北 京 市 交 通 标 准 化 技 术 文 件

BJJT/0038-2019

轨道交通 AFC 基础网络技术要求

Rail transit AFC basic network technical requirements

2019-10-30 发布

北 京 市 交 通 委 员 会　　发 布

前　言

本部分按照GB/T 1.1－2009给出的规则起草。

本部分由北京市交通委员会提出并归口。

本部分由北京市交通委员会组织实施。

本部分起草单位：北京市轨道交通指挥中心。

本部分主要起草人：张莉、金晨、赵燕红、隋丽莉、王照华、赵冰、王征、于涛、戴国强、边毅、周鳞真。

目　　次

前言 I
目次 II
1 范围 1
2 规范性引用文件 1
3 术语与定义 1
4 缩略语 2
5 多线路中心（MLC）层 2
5.1 网络技术要求 3
5.2 网络设备硬件要求 7
5.3 网络配置协议要求 8
6 线路中心（汇聚节点）层 12
6.1 网络技术要求 12
6.2 网络设备硬件要求 17
6.3 网络配置协议要求 18
7 车站（SC）层 22
7.1 网络技术要求 23
7.2 网络设备硬件要求 27
7.3 网络配置协议要求 28

轨道交通AFC基础网络技术要求

1 范围

轨道交通AFC基础网络范围包括：ACC、AFC监视中心、互联网票务平台、多线路中心MLC、线路中心汇聚节点及车站SC。

本技术要求规定了轨道交通自动售检票系统多线路中心（MLC）层、线路中心（汇聚节点）层、车站（SC）层三个部分的基础网络技术要求、网络设备硬件要求和网络配置协议要求。

本部分适用于北京市轨道交通与运营生产相关的自动售检票系统网络的建设、既有线路系统网络的改造和运营维护工作。

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。

GB/T 25068 信息技术 安全技术 IT网络安全

GB/T 35317 公安物联网系统信息安全等级保护要求

GB 50157 地铁设计规范

3 术语与定义

下列术语与定义适用于本文件。

3.1

自动售检票系统 automatic fare collection

基于计算机、通信、网络、自动控制等技术，实现自动售票、检票、计费、收费、统计、清分、管理等全过程的自动化系统。

3.2

多线路管理中心 multiple line center

用于管理多条线路自动售检票系统的计算机系统。

3.3

单线路管理中心 line center

用于管理一条线路自动售检票系统的计算机系统。

3.4

车站计算机 station computer

用于管理车站的票务、设备运行、客流统计等的计算机系统。

3.5

stub 类型数据　stub type data
在数据传输中，目的IP地址为本地网络地址，数据到达本地网络后传输结束，数据不再继续转发

3.6

pass 类型数据　pass type data
在数据传输中，目的IP地址为非本地网络地址，数据需经过本地网络进行转发，终到达目的地址

3.7

单站双向　single station bidirectional
本地网络与单一车站之间双向

3.8

中心双向　centrally bidirectional
本地网络与轨指中心之间双向

4　缩略语

下列缩略语适用于本文件。
ACC：自动售检票清算管理中心（AFC Clearing Center）
AFC：自动售检票系统（Automatic Fare Collection）
MLC：多线路管理中心（Multiple Line Center）
SC：车站计算机（Station Computer System）
API：应用程序接口（Application Program Interface）
OSPF：开放式最短路径优先（Open Shortest Path First）
UI：用户数据接口（User Interface）
QoS：服务质量（Quality of Service）
FTP：文件传输协议（File Transfer Protocol）
SFTP：安全文件传送协议（Secure File Transfer Protocol）
TCP/IP：传输控制协议/因特网互联协议（Transmission Control Protocol/Internet Protocol）
NTP：网络时间协议（Network Time Protocol）
IPS：入侵防御系统（Intrusion Prevention System）
IDS：入侵检测系统（Intrusion Detection Systems）
SNMP：简单网络管理协议（Simple Network Management Protocol）
ICMP：控制报文协议（Internet Control Message Protocol）
VRRP：虚拟路由冗余协议（Virtual Router Redundancy Protocol）
VLAN：虚拟局域网（Virtual Local Area Network）
MTBF：平均无故障时间（Mean Time Between Failure）
BFD：双向转发检测协议（Bidirectional Forwarding Detection）
SLA：服务等级协议（Service-Level Agreement）
ACL：访问控制列表（Access Control List）
STP：生成树协议（Spanning Tree Protocol）
OBPS-SC：车站互联网认证服务器

5　多线路中心（MLC）层

5.1 网络技术要求

5.1.1 总体要求

基于现有AFC网络结构及业务特点，MLC层位于线路汇聚节点、车站、互联网综合业务与AFC监视中心的连接位置，在满足各运营公司MLC自身业务的基础上，应具备链路层和网络层的高可靠性要求。

为满足国家法律法规对网络安全的相关要求，对于AFC系统的网络安全及运营安全的整体要求，制定不低于信息安全等级保护二级的标准。

对AFC网络的整体运行状态增加设备硬件状态信息、接口流量信息等相关采集要求，以达到网络设备可监视，链路状态可监视。

为适应未来新型业务要求及新网络标准，整体网络应具备可扩展能力。

5.1.2 业务说明

5.1.2.1 在线文件传输

表 1 在线文件传输业务说明

通信协议	FTP 协议、SFTP
交互数据类型	参数数据、程序文件、日志文件
概要说明	上位下发文件到指定目录
	下位上传文件到指定目录
业务特点	非实时性业务，重要级
备注	现阶段使用 FTP 为不安全链接，应采用 SFTP 或对文件进行压缩加密等

5.1.2.2 在线数据传输

表 2 在线数据传输业务说明

通信协议	基于 TCP/IP 的 SOCKET 方式
交互数据类型	交易数据、状态数据、控制数据、业务数据、参数版本、开机/断线续连、业务结束
概要说明	上位与下位的数据业务
业务特点	实时性业务，重要级
备注	无

5.1.2.3 时钟同步

表 3 时钟同步说明

通信协议	NTP 协议
交互数据类型	时钟同步
概要说明	与上位 ACC 进行时钟同步（客户端）
	与下位 SC 进行时钟同步（服务器）

业务特点	实时性业务，次要级
备注	无

5.1.2.4 网络通信业务

表 4 网络通信业务说明

通信协议	TCP/IPv4、TCP/IPv6
交互数据类型	AFC 业务数据、网络监控数据
概要说明	MLC 系统内数据、ACC 认证数据、互联网认证数据、监视中心旁站数据
业务特点	实时性业务，重要级
备注	MLC 内数据为 stub 类型数据；其他数据为 pass 类型数据

5.1.3 网络拓扑简图

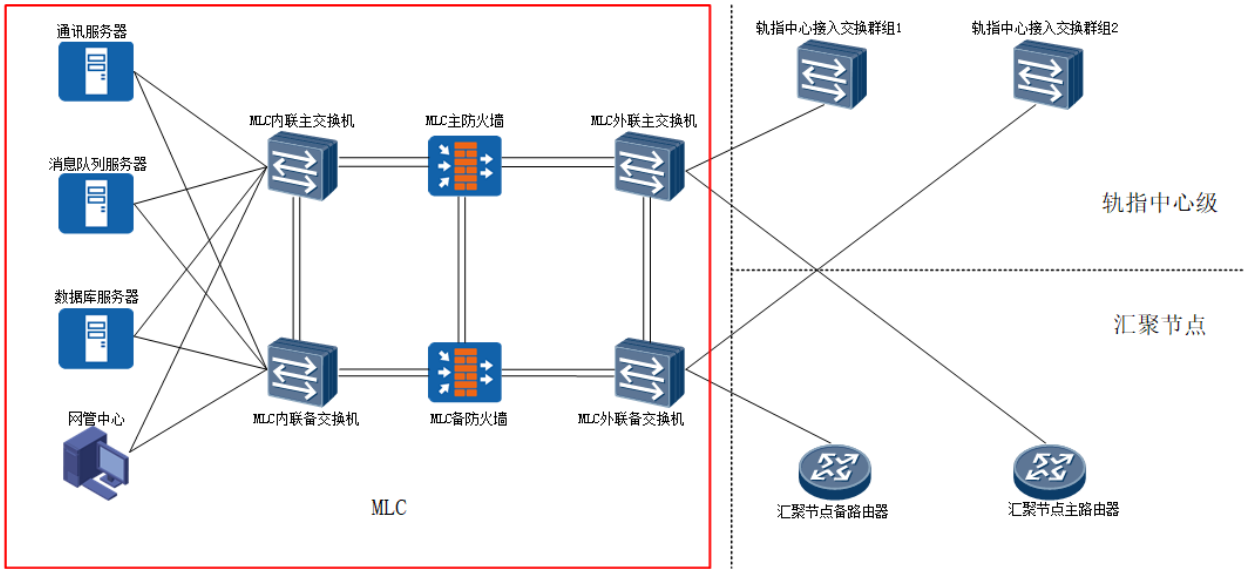

图 1 MLC 网络拓扑简图

5.1.4 网络拓扑简图说明

5.1.4.1 外联交换机

外联交换机的网络拓扑要求如下：

a) 须设置 MLC 外联主交换机用于与各线路汇聚节点的主路由器网络通信，同时须与轨指中心主交换区组连接；

b) 须设置 MLC 外联备交换机用于与各线路汇聚节点的备路由器网络通信，同时须与轨指中心备交换区组连接；

c) MLC 外联主/备交换机之间须配置不少于两条物理链路，以保证链路的高可用性。

5.1.4.2 防火墙

防火墙的网络拓扑要求如下：

a) 须设置 MLC 主防火墙用于外联主交换机与内联主交换机连接，起到安全防护的作用；
b) 须设置 MLC 备防火墙用于外联备交换机与内联备交换机连接，起到安全防护的作用；
c) 防火墙与外/内联交换机之间须配置不少于两条物理链路，以保证链路的高可用性；
d) 防火墙之间须有“配置同步线”，所有安全策略须保持一致。内联交换机

