

# 电力通信集成监控系统网络改造实践

俞 浩

(泰州供电公司, 江苏 泰州 225300)

**摘 要:** 为了保证电力通信网络的安全健康运行, 通信监控系统得到了广泛的应用, 本文通过介绍在泰州电力通信集成监控系统推广建设过程中, 对该系统原有网络架构的改造实践, 分析了系统的网络安全设计以及为提高网络安全的解决方案。通过具体实施方案阐述了访问控制列表、正向隔离装置、防火墙在该系统中的应用。

**关键词:** 电力通信; 集中监控; 安全

## 0 引言

为保证电力通信网的安全可靠运行，泰州供电公司于2010年整合了原有的动力环境监控、传输网监控、资源管理等多个专业应用子系统，在此基础上推广建设了通信集成监控系统，实现了通信资源的共享，为通信网运行维护提供一个信息支撑综合技术平台。由于整合的各个子系统分属于电力安全防护二区、三区不同区域，对数据流的传输控制有着严格的要求，因此整合过程中对原有网络架构进行了设计改造，通过采取访问控制列表、正向隔离装置、防火墙等网络安全工具，实现不同区域间及区域内的网络访问控制，确保网络安全。

## 1 改造前网络概况

在开展通信集成监控系统推广工作前,泰州通信动力环境监控、传输网监控、通信资源管理等专业应用虽然分属于不同的系统,但在网络结构上均连接于同一内部网络,结构如图1所示。

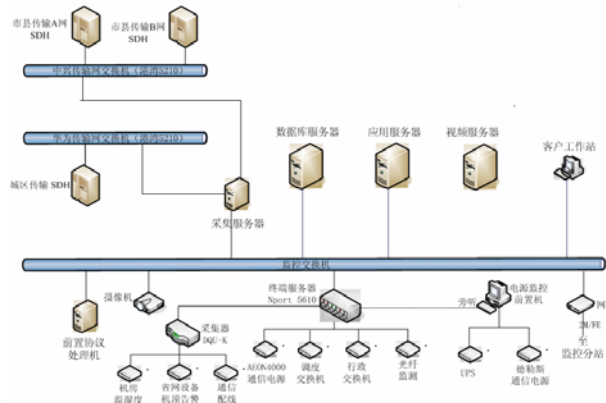


图1 改造前监控系统网络结构

图1中在采集服务器上配置多块网卡,分别与华为网管交换机、中兴网管交换机及监控系统交换机互联,采集服务区从中兴、华为网管通过CORBA接口采集网管实时信息后,通过监控系统交换机传送至数据服务器;应用服务器通过监控系统交换机互联的2M/FE等通道与各个监控分站、主站终端服务器互联,接入主站及监控分站的动力环境告警信息。由于网络所有连接均依赖于同一台二层交换机,采用的是二层网络结构,因而不具备安全防护能力,且无法抵御网络风暴,不满足电力安全防护的要求。同样由于未配置防火墙,未能实现与省公司的互联。

## 2 网络域划分设计

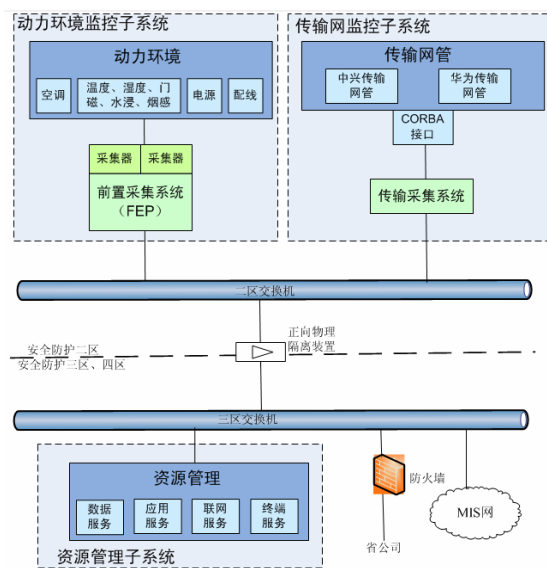


图2 网络域划分结构

为提高通信监控系统的网络安全防护水平,在通信集成监控系统推广建设过程中,根据《电力二次系统安全防护规定》中安全防护相关原则,对监

控系统的网络结构进行了设计、改造，对各个专业应用子系统进行区域划分，将传输网监控子系统、动力环境监控子系统划入二区，将通信资源管理子系统划入三区，二区、三区之间使用正向隔离装置进行物理隔离，二区内的不同子系统之间使用访问控制列表(ACL)进行数据访问控制，同时在三区内增加防火墙，实现与省公司的互联。网络域划分结构如图2所示。

