ICS 33.040.40
M 32

YD

中华人民共和国通信行业标准

YD/T 2029-2009

基于软线技术的互联网 IPv6 过渡技术框架

Softwire based mesh framework for internet IPv6 transition

2009-12-11 发布　　2010-01-01 实施

中华人民共和国工业和信息化部　发布

目　　次

前　言

本标准是“IPv6 协议”系列标准之一，该系列标准预计的结构及名称如下：

1. YD/T 1341-2005　IPv6 基本协议——IPv6 协议
2. YD/T 1442-2006　IPv6 网络技术要求——地址、过渡及服务质量
3. YD/T 1343-2005　IPv6 邻居发现协议——基于 IPv6 的邻居发现协议
4. IPv6 技术要求——IPv6 路由器重配置协议
5. IPv6 技术要求——IPv6 反向邻居发现协议
6. IPv6 技术要求——IPv6 路径 MTU 发现协议
7. IPv6 技术要求——IPv6 动态主机配置协议
8. IPv6 技术要求——支持计算机移动部分
9. YD/T 1344-2005　IPv6 地址结构协议——IPv6 无状态地址自动配置
10. YD/T 1612-2007　IPv4 网络向 IPv6 网络过渡中的互联互通技术要求
11. YD/T 1635-2007　IPv6 网络技术要求——面向网络地址翻译（NAT）用户的 IPv6 隧道技术
12. YD/T 1656-2007　采用边界网关协议多协议扩展（BGP-MP）的基于 IPv6 骨干网的 IPv4 网络互联（4 over 6）技术要求
13. YD/T 1915-2009　IPv6 技术要求——移动 IPv6 快速切换
14. IPv6 邻居发现安全性技术要求
15. YD/T 2029-2009　基于软线技术的互联网 IPv6 过渡技术框架

本标准由中国通信标准化协会提出并归口。

本标准起草单位：清华大学、工业和信息化部电信研究院、中国移动通信集团公司、中国电信集团公司、华为技术有限公司、中兴通讯股份有限公司。

本标准主要起草人：崔　勇、徐明伟、吴建平、李　星、徐　恪、赵　锋、何宝宏、蒋林涛、段晓东、解冲锋、刘恩慧、曹　伟、罗　鉴。

基于软线技术的互联网 IPv6 过渡技术框架

1 范围

本标准对在 IPv4 网络向 IPv6 网络过渡中可能出现的若干相同地址簇（如 IPv4）接入网穿越另一种地址簇（如 IPv6）骨干网互联互通的过渡技术——软线式网状架构做了规范性描述。IPv4 向 IPv6 过渡涉及到多方面内容。

本标准适用于同地址簇网络间穿越另一种地址簇网络互通的场景。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

IETF RFC 2385（1998）	使用TCP MD5签名保护BGP会话的方法
IETF RFC 4459（2006）	隧道技术中的MTU及分片问题
IETF RFC 4798（2007）	通过IPv4 MPLS网络连接IPv6网络孤岛
IETF draft-ietf-idr-v4nlri-v6nh-02	使用IPv6下一跳地址通告IPv4路由可达信息

3 术语、定义和缩略词

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

封装 encapsulation

把一种协议的完整数据分组作为内容数据，完整地放到另一协议数据分组内的过程称为封装。

3.1.2

解封装 decapsulation

把封装过的数据分组内的内容数据恢复成原来的协议数据分组的过程称为解封装。

3.1.3

节点 node

实现 IPv4 或 IPv6 的网络设备。

3.1.4

路由器 router

负责转发最终目标地址不是它本身的数据分组的节点。

3.1.5

P路由器 P router

传输网中网络服务提供商所拥有的网络服务提供商内部骨干路由器。

3.1.6

PE路由器　PE router

传输网中网络服务提供商所拥有的提供网络接入功能的边缘路由器。

3.1.7

入口PE路由器　ingress PE router

按照一定封装规则对数据分组进行封装的边缘路由器。

3.1.8

出口PE路由器　egress PE router

对按照一定封装规则封装过的数据分组进行解封装的边缘路由器。

3.1.9

CE路由器　CE router

客户接入网络中的边缘路由器。

3.1.10

链路　link

相邻节点之间通信所依赖的数据链路层连接，例如 Ethernet、PPP 链路、帧中继、ATM 网络。

3.1.11

接口　interface

节点到链路的连接点。

3.1.12

地址簇　address family

IPv4 和 IPv6 分别构成 IPv4 地址簇和 IPv6 地址簇。

3.1.13

地址簇边界路由器AFBR　address family border router

运行 IPv4/v6 双协议栈的路由器，该路由器同时分别连接 IPv4 地址簇网络和 IPv6 地址簇网络。在本标准所定义的网状互联机制中，AFBR 具体实现在 PE 路由器上。

