

ICS 33.040.40
M 32



中华人民共和国通信行业标准

YD/T 3020-2016

基于 SDN 的 IP RAN 网络技术要求

Technical requirement for SDN based IPRAN network

2016-01-15 发布

2016-04-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
4 基于 SDN 的 IP RAN 的网络功能架构	3
4.1 基于 SDN 的 IP RAN 业务需求和应用场景	3
4.2 基于 SDN 的 IP RAN 网络功能架构	5
5 基于 SDN 的 IP RAN 网络控制面的技术要求	10
5.1 管理通道建立	10
5.2 控制通道建立	11
5.3 控制器与转发节点整体交互过程	12
5.4 SDN 控制域建立的技术要求	13
6 基于 SDN 的 IP RAN 网络转发面的技术要求	16
6.1 基于 SDN 的 IP RAN 转发节点系统架构	16
6.2 基于 SDN 的 IP RAN 转发节点协议需求	17
6.3 OpenFlow 化 IP RAN 转发节点	18
7 基于 SDN 的 IP RAN 网络管理的技术要求	19
7.1 控制器管理接口	19
7.2 转发节点管理接口	19
8 传统 IP RAN 网络向基于 SDN 的 IP RAN 网络迁移技术要求	19
附录 A (规范性附录) 网元自通实现方案	21
附录 B (资料性附录) SDN 域拓扑收集技术	24

前　　言

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国电信集团公司、中国联合网络通信集团有限公司、华为技术有限公司、中兴通讯股份有限公司、武汉烽火科技集团有限公司（武汉邮电科学研究院）、南京爱立信熊猫通信有限公司、上海贝尔股份有限公司、杭州华三通信技术有限公司。

本标准主要起草人：杨广铭、孙嘉琪、尹远阳、曹　畅、王海军、黄永亮、胡杰辉、陈国义、王丽星、曲延峰、古　渊、肖　敏、魏月华、魏学勤、付胜波、周国华、王　剑。

广东省网络空间安全协会受控资料

基于SDN的IP RAN网络技术要求

1 范围

本标准规定了基于SDN的IP RAN网络技术要求，包括基于SDN的IP RAN网络参考架构及网络转发面、控制面和管理面等功能要求。

本标准适用于基于SDN的IP RAN网络。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 2603-2013 支持多业务承载的IP/MPLS网络技术要求

YD/T 2374-2011 分组传送网（PTN）总体技术要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

IP RAN 网络 IP radio access network

基于 IP 的无线接入网络，这里指以 IP/MPLS 协议及关键技术为基础的电信级承载网络，当前主要面向承载移动回传业务。

3.1.2

基于 SDN 的 IP RAN 网络 SDN based IP RAN network

采用软件定义网络（SDN）技术的IP RAN网络，提升网络自动化部署、运维、管理能力，并为未来新业务的快速开放提供能力。

3.1.3

接入 SDN 化 SDN access

IP RAN网络接入、汇聚层的SDN化，存在两种形式，一种形式接入层设备控制面上移，汇聚层设备集成SDN控制器，实现对接入层转发行为的控制；另一种形式接入层与汇聚层设备控制面全部上移，通过单独的SDN控制器，实现对接入层及汇聚层转发行为的控制。

3.1.4

全网 SDN 化 Whole network built on SDN technologies

IP RAN网络从接入、汇聚到核心层的SDN化，接入层、汇聚层及核心层设备控制面均上移，由全网的SDN控制器，对全网转发行进行控制。

3.1.5

网元自通 Plug-and-play

新上线网元插入网络中后，只需设备上电，即可实现与网管或SDN控制器的互通。

3.1.6

网络虚拟化（IP RAN） Network virtualization based on IP RAN

通过SDN的集中控制和路径自动化计算部署技术，实现IP RAN网络的虚拟化，IP RAN虚拟化网络业务部署与管理不再关注网络内部细节，对外虚拟化为一台路由器。

3.1.7

南向接口 Southbound interface

控制器与网络转发设备之间控制接口。

3.1.8

北向接口 Northbound interface

控制器与应用层应用，或与网管之间控制接口。

3.2 缩略语

下列缩略语适用于本文件。

API	Application Programming Interface	应用编程接口
ATM	Asynchronous Transfer Mode	异步传输模式
BGP	Border Gateway Protocol	边界网关协议
CE	Custom Edge	用户边缘设备
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
FIB	Forwarding Information Base	转发表
IGMP	Internet Group Management Protocol	Internet 组管理协议
IGP	Interior Gateway Protocols	域内网关协议
IP	Internet Protocol	互联网协议
IP RAN	IP Radio Access Network	互联网协议的无线网络接入
OF	Open Flow	开放流协议
ONF	Open Networking Foundation	开放网络基金会
OSPF	Open Shortest Path First	开放式最短路径优先协议
QoS	Quality of Service	服务质量
RAN	Radio Access Network	无线接入网
SDN	Software Defined Networking	软件定义网络
SNMP	Simple Network Management Protocol	简单网络管理协议
TTL	Time to Live	生存时间
VLAN	Virtual LAN	虚拟局域网
VPN	Virtual Private Network	虚拟专用网络
TDM	Time Division Multiplex	时分复用
L2VPN	Layer Two Virtual Private Networks	二层虚拟专网
L3VPN	Layer Three Virtual Private Networks	三层虚拟专网
SDH	Synchronous Digital Hierarchy	同步数字体系

VPWS	Virtual Private Wire Service	二层点到点服务
PW	Pseudo Wire	伪线

4 基于 SDN 的 IP RAN 的网络功能架构

4.1 基于 SDN 的 IP RAN 业务需求和应用场景

4.1.1 业务承载需求

基于SDN的IP RAN网络主要为以下4种模型提供业务承载能力：

- a) TDM业务模型：支持提供E1、CSTM-1等PDH、SDH业务的承载；
- b) 以太业务模型：支持提供点到点、点到多点、多点到多点等L2VPN和L3VPN业务的承载；
- c) IP业务模型：主要提供纯IP、L3VPN等业务的承载；
- d) ATM业务模型：支持提供ATM业务的承载。

基于SDN的IP RAN网络现阶段主要承载移动回传业务。不同制式的移动网络业务接口类型与业务模型的对应关系详见表1。

表 1 移动回传业务承载需求表

业务分类	接入模型	业务承载方案
GSM/GPRS/EDGE (2G/2.5G)	TDM	VPWS
UMTS (3G)	TDM	VPWS
	TDM	VPWS
	以太、IP	L3VPN/L2VPN
CDMA 1x-RTT (3G)	TDM	VPWS
CDMA 1x EV-DO (3G)	以太、IP	L3VPN/L2VPN
TD-SCDMA (3G)	TDM	VPWS
	以太、IP	L3VPN/L2VPN
LTE	以太、IP	L3VPN/L2VPN
eMBMS	以太、IP	Simple IP、组播 VPN

4.1.2 网络承载功能需求

本节提到的各种 SDN IP RAN 网络的承载需求，其承载能力均应满足 YD/T 2603-2013 《支持多业务承载的 IP/MPLS 网络技术要求》第 6 章：通用技术规范中的指标要求。

4.1.2.1 OAM 机制

基于 SDN 的 IP RAN 网络应提供接入链路 OAM、网络 OAM 及业务 OAM 各类 OAM 机制。实现持续的端到端连通性检测、故障检测、故障定位及网络丢包率、时延等指标性能监测。

4.1.2.2 快速保护倒换

基于 SDN 的 IP RAN 网络应提供多层次快速保护倒换技术，实现故障情况下业务的快速恢复。

4.1.2.3 QoS

基于 SDN 的 IP RAN 网络应对不同业务的应用需求，如丢包率、延迟、抖动和带宽等，提供不同的服务质量保证，以实现同时承载数据、语音和视频业务。

4.1.2.4 网络管理

基于 SDN 的 IP RAN 网络应提供完善的网络管理系统，采用图形化界面实现拓扑管理、配置管理、故障管理、性能管理和安全管理等。同时由于控制器引入，网络管理系统同时要负责控制器与转发节点

间的通道建立和管理；并通过北向接口与上层网管系统相连。

4.1.2.5 时钟同步

基于 SDN 的 IP RAN 网络应支持同步以太及 1588v2 时间同步功能。

4.1.3 IP RAN 网络应用现状

IP RAN 网络目前主要定位于承载 2G、3G 及 LTE 等移动回传业务。IP RAN 网络采用三层路由器设备组网，核心汇聚层网络采用双星形，口字形或环形结构组网；接入层设备以环形结构为主，同时考虑到地理环境及资源因素，应支持采用双上联、链形等多种结构组网。

接入设备为网络的边缘，用于提供灵活业务接入；汇聚设备用于接入流量的汇聚；核心层设备用于业务流量的转发。

IP RAN 网络的组网结构如图 1 所示，主要有三种业务承载方式：

- 方式1：端到端采用分段L2VPN方式，在汇聚设备进行分段；
- 方式2：接入层采用L2VPN方式，在核心汇聚层采用IP/MPLS L3VPN方式；
- 方式3：端到端采用分段L3VPN方式，在汇聚设备进行分段。

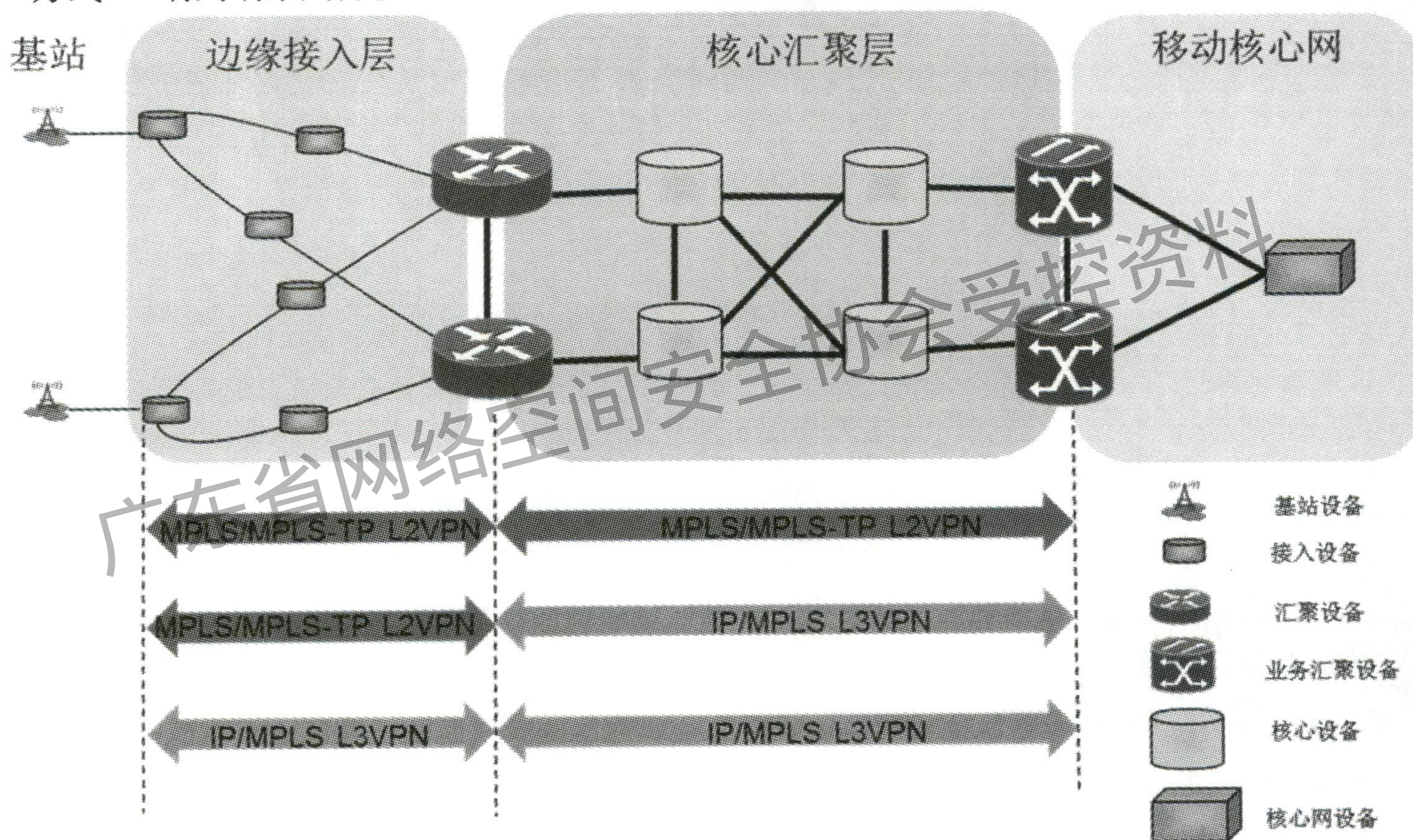


图 1 IP RAN 网络架构

其他采用非三层路由设备场景不在本标准进行定义。

4.1.4 IP RAN 网络对 SDN 的需求

运营商 IP RAN 网络引入 SDN 主要基于以下需求：

- a) 海量 IP/MPLS 设备部署带来的业务开通复杂和运维复杂；
- b) 对新业务响应速度慢，无法快速开通业务；
- c) 网络能力只针对内部运营人员，缺乏对网络用户的能力开放；
- d) 降低 IP RAN 设备复杂度，降低网络建设成本；
- e) 降低异厂家 IP RAN 设备互通难度。

