



中华人民共和国通信行业标准

YD/T 2329.6-2011

分组通信数据网（PTDN）体系架构 第 6 部分：安全与服务质量

The technical architecture for packet telecommunication
data network (PTDN)
part 6: security and quality of service

2011-12-20 发布

2012-02-01 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 术语、定义和缩略语.....1

 2.1 术语和定义.....1

 2.2 缩略语.....1

3 安全.....2

 3.1 安全威胁.....2

 3.2 PTDN安全参考模型.....2

 3.3 接入安全.....4

 3.4 控制平面安全机制.....5

 3.5 管理平面安全机制.....5

 3.6 数据平面安全机制.....6

 3.7 日志和安全报告.....6

 3.8 网络监管和其他.....7

4 服务质量.....7

 4.1 PTDN QoS域.....7

 4.2 PTDN QoS参考模型.....7

 4.3 控制平面QoS机制.....8

 4.4 管理平面QoS机制.....9

 4.5 数据平面QoS机制.....10

前 言

本部分按照GB/T 1.1-2009 规则起草。

YD/T 2329《分组通信数据网（PTDN）体系架构》分为7个部分：

第1部分：总则

第2部分：链路层

第3部分：网络层

第4部分：路由

第5部分：可靠性

第6部分：安全与服务质量

第7部分：网络互通

本部分由中国通信标准化协会提出并归口。

本部分起草单位：工业和信息化部电信研究院、北京中京创原通信技术有限公司、迈普通信技术股份有限公司、华为技术有限公司、中兴通讯股份有限公司、杭州华三通信技术有限公司、福建星网锐捷网络有限公司。

本部分主要起草人：朱 伟、金 伟、蒋林涛。

分组通信数据网（PTDN）体系架构

第6部分：安全与服务质量

1 范围

本部分规定了分组通信数据网（PTDN）的安全与服务质量，包括PTDN的安全参考模型和安全机制、服务质量参考模型和保障机制。

本部分适用于PTDN网络和相关网络设备。

2 术语、定义和缩略语

2.1 术语和定义

下列术语和定义适用于本文件。

2.1.1

控制平面 Control Plane

一类特殊的数据平面，用于传输与控制相关实体操作的信息流以及支持此类控制所需的功能集。

2.1.2

管理平面 Management Plane

一类特殊的数据平面，用于传输与管理相关实体操作的信息流以及支持此类管理所需的功能集。

2.1.3

数据平面 Data Plane

网络中用于传输数据、具有若干相同特征的虚拟网络资源集合。数据平面之间信息隔离。赋予特定标识的数据平面用于提供虚拟专用网络（VPN）业务。

2.1.4

面向连接 Connection-Oriented Packet Switched

一种端到端通信的工作方式，需要有建立通信连接、通信、拆除通信连接3个过程。通信中沿途节点设备通过逻辑信道交换实现数据分组的转发。

2.1.5

不面向连接 Connectionless Packet Switched

一种端到端通信的工作方式，不需要有建立通信连接、通信、拆除通信连接3个过程。通信中沿途节点设备通过目的网络地址实现数据分组的转发。

2.2 缩略语

下列缩略语适用于本文件。

ADT	ADdress Translator	地址翻译器
CR	Core Router	核心路由器
ED	Edge Device	边缘设备
OAM	Operation Administration and Maintenance	运营、管理和维护

P-NNI	Ptdn-Network and Network Interface	PTDN网络与网络接口
P-UNI	Ptdn-User and Network Interface	PTDN用户与网络接口
PTDN	Packet Telecommunication Data Network	分组通信数据网
QoS	Quality of Service	服务质量

3 安全

3.1 安全威胁

从网络本身看，通信网络通常可能面临以下潜在安全威胁。

- 数据欺骗：一种第三方通过插入、篡改、或丢弃特定数据等方式来改变数据发送方或接收方的数据分组，从而对合法通信方造成欺骗的攻击行为；
- 协议攻击：利用网络中一些协议在设计或实现上的漏洞进行危害网络安全的行为；
- 数据嵌入攻击：第三方非法将正常的的数据分组发送给特定用户或网络，造成用户欺骗或网络故障；
- 数据丢弃/重定向攻击：合法数据分组在到达接受者之前被丢弃，或被重新定向到一个不属于接收者者目的端；
- 非授权监听：在未经授权情况下监听目标网络的数据、信息，探知目标网络的拓扑或特定设备信息，用于开展危害网络安全的行为。

目前常见的网络安全事故一般都是由上述一种或几种安全威胁行为造成的。

PTDN涉及OSI 7层模型中的链路层和网络层技术，为应对上述安全威胁，同时满足网络监管等需求，PTDN应在网络层/链路层至少满足以下安全要求：

- 网络和用户相互隔离；
- 不同用户/业务流接入控制；
- 控制平面流量不受外部攻击，并确保其在高强度外部攻击下的安全和稳定；
- 管理平面流量不受外部攻击，并确保其在高强度外部攻击下的安全和稳定；
- 管理平面拒绝非授权用户获得控制和管理功能；
- 数据平面之间相互隔离、相互隔离；
- 控制平面、数据平面、管理平面之间的逻辑隔离；
- 针对 PTDN 数据的合法监听；
- 全网监测；
- 快速故障检测和恢复；
- 溯源；
- 支持紧急通信服务。