3.1.14

软线　softwire

在某种地址格式的网络中，用于连接两个或多个另一种地址格式网络的隧道。

3.1.15

最大传输单元　maximum transmission unit

某条物理链路所能传输的最大数据单元（以字节为单位）。

3.1.16

路径最大传输单元　path maximum transmission unit

某条传输路径所允许的最大传输单元，传输路径由若干物理链路组成，路径最大传输单元的取值为该路径上所有链路的最大传输单元中的最小值。

3.2　缩略语

下列缩略语适用于本标准。

AFBR	Address Family Border Router	地址簇边界路由器
BSR	Bootstrap Router	自举路由器
BGP	Border Gateway Protocol	边界网关协议
EBGP	External Border Gateway Protocol	外部边界网关协议
DSCP	Differentiated Services Code Point	区分服务代码点
E-IP	External IP	骨干网外部 IP 协议
GRE	Generic Routing Encapsulation	通用路由封装
IBGP	Internal Border Gateway Protocol	内部边界网关协议
I-IP	Internal IP	骨干网内部 IP 协议
IKE	Internet Key Exchange Intenet	密钥交换协议
IP	Internet Protocol	互联网协议
IPSec	IP Security	IP 安全协议
IPv4	Internet Protocol Version 4	互联网协议版本 4
IPv6	Internet Protocol Version 6	互联网协议版本 6
L2TPv3	Layer 2 Tunneling Protocol v3	二层隧道协议（第 3 版）
L3VPN	Layer 3 Virtual Private Network	三层虚拟专用网
LDP	Label Distribution Protocol	标签分发协议
LSP	Label Switch Path	标签交换路径
MP-BGP	Multi-Protocol extension to BGP	边界网关协议多协议扩展
MPLS	Multi-Protocol Label Switch	多协议标签交换
MTU	Maximum Transmission Unit	最大传输单元
MVPN	Mobile Virtual Private Network	移动虚拟专用网
NH	Next Hop	下一跳地址
NLRI	Network Layer Reachability Information	网络层可达信息
PE	Provider Edge	网络边界设备
PIM	Protocol Independent Multicast	协议无关组播
PIM-SM	PIM-Sparse Mode	稀疏模式独立组播
PIM-SSM	PIM-Source Specific Multicast	特定源独立组播
PMTU	Path Maximum Transmission Unit	路径最大传输单元
QoS	Quality of service	业务质量
RPF	Reverse-Path Forwarding	逆向路径转发
RSVP-TE	Resource ReSerVation Protocol-Traffic Engineering	基于流量工程扩展的资源预留协议
TTL	Time To Live	生存时间

4 软线式网状架构概述

4.1 软线的概念及功能

网络运营商骨干网中的路由分为两类，一是“内部路由”，二是“外部路由”。内部路由指的是那些终止于网络内部节点的路由，而外部路由的终点则是在骨干网之外。运营商提供的“网络穿越”服务，

是为那些起始和终止于骨干网之外的数据分组提供传输服务。本标准将分组进入骨干网时到达的路由器称为入口 PE(Provider Edge)路由器，而离开骨干网之前最后一个到达的路由器称为出口 PE 路由器。

当为了提供网络穿越服务时，将外部路由信息在整个骨干网内分发，此时骨干网内的路由器可正确的将分组转发至相应的出口 PE 路由器。此时骨干网的路由将很容易被接入网影响，导致核心路由器开销增加。软线式网状技术框架则通过在骨干网内建立隧道的方式避免引入接入网路由，即骨干网路由器仅维护内部路由，而不需知道外部路由。外部路由信息完全由 PE 路由器维护，当需要穿越骨干网的分组到达入口 PE 路由器时，该路由器根据外部路由信息将分组进行封装，并通过骨干网转发至出口路由器，由出口路由器解封装后继续转发。这里在入口和出口 PE 路由器之间建立的隧道即被称为“软线”。

注：从 IPv4 向 IPv6 过渡的情况来看，互联网可能会出现仅能处理 IPv4 或 IPv6 分组的网络，如 IPv6 骨干网、IPv4 接入网等。其中一种网络的路由器仅能解析 IPv6 分组格式以及处理 IPv6 路由信息，而另一种则是仅能解析 IPv4 分组格式和处理 IPv4 路由信息。很多情况下这两种网络中的任何一种网络需要为另一种网络提供“穿越”服务，为了达到这一目标，需要在其中建立软线，以提供穿越服务。

在软线式网状架构中，场景主要有两种，一是 IPv6 网络通过 IPv4 骨干网互联，另一种是 IPv4 网络通过 IPv6 骨干网互联。在本标准中，将骨干网中所使用的 IP 协议称为 I-IP，将接入网中使用的 IP 协议称为 E-IP。如无特殊规定，骨干网内部路由器仅支持 I-IP 协议，接入网路由器及主机仅支持 E-IP 协议，而骨干网 PE 路由器同时支持 I-IP 和 E-IP。

