

全国行业信息化优秀产品
国家科技部项目

香农集成 IT 架构管理平台
----综合网络管理系统
行业解决方案集锦

2009年8月

云南香农信息技术有限公司

Http: //www. shanon. org

全国免费服务电话: 800 889 0700

目 录

一、Intraware 某政府网络 ARP 病毒自动控制阻断	3
二、保障我的网络带宽	5
----- 某厅级机关网络的BT、迅雷等异常流量控制	5
三、INTRAWARE 的制胜秘诀之一 ---- 提升执行力	6
四、INTRAWARE 的制胜秘诀之一 ---- 精细化管理	8
五、金融行业广域网络链路管理案例	14
六、从云南机场集团有限公司各机场的综合网络管理系统应用看智能化的网管实现	15
七、多种网络准入控制技术的组合应用- Intraware	17
八、谈INTRAWARE 大学校园网络管理	18
九、市级电网公司如何管好广域网络？	24
十、网络管理，从用户管理开始(在特大国有企业的应)	26
十一、INTRAWARE ,护航国家重点工程“金质工程”	30

一、Intraware 某政府网络 ARP 病毒自动控制阻断

某政府单位局域网内的有 400 台电脑, 23 台交换机, 交换机分布在 11 个楼层, ARP病毒是让这里的网络管理员最头疼的事, “ARP病毒”发作时发出大量的数据包, 导致网络运行不稳定, 频繁断网、IE 浏览器频繁出错以及一些常用软件出现故障等问题, 极大地影响了局域网用户的正常使用。arp欺骗有一个特点就是隐蔽性强, 一台机器感染后全网段机器都受影响, 故障一样。所以网络管理员很难找出真正的病毒来源。

最近, 该政府单位网络中心根据网络管理的需要, 降低网络运维难度, 在对众多品牌的网管软件招投标、筛选、评估之后, 引进了香农 Intraware 综合网络管理系统。在实施后, 困扰这里网络管理员和用户的最大问题得到了解决, 该单位对香农 Intraware 综合网络管理系统非常满意。

香农 INTRAWARE 综合网络管理系统的 ARP 病毒控制功能具有以下特点:

1、零客户端部署。不在客户端安装任何软件, 也不改变客户端电脑的任何配置。

2、快速发现病毒。当网络中有 ARP 病毒时, Intraware 这个放大镜能快速找出真凶, 并把病毒源所在设备的接口、接口连接的用户数、病毒主机的 mac 地址、病毒主机当前的状态、攻击的次数, 攻击时间等信息显示出来。

3、多种处理方式

当发现网络中有 ARP 病毒时, 香农 Intraware 综合网络管理系统有多种处理方式, 可以定制策略让系统自动处理, 也可以手动处理, 自动处理和手动处理又分为如下方式:

(一) 自动方式

封 MAC 自动对中病毒主机的 MAC 进行封锁, 中断通病毒主机通信。

关端口 自动对中病毒主机所在设备的端口进行关闭, 中断病毒主机通信。

邮件告警 通过邮件，自动把中病毒主机信息告知网络管理员

图形告警 自动在系统界面上以其它的明显图标显示中病毒主机。

(二) 手动方式

封 MAC 手动对中病毒主机的 MAC 进行封锁，中断通病毒主机通信。

关端口 手动对中病毒主机所在设备的端口进行关闭，中断病毒主机通信。

4、坚固的 LINUX 操作系统运行平台, 自身很少受到病毒滋扰。

二、保障我的网络带宽

----- 某厅级机关网络的BT、迅雷等异常流量控制

某厅级机关外网网络有近 200 台电脑，通过 10M 的互联网出口上网，但网络使用一直不畅，网内少数人上班时使用 BT、迅雷、快车等下载，产生了大量的网络流量，占用了宝贵的网络带宽。很多时候正常的网页浏览、邮件收发都经常受到影响。

该厅机关网络部署了香农 INTRAWARE 综合网络管理系统后，不但从技术上保障了网络使用正常化，而且还真正捍卫执行了相关的公务员工作规范！加强了机关文化建设。

保障网络带宽，INTRAWARE 是从如下方面做到的：

一、只须部署一套综合网络管理服务器，不在客户端安装任何软件，也不改变客户端电脑的任何配置。

二、BT、迅雷等下载工具会极大占用网络带宽，如不加以疏导与防范控制，数个下载用户即将耗尽有限的网络带宽资源。BT、迅雷类下载工具的数据特征与病毒攻击数据差异如下：病毒攻击数据包绝大多数为短包，流量不大，而网络连接会话数极大，端口数变化或不变化。BT 下载数据包大多数为长包，流量大，网络连接会话数极大，端口数变化。