本部分不涉及针对 PTDN 网络节点设备本身的安全要求。

3.2 PTDN 安全参考模型

3.2.1 参考模型

本节规定PTDN的安全参考模型。包括PTDN网络安全区、过渡区、非安全区的界定，对涉及网络安全的网络元素的安全要求，安全保障机制等。

根据信任程度的不同，PTDN网络可分成3个区域：

a) 安全区

PTDN 网络边界由直接与 PTDN 以外的用户网络连接和通信的网络元素构成。所有 PTDN 网络边界以内（不包括网络边界）的网络元素（网络节点设备、内部网络管理、运维设备等）处于安全区。

安全区内的网络元素对 PTDN 网络之外是不可见的，不直接与 PTDN 网络之外的用户设备或网络进行通信。位于安全区的网络元素只与位于安全区和位于过渡区的网络元素通信。安全区内的数据传输不需加密即能保证安全。

PTDN 用户与 PTDN 网络的接口称为 P-NNI。P-NNI 位于安全区，即 PTDN 网络之间通过 P-NNI 互连是可信的，不存在安全威胁。

b) 过渡区

过渡区由位于 PTDN 网络边界的网络元素构成，是 PTDN 的安全过渡区域。过渡区内的网络元素直接与 PTDN 网络之外的用户（其他网络）进行通信，亦与安全区内的网络元素进行通信。PTDN 用户与 PTDN 网络的接口称为 P-UNI，位于过渡区。