4.2 IPv6 over IPv4 场景

在本场景中，客户网络运行 IPv6 协议，骨干网运行 IPv4 协议，即 I-IP 为 IPv4，E-IP 为 IPv6。该场景的拓扑如图 1 所示。

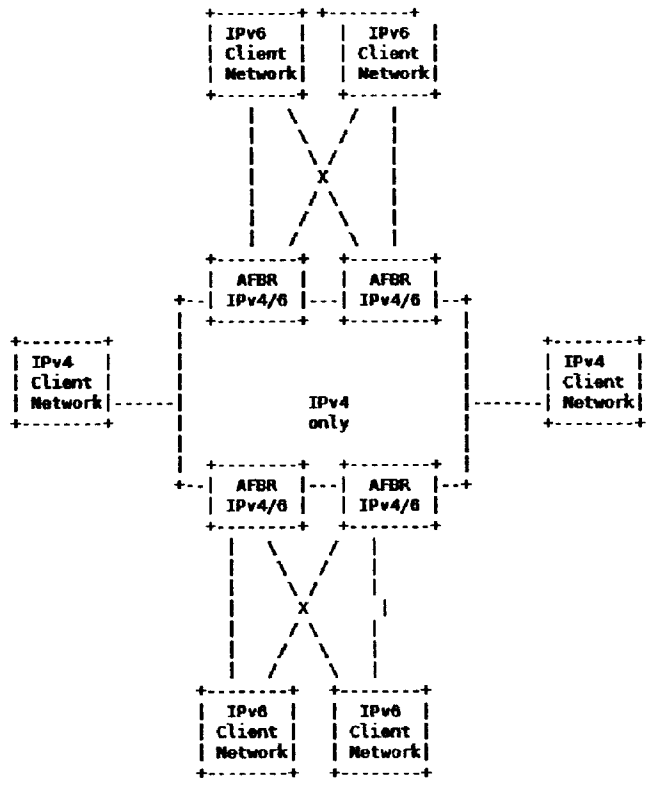

图1 IPv6 over IPv4 网络拓扑

图 1 所示拓扑中，IPv4 传输网可能运行 MPLS 协议。此时，MPLS 可作为解决方案的一部分。

图 1 并没有明确指出在各个客户网络之间是否有内部连接，但是本节允许存在这样的连接，即客户网络之间的转发路径并不必须要通过核心传输网。在这种情况下，要能够适应各种不同的拓扑情况。同时，IPv4 核心传输网可能会对 IPv6 接入网提供多接入服务，即一个客户网可能连接至多个核心网的 PE 路由器，形成一个网状的网络（该场景应该能够支持这种连接方式，但是这样的连接方式并不是必须的）。

注：近几年来，已经有不少基于 IPv4 骨干网的 IPv6 网络互联的方案，其中使用了不少隧道机制，某些使用了手动配置的方法，有些则是基于特殊地址的自动配置。在本标准中，隧道机制的使用是十分自由的，可以使用 MPLS，但并非必须使用。本标准使用的是自动隧道，且无特殊地址要求。

4.3 IPv4 over IPv6 场景

在本节中，客户网络运行 IPv4 地址而骨干网运行 IPv6 地址，即 I-IP 为 IPv6，E-IP 为 IPv4。如图 2 所示。

图 2 所示拓扑中，IPv6 传输网可能运行 MPLS 协议，此时，MPLS 可作为解决方案的一部分。

与前一种场景类似，图 2 并没有明确表示出在各个客户网络之间是否有内部连接，但是本架构假设可能存在这样的连接。也就是说，客户网络之间的转发路径并不必须要通过核心传输网，在这种情况下，方案要能够适应各种不同的拓扑情况。同时，IPv6 核心传输网可能会对 IPv4 接入网提供多接入服务，即一个客户网可能连接至多个核心网的 PE 路由器，形成一个网状的网络。需要指出的是，应该能够支持这种连接方式，但是这样的连接方式并不是必须的。

注：在过去的一段时间内，IPv6 over IPv4 的问题已经得到了很大的关注，但是 IPv4 over IPv6 问题却没有得到足够的研究，然而随着越来越多的服务供应商建立 IPv6 骨干网，并且不希望在骨干网中支持 IPv4，这个问题将变得越来越紧迫。当前服务供应商拥有大量的 IPv4 客户网络以及相关的应用，这些客户将希望其数据能够穿越供应商的 IPv6 骨干网。目前这个问题还没有很好的解决，因为人们总是认为将来的骨干网络是双栈的。

