ICS 13.310
A90

DB33

浙　江　省　地　方　标　准

DB33/T 2016—2018

监狱网络信息系统建设规范

Specifications for prison network information system construction

2018-04-12 发布　　2018-05-12 实施

浙江省质量技术监督局 发布

目　次

前　言

本标准依据 GB/T 1.1—2009《标准化工作导则 第 1 部分：标准的结构和编写》给出的规则起草。

本标准由浙江省监狱管理局提出并归口。

本标准主要起草单位：浙江省监狱管理局、浙江省超维建筑设计院、浙江省第四监狱、浙江省第五监狱、浙江省第六监狱、浙江省乔司监狱、浙江省金华监狱、浙江省长湖监狱。

本标准参与起草单位：新华三技术有限公司。

本标准主要起草人：倪平、包应正、单君、王华海、白哲旭、丁春林、陈沛然、陈明喜、沈学明、董溪亭、袁汝钢。

监狱网络信息系统建设规范

1 范围

本标准规定了监狱网络拓扑结构及主要联网技术、业务子网、基础网络传输标准、网络设备命名规则、网络边界交互及连接技术、网络安全技术、网络运行管理及运维服务管理技术、监狱数据中心技术等内容。

本标准适用于新建、改建、扩建监狱网络信息系统的建设，是监狱网络信息系统设计、实施和验收的基本依据。

监狱中心医院网络信息系统建设可参照本标准执行。

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 20270—2006 信息安全技术 网络基础安全技术要求

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 20272—2006 信息安全技术 操作系统安全技术要求

GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求

GB/T 21028—2007 信息安全技术 服务器安全技术要求

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

SF/T 0012—2017 全国司法行政系统网络平台技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

局域网 local area network

在监狱的地理范围内，将各种计算机，外部设备和数据库等互相联接起来组成的信息通信网络。

3.2

省电子政务外网 provincial electronic government external network

按照要求建设的省电子政务重要公共基础设施，是服务于省级党委、人大、政府、政协、法院和检察院等政务部门，满足其经济调节、市场监管、社会管理和公共服务等方面需要的政务共用网络。

3.3

省政法专网 private network of provincial politics and law committee

省政法部门内部工作专用网络。

3.4

IP专网 ip private network

以IP协议为网络层协议与国际互联网物理隔离的网络。

3.5

虚拟专网网络 virtual private network

在公用网络（互联网）上建立专用网络的技术，帮助远程用户、分支机构建立内部的可信安全连接，主要采用了隧道技术、加解密技术、密钥管理技术和使用者与设备身份认证技术，保证数据的安全传输。

3.6

VPN防火墙 vpn firewall

集成了VPN功能的防火墙，保护网络内部的安全，阻止外部的非法用户或是数据通过防火墙，使只允许授权的数据通过，同时在不安全的互联网上提供一个虚拟专用网络，保证私有数据的安全。

3.7

视联网 video internet

浙江省电子政务视联网，由浙江省人民政府办公厅建设，覆盖省、 市县（区）乡镇 （街道 ）行政机关及县（市、区）以上部门单位，具备视频会议、监控应急指挥等多种功能，实现了一个平台兼容所有视频业务。

4 缩略语

下列缩略语适用于本文件。

3G/4G 第三代移动通信技术/第四代移动通信技术

AC (Wireless Access Point Controller) 无线控制器

AP (Wireless Access Point) 无线访问接入点

ATM (Asynchronous Transfer Mode) 异步传输模式

bps (bits per second) 比特/秒

BW (Band Width) 频带宽度

CLOS以减少交叉点数，实现无阻塞网络

DNS (Domain Name System) 域名系统

G.711/G.723.1/G.729a 国际电信联盟制定的音频编码方式

IP (Internet Protocol) 因特网协议

IPv4/IPv6 (Internet Protocol Version 4/Internet Protocol Version 6) IP协议的版本4号/ IP协议的版本6号

MPLS (Multi-Protocol Label Switching) 多协议标签交换

MSO (Mobile Switching Office) 移动通信交换控制中心

MSTP (Multi-Service Transfer Platform) 基于SDH 的多业务传送平台

MCU (Multi-point Control Unit)视频会议中协调及控制多个终端间的视讯传输

NO.7/Pri (NO.7 Signaling System/Primary Rate Interface) 七号信令系统/基群速率接口

NTP (Network Time Protocol) 网络时间协议

OSPF (Open Shortest Path First) 开放式最短路径优先

PBX (Private Branch Exchange) 电话业务网络用户级交换机

PSTN（Public Switched Telephone Network ）公共交换电话网络
QoS（Quality of Service）服务质量
SONET（Synchronous Optical Network）同步光纤网络
SDH（Synchronous Digital Hierarchy）同步数字体系
SIP（Session Initiation Protocol）会话初始协议
SDN（Software Defined Network）软件定义网络
TDM（Time Division Multiplexing）时分复用模式
VPN（Virtual Private Network）虚拟专用网
VoIP（Voice over Internet Protocol）模拟信号数字化
VXLAN（Virtual Extensible LAN）虚拟可扩展局域网
Wi-Fi（Wireless Fidelity）基于 IEEE 802.11 系列标准的无线网路通信技术