4.2 基于 SDN 的 IP RAN 网络功能架构

4.2.1 基于 SDN 的 IP RAN 的技术特征

IP RAN为三层IP网络，主要运用IP/MPLS协议完成业务承载，解决无线接入的IP化。基于SDN思想的网络具有转发与控制分离、集中控制及开放可编程等特点。通过在IP RAN网络中引入SDN架构及相关技术，实现基于SDN的IP RAN网络，简化IP RAN网络设备，提高网络自动化部署、运维、管理能力，并为未来新业务的快速开放提供能力。

本标准主要规范采用SDN思想及相关技术的IP RAN网络，基于SDN的IPRAN的网络应具有以下基本特征：

- 网络虚拟化：控制器控制的网络被虚拟化成一台路由器，简化网络配置，网络规划及业务部署更为简单，接入层网络的拓扑发现、路径建立、业务部署、OAM和保护的建立由控制器完成；
- 以业务为中心的业务发放模式：业务发放不再关注网络设备之间转发路径如何建立，只关注业务的接入点和业务终结点，以及业务带宽等约束条件；
- 转发控制分离：控制面上移，无需关注内部协议交互和部署；
- 网络可编程：从应用层面看，下层网络被抽象出来，网络具备可编程性；
- 集中控制化：控制面集中，所有的网络行为都由其控制，实现流量工程、负载均衡等网络的全局优化；
- 自动部署OAM和业务保护，快速故障定位，通过控制器的集中控制实现高可靠性；
- 易于实现新业务的引入，业务升级简单，与转发平面解耦。

4.2.2 参考架构

引入SDN之后，基于SDN的IP RAN的网络架构可以如图2所示进行描述，主要包含转发层、控制层、应用层三个层面及网管功能。

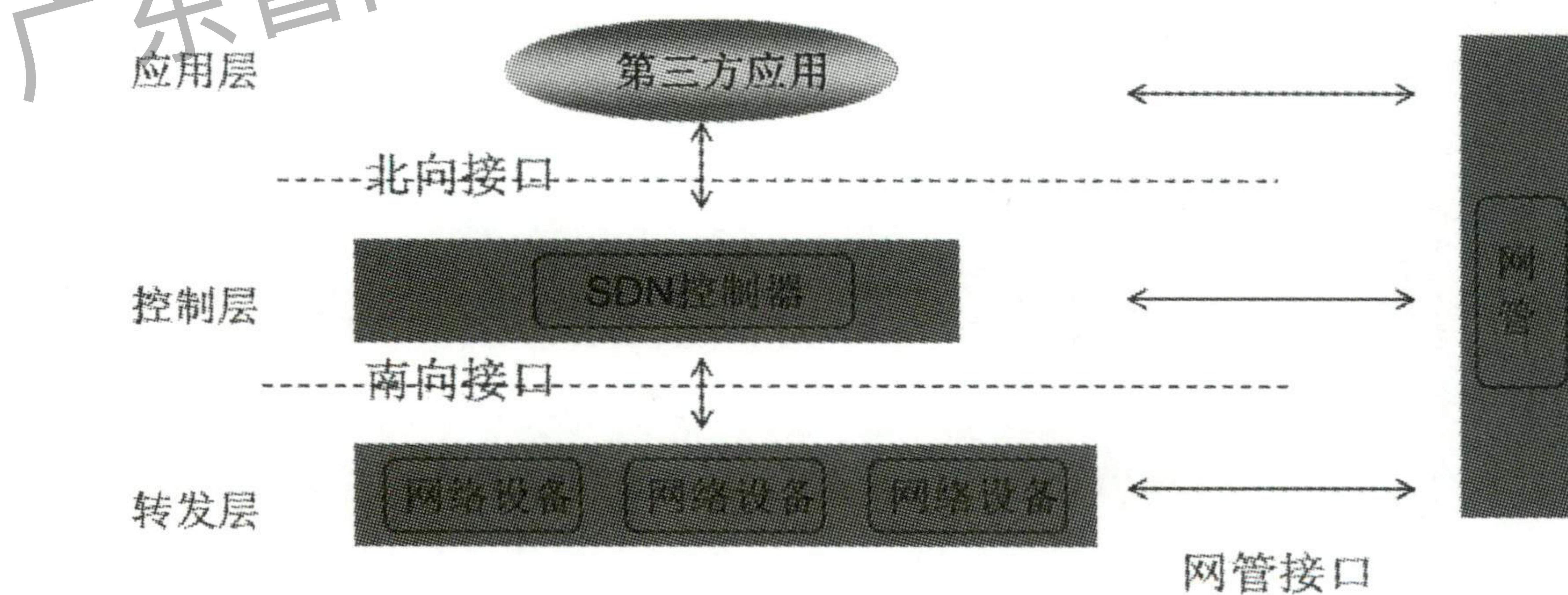


图2 基于SDN的IP RAN参考架构

转发层：根据SDN控制器下发的控制信息完成数据转发。应具有基本的路由功能，以保证转发节点与控制器和网管之间控制通道和管理通道的自动建立。转发节点接受控制器的控制及向控制器上报自身的资源和状态。转发节点同时仍然需要提供传统的网管北向接口。但是北向接口功能不再包括网络业务和协议的功能，只提供转发节点设备本身的管理接口，如电源、电压、单板等管理功能。考虑到现网已大规模部署，为了兼容现有网络硬件条件，初期转发层网络设备的互联互通及数据流转发需兼容IP/MPLS协议集（MPLS-TP为其子集）。后期，待openflow流表芯片发展成熟，逐步向openflow流表转发演进。

控制层：逻辑上集中的控制实体，通过南向接口向转发层网络设备下发控制信息，通过北向接口向上层应用开放底层网络资源和能力。该层的SDN控制器是一个软件系统，可以内置在网络设备中，也可以部署在一个独立的服务器中。控制器是整个网络的控制面，对整个网络进行集中控制。控制器控制的网络范围根据实际情况，可由网络管理员进行定义。南向接口主要做业务级的控制平面定义，完成网络拓扑的发现、业务配置下发、业务PW/LSP路径的计算及表项的下发。北向接口包括：网管北向接口，向网管提供网络的业务部署，监控，故障处理，故障定位等功能，可以提供对网络拓扑和虚拟网络的操作；应用层北向接口，向第三方应用开放编程接口，提供API编程接口。用于第三方应用利用控制器获取网络资源（如网络拓扑），提供针对网络的诊断，故障定界定位，性能监控等应用，以及未来创新的应用。

设备侧具有控制层的控制代理，除此之外，也可保留一部分控制功能，按照所保留的控制功能强弱，分为如下三种实现方式：

- a) 强控制能力：设备上保留基本IGP, BGP, LDP, BFD等动态路由协议,SDN控制器功能相对简单,只做基本配置下发。
- b) 弱控制能力：设备上保留静态转发表，并具备故障检测等机制,故障后设备侧可以自行切换，其余配置主要在控制器完成。
- c) 无控制能力：设备上保留静态转发表,所有表项都由控制器来配置和下发，即网络的所有功能均由控制器下发实现。

应用层：基于控制层数据进行应用管理。

网管：完成转发面网络设备、SDN控制器各类对象的管理及控制器或第三方应用策略的配置。转发面网络设备在网管上可作为独立网元管理，但是由于业务已经由控制器进行集中控制，因此网元管理面只提供网元设备管理功能。

4.2.3 功能模块

在基于SDN的IP RAN网络参考架构中,功能模块分为控制器相关功能模块和转发节点相关功能模块两部分。

- a) 控制器相关功能模块：
 - **控制协议模块：**提供对转发设备的控制协议（例如，Openflow等控制协议），与转发节点建立控制协议连接。其他功能模块可以通过控制协议对转发节点进行控制。
 - **网络资源管理模块：**收集网络中转发节点资源信息，包括转发节点的端口、拓扑资源等。其他功能模块可以利用资源层收集的资源进行路径计算，业务部署，生成转发表项等,对网管和第三方应用开放网络资源编程和管理接口。
 - **路径计算模块：**利用资源层收集的资源计算业务路径，可以支持动态或静态两种方式,分配LSP标签或流表项，通过已建立好的通道下发给转发设备。
 - **网络抽象化模块：**对网络进行抽象，将物理网络虚拟为一台路由器，屏蔽物理网络细节。业务模块可以基于抽象网络进行部署，无需关注虚拟网络内部转发路径的打通。在IP RAN网络中，网络内部承载采用IP/MPLS，因此在IP RAN场景下，网络抽象化功能针对IP/MPLS网络的虚拟化功能。
 - **网络协议层模块：**提供传统路由器具备的路由协议栈，用于控制器与传统网络的互通。
 - **网络业务层模块：**在IP RAN场景下需要提供L2VPN和L3VPN业务。L2VPN包括VPWS和VPLS。
 - **支撑模块：**提供基本的故障定位工具，告警，北向接口等对SDN域的维护和管理功能。

b) 转发节点功能:

- 网元自通模块: 负责网络基本路由的打通, 在控制器控制转发节点之前, 建立控制通道, 及与网管的管理通道的建立。
- 控制代理模块: 适配与控制器间控制协议, 负责与控制器建立和维持控制协议连接。负责向控制器注册, 上报信息, 收集本地拓扑。接受控制器下发的控制信息和转发表项, 并下发到转发面, 指导转发。
- 转发模块: 对报文进行转发和处理。
- 管理代理模块: 提供对转发节点的调试诊断接口, 以及设备管理功能, 向网管提供设备管理的接口(如电源、电压、单板等)。

4.2.4 参考模型

基于SDN的IP RAN网络, 有两种不同的组网模型:

1) 模型一: IP RAN网络接入SDN化

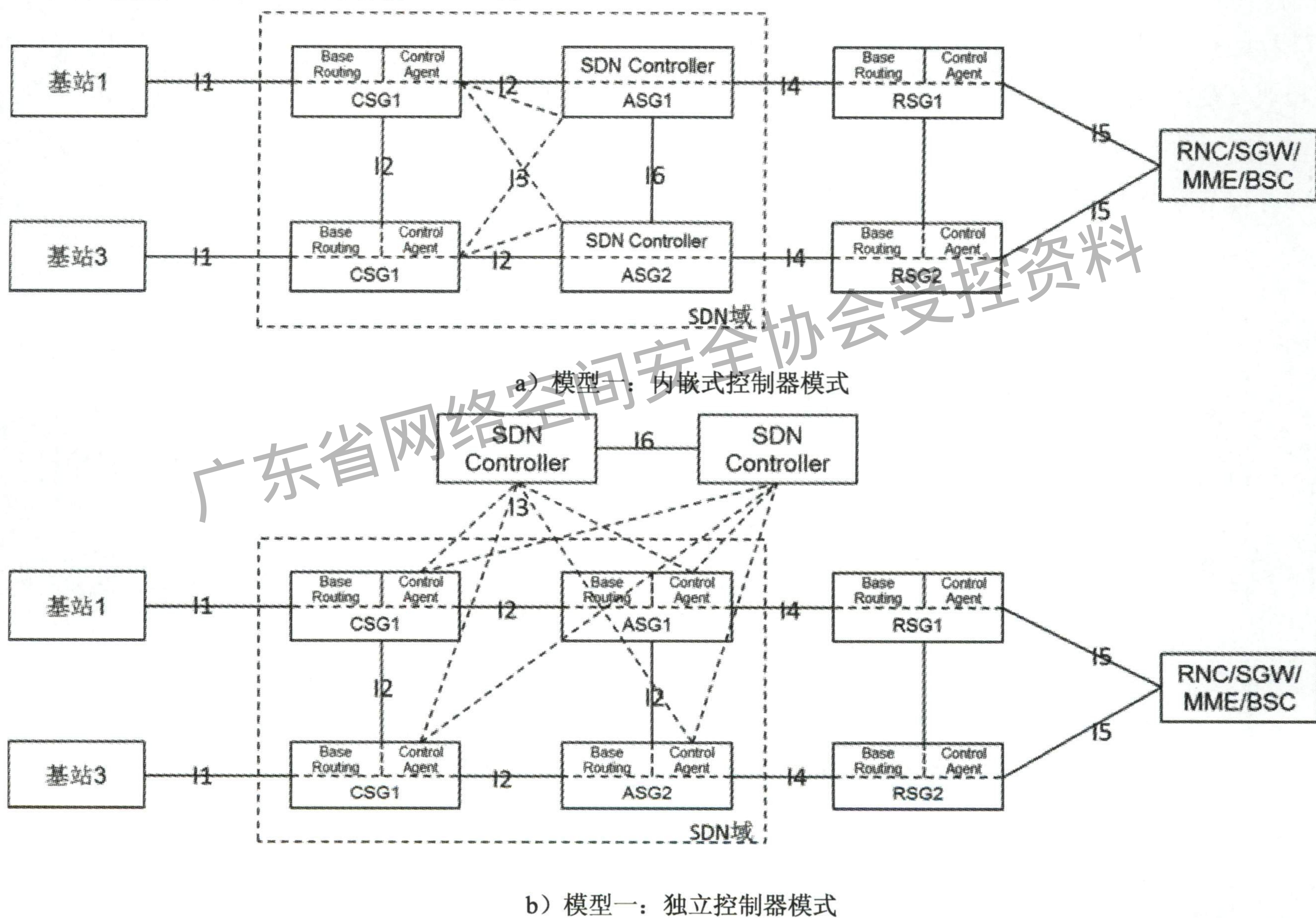


图3 基于SDN的IP RAN网络组网模型

对于接入SDN化的IP RAN网络, 可以采用内嵌式控制器模式(如图3a所示)以及独立控制器模式(如图3b所示)。

内嵌式控制器模式, 在汇聚层汇聚设备上集成控制器功能。在这种方式中, SDN域中有多个控制器(多个汇聚设备)。每个控制器只控制自己下挂的接入设备。对于每台接入设备同时下挂在两个(或者多个)控制器的情况下(如环网), 选择其中一个控制器作为主用控制器, 其他控制器作为备用控制器。而从网络层面看, 控制器也可做负载分担, 每个接入设备的主备控制器可以不同。一部分接入设备以一