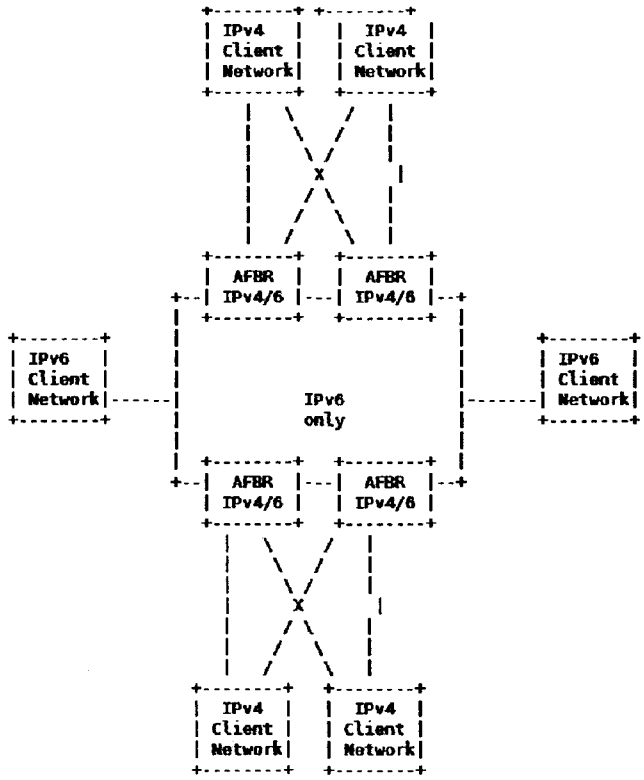

图2 IPv4 over IPv6 网络拓扑

5 软线架构中路由信息分发

AFBR 路由器与所连接的 E-IP 客户网络路由器形成邻居关系，以传输 E-IP 路由信息。

AFBR 使用 BGP 会话在互相之间分发 E-IP 路由信息，这可以通过 IBGP 的网状会话关系来完成，也可以通过使用 BGP 反射器来完成，即 AFBR 与反射器建立一个 IBGP 会话，而不是与其他 AFBR 建立会话。

AFBR 与 AFBR 或反射器之间形成的 BGP 会话是基于 I-IP 地址簇的。也就是说，如果核心传输网仅支持 IPv6，那么用于分发 IPv4 网络路由信息的 IBGP 会话将运行在 IPv6 之上；如果核心传输网仅支持 IPv4，那么用于分发 IPv6 网络路由信息的 IBGP 会话将运行在 IPv4 之上。BGP 会话使用的是核心网的本地路由，BGP 消息并不通过软线或其他任何隧道机制进行转发。

在 BGP 中，一个路由更新会将一个地址前缀（或 NLRI）与一个下一跳（NH）地址关联起来。NLRI 与 NH 都属于某个特定的地址簇，两者可能一样，也可能不同。通常来说，NH 地址的地址簇与该更新的发布路由器地址簇相同。

由于包含 E-IP 地址前缀信息的路由更新是通过基于 I-IP 的 BGP 会话来分发的，并且由于 BGP 消息并不经过隧道，因此 BGP 更新消息将包含 E-IP 地址簇的前缀信息以及 I-IP 地址簇的下一跳地址（当 NLRI 与 NH 地址簇不同的时候，NH 如何编码并非一件显而易见的事情）。对于每一种地址组组合都有着不同的编码过程。

对于 NLRI 是 IPv6 地址，NH 是 IPv4 地址的情况，IETF RFC 4798 定义了 NH 的编码方式；对于 NLRI 是 IPv4 地址，NH 是 IPv6 地址的情况，IETF draft-ietf-idr-v4nlri-v6nh-02 定义了 NH 的编码方式。

若一个 BGP 发布者（speaker）发送某个 E-IP 地址簇的 NLRI 更新消息，并且该消息是通过运行于 I-IP 网络中的 BGP 会话来分发的，并且该 BGP 发布者将其自身宣称为 NH 的话，那么该 BGP 发布者必须（除非由其他策略显式规定）以 I-IP 地址簇指定其 NH 地址，并且该 NH 地址不应被反射器更改。

在某些情况下，BGP 发布者必须在其邻居宣称其有相应能力（capability）的时候才可以发布这样的更新消息，这将导致如下的软线部署问题：若定义了一种表示 E-IP NLRI 对应 I-IP NH 的能力，那么传输网的所有 AFBR 都必须通告该能力。

如果 AFBR 拥有多个 IP 地址，网络管理员通常可随意选择一个作为 BGP 更新消息中的 NH 地址。然而，如果 AFBR 需要通过某种特定的隧道机制所建立的软线接收分组，并且该隧道机制是使用了某个特定 IP 建立的，那么就必须在更新消息中将该 IP 指定为 NH。举例来说，如果使用了 L2TPv3，那么建立 L2TPv3 隧道时所发送的信令中使用的 IP 地址必须作为更新消息中的 NH 地址。