5 网络结构及主要组网技术要求

5.1 总体网络结构

监狱网络信息系统应为监狱机关各类系统及业务应用的承载，主要实现园区内网络互联、服务输出和安全管控等服务，实现省监狱管理局网络组成的基本接入单元和延伸。上行分别通过省级综合业务网及省视联网与省政法专网和省电子政务外网安全对接，实现与省委省政府、省司法厅和省政法机关以及司法部的政(业)务网数据交换与共享，同步依托上行网络实现省政法云和省政务云等云计算服务的落地应用。

5.2 局域网技术要求和分类

5.2.1 基本要求

局域网应为监狱单位园区各类网络的总称，分为局域内网和局域外网。局域内网应为监狱单位内部各类业务应用互联园区网络，其上联出口为省级综合业务网和省视联网；局域外网应为监狱单位为接驳政法系统以外业务应用而互联的园区网络，其上联出口包括省电子政务外网互联网、社会单位业务专网等。

5.2.2 技术要求

5.2.2.1 网络架构要求

5.2.2.1.1 监狱局域网应按功能配置进行区域划分，网络架构遵循模块化分区设计原则，整体网络架构应分为多个相对独立的功能区，包括核心交换区、联网区、服务器(云)区、安防设施区、普通用户区、特别用户区、运维管理区和外网办公区等，服务器(云)区服务器采用云计算模式，网络采用虚拟化技术，具体局域网网络架构见图 1。
5.2.2.1.2 核心交换区：负责监狱园区局域网网络核心架构与安全核心业务。
5.2.2.1.3 联网区：负责接入省级综合业务网、省视联网、省政法专网等政府类网络的边界连接，以及省政法云、省政务云等云平台服务，并负责安全交换外网办公区数据。
5.2.2.1.4 服务器(云)区：负责提供全网各类系统、应用、存储与安全等私有云计算服务。
5.2.2.1.5 安防设施区：负责接入监管安防前端基础设施及终端采集服务。
5.2.2.1.6 运维管理区：负责网络基础设施的监管和数据中心网络的运维和管理。
5.2.2.1.7 普通用户区：负责接入局域网内所用职员用户和网络终端。
5.2.2.1.8 特别用户区：独立组网负责接入服刑人员用户和改造网络终端。
5.2.2.1.9 外网办公区：独立组网负责接入互联网应用于局域外网内所用职员用户和网络终端。

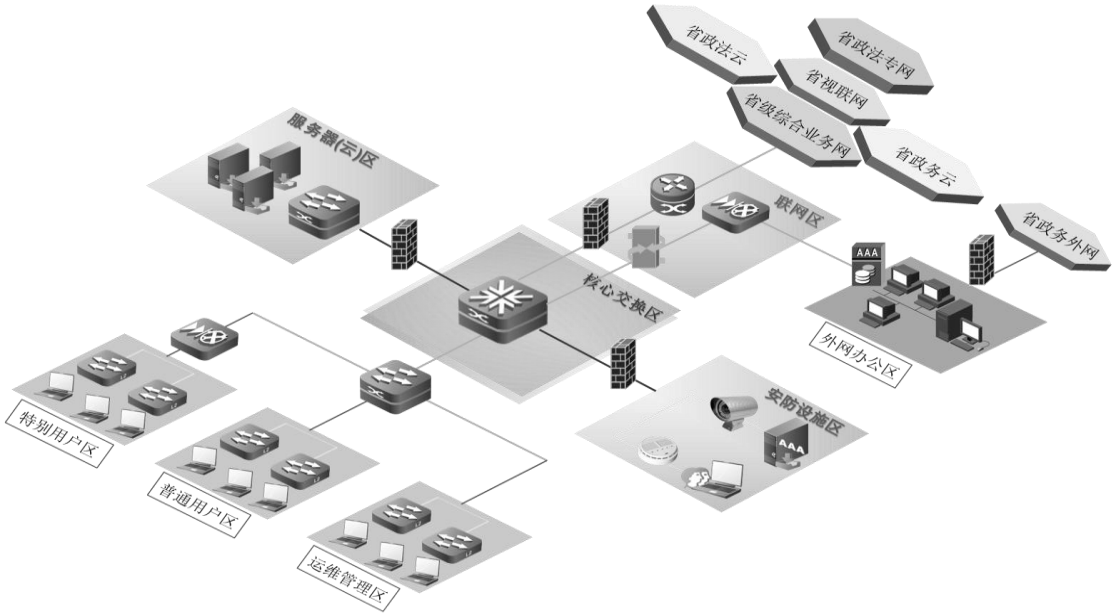

图 1 局域网网络架构

5.2.2.2 网络性能要求

5.2.2.2.1 局域网核心交换机需至少采用 CLOS 多级多平面交换架构，配置冗余主控、交换网板，提供持续的带宽升级能力，支持多种虚拟化技术，业务槽位满足业务需求，需具备全线速转发能力，需具备高密万兆转发能力，支持 40G、100G 接口扩展以满足数据中心业务流量高速转发要求，支持丰富的业务特性，业务槽位满足业务需求，适应融合业务网络发展趋势。

