中华人民共和国行业标准

铁路数据通信网设计规范

Specification of engineering design for railway data communication network

TB 10087—2010

J 977—2010

主编单位：北京全路通信信号研究设计院

批准部门：中华人民共和国铁道部

施行日期：2010年1月4日

中 国 铁 道 出 版 社

2010年·北 京

中华人民共和国行业标准

铁路数据通信网设计规范

TB 10087—2010

J 977—2010

*

中国铁道出版社出版发行

（100054，北京市宣武区右安门西街 8 号）

出版社网址：http://www.tdpress.com

中国铁道出版社印刷厂印

开本：850 mm×1 168 mm 1/32 印张：1.375 字数：36 千字

2010 年 2 月第 1 版 2010 年 2 月第 1 次印刷

统一书号：15113·3200 定价：6.00 元

关于印发铁路数据通信网设计规范的通知

铁建设〔2010〕3号

现印发《铁路数据通信网设计规范》(TB 10087—2010)，自印发之日起施行。

本标准由铁道部建设管理司负责解释，由铁路工程技术标准所、中国铁道出版社组织出版发行。

中华人民共和国铁道部

二〇一〇年一月四日

前　言

本规范是根据铁道部《关于编制2006年铁路工程建设标准计划的通知》（铁建设函〔2005〕1026号）的要求进行编制的。

本规范在编制过程中，考虑了新形势下铁路数据通信网发展的需要，调查了铁路信息系统业务及通信系统数据业务的需求，借鉴了国、内外相关标准的规定，在广泛征求意见的基础上，经审查定稿。

本规范共分12章，主要内容包括：总则、术语及缩略语、基本规定、网络结构、路由协议及路由策略、自治域号码分配及IP地址分配、域名系统、网络管理、网络安全、服务质量、设备配置原则、设备安装及运行环境要求。

工程技术人员必须按照“以人为本、服务运输、强本减末、系统优化、着眼发展”的铁路建设理念，结合工程具体情况，因地制宜，充分发挥主观能动性，积极采用安全、可靠、先进、成熟、经济、适用的新技术，不能生搬硬套标准。勘察设计单位执行（或采用）单项或局部标准，并不免除设计单位及设计人员对整体工程和系统功能质量问题应承担的法律责任。

本规范系首次编制。在执行过程中，希望各单位结合工程实践，认真总结经验，积累资料，如发现需要修改和补充之处，请及时将意见和有关资料寄交北京全路通信信号研究设计院（北京市丰台区华源一里18号，邮政编码100073），并抄送铁道部经济规划研究院（北京市海淀区北蜂窝路乙29号，邮政编码100038），供今后全面修订时参考。

本规范由铁道部建设管理司负责解释。

本规范主编单位：北京全路通信信号研究设计院。

本规范参编单位：铁道部信息技术中心。

本规范主要起草人：岳铭凯、赵军武、涂慧敏、尹福康、庄文林、吴丽、范宁、洪波、田绵石。

目　　次

1 总　　则

1.0.1 为统一铁路数据通信网工程设计标准，适应铁路数据通信网建设需要，制定本规范。

1.0.2 本规范适用于新建、改建的铁路综合 IP 数据通信网广域网设计和局域网业务接入方式设计。

1.0.3 铁路数据通信网为铁路信息系统业务及 GSM－R 的 GPRS、铁路图像等通信系统数据业务提供承载平台。

1.0.4 铁路数据通信网工程设计应符合国家有关信息安全的规定。

1.0.5 铁路数据通信网不得直接与公众互联网互联。

1.0.6 铁路数据通信网工程设计应符合可靠性、可扩充性、可管理性等要求，并做到技术先进，经济合理。

1.0.7 铁路数据通信网工程设计应遵循统一规划、统一标准、合理布局、资源共享的原则，应充分利用既有资源。

1.0.8 铁路数据通信网工程设计应与业务需求和发展规划相适应，以近期业务需求为主，兼顾远期业务发展。机房等不易改、扩建的基础设施宜按远期设计，系统容量和电源等宜按近期设计，系统设备等可按交付运营后五年设计。

1.0.9 铁路数据通信网工程设计除应符合本规范外，尚应符合《铁路运输通信设计规范》TB 10006 和国家现行有关标准的规定。

2 术语及缩略语

2.1 术　　语

2.1.1 大区节点　main region node

将全国地域划分为不同的大区，在各大区中选定一个节点，此节点即为大区节点。大区节点在地理位置上为铁道部及某些铁路局所在地，在网络中的位置为本大区内业务汇聚点及传输电路汇聚点。

2.1.2 核心节点　core node

位于铁路局所在地，完成本铁路局业务汇聚和处理，并向骨干网络转发数据。

2.1.3 汇聚节点　distribution node

位于本铁路局一定地域范围的业务汇聚地点，是该地域范围内业务量的相对集中点及传输电路汇聚点。

2.1.4 接入节点　access node

位于铁道部、铁路局、客专调度所、客专综合维修中心、客专动车检测基地以及车站、段（所），为铁路数据通信网承载的业务提供接入。

2.1.5 骨干网络　backbone network

由大区节点组成的网络。

2.1.6 区域网络　region network

指覆盖铁路局管辖范围或铁道部的网络。铁路局区域网络由核心节点、汇聚节点、接入节点组成；铁道部区域网络由铁道部接入节点组成。

2.2 缩略语

英文缩写	英文解释	中文解释
AS	Autonomous System	自治系统
BGP	Border Gateway Protocol	边界网关协议
CPOS	Channeled Packet Over SDH	基于 SDH 帧结构的可信道化数据包
DiffServ	Differentiated Services	差分服务
EBGP	External Border Gateway Protocol	外部边界网关协议
FRR	Fast Re-Route	快速重路由
GE	Gigabit Ethernet	千兆以太网
IBGP	Internal Border Gateway Protocol	内部边界网关协议
IGP	Internal Gateway Protocol	内部网关协议
IntServ	Integrated Services	集成服务
IP	Internet Protocol	互联网协议
IS-IS	Intermediate System-to-Intermediate System	中间系统到中间系统协议
MPLS	Multiprotocol Label Switching	多协议标记交换
MP-BGP	Multi-Protocol BGP	多协议 BGP
MSTP	Multi-Service Transport Platform	多业务传输平台
OSPF	Open Shortest Path First	开放最短路径优先路由协议
QoS	Quality of Service	服务质量
RR	Route Reflector	路由反射器
SNMP	Simple Network Management Protocol	简单网络管理协议
TCP	Transmission Control Protocol	传输控制协议
TE	Traffic Engineering	流量工程
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网
VRR	VPN Route Reflector	VPN 路由反射器

3 基本规定

3.0.1 铁路数据通信网工程设计应包括网络结构、路由协议及路由策略、地址分配、域名系统、网络管理、网络安全、服务质量、设备配置、设备安装及运行环境要求等内容。

3.0.2 铁路数据通信网的系统处理能力、业务接入能力等方面应适度留有余量。

3.0.3 铁路数据通信网工程设计应符合所承载的业务需求，网络性能指标应符合通信行业相关标准的要求。

3.0.4 铁路数据通信网设计应基于 TCP/IP 技术。

3.0.5 铁路数据通信网设计应支持 MPLS VPN、MPLS QoS、组播等技术。

3.0.6 铁路数据通信网广域网的传输网应以光传输网为主，宜采用 IP over SDH 和基于 SDH 帧结构的 IP over WDM 技术。

3.0.7 铁路数据通信网骨干网络路由器及铁道部区域网络路由器应以铁路一级时间同步节点时间服务器的时间作为基准，各铁路局区域网络路由器以铁路二级时间同步节点时间服务器的时间为基准。

