ICS 33.040.40
M 33

中华人民共和国国家标准

GB/T 21645.1—2008

自动交换光网络(ASON)技术要求 第1部分:体系结构与总体要求

Technical requirements for automatically switched optical network—Part 1:Architecture and general requirements

2008-04-10 发布　　2008-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

《自动交换光网络(ASON)技术要求》部分标准的结构及名称如下：

自动交换光网络(ASON)技术要求　第1部分：体系结构与总体要求

自动交换光网络(ASON)技术要求　第2部分：术语和定义

自动交换光网络(ASON)技术要求　第3部分：数据通信网(DCN)技术要求

自动交换光网络(ASON)技术要求　第4部分：信令技术要求

自动交换光网络(ASON)技术要求　第5部分：用户-网络接口(UNI)技术要求

自动交换光网络(ASON)技术要求　第6部分：管理平面技术要求

自动交换光网络(ASON)技术要求　第7部分：自动发现技术要求

本部分是《自动交换光网络(ASON)技术要求》的第1部分。

本部分对应了以下ITU-T建议：

——ITU-T G.8080《自动交换光网络体系结构》(英文版)；

——ITU-T G.807《自动交换传送网的要求》(英文版)；

——ITU-T G.7712《数据通信网结构和规范》(英文版)；

——ITU-T G.7713《分布式呼叫和连接管理》(英文版)；

——ITU-T G.7714《传送实体通用自动发现》(英文版)；

——ITU-T G.7715《ASON路由结构和要求》(英文版)；

——ITU-T G.7718《ASON管理框架》(英文版)。

本部分与以上ITU-T建议的一致性程度为非等效。

本部分在技术内容上与下列的ITU-T建议内容协调一致：

——第4章对应ITU-T G.807第5章和第7.1节，ITU-T G.8080第5.2节和第8章，并增加了网络模型等内容；

——第6章对应ITU-T G.8080第6章；

——第7章对应ITU-T G.8080第7章；

——第8章对应ITU-T G.807第6.2、6.3节，ITU-T G.8080第5.1节，ITU-T G.7713第6.2节，并增加了信令协议要求；

——第9章对应ITU-T G.7715第5、6、7章，ITU-T G.8080第7.5节，并增加了路由协议要求；

——第10章对应ITU-T G.7714第6、7、8、9、10章；

——第12章对应ITU-T G.8080第10章，ITU-T G.7718第9章；

——第13章对应ITU-T G.7718第8章；

——第14章对应ITU-T G.7712第6章；

——第15章对应ITU-T G.8080第11章，并增加了保护恢复类型和倒换准则等要求；

——第16章对应ITU-T G.8080第12章。

此外，本部分还参考了OIF、IETF等国际标准化组织有关自动交换光网络的建议和草案。

本部分的附录A、附录B、附录C为资料性附录。

本部分由中华人民共和国信息产业部提出。

本部分由中国通信标准化协会归口。

本部分起草单位：信息产业部电信研究院、中国电信集团公司。

本部分主要起草人：张国颖，张海懿，荆瑞泉，李芳，李允博，王郁，徐云斌，霍晓莉，王健全。

自动交换光网络(ASON)技术要求 第1部分:体系结构与总体要求

1 范围

本部分规定了自动交换光网络体系结构、控制平面参考结构和基本结构元件、呼叫和连接控制、路由、自动发现和资源管理要求、管理平面和数据通信网要求、命名和地址、保护和恢复、网络可靠性和安全性,以及业务要求等。本部分规定的自动交换光网络要求与其承载的客户层和具体实现技术无关,传送网络的具体技术细节不在本部分范围内。

本部分适用于ITU-T G.803定义的SDH传送网络和ITU-T G.872定义的光传送网络(OTN)。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。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部分,然而,鼓励根据本部分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,其最新版适用于本部分。

YD/T 1078—2000 SDH传送网技术要求 网络保护结构间的互通

YD/T 1289.2 同步数字体系(SDH)传送网网络管理技术要求 第2部分:网元管理系统(EMS)功能

YDN 099—1998 光同步传送网技术体制

ITU-T G.7712 数据通信网的体系结构与规范

ITU-T G.7713 分布式呼叫和连接管理

ITU-T G.7713.1 采用PNNI的DCM信令

ITU-T G.7713.2 采用GMPLS RSVP-TE的DCM信令

ITU-T G.7713.3 采用GMPLS CR-LDP的DCM信令

ITU-T G.7715 ASON路由结构和要求

ITU-T G.7715.1 链路状态路由协议需求

ITU-T G.784 SDH管理

ITU-T G.803 基于同步数字系列(SDH)的传送网体系结构

ITU-T G.805 传送网通用体系结构

ITU-T G.8080 自动交换光网络体系结构

ITU-T G.872 光传送网络的体系结构

ITU-T G.873.1 光传送网(OTN)——线性保护

ITU-T G.873.2 光传送网(OTN)——环保护

ITU-T G.874 光传送网元的管理方面

ITU-T M.3010 电信管理网(TMN)总则

ITU-T M.3100 通用网络信息模型

ITU-T Y.1313 一层虚拟专用网业务和网络结构

OIF-UNI-01.0 用户-网络接口1.0信令规范

OIF-ENNI-SIG-01.0 运营商内部E-NNI信令规范

IETF RFC 4204 GMPLS链路管理协议

IETF RFC 4207　GMPLS LMP 的 SDH 扩展

IETF RFC 4209　GMPLS LMP 的 WDM 光线路系统扩展

3　术语和定义、缩略语

3.1　术语和定义

下列术语和定义适用于本部分。

3.1.1

代理　agent

描述代表一个资源的特定属性和行为的实体。代理允许在各种资源和管理以及控制功能之间的交互。一个资源可以有多个代理。

3.1.2

管理域　administrative domain

管理域表示属于同一个网络层次内部的某一个区域内部的资源，如网络运营者、服务提供商、终端用户等。

3.1.3

自动交换传送网　ASTN

ASTN 是一个由控制平面来执行连接控制、完成配置和连接管理的传送网络。

3.1.4

自动交换光网络　ASON

ASON 是自动交换传送网在面向连接的电路交换网络(ITU-T G.805 规范)上的应用，例如 ITU-T G.803 规范的 SDH 传送网、ITU-T G.872 规范的光传送网(OTN)等。

3.1.5

呼叫　call

两个或者多个用户和一个或者多个域之间的关联，支持通过一个或者多个域的业务实例。在域内部，此关联由包含呼叫状态的网络实体所支持。在用户和网络呼叫控制实体之间以及在网络呼叫控制实体之间，存在多个呼叫段。一条呼叫由多个呼叫段级联而成。

3.1.6

呼叫允许控制　callAC

呼叫允许控制是一个策略功能，由网络中的呼叫发起方调用，同时可能需要呼叫终结方的参与。

3.1.7

呼叫控制　call control

是一个或者多个用户应用之间的信令关系，用于在网络中建立、释放、调整和维护一组连接。

3.1.8

呼叫控制器　call controller

呼叫由呼叫控制器进行控制，有两种类型的呼叫控制器元件，即主叫方呼叫控制器和被叫方呼叫控制器。

3.1.9

呼叫段　call segment

两个呼叫控制实体(如呼叫控制器)之间的关联。每一个呼叫段可以关联 0 个或者多个连接。网络呼叫控制器实体之间的呼叫段可以关联 0 个或者多个支撑它的服务层呼叫。

3.1.10

连接控制器接口　CCI

控制平面和传送平面之间的接口。

3.1.11

客户—服务者 client-server

两个属于不同网络层次的实体之间的关系，通过适配功能实现，如客户层网络的链路连接可以由服务层网络的路径支持。

3.1.12

封闭用户组 closed user group

封闭用户组是进行呼叫时所使用的一种可选用户功能，此用户功能可以使得用户终端设备属于一个或者多个封闭用户组。封闭用户组功能允许属于同一组内的用户终端设备相互之间进行通信，但是禁止同其他组的用户终端设备进行通信。

3.1.13

元件 component

元件是功能实体的抽象描述，用于解释 ASON 体系结构的操作过程。在本部分中，元件不代表具体程序代码的实例。

3.1.14

连接 connection

连接是链路连接和子网连接的串联，可允许在一个子网的输入和输出点之间传送用户信息。

3.1.15

连接允许控制 connection admission control

连接允许控制用于确定是否有足够的资源来接纳一个连接(或者在呼叫过程中重新协商资源)。

3.1.16

连接控制器 connection controller

连接控制器是 ASON 控制平面中的元件。连接控制器负责协调链路资源管理器、路由控制器以及对等和从属的连接控制器，以管理和监测连接的建立、释放和参数调整等操作。

3.1.17

控制域 control domain

控制域是一种或者多种用于分布式应用的特殊元件的集合，并且封装和隐藏了这些应用的细节。控制域中的实体是控制平面中的元件的集合。

3.1.18

控制平面 control plane

控制平面完成呼叫控制和连接控制功能，通过信令来建立和释放连接，并且在故障情况下参与完成连接的保护恢复功能。控制平面还实现用于支撑呼叫和连接控制的其他功能，例如路由信息的发布。

3.1.19

业务等级 CoS

用于呼叫和连接的策略属性。CoS 指定服务的类型，满足客户的 SLA 需求，如可用性、中断周期、误码秒等。对呼叫来说，CoS 是端到端透明的，在不同的区域之间不会改变；对连接来说，CoS 在同一个区域内部唯一，在区域之间可以改变。CoS 中可包括服务类型的列表信息。

3.1.20

连接点 CP

在本部分中，一个连接点代表一个适配功能的北向输入端口。

3.1.21

回溯 crank-back

当连接建立请求未成功并从失败点返回建立失败的信息时，回溯机制允许发起新的连接建立请求，尝试重新建立连接以避免资源的阻塞。回溯机制也可以用于连接的恢复机制。

3.1.22

连接终端点 CTP

一个连接终端点代表 CP 的信号状态。

3.1.23

分集 diversity

分集指在一对输入和输出端口之间，配置使用不同的网络资源（链路和节点）的多个并行连接。根据链路、节点或管理策略等因素，分集可以有不同的级别。若两个连接除了入口和出口节点外，不共享任何节点，称之为节点不相关分集。如果两个连接的通道不共享任何链路，称之为链路不相关分集。

3.1.24

域 domain

表示用于特定目的的一系列实体的集合。

3.1.25

外部网络—网络接口 E-NNI

在属于不同控制域的控制平面元件之间的双向信令接口。

3.1.26

显式路由 explicit route

显式路由最初是为 MPLS 流量工程功能定义的，通过基于约束的路由算法获得，在请求信息中表示为经过路由上的一系列抽象节点的列表。显式路由又分为严格显式路由和松散显式路由两种。

3.1.27

联邦 federation

为了连接管理而形成的一些域的共同体，通过连接控制器之间的协作关系来表示。

3.1.28

服务等级 GoS

用于呼叫或连接的策略属性。GoS 是一些网络设计变量，可用于在指定条件下提供对一组资源的测量手段。对呼叫来说，GoS 是端到端透明的，在不同的区域之间不会改变；对连接来说，GoS 在同一个区域内部唯一，在区域之间可以改变。GoS 变量可以为路由分集信息、一系列网络控制器名称的列表等。

3.1.29

硬重路由 hard rerouting

硬重路由服务提供了呼叫连接失效时的恢复机制，并能响应失效事件。对于一个已激活硬重路由的呼叫连接，源节点阻止呼叫释放，并试图在重路由域边界建立一个到宿节点的替代连接段，即重路由连接。在重路由域边界的宿节点同样阻止呼叫连接的释放，并等待重路由域边界的源节点建立一个重路由连接。

3.1.30

接口 interface

在本部分中，接口表示 ASON 控制元件之间的逻辑关系，并通过这些元件之间的信息流来定义。这种关系允许元件的各种分布，以支持不同的设备实现和网络结构。

3.1.31

内部网络—网络接口 I-NNI

在属于一个或多个有信任关系的域的控制平面元件之间的双向信令接口。

3.1.32

层网络 layer network

层网络是一种拓扑元件，包括传送实体和传送处理功能，完成特征信息的产生、传送和终结。

3.1.33

链路 link

链路是一种拓扑元件，描述了子网和接入组同其他的子网或者接入组之间的关系。

3.1.34

链路聚合 link aggregation

可以把一些路由目的相同的链路连接聚合成一些逻辑链路，这种聚合可以基于链路代价、时延、链路质量或多样性等参数。聚合后的逻辑链路可以隐藏链路连接的细节，这些细节对一些网络层功能（如路径选择）是不必要的。

3.1.35

链路捆束 link bundle

网络中多个属性相同的链路可以捆绑在一起，作为一个链路组，在链路维护和广播时这一组链路可以通过单个链路状态广播消息公布出去，从而显著减少网络中的广播信息。

3.1.36

链路连接 link connection

在一条链路的端口之间传送信息的传送实体。

3.1.37

链路资源管理器 link resource manager

链路资源管理器一种控制平面元件，负责管理 SNPP 链路，包括 SNP 链路连接的指配和去指配，提供拓扑和状态信息。链路资源管理器向路由控制器提供所有相关的 SNPP 链路信息，同时将所控制的链路资源的任何状态改变通知路由控制器。

3.1.38

松散路由 loose route

松散路由为一系列松散抽象节点的列表，在松散抽象节点之间的路径可以穿越其他的网络节点。

3.1.39

管理平面 management plane

管理平面执行传送平面、控制平面以及整个系统的管理功能，它同时提供这些平面之间的协同操作。管理平面执行的功能包括：性能管理、故障管理、配置管理、计费管理、安全管理。

3.1.40

多归属 multi-homing

在一个终端点和一个或多个传送网之间的多条链路，可被用于进行负载均衡或采用不同路由的保护。

3.1.41

名称 name

名称是一个与位置无关的字符串，可以用于源端或者宿端的标识。如果宿端名称是一个字符串，当宿端的位置发生变化时其名称应该保持不变。

3.1.42

网络呼叫控制器 network call controller

网络呼叫控制器提供两种角色，一种支持主叫方实体，另一种支持被叫方实体。

3.1.43

编号 numbered

编号方式通过 IP 地址对端口进行标识，每一个链路由其终端的 IP 地址进行标识。

3.1.44

永久连接 PC

PC是一种由管理系统配置并维护的连接类型。

3.1.45

策略 policy

是指应用在系统边界接口的一系列原则，可过滤消息使之成为一个允许的消息集。策略由“端口控制器”元件来执行。

3.1.46

端口控制器 port controller

执行应用于系统的一系列原则的元件。

3.1.47

协议控制器 protocol controller

协议控制器将控制元件的抽象接口参数映射成消息，并通过接口协议进行传输。协议控制器是策略端口的一个子类。

3.1.48

终端和适配执行器 termination and adaption performer

终端和适配执行器位于提供适配和终端功能的设备上。它提供链路连接的控制平面视图，同时隐藏了适配和终端控制的所有硬件和技术上的细节。

3.1.49

路由区 RA

路由区定义为一组子网、连接这些子网的SNPP链路以及描述路由区边界上的SNPP链路端点的SNPP。路由区可以进一步划分为通过SNPP链路互联的更小的路由区。进一步划分的限制是，在一个路由区内仅包含一个子网。

3.1.50

路由 route

是一个SNP名称、SNPP名称、路由区名称和/或传送资源名称的序列，用于控制平面创建网络连接。

3.1.51

路由控制器 routing controller

是完成下列功能的元件：

——响应来自连接控制器的路由信息请求，这些信息可以是端到端的(如源路由)，也可以是基于下一跳的。

——响应来自网络管理目的的拓扑信息请求。

3.1.52

路由层次 routing level

路由层次是一个路由区与包含它的路由区，或与被它包含的路由区之间的关系。路由区的包含等级形成了路由层次。

3.1.53

交换连接 SC

SC是一种由终端用户请求而建立的连接类型，即通过控制平面信令单元之间的信令消息动态交换，在连接终端点之间建立的连接。

3.1.54

服务级别协议 SLA

服务级别协议是一个双方之间的合同，如一个服务提供商和一个客户之间。它定义了提供给客户的服务和服务的等级，还描述了服务的保证以及服务劣化降级或失效情况下所需的赔偿。

3.1.55

子网 subnetwork

用于对特征信息进行路由的拓扑元件。在本部分中，子网以子网点为边界。

3.1.56

子网连接 SNC

子网连接是指在同一子网边界处的两个或多个(在广播连接时)子网点之间的一个动态关系。

3.1.57

子网点 SNP

SNP 是对一个实际或潜在的 CP(或 CTP)，或者一个实际或潜在的 TCP(或 TTP)的抽象描述。几个 SNP(在不同的子网分割中)可代表同一个 TCP 或 CP。

3.1.58

子网点池 SNPP

是指出于路由目的而组合在一起的一组子网点。一个子网点池与链路终端有密切关系。

3.1.59

子网点池链路 SNPP Link

位于不同的子网的 SNPP 之间的关联关系。

3.1.60

软重路由 soft rerouting

软重路由机制是一种出于管理目的(如路由优化，网络维护，工程规划工作)的呼叫重路由机制。当一个软重路由操作被激活(通常由管理平面发起请求)，重路由元件建立一个到指定元件位置的重路由连接，一旦该连接被建立，重路由元件使用这个连接并删除初始的连接，这称为“先建后拆”(make-before-break)。

3.1.61

软永久连接 SPC

SPC 是一个用户到用户的连接，其中端到端连接中的用户到网络部分是通过网络管理系统建立的一个永久连接(PC)，而端到端连接的网络部分是通过控制平面建立的一个交换连接。在连接的网络部分，连接建立的请求是由管理平面发起，而由控制平面完成连接建立。

3.1.62

共享风险组 SRG

共享相同的风险的一组资源，一个资源的故障同时也会引起组中所有资源的故障。

3.1.63

共享风险链路组 SRLG

是指共享相同风险的一组链路，一条链路可以分别属于多个不同的 SRLG。

3.1.64

严格路由 strict route

严格路由为一系列严格网络资源(例如节点、SNPP 链路、SNP 链路连接、时隙)的列表，在严格抽象节点之间的路径不能够穿越其他的网络节点。

3.1.65

终端连接点 TCP

在本部分中，一个终端连接点代表一个路径终端功能的输出或者一个路径终端宿功能的输入。

3.1.66

传送网络分配地址 TNA

TNA 地址用于标识 UNI 连接终端，由传送网络分配。每一个 TNA 地址是全局唯一的地址，地址类型可以是 IPv4、IPv6 或者 NSAP。

3.1.67

路径 trail

路径是一个传送实体，包括一对相互关联的单向路径，能够同时向两个相反的方向传送信息。单向路径负责在一个路径终端源的输入端和一个路径终端宿的输出端之间传送信息，同时监视被传送信息的完整性。单向路径由路径终端功能和一个网络连接组成。

3.1.68

传送平面 transport plane

传送平面提供两点之间的双向或单向的用户信息传送，也可以提供控制和网络管理信息的传送。传送平面采用分层结构，等同于 ITU-T G.805 中定义的传送网。

路径终端点 TTP

路径终端点表示 TCP 点的信号状态。

3.1.69

用户网络接口 UNI

位于业务请求者和业务提供者的控制平面元件之间的双向信令接口。

3.1.70

无编号 unnumbered

无编号方式不为每一个链路或者端口分配 IP 地址，而是分配一个接口标识，通过节点 IP 地址以及接口标识的组合来唯一地标识端口或者链路。

3.1.71

虚拟专用网络 VPN

VPN 是虚拟指定的一系列传输资源，支持封闭用户组，可以在多个用户之间共享传送链路。

3.2 缩略语

下列缩略语适用于本部分。

AD	Administrative Domain	管理域
AGC	Access Group Container	接入组容器
AIS	Alarm Indication Signal	告警指示信号
AP	Access Point	接入点
ASON	Automatically Switched Optical Network	自动交换光网络
ASTN	Automatically Switched Transport Network	自动交换传送网
ATM	Asynchronous Transfer Mode	异步转移模式
BER	Bit Error Rate	比特差错率
BoD	Bandwidth on Demand	带宽按需分配
CAC	Connection Admission Control	连接允许控制
CallAC	Call Admission Control	呼叫允许控制
CallC	Call Controller	呼叫控制器
CC	Connection Controller	连接控制器

CCC	Calling/Called Party Call Controller	主叫方和被叫方呼叫控制器
CCI	Connection Controller Interface	连接控制器接口
CoS	Class of Service	业务等级
CP	Connection Point	连接点
CR-LDP	Constraint-based Routed Label Distribution Protocol	基于约束路由的标签分发协议
CTP	Connection Termination Point	连接终端点
CUG	Closed User Group	封闭用户组
DA	Discovery Agent	发现代理
DCC	Data Communications Channel	数据通信通路
DCF	Data Communications Function	数据通信功能
DCN	Data Communications Network	数据通信网络
DT	Discovery Trigger	发现触发
ECC	Embedded Control Channel	嵌入式控制通路
EMS	Element Management System	网元管理系统
E-NNI	External Network-Network Interface(reference point)	外部网络-网络接口(参考点)
FIS	Fault Indication Signal	故障指示信号
GMPLS	Generalized Multi-Protocol Label Switching	通用多协议标记交换
GoS	Grade of Service	服务等级
ID	Identifier	标识符
I-NNI	Internal Network-Network Interface(reference point)	内部网络-网络接口(参考点)
IPCC	IP Control Channel	IP 控制通路
IS-IS	Intermediate System-Intermediate System	中间系统—中间系统路由协议
L2TP	Layer 2 Tunnel Protocol	二层隧道协议
LAD	Layer Adjacency Discovery	层邻接发现
LAN	Local Area Network	局域网
LAPD	Link-Access Procedure D-Channel	D 通路链路接入规程
LC	Link Connection	链路连接
LOF	Loss of Frame	帧丢失
LOS	Loss of Signal	信号丢失
LRM	Link Resource Manager	链路资源管理器
MCN	Management Communication Network	管理通信网络
MI	Management information	管理信息
MO	Managed Object	管理对象
MP	Management plane	管理平面
MP	Management point	管理点
MPLS	Multi-Protocol Label Switching	多协议标记交换
MS	Multiplex Section	复用段
MSP	Multiplex Section Protection	复用段保护
NC	Network Connection	网络连接
NCC	Network Call Controller	网络呼叫控制器
NE	Network Element	网络单元
NEF	Network Element Function	网络单元功能
NMS	Network Management System	网络管理系统

NMI	Network Management Interface	网络管理接口
NNI	Network-to-Network interface	网络—网络接口
NSP	Network Service Provider	网络服务提供商
OAM	Operation, Administration and Maintenance	操作、管理和维护
OS	Operations System	操作系统
OSI	Open System Interconnection	开放系统互联
OTN	Optical Transport Network	光传送网络
OVPN	Optical Virtual Private Network	光虚拟专用网络
PBS	Provided Bandwidth Service	指配带宽业务
PC	Permanent Connection	永久连接
PC	Protocol Controller	协议控制器
PC	Port Controller	端口控制器
PDP	Policy Decision Point	策略决定点
PEP	Policy Enforcement Point	策略执行点
PNNI	Private Network-Network Interface	专用网络—网络接口
PPP	Point to Point Protocol	点到点协议
QoS	Quality of Service	服务质量
RA	Routing Area	路由区
RC	Routing Controller	路由控制器
RCD	Routing Control Domain	路由控制域
RDB	Routing Information Database	路由信息数据库
RP	Route Performer	路由执行器
RSVP—TE	Resource Reservation Protocol—Traffic Engineering	资源预留协议——流量工程
SAN	Storage Area Network	存储区域网络
SC	Switched Connection	交换连接
SCN	Signalling Communication Network	信令通信网络
SD	Signal Degraded	信号劣化
SDH	Synchronous Digital Hierarchy	同步数字体系
SF	Signal Failure	信号失效
SLA	Service Level Agreement	服务等级协议
SNC	Subnetwork Connection	子网连接
SNCP	Subnetwork Connection Protection	子网连接保护
SNP	Subnetwork Point	子网点
SNPP	Subnetwork Point Pool	子网点池
SNTP	Sub-network Termination Point	子网终端点
SPC	Soft Permanent Connection	软永久连接
SRLG	Shared Risk Link Group	共享风险链路组
STM	Synchronous Transport Module	同步传送模块
TAP	Termination and Adaptation Performer	终端和适配执行器
TCP	Termination Connection Point	终端连接点
TE	Traffic Engineering	流量工程
TTP	Trail Termination Point	路径终端点
UNI	User-Network Interface (reference point)	用户—网络接口(参考点)

UNI-C	User-Network Interface-Client	UNI 客户侧
UNI-N	User-Network Interface-Network	UNI 网络侧
UML	Unified Modelling Language	通用建模语言
VC	Virtual Container	虚容器
VCAT	Virtual Concatenation	虚级联
VPN	Virtual Private Network	虚拟专用网
WAN	Wide Area Network	广域网
WDM	Wavelength-Division Multiplexing	波分复用
WTR	Wait Time to Restore	恢复等待时间

4 自动交换光网络的基本结构

4.1 自动交换光网络的功能结构

自动交换光网络(ASON)是符合 ITU-T G.8080 框架要求的,通过控制平面来完成自动交换和连接控制的光传送网,它是以光纤为物理传输媒质,SDH 和 OTN 等光传输系统构成的具有智能的光传送网。ASON 网络具有呼叫和连接控制、路由和自动发现等功能,以实现智能化网络控制。

自动交换光网络结构根据功能可以分为三个平面:传送平面、控制平面和管理平面,此外还包括用于控制和管理通信的数据通信网。

a) 控制平面

ASON 的控制平面由提供路由和信令等特定功能的一组控制元件组成,并由一个信令网络支撑。控制平面元件之间的互操作性以及元件之间通信需要的信息流可通过接口获得。

控制平面的主要功能包括:通过信令支持建立、拆除和维护端到端连接的能力,通过选路为连接选择合适的路由;网络发生故障时,执行保护和恢复功能;自动发现邻接关系和链路信息,发布链路状态(例如可用容量以及故障等)信息以支持连接建立、拆除和恢复;提供适当的命名和地址机制等。

ASON 控制平面应该是可靠的、可扩展的和高效的,适用于不同传送技术(例如 SDH 和 OTN)、不同业务需求和不同的功能分布。控制平面结构不应限制连接控制的实现方式,如集中的或全分布的。

b) 传送平面

传送平面提供从一个端点到另一个端点的双向或单向信息传送,监测连接状态(如故障和信号质量),并提供给控制平面。传送平面还可以提供控制信息和网络管理信息的传送。

ASON 网络按照 ITU-T G.805 建议进行分层,层网络之间是客户和服务者关系。传送平面应支持 ITU-T G.803 定义的基于 TDM 的 SDH 网络和 ITU-T G.872 定义的 OTN 网络。传送平面完成光信号传输、复用、配置保护倒换和交叉连接等功能,并确保所传光信号的可靠性。

传送平面的技术细节不在本部分范围内。

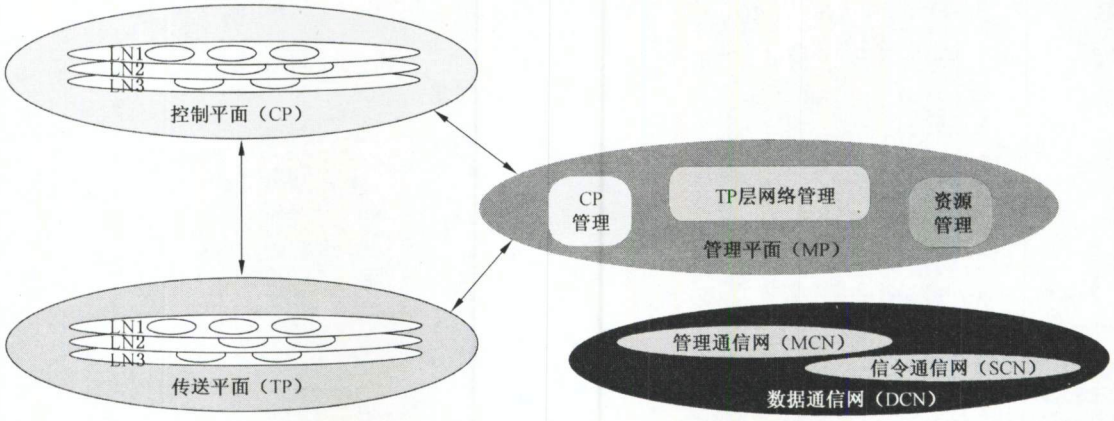
c) 管理平面

管理平面实施对传送平面、控制平面以及系统的管理功能,它也确保所有平面之间的协同工作,管理平面提供 ITU-T M.3010 规定的管理功能,包括性能管理、故障管理、配置管理、计费管理和安全管理。

d) 数据通信网

数据通信网(DCN)为管理平面、控制平面、传送平面内部以及三者之间的管理信息和控制信息通信提供传送通路。DCN 是一种支持第一层(物理层)、第二层(数据链路层)和第三层(网络层)功能的网络,主要承载管理信息和分布式信令消息。

图1给出了ASON控制平面、管理平面、传送平面以及数据通信网之间的互操作性的示意。



LNx：层网络x

图1 ASON体系结构各组成部分之间的关系

在ASON网络结构中引入控制平面具有以下优势：

a) 支持快速的业务配置；

b) 支持流量工程，允许网络资源的动态分配；

c) 采用专门的控制平面协议，可适用于各种不同的传送技术；

d) 根据实时的传送网络状态实现恢复功能；

e) 支持多厂家环境下的连接控制；

f) 可引入新的补充业务（例如，封闭用户组和虚拟专用网）；

g) 减少运营商开发和维护支持新技术的运行支撑系统软件的需求。

4.2 控制、传送和管理平面的交互

控制平面、管理平面和传送平面是独立的，同时三个平面之间存在交互。

a) 管理平面—传送平面交互

管理平面负责传送平面中网络资源的管理。管理平面可以划分管理平面和控制平面分别使用的网络资源。传送平面监控和检测连接的失效和质量劣化，并向管理平面提供相关的故障信息。管理平面失效不应影响传送平面的正常操作。

管理平面通过操作一个管理信息模型来实现对底层传送资源的管理。信息模型表示了传送资源的管理视图，并通过管理信息（MI）接口与传送资源进行交互。

b) 控制平面—传送平面交互

控制平面通过与传送平面交互来实施配置交换矩阵和端口等操作。传送平面应监测信号失效和信号质量劣化，并向控制平面提供信号失效和信号劣化告警，以便控制平面执行故障定位和网络恢复等功能。

与物理传送资源有密切关系的控制平面元件包括：连接控制器（CC）（见7.4.1）以及终端和适配执行器（TAP）（见7.4.7）。连接控制器提供一个用于控制传送平面的连接功能的接口，可以采用协议实现连接控制器与连接功能之间的通信。终端和适配执行器可以提供链路连接的控制平面视图，它隐藏了与硬件之间交互的细节。

c) 管理平面—控制平面交互

控制平面与传送平面一样是网络中可管理的实体。控制平面应为管理平面的请求提供服务，例如端到端连接指配（如SPC连接）和控制平面信息查询。管理平面可以配置控制平面的路由、信令和发现等控制参数。控制平面应向管理平面报告控制平面故障、通知等信息，管理平面根据需要可以拆除由控制平面建立的连接。

管理平面通过信息模型与控制元件交互。信息模型表示了控制元件的管理视图，信息模型通过控制元件的监视和配置接口与这些元件交互。控制平面的每个元件提供一组特殊接口，用于监视控制元件操作，进行策略控制和完成内部行为。这些接口与传送功能模型的 MI 接口相同，允许元件向管理系统提供视图，并被管理系统配置。

图 2 给出了控制平面、管理平面与传送资源之间的交互关系。最下面的部分是物理传送资源，表示真实的物理设备，这些物理资源在 ITU-T G.805 中被描述为原子功能。管理对象(MO)表示设备的外部管理视图，它通过设备内部的管理信息(MI)参考点来实现与设备功能模块之间的交互。

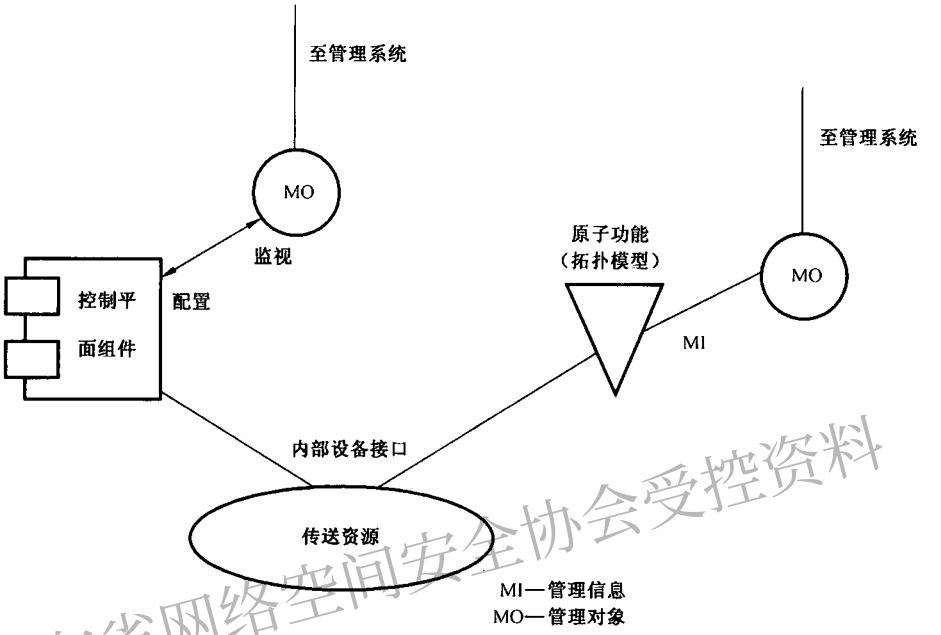


图 2　管理和传送平面与传送资源的交互

从控制平面视图看，控制平面元件直接对传送资源进行操作，因此控制平面的操作与管理平面相独立。同样，管理平面的操作与控制平面独立。虽然呈现给控制平面的信息与呈现给管理平面的信息相似，但控制平面信息与 MI 信息不相同。控制平面只需要部分而不是全部的管理信息，因此控制平面得到的信息是 MI 信息的子集。

5　ASON 控制域、参考点和网络模型

5.1　ASON 控制域

ASON 控制平面要根据各种商业和运营的考虑，以及各种类型的传送网络环境来进行部署。因此，ASON 体系结构支持按照管理、策略、传送网络的内在差异等因素，将网络分割成不同的域。ITU-T G.805 定义了管理域(Administrative Domain)和 Internet 管理域(如自治系统)的概念。这个概念被应用于 ASON 控制平面，形成控制域(Control Domain)，用来区分不同行政上或者管理上的职责、信任关系、地址方案、基础设施能力、生存性技术、控制功能的分布等。

ASON 控制域由一组具有同种目的的控制元件组成。控制域可以隐藏控制元件实现的细节，并通过控制域接口来描述这些控制元件。ASON 控制域概念可被应用到路由、信令、保护和恢复等方面，以形成独立的控制功能域。例如一个路由(控制)域由一组路由控制元件组成，一个重路由域由一组连接控制器和网络呼叫控制器组成，这些元件负责对经过域的呼叫或连接进行重路由或恢复。

ASON 控制域内部以及控制域之间的互连通过参考点来描述。控制域根据运营者策略来建立，域间的参考点是一个服务层的服务分界点(也就是提供呼叫控制的点)。通过这些参考点交换的信息由控制元件之间的多个抽象接口描述。物理接口是通过把一个或者多个抽象的元件接口映射到一个协议来

实现的。多个抽象接口可以复用到一个物理接口上。

客户和服务提供商控制域之间的参考点是用户—网络接口(UNI),表示了一个客户到服务提供商的服务分界点。ASON 控制域之间的参考点为外部网络接口(E-NNI),表示了支持多控制域连接建立的服务分界点。在一个控制域内部的参考点为内部网络接口(I-NNI),表示支持控制域内部连接建立的连接点。控制平面还可被进一步划分来实现资源隔离,例如光虚拟专用网络(OVPN)。ASON 控制域和参考点的示例如图 3 所示。

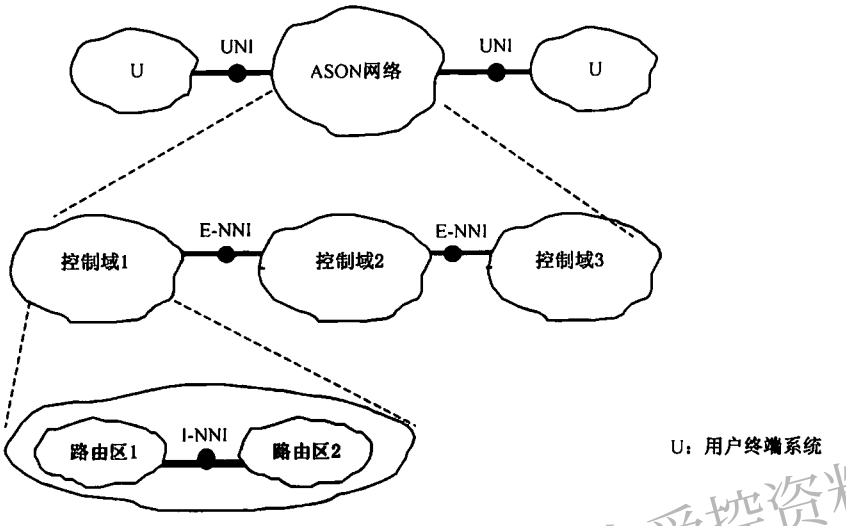


图 3　ASON 控制域和参考点

5.2　参考点与逻辑接口

ASON 网络中定义了多种参考点(即逻辑接口),控制平面通过参考点进行信令、路由和发现等控制信息的交换。参考点表示一组服务,由一对或者多对控制元件的接口实现,如图 4 所示。控制元件的接口独立于参考点,即一个控制元件接口提供多个参考点,同时一个参考点也可由多个接口来支持。

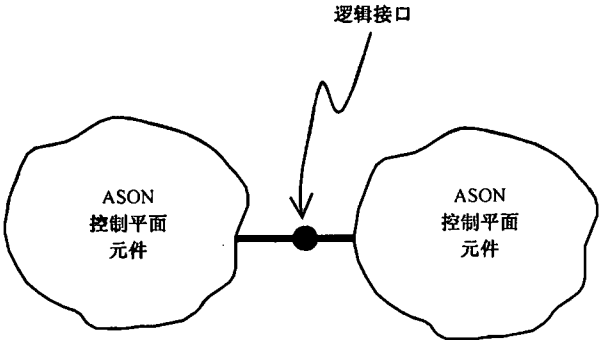


图 4　自动交换光网络的逻辑接口(参考点)

ASON 网络的参考点包括 UNI、I-NNI 和 E-NNI。下面描述这些参考点实现的具体功能以及传递的信息要求。

5.2.1　参考点功能

5.2.1.1　UNI

UNI 是业务请求者和业务提供者的控制平面实体间的双向信令接口,用户侧称为 UNI-C(客户),网络侧称为 UNI-N。UNI 应支持以下功能:

a)　呼叫控制;

b)　资源发现;

c)　连接控制;

d) 连接选择。

需要说明的是，UNI 接口不具有路由功能。另外在以上功能的基础上，UNI 接口可增加呼叫的安全和认证、增强的目录服务等其他功能。

5.2.1.2 **I-NNI**

I-NNI 是控制平面内，属于同一控制域或多个具有信任关系的控制实体之间的双向信令接口。I-NNI 应支持以下功能：

a) 资源发现；

b) 连接控制；

c) 连接选择；

d) 连接路由。

5.2.1.3 **E-NNI**

E-NNI 是控制平面内，属于不同控制域，无信任关系或有一定信任关系的控制实体之间的双向信令接口。采用 E-NNI 接口可以将 ASON 划分为多个控制域，每个控制域能够独立管理，并且能跨过多个控制域建立端到端连接。E-NNI 应支持以下功能：

a) 呼叫控制；

b) 资源发现；

c) 连接控制；

d) 连接选择；

e) 连接路由。

另外在以上功能的基础上，E-NNI 接口可增加呼叫的安全和认证、增强的目录服务等其他功能。

E-NNI 接口根据其信任关系，可以进一步分为运营商内部的 E-NNI 和运营商之间的 E-NNI。在一个运营商的控制域内部某些情况下宜采用运营商内部 E-NNI 划分为多个子控制域，例如：

- 使用了不同设备商产品的子网；
- 不同子网的互联由不同的业务部门管理；
- 为了降低交换的拓扑状态信息量等。

当 ENNI 参考点位于一个 VPN 客户域和一个服务提供者域的 VPN 之间时，可能需要支持补充业务，例如：

- VPN 用户认证和授权；
- VPN 用户策略管理，包括连接限制；
- 在 VPN 用户之间透明传送控制信息；
- 在客户路由域中进行 VPN 共享。

5.2.2 **接口传递的信息要求**

接口表示了 ASON 控制平面元件之间的逻辑关系，并由这些元件之间的信息流来定义。穿过这些逻辑接口的信息流包括以下内容：

a) 终端节点的名字和地址；

b) 可达性和概括的网络地址信息；

c) 拓扑和路由信息；

d) 认证和连接允许控制信息；

e) 连接业务消息；

f) 网络资源控制信息(仅适于 I-NNI)。

穿过 UNI 参考点的信息流应至少支持以下信息单元：

a) 终端节点的名字和地址；

b) 认证和连接允许控制信息；

c） 连接业务消息。

穿过 I-NNI 参考点的信息流应至少支持下列信息单元：

a） 拓扑和路由信息；

b） 连接业务消息；

c） 控制网络资源所需的信息。

穿过 E-NNI 参考点的信息流应至少支持以下信息单元：

a） 可达性和概括的网络地址信息；

b） 认证和连接允许控制信息；

c） 连接业务消息。

经过参考点的信息流由控制平面元件产生或终结，多个流可以在不同的物理位置终结。信息流可以经过不同的参考点序列，如图 5 所示。

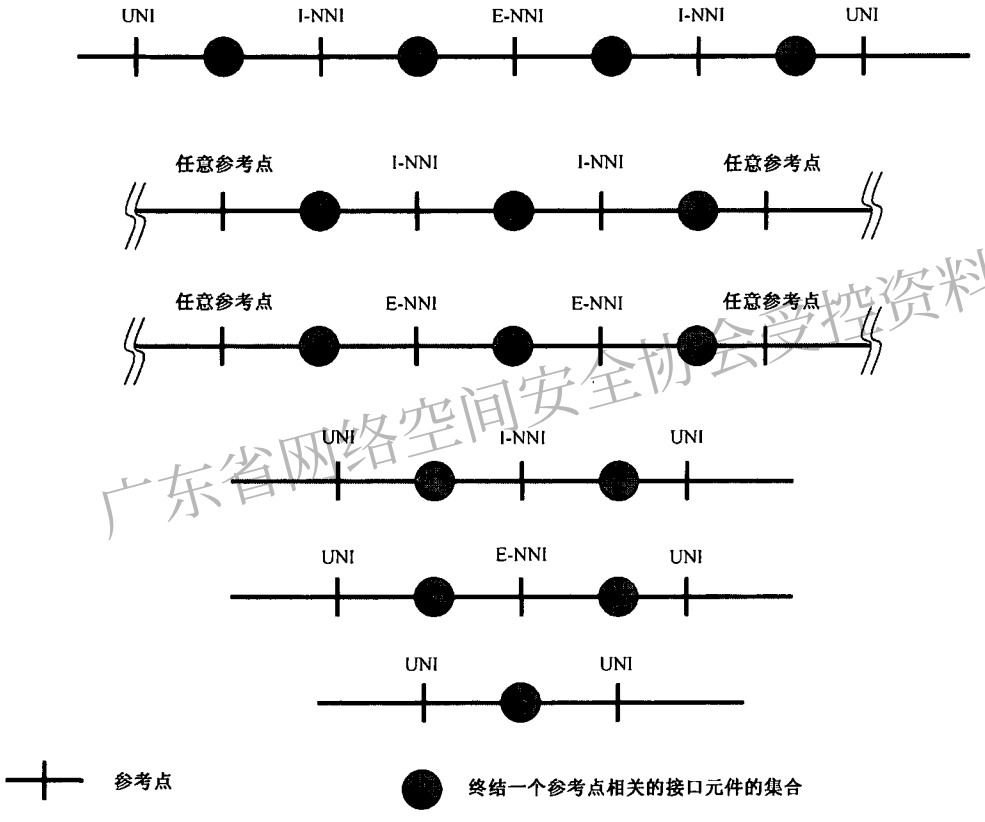


图 5 信息流穿过的参考点序列

5.2.3 接口之间的信任关系

考虑到安全和访问控制，不同类型的接口在信任关系方面不同。此信任关系不是简单的“有”和“无”两种状态，而是根据运营商的商业需要和业务需要，适当地限制接口上交换信息的数量和类型。一般的，如果两个网络处于同一控制域，可以认为它们具有完全的信任关系，控制信息可以不受约束地在两个网络之间交换；否则控制信息将受到管理策略的限制，限制其数量和类型。