应用主动 BT 防御策略，可以设置网络连接数或流量阈值，对超出阈值的用户自动实施相应的定制策略。目前的 BT 下载及迅雷等工具，为了达到极速下载的目的，基于网格原理，采用了多资源超线程技术，采用了各种网络传输协议，所以单靠传统的封堵方式是无法封堵迅雷的封堵的，香农 Intraware 在采用多协议交叉封堵等技术基础上，结合了大量的实际管控经验，采取用户分组，分配不同带宽优先级的策略，专设一个低带宽（如 1K 或 10K）的黑名单用户组，对 BT 或迅雷使用达到一分钟（时间可定义）的用户，就自动打入黑名单，从而达到控制目标。

三、INTRAWARE 的制胜秘诀之一 ---- 提升执行力

网络管理永远是一场未决胜负的战争！

赢得一场现代战争，需要多兵种协同作战、多层次火力相互掩护，要求指挥系统获取信息及时准确、决策前瞻、执行有力。Intraware 正是这样一套以立体化、系统化、集成化为支点，集成网络设备管理统合用户管理、拓扑管理、流量与协议分析、带宽与流量控制、主机及业务应用性能监测、IT 资源管理、身份认证、上网行为管理为一体的统一管理平台。而强大的执行力，则是 Intraware 在众多网管软件中脱颖而出的制胜法宝！

一、平台之争

Windows 平台与 Linux 平台之争从未平息。但在网络运维工作中，网络病毒肆虐、各种突发与异常事件横行，得先保证咱网络管理软件系统自身平台健康运行吧？这就相当于，你驾驶木船去营救木船或你驾驶军舰去营救木船一样的区别。谁是军舰，谁是木船，呵呵，不言而喻。

二、拓扑图不是用来看的

网络拓扑图到底有什么用？对 IT 运维人员起到什么样作用？

对于一般用户而言，那么几百台电脑，一、二十台网络交换机，网络拓扑图早已烂熟在心，这个拓扑图不看也罢！因此，我们发现，用户希望看到的不是拓扑图，而是当前网络运行的一个全盘状况！

B/S 架构已经是当前软件技术架构不争的标准。但 J2EE 开发技术应用在网管软件上，则具有网络拓扑图交互操作能力的巨大优势。

香农 INTRAWARE 的网络拓扑图突出的是对网络运行管理维护的执行力提升，在这个拓扑图上，方便即时地得到所有服务器、PC 机、交换机、路由器、链路的实时状态，包括：故

障情况、接入情况、流量情况、链路连接及双向速率、用户访问日志，可以在实时获得的拓扑图形上针对设备进行配置、监测、分析、以及运用各种运维策略。

三、从什么方面提升网络运维管理执行力

传统的设备厂商网络管理软件，重点是解决一些设备性能的监测，提供一些方便的配置、调试工具。而第三方网管软件，则把重点放在了支持多厂商的能力、提供一些综合分析统计的报表和工具等等。这些网管软件系统，强调了监测、分析，却忽视了最重要的“管理”角色。香农 INTRAWARE 认为，真正的 IT 运维管理系统，最重要的是管理与控制的执行能力，如果在针对一大堆各种各样的报表进行大量人工分析之后，才能做出一些判断的系统，是没有执行力的系统。仅根据统计报表数据，提供大量趋势分析的系统，不可能变被动为主动。当今的 IT 运维应该是运用知识与经验，懂得学习与分享，有前瞻与策略的运维。香农 INTRAWARE 是一个具备强大控制与管理策略定制能力的系统，真正实现 IT 运维的可管理，全面提升了网络运维管理执行力。

四、INTRAWARE 的制胜秘诀之一 ---- 精细化管理

精细化不是什么新东西，作为一种追求精益求精的努力，自古以来那些做事认真的人就已经在做了！

精细化管理是超越竞争者、超越自我的需要，是管理者实现从监督、控制为主的角色向服务、指导为主的角色转变，更多关注满足被服务者的需求，实现 IT 系统可持续发展的必然途径。

“管理好的 IT 系统，总是单调无味，没有任何激动人心的事件。那是因为凡是可能发生的危机早已被预见，并已将它们转化为例行作业了。”对 IT 系统来说，没有激动人心的事发生，说明 IT 系统的运行时都处于正常控制之中，而这只有通过每天、每个瞬间严格地对细节加以控制才有可能实现。IT 系统的运维管理从粗放走向精细非常重要，这已成为有效管理的关键一环。

理解香农 INTRAWARE 的 IT 运维精细化管理

IT 运维的精细化管理是一种管理理念和管理技术，是通过规则的系统化和细化，运用程序化、标准化和数据化的手段，使组织管理各单元精确、高效、协同和持续运行。精细化管理要求在管理中多用“数学”，重点是关注细节、数据和工具！少用或不用“语文”，而不应该是权力、经验、感觉、判断！