过渡区的安全功能是在安全区和非安全区之间构建安全屏障，防止安全区内的网络元素受到攻击，拒绝存在安全威胁的用户和数据流量接入到安全区。

c) 非安全区

涵盖 PTDN 网络以外的网络区域，主要包括 PTDN 网络之外的各类 PTDN 用户网络(非 PTDN)、PTDN 注册认证实体。

PTDN 安全参考模型如图 1 所示，包括过渡区、安全区和非安全区。其中过渡区和安全区共同构成 PTDN 域；非安全区构成用户域。

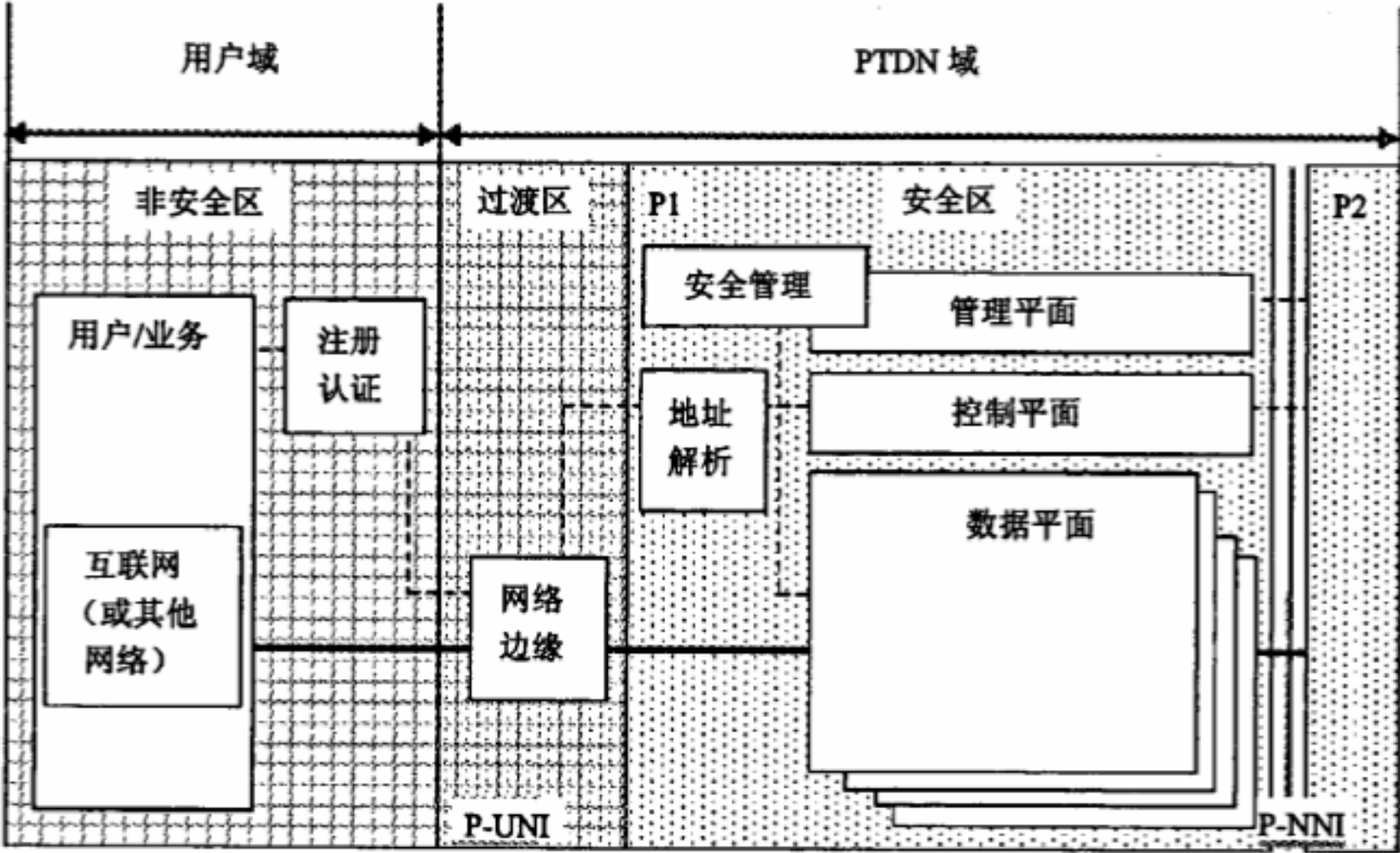


图1 PTDN 安全参考模型

非安全区主要由用户/业务网络和注册认证实体构成，后者包括两大安全功能：注册功能和认证功能。一般情况下，用户/业务接入 PTDN 网络前需要进行注册登记，确定用户/业务级别、所需的网络资源数量、服务质量、安全要求等诸多内容。认证功能主要是根据注册信息对用户/业务进行安全认证，确定其合法性和服务类别，并通知网络边缘实体，后者根据认证结果进行接入控制。

过渡区主要由网络边缘实体构成。功能包括数据接入、数据接入控制、安全隔离和协助地址解析等。非安全区的数据通过过渡区的网络边缘实体进入 PTDN，边缘实体需根据用户/业务合法性进行数据验

证，阻止和隔离非法接入请求，协助为合法用户/业务数据提供地址解析服务，负责将合法数据安全转发到安全区，防御针对地址解析功能的攻击行为；此外，网络边缘实体应阻止安全区内控制、管理报文流向非安全区。

安全区是 PTDN 承载数据的主要区域，位于 PTDN 网络边缘实体之间，主要功能是数据传输。安全区从功能上可划分成控制平面、管理平面和数据平面。各平面都需满足一定的安全要求，其安全功能由安全管理实体进行维护；地址解析实体主要负责接收来自过渡区边缘实体的地址查询请求并返回查询结果。

非安全区是 PTDN 网络安全威胁的来源。

P1 和 P2 是两个不同的 PTDN 网络运营商，通过 P-NNI 相连。P1 和 P2 同属于安全区，P-NNI 由 PTDN 运营商协商机制确定，绝对保证安全，普通用户无需关心 P-NNI 的接口问题。

3.2.2 安全措施

PTDN 安全措施的基本特征是隔离。用户和网络、安全区与非安全区之间完全隔离；控制平面、管理平面、数据平面 3 个平面之间严格隔离；数据平面之间相互隔离。

非安全区进行用户/业务注册认证，过渡区实施接入控制。这两个区域共同负责 PTDN 用户/业务的接入安全。

安全区负责 P-UNI 之间的数据安全。确保控制平面、管理平面、数据平面 3 个平面的安全。

PTDN 还应提供支持日志和安全报告、故障恢复、网络监管以及其他与安全有关的需求的安全措施。

3.3 接入安全

3.3.1 注册认证

注册认证是 PTDN 用户/业务注册认证中心（以下简称注册认证中心）、PTDN 边缘实体、用户/业务三方之间的一个协商过程，目的是为合法用户/业务提供授权，允许其通过边缘实体接入到 PTDN 安全区，拒绝非法用户/业务接入 PTDN 安全区。

一般情况下，PTDN 用户/业务直接与 PTDN 边缘实体连接，是 PTDN 网络安全威胁的主要来源。PTDN 在非安全区内完成用户/业务认证，这个过程是加密的过程，通过一定的密钥授权机制确保安全。

用户/业务在接入到 PTDN 之前，皆需向 PTDN 运营商进行用户/业务注册；以后注册认证中心即根据注册信息验证每次发起接入 PTDN 的用户/业务请求是否合法。对于合法用户/业务，注册认证中心将分别向 PTDN 网络边缘实体和用户/业务端发送一对验证密钥授权书中的一个，前者根据自己的授权书和后者提供的授权书来确定用户/业务是否合法和为合法用户/业务分配数据平面标识。对于非法用户/业务，网络边缘实体应拒绝其接入。

3.3.2 接入控制

接入控制指 PTDN 网络边缘实体依据注册认证中心提供的信息决定是否将用户/业务数据转发到安全区内特定数据平面的过程；此外，接入控制还负责安全区与非安全区的隔离。接入控制允许合法用户/业务进入安全区，拒绝非法用户/业务的接入；实施恶意地址解析请求控制策略；实施流量安全控制策略；防止安全区内控制、管理报文进入非安全区。