个控制器（例如控制器1）为主，另一控制器（例如控制器2）为备；同时另一部分接入设备以控制器2为主，以控制器1为备，实现控制器1和控制器2的负载均衡。建议一个接入环的A类设备以同一控制器为主，这样可以减少互为主备的控制器间的数据同步的流量和业务控制联动导致的时延。

内嵌式控制器完成网络虚拟化功能后，SDN域内部接入设备的拓扑对外不可见。对于外部的路由设备，只与接入设备建立路由邻居，并且也认为只有到汇聚设备的路由。对外的路由设备认为控制器控制的网络就是一个虚拟的路由器。

利用内嵌式控制器模式，可以利用现有的网络设备，进行软件的升级，即可在接入层应用SDN技术。对网络架构和网络管理模式改动小，利于快速部署SDN。

独立控制器模式，利用服务器等IT硬件，处理能力强，能够控制更大范围和更多节点，而且独立控制器运行的网络设备不再参与网络数据流量的转发，因此控制器可部署到远端数据中心，不受限于网络物理位置。

与内嵌式控制器只控制所附着的汇聚设备下挂的接入设备不同，独立控制器可以控制多个汇聚设备下挂的接入设备，并且包括汇聚设备本身。在独立控制器情况下，接入设备、汇聚设备都集成控制代理模块（视控制范围），用于向控制器上报状态，接受控制器控制等。

2) 模型二：IP RAN网络整网SDN化

IP RAN网络整网SDN化模型如图4所示。

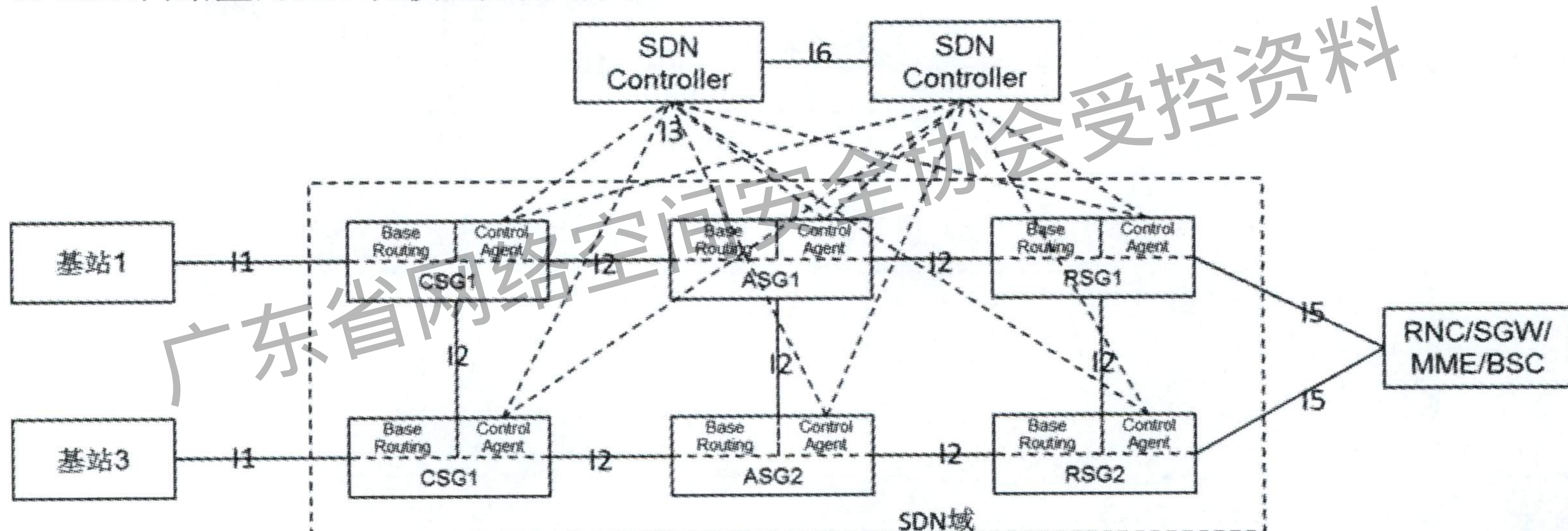


图 4 模型二

注：图3、图4中各接口的定义详情参见4.2.5。

基于SDN的IP RAN另一个组网模型是IP RAN网络整网SDN化如图4所示，将核心设备、CE也纳入到控制器控制范围内。接入SDN化能解决当前网络急剧扩张带来的管理和运维上的突出问题，但是也带来了SDN控制域与非SDN控制域间业务交互的复杂性。从长远来看，IP RAN全网统一管理，在网络优化、路径调整、运维简化方面的优势更明显。

在这种模式下，独立控制器可以控制全网节点，包含接入设备、汇聚设备和核心设备。这些设备都集成控制代理模块，用于向控制器上报状态，接受控制器控制等。

以典型的两层控制器层次结构为例，层次控制器结构图如图5所示。

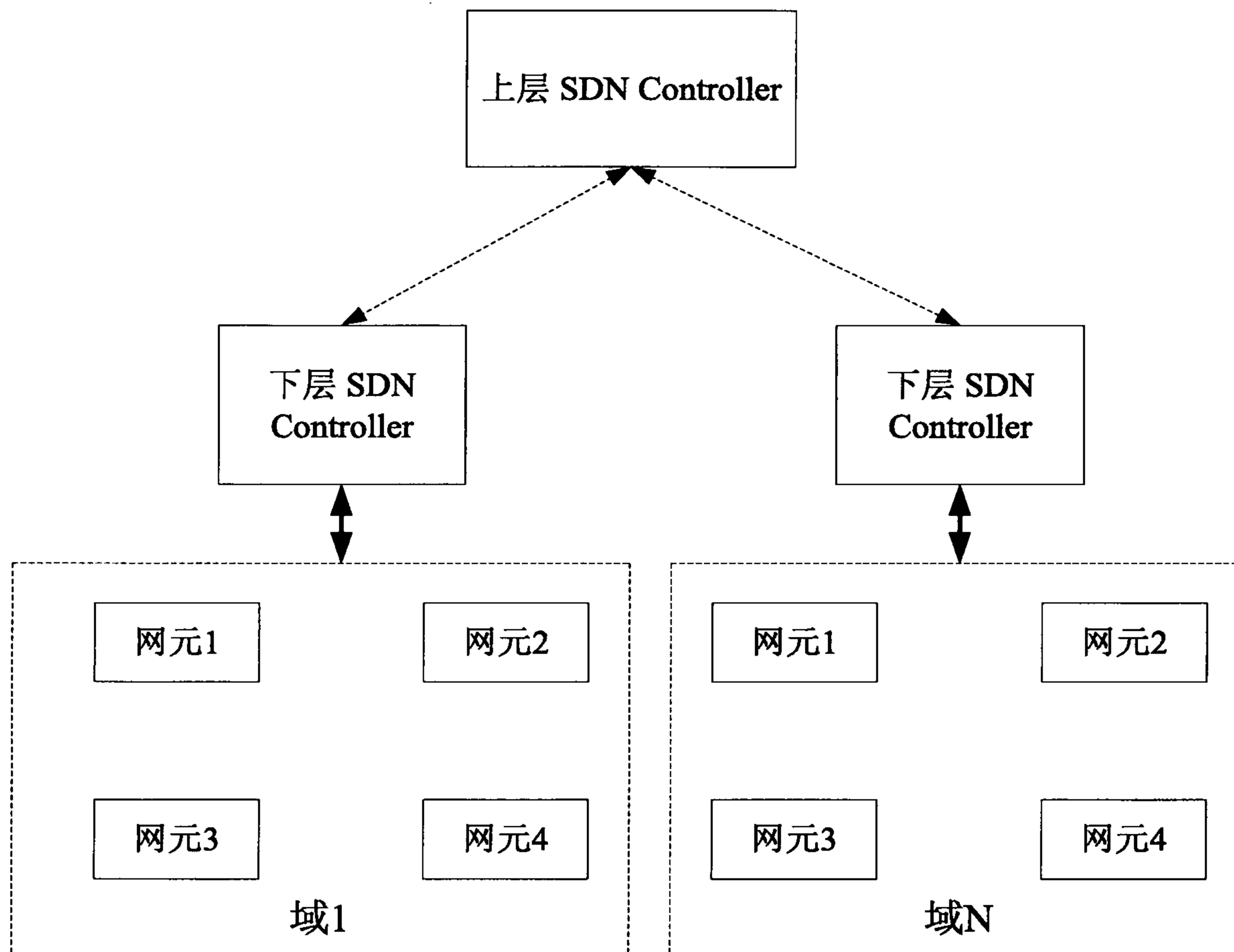


图 5 多个控制器的层次结构示意

其中控制器应该采用层次结构，单域控制器负责管理本域内的网元，完成由上层Controller下发的业务部署、查询、路径计算功能，上报本域内的物理拓扑或抽象拓扑给上层 controller，上层 controller 管理的资源可以为下一层的 controller 使用。

4.2.5 控制面

控制面完成网络拓扑收集，网络资源统一管理，网络虚拟化和业务处理，根据业务诉求为每个转发节点生成转发表项或流表项，并安装和下发到各转发节点，控制网络的业务转发、保护倒换等行为。

基于SDN的IP RAN包括如下接口定义（接口编号如图3和如图4所示）：

- I1：基站与接入转发节点之间的接口，与传统IP RAN网络与基站的接口保持一致。
- I2：转发节点之间接口。转发节点间接口完成管理和控制通道建立，以及拓扑收集。
- I3：转发节点与控制器之间接口。该接口运行控制协议（例如，Openflow协议等），通过该协议完成转发节点的注册，信息上报以及接受转发控制信息。在独立控制器方式下，拓扑代理节点收集的拓扑信息也需要通过控制协议上报到控制器。在IP RAN网络中涉及IP/MPLS转发，因此本标准也只定义IP RAN网络转发中需要使用的控制协议内容，非IP RAN业务所需的协议内容，不再定义。
- I4：控制器与SDN域外路由器接口，运行传统路由协议，如BGP，ISIS，RSVP，LDP。
- I5：CE节点与基站控制器之间的接口，保持原有接口不变。
- I6：控制器之间主备备份接口，基于单播TCP连接接口，用于主备控制器之间备份路径。

4.2.6 管理与应用面

控制器提供北向接口，用于网管和OSS集成。同时，控制器需要提供开放编程接口，用于第三方应用的集成开发。例如，第三方的性能监控应用在监控到网络某条路径出现丢包等链路质量劣化情况下，可以使用控制器的编程接口，控制控制器对某条路径进行主备倒换。控制器提供的北向接口分为以下几类：

- 策略控制接口，包括路由策略，ACL等。

- 业务接口，包括L2VPN，L3VPN等。
- 路径控制接口，对转发路径的控制，如主备倒换，定义带宽约束等。
- 监控接口，故障事件，网络质量阈值，系统状态监控，统计。
- 资源接口，带宽资源，网络拓扑，标签资源，接口资源等。
- 诊断工具，ping，tracert，NQA等。

网管与转发节点间接口：

管理通道采用独立的VPN，与业务通道区分开。网管可通过管理通道管理转发节点。转发节点的控制面已经上移到控制器，因此转发节点对网管提供的可管理功能，只是对转发节点设备本身的设备管理功能：

- 设备升级。
- 设备管理协议，如SNMP、telnet、ftp、OF-config等。
- 端口管理。
- 设备本身电源、电压、单板硬件的管理功能，如告警、单板重启等。
- 设备本身的环境监控，如温度告警。

4.2.7 转发面

考虑到现网已大规模部署，为了兼容现有网络硬件条件，初期网络层网元级的互联互通及数据流转发兼容IP/MPLS协议集(MPLS-TP为其子集)。后期，待openflow流表芯片发展成熟，逐步向openflow流表转发演进。

转发面接收控制器配置的业务流转发指令转发业务。在保证控制器和转发面之间支持标准的协议(如OpenFlow等)前提下，转发面转发方式的选择对于SDN架构的开放性没有影响。转发面内部的具体实现方式可以有多种选择，如采用符合OpenFlow标准的多级流表转发方式，或传统的IP/MPLS转发方式等。因此对于转发面的实现应遵循尽量简化原则，对其具体实现方式不做限制。

5 基于 SDN 的 IP RAN 网络控制面的技术要求

在基于SDN的IP RAN中，由控制器对网络业务进行集中控制。控制器通过控制协议对转发节点进行控制，需要具有收集网络信息（如拓扑信息），集中路径计算，控制转发节点建立转发路径的功能。转发节点需要具有向控制器注册，上报信息，接受控制器下发的转发控制功能。控制器与转发节点的控制协议可以基于OpenFlow协议，也可以是其他协议，如I2RS，本章主要定义对协议的功能要求，不涉及具体的协议封装格式。

SDN能够集中控制，则应要求控制器与转发节点之间能够建立起控制协议连接。由于控制协议是基于TCP/IP（如OpenFlow），因此要求控制器与转发节点之间IP可达。是选择独立的控制通道，还是控制通道使用业务通道，需要视具体网络部署，为了保证控制通道的可靠性，建议采用物理或者逻辑独立的控制通道。控制器与转发节点的IP可达性保证建议采用现有网元自通方案。