4 网络结构

4.1 网络层次

4.1.1 铁路数据通信网广域网包括骨干网络、区域网络，网络层次结构如图 4.1.1 所示。

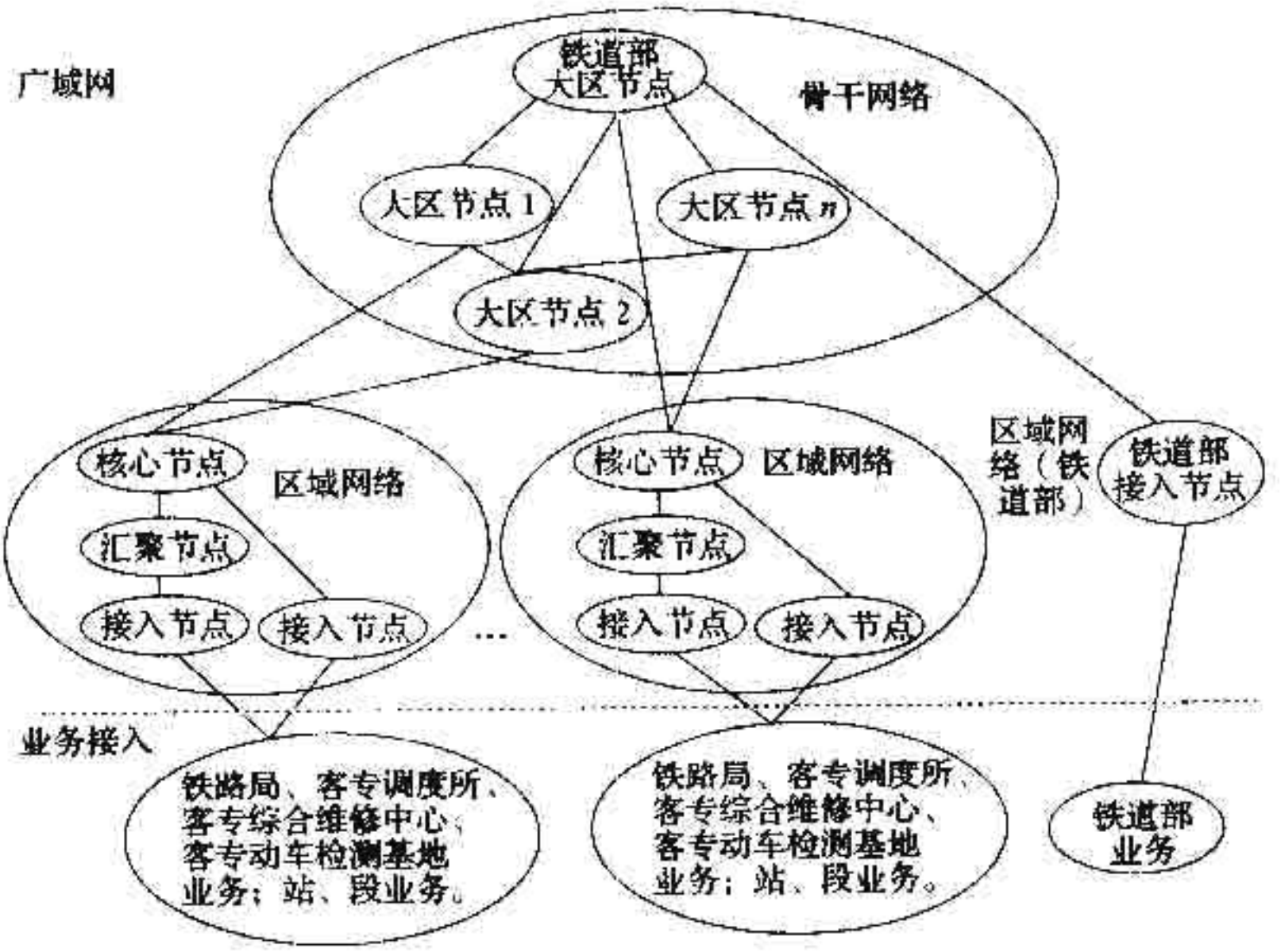

图 4.1.1 铁路数据通信网的网络层次结构图

4.2 骨干网络

4.2.1 铁路数据通信网骨干网络结构如图 4.2.1 所示。

4.2.2 骨干网络大区节点的设计应符合下列规定：

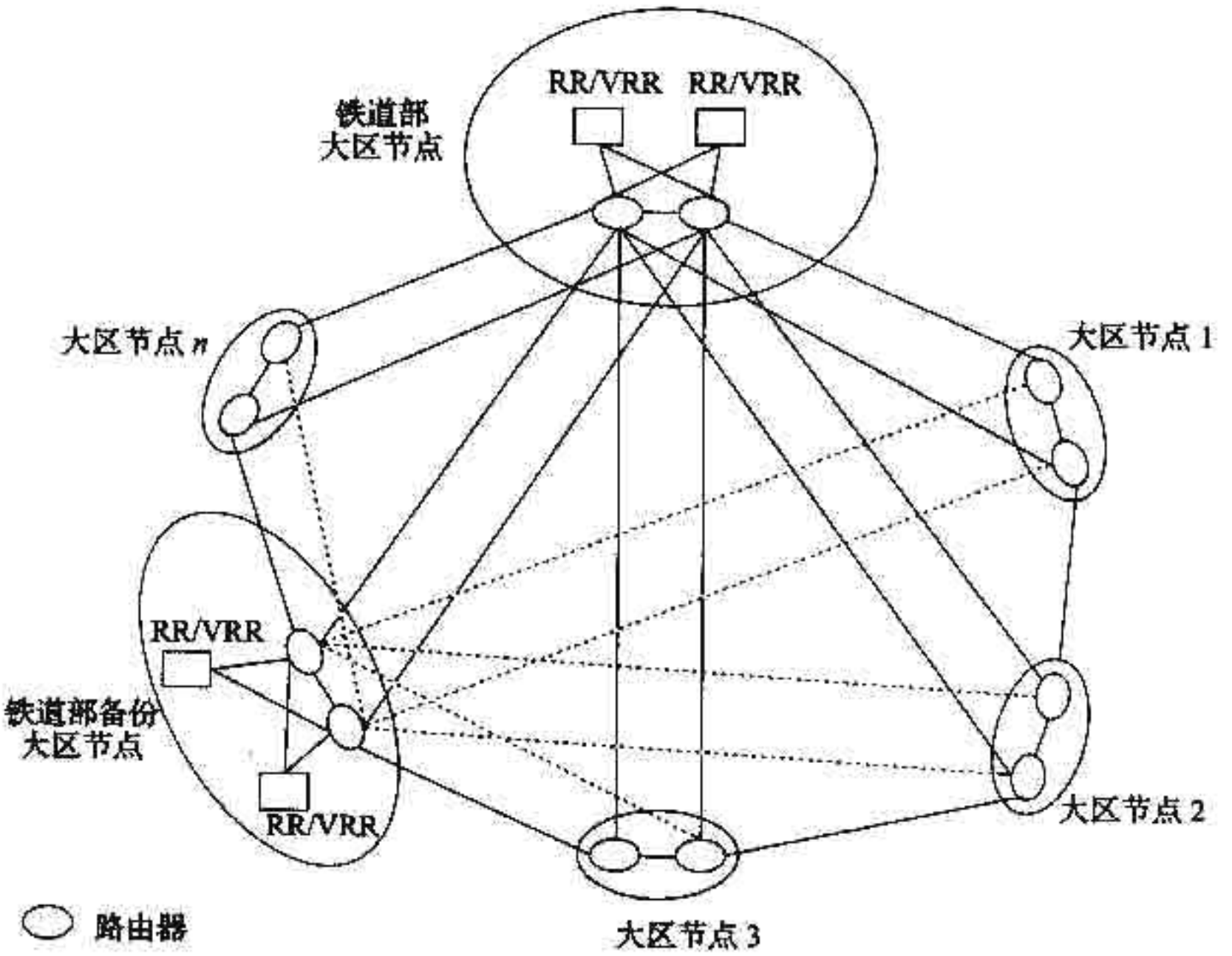

图 4.2.1　铁路数据通信网骨干网络结构图

1　铁道部应按大区节点设计，并宜选择一个异地大区节点作为铁道部大区节点的备份节点。

2　每一大区节点应设置 2 台路由器。

3　各大区节点间形成网状或部分网状连接，每一大区节点应与其地理位置上相邻的另两个大区节点连接。

4　各大区节点与铁道部大区节点、铁道部备份节点间应设置直连链路。

5　各个大区节点间的互联链路带宽应根据业务流量设置。在符合业务近期需求的情况下具有一定的余量，带宽应不低于 155 Mb/s。

6　各大区节点间的互联链路应由具有保护能力的传输网络提供；各大区节点与铁道部大区节点、铁道部备份节点间的链路

数量不应少于2条，并应采用不同物理路由；当其他大区节点间的互联链路数量多于1条时，应采用不同物理路由。

4.2.3 骨干网络应设置RR及VRR。RR及VRR宜合设，并应冗余配置。

4.2.4 铁道部大区节点及铁道部备份大区节点应分别设置两台RR/VRR，每台RR/VRR应与本大区节点的两台路由器相联。

4.3 区域网络

4.3.1 铁路局区域网络结构如图4.3.1所示。

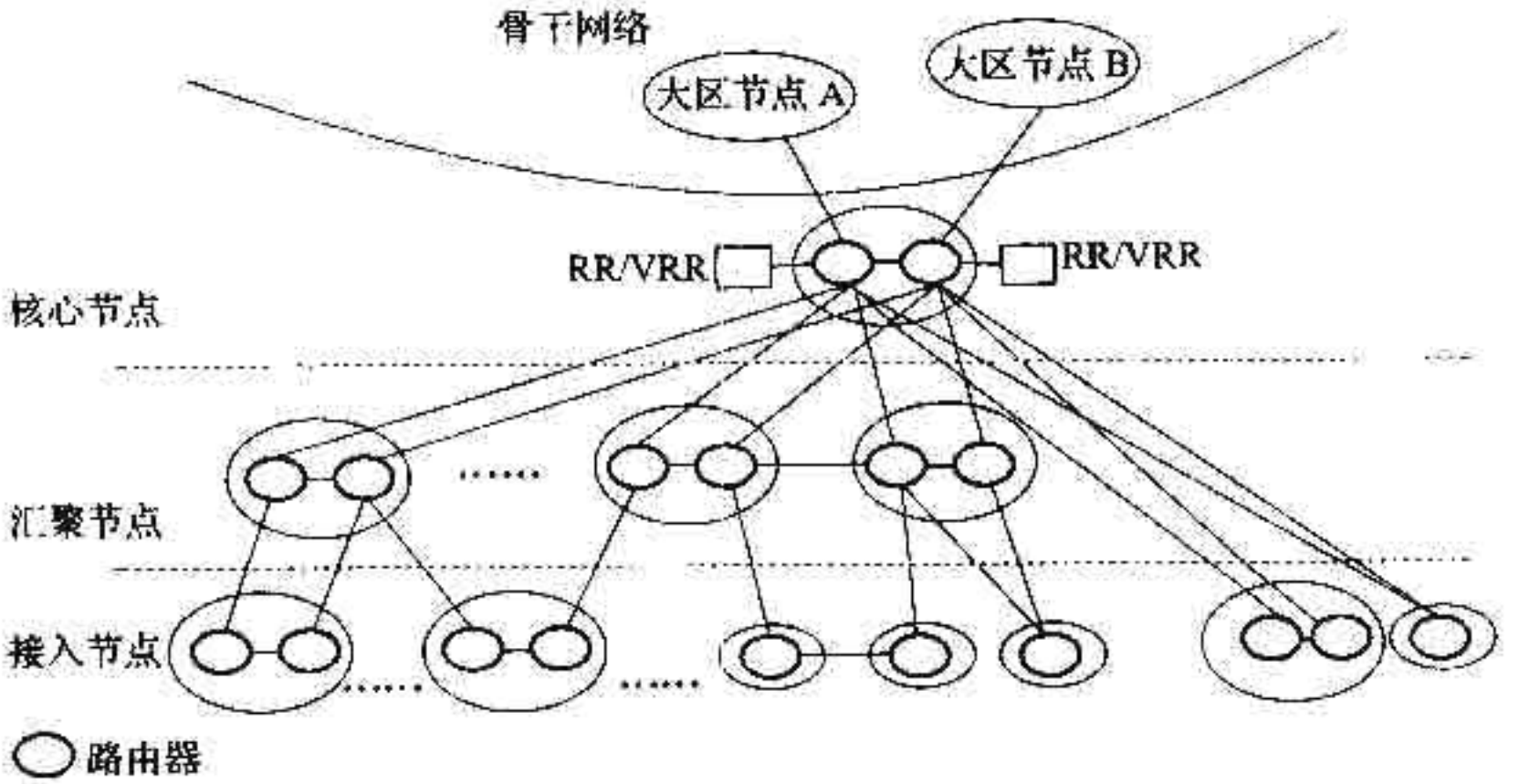