5.2.2.2.2 服务器接入交换机至少实现双千兆上行，并可提供 10G、40G 接入能力。

5.2.2.2.3 控制网络流量收敛比，链路收敛比不超过 4:1。

5.2.2.3 网络功能要求

局域网网络核心节点设备应支持 SDN、VXLAN、QOS 等特性，支持 IPv4/IPv6 动态路由。

5.2.3 局域外网

5.2.3.1 拓扑结构

局域外网拓扑结构见图 2。

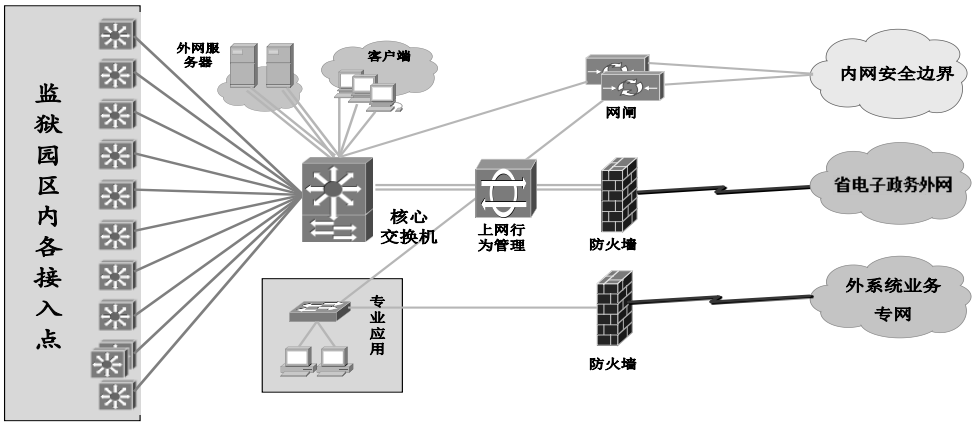

图 2 局域外网拓扑结构

5.2.3.2 基本组成和配置

5.2.3.2.1 局域外网基本主要组成单元有核心交换机、防火墙、上网行为管理等设备。

5.2.3.2.2 核心交换机应为局域外网的中心节点和网络枢纽。基本技术要求应满足企业级网络的互联；交换容量大于 7Tbps；设备具备高可靠性，主控单元、电源、风扇等基础组件具备冗余配置，模块具备热插拔技术，并支持虚拟化特性，支持标准的以太网协议（OSPF/VPN/MPLS/组播等）及可靠性协议（多实例生成树/链路聚合/双向转发检测等），并具备良好的扩展性，便于后续业务演进。