5.1 管理通道建立

网管作为网络中各转发节点的管理与配置实体，也是必不可少的组成构件，网管使用网管自通方案与转发节点建立管理通道。

为了实现网管与接入设备间管理通道的建立，要求接入设备、汇聚设备和网管支持以下功能要求和控制协议流程：

- 1) 接入设备的I2接口和汇聚设备的I2接口都应支持标准的OSPF协议及附录A所描述的OSPF协议扩展TLVs;
- 2) 接入设备的I2接口、汇聚设备的I2接口、汇聚设备的网管接口都应支持标准的LLDP协议及附录A所描述的LLDP TLV，或者都应支持标准的ARP协议；
- 3) 接入设备应支持上电后自动创建网管自通环回口Loopback管理接口、自动生成管理IP地址、自动创建OSPF进程、自动创建DCN VRF、自动在I2接口使用特定的VLAN（4094）创建P2P（无编号）类型的子接口并绑定DCN VRF，该子接口借用网管自通Loopback接口IP地址；
- 4) 汇聚设备应支持P2P（无编号）类型的子接口，汇聚设备的管理IP地址等参数由网管配置；
- 5) 接入设备与汇聚设备利用OSPF协议建立起DCN VRF的路由连接，汇聚设备把通过OSPF协议获取的接入设备信息上报给网管，网管与接入设备之间建立起经过汇聚设备的管理通道。网管自通的详细实现规范见附录A。

注：I2接口在第4章已定义。

5.2 控制通道建立

在基于SDN的IP RAN网络中，控制器（SDN Controller）作为网络中接入设备和汇聚设备的控制实体，是其必不可少的组成构件，控制器在网络中的位置如图6所示。

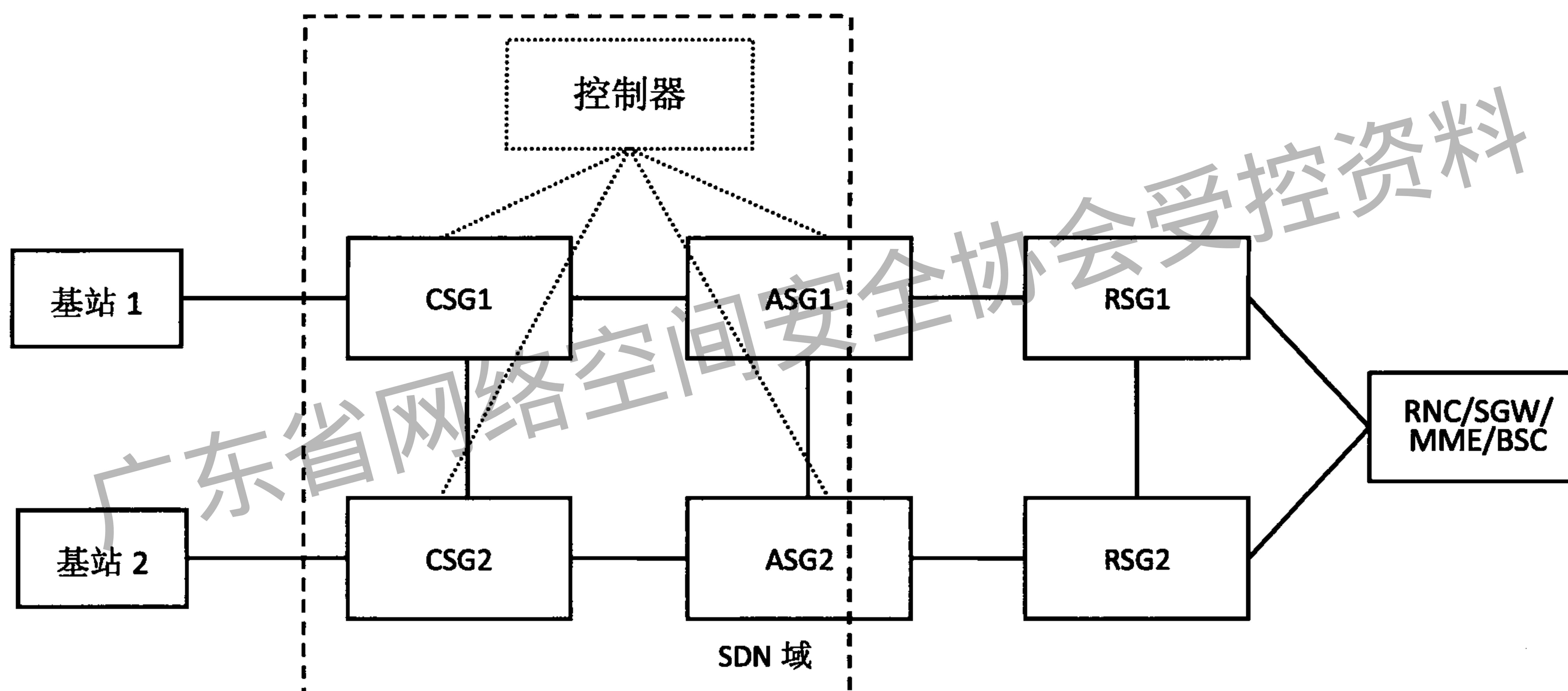


图 6 控制器在网络中的位置示意图

与管理通道的建立相类似，控制器与接入设备、汇聚设备之间控制通道的建立也要求IP可达，所以控制通道的建立也可以采用类似于现有网管自通的方案。二者的区别在于，网管同时负责SDN域内网元和SDN域外网元的管理，所以网管与核心设备、汇聚设备之间的管理通道是现成的，而控制器只负责本SDN域内网元的控制，所以控制器与接入设备、汇聚设备之间的控制通道都需要从零开始建立，可采用与管理通道建立类似的方法，以下为控制通道建立方案的描述。

为了实现控制器与接入设备、汇聚设备间控制通道的建立，要求接入设备、汇聚设备和控制器支持以下功能要求和控制协议流程：

- 1) 接入设备的I2接口和汇聚设备的I2接口都应支持标准的OSPF协议；
- 2) 接入设备的I2接口、汇聚设备的I2接口、汇聚设备的控制器接口都必须支持标准的LLDP协议及附录A所描述的LLDP TLV，或者都应支持标准的ARP协议；

3) 接入设备和汇聚设备由网管利用已建立的管理通道配置控制器的IP地址、控制通道所采用的TCP端口号（根据ONF发布的《OpenFlow交换机规范》（其中包含OF-Switch协议）的规定，默认端口号为6653）以及是否使用TLS加密协议；

4) 接入设备与汇聚设备利用OSPF协议建立起Control VRF的路由连接，接入设备和汇聚设备根据所配置的控制器IP地址发起与控制器之间的TCP连接（可以采用TLS加密），控制器与接入设备之间建立起经过汇聚设备的控制通道，控制器与汇聚设备之间也建立起控制通道。

注：I2接口在第4章已定义。

5.3 控制器与转发节点整体交互过程

本节描述在IP可达之后，控制器与转发节点之间的整体交互过程。

根据第4章的需求描述，IP RAN承载业务是L2VPN和L3VPN业务。因此基于SDN的IP RAN在端到端的业务路径控制上可以分为三个阶段来描述：

阶段一：SDN控制域的建立。这个阶段控制器进行拓扑发现，转发节点向控制器注册。这个阶段与转发业务无关，是SDN域的建立过程。这个阶段基于控制器与转发节点之间已经IP可达。

阶段二：路径计算。这个阶段控制器集中路径计算，集中控制建立转发路径，对外呈现一个边缘节点全连接互通的抽象网络。

阶段三：L2VPN和L3VPN业务的建立。在第二阶段建立的虚拟化网络基础上，控制器集中控制L2VPN和L3VPN的建立，包括L3VPN路由的交叉和优选等。

本节首先描述控制器与转发节点之间的基本功能分工和运行过程，然后在后续章节详细描述控制面的三个阶段技术要求。本节假设控制器已经与转发节点IP可达，可以建立TCP链接。总体交互过程如图7所示。

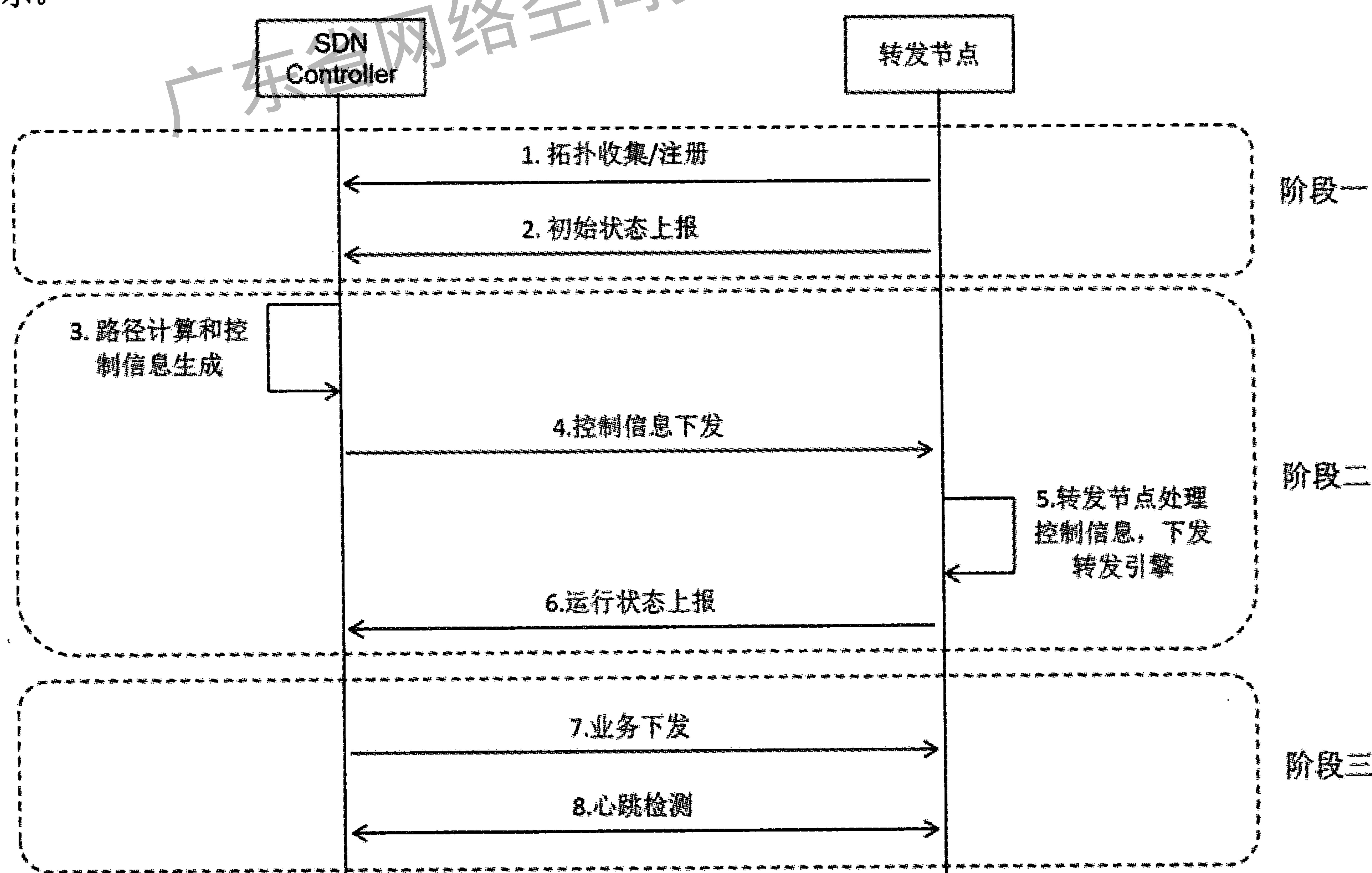


图7 控制器与转发节点交互

步骤1) 控制器需要首先收集网络拓扑信息和注册。

- 步骤2) 转发节点注册后向控制器上报信息，如端口信息。
- 步骤3) 控制器根据拓扑生成转发路径和表项。
- 步骤4) 控制信息通过控制协议下发到转发节点。
- 步骤5) 转发节点根据控制器下发的控制信息设置转发表项。
- 步骤6) 在运行过程中转发节点上报状态，如端口状态，统计信息等。
- 步骤7) IP RAN业务建立和下发。
- 步骤8) 在运行过程中控制器与转发节点之间应该维持心跳检测，以确定转发节点是否正常。

5.4 SDN 控制域建立的技术要求

5.4.1 拓扑收集

作为控制器集中控制的基础，控制器需具备网络的拓扑信息收集功能，从而基于拓扑信息计算路径和控制转发。控制器拓扑收集完成提供各转发节点端口信息及两两网元间的链路信息，获取整网网络拓扑。

拓扑发现可通过LLDP等拓扑收集技术，具体实现过程可参考附录B。

5.4.2 转发节点注册

控制器与转发节点之间采用客户端-服务器端（Client-Server，简称CS）模式进行注册。CS模式被广泛用于互联网服务。这种模式中，服务器端处于被动状态，由客户端主动发起连接和请求服务。这种模式适用于客户端不固定，而服务器端提供固定服务的形式，控制器与转发节点之间的关系类似客户端-服务器模式。控制器作为提供路径计算，转发路径建立等控制服务的服务器端，转发节点作为请求路径计算服务的客户端。