内联交换机的网络拓扑要求如下：
a) 须设置 MLC 内联主交换机用于与 MLC 内部服务器通信且做为主网关；
b) 须设置 MLC 内联备交换机用于与 MLC 内部服务器通信且做为备网关；
c) MLC 内联主/备交换机之间须配置不少于两条物理链路，以保证链路的高可用性。

5.1.4.3 其他网络设备

内联交换机的网络拓扑要求如下：
a) 须设置相关网络安全产品，如 IPS/IDS、防毒墙等，宜以旁路方式部署，如需以串联方式部署须配置 bypass 功能；
b) 须预留网络流量采集接口，以备后续抓包等操作进行故障分析；
c) 须配置网络管理系统，用于网络监控等。

5.1.5 可靠性要求

可靠性是AFC网络系统能够在规定条件下和规定的时间内完成规定的功能的特性。AFC系统网络的可靠性维度主要有三种：抗毁性、生存性和有效性。

抗毁性是指系统在人为破坏下的可靠性。比如，部分线路或节点失效后，相关网络配置变更错误后，系统应能够提供全部或部分业务。

生存性是指系统在随机破坏下的可靠性，生存性主要反映随机性破坏和网络拓扑结构对系统可靠性的影响，随机性破坏是指系统部件因为自然老化等造成的自然失效。

有效性主要反映在部分链路失效情况下，满足业务性能要求的程度。比如，网络部件失效虽然没有引起连接性故障，但是却造成质量指标下降、平均延时增加、线路阻塞等现象。

AFC网络应具有自愈功能，当出现人力、环境及老化等相关问题后，可以自愈或通过人为干预在最短时间内解决。

基于AFC业务特点，可按照实时性要求及业务重要等级要求确定高可用性参考基线，网络整体运行丢包率应不高于1%，负载率应不高于50%，非破坏性故障自愈延迟应小于180秒。详见表 5：

表 5 高可用性参考基线

网络状态	状态参数自愈时间
完好率=100%	单站双向网络延迟<50ms，丢包率<1%，资源可用率>40% 中心双向网络延迟<20ms，丢包率<1‰，资源可用率>60%
完好率≥50%	单站双向网络延迟<150ms，丢包率<3%，资源可用率>20% 中心双向网络延迟<50ms，丢包率<1‰，资源可用率>50% 自愈时间<30s，自愈状态不低于 75%
完好率≤50%	单站双向网络延迟<250ms，丢包率<5%，资源可用率>10% 中心双向网络延迟<100ms，丢包率<1%，资源可用率>30% 自愈时间<300s，自愈状态不低于 50%

5.1.6 网络安全要求

5.1.6.1 终端安全

终端安全是以终端安全保护系统全方位综合保障终端安全，并以数据安全保护系统重点保护终端敏感数据的安全。终端安全保护系统以“主动防御”理念为基础，采用基于标识的认证技术，以智能控制和安全执行双重体系结构为基础，将全面安全策略与操作系统有机结合，通过对代码、端口、网络连接、移动存储设备接入、数据文件加密、行为审计分级控制，实现操作系统加固及信息系统的自主、可控、可管理，保障终端系统及数据的安全。

5.1.6.2 数据安全

数据安全保护系统能够实现数据文档的透明加解密保护，可指定类型文件加密、指定程序创建文件加密，杜绝文档泄密。实现数据文档的强制访问控制和统一管理控制、敏感文件及加密密钥的冗余存储备份，包括文件权限管理、用户管理、共享管理、外发管理、备份管理、审计管理等。对各种敏感数据文档，包括设计文档、设计图纸、源代码、用户人员账号信息、财务报表及其他各种涉及商业秘密的文档，都能实现稳妥有效的保护。

5.1.6.3 网络通信安全

本标准只涉及网络通信安全，须在网络设备上对已知业务和业务网段需求启动白名单机制，控制粒度不低于网络级，如可使用访问控制列表，策略路由，源地址检测等相关安全手段及技术，对汇聚节点侧增加访问控制策略，所涉及的业务网段详见表 6：

表 6 业务网段列表

涉及业务	IP 网段	IP 地址范围
AFC 清分清算中心	10.0.0.0/16	10.0.0.1~10.0.255.254
AFC 监视中心	10.61.0.0/16	10.61.0.1~10.61.255.254
互联网平台	10.62.0.0/16	10.62.0.1~10.62.255.254
一卡通认证中心	222.222.0.0/16	222.222.0.1~222.222.255.254
MLC 内部业务路由		

须配置相关路由策略控制线路之间的互通访问，网络通信安全须遵循如下配置原则：

a) 动态路由协议开启之后须建立邻居认证机制；
b) 核心设备须配置物理地址绑定等认证策略；
c) 其他点对点链路宜配置 ARP 保护机制等；
d) 设备的相关密码须以密文形式呈现，如 enable、登陆密码等。

5.1.7 网络管理系统技术要求

5.1.7.1 网络管理系统功能

网络管理系统功能要求如下：

a) 故障监视功能：故障报警，故障信息管理等
b) 日志管理功能：日志收集，日志信息管理等
c) 性能监视功能：性能可视化，阈值控制，性能主动检测等
d) 网络测试功能：可达性测试、功能性测试等
e) 故障分析功能：故障可追溯、故障可分类等
f) 系统评价功能：硬件设备可评价、网络性能可评价等
g) 网络批量管理：在网设备批量升级、批量备份，批量转移等
h) 拓扑管理功能：自动拓扑发现，拓扑震荡告警，拓扑迁移备份

i） 链路监视功能：链路状态、带宽利用率及其它性能参数等
j） 端口监视功能：端口状态、端口类型、端口速率等

5.1.7.2 网络管理协议

网络管理协议要求如下：
a） 通用管理协议：SNMPv2c，SNMPv3 ，RMON 等
b） 流量分析协议：netflow 或 Sflow 等
c） 可用性管理协议：ICMP，WEB、Telnet
d） 日志管理协议：Syslog

5.1.8 扩展性要求

基于 AFC 新业务的发展，整体网络须具备扩展性要求如下：
a） 接入能力：满足轨指中心和线路侧的接入接口数量要求
b） 处理能力：满足新业务的业务处理能力，避免网络瓶颈
c） 带宽能力：满足新业务的带宽需求，支持 QoS 相关功能

5.2 网络设备硬件要求

5.2.1 外联交换机

外联交换机硬件要求如下：
a） 单板支持不少于 24 个千兆光口或 24 个千兆电口
b） 交换机采用模块化结构，扩展方便，扩展率不低于 40%
c） 支持不少于两路冗余供电
d） 单台交换机 MTBF≥8 年
e） 支持高可用性的常规技术，VRRP 或集群堆叠等类似技术
f） 应具备三层网络功能且包转发率≥2000Mpps
g） MAC 地址表大小≥64k 项
h） 支持 256 个并发 VLAN
i） 交换机支持链路层邻居发现协议
j） 支持端口隔离技术
k） 支持 BFD 或 NQA 或 SLA 或同等链路快速检测及收敛技术
l） 支持 STP/RSTP/MSTP 多种生成树协议、动态/静态链路聚合
m） 支持多种路由协议，如静态路由、OSPF 等
n） 支持通过 Web 界面、命令行（Console、Telnet、SSH）对设备进行管理
o） 支持 SNMP 网管协议，支持 netflow 或 Sflow 技术对流量进行监控
p） 支持端口镜像且应不少于两组端口镜像功能

5.2.2 防火墙

防火墙硬件要求如下：
a） 吞吐量 ≥10Gbit/s 最大并发≥8000000 条，每秒新建数≥300000 个
b） 固定接口数量不低于 8 个千兆电口和 4 个千兆光口
c） 支持不少于两路冗余供电，输入电压交流 220V
d） 在识别业务应用的基础上，可管理每 IP 使用的带宽，确保关键业务

e) 支持管控方式：限制最大带宽或保障最小带宽、应用的策略路由、修改应用转发优先级等
f) 支持可基于业务访问地址和内容进行审计、溯源
g) 支持服务器负载均衡和链路负载均衡
h) 支持多种路由协议，如静态路由、OSPF 等
i) 支持双机热备的工作模式，能够检测链路状态并实现自动主备切换
j) 支持通过 Web 界面、命令行（Console、Telnet、SSH）对设备进行管理
k) 支持 SNMP 网管协议，支持 netflow 或 Sflow 技术对流量进行监控