5.2.4 局域内网

5.2.4.1 拓扑结构

局域内网拓扑结构见图 3。

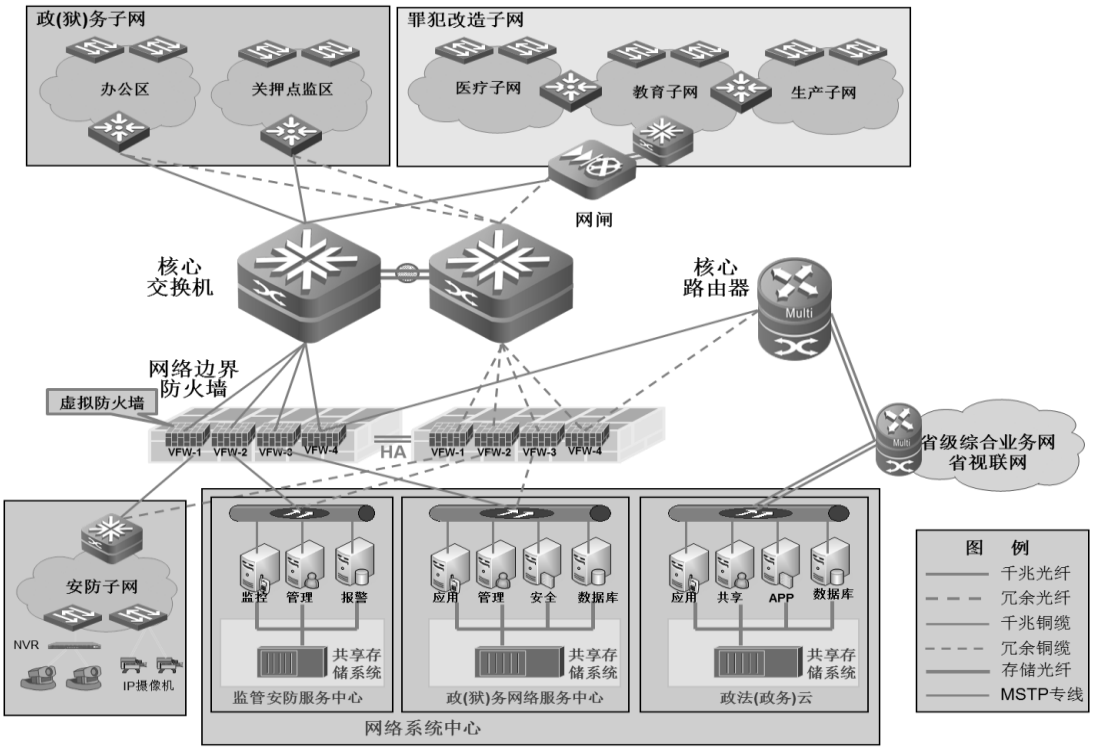

图 3 局域内网拓扑结构

5.2.4.2 基本组成和配置

5.2.4.2.1 局域内网主要组成单元有核心路由器、核心防火墙、核心交换机、汇聚与接入交换机、网闸等设备。

5.2.4.2.2 数据中心与政务子网、安防子网、改造子网等各个子网通过核心防火墙进行互通，核心防火墙通过虚拟化对不同业务系统的跨网访问作访问控制。通过网闸实现内网与其他不信任网络进行信息交换。

5.2.4.2.3 核心防火墙应实现整个局域内网的控制和互联枢纽。基本技术要求应满足各业务内网之间的互联控制需求；吐量大于 80G，具备高稳定性和高可靠性，主控、电源、风扇等基础组件具备冗余配置，部件支持热插拔等技术；支持防火墙虚拟化技术，基于用户组的安全访问控制功能；支持业界标准的路由协议及以太网协议；并支持良好的扩展能力保证业务的演进需求。

5.2.4.2.4 核心交换机应实现局域内网的中心节点和网络枢纽。基本技术要求应满足企业级

网络的互联；交换容量大于 14Tbps；设备具备高可靠性，主控单元、电源、风扇等基础组件具备冗余配置，模块具备热插拔技术，并支持虚拟化特性，支持标准的以太网协议（OSPF/VPN/MPLS/组播等）及可靠性协议（多实例生成树/链路聚合/双向转发检测等），并具备良好的扩展性，便于后续业务演进。

5.2.4.2.5 核心路由器应实现监狱单位局域内网的边界出口和唯一上联单元；基本技术要求应满足网络的互联，背吞吐量在 25Gbps~40Gbps 之间，包转发率在 5Mpps~40Mpps 之间，设备具备内置双电源，部件热插拔等可靠性技术，支持多种接口模式保证互联互通需求。

5.2.4.3 业务子网

5.2.4.3.1 基本要求

业务子网应为承载监狱特定安全边界类型应用的园区网络系统，根据承载应用特性而划分建立的业务二级网络，应为局域内网的基本组成单元。

5.2.4.3.2 政务子网

政务子网(简称政务网)应实现监狱单位基本行政办公及狱务管理应用而建立的业务终端网络。主要组成单元为监狱民警办公(狱务)应用而使用的各类智能终端，对应局域网网络架构普通用户区。

5.2.4.3.3 安防子网

安防子网(简称安防网)应实现狱内监管安全和指挥调度及处置应用建立的基础设施网络，主要组成单元为安全应用所需的各类智能基础设施和前端感知系统，对应局域网网络架构安防设施区。

5.2.4.3.4 改造子网

改造子网应狱内独立组网，实现服刑人员完成改造应用的终端网络，主要组成单元应为服刑人员操作终端，通过安全隔离网闸(GAP)使用改造应用与服务。对应局域网网络架构中的特别用户区。改造子网拓扑结构见图 4。改造子网具体由教育网、生产网、医疗网等组成：