IT 运维精细化管理的，可以从以下方面理解：

（一）、IT 运维精细化管理首先是一种科学的管理方法。管理是组织将有限的资源发挥最大效能的过程。要实现精细化管理，必须建立科学量化的标准和可操作、易执行的作业程序，以及基于作业程序的管理工具；

1、科学量化的标准

香农 INTRAWARE 满足各种设备的管理数据读取，具有强大的数据统计与分析报表工具，各种统计图形工具提供了直观的取数、对比、分析的方法。同时，一个管理知识库的建立非常重要，管理知识库形成一个科学量化的管理标准库，比如：网络设备故障的判定依据、异常流量的判定依据、控制策略的执行依据、控制规范的制定方法等等。

2、可操作、易执行的作业程序

如前所述，管理者要实现从监督、控制为主的角色向服务、指导为主的角色转变，更多关注满足被服务者的需求，IT 运维精细化管理，应是对 IT 运维管理人员以及被服务者的解放。尊重管理者与服务者两者的习惯很重要，INTRAWARE 尊重和保留甚至优化产生客户价值的流程，精简和剔除不产生客户价值的流程，比如：INTRAWARE 在实现强大的管理、控制，优化 IT 服务质量的同时，零客户端软件部署的方式，不给 IT 运维管理人员与被服务者增加任何格外的负担。再比如：即使是实现如此强大的端对端管理与控制策略，INTRAWARE 系统在安装部署到系统的投入应用，均无须人工干预初始数据的设定，自动执行从宏观拓扑发现、综合系统运行状态、IP-MAC-交换机接口的对应关系或绑定、IP MAC 变化前后的状态、链路连接各端口的前后变化、ARP 病毒的影响等等，

3、基于作业程序的管理工具

在 IT 运维管理系统中，立体化、系统化、智能化的集成运维管理平台是 IT 运维中管理者、被服务者双赢的关键。智能化地应对即时的管理问题，则是管理作业程序中能决定成败的细节。基于大量的数据统计分析（甚至包括所谓的趋势分析），对于追溯历史有着根本的意义，而当今的 IT 运维风险来自于各个不可预知的领域，单纯依靠一些所谓趋势分析预测工具来进行即时管理就力不从心了。INTRAWARE 认为，所有 IT 运维工作中遇到的即时风险和问题，尽管有着各不相同的外在表现，但从技术根源来看，都可以归纳为对应用、设备、流量、协议、用户五个方面不同的影响，对其进行重点监护，自动实施管控策略，详细定义触发规则、触发流程，一切均可根据精细化管理战略制定详尽的目标与策略，成为香农 IT 运维管理系统的核心竞争力。

(二)、实施 IT 运维的精细化管理目的是基于组织战略清晰化、内部管理规范化、资源效益最大化的基础上提出的，它是组织个体利益和整体利益、短期利益和长期利益的综合需要。