图4.3.1 铁路局区域网络结构图

4.3.2 铁路局区域网络核心节点的设计应符合下列规定：

1 核心节点应设置2台路由器。

2 设有大区节点铁路局的核心节点2台路由器应上联至本铁路局大区节点及另外一个在地理位置上相邻的大区节点。

3 未设置大区节点铁路局的核心节点2台路由器应分别上联至地理位置上相邻的两个大区节点。

4 核心节点与大区节点间互联链路的带宽应根据业务流量设置，在符合业务近期需求的情况下，具有一定的余量。

5　核心节点与一个大区节点间的互联链路仅为1条时，此链路应由具有保护能力的传输网络提供；当多于1条时，应采用不同物理路由。

4.3.3　铁路局区域网络汇聚节点的设计应符合下列规定：

1　汇聚节点应设置2台路由器。

2　汇聚节点的路由器宜直接上联至核心节点的2台路由器。汇聚节点与核心节点及汇聚节点间可形成网状或部分网状连接。

3　汇聚节点与核心节点及汇聚节点间的互联链路带宽应根据业务流量设置。在符合业务近期需求的情况下，应具有一定的余量。

4　汇聚节点与核心节点间的互联链路应采用不同物理路由。

5　两个汇聚节点间的互联链路仅为1条时，此链路应由具有保护能力的传输网络提供；当多于1条时，应采用不同物理路由。

4.3.4　铁路局区域网络接入节点的设计应符合下列规定：

1　客运专线铁路接入节点应在铁路局、客专调度所、客专综合维修中心、客专动车检测基地、车站及段（所）等设置。

2　客货共线等铁路接入节点应设置在铁路局及业务需求量较多的车站、段（所）等；未设置接入节点的车站、段（所），通过传输网络将业务接入到邻近的接入节点。

3　铁路局、客专调度所、客专综合维护中心、客专动车检测基地及通用分组无线业务（GPRS）的接入节点应设置2台接入路由器；其他接入节点根据需要设置1台或2台接入路由器。