I-NNI 具有完全信任关系，通过该参考点信息交换是没有限制的。不同运营商之间的 E-NNI 接口、客户与运营商光网络之间的 UNI 接口不具备完全信任关系。但 E-NNI、UNI 各自的信任度不同。E-NNI 的信任度与其是否在运营商内有关，一般的，运营商内 E-NNI 的信任度会比运营商间 E-NNI 的信任度高。

可以在支持参考点的接口上应用策略，来限制通过接口的信息，具体的策略依赖于不同参考点和所支持的功能。例如在 UNI 和 E-NNI，可以将策略应用于呼叫和连接控制；在 I-NNI 和 E-NNI，可以将

策略应用于路由。控制平面应支持配置参考点上的策略，以便修改经过参考点交换的信息类型和数量。

由于不同的接口具有不同的信任关系，因此对通过的信息有不同的限制和要求，具体的要求如下：

a） UNI 和运营商间的 E-NNI 不应交换网络拓扑信息和网络内部地址信息；

b） 控制平面应该允许运营商对经过不同接口的控制信息的类型和范围进行配置；

c） 如果没有寻址目录服务，则需要在 UNI 进行地址解析。

5.3 用户结构和多归属

UNI-C 结构包含一个称为接入组容器（AGC）的传送实体，可以终结多条 SNPP 链路，并且具有支持用户呼叫和连接的控制功能。AGC 是一个单层实体，包含 ITU-T G.805 接入组、LRM 和 TAP。不同层网络的多个 AGC 可以位于同一设备中。

多归属是指在一个终端用户与一个或多个 ASON 网络之间支持多条 SNPP 链路。同时，在用户（UNI-C）和网络（UNI-N）之间还存在一个服务协议，使网络能够为多归属 SNPP 链路上承载的连接提供可靠性、分集或其他业务特征。

ASON 控制平面应提供和支持多归属。多归属可以细分为两类：对单个网络运营商的多归属和对多个网络运营商的多归属。多归属可以用于负载均衡或者提高网络生存性等。

5.4 网络分层与分级

5.4.1 网络分层

ASON 传送平面按照 ITU-T G.805 建议进行分层，如图 6 所示。因此，对 ASON 控制平面的描述可以分为与单层网络相关的方面，例如路由、连接创建和删除等，以及与多层网络相关的方面。

ASON 层网络之间是客户和服务者关系，这种关系通过终端和适配执行器管理（见 7.4.7）。所有服务层的拓扑和连接性对于客户层是不可见的，服务层资源以 SNPP 链路的形式呈现给客户层网络。

当客户层由于服务层资源缺乏不能建立连接时，可以在一个或多个服务层网络中建立新连接，然后在客户层网络中创建新的 SNP 链路连接。这一过程可以在每个层网络中重复执行。

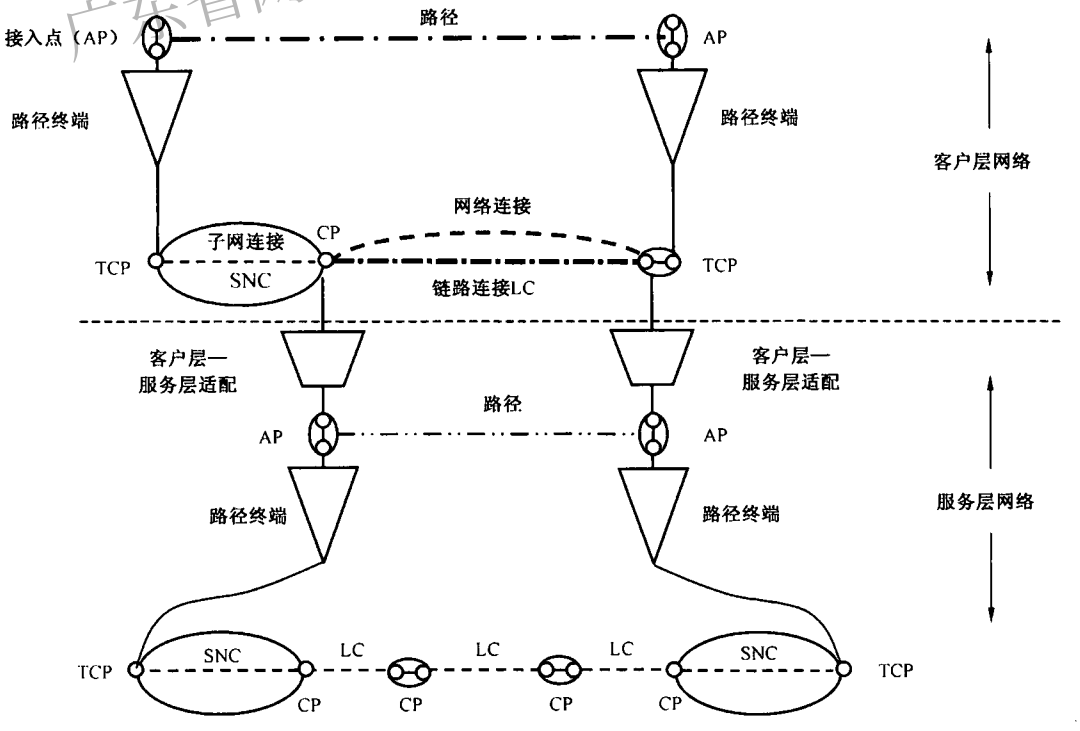


图 6 ITU-T G.805 网络分层模型

5.4.2 网络分级

ASON 网络分级可以通过控制域层次来实现。为了实现 ASON 网络的可扩展性和可管理性，可以将 ASON 网络划分成多个路由域，并采用分级路由的方式。图 7 从分级路由的角度给出了一个 n 级网络的结构的示例。

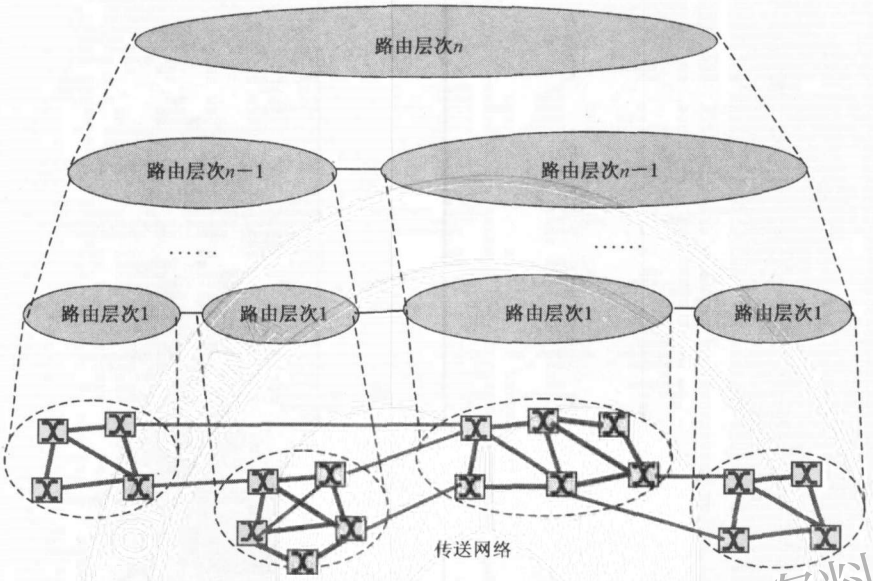


图 7 网络分级结构示例

5.5 ASON 网络参考模型

ASON 网络的参考模型包括多运营商和单运营商两种参考模型，其中包括了控制域和各种接口。

a) 在多运营商 ASON 网络参考模型中，不同运营商之间通过运营商间 E-NNI 接口互连，该接口一般不具有信任关系。

b) 在单运营商 ASON 网络参考模型中，可以将网络进一步划分为多个控制域，例如核心网、区域网和城域网。不同控制域之间通过运营商内部 E-NNI 接口互连，该接口具有一定程度的信任关系。用户和网络之间通过 UNI 接口互连，在一个控制域内部使用 I-NNI 接口。

ASON 网络模型的规划设计，主要应依据运营商的需求和网络结构。图 8 和图 9 提供了多运营商和单运营商 ASON 网络参考模型的示例。

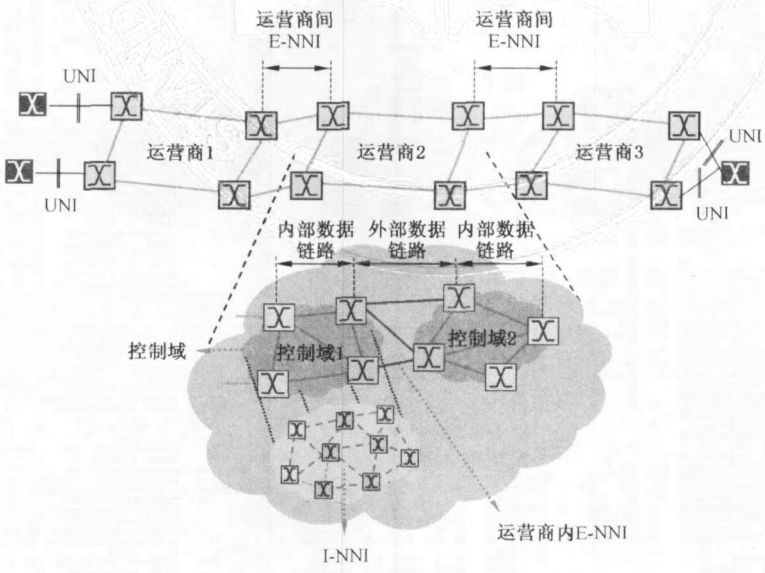


图 8 多运营商 ASON 网络参考模型示例

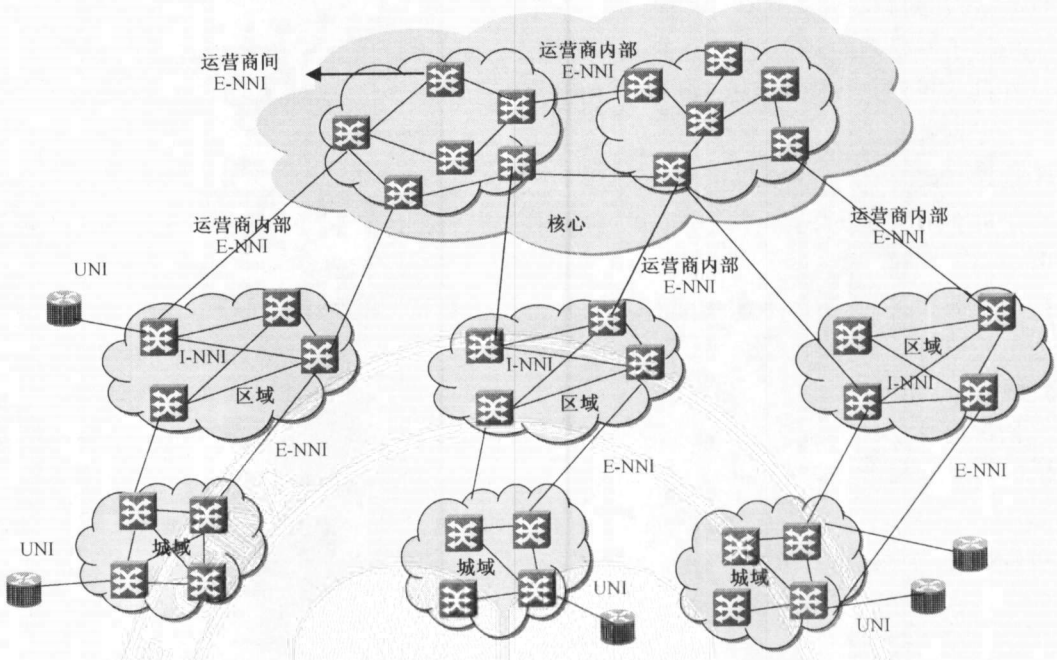


图 9　单运营商 ASON 网络参考模型示例

6　传送资源及组织结构

6.1　传送实体

为了实现 ASON 的连接控制和管理功能，需要对传送资源的功能结构进行描述。每个传送资源采用一个代理来表示。这些代理和参与控制管理的其他功能交互，提供所需的信息或执行传送资源操作。

在 ASON 网络中，传送平面资源在控制平面内表示为一些实体。图 10 给出了 ITU-T G.805 描述的传送资源、ITU-T M.3100 描述的表示传输资源的实体，以及控制平面的传送资源视图。

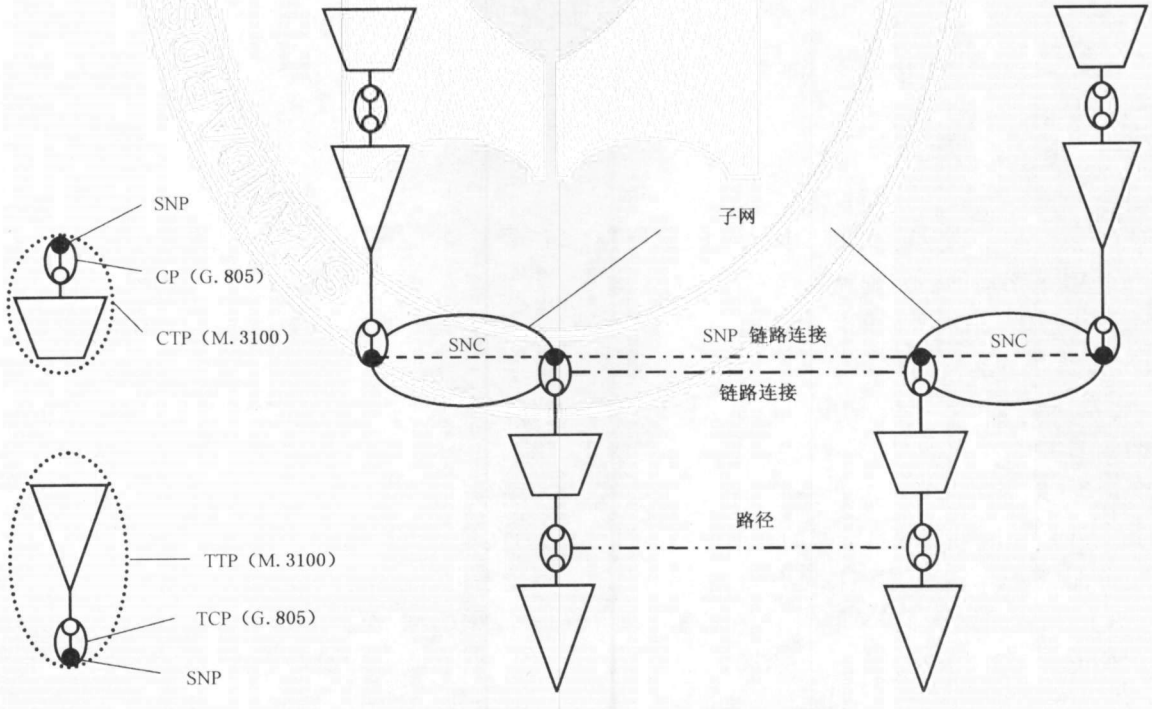


图 10　传送平面、管理平面和控制平面中结构实体之间的关系

子网点(SNP)与其他 SNP 有多种关系：

a) 位于不同子网的两个 SNP 之间的一种静态关系，称为一个 SNP 链路连接。

b) 在同一子网边界上的两个(或在广播连接情况下为多个)子网点之间的一种动态关系，称为一个子网连接。

出于选路目的，一个子网点也可与其他子网点组合为一个子网点池(SNPP)。SNPP 可被进一步划分为多个小的 SNPP，这种结构可用来描述不同程度的路由分集。不同子网的 SNPP 之间的关联是一个 SNPP 链路。

与控制平面相关的 SNP 和 SNP 链路连接状态在 7.4.7 终端和适配执行器及 7.4.3 链路资源管理器中描述。

6.1.1 多种适配功能

许多传送系统支持多种适配功能，单个服务层路径也可动态支持多种不同的复用结构。这可以抽象为给不同适配结构中的每个 CP 分配 SNP，并将这些 SNP 置于各自的分层子网中。当分配一个特定 SNP 时，将激活适配功能中相关的客户进程，并生成关联的 CTP。相应的，位于其他分层网络中使用相同资源的 SNP 将变为忙的状态。图 11 给出了可支持一个 VC-4 或 3 个 VC-3 的一个 STM-1 路径的实例。

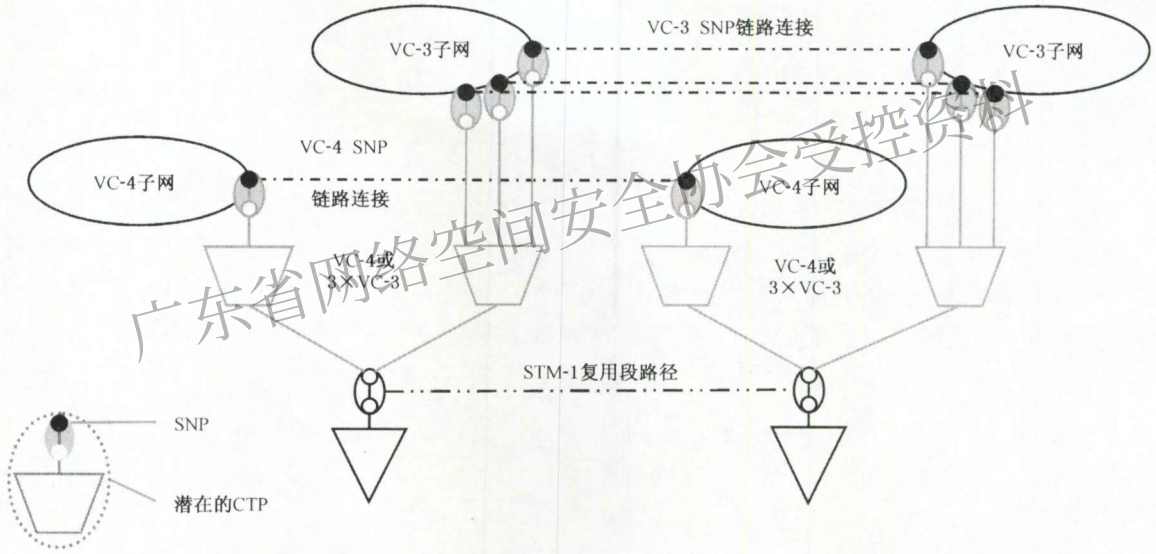


图 11 多种适配功能举例(STM-1 路径支持 3×VC-3 或 1×VC-4)

6.1.2 VPN 之间的链路资源共享

ASON 体系结构可以提供 ITU-T Y.1313 规范的一层 VPN 业务。VPN 是一个封闭用户组，可以使用定义好的一组网络资源。

在控制平面中，一个 SNPP 可以是公共的，即不与任何一个 VPN 相关；也可以是私有的，即仅由一个 VPN 使用。在一个 VPN 中，连接选路时只能使用与该 VPN 关联的 SNPP。

在传送平面中，CP 可以被分配给位于多个 SNPP 中的一个 SNP，这个 SNP 可以是公共的或者私有的。不同 VPN 可以共享链路的连通性，这可以抽象为在每个 VPN 中为共享 CP 创建一个 SNP。当 CP 被分配给一个 VPN 中的特定 SNP，在其他 VPN 中代表相同资源的 SNP 变为不可用。

图 12 给出了两个 VPN 的例子，在控制平面中每一个 VPN 包含两个 SNP。在传送平面中，第一个 CP 被分配给 VPN2 中的第二个 SNP，第三个 CP 被分配给 VPN1 中的第二个 SNP，第二个 CP 被同时分配给 VPN1 和 VPN2 中的第一个 SNP。如果第二个 CP 被 VPN1 中的第一个 SNP 占用，那么该 SNP 状态为可用，而 VPN2 中的第一个 SNP 状态变为忙。

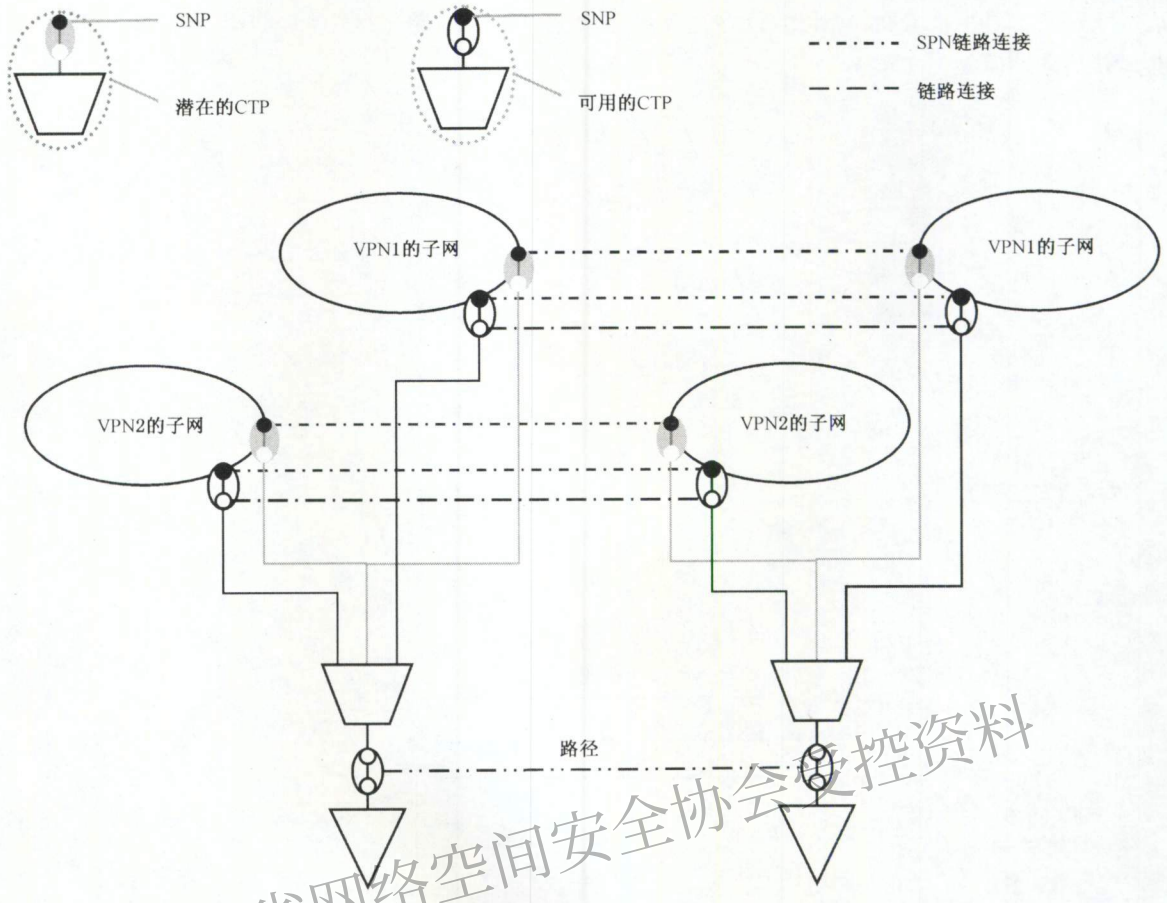


图 12 VPN 资源之间的链路资源分配

6.2 路由区

一个路由区位于一个单层网络内。路由区定义为一组子网、连接这些子网的 SNPP 链路，以及描述路由区边界上的 SNPP 链路端点的 SNPP。路由区可以进一步划分为通过 SNPP 链路互联的更小的路由区。进一步划分的限制是，在一个路由区内仅包含一个子网。

路由区和子网密切相关，因为它们在网络分割中提供相同功能。二者的区别在边界上，链路端点在路由区内部是可见的，而在子网内部只有连接点是可见的。从外部来看，子网和路由区是一样的，二者在术语上同义。从外部不可能看到子网或路由区的任何内部细节，子网和路由区在网络拓扑图上表示为一些点。

在一个 SNPP 链路跨越一个路由区边界的地方，共享此公用边界的所有路由区包含相同的 SNPP 链路，如图 13 所示。

6.2.1 链路聚合和路由区

路由区和 SNPP 链路可通过分层方式相关联。图 14 表示了路由区和子网点池(SNPP 链路)之间的关系。图中，路由区 A 被分割为较低等级的路由区 B、C、D、E、F、G，以及连接它们的 SNPP 链路。这种分割可以根据需要继续循环进行。例如，路由区 E 被进一步分割为路由区 H 和 I。该例子中存在一个顶级路由区。在基于“包含”关系(低等级的路由区完全包含在一个较高等级的路由区内)创建一个路由区等级结构时，在高等级路由区的边界，仅包含低等级路由区的一个子集和这些路由区 SNPP 链路的一个子集。从路由区 A 内部来看，低等级路由区内部结构是可见的，而从路由区 A 的外部来看，则是不可见的。从 A 的外部来看，只有位于高等级和低等级路由区之间的边界上的 SNPP，对高等级路由区是可见的。因此，从 A 的外部来看，路由区 B、C、F 和 G 最外面的 SNPP 链路是可见的，而位于 D 和 E、B

和 D、C 和 D、C 和 E、E 和 F，以及 E 和 G 之间的内部 SNPP 链路是不可见的。对不同等级路由区之间边界的可见能力是可嵌套的。因此，仅在高等级路由区以低等级路由区中的 SNPP 链路为边界的地方，创建 SNPP 链路等级。

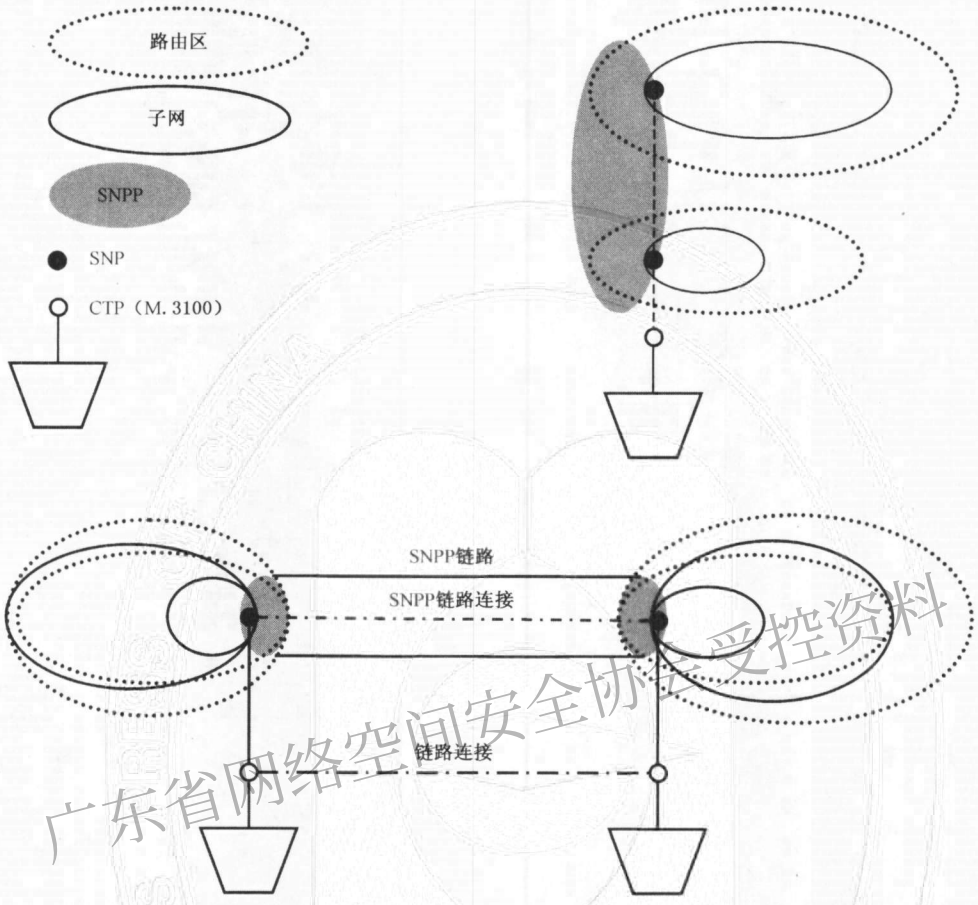


图 13　路由区、子网、SNP 和 SNPP 之间的关系

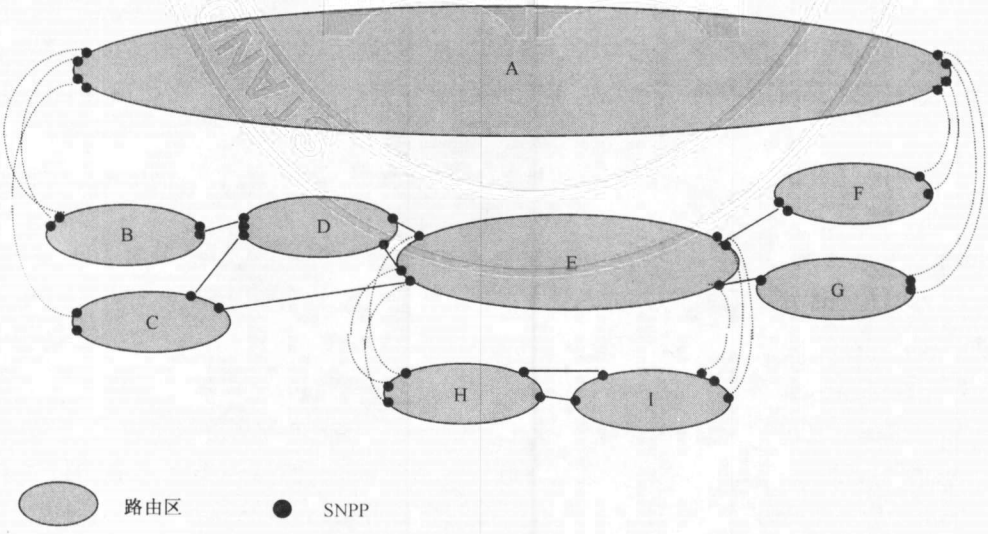


图 14　路由区等级结构和 SNPP 链路关系

子网点分配给路由结构中最低等级的一个 SNPP 链路，而且仅能分配给该等级的一个子网点池。在路由区等级边界上，低等级的 SNPP 链路池完全包含在一个高等级的 SNPP 链路内。一个高等级 SNPP 链路池可以包含一或多个较低等级的 SNPP 链路。在路由区等级结构的任何层次中，路由区互相不重合。因此在任一层次中，一个 SNPP 链路仅与一个路由区关联。位于路由区等级结构内某一等级的 SNPP 链路，它不是高等级路由区的边界，但可能是低等级路由区的边界，因此可以在该点构成 SNPP 链路的分级结构(例如路由区 E)。这样可以创建 SNPP 链路的包含等级。

一个路由区可以有一个 SNPP 名称空间，此名称空间同其他路由区使用的名称空间相独立。SNPP 名字属于路由区的 SNPP 名称空间，可用于在路由区中进行选路。

6.2.2 链路和链路聚合的关系

一个路由区内的一些 SNP 链路连接，仅当它们位于相同的两个子网之间时，可以分配相同的 SNPP 链路。如图 15 所示，在一个路由区内存在四个子网 SNa、SNb、SNc、SNd 和 SNPP 链路 1、2、3。SNP 链路连接 A 和 B 属于 SNPP 链路 1。SNP 链路连接 B 和 C 没有连接到相同的两个子网，因此它们不能属于同一个 SNPP 链路。在路由区之间聚合多个 SNP 的情况与此类似。

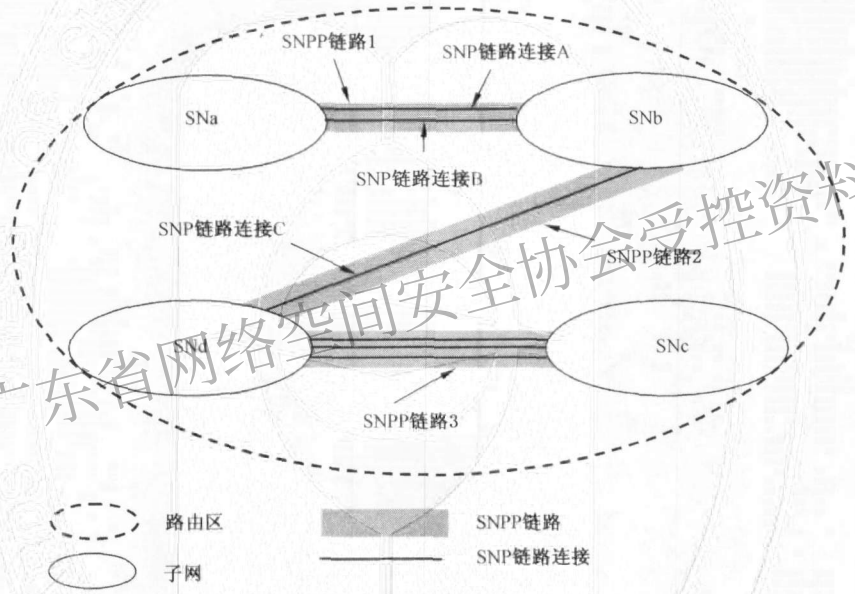


图 15 SNPP 链路与子网的关系

图 16 包含三个路由区 RA-1、RA-2 和 RA-3，以及 SNPP 链路 1 和 2。SNP 链路连接 A、B、C 不能属于相同的 SNPP 链路，因为它们的端点位于两个以上的路由区。对于路由区 3(RA-3)的选路来说，SNP 链路连接 A、B 与 SNP 链路连接 C 不同。

位于两个路由区或子网之间的多条 SNP 链路连接，可以聚合为一或多个 SNPP 链路。在以下情况下，可能需要聚合为多条 SNPP 链路：

- 如果从 SNPP 链路连接所互联的路由区，或包含 SNPP 链路连接的路由区的角度看，这些 SNPP 链路连接的路由作用不同。
- 如果出于管理目的需要划分更小的组。

当聚合 SNP 链路连接为 SNPP 链路时，可能需要考虑不止一个路由范围。在图 17 中，路由区 1 和 3 之间存在两个 SNP 链路连接。如果两个路由区位于路由层次的顶级(即没有单个顶级路由区)，那么需要根据 RA-1 和 RA-3 的路由范围，来确定这两条 SNP 链路连接的路由作用是否等同。RA-0 是一个包含路由区。从 RA-0 的角度看，SNPP 链路连接 A 和 B 可以在一个(图 17a))或两个(图 17b))SNPP 链路中。如果 RA-0 的路由方式是逐跳路由，只需要一条 SNPP 链路，因为对于 RA-1 到 RA-2 的下一跳路由计算，选择 SNP 链路连接 A 或 B 没有差别。

但从 RA-1 和 RA-3 的角度看，这两条 SNP 链路连接的路由作用有很大差别。选择 SNP 链路连接 A，从链路代价、保护等其他方面可能比 SNP 链路连接 B 更好。这时，应把两个 SNP 链路连接分别聚合为各自的 SNPP 链路。在图 17 中，SNPP 链路 11、链路 12 和链路 1 可以同时存在。

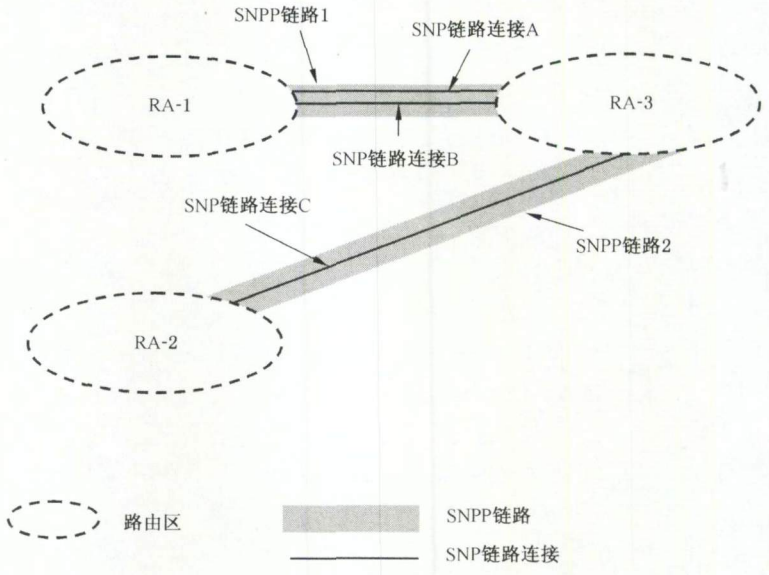
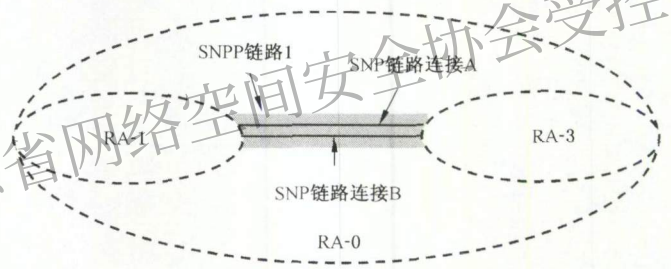
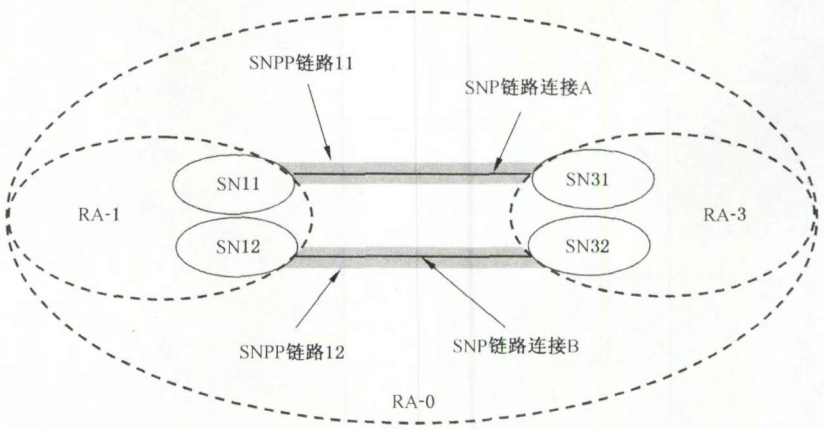


图 16 SNPP 链路与路由区的关系



a)



b)

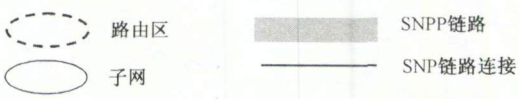


图 17 路由范围

选择 SNPP 链路 11 而非 SNPP 链路 12 的另一个原因是，通过 SNPP 链路 11 和 SNPP 链路 12 穿过 RA-3 所需要花费的成本不同。因此，有必要提供一个机制来比较通过链路 11 或链路 12 穿越 RA-3 的相关成本。递归使用这一机制可以确定穿越 RA-0 所需要花费的相关成本。这种机制不会把网络拓扑扩散到路由区范围以外。获得特定路由选择的成本可通过调用查询功能来实现。查询所返回的成本由每一个路由区所使用的策略决定。所有路由区应采用同样的策略，以使结果具有可比性。在计算成本之前，查询功能还可以使用路由约束条件。

6.3 拓扑和发现

路由功能可通过 SNPP 链路来了解拓扑。在 SNPP 链路生成之前，下层的传送拓扑，即 CTP 之间的链路连接关系必须建立。这些关系可通过多种不同技术来发现，例如使用一种测试信号或服务层的路径踪迹。这些功能也可根据网络规划由管理系统来提供。传送设备支持灵活适配的能力（即支持多种客户层网络的链路连接）也可以被发现和报告。

路由目的相同的 SNP 链路连接被聚合成 SNPP 链路。这种聚合是基于一些参数，如链路代价、时延、质量或分集属性。其中一些参数可来自于服务层，但总体上这些参数由管理平面配置。

为了在不同的 ASON 网络（如不同的 VPN）的资源之间，或者由 ASON 控制和由管理平面控制的资源之间进行资源划分，可以创建多条链路，例如一些路由目的相同的链路连接可被划分为不同的链路。

链路信息（例如链路连接和 CTP 对的名称）被用于配置与 SNPP 链路相关的 LRM 实例（如 7.4.3 所述）。根据链路连接的参数，还可以提供此链路的其他特征。每个链路终端的 LRM 必须建立一个与 SNPP 链路对应的控制平面邻接关系。接口 SNPP id 可在邻居发现期间协商或由 LRM 配置来提供。然后，链路连接和 CTP 名称被映射到接口 SNP id（和 SNP 链路连接名称）中。在链路的两个端点都位于同一路由区内的情况下，本地和接口 SNPP id 以及本地和接口 SNP id 可能相同。否则，在每个链路终端，接口 SNPP id 被映射到一个本地 SNPP id 中，接口 SNP id 被映射到本地 SNP id 中，如图 18 所示。

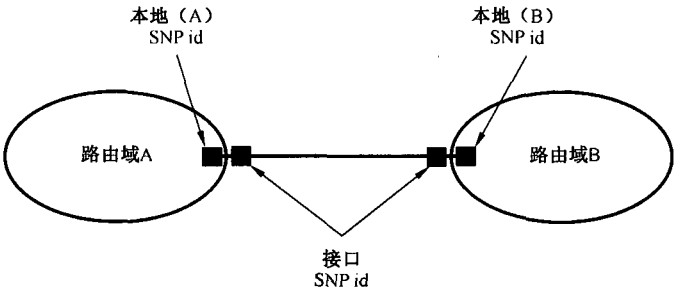


图 18 本地和接口 id 之间的关系

SNP 链路连接可由一个发现进程来验证。这个阶段要求的验证程度依赖于由控制平面或管理平面最初提供的链路连接关系的完整性以及用来把 CTP 映射到 SNP 的程序的完整性。

验证可通过服务层的路径踪迹或采用一个测试信号和测试连接。如果使用测试连接，发现进程可通过管理平面或控制平面来建立和释放这些连接。如果使用控制平面，链路必须暂时对路由和连接控制可用，仅用于测试连接。一旦 SNPP 链路确认完成，LRM 通知 RC 元件 SNPP 链路邻居和链路特征，如代价、性能、质量和分集属性。