1) 转发节点发现控制器：

- 依据5.2节过程，转发节点完成控制器的自动发现。

2) 转发节点向控制器发起注册：

- 转发节点在发现控制器后，向控制器发起注册，主动建立协议连接。

● 为了保证安全性，转发节点与控制器之间可选使用认证机制，如SSH。认证建议是双向的，控制器需要防止非法的转发节点接入，转发节点也要防止非法的控制连接，因此转发节点也可选对控制器进行认证。

● 转发节点可向多个控制器发起注册，如主备控制器。同时控制器也应该可以接受多个转发节点的注册。

● OpenFlow协议已经有具体的注册过程，具体过程参考OpenFlow协议。如果使用其他控制协议，注册过程按照相应的协议处理。

3) 转发节点与控制器之间进行能力协商：

● OpenFlow协议已定义能力协商功能。如果使用其他控制协议，能力协商功能按照相应的协议处理。

- 控制器能够控制的功能是控制器与转发节点支持的交集。

4) 转发节点状态上报：

认证和能力协商后，转发节点上报自身的状态信息，包括：

- 端口信息和状态——控制器需要根据节点的端口和端口状态进行路径计算和路径调整。

- 标签空间/流表大小——控制器在进行路径计算和路径建立时需要为每个转发节点下发表项。
- 转发节点注册的控制器——控制器需要了解被控制的转发节点，向哪些控制器进行了注册，以便在控制器之间进行信息同步。

5.4.3 路径建立

基于SDN的IP RAN的网络将IP RAN网络抽象（虚拟）化成一台路由器，使得在业务部署时不用再关注网络侧内部的协议和路径，简化网络部署。IP RAN网络虚拟化手段通过SDN的集中算路和路径自动化计算功能实现，IP RAN网络抽象为汇聚模型的Fabric。采用汇聚模型的Fabric，因为IP RAN网络实际的网络流量模型主要为汇聚模型，从接入层接入设备汇聚到汇聚层（汇聚设备），最终汇聚到核心设备节点。对于LTE的X2流量，流量占整个IP RAN承载业务的流量比重不大，X2建议采用业务触发建立路径的方式。

由于是汇聚型Fabric，系统需要清晰的知道流量的汇聚点。因此在网络组网时，需要为每个转发节点指定其角色，即接入设备、汇聚设备、核心设备。

- 接入设备为业务的接入点，接入设备的UNI侧接入基站，接入设备的NNI侧接入网络。
- 汇聚设备为网络的汇聚分层点。
- 核心设备为流量的最终汇聚点，网络流量经过核心设备汇聚到无线核心网。

所有转发节点都具有NNI侧接口和UNI侧接口。NNI侧接口在业务部署时不可见，网络虚拟化使用NNI侧接口建立Fabric。UNI侧接口是在业务部署时可见的接口，接入基站或者接入无线核心网。控制器可以通过拓扑发现NNI接口，其他接口可以作为UNI接口。

路径建立（网络虚拟化）过程具备以下能力：

1) 触发路径的计算

当转发节点注册成功后，控制器即自动触发对该转发节点的转发路径的计算。控制器基于拓扑收集阶段收集的全局拓扑进行计算，并需要为路径的每一跳生成转发表项。

2) 路径的约束

路径默认建立为双向共路的路径，以便于将来的故障定位和日常维护。

路径可以增加带宽约束。

3) 主备路径

控制器应该自动的为转发路径生成主备路径，除非拓扑不允许（如（图8 a）链形组网的情况）。且主备路径应该避免出现共链路的情况，以保证可靠性，除非拓扑不允许（如（图8 b）链带环的情况）。图8描述了这两种组网。

4) 转发路径的下发

通过控制协议向路径中每个转发节点下发转发路径。控制转发路径下发顺序，避免先成功建立头节点路径，引入流量，中间节点/尾节点滞后，导致流量过早注入网络的情况。

5) 可靠性

为了保证故障的快速检测和切换，建议故障检测、故障场景下保护倒换处理在转发节点实现。故障检测可选部署BFD或者MPLS-TP。

BFD或者MPLS-TP在转发路径建立时由控制器下发，同步自动部署。

故障检测机制要求见6.3.2节。

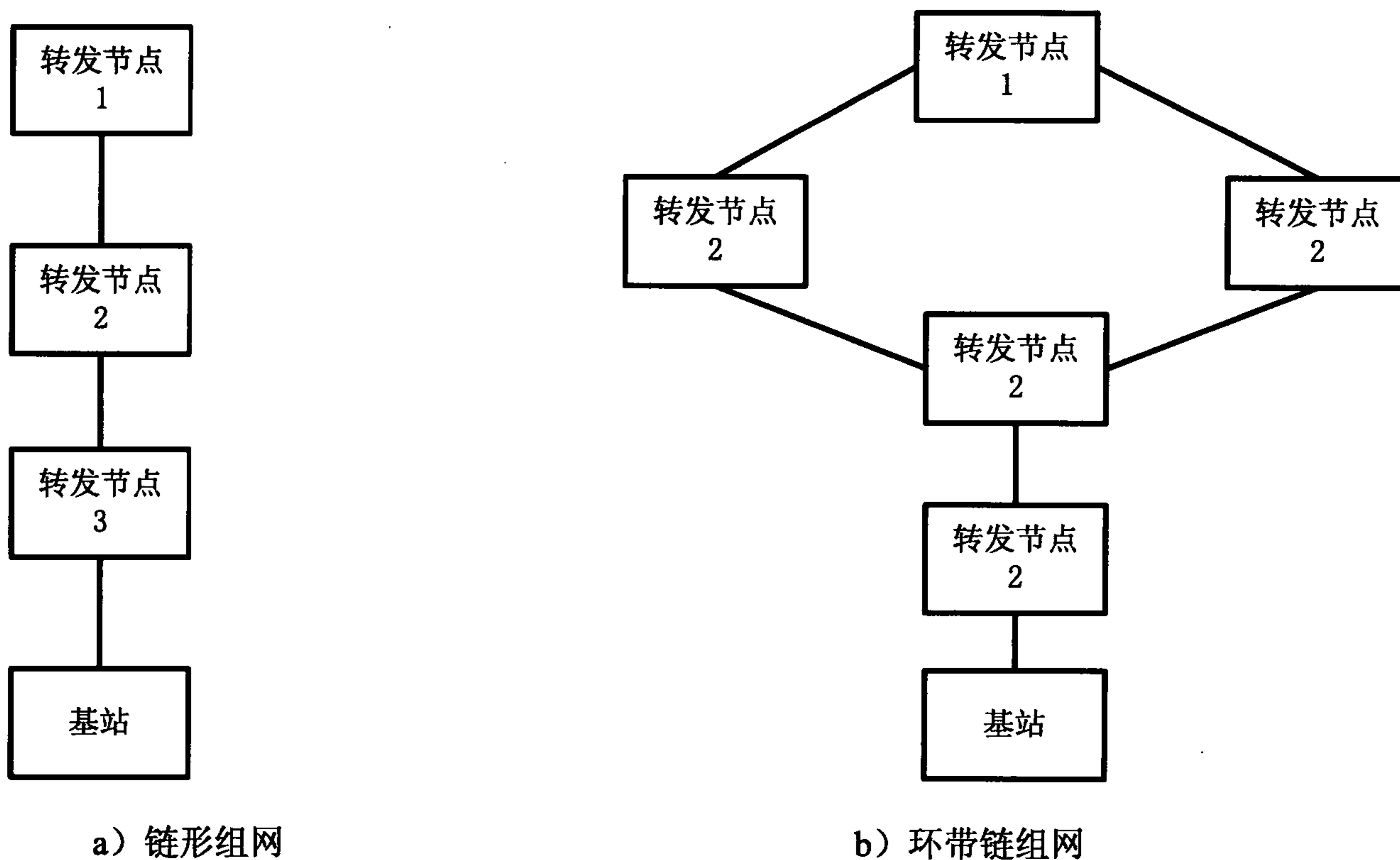


图 8 两种组网拓扑

5.4.4 VPN 业务建立

IP RAN的VPN业务是L2VPN和L3VPN业务。传统的VPN业务需要配置接入端口，在PE之间配置协议传递私网信息，在各PE上配置VPN路由的交叉关系，以及配置中间隧道，业务开通和运维较复杂。实际上PE之间的网络，VPN业务本身并不关注，只用提供隧道即可。基于SDN的IP RAN通过路径建立过程，对网络进行了抽象，达到VPN的业务发放就如在一台路由器上进行业务配置的效果。本节描述VPN业务的发放和技术要求。

1) 逻辑业务端口与实际业务端口进行匹配

L2VPN和L3VPN业务在控制器上进行配置。为了能够在控制器上对网络中所有的转发节点UNI接口进行统一操作，在控制器上创建逻辑业务端口，并将逻辑业务端口与实际端口进行绑定。

2) L2VPN创建

a) 在逻辑端口进行AC端口配置，指定加入L2VPN的AC端口。

b) 控制器根据AC端口对应的实际物理的转发节点，与对应的Fabric进行迭代。

c) 控制器为L2VPN的PE生成表项，并下发。由控制器分配标签，转发节点不必运行标签分发协议（如LDP）。

d) 业务建立时，控制器自动部署可靠性，PW Redundancy，BFD或者MPLS-TP。可靠性应该提供可调整的配置接口，以便满足各种网络诉求。

3) L3VPN创建

a) 在控制器上创建VRF。

b) 在控制器上将逻辑端口加入VRF。

c) 控制器进行VPN的路由交叉和并为每个PE优选VPN路由。并为VPN路由分配私网标签。转发节点之间不再运行BGP协议来扩散VPN路由和标签。

d) 控制器对VPN路由进行迭代，并将每个PE的VPN路由下发到对应的PE。

在业务建立时，控制器应该自动部署可靠性，如VPN FRR。控制器也应该提供可调整的配置接口，以满足各种网络的特殊诉求。

6 基于 SDN 的 IP RAN 网络转发面的技术要求

6.1 基于 SDN 的 IP RAN 转发节点系统架构

转发节点由数据平面模块、控制代理模块、管理代理模块和网元自通模块组成，如图9所示。

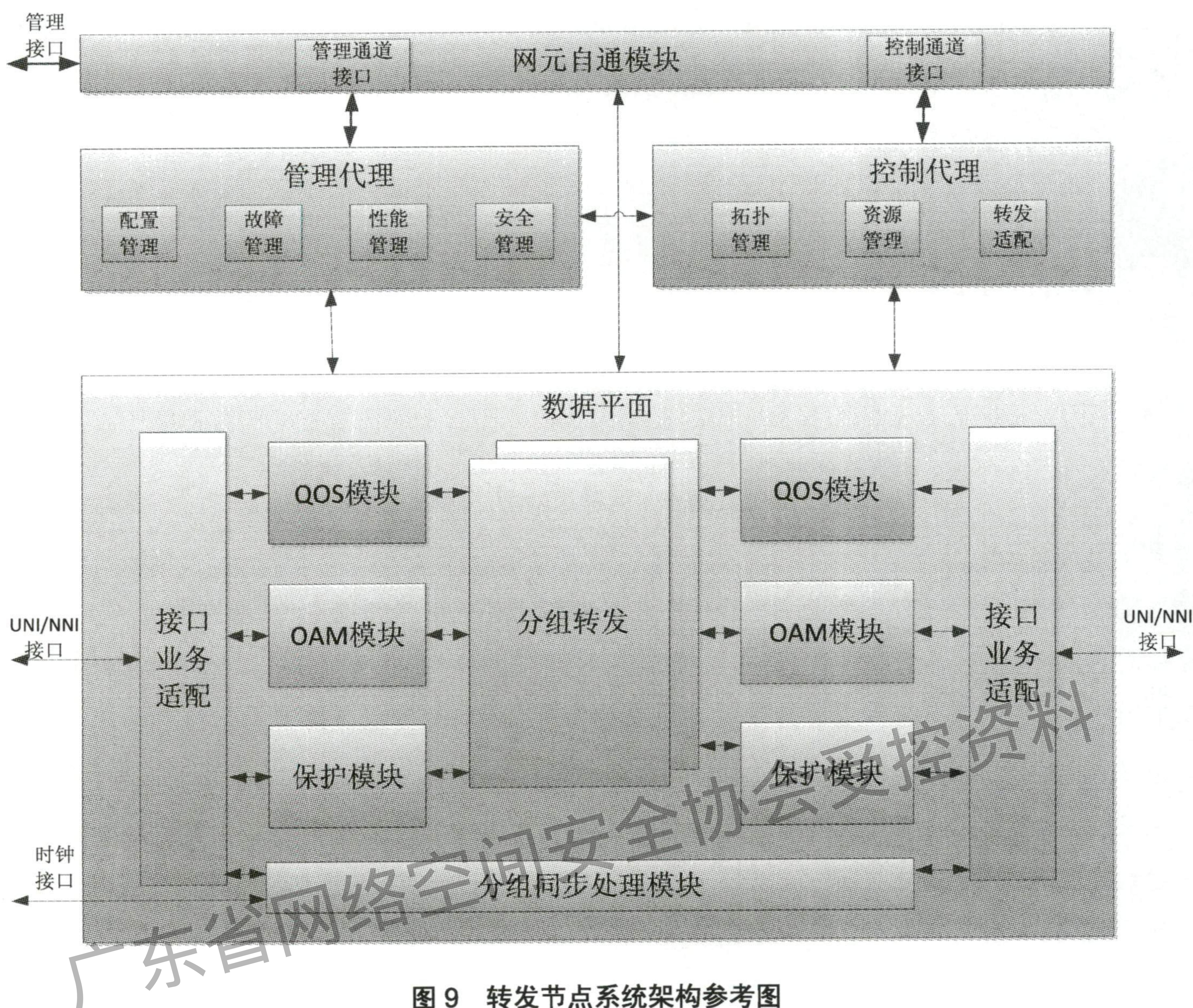


图 9 转发节点系统架构参考图

转发节点的控制面已经上移到控制器，转发节点对网管提供的可管理功能主要为转发节点的设备管理功能。管理代理接收来自网管的配置信息，提供向网管的设备端口、电源/电压，环境监控等信息。

