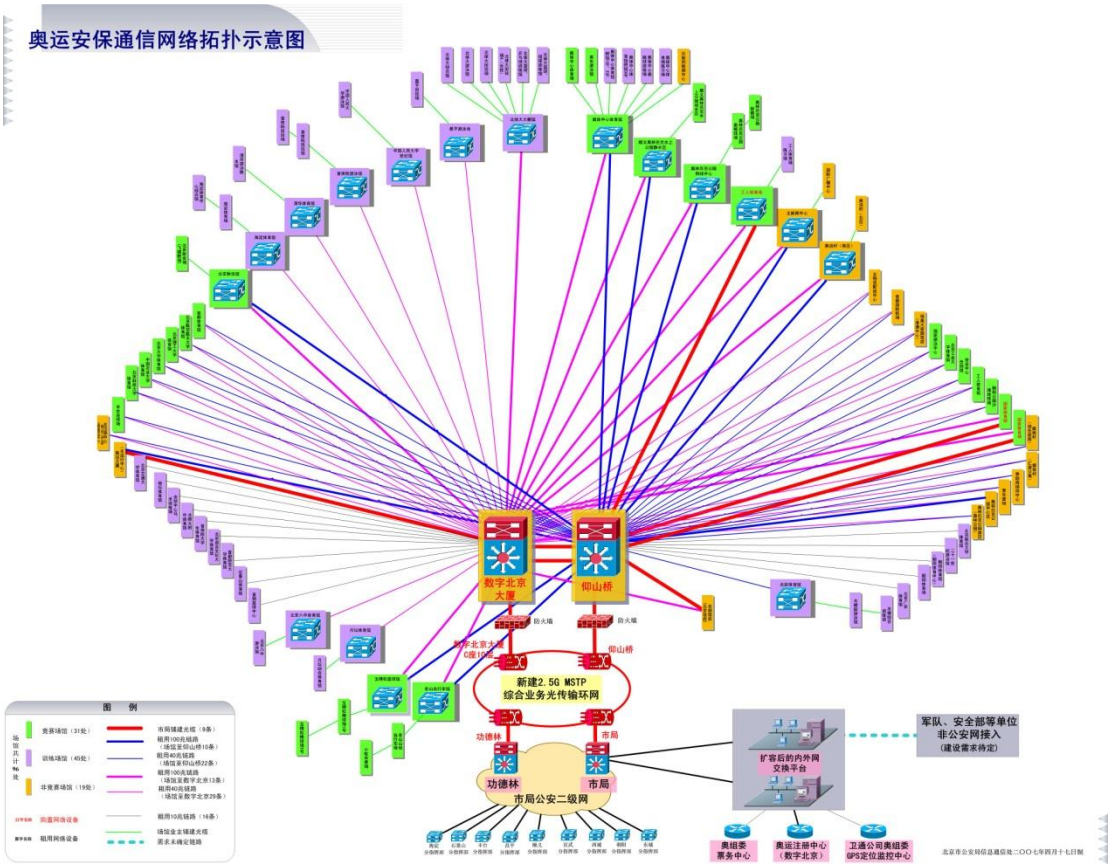
论信息系统建设的网络规划

2008 年奥运会期间的安全保卫工作对于奥运会能否成功举办有着至关重要的作用，为坚实有力地支持奥运安保工作，北京市公安局需要在所有奥运竞赛、非竞赛，以及相关训练场馆之间构建北京市公安局奥运安保信息专网。作为市局信息通信处的一名技术骨干，我有幸参与了奥运安保网的规划、设计，并组织参与了整个项目的招标、工程建设，以及奥运期间该网络的运行维护工作。

此次网络建设任务涉及 31 个竞赛场馆、19 个非竞赛场馆、45 个训练场馆共 95 个网络节点，并且需要与现有公安专网实现安全的互联互通。经过反复论证与综合比较，并考虑到奥运资金预算情况。我们选择“租用为主，自建为辅”的建网方式，也就是网络设备租用 CISCO 的，链路租用网通的，个别重要节点链路选择自行建设。最终整个网络系统分 3 层，分别是市局核心网络、奥运核心网络、场馆局域网。如图所示



1.拓扑规划

奥运会的特殊性，以及安全保卫工作的重要性决定了安保网的可靠性是第一位的。由于各个场馆物理位置分散，因此奥运安保网总体拓扑选择星性结构，任意节点故障不会影响其他节点。奥运安保网核心采用异地双核心结构，从根本上避免出现单点故障。为了与原有公安专网互联，同时为了保证 4 个核心之间的链路可靠。在 4 个核心处建设一套 2.5G 的 MSTP 环网，4 个核心之间的互联链路构建在这个环网之上，考虑到奥运赛时网络通信流量主要集中在奥运安保网内部，因此奥运两核心之间的传输带宽分配 800M，其他 3 条链路分别是 500M。