6.4 域

ITU-T G.805 定义了域的概念，包括行政和管理域、Internet 管理域，用于区分不同的行政和管理上的能力、信任关系、地址结构、基础结构、生存性技术、控制功能的不同分布等。因此，域代表一系列用于特殊目的的实体的集合。

控制域由控制平面元件的集合构成，控制域提供了一个封装和隐藏各种结构元件的分布实现细节

的结构。域可以把一组分布式元件描述为一个实体(即域)的分布接口,域的接口与原来的元件分布式接口具有相同的特性。控制域之间交互的信息,采用了元件分布式接口上交换信息所使用的公共语义,但允许在域内部使用不同的表示方法。

控制域通常从一种或一些特定的元件类型派生,这些元件为某种目的进行交互。例如,路由(控制)域从路由控制器元件派生,重路由域从一组负责对经过域的呼叫/连接进行重路由/恢复的连接控制器和网络呼叫控制器派生。在以上的两个例子中,路由或重路由操作完全发生在域内。控制域的描述与一个层网络内的元件相关。

不同类型的控制域不一定需要重合。对相同类型的控制域应遵循以下约束:

a) 完全包含其他相同类型的域,但不重合;

b) 控制域边界共用;

c) 控制域相互隔离。

图 19 给出了元件、域和参考点之间关系的例子。图中给出了域 B 和域 A、C、D 之间的关系。每个域从类型 Z 的元件派生。每个域内部的结构和交互可能不同,例如它们可能采用不同的联邦模型。图 20 给出了一个相同的例子,描述元件、域和接口之间关系。元件通过协议控制器交互,在 I-PC 元件上使用协议 I,在 E-PCs 元件上使用协议 E。在 A 和 B 内部使用的协议可以不同。I-NNI 接口位于域内的协议控制器之间,E-NNI 接口位于域间的协议控制器之间。

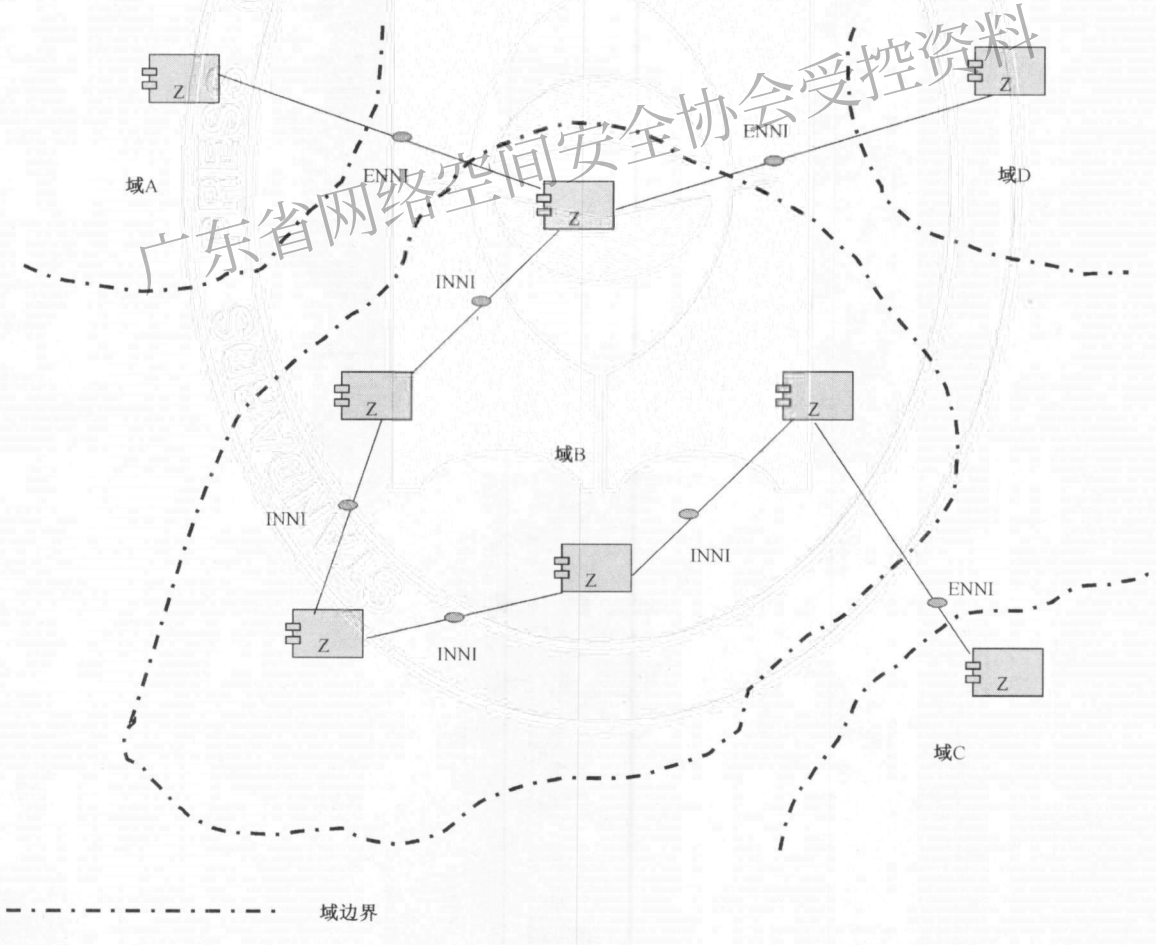


图 19 域、协议控制器和参考点的关系

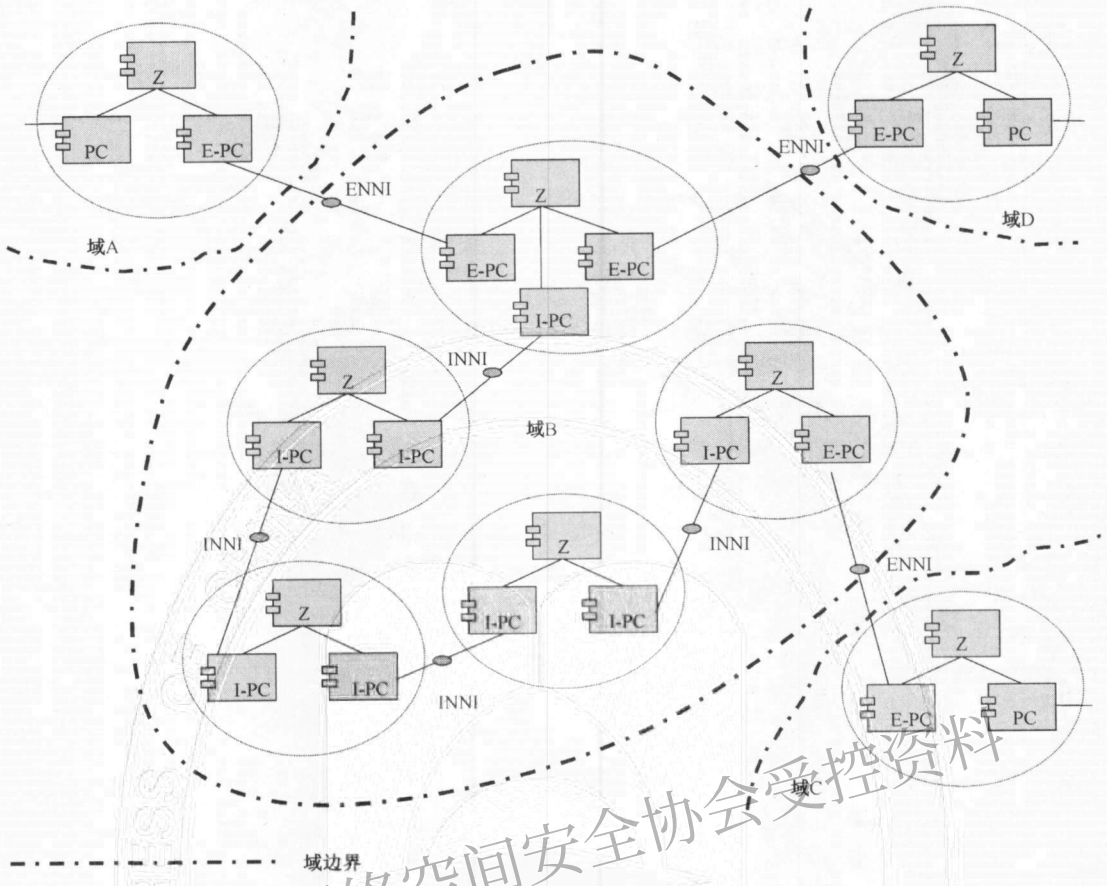


图 20 域、协议控制器和接口的关系

6.4.1 控制域和控制平面资源之间的关系

根据控制域中元件的目的，元件可以反映底层的传送网络资源。例如，根据在整个路由控制域内所采用的路由方式和路由协议，路由控制域可以包含一些元件，这些元件代表了位于一个或多个聚合层次上的一个或多个路由区。

6.4.2 控制域、接口和参考点的关系

I-NNI 和 E-NNI 接口总位于协议控制器之间。协议控制器之间运行的协议可以使用也可以不使用传送网络的 SNPP 链路，因此在 SNPP 链路上表示 I-NNI 和 E-NNI 接口是不正确的。

I-NNI 和 E-NNI 参考点位于相同类型的元件之间，这种元件类型不是协议控制器，这些参考点表示原语消息流(见第 7 章)。在仅给出域和域间关系的图中(不显示域的内部结构)，假定信息传送是通过一个参考点进行的。

6.5 多层次方面

对控制平面的描述可以分为与单层网络相关的方面，例如路由、连接创建和删除等，以及与多层网络相关的方面。层网络之间的客户/服务者关系通过终结和适配执行器管理(见 7.4.7)。

所有服务层的拓扑和连接性对于客户层是不可见的，这些服务层的资源被封装，作为一个 SNPP 链路呈现给客户层网络。当客户层由于资源缺乏不能得到所需的连接性时，可以通过在一个或多个服务层网络中建立新连接，来获得更多的资源，继而在客户层网络中创建新的 SNP 链路连接。这可以通过修改潜在的 SNP 为可用的 SNP 来实现，或者根据规划软件输出的规划结果增加更多的基础设施。因此，通过在一或多个服务层网络中建立新的连接，创建新的客户层资源的能力，是在客户层网络提供连接性的首要条件。这一过程可以在每一层网络中重复执行。

服务层网络何时提供连接用于建立客户层拓扑，取决于一些外部限制条件(例如链路的远期流量预

测，网络规划和财政管理权），并且与运营者相关。ASON 体系结构支持根据客户层新的拓扑需求，通过发现所需的潜在 SNP，创建服务层连接性。

6.6 层间客户支持

在传送网络中，网元可以支持多个传送分层。例如在一个多层网络的边界，存在较小带宽的适配功能，而多层网络的中央则不支持这些适配功能。问题在于在两个客户 AGC 之间，当不存在连续的或者连接好的客户层网络时，如何传输客户的特性信息（CI）。解决此问题存在两种方案。第一种，根据服务层连接来创建客户层链路，客户层链路创建后被呈现给该路由区的路由控制器。第二种，客户特性信息（CI）被适配到服务层连接上，这对于客户层路由控制器是不可见的。

第二种方案使用了不同层网络中的网络呼叫控制器（NCC）之间的接口，来提供 ASON 功能。这种层间接口在客户—服务层关系的呼叫之间形成关联。这种关联关系可以递归，表示一组堆栈式的适配关系，也就是说 NCC 可以在 ITU-T G.805 定义的层次中递归存在。在不同层次中可以存在不同的 NCC 实例。例如，在客户层中的 NCC 是分布式的，而在服务层中的 NCC 是集中式的。服务层的连接控制器（CC）首先创建连接，然后客户 CI 被映射到服务层的连接，并通过客户/服务层的 NCC 关系来维护这一映射关系。在这种情形下，客户层的链路连接创建，是服务层创建连接和 CI 映射的结果，但是客户层的 CC 不参与此过程。这一过程可以向上逐层递归，在每一个相关的客户层创建链路连接。附录 C 给出了此应用的例子。

7 ASON 控制平面结构

7.1 概述

ASON 控制平面结构描述了控制平面支持各种 ASON 功能的参考结构，包括主要的功能元件以及它们之间的交互。ASON 控制平面结构应具有以下特征：

a) 支持多种传送技术，例如 ITU-T G.803 定义的 SDH 传送网、G.872 定义的光传送网（OTN）。

b) 与所选择的特定控制协议无关，即控制平面结构独立于所选用的连接控制协议。

c) 控制平面结构的适用性与控制平面和路由区的划分方式无关，同时与传送资源如何划分给不同子网的方式无关。

d) 无论连接控制的实施方法是基于全分布式还是集中式，控制平面结构均适用。

ASON 控制平面结构主要描述以下内容：

a) 控制平面的功能元件，包括抽象接口和原语；

b) 呼叫控制器元件之间的交互；

c) 在连接建立过程中，元件之间的交互；

d) 在外部接口上，将抽象元件接口转换成协议的功能元件。

控制平面的基本结构元件包括：连接控制器（CC）、路由控制器（RC）、链路资源管理器（LRM）、流量策略（TP）、呼叫控制器（CallC）、发现代理（DA）、终端和适配执行器（TAP），以及协议控制器（PC）。其中呼叫控制器又分为：主叫方呼叫控制器（Calling Party Call Controller）、被叫方呼叫控制器（Called Party Call Controller）和网络呼叫控制器（NCC）。

图 21 给出了各元件之间相互关系的例子。

ASON 控制平面还定义了一些特殊元件来增强实现的灵活性，这些元件包括协议控制器和端口控制器，这些元件的接口细节不在本部分中规范。

协议控制器的功能是把由一个或多个结构元件的原语接口复用到一个协议实例，参见 7.4.8 和图 40 的描述。这样，协议控制器消除了不同协议选择之间的差别，从而使体系结构保持不变。由一个或多个协议控制器负责管理通过参考点的信息流。

端口控制器用于在系统接口上应用规则。其目的是为结构元件提供一个安全的运行环境，使结构元件不必考虑安全问题。特别是，端口控制器可以使控制平面结构在确定其分布时，不必考虑涉及安全方面的问题，参见 7.3.1 和图 23 中的描述。

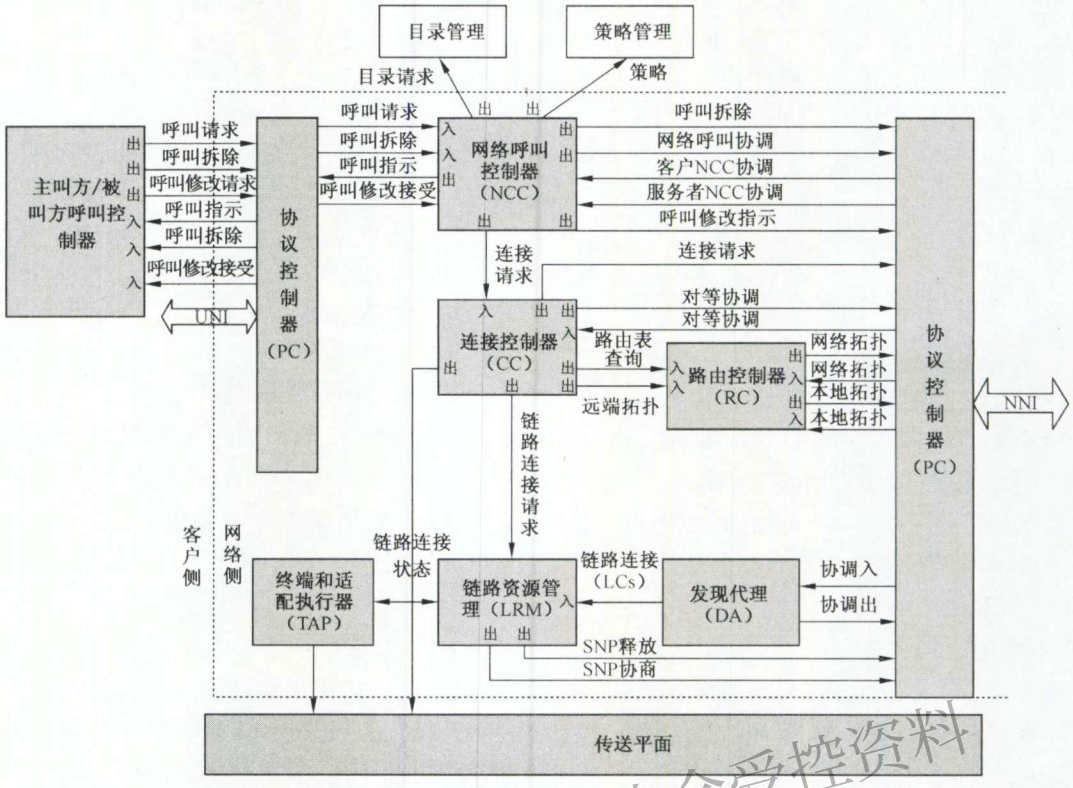


图 21　控制平面各元件的交互关系

7.2　描述符号

本节基于通用建模语言（UML）对控制平面元件结构的描述符号进行规范。

a）　接口：接口支持一组操作，它规范了一个元件所提供的服务，且接口独立于使用或提供这种服务的元件。操作规范了基于约束条件下进出接口的信息。接口定义是以表格的方式表示，如表 1 和表 2 所示。每个接口都有一个表示其角色的名称。输入接口表示由元件提供的服务，基本输入参数是执行特定任务所需要的参数，基本返回参数是对输入参数动作的结果。输出接口表示元件使用的服务，基本输出参数定义了接口提供的信息，基本返回参数（如果需要）用于响应输出参数。通知接口表示元件的主动输出动作，并由一个没有返回参数的输出接口表示。这三个接口类型在接口规范中分别描述。

表 1　通用接口描述（1）

输入接口	基本输入参数	基本返回参数

表 2　通用接口描述（2）

输出接口	基本输出参数	基本返回参数

b）　角色：是一个实体参与一个特定活动时的行为。角色允许不同实体在不同时间参与活动，并通过说明与接口名称的关系来表示。

c）　元件：元件表示抽象的实体，而不是一个具体实现的代码实例。元件用于构建场景，来描述控制平面结构的操作。元件由带标注的方框表示，如图 22 所示。

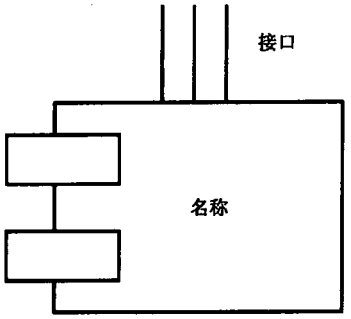


图 22　一个元件的表示

通常，每个元件具有一组特定接口来监视元件操作、动态地设置策略和控制内部的行为。这些接口不是强制要求的，只是有需要的特定元件才提供这些接口。监测接口的使用在每个元件中描述。在描述元件的接口时，只描述不同类型的接口。所有元件都具有支持多个呼叫者和多个提供者的特性，但并发请求的解决方案不在本部分规范的范围内。由于元件是以一种抽象的方式使用，可以通过划分子类和合并的技术对结构元件的规范进行扩展。

7.3　策略和联邦

7.3.1　策略的通用模型

在策略模型中，系统表示元件的集合，在系统边界上提供可以应用策略的点。策略被定义为应用于系统边界接口的一套规则，并由端口控制器元件来实现。策略端口用于简化应用在多个端口上的策略模型。系统边界是可以嵌套的，允许对应用于任何范围（全系统、一组元件或单个元件）的共享策略进行建模。策略应用的顺序由嵌套的顺序指定。在图 23 中，虚框表示系统边界，在边界上的封闭方框称为端口，表示端口控制器元件。

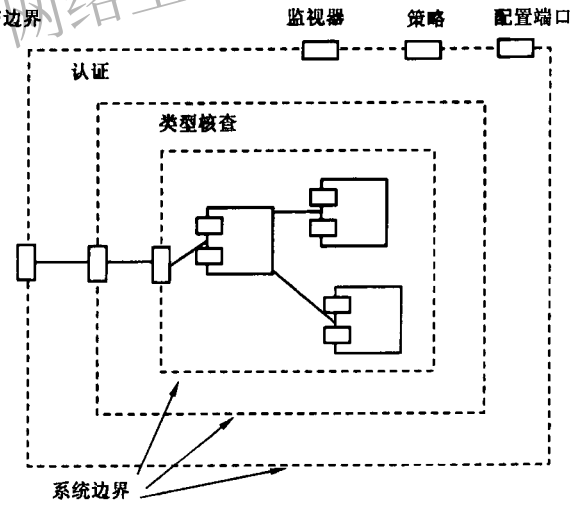


图 23　与策略控制相关的系统边界

监视、策略和配置端口可用于任何系统和元件，不需要进一步的结构规范。监视端口允许性能劣化、故障事件、失效等满足策略条件的相关管理信息通过边界。策略端口允许交换与元件相关的策略信息。配置端口允许交换（服从于策略约束）与元件相关的配置、指配和管理信息，可能会动态调整系统的内部行为。

图 23 表示加密、认证和类型核查作为一组三层嵌套的端口控制器的实例，其中策略应用的顺序是按照嵌套的顺序进行的。认证边界内的元件不需要规范加密或认证的要求，因为这些是元件环境的特性。对每个独立的端口策略要定义端口控制器，策略的组合通过端口控制器的集合来实现。这样就允许创建可重用的元件，并通过描述性的前缀来区别。违背策略的情况通过监测端口上报。

策略端口可被看作输入信息的一个过滤器，违反策略的信息都将被拒绝。通过系统策略端口可以动态地改变策略，这样可以描述动态的行为变化。策略如何在参考点上应用是一个普遍的问题。策略只能应用在穿过参考点的单个接口上。在后面的协议控制器部分，将描述把多个接口合并为一个实现接口的方法。

策略的其他方面与元件不同的行为(如时间表、接入权等)有关，这些方面由元件来规范和实现。元件行为也可以动态的改变，这种能力可由策略来控制，因此管理者可以决定在哪里规范哪些系统行为。

与系统的其他方面一样，策略也可以是分布的。RFC2753 规范的 COPS 协议模型就是一个分布式模型的例子。模型的策略执行点(PEP)(策略决定被执行的点)对应于该模型中的端口。策略决定点(PDP)是进行策略决策的点，策略决定可以在端口内完成，也可能分布到其他的系统上完成。这种分布式的决定依赖于多种因素，而这些因素又依赖于实际的策略。例如，由于性能原因(加密)可能要求 PDP 在端口内实现，而安全因素(密码查找)可能迫使 PDP 在其他位置实现。当 PEP 和 PDP 不在一起时，它们之间需要协作。

7.3.2 联邦的通用模型

ASON 网络种需要跨多个域进行连接的创建、维护和删除，这是通过不同域中的控制器之间的协作来完成的。联邦是通过相互协作完成连接管理的域的集合，可通过连接控制器间的合作关系来描述(连接控制器在 7.4.1 描述)。

联邦模型包括两类：

a) 关联联邦模型

在关联联邦模型中，父连接控制器管辖着位于不同域内的连接控制器。当一个连接需要跨多个域时，最高级别的连接控制器(父连接控制器)作为协调者。该连接控制器了解每个域内的最高级别连接控制器。父连接控制器负责下级连接控制器之间网络连接职责的划分，每个连接控制器负责自己部分的网络连接，如图 24 所示。这个模型为递归方式，在某一层次内的父连接控制器，在更高层次中作为子连接控制器。

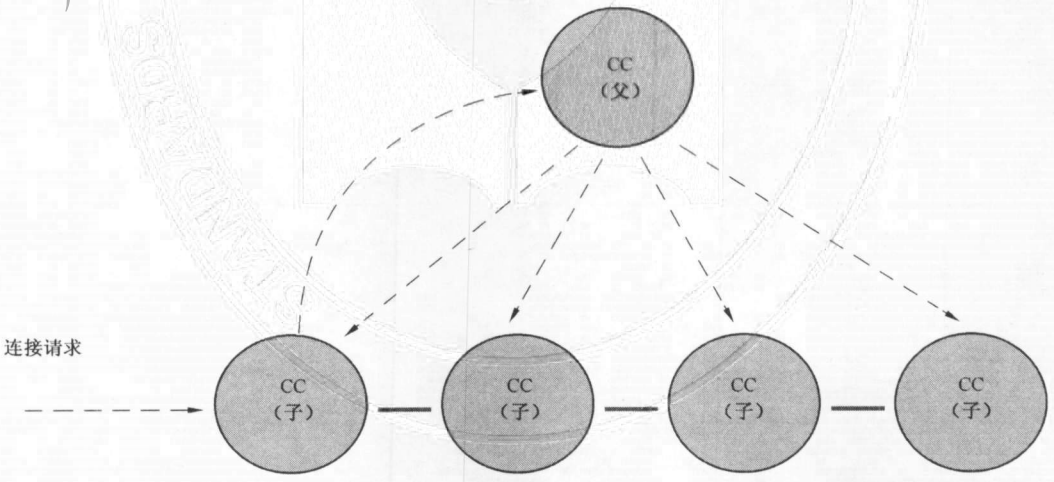


图 24 关联联邦模型

b) 合作模型

在合作模型中，没有父连接控制器的概念。当发出连接请求时，发起方连接控制器自主地与各个域相关的连接控制器联系，而不需要整体协调。实现合作模型最简单的方式是发起方连接控制器与连接控制器链上的下一个连接控制器直接进行交互。如图 25 所示，每个连接控制器计算它所能提供的连接部分，以及下一个连接控制器是什么，这一过程将持续到连接配置完成为止。

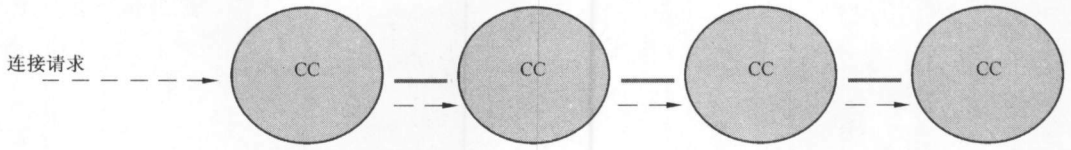


图 25　合作联邦模型

管理域之间的联邦采用合作模型，所有管理域具有与其他管理域联合的能力。一个管理域内的父连接控制器可通过合作模型与其他管理域内的父连接控制器联合。管理域可以被进一步划分，在一个管理域内的不同域间采用何种联邦模型可以独立于其他管理域。因此，如图 26 所示，将两种联邦模型相互结合，可以组建大型网络。上述原则同样适用于呼叫控制器的联邦。

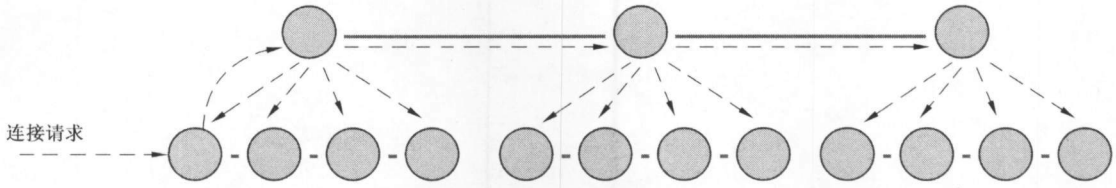


图 26　混合联邦模型

7.4　结构元件

本条描述控制平面结构元件的基本功能、元件接口和操作。对于连接控制器、路由控制器、主叫方/被叫方呼叫控制器和网络呼叫控制器，这些元件可以是公共的（在这种情况下它们仅使用公共的 SNPP），或者是私有的（在这种情况下它们使用与一个特定 VPN 关联的 SNPP）。控制平面元件的 VPN 关系，由与该元件关联的协议控制器提供。

7.4.1　连接控制器（CC）

连接控制器（CC）负责协调链路资源管理器、路由控制器以及对等和从属的连接控制器，来管理和监控连接的建立、释放以及修改现有连接的连接参数。

该元件服务于单个子网，为其他控制平面元件提供抽象接口，如表 3 和表 4 所示。图 27 描述了连接控制器元件。需要说明的是，路由参数不适用于 UNI 参考点上的 CC 接口。

此外，CC 元件提供了一个连接控制器接口（CCI），该接口位于传送平面中的一个子网和控制平面之间。CCI 接口用于控制元件发送指令，建立、修改和删除 SNC。CCI 接口不应用策略。

表 3　连接控制器元件接口（1）

输入接口	基本输入参数	基本返回参数
连接请求入	一对本地 SNP 名称和一个可选的路由	一个子网连接
对等协调入	1. 一对 SNP 名称；或 2. SNP 和 SNPP；或 3. SNPP 对；或 4. 路由	确认信号

表 4　连接控制器元件接口（2）

输出接口	基本输出参数	基本返回参数
路由表查询	未确定的路由片段	路由
链路连接请求	—	一个链路连接（一个 SNP 对）
连接请求出	一对本地 SNP 名称	一个子网连接

表 4（续）

输出接口	基本输出参数	基本返回参数
对等协调出	1. 一对 SNP 名称；或 2. SNP 和 SNPP；或 3. SNPP 对	确认信号
远端拓扑出	拓扑信息（链路和/或子网），包括资源的可用性	—

注：远端拓扑出接口用于提供连接控制器了解的拓扑信息。

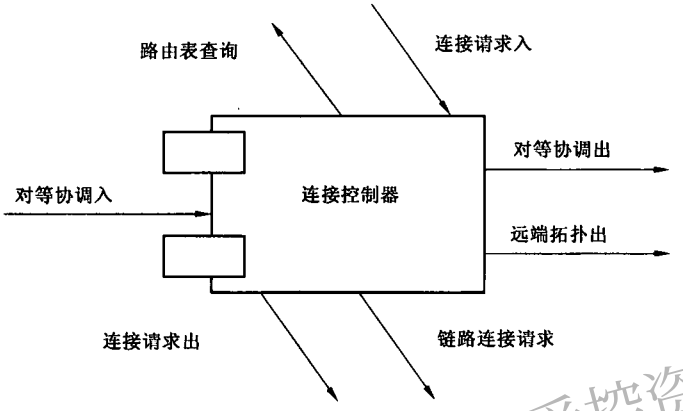


图 27 连接控制器元件

连接建立通过响应来自于规定范围内的连接控制器或对等连接控制器的连接请求来完成。在分级路由的情况下，上级（即父）连接控制器选择源和目的 SNP 时，使用连接请求入和连接请求出接口；而在其他情况下，使用对等协调入和对等协调出接口。这两种情况的元件操作相同。

通过路由表查询接口，路由的第一个未分配部分被确定为将要经过的一组链路，并在路由中增加这一组新链路。连接控制器核查这一组新链路中的哪一条链路可用于链路连接分配，获得链路连接后，将它们所属的链路从链路组中删除。下一步，下级连接控制器（即子连接控制器）通过连接请求出接口来请求相应子网连接。未分配的路由部分向下游传递，到达下一个对等连接控制器。操作的实际顺序取决于多种因素，包括可用的路由信息数量以及接入链路资源管理器，但连接控制器的操作是不变的。连接拆除同连接建立操作类似，只是操作过程相反。

7.4.2 路由控制器（RC）

路由控制器的作用是：

a） 响应来自连接控制器的请求，提供用于建立连接的路由信息，该信息可以是端到端的（例如源路由），也可以是逐跳的。

b） 响应用于网络管理的拓扑信息（SNP 及其抽象）请求。

路由控制器维护它所负责的域内的路由信息，根据这些信息在该域内提供路由。路由信息包括拓扑信息（SNPP、SNP 链路连接）和与给定层的终端系统地址相关的 SNP 地址（网络地址）。路由控制器还维护在同一层的其他子网（对等子网）的地址信息，同时维护 SNP 状态信息来支持基于约束的路由。路由控制器可以根据路由约束条件，在两个或多个 SNP 之间确定一条可能的路由。路由信息包含以下不同级别的路由细节：

a） 可达性（例如距离矢量视图——维护地址和下一跳）；

b） 拓扑视图（例如链路状态——维护地址和拓扑位置）。

表 5、表 6 和图 28 描述了路由控制器的接口。

表 5　路由控制器接口(1)

输入接口	基本输入参数	基本返回参数
路由表查询	未定路由元素	按顺序排列的 SNPP
本地拓扑入	本地拓扑更新	—
网络拓扑入	网络拓扑更新	—
远端拓扑入	拓扑信息(链路和/或子网),包括资源的可用性	—

表 6　路由控制器接口(2)

输出接口	基本输出参数	基本返回参数
本地拓扑出	本地拓扑更新	—
网络拓扑出	网络拓扑更新	—

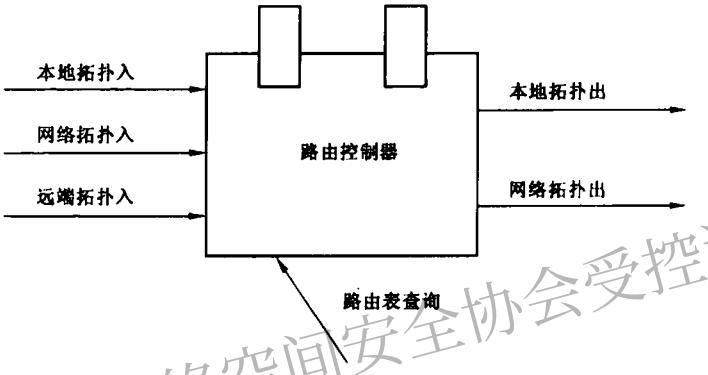


图 28　路由控制器元件

路由查询接口:该接口接受一个未定路由元素,并返回该路由控制器所负责域内的一组链路。返回的参数包括逐跳路由的下一跳和源路由等。查询结果的示例如下:

a) 返回该子网的一个出口 SNPP,它位于到达给定目的 SNPP 的路径上;

b) 返回一个子网序列,在给定源和目的 SNPP 对之间构成一条路径;

c) 返回一个子网序列,在两组 SNPP 之间构成一条路径;

d) 返回一个 SNPP 序列,在给定源和目的 SNPP 对之间构成一条路径;

e) 返回一个 SNPP 序列,在给定源和目的 SNPP 对之间构成一条包含一个或多个特定 SNPP 的路径;

f) 返回一个 SNPP 序列,在给定源和目的 SNPP 对之间构成一条与给定路径相分离的路径。

路由查询接口返回的 SNPP 必须全部是公用的或全部与同一个 VPN 相关联。

本地拓扑接口:该接口用于配置具有本地拓扑信息和本地拓扑更新信息的路由表。这些拓扑信息来自路由控制器所负责的域的内部。本地拓扑信息可以是公共的或者与一个特定 VPN 相关联。

网络拓扑接口:该接口用于配置具有网络拓扑信息和网络拓扑更新信息的路由表。这些信息是简化的拓扑信息(例如概括的拓扑),来自路由控制器所负责的域的外部。网络拓扑信息可以是公共的或者与一个特定 VPN 相关联。

远端拓扑入:该接口用于接受来自连接控制器的拓扑信息。

7.4.3　链路资源管理器(LRMA 和 LRMZ)

LRM 元件负责管理 SNPP 链路,包括指配和去指配 SNP 链路连接,并提供拓扑和状态信息。由于 SNPP 链路可以是公共或私有的,所以 LRM 也可以是公共的或与某个 VPN 相关联。

存在两种 LRM 元件——LRMA 和 LRMZ。一条 SNPP 链路由一对 LRMA 和 LRMZ 元件管理,

每个元件管理链路的一端。SNP 链路连接的指配请求仅发送给 LRMA。

图 29 给出 SNPP 链路的两种情况。

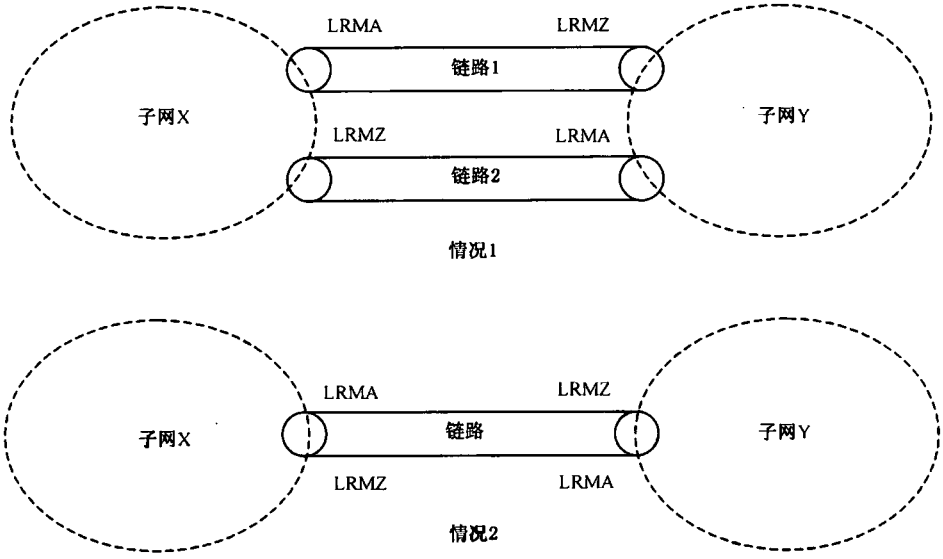


图 29 SNPP 链路情况

在情况 1 中，链路 1 专用于子网 X 发起的连接建立。来自子网 X 的 SNP 链路连接请求被发给邻近的链路 1 LRMA。该 LRMA 可以不与链路 1 的 LRMZ 协商就分配 SNP 链路连接。同样，链路 2 专用于子网 Y 发起的连接建立。来自子网 Y 的 SNP 链路连接请求被发给邻近的链路 2 LRMA。该 LRMA可以不与链路 2 的 LRMZ 协商就分配 SNP 链路连接。

在情况 2 中，链路被子网 X 和子网 Y 共享，用于连接建立。来自子网 X 的 SNP 链路建立请求被发给邻近的 LRMA，由于在链路远端的另一个 LRMA 元件也可以分配 SNP 链路连接，因此 LRMA 可能需要与远端的 LRMZ 协商来完成分配。子网 Y 发送到邻近 LRMA 的连接请求过程与此类似。

7.4.3.1 LRMA

LRMA 负责管理 SNPP 链路的 A 端，包括对链路连接的指配和去指配，并提供拓扑和状态信息。LRMA 元件接口如图 30、表 7 和表 8 所示。

表 7 LRMA 元件接口(1)

输入接口	基本输入参数	基本返回参数
SNP 链路连接指配请求	请求 id SNP id(可选)	请求 id 一个 SNP id 对或拒绝
SNP 链路连接去指配请求	SNP id	确认或拒绝
配置	链路信息	—
翻译	本地 id	接口 id

表 8 LRMA 元件接口(2)

输出接口	基本输出参数	基本返回参数
SNP 协商 (只适用情况 2)	请求 id SNP id 列表	请求 id SNP id
SNP 释放 (只适用情况 2)	SNP id	确认
拓扑	链路信息	—

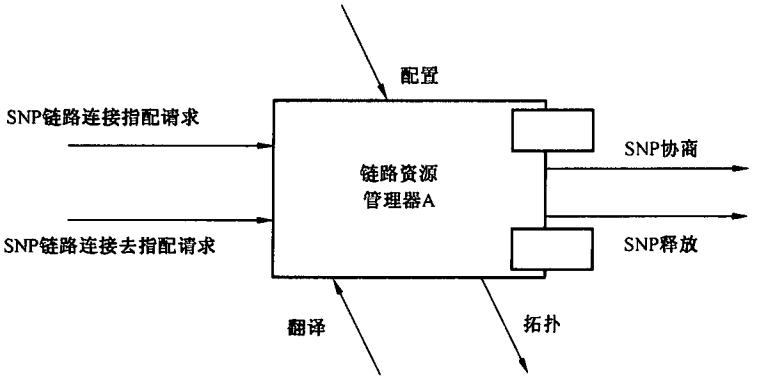


图 30 链路资源管理 A 元件

LRMA 元件接口的主要功能如下：

a) 指配链路连接

当收到一个指配链路连接的请求时，调用连接允许控制功能确定是否有足够的空闲资源来建立一个新的连接。连接允许也可以基于优先级或其他策略决定机制。

如果没有足够的资源，则拒绝请求。

如果有足够的资源可用，则连接请求被允许，其处理过程存在下列两种情况：

情况 1：由于 SNP 链路连接仅在 SNPP 链路的一端进行分配，LRMA 可以不与链路远端的 LRMZ 进行协商就选择 SNP 链路连接。

情况 2：由于 SNP 链路连接可以被 SNPP 链路任意一端的 LRMA 使用，LRMA 将一组可用的 SNP id 传到 LRMZ。LRMZ(与其本地的 LRMA 协调)选择一个 SNP，并将这个 id 返回到源的 LRMA。

b) 去指配链路连接

当接收到一个 SNP 链路连接去指配请求时，相应的 SNP 被标识为可用。在情况 2 中，需要通知相关的 LRMZ。

c) 接口 id 到本地 id 的翻译

如果需要，LRM 提供接口 id 到本地 id 的翻译。例如，如果 SNPP 链路的端点位于不同的路由区内，可以应用这个功能。

d) 拓扑

该功能通过接口 SNPP id 和其中包含的 SNP id 来提供链路拓扑信息。

该功能还能提供链路特性，如链路成本、路由分集和质量。一些属性(如链路成本)可能随链路利用率的不同而变化。修改链路特性的进程由一个本地策略控制。

7.4.3.2 LRMZ

LRMZ 负责管理 SNPP 链路的 Z 端，它也提供拓扑信息。LRMZ 元件的接口如表 9、表 10 和图 31 所示。

表 9 LRMZ 元件接口(1)

输入接口	基本输入参数	基本返回参数
SNP 协商人 (仅适于情况 2)	请求 id SNP id 列表	请求 id SNP id 或拒绝
SNP 去指配 (仅适于情况 2)	SNP id	确认
配置	链路信息	—
翻译	本地 id	接口 id

表 10 LRMZ 元件接口(2)

输出接口	基本输出参数	基本返回参数
拓扑	链路信息	—

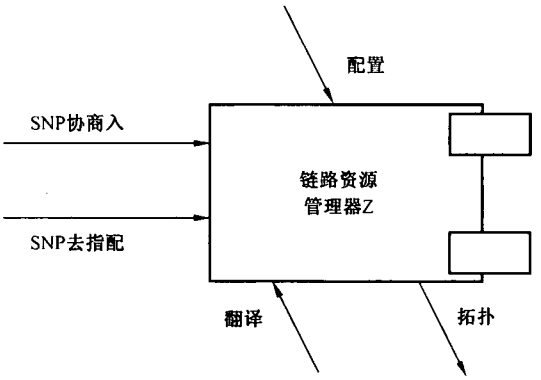


图 31 链路资源管理 Z 元件

LRMZ 元件的接口功能如下：

a) SNP 指配(仅用于情况 2)

当接收到一个可使用的 SNP 列表时，从中选择一个 SNP 并向 LRMA 返回此信息。

b) SNP 去指配(仅用于情况 2)

当关联的 LRMA 指示一个 SNP 已被去指配时，将该 SNP 标识为可用。

c) 接口 id 到本地 id 的翻译

如果需要，LRM 提供接口 id 到本地 id 的翻译。例如，如果 SNPP 链路的端点位于不同的路由区内，可以应用这个功能。

d) 拓扑

该功能通过接口 SNPP id 来提供链路拓扑信息。

7.4.4 流量策略(TP)

