包钢轨梁厂局域网建设案例*

何亚利[1], 付志勇[2]

(1. 内蒙古包钢钢联股份有限公司轨梁轧钢厂, 内蒙古 包头 014010;
2. 包头轻工职业技术学院, 内蒙古 包头 014035)

摘 要: 包钢轨梁厂为实现办公自动化, 提高管理水平, 高效有序地组织生产, 最大限度地共享厂内资源, 构建了厂局域网。通过对局域网的设计、VLAN的重新划分、防火墙的配置和IP地址的分配, 实现了办公网络和生产网络相互隔离, 为轨梁厂信息化建设提供了有力的保障。

关键词: 局域网; VLAN; 防火墙; IP地址
中图分类号: TP393.1 **文献标识码:** B **文章编号:** 1009-5438(2017)04-0081-03
DOI:10.13647/j.cnki.btgkj.2017.04.023

LAN Construction Case of Rail and Beam Plant in Baotou Steel

HE Ya-li[1], *FU Zhi-yong*[2]

(1. *Rail and Beam Plant of Steel Union Co. Ltd. of Baotou Steel (Group) Corp.*, *Baotou* 014010, *Nei Monggol*, *China*;
2. *Bao Tou Light Industry Vocational Technical College*, *Baotou* 014010, *Nei Monggol*, *China*)

Abstract: In order to realize office automation, improve management level, organize production efficiently and orderly, and maximally share plant resources, Rail and Beam Plant in Baotou Steel has constructed LAN. Through the design of LAN, VLAN re-division, firewall configuration and IP address allocation to achieve the isolation between office network and production network, provide the strong guarantee for information construction in Rail and Beam Plant.

Key words: LAN; VLAN; firewall; IP address

包钢轨梁厂是以钢轨和型钢为主要产品的大型轧钢厂, 现有百米重轨和大H型钢两条生产线。这两条生产线的纵向长度可达1.5 km, 包括周边的附属工业建筑物, 全厂占地面积近25万m^2, 因此轨梁厂局域网具有传输距离远、覆盖范围广的特点。在运行过程中, 轨梁厂局域网除了要满足办公需求外, 还要满足生产需求。办公网络中的计算机频繁使用USB设备, 极易传染病毒而造成计算机或网络瘫痪, 但生产运行是7×24 h不间断的, 因此服务生产的网络7×24 h不能间断, 否则与生产有关的二级计算机控制、产量统计、检化验等操作不能实时进行。所以, 为轨梁厂局域网架设了防火墙, 对交换机进行了路由配置, 并重新划分了VLAN, 实现办公网络和生产网络相互隔离, 有效地解决了办公网络对生产网络造成干扰而影响生产的问题。

1 局域网设计

网络设计是一项富有挑战性的任务, 它不仅仅是把多台计算机简单的连接在一起, 还应具有多种特性以便于升级和管理。轨梁厂网络建设必须要:

* 收稿日期: 2017-05-08
作者简介: 何亚利(1982-), 女, 内蒙古包头市人, 高级工程师, 现从事软件开发、网络规划设计工作。

中国知网 https://www.cnki.net

①满足信息化发展的要求，为各类应用系统提供方便、快捷的信息通路；②具有良好的性能，能够支持大容量和实时性的各类应用；③能够可靠运行，具有较低的故障率和维护要求；④提供网络安全机制，满足信息安全的要求；⑤具有较高的性价比，未来升级扩展容易，保护投资。为此进行了网络设计、网络拓扑结构设计、综合布线系统总体结构设计和工作区子系统设计。

1.1 网络设计

网络设计要根据工程项目对网络的需求及采用技术的成熟性、可扩充性和发展空间而进行的，因此网络设计需要满足的原则如下：①满足工程项目对计算机网络系统的总体要求，符合兼容的系统运行环境要求；②先进性与实用性结合，设计时效年限至少为五年，充分利用设备的扩充能力可保证十年的设计时效；③极大的灵活性和扩充性，满足业务数据快速增长的需要；在保证系统需求的前提下，尽量节约开支，降低运营成本；④高度的可靠性，网络设备和网络拓扑应具有冗余性，在连接失败时，能有迂回路由；⑤高度的安全性，能防止网络的非法访问，保护关键数据不被非法窃取、篡改或泄露；⑥良好的管理性，简化网络日常维护工作，增强故障处理能力；为主机系统、应用系统、数据库系统提供良好的网络平台，保证应用系统的反应速度不会因为网络性能的原因而降低[1]。