5.2.3 内联交换机

内联交换机硬件要求如下：
a) 单板支持不少于 24 个千兆光口或 24 个千兆电口
b) 交换机采用模块化结构，扩展方便，扩展率不低于 40%
c) 支持不少于两路冗余供电
d) 单台交换机 MTBF≥8 年
e) 支持高可用性的常规技术，VRRP 或集群堆叠等类似技术
f) 应具备三层网络功能且包转发率≥2000Mpps
g) MAC 地址表大小≥64k 项
h) 支持 256 个并发 VLAN
i) 交换机支持链路层邻居发现协议
j) 支持端口隔离技术
k) 支持 BFD 或 NQA 或 SLA 或同等链路快速检测及收敛技术
l) 支持 STP/RSTP/MSTP 多种生成树协议、动态/静态链路聚合
m) 支持多种路由协议，如静态路由、OSPF 等
n) 支持通过 Web 界面、命令行（Console、Telnet、SSH）对设备进行管理
o) 支持 SNMP 网管协议，支持 netflow 或 Sflow 技术对流量进行监控
p) 支持端口镜像且应不少于两组端口镜像功能

5.2.4 网络安全设备

网络安全设备硬件要求如下：
a) 固定接口数不少于 4 个千兆电口和 2 个光电复用口
b) 支持流量模型自学习
c) 支持检测应用层 DDoS 攻击：HTTP Flood、HTTPS Flood、DNS Flood、SIP Flood
d) 支持检测多种单包攻击，扫描类攻击：IP 地址扫描、端口扫描
e) 畸形报文类攻击： LAND 攻击、Smurf 攻击、Fraggle 攻击、WinNuke、Ping of Death、Tear Drop、IP 分片报文检测、TCP 标记合法性检查
f) 特殊报文控制类攻击：超大 ICMP 报文控制、ICMP 不可达报文控制、ICMP 重定向报文的控制、Tracert、源站选路选项 IP 报文控制、路由记录选项 IP 报文控制、时间戳选项 IP 报文控制
g) 基于特征库防御蠕虫、木马、僵尸网络、跨站攻击、SQL 注入等常见攻击，同时还支持自定义签名应对突发攻击
h) 支持特征库在线、离线升级功能
i) 支持通过 Web 界面、命令行（Console、Telnet、SSH）对设备进行管理
j) 支持 SNMP 网管协议，netflow 等流监控协议

5.3 网络配置协议要求

5.3.1 设备命名标准

为保证设备在配置时及后续运维中方便识别，设备名称须具有统一规范性，须含有设备简要说明缩写，包括运营企业MLC，主备中心等，如图 2所示：

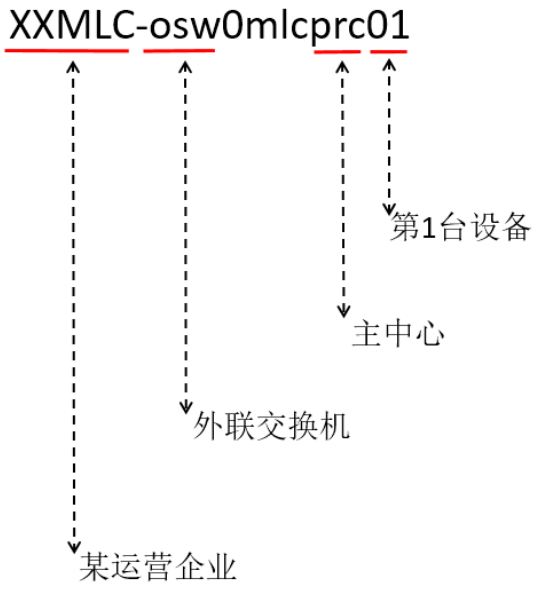

图 2 设备命名规则

实例1：

a) 京港地铁 MLC 主中心外联主交换机 01：JGMLC-osw0mlcprc01
b) JGMLC：京港地铁 MLC
c) OSW：外联交换机
d) prc01：主中心交换机 01
e) 描述说明：京港地铁 MLC 主中心外联主交换机 01

5.3.2 接口描述标准

须配置接口描述信息，为后续运维工作提供重要指导意义，接口描述应包含上（下）互联的设备信息，开启（关闭）时间，设备接口等，如图 3所示：

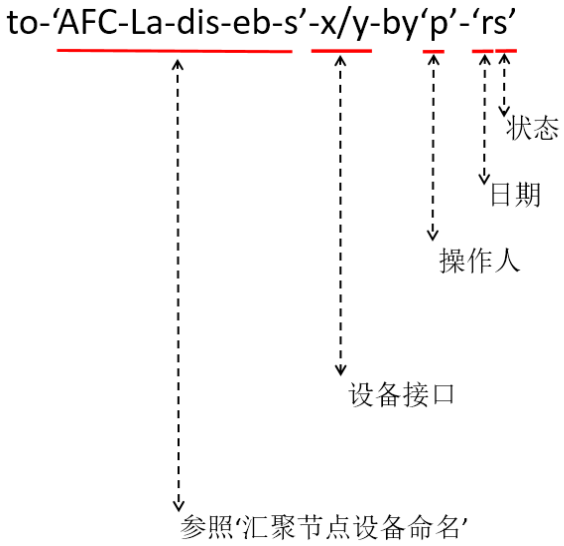

图 3 接口描述规则

实例1：与小营中心的1号线汇聚节点主路由器的互联口

to-‘AFC-L1-dis-RTM-XY’-G0/0/1-by‘zhangsan’-‘20180229up’

描述说明：与小营中心的1号线汇聚节点主路由器的G0/0/1接口，于2018年2月29日由张三开启

5.3.3 IP 地址使用标准

IP地址使用要求如下：

a) 点对点链路应以节约 IP 地址为原则，使用/30 为地址作为互联
b) 在规范的 IP 地址范围内使用 loopback0 地址作为管理地址掩码为/32 位
c) 上层设备 IP 地址为奇数，下层设备 IP 地址为偶数
d) 禁止使用非规定类的地址，同时禁止通告无用接口地址

5.3.4 用户名及密码权限标准

用户名及密码权限要求如下：

a) 禁止使用类似 admin，root 等用户名
b) 禁止使用长度小于 8 位复杂度单一性的密码
c) 禁止用户名和密码相同
d) 禁止多层设备共用同一组用户名和密码
e) 不同用户名禁止密码相同
f) 避免多人使用同一组账号和密码管理设备
g) 用户权限至少分为管理级和维护级
h) 删除账户，修改权限，修改密码等应作出合理解释后操作

5.3.5 链路层协议配置标准

链路层协议配置要求如下：

a) 须提供全双工链路，不得提供单工链路
b) 须提供不小于 100Mb/S 的网络带宽
c) 链路层技术须可支持向下兼容协议等
d) 链路层须满足高可用性标准

e） 链路层在高可用的前提下须有防环保护机制

5.3.6 网络层协议配置标准

网络层协议配置要求如下：

a） 路由协议选择遵循满足业务，配置不复杂同时易维护的原则
b） 使用动态路由协议时，宜使用 OSPF 协议
c） 避免路由协议间的重分发
d） 使用 metric 来作为优选路由的条件
e） 使用 BFD 或 NQA 或 SLA 或同等链路快速检测及收敛技术
f） 严禁下发和学习类似默认路由和超网路由等非法路由
g） 防火墙优先使用透明模式，同时配置可路由的管理 IP 地址
h） 严禁配置 any-to-any 或等效不安全配置
i） 外联交换机下联到车站接口主备对称
j） 下联接口须做端口描述
k） 交换机网管地址可路由，CLI 可全功能配置
l） 通过 metric 来区分主备链路
m） 应避免次优路径及路由环路
n） ACL、路由前缀列表及 policy 应配置相关说明
o） 外联交换机须配置线路间逻辑隔离的安全配置
p） 网络节点切换时应具备纵向整体切换的功能
q） 网络节点切换时应总体时间小于 30 秒
r） 网络节点须具备自动和手动两种方式切换的模式
s） 入侵防御系统应不少于 1 次/季度进行特征库更新
t） 支持 netflow 或 Sflow 技术对流量进行监控
u） 支持 SNMPv2c 或 v3 标准，使其做到细项化监控
v） 支持并配置 NTP 协议
w） 动态路由协议开启后需建立邻居认证机制

5.3.7 业务白名单配置标准

业务白名单配置要求如下：

a） 先配置允许流量，再配置拒绝所有流量，配置粒度不低于网络层
b） 禁止使用数字类策略，须配置名称且简明易懂

实例 1：进入 MLC 的策略流量配置

```
ip access-list extended mlc-in//扩展访问控制列表‘mlc-in’
permit ip 10.0.0.0 0.0.255.255 any//ACC流量
permit ip 10.61.0.0 0.0.255.255 any//AFC监视中心流量
permit ip 10.62.0.0 0.0.255.255 any//互联网平台流量
permit ip 222.222.0.0 0.0.255.255 any//一卡通流量
deny ip any any//拒绝其他一切流量
```

5.3.8 网络配置管理标准

网络配置管理要求如下：

a) 须配置对应的 RO 权限

b) 须配置 community 字符串复杂度不低于中等

c) 须配置 trap 消息

实例1：

```
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flash insertion removal
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps rf
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
```