流量策略(TP)元件是策略端口的一个子类，它的作用是检查用户连接是否按照达成一致的参数来发送业务。当一个连接违反了达成一致的参数时，TP 可以采取措施进行修正。

流量策略元件对于连续比特率的传送层网络是不需要的，因此在本部分中不进行规范，同样 TP 策略接口也不在本部分中详述。

7.4.5 呼叫控制器

呼叫是通过呼叫控制器来控制的。呼叫控制器元件包括两类：

a) 主叫方/被叫方呼叫控制器：该控制器与呼叫终端相关，可以与终端系统在一起，或位于远端作为终端系统的代理。该控制器可以承担一个角色或同时承担两个角色，一个支持主叫方，另一个支持被叫方。

b) 网络呼叫控制器：网络呼叫控制器承担两种角色，一个支持主叫方，另一个是支持被叫方。

主叫方呼叫控制器和被叫方呼叫控制器通过一个或多个中间网络呼叫控制器进行交互。

7.4.5.1 主叫方/被叫方呼叫控制器

该元件的任务是：

a) 生成输出的呼叫请求；

b) 接受或拒绝输入的呼叫请求；

c) 生成呼叫终结请求；

d) 处理输入的呼叫终结请求；

e) 呼叫状态管理。

该元件支持的接口如表 11 和表 12 所示，图 32 描述了主叫方/被叫方呼叫控制器元件。

表 11 主叫方/被叫方呼叫控制器元件接口(1)

输入接口	基本输入参数	基本返回参数
呼叫接受	传送资源名称或 VPN 传送资源名称	呼叫请求的确认或拒绝
呼叫释放入	传送资源名称或 VPN 传送资源名称	呼叫释放的确认
呼叫修改接受	呼叫名称； 需要改变的参数	呼叫修改的拒绝或者确认

表 12 主叫方/被叫方呼叫控制器元件接口(2)

输出接口	基本输出参数	基本返回参数
呼叫请求	传送资源名称或 VPN 传送资源名称； 路由(可选，仅对 VPN 适用)	呼叫请求的确认或拒绝
呼叫释放出	传送资源名称或 VPN 传送资源名称	呼叫释放的确认
呼叫修改请求	呼叫名称； 需要修改的参数	呼叫修改的确认或拒绝

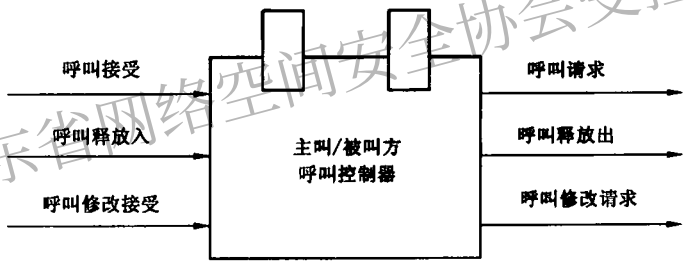


图 32 主叫方/被叫方呼叫控制器元件

呼叫请求：该接口用于发出呼叫建立、维护和释放的请求，它也接收一个呼叫请求的确认或拒绝。

呼叫接受：该接口用于接受输入的呼叫请求，它也确认或拒绝输入的呼叫请求。

呼叫释放：该接口用于发出、接收和确认呼叫释放请求。

呼叫修改请求：该接口用于发出一个修改已有呼叫的请求，它也接收该请求的确认或拒绝。

呼叫修改接受：该接口用于接受一个修改已有呼叫的请求，它也对该请求进行确认或拒绝。

同一个主叫方/被叫方呼叫控制器在不同的过程中，可以起到发起者或终结者的作用。

7.4.5.2 网络呼叫控制器

该元件的任务是：

a) 处理输入的呼叫请求；

b) 生成输出的呼叫请求；

c) 生成呼叫终结请求；

d) 处理呼叫终结请求；

e) 将 VPN 呼叫源和目的标识符转换为传送资源名称；

f) 基于呼叫参数、用户权利和访问网络资源的策略，进行呼叫允许控制；

g) 呼叫状态管理。

该元件的接口如表 13 和表 14 所示，并在图 33 中进行了描述。

表 13　网络呼叫控制器元件接口(1)

输入接口	基本输入参数	基本返回参数
呼叫请求接受	UNI 传送资源名称或 UNI 传送资源名称别名	呼叫请求的确认或拒绝
网络呼叫协调入	UNI 传送资源名称或 UNI 传送资源名称别名	确认或拒绝
呼叫释放入	UNI 传送资源名称或 UNI 传送资源名称别名	呼叫释放的确认
客户 NCC 协调入	可选的客户呼叫参数； 可选的客户层标识符； 传送资源名称	客户层中的一对 SNP
服务者 NCC 协调入	一对 SNP	确认或拒绝使用
呼叫修改接受	呼叫名称； 需要修改的参数	呼叫修改的确认或拒绝

表 14　网络呼叫控制器元件接口(2)

输出接口	基本输出参数	基本返回参数
呼叫指示	UNI 传送资源名称或 UNI 传送资源名称别名	呼叫请求的确认或拒绝
连接请求出	UNI 传送资源名称或 UNI 传送资源名称别名	一对 SNP
网络呼叫协调出	UNI 传送资源名称或 UNI 传送资源名称别名	呼叫请求的确认或拒绝
目录请求	UNI 传送资源名称或 UNI 传送资源名称别名	本地名称
策略出	呼叫参数	呼叫的接受或拒绝
呼叫释放出	UNI 传送资源名称或 UNI 传送资源名称别名	呼叫释放的确认
客户 NCC 协调出	客户层中的一对 SNP	确认或拒绝使用
服务者 NCC 协调出	可选的呼叫参数； 层标识符； 传送资源名称	一对 SNP
呼叫修改请求	呼叫名称； 需要修改的参数	呼叫修改的确认或拒绝

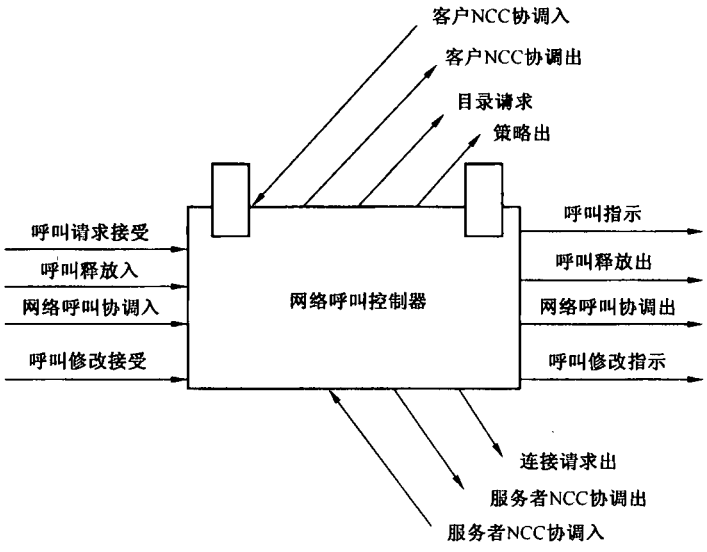


图 33　网络呼叫控制器元件

呼叫请求接受：该接口用于接受一个呼叫的源和目的标识对，它也确认或拒绝输入的呼叫建立请求。

连接请求出：该接口用于向连接控制器发送连接建立请求，来请求一个 SNP 对。

目录请求：该接口用于根据 UNI 传送资源名称或别名得到一个 SNPP 名称。对于别名，如果对应多个 SNPP，应根据策略决定返回哪个 SNPP。

网络呼叫协调：该接口用于网络级的呼叫协调。

呼叫释放入或出：该接口用于发送、接收和确认呼叫拆除请求。

策略出：该接口提供策略检查。

客户 NCC 协调入：该接口用于接受客户层 NCC 发出的对一个 SNP 对的请求。为 NCC 提供其所在层的源和目的标识符，使 NCC 能够为客户层提供网络连接。该接口返回一个适配到网络连接的客户层 SNP 对。客户还使用该接口释放或修改 SNP 对。NCC 返回该动作的结果。

客户 NCC 协调出：该接口用于向客户层提供一个适配到网络连接的客户层 SNP 对。客户层 NCC 指示它是否接受这个资源。服务者还使用该接口来释放或提供一个修改的 SNP 对。客户 NCC 返回该动作的结果。

服务者 NCC 协调出：该接口请求一个可被呼叫用于传递特征信息的 SNP 对(输入或输出)。它与连接请求出接口返回的参数相同，但不创建该层的一个网络连接。该接口也被用于释放或请求修改由服务层提供的 SNP 对。服务者 NCC 返回该动作的结果。

服务者 NCC 协调入：该接口用于接受由服务层 NCC 提供的一个 SNP 对(输入或输出)。它可能被接受或拒绝。服务者还使用该接口释放或提供一个修改的 SNP 对。NCC 返回该动作的结果。

呼叫修改接受：该接口用于接受一个呼叫修改请求。该接口也用于确认或拒绝一个输入的呼叫修改请求。

呼叫修改指示：该接口用于将一个呼叫修改请求继续传递到另一个 NCC。它也接收对该请求的确认或拒绝。

在主叫方网络呼叫控制器中，呼叫允许控制的任务是检查提供的被叫用户名称和业务参数是否有效。业务参数的检查是根据业务级别规范进行的。如需要，这些参数可以与主叫方呼叫控制器再次协商，协商范围由源自初始的业务级别规范得到的策略确定，而业务级别规范源自业务级别协议(SLA)。

在被叫方网络呼叫控制器中，如果存在呼叫允许控制，其任务是根据主叫方和被叫方的服务合同来检查被叫方是否有权接受呼叫。例如，主叫方的地址被屏蔽，该呼叫会被拒绝。

7.4.5.3 呼叫控制器交互

呼叫控制器元件之间的交互作用取决于呼叫和连接的类型，如下所述：

交换连接：主叫方呼叫控制器(与一个终端关联)与网络呼叫控制器交互而产生一个输入呼叫；网络呼叫控制器与被叫方呼叫控制器(与一个终端关联)交互而产生一个输出呼叫。网络呼叫控制器与连接控制器交互作用来提供呼叫。图 34 举例说明了这种交互关系。需要注意的是，主叫方/被叫方呼叫控制器和与网络呼叫控制器相关联的连接控制器之间没有直接的交互。

图 34 表示在入口网络呼叫控制器请求连接之前，被叫方呼叫控制器先接受呼叫的情况。图 35 所示表示呼叫请求发送时就建立连接的情况。

软永久连接：网管系统可以看作是同时包含主叫方/被叫方呼叫控制器。网管系统发出配置命令给主叫方呼叫控制器，主叫方呼叫控制器将呼叫配置命令发送到控制平面，启动控制平面的网络呼叫控制器。控制平面对呼叫配置命令的响应，被管理平面看作是呼叫建立的确认。这表示一个没有业务的空呼叫。管理平面和控制平面之间的协议是指令和指令响应接口。其交互过程如图 36 所示。

代理呼叫：主叫方/被叫方呼叫控制器通过呼叫协议与网络呼叫控制器交互，但与用户之间并不发生协议交互。

图 37 举例说明了网络呼叫控制器之间为支持呼叫允许控制策略所需的交互。

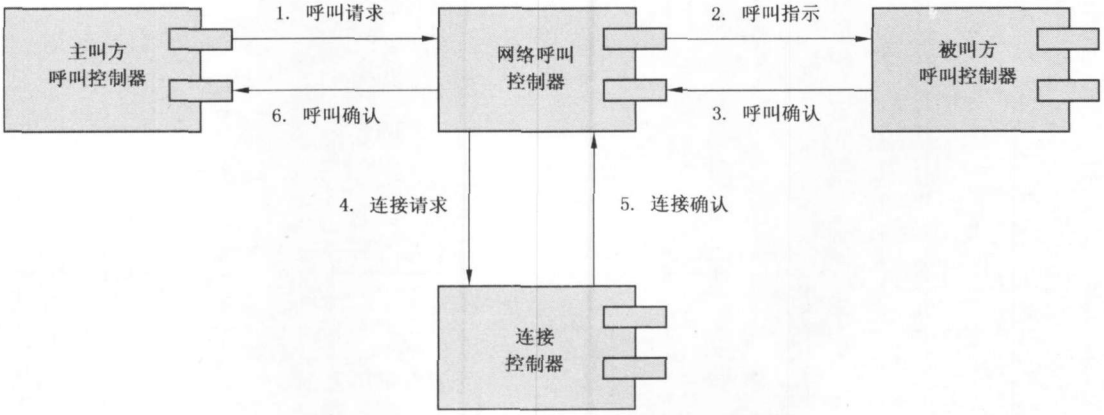


图 34　对于交换连接的主叫方/被叫方呼叫控制器的交互作用:示例 1

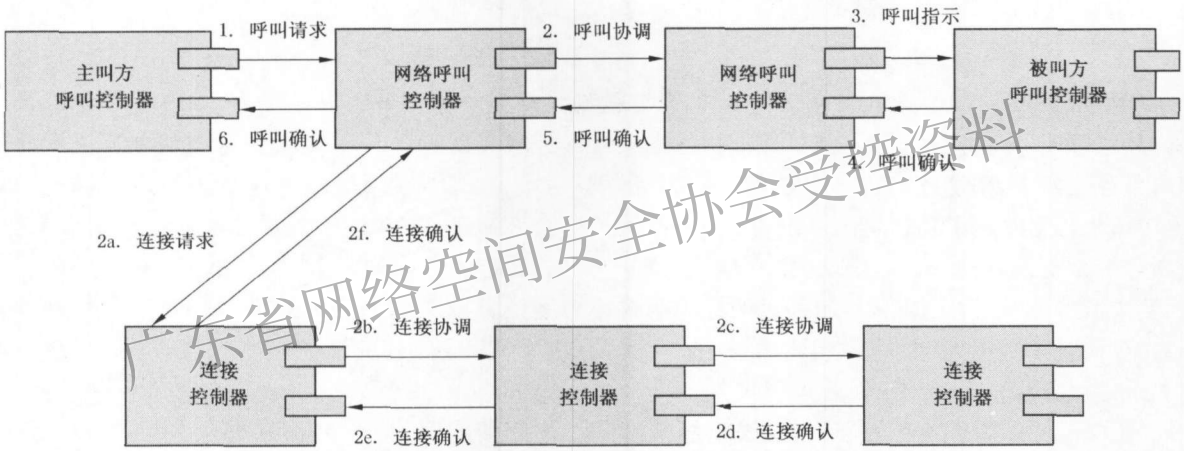


图 35　对于交换连接的主叫方/被叫方呼叫控制器的交互作用:示例 2

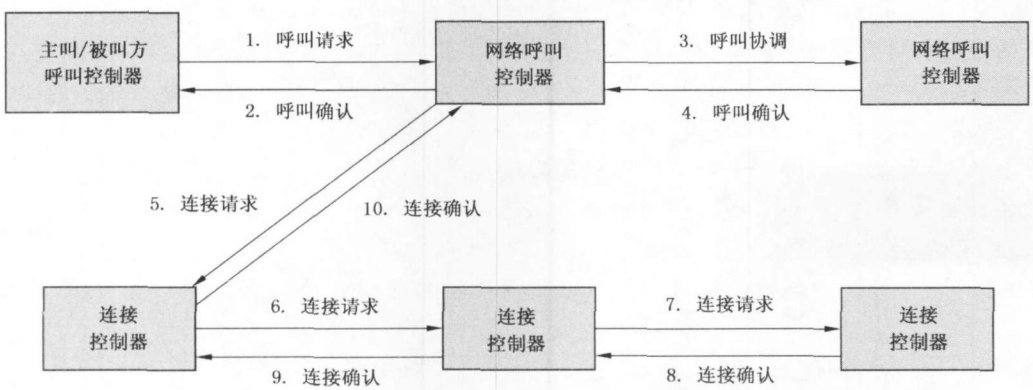


图 36　对于软永久连接的呼叫控制器的交互作用

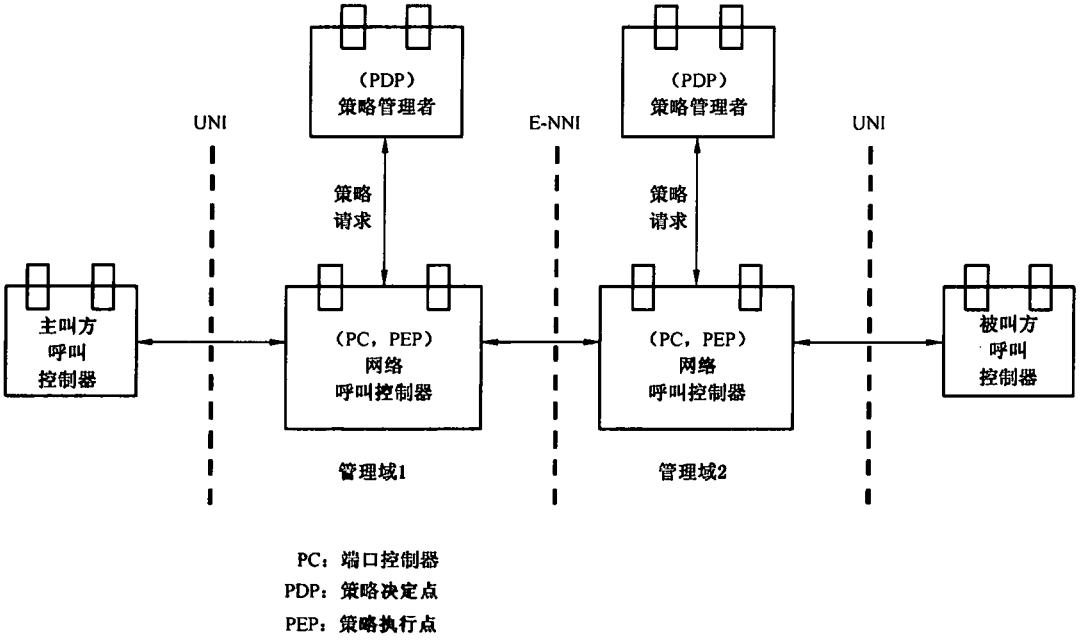


图 37　呼叫允许控制策略交互作用举例

分层呼叫：不同层的两个 NCC 可以协作以便在服务层支持客户 CI。该操作可以从服务层发起，或者向服务层发出，取决于该操作是从哪一层开始的。一个 NCC 向服务层 NCC 发送的请求，将返回与“连接请求出”接口相同的结果。不同之处是产生了一个与服务者 NCC 的关联。该动作的结果是使用或创建一个支持客户 NCC 的服务层呼叫段。如果使用“服务者 NCC 协调出”或“客户 NCC 协调入”接口，要求服务层创建一个呼叫，源和目的标识符将作为呼叫参数。如果确定服务层的连接可正确进行，则对“呼叫请求接受”接口执行相同的操作。服务层 NCC 可以递归使用“服务者 NCC 协调出”接口，向它的下一服务层的 NCC 请求一个 SNP 对。

NCC 也可以向客户层发起操作，提供可被客户层用于传递客户 CI 的一个 SNP 对。这种情况下，将使用“客户 NCC 协调出”或“服务者 NCC 协调入”接口。使用了这些接口后，提交的 SNP 对可以开始传递客户 CI，而在服务层不需进行任何呼叫动作。这种情况适用于服务层已经建立起一个呼叫，并随后提供给客户层。客户层可以接受或拒绝使用服务层提供的 SNP 对。

7.4.5.4　呼叫修改

呼叫提供的业务可以被一个 CCC 或者 UNI 上作为 NCC 的网络管理应用发起的动作修改。修改的程度由运营策略来决定，该策略可以与终端用户共享（如通知用户允许什么样的带宽增长），也可不与终端用户共享。呼叫修改应符合下列原则：

a)　在 UNI 处与该呼叫关联的 CI 不能被修改；

b)　在 UNI-N 处与该呼叫关联的链路连接终端点不能被修改。

修改操作可以是对一个呼叫段进行修改，而 NCC 保持不变；或者是在整个呼叫中创建或删除某些呼叫段，这时相应的 NCC 将被创建或删除。

在 UNI 处可以修改的参数包括：带宽（如以太网呼叫的速率）、呼叫涉及的 CCC 的数量（如多方呼叫）等。

收到 UNI 呼叫修改请求后，网络内可能发生的事件举例如下：

- 改变支持一个以太网业务的虚级联（VCAT）呼叫所关联的服务层连接数量；
- 响应一个提高呼叫的可用性的请求，增加一个额外的连接来创建 1+1 配置。

7.4.6　发现代理（DA）

发现代理的联邦工作在传送平面的名称空间，并提供对传送平面名称空间和控制平面名称空间的

隔离。发现代理联邦了解网络中的连接点(CP)和终端连接点(TCP),而一个本地 DA 仅了解分配给它的那些点。

发现协调包括接受关于预先存在的 CP 和链路连接的潜在提示信息。DA 掌握 CP-CP 链路连接信息,使 SNP-SNP 链路连接能够被绑定到 CP-CP 链路连接。解析接口可以协助发现过程,提供从全局 TCP 句柄到负责该点的 DA 地址的名称翻译,以及提供 TCP 的本地名称。提示信息可通过与其他元件的协作获得,或者来自于外部指配系统。发现代理没有专门的设备接口,并可位于任何适当的平台上。

表 15 发现代理(DA)元件接口(1)

输入接口	基本输入参数	基本返回参数
协调入	—	—
提示信息入	CP 对	—
解析请求	TCP 名称	—

表 16 发现代理(DA)元件接口(2)

输出接口	基本输出参数	基本返回参数
协调出	—	—
CP 链路连接	CP 对	—
解析结果	—	DA DCN 地址、TCP 索引

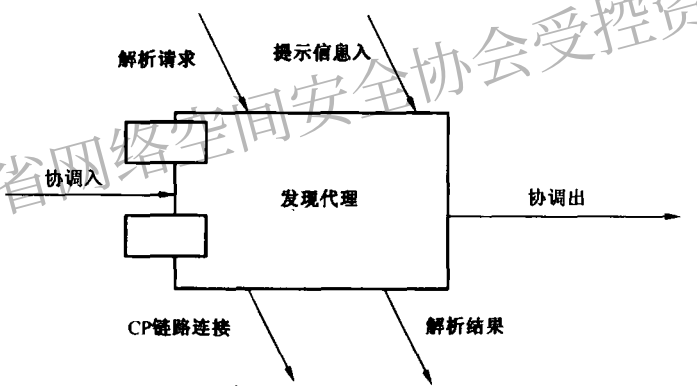


图 38 发现代理元件

7.4.7 终端和适配执行器(TAP)

终端和适配执行器(TAP)位于提供适配和终端功能的设备上。它为控制平面(LRM)提供支持 SNP 的链路连接的资源视图,并隐藏所有适配和终端控制的硬件和技术细节。

TAP 工作在两个不同的时间,并提供两种不同的功能。当一个资源分配给控制平面时,将配置 TAP 到 SNP 的一个绑定,并由此在 LRM 范围内创建一个 SNP(在链路的一端)。如果该资源在多个控制平面之间共享(例如不同的层网络或不同的 L1 VPN),则 TAP 要保存一个绑定列表。TAP 控制一个 CTP 和代表该 TAP 范围内任意资源的每个 SNP 之间的绑定。表示绑定关系的 SNP 状态如表 17 所示。

表 17 SNP 绑定状态

状态	描　　述
忙	允许绑定,所代表的资源当前被分配给另一个控制平面或管理平面
潜在的	允许绑定,所代表的资源当前没有被分配给任何一个控制平面或管理平面
分配的	允许绑定,资源被配置和分配给该 LRM

表 17（续）

状态	描　　述
关闭	TAP 通知资源必须在一个确定的时间内被返回，例如： 立刻（中断当前的呼叫）； 很快的（在丢弃前重路由呼叫）； 下一个维护窗口； 当呼叫已被丢弃
释放	LRM 不再使用该资源

当 SNP 处于分配的状态时，TAP 必须正确的配置资源（例如多种适配），并把代表同一个资源的其他 SNP 的状态设置为忙。

当 SNP 链路连接被绑定到相应的 CP 链路连接时，TAP 负责保持该 SNP-CP 绑定。当建立 CP 链路连接时，本地 TAP 与远端 TAP 合作来协调多种适配或其他问题。

如果 LRM 希望使用一个处于潜在的状态的 SNP 来满足一个连接请求，那么在连接建立期间，一对 TAP 要通过 LRM 来协调链路连接所需的适配功能。

TAP 提供链路连接传输状态信息，并接受链路状态信息来保证与管理平面指示的一致性。管理平面的一致性包括保证链路连接告警状态的一致性，从而不会产生或报告虚假告警。

表 18　终端和适配执行器（TAP）元件接口（1）

输入接口	基本输入参数	基本返回参数
LC 连接状态（SNP-SNP）	枚举：在线、离线	—
协调入	技术相关	—

表 19　终端和适配执行器（TAP）元件接口（2）

输出接口	基本输出参数	基本返回参数
LC 传送状态（SNP-SNP）	枚举：Up、Down	—
协调出	技术相关	技术相关
控制	特定硬件的	特定硬件的

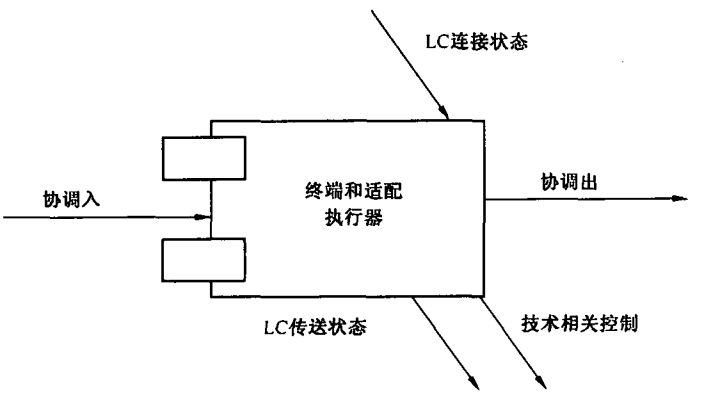


图 39　终端和适配执行器元件

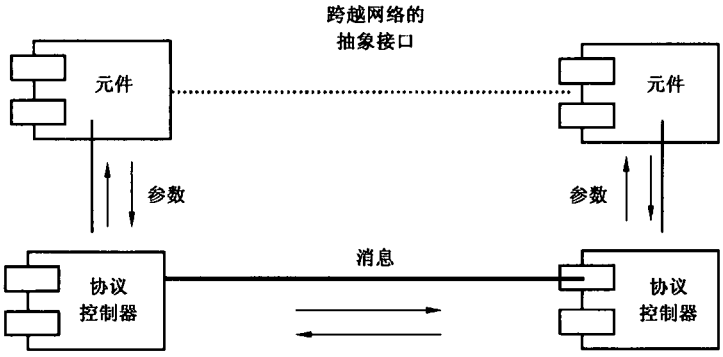
7.4.8　协议控制器（PC）

协议控制器的功能是将控制元件抽象接口的参数映射到接口互联协议所承载的消息中。协议控制器是策略端口的一个子类，并提供与这些元件相关的所有功能。PC 能够向其监视端口上报协议违例。PC 还支持将几个抽象接口复用到单个协议实例中，如图 40 所示。协议控制器的细节属于协议设计的

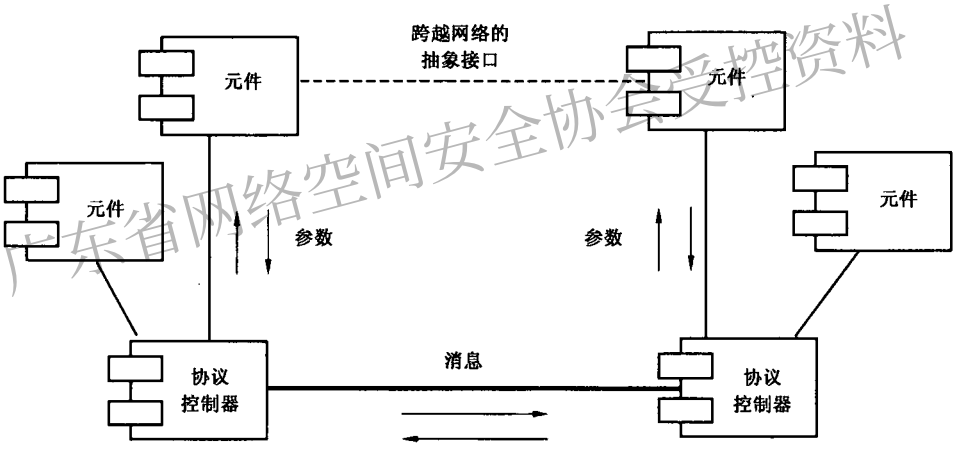
范畴，因此本部分中仅给出几个示例。

传送协议控制器的任务是通过一个定义好的接口为控制原语提供授权、安全和可靠的跨越网络的传递。控制器的处理过程允许被追踪，并且保证接收到预期的反馈，或向发起者上报异常。协议控制器在提供安全功能时，将通过其监视端口来上报安全违例。

在连接控制器和协议控制器之间进行信令原语传递，需要与外部交互协议消息，所以协议控制器在语义上对消息原语是透明的。信令消息在两个协议控制器之间传递的过程如图 41 所示。

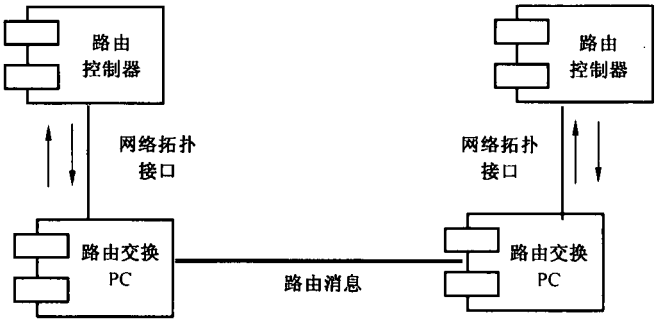


a） 协议控制器元件的一般应用



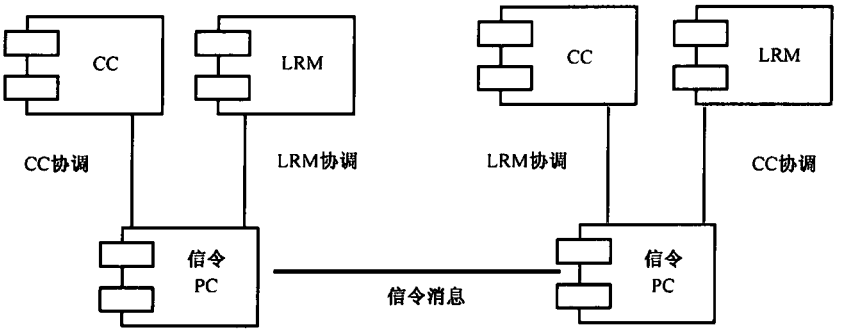
b） 将多个不同的原语流复用到单个协议中

图 40 协议控制器



a） 使用路由交换 PC 进行路由表交换

图 41 协议控制器应用举例



b) 使用信令 PC 对 LRM 和 CC 协调进行复用

图 41（续）

使用协议控制器传递的信息，包括以下实例：

a) 通过路由交换协议控制器传递路由表更新消息（如图 41(a)所示）；

b) 通过链路资源管理器的协议控制器传递链路资源管理器协调消息（适用于可用比特率连接）；

c) 通过连接控制器的协议控制器传递连接控制协调消息，如图 41(b)所示。LRM 和 CC 的协调接口可复用到同一个协议控制器。

8 呼叫和连接控制要求

8.1 呼叫和连接的分离

呼叫是表示为一个网络层次的用户提供的服务，连接是网络用于提供该服务的一种手段。ASON 控制平面规范了呼叫和连接控制的分离，目的是减少中间连接控制节点的冗余呼叫控制信息。

呼叫控制功能在网络入口（即 UNI 参考点）或在域间的网关处（即 E-NNI 参考点）提供，中间设备仅需要支持连接控制功能，而不需要提供呼叫控制功能。域边界的呼叫控制器根据运营者定义的域间交互策略来执行操作。根据呼叫是否穿越多个域，一个端到端呼叫可能由多个呼叫段组成，这允许在不同域中灵活地选择信令、路由和恢复机制。

8.2 连接类型

根据提供连接的能力和方向，ASON 的呼叫和连接管理应支持：

- 单向点到点连接；
- 双向点到点连接；
- 单向点到多点连接。

此外，还可能存在另一种连接类型，称为不对称连接。这种连接可以由两个单向点到点连接构成，这两个连接在各自的方向有不同的特性；或者这种连接可作为一个双向连接的特殊情况。

根据控制连接建立的主体不同，呼叫和连接管理支持以下三种基本连接类型：

a) 永久连接（PC）：是一种由管理系统配置的连接类型，又称为指配型连接。这种连接是将路径上的每一个网元都按指定的信息进行配置，从而建立端到端连接，指配由网管系统或人工干预来完成。如果使用了网管系统，通常首先要求接入到网络的数据库模型，建立最适合的路由，然后向支持该连接的网元发送命令。永久连接的建立如图 42 所示。

b) 交换连接（SC）：是一种由终端用户请求而建立的连接，又称为信令型连接。这种连接是由控制平面的通信终端点利用信令协议消息交换建立的连接。这些消息流通过控制平面内的 I-NNI 或E-NNI。交换连接的建立如图 43 所示。

c) 软永久连接（SPC）：是一个用户到用户的连接，其中端到端连接中的用户到网络部分是通过网络管理系统建立的一个永久连接（PC），而端到端连接的网络部分是通过控制平面建立的一个

交换连接。在连接的网络部分，连接建立的请求是由管理平面发起，而由控制平面执行。这种连接又成为混合型连接。从终端用户的角度来看，软永久连接与网管控制的永久连接相同。软永久连接的建立如图 44 所示。

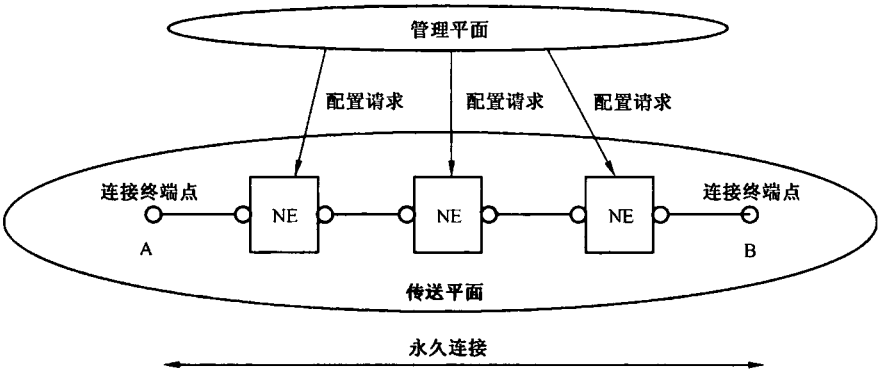


图 42　建立端到端永久连接示意图

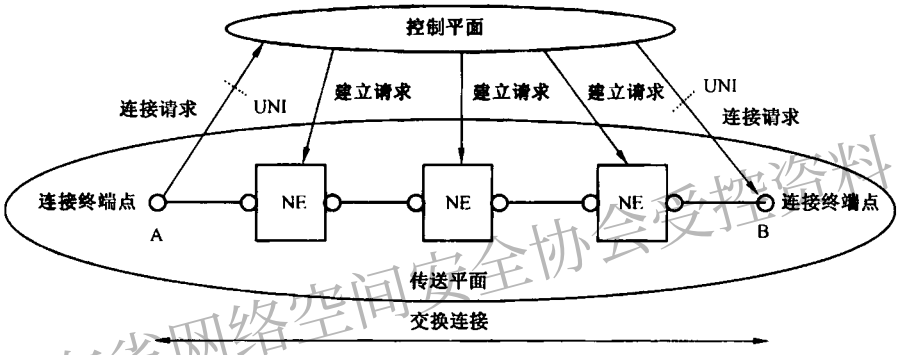


图 43　建立端到端交换连接示意图

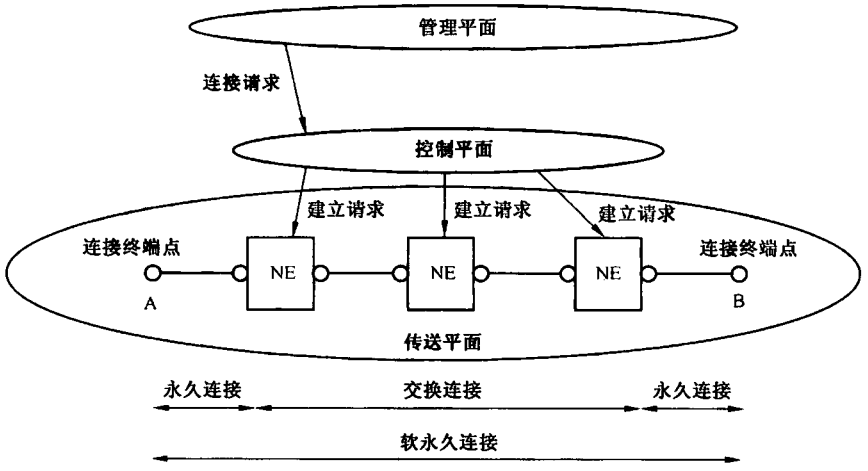


图 44　建立端到端软永久连接示意图

8.3　呼叫和连接控制功能

8.3.1　呼叫控制功能

呼叫控制是在一个或多个用户应用和网络之间的一个信令功能，用于控制建立、释放、修改和维护连接组。呼叫控制用于维护多方之间的关系。一个呼叫在任意时间可关联任意数量的潜在连接，一个呼叫也可不关联任何连接。

呼叫控制可通过下列方法之一来实现：

a) 将呼叫信息分解成若干个参数，这些参数由同一个呼叫或连接协议消息来承载。在实现呼叫/连接的协议中，根据不同的参数区分呼叫和连接控制信息。

b) 呼叫控制和连接控制采用不同的状态机，而信令消息采用同一个信令协议。

c) 通过不同的信令协议实现呼叫控制和连接控制，区分信息和状态机。

呼叫控制必须提供连接之间（在一个多连接呼叫中）的协调以及呼叫方之间（多方呼叫）的协调。为了协调多个连接，需要在网络中进行下列动作：

——所有的连接必须被选路，因此它们可被至少一个呼叫控制实体监控；

——呼叫控制关系的建立应在连接建立之前进行。当与一个呼叫关联的所有连接被拆除后，才可以释放这个呼叫。一个呼叫也可在没有任何连接的情况下存在（有利于复杂的连接重整）。

一个呼叫可分为三个阶段：

a) 建立：在该阶段，在用户和网络之间交换信令消息来协商呼叫特性。在主叫方和网络之间的信令消息交换被称为一个输出呼叫。在网络和被叫方之间的信令消息的交换被称为一个输入呼叫。

b) 激活：在该阶段，数据可在呼叫关联的连接上交换，呼叫参数可被修改（例如，在一个点到多点的呼叫中增加新的呼叫方）。

c) 释放：在该阶段，信令消息在主叫方、被叫方和网络之间交换，以结束该呼叫。一个呼叫可由主叫方或被叫方释放，或通过代理、网络管理来释放。

8.3.2 呼叫允许控制功能

呼叫允许控制是一个可选功能，它是由网络中的呼叫方发起的一种策略功能，可能需要与网络中的被叫方进行协作。一旦呼叫被允许，说明该呼叫可请求一条或多条连接，但并不表明任何一条连接请求将会成功。呼叫允许控制也可在其他网络边界调用。

发起方的呼叫允许控制功能负责检查是否提供了有效的被叫用户名和参数，并根据服务级别规范（网络运营商和客户之间为某个特定业务而达成的一组参数和价格，表明了业务的范围）来核对业务参数。如果需要，这些参数可与发起的用户重新协商。协商的范围由业务级别规范中的策略来确定，该规范来源于业务级别协议（SLA）。

终结方呼叫允许控制功能负责依据呼叫方和被叫方之间的服务合同来检查被叫方是否有资格接受该呼叫。例如，一个呼叫方地址可被屏蔽。

8.3.3 连接控制功能

连接控制负责全面控制一个连接，即与一个连接相关的建立、释放以及连接状态的保持，并通过协议来实现。ASON 的连接控制过程如下：

a) 连接建立和验证。连接建立涉及多个属性，根据请求的业务类型，这些属性可以有选择的提供。运营者可在向用户提供连接前根据业务级别协议来验证该连接。

b) 数据转发。

c) 连接释放。

ASON 的连接控制功能包括：

- 连接建立；
- 连接释放；
- 连接状态维护；
- 连接属性查询；
- 连接属性修改；
- 保护和恢复（注：保护和恢复要求参见第 15 章）。

此外，连接控制还可以支持一组连接。

8.3.3.1 连接建立

连接建立功能是在两个或者多个端点间，建立一条具有特定属性（由用户或策略管理者确定）的连接。连接建立应满足以下要求：

a) 控制平面应支持跨域的连接建立请求。

b) 控制平面应支持基于策略处理连接建立的请求。

c) 收到连接请求后，控制平面应生成一个与该连接相关的网络唯一的连接 ID，用于信息获取或者其他有关该连接的动作。

d) 收到一个连接请求后，控制平面应通过 CAC（连接允许控制）过程，确定下游子网是否有可用资源来建立这条连接。

e) 控制平面应向管理平面上报连接请求成功/失败的通知。

f) 当一个连接请求成功时：

1) 一条连接被成功建立后，应返回一个肯定的确认。

2) 肯定确认应通过 NNI 或者管理平面（如果连接请求从管理平面发出）同时向上游和下游发送。

g) 在一个连接请求失败时：

1) 控制平面应向管理平面报告一个原因代码，指示失败的原因。

2) 应返回一个包含适当错误代码的否定确认。

3) 所有分配的资源应被释放。

4) 原因代码应包含足够信息，以便采取修正措施。

h) 在建立连接过程中，应支持发起一次以上的连接建立尝试。为了解决拥塞问题，控制平面元件应能限制连接建立请求尝试次数。

8.3.3.2 连接释放

连接释放功能应满足以下要求：

a) 控制平面应支持通过连接 ID 发起连接释放请求。

b) 不论连接是否已经建立，控制平面应允许管理平面对任意连接发起连接释放请求。

c) 连接释放结果应上报管理平面。

d) 对于交换连接和跨域的连接，控制平面应允许任意端点或者中间节点发起连接释放过程。

e) 在连接释放完成后，所有与该连接相关的资源应被释放。在网络中不能存在被部分拆除而残留的连接。

f) 管理平面应能够根据需要强制释放控制平面建立的连接。

g) 连接释放请求应使用端到端确认。

h) 连接释放不应引起任何保护或者恢复动作。

8.3.3.3 连接状态维护和属性查询

连接状态维护和属性查询功能应满足以下要求：

a) 控制平面应维护在其控制下的呼叫、连接的当前状态。

b) 控制平面应支持管理平面及其相邻设备（客户或中间节点）发起请求查询连接属性或者状态。

8.3.3.4 连接属性修改

连接修改是一个可选功能，它对一条已经建立连接提供特定连接属性的修改。该功能可使运营商提供一些新业务，使光传送网在提供传统业务的同时，更适应以数据为主的业务。

属性修改功能应不引起业务或者网络的中断。因此某些属性不允许修改，例如编码类型、透明性、逻辑端口标识或者端点。可修改的属性包括：

- 带宽；
- 业务等级；

- 恢复优先级。

连接属性修改功能应满足以下要求：

a) 只允许接受非破坏性的属性修改请求。

b) 任何连接的属性修改作为一个网络可配置的操作应根据已建立的策略和 SLA 执行。

c) 属性修改不应引起连接失效。

d) 控制平面应向管理平面上报一个连接修改请求成功/失败的通知。

e) 如果一个连接修改失败：

1) 控制平面应向管理平面报告一个原因代码，指示失败的原因。

2) 经过 UNI 或者 NNI 返回一个否定确认。

3) 已经分配的修改的资源应被释放。

4) 连接应维持其初始属性。

f) 当一个连接被成功修改后，应经过 UNI 或者 NNI 接口返回一个肯定确认。

g) 属性修改不应引起网络启动保护或恢复。

h) 如果属性修改影响了资源分配，控制平面在属性修改后应更新资源可用性。

i) 属性修改可作为网络提供的一种业务。业务发现协议应支持发现网络支持属性修改的能力。

j) 属性修改应支持通过发起带宽修改请求，实现带宽增加和减少功能。

k) 属性修改应作为一种可计费的事件，控制平面应把所有相关信息传递给管理平面。

8.3.4 连接允许控制功能

连接允许控制(CAC)本质上是一个决定是否有足够资源来接纳一个连接(或在一个呼叫过程中重新协商资源)的过程。对于用户认证和控制网络资源的接入来说，连接允许控制是必需的。