所有 PTDN 用户/业务数据只能通过边缘实体进入 PTDN 安全域。边缘实体依据注册认证中心提供的密钥验证用户/业务信息的合法性，并将合法用户/业务进行特定数据平面标记和分类，接入到不同的数据平面，后者为该用户/业务提供特定的网络资源和连接服务。非法用户/业务将被隔离在过渡区之外；对于 B 类用户/业务，边缘实体直接将其标记到 PTDN 普通因特网通道。非法用户/业务将被直接丢弃。

边缘实体在将用户数据转发到安全区之前还需要将合法用户的网络地址提交到ADT进行解析。为防止恶意地址解析，边缘实体应支持ADT的恶意地址解析请求控制功能。

边缘实体对超出资源限制的流量实施流量安全控制策略。当某数据平面的用户/业务流量超出该数据平面资源限制时，边缘实体将根据该数据平面的控制策略对流量进行流量安全控制。

边缘实体应阻止一切安全区内的非数据报文（如PTDN控制、管理报文等）进入非安全区。

3.4 控制平面安全机制

3.4.1 控制信令隔离

PTDN通过控制信令与其他类型报文的隔离来确保控制报文的安全。

PTDN提供控制平面用于控制信令转发。控制平面处于安全区，与PTDN其他平面完全隔离，与用户完全隔离。所有PTDN控制信令都由控制平面进行承载，控制平面具有最高级别优先保障权限。

PTDN控制信令只能存在于安全区和过渡区。边缘设备应阻止一切控制PTDN控制信令报文进入非安全区。

3.4.2 路由安全

PTDN路由处于安全区，与非安全区完全隔离，一般不受到来自PTDN网络之外的攻击。PTDN路由安全主要包括路由隔离、路由协议自身健壮性、备份路径3个方面。

PTDN路由报文仅存在于安全区和过渡区，过渡区内的边缘实体不应收到任何去向非安全域的路由报文，如收到应立刻丢弃并写入日志，并可在不影响安全区内安全管理中心正常功能的前提下报告给后者。

路由协议自身健壮性在其他PTDN标准中另行规定。

备份路径在其他PTDN标准中另行规定。PTDN路由至少支持双路由备份和快速收敛。

3.4.3 地址解析安全

地址解析发生于PTDN边缘实体和地址解析实体之间，非安全区的用户端向过渡区PTDN边缘实体发送数据报文，边缘实体需向地址解析实体发起地址解析请求，进行注册，地址解析实体将分配一个对应的PTDN地址标识用于该用户/业务的数据转发地址，这对地址解析实体将产生潜在安全威胁。

为避免用户利用这一过程针对地址解析实体发起恶意攻击，相应的地址解析协议应针对地址解析过程规定安全控制机制，确保在拒绝服务等攻击行为下的健壮性和可用性。

3.5 管理平面安全机制

3.5.1 管理报文隔离

PTDN通过管理报文与其他报文的隔离来确保管理报文的安全。

PTDN提供管理平面用于管理报文的转发。管理平面处于安全区，与PTDN其他平面完全隔离，与用户完全隔离。所有PTDN管理报文都由管理平面进行承载，管理平面具有最高级别优先保障权限。

PTDN管理报文只能存在于安全区和过渡区。边缘设备应阻止PTDN管理报文进入非安全区。

3.5.2 安全监控

PTDN安全管理实体通过管理平面监控整个安全区和过渡区的数据流量情况，可根据需要采集和监控流量、用户信息、网络拓扑、路由信息、路径信息等信息：

- 可获取整个安全区域内的实时网络拓扑；
- 可针对特定一个或多个数据平面监控实时流量及其相关数据信息；
- 可针对整个数据平面监控实时流量及其相关数据；

- 可实时监控网络异常和安全事件；
- 在流量超过限制、特定数据平面发生拥塞之前发起拥塞告警；
- 可提供虚拟网管接口，为特定数据平面需用户提供可配置、可管理的虚拟网络管理服务；
- 其他与安全有管的监控数据采集和显示。

PTDN安全管理实体的监控内容是确定网络安全状态的主要依据。

3.5.3 安全管理

PTDN安全管理实体为不同安全级别用户提供具有不同权限的虚拟网管安全管理功能。安全级别低的用户不具有超过其可用范围的网络安全管理功能。

安全管理实体对管理平面实施最严格的安全准入制度，只有最高安全级别的主体（网络运营者）具备管理平面直接进入和维护的权限。

3.6 数据平面安全机制

3.6.1 数据隔离

PTDN采用多数据平面承载不同类型的数据报文，不同类型数据报文之间相互隔离，互不影响。

非安全区合法数据通过过渡区接入到安全区，根据其不同数据平面标识被转发到特定的数据平面中，属于同一类型的数据有自己的专用数据平面。数据平面之间严格隔离，即数据平面a的数据无法进入数据平面b，数据平面a只转发具有本数据平面标识的数据，如收到具有其他数据平面标识的数据（这种情况不应出现）将被直接丢弃；当数据平面a发生拥塞时，亦不能挤占其他数据平面的资源。在极端情况下，即使数据平面a受到攻击，安全威胁也将被限制在数据平面a内，不能影响其他数据平面用户/业务的安全。

