基于冗余与链路聚合技术的网络安全架构设计

张浪

中国民用航空西南地区空中交通管理局贵州分局，贵州贵阳，550012；

摘要：随着《民航航空 VoIP 语音通信技术规范》的发布，关于如何正确运用 VoIP 技术为空管地空通信系统提供更加安全可靠的使用方式也随之展开，传统地空通信系统以模拟技术为主，不同的频率资源对应不同的物理线路，而 VoIP 技术以数字技术为主，通过网络让不同的资源在同一线路中传输。本文结合中国民航空管运行情况和需求，设计规划空管系统 VoIP 组网方案和安全策略，采用冗余与链路聚合技术完成网络安全架构设计。

关键词：VoIP 技术；网络安全；地空通信；链路聚合；冗余架构

DOI：10.69979/3041-0673.26.05.020

引言

近年来，随着我国民航事业的快速发展，空中交通流量呈现持续增长态势。据统计，2023 年全国民航起降架次突破 1000 万次，较十年前增长近 300%[1]。传统空管地空通信系统基于模拟技术，采用电路交换模式，存在三大核心缺陷：

（1）资源利用率低：每个甚高频（VHF）台站需独占独立物理线路，带宽资源浪费严重；

（2）扩展性差：新增台站需重新布线，难以适应突发流量需求；

（3）安全隐患突出：单点故障易导致通信中断，缺乏有效的防护机制。

随着通信技术的快速发展，空管地空通信设备的技术体制正在逐渐向以 VoIP 技术为核心演进。民航贵州空管分局分别结合本地区情况针对性的开展了大量的地空通信 VoIP 技术研究和验证等工作。VoIP 是一种在 IP 网络上使用 IP 协议以数据包的方式传输语音的技术，存在四大核心优势：

（1）降低成本：基于 VoIP 技术可以通过一个核心交换单元接入所有运行业务；

（2）维护方便：通过网络监控技术可以有效发现链路故障；

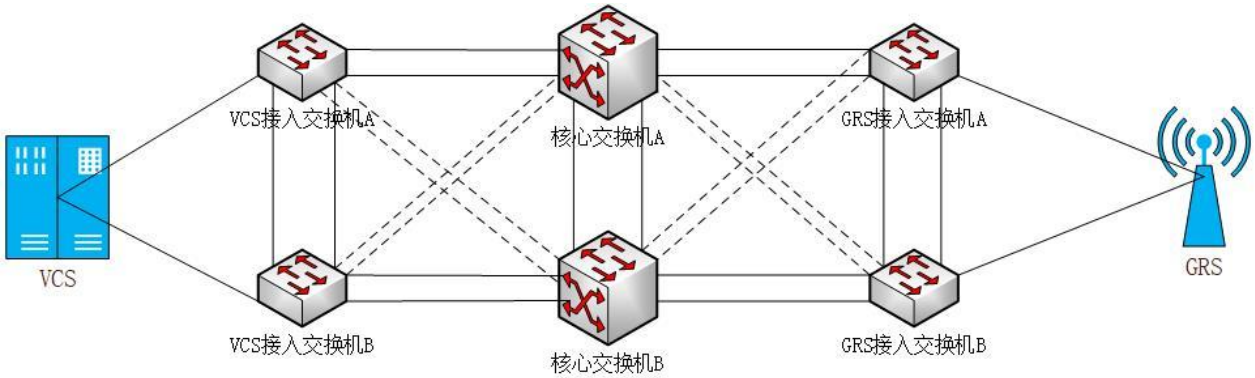
（3）业务灵活多样：可以实现多种业务类型，方便异地资源调用指挥；

（4）完备的协议体系：可以支撑未来空管语音通信实现数字化、网络化和智能化发展。

在此背景下，VoIP 技术凭借其数字化、分组化优势成为行业转型升级的关键路径。本文结合中国民航空管实际运行环境，提出基于冗余与链路聚合技术的安全架构设计方案，通过多种安全技术解决传统通信系统的痛点问题。