连接允许控制的执行通常根据本地条件和策略逐段链路进行，对一个简单的电路交换网络，这可能简化为是否有可用的空闲资源。相反，对于有许多服务质量参数的分组交换网络如 ATM，连接允许控制需要保证新连接的允许应与现有连接的服务质量协议一致。否则，连接允许控制可能拒绝这个连接请求，连接的拒绝可根据能提供的空闲容量、优先权机制或其他策略决定。

连接允许控制功能应满足以下要求：

a) 控制平面功能应提供连接允许控制功能。

b) 连接允许控制功能应确定网络是否有足够的空闲资源可以允许一条新的连接。

1) 如果有足够的可用资源，CAC 可以允许连接请求的继续传送。

2) 如果没有足够的可用资源，CAC 将向连接请求的发起者发送适当的通知，指示请求被拒绝。

c) 连接允许控制功能应决定网络是否具有足够的可用资源允许连接修改操作。

8.4 竞争处理要求

竞争是当两个独立的连接请求同时申请相同的资源时发生的问题。控制平面中未解决的竞争可能引起呼叫阻塞。控制平面应具有相应机制避免或减少竞争的发生。在发生竞争时，控制平面应具有竞争解决机制。

竞争解决的一般要求如下：

a) 当发生竞争时，在网络有资源的情况下应保证其中一方成功，失败的一方在返回一个连接请求的否定确认之前，应进行 1～N 次竞争解决尝试。

b) 如有未解决的资源竞争，则相关请求的信令不能在网络中继续传送。

c) 如有未解决的资源竞争，则控制平面不应执行相关请求的交叉连接配置。

d) 在所有必要的确保请求完成的步骤成功实施以前，不应发送响应。

e) 解决竞争的尝试不应出现无限循环现象。

f) 竞争解决机制必须尽量减少控制信令和时延开销。

8.5 异常处理要求

ASON 网络中会发生不同层次的异常情况，影响呼叫和连接控制，例如：

- 信令通信网缺陷引起通信信道中断；
- 通信信道缺陷引起组成控制器的不同代理的失效，例如连接建立代理失效；
- 呼叫/连接控制器故障(例如超时、未发送确认等)；
- 连接允许控制故障；
- 路由控制器故障；
- 链路资源管理器故障；
- 不可识别的信令消息；
- 传送平面(包括链路连接和子网连接)故障等。

控制平面应提供呼叫和连接控制的异常处理功能，从这些异常中恢复：

a) 控制平面应支持分布式呼叫和连接控制的异常处理，并符合 ITU-T G.7713 的要求。

b) 呼叫/连接建立过程中的异常，应引起呼叫建立拒绝。为清除所有状态，应通过释放请求来释放已经分配的连接。

c) 对于已经存在的呼叫/连接，各种故障将可能影响呼叫。对于控制平面的部分故障或全部故障，不应影响已建立的呼叫和连接。对于传送平面资源失效，恢复进程可以启动对连接的保护恢复(这主要依赖呼叫的特征，例如呼叫的 CoS/QoS，路由类型)。如果保护恢复不成功，应向管理系统发送通知。呼叫仍然保持，直到收到显式的释放消息。

d) 在连接释放请求过程中，应支持释放请求的异常处理。在释放操作期间由于异常引起部分连接未拆除，连接控制器应将相应的异常情况通知管理平面，允许管理平面对部分未释放的连接进行清除。应允许用户采用其他手段释放呼叫，如手动方式。由于客户计费与呼叫状态有关，客户发出的释放命令应得到释放确认。

8.6 信令协议功能和协议选择

分布式呼叫和连接控制管理通过信令协议完成，以实现端到端连接的建立、修改、状态查询、释放以及保护恢复。信令协议功能应满足以下要求：

a) 信令协议功能应遵循 ITU-T G.8080 和 ITU-T G.7713。

b) 信令协议应支持对每个呼叫和连接的全局唯一标识。

c) 信令协议应支持所有的呼叫和连接属性。

d) 信令协议应对所有请求进行肯定或否定的响应，必要时包括原因。

e) 信令协议应支持显式路由方式，可采用严格显式路由或松散显式路由方式。

f) 应支持单一连接和一组连接两种连接管理方式，包括连接的建立、拆除和查询等。

g) 信令协议应支持故障通告，以及呼叫和连接状态的通告。

h) 信令协议应支持回溯机制(Crankback)，即回溯到中间节点(一般是域边界节点)或是回溯到源节点进行重路由。当连接建立失败时，回溯机制允许避开阻塞的节点或链路并重新尝试连接建立。回溯机制还可以用于对连接的保护和恢复，通过指示失效节点或链路的位置，重新尝试连接恢复，提高恢复率。回溯功能应满足以下要求：

   1) Crankback 重试的次数应可设置。

   2) 任何一次域内的 Crankback 和造成 Crankback 的原因都要向管理平面上报。

   3) 信令协议可支持动态的、不同程度的 Crankback，可以回溯到源节点或中间节点进行重路由。对于回溯到中间节点(一般是域边界节点)的方式，在 Crankback 过程中信令的控制权应依次向上游传递，由上游节点尝试重新建立这个连接。

   4) 具有后向兼容的能力，没有 Crankback 能力的节点，不对 Crankback 相关消息做处理，继续向上回溯。

   5) 支持域内和域间的 Crankback。

对于 ASON 网络内的所有控制域，域间信令协议应与域内信令协议的选择无关，UNI、I-NNI 和 E-NNI 接口的信令协议选择应相互独立。

a) UNI 接口涉及 ASON 网络与客户设备的互联互通，因此应采用统一的信令协议 RSVP-TE。UNI 接口的信令协议应符合 OIF 关于用户—网络接口的信令规范的要求。

b) E-NNI 接口涉及 ASON 网络中不同域之间的互联互通，因此应采用统一的信令协议 RSVP-TE。

c) I-NNI 接口为域内部接口，一般由单一供应商的设备组成。因此 I-NNI 接口信令协议，可以采用 PNNI、RSVP-TE、CR-LDP 三种协议的任何一种，应分别符合 ITU-T G.7713.1、ITU-T G.7713.2 和 ITU-T G.7713.3 的要求。

d) UNI、E-NNI 和 I-NNI 接口如果选择了不同的信令协议，应在接口上提供不同协议转换的网关功能。

9 路由要求

9.1 ASON 路由结构

9.1.1 路由功能结构和元件

ASON 路由功能用于为跨越一个或多个运营商网络的连接建立提供选路服务。路由功能包括可达性信息传播、网络拓扑/资源信息发布以及通道计算。

ASON 路由功能结构包括与协议无关的元件，如路由控制器(RC)和链路资源管理器(LRM)，以及与协议相关的元件，如协议控制器(PC)。路由控制器负责处理路由所必需的抽象信息。协议控制器根据信息交换所经过的参考点(如 E-NNI，I-NNI)，处理与协议相关的消息，并将路由原语传递给路由控制器。图 45 给出了路由功能结构和元件的示意图。

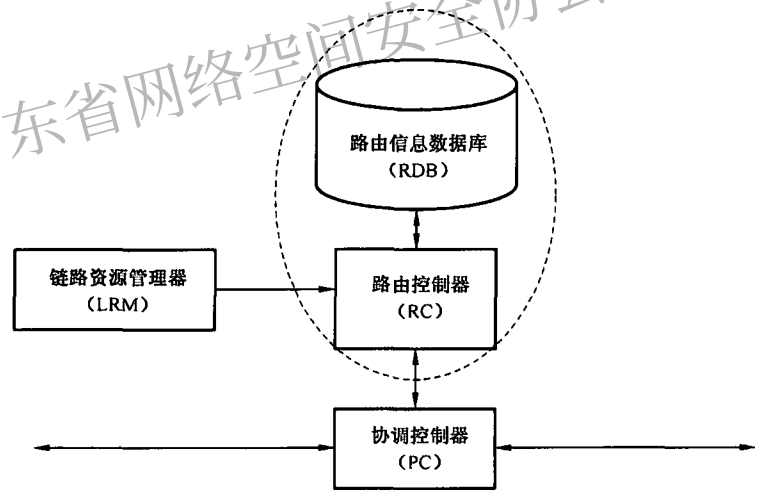


图 45 路由功能元件关系图

ASON 路由结构中各功能元件的作用如下：

a) 路由控制器：RC 功能包括与对等的 RC 交换路由信息，并通过操作路由信息数据库对路由查询(通道选择)进行响应。RC 与具体协议无关。

b) 路由信息数据库(RDB)：RDB 负责存储本地拓扑、网络拓扑、可达性和其他通过路由信息交换获得的路由信息，还可以包括配置信息。RDB 可以存储多个路由区的路由信息。路由控制器可以接入 RDB 的一个视图，图 45 中虚线框表示了这种关系。RDB 与具体的协议无关。因为 RDB 可以包含多个路由区(也可能是多层网络)的路由信息，因此访问 RDB 的路由控制器可以共享路由信息，如图 46 所示。

c) 链路资源管理器：LRM 负责向 RC 提供所有相关的 SNPP 链路信息。LRM 将其控制的链路资源的任何状态改变通知 RC。

d) 协议控制器：PC 将路由原语转换成特定的路由协议消息，因此 PC 是与协议相关的。PC 还处理路由信息交换和与协议相关的控制信息。在一个路由区中，有可能采用多种路由协议。

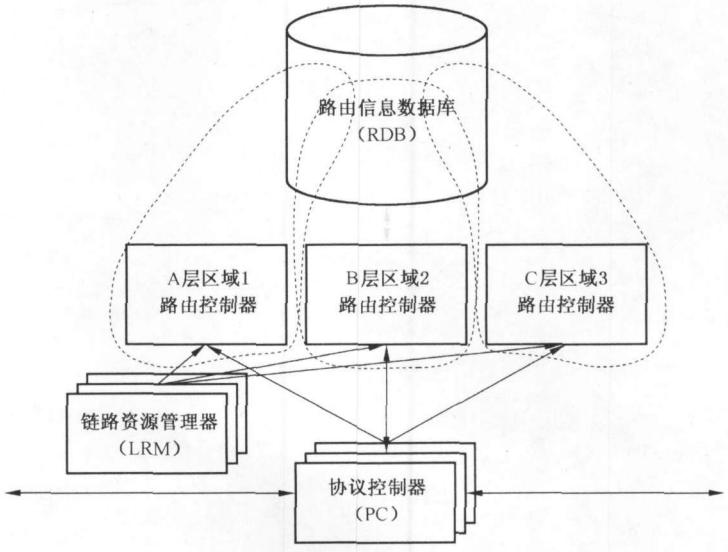


图 46 多路由域中 RDB 与 RC 的关系

9.1.2 分级路由结构

运营商可以根据地域、管理、技术等运营策略，把网络分为提供路由服务的多个路由区。路由区提供路由信息抽象，使路由信息的表示具有可扩展性。路由区可以进一步划分为更小的路由区，从而构成分等级的路由层次。

路由区需要通过路由执行器(RP)(路由控制器的联合)提供服务，每个 RP 只负责一个路由区。路由分级结构中，每个层面可以使用支持不同路由模式的 RP。

RP 通过分布式的路由控制器来实现。路由控制器提供路由服务接口，即业务接入点。RC 同时负责路由信息的协调和分发。路由控制器服务接口在路由分级层面上经由 NNI 参考点提供路由服务。

路由控制器可以作为一组分布式实体实现，这样的一组实体被称为路由控制域(RCD)。路由控制域是一个抽象实体，它隐藏了内部的分布细节，而提供与那些 RC 分发接口具有相同特性的分发接口。

RA、RP、RC 和 RCD 之间的关系如图 47 所示。

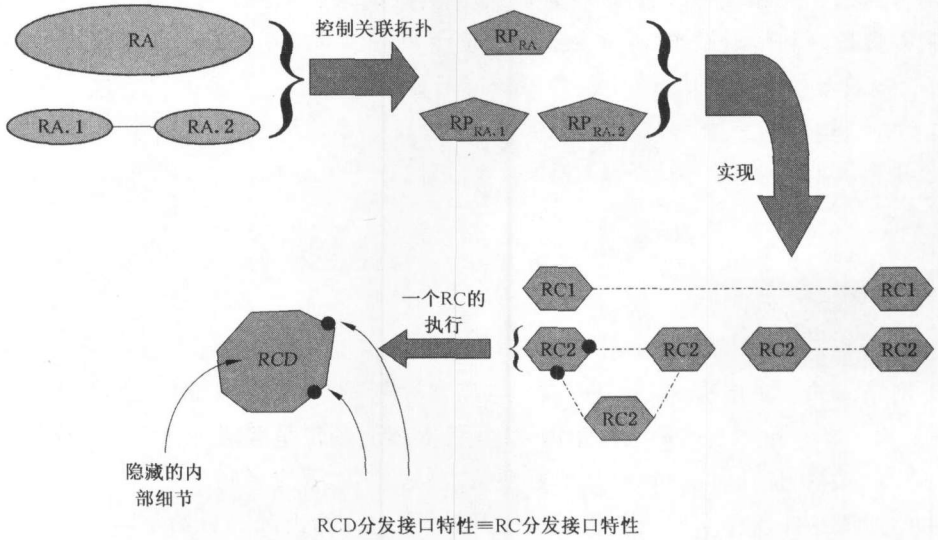


图 47 RA、RP、RC 和 RCD 之间的关系

ASON 路由等级结构的示例如图 48 所示。

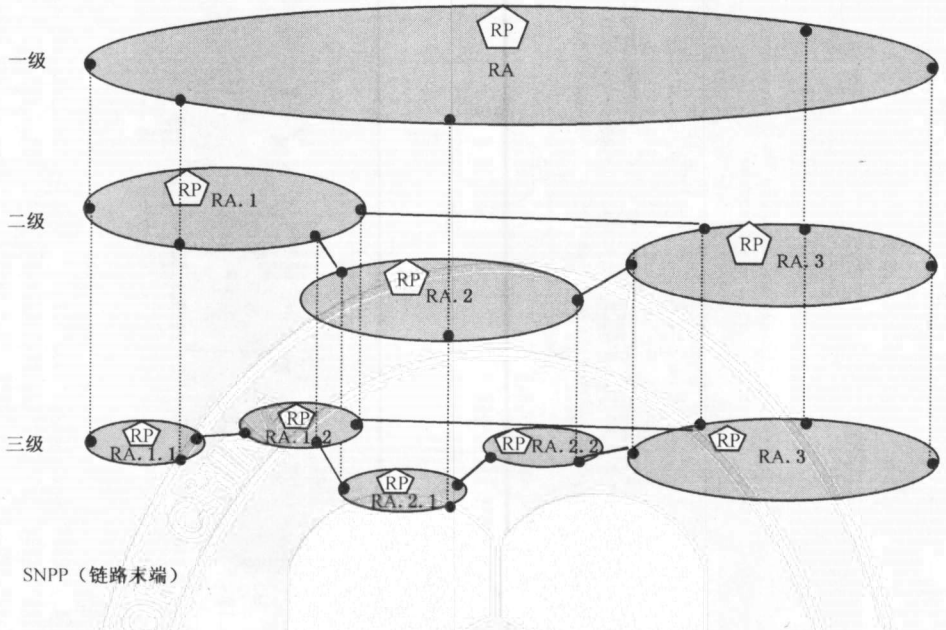


图 48　路由域等级结构示例

9.1.3　路由结构的要求

ASON 的路由结构应满足以下要求：

a）　ASON 路由结构应满足 ITU-T G.8080 和 ITU-T G.7715 建议的要求。

b）　域间路由协议应与域内路由协议及其控制分布模式（如集中式、完全分布式）无关。

c）　应支持多路由等级，应支持链路、节点和路由等级数目的可扩展性。

d）　不同路由等级的路由协议和路由方式可以不同。

e）　不同传送网层面的路由协议和路由方式可以不同。

f）　ASON 路由结构应允许一个路由域支持多种路由协议，可以有多个协议进行路由信息交换。

g）　ASON 路由结构应支持多种 OVPN 模式，如专用资源模式和共享资源模式等。

h）　路由邻接拓扑和传送网拓扑不一定一致，应支持路由邻接拓扑的自动生成。

i）　在一个运营者的网络内，每一个路由域应能唯一标识。

j）　路由信息应提供对单个域的抽象视图，抽象的程度由运行策略决定。

k）　路由执行器 RP 应提供系统故障恢复功能（如内存耗尽等）。

9.2　路由模式

ASON 具有三种路由模式：分级路由、源路由和逐跳路由。不同路由模式要求节点间不同的元件分布，以及连接控制器之间不同的关系。

9.2.1　分级路由

在分级子网结构的一个层次中，每个节点包含路由控制器、连接控制器和链路资源管理器。层网络可按 ITU-T G.805 分解为一系列等级的子网，连接控制器之间也呈等级关系。每个子网有自己的动态连接控制，了解本子网的拓扑，但不了解其他子网（该层之上、之下或者同层）的拓扑。

分级路由的通道选择操作从网络等级的顶层开始，首先计算出源和目的节点之间的路径必须经过的一系列子网。然后对于每个子网，还需要在子网内部拓扑的基础上进行进一步通道选择，此循环递归操作，直到通道选择最终得到实际链路为止。分级路由模式如图 49 所示。

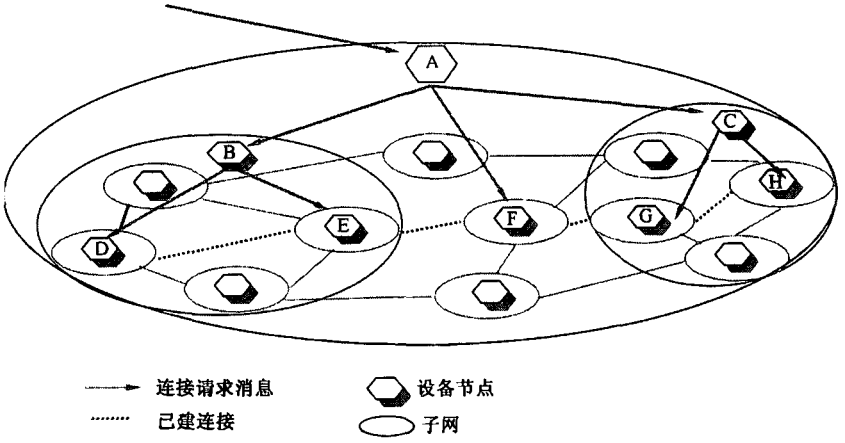


图 49　分级路由模式

采用分级路由模式建立连接的操作顺序如图 50 所示，具体步骤如下：

1）　一个连接请求到达连接控制器(CC)，指定在子网边缘的一对 SNP。

2）　CC 通过路由表查询接口查询路由控制器(RC)(使用 Z 端 SNP)，并返回一组相关的链路和子网。

3）　通过链路连接请求接口，从链路资源管理器(LRM)获得链路连接(可以以任意顺序，即图 50 中的 3a 或 3b)。

4）　在获得链路连接后(表示为 SNP 对)，可以经过连接请求入接口传递一个 SNP 对，从各下级子网请求子网连接，并通过连接请求出接口向 CC 确认子网连接。这些操作的顺序不是固定的，唯一要求是在子网连接建立前需获得链路连接。这一过程以递归方式重复进行。

5）　下级路由控制器解析指定的 SNP 之间的路由。

6）　通过链路连接请求接口从链路资源管理器(LRM)获取链路连接(以任意顺序)。

7）　由不具备任何路由和链路分配能力的最底层交换节点来提供所需的子网连接。

8）　其余的步骤是确认连接已经建立起来，最后确认信息经过步骤 9 和 10 返回到发起连接的用户。

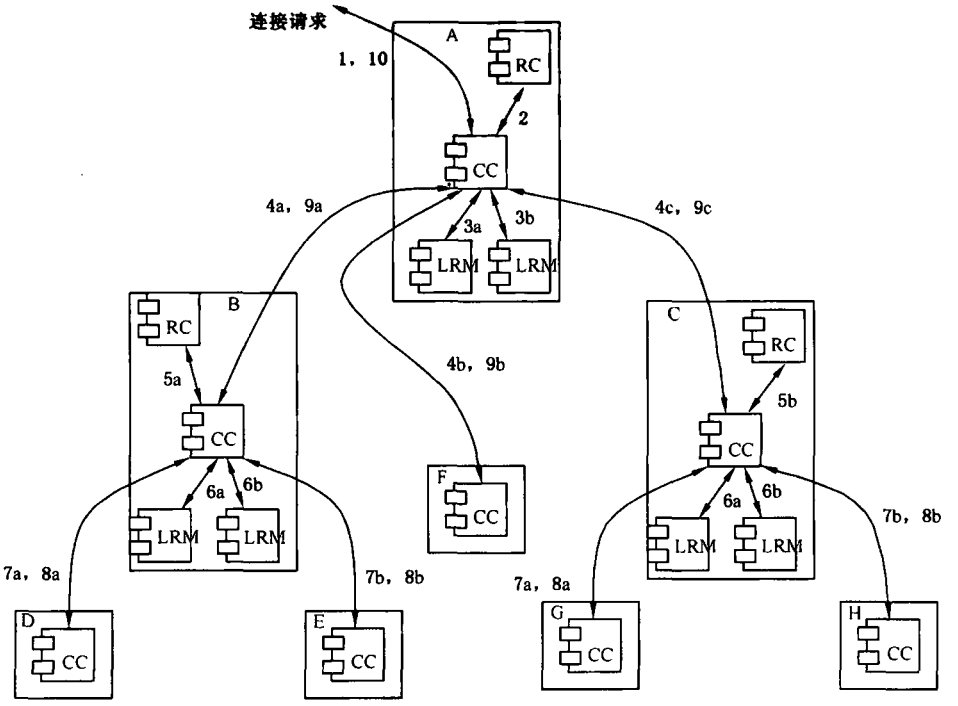


图 50　分级路由的操作过程

9.2.2 源路由

源路由与分级路由模式相似，连接控制进程由分布的连接和路由控制器的联邦完成。源路由与分级路由的最大差别是连接控制器工作在路由区，而分级路由是工作在子网上。为了减少每个控制域内的网络拓扑信息数量，一个路由控制器只负责本路由区内的拓扑。

源路由通道选择的发起通常是一个通道源节点，也可能是通道的一个中间节点。从源节点开始所经过的每个路由域，入口节点负责本路由域内的通道计算选择，并判断连接经过的下一个路由域的入口节点，这样逐个路由域进行选路，直到到达目的节点所在的路由域。源路由模式如图 51 所示。

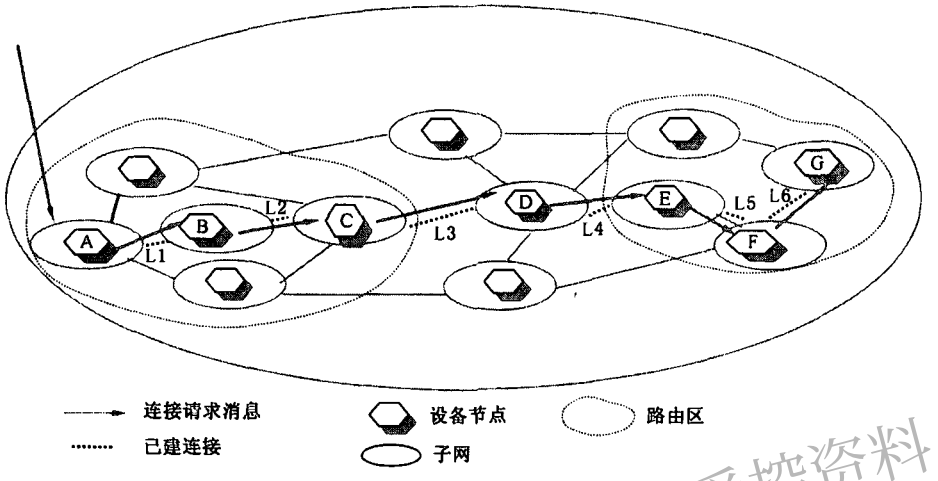


图 51 源路由和逐跳路由模式

采用源路由模式的操作过程如图 52 所示，其中 X_A 表示节点 A 的最高级别元件，X_{An} 表示节点 A 的最高级下第 n 个级别。具体步骤如下：

1) 一个连接请求经过连接请求入接口到达连接控制器(CC_A)，指定在子网边缘的一对名称(A 和 Z)。
2) CC_A 通过路由表查询接口查询路由控制器(RC_A)(使用 Z 端 SNP)，并返回出口链路 L3。
3) 由于 CC_A 没有接入链路资源管理器(LRM_C)的权力，该请求(A，L3，Z)被传递到一个对等的 CC_{A1}，它在该路由域内控制选路。
4) CC_{A1} 向 RC_{A1} 查询关于链路 L3 的情况(通过路由表查询接口)，得到一组的附加链路 L1 和 L2；
5) 链路 L1 为节点的本地链路，通过链路请求查询接口从 LRM_A 获得 L1 的一个链路连接。
6) 通过本地交叉建立子网连接 SNC(控制器未显示)。
7) 包含路由剩余部分(L2，L3 和 Z)的请求，被转发给下一个对等 CC_B(经过对等协调出/入接口)。
8) LRM_B 控制 L2，因此通过链路连接请求接口从该链路获得一个链路连接。
9) 通过本地交叉建立子网连接 SNC(控制器未显示)。
10) 包含路由剩余部分(L3 和 Z)的请求，被转发给下一个对等 CC_C(经过对等协调出/入接口)。
11) LRM_C 控制 L3，因此通过链路连接请求接口从该链路获得一个链路连接。
12) 通过本地交叉建立子网连接 SNC(控制器未显示)。
13) 包含路由剩余部分(Z)的请求，被转发给下一个对等 CC_D(经过对等协调出/入接口)。
14) CC_D 向 RC_D 查询关于 Z 的情况(通过路由表查询接口)，获得链路 L4。
15) LRM_D 控制 L4，因此通过链路连接请求接口从该链路获得一个链路连接。
16) 通过本地交叉建立子网连接 SNC(控制器未显示)。
17) 包含路由剩余部分(Z)的请求，被转发给下一个对等 CC_E(经过对等协调出/入接口)。
18) CC_E 向 RC_E 查询关于 Z 的情况(通过路由表查询接口)，获得链路 L5 和 L6。

在下一路由域的连接处理过程(图 52 中步骤 19 到 25)与上述过程基本一致，步骤 26 到 33 描述了确认信号传递到连接发起者的流程。

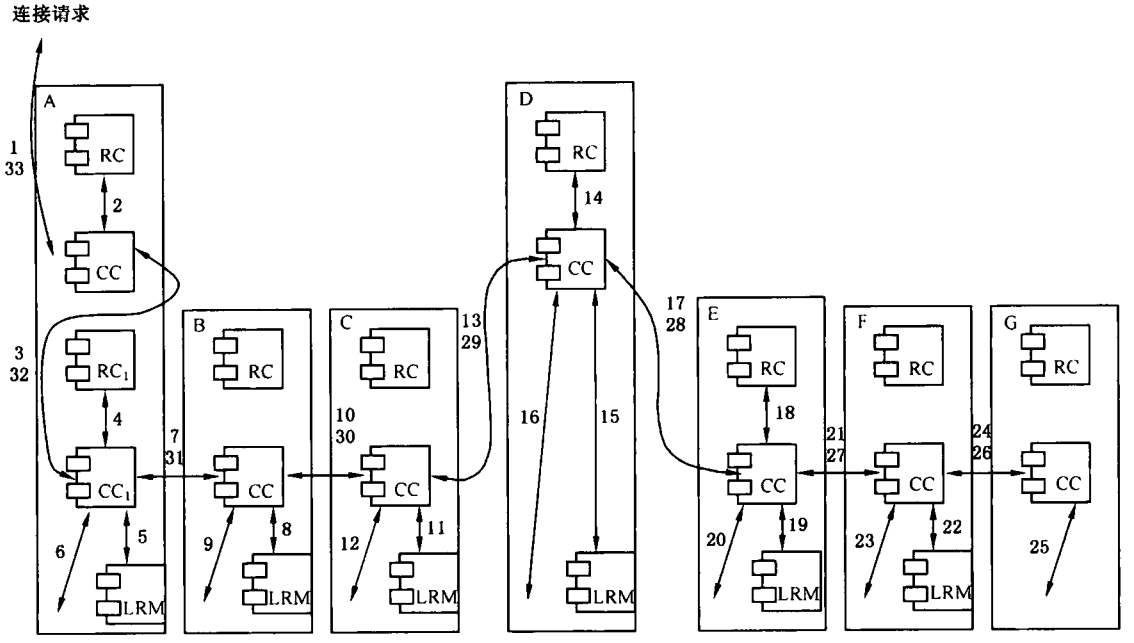


图 52　源路由的操作过程

9.2.3　逐跳路由

在逐跳路由模式中，进一步减少了节点内的路由信息，同时限制了跨越子网的路由选择的方式。逐跳路由的通道选择在每个节点上逐跳地执行，每个节点计算出到达目的地的下一跳链路。逐跳路由模式要求最终应该产生一个无环路的通道。逐跳路由模式如图 51 所示。

逐跳路由与源路由的操作步骤基本类似，主要存在几点差别：路由控制器 RC_{A1} 只能提供链路 L1，不能提供链路 L2；CC_B 为了获得 L2 必须向 RC_B 查询链路 L2（经过路由表查询接口）；当连接跨越第二个路由区时，获取链路的方法和前面过程的相同。逐跳路由的操作过程如图 53 所示。

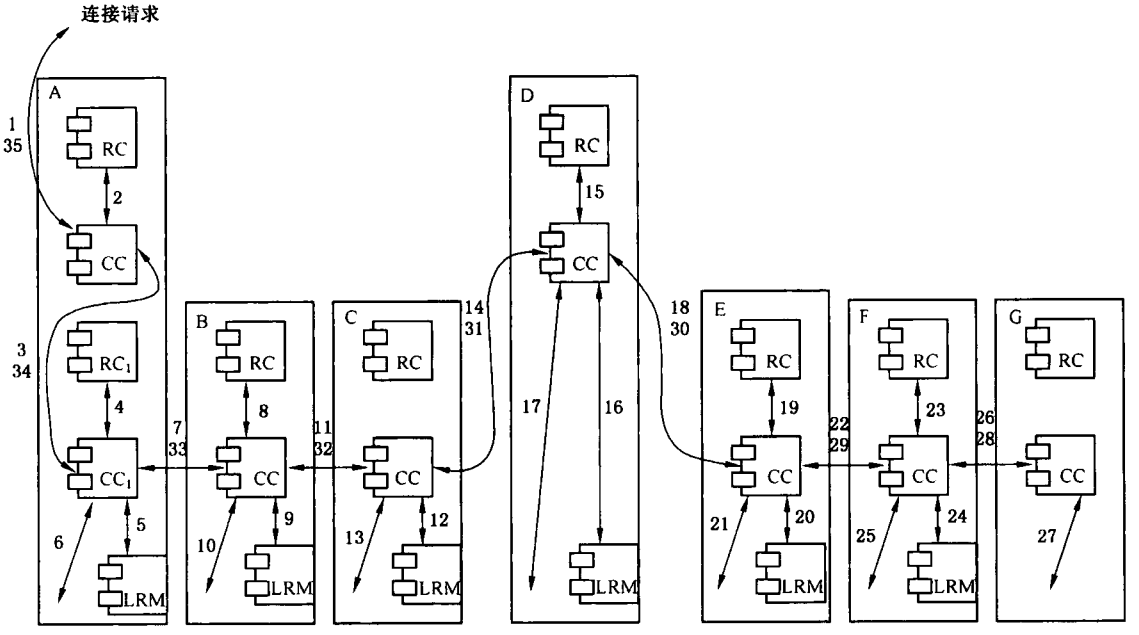


图 53　逐跳路由的操作过程

9.3 路由功能要求

ASON 路由功能包括可达性信息传播、网络拓扑/资源信息发布以及通道路由计算。ASON 路由功能应满足以下要求：

a) 支持逐跳路由、源端显式路由和分级路由方式三种选路方式之一。

b) 网络拓扑应由控制平面实现自动发现。路由功能应支持网络拓扑的维护，当网络拓扑发生变化时，应自动更新节点的拓扑信息。

c) 应支持在本控制域内进行节点和链路状态信息的发布，发布的信息应包括节点可达性、链路容量、链路权重、节点和链路分集、链路保护类型等。

d) 应支持分级路由结构，域间路由支持拓扑抽象和概要信息的发布。

e) 路由功能应支持把两个 ASON 节点间具有相同特性的多条链路组成一个链路捆束(Link bundle)，减少链路状态更新信息。

f) 应支持基于约束条件的通道选择，包括链路代价、分集、业务级别、网络性能指标、管理策略、传输层特定约束条件(例如波长，光层损伤)等。

9.3.1 通道路由计算功能

通道路由计算功能是根据连接请求返回一条通道路由，连接控制器可用这条路由作为信令连接的一个参数。路由计算主要依赖于路由算法复杂度、可用的拓扑信息以及特定的网络环境等。

通道路由计算可通过脱机操作实现或实时在线实现，也可以同时支持脱机和在线方式进行通道选择。例如，运营商可使用在线方式计算部分通道路由，并使用脱机方式处理复杂的流量工程，以及诸如需求规划、业务安排、成本模型和全局优化等与策略相关的问题。

ASON 的通道路由计算选择应满足以下要求：

a) 通道路由计算应产生无环路路由。

b) 通道路由计算应支持最短路径路由。

c) 通道路由计算应至少支持分级路由、源路由和逐跳路由三种方式中的一种。

d) 通道路由计算应支持工作通道和保护恢复通道的路由计算。

e) 通道路由计算应支持以下路由约束条件以及它们之间的组合：

1) 链路代价；

2) 包含特定网络资源(节点、SNPP 链路、SNP 链路连接)；

3) 排斥特定网络资源(链路和节点)；

4) 业务等级(保护和恢复类型约束)；

5) 路由分集约束，包括链路分离、节点分离和 SRLG 分离；

6) 负载均衡；

7) 网络性能指标(如时延、误码率)(可选)；

8) 传输层特定约束条件(例如波长，光层损伤等)(可选)；

9) 其他出于管理目的的策略。

f) 通道路由计算应支持各种业务和多种业务级别的能力。例如与业务类型、透明性、带宽、时延和比特率等有关的参数。

9.3.2 路由信息发布功能

ASON 路由消息分为路由功能的维护消息(如邻居维护)和网络路由信息的发布消息。

维护消息在具有逻辑邻接关系的协议控制器(PC)之间进行交互，逻辑邻接关系可以通过人工配置或动态建立。消息交互的范围限制在组成邻接关系的 PC 之间。

路由消息在两个相邻的路由控制器(RC)之间进行交换，路由算法利用这些消息为通过网络的连接请求计算路由。路由信息交互的范围限制在路由区内，消息的发布可以通过增量方式、逐跳的本地交互或全网范围的泛洪机制实现。

路由发布的信息应包含以下内容：

a） 节点属性

节点属性主要包括可达性和分集属性。根据参考点的策略，节点可以控制自身信息的共享。

1） 可达性属性：经过给定节点可到达的一系列节点，通过显式或概括的地址列表进行共享。

2） 分集属性：提供用于约束路由计算的节点属性，如共享风险组(SRG)。

3） 其他属性：与实施特定传送业务能力有关的能力信息，如保护/恢复功能；子路由区内的拓扑信息子集，可以用于提供多种传送业务，流量工程以及全网资源优化。

b） 链路属性

链路属性主要包括链路状态和分集信息。

1） 链路状态：包括三个部分，存在性、权重和容量。

存在性表示路由信息库中两个节点间存在一条链路。由存在性信息可以得到基本的网络拓扑(连通性)。链路的存在性并不依赖于该链路是否具有可用容量。

链路权重是一个由多个度量值(metric)评估得到的属性，度量值可以根据链路策略或约束条件进行修改。链路权重的值代表了一条链路在进行路由计算时被选中的可能性，权重越大，被选中的可能性越小，反之则越大。通过改变链路的权重值，可以防止选择容量快要耗尽的链路。

容量主要与该链路上的链路连接数目有关。容量信息的发布由运营策略决定。

2） 分集属性：与节点分集类似。

3） 其他属性：例如可用性、资源属性、保护属性等。

路由信息的发布应考虑策略和安全因素。经过不同参考点进行路由消息发布，应满足以下要求：

a） 不允许经过 UNI 参考点传递路由信息。

b） 通过 NNI 参考点的信息流应受到每个 NNI 的策略约束。

c） 经过不信任的 E-NNI 参考点发布的消息，不应包含关于内部网络拓扑的细节信息。

9.4 路由协议要求

路由协议是用于路由选择和链路状态分发的协议。路由协议包括域内路由协议和域间路由协议。ASON 路由协议应满足以下要求：

a） 应采用基于链路状态的路由协议，并满足 ITU-T G.7715.1 建议的要求。

b） 应支持 ITU-T G.7715 中定义的分级路由结构。

c） 路由协议应支持多层网络。

d） 路由协议应至少支持源路由、分级路由、逐跳路由方式中的一种。

e） 路由协议应支持将节点间存在的具有相同特性的多条链路组成链路捆束的功能。

f） 路由协议应支持不同级别的保护/恢复要求。

g） 路由协议应支持 Crankback 机制：

1） 要求路由协议支持在连接建立或恢复失败时，为连接重新计算另一条路由，应避开发生错误的链路和节点。

2） 支持链路、节点、SRLG 不相关的端到端或分段重路由。

3） 支持分级路由中的 Crankback。

h） 域间路由协议应独立于网络中任何域内的路由协议。

i） 域间路由协议应支持基于策略的路由信息交换。

j） 域间路由协议应支持域的拓扑和资源信息抽象，支持可达性信息聚合。

k） 域间路由协议应支持分级的路由信息分发，包括以下路由信息：

1） 域间拓扑；

2） 每个域的拓扑抽象；

3） 每个域的可达性信息；

4） 支持权重、负载均衡、各种业务颗粒和业务类型、保护恢复属性、分集和策略。

为支持路由协议稳定性和可扩展性，以下路由协议要求为可选：

a） 路由协议可支持基于触发和基于超时的路由更新。

b） 路由协议可控制动态信息的更新频率，例如设置不同类型的阈值或策略。

c） 路由协议可区分静态路由信息和动态路由信息。路由协议操作应以不同的方式更新动态和静态路由信息。只有动态路由信息才被实时更新。

d） 路由协议可避免过多的拓扑发布、资源和可达性信息更新，以及较长的路由收敛时间可能引起的控制网络不稳定。

e） 对于路由事件（例如拓扑更新、可达性信息更新），提供路由数据库信息收敛和适当的路由振荡抑制机制。

10 自动发现要求

10.1 自动发现概述

自动发现功能用于确定网元之间、控制域之间的链路连接关系，包括链路连接所支持的业务，其目的在于帮助进行资源管理和选路。自动发现不仅有利于控制平面的控制操作，也有利于管理平面对网络的智能化管理。

自动发现过程一般分为两个独立的阶段和名称空间。第一部分完全发生在传送平面名称空间（CP和CTP）内。发现代理（DA）完全工作在传送名称空间内，并负责保持链路连接（与每个CP相关）的传送名称。这些信息可通过使用对控制平面名称空间不可见的传送机制、保存预先获得的相关信息或指配方式来获得。DA通过与网络中所有DA之间的协作来解析传送CP名称，协助底层的自动发现进程，从而使负责传送链路连接的每一端的DA（或其他元件）能够就该链路连接进行通讯。见图54。

一个CP可以被分配给一组VPN。这组VPN可以用一个所有权标签来表示。DA需要验证一条链路连接的每个CP的所有权标签都是相同的。

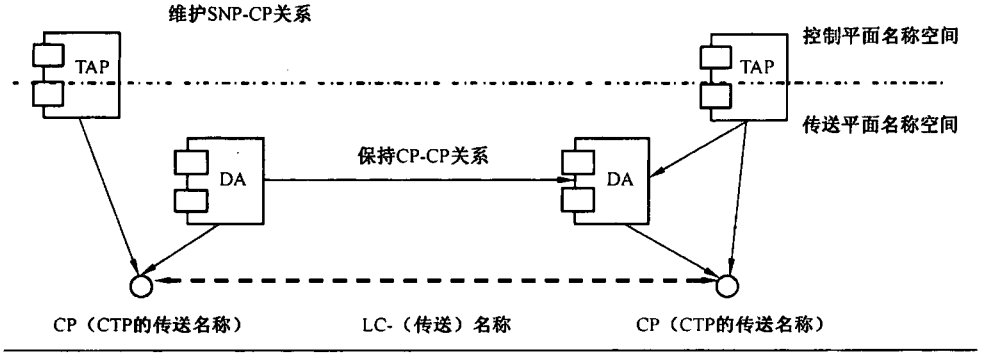


图54 传送平面的链路连接（LC）发现

第二部分完全发生在控制平面名称空间（SNP）内。链路资源管理器（LRM）保存链路连接的控制平面名称所需的SNP-SNP绑定信息，而TAP保存资源的控制平面名称（SNP）和传送平面名称（CP）之间的关系。这允许控制平面名称与传送平面名称完全分离，并完全独立于DA与传送名称关联所使用的方法。

为了给SNPP链路分配一个SNP-SNP链路连接，仅需要了解该链路连接的传送名称。因此，链路连接有可能不需要物理上连接起来，就能被分配给控制平面。这种分配程序可通过LRM交换与该SNP相关的传送链路名称来验证。完全合格的SNPP链路名称是能够反映传送平面资源结构的控制平面名称。见图55。

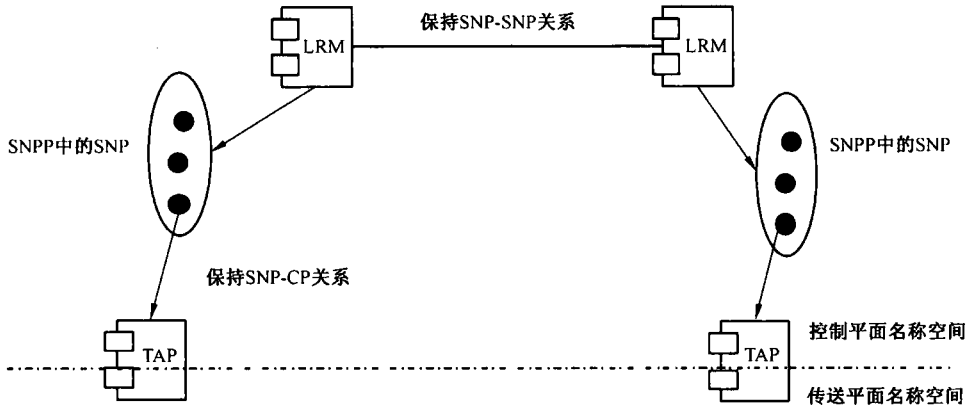


图 55 控制平面的链路连接发现

10.2 发现进程

对传送实体的发现进程是一个通用进程，如图 56 所示，可用于 ITU-T G.805 描述的多层网络中的任意层面。发现进程分为以下三个子进程：

a) 发现触发(DT)：负责触发 LAD 和 TCE 进程。

b) 层邻接发现(LAD)：LAD 进程用于获取在一个特定层网络中构成网络连接或链路连接的两个 TCP 或 CP 之间的关联关系。如果支持链路连接的路径是有效的，则通过层邻接发现得到的这种关联关系是有效的。LAD 进程在执行之前首先要了解 TCP 或 CP 的标识符。

c) 传送实体能力交换(TCE)：TCE 进程用于交换传送实体能力相关的信息(例如链路连接、路径)，用来帮助协商一个双方都同意的能力集。TCE 进程的前提条件是了解层邻接信息和本地能力信息。