3.6.2 资源独立

PTDN数据平面资源包括与数据转发密切相关的CPU、内存、端口、带宽、转发路径等。这些资源的安全是确保数据平面功能的基础，PTDN应保持数据平面资源的独立性。

PTDN节点应依照各个数据平面预先确定的需求，在数据转发过程中为各个数据平面合理配置CPU、内存、端口等设备资源，确保各个数据平面所需的带宽、转发路径等网络资源，不同数据平面之间的资源相互独立，一个数据平面的资源不能被另一个数据平面挤占。

PTDN只能由网络管理者在安全区内通过控制平面和管理平面操控数据平面的资源。数据平面资源对非安全区不可见。

3.6.3 拓扑稳定

数据平面拓扑应当是稳定的，即非经网络管理者授权，任何第三方都不能改变网络拓扑和通过改变网路拓扑窃取数据。

数据平面的拓扑应对非安全区不可见。PTDN用户无需知晓数据平面拓扑。自安全区向非安全区转发的数据报文不应携带任何安全区内数据平面拓扑信息，此类报文的PTDN地址等与网络拓扑有关的信息应在过渡区以内移除。

3.7 日志和安全报告

3.7.1 日志

PTDN网络管理员在安全区内的所有操作都应由安全管理实体记录到日志。

PTDN网络用户的注册、注销、信息变更等信息都应由安全管理实体记录到日志。

其他涉及网络操作和用户/业务的信息都应由安全管理实体记录到日志。

PTDN日志功能不应影响正常网络功能。当日志功能影响正常网络功能时，后者具有比前者高的优先级。

3.7.2 安全报告

PTDN网络安全威胁事件应以安全报告的形式主动报告给安全管理实体。

3.8 网络监管和其他

3.8.1 网络溯源

PTDN应支持网络溯源。通过日志、安全报告和用户注册记录等信息，PTDN应能够溯源到安全区内、过渡区内引发网络事件的实体，应能够溯源到引发网络事件的非安全区注册用户/业务。

3.8.2 执法监听

PTDN应支持执法监听。所有安全区内的数据都应是非私有加密的，以支持执法监听，满足国家法律规定的**安全需求。

3.8.3 紧急通信保障

PTDN应支持紧急通信保障。当数据平面满载，普通用户/业务无法接入时，仍能确保紧急通信的网络资源需求，并确保通信质量。

4 服务质量

4.1 PTDN QoS 域

本部分涉及的QoS区域位于端到端PTDN QoS域，即P-UNI之间的区域（如图2所示），该区域由一个或多个PTDN网络构成。每个PTDN网络本身构成一个PTDN QoS域。PTDN网络实体可分为网络边缘实体和节点实体（R节点）两类，其中网络边缘实体对应于P-UNI，R节点（如CR）对应于P-NNI。