对于骨干网使用 MPLS IPv4 的情况，IETF RFC 4798 描述了一种使用标签方式来分发 IPv6 路由信息的方法，使得出口 PE 路由器为每一个 IPv6 前缀分配一个 MPLS 标签。这种方式也可用于分发 IPv4 路由信息。对于软线式过渡框架来说，使用 MPLS 标签的方法是一种可选的方法。

6 软线架构中的数据转发

6.1 数据转发概述

当入口 AFBR 在其与客户网络相连的接口接收到一个 E-IP 分组时，它将查看该分组的目的地址，在本标准中，与该目的地址所匹配的最佳路由应该是由 BGP 分发的下一跳地址为 I-IP 地址的路由。该 I-IP 地址即为骨干网中相应的出口 AFBR 的地址。

入口 AFBR 必须将该分组通过隧道（即“软线”）转发至出口 AFBR。通过在 E-IP 分组上加上一个 P 路由器可处理的封装头部，使得 P 路由器可将分组转发至出口路由器。然后由出口路由器将载荷（即原始的 E-IP 分组）还原出来，根据其目的 IP 地址继续向客户网转发。

可支持多种隧道机制，某些隧道机制会要求在建立隧道之前在 AFBR 之间有显示的信令过程。

6.2、6.3、6.4 节将分别从软线信令、隧道选择和 MTU 三个方面规定如何进行数据转发。

6.2 软线信令

在客户网之间开始数据传输之前必须先在传输网中建立起 AFBR 间的软线网状网络。在有 N 个双栈路由器的情况下，这将需要有 N^2 个“点到点 IP”或“标签交换路径”隧道。这些隧道可以手动配置，但这将导致高达 $O(N^2)$ 复杂度的配置问题。因此，本标准中不考虑手动点到点隧道配置。

由于传输网提供的是 3 层穿越服务，在本标准中点到点隧道并不是必须的，多点到点隧道也可满足要求。多点到点隧道是指，当分组离开隧道时，无法知道它是从哪里进入该隧道的。这与本地 IP 转发模型一致，即出口路由器无法知道哪个是分组的入口路由器。当然，在本标准的范围外，可能会需要使用点到点隧道，例如在有 QoS 或者安全考虑的情况下。因此，点到点隧道可在本标准中使用，但不是必须的。

无论是点到点还是多点到点的隧道，都可能需要一定的信令过程来在 PE 路由器上建立隧道状态。这个信令过程与具体使用的隧道类型有关，描述如下：如果软线使用了某种特定的隧道机制，并且该隧道机制有其自身的信令方法，那么将使用该信令方法。对于基于 MPLS 的软线来说，可使用 LDP 或 RSVP-TE 作为其信令方法，而基于 IPSec 的软线将使用标准的 IKE 和 IPSec 信令的方法。

基于 GRE 的软线可能不需要信令，这取决于是否使用了多种 GRE 头部选项。GRE 自身并没有什么信令机制，需要另外设计用于软线的信令方法。

对于 L2TPv3 机制来说，它本身有信令机制，并且建立的是点到点隧道。而本标准中软线并不需要点到点隧道，本标准建议使 L2TPv3 工作在多点到点模式下，这就需要另外设计信令方法。

如果使用 IP-IP 隧道或无选项的 GRE 隧道，那么就不需要有信令过程，因为在这种情况下入口路由器封装 IP 分组时需要的惟一信息就是相应的出口路由器的地址，而这一信息已经通过 BGP 分发过了。

当构建 IP 封装包头部的时候，某些域的取值既不是由信令决定，也不是由 BGP 分发的信息决定，而是由入口路由器本地策略决定，比如 TTL 域、DSCP 位等。

在数据传输开始之前必须先建立好所有必须的软线。也就是说，软线必须时刻保持连通状态。从任何一个 AFBR 的角度来看，软线的终点始终是 BGP 消息的 NH 地址。这也就是说，任何一种隧道的信令过程或者在系统启动的时候进行，或者在收到 BGP 更新消息的时候进行。

6.3 隧道选择

将分组通过软线转发而非从本地直接转发的决策是由入口路由器基于某种策略做出的。

本标准建议的策略如下：

— 如果路由选择为将 E-IP 分组从面向核心网的接口向 I-IP 核心网发送的话，将其通过软线转发；

— 如果路由选择为将 E-IP 分组从仅支持 I-IP 分组的接口发送的话，将其通过软线转发；

— 如果路由选择表明 E-IP 分组对应的 BGP 下一跳地址是一个 I-IP 地址的话，将其通过软线转发；

— 如果匹配某分组目的地址的最佳路由是由 BGP 分发的路由，那么将其通过软线转发（也就是说，使用软线转发所有的 BGP 路由的分组）。

更复杂的策略也可被使用，但不在本标准的范围内。

对隧道机制的选择是由入口路由器所配置的策略决定的。

在大多数情况下，策略将会是非常简单的，并对于同一个传输网的所有 AFBR 都相同。比如，“总是使用基于 LDP 的 MPLS”，或者“总是使用 L2TPv3”等。