4　铁路局、客专调度所、客专综合维修中心、客专动车检测基地以及铁路局所在地的段（所）接入节点可直接上联至本区域网络核心节点。

5　车站、段（所）接入节点连接至汇聚节点的连接方式

1）直接连至汇聚节点的2台路由器；

2）分别连至地理位置相邻的2个汇聚节点；

3）多个接入节点串接后与1个或2个汇聚节点连接。

6 接入节点与汇聚或核心节点间及接入节点间互联链路的带宽应根据网络流量设置，在符合业务近期需求的情况下，具有一定的余量。

7 接入节点与汇聚或核心节点间及接入节点间的互联链路仅为1条时，此链路应由具有自愈能力的传输网络提供；当多于1条时，应采用不同物理路由。

4.3.5 铁路局区域网络应设置RR及VRR。RR及VRR宜合设并应冗余配置。

4.3.6 铁路局区域网络每台RR/VRR与核心节点的两台路由器互联。

4.3.7 铁道部区域网络结构如图4.3.7所示。

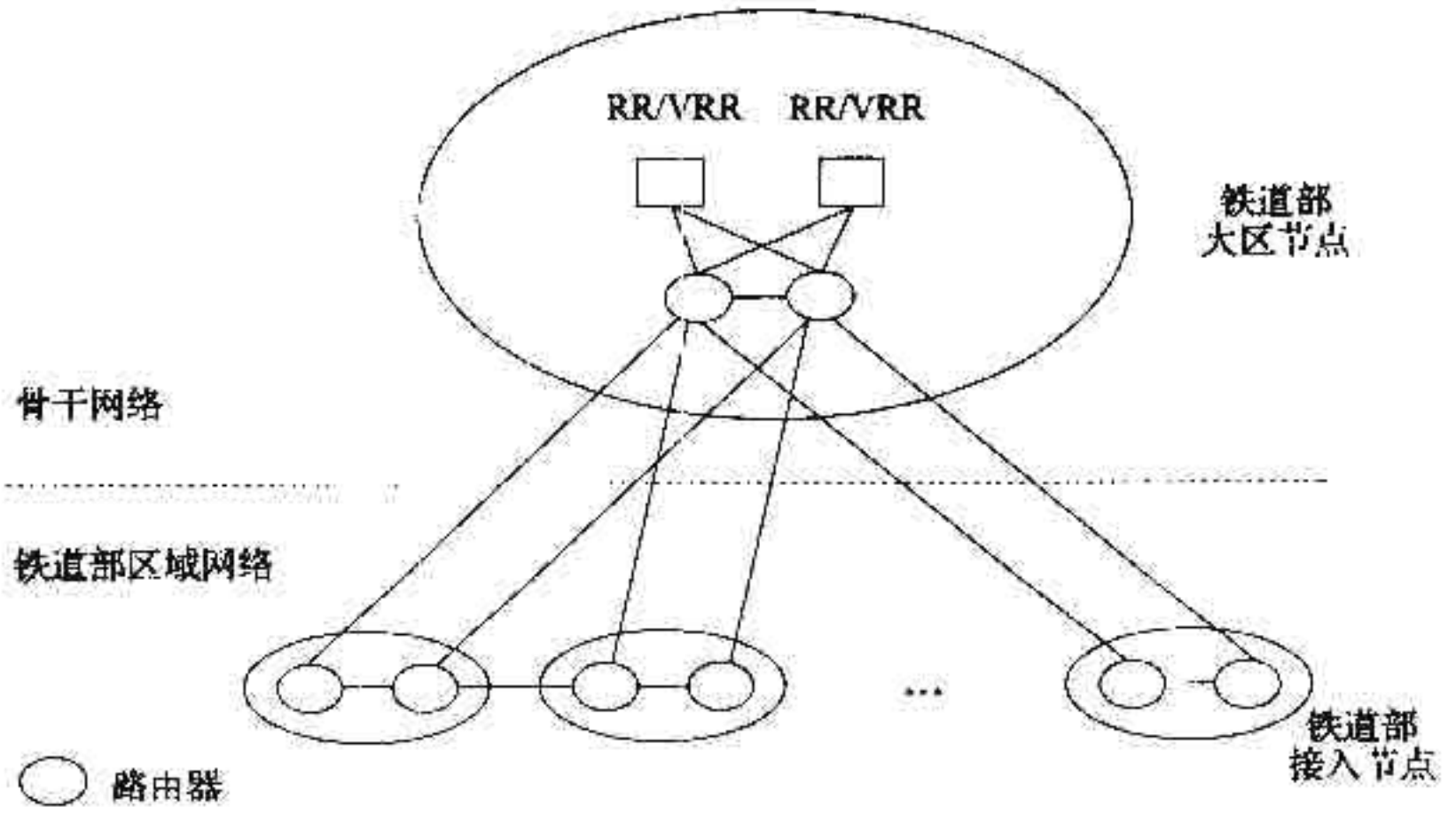

图4.3.7 铁道部区域网络结构图

4.3.8 铁道部接入节点的设计应符合下列规定：

1 根据业务需要，铁道部设置一个或多个接入节点，每个接入节点应设置2台接入路由器。

2 铁道部每个接入节点的2台路由器应与铁道部大区节点

2 台路由器直连。

3 铁道部接入节点与铁道部大区节点间互联链路的带宽应根据网络流量设置，在符合业务近期需求的情况下，具有一定的余量；并应采用不同物理路由。

4 铁道部各接入节点间根据业务需要可设置直连链路。

4.4 业务接入方式

4.4.1 铁路数据通信网应支持专线接入、有线宽带接入、区域多点传输服务（LMDS）及无线局域网（WLAN）等无线接入的多种业务接入方式。

4.4.2 重要业务应采用专线接入方式，并宜具有迂回保护措施。

4.4.3 当用户业务接入点信息流量较大、业务种类较多且距离铁路数据通信网边缘较远时，可采用光纤以太网或 MSTP 等接入方式；当距离较近时，也可采用电缆等其他以太网接入方式。

4.4.4 在敷设光电缆困难的节点，可采用 LMDS、WLAN 等无线接入方式，使用频率等应符合国家无线电管理的相关规定。

5 路由协议及路由策略

5.1 路 由 协 议

5.1.1 铁路数据通信网广域网应按多个自治域进行设计。骨干网络及铁道部区域网络应构成Ⅱ个自治域系统；各铁路局区域网络应构成各自独立的自治域系统。

5.1.2 铁路数据通信网骨干网络自治域及各铁路局区域网络自治域之间宜采用 BGP-4 路由协议。跨域 MPLS VPN 互通宜采用“背靠背的 VRF 到 VRF”技术。