1 网络拓扑结构设计

地空通信全链条分为三个部分，一是管制终端的内话系统（Voice Communications System,VCS），二是地面台站的甚高频系统（Ground Radio Station,GRS），三是内话系统与甚高频系统互联的数据传输系统，共同组成了地空通信系统全业务链。现根据地空通信特点，结合组网架构，将 VoIP 地空通信系统网络结构设计如下：



网络拓扑结构图一共分为两层（接入层、核心层）[7]，VCS 接入交换机与核心交换机位于本地机房，GRS

接入交换机位于远端台站，在核心交换机与 VCS 接入交换机之间通过自建光纤连接，与 GRS 接入交换机之间通过运营商链路传输至本地机房，拓扑图中忽略运营商部分，使用简化的拓扑图直观的表达地空通信基于 VoIP 技术的全链条流程图。

核心层：网络的高速骨干和中心枢纽。

关键职责：

高速数据转发：核心交换机拥有极高的交换容量（背板带宽）和端口密度，专注于以尽可能快的速度（线速）在不同接入层交换机之间、以及网络的关键资源（如管制话音数据、外部接口数据、信令链路）之间转发数据包。目标是最小化延迟[4]。

路由决策（通常）：在两层模型中，核心层通常承担主要的第 3 层路由功能。它维护着整个地空网络的路由表，负责在内话与电台子网之间做出路由决策。它通常是网络的默认网关所在。

核心层设计应尽可能简单、快速、可靠。避免在此层实施复杂的策略（如访问控制列表 ACLs、QoS 标记等），这些策略会降低转发速度，应下沉到汇聚层（在两层模型中，核心层可能承担部分汇聚策略功能）或接入层实施。

接入层：连接终端用户和设备到网络的边缘点。

关键职责：

终端设备连接：直接通过有线（以太网端口）的方式连接最终用户设备（内话、电台）。

第 2 层交换：主要工作在 OSI 模型的数据链路层（第 2 层）。负责基于 MAC 地址在本地端口之间进行帧交换。为连接的设备提供网络接入点。

广播域控制（VLAN）：

将端口划分到不同的 VLAN 中，以隔离广播域，提高安全性和性能。

实现用户、设备或功能组的逻辑分段（例如，飞坤内话 VLAN、天奥电台 VLAN、优创电台 VLAN）。

接入层设计强调广泛的连接性、用户/设备的接入控制、安全策略的初始实施点以及基本的 QoS 保障。

两层架构中功能交互总结

接入层是用户和设备的“门卫”和“接线员”，负责安全接入、初步分类标记和本地交换，并通过高可靠聚合链路上联。

核心层是网络的“高速公路系统”和“交通枢纽”，专注于在接入层之间以及接入层与关键资源之间提供超高速、可靠的路由和交换。它确保数据能在网络的骨干部分快速、无阻塞地流动，并具备故障自愈能力。

这种简洁的两层模型通过将路由决策和高速骨干集中在核心层，并将用户接入和边缘策略集中在接入层，有效地满足了中小型网络对性能、可靠性和可管理性的需求。

2 冗余配置的必要性和实现方式（双机冗余、堆叠）

2.1 冗余配置的必要性分析

空管通信系统的可靠性直接影响飞行安全。美国联邦航空管理局（FAA）统计数据显示，通信系统中断事故中 73%源于单点故障[2]。

空管地空通信系统被比喻为管制员的耳朵，是空中交通指挥的关键设备，为确保空中交通指挥正常，避免因设备原因导致空中交通管制运行方式和飞行方式改变，冗余的网络设备配置不可或缺。使用堆叠配置是将冗余交换机通过堆叠线缆连接在一起，从逻辑上虚拟成一台交换设备的技术，可以提高网络的可靠性、扩展端口数量，增大带宽，并简化网络部署和管理。通过冗余设计可以实现：