注：如果预先配置了层邻接关系，那么 LAD 进程可以省略。

发现进程的实体可以分布在网元中或者位于管理系统内部，允许控制平面或者管理平面使用发现进程。管理平面可以使能或禁止发现进程及其子进程。

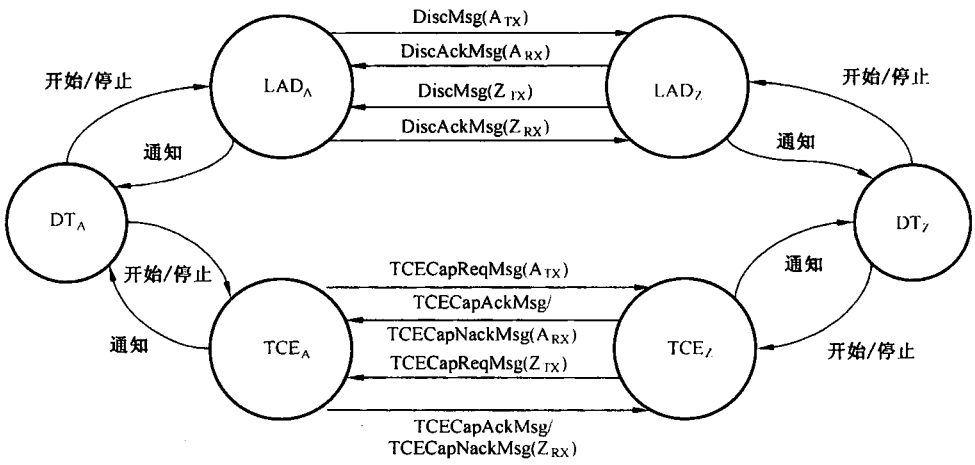


图 56 发现子进程的交互作用

10.2.1 发现触发(DT)

发现触发进程由管理平面使能，管理平面规定了需要支持的情景类型。情景描述文件具有多个参数，包括是否支持特定的发现子进程、是哪种类型、在什么情况下以及在各种情况下需要提供哪些管理信息。缺省文件是一个策略决定。例如：

a) 是否使用 LAD 进程。如果不使用 LAD，管理平面应当提供 TCP 或 CP 的绑定信息。如果使

用 LAD 进程，需要确定采用什么机制来携带发现消息，以及采用什么触发机制。

b) 是否使用 TCE 进程。如果不使用 TCE，管理平面将提供本地和远端信息。如果使用 TCE 进程，应当由策略来控制，并提供端点传送实体的详细能力。

10.2.2 层邻接发现(LAD)

传送实体的发现分别在每一个 ITU-T G.805 的层面上发生。LAD 进程用于在一个特定层面内部发现链路连接(LC)或者网络连接(NC)的终端点(如在组成连接的两个 TCP/CP)之间的关系。发现进程的前提是对于被发现的终端点应存在(T)CP ID。管理平面可以基于每一个(T)CP 启动或者禁止 LAD 过程。

LAD 进程在一个特定层的 LC 或者 NC 的终端点之间发送发现消息和发现确认消息，这些终端点如图 56 中的“A”和“Z”所示。A 端的 LAD 进程周期性地发送发现消息到 Z 端，其中包含的信息允许 Z 端决定 A 端的(T)CP ID 和与此(T)CP ID 相关的发现代理(DA)ID。当 Z 端接收到此消息以后，它发送一个发现确认消息给 A 端，此消息包括：

a) Z 端从 A 端接收到的信息；

b) 接收发现消息的 Z 端终端点的信息。

两个端点通过交换发现消息来识别一条 A 到 Z 的单向连接。此过程在 A 到 Z 方向同样进行，识别从 Z 到 A 的单向连接。与(T)CP 关联的两个单向连接识别完成以后，需要验证这两个单向链路是否位于同一对(T)CP 之间。如果验证结果它们不位于同一对(T)CP 之间，将报告错连信息。如果两条单向链路是位于相同一对(T)CP 之间，就认为 LAD 进程完成。管理平面可以停止 LAD 进程，或者使之保持激活以继续监测邻接状态。

图 57 显示了在客户层和服务层的发现进程，用于发现层网络拓扑。两个 AP 通过一条服务层网络连接关联，形成一条服务层路径。在此例中，服务层的路径支持 3 对客户层的 CP 关联，形成一条由三个 LC 组成的客户层链路。这里 LAD 进程发现在服务层的两个 TCP 之间的关系，同时发现在客户层的两个 CP 之间的关系。只有在服务层的网络连接有效时，两个层面中建立的关联关系才能有效。

多层网络的 LAD 进程可以通过从服务层邻接关系推出客户层邻接关系来进行优化，此进程采用 TCE 进程提供的 TCE 信息。

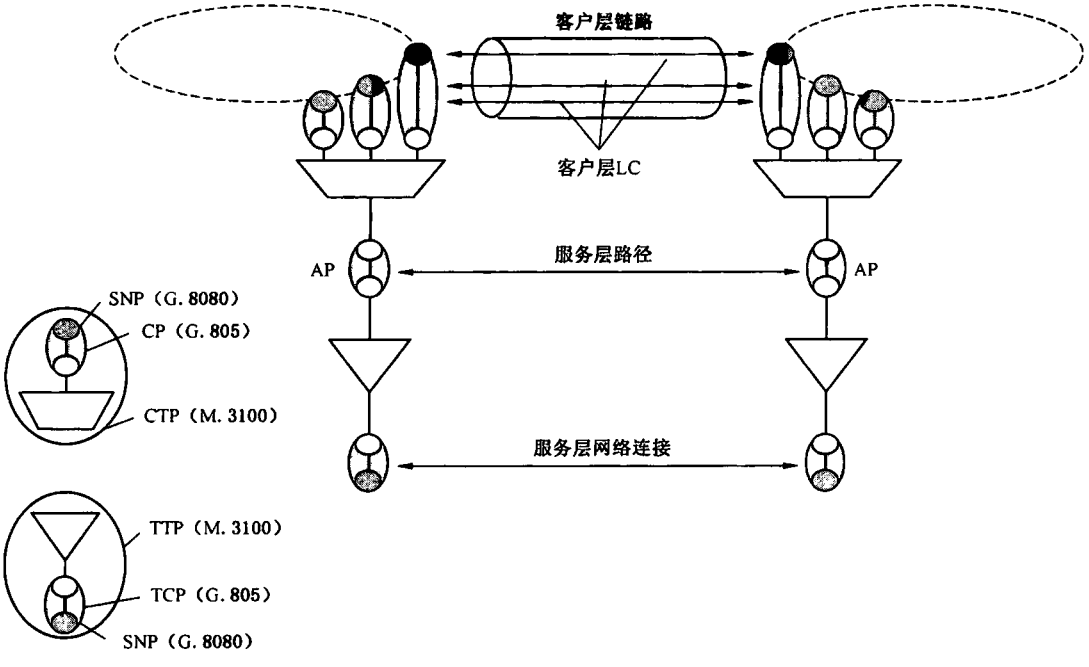


图 57 层邻接发现示例

层邻接发现可以采用两种方法：

a) 使用服务层的路径开销：在发现过程中，服务层的路径开销用于发现对等 TCP。服务层路径开销携带发现消息。依靠本地适配功能的配置信息以及适配功能同路径终结功能之间的关系，CP 到 CP 的关系可以从 TCP 到 TCP 的关系中导出。

b) 采用客户层的净荷：发现进程在客户层的净荷中传送发现消息来发现对等 TCP。CP 到 CP 的关系通过本地的交叉连接信息导出，交叉连接被预先建立用于把测试信号连接到相应的 CP。

10.2.3 传送实体能力交换(TCE)

TCE 进程交换信息来通知两端的传送实体它们所能支持的能力。这些能力包括两个邻接(T)CP 所支持的适配功能、特征信息等。与 LAD 进程不同，TCE 是一个在链路两端网元之间协商能够支持的能力的多阶段进程。

如图 58 所示，TCE 信息可以同 LAD 进程的结果相结合，导出潜在的客户层 CP。

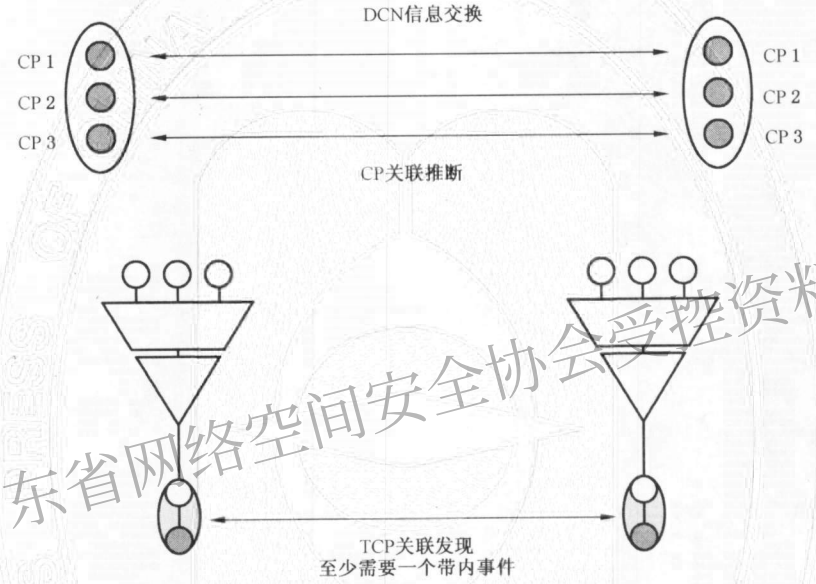


图 58 传送实体能力交换示例

在每个端点的 TCE 进程首先发出 TCECapReqMsg 消息(如图 56)，携带本地终端点所支持的能力。当远端的 TCE 进程接收到此信息后，它将消息中所支持的能力列表同它希望支持的能力列表进行比较，如果不匹配，返回 TCECapNackMsg 消息，并在其中指示它希望支持的能力。当源端接收到调整的能力列表以后，可以通过发送 TCECapAckMsg 消息以同意支持这些能力，或者发送新的 TCECapReqMsg 消息，携带新的调整后的能力列表，进行进一步的协商。如果两端对能力列表达成一致，两端会停止传送这些能力消息。应当注意的是，在一条双向链路的两个方向上交换的能力可以是不对称的。

10.3 自动发现的基本要求

ASON 自动发现功能应满足以下基本要求：

a) 发现代理

——发现代理应发现其 TCP 或 CP 所支持的链路拓扑。

——发现代理在一个发现进程操作范围内应具有唯一的标识。

——TCP 或 CP 的链路拓扑信息应由发现代理提供给相应的控制和管理实体。

b) 由发现代理负责的 TCP 或 CP

——在发现代理的范围内，TCP 或 CP 应具有唯一的标识符。

——对于发现代理管理的每一个(T)CP 应具有一个发现进程实例。

c) 发现进程实例

——发现进程实例应标识双向的传送实体，这些实体通过以下两个过程之一绑定到本地(T)

CP：由管理平面配置或者由 LAD 配置。

——双向传送实体应由本地 TCP 或 CP、本地 DA、远端 TCP 或 CP 和远端 DA 标识符共同来进行标识。

——发现进程应该能够标识远端 TCP 或 CP 的交换能力。

——发现进程应能够重新获取本地 TCP 或 CP 的交换能力。

——发现进程应能够协商由远端运营者策略所允许的本地 TCP 或 CP 的交换能力。

——发现进程应能协商由本地运营者策略所允许的远端 TCP 或 CP 的交换能力。

——发现进程应允许与远端 TCP 或 CP 协商的能力，和与本地 TCP 或 CP 协商的能力有所不同。

d) 双向传送实体的发现

——当标识双向传送实体的方法设置为由 LAD 完成时，发现进程应能够使能 LAD 进程。

——当标识双向传送实体的方法设置为由管理平面完成时，不应运行 LAD 进程。

——LAD 进程在标识双向传送实体时，应分别标识同本地 TCP 或 CP 相关的入口和出口单向传送实体。

——LAD 进程应标识连接到相同 TCP 或 CP 上面的两个单向传送实体。

——如果两个单向传送实体没有连接到同一个远端 TCP 或 CP 上面，LAD 进程应通知发现进程实例。

e) 单向传送实体的发现

——为了便于发现单向传送实体，发现进程应周期地在与本地 TCP 或 CP 关联的带内通道上发送发现消息，携带用于唯一标识本地 TCP 或 CP 的信息。

——通过监听与本地(T)CP 关联的带内通道上的发现消息，LAD 进程应能标识绑定到入口单向传送实体的远端 TCP 或 CP。

——本地 LAD 进程应通知入口单向传送实体的远端 LAD 进程，发送包含接收 TCP 或 CP ID、接收 DA ID 以及本地 TCP 或 CP 的 TCP 或 CP ID 和 DA ID 的发现确认消息。

——LAD 进程应支持使用下面一种或者两种带内通道：与本地 TCP 或 CP 相关的路径开销；或者与本地 TCP 或 CP 相关的路径净荷。

——一旦传送实体发现完成，发现进程应能够停止传输发现消息。

——管理平面应该能够禁止或者使能发现消息的传输。

f) 传送实体能力发现

——TCE 进程至少应支持连接到传送实体的终端点的传送平面能力的交换功能。

——应使用一个通用的进程，支持所有类型的传送实体能力信息。

——应支持增加附加的 TCE 信息类型，而无需对 TCE 进程重新规范。

——同路径相关的多种类型的传送实体能力信息应允许使用分离、独立的 TCE 进程。

——应能够更新传送实体能力信息，而不需要中断链路或者路径上的业务。

——TCE 进程应记录失败的能力协商尝试次数，当超过了管理平面配置的门限以后应终止重试。

——如果对新能力的协商不能够完成，TCE 进程应继续使用已经协商好的能力。

——TCE 重新协商失败后的后续动作应由管理平面的策略定义。

——在重新协商完成以后，TCE 应只使用新的能力。

10.4 自动发现的协议要求

ASON 自动发现应满足以下协议和接口要求：

a) 自动发现协议可采用 IETF 规范的链路管理协议(LMP)来实现。LMP 协议应符合 IETF RFC 4204 规范的要求，LMP 协议用于 SDH 和 WDM 网络时，应分别符合 IETF RFC 4207

(LMP 的 SDH 扩展)、IETF RFC 4209(LMP 的 WDM 光线路系统扩展)的要求。

b) 对于 UNI 接口,自动发现过程包括邻居自动发现、IP 控制信道(IPCC)维护和业务发现,这三个过程为可选项,可采用带内或带外两种方式来实现。UNI 的邻居自动发现和 IPCC 维护是基于链路管理协议(LMP)及其扩展来实现的。

——邻居自动发现进程用于在客户和传送网网元(TNE)之间交换它们的节点 ID,确定本地和远端端口(是指本地接口 ID 和远端接口 ID)之间的映射关系,以及和相应数据链路相关的配置参数。如果客户侧和 TNE 不支持自动邻居发现进程,则必须在相应的 UNI-C 和 UNI-N 中人工配置相邻和远端端口的标识。

——IPCC 维护进程用于在一对信令对等实体之间建立和维护控制信道的连通性。

——通过业务发现进程,一个 UNI-C 可交换它代表的客户设备的能力,并且获得关于 UNI-N 传送网的业务信息。如果不支持业务发现,则必须在 UNI-C 和 UNI-N 中用手工配置业务的所有信息。

——UNI 接口的自动发现应符合 OIF 关于 UNI 的接口规范。

c) 对于 I-NNI 接口,自动发现机制的实现可以基于带内或带外两种方式,带内方式的自动发现可采用 SDH 的踪迹字节或 DCC、OTN 的段/通道监视字节或 GCC 承载发现消息来实现。

d) 对于 E-NNI 接口,可采用自动发现和手工配置两种方式,手工配置为必选,具体应符合 OIF 关于 E-NNI 的接口规范。

11 链路资源管理功能要求

ASON 的链路资源管理器(LRM)元件负责维护 SNPP 链路信息,并将这些信息按照需要提供给其他 ASON 元件。在一个链路两端的 LRM 元件相互合作来发挥其链路管理的能力,并为其他依赖于链路信息而工作的 ASON 元件之间建立控制邻接关系起协调作用。

LRM 应提供以下基本功能:

a) 管理 SNP 链路连接:通过与管理平面的相互作用,SNP 链路连接可被分配或去分配给一个特定 LRM。作为自动发现进程的结果,管理平面可由此发现 SNP 链路连接。

b) 将可用的和潜在的 SNP 进行分组,并构成一个链路的相关 SNPP(SNP 聚合到 SNPP)。

c) 管理 SNPP 的状态(例如已配置的或忙的)和相关的 SNP 的状态(例如潜在的、可用的、或已分配即正使用的)。

d) 将本地链路(SNPP)及其链路状态提供给路由控制器(RC),RC 使用适当的路由协议将拓扑链路的链路状态信息发布到网络中。

e) 按照来自连接控制器(CC)的请求指配和去指配 SNP,这可能需要在同层网络中进行一次适配功能的重新配置(例如将潜在的 SNP 转化为可用的 SNP,或者反之,取决于来自 CC 的连接建立或连接释放请求)。

f) 通过与下层传送资源的链路相关的 TAP 相互作用,来管理变化的适配功能。这需要与链路另一端的 LRM(TAP)协调来完成。

g) 在适配功能变化的情况下,应保证链路两端的传送资源配置一致。

h) 保证 SNP 链路连接的完整性。

i) 隔离专用和/或共享链路资源,这些资源只能在一个特定 VPN 或多个 VPN 内使用。

j) 响应下层传送资源的 SF 或 SD 条件(故障处理)。

12 地址和名称

12.1 标识符空间

由于 ASON 引入了控制平面,因此产生了新的标识符空间。ASON OAM 功能和协议控制器设计

需要考虑这些标识符空间与其他传送标识符空间的交互。ASON 使用四类标识符，包括传送平面标识符、控制元件标识符、DCN 标识符和管理平面标识符。

a) 传送平面标识符：用于控制平面标识传送平面资源，包含以下两个子类：
   1) SNPP 和 SNP 标识符：控制平面使用这些标识符表示传送平面资源。SNP 通过 SNPP 标识符来描述其路由和嵌套子网环境。SNP 标识符从 SNPP 标识符导出，增加了一个本地的 SNP 索引。ASON 允许对同一个资源存在多个 SNPP 名称空间。
   2) UNI/ENNI 传送资源标识符：这些标识符用于表示在 UNI/ENNI 参考点上的传送资源（不一定要求在参考点上存在 SNPP 链路）。这些标识符代表位于客户和网络之间（或者在网络之间）的资源，而不是传送网端点。呼叫控制器使用这些标识符来指示呼叫的目的地。

b) 控制平面元件标识符：控制平面由一系列实现路由和连接管理的功能元件组成。可以采用统一的标识符来标识不同的控制元件，也可以采用不同的标识符来标识控制元件。由于控制元件在不同的 ASON 网络中可以具有不同的实例，例如 ASON 网络可以采用分布式信令和集中式路由，因此可能需要对以下元件给予独立的标识：

   ——路由控制器（RC）；

   ——网络呼叫控制器（NCC）；

   ——连接控制器（CC）。

   此外，不同元件使用不同的协议控制器（PC）进行特定的协议通信。因此协议控制器可能需要与抽象元件相独立的标识符。

c) DCN 标识符：DCN 用于控制平面元件之间的相互通信，实现控制平面通信功能的协议控制器（PC）需要使用 DCN 标识符。DCN 标识符用于指示协议控制器和 DCN 之间的接入点。多个协议控制器可以共享一个 DCN 接入点，每个网元可以具有多个 DCN 接入点。

d) 管理平面标识符：这些标识符用于表示 EMS 和 NMS 中的管理实体。其中包括 EMS 和 NMS 用于 OAM 的标识符，例如 ITU-T M.3100 规范的 TTP 和 CTP。通常，这些标识符描述了支持维护和故障关联的一个物理位置。CTP 标识符表示 ITU-T G.805 规范的连接点（时隙），TTP 标识符表示传送设备的物理环境（例如电路组）。

各种标识符空间的关系如图 59 所示。

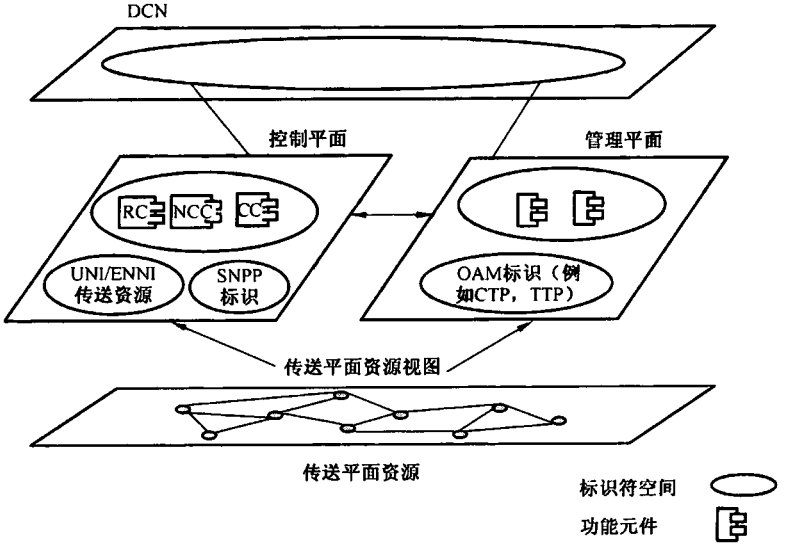


图 59 标识符空间的关系

12.2 传送平面名称

12.2.1 SNPP 名称

ASON 定义了 3 个独立的传送平面名称空间：

a) 路由区名称空间；

b) 子网名称空间；

c) 链路名称空间。

前面两个名称空间符合传送网的子网结构，可以不相关。这两个名称空间结合在一起可以确定 SNPP 的拓扑位置。链路名称空间规定了 SNP 在 SNPP 中的位置，它用于反映 SNPP 的内部结构和不同类型的链路名称。

SNPP 名称由下面几部分组成：

a) 一个或多个嵌套的路由区名称；

b) 在最低路由区等级中的一个可选的子网名称，仅当包含该子网的路由区名称出现时存在；

c) 一个或多个嵌套的链路资源名称。

这种命名方案允许在任意的路由等级内对 SNP 进行标识。SNP 地址用于链路连接分配和路由，SNP 名称由 SNPP 名称和一个具有本地意义的 SNP 索引组成。

同一子网可以具有多个 SNPP 地址空间。如果每个路由区使用不同的 SNPP 地址空间，则需要维护不同 SNPP 名称之间的映射关系。

SNPP 别名是在另一个 SNPP 名称空间产生的对于同一个 SNPP 链路的另一个名称。SNPP 别名如果在一个路由区中出现，它对于与 RA 相关的 RC 是可用的。

12.2.2 UNI 传送资源名称

对于主叫方呼叫控制器和网络呼叫控制器，UNI 的 SNPP 链路需要一个名称来指明目的地。这些名称应全球唯一并由 ASON 网络分配。可以为 SNPP 分配多个名称，这允许主叫方/被叫方将具有特定名称的不同应用与一个公用链路相关联。一组 UNI 传送资源名称可以存在一个别名。

OIF UNI1.0 的传送网络分配地址(TNA)是 UNI 传送资源名称的一个实例。由于不能给用户分配网络内部地址，UNI 传送资源地址应与 SNPP 名称相分离。需要地址解析功能来完成 UNI 传送资源地址与 SNPP 之间的映射。可以改变这种映射关系而不改变某些业务属性。

当连接管理器采用目的 TNA 地址建立连接时，需要提供地址解析功能来完成 TNA 地址到对应 SNPP 链路的 SNPP 地址之间的映射。

由于一个 UNI 可以包含多条 SNPP 链路，在此情况下应考虑 TNA 地址分配问题。

a) 当一个 UNI 包含多条 SNPP 链路时，应为 UNI 的多个 SNPP 链路分配多个全局唯一地址。

b) 当一个 UNI 支持多条 SNPP 链路时，应采用传送资源地址(TNA)地址来区分使用哪一条 SNPP 链路。呼叫方可使用一些参数，如分集、代价，来选择适合的 SNPP 链路。

c) 当一个用户具有多个 UNI 时，每一个 UNI 应有各自的 UNI 传送资源地址，而不应共享一个公共地址。

12.2.3 ENNI 传送资源名称

ENNI SNPP 链路可以被分配一个名称用于网络呼叫控制器指定 ENNI。这些名字必须是全球唯一的，并由 ASON 网络来分配。可以为一条 SNPP 链路分配多个名称。对于一组 ENNI 传送资源名称可以存在一个别名。

当 ENNI 参考点位于一个 VPN 客户域和一个服务提供者域的 VPN 之间时，ENNI 传送资源名称在 VPN 分配的所有其他 ENNI SNPP 链路内唯一，但不需要全球唯一。

12.3 控制平面地址

控制平面的地址包括用于路由、呼叫和连接控制等功能的地址。

用于 ASON 路由功能的地址包括：

a) RC 的标识符，来自控制平面的地址空间；

b) RC 的协议控制器标识符，来自控制平面的地址空间；

c) 用于和 RC 的协议控制器通信的标识符，来自 DCN 地址空间；

d) 用于表示 RC 所代表的传输资源的标识符，来自 SNPP 名称空间。

用于网络呼叫控制器和连接控制器的地址包括：

a) 网络呼叫控制器标识符，来自控制平面地址空间；

b) 连接控制器标识符，来自控制平面地址空间；

c) 用于 NCC 的协议控制器的标识符，来自控制平面地址空间；

d) 用于 CC 的协议控制器的标识符，来自控制平面地址空间；

e) 用于和 NCC 的协议控制器通信的标识符，来自 DCN 地址空间；

f) 用于和 CC 的协议控制器通信的标识符，来自 DCN 地址空间；

g) 用于一个 CC 所能控制的传输资源的标识符，来自于 SNPP 名称空间。

控制平面协议要求对传送资源地址使用 SNPP 标识符，一对 SNPP 标识符可以标识一个 SNPP 链路。需注意的是 SNPP 名称属于传送平面地址空间，控制平面不能使用控制平面的地址和名称(如 RC 或 CC 标识符)来标识 SNPP 链路。

12.3.1 控制平面元件对 SNPP 名称的可见性

控制平面的元件之间可以形成多种实体关系。例如在一个传送网络中，一个 RC 可以对应一个或多个 CC。在分布式的信令系统中，RC 所能控制的 SNPP 范围比较大，当 RC 计算一条路由并将它转送给 CC 时，其中部分路由段落有可能超出了 CC 所能控制的范围。

在上述 RC 和 CC 的关系中，CC 可以不必了解超出它所知范围的 SNPP，例如它不需要了解一条链路的远端 SNPP 名称，只需要了解本地的 SNPP 转发地址就足够了。

在 Crankback 过程中，CC 不需要了解产生 Crankback 的故障原因，而 RC 则需要了解这些对 CC 透明的信息。

另外 RC 在创建显示路由的过程中，应尽量采用本地 SNPP 名称来指定下一跳的 SNPP 链路。

12.3.2 名称空间在不同元件之间的交互

在路由计算过程中，RC 传送给 CC 的路径信息采用 SNPP 名称，为了使 RC 提供给 CC 的路径有意义，RC 和 CC 必须使用相同的 SNPP 地址空间。SNPP 命名可以采用多种形式，它们应采用统一的命名机制。

NCC 在解析 UNI 传输地址时，RC 和 CC 必须能够了解 NCC 所使用的 SNPP 名称。

不同的名称空间采用统一的命名机制是非常重要的。例如可以采用 NE 所使用的最低等级的 SNPP 名称(子网名称)来统一不同的名称空间。

12.3.3 多个 SNPP 名称空间

ASON 的体系结构允许一个 CP 使用多个 SNP，因此对于同一个子网可以存在多个 SNPP 名称空间。在分级路由中，应考虑采用一个或多个 SNPP 名称空间。如图 60 中，RA-1 包括 RA-2 和 RA-3。如果每一个 RA 使用一个独立的 SNPP 名称空间，那么需要完成不同 RA 的 SNPP 名称空间之间的映射。

这三个 RA 也可以使用统一的 SNPP 名称空间，类似于一种层次结构。在这种结构中，名称的长度会因为层次的不同而发生变化。

分级路由使用独立的 SNPP 地址空间的优点是便于路由等级的插入和删除，而不需要调整名称的长度，缺点是需要维护一个地址映射表。采用多个名称空间也会对 UNI 传输地址和 SNPP 名称之间的映射产生影响。

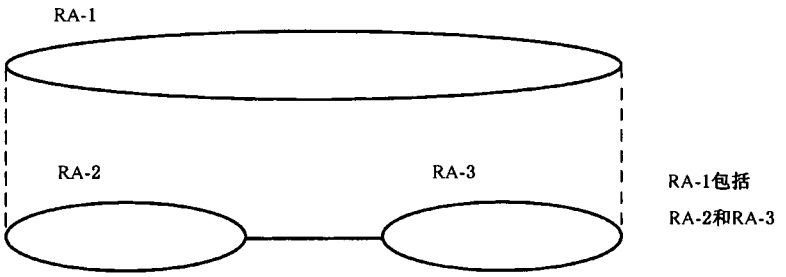


图 60　多个 SNPP 名称空间和路由层次

12.4　对地址和名称的要求

对 ASON 地址和名称的基本要求如下：

a) 运营商网络中的每个控制域和每个网元都必须是唯一标识的。所有的业务接入点也要求唯一标识。

b) 控制平面、管理平面、传送平面和 DCN 的地址和名称空间应相互独立。

c) 控制平面的引入带来了新的名称空间，需要考虑不同元件实体的名称空间之间的交互作用。各个元件对命名的语义应该统一，不应产生歧义。

d) 应该支持层次化的地址结构。

e) 应该支持地址的聚合和概括。

f) 域间多点互连时，每个控制实体(如 E-NNI)不应需要多个内部地址。

g) 应支持多种地址格式(IPv4，IPv6，NSAP)中的一种。

h) 地址空间应足够大以避免地址耗尽。

i) 终端用户设备和其他传送网运营商不应从 UNI 和 NNI 接口获得内部网络地址，包括端口信息等。

j) 应支持不同名称空间之间的地址解析和翻译，支持 TNA 地址到 SNPP 链路之间的映射。

k) 地址解析可以作为连接建立过程的一部分，或者作为一个独立的网络服务。

l) UNI 应采用 TNA 地址进行连接请求。

m) 对于 UNI 和 E-NNI 上的 TNA 地址可以通过手工分配和解析服务器的方式进行地址解析。

n) 对 SNPP 链路的标识可采用编号方式或者无编号方式。

o) 应支持对链路捆束的标识，对链路捆束中的成员链路可以采用链路捆束标识加具有本地意义的成员链路标识。

13　ASON 的管理平面要求

13.1　ASON 网络管理分层结构

ASON 管理平面的管理对象包括传送平面、控制平面、数据通信网等。管理平面与传送平面、控制平面之间通过 NMI 接口进行信息交互。NMI 接口包括传送平面网络管理接口(NMI-T)和控制平面网络管理接口(NMI-A)。ASON 管理平面应符合 ITU-T M.3010 规范的管理功能要求和 ITU-T G.8080 规范的 ASON 框架要求。

ASON 网络管理的分层结构应符合 ITU-T M.3010 建议的规范。从逻辑功能上划分，ASON 网络管理主要分为三层：网元层、网元管理层和网络管理层。ASON 管理平面逻辑分层结构所示。

网元层主要是指不同物理网元设备，一般情况下接受网元管理层的管理，但是网元本身也应具有一定的管理功能。网元管理层主要完成不同网元设备的管理，网元管理系统(EMS)属于网元管理层。EMS 对上层 NMS 提供管理接口。网络管理层主要面向 ASON 网络，负责对所辖管理区域内的网络进行监控管理。网络管理系统(NMS)属于网络管理层，它可以给网络运营商一个全局的网络概念。网络操作者通过 NMS 管理所辖区域内的端到端网络连接。EMS 和 NMS 可以集成在同一网管系统中。

ASON 网管系统的设置可以根据传统的管理域划分方式进行，也可以按照 ASON 控制域方式进行。图 61 同时给出了 ASON 网管系统设置的实例。根据不同网络运营商设置不同的 ASON 网管系统，即：一套网管系统(EMS. X/Y 和 NMS. X/Y)管理同一运营商网络(X/Y)。当在同一运营商网络内部存在多个控制域时，可以根据控制域的划分设置不同的网管系统(EMS. X1 和 EMS. X2)，也可以采用同一网管系统(EMS. Y)管理多个控制域网络。

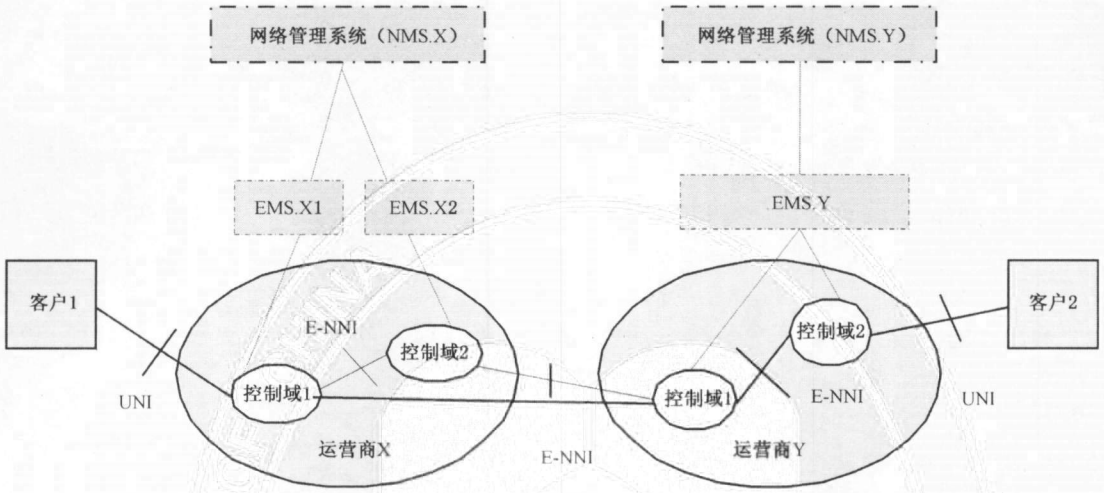


图 61　ASON 网络管理逻辑分层结构

13.2　ASON 管理平面一般要求

管理平面执行对传送平面、控制平面和系统整体的管理功能，它还提供所有平面之间的协调功能。管理平面应支持 ITU-T M. 3010 中规定的下列管理功能：

——性能管理；
——故障管理；
——配置管理；
——计费管理；
——安全管理。

管理平面在以下情况下不应影响控制平面和传送平面的正常工作：

a)　与传送平面交互

当管理平面与传送平面交互时，在以下情况下，管理平面不应影响它管理的传送平面中网元的正常运行，也不能影响传输网络的正常业务：

——当管理平面出现故障时；
——投入服务和退出服务时；
——网元中与网管有关的机盘的插入和拔出等；
——当网络中断时，管理平面应能提示用户，并自动尝试重建连接。

b)　与控制平面的交互

当管理平面与控制平面交互时，管理平面应满足以下要求：

——当管理平面出现故障时，它不能影响控制平面的正常运行；
——当控制平面出现故障时，它不能影响管理平面的正常运行；
——管理平面应能拆除控制平面建立的连接；
——如果控制平面失去了对底层网络资源的有效控制，管理平面必须能够释放这些资源。

13.3　ASON 管理平面功能需求

从宏观功能结构上，ASON 管理平面应提供的基本功能包括：

a) 传统管理功能，如对传送平面的管理以及永久连接(PC)的管理功能；

b) 配置和监控控制平面，管理软永久连接(SPC)和交换连接(SC)；

c) 提供不同逻辑层网络和连接的整体视图；

d) 提供跨不同管理域、控制域的端到端整体视图；

e) 配置和监控管理信息及控制信令的数据通信网络(DCN)；

f) 对 ASON 智能化新业务的管理，如 OVPN、BoD 等业务。

因此，ASON 管理平面功能主要概括为四部分：传送平面管理、控制平面管理、DCN 管理和业务管理。

13.3.1 传送平面管理功能

传送平面管理功能应满足传统的管理功能要求，支持故障、性能、配置、安全四大管理功能。概括的描述，传送平面的管理主要包括以下内容：

——基本的传送平面网络资源的配置，包括基本的网络资源和拓扑连接配置等；

——永久连接(PC)建立过程中传送平面和管理平面的交互；

——对传送平面光网络(SDH、OTN)的性能和故障管理；

——多层、多区域网络环境下的资源管理功能。

传送平面的管理功能应满足 ITU-T G.784、ITU-T G.874、YD/T 1289.2 的规定。

13.3.2 控制平面管理功能

控制平面的管理功能主要包括：ASON 初始化配置、资源管理、发现管理、呼叫和连接管理、策略管理、保护与恢复管理、控制平面故障和性能管理以及计费管理等。

13.3.2.1 初始化配置

为了能够在 ASON 节点上应用控制平面功能，管理平面应支持对 ASON 节点的初始化配置。初始化配置主要包括节点信息、控制平面采用的信令、路由、链路资源管理等协议、控制平面标识、地址和控制平面通信等方面相关参数的配置功能。在节点上配置和管理的主要参数包括：

——节点标识与名称；

——节点的管理标识；

——控制平面接口模式：UNI-C、UNI-N、I-NNI、E-NNI；

——协议控制器的协议类型和参数：信令协议，路由协议和发现协议(可选)；

——控制平面相关地址；

——控制平面的使能(启用/禁止)。

13.3.2.2 资源管理

资源管理主要提供资源配置和再分配功能，管理平面应支持以下资源管理功能：

a) 负责 ASON 网络资源的标识，为连接终端点(CTP)分配标识(SNP 和 SNP 绑定(BUNDLE))；

b) 管理平面应能为链路资源分配共享风险链路组(SRLG)；

c) 管理平面应能为 UNI 参考点分配 TNA 和逻辑端口标识符；

d) 链路资源的识别和同步：支持链路资源在传送平面和控制平面之间的映射和同步；

e) 管理平面应支持资源控制功能，管理平面应能分配控制平面所使用的网络资源；

f) 管理平面可通过控制平面获得资源利用率信息(包括链路、端口等)，并可查询每一客户设备或连接在网络中的资源占用情况；

g) 为特定用户分配传送资源以创建 VPN。

13.3.2.3 控制域管理

管理平面可支持以下控制域管理功能：

a) 管理平面应支持为控制域分配控制平面元件；

b) 管理平面应支持为控制域内的路由区分配控制平面元件；

c) 管理平面应支持多种控制域类型的划分；

d) 支持控制域的划分和聚合；

e) 支持控制平面的分层管理。

13.3.2.4 **发现管理**

管理平面应支持以下发现管理功能：

a) 管理平面应支持控制平面的资源和邻居发现功能。管理平面应配合控制平面的自动发现，对控制平面向管理平面上报的拓扑信息实施管理。管理平面应能有效管理发现的拓扑信息，包括域内和域间拓扑信息。

b) 当控制平面不使用自动发现功能时，网管应能够进行人工配置节点所需要的邻接信息。

c) 管理平面应能够禁止或者使能控制平面的自动发现功能。

d) 管理平面应支持由控制平面发现的网络拓扑的实时监视功能。

13.3.2.5 **呼叫和连接控制功能**

13.3.2.5.1 **连接管理**

管理平面应支持对三种连接的分类管理，即永久连接(PC)、软永久连接(SPC)和交换连接(SC)。

a) 永久连接(PC)

与传统电路管理相同，管理平面应提供对 PC 的管理，具体要求应符合 YD/T 1289.2 的规范。

b) 软永久连接(SPC)

管理平面应提供发起 SPC 建立或拆除指令、查询路由信息等功能，基本管理功能包括：

1) 支持 SPC 属性的设置，包括：A/Z 端点、业务类型、信号带宽、保护恢复类型、业务透明性等；

2) 支持严格和松散显式路由的指配；

3) 支持路由约束条件的定制；

4) 管理平面应支持发起 SPC 连接建立或拆除请求；

5) 管理平面应支持人工发起 SPC 重路由；

6) 管理平面应能查询和显示 SPC 的状态、路由、连接属性等信息；

7) 管理平面应支持 PC 到 SPC 的迁移，在迁移过程中与该 PC 相关的传送资源被分配给控制平面，且不会造成业务中断。

c) 交换连接(SC)

管理平面应提供 SC 的查询、拆除等功能，基本管理功能如下：

1) 接收 SC 的建立、拆除和修改通知；

2) 查询和显示 SC 的状态、路由、连接属性等信息；

3) 管理平面应能发起拆除 SC 连接请求；

4) 管理平面应支持启动 SC 的重路由功能。

另外，管理平面应支持以下连接信息的永久存储：

——路由；

——速率；

——方向；

——端口资源；

——状态；

——保护恢复状态；

——连接建立时间；

——连接拆除时间；

——连接的类型(PC,SPC,SC);

——客户信息等。

13.3.2.5.2 **呼叫管理(可选)**

呼叫管理功能主要包括:

a) 对于每一个呼叫,管理平面应支持连接的增加、删除和修改功能;

b) 管理平面应能配置呼叫的属性信息,如呼叫标识;

c) 管理平面应能查询所有呼叫的当前状态;

d) 记录并统计所有呼叫的保持时间,包括开始时间和结束时间。

13.3.2.6 **策略管理**

管理平面应具有为连接提供策略管理的能力,为不同用户定制满足服务需求的业务级别协议(SLA)。主要策略管理包括:

a) 管理平面应能配置 SLA 参数,例如带宽参数、连接类型、保护与恢复策略、QoS 等。

b) 管理平面应支持控制平面对服务策略的访问。控制平面通过与管理平面交互策略信息,确定 SC 发起者是否有权建立连接;在连接请求被接受后,根据设置的策略参数建立满足要求的连接服务。

13.3.2.7 **保护与恢复管理**

对于保护和恢复管理,管理平面应配合控制平面的保护恢复机制,主要完成以下管理功能:

——管理平面应支持在连接建立时选择保护恢复策略;

——管理平面应能指定连接的保护和恢复路由的约束条件;

——管理平面应支持下发软重路由和保护恢复操作命令;

——管理平面应支持保护与恢复的状态监视,收集与查询与控制平面保护和恢复相关的信息;

——保护恢复属性的在线修改功能(可选)。

13.3.2.8 **故障管理**

作为故障管理的一部分,管理平面应提供针对控制平面的故障管理功能。对控制平面的异常运行情况进行实时监视,完成对告警事件的监视、报告和存储;完成故障诊断、故障定位等功能。与控制平面相关的告警类型包括:

——控制平面节点或元件失效告警;

——控制信道失效告警;