控制代理接收从控制器下发的外部信令信息和转发信息，经过控制器的信令和转发适配等模块处理后，结合自身的信令与转发信息，将必要的转发信息下发给数据平面，实现控制代理对数据平面的控制。

数据平面完成数据的转发，同时具备发送转发状态信息到控制代理，实现对控制代理相应模块的查询、响应和反馈能力。控制代理将需要传送到外部的转发状态信息通过信令通信接口发送给控制器。

6.1.1 数据平面

数据平面由接口业务适配、分组转发、QoS、OAM、保护、同步模块组成，提供分组转发、OAM、QoS、保护、同步等功能，通过接口业务适配模块实现UNI侧各类业务的接入处理，以及实现NNI侧业务入出或穿通MPLS隧道。数据平面还可为控制代理和管理代理提供控制信息和网络管理信息的传送功能。

QoS、OAM、保护功能要求见YD/T 2603-2013第6章相关规定。

6.1.2 控制代理模块

控制代理的作用是建立标准的安全通道，并和控制器建立控制协议通道；OpenFlow是可选控制协议之一，未来还可能有其他控制协议，如I2RS。控制代理应该提供协议适配，对数据平面屏蔽协议之间差异，可扩展支持其他控制协议。

对当前OpenFlow协议未支持的数据，提供上下双向的传输通道，并提供适配，以完成例如OAM/QoS/APS等功能数据的配置和设置。

控制代理应为管理代理平面提供服务响应和故障上报，包括对控制代理的信息查询响应和转发信息、信令等控制参数的配置响应，以及向管理代理报告控制代理故障信息等。控制代理建立的连接可根据需要由管理代理拆除。

控制代理提供拓扑收集功能，收集本地网络拓扑，并将网络拓扑信息上报给控制器。

控制代理提供资源管理功能，收集本地转发资源，如端口，标签空间等，并通过控制协议上报给控制器。

6.1.3 管理代理模块

管理代理提供配置管理、故障管理、性能管理和安全管理等功能。管理代理实现对数据平面、控制代理和网元自通模块的管理。

管理代理实施对数据平面、控制代理以及系统的管理，并提供完备的管理功能和辅助接口，确保各平面之间的协同，管理代理失效不应影响数据平面的正常工作。

配置管理实现对子网、网元、端口、业务、路径、保护、OAM、QoS、同步等的配置，故障管理提供对告警的采集、显示、存储、处理、查询、同步等功能。

性能管理实现对各层面对象（端口、隧道、伪线、段等）性能的监测、门限管理和数据处理（上报、查询、统计、存储等）。对于支持OpenFlow的设备，基于流表的统计也可以通过OpenFlow协议上报。

安全管理用于用户和日志管理以及权限控制。

6.1.4 网元自通模块

网元自通模块负责打通控制器/网管和转发节点之间的管理/控制通道，保证控制器/网管和转发节点之间能够IP可达。网元自通模块建立了一张IP网络，管理连接和控制连接均使用该网络进行通信。

6.1.5 业务接口

具体功能接口需求见YD/T 2603-2013的6.10。

6.2 基于 SDN 的 IP RAN 转发节点协议需求

基于SDN的IPRAN设备不再使用传统的分布式协议（如BGP, LDP），业务的建立和管理由控制器实现。为了保证转发节点的即插即管理，转发节点可保留一些基本路由协议，如网元自通的OSPF协议。同时具备管理协议（Netconf, SNMP等），控制协议（如OpenFlow、I2RS等）。

6.3 OpenFlow 化 IP RAN 转发节点

基于SDN的IP RAN设备则需裁减大部分IP RAN路由及信令功能，只保留基本的路由功能，提供与控制器及网管之间建立控制通道和管理通道的功能。网络拓扑管理。通过控制代理模块接受控制器的控制和上报本身的资源和状态（如端口）。需要提供传统的网管接口，提供设备本身的管理接口，如，电源，电压，单板等管理功能。转发节点提供基本的网元自通功能和基于OF流表的转发功能。典型的基于OPENFLOW的SDN化IP RAN设备主要处理模块结构关系图如图10所示。

所有的标签由控制器集中控制生成，不需要分布协议来生成，因此也不需要进行层层配置查找。在SDN网络中，控制器负责端到端业务的创建并转换为控制协议下发给各设备。控制器通过控制协议，将转发表下发给设备，设备根据转发表执行相应的动作。其他OAM、保护配置等通过OF-Config或者Netconf协议或者其他扩展协议由控制器下发给管理代理模块后，由管理代理转换成配置下发给设备。

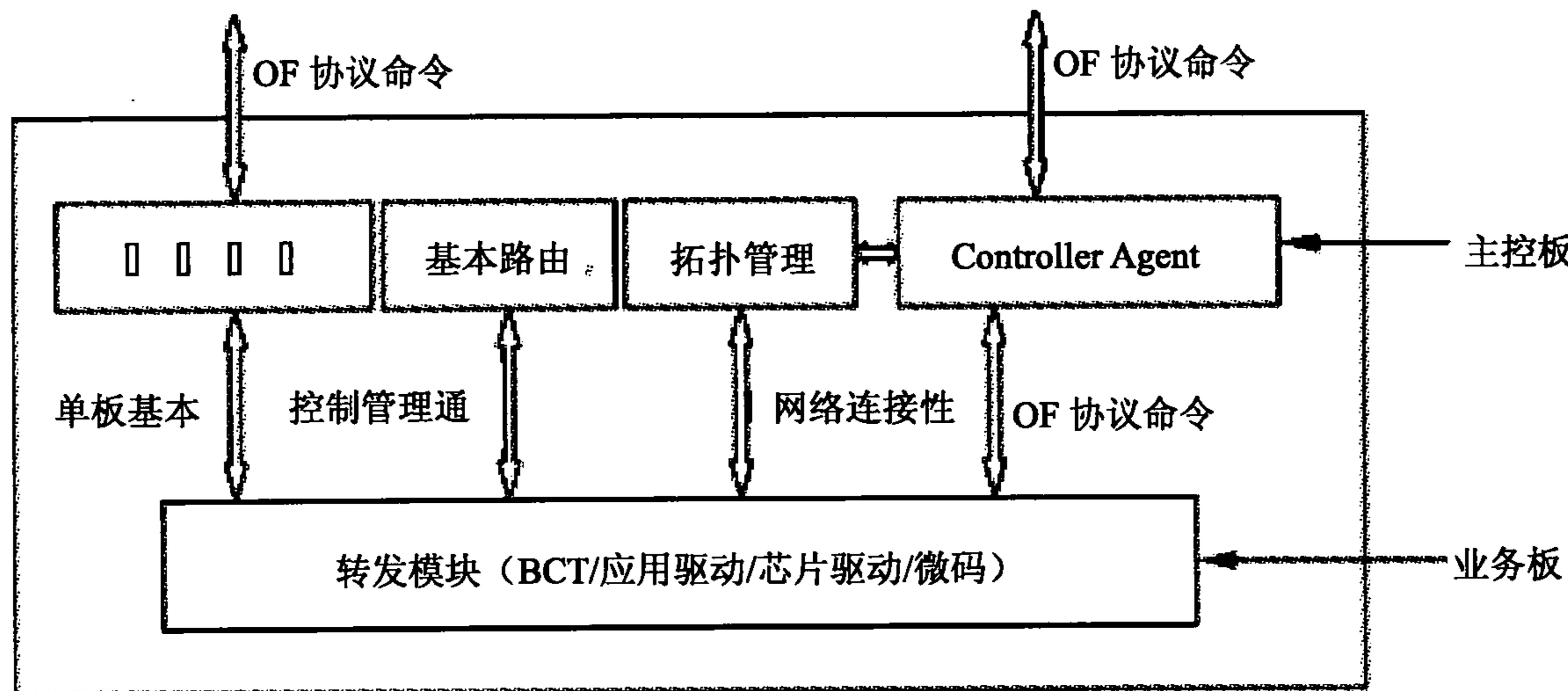


图 10 主要处理模块结构关系图

6.3.1 基于业务流处理流程

OpenFlow化的IP RAN数据平面接收OpenFlow流表并在此基础上执行转发，但是需要实现的转发功能仍然要满足YD/T 2603-2013中定义的功能。

6.3.2 OAM 处理过程

根据 OpenFlow 协议，任何流的建立和删除都需要通过控制器来实现。当需要进行流保护时，OAM 信息检测设定流保护对，当主用出现故障时，控制器更新流表的内容，交换设备完成业务的重新定向。

基于上述控制器的 OAM 实现方案存在三个方面的问题：

- 1) 控制器和交换机之间的信息交互机制会带来 OAM 信息的延时，这种延时会使倒换时间不能满足要求。
- 2) 控制器和交换机之间的信息交互机制会给控制器带来巨大的报文处理压力。
- 3) 控制器和交换机之间的安全通道的失效会触发错误的倒换机制。

因此，对于 OpenFlow 化的 IP RAN 网络 OAM 的实现需要满足如下技术要求：

- 1) 控制器完成对位于 OpenFlow 设备上的 OAM 引擎的启动、配置；
- 2) OpenFlow 设备上的 OAM 引擎完成所有的 OAM 的功能，包括故障检测，业务倒换，环回建立，延时、抖动测量等；
- 3) OAM 需要满足多层次业务检测需求，如 LSP 层，PW 层及 Section 层 OAM 功能；
- 4) OAM 检测性能需要满足 YD/T 2603-2013 中的定义。

除此之外，OpenFlow 的 OAM 实现要根据 ONF 标准组织的进展而定，必要时可采用私有扩展方式。

6.3.3 保护信息流处理过程

基于 SDN 的 IP RAN 设备需要支持多保护类型和功能性能要求应符合 YD/T 2603-2013 的规定。

根据 OpenFlow 协议，任何业务流的建立和删除都需要通过控制器来实现。当需要进行流保护时，控制器配置业务流的主备路由，当主用路由出现故障时，IP RAN 设备完成业务的重新定向。

注：YD/T2603-2013 规范的保护类型都涉及到工作通道和保护通道的建立，OpenFlow 协议中定义了 Group Table 的概念，其功能之一是有效地实现报文的多径转发，利用 OpenFlow 多径转发的特性，可以建立所需的工作通道和保护通道。IP RAN 网络有不同保护类型，它们保护的对象属于网络的不同层次，OpenFlow 协议虽然支持多径转发，但如何处理这些不同层次的保护却没有明确的定义，因此，需要针对这个问题对 OpenFlow 协议的进行相应的扩展来实现不同层次的 APS 功能。OpenFlow 协议在保护方面的扩展 FFS。

6.3.4 时钟同步功能

同步时钟功能要求见YD/T 2374-2011第9章的相关规定。

7 基于 SDN 的 IP RAN 网络管理的技术要求

7.1 控制器管理接口

基于SDN的IP RAN网络管理技术中对控制器的管理接口要求如下：

- 1) 控制器应提供基于RESTful的北向接口，为第三方开发使用，提供拓扑上报、业务部署、故障上报、性能统计等常见功能。
- 2) 为了保持与现有网络平滑过渡，也应提供传统的Netconf, SNMP接口。
- 3) 控制器应提供syslog等接口用于日志上报。
- 4) 由于网络的控制面集中到了控制器，因此网络的业务配置、告警、监控等接口均应由控制器提供。

7.2 转发节点管理接口

基于SDN的IP RAN，转发节点仍然保持了一部分管理面功能，因此转发节点也应该提供传统的网管接口，如Netconf, SNMP。转发节点的管理接口用于日常设备的维护，如电源，电压等。但是业务的配置，监控等接口，不再由转发节点提供。但是为了定位问题，转发节点应该提供对应的debugging接口，配合在控制器进行问题定位。转发节点提供性能管理接口，网管可以通过管理接口采集性能数据，同时转发节点应提供syslog日志接口，上报日志。

8 传统 IP RAN 网络向基于 SDN 的 IP RAN 网络迁移技术要求

考虑到IP RAN产品在现网已经有较多部署，在从传统IP RAN网络向基于SDN的IP RAN网络演进和迁移的过程中，需要充分考虑到，与原有网络的兼容，共同组网，互通等场景的要求。

1. 与原有IP RAN网络的兼容

当原IP RAN网络部署基本完整，仅部分节点需要增加时，需要考虑新部署的节点是支持SDN的新型设备。在这种情况下，基于SDN的IP RAN网络节点需要能与原有网络完全兼容。

a) 基于SDN的IP RAN网络节点设备应能完整支持现有IP RAN网络部署的对应所有功能集合，如不同规格对应的设备类型相应功能要求。

b) 基于SDN的IP RAN网络节点设备的SDN相关功能可以通过配置进行使能和关闭。缺省是关闭的。

2. 共同组网

在某些部署场景中，可能出现支持SDN的IP RAN网络节点和传统IP RAN网络节点共存的情况。此时，IP RAN网络已经部署了SDN的架构，如SDN控制平台，相关的网管平台也已经支持通过SDN的方式获取网络资源情况，拓扑结构等。在这种情况下，基于SDN的IP RAN网络节点设备需要支持：

a) 基于SDN的IP RAN网络节点设备需要支持原有IP RAN网络的协议功能及协议互通；
b) 原有IP RAN节点设备需要支持对协议的透传。

3. 长期演进

由于IP RAN网络节点数目众多，现网业务部署的复杂性，还有设备平台设计及芯片升级等因素，向基于SDN的IP RAN网络演进将是一个长期的过程。

在初始阶段，对混合的区域可以通过增加SDN控制平台，升级网络管理系统来进行部署，此时主要需考虑混合组网模式下，网络结点互通的问题，及传统IP RAN节点设备和SDN IP RAN设备的拓扑信息融合，混合管理模式兼容等问题。