故障快速切换：设备级冗余可将故障恢复时间（MTTR）从小时级缩短至秒级；

流量无缝转移：链路级冗余支持 ECMP（Equal-Cost Multi-Path）动态负载均衡；

抗毁能力提升：核心节点双活部署可抵御区域性自然灾害影响。

2.2 冗余实现技术方案

2.2.1 设备级冗余

双机热备（HSRP/VRRP）：在核心交换机间配置虚拟路由器冗余协议，优先级动态调整确保主备切换无感；

堆叠技术应用：通过专用堆叠线缆实现交换机物理堆叠，支持跨设备链路聚合（CSS+LACP）。

2.2.2 链路级冗余

多归属设计：每个 VCS 和 GRS 接入交换机通过双上行链路分别接入两台核心交换机；

BFD 联动机制：部署双向转发检测协议，实现链路故障毫秒级检测。

内话系统、甚高频电台本地接入交换机与核心交换

机采用 A/B 冗余配置，内话接入交换机、电台接入交换机、核心交换机之间采用堆叠方式，同时内话系统、甚高频电台分别接入两台本地接入交换，接入交换机采用双链路分别接入两台汇聚交换机实现链路冗余，在链路与设备双重冗余下避免了单点故障导致业务中断，提升了安全裕度。

3 链路聚合技术的应用和优势

3.1 技术原理与标准化进程

链路聚合控制协议（LACP）遵循 IEEE 802.3ad 标准，通过动态协商实现多链路捆绑。

负载均衡算法：源目 MAC 地址哈希。

在网络拓扑图中交换机之间的连接采用了双链路是为了使用链路聚合技术。链路聚合是将多个物理端口绑定成一个逻辑端口，指在提升带宽、增强可靠性并优化流量负载。通过聚合，多条物理链路对外表现为单一逻辑链路，实现高效的数据传输与管理。