然而，在某些部署情况中，可能会混合使用路由器，其中某些可能同时支持 GRE 和 L2TPv3，但其他路由器只支持其中一种，因此管理员应该可以为路由器创建一些分类集合，将每一个 AFBR 设为某一类或多类，路由器可互相传递分类信息，这样一来，隧道封装策略可表述为“在 X 分类路由器上使用 L2TPv3 隧道机制，在 Y 分类路由器上使用 GRE 封装机制”。为了能够支持这种策略，AFBR 需要能够通告自身的分类信息。

策略也可能会对部分流量的服务质量做出要求，这可能对该类分组的隧道选择产生影响。本标准允许使用多种不同的隧道机制，而具体软线使用哪种隧道则是一个策略问题，正如 6.2 所讨论的那样。

在许多情况下，策略可能是无条件的，比如“软线总是使用 L2TPv3 隧道”，而在其他一些情况下隧道的选择可能与软线的远程节点有关。比如“与 X 类路由器建立 L2TPv3 隧道，与 Y 类路由器建立 GRE 隧道”。这就要允许网络管理员为路由器创建分类集合，并且将路由器添加至一个或多个分类中。

当已经决定通过软线转发一个分组时，需要进行的主要就是一个加封装和解封装的过程。在大多数情况下，只要知道了对端PE的地址即可完成对分组的封装操作，例如使用的隧道技术是基于LDP的MPLS技术、IP-in-IP封装技术或者无选项头的GRE隧道等。然而，当使用L2TPv3或者带选项头的GRE隧道时，还需要额外的信息来进行封装。

6.4 MTU 考虑

无论软线使用何种隧道机制，都将带来一定的开销，具体体现在对分组的封装上，即封装一个分组将导致其大小增加。这样除了会增加路由器负担之外，还可能引起分组分片的问题。因此，需要采取一定的措施防止封装后的分组在经过核心传输网时发生分片。对于 MTU 的通用见 IETF RFC 4459。

7 软线组播

那些连接在 I-IP 的传输网上的 E-IP 网络可能需要运行 IP 组播应用。实现跨传输网的组播有多种方式，每种方式都有各自的优缺点。大部分方式都与 L3VPN 所定义的方法有一定程度的区别。

本标准将重点关注那些常见的跨服务商边界的组播协议和功能。这主要包括 PIM-SM、PIM-SSM。而双向独立组播协议（BIDIR-PIM）、独立组播协议的自举路由器机制（BSR）以及自动聚合点检测（AutoRP）等技术由于并不常用，所以不对其提供支持。

本标准所提出的方案是“一对一映射”方案，在该方案中每一棵客户网的组播树都会在核心网中有一个扩展，也就是说，对于客户网中的每一棵组播树，在核心网中都会有与之对应的组播树。

一对一映射的方案并没有被 L3VPN 组播所采用，这是由于它需要在核心网路由器中记录大量的状态，状态的数量与客户网的组播树数量成比例。在 VPN 环境中，这是不可接受的，因为状态数量没有上限，并且超出了服务商的控制范围。然而，对于客户网与组播网使用相同地址簇的情况来说，这种一对一方案是一种典型的互联网跨域组播解决方案，如果在这种情况下该方案能有很好的可扩展性，那么当传输网与客户网使用不同地址簇的时候也应该有良好的可扩展性。

当 AFBR 从某个 CE 接收到 E-IP 的 PIM 控制消息时，将其转换成 I-IP 格式，并且向源进行转发。但由于核心网中的路由器并没有指向源的路由，因此 AFBR 需要在 PIM 消息中包含一个“RPF 向量”。

假设某个 AFBR A 从 CE 接收到一个 E-IP 的 PIM 加入/剪枝消息，对应(S,G)或(*,G)树，该 AFBR 需要将此消息从 E-IP 格式转换成 I-IP 格式，然后要将该消息向通往源的下一跳邻居转发。对于(S,G)树来说，树的根节点是源 S，对于(*,G)来说，树的根节点是组 G 的汇聚点（RP）。

值得注意的是这里树的根节点地址是一个 E-IP 地址，由于核心网的 P 路由器没有 E-IP 路由，所以需要在消息中包含一个 RPF 向量，该向量将会以 I-IP 形式指定通往组播树根节点的出口 AFBR 路由器 B 的地址。RPF 向量的引入，可使得 P 路由器在没有 E-IP 路由的情况下仍然可以将组播加入/剪枝消息向树的根节点转发。