在中间阶段，全网设备结点可通过软件或者硬件升级来支持SDN，此时SDN架构在IP RAN网络中得到应用，此时基本能解决提高网络运维效率，统一网络资源管理，拓扑自动发现，数据转发路径控制等。同时北向和南向协议接口更加完善。

随着设备的不断完善和升级，包括芯片的普及，在第三阶段，基于SDN的IP RAN网络能实现低成本的数据面设备，设备根据SDN控制器下发的流表控制建立转发表，网络整体性能和效率提升，同时OPEX得到完整优化。

广东省网络空间安全协会受控资料

附录 A
(规范性附录)
网元自通实现方案

A.1 网元自通协议流程

网元自通示意图见图 A.1 所示。网管自通方案要求免配置接口 IP 地址，使用无编号以太网接口，实现对自动生成的网管自通环回口 loopback 进行地址借用，在运行 OSPF 的点到点网络基础上，进行路由自动打通，从而实现网管自通，网管自通环回口 loopback 的 IP 地址支持自动分配和人工指定（用于后端地址重新规划）两种方式。

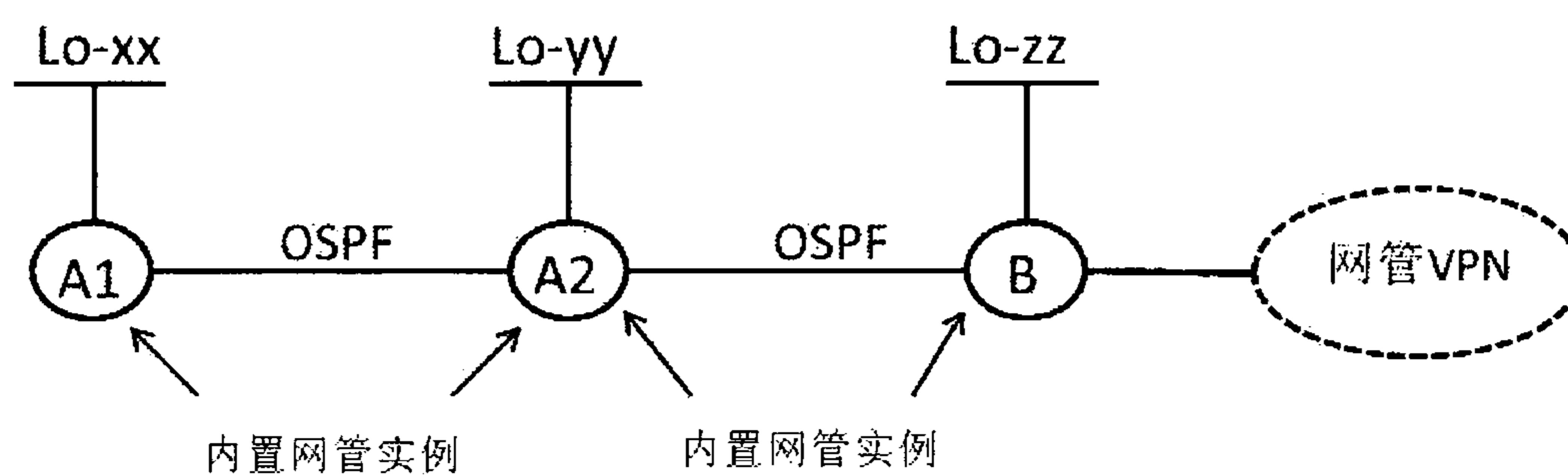


图 A.1 网元自通示意图

A.2 网管自通协议原理

接入设备上电后，自动创建网管自通环回口 loopback 管理接口，根据默认规则生成的 32 位管理地址，自动创建 OSPF 进程，自动创建 DCN VRF，在使能网管自通的接口上，使用特定的 VLAN (4094)，创建子接口，子接口类型为 P2P (无编号接口) 类型，绑定 DCN VRF，借用网管自通 loopback 接口 IP 地址。

该子接口缺省使能 OSPF 协议，使用 OSPF 标准流程进行协商、路由计算，形成网管通道 IP 路由表 (IP 路由表中 DMAC 的确定见下一节)；使用特定的 type 10 LSA 泛洪相关网元信息，包括：厂家标识、设备型号、设备 MAC、NEID、NEIP V4、NEIP V6 等信息。OSPF 网络类型为 P2P，以组播形式 (224.0.0.5) 发送协议报文 (Hello 报文、DD 报文、LSR 报文、LSU 报文、LSAck 报文)；以组播形式重传 LSU 报文。

OSPF 协议报文格式：

DA	SA	802.1Q tag
0x01005E000005	接口MAC	0x8100 4094 0x0800 OSPF IP报文

在物理接口下，可以去使能网管自通功能，删除 VLAN 子接口及相关资源，修改网管自通 loopback 接 IP 后，OSPF 需要重新协商。

汇聚设备支持 P2P (无编号接口) 类型的子接口，相关参数可以进行手工配置，支持对接入设备网元信息发现和统一网管上报，从而实现接入设备与网管自通。

A.3 网管自通管理报文封装

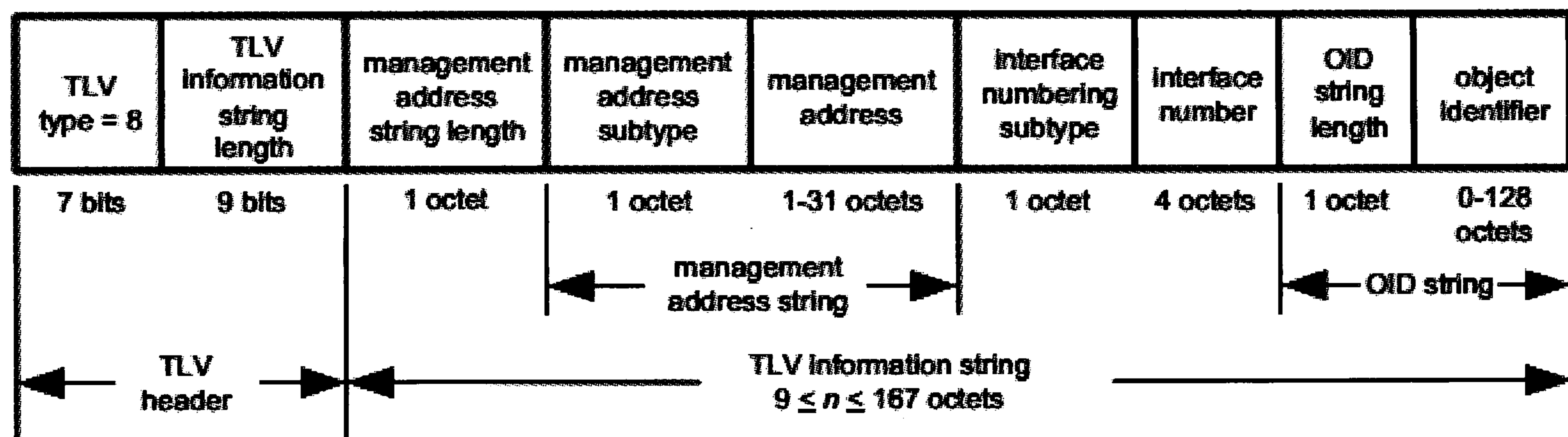
网管自通管理报文格式：

DA	SA	802.1Q tag
对端接口MAC	接口MAC	0x8100 4094 0x0800 IP报文

对端接口 MAC 确定两种方式:

1) 接口默认自动运行 LLDP (IEEE802.1ab, Link Layer Discovery Protocol, 链路层拓扑发现协议), 各网元在 LLDP 协议的 Management Address TLV 中通告网管自通环回口 loopback 的 IP 地址, 也就是对端网元的 NEIP, 保证邻居网元管理地址信息的正确发现。

该 Management Address TLV (报文中可含有多个该 TLV) 的格式如下:



相关子类型如下:

subtype 1: NEIPV4, loopback ipv4 (必选);

subtype 2: NEIPV6, loopback ipv6 (可选)。

同时通过 LLDP 协议报文中的源 MAC, 学习对端接口的 MAC address (该 MAC 支持 L3 可路由), 后续作为网管自通管理报文的目的 MAC 使用。

LLDP 协议发出报文时, 必须同时携带本端的管理 IP 和端口 MAC (支持 L3 可路由), 用于自动发现 IP-MAC 的绑定。

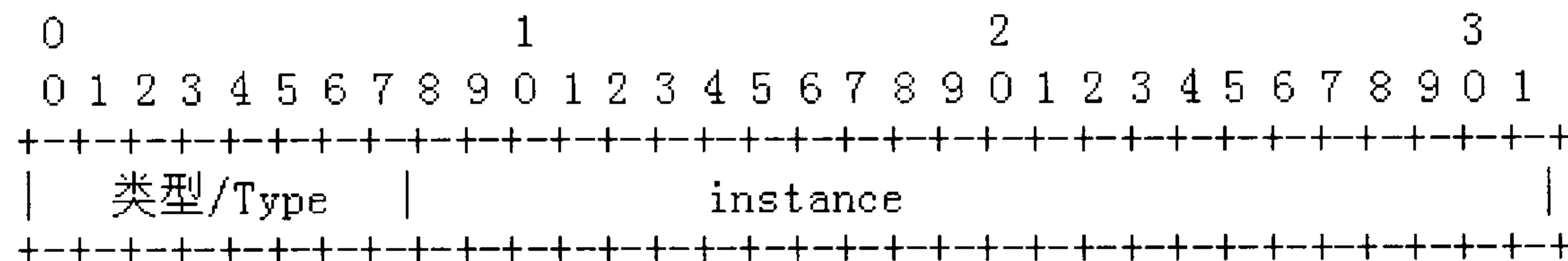
2) 通过 OSPF 学习 P2P 网络类型的网管路由时, 可以学习到下一跳 IP 地址, 即对端设备的 NEIP。设备使用该下一跳 IP 地址发送 ARP 请求, 对端设备回应 ARP 响应报文, 回应接口的 MAC 地址。

3) 网管自通管理报文 DMAC 发现两种方式: 利用 LLDP 进行 DMAC 地址发现; 或者利用 ARP 学习到对端的 DMAC; 但设备应兼容对端采用上述某种方式进行 DMAC 地址发现, 即应支持 LLDP 报文发送和 ARP 响应。

A.4 OSPF LSA 和 TLV 格式

A.4.1 LSA ID

OSPF 通过 Opaque LSA 将本机的网管信息 flood 到区域内的其他设备。Opaque LSA 的 LSA ID 格式如下:



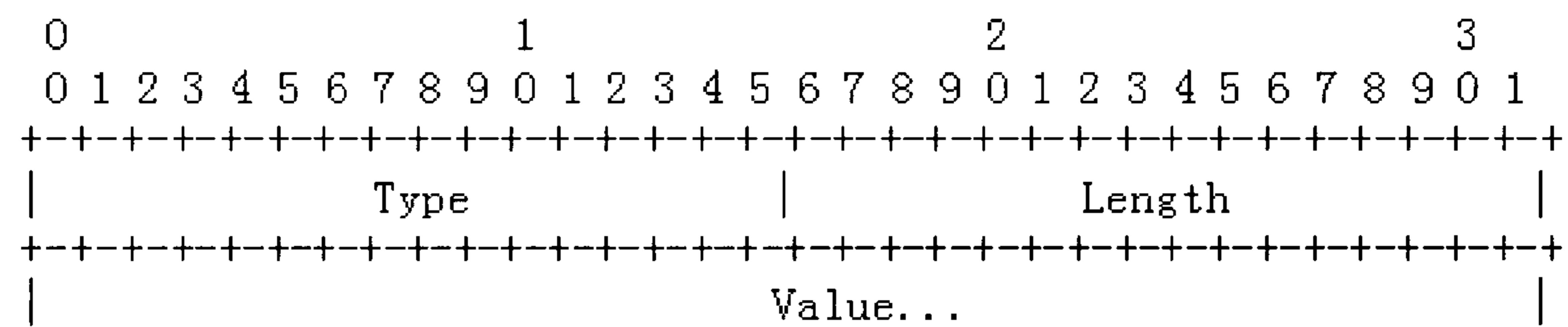
对于网管自通, LSA ID 定义为 202.255.238.0, 其中 202 为 opaque type, 255.238.0 (ffee00) 为 instance 信息;

A.4.2 TLV 格式

Opaque lsa 中通过 TLV 格式携带以下信息: 厂家标示、设备型号、设备桥 MAC、NEID、NEIPV4、

NEIPV6 等 TLV。

通用 TLV 头部如下：



厂家标示： Type: 0x8000; Length: 标示名称长度；

设备型号： Type: 0x8001; Length: 型号名称长度；

设备桥 MAC: Type: 0x8002; Length: 6;

NEID: Type: 0x8003; Length: 4;

NEIP IPV4: Type: 0x8004; Length: 4;

NEIP IPV6: Type: 0x8005; Length: 16.