——控制平面失效所影响的呼叫和连接告警等。

13.3.2.9 **性能管理**

作为性能管理的一部分,管理平面应提供针对控制平面的性能管理功能。性能管理最基本的功能是完成对控制平面的性能监视,收集性能数据,提供控制平面实际运行的当前性能。与控制平面相关的性能参数主要包括:

——连接数目统计(可按连接类型 SC/SPC/PC 进行统计);

——连接运行时间(包括建立时间和拆除时间);

——节点上连接建立失败计数;

——节点上发生 CrankBack 计数;

——发生的连接保护倒换或重路由次数等。

13.3.2.10 **事件管理**

当控制平面发生状态改变或异常事件时,控制平面应将其上告给管理平面。控制平面上报的事件和通知类型包括:

——控制节点状态(Down/Up)更新事件;

——控制信道状态(Down/Up)更新事件;

——连接建立/删除成功/失败通知；

——连接保护恢复成功/失败通知；

——光纤错连事件通知等。

13.3.2.11 计费管理

管理平面应支持连接计费功能，用户可查询相关连接的计费信息。管理平面主要提供的基础计费数据包括：

——连接类型(SC/SPC/PC)；

——连接建立时间和结束时间(年/月/日、时/分/秒)；

——连接方向(单向/双向)；

——业务量参数(信号类型、带宽和透明性等)；

——业务等级：根据保护恢复方式划分；

——源、宿节点或 TNA 地址；

——源、宿逻辑端口标识符；

——连接标识符；

——分集等。

13.3.3 数据通信网管理

管理平面应支持对信令通信网(SCN)和管理通信网(MCN)的管理。本部分主要规范对 SCN 的管理要求。

a) 管理平面能够为信令通信网配置信令通道和信令地址，并选择使用的 SCN 传送方式(带内/带外)；

b) 当控制通道出现故障时，管理平面应能正确接收控制通道的故障通知。故障通知应指示出故障发生时间、故障原因、故障根源和严重等级；

c) 管理平面必须能够向控制平面查询指定控制通道的状态；

d) 管理平面应支持配置控制信道的冗余保护和恢复；

e) 应支持信令通信网拓扑信息的显示和查询。

13.3.4 业务管理

管理平面应提供 ASON 新业务管理功能，例如 OVPN、BoD 等，实现对它们的基本配置和管理。具体管理功能要求待研究。

13.4 管理平面的可靠性

管理平面的故障主要包括网管系统服务器故障，用户界面程序故障和与传送平面/控制平面通信中断。为了保证管理平面的可靠性，在故障发生时，管理平面应满足下面的要求：

a) 管理平面故障不应影响控制平面和传送平面的正常工作。

b) 网管系统应支持(1+1)热备用(Hot-Standby)或温备用(Warm-Standby)配置；在热备用的方式下，主用到备用的切换应为实时切换；在温备用的方式下，主用到备用的平均切换时间应小于 20 分钟。

c) 应支持对网管数据的备份，包括人工备份和自动定期备份。

d) 用户界面程序异常停止后，不应影响服务器端和其他用户界面的正常运行。

e) 与传送平面/控制平面的通信中断时，系统应在一定时间内自动尝试重建连接。通信恢复后，应支持自动和手工方式实现网管数据的同步和更新。

14 ASON 数据通信网要求

14.1 DCN 总体要求

数据通信网(DCN)是为网络提供管理信息和信令消息的传送通道，它提供了一种基于分组的传送

网络，从而可以在不同网元之间传送信息。DCN 的主要应用包括管理通信、信令通信以及其他通信，如图 62 所示。

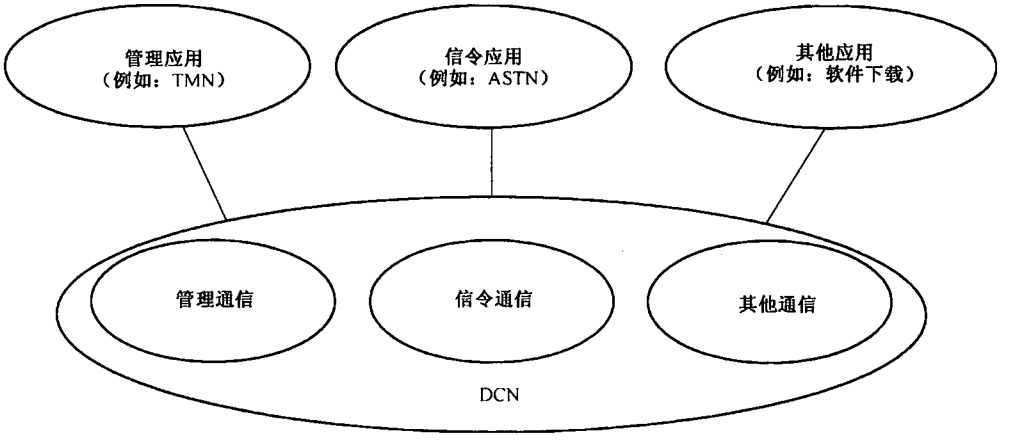


图 62　DCN 应用

ASON 的 DCN 应由两部分组成：管理通信网（MCN）和信令通信网（SCN）。MCN 主要是为 ASON 中管理平面与其他平面之间的信息交互传递管理信息；SCN 主要是为 ASON 中控制平面的分布式控制提供信令的传送通道。信令传送通道是在网络节点之间以及穿越 UNI 传送控制消息的通信信道。控制消息包括信令消息、路由消息、控制维护协议消息如邻居和业务发现等。MCN 和 SCN 可以使用相同的物理传送通道，也可以采用不同的物理传送通道。

DCN 应支持网络的第一层（物理层）、第二层（数据链路层）和第三层（网络层）功能，并提供路由/交换功能。DCN 的通信链路由各种接口实现，包括嵌入式控制通路（ECC）、局域网（LAN）接口和广域网（WAN）接口。

14.1.1　DCN 传送方式

DCN 主要采用两种消息传送方式：光纤内方式和光纤外方式。

a）　光纤内（In-fiber）方式：光纤内方式是指管理和信令消息由光纤链路内部的嵌入在传送业务信息中的 ECC 或专用信道承载，例如：SDH 中的 DCC 开销、OTN 中的 GCC 开销和光监控信道（OSC）中的通信开销。

b）　光纤外（Out-of-fiber）方式：管理和信令消息由专用的通信通道来承载，它与承载业务信息的光纤链路分离，例如：外部 IP 网络或专用电路。

在 ASON 网络中，DCN 可以采用光纤内方式，也可以采用光纤外方式，或者两者相互混合实现。

当 DCN 采用光纤内方式（如 ECC）时，上层协议封装可选择以下方式实现：

——OSI/LAPD/DCC；

——IP/PPP（HDLC）/DCC；

——MPLS/PPP/DCC。

当 DCN 采用光纤外方式（如 LAN）时，上层协议封装可选择以下方式实现：

——OSI（CLNP/IS-IS/ES-IS）/802.3；

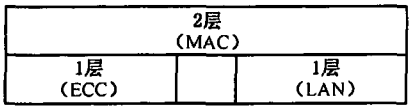
——IP/ETHERNET II；

——MPLS/ETHERNET II。

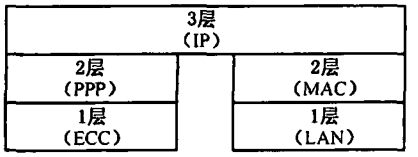
14.1.2　DCN 协议互连要求

ASON 可采用基于 IP 的 DCN、基于 OSI 的 DCN 或混合（IP 和 OSI）DCN 网络。当 DCN 是 ECC 和 LAN 的混合网络时，应考虑 ECC 与 LAN 之间的 DCN 互连。

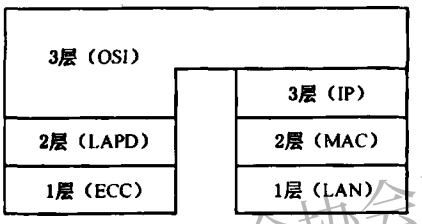
图 63 描述了 DCN 协议互连的实例。实例 a)描述了不同物理层通过公共的第二层协议实现互连，即：将 MAC 帧从 LAN 接口桥接到 ECC 接口。实例 b)描述了不同数据链路层协议通过公共的第三层协议实现互连，即：将 LAN 接口的 IP 分组路由到 ECC 接口上。实例 c)描述了不同网络层协议通过第三层隧道功能来实现互连，该实例是将 OSI 分组封装到 IP 报文中，当然 IP 分组也可以封装到 OSI 报文中。



a) 第二层协议互连



b) 第三层协议互连



c) 第三层隧道功能

图 63 DCN 互连实例

14.2 管理通信网(MCN)要求

电信管理网(TMN)应具有一个管理通信网(MCN)，用来在 TMN 组件(如 NEF 构件和 OSF 构件)之间传递管理信息。由于 ASON 管理平面可以看作是 TMN 的功能延伸，因此 ASON 中的管理平面与 TMN 所使用的管理通信网应是等效的。

14.2.1 MCN 可靠性要求

MCN 应满足以下可靠性要求：

a) 当发生单个故障时，MCN 的设计仍然能保证重要管理消息的传送；

b) 当 MCN 发生网络拥塞时，MCN 的设计应保证用于纠正失效或网络故障的管理消息不会被阻塞或过度延迟；

c) MCN 冗余设计：提供紧急功能的网管系统和网元需要多条通道接入 MCN。

14.2.2 MCN 安全性要求

MCN 应满足以下安全性要求：

a) MCN 应保证用户在未经许可的情况下无法获取网管和网元中的信息；

b) MCN 应保证通信和存储的数据的私密性；

c) MCN 应保证通信和存储的数据的完整性；

d) MCN 应对安全相关的行为进行记录，对非法的动作提供告警；

e) MCN 中的网元应该提供关闭组网中未用的通信通道的功能，以避免不安全的接入；

f) MCN 安全性要求可参考 ITU-T M.3016 的规定。

14.3 信令通信网(SCN)要求

ASON 的信令通信网(SCN)用来在控制平面元件(如 CC 元件)之间传送信令消息。SCN 应符合 ITU-T G.7712 的规定。

14.3.1 SCN 一般要求

SCN 应符合 ITU-T G.7712 的要求，还应满足以下一般要求：

a) 应保证各通信节点可靠地访问信令通信网。

b) 信令通信网应支持可靠的消息传递，应具有拥塞控制机制。

c) 信令通信网应具有自己的管理和维护机制。

d) 信令通信网应支持消息的优先级，使对时间敏感的消息（如用于恢复的消息）比其他消息（如连接信令消息、拓扑、资源发现消息）具有更高的优先级。

e) 信令通信网应具有高可靠性和故障恢复的能力。

f) 如果采用隧道技术在 IP 数据网上组建 SCN，必须采用基于标准的隧道技术，如 L2TP，GRE，MPLS 等。

g) SCN 应具有相应的安全机制，防止未经授权的用户非法接入。

14.3.2 SCN 可靠性要求

SCN 应满足以下可靠性要求：

a) 为了提高 SCN 的可靠性以满足 ASON 保护恢复要求，SCN 自身应能提供保护和恢复机制。

1) 对于无连接的 SCN 网络，可通过路由更新或其他方式提高 SCN 的可靠性；

2) 对于面向连接的 SCN 网络（例如在 SCN 中支持 MPLS），可通过 1+1 保护方式提高 SCN 的可靠性。（可选）

b) SCN 应保证恢复消息的可靠和快速传送。

14.3.3 SCN 安全性要求

SCN 可以在不同管理域之间提供信令传送通道。在管理域边界，只允许管理域之间满足要求的消息通过域间接口，不满足要求的消息禁止通过域间接口。SCN 必须保证只有两个管理域都允许的消息才能通过域间接口。

15 ASON 网络的保护和恢复要求

15.1 保护和恢复的定义

15.1.1 保护的定义

“保护”是指用一个预先分配的备用资源来代替一个失效资源。一旦该资源因为保护的目的而被分配，则不能用于重路由，在中间节点为保护配置的资源不因保护倒换而改变。

控制平面（特别是连接控制元件）负责连接的建立，包括工作连接和保护连接的建立，或者为某种保护方式提供连接配置信息。ASON 网络支持的保护机制可分为两种类型：基于传送平面的保护和基于控制平面的保护。基于传送平面的保护，保护的配置由管理平面完成。基于控制平面的保护，保护的配置是由控制平面完成。基于控制平面的保护发生在控制平面保护域的源节点和宿节点之间，通过源节点和宿节点之间的协调来完成保护机制的操作。出现故障的时候，保护不涉及重路由，也不涉及在中间的连接控制器处建立另外的连接，仅涉及源节点和宿节点的连接控制器。

15.1.2 恢复的定义

“恢复”是指通过使用网络的空闲容量重新选路来替代出现故障的连接。与保护相比，在恢复过程中，支持连接的部分或全部 SNP 可能被更改。

基于控制平面恢复的发生与重路由域相关。重路由域是一组呼叫和连接控制器的元件集合，共同承担基于域的重路由的控制。基于域的重路由操作发生在重路由域的边界，并且完全包含在这个域内。在重路由域边缘的元件负责协调基于域的的重路由操作，这些操作涉及到穿越重路由域的所有呼叫和连接。

重路由域必须完全包含在路由域或路由区内，一个路由域可以完全包含若干个重路由域。与重路由域相关的网络资源必须完全包含在一个路由区内。对于单个重路由域，域内重路由操作在该域内的

源和宿元件之间协商，域内重路由请求不超越域的边界。当涉及多个重路由域时，每个重路由域边界的元件为呼叫协商穿越该域的重路由操作。虽然重路由是基于端到端的请求，但这种操作是在每个重路由域基础上执行的。恢复可分为硬重路由和软重路由两种类型。

硬重路由机制提供了呼叫连接失效时的恢复机制，并能响应失效事件。

对于一个已激活硬重路由的呼叫连接，源节点阻止呼叫释放，并试图在重路由域边界建立一个到宿节点的替代连接段，即重路由连接。在重路由域边界的宿节点同样阻止呼叫连接的释放，并等待重路由域边界的源节点建立一个重路由连接。对于硬重路由，可以采用“先拆后建”(初始的连接段在重路由连接建立之前被释放，即 break-before-make)或“先建后拆”(初始的连接段在重路由连接建立之后被释放，即 make-before-break)的方式。

根据重路由的呼叫在故障清除后是否返回初始连接，可有非返回和返回两种操作方式。如果要求重路由支持返回操作，当故障清除后呼叫连接必须返回到初始连接。

软重路由机制是一种出于管理目的(如路由优化，网络维护，工程规划工作)的呼叫重路由机制。当一个软重路由操作被激活(通常由管理平面发起请求)，重路由元件建立一个到指定元件位置的重路由连接，一旦该连接被建立，重路由元件使用这个连接并删除初始的连接，这称为“先建后拆”(make-before-break)。

在软重路由过程中，初始连接可能会失效，此时硬重路由操作的优先级高于软重路由，在重路由域内的源和宿节点按照硬重路由进行操作。

15.2 保护和恢复的基本要求

ASON 网络的保护和恢复机制应支持以下基本要求：

a) 保护和恢复机制应与传送网所承载的业务无关，并支持多种业务(如 IP、ATM、SDH、以太网)。

b) 保护和恢复机制必须满足网络的可扩展性，即随着网络规模的扩大，保护恢复时间仍应满足性能要求。

c) 保护和恢复机制应提供相应的机制来适应服务层的灾难性故障，如光缆切断将会引起大量的客户层连接同时发生保护和恢复。

d) 保护和恢复机制应采用可靠有效的信令机制并结合 SCN 自身的可靠性机制，最大程度的保证保护恢复机制在各种网络状态下维持其功能。

e) 传送平面上的信号失效和劣化应由传送平面自身进行监视和检测，并实时通告给控制平面和管理平面来产生信号失效告警和信号劣化告警。保护和恢复的启动可以采用基于传送平面的故障检测、定位和通告机制(如 LOS、AIS 和 BER 越限等)，或者利用控制平面的故障定位和通告机制。

f) ASON 设备应支持基于传送平面的保护(如传统的 SDH 网络保护、OTN 的网络保护)、基于控制平面的保护、基于控制平面的恢复机制。

g) 出于管理和维护的目的，管理平面应支持人工发起的保护和恢复的倒换操作，以及对保护和恢复参数的修改。

h) 保护和恢复机制应支持故障清除后的自动返回或人工返回机制，管理平面应可设定返回的等待恢复(WTR)时间。

i) 正常的连接管理操作不应导致保护和恢复的发生。

j) 根据业务的服务级别协议，在保护机制失败后可对业务进行实时的动态恢复。

k) 当受故障影响的连接无法恢复时，应释放未完成的恢复连接所占用的全部资源，并通知上下游节点和网管系统。

l) 在恢复过程中，可能出现以下异常情况：

1) 控制信道拥塞或者控制平面失效，导致网络未能进行重路由；

2） 选定恢复路径后，此时恢复路径出现故障，导致业务倒换后仍然是中断状态；

3） 网络中资源不足或选定的恢复路径上资源不足，不能承载所有被恢复业务。

以上情况导致部分或全部业务不能正常被恢复，此时应当周期性地尝试建立恢复路径，并完成恢复操作。

m） 保护和恢复机制应能支持域内的保护恢复和域间的保护恢复。

以下保护和恢复要求为可选：

a） 共享的保护通道和空闲的恢复资源可用于承载额外业务，该额外业务为低等级的无保护业务，当保护通道和空闲资源需要被发生保护恢复的业务占用时，该额外业务应被预先清空。

b） 可支持不同的连接优先级，包括建立优先级和恢复优先级。

1） 连接的保护恢复操作高于具有相同优先级的连接建立请求。

2） 当多个连接同时发生故障时，连接的源节点可以按恢复优先级对连接进行恢复，即优先执行高优先级的连接恢复。

3） 在连接恢复过程中，当不同连接发生资源竞争时，应按照连接的恢复优先级分配资源，即高恢复优先级的连接可以得到资源。

15.3 基于传送平面的保护

基于传送平面的保护可分为 SDH 的网络保护和 OTN 的网络保护。

SDH 网络保护的实现机制、保护目标、倒换准则、倒换命令、保护倒换协议和保护倒换时间应符合 YDN 099—1998 和 YD/T 1078—2000 的具体规范。

OTN 网络保护的实现机制、保护目标、倒换准则、倒换命令、保护倒换协议和保护倒换时间应符合 ITU-T G.873.1 和 ITU-T G.873.2 的具体规范。

15.4 基于控制平面的保护

15.4.1 基于控制平面的保护类型

基于控制平面的保护的配置由控制平面完成，保护倒换的实施可基于传送平面或者控制平面。基于控制平面的保护类型可分为路径保护和子网连接(SNC)保护。

15.4.1.1 路径保护

路径保护用于保护跨越一个或多个运营者网络的业务路径，适用于网状网、环网等网络拓扑结构，对路径上的节点数目没有限制。路径保护主要保护服务层上的故障，以及用户层的连接故障和性能劣化。

按照保护对象的数目，路径保护可以分为单个保护和组保护。单个保护是指仅保护所有业务中的一个业务，网络中的其余业务不受保护；而组保护可以保护在同一个服务层路径中传送的大部分业务，组保护可以通过逻辑捆绑的方式实现快速倒换。

15.4.1.1.1 单个路径保护

在路径保护中，两个独立的路径分别作为被保护业务的工作和保护传送实体。路径终端设备的功能是生成和插入、监测并提取端到端开销/OAM 信息，以此判断工作和保护传送实体的状态。单个路径保护包括 1+1、1∶1/1∶n 和 m∶n 保护。

a） 1+1 路径保护

1+1 路径保护可以采用单向或双向倒换机制。

在单向 1+1 路径保护中，业务在源节点被永久桥接到工作路径和保护路径，并且在宿节点选择接收。出现故障时，只有受影响方向上的业务会发生倒换。

在双向 1+1 路径保护中，业务在源节点被永久桥接到工作路径和保护路径，在正常情况下，源节点和宿节点分别从工作路径上的相应方向接收业务。出现故障时，业务的两个方向都会发生倒换。

b） 1∶1/1∶n 路径保护(可选)

在 1∶1/1∶n 路径保护方式下，为两个节点之间的 n 个工作路径事先设置好 1 个保护路径，该保护路径可以承载额外业务。n 个工作路径中任何一个出现故障，将会导致受影响的业务倒换到保护路径上，保护路径上的额外业务应预先清空以承载被保护的业务。当多个工作路径发生故障时，只能有 1 个工作路径被保护。

c) m∶n 路径保护(可选)

m∶n(m,n≥1,m≤n)保护，n 条工作路径被 m 条保护路径保护。n 条工作路径中的任何一条路径出现故障，可以倒换到 m 条保护路径中的一条。m∶n 路径保护方式如下：

1) 任何时间，两个节点之间存在两组路径，n 条工作路径和 m 条保护路径，保护路径可以承载额外业务，在两个路径组内的路径之间没有一一对应关系。

2) 当业务从工作路径倒换到保护路径时，路径两端的节点应协调由其中一个节点来选择保护路径。

3) n 条工作路径可以支持优先级，当多条工作路径同时发生故障时，高优先级的工作路径优先倒换到保护路径。

15.4.1.1.2 组路径保护(可选)

在组路径保护中，采用 2×n 个并行独立的路径分别作为被保护业务的 n 个工作和保护传送实体，由路径保护子层连接功能实现该组内 n 个并行的业务信号的保护操作。路径终端的功能是生成和插入、监测并提取端到端开销/OAM 信息，以此判断工作和保护传送实体的状态。

组路径保护包括 1+1、1∶1/1∶n 和 m∶n 保护。

15.4.1.2 子网连接(SNC)保护

子网连接(SNC)保护可用保护完整的端到端路径，或者仅保护路径的一部分。在子网连接(SNC)保护中，缺陷条件的检出在服务层网络或传送层网络，保护倒换的激活发生在客户层网络。子网连接保护适用于任何网络结构(网状网，环网或者混合结构)，被保护的子网连接可以位于两个连接点 CP 之间，一个 CP 和一个 TCP 之间，或者是在两个 TCP 之间的完整的端到端网络连接。

根据对缺陷条件的监视的不同，子网连接保护可以划分为固有监视(Inherent)、非介入监视(Non-intrusive)和子层路径监视(Sublayer)三种方式。

a) 固有监视(Inherent)：由服务层路径终端和适配功能模块判决 SF/SD 状态，只支持监测服务层缺陷。

b) 非介入监视(Non-intrusive)：由非介入监测模块判决 SF/SD 状态，可监测端到端或子层网络的服务层缺陷、分层网络的连续性/连接性缺陷和误码劣化状态。该监视启用了端到端或者子层的开销/OAM。

c) 子层路径监视(Sublayer)：由串联连接/段子层模块判决 SF/SD 状态。可监测端到端或子层网络的服务层缺陷、分层网络的连续性/连接性缺陷和误码劣化状态。该监视启用了子层的开销/OAM。

SNC 保护需要在工作和保护链路上创建子层路径(串联连接，段)，以确定故障或劣化是在被保护域之前，还是在被保护域之后发生的。当子层路径仅包含一个服务层路径时，可以使用该服务层路径的固有监视。如果被保护域的入口节点和出口节点之间没有创建子层路径，或者服务层路径不可用，可以通过向工作和保护链路同时馈入业务信号的方式实现 SNC 保护，在出口节点非介入监测两个路径来的信号，对比 SF/SD 状态。如果故障或劣化发生在被保护域之前，工作和保护监测器可以发现损伤但不作出任何保护倒换操作。如果故障或劣化发生在被保护域之后，工作和保护监测器中的一个将检测到 SF/SD 状态，执行保护倒换操作。

SNC 保护类型可以分为单个保护和组保护，其中组保护为可选。单个保护可以分为 1+1、1∶n、m∶n SNC/S 保护，1+1 SNC/N 保护和 1+1/1∶n SNC/I 保护，其中 1∶n、m∶n 保护为可选。组保护可以分为 SNC/S、1+1 SNC/N、1+1 SNC/I 和 SNC/T 保护。

15.4.2 保护路径计算的约束条件

保护路径计算的约束条件可以遵循以下原则：

a) 保护路径经过的节点数量最少；

b) 保护路径经过的链路代价之和最小；

c) 保护路径与工作路径应满足：

1) 节点分离约束：除源节点和宿节点外，保护路径与工作路径经过的节点完全不同。

2) 链路分离约束：保护路径与工作路径经过的链路完全不同。

3) 共享风险链路组(SRLG)分离约束：保护路径与工作路径采用的 SRLG 完全不同的链路。

15.4.3 保护倒换准则和倒换命令

15.4.3.1 路径保护

基于控制平面的 SDH 路径保护应支持的倒换准则为：

a) 信号丢失(LOS)；

b) 帧丢失(LOF)；

c) 复用段的告警指示信号(MS-AIS)(针对复用段层路径保护)；

d) 复用段信号的误码超过信号失效或劣化门限(针对复用段层路径保护)；

e) 高阶/低阶通道的告警指示信号(AU-AIS 或 TU-AIS)(针对 VC 路径保护)；

f) 指针丢失(AU-LOP 或 TU-LOP)(可选)(针对 VC 路径保护)；

g) 通道信号的误码超过信号失效或劣化门限(针对 VC 路径保护)。

基于控制平面的 OTN 路径保护应支持的倒换准则为：

a) 信号丢失(LOS)、净荷丢失(LOS-P)；

b) 复帧丢失(LOM)、净荷失配(PLM)；

c) 前向缺陷指示(FDI)、净荷前向缺陷指示(FDI-P)。

基于控制平面的路径保护应支持强制倒换、人工倒换、保护锁定、清除等网管倒换命令，并满足相应的优先级原则。

15.4.3.2 子网连接(SNC)保护

基于控制平面的 SDH 子网连接保护应支持的倒换准则为：

a) 信号丢失(LOS)；

b) 帧丢失(LOF)；

c) 高阶/低阶通道的告警指示信号(AU-AIS 或 TU-AIS)；

d) 指针丢失(AU-LOP 或 TU-LOP)(可选)；

e) 通道信号的误码超过信号失效或劣化门限。

基于控制平面的 OTN 子网连接保护应支持的倒换准则为：

a) 信号丢失(LOS)、净荷丢失(LOS-P)；

b) 复帧丢失(LOM)、净荷失配(PLM)；

c) 前向缺陷指示(FDI)、净荷前向缺陷指示(FDI-P)。

基于控制平面的子网连接保护应支持强制倒换、人工倒换、保护锁定、清除等网管倒换命令，并满足相应的优先级原则。

15.4.4 返回机制

基于控制平面的保护可以支持被保护业务的自动返回或人工返回功能。对于自动返回方式，在消除造成倒换的故障后，经过一定返回等待时间(WTR)，被保护业务应自动返回到原来的工作路由，返回等待时间应可以设置。

返回操作对业务的受损时间应在 50 ms 以内。

15.4.5 保护倒换时间要求

a) 基于控制平面的1+1路径保护和1+1子网连接保护，业务受损时间应在50 ms以内。

b) 基于控制平面的1∶1/1∶n、m∶n路径保护和1∶1/1∶n、m∶n子网连接保护，业务受损时间应小于200 ms(暂定)。

15.5 网络恢复

15.5.1 网络恢复的类型

ASON网络恢复的类型可以分为端到端恢复和本地恢复。本部分主要提出端到端恢复的要求，对于本地恢复的要求待研究。

根据端到端恢复路径的建立方式，可以进一步划分恢复类型。恢复路径的建立过程可以分为计算路由、交换建立恢复路径的信令和选择资源三个部分，如图64所示。

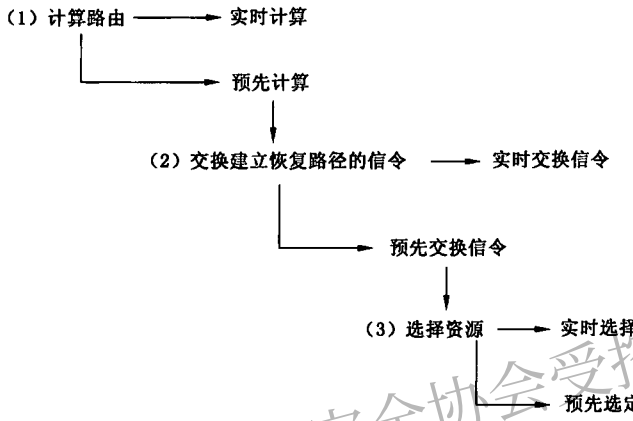


图64 恢复路径的建立过程

恢复路径的建立过程为：

a) 恢复路径可以是预先计算好或按需实时计算。

b) 考虑到信令交换过程的差异，分为预先完成信令交换或实时进行信令交换。如果是预先进行信令交换，控制平面在故障发生前需要将与恢复相关的信令传送各个相应节点。如果实时进行信令交换，则在故障发生后交换信令。

c) 当信令是预先交换的，恢复资源的选择可以是预先选定或实时选择。

d) 对于网络恢复机制，故障发生前恢复路径上不进行交叉连接资源配置。

根据建立恢复路径的信令交换时机，网络恢复类型可以分为预置重路由恢复和动态重路由恢复，其中预置重路由恢复为可选。预置重路由恢复在故障发生前预先进行信令交换建立恢复路径，而动态重路由则是在故障发生后才进行信令交换来建立恢复路径。

15.5.1.1 预置重路由恢复(可选)

预置重路由的特征是在故障发生前，为工作路径预先计算出一个端到端恢复路径，并预先交换信令来预留资源。对于源节点和宿节点，同时建立工作路径和恢复路径，但此时恢复路径并未被完全启用，不能承载业务，在故障发生后需要激活这个恢复路径以承载受影响业务。

根据恢复资源是否预先选定有两种情况：

a) 资源预留但不预先选定资源

建立恢复路径的信令沿着预先选定的路径传送，在每个节点将资源预留下来，但不具体选定资源。

b) 资源预留且资源预先选定

建立恢复LSP的信令沿着预先选定的路径传送，在每个节点将资源预留下来，并选定具体资源，但不做交叉连接。

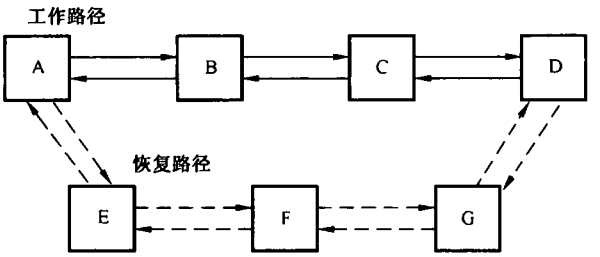


图 65 预置重路由恢复

预置重路由恢复的示例如图 65 所示。工作路径为 A-B-C-D,恢复路径为 A-E-F-G-D,正常状态下,只有工作路径是激活的,恢复路径上不承载业务。假设工作路径上的 B 节点检测到故障,就会通知节点 A,开始激活恢复路径。

恢复路径可以是专用的或共享的。如果是共享的,则网络中其他工作路径出现故障后,可以使用该恢复路径上的资源,此时,控制平面应当自动为该恢复路径对应的工作路径再建立一条恢复路径。

共享网状网恢复,是预置重路由恢复的一种特例。在假设多个工作路径不重合(链路、节点、SRLG)的前提下,允许多个工作路径可以共享恢复路径的资源,这些工作路径的源节点和宿节点可以相同或不同。从参与恢复的节点的反馈信息中可以了解到资源共享的情况。

共享网状网恢复的示例如图 66 所示。两个业务工作路径分别为 A-B-C-D 和 H-I-J-K,各自的恢复路径分别是 A-E-F-G-D 和 H-E-F-G-K,因此 E-F-G 是被两个工作路径共享的恢复路径。

假设 B 节点检测到故障,通知到节点 A,将激活恢复路径 A-E-F-G-D。这种情况下,如果节点 I 再检测到故障,这时节点 H 就不应当再将 H-E-F-G-K 作为恢复路径。因此,在恢复路径 A-E-F-G-D 被激活后,节点 E 应当通知节点 H 恢复路径 H-E-F-G-K 不再可用,需要再计算新的恢复路径。

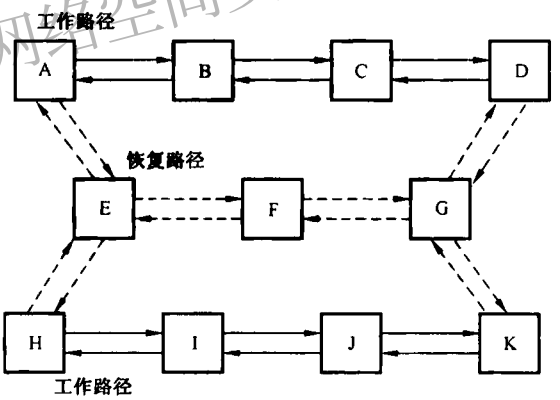


图 66 共享网状网恢复

15.5.1.2 动态重路由恢复

对于动态重路由恢复,在故障发生前,恢复路径不事先建立。一旦故障发生,利用信令实时地建立恢复路径。如果当前的工作路径再出现故障,又会再次进行重路由。恢复路径的计算依赖于故障信息、网络路由策略和网络拓扑信息等。

恢复路由的计算应采用一定的机制,来排除故障节点和链路。恢复路由可以选择原工作路由中未发生故障的节点和链路。

当故障发生后,检测到故障的节点应判断该故障是否需要启动恢复进程,然后该节点应向业务的上游节点发送一个故障指示信号(FIS)。FIS 可以由中间节点逐跳传递并最终到达源节点,也可以直接被传递到源节点。源节点终结 FIS 并触发恢复操作。由于 FIS 是控制消息,它的传送应设为高优先级。

恢复操作可以由源节点发起,也可以由外部命令(管理平面)发起。

15.5.2 恢复路由计算的约束条件

ASON 控制平面应支持以下恢复路由计算的约束条件及其组合：

a) 恢复路径经过的节点数量最少。

b) 恢复路径经过的链路代价之和最小。

c) 恢复路径与工作路径满足以下条件之一：

1) 节点分离约束；

2) 链路分离约束；

3) SRLG 分离约束。

d) 负载均衡。

15.5.3 网络恢复的倒换准则

基于 SDH 机制的网络恢复应支持的倒换准则为：

a) 信号丢失(LOS)；

b) 帧丢失(LOF)；

c) 高阶/低阶通道的告警指示信号(AU-AIS 或 TU-AIS)(可选)；

d) 指针丢失(AU-LOP 或 TU-LOP)(可选)；

e) 高阶/低阶通道信号超过信号失效或劣化门限。

基于 OTN 机制的网络恢复应支持的倒换准则为：

a) 信号丢失(LOS)、净荷丢失(LOS-P)；

b) 复帧丢失(LOM)、净荷失配(PLM)；

c) 前向缺陷指示(FDI)、净荷前向缺陷指示(FDI-P)。

15.5.4 恢复的倒换方式和返回机制

a) 恢复的倒换方式

恢复的倒换方式可以分为单向倒换和双向倒换。

在单向倒换中，只有受影响方向上的业务会发生倒换，另外一个方向上的业务不倒换。

在双向倒换中，业务的任一方向出现故障，将会导致业务的双方向都倒换到恢复路径。

b) 恢复的返回机制

恢复的返回机制定义为当工作路径上的故障清除后，经过等待恢复(WTR)时间，业务从恢复路径自动返回到工作路径。等待恢复(WTR)时间应可以设置。在原工作路径上的一个 SF 或 SD 状态会导致 WTR 计时器重新开始。

应支持对业务设置返回或者非返回方式。返回操作对业务的受损时间应小于 50 ms。

返回进程包括：

1) 业务在故障清除后自动返回到工作路径；

2) 在 1)之后，具有将恢复路径去激活的能力，该操作不应影响正常业务；

3) 单向倒换的返回不应影响业务另一方向的正常工作。双向倒换的返回操作应在两个方向进行。

15.5.5 恢复的倒换时间要求

由于恢复的倒换时间与网络规模、网络配置的业务量等具体情况密切相关，因此恢复倒换时间的具体指标待定。

15.5.6 软重路由

软重路由可应用于无保护业务，保护(工作连接和保护连接)和恢复的业务。

软重路由的路径选择可以支持人工指定和自动选择。在自动选择方式下，路由选择应遵循动态重路由的约束条件。

软重路由的业务受损时间应小于 50 ms。

15.5.7 恢复的优先级(可选)

ASON 网络可为连接配置相应的恢复优先级。当多个连接同时发生故障时,如果空闲的网络资源不足以恢复所有连接,连接的源节点可以按恢复优先级对连接进行恢复,即优先执行高优先级的连接恢复。在连接恢复过程中,当不同连接发生资源竞争时,应按照连接的恢复优先级分配资源,即高恢复优先级的连接可以得到资源。

15.6 保护和恢复结合(可选)

ASON 网络可支持基于传送平面的保护与动态恢复的结合。在配置了传送平面保护机制的网络中,如果工作路径出现故障,业务首先会被倒换保护路径上,如果保护路径再出现故障,为保证业务的生存能力,ASON 网络可为其提供相应的恢复能力;在保护路径出现故障的前提下,工作路径再出现故障时可直接启动业务的恢复。

可以支持以下基于传送平面的 SDH 保护与动态恢复的结合:

a) 2 纤/4 纤复用段环网保护与动态恢复结合;

b) 1+1/1∶n MSP 与动态恢复结合;

c) SNCP 与动态恢复结合。

保护与动态恢复的结合可支持在所有的故障清除后,业务返回到原工作路径。由于保护与恢复是在不同的层面中实现,应采用一定的机制协调二者之间的关系。

基于传送平面的 OTN 保护与动态恢复的结合待研究。

ASON 网络可支持基于控制平面的保护与动态恢复的结合。如果工作路径出现故障,业务首先会被倒换保护路径上,如果保护路径再出现故障,可为其提供相应的恢复能力;在保护路径出现故障的前提下,工作路径再出现故障时可直接启动业务的恢复。可以支持以下基于控制平面的保护与动态恢复的结合:

a) 1+1 路径保护与动态恢复结合;

b) 1∶n/m∶n 路径保护与动态恢复结合;

c) 1+1 子网连接保护与动态恢复结合;

d) 1∶n/m∶n 子网连接保护与动态恢复结合;

e) 永久 1+1 保护,即控制平面同时监测工作路径和保护路径的故障情况,若其中任何一个路径发生故障,则在业务发生倒换的同时启动重路由机制为当前的工作路径建立一条新的保护路径,以保证最高服务质量的业务几乎在任何时间均具有 1+1 保护。

保护与动态恢复的结合可支持在所有的故障清除后,业务返回到原工作路径。基于控制平面的保护与动态恢复的结合应采用一定的机制协调二者之间的关系。

15.7 多域的保护恢复

单层网络可分为若干域。多域的保护恢复分为域内保护恢复和域间保护恢复。域内故障应仅触发域内的保护恢复机制,域间故障应触发域间的保护恢复机制。

15.7.1 域内保护恢复

任何在重路由域内的故障都应当触发重路由操作,下游域只监测到瞬间的输入信号失效而不进行任何重路由操作。恢复后的连接应继续使用重路由域内原来的入口和出口网关节点。

15.7.2 域间保护恢复

重路由域的域间故障包括两种情况:域间链路故障和域间网关网元故障。

a) 域间链路故障

当在重路由域间出现故障时(重路由域 A 和 B 内的两个网关网元间的链路,见图 67),域内应不执行重路由操作,域间可启用链路保护机制。

图 67 中域 A 和域 B 之间的网关节点 A-2 和 B-1 之间配置了两条链路,当工作链路失效时会启动域间链路保护操作,连接仍然使用相邻域间原来的入口和出口网关网元。

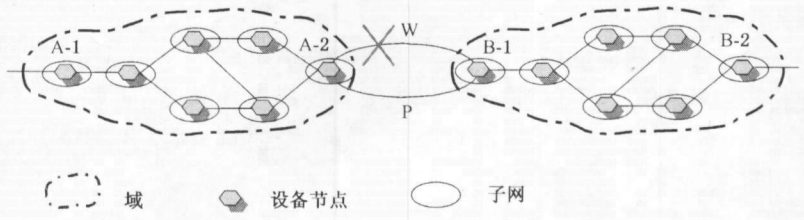


图 67　域间链路故障

b)　域间网关网元故障

为了实现对域间网关网元故障的保护，每个域内可设置两个不同的网关网元。

图 68 中，当 B-1 失效时，为了恢复连接，应启用另外一个网关节点 B-3。同样还要求启用域 A 内的另外一个网关节点 A-3。在域 A 内应启用 A-1 到 A-3 的连接，并避免 A-1 和 A-2 之间的重路由。

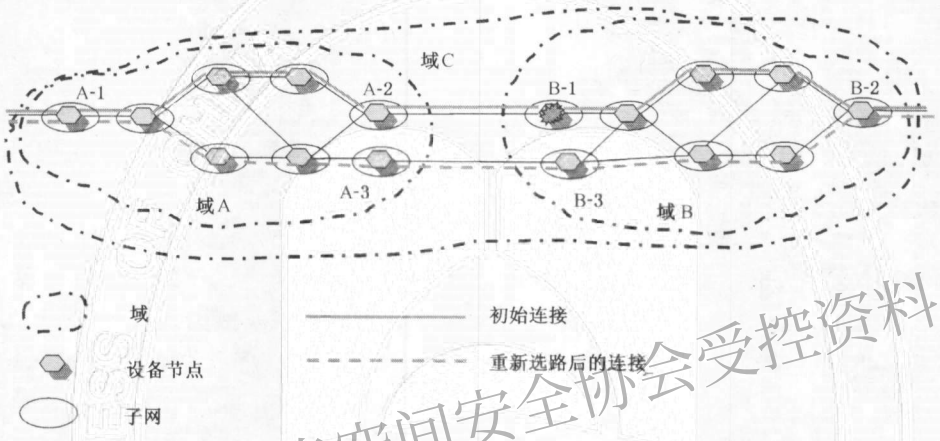


图 68　域间网关网元故障

15.8　多层次的保护恢复

当 ASON 网络的传送平面为多层网络时，每个层网络具有一定的保护恢复机制。为了实现强壮和快速的恢复，多层的保护恢复机制需要有机的协调，一般底层恢复机制比高层更有效和快速，可以通过禁止或延缓高层恢复的方式来实现。