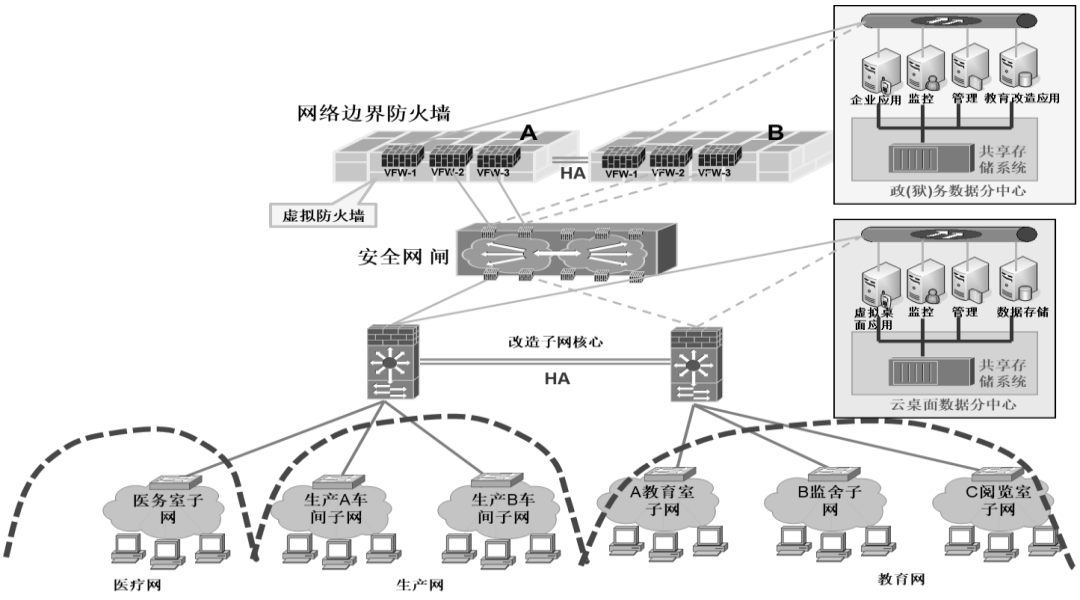

图 4 改造子网拓扑结构

a) 教育网:为狱内服刑人员完成教学学习与技能培训等教育改造应用建立的终端网络；

b) 生产网:为狱内服刑人员完劳动改造应用建立的终端网络;
c) 医疗网:为服刑人员完成生活卫生与医疗基础服务应用建立的终端网络。

5.3 有线数字组网技术要求

5.3.1 基本网络设计要求

5.3.1.1 监狱网络宜采用三层网络架构与二层网络架构混合结构设计，一般包括：接入层、汇聚层、核心层。
5.3.1.2 核心层应实现核心设备之间应该具有最高速的链路，比较粗的 QoS 控制粒度，最高的路由前缀，为网络其他模块提供互联;
5.3.1.3 汇聚层应实现细到粗 QoS 粒度的转换，提供到核心的路由合并，提供到访问层的路由过滤;
5.3.1.4 接入层应实现高密度的用户端口，包括安全控制和 QoS 控制的许可控制。
5.3.1.5 应采用多层网络的设计方法，必须依赖于利用网络的高弹性和扩充性。
5.3.1.6 接入层为终端用户提供不低于 100/1000M 交换端口，并提供到网络汇聚层的上联链路。
5.3.1.7 各子网汇聚层汇聚子网内所有的接入交换机,应提供千兆/万兆链路连接到核心层网络中，并提供故障或问题的隔离，使得核心网络免于外围故障的影响。
5.3.1.8 核心网络设备之间应提供冗余的、高带宽的交换数据通道，采用虚拟化技术，形成网络的核心结构。

5.3.2 通信链路设计

5.3.2.1 应考虑应用系统对链路带宽的要求。
5.3.2.2 应考虑核心层和汇聚层接入数量及带宽聚合需求。
5.3.2.3 应考虑分散关押点选择何种链路类型。

5.3.3 监狱各节点网络设计

5.3.3.1 核心节点设计

监狱网络系统的网关核心节点采用两台高性能的防火墙，负责各专业子网及全省政务专网间访问控制和数据转换。子网中路由交换核心节点与汇聚节点间采用双链路方式进行连接，物理链接上：路由交换核心节点与汇聚节点间采用双链路或者口字形方式进行连接，网关核心节点与省局网络平台接入路由器采用双链路或者口字形方式进行连接。在逻辑链接上：核心节点两台设备做虚拟化配置，简化网络结构，与汇聚节点建议启用 OSPF 协议互联，保证网络的灵活性。

5.3.3.2 汇聚节点设计

监狱网络数据中心设立汇聚节点，物理链接上：汇聚节点向上通过双链路分别连接两台核心节点；向下通过链路捆绑或者口字形连接监狱机关科室和监区的接入设备。逻辑链接上：汇聚节点可以采取虚拟路由器冗余协议(VRRP)方式或者堆叠方式与接入节点互联，提供接入部分得网关需求，若接入节点数量巨大，可以采用 OSPF 方式接入，网关设置在接入节点。

5.3.4 互联接入组网技术要求

5.3.4.1 网络结构

监狱局域节点采用冗余结构设计。

5.3.4.2 网络设备

网络平台中，核心网络设备关键部件（如主控板、交换网板、电源等）采用冗余备份设计，支持 VPN 功能，满足 MPLS VPN 部署要求。

5.3.4.3 互联链路及带宽

网络平台省局到监狱每个广域网节点互联链路应具备冗余能力，互联链路带宽需具备平滑的升级能力。省局到监狱广域网链路传输带宽不低于 100Mbps，正常情况带宽峰值利用率不超过 70%。

具体网络带宽可参考以下公式计算：

BW=（A+B+C+D）*X

A:IP 通信业务和无线通信业务承载带宽值，原则上不低于 8Mbps；

B:视频会议及其他远程视讯业务承载带宽值，原则上不低于 20Mbps，保证 5 路并发；

C:应急指挥和安全防范视频监控业务承载带宽值，原则不低于 20Mbps，保证 5 路并发；

D:其他纵向业务承载带宽值，原则上不低于 10Mbps。

X:系数值为 140%，作为带宽预留。

5.3.5 外联网接入组网技术要求

5.3.5.1 监狱外联网是全省监狱系统网络互联的基础组成网络，是监狱网络信息系统关键组成部分。省局和全省各监狱单位的网络为政法网络的基本接入单元，上行与省综合业务网和省政法专网安全对接，实现与省委省政府、省司法厅以及省政法机关的政务网数据交换。