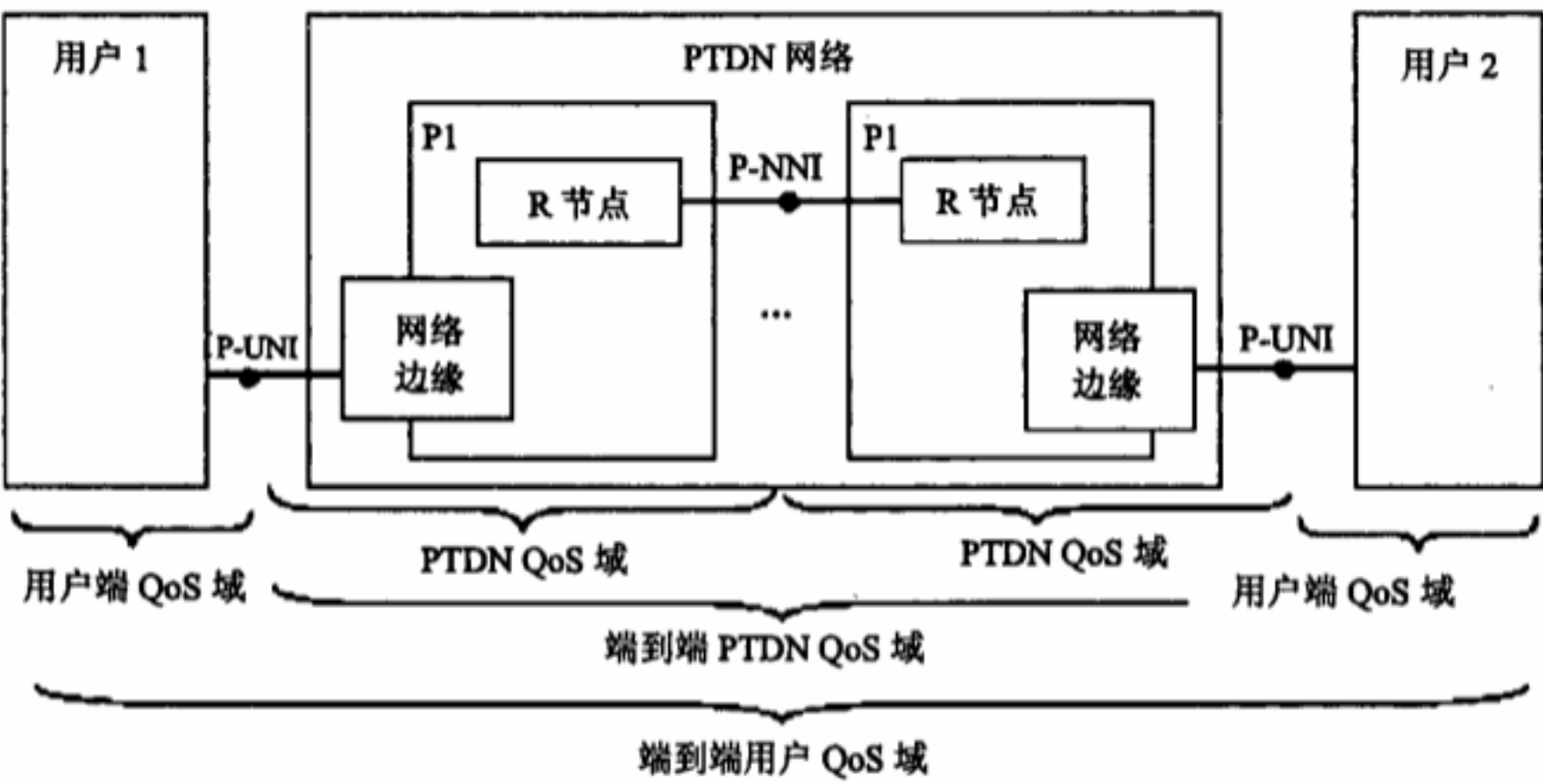


图2 PTDN QoS 范围

端到端PTDN QoS域包括一个或多个PTDN QoS域、P-UNI，可能还包含P-NNI（当包含一个以上PTDN QoS域时）。

P1和P2是两个不同的PTDN网络运营商，通过PTDN网络-网络接口（P-NNI）相连，它们之间可能还有更多的PTDN网络运营商。

PTDN应具备为用户提供端到端PTDN QoS域内QoS的能力。

4.2 PTDN QoS 参考模型

本部分规定PTDN QoS参考模型。

PTDN QoS参考模型（如图3所示）规定PTDN控制平面、管理平面、数据平面的QoS功能。

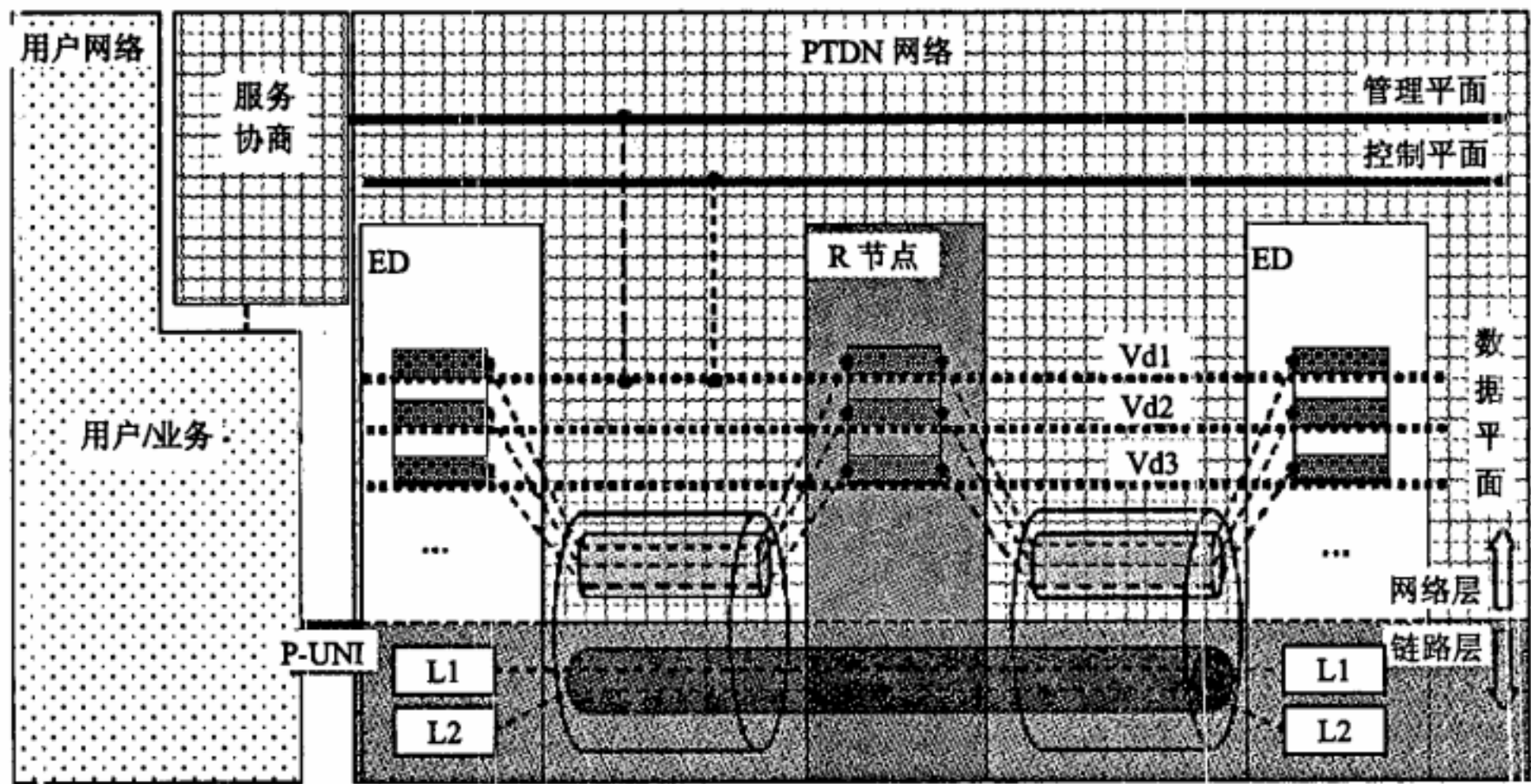


图3 PTDN QoS 参考模型

PTDN控制平面的主要功能是处理用户数据流的发送路径问题。在面向连接的工作方式下，PTDN控制平面完成端到端连接的建立和连接状态的维护，包括端到端（PTDN网络边缘）虚电路建立（见图3的L1、L2）、拆除和状态报告等，在这种工作方式下，QoS是可以保证的。在不面向连接的工作方式下，PTDN控制面负责差错报告、数据平面建立、与路由相关的部分功能等；PTDN控制平面QoS机制围绕上述功能展开，从控制平面实施PTDN网络QoS保障机制，包括接入控制、数据平面建立、资源控制和QoS路径。

PTDN管理平面的功能包括OAM的一些功能。PTDN管理平面QoS机制围绕管理平面功能展开，从管理平面实施PTDN网络QoS保障机制，包括服务协商、网络监测和记录、管理策略。

PTDN数据平面直接处理与用户数据及其传输相关的问题。PTDN数据平面包括两类：

——面向连接的虚电路连接（见图3的L1、L2），由链路层数据平面完成数据转发，由网络层控制平面完成端到端的资源预留，因而具备良好的QoS保障能力；

——不面向连接的连接（见图3的Vd1、Vd2、Vd3），由网络层数据平面实施数据转发，PTDN数据平面QoS机制主要围绕网络层数据平面功能展开，从网络层数据平面实施PTDN网络QoS保障机制，包括缓存管理、拥塞避免、报文标记、队列计划、流量分类、流策略和整形。