为了能将 E-IP 的 PIM 消息转换成一个 I-IP 的 PIM 消息，AFBR A 必须将 S 的地址（对于(S,G)组的情况）或者组播组汇聚点的地址从 E-IP 翻译成 I-IP，而 AFBR B 则必须将其翻译回去。

对于 E-IP 是 IPv4 而 I-IP 是 IPv6 的情况来说，这样的翻译可以用某种算法自动完成。A 可以将 IPv4 的 S 和 G 的地址直接转换成 IPv4 映射的 IPv6 地址，B 可将其翻译回去。具体实施的方式则是由策略来决定的。

当然，这个转换过程并不适用于客户网为 IPv6，核心网是 IPv4 的情况。对于这样的情况，需要在 AFBR 之间进行额外的信令过程。每一个下游的 AFBR 要先通知上游 AFBR 自己需要针对(S,G)的组播隧道，然后上游 AFBR 则为该请求分配一个组播地址 G’，并告知下游 AFBR。然后下游 AFBR 使用 IPv4 PIM 消息来加入(S’,G’)树，其中 S’是上游自治系统边界路由器（ASBR）的 IPv4 地址。(S’,G’)树应该是 SSM 树。

从上可见，这一过程可以同时支持客户网为 IPv4 或 IPv6 并且穿越另一种协议核心网的组播。然而，该过程仅支持客户网组播为 SSM 的情况，因为它无法提供将针对(*,G)树的源剪枝的消息翻译至(S’,G’)情况下的操作。

除了以上的方案以外，对软线组播来说，还可以使用一些类似 MVPN 的方案，即不在骨干网与接入网之间一一对应的建立组播树，而是使用一些类似“广播”的方法来完成数据传递。即，对于组播信令的转发，可在骨干网构建单一双向组播树或者分别以各个 PE 为根构建组播树，使得组播信令可以被所有 PE 收到。另外也可使用 BGP 来传递组播信令。对于数据来说，可以通过一个虚拟的局域网来转发数据，也可在骨干网建立一些静态组播树进行数据转发。

8 域间考虑

本标准仅考虑核心传输网是单个自治系统（AS）的情况，如果传输网包含了多个 AS 的话，就需要使用 AFBR 连接至不同 AS 的软线方案了。在这种情况下，软线的另一端点地址就不是所传输分组对应的 BGP 下一跳地址了。由于之前所描述的方法需要软线另一端点地址为 BGP 下一跳地址，因此就不适用于这里的传输网包含多个 AS 的情况了。

以下列出了一些可用于处理这种情况的方案。

— 不处理这种情况，在每个 AS 边缘都部署 AFBR，这样传输网就不会包含多个 AS 了；

— 使用多跳 EBGP 来使 AFBR 可互相发送 BGP 路由；

— 确保不是 AFBR 的自治系统边界路由器，不修改用于封装的路由中下一跳地址。

在后两种方案中，需要解决 BGP 递归下一跳的处理，并且可能会用到叠加的封装。

举例来说，考虑分组 P 的目的 IP 地址是 D，假设它到达了 AFBR A1，并且与地址 D 匹配的最佳路由下一跳地址是 B1。因此 A1 会将分组封装后发送给 B1。如果 B1 不在 A1 的 AS 内的话，A1 会查找路

由表，并且寻找到B1的下一跳地址，比如B2。如果A1所在AS内部路由器没有到B1的路由的话，A1需要将分组再一次封装，封装的目的地址是B2。

9 安全考虑

9.1 软线安全性分析

在软线式网状架构中，E-IP 数据分组将被封装并且穿越互联网。这些数据分组（软线载荷）有可能需要（也有可能不需要）诸如认证、完整性保证、加密或恢复之类的安全保护措施。然而，数据分组的安全需求与它本身是否穿越软线无关。

因此，在这里本标准所需要关注的安全问题并不是关于E-IP载荷的，而是关于I-IP封装头部。

由于封装头部的作用是确定用来穿越软线的路由，因此它必须以“显式”的方式存在，而没有任何安全需求。从软线的定义及其工作原理可知，AFBR 将主要用于对分组进行封装和解封装的操作，因此本标准对I-IP封装头部的安全性考虑主要体现在对AFBR本身的安全考虑上。对AFBR可能进行的攻击主要可以分为两类，一是对其数据传输进行的攻击，二是对其路由进行的攻击。其中，AFBR 之间使用了扩展的BGP作为路由信息交换协议，因此在这部分并不需要额外的安全考虑，而对数据封装进行的安全考虑将在后续部分进行讨论。

在软线架构中，针对每一个隧道接收端点，会有一个或多个“有效”的传输端点，所谓的有效传输端点就是那些授权可将分组封装发送给接收端点的端点。如果封装头部没有任何安全认证或完整性保证的话，那么就有可能对其发起欺骗攻击，即非授权节点向隧道接收节点发送封装分组，使得接收节点认为这些分组是通过软线转发过来的。重发攻击也可能发生。