5.3.9 其他配置标准

5.3.9.1 设备登录描述

```
banner login ^C
--------------------------------------------------------------------------------
********WARNING*** WARNING*** WARNING*** WARNING *** WARNING*** WARNING********
********************YOU ARE CONNECTED TO THE AFC NETWORK ********************
**Unauthorized access and use of this network will be vigorously prosecuted! **
********************Please contact your authorized partner********************
***************OR If you need help,please call 86-010-84680077***************
********WARNING*** WARNING*** WARNING*** WARNING *** WARNING*** WARNING********
--------------------------------------------------------------------------------
```

在登陆之后须显示登陆告警信息：

“你已经连接至AFC的网络，非法的授权登陆将会被起诉，请联系授权你的伙伴，如需帮助请致电服务电话”

6 线路中心（汇聚节点）层

6.1 网络技术要求

6.1.1 总体要求

基于现有AFC网络结构及业务特点，线路中心（汇聚节点）层位于各线路的车站到其运营公司MLC网络的连接位置，在满足网络流量基础上，应具备链路层和网络层到MLC网络的高可靠性要求。

为满足国家法律法规对网络安全的相关要求，对于AFC系统的网络安全及运营安全的整体要求，制定不低于信息安全等级保护二级的标准。

对AFC网络的整体运行状态增加设备硬件状态信息、接口流量信息等相关采集要求，以达到网络设备可监视，链路状态可监视。

为适应未来新型业务要求及新网络标准，整体网络应具备可扩展能力。

6.1.2 业务说明

6.1.2.1 时钟同步

表 7 时钟同步业务说明

通信协议	NTP 协议
交互数据类型	UDP port 123
概要说明	网络设备时钟须与 TCC 时钟同步
备注	无

6.1.2.2 网络通信业务

表 8 网络通信业务说明

通信协议	TCP/IPv4、TCP/IPv6
交互数据类型	AFC 业务数据、网络监控数据
概要说明	MLC 系统内数据、ACC 认证数据、互联网认证数据、监视中心旁站数据
备注	传输区域无具体 AFC 业务

6.1.3 网络拓扑简图

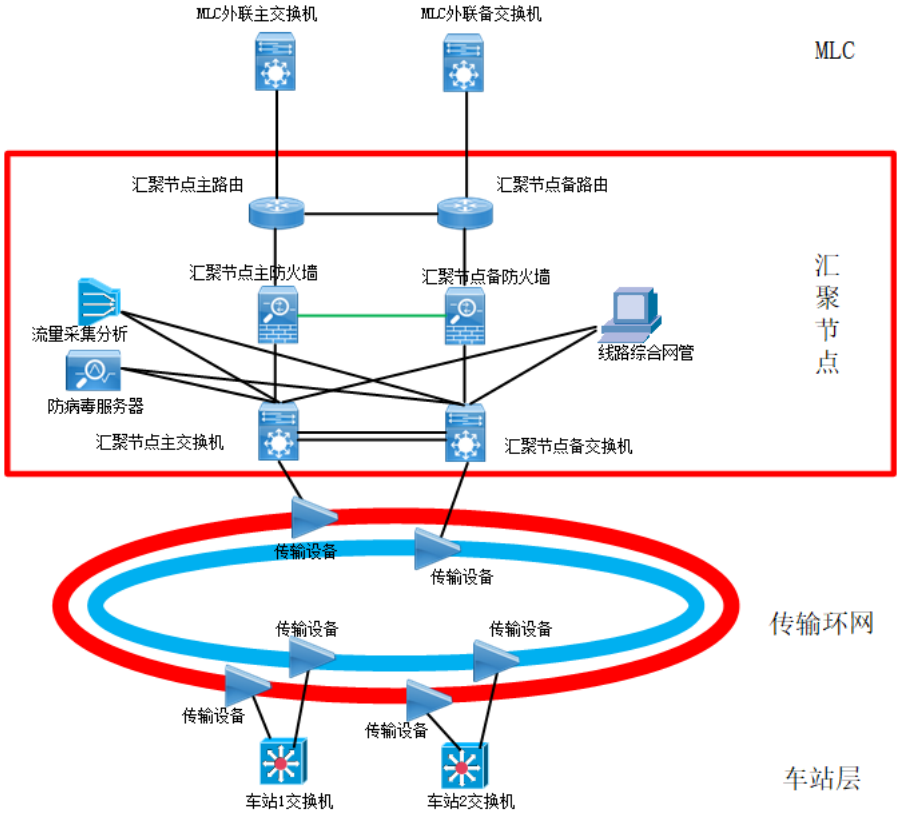

图 4 MLC 网络拓扑简图

6.1.4 网络拓扑简图说明

6.1.4.1 路由器

汇聚节点路由器的网络拓扑要求如下：

a) 须设置汇聚节点主路由器用于与 MLC 外联主交换机网络通信；

b) 须设置汇聚节点备路由器用于与 MLC 外联备交换机网络通信；

c) 汇聚节点主/备路由器之间须配置不少于一条物理链路，同时配置逻辑网络信息，以保证链路的高可用性。

6.1.4.2 防火墙

汇聚节点防火墙的网络拓扑要求如下：

a) 须设置汇聚节点主防火墙用于汇聚节点主路由器与汇聚节点主交换机连接并实施安全策略的作用；

b) 须设置汇聚节点备防火墙用于汇聚节点主路由器与汇聚节点备交换机连接并实施安全策略的作用；

c) 防火墙宜采用“透明模式”部署，须配置带外管理接口；

d) 防火墙与主/备路由器、主/备交换机之间须配置不少于一条物理链路，若连接多条链路时须采用链路绑定技术；

e) 防火墙之间须有“配置同步线”，所有安全策略须保持一致。

6.1.4.3 交换机

汇聚节点交换机的网络拓扑要求如下：

a) 须设置汇聚节点主交换机用于各车站三层交换机通信且为主链路；
b) 须设置汇聚节点备交换机用于各车站三层交换机通信且为备链路；
c) 汇聚节点主/备交换机之间须配置不少于两条物理链路，以保证链路的高可用性。

6.1.4.4 其他网络设备

其他网络设备的网络拓扑要求如下：

a) 须设置相关网络安全产品，如 IPS/IDS、防毒墙等，宜以旁路方式部署，如需以串联方式部署须配置 bypass 功能；
b) 须预留网络流量采集接口，以备后续抓包等操作进行故障分析；
c) 须配置网络管理系统，用于网络监控等。

6.1.5 可靠性要求

可靠性是AFC网络系统能够在规定条件下和规定的时间内完成规定的功能的特性。AFC系统网络的可靠性维度主要有三种：抗毁性、生存性和有效性。

抗毁性是指系统在人为破坏下的可靠性。比如，部分线路或节点失效后，相关网络配置变更错误后，系统应能够提供全部或部分业务。

生存性是指系统在随机破坏下的可靠性，生存性主要反映随机性破坏和网络拓扑结构对系统可靠性的影响，随机性破坏是指系统部件因为自然老化等造成的自然失效。

有效性主要反映在部分链路失效情况下，满足业务性能要求的程度。比如，网络部件失效虽然没有引起连接性故障，但是却造成质量指标下降、平均延时增加、线路阻塞等现象。

AFC网络应具有自愈功能，当出现人力、环境及老化等相关问题后，可以自愈或通过人为干预在最短时间内解决。

基于AFC业务特点，可按照实时性要求及业务重要等级要求确定高可用性参考基线，网络整体运行丢包率应不高于1%，负载率应不高于50%，非破坏性故障自愈延迟应小于180秒。详见表 9：

表 9 高可用性参考基线

网络状态	状态参数自愈时间
完好率=100%	单站双向网络延迟<50ms，丢包率<1%，资源可用率>40% 中心双向网络延迟<20ms，丢包率<1‰，资源可用率>60%
完好率≥50%	单站双向网络延迟<150ms，丢包率<3%，资源可用率>20% 中心双向网络延迟<50ms，丢包率<1‰，资源可用率>50% 自愈时间<30s，自愈状态不低于 75%
完好率≤50%	单站双向网络延迟<250ms，丢包率<5%，资源可用率>10% 中心双向网络延迟<100ms，丢包率<1%，资源可用率>30% 自愈时间<300s，自愈状态不低于 50%

6.1.6 网络安全要求

6.1.6.1 终端安全

终端安全是以终端安全保护系统全方位综合保障终端安全，并以数据安全保护系统重点保护终端敏感数据的安全。终端安全保护系统以“主动防御”理念为基础，采用基于标识的认证技术，以智能控制和安全执行双重体系结构为基础，将全面安全策略与操作系统有机结合，通过对代码、端口、网

络连接、移动存储设备接入、数据文件加密、行为审计分级控制，实现操作系统加固及信息系统的自主、可控、可管理，保障终端系统及数据的安全。

6.1.6.2 数据安全

数据安全保护系统能够实现数据文档的透明加解密保护，可指定类型文件加密、指定程序创建文件加密，杜绝文档泄密。实现数据文档的强制访问控制和统一管理控制、敏感文件及加密密钥的冗余存储备份，包括文件权限管理、用户管理、共享管理、外发管理、备份管理、审计管理等。对各种敏感数据文档，包括设计文档、设计图纸、源代码、用户人员账号信息、财务报表及其他各种涉及商业秘密的文档，都能实现稳妥有效的保护。