5.1.3 铁路数据通信网自治域内部应采用 IGP 承载网络拓扑路由信息，采用 IBGP 承载用户路由信息，采用 MP-BGP 承载 VPN 用户路由信息。IGP 可选用 IS-IS 或 OSPF。

5.1.4 业务接入宜采用静态路由协议及 BGP-4 协议。根据业务需要，也可采用 OSPF 等动态路由协议。

5.2 路 由 策 略

5.2.1 铁路数据通信网路由策略的设计应符合下列规定：

1 路由策略应保证正确路由信息的接收与宣告。

2 在网络拓扑的配合下，路由策略应避免网络中出现单故障点，提高网络的生存能力。

3 路由策略应保证业务流量合理的分配。

4 路由策略应采用无类域间路由（CIDR）等方式最大化地进行路由聚合。

5 路由策略应便于网络的管理维护，对业务流量流向的变化具有适应性。

5.2.2 根据网络所承载的业务种类，在存在多条路由的情况下，可采用下列方式对流量、流向进行设计：

1 使用静态路由协议的网络，宜采用主备疏通方式。

2 使用动态路由协议的网络，宜采用分担疏通方式。

5.2.3 路由选择应合理设计域内路由协议的链路权值，合理设计使用域间路由协议的各种属性赋值。

5.2.4 路由选择应符合下列规定：

1 骨干网络各大区节点间应优选节点间直连链路。

2 各区域网络之间互访应通过骨干网络转接。

3 网络中不应存在路由选择循环，不应存在路由黑洞。

5.2.5 铁路数据通信网两种路由协议间不宜进行路由信息的互相注入。

5.2.6 铁路数据通信网宜采用路由协议的快速收敛技术。

5.2.7 铁路数据通信网宜采用路由协议的平稳重启技术。

5.2.8 铁路数据通信网宜在接入节点路由器以及实现域间互联的区域网络核心路由器、骨干网络大区节点路由器上采用 BGP 阻尼的方式，减少由于链路不稳定对网络产生的影响。

6 自治域号码分配及 IP 地址分配

6.0.1 铁路数据通信网自治域号码分配、IP 地址分配应符合铁道部相关规定。

6.0.2 铁路数据通信网使用的 IP 地址应划分不同的区段，并分为网络基础设施地址和业务地址。网络基础设施地址主要包括网络设备端口互联地址、网络设备管理地址、网络管理系统地址、域名服务器地址等；业务地址为各种业务的应用地址。

6.0.3 铁路数据通信网的 IP 地址分配应符合下列规定：

1 按需分配 IP 地址，并预留一定的发展空间。

2 IP 地址分配应考虑连续性，宜按业务连续并兼顾地域连续分配 IP 地址。

3 IP 地址的分配应采用 CIDR 方式及可变长子网掩码（VLSM）技术，合理、高效地使用 IP 地址。不应使用 24 位子网掩码作为最小分配单位。划分子网掩码时应保持地址的连续和路由表的优化。

7 域名系统

7.0.1 铁路数据通信网域名系统设计应采用树型结构，并由铁道部根域名系统和铁路局二级域名系统构成。

7.0.2 铁道部应设置根域名服务器，并对骨干网络及各铁路局区域网络的路由器进行域名解析。

7.0.3 铁路局应设置二级域名服务器，并对各铁路局区域网络的路由器进行域名解析。

7.0.4 域名服务器应支持域名解析的冗余备份。

8 网络管理

8.0.1 铁路数据通信网的网络管理系统（以下简称网管系统）应包括网元管理及 VPN 管理，采用铁道部、铁路局两级结构。

8.0.2 铁道部应设置骨干网络网元管理系统，负责骨干网络及铁道部区域网络网元的管理；铁路局应设置区域网络网元管理系统，负责本区域网络网元的管理。

8.0.3 铁道部应设置骨干网络 VPN 管理系统，负责骨干网络及铁道部区域网络 VPN 的维护和管理；铁路局应设置区域网络 VPN 管理系统，负责本区域内 VPN 的维护和管理。

8.0.4 网络维护管理终端的设置应符合维护和管理要求。

8.0.5 网管系统宜采用带内管理方式，根据需要可采用带外管理方式。

8.0.6 网管接口应符合下列规定：

1 网管系统应提供接入综合网管系统的接口。

2 网管系统与被管理网元之间宜采用 SNMPv3 协议。

3 区域网络网管系统与骨干网络网管系统之间的接口可采用 SNMPv3 协议或基于 XML 的 Web Services 接口。

4 网络设备应支持网管接口故障管理、计费管理、配置管理、性能管理和安全管理功能要求，应提供实时告警信息、准实时的性能信息、动态的资源配置信息以及计费和安全信息。

5 网络设备应支持通用的公有信息模型，通用的公有信息模型应为 MIB 2.0 及以上版本。

6 网络设备可提供针对自身产品特色的私有信息模型，但供货商应提供接口标准、协议等相关信息。

8.0.7 网管系统应提供图形化管理，具备资源管理、拓扑管理、

配置管理、故障管理、性能监测、路由管理、QoS 配置管理、安全管理、VPN 管理、流量采集、报表统计等功能。

8.0.8 根据需要，网管系统可提供性能分析、基于 QoS 的性能监测及流量分析等功能。

9 网络安全

9.0.1 铁路数据通信网网络安全设计应包括承载网络安全、入侵防范、网络管理安全、网络安全审计、安全运行管理等。

9.0.2 铁路数据通信网承载网络安全应符合下列规定：

1 根据网络功能及安全等级的不同，划分为铁路数据通信网广域网、网管及域名系统、业务接入等安全域。

2 各安全域之间可采用防火墙等技术或组件进行隔离。

3 广域网应通过 MPLS VPN 隔离承载的业务。业务接入可采用 VLAN 划分等方式隔离。

4 有条件时，大区节点路由器及核心节点路由器设备宜设置在不同机房内。

5 在网络关键节点，可根据源地址/端口、目的地址/端口以及协议类型等参数实施访问控制（ACL），可根据路由表中的网段和物理接口实施单播反向路径查找（uRPF）。

6 在 OSPF、IS-IS、BGP 等协议中可启用校验和认证功能。

7 通过 TE FRR 等快速重路由技术，在汇聚及以上节点之间进行链路保护；也可通过其他专有 FRR 技术（如 IP FRR、VPN FRR），对端口和链路等层级进行保护。

8 可采用双向转发监测（BFD）技术进行各节点之间链路的快速故障检测。

9 可采用具有主备方式保障的虚拟路由器冗余协议（VRRP）技术进行业务系统接入的故障快速恢复。

10 可采用平稳重启（GR）等技术，在不中断数据转发时进行路由功能交替。

11 各业务系统及接入的安全防护，根据其需要进行自行设

置。

12 网络设备应支持鉴别、授权、计费（AAA）认证。

13 网络设备的服务配置应遵循最小化服务原则，关闭所有不需要的服务。对于必需开启的服务，可通过访问控制列表等手段限制主机地址。

14 网络设备应具有交互式访问安全的控制能力，应限制远程终端的 IP 地址，远程登录应加密。

9.0.3 入侵防范应符合下列规定：

1 可根据需要设置入侵检测系统、入侵防御系统、流量监测和清洗系统。

2 基于主机的入侵监测系统（HIDS）应设置在所监测的主机上。

3 基于网络的入侵监测系统（NIDS）应设置在所监测的网络的进出口处或数据交换区域，对关键链路或数据交换区进行安全检测。可采用链路旁路设置，也可利用网络设备的端口镜像功能以旁路方式设置在数据交换区域。