16　控制平面生存性要求

16.1　控制平面生存性

控制平面生存性是指在控制平面出现失效的情况下，ASON 能够继续工作的能力。控制平面的故障主要由信令网络的连接故障和软件故障(比如信令，拓扑和资源发现模块)引起。各种 ASON 控制元件的故障会造成不同的影响：

a)　呼叫控制器：其故障会导致无法建立新的呼叫和拆除已存在呼叫。

b)　连接控制器：其故障会导致无法建立新的连接和拆除已存在连接。由于呼叫控制信令需要经过连接控制器执行，所以连接控制器的故障也可能影响呼叫控制器。

c)　路由控制器：其故障会导致新的连接建立请求和路由数据库同步请求无法完成。路由控制器故障还将影响连接控制器以及网管对于路由信息的请求。

d)　链路资源管理器：其故障会导致无法进行新的连接建立、已存在连接的拆除和 SNP 数据库同步。路由控制器也会受到链路资源管理器故障的影响。

ASON 必须采取一定的措施，保障控制平面的生存性。控制平面生存性应满足以下要求：

a)　控制平面应能监测控制信道失效和软件进程失效。

b)　控制平面的部分故障或全部故障不能影响已建立的呼叫和连接，仅影响新到达的呼叫和连接

建立请求，新连接的建立可以由网管完成。

c) 控制平面应能利用信令消息的优先级机制来保证保护和恢复消息得到优先处理，从而保证网络保护和恢复得到快速执行。

d) 信令网络应支持自身的保护和恢复机制，信令网络内部出现失效时可以进行自愈。同时，信令网络的保护恢复机制不能与传送平面的保护恢复机制发生冲突。

e) 信令网络故障不应引起呼叫和连接的释放。如果信令通道故障不能恢复，控制平面应将信令通道的故障通知管理平面。在信令通道恢复后，控制平面应能继续接受新的请求。

f) 应支持控制模块的冗余配置，以便应对控制模块自身的故障。当故障发生时应能自动倒换到备用模块上，并且不丢失消息和状态信息。

g) 控制平面的生存性机制应支持单点失效和多点失效。控制平面应支持故障定位技术，以隔离失效的控制资源。

h) 控制平面故障恢复后，应释放或继续完成等待中的呼叫和连接建立请求，完成等待中的呼叫和连接拆除请求。

i) 控制平面的失效应通知管理平面。当控制平面上发生持久故障或在特定情况下，应由能通知管理平面接替其控制工作并进行人为干预。

j) 控制平面节点应支持相关信息的永久存储，例如对呼叫和连接状态信息，以及控制平面邻居信息进行永久存储。

k) 控制平面节点应支持与外部元件的通信，在故障恢复以后，对由于控制平面失效而造成丢失的信息应进行同步。外部元件包括相邻控制平面节点的元件和集中的永久存储元件（例如管理平面）。

l) 控制平面节点在不能恢复相关信息时应通知管理平面。管理平面可采取以下措施：

1) 释放受影响的连接；

2) 保留受影响的连接。这时连接与控制平面处在不同步状态，但连接仍然有效。

16.2 控制平面生存性的保证机制

16.2.1 控制平面和传送平面的交互原则

控制平面和传送平面之间的交互应遵循以下原则：

a) 控制平面依赖于传送平面所提供的传送平面资源信息。

b) 首先应建立控制平面和本地传送网络单元之间的一致性（垂直一致性）。

c) 当垂直一致性建立后，应建立控制平面视图的水平一致性。控制平面元件与其邻居控制元件进行同步，建立路由、呼叫和连接状态的统一视图。

d) 控制平面发生故障以及故障恢复时，传送平面已有的连接不应被修改。

为了满足控制平面生存性要求，应采用一个永久存储器来保存传送平面资源信息、子网连接（SNC）状态信息、有关控制平面的 SNC 的状况（包括 SNC 是否通过连接管理模块建立以及 SNC 是如何使用的）。

在任意 ASON 节点上，控制平面必须保证其资源、SNC 状态信息与传送网元维护的资源和 SNC 状态信息一致。如果发生不一致，ASON 节点的控制元件应：

——向邻居节点发布可用资源为零的信息，保证新的连接请求不应经过该节点进行路由。

——不进行任何连接修改（例如拆除）。

在控制平面恢复期间，控制平面重新建立已有连接的呼叫和连接状态。控制平面元件与传送网元之间重新建立信息一致性的工作，应按照以下顺序进行：

——链路资源管理器与传送网元状态信息进行同步。

——连接控制器与链路资源管理器进行同步。

——网络呼叫控制器与连接控制器进行同步。

在本地状态一致性建立后，控制平面应在重新参与连接建立或拆除请求之前，保证与邻居节点的SNC状态信息一致。

16.2.2 协议控制器通信的原则

a) 协议控制器实现控制平面元件的通信和协议翻译，协议控制器的生存性对控制平面生存性具有重要影响。

b) 当协议控制器之间的通信中断时，已创建的呼叫和连接不应被改变。如果故障持续并需要操作人员介入(例如释放一个呼叫)，可以通知管理平面。

c) 信令通信网故障可能影响一个或多个协议控制器之间的通信会话。与信令通道关联的协议控制器应监测并上报信令通道故障告警。

d) 当协议控制器之间的通信会话恢复正常后，应进行协议控制器之间的状态重新同步。

e) 协议控制器采用的故障处理方法，与协议控制器之间通信会话的故障处理方法相同。

16.2.3 控制平面和管理平面的交互原则

如果管理平面功能不可用，控制平面功能可能会被削弱。当管理平面功能恢复后，控制平面元件应向管理平面报告在管理平面失效期间进行的操作(例如呼叫记录)。

17 可扩展性要求

17.1 网络可扩展性

可扩展性指ASON控制平面支持不断增长的网络规模和业务请求的扩展能力。为了使ASON业务能够扩展到全球范围，并支持不同的客户信号，控制平面信令和路由机制应具有良好的可扩展性，以便即时响应业务请求。同时，保护和恢复机制应确保业务受损时间在可接受的范围内。

ASON应满足以下网络可扩展性要求：

a) ASON控制平面的地址结构应支持控制平面未来不断增长的需求。

b) ASON控制平面应支持传送平面未来不断增长的需求，应支持光网络节点和端口数量的扩展。

c) 一对节点之间的连接数量不应受到控制平面的限制。

d) 信令通信网(SCN)的拓扑结构应具有可扩展性。

17.2 控制域的分割和合并

随着ASON网络的不断扩大和业务增长的需要，可能需要对ASON控制域进行分割和合并。对分割和合并的要求如下：

a) 控制平面应支持将一个控制域分割为多个控制域。

b) 控制平面应支持将多个控制域合并为一个控制域。

c) 这种分割/合并可以人工进行，也可以自动完成。

d) 这种分割/合并操作不应影响已经建立的连接。

e) 应支持控制域层次的可扩展性。

17.3 路由协议的可扩展性

a) 路由协议应该具有可扩展性，以支持ASON网络在链路容量、链路数量、节点数量、控制域分级数量和网络数量等方面的增长。网元、链路、用户或控制域的增加不应引起路由协议的修改。

b) 随着网络规模的扩展，路由协议应满足其性能指标(具体指标待研究)，路由协议的设计应该使网络规模对其性能的影响最小。

c) 路由协议应使全局性信息尽量少，即尽量使信息留在本地。

d) 路由协议应支持拓扑抽象和连通性摘要，以便使网络具有可扩展性。

17.4 信令协议可扩展性

a) 信令协议应具有可扩展性，以支持 ASON 网络在链路容量、链路数量、节点数量、控制域分级数量和网络数量等方面的增长。网元、链路、用户或控制域的增加不应引起信令协议的修改。

b) 随着网络规模的的扩展，信令协议应满足其性能指标。

18 安全性要求

18.1 ASON 的安全性

由于传送网络是电信网络的基础设施，因此对 ASON 网络需要实施严格的安全措施。ASON 网络的安全性由四部分组成：传送平面的安全性、控制平面的安全性、管理平面安全性以及 SCN 的安全性。

18.1.1 传送平面安全性

传送平面应提供足够的安全机制以保证数据的保密性和完整性。具体要求包括：

a) 应避免传输链路的误连接以确保用户的数据不被传到错误的接收方。

b) 传送平面应能产生告警并向管理平面通告安全相关事件。

18.1.2 控制平面安全性

控制平面的安全是指对控制平面信息流的保护，主要目的是用于保护在不同管理域之间控制信息的交互。ASON 控制平面安全性要求体现在以下几个方面：

a) 应支持 OIF 定义的“UNI 和 NNI 安全扩展”。

b) 敏感的网络信息不能经过外部接口（UNI 或 E-NNI），经过 E-NNI 的信息需要根据设置的策略受到控制和限制，只有在经过认证的实体间才可以进行信息交换。

c) 信令网络应能够拒绝所有未认证的接入。

d) 信令网络的拓扑和地址信息不能泄漏到运营商不信任的区域。

e) 在 UNI 和 E-NNI 交换发现、信令和路由消息时，应支持认证、完整性和机密性等安全机制。

f) 在接入控制平面时，网络操作者需要使用严格的标识、认证和接入控制策略。

g) 控制平面应能够产生告警并向管理平面通告安全相关事件，并在管理平面上建立安全日志。管理平面应能够分析和使用日志中的数据以判断是否威胁到控制平面的安全。

h) 控制平面应能够从侵入攻击中恢复。

i) 允许用户选择其他方法进行保护，比如区域接入控制和防火墙。所选用的机制应不存在已知缺点或严重缺陷。

j) 应保证不同厂家安全机制之间的互通性。

18.1.3 管理平面安全性

管理平面的安全性包括以下几个方面：

a) 能够划分不同权限的用户等级，禁止低权限用户使用高权限的管理操作功能。

b) 建立登录日志和操作日志并对其进行管理。

c) 网管系统应具备安全保护措施，防止外部侵入和病毒破坏。

18.1.4 SCN 安全性

ASON 控制平面通过 SCN 进行连接建立和信息交互，SCN 必须保证传送网免受攻击，避免非授权用户非法使用网络资源，并确保 SCN 自身的安全性。同时，SCN 网络还应保证仅让那些允许在两个管理域之间传送的消息（如 E-NNI 消息和 UNI 消息）通过域间的接口，而禁止那些不能在两个管理域间传送的消息（如 I-NNI 消息）通过域间的接口。

SCN 应提供一定的安全机制来满足上述需求。在 SCN 中，不同控制域之间的接口可以分为三类：UNI、I-NNI 和 E-NNI。在不同的接口上可以采用不同等级的安全机制，其中 UNI、E-NNI 接口的安全性要求较高。

a) 信息交换安全性

1) SCN 应保证邻居发现信息交换的安全性。错误的邻居地址或端口 ID 可能会导致控制消息不能到达正确的目的地，或者导致不能在正确的端口上建立业务连接。
2) SCN 应保证传送实体能力发现信息交换的安全性。错误的传送能力发现（例如接口两边的实体不能就支持的信令协议和提供的数据服务达成一致）可能会导致接口不可操作。
3) SCN 应保证可达性信息交换的安全性。错误的可达性信息可能会导致连接建立请求被路由到非最优的路径上，或根本不能到达目的地。

b) 连接管理安全性

SCN 应能够提供连接管理消息的来源验证和完整性验证功能。非授权的连接管理消息可能对传送网的控制平面和传送平面进行非法攻击。这种攻击方式会是有恶意的用户模仿合法请求消息，制造大量的连接建立请求消息试图获取服务。如果 SCN 没有验证消息来源的安全机制或这种机制较弱，这些消息一旦被接受，将会导致传送网络资源耗尽。

c) 路由安全性

控制平面应保证 NNI 接口之间安全地交换路由信息。错误的可达性信息和拓扑信息可能会导致连接提供请求失败或被路由到非最优路径上，并且还可能会导致运营商网络性能的下降甚至不可操作。路由信息的安全性主要体现在 E-NNI 接口上，E-NNI 接口上要求具有以下路由安全机制：

1) 路由信息的鉴权：为了使本区域内的网络免受攻击，可采用基于密码鉴权机制；
2) 路由信息的完整性：路由信息包括拓扑信息、可达性信息和资源状态信息。保证路由信息的完整性可以通过在不同的层次使用安全机制来满足，例如可以在每个路由消息中嵌入关键消息摘要，也可以使用 IPSEC 机制在路由实体之间建立安全联盟；
3) 路由消息的私密性：在某些情况下需要在 E-NNI 接口上提供路由信息私密性机制。例如，某运营商只想向某一个运营商通告路由信息，而当不想公开发布这些路由信息让其他的运营商知道。

18.2 安全机制

为满足上述安全性要求，ASON 应提供以下一些安全机制：

a) 鉴权认证机制：防止怀有恶意的用户发送大量的连接提供请求发起攻击，使传送网资源耗尽，同时也可防止数据通信网自身遭受攻击；
b) 防重发攻击机制：防止非法用户采用记录、复制、截取或其他手段来影响正常的消息序列，从而使网络免受攻击；
c) 消息完整性验证机制：防止错误的或不完整的协议消息（设备制造商的软件错误或传输错误造成的协议消息错误）对网络造成冲击；
d) 消息的私密性机制：只在一定的实体之间交换某种信息而不让第三方得知。

其中，前三种安全机制可归结为鉴权（使用 MD5 或类似的鉴权技术就可以同时实现这三种机制），后一种称为加密。鉴权机制提供来源验证、消息完整性和防重发攻击的能力，加密机制防止第三方截获和破译协议消息的内容。鉴权和加密机制可以使用对称或公共密钥加密算法来实现。

19 ASON 业务要求

19.1 业务和连接类型

根据业务的信号特性（格式、比特率等）不同，ASON 支持的主要业务类型包括：

a) SDH/PDH 业务；
b) OTN 业务；
c) 光波长业务（透明或不透明传送方式）；
d) 以太网业务：10/100 Mbps、GE 和 10GE 业务等；

e) 基于 FICON、ESCON 和光纤通道等接口的存储业务(可选);

f) 其他业务。

ASON 应该支持以下的连接拓扑类型:

a) 双向点到点连接;

b) 单向点到点连接;

c) 单向点到多点连接。

根据连接建立方式的不同,ASON 网络应支持以下 3 种连接类型:

a) 永久连接(PC);

b) 软永久连接(SPC);

c) 交换连接(SC)。

ASON 应能提供对上述所有业务的配置、控制和管理功能。

19.2 业务调用方式

根据业务提供的连接类型,业务调用方式应支持以下两种类型:

a) 业务提供者发起的业务调用方式:业务提供者通过管理平面发起的业务请求。由管理平面发起连接管理请求,主要包括连接的建立、拆除、查询和修改操作。PC 和 SPC 连接采用该业务调用方式。

b) 用户发起的业务调用方式:用户通过控制平面(包括信令代理)中的 UNI 接口向业务提供者发起的业务请求。直接由用户设备或其信令代理发起连接管理请求,主要包括连接的建立、拆除、查询和修改操作。SC 连接采用该业务调用方式。

19.3 业务接入方式

为了将业务接入 ASON,用户首先需要在传送平面上与运营商网络建立物理连接。是否需要控制平面的连接依赖于向客户提供的业务请求模式(指配或信令方式)。采用直接信令方式还是间接信令方式由客户端是否具有 UNI 代理决定,参见 OIF UNI1.0。

ASON 应支持以下业务接入方式:

a) 局内接入:用户设备和光传输设备在同地,局内直接连接到用户;

b) 直接远程接入:利用专用链路远程接入到用户;

c) 子网远程接入:通过复用/解复用设备构成的子网远程接入到用户。

为了提高用户业务的生存性和提供负载均衡等功能,用户和网络之间可以采用多归属方式。例如,客户设备可以以双归的方式(即两条不同的路径,双归是多归属的一种情况)接入相同或不同的网络。

19.4 业务访问控制

从网络安全的角度考虑,网络资源不应被非授权实体访问,而且不能由非授权实体使用。业务访问控制是对企图访问网络资源的实体采取的一种限制和控制机制。对于 UNI 和 E-NNI,连接允许控制(CAC)应支持以下安全机制:

a) 根据操作者设置的管理策略,应能向每个实体授权所使用的网络资源。

b) CAC 应对任何企图通过 UNI 或 E-NNI 访问网络资源的实体进行验证,以防止网络资源被非法访问和控制。通过验证的实体可由网络授予不同的业务访问级别。

c) UNI 和 E-NNI 应对连接请求(如连接建立、拆除和修改等)的信令消息提供一种完整性验证机制,以防止对业务的攻击。

19.5 服务级别协议(SLA)

服务级别协议(SLA)是指网络业务提供商(NSP)与客户之间关于某项服务所应达到的水平而签署的协议。在该协议框架下,NSP 必须向客户提供相应的服务水平,否则将向客户做出经济赔偿。

SLA 通常定义了提供给客户的业务和业务等级,还描述了业务的保证以及业务劣化或失效情况下可能的赔偿。根据 SLA 协议 ASON 网络应能向客户提供多种等级的业务,SLA 的主要内容可包含以

下几方面：

——网络的服务水平和服务质量：例如网络可用性等；

——各种业务的服务水平要求：例如业务的可用性、误码率、时延等；

——业务开通时间；

——故障恢复时间：例如网络的保护与恢复策略、故障修复时间等。

19.6 ASON 业务模型

ASON 网络的业务模型包括：光虚拟专用网业务(OVPN)、按需带宽分配业务(BoD)和指配带宽业务(PBS)等。这三种业务模型的示例见附录 B。

附 录 A
（资料性附录）
ASON 与传统网络的互通

A.1 ASON 与传统网络的互通的实现方式

现有光传送网络设备不具备智能，使得网络端到端连接动态控制无法实现，成为全网智能化的瓶颈。因此 ASON 的引入必须解决与现有传送网的互连互通，最大限度保证运营商现有投资。ASON 与现有的光网络设备实现兼容和互通，存在以下几种解决方案。

a） 基于网管操作实现

通过网络管理系统(NMS)来管理 ASON 网络区域和传统网络区域。NMS 需分段建立一条完整的端到端连接，这些分段连接独立于穿越整个运营商域的端到端连接。连接 ASON 域与传统管理域之间的链路不能参与 ASON 控制平面。在 ASON 域中，采用 SPC 方式创建连接，在传统网络区域通过 PC 方式提供连接。图 A.1 和图 A.2 描述了基于网管系统实现互通的实例。

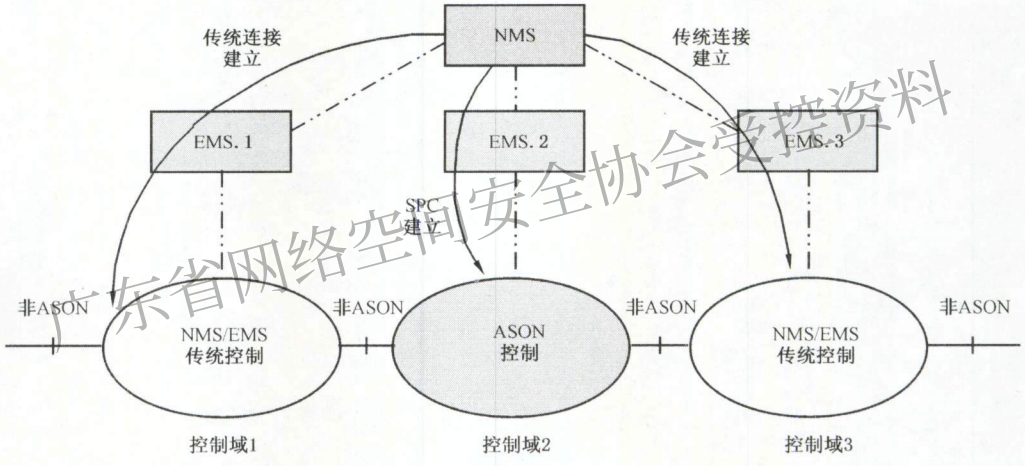


图 A.1 两个传统网络域之间通过 ASON 域互通

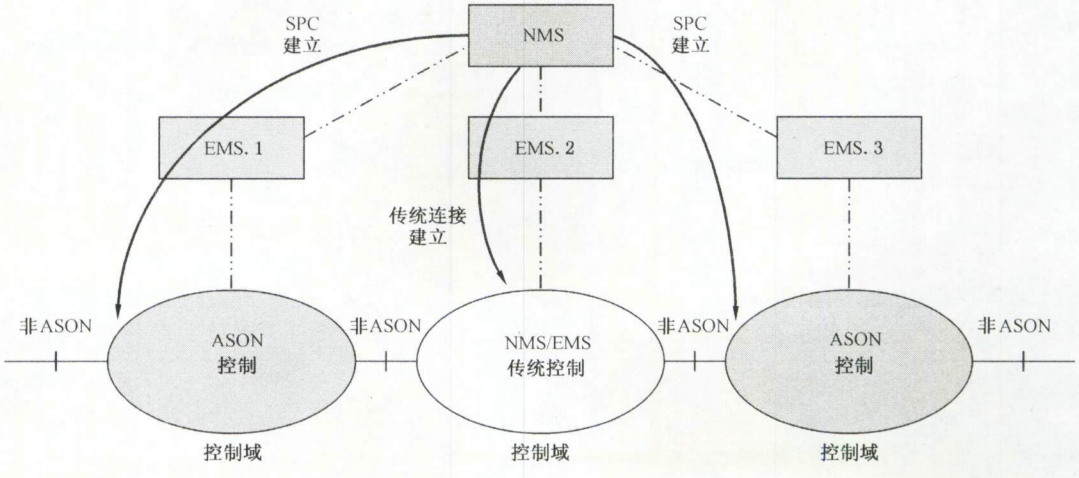


图 A.2 两个 ASON 控制域通过传统网络域互通

b) 对网络管理系统进行升级

对管理系统进行升级，使它成为具有智能的集中控制平面，原来的传送网络就成为 ASON 网络中的一个集中控制域。管理系统利用集中控制方式，实现控制域内连接的自动建立，在该控制域内部使用私有控制协议，对外通过在管理系统中增加标准的信令接口（UNI 和 E-NNI），实现与其他控制域的配合，从而最终达到全网内的自动交换，支持端到端的 SPC 和 SC 连接。

对于 ASON 网络与传统网络互通的配置，存在两种情况，如图 A.3 和图 A.4 所示：

——两个传统网络域通过一个 ASON 控制域的交互而互通；

——两个 ASON 控制域通过传统网络域的交互而互通。

其中，图 A.4b)是图 A.4a)的一种补充或者可选方案，即在某些情况下，单个 EMS 可以同时管理 ASON 域和传统域。图 A.4c)描述了两个 ASON 控制域之间通过传统网络域，采用单个 E-NNI 代理的方式而互通的情况，即两个 ASON 控制域通过 E-NNI 直接互连。在这种情况下，ASON 控制域通过 E-NNI 代理与传统管理域的 NMS 互通，而传统网络域内部对于 ASON 控制域来说是不可见的。

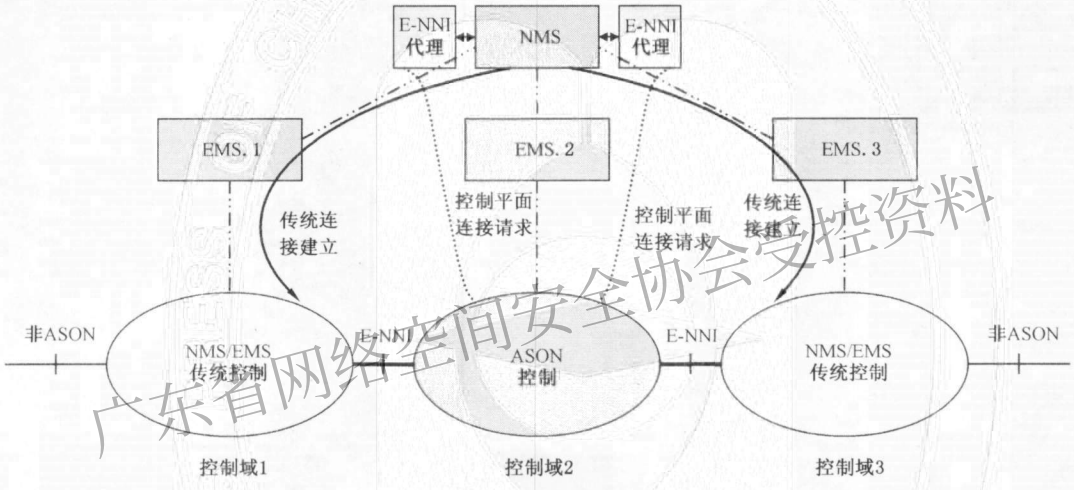
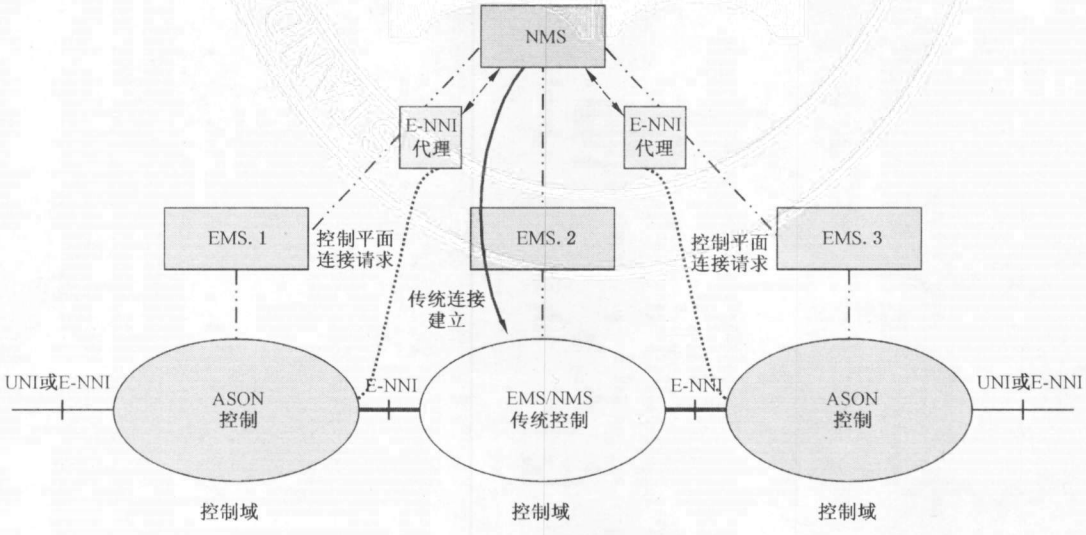
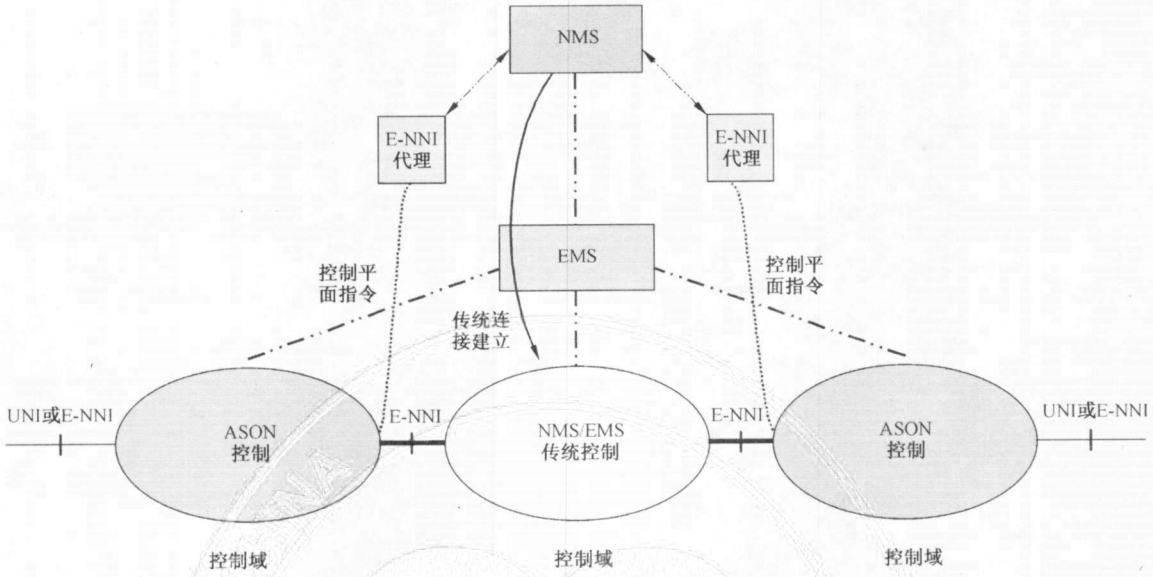


图 A.3 两个传统网络域通过 ASON 域互通

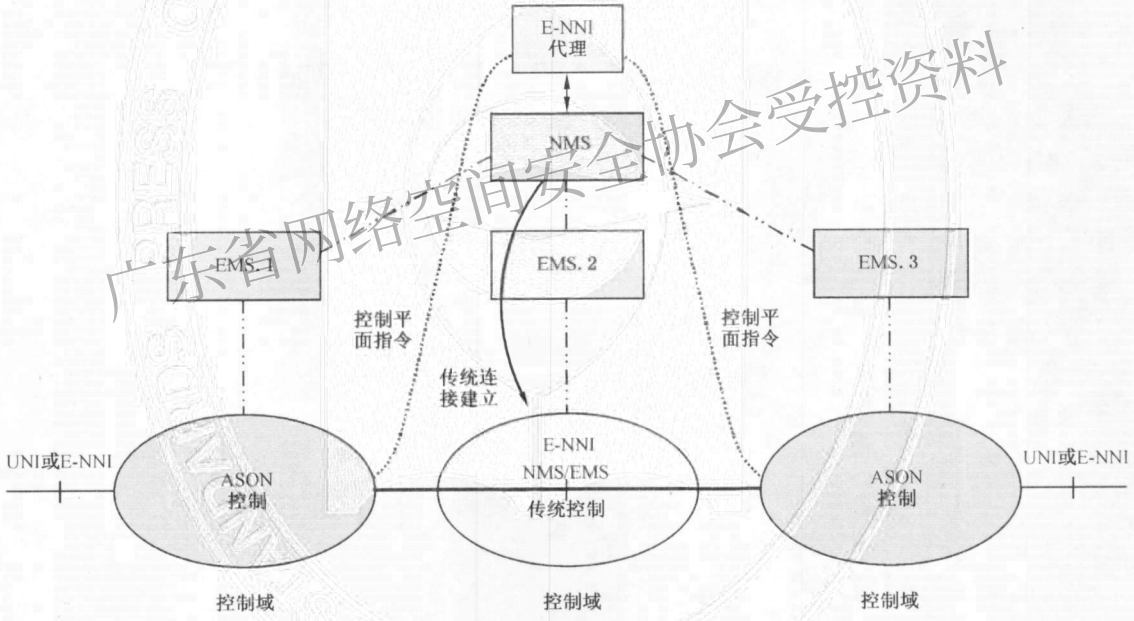


a) 多个 E-NNI 代理

图 A.4 两个 ASON 控制域通过传统网络域的交互而互通



b) 多个 E-NNI 代理，一个 EMS 管理多个控制域



c) 单个 E-NNI 代理

图 A.4（续）

c) 对传统网络设备进行升级

对现有光网络的每个设备增加智能控制单元。这种方案可能需要对每个设备的软硬件进行升级工作。

综合来看，采用管理系统升级为集中控制的方式，兼顾了 ASON 网络建设的迫切需求与传统网络技术的现状，可以实现旧的传送网络与 ASON 网络的兼容和平滑演进。

A.2 ASON 与传统网络之间的业务应用

A.2.1 传统网络与 ASON 网络组网

传统网络与 ASON 网络混合组网时，两者之间可以采用单节点互通结构和双节点互通结构。其他互通的方式待研究。

单节点互通结构示例见图 A.5。

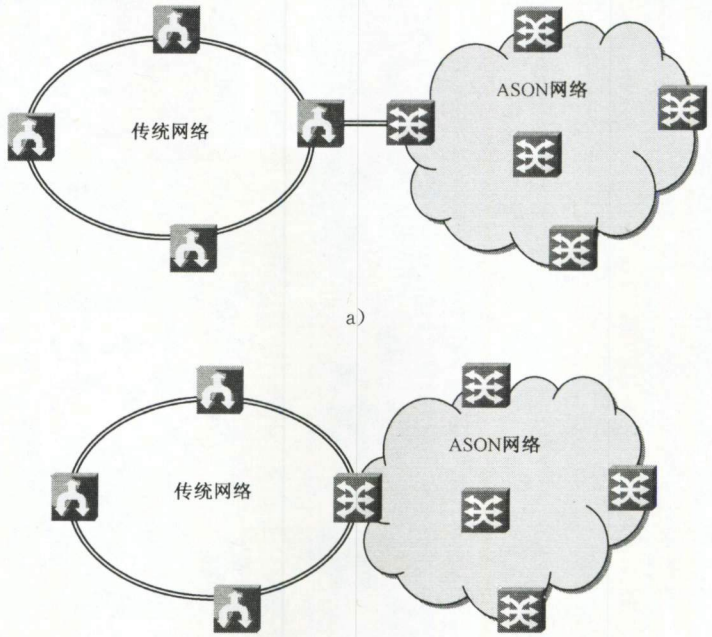


图 A.5　传统网络和 ASON 网络之间的单节点互通示例

图 A.5a)中单节点互通情况下，传统网络和 ASON 网络边界节点之间的链路可以为有保护，也可以为无保护。

图 A.5b)中的情况一般只在同一设备厂商的设备之间实现，因为这种拓扑下要求传统网络和 ASON 网络支持相同的 APS 协议。

双节点互通结构示例见图 A.6。

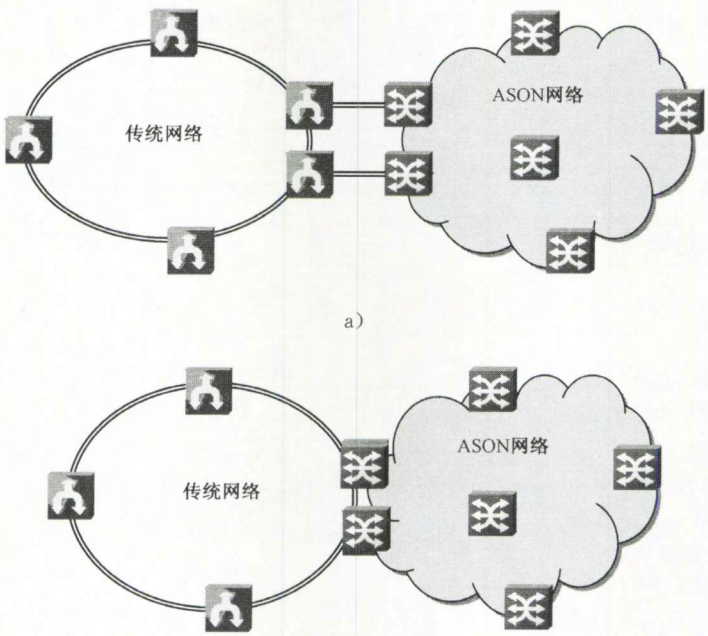


图 A.6　传统网络和 ASON 网络之间的双节点互通示例

图 A.6a)中双节点互通结构下，既可以提供对域间链路失效的保护，又可以提供传统网络域和 ASON 网络域边界节点故障保护，跨域业务的生存性得到大大提高。

图 A.6b)中的情况一般只在同一设备厂商的设备之间实现，因为这种拓扑下要求传统网络和 ASON 网络支持相同的 APS 协议。

A.2.2　跨域的保护机制

由于传统网络中不提供分层恢复功能，故跨 ASON 网络和传统网络之间业务采用保护机制。参见 14.6.2 和 A.2.2 中的内容，域间保护可以分为能完成链路失效保护的单节点互通和能完成节点失效保护的双节点互通。

A.2.2.1　能完成链路失效保护的单节点互通保护机制

传统网络和 ASON 网络之间采用单节点互通时，域间边界节点间采用链路保护方式，如 1+1/1:1、$m:n$ 线性复用段保护。此外承载该链路的底层传送网也可以提供对该链路的保护，如 WDM 系统提供的保护。

A.2.2.2　能完成节点失效保护的双节点互通保护机制

根据 ASON 网络域内采用的保护和恢复方式的不同，以及传统网络中采用的保护方式的不同，双节点互通保护机制下可以有多种情况。双节点互通保护机制下，传统网络内部配置成 Drop and Continue 方式，业务通过两个节点和两条链路分别进入 ASON 网络。在 ASON 网络内可采用恢复机制或保护机制来保证业务的生存性。双节点互通和 Drop and Continue 功能的采用，使得传统网络和 ASON 网络之间的链路和边界节点故障情况下，业务的生存性大大提高。

在双节点互通保护机制下，业务在传统网络中的部分，可以采用两纤/四纤双向复用段共享保护环或 SNCP/UPSR 保护。在双节点互通保护机制下，业务在 ASON 网络中的部分，可以采用无保护、恢复、基于控制平面的 1+1/1:$n/m:n$ 的路径或子网连接保护、1+1/1:1 线性复用段保护、$M:N$ 线性复用段保护、两纤/四纤双向复用段共享保换环，以及保护与恢复的结合等。其中在 ASON 网络内根据业务配置的需要，对于 Drop and Continue 功能可选用，具体情况视以上情况的不同而不同。对于业务的 ASON 网络承载部分，也可采用保护与恢复结合的方式。

A.2.3　跨域业务的建立

跨域业务的建立是实现跨 ASON 网络域和传统网络区域的自动端到端连接建立和管理。跨域业务的建立可以采用如下两种方式：

a)　在网管上将该业务分成两类分别建立(参见附录 A.1a))，一类为传统网络上的端到端连接建立，采用 PC 方式；一类为 ASON 网络上的端到端连接建立，采用 SPC 方式。

b)　在网管系统上增加集中式控制代理(参见附录 A.1b))，使传统网络具有智能。业务在传统网络和 ASON 网络上可通过网管实现端到端 SPC 建立，也可通过 UNI 接口发起 SC 连接的建立。

附 录 B
（资料性附录）
ASON 业务模型举例

B.1 按需带宽分配业务(BoD)

BoD 是指最终用户或网络设备以某一应用在规定时间内所要求的速率获取网络可用容量的能力。按需分配带宽业务通过 UNI 信令接口提供按需带宽动态连接，以提高网络的带宽利用率。BoD 使用交换连接(SC)类型，并且连接的建立是实时的。BoD 的特点与要求如下：

a) 通过 UNI 信令接口，客户或其代理直接发起连接请求；
b) 客户没有或只具有部分的网络可见性，这取决于采用的控制平面互连模型和网络管理策略；
c) 客户到达网络的请求需要经过安全认证；
d) 允许用户同服务提供商之间进行 SLA 协商，包括业务等级、按需带宽、业务持续时间等内容；
e) 对 BoD 业务，需要提供相应的计费信息。

用户可通过管理平面选择设置 BoD 属性，可管理的参数包括：

a) 时间帧(起始时间和结束时间)：将网络按时间段分配不同带宽；
b) 带宽(平均带宽，峰值带宽等)：在某一特定时间段内的带宽属性设置；
c) 服务质量：按策略管理划分不同的服务质量等级；
d) 计费标准查询：根据用户需求设定的相应 BOD 计费标准。

B.2 光虚拟专网业务(OVPN)

OVPN 业务在光层为特定的用户组提供虚拟专用网业务。OVPN 不用建设专用的网络，而是利用控制和管理技术，将光网络中的某一部分资源划分给一些跨地域的公司和企业专用。通过 OVPN，运营商可以将网络资源及其配置管理的权力分配给用户；用户可将租用的网络看作是自己的私有网络，完全拥有配置、监控和维护网络的权力。OVPN 业务的主要特点是：

a) 用户为一组特定的网络资源，如光连接端口、波长等签订合同；
b) 支持一般 VPN 的封闭用户组概念；
c) 根据采用的业务提供方式，支持 PC、SPC 或 SC 连接类型；
d) 在同一 CUG 内部，OVPN 站点可以请求站点之间的动态重新配置；
e) 客户可以根据客户服务合同中的规定对自己的网络资源具有可见性及控制权利。

OVPN 是光网络中的一种新的服务方式，也是一种新的增值业务。OVPN 应包括以下功能：

a) 根据用户需求，支持 PC、SPC 或者 SC 的连接类型。
b) OVPN 资源划分：按照业务类型、端口、地域等为客户分配专用的或者是多客户共享的网络资源，用户不必考虑与其他客户之间的边界。对用户而言，OVPN 是独立的专用网。
c) 用户安全访问控制：OVPN 业务提供者可为终端用户分配用户名和密码并设置权限，使得终端用户可以查看、修改和控制他们租用的网络资源。
d) OVPN 网络的管理与维护：包括网络资源的路由配置、拓扑管理、性能监视、故障管理、业务指配、业务级别设置、端到端保护与动态恢复等。在日常维护中，用户只能看见与之相关的数据信息，而运营商应具有 OVPN 服务的管理视图。
e) OVPN 的成员管理：支持一般的 OVPN 封闭用户组(CUG)概念，在统一 CUG 内部，OVPN 站点可以请求站点之间的动态重新配置。
f) 管理区域控制(扩大或缩小)等。

g） 提供相应的计费信息。

对于管理平面，应支持以下 OVPN 管理功能：

a） 服务器端管理功能

1） 为用户划分 OVPN 域，分配特定网络资源，如光连接端口、VC 等；

2） 设定 OVPN 的相关属性：包括名称、类型等；

3） 根据客户服务合同的规定，为网管客户端配置所属的 VPN 网络资源，设置客户端对资源的可见性和控制能力；

4） 监视和记录每个 OVPN 客户端的操作行为；

5） 定义不同 OVPN 域的客户终端和操作者，相关信息包括：用户名、密码、终端 PC 的 IP 地址、客户所属 OVPN 域等。

b） 客户器端管理功能

1） 查看属于其 OVPN 域的网络拓扑和资源；

2） 实时查询其 OVPN 域内的告警和性能；

3） 支持在其 OVPN 域内建立和删除连接等。

B.3 指配带宽业务（PBS）

PBS 提供了增强的租用线/专线业务，此业务通过管理平面使用 PC 和 SPC 方式建立，是实时或近实时的。PBS 应具有以下特点：

——通过管理接口发起连接请求；

——用户与光网络之间是客户与服务者的关系；

——光网络对于用户是不可见的；

——提供相应的计费信息。

附 录 C
（资料性附录）
分层呼叫控制举例

图 C.1 描述了两个以太网客户的层间呼叫模型。以太网客户被连接到不具有以太网交换功能的 VC-3 网络上。假设从千兆以太网 UNI 接口发起一个 40 Mbit/s 呼叫请求，为了承载以太网 CI，需要建立 VC-3 连接（VC-3-3vc）。图中显示了两个层面，只有 VC-3 层具有一条网络连接。一旦 VC-3 连接建立起来，在两个 NCC_{MAC} 之间就会存在相应的 MAC 链路连接。

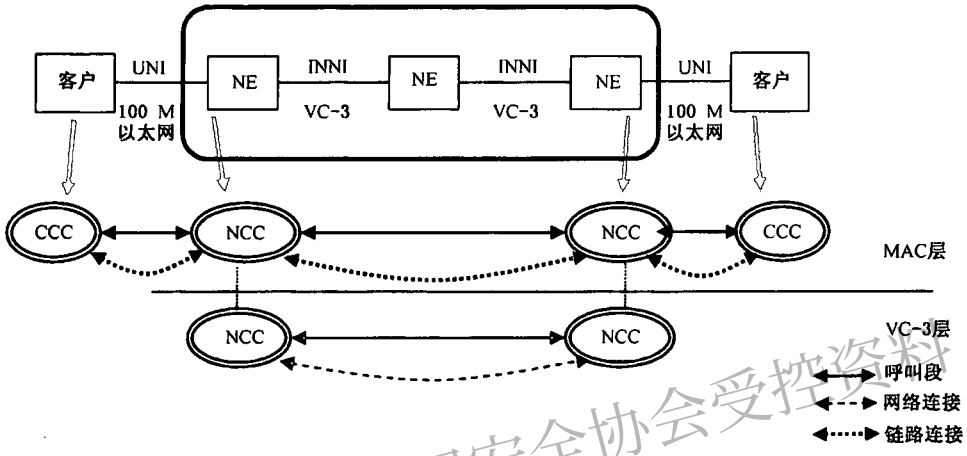


图 C.1 VC-3 承载以太网实例

在呼叫过程中，不同服务层呼叫的建立在时间上可以是相互独立的。例如：到达的以太网呼叫会触发 VC-3 连接，或者 VC-3 连接已经建立并与一个 MAC 呼叫关联。

此外还有很多其他的层间呼叫的实例，例如 SDH/OTN 承载 Fibre Channel 等。

中华人民共和国
国家标准
自动交换光网络(ASON)技术要求
第1部分:体系结构与总体要求
GB/T 21645.1—2008
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 7 字数 210千字
2008年6月第一版 2008年10月第二次印刷
*
书号:155066·1-31865 定价 56.00 元

GB/T 21645.1-2008

GB/T 21645.1—2008