6.1.6.3 网络通信安全

本标准只涉及网络通信安全，须在网络设备上对已知业务和业务网段需求启动白名单机制，控制粒度不低于网络级，如可使用访问控制列表，策略路由，源地址检测等相关安全手段及技术，对汇聚节点侧增加访问控制策略，所涉及的业务网段详见表 10：

表 10 业务网段列表

涉及业务	IP 网段	IP 地址范围
AFC 清分清算中心	10.0.0.0/16	10.0.0.1~10.0.255.254
AFC 监视中心	10.61.0.0/16	10.61.0.1~10.61.255.254
互联网平台	10.62.0.0/16	10.62.0.1~10.62.255.254
一卡通认证中心	222.222.0.0/16	222.222.0.1~222.222.255.254
MLC 内部业务路由		

须配置相关路由策略控制线路之间的互通访问，网络通信安全须遵循如下配置原则：

a) 动态路由协议开启之后须建立邻居认证机制；
b) 核心设备须配置物理地址绑定等认证策略；
c) 其他点对点链路宜配置 ARP 保护机制等；
d) 设备的相关密码须以密文形式呈现，如 enable、登陆密码等。

6.1.7 网络管理系统技术要求

6.1.7.1 网络管理系统功能

网络管理系统功能要求如下：

a) 故障监视功能：故障报警，故障信息管理等
b) 日志管理功能：日志收集，日志信息管理等
c) 性能监视功能：性能可视化，阈值控制，性能主动检测等
d) 网络测试功能：可达性测试、功能性测试等
e) 故障分析功能：故障可追溯、故障可分类等
f) 系统评价功能：硬件设备可评价、网络性能可评价等
g) 网络批量管理：在网设备批量升级、批量备份，批量转移等
h) 拓扑管理功能：自动拓扑发现，拓扑震荡告警，拓扑迁移备份
i) 链路监视功能：链路状态、带宽利用率及其它性能参数等
j) 端口监视功能：端口状态、端口类型、端口速率等

6.1.7.2 网络管理协议

网络管理协议要求如下：

a) 通用管理协议：SNMPv2c，SNMPv3 ，RMON 等
b) 流量分析协议：netflow 或 Sflow 等
c) 可用性管理协议：ICMP，WEB、Telnet
d) 日志管理协议：Syslog

6.1.8 扩展性要求

基于 AFC 新业务的发展，整体网络须具备扩展性要求如下：

a) 接入能力：满足轨指中心和线路侧的接入接口数量要求
b) 处理能力：满足新业务的业务处理能力，避免网络瓶颈
c) 带宽能力：满足新业务的带宽需求，支持 QoS 相关功能

6.2 网络设备硬件要求

6.2.1 路由器

路由器硬件要求如下：

a) 包转发性能≥3Mpps
b) 支持 4 个千兆光口，4 个千兆电口
c) 支持不少于两路冗余供电
d) 自带 WAN 口≥3*GE
e) 整机可扩展插槽数，板卡及模块热拔插
f) 可靠性支持 VRRP，BFD 等协议
g) 支持多种路由协议，如静态路由、OSPF 等
h) 支持 QoS 等相关流量标示及流量控制的技术
i) 支持本地或远端认证及授权
j) 配置支持命令行（Console、Telnet、SSH）对设备全部功能进行管理
k) 支持 SNMP 网管协议，支持 netflow 或 Sflow 技术对流量进行监控
l) 宜支持 Web 界面简单管理功能

6.2.2 防火墙

防火墙硬件要求如下：

a) 吞吐量 ≥10Gbit/s 最大并发≥600000 条，每秒新建数≥150000 个
b) 支持 4 个千兆电口和 4 个千兆光口
c) 支持不少于两路冗余供电
d) 在识别业务应用的基础上，可管理每 IP 使用的带宽,确保关键业务
e) 支持管控方式：限制最大带宽或保障最小带宽、应用的策略路由、修改应用转发优先级等
f) 支持可基于业务访问地址和内容进行审计、溯源
g) 支持链路负载均衡技术
h) 支持多种路由协议，如静态路由、OSPF 等
i) 支持双机热备的工作模式，能够检测链路状态并实现自动主备切换
j) 支持通过 Web 界面、命令行（Console、Telnet、SSH）对设备进行管理
k) 支持 SNMP 网管协议，支持 netflow 或 Sflow 技术对流量进行监控

6.2.3 交换机

交换机硬件要求如下：

a) 支持 12 个千兆光口，24 个千兆电口
b) 交换机采用模块化结构，扩展方便，扩展率不低于 40%
c) 支持不少于两路冗余供电
d) 单台交换机 MTBF≥8 年
e) 支持高可用性的常规技术，VRRP 或集群堆叠等类似技术
f) 应具备三层网络功能且包转发率≥80Mpps
g) MAC 地址表大小≥16k 项
h) 支持 256 个并发 VLAN
i) 交换机支持链路层邻居发现协议
j) 支持端口隔离技术
k) 支持 BFD 或 NQA 或 SLA 或同等链路快速检测及收敛技术
l) 支持 STP/RSTP/MSTP 多种生成树协议、动态/静态链路聚合
m) 支持多种路由协议，如静态路由、OSPF 等
n) 支持通过 Web 界面、命令行（Console、Telnet、SSH）对设备进行管理
o) 支持 SNMP 网管协议，支持 netflow 或 Sflow 技术对流量进行监控
p) 支持端口镜像且应不少于两组端口镜像功能

6.2.4 网络安全设备

网络安全设备硬件要求如下：

a) 固定接口数不少于 4 个千兆电口和 2 个光电复用口
b) 支持流量模型自学习
c) 支持检测应用层 DDoS 攻击：HTTP Flood、HTTPS Flood、DNS Flood、SIP Flood
d) 支持检测多种单包攻击，扫描类攻击：IP 地址扫描、端口扫描
e) 畸形报文类攻击： LAND 攻击、Smurf 攻击、Fraggle 攻击、WinNuke、Ping of Death、Tear Drop、IP 分片报文检测、TCP 标记合法性检查
f) 特殊报文控制类攻击：超大 ICMP 报文控制、ICMP 不可达报文控制、ICMP 重定向报文的控制、Tracert、源站选路选项 IP 报文控制、路由记录选项 IP 报文控制、时间戳选项 IP 报文控制
g) 基于特征库防御蠕虫、木马、僵尸网络、跨站攻击、SQL 注入等常见攻击，同时还支持自定义签名应对突发攻击
h) 支持特征库在线、离线升级功能
i) 支持通过 Web 界面、命令行（Console、Telnet、SSH）对设备进行管理
j) 支持 SNMP 网管协议，netflow 等流监控协议

6.3 网络配置协议要求

6.3.1 设备命名标准

为保证设备在配置时及后续运维中方便识别，设备名称须具有统一规范性，须含有所属线路缩写，设备名称缩写，主备关系缩写、位置等，如图 5所示：

图 5 设备命名规则

注：a 可选范围：1-99

b 可选范围：M/B

cd 可选范围：BT/CP/DX/FS/JC/S1/XJ/YF/YZ

e 可选范围：RT/SW/FW/IDS/IPS

s 可选范围：XY/XZM/xxCLD

实例 1：汇聚节点主路由器　AFC-L1-dis-RTM-XY

AFC：AFC 网络

L1:代表 1 号线

dis：汇聚节点

RTM：主路由器

XY：小营中心

描述说明：AFC 网络在小营中心的 1 号线汇聚节点主路由器

实例 2：汇聚节点主路由器　AFC-L1-dis-SWM-sihuiCLD

AFC：AFC 网络

L1:代表 1 号线

dis：汇聚节点

SWM：主交换机

sihuiCLD：四惠车辆段

描述说明：AFC 网络在四惠车辆段的 1 号线汇聚节点主交换机

6.3.2　接口描述标准

须配置接口描述信息，为后续运维工作提供重要指导意义，接口描述应包含上（下）互联的设备信息，开启（关闭）时间，设备接口等，如图 6所示：

图 6 接口描述规则

实例1：与京港地铁MLC主中心外联交换机1的互联口

to-‘JGMLC-osw0mlcprc01’-G0/0/1-by‘zhangsan’-‘20180229up’

描述说明：与京港地铁MLC主中心外联交换机1的G0/0/1接口，于2018年2月29日由张三开启

6.3.3 IP 地址使用标准

IP地址使用要求如下：

a) 点对点链路应以节约 IP 地址为原则，使用/30 为地址作为互联
b) 在规范的 IP 地址范围内使用 loopback0 地址作为管理地址掩码为/32 位
c) 上层设备 IP 地址为奇数，下层设备 IP 地址为偶数
d) 禁止使用非规定类的地址，同时禁止通告无用接口地址

6.3.4 用户名及密码权限标准

用户名及密码权限要求如下：

a) 禁止使用类似 admin，root 等用户名
b) 禁止使用长度小于 8 位复杂度单一性的密码
c) 禁止用户名和密码相同
d) 禁止多层设备共用同一组用户名和密码
e) 不同用户名禁止密码相同
f) 避免多人使用同一组账号和密码管理设备
g) 用户权限至少分为管理级和维护级
h) 删除账户，修改权限，修改密码等应作出合理解释后操作