4 基于主机的入侵防御系统（HIPS）应设置在被保护的服务器上。

5 基于网络的入侵防御系统（NIPS）应设置在网络的进出口处，对入侵活动和攻击流量进行拦截。可采用串行方式设置，也可采用旁路方式设置。

6 流量监测系统可选择流采样、链路分光、端口镜像等监测方式。

7 流量监测系统可设置在被保护网络的边界。

8 流量清洗系统应根据网络实际情况选择引流、过滤、回注策略。

9 流量监测系统与流量清洗系统应能够实现系统间的联动，应在发现攻击流量后以手动或自动方式对攻击流量进行清洗过滤。

9.0.4 网络管理安全应符合下列规定：

1 在骨干网络各节点及区域网络的核心节点、汇接节点可采用带外网管方式。

2 网络管理应分权、分域，并严格控制网络访问的权限。

3 在采用 SNMP 做为网络管理协议时应采用 v3 及以上版本，在配置 SNMP 时宜具有信息—摘要算法（MD5）认证和数据加密标准算法（DES）加密。

4 可设置认证授权服务器，对登录用户进行集中认证和管理。

5 宜设置日志服务器，集中存储日志、告警和调试信息。

9.0.5 网络安全审计应符合下列规定：

1 网络安全审计应由专用审计系统或相关网络安全设备实现。

2 专用审计系统宜包括日志采集、主机审计、网络审计等。

3 网络安全设备宜包括网络漏洞扫描、防火墙、入侵检测系统/入侵防御系统等。

4 网络安全审计的对象应包括路由器等网络设备、服务器、网络安全设备等，所有审计对象应开启日志记录功能。

9.0.6 安全运行管理应符合下列规定：

1 安全运行管理应具有安全事件管理、安全策略管理、安全预警管理、安全日志审计、知识库管理、流程管理、关联分析、风险管理等功能。

2 安全运行管理应支持对各类被管理对象的多种数据采集方式，实现安全事件收集、安全日志收集功能。

10 服务质量

10.0.1 铁路数据通信网的链路带宽应在估算所承载各种业务系统的平均流量和峰值流量的基础上设计。

10.0.2 在采用主备疏通方式时，链路带宽平均峰值利用率宜为50% ~70%；在采用分担疏通方式时，链路带宽平均峰值利用率宜为40% ~45%。

10.0.3 根据业务需要，铁路数据通信网可采用基于差分服务代码点（DSCP）的DiffServ等技术保证服务质量。

11 设备配置原则

11.0.1 根据需要，铁路数据通信网应配置网络设备和配套设备。网络设备包括路由器、网管设备以及防火墙设备、域名服务器等。配套设备包括电源设备、配线架等。

11.0.2 铁路数据通信网设备应符合相关技术标准的规定，以及安全可靠、技术先进、经济合理、兼容性好、扩展性强等的要求。

11.0.3 铁路数据通信网路由器设备应符合下列要求：

1 支持整机满负荷情况下端口全双工线速转发。

2 支持 OSPFv2、IS-IS、BGP-4 等路由协议。

3 支持 PIM-SM、PIM-DM、DVMRP、MBGP、MSDP 等组播路由协议。

4 支持拥塞控制机制。

5 支持差分服务功能。

6 支持路由冗余协议。

7 支持 MPLS VPN。

8 支持 SNMPv2/v3 协议。

9 宜支持 10/100 Mb/s、GE、POS/ CPOS 155 Mb/s 及以上速率的接口及同步串口。

10 宜具备通过软件升级支持 IPv6 的能力。

11.0.4 大区节点、核心节点、汇聚节点路由器的路由引擎、交换矩阵、电源模块、冷却风扇等关键部件应冗余配置。

11.0.5 接入节点路由器的路由引擎、交换矩阵、电源模块、冷却风扇等宜冗余配置。

11.0.6 大区节点、核心节点、汇聚节点路由器应采用模块化结

构，并应支持流量分析功能。

11.0.7 接入节点路由器宜采用模块化结构，并宜支持流量分析功能。

11.0.8 路由器设备的交换容量及包转发能力等性能应符合铁路相关技术标准的规定。

11.0.9 路由器设备的接口板应根据网络中继电路设计情况进行配置。当一个节点存在多条对外连接中继电路时，电路与接口板的对应应符合安全可靠性要求。

11.0.10 防火墙设备的配置应符合下列要求：

1 宜采用双机冗余配置，并具有负载均衡功能。

2 应具有包过滤功能，支持状态检测。

3 应具有防范扫描窥探功能，支持多种过滤及端口隐藏机制、端口到应用的映射。

4 应具有审计日志功能。

5 应支持地址及端口转换、端口映射和负载分配。

6 宜集成入侵检测功能。

11.0.11 配线架等配套设备应根据工程实际需要配置。

11.0.12 备品备件的配置应根据设备的重要性、维修管理要求等情况确定。

12 设备安装及运行环境要求

12.0.1 铁路数据通信网设备房屋应符合《铁路运输通信设计规范》TB 10006 等标准的有关规定。

12.0.2 铁路数据通信网设备的安装应符合下列规定：

1 有专用的数据设备房屋及监控室时，数据通信网设备应安装在相应房屋内。

2 与其他通信设备合用房屋时，数据通信网设备应安装在靠近传输设备的位置，网管设备安装在合设的监控室。

12.0.3 铁路数据通信网设备供电等级应符合《铁路电力设计规范》TB 10008 等标准的相关规定。

12.0.4 铁路数据通信网设备宜采用直流供电方式。当采用交流供电时，应配置 UPS 设备。

12.0.5 铁路数据通信网设备防雷、电磁兼容及接地应符合《铁路运输通信设计规范》TB 10006 及相关技术标准的规定。

12.0.6 维修维护仪表及工具应根据维修维护需要配置，主要的仪表可包括流量发生器、误码仪、协议测试仪、性能测试仪、协议分析仪等；主要的工具包括网线钳。

本规范用词说明

执行本规范条文时，对于要求严格程度的用词说明如下，以便在执行中区别对待。

（1）表示很严格，非这样做不可的用词：

正面词采用“必须”；

反面词采用“严禁”。

（2）表示严格，在正常情况下均应这样做的用词：

正面词采用“应”；

反面词采用“不应”或“不得”。

（3）表示允许稍有选择，在条件许可时首先应这样做的用词：

正面词采用“宜”；

反面词采用“不宜”。

（4）表示有选择，在一定条件下可以这样做的，采用“可”。

引用标准名录

1 《铁路运输通信设计规范》TB 10006—2005。

2 《铁路电力设计规范》TB 10008—2006。

3 《公用计算机互联网工程设计规范》YD/T 5037—2005。

4 《IP 网络技术要求—网络性能参数与指标》YD/T 1171—2001。

《铁路数据通信网设计规范》
条文说明

本条文说明系对重点条文的编制依据、存在的问题以及在执行中应注意的事项等予以说明。为了减少篇幅，只列条文号，未抄录原条文。

1.0.2 目前铁路信息系统业务及 GSM-R 的 GPRS、图像等通信系统数据业务主要由两种 IP 数据通信网来承载，即独立 IP 数据通信网和综合 IP 数据通信网。根据国家政策及铁路有关规定，对于涉及铁路运输安全控制、资金往来等系统的业务（包括 CTC/TDCS、列车控制及联锁、客票、公安等系统），使用独立 IP 数据通信网承载；铁路其他信息系统业务及通信系统数据业务，使用综合 IP 数据通信网承载。