5.3.5.2 监狱外联网是以星型结构为基本拓扑构建的省内跨地区数字广域网络。其主要组成单元有核心路由器、接入路由器、广域数字链路等。

5.3.5.3 核心路由器：是政务专网星型拓扑的中心节点和网络枢纽。基本技术要求：采用骨干级路由器实现企业级网络的互联；吐量大于 40Gbps；采用 OSPF 协议技术组网；具备平滑演进 VPN/IPv6/组播等技术的能力；设备本身具备高可靠和高稳定性，主控、电源、风扇等基础组件具备冗余配置，并支持可靠的不间断重启，热插拔等可靠性技术。

5.3.5.4 接入路由器：是政务专网星型拓扑的接入节点，也是监狱单位局域内网的边界出口和唯一上联单元。基本技术要求：采用企业级路由器实现网络的互联，背吞吐量在 25Gbps~40Gbps 之间，包转发率在 5Mpps~40Mpps 之间，设备具备内置双电源，部件热插拔等可靠性技术，支持多种接口模式保证互联互通需求。

5.3.5.5 广域数字链路：是政务专网星型拓扑的数字传输链路，分别采用 MSTP 技术和 SDH 技术，并多数据通路，多运营商等技术提高数字链路的可靠性、容错性和稳定性。

5.4 无线网络组网技术要求

5.4.1 监狱内的无线网主要有 Wi-Fi、无线射频识别(RFID)和 3G/4G 等网络。

5.4.2 各区域 Wi-Fi 组网采用 AC+AP 的方式组网实现无线覆盖，主要覆盖区域为办公楼、监舍、厂区等；需满足无线终端移动过程中自动切换接入点，网络不断线，即无线漫游；无线网络主要供内部办公使用，AP 需支持设置办公网络和访客网络等多个服务集标识符(SSID)，且不同的服务集标识符(SSID)有不同的网络权限，相互隔离； 无线安全性要求高，尤其是办公网络，须进行身份认证，限制非法终端接入，如采用硬件地址(MAC)认证；AP 外形应支持以太网供电(PoE)，满足消防及布线需求；通过 AC 统一管理、配置，并实时监控各 AP 工作状态，运维简便，并记录上网行为数据；监内 Wi-Fi 无线网络从属政(狱)务子网，通过防火墙管控访问对象。

5.4.3 3G/4G 无线移动通讯专网是监狱系统警务通终端基础通讯网络，是监狱指挥调度网络

的无线通讯基础平台，同时也是广域专网的 VoIP 无线通讯接入单元。

5.4.4 组成单元包括：数字专线，无线通讯基站，语音网关等。

5.4.5 数字专线：无线移动通讯运营商将无线通讯网络通过数字专线对接政务专网，实现有线无线移动通讯的融合。

5.4.6 无线通讯基站：无线移动通讯运营商为无线移动终端提供接入。

5.4.7 语音网关：监狱单位采用多业务路由器实现监狱 VoIP 有线通讯与无线移动通讯的对接网关。

5.5 有线、无线音视频通讯网络组网技术要求

5.5.1 有线通讯系统

5.5.1.1 有线程控交换通讯系统

5.5.1.1.1 PBX 与 PSTN 互联，PBX 通过中继网关转换后接入司法行政系统网络，中继网关具有数字中继接口以及 IP 中继接口，能够完成 PBX 通信系统到 IP 网络转换。

5.5.1.1.2 中继网关完成 SIP/H.323 协议与 NO.7/Pri 信令的转换,完成 PBX 通信系统与司法行政有线通信网的融合。

5.5.1.2 VoIP 系统

基于全国司法行政系统网络平台通道，利用 IP 网络承载语音的传输服务技术（VoIP），实现司法行政网络之间有线通信系统互联互通。已实现 VoIP 系统接入的单位，需能够通过中继接口（SIP 协议）与全国司法行政网络平台的有线通信平台系统互联。

VoIP 系统接入的设备 IP 地址采用统一规范的全国司法行政纵向业务系统 IP 地址。

5.5.1.3 有线网络与公网的融合

5.5.1.3.1 PBX 通信系统通过数字中继接口（NO.7/Pri 信令）与 PSTN 相连，实现与市话、手机的互通。

5.5.1.3.2 VoIP 系统接入方式通过数字中继接口（NO.7/Pri 信令）与 PSTN 相连，实现与市话、手机的互通。

5.5.1.4 有线通信系统对基础网路平台技术要求

采用 G.711 编码时,环回时延<120ms,实际占用带宽每线 90.4kbit/s 采用 G.729a 编码时，环回时延实际占用带宽每线 34.4kbit/s;采用 G.723.1 编码时，环回时延<200ms,实际占用带宽每线 22.9kbit/s。

5.5.1.5 有线通信系统电话编制要求

各监狱行政电话号码编制采用统一规范，自行编制的原则，并统一上报至省监狱管理局。

5.5.2 无线通信系统接入技术要求

5.5.2.1 无线通信系统要求

基于全国司法行政网络，建立异地间无线通信数据传输通道，实现司法行政无线通信系统的互联互通,自动漫游。

5.5.2.2 无线通信系统接入方式

无线通信系统通过 MSO 接入司法行政系统网络，通过 MSO 的互联，实现互联互通。MSO

的 IP 地址采用统一规范的全国司法行政向业务系统 IP 地址。

5.5.2.3 无线通信系统对网络的承载要求

无线通信系统以司法行政系统网络为承载，窄带无线每路带宽 32kbps,网络延时≤50ms,网络抖动≤10ms；跨系统组呼叫时建立时间<500ms，系统丢包率<0.1%；宽带无线每路带宽≥2Mbps，网络延时≤50ms，网络抖动≤10ms。