6.3.5 链路层协议配置标准

链路层协议配置要求如下：

a) 须提供全双工链路，不得提供单工链路

b) 须提供不小于 100Mb/S 的网络带宽
c) 链路层须满足高可用性标准
d) 链路层在高可用的前提下须有防环保护机制

6.3.6 网络层协议配置标准

网络层协议配置要求如下：
a) 路由协议选择遵循满足业务，配置不复杂同时易维护的原则
b) 使用动态路由协议时，宜使用 OSPF 协议
c) 避免路由协议间的重分发
d) 使用 metric 或 cost 来作为优选路由的条件
e) 使用 BFD 或 NQA 或 SLA 或同等链路快速检测及收敛技术
f) 严禁下发和学习类似默认路由和超网路由等非法路由
g) 防火墙优先使用透明模式，同时配置可路由的管理 IP 地址
h) 严禁配置 any-to-any 或等效不安全配置
i) 汇聚交换机下联到车站接口主备对称
j) 下联接口须做端口描述
k) 汇聚交换机间应做链路聚合
l) 汇聚交换机网管地址可路由，CLI 可全功能配置
m) 须避免次优路径及路由环路
n) ACL、路由前缀列表及 policy 应配置相关说明
o) 汇聚节点须配置站间逻辑隔离的安全配置
p) 汇聚节点切换时应优先横向同层切换的原则
q) 汇聚节点切换时应具备纵向整体切换的功能
r) 汇聚节点切换时应总体时间小于 30 秒
s) 汇聚节点须具备自动和手动两种方式切换的模式
t) 入侵防御系统应不少于 1 次/季度进行特征库更新
u) 支持 netflow 或 Sflow 技术对流量进行监控
v) 支持 SNMPv2c 或 v3 标准，使其做到细项化监控
w) 支持并配置 NTP 协议
x) 动态路由协议开启后需建立邻居认证机制

6.3.7 业务白名单配置标准

业务白名单配置要求如下：
a) 先配置允许流量，再配置拒绝所有流量，配置粒度不低于网络层
b) 禁止使用数字类策略，须配置名称且简明易懂
实例 1：进入 MLC 的策略流量配置

```
ip access-list extended mlc-in //扩展访问控制列表‘mlc-in’
   permit ip 10.0.0.0 0.0.255.255 any          //ACC 流量
   permit ip 10.61.0.0 0.0.255.255 any     //AFC 监视中心流量
   permit ip 10.62.0.0 0.0.255.255 any     //互联网平台流量
   permit ip 222.222.0.0 0.0.255.255 any       //一卡通流量
   deny ip any any                          //拒绝其他一切流量
```

6.3.8 网络配置管理标准

网络配置管理要求如下：

a) 须配置对应的 RO 权限

b) 须配置 community 字符串复杂度不低于中等

c) 须配置 trap 消息

实例 1：

```
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flash insertion removal
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps rf
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
```

6.3.9 其他配置标准

6.3.9.1 设备登录描述

```
banner login ^C
--------------------------------------------------------------------------------
********WARNING*** WARNING*** WARNING*** WARNING *** WARNING*** WARNING********
**********************YOU ARE CONNECTED TO THE AFC NETWORK **********************
**Unauthorized access and use of this network will be vigorously prosecuted! **
**********************Please contact your authorized partner**********************
****************OR If you need help,please call 86-010-84680077****************
********WARNING*** WARNING*** WARNING*** WARNING *** WARNING*** WARNING********
--------------------------------------------------------------------------------
```

在登陆之后须显示登陆告警信息：

“你已经连接至AFC的网络，非法的授权登陆将会被起诉，请联系授权你的伙伴，如需帮助请致电服务电话”

7 车站（SC）层

7.1 网络技术要求

7.1.1 总体要求

基于现有AFC网络结构及业务特点，车站（SC）层位于AFC网络系统的末节区域，是连接AFC终端设备，SC服务器及汇聚节点的重要组成部分，在满足各运营公司SC自身业务的基础上，应具备链路层和网络层到上位线路汇聚节点的高可靠性要求。

为满足国家法律法规对网络安全的相关要求，对于AFC系统的网络安全及运营安全的整体要求，制定不低于信息安全等级保护二级的标准。

对AFC网络的整体运行状态增加设备硬件状态信息、接口流量信息等相关采集要求，以达到网络设备可监视，链路状态可监视。

为保证未来新型业务要求及新网络标准，整体网络应具备可扩展能力

7.1.2 业务说明

7.1.2.1 在线文件传输

表 11 在线文件传输业务说明

通信协议	FTP 协议
交互数据类型	参数数据、程序文件、日志文件
概要说明	上位下发文件到指定目录
	下位上传文件到指定目录
业务特点	非实时性业务，次要级
备注	现阶段使用 FTP 为不安全链接，应采用 SFTP 或对文件进行压缩加密等

7.1.2.2 在线数据传输

表 12 在线数据传输业务说明

通信协议	基于 TCP/IP 的 TCP 或者 UDP 协议
交互数据类型	交易数据、状态数据、控制数据、业务数据、参数版本、开机/断线续连、业务结束
概要说明	实时性业务，重要级
业务特点	上位与下位的数据业务
备注	无

7.1.2.3 时钟同步

表 13 在线文件传输业务说明

通信协议	NTP 协议
交互数据类型	时钟同步
概要说明	与上位 MLC 进行时钟同步（客户端）; 与下位 SLE 进行时钟同步（服务端）;
业务特点	实时性业务，一般级
备注	无

7.1.2.4 网络通信业务

表 14 在线文件传输业务说明

通信协议	OSI、TCP/IPv4、TCP/IPv6
交互数据类型	AFC 业务数据、网络监控数据
概要说明	MLC 系统内数据、ACC 认证数据、互联网认证数据、监视中心旁站数据
业务特点	实时性业务，重要级
备注	站内终端应仅与站内服务器进行通信； 旁站业务、网络监控业务须与中心进行通信；