(三)、实施 IT 运维的精细化管理不是一场运动，而是持续改善的“计划-执行-检查-改进”循环的过程，是自上而下的积极引导和自下而上的自觉响应的常态式管理模式。

IT 运维管理的精细化管理原则

IT 运维精细化管理有三大原则：1，注重细节；2，立足专业；3，科学量化。只有做到这三点，才能使精细化管理落实到位。

举几个例子，来看一看 IntraWare 的 IT 运维精细化管理是如何实现的：

图 1 用户管理：用户信息、组织信息、IP、MAC、信息插座等等

序号	区域	姓名	帐号	部门	属性	认证方式	IP地址	MAC地址	开户日期	信息插座	办公室序号	备注
1	办公室	1104-1	张德强	市场部	普通	IP	10.1.18.133	0030-e637594	2008-12-25	94102	3104	
2	办公室	1104-2	张德强	市场部	普通	IP	10.1.18.80	0030-e6375d4	2008-12-25	94101	3104	
3	营销中心	1105-1	张德强	市场部	普通	IP	10.1.18.138	0030-e6375e1	2008-12-25	94103	3105	
4	营销中心	1105-1	张德强	市场部	普通	IP	10.1.18.81	0030-e6375d2	2008-12-25	94106	3105	
5	营销中心	1105-2	张德强	市场部	普通	IP	10.1.18.82	0030-e6375d3	2008-12-25	94105	3105	
6	营销中心	1105-3	张德强	市场部	普通	IP	10.1.18.140	0030-e6375e4	2008-12-25	94108	3105	
7	营销中心	1105-1	张德强	市场部	普通	IP	10.1.18.79	0030-e6375d7	2008-12-25	94107	3105	
8	营销中心	1105-2	张德强	市场部	普通	IP	10.1.18.139	0030-e6375e2	2008-12-25	94104	3105	
9	营销中心	1105-3	张德强	市场部	普通	IP	10.1.18.136	0030-e6375e3	2008-12-25	94103	3105	
10	营销中心	1105-1	张德强	市场部	普通	IP	10.1.18.111	0030-e6375d5	2008-12-25	94109	3105	
11	营销中心	1105-2	张德强	市场部	普通	IP	10.1.18.84	0030-e6375d6	2008-12-25	94110	3105	
12	营销中心	1105-3	张德强	市场部	普通	IP	10.1.18.83	0030-e6375d8	2008-12-25	94112	3105	
13	营销中心	1105-4	张德强	市场部	普通	IP	10.1.18.87	0030-e6375d9	2008-12-25	94111	3105	
14	营销中心	1105-1	张德强	市场部	普通	IP	10.1.18.135	0030-e6375d4	2008-12-25	94107	3105	
15	营销中心	1105-2	张德强	市场部	普通	IP	10.1.18.85	0030-e6375d5	2008-12-25	94108	3105	
16	营销中心	1115-1	张德强	市场部	普通	IP	10.1.18.148	0030-e6375e4	2008-12-25	94113	3115	
17	营销中心	1115-2	张德强	市场部	普通	IP	10.1.18.86	0030-e6375d6	2008-12-25	94114	3115	
18	营销中心	1115-3	张德强	市场部	普通	IP	10.1.18.122	0030-e6375d6	2008-12-25	94113	3115	
19	营销中心	1115-4	张德强	市场部	普通	IP	10.1.18.130	0030-e6375d4	2008-12-25	94113	3115	
20	营销中心	1115-1	张德强	市场部	普通	IP	10.1.18.100	0030-e6375d8	2008-12-25	94115	3114	
21	营销中心	1115-2	张德强	市场部	普通	IP	10.1.18.144	0030-e6375e7	2008-12-25	94115	3114	
22	营销中心	1115-3	张德强	市场部	普通	IP	10.1.18.101	0030-e6375d9	2008-12-25	94116	3114	
23	营销中心	1115-4	张德强	市场部	普通	IP	10.1.18.146	0030-e6375e9	2008-12-25	94118	3114	
24	营销中心	1104-3	张德强	市场部	普通	IP	10.1.18.77	0030-e6375d7	2008-12-25	94108	3104	
25	营销中心	1104-4	张德强	市场部	普通	IP	10.1.18.125	0030-e6375d7	2008-12-25	94108	3104	营销中心