然而这样的攻击影响是十分有限的。接收端点会将收到的封装分组解封装，然后按照载荷的目的地址进行进一步转发，由于载荷分组是在互联网上传输的，使用的是全球惟一地址（而并非某种私有地址），因此这种攻击只能使载荷分组发送到指定的地址上。

不过这种攻击可能会导致策略冲突。认证的传输端点可能会遵循一定的策略来限制通过软线的分组，而如果非认证的节点能够伪装成认证端点向接收端点发送封装分组，并使得接收端点认为该分组是合法的，那么就可能违反配置的策略。

另一种可能的攻击是对接收端点的拒绝服务攻击。但是这种攻击无法通过使用加密等手段来防止，事实上，加密认证的引入会使得拒绝服务攻击的后果更加严重。

9.2 非加密技术

如果隧道完全位于单个管理域内，那么从某种程度上来说，可以使用一些非加密的技术来防止欺骗攻击的发生。举例来说，当隧道封装基于IP时：

— 可为接收端点分配特定的IP地址，并且将这些地址告知边界路由器，边界路由器可将来自域外的、目的地址为接收端点的分组过滤掉；

— 为接收端点分配特定的IP地址，并将这个IP地址集合告知边界路由器和所有接收端点。边界路由器可将所有来自域外的且目的地址在此集合中的分组过滤掉，而接收端点可将所有目的地址为自身且源地址不在该集合内的分组过滤掉。

如果使用基于MPLS的封装，边界路由器可丢弃来自域外的MPLS分组，或者丢弃那些顶层标签是隧道接收端点的分组。

这几种技术使用的前提是域内网络自身能够确保没有伪造的分组产生，然而这在很多情况下不一定

成立，并且这些技术也无法应用在跨域的隧道中。

还有一种方法是在封装头部包含一个明文的密码（比如 L2TPv3 的 64 位 cookie）。这种方法在域内还是可行的，因为一般来说攻击者对于那些产生于域内并且不离开本域的分组很难监听到，因此就无法得到这样的密码，穷举一个 64 位的二进制串是一件很困难的事情。这种方法比之前所述的入口检测要容易，而且如果假设成立的话，那么效果应该不比入口检测差。但是与入口检测一样，这种方法对跨域的隧道是无效的。

因此还是有必要考虑使用加密技术来建立隧道以及传输数据。

9.3 加密技术

如果隧道两个端点之间的路径并不足够可靠的话，本标准可以采取如下措施来保证安全：

— 如果隧道的建立使用了某种控制协议（比如用来通知隧道某一个端点另一端的 IP 地址），那么该控制协议必须使用认证机制，并应该在隧道建立的过程中应用。假设隧道是利用 BGP 消息所获得的信息自动建立的，那么 BGP 的基于 MD5 的认证机制（见 IETF RFC2385）就可满足要求；

— 数据传输应该使用 IPSec 来加密。下面本标准将说明 IPSec 应用的方式。

本标准仅考虑 IPSec 与基于 IP 的隧道技术一起使用的情况。应用于 MPLS 隧道的 IPSec 将作为进一步的研究。

当使用 IPSec 时，隧道的起点和终点将被看成是一个安全关联（SA）的两个端点。出于这样的考虑，隧道起点的单个 IP 地址将被作为源 IP 地址，而隧道终点的单个 IP 地址将被作为目的 IP 地址。

封装分组将被看作是从隧道起点发出的，目的地为隧道终点的分组，因此应该使用 IPSec 的传输模式。

封装分组的头部将称为传输分组的外层头部，然后紧接一个 IPSec 头部，然后是具体的载荷。

当在软线中使用 IPSec 时，IPSec 必须要提供认证和完整性保证。因此实现时需要支持非加密的 ESP，而加密的 ESP 也可支持。如果使用了 ESP，那么隧道终点必须确认收到的任何一个分组源地址与 SA 中确定的一致。

由于软线是在路由信息分发时动态建立的，密钥分发必须通过 IKE 自动完成。

与 SA 关联的选择器包含封装头部的源、目的地址和使用的 IP 协议号。

10 软线管理

软线过渡系统从本质上来说是使用隧道连接的路由器。现有的不少技术可用来监控和管理隧道端点的AFBR路由器以及中间路由器，包括软线路径追踪、软线对端节点探测以及故障检测等等。

具体来看，可以使用的技术手段包括：

— AFBR之间BGP/TCP超时；

— 使用ICMP或LSP对特定AFBR的回显检测；

— AFBR间的双向转发检测（BFD）。

可通过定期的基于UDP的请求/响应机制对对端AFBR的可达性进行探测，从而及时地发现软线故障并判断故障的原因和进行排除。