7.1.3 网络拓扑简图

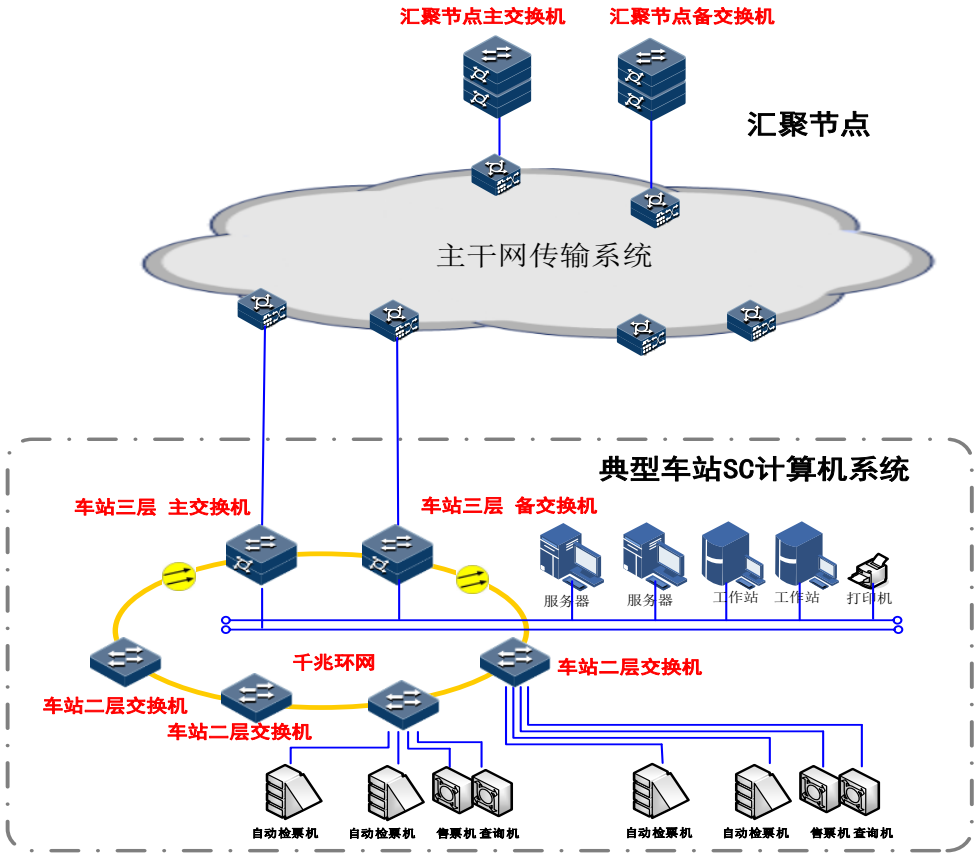

图 7 网络拓扑简图

7.1.4 网络拓扑简图说明

7.1.4.1 三层交换机

三层交换机的网络拓扑要求如下：

a) 须设置三层主交换机用于与各线路汇聚节点的主交换机网络通信，须与车站内 SC 服务器、OBPS-SC 服务器连接，并为工作站、打印机提供接口；

b) 须设置三层备交换机用于与各线路汇聚节点的备交换机网络通信，须预留出与车站内 SC 服务器、OBPS-SC 服务器备用接口；

c) 主/备三层交换机之间须配置不少于两条物理链路，以保证链路的高可用性；

d) 主三层交换机须作为终端的主网关，备三层交换机须作为终端的备网关。

7.1.4.2 二层交换机

二层交换机的网络拓扑要求如下：

a) 须设置二层交换机与三层主/备交换机组成环网，二层交换机用于 SC 各设备接入；

b) 二层交换机须支持任意端口成环，实现千兆环网保护，禁止使用光电转换设备；

c) 须配置二层交换机接口的隔离技术，满足站台系统间业务隔离需要。

7.1.4.3 维修中心、测试培训中心

维修中心、测试培训中心网络拓扑参考车站网络拓扑实现，须设置主/备三层交换机及二层交换机，其他要求均参考车站网络要求。

7.1.5 可靠性要求

可靠性是AFC网络系统能够在规定条件下和规定的时间内完成规定的功能的特性。AFC系统网络的可靠性维度主要有三种：抗毁性、生存性和有效性。

抗毁性是指系统在人为破坏下的可靠性。比如，部分线路或节点失效后，相关网络配置变更错误后，系统应能够提供全部或部分业务。

生存性是指系统在随机破坏下的可靠性，生存性主要反映随机性破坏和网络拓扑结构对系统可靠性的影响，随机性破坏是指系统部件因为自然老化等造成的自然失效。

有效性主要反映在部分链路失效情况下，满足业务性能要求的程度。比如，网络部件失效虽然没有引起连接性故障，但是却造成质量指标下降、平均延时增加、线路阻塞等现象。

AFC网络应具有自愈功能，当出现人力、环境及老化等相关问题后，可以自愈或通过人为干预在最短时间内解决。

基于AFC业务特点，可按照实时性要求及业务重要等级要求确定高可用性参考基线，网络整体运行丢包率应不高于1%，负载率应不高于50%，非破坏性故障自愈延迟应小于180秒。详见表 15：

表 15 高可用性参考基线

网络状态	状态参数自愈时间
完好率=100%	汇聚节点网络延迟<20ms，丢包率<1‰，资源可用率>60% 到达终端网络延时<5ms，丢包率<1‰
完好率≥50%	汇聚节点网络延迟<50ms，丢包率<1‰，资源可用率>50% 到达终端网络延时<5ms，丢包率<1‰ 自愈时间 30s，自愈状态不低于 75%
完好率≤50%	汇聚节点网络延迟<100ms，丢包率<1%，资源可用率>30% 到达终端网络延时<5ms，丢包率<1‰ 自愈时间 300s，自愈状态不低于 50%

注：由于终端上联为单链路，当出现交换机失效后需进行手动切换连接，上述自愈状态参数为网络设备自愈能力。

7.1.6 网络安全要求

7.1.6.1 终端安全

终端安全是以终端安全保护系统全方位综合保障终端安全，并以数据安全保护系统重点保护终端敏感数据的安全。终端安全保护系统以“主动防御”理念为基础，采用基于标识的认证技术，以智能控制和安全执行双重体系结构为基础，将全面安全策略与操作系统有机结合，通过对代码、端口、网络连接、移动存储设备接入、数据文件加密、行为审计分级控制，实现操作系统加固及信息系统的自主、可控、可管理，保障终端系统及数据的安全。

7.1.6.2 数据安全

数据安全保护系统能够实现数据文档的透明加解密保护，可指定类型文件加密、指定程序创建文件加密，杜绝文档泄密。实现数据文档的强制访问控制和统一管理控制、敏感文件及加密密钥的冗余存储备份，包括文件权限管理、用户管理、共享管理、外发管理、备份管理、审计管理等。对各种敏感数据文档，包括设计文档、设计图纸、源代码、用户人员账号信息、财务报表及其他各种涉及商业秘密的文档，都能实现稳妥有效的保护。

7.1.6.3 网络通信安全

本标准只涉及网络通信安全，须在网络设备上对已知业务和业务网段需求启动白名单机制，控制粒度不低于网络级，如可使用访问控制列表，策略路由，源地址检测等相关安全手段及技术，对汇聚节点侧增加访问控制策略，所涉及的业务网段详见表16：

表 16 业务网段列表

涉及业务	IP 网段	IP 地址范围
AFC 清分清算中心	10.0.0.0/16	10.0.0.1~10.0.255.254
AFC 监视中心	10.61.0.0/16	10.61.0.1~10.61.255.254
互联网平台	10.62.0.0/16	10.62.0.1~10.62.255.254
一卡通认证中心	222.222.0.0/16	222.222.0.1~222.222.255.254
MLC 内部业务路由		

须配置相关路由策略控制线路之间的互通访问，网络通信安全须遵循如下配置原则：

a) 核心设备须配置物理地址绑定等认证策略；
b) 其他点对点链路宜配置 ARP 保护机制等；
c) 设备的相关密码须以密文形式呈现，如 enable、登陆密码等。

7.1.7 网络管理系统技术要求

7.1.7.1 网络管理系统功能

网络管理系统功能要求如下：

a) 故障监视功能：故障报警，故障信息管理等
b) 日志管理功能：日志收集，日志信息管理等
c) 性能监视功能：性能可视化，阈值控制，性能主动检测等
d) 网络测试功能：可达性测试、功能性测试等
e) 故障分析功能：故障可追溯、故障可分类等
f) 系统评价功能：硬件设备可评价、网络性能可评价等
g) 网络批量管理：在网设备批量升级、批量备份，批量转移等
h) 拓扑管理功能：自动拓扑发现，拓扑震荡告警，拓扑迁移备份
i) 链路监视功能：链路状态、带宽利用率及其它性能参数等
j) 端口监视功能：端口状态、端口类型、端口速率等

7.1.7.2 网络管理协议

网络管理协议要求如下：

a) 通用管理协议：SNMPv2c，SNMPv3 ，RMON 等
b) 流量分析协议：支持流量监控技术、支持流量监控结果输出
c) 可用性管理协议：ICMP，WEB、Telnet
d) 日志管理协议：Syslog

7.1.8 扩展性要求

基于 AFC 新业务的发展，整体网络须具备扩展性要求如下：

a) 接入能力：满足轨指中心和线路侧的接入接口数量要求
b) 处理能力：满足新业务的业务处理能力，避免网络瓶颈
c) 带宽能力：满足新业务的带宽需求，支持 QoS 相关功能

7.2 网络设备硬件要求

7.2.1 三层交换机

三层交换机硬件要求如下：

a) 单台设备端口数量不少于：4 个千兆 SFP 光口（配置单模光模块），20 个千兆电口
b) 交换容量≥24Gbps
c) 支持不少于两路冗余供电，输入电压交流 220V
d) 单台交换机 MTBF≥8 年
e) 机架式安装，全金属外壳，无风扇散热设计，IP30 防护
f) 工作温度：-40℃~+75℃
g) 支持高可用性的常规技术，VRRP 或集群堆叠等类似技术
h) 应具备三层网络功能且包转发率≥30Mpps
i) MAC 地址表大小≥8k 项
j) 支持 256 个并发 VLAN
k) 交换机支持 LLDP(链路层发现协议)，支持拓扑自动发现
l) 支持端口隔离技术
m) 支持 BFD 或 NQA 或 SLA 或同等链路快速检测及收敛技术
n) 支持环网协议，自愈时间小于 1s，支持任意端口成环
o) 支持人工选择环网阻塞端口可自定义配置及修改
p) 支持 STP/RSTP/MSTP 多种生成树协议、动态/静态链路聚合
q) 支持多种路由协议，如静态路由、OSPF 等
r) 支持 WEB、CLI、telnet、SSH、Console、RMON、支持 SNMP v1/v2c/v3 等多种系统管理方式
s) 支持流量监控技术、支持流量监控结果输出
t) 支持多对一的端口镜像，支持端口输入和输出的分别镜像
u) 支持端口环路检测功能，发现环路时，自动关闭端口，当环路解除时自动恢复端口
v) 提供 CE、FCC、UL61010 等安全认证证明文件

7.2.2 二层交换机（导轨）

二层交换机（导轨）硬件要求如下：

a) 单台设备端口数量不少于：2 个千兆 SFP 光口（配置单模光模块），8 个千兆电口
b) 交换机电源要求采用交直流自适应 220V 电源，可以通过电源转换装置实现
c) 交换机须满足车站现场的要求：二层交换机采用导轨安装；导轨交换机安装在终端设备内，满足牢固、抗震要求，一体化设计、无风扇散热
d) 交换容量≥12Gbps
e) 应配置至少 2 个千兆单模 SFP 模块，传输距离不小于 2KM
f) 单台交换机 MTBF≥8 年
g) 全金属外壳，无风扇散热设计，IP30 防护
h) 工作温度：-40℃~+75℃
i) MAC 地址表大小≥8k 项
j) 支持 256 个并发 VLAN
k) 交换机支持 LLDP(链路层发现协议)，支持拓扑自动发现
l) 支持端口隔离技术
m) 支持 STP/RSTP/MSTP 多种生成树协议、动态/静态链路聚合
n) 支持多对一的端口镜像，支持端口输入和输出的分别镜像
o) 支持端口环路检测功能，发现环路时，自动关闭端口，当环路解除时，自动恢复端口
p) 支持 WEB、CLI、telnet、SSH、Console、RMON、支持 SNMP v1/v2c/v3 等多种系统管理方式
q) 支持环网协议，自愈时间小于 1s，支持任意端口成环
r) 支持 IP 地址配置及用于网管的静态路由配置
s) 支持人工选择环网阻塞端口可自定义配置及修改
t) 提供 CE、FCC、UL61010 等安全认证证明文件