图 2 IP+MAC+端口：IP、MAC、设备名称及设备端口对应表

序号	IP地址	Mac地址	设备名称	设备IP	设备接口	允许绑定	index
1	10.1.1.30	001243f051e0	VMXC-5F-6506-W	10.1.0.1	E4/0/4	允许	268435970
2	10.1.1.166	00127955ba40	VMXC-5F-6506-W	10.1.0.1	E4/0/3	允许	268435842
3	10.1.200.18	001517877e11	VMXC-5F-6506-W	10.1.0.1	E4/0/2	允许	268435714
4	10.1.36.41	0010a5f76949	VMXC-23F-3050...	10.1.0.4	E0/40	允许	6658
5	10.1.36.90	00a0a000144d	VMXC-23F-3050...	10.1.0.4	E0/36	允许	5122
6	10.1.36.92	00a0a000544e	VMXC-23F-3050...	10.1.0.4	E0/44	允许	6146
7	10.1.39.35	0010e6074e0a	VMXC-23F-3050...	10.1.0.4	E0/45	允许	6274
8	10.1.39.39	001e90815344	VMXC-23F-3050...	10.1.0.4	E0/39	允许	5506
9	10.1.39.41	001921496407	VMXC-23F-3050...	10.1.0.4	E0/8	允许	1410
10	10.1.39.55	0010a5f7f08a	VMXC-23F-3050...	10.1.0.4	E0/12	允许	1922
11	10.1.39.183	0010a5f7e17b	VMXC-23F-3050...	10.1.0.4	E0/47	允许	6530
12	10.1.31.54	0019214c49c9	VMXC-23F-3050...	10.1.0.5	E0/18	允许	2690
13	10.1.31.87	001e904b2c36	VMXC-23F-3050...	10.1.0.5	E0/41	允许	5762
14	10.1.31.67	002354665eef	VMXC-23F-3050...	10.1.0.5	E0/33	允许	4738
15	10.1.31.98	0019214f4c24	VMXC-23F-3050...	10.1.0.5	E0/12	允许	1922
16	10.1.31.128	0019214d3fe4	VMXC-23F-3050...	10.1.0.5	E0/20	允许	2946
17	10.1.36.32	00105cb2c34f	VMXC-23F-3050...	10.1.0.5	E0/21	允许	3074
18	10.1.36.40	00a0a0000560	VMXC-23F-3050...	10.1.0.5	E0/19	允许	2818
19	10.1.36.42	001bfec15467	VMXC-23F-3050...	10.1.0.5	E0/21	允许	3074
20	10.1.36.43	00a060a90441	VMXC-23F-3050...	10.1.0.5	E0/17	允许	2562
21	10.1.36.53	0010a5f80444	VMXC-23F-3050...	10.1.0.5	E0/11	允许	1794
22	10.1.36.61	0040b7e08c7b	VMXC-23F-3050...	10.1.0.5	E0/17	允许	2562
23	10.1.38.108	00090ba18307	VMXC-20F-3050...	10.1.0.6	E0/25	允许	3714
24	10.1.38.29	00a0a038a011	VMXC-20F-3050...	10.1.0.6	E0/33	允许	4738
25	10.1.38.49	001e4fe48338	VMXC-20F-3050...	10.1.0.6	E0/31	允许	4482
26	10.1.38.70	0016e4758970	VMXC-20F-3050...	10.1.0.6	E0/27	允许	3970
27	10.1.39.22	001e90814a46	VMXC-20F-3050...	10.1.0.6	E0/5	允许	1026
28	10.1.39.33	000180362282	VMXC-20F-3050...	10.1.0.6	E0/15	允许	2306
29	10.1.39.34	0010a5f743eb	VMXC-20F-3050...	10.1.0.6	E0/37	允许	5250
30	10.1.39.45	000795e11b06a	VMXC-20F-3050...	10.1.0.6	E0/47	允许	6530
31	10.1.39.51	001e908151e4	VMXC-20F-3050...	10.1.0.6	E0/3	允许	770
32	10.1.39.85	000795e11a46	VMXC-20F-3050...	10.1.0.6	E0/43	允许	6018

图 3 ARP 攻击发现与自动阻断:

序号	设备名称	主机IP	主机MAC地址	主机设备	设备IP	设备接口	接口IP	接口MAC	接口速率	接口类型	接口描述	接口状态	时间
1	VMXC-5F-6506-W	10.1.1.30	001243f051e0	VMXC-5F-6506-W	10.1.0.1	E4/0/4	10.1.1.30	001243f051e0	10000	GE	E4/0/4	up	2009-11-14 09:24:00
2	VMXC-5F-6506-W	10.1.1.166	00127955ba40	VMXC-5F-6506-W	10.1.0.1	E4/0/3	10.1.1.166	00127955ba40	10000	GE	E4/0/3	up	2009-11-14 09:24:00
3	VMXC-5F-6506-W	10.1.200.18	001517877e11	VMXC-5F-6506-W	10.1.0.1	E4/0/2	10.1.200.18	001517877e11	10000	GE	E4/0/2	up	2009-11-14 09:24:00
4	VMXC-23F-3050...	10.1.36.41	0010a5f76949	VMXC-23F-3050...	10.1.0.4	E0/40	10.1.36.41	0010a5f76949	10000	GE	E0/40	up	2009-11-14 09:24:00
5	VMXC-23F-3050...	10.1.36.90	00a0a000144d	VMXC-23F-3050...	10.1.0.4	E0/36	10.1.36.90	00a0a000144d	10000	GE	E0/36	up	2009-11-14 09:24:00
6	VMXC-23F-3050...	10.1.36.92	00a0a000544e	VMXC-23F-3050...	10.1.0.4	E0/44	10.1.36.92	00a0a000544e	10000	GE	E0/44	up	2009-11-14 09:24:00
7	VMXC-23F-3050...	10.1.39.35	0010e6074e0a	VMXC-23F-3050...	10.1.0.4	E0/45	10.1.39.35	0010e6074e0a	10000	GE	E0/45	up	2009-11-14 09:24:00
8	VMXC-23F-3050...	10.1.39.39	001e90815344	VMXC-23F-3050...	10.1.0.4	E0/39	10.1.39.39	001e90815344	10000	GE	E0/39	up	2009-11-14 09:24:00
9	VMXC-23F-3050...	10.1.39.41	001921496407	VMXC-23F-3050...	10.1.0.4	E0/8	10.1.39.41	001921496407	10000	GE	E0/8	up	2009-11-14 09:24:00
10	VMXC-23F-3050...	10.1.39.55	0010a5f7f08a	VMXC-23F-3050...	10.1.0.4	E0/12	10.1.39.55	0010a5f7f08a	10000	GE	E0/12	up	2009-11-14 09:24:00
11	VMXC-23F-3050...	10.1.39.183	0010a5f7e17b	VMXC-23F-3050...	10.1.0.4	E0/47	10.1.39.183	0010a5f7e17b	10000	GE	E0/47	up	2009-11-14 09:24:00
12	VMXC-23F-3050...	10.1.31.54	0019214c49c9	VMXC-23F-3050...	10.1.0.5	E0/18	10.1.31.54	0019214c49c9	10000	GE	E0/18	up	2009-11-14 09:24:00
13	VMXC-23F-3050...	10.1.31.87	001e904b2c36	VMXC-23F-3050...	10.1.0.5	E0/41	10.1.31.87	001e904b2c36	10000	GE	E0/41	up	2009-11-14 09:24:00
14	VMXC-23F-3050...	10.1.31.67	002354665eef	VMXC-23F-3050...	10.1.0.5	E0/33	10.1.31.67	002354665eef	10000	GE	E0/33	up	2009-11-14 09:24:00
15	VMXC-23F-3050...	10.1.31.98	0019214f4c24	VMXC-23F-3050...	10.1.0.5	E0/12	10.1.31.98	0019214f4c24	10000	GE	E0/12	up	2009-11-14 09:24:00
16	VMXC-23F-3050...	10.1.31.128	0019214d3fe4	VMXC-23F-3050...	10.1.0.5	E0/20	10.1.31.128	0019214d3fe4	10000	GE	E0/20	up	2009-11-14 09:24:00
17	VMXC-23F-3050...	10.1.36.32	00105cb2c34f	VMXC-23F-3050...	10.1.0.5	E0/21	10.1.36.32	00105cb2c34f	10000	GE	E0/21	up	2009-11-14 09:24:00
18	VMXC-23F-3050...	10.1.36.40	00a0a0000560	VMXC-23F-3050...	10.1.0.5	E0/19	10.1.36.40	00a0a0000560	10000	GE	E0/19	up	2009-11-14 09:24:00
19	VMXC-23F-3050...	10.1.36.42	001bfec15467	VMXC-23F-3050...	10.1.0.5	E0/21	10.1.36.42	001bfec15467	10000	GE	E0/21	up	2009-11-14 09:24:00
20	VMXC-23F-3050...	10.1.36.43	00a060a90441	VMXC-23F-3050...	10.1.0.5	E0/17	10.1.36.43	00a060a90441	10000	GE	E0/17	up	2009-11-14 09:24:00
21	VMXC-23F-3050...	10.1.36.53	0010a5f80444	VMXC-23F-3050...	10.1.0.5	E0/11	10.1.36.53	0010a5f80444	10000	GE	E0/11	up	2009-11-14 09:24:00
22	VMXC-23F-3050...	10.1.36.61	0040b7e08c7b	VMXC-23F-3050...	10.1.0.5	E0/17	10.1.36.61	0040b7e08c7b	10000	GE	E0/17	up	2009-11-14 09:24:00
23	VMXC-20F-3050...	10.1.38.108	00090ba18307	VMXC-20F-3050...	10.1.0.6	E0/25	10.1.38.108	00090ba18307	10000	GE	E0/25	up	2009-11-14 09:24:00
24	VMXC-20F-3050...	10.1.38.29	00a0a038a011	VMXC-20F-3050...	10.1.0.6	E0/33	10.1.38.29	00a0a038a011	10000	GE	E0/33	up	2009-11-14 09:24:00
25	VMXC-20F-3050...	10.1.38.49	001e4fe48338	VMXC-20F-3050...	10.1.0.6	E0/31	10.1.38.49	001e4fe48338	10000	GE	E0/31	up	2009-11-14 09:24:00
26	VMXC-20F-3050...	10.1.38.70	0016e4758970	VMXC-20F-3050...	10.1.0.6	E0/27	10.1.38.70	0016e4758970	10000	GE	E0/27	up	2009-11-14 09:24:00
27	VMXC-20F-3050...	10.1.39.22	001e90814a46	VMXC-20F-3050...	10.1.0.6	E0/5	10.1.39.22	001e90814a46	10000	GE	E0/5	up	2009-11-14 09:24:00
28	VMXC-20F-3050...	10.1.39.33	000180362282	VMXC-20F-3050...	10.1.0.6	E0/15	10.1.39.33	000180362282	10000	GE	E0/15	up	2009-11-14 09:24:00
29	VMXC-20F-3050...	10.1.39.34	0010a5f743eb	VMXC-20F-3050...	10.1.0.6	E0/37	10.1.39.34	0010a5f743eb	10000	GE	E0/37	up	2009-11-14 09:24:00
30	VMXC-20F-3050...	10.1.39.45	000795e11b06a	VMXC-20F-3050...	10.1.0.6	E0/47	10.1.39.45	000795e11b06a	10000	GE	E0/47	up	2009-11-14 09:24:00
31	VMXC-20F-3050...	10.1.39.51	001e908151e4	VMXC-20F-3050...	10.1.0.6	E0/3	10.1.39.51	001e908151e4	10000	GE	E0/3	up	2009-11-14 09:24:00
32	VMXC-20F-3050...	10.1.39.85	000795e11a46	VMXC-20F-3050...	10.1.0.6	E0/43	10.1.39.85	000795e11a46	10000	GE	E0/43	up	2009-11-14 09:24:00