4.3 控制平面 QoS 机制

4.3.1 接入控制

接入控制的功能是控制进入PTDN网络实体的流量，包括控制进入网络边缘的流量、控制进入R节点的汇聚流量。

接入控制基于用户在PTDN运营商的注册信息和PTDN资源利用状况；前者提出流的QoS需求，后者确保一般的新增流量不会使网络过载而影响正在转发的流量的QoS。接入控制方法就包括两类：基于QoS参数和基于测量。

基于QoS参数的方法下，数据流报头自身携带一系列QoS要求信息（用户标识、服务等级、业务流类型、业务分类等）成为PTDN进行呼叫控制的首要依据。PTDN采用这种方法确保实时性业务和紧急通信业务等的QoS需求。

基于测量的方法下，PTDN已有流量的资源利用状态信息将成为进行呼叫控制的首要依据。这种方法不保证特定分组的分组丢失率、时延等QoS指标，用于提供相对QoS保障，PTDN可在一些承载普通业务的数据平面实施基于测量的接入控制。

4.3.2 资源控制

4.3.2.1 面向连接工作方式下的资源控制

在PTDN面向连接工作方式下，资源控制的功能是端到端连接的建立和连接状态的维护。包括端到端（PTDN网络边缘）虚电路建立、维持、拆除和状态报告等。

4.3.2.2 不面向连接工作方式下的资源控制

在PTDN不面向连接工作方式下，资源控制的功能是通过PTDN控制信令发起自网络边缘到网络边缘的数据平面配置过程。包括数据平面一系列资源的添加、删除、修改。这些资源中许多与数据平面的QoS密切相关。PTDN支持对数据平面带宽、端口、阈值（拥塞门限和拥塞解除门限）等的实时配置。

PTDN通过数据平面建立和修改功能、阈值配置功能实现对特定数据平面QoS能力的控制。

4.3.3 路由的 QoS

针对特定数据平面的PTDN路由应满足该数据平面用户流的QoS需求。对于PTDN来说，任何一对网络边缘实体之间一般有相对独立的主、备路径，路由相对确定，应确保数据流在主、备路由之间的合理切换。