3.2 空管应用场景

高带宽需要：在管制繁忙时段，开放扇区数量多，主用频率话音收发频繁，导致数据量突然增大，当服务器需要与交换机传输大量数据时，通过聚合多个端口，显著提升上行带宽。

冗余容灾：通过聚合多条物理链路，确保单链路故障时业务不中断。

负载均衡优化：根据业务类型选择负载均衡算法（如基于源 IP、目的 IP、或五元组），避免单链路拥塞。

3.3 优势

带宽叠加，提升传输效率：通过聚合 2 条物理链路，总带宽可达到单链路的 2 倍，满足大数据传输需求[5]。

冗余容灾，增强网络可靠性：某条物理链路中断，流量会立即切换到其他正常链路，切换时间小于 50ms，业务无感知。

负载均衡，优化资源配置：根据预设算法（如源-目的 IP 哈希、轮询）将流量均匀分布到各物理链路，避免链路拥塞。

简化管理与扩展：多个物理端口合并为单一逻辑接口，降低配置复杂度。

消除环路与阻塞： 在生成树协议环境中，链路聚合组被视为一条逻辑链路，避免了多条平行物理链路因 STP 阻塞而造成带宽浪费（聚合组内所有端口都处于转发状态）。

3.4 实现方式

静态聚合： 手动在交换机两端配置聚合组，无需协商协议。配置简单，但容易因一端配置错误导致环路等问题。

动态聚合（LACP）：使用 LACP 协议自动协商、管理和维护聚合链路[6]。这是最推荐和最常用的方式：

（1）自动协商：设备间通过 LACP 数据单元协商哪些端口可以加入同一个聚合组。

（2）状态检测：持续监控成员链路的状态（Active/Inactive）。

（3）防止错误配置：提供一定程度的防环机制，两端配置不一致（如速率、双工模式、VLAN）的端口不会被激活加入聚合组，增加了安全性。

4 链路聚合和堆叠配置如何提升网络安全性

4.1 链路聚合

4.1.1 冗余链路防止单点故障

抗 DDoS 攻击：链路聚合通过多链路负载均衡，可将攻击流量分散到多条物理链路，避免单链路被攻击流量占满而导致服务中断[3]。

快速故障切换：若某条链路因物理破坏或协议攻击（如 ARP 欺骗）失效，流量可立即切换到其他正常链路，保障业务连续性。

4.1.2 动态协议增强链路合法性验证

LACP 认证：启用链路聚合控制协议（LACP）的动态协商功能，要求对端设备提供合法认证（如密钥），防止非法设备接入聚合组[11]。

端口安全绑定：结合 MAC 地址或 IP 绑定技术，确保只有授权设备能够加入链路聚合组。

4.2 堆叠

4.2.1 逻辑统一管理降低配置风险

集中化安全策略：堆叠后的交换机作为单一逻辑设备，可统一配置 ACL、防火墙规则、VLAN 隔离等策略，减少因配置分散导致的漏洞。

简化运维：通过堆叠主控节点统一管理，避免因多设备独立配置印发的策略冲突或疏漏。

4.2.2 物理与逻辑隔离增强防护

堆叠端口专用化：将堆叠端口划入独立的管理

VLAN，禁止业务流量访问，降低横向渗透风险。

堆叠成员认证：通过堆叠协议（如华为的 iStack）的成员认证机制，仅允许合法设备加入堆叠组，防止恶意设备仿冒接入。

5 可能的安全风险及应对措施

5.1 堆叠系统安全威胁

表 1 堆叠威胁

威胁类型	攻击手段	防护措施
主控劫持	伪造堆叠协议报文	启用 SHA-256 成员认证
配置泄露	未加密的堆叠通信	部署 TLS 1.3 加密隧道
物理攻击	直接接触堆叠端口	机房门禁+操作审计日志

5.2 聚合链路泛洪攻击

风险：攻击者向聚合组发送海量立即流量，占满带宽。

应对：在核心交换启用流量分析，结合 ACL 动态阻断异常流量源。

5.3 配置泄露风险

风险：堆叠或聚合配置未加密存储或传输，可能被窃取。

应对：启用配置文件的加密存储（如 AES-256），管理流量强制使用 SSH/HTTPS。

6 总结和建议

本文提出的冗余与链路聚合融合架构，通过双机堆叠冗余、链路聚合技术及多层次安全策略的网络架构设计，可实显著提升空管地空通信系统 VoIP 网络安全：

（1）冗余与高可用性：抵御单点故障和 DDoS 攻击、保障业务连续性。

（2）动态协议防护：通过 LACP 认证、堆叠加密等技术，防止非法接入和中间人攻击。

（3）统一安全管理：简化策略配置，降低认为错误风险。

通过合理设计，链路聚合与堆叠不仅是性能与可靠的基石，更是构建纵深防御网络安全架构的关键组件，可以有效满足空管地空通信 VoIP 运行需求。

最后建议：在堆叠链路和聚合端口上启用加密与认证机制。定期进行冗余切换演练和安全渗透测试。结合网络流量监控与 AI 驱动的威胁检测系统，实现主用防御。

参考文献

[1]中国民用航空局. 2023 年民航行业发展统计公报[R]. 北京：中国民航出版社，2024.

[2]FAA. Air Traffic Organization Safety Management System Manual[M]. Washington: FAA, 2022.

[3] 李明,等.民航通信网络安全防护体系构建[J].中国民航大学学报，2023，41(2)：12-18.

[4]吴魏，郭芳.基于 eNSP 的计算机网络实验课程设计[J].网络安全技术与应用，2022（12）：76-78.

[5]赵琦.基于 UDT 的无线网络链路聚合软件设计与实现[D].成都：西南交通大学，2023.

[6]高芳,刘晨旭,何钰.浅析静态和动态链路聚合优缺点[J].网络安全和信息化,2021(9):152-153.

[7]陈岳.园区级校园网络规划与方案设计[J].信息技术与信息化 ,2020(11):167-170.