奥运竞赛场馆、非竞赛场馆作为奥运会主要的比赛、工作地点，链路的可靠性也是第一位的。因此所有场馆租用网通 2 条不同路由走向的电路分别接入到奥运两个核心。并且每条

电路都构建在网通 ASON 传输环网之上。

训练场馆由于不对外开放，因此安保级别有所降低，从经济性、实用性的角度考虑，每个场馆租用 1 条网络电路到奥运其中一个核心。

2.设备选型

设备选择也是把可靠性放在第一位。由于原有公安专网全部都是 cisco 网络设备，同一厂商的设备兼容性更好，并且现有技术人员对 CISCO 设备比较熟悉，因此奥运所有网络设备都选择 CISCO 品牌。奥运双核心使用 CISCO6509，竞赛、非竞赛场馆选择 CISCO ME 3750，训练场馆选择 CISCO 2821。其中为了保证绝对可靠，CISCO6509 采用双引擎 SSO 方式、双电源热备，风扇、板卡等不能热备的部件采用冷备的方式。所有场馆 CISCO ME 3750 采用双电源模块，分别接场馆 UPS 以及市电。部分重要场馆配备 2 台 CISCO ME 3750，通过 TRUNK 互联，使用 HSRP 协议防止出现单点故障。

3.路由协议规划

原有公安专网内部路由使用 OSPF 协议，已经稳定运行 8 年。奥运安保网必须在对现有网络影响最小的情况下与之实现互联互通。考虑到 OSPF 路由协议调整策略更灵活，易于网络维护和排障，并且现有技术人员对 OSPF 协议熟悉程度更高。因此我们选择将奥运安保网作为现有 OSPF 区域中的一个子区域与整个公安专网实现互联互通。现今三层交换机处理性能已经得到极大提升，一个 OSPF 区域可以支持上百台设备，因此所有双上联链路场馆直接加入这个 OSPF 子区域。单上联链路场馆由于只有唯一出口链路，因此使用静态路由方式注入奥运安保网子区域。

为了与现有公安专网实现安全的互联互通，奥运安保网与公安专网之间的两条链路上都必须部署防火墙。由此就会产生一个严重的问题，同一个网络会话的请求与响应将可能走不同的防火墙，防火墙将会认为这个会话是不完整连接而直接丢弃，造成部分网络中断。为了避免这个情况的产生，需要调整 OSPF 路由协议的参数，增加其中一条链路两端的 OSPF COST 数值，使之变成不等效路由。并且需要在原有网络核心 6509 之间增加一条奥运安保子 AREA 的链路，避免出现子 AREA 路由优先的情况。

4.场馆局域网优化

奥运场馆内网络的主要应用是视频监控、可视化指挥、信息查询比对等。通过分析信息流向以及信息流数据大小，我们使用 VLAN 手段把不同应用类型流量隔离开。部分配备了 2 台 CISCO ME 3750 的场馆，通过使用 HSRP 技术，调整每个交换机 VLAN 的 priority 值，使不同的 VLAN ACTIVE 在不同的交换机上。即充分利用两条上联链路实现流量分担，又保证两个交换机实现简单备份，还能使不同类型流量互不影响，减少视频数据的延迟、抖动。

5.网络管理设计

全网采用静态 IP 地址，每个入网设备需要注册才能使用，做到每个 IP 地址责任到人。

奥运双核心 CISCO 6509 配备了 NAM 模块，可以监控各种应用情况，如协议分布比例、使用此协议的主机、流量最大的前 10 台主机、服务器响应时间等。通过实时监控这些数据，发现非正常流量，定位异常主机 IP，再根据静态 IP 地址分配数据库找到责任人，及时把故障消灭在萌芽状态。

由于全网使用 CISCO 设备，因此网管软件使用是 CISCOWORKS2000 网管系统，通过它实现网络拓扑展现、故障节点告警、SYSLOG 日志保存等工作。虽然 CISCOWORKS2000 支持网络配置管理，但它是基于软件通过 SNMP 写口令完成相关操作，为了保证万无一失，所有设备必须关闭 SNMP 写权限，只开通 SNMP 只读权限并且通过 ACL 限制管理服务器 IP。

经过“好运北京”测试赛以及奥运会的检验，建成后的网络系统完全满足公安各业务单位的应用需求，并且实现了奥运期间零故障的佳绩，为最终安全举办一届“无与伦比”的奥运会提供了技术保证。由于此次项目的重要性以及特殊性，在网络方案设计时首先考虑的是

安全性和可靠性，导致最后因为安全原因或者实现起来复杂程度过高，一些很好的功能最终不能使用。一是全网缺少 IP-SLA 服务水平检测，当出现服务质量问题的时候不能准确的定量、定性分析故障发生的原因，并且在故障的责任认定上缺少技术手段。CISCO6509、CISCO ME 3750 的 IOS 都支持 IP-SLA，网管软件 CISCOWORKS2000 也有 IPM 模块可以统一进行网络性能监视，可是因为需要在交换机配备 SNMP 写权限，最终这个功能被放弃了。二是全网没有部署 QOS 机制，只有个别配备了 2 台 CISCO ME3750 的场馆实现了部分流量分担，其他大部分场馆视频、语音、数据流量混杂在一条链路中传输，当出现大规模监控视频调用时存在潜在威胁。