4.4 管理平面 QoS 机制

4.4.1 服务协商

服务协商是PTDN运营商和网络用户就前者为后者提供的服务的可用性、有效性、性能、价格等进行协商的过程。从网络本身的角度看，服务协商的结果最终映射为进入PTDN网络的用户数据流上一系列可表征QoS需求和要求的参数。这些参数至少应包含：

- 业务流类型。用于在PTDN数据平面区分不同的业务流，对不同的业务流采取不同的汇聚方法；
- 数据平面标识。用于标识不同的数据平面，不同数据平面可提供不同QoS。

用户在进入PTDN之前进行服务协商，PTDN根据协商结果参数（上述参数和其他参数）实施不同QoS策略。

4.4.2 网络监测和记录

通过网络监测，管理平面实时获取PTDN某个点的流量、资源利用情况等信息，并依据这些信息做出必要的决策（告警、报文丢弃、流量整形等），以确保特定业务的QoS。

PTDN应支持端到端PTDN QoS域内任何节点端口和路径带宽利用率、资源状况等信息的实时监测，提供全网拓扑监测和管理，提供节点及其工作状态、资源利用情况监测的功能。

管理平面提供记录监测信息的功能，用于网络分析。

4.4.3 管理策略

管理策略是一系列与管理、维护PTDN网络资源的规则的集合。

管理策略反映了服务协商的结果，可由控制平面或数据平面具体实施。它分为节点管理策略和数据平面管理策略。

PTDN节点管理策略包括通过设置阈值来实施不同网络资源利用率下的QoS策略。一般情况下，PTDN的两类阈值将数据平面资源利用区间分成3个区域，可在不同区域实施不同的QoS策略。

PTDN数据平面管理策略包括虚拟网络管理机制和区分管理机制。虚拟管理机制是指PTDN为不同数据平面提供虚拟管理平台服务，每个虚拟管理平台仅针对本数据平面进行管理，与其他数据平面相互隔离。区分管理机制指不同数据平面的虚拟管理平台可以有不同权限，管理平面可以根据需要对这些权限进行设置。

PTDN应支持数据平面管理策略，并在必要时提供针对特定节点管理策略的支持。

4.4.4 资源管理

资源管理是通过PTDN管理平面对数据平面进行资源配置，包括数据平面一系列资源的添加、删除、修改。这些资源许多与数据平面的QoS密切相关。

PTDN支持通过管理平面对数据平面带宽、端口、阈值（拥塞门限和拥塞解除门限）等的实时配置。

4.5 数据平面 QoS 机制

4.5.1 缓存管理和队列管理

缓存管理指PTDN节点依据一定的规则对到达的不同数据报文进行缓存、转发或丢弃处理。缓存管理的目的是将缓存队列长度限制在一定范围，并能对不同报文实施不同的队列管理策略，防止某一类报文对缓存空间的独占，防范不可预知的队列溢出或报文丢弃，确保节点有效转发。

PTDN应支持基于用户数据报文QoS要求的缓存管理。

队列管理指PTDN节点依据一定的规则决定数据报文在队列中的转发方式。根据PTDN数据报文QoS要求的不同，PTDN中间节点应支持对不同数据平面的数据报文实施队列管理。同一数据平面内部的流也可根据需要依据排队计划采取差异性的转发方式。具体排队计划才可根据QoS要求采用一种或几种队列管理。

PTDN应支持基于用户数据报文QoS要求的队列管理。

4.5.2 拥塞避免

当数据流量超过网络资源（链路带宽、节点缓存等）的处理能力时，就会发生拥塞，此时节点可能对一些报文进行丢弃，造成一些报文的重传，结果将引起更加严重的拥塞。PTDN应采用拥塞避免机制，确保数据流量被限制在其数据平面资源承载能力之内，避免拥塞的发生，保证数据流的QoS。

4.5.3 报文标记

PTDN应支持对数据报文基于服务类别的报文标记，即在网络边缘对数据报文报头的业务流类型字段进行基于服务类别的标记。

4.5.4 流量分类

流量分类指用户数据在进入PTDN网络边缘后，后者根据用户和PTDN的协商对不同数据报文分配不同的标识，在数据报文报头中进行数据平面分类，将数据流映射到不同的数据平面的过程。

PTDN应支持流量分类。

4.5.5 数据平面隔离

PTDN不同数据平面之间应相互隔离，一个数据平面的带宽资源不应被其他数据平面的数据报文挤占。

4.5.6 流量整形

PTDN应支持针对特定数据平面的流量整形，能够控制进入特定数据平面的数据报文的速率。

中 华 人 民 共 和 国
通 信 行 业 标 准
分组通信数据网（PTDN）体系架构
第 6 部分：安全与服务质量
YD/T 2329.6-2011

*

人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码：100061

*

版权所有 不得翻印

*

本书如有印装质量问题，请与本社联系 电话：(010)67114922