5.5.3 有线通信系统与无线通信系统对接

无线通信系统是有线通信系统的无线延伸，通过有限与无线系统的互联，实现监狱应急指挥和管理的通信保障。

无线通信系统通过数字中继接口(NO.7/Pri 信令)与 PBX 通信系统和 PSTN 相连，实现与内线电话,市话,手机的互联。

5.5.4 视频会议系统技术规范

5.5.4.1 网路承载基本要求

基础传输网络需使用专用线路通道，采用基于 SONET/SDH 平台的 MSTP 技术，同时实现 TDM、ATM、以太网等业务接入、处理和传送，带宽应不低于 6Mbps。

5.5.4.2 网络承载带宽指标

应满足视频宽带的 1.2 倍作为网络承载带宽的基本要求。

5.5.4.3 网络承载性能要求

网络的时延抖动<50ms；网络的丢包率<0.05%；端到端的时延宜<150ms。

5.5.4.4 组网技术

视频会议终端、多点控制单位 MCU 等设备，采用 IP 网络接入，依托视联网进行组网传输，与司法部、省监狱管理局、各省市属监狱、各县市司法局互联互通。

5.5.4.5 视频会议终端注册方式

视频会议终端采用 IP 地址方式进行注册，出口互联地址由省监狱管理局 GK 统一规划，内部地址由各单位自行分配。

5.5.4.6 可靠性要求

在全省监狱系统网络平台主干和监狱接入设备上针对视频会议业务做 QoS 设置，以保障视频业务获得低时延和高带宽。

6 网络边界交互及连接技术要求

6.1 基本要求

网络边界交互及连接应符合 SF/T 0012—2017 的相关要求。网络边界安全防护也叫边界网络防护，主要包括网络层、传输层的包过滤和应用层代理深度检测过滤。主要网关设备有防火墙和网闸。

6.2 与政法系统专网

监狱单位的各类网络系统在出入口必须统一配置核心防火墙，核心防火墙须配置双机，已实现高可用和冗余。重要的业务子网(如监狱安防监控子网)与全省政务主干网之间也统一接入核心防火墙。边界路由应采用 OSPF 协议进行互联，同时要求支持 VoIP 功能，便于语音、数据、视频等综合多媒体的通信业务的“三网融合”。

6.3 与外系统专网

监狱与检察院、公安等外系统专网对接时，需要通过防火墙进行连接，并专门为其设立单独的 VPN 实例进行内网路由连接。

6.4 与涉密专网

原则上不与涉密专网对接，物理隔离。

6.5 与互联网

6.5.1 监狱互联网入口处设置防火墙、并建立入侵防御系统(IPS),监狱内部政务外网再通过网闸与政务内网进行数据交互。
6.5.2 入侵防御系统(IPS)对网络七个层次进行全面检测以及防护的软、硬结合的系统。它将防火墙、入侵检测系统(IDS)、防病毒和脆弱性评估技术的优点与自动防止攻击的功能融为一体。

6.6 与其他非涉密专网

监狱与社会医院病房监控、远程会诊等网络采用运营商 VPN 线路或数字传输链路进行连接，并为其设立单独的 VPN 实例进行内网路由连接，范围控制通过防火墙进行控制。

7 网络安全技术要求

7.1 应符合 SF/T 0012—2017 网络平台安全的相关技术要求。
7.2 应当按照 GB/T 22239—2008 技术标准，参照 GB/T 20270—2006、GB/T 20271—2006、GB/T 20272—2006、GB/T 20273—2006、GB/T 21028—2007 等技术标准建设符合等级保护三级要求的信息安全系统。

8 网络运行管理与运维技术服务要求

8.1 基本要求

8.1.1 应符合 SF/T 0012—2017 网络平台运行管理的相关技术要求。
8.1.2 运维服务包括：运维监控管理平台、运维审计平台、运维管理机制；
8.1.3 技术服务包括：技术支持服务管理平台、技术服务管理机制。

8.2 运维监控管理平台

8.2.1 平台应对监狱各类信息系统软硬件基础设施状态信息进行实时采集，通过拓扑关系予以监控，即时对报警故障和系统缺陷进行技术修复和改进；
8.2.2 平台应对监狱各类信息系统软硬件资产进行管理，即时跟踪相关资产的生命周期和服务周期生态，并提供关键资产的应急预案；

8.2.3 平台应对监狱各类信息系统软硬件资产及其涵盖项目的技术资料进行管理，同时建立运维、管理策略、安全策略等知识库；
8.2.4 平台应建立和规范运维管理与处置的线上线下流程的衔接和机制，保障信息系统的安全与稳定；
8.2.5 平台应建立和规范信息系统应急预案处置与评估响应流程和机制。