图 4 交互式操作的网络拓扑图:

在此图上可获得全部网元的即时性能指标信息，并可实时全面执行管理与控制。

五、金融行业广域网络链路管理案例

“我们的网络链路是 7*24 小时不间断业务的关键保证，需要一个智能化、立体化、系统化的网络管理平台！”

“我们的网络规模很大，往往一个市级网络的各种路由、交换设备数量就轻松突破 500 台以上，有效率的拓扑发现变得很难！”

“自动发现网络拓扑，说起来容易，做起来难！我们的网络有多种异构广域网传输技术，SDH、帧中继，一般都设有异构技术的备份路由，在 SDH 等线路模式下，找不到一个有效的网络管理软件自动发现并管理网络拓扑！”

“在主、备链路自动切换的模式下，我无法掌握主链路的真实链接状态，这样以来，主链路掉线后，容易造成链路漏检，当备链路相继掉线的情况下，将处于通信中断的尴尬境地！”

金融行业的网管人员常发出这样的感叹！的确，网管软件产品竞争风起云涌，良莠不齐，管理能力、技术水平和侧重点都不尽相同。

香农 INTRAWARE 强大的网络拓扑管理能力圆满地解决了以上问题。该解决方案有如下特点：

1、 高度自动化、高度精确，全网拓扑自动发现并绘制出可任意编辑、拖拽，缩放自如的交互式操作拓扑图。

2、 拓扑图自动发现并绘制主、备链路。

3、 以虚拟端口提供透过 SDH 的端到端链路连接。

4、 对主链路故障实现实时自动告警。

六、从云南机场集团有限公司各机场的综合网络管理系统应用看智能化的网管实现

云南机场集团有限公司总部及各下属共 10 个机场通过 2M E1 专线构建广域网。集团网络分生产网、办公网两个网络，网间配置了网闸等安全设备，进行两网分离。

由于集团各机场设备众多，共有交换机、路由器近 400 台，监测监控设备的运行成为工作量巨大而重要的工作内容之一。

(一) 众所周知，导致网络交换机设备故障的原因众多，比如：1、硬件故障；2、软件故障；3、网络流量拥塞；4、风扇损坏导致温度上升，最终导致性能下降甚至软硬件故障。因此，监测网络交换机设备的 CPU、内存、温度甚至风扇的工作状态，对 24 小时不间断关键业务的重要网络应用系统，就尤其重要。以前，集团信息中心的网管人员接班要做的第一件事就是手工登录每台设备，记录获取详尽的设备日志，作为交接班工作记录。香农 Intraware 可以设定设备巡检功能，在不到一分钟的时间，对全网 400 余台设备快速巡检并生成各设备的综合统计报表，把以前需要花费 3 小时左右的工作，化为轻松一分钟。通过综合统计分析报表，不但可以对设备 CPU、内存等进行监测，还可以及早发现诸如风扇损坏等小故障，避免更大的损失发生，可谓防患于未然。

(二) 网络规模巨大，用户行为不规范，由于管理的人性化需求，不能采用武断粗暴的管理手段。由于办公网与生产网共用一个 Internet 出口，大量的用户 BT 下载、甚至网络病毒，经常会占用大量宝贵的带宽，甚至影响业务应用的正常带宽使用。Intraware 不仅能发现这些即时出现的问题，更能定制好诸多管理策略对此等用户行为进行自动疏导、自动阻断、以及各种表现形式的告警。对非正常流量用户的管理，Intraware 系统自动发现，并在其行为连续达到设定时间（比如 1 分钟）后，自动将其并入设定了共享定值带宽（比如 10K）的特别用户组，不得在流量带宽上有所突破，是一个行之有效而人性的管理策略。值得一提的是，以往依靠各种杀毒软件不能清理干净的 ARP 病毒，如今借助香农 Intraware 零客户端部署的方式，得到了集中有效的控制处理，再也不用担心暴发。