### 3 二区网络安全改造

#### 3.1 二区网络控制要求

通信集成监控系统二区内部署了动力环境监控、传输网监控等多个应用子系统，根据各个子系统的业务需求，这些子系统内部、子系统之间以及子系统与三区应用服务器之间对数据的传递存在着一定的访问控制要求，具体要求如下：

①只允许动力环境监控数据单向传送给三区资源管理应用服务器；

②只允许传输网监控子系统内采集服务器数据单向传送给三区资源管理应用服务器；

③只允许传输网监控子系统内中兴、华为网管和采集服务器双向通信。

#### 3.2 访问控制列表安全解决方案

访问控制列表(Access Control List,ACL)是一系列指令的列表，用来告诉路由器(或三层交换机)哪些数据可以接收、哪些数据需要拒绝，由于访问控制列表应用于网络设备时，能有效地限制网络流量，拒绝外部用户对网络的非法访问，因此在二区内部，可使用访问控制列表实现网络安全要求<sup>[1]</sup>。

根据各个业务应用子系统的控制要求，可在二区部署一台三层交换机，交换机上共配置6个vlan，如表1所示。

表1 二区三层交换机vlan配置

vlan序号	vlan名称	端口	说明
7	caiji	fa0/45-46	用于与采集服务器互联
8	laojiankong	fa0/7-20	用于互联监控分站
10	geli	fa0/47-48	用于互联正向隔离装置
11	huawei	fa0/3-4	互联华为网管
12	zhongxing	fa0/5-6	互联中兴网关

在特定vlan的in方向，可配置访问控制列表，控制特定数据流传输。如在vlan12的in方向，配置ACL 101，实现只允许vlan28(中兴网管)去往vlan7(采集服务器)的数据包通过，配置语句如下：

```
access-list 101 permit ip 192.112.1.0 0.0.0.255
192.168.26.0 0.0.0.255
```

```
access-list 101 deny ip any any
```

```
int vlan 12
```

```
ip access-group 101 in
```

### 4 二三区物理隔离

#### 4.1 物理隔离的必要性及依据

在物理隔离技术出现之前，针对网络的信息安全可采取配置防火墙、进行入侵检测等措施，由于此类技术的保护是一种逻辑保护，对于逻辑实体而言容易被操纵。因此必须有一道绝对安全的大门，保证内网的信息不被泄露和破坏，这就是物理隔离所起的作用。

物理隔离是指内部网不直接或间接地连接外部网络，保护电力系统网络的路由器、工作站、网络服务器等硬件实体和通信链路免受自然灾害、人为破坏和恶意攻击。根据电力系统安全防护相关规定的要求，在安全区I/II与安全区III/IV之间必须进行物理隔离，实现最高的安全防护强度，这也是安全区I/II横向防护的要点<sup>[2]</sup>。

#### 4.2 二三区物理隔离改造方案

为实现安全区I/II与安全区III/IV之间的物理隔离，可在二区交换机与三区交换机间配置正向隔离装置一台，实现安全区I/II到安全区III/IV的单向数据传输。

由于正向隔离装置采用综合过滤技术，需预先设定规则检查数据包以决定哪些数据包允许通过。当隔离装置收到数据包后，将检查包头中的协议类型、源IP地址、目的IP地址、源端口号、目的端口号、源MAC地址、目的MAC地址等信息，再与设定的规则逐条匹配，以决定是否允许数据包通过。