8.3 运维审计系统

8.3.1 系统应建立对主机、数据库以及网络、安全设备上的数据访问实现单点登录，进行安全、有效的操作审计，支持实时监控和事后回放。集身份认证、授权、审计为一体，有效地实现事前预防、事中控制和事后审计。
8.3.2 系统应建立对主机、数据库以及网络、安全设备上的系统日志统一采集，进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，确保业务的不间断运行。

8.4 技术支持服务管理平台

8.4.1 平台建设体现应自下而上一体化 IT 运维管理，应实现运维管理业务的分层管理、垂直监督及安全生产的预控、可控。应为各信息技术部门的运维管理提供全面的业务功能支持。
8.4.2 平台应面向业务流程管理，建设应引入包括设备全过程管理、全面设备维护、预防性维护、状态检修等在内的先进资产管理理念和最佳业务实践，分层及个人资产分布的管理模式。应设计“应急预案”管理模式，提供预案演习、预案执行等多项功能。
8.4.3 提供的“知识库”功能应包括常见问题、运维规范制定执行、历史运维积累等多个项目的资料查询调阅。
8.4.4 基本模块应包括：IT 资产管理、平台门户、运维任务管理、维护商管理、知识库管理、系统维护等功能。

9 网络设备命名规则

9.1 基本要求

应符合 SF/T 0012—2017 网络设备命名规则的相关要求。

9.2 网络设备命名

9.2.1 设备的命名格式为：空间地理位置_单位标识_网络层次_设备类型及设备编号。
9.2.2 设备的编码规则为：A_B_C_Dn，具体如下：

A：省级标识，用汉语拼音字母缩写(ZJ)来标识。
B：监狱系统级标识，由全省各单位保证标识的唯一性，具体见表 1。
C：网络层次，用 2 位字母表示，参考 SF/T 0012—2017 网络层次代码表。
D：设备类型，用 2 位字母表示，参考 SF/T 0012—2017 设备类型代码表。
n：设备编号，用 2 位数字表示。

表 1 监狱系统级标识表

序号	地区单位名称	标识	序号	地区单位名称	标识
1	省监狱管理局	SJYJ	15	省临海监狱	SLH
2	省第一监狱	S1J	16	省之江监狱	SZJ

表 1 监狱系统级标识表（续）

序号	地区单位名称	标识	序号	地区单位名称	标识
3	省第二监狱	S2J	17	省第二女子监狱	S2NJ
4	省第三监狱	S3J	18	省未成年犯管教所	SWGS
5	省第四监狱	S4J	19	省监狱中心医院	SYY
6	省第五监狱	S5J	20	杭州市西郊监狱	HZXJ
7	省第六监狱	S6J	21	杭州市南郊监狱	HZNJ
8	省女子监狱	SNJ	22	杭州市东郊监狱	HZDJ
9	省乔司监狱	SQS	23	杭州市北郊监狱	HZBJ
10	省十里丰监狱	SSLF	24	宁波市黄湖监狱	NBHH
11	省十里坪监狱	SSLP	25	宁波市望春监狱	NBWC
12	省金华监狱	SJH	26	宁波市高桥监狱	NBGQ
13	省南湖监狱	SNH	27	湖州市湖州监狱	HZHZ
14	省长湖监狱	SCH			

以省第一监狱汇聚路由器设备命名示例，见表 2：

表 2 监狱系统级标识表（示例）

命名编码规则	A_B_C_Dn
设备命名	ZJ_S1J_AG_RT01

10 其它

10.1 域名解析系统

10.1.1 基本要求

应符合 SF/T 0012—2017 域名解析系统的相关要求。

10.1.2 域名的规划与管理

监狱网络信息系统采用司法行政系统网络独立的域名系统，域名由根域和二级域以及若干个子域名用“.”连接而成，采用 sf 作为根域名和 zjsjy.sf 作为二级域名。

10.1.3 域名命名规范

域名应以 4-5 段为主，总长度不应超过 25 个字符。如：“主机名.单位名.zjsjy.sf”。

10.1.4 域名体系管理

域名的体系管理应符合下列要求：

a) 司法部信息中心负责一级域名（sf）及一级 DNS 的管理，省监狱管理局负责本省监狱系统建设二级子域（zjsjy.sf）及二级 DNS 的管理。

b) 监狱三级域名分配方案采用监狱名称首字母缩写规则统一定义，例如省第一监狱（s1jian.zjsjy.sf），所有监狱单位的三级域名均在本单位 DNS 中注册。
c) 监狱 DNS 服务应建立对上一级 DNS 域名的转发。

10.2 网络时钟系统

网络时钟系统应符合 SF/T 0012—2017 网络时钟系统的相关要求，并满足以下要求：

a) 省监狱管理局采用全球定位系统(GPS)/北斗双卫星为 NTP 服务器提供全省监狱网络统一标准的时间源；
b) 监狱部署 2 台 NTP 服务器（双机冗余热备），实现省局-监狱两级 NTP 服务器时钟同步；
c) NTP 服务器采用客户机/服务器(C/S)模式单波通信工作模式，客户机采用环回接口和 NTP 服务器通信；
d) 监狱网络中各类终端、网络设施、安防系统、应用系统、通信系统等设备应于 NTP 服务器进行时间信号同步。