本规范中的铁路数据通信网，特指铁路综合 IP 数据通信网。独立 IP 数据通信网的设计可参照执行。除业务接入方式之外，局域网工程设计的其他内容要符合相关技术标准的规定。

1.0.4 铁路数据通信网为铁路信息系统提供数据承载，其中许多信息关系到国家和铁路运输安全保密，因此其工程设计应符合国家有关信息安全的规定。

1.0.5 根据信息安全的需要和电信市场管理的规定，铁路数据通信网是铁路运输专用网络，不直接与公众互联网互联。铁路的门户网站等为公众服务的系统，可通过物理隔离的技术手段（如网闸等）从铁路相应信息系统中得到所需要的数据。

1.0.8 系统设备等是指便于升级扩容、易老化的系统设备。

3.0.2 目前，在建客运专线的铁路数据通信网工程的系统处理能力及业务接入能力的预留余量设计按照50%以上进行了考虑。

3.0.3 《IP网络技术要求—网络性能参数与指标》YD/T 1171规定了IP网络性能参数与指标，端到端主要性能指标见说明表1。

说明表1 IP网络性能参数与指标

性能名称	QoS			
	0级	1级(交互式)	2级(非交互式)	3级(U级)
IP包传输时延(平均包传输时延的上限值)	150 ms	400 ms	1 s	U
IP包传输时延变化(包传输时延的1－10^{-3}百分位值减去包传输时延的最小值)	50 ms	50 ms	1 s	U
IP包丢失率(上限值)	1×10^{-3}	1×10^{-3}	1×10^{-3}	U

3.0.7 本条参考铁道部运输局发布的《铁路时间同步网技术条件（V1.0）》（运基通信〔2008〕599号）的相关要求制定。根据该文件规定，铁路时间同步网地面时间同步部分按三级结构组成，一级时间同步节点设置在铁道部调度中心，二级时间同步节点设置在各铁路局调度所/客专调度所，三级时间同步节点设置在车站、段（所）。铁路时间同步网为铁路运输各业务系统提供统一标准时间信号，使各系统时钟设备与本系统同步，保证铁路各系统运行计时准确。随着客运专线的建设，北京、武汉等铁路局调度所已设置了二级时间同步节点设备。

4.2.2

1 由于铁路以铁道部为中心，大多数业务系统均需汇聚到

铁道部，因此，铁道部应设置为大区节点。

4　大多数业务系统均需汇聚到铁道部及备份节点，因此，每一大区节点都应设置与铁道部或备份节点的直连链路。

6　铁路数据通信网的设备互联链路由光传输网提供或采用光纤直连方式，因此，不同物理路由是指不同物理路由的光传输网或不同物理路由的光纤。本规范中的不同物理路由均为此含义。

4.2.3　路由反射方式是指某台路由器被配置为允许将通过 IBGP 所学到的路由通告（或反射）到其他 IBGP 对等体的路由方式。设置路由反射器（RR）及 VPN 路由反射器（VRR），是为了提高 IBGP 及 MP-BGP 会话的扩展性。

4.4.1　专线接入特指一个用户通过专用通道接入，可以采用宽带以太网方式、基于光纤的无源光网络、MSTP、LMDS 或 3.5 GHz 等固定无线方式接入铁路数据通信网。

有线宽带接入指一个以上用户通过 xDSL、宽带以太网、基于光纤的无源光网络、MSTP 等方式接入铁路数据通信网。

多用户也可通过 LMDS、WLAN 覆盖方式接入铁路数据通信网。

4.4.2　重要业务是指 GPRS、信号集中监测、综合视频监控、旅客服务、运营维护调度等。迂回保护措施包括两种方式，其一为业务接入设备与 2 台接入节点路由器互联；其二为业务接入设备与 1 台接入节点路由器通过两对接口间的两条链路互联，以防端口故障。

5.1.1　自治域系统就是由使用同一种路由协议、相互连接的路由器组成的网络区域。目前覆盖全国的电信运营商 IP 数据网络多数采用多自治域方式组网。本规范推荐采用多自治域方式组网，主要是由于铁路业务主要流向铁路局，铁路局内业务相对独立，并且有利于工程项目分期分批实施。多自治域及单自治域组网方式优缺点比较见说明表 2。

说明表 2　多自治域及单自治域组网方式优缺点比较

项目	多自治域方式	单自治域方式
目前应用情况	较多	较少
MPLS-VPN 配置工作量	多	少
多厂家的选择	在启用 MPLS VPN 时，一个域内 PE 设备厂家尽量少，但各个域的厂家选择不受限制	在启用 MPLS VPN 时，PE 设备厂家尽量少
分期、分批实施灵活性	好	一般
投资成本	较高	较低

5.1.2　根据 IETF 的 RFC 2547bis，跨自治系统（AS）实现 BGP/MPLS VPN的解决方案有下列三种：

方式 A（背靠背的 VRF 到 VRF）实施较简单，当 VPN 数量增加时，需要维护较多的 VRF 子接口，需要在 ASBR 之间运行多个 EBGP 会话。

方式 B（MP-EBGP）是 ASBR 之间通过 MP-EBGP 会话交换跨域的 VPN-IPv4 路由，并且为相应的 VPN 路由分配一个标签。ASBR 设备仍然作为 PE 设备，此种方式需要维护所有跨域的 VPN-IPv4 路由，但不需要在 ASBR 之间的接口上建立所有跨域的 VPN 所对应的 VRF 接口，也不需要在 ASBR 之间运行多个 EBGP 协议。但这种方式应用不如背靠背的 VRF 到 VRF 的模式广泛。

方式 C（RR 间多跳的 MP-EBGP）配置比较复杂，目前基本不被采用。

目前，电信运营商基本采用方式 A。

5.2.1　路由策略是指通过改变路由规则中影响路由发布、接收或路由选择的参数而改变路由发现的结果，最终改变的是路由表的内容，路由策略是在路由发现的时候产生作用。其目的是通过

路由策略的实施，实现正确的路由信息接收和宣告；使网络业务流量合理地分配在各条链路上；保证网络具有可扩展性，全部资源可以被优化利用；对业务流向流量的变化具有适应性。

