资源而触发 DoS 条件。

6) Router Alert Label 的强制施加：

使用 MPLS Router Alert Label 的 MPLS 数据包会被 LSR 以异常方式处理，效率较低。在入站 LER 处强制使用基于前缀的 FEC 的特定 IPv4 选项（如 Router Alert）可能会让攻击者在入站 LER 处强制应用 MPLS Router Alert Label，从而触发下游 LSR 的 DoS 条件。