7.2.3 二层交换机（非导轨）

二层交换机（非导轨）硬件要求如下：
a) 单台设备端口数量不少于：2 个千兆 SFP 光口（配置单模光模块），8 个千兆电口
b) 交换机电源要求采用交直流自适应 220V 电源，可以通过电源转换装置实现
c) 交换容量≥12Gbps
d) 应配置至少 2 个千兆单模 SFP 模块，传输距离不小于 2KM
e) 单台交换机 MTBF≥8 年
f) 全金属外壳，无风扇散热设计，IP30 防护
g) 工作温度：-40℃~+75℃
h) MAC 地址表大小≥8k 项
i) 支持 256 个并发 VLAN
j) 交换机支持 LLDP(链路层发现协议)，支持拓扑自动发现
k) 支持端口隔离技术
l) 支持 STP/RSTP/MSTP 多种生成树协议、动态/静态链路聚合
m) 支持多对一的端口镜像，支持端口输入和输出的分别镜像
n) 支持端口环路检测功能，发现环路时，自动关闭端口，当环路解除时，自动恢复端口
o) 支持 WEB、CLI、telnet、SSH、Console、RMON、支持 SNMP v1/v2c/v3 等多种系统管理方式
p) 支持环网协议，自愈时间小于 1s，支持任意端口成环
q) 支持 IP 地址配置及用于网管的静态路由配置
r) 支持人工选择环网阻塞端口可自定义配置及修改
s) 提供 CE、FCC、UL61010 等安全认证证明文件

7.3 网络配置协议要求

7.3.1 设备命名标准

为保证设备在配置时及后续运维中方便识别，设备名称须具有统一规范性，须含有所属线路、车站，设备名称，主备关系等，如图 8所示：

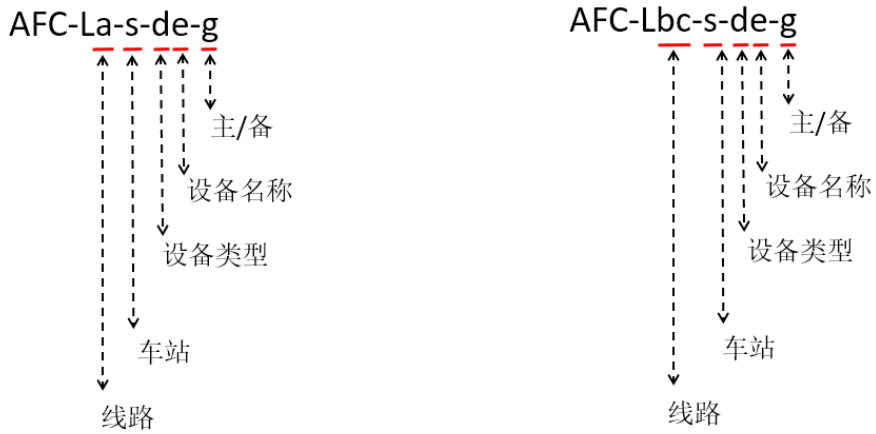

图 8 设备命名规则

注：a 可选范围：1-99

bc 可选范围：BT/CP/DX/FS/JC/S1/XJ/YF/YZ

d 可选范围：L3/L2

e 可选范围：SW

g 可选范围：M/B

s ：车站名称首字母（大写）

实例 1：1 号线四惠车站三层主交换机　AFC-L1-SH-L3SWM

L1：代表 1 号线

SH：代表四惠车站

L3SWM：代表三层主交换机

描述说明：1 号线四惠车站三层主交换机

7.3.2 接口描述标准

须配置接口描述信息，为后续运维工作提供重要指导意义，接口描述应包含上（下）互联的设备信息，开启（关闭）时间，链路接口等。命名规则，如图 9所示：

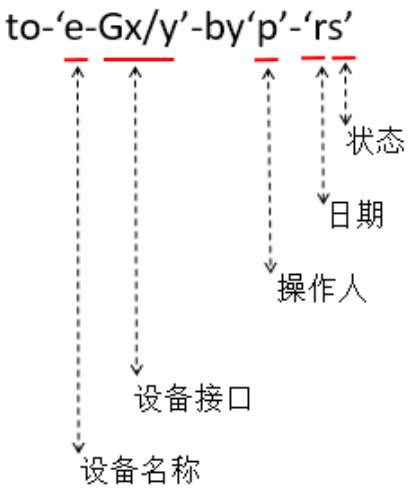

图 9 设备命名规则

实例1：三层交换机下连接SC服务器链路：
to-‘SC-ETH0’-by‘zhangsan’-‘20180229up’
描述说明：连接本车站SC服务器的ETH0接口，于2018年2月29日由张三开启
实例2：三层交换机下连接二层接入交换：
to-‘L2SW01-G0/1’-by‘zhangsan’-‘20180229up’
描述说明：连接本车站二层接入交换机01的G0/1接口，于2018年2月29日由张三开启

7.3.3 IP 地址使用标准

IP地址使用要求如下：

a) 点对点链路应以节约 IP 地址为原则，使用/30 为地址作为互联
b) 在规范的 IP 地址范围内使用 loopback0 地址作为管理地址掩码为/32 位
c) 上层设备 IP 地址为奇数，下层设备 IP 地址为偶数
d) 禁止使用非规定类的地址，同时禁止通告无用接口地址

7.3.4 用户名及密码权限标准

用户名及密码权限要求如下：

a) 禁止使用类似 admin，root 等用户名
b) 禁止使用长度小于 8 位复杂度单一性的密码
c) 禁止用户名和密码相同
d) 禁止多层设备共用同一组用户名和密码
e) 不同用户名禁止密码相同
f) 避免多人使用同一组账号和密码管理设备
g) 用户权限至少分为管理级和维护级
h) 删除账户，修改权限，修改密码等应作出合理解释后操作

7.3.5 链路层协议配置标准

链路层协议配置要求如下：

a) 须提供全双工链路，不得提供单工链路
b) 须提供不小于 100Mb/S 的网络带宽
c) 不宜使用光电转换设备
d) 应启用环网协议，以满足链路秒级快速收敛
e) 链路层技术须可支持向下兼容协议等

7.3.6 网络层协议配置标准

网络层协议配置要求如下：
a) 路由协议选择遵循满足业务，配置不复杂同时易维护的原则
b) 如三层交换机使用动态路由协议，宜使用 OSPF 协议
c) 二层交换机使用静态路由或默认网关，用于网管流量
d) 使用 metric 来作为优选路由的条件
e) 支持 BFD 或 NQA 或 SLA 或同等链路快速检测及收敛技术
f) 严禁配置默认路由及超网路由
g) 严禁配置 any-to-any 或等效不安全配置
h) 三层及二层交换机网管地址可路由
i) 通过 metric 来区分主备链路
j) 应避免次优路径及二层环路
k) 支持 netflow 或 Sflow 技术对流量进行监控
l) 支持 SNMPv2c 或 v3 标准，使其做到细项化监控
m) 支持并配置 NTP 协议
n) 动态路由协议开启后需建立邻居认证机制

7.3.7 业务白名单配置标准

业务白名单配置要求如下：
a) 先配置允许流量，再配置拒绝所有流量，配置粒度不低于网络层
b) 禁止使用数字类策略，须配置名称且简明易懂
实例 1：进入 MLC 的策略流量配置

```
ip access-list extended mlc-in //扩展访问控制列表‘mlc-in’
   permit ip 10.0.0.0 0.0.255.255 any          //ACC 流量
   permit ip 10.61.0.0 0.0.255.255 any     //AFC 监视中心流量
   permit ip 10.62.0.0 0.0.255.255 any     //互联网平台流量
   permit ip 222.222.0.0 0.0.255.255 any       //一卡通流量
   deny ip any any                         //拒绝其他一切流量
```

7.3.8 网络配置管理标准

网络配置管理要求如下：
a) 须配置对应的 RO 权限
b) 须配置 community 字符串复杂度不低于中等
c) 须配置 trap 消息
实例 1：

```
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
```

```
snmp-server enable traps flash insertion removal
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps port-security
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps rf
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
```

7.3.9 其他配置标准

7.3.9.1 设备登录描述

```
banner login ^C
--------------------------------------------------------------------------------
********WARNING*** WARNING*** WARNING*** WARNING *** WARNING*** WARNING********
**********************YOU ARE CONNECTED TO THE AFC NETWORK **********************
**Unauthorized access and use of this network will be vigorously prosecuted! **
**********************Please contact your authorized partner**********************
****************OR If you need help,please call 86-010-84680077*****************
********WARNING*** WARNING*** WARNING*** WARNING *** WARNING*** WARNING********
--------------------------------------------------------------------------------
```

在登陆之后须显示登陆告警信息：

“你已经连接至AFC的网络，非法的授权登陆将会被起诉，请联系授权你的伙伴，如需帮助请致电服务电话”