1.2 网络拓扑结构设计

在网络拓扑结构设计中采用层次型拓扑结构设计，它是一种使用分层的、模块化的模型设计局域网的技术。层次型拓扑结构设计自上而下分为三层：即核心层、汇聚层和接入层。层次型拓扑结构设计可以按层设计拓扑结构，每层的重点集中于特定的功能上，这样有利于分配、规划带宽，选择适当的网络设备等。结合层次型拓扑结构设计的优点和轨梁厂网络需求分析，轨梁厂局域网选用了这种层次型拓扑结构，通过多级交换机分级连接实现。核心层部署在集团公司信息处，从核心层以下部署在轨梁厂，核心层到汇聚层通过光纤连接，轨梁厂局域网从汇聚层开始设计，深信服防火墙、思科3750交换机、思科3560交换机、360卫士防火墙作为主要的网络设备，对它们进行了路由、NAT地址转换、访问控制策略等配置和VLAN的划分，不同的部门接入不同的VLAN，这样个别网点出现故障不会影响全局，从而使网络具有可靠性高、可扩展性好、易于管理等特性。轨梁厂局域网具体建设方案如图1所示。

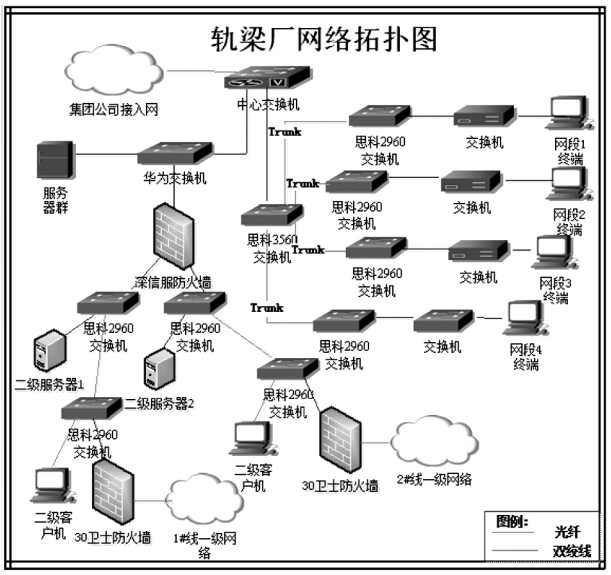


图1 轨梁厂网络建设规划方案图

根据设计好的网络规划图，尽量利旧现有网络设备，补充必要的核心网络设备，在选取经济最优方案减少二次投资的指导思想下，将网络规划方案图转化为网络拓扑图。

1.3 综合布线系统总体结构设计

布线是一项隐蔽工程，有大量线缆是预埋的，不易调整和更换，正常情况下，在十年以内是不应该出问题的[2]。而且布线也要选择好的环境，要尽量远离电磁波等的干扰。另外，综合布线是整个网络建设的基础，如果做得不好，会成为网络的瓶颈，因此要从材料的选择到施工的规范上进行严格的现场监督。轨梁厂根据传输距离的远近、周围的环境、传输速度的要求等情况，选择使用多模、单模光纤以及UTP双绞线相互结合的方式布线。与集团公司主干网采用单模光纤连接，各办公地点楼宇间与中心机房采用多模光纤布线，工作区与用户终端采用UTP双绞线接入。在布线过程中也严格遵循国际标准，如EIA/TIA568A或EIA/TIA568B，并有专人专责现场监督，保证施工质量。

1.4 工作区子系统设计

工作区子系统由各个单元区域构成，是计算机、电话和信息插座的连接部分，包括连接跳线和信息插座。信息插座面板具备：通用、超薄、简易、防尘等特点；信息插座的模块采用RJ-45模块；线缆采用超五类双绞线；水晶头采用RJ-45标准水晶头。为

中国知网 https://www.cnki.net

降低成本和结合客户终端的位置多变的特点，跳线可采用原装跳线与自制跳线相结合的方式，中心机房内设备之间、楼宇机柜内设备之间、服务器、重点客户终端的跳线采用原装成品跳线，其余采用自制跳线。跳线制作统一采用 EIA/TIA 568B 标准，以使系统具有更好的兼容性。

2　VLAN 划分

虚拟局域网(VLAN，Virtual Local Area Network) 技术在局域网中起到了举足轻重的作用，应用 VLAN 技术可以提高局域网的效率和安全性，便于对用户的管理。一方面，如果将业务来往比较频繁，通信量较大的部门分配在一个 VLAN 中，就可以保证这些部门之间使用二层交换协议，而业务来往少、通信量少的部门则采用三层交换协议通信，这无疑大大提高了网络的效率; 另一方面，一个 VLAN 就是一个独立的广播域，划分 VLAN 可以减少广播风暴，节约带宽; 且 VLAN 之间是互相隔离的，这样也确保了网络的安全性和保密性。

VLAN 可以根据功能、用途、工作组以及应用等因素将用户逻辑上划分为一个相对独立的网络，是一个可跨越不同地理位置的端到端的网络。根据 VLAN 在交换机上的实现方式可分为: ①基于端口的 VLAN; ②基于 MAC 地址的 VLAN; ③基于网络地址的 VLAN; ④基于用户的 VLAN。其中后三者为动态 VLAN。