6.0.3

1 IP 地址预留是考虑今后业务发展的需要；限定一定的空间是因为 IP 地址数量有限，避免闲置和浪费，提高利用率。

2 IP 地址分配考虑连续性是简化路由表的需要。在某一地域内，同一业务系统之间信息互通较多，跨业务系统信息互通相对较少，因此应首先考虑业务的连续性。

7

本章所述域名系统是指铁路数据通信网的域名系统。各业务系统的域名解析由各自的业务系统完成。

8.0.5 带内管理方式是指管理信息由本铁路数据通信网承载；带外管理方式是指管理信息由其他网络承载。

8.0.6

2 SNMP 是由互联网工程任务组（IETF）定义的网络管理协议。通过 SNMP，一个管理工作站可以远程管理所有支持这种协议的网络设备，包括监视网络状态、修改网络设备配置、接收网络事件警告等。

3 Web Services 是一个基于网络的应用程序，它向外部程序提供一定的调用接口。对 Web Services 的调用，通过 SOAP（简单对象访问）协议进行。XML 是 SOAP 的数据编码方式。

8.0.7 根据《公用计算机互联网工程设计规范》YD/T 5037，网管功能具体含义如下：

资源管理包括设备管理、链路管理、路径管理、IP 地址管理、软件版本管理、MPLS VPN 管理、资源报表统计、资源预警等功能。

拓扑管理包括根据不同的视角和不同的侧重层次，拓扑图可

以有不同的视图：实现拓扑自动发现、监视与浏览；实现基于拓扑的流量显示、资源显示、配置显示和故障显示等。

配置管理包括对网元设备及 MPLS VPN 的配置，可保存历史配置信息并可对不同配置进行比较。

故障管理包括提供列表形式的告警监视窗口，可在窗口视图上监视到网元的实时告警、对相关告警进行操作或启动相关网元的告警历史信息查询浏览功能；具备各种告警提示手段；支持告警过滤、告警转发、告警确认、告警升级和告警清除；支持故障关联分析。

性能监测包括对网络性能进行监测。

路由管理包括对网络中的路由实体进行监视，对网络路由信息及其变化情况进行分析。

QoS 配置管理包括网络层 QoS 参数配置。

安全管理功能是指本规范第 9.0.4 条的有关规定。

流量采集包括对各个网络层次的电路进行流量的采集。

报表统计包括对网络业务、资源、故障以及性能等信息进行统计，提供多种形式的报告和图表。

8.0.8 性能分析包括针对网元、路由信息、端到端路径、网络应用等不同层次、不同方面，对网络的性能进行分析，及时发现故障征兆，并进行前期预警。

基于 QoS 的性能监测及性能分析是指针对不同 QoS 要求的不同业务，进行性能监测及流量分析。

流量分析包括对各个网络层次的电路负载和电路拥塞的分析、网络流量流向及网络业务类型分布的分析。

9.0.3

1 入侵防范是指从 IP 网络的若干关键点收集信息并对其进行分析，从中发现网络中是否有违反安全策略的行为或遭到入侵的迹象，并依据既定的策略采取一定的安全措施。

2～3 入侵检测系统可以实现对网络或主机中的信息探测、

拒绝服务、蠕虫病毒、权限获取和可疑网络活动等威胁进行检测和识别，必要时提供安全记录和告警，为了解安全状况和阻断非法访问提供依据。

4~5 入侵防御系统可以实现对网络或主机中的信息探测、拒绝服务、蠕虫病毒、权限获取和可疑网络活动等威胁进行检测和识别，并主动、实时地采取措施对攻击或恶意数据包进行限制和阻断。

6~7 流量监测系统对网络中的路由设备发出的流信息进行采集分析，关联网络的路由信息，可以发现、定位网络中的DDoS等攻击流量，保证网络的安全性和可用性，为网络优化改造提供依据。

采用流（Flow）采样方式，通过合理设置被监测路由设备的流采样比例，确保路由设备开启流采集不影响正常流量转发。

9.0.5 网络安全审计的设计目标是实现对系统的记录及活动进行独立的复查及检查，以便监测系统控制是否充分，确保系统控制与现行策略及操作程序保持一致，探测违背安全性的行为，并通告控制、策略、程序中所显示的任何变化，为今后取证和安全策略的调整提供依据。

9.0.6 安全运行管理中心是实现安全管理的技术平台，提供对防火墙、网络安全设备等的统一安全管理，实现对风险及安全状况的集中呈现和管理。

10.0.2 本条参考《公用计算机互联网工程设计规范》YD/T 5037相关要求，并考虑铁路数据通信网承载业务的重要性而确定。

10.0.3 服务质量（QoS）是指IP网络的一种性能要求，可为特定的业务提供其所需要的服务。通过采用保证QoS的技术，能有效地控制网络资源及其使用，针对不同的客户需求提供差异的服务。

目前，保证QoS的要求主要包括下列技术：

1 基于DSCP的DiffServ方案是一种基于类的QoS技术，通

过将业务定义为有限的类型，可以较好地解决扩展性问题。此技术目前较多采用。

2　基于资源预留协议（RSVP）的 IntServ 方案是一种端到端基于流的 QoS 技术，目前粒度为单个流的资源预留的解决思路在 IP 网上的扩展性无法保证。此技术目前较少采用。

3　MPLS 可以与 DiffServ 结合，提供 MPLS CoS。MPLS 与 DiffServ 的结合可以将 DS 字节的设置融入 MPLS 的标记分配过程中，使得 MPLS 标记具有区分分组服务质量的能力。包括 E-LSP 方案和 L-LSP 方案，目前主要采用 E-LSP 方案。

4　MPLS-TE 是一种间接改善 QoS 的技术。MPLS-TE 利用了 LSP 支持显式路由的能力，在网络资源有限的前提下，将网络流量合理引导，间接改善网络服务质量。MPLS DiffServ-AwareTE 在 MPLS TE 的基础上，增加了基于类别的资源管理，充分利用了 DiffServ 的可扩展性以及 MPLS 的显式路由能力，是解决 IP QoS 的较好技术之一。此技术目前较少采用。

以下为在铁路数据通信网建设中采用 DiffServ 保证 QoS 的设计参考，见说明表3。

说明表3　QoS 设计示例

优先级（高至低）	等级名称	DSCP	IPPre/EXP/802.1p	类别	队列调度	拥塞避免
5	重要业务	101000	101	EF	严格优先	不丢包
4	高优先级	100000	100	AF4	CBWFQ	WRED
3	中优先级	011000	011	AF3	CBWFQ	WRED
2	低优先级	010000	010	AF2	CBWFQ	WRED
0	普通业务	000000	000	BE	尽力转发 FIFO	WRED

在设计 QoS 时，首先根据业务需要，定义服务等级；其次，在网络接入边缘，采用业务分类与标记、速率限制等技术；在网络核心，主要采用队列调度、拥塞控制等技术。

11.0.3

3　组播路由协议分为域内组播路由协议和域间组播路由协议，域内组播路由协议包括 PIM-SM、PIM-DIM、DVMRP 等，域间路由协议包括 MBGP、MSDP 等。较为典型的组播协议配置方式为 PIM-SM/MSDP/MBGP，其中域内运行 PIM-SM 协议，域间建立外部 MBGP 对等会话，RP 之间建立外部 MSDP 对等。

11.0.4　大区节点、核心节点、汇聚节点的设备故障，将影响多个接入节点的业务，因此要求对路由引擎、交换矩阵、电源模块、冷却风扇等关键部件冗余配置。

12.0.6　流量发生器按照需求发送数据流；误码仪用于测试误码率；协议测试仪用于对 CHAP、PAP、ARP、ICMP、IGMP、IP、TCP、UDP 等协议的测试；路由协议测试仪用于对 OSPF、IS-IS、BGP 等路由协议及组播协议的测试；性能测试仪用于对时延、丢包率、QoS 等性能及吞吐量、路由表容量等的测试；协议分析仪用于 SNMP 等网管相关协议的分析。