(三) 分层的网络管理。可以设定集团网络管理员、各机场网络管理员等。实现集中-分布式的全新管理操控模式。

(四) Intraware 可以方便地穿透专线广域网，实现轻松的全局拓扑管理。

七、多种网络准入控制技术的组合应用-- Intraware

网络准入控制常见有这么几种技术手段：

1、802.1x 认证。基于网络二层的认证协议，需要交换机硬件设备对此协议的支撑，可以利用 WINDOWS 操作系统的 802.1x 认证模块或者定制的 802.1x 认证客户端软件进行客户端认证。

2、WEB Portal 认证。一般采用 URL 连接重定向技术，首次网络连接定向到指定页面进行认证。

3、PPPoE 认证。一般用于 ADSL 等连接。

802.1x 认证的优势：以硬件设备所支持的协议为依托，可以控制到设备端口的链路连接。几乎不占用任何网络及设备资源，具有认证效率高的特点。

802.1x 认证的弱点：如果接入层存在大量的不支持 802.1x 协议的设备，则需要把接入端口的管理上提到直到上级支持 802.1x 协议的设备。因此，管理粒度依赖于设备对协议的支持。

Web Portal 认证的优势：集中部署方式，客户端不需要做任何软件的安装。

Web Portal 认证的弱点：耗用一定的网络资源，处理性能与自身运行服务器平台有关，需要服务器有一定的负荷承载能力。

Intraware 实现了 802.1x 与 Web Portal 认证在同一网络中的组合应用。

八、谈INTRAWARE 大学校园网络管理

XX 大学校园网背景:

XX 大学校园内现有信息点近 10000 个。共有核心交换机 2 台(华为 S8016), 汇聚交换机 14 台 (cisco6506 一台, S5516 七台, S6503 二台, S6506 一台, S7503 二台, 港湾 6802 一台), 接入交换机 250 多台 (港湾交换机 μ 24 、Hammer48 84 台, 华为系列接入交换机 S3050C 34 台、S3900 21 台、S3100 33 台, 锐捷的其它型号接入交换机约 50 多台)。联想网御 UTM3000、UTM2000 防火墙各一台, 出口路由器华为 NE40 一台。校园网配置了多操作系统平台服务器, 其中, SUN 服务器 17 台、Linux 服务器 5 台, Windows 服务器 10 余台及其它院系机关托管服务器若干台。XX 大学校园网以千兆光纤接入 CERNET 城域网, 两条百兆接入中国电信。启用的公共应用有: WWW、DNS、EMAIL、FTP、VOD 等服务。为改善公网访问校园网对外内容, 通过动态域名解析加 SQUID 反向代理实现 WEB、精品课程、教务等内容。数字化校园应用, 包括 OA、学工、人事、就业、门户等。

校园网络存在的主要问题:

- 1、 部分校园网用户在某些时段反映不能获取 IP 地址。部分是用户自接路由设备开启 DHCP 服务, 部分用户是个人计算机原因。
- 2、 办公、教工网段用户反映上网速度较慢。学生线路普遍反映速度很慢, 经过观测, 在上午 11 点前网速较好, 之后至凌晨都较慢。
- 3、 遇有些病毒爆发不能及时定位进行处理, 对 ARP 等病毒没有有效的解决办法。无奈之下只能是对少部分具备条件的设备端口进行逻辑隔离, 但带来很大的工作量。
- 4、 因维护人员、校区、网络规模等原因, 校园网终端用户的网络维护难以快速响应, 平均每天大约有 3-5 次上门维护, 电话咨询约 20 次, 上门维护过程中的问题多是计算机终端问题, 网管人员疲以应对。

5、 缺乏对上网人员的行为进行审计和日志记录，同时对公安部门要求的相关数据追查无法进行。

6、 在交换设备及路由上对不同应用进行 ACL 或 QOS 控制，对网络性能改善效果不明显。

7、 设备众多，根据网络运维的需要，经常需要批量地改变交换机配置。

香农 INTRAWARE 解决方案：

我们在采用香农 INTRAWARE 网管软件后，从以下方面获得了充分的解决办法。

1、集成统一的 IT 架构管理平台

如今的校园网 IT 运维表现出故障原因多元化的特点，比如，OA 系统访问速度下降，有可能是以下原因的一个或多个：服务器故障、服务器数据库系统故障、中间件故障、OA 应用软件故障、网络设备故障、网络链路故障、网内病毒异常流量暴发等等。以往的管理需要从多个运行系统做大量的数据采集，逐一分析，才能得到一些关键的数据。即便一些号称提供综合管理的网络管理软件，也必须在几个不同的软件界面，才能得到相关性比较差的一些数据。INTRAWARE 的管理以立体化、系统化、集成化为支点，首先，INTRAWARE 提供的一个统一管理