附录 B
(资料性附录)
SDN 域拓扑收集技术

B.1 LLDP 拓扑收集技术

在支持标准的OpenFlow情况下，可以使用LLDP来进行拓扑收集。在使用LLDP的情况下，由于LLDP报文需要通过OpenFlow传递到控制器，因此在LLDP运行前，需要首先建立控制器与转发节点之间的控制协议链接，转发节点向控制器进行注册。控制通道的建立参见5.2节。

如图B.1所示，本标准推荐的控制器获取网络拓扑的协议流程如下：

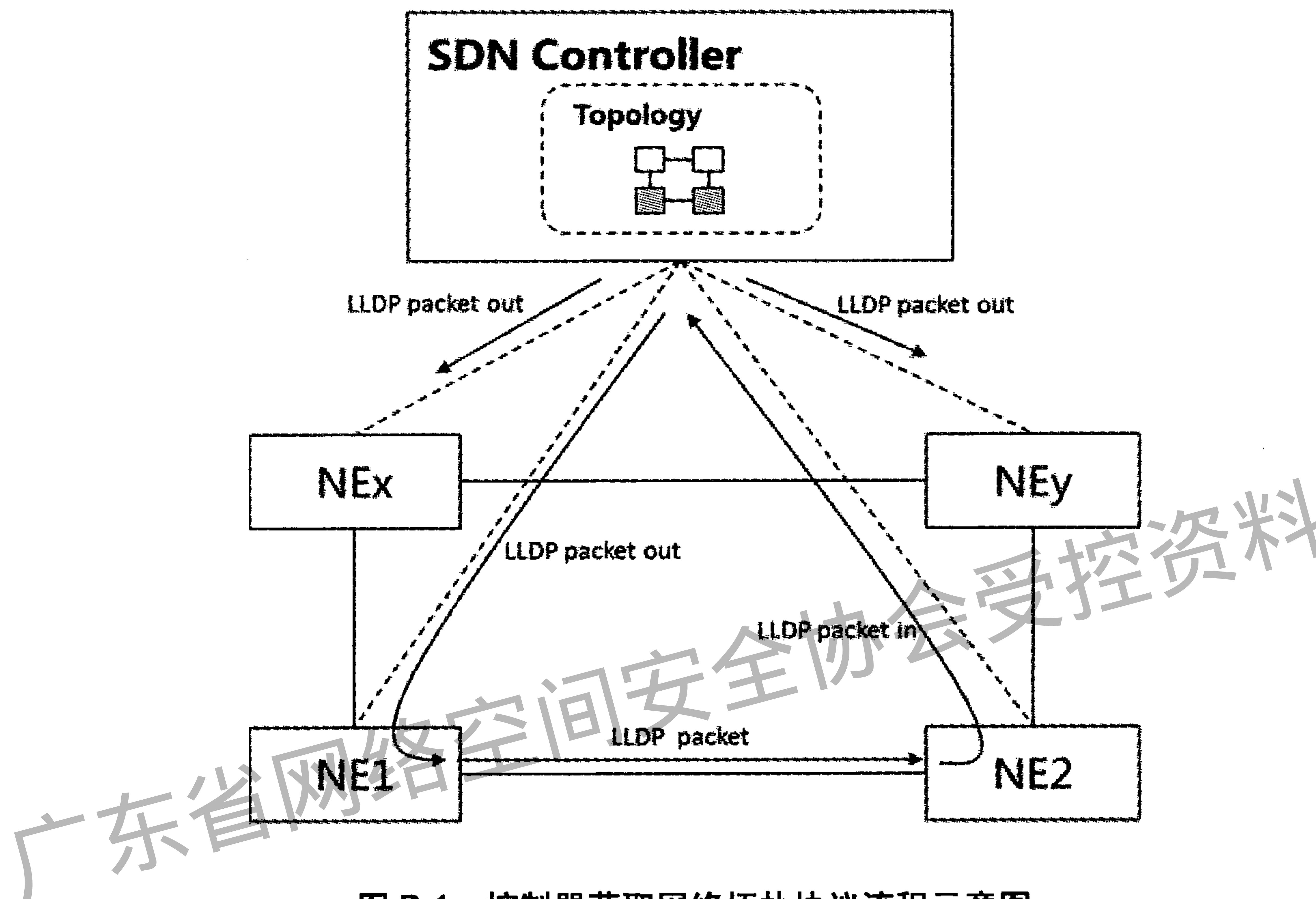


图 B.1 控制器获取网络拓扑协议流程示意图

- 1) 控制器向所有接入设备和汇聚设备发送OFPT_FEATURES_REQUEST消息获取其Datapath ID。
- 2) 控制器向所有接入设备和汇聚设备发送REQUEST消息获取其端口信息。
- 3) 控制器向所有接入设备和汇聚设备下发流条目，要求针对LLDP协议报文（Ethertype为0x88CC）执行上送控制器的动作。
- 4) 控制器通过packet out消息封装LLDP协议报文发送给所有接入设备和汇聚设备，并在packet out消息中要求网元把其中携带的LLDP报文从某个网元端口发送出去。LLDP报文中携带的Chassis ID为控制器获取的Datapath ID中包含的MAC地址，LLDP报文中携带的Port ID为控制器获取的端口信息中包含的端口号。
- 5) 网元接收封装了LLDP报文的packet out消息，解析后将LLDP报文从对应的网元端口发送出去。
- 6) 邻居网元接收到LLDP报文，匹配控制器预先下发的流表条目，将LLDP报文封装成packet in消息上送给控制器。
- 7) 控制器接收到邻居网元上送的封装了LLDP报文的packet in消息：
 - 解析LLDP报文中携带的Chassis ID和Port ID，确定发送该LLDP报文的网元及端口；
 - 解析packet in消息中携带的入端口，确定收到该LLDP报文的网元及端口；
- 8) 控制器通过上述流程完成两两网元之间的链路发现，进而获取整网的网络拓扑；

B.2 ISIS 收集拓扑

现在网络中使用两种IGP协议，OSPF和ISIS。在基于SDN的IP RAN中为了简化网络的规划和配置，设备互联接口要求免IP地址配置，而OSPF基于IP层，ISIS是基于二层，因此ISIS更适合作为基于SDN的IP RAN的拓扑收集协议。ISIS拓扑网关选择如图B.2所示。

a) 拓扑收集方式

ISIS协议本身具有在网络中进行拓扑扩散的功能，因此无需每个转发节点都向控制器上报拓扑，而可以在网络中选取某个节点向控制器上报拓扑（将上报拓扑的节点称为拓扑网关）。推荐ABR或者ASBR节点向控制器上报拓扑。拓扑网关向控制器上报拓扑可以有多种方式：

- 1) 扩展OpenFlow协议，在OpenFlow协议中上报拓扑信息。当前OpenFlow协议并不支持拓扑上报。
- 2) 使用I2RS上报拓扑信息。
- 3) 控制器通过OF-Config或者Netconf主动到拓扑网关获取拓扑信息。在OF-Config或者Netconf定义拓扑的对象，控制器通过这些协议主动到拓扑网关获取拓扑信息。

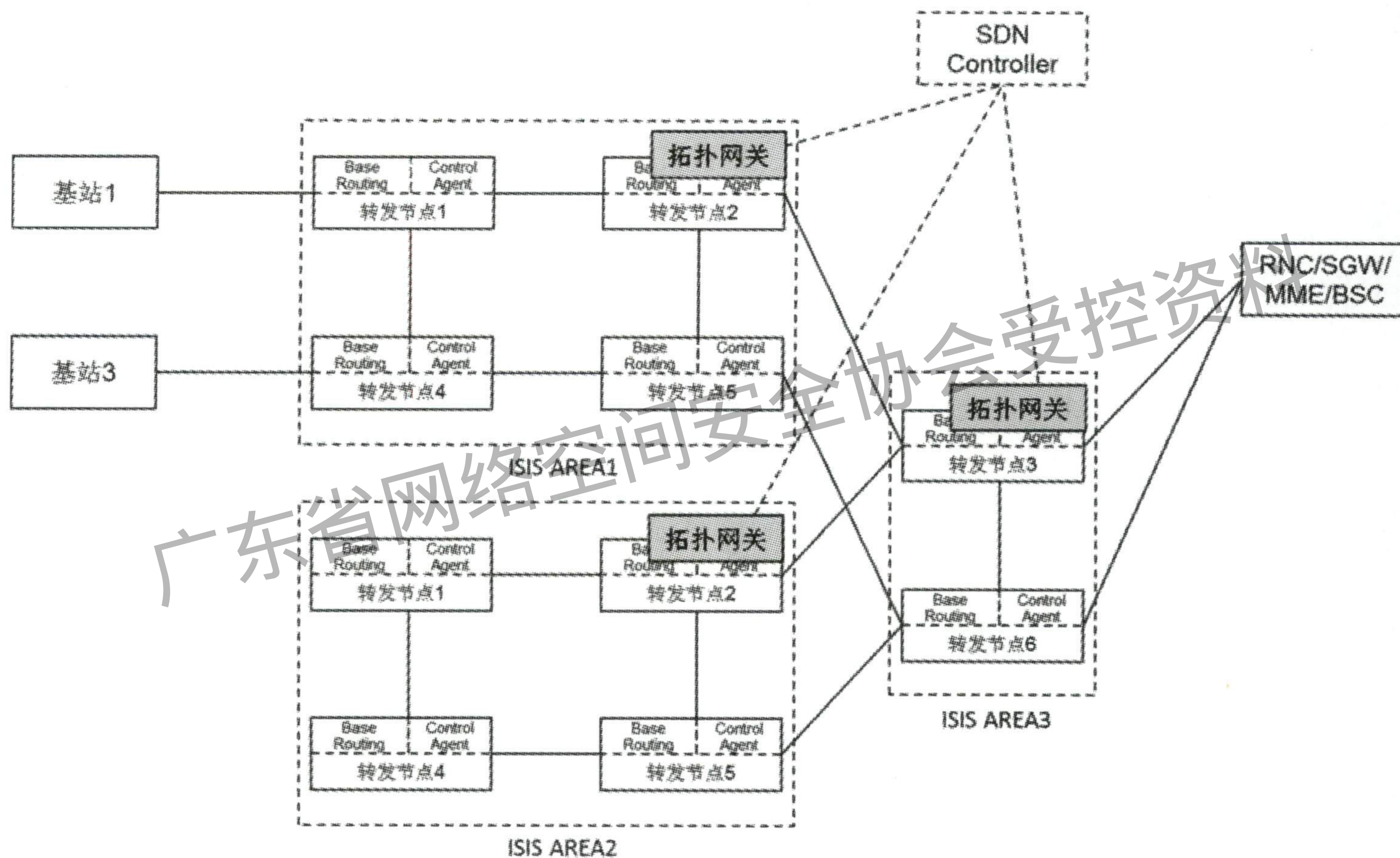


图 B.2 ISIS 拓扑网关选择

b) 内嵌式控制器的拓扑收集：

对于内嵌式控制器，控制器本身是嵌入到现有网络设备中，因此现有网络设备可以与转发节点直接建立ISIS的连接，通过ISIS协议邻居获取到网络的拓扑，而无需通过拓扑网关来上报。

但是在内嵌式控制器这种场景下可以对拓扑收集进行增强，以简化即插即用功能。在内嵌式控制器中的网络中同时存在多个控制器。例如，控制器内嵌到ASG设备中，对于环组网，那么环上的转发节点将会有两个控制器。为了做到即插即用，转发节点需要自动发现网络中有哪些控制器。在拓扑收集阶段，虽然通过ISIS的扩散，每个转发节点都能够发现网络中其他的节点，但是并没有角色信息，也就是转发节点并不清楚网络中哪些是控制器。通过扩展ISIS，可以在拓扑收集阶段将节点的角色信息扩散到转发节点和其他控制器。

1) ISIS协议内容扩展:

增加设备角色TLV，标识本设备是控制器还是转发器。控制器和转发节点均在向外发布节点的Link-State时带上设备角色TLV，接收者可识别网络中哪些是控制器，哪些是转发节点。

增加控制器 ID TLV，标识转发节点被哪些控制器控制，包括主备控制器的ID。该TLV由转发节点在选择了主备控制器后，向外扩散Link-State时带上。控制器通过该TLV可以获知转发节点选择的主备控制器。

2) 兼容性考虑:

增加TLV不影响现有协议交互，属于兼容性扩展。在内嵌式控制器场景中应用。

B.3 手工注入拓扑

除了通过ISIS协议和标准的OpenFlow协议来获取网络拓扑，控制器获取网络拓扑的另一种可选方式是由网管直接向控制器注入网络拓扑，然后由控制器对网管注入的网络拓扑进行验证。如果采用这种方式，本标准推荐采用上述同样的协议流程来完成控制器对网络拓扑的验证。

广东省网络空间安全协会受控资料

中华人民共和国
通信行业标准
基于 SDN 的 IP RAN 网络技术要求

YD/T 3020—2016

*

人民邮电出版社出版发行

北京市丰台区成寿寺路 11 号邮电出版大厦

邮政编码：100164

北京康利胶印厂印刷

版权所有 不得翻印

*

开本：880×1230 1/16

2016 年 6 月第 1 版

印张：2

2016 年 6 月北京第 1 次印刷

字数：53 千字

15115 • 971

定价：20 元

本书如有印装质量问题，请与本社联系 电话：(010)81055492