根据通信监控系统各个业务应用子系统的控制要求，决定安全区I/II到安全区III/IV的数据控制目标如表2所示。

表2 安全区I/II至安全区III/IV数据控制目标

序号	数据控制目标
1	II区协议处理机1到III区应用服务器的单向UDP数据传送
2	II区协议处理机2到III区应用服务器的单向UDP数据传送
3	II区协议处理机3到III区应用服务器的单向UDP数据传送
4	II区协议处理机4到III区应用服务器的单向UDP数据传送
5	II区采集服务器到III区数据服务器的单向TCP数据传送

根据以上数据控制目标，需在正向隔离装置上

配置5条匹配规则，如表3所示。

表3 正向隔离装置配置规则

规则名称	内网侧配置	外网侧配置	协议
fep20	IP:192.168.9.*	IP:172.23.206.*	UDP
	MAC:F4ACC17D0D43	MAC:000000000000	
	虚拟IP: 172.23.206.*	虚拟IP:192.168.17.*	
fep21	IP:192.168.9.*	IP:172.23.206.*	UDP
	MAC:F4ACC17D0D43	MAC:000000000000	
	虚拟IP: 172.23.206.*	虚拟IP:192.168.17.*	
...			

通过在二三区之间配置正向隔离装置，实现了II区协议处理机到III区应用服务器的单向UDP数据传送，以及II区采集服务器到III区数据服务器的单向TCP数据传送。

## 5 互联省公司

防火墙是设置在内部网络与外部网络之间的一道屏障,用于控制出入两个网络之间的数据流,具备很强的抗攻击能力和审计、报警功能<sup>[3]</sup>。

为了满足省市公司联网服务器的数据交互要求，需实现省市公司三区网络的安全互联，为此在泰州通信监控系统的三区交换机与省通信数据网Cisco7606路由器间配置一台天融信硬件防火墙，并完成防火墙区域、网络对象、访问策略、通信策略、路由表等各项配置，从而确保省市公司三区网络间数据流量的安全传输及控制，保障网络自身安全。

## 6 改造后网络架构

改造完成后的通信集成监控系统网络架构如图3所示。

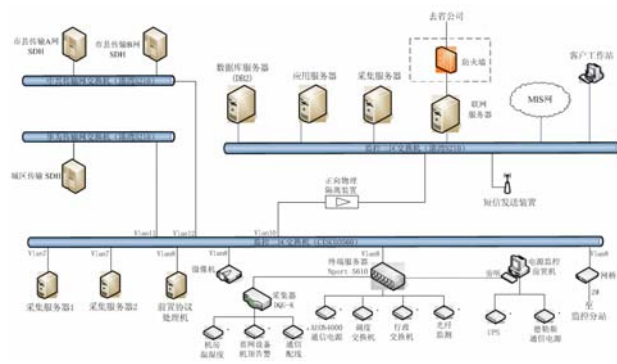


图3 改造后监控系统网络结构

图3中,同一区域内的各个子系统,如二区内传输网监控、动力环境监控等通过三层交换机上的ACL实现访问控制,不同区域间则通过正向隔离装置实现物理隔离,与省公司网络间又加装了硬件防火墙,从而确保了网络自身及内部各个子系统的运行安全。

## 6 结束语

在泰州电力通信集成监控推广建设过程中，通过对网络域进行细化划分，以及在不同区域间安装物理隔离装置，在不同子系统间配置访问控制列表，在省市公司三区网络间配置防火墙确保网络自身安全，从而实现了不同区域、不同子系统间的数据访问控制，优化了网络体系架构，降低了安全风险，提高了通信管理网络的安全管理水平，从而提高通信监控网络的运行管理效率，提高了运行维护水平和服务质量。

## 参考文献:

- [1] 王芳,韩国栋,李鑫. 路由器访问控制列表及其实现技术研究[J]. 计算机工程与设计,2007(12).
- [2] 王子,徐澄宇. 正向隔离装置在电力信息外网中的应用[J]. 电脑开发与应用,2010(08).
- [3] 张梁,赵翊军,肖丹. 硬件防火墙在数字图书馆中的应用[J]. 河北科技图苑,2008(05).

作者简介:

俞 浩 (1977—), 男, 江苏泰州人, 工程师, 主要从事通信运行管理、通信监控系统运行维护工作。