包钢轨梁厂采用了基于端口的静态 VLAN。将整个轨梁厂的局域网根据地理位置的不同和部门的不同划分成不同的区域，每个区域属于一个 VLAN，每个区域之间都不能相互通讯，但通过对思科 3750 交换机进行路由配置，使得每个区域都可以与服务器群通讯。这样防止了病毒的蔓延，也提高了网络的安全性和保密性。VLAN 划分具体在思科 3750 交换机上实现。轨梁厂具体的 VLAN 划分如图 2 所示。

3　防火墙的配置

3.1　配置地址转换

地址转换是为了实现内外网络之间的通信而将 IP 数据报中的一个 IP 地址转换成另一个 IP 地址的过程，地址转换分为静态地址转换和动态地址转换，轨梁厂局域使用静态地址转换，把两条生产线的二级服务器及二级客户端的私有地址都转换成可以访问办公网络的地址，防火墙地址转换如图 3 所示，这样就保证了二级客户端既可以访问二级服务器，也可以在网上进行交接班点巡检、办公自动化等操作。

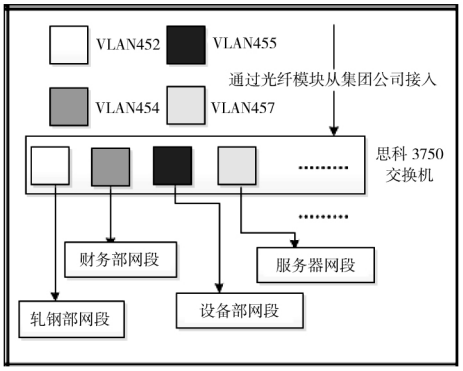


图 2　思科 3750 交换机上的 VLAN 划分



图 3　防火墙地址转换

3.2　配置路由

配置路由是为了使转换后的地址可以访问集团公司网络，二级服务器可以和 ERP 进行通讯，并收发电文。如果没有该路由，即使地址转换了，也只可以访问轨梁厂办公网络，无法访问集团公司网络，因为转换后的地址是处于 10.11.18.224(网络号) 网段，在思科 3750 交换机上该网段是通过地址 10.11.18.254 出去的，所以在图 4 所示的路由配置窗口中，目的地址和子网掩码输入公司网的网络地址和掩码，下一跳地址输入是 10.11.18.254。



图 4　防火墙静态路由配置

(下转第 98 页)

中国知网　https://www.cnki.net

主梁下挠缺陷的桥式起重机的修旧利废、节约维修成本、恢复和增强起重机性能及保证安全生产等提供了技术保障。诸多措施保障了主梁的承载能力和性能，修复后在同样的载荷条件下，保证了起重机主梁的工作安全和保持拱度数值及增强效果的长久稳定性。使用若干年后，如果拱度数值及增强效果万一发生变动可再调整撑顶器螺母或二次张拉，恢复效果非常简单。

参 考 文 献

[1] 王冠华. 梁式起重机主梁下挠的修复方法及其梁式起重机 [P]. 中国专利: 200610166875.4，2016－12－17.

[2] GB/T 14405—93，通用桥式起重机 [S].

[3] GB 5905—86，桥式起重机试验规范和程序 [S].

(上接第83页)

3.3 配置访问控制策略

为了保证网络的安全性，还配置了访问控制策略，如图5所示。



图5 防火墙访问控制策略

4 IP地址分配

所谓IP地址就是给每一个直接与局域网相连的计算机分配一个在轨梁厂范围唯一的网络地址。目前，使用的是32位的IPV4地址，寻址时先按IP地址中的网络号net－id把网络找到；当找到目的网络后，再用ARP协议使用主机号host－id找到主机[3]。

轨梁厂使用了4个私有的A类IPV4网络地址10.X.18.0、10.X.16.0、10.X.19.0、10.X.17.0来构建自己的局域网，其中10.X.16.0和10.X.17.0只在轨梁厂内部使用，10.X.18.0和10.X.19.0可以接入集团公司，方便访问集团公司的主页、与集团公司相互传递文件以及上报轨梁厂生产数据等。IP地址都是静态分配的，没有设置专门DHCP服务器。为了达到较好的网络质量，方便管理，防止病毒的蔓延，又把这4个网络地址划分了不同的网段，分别分配给不同的部门。

5 结束语

包钢轨梁厂局域网建成以后，最大限度地共享了厂内的硬件资源，如打印机、扫描仪等，节约了厂内的开支；减少办公文件的流转时间，提高了员工的工作效率，提升了管理水平；同时也节约了纸张，为轨梁厂信息化建设提供了有力的保障，也为以后接入集团公司ERP打下了坚实的基础。

参 考 文 献

[1] 谢希仁. 计算机网络(第4版) [M]. 北京：电子工业出版社，2003.

[2] 刘晓辉. 网络设备配置与管理实战详解 [M]. 北京：化学工业出版社，2010.

[2] 金刚善，包英捷，赵博，等. 局域网组建和管理入门与提高 [M]. 北京：人民邮电出版社，2004.

中国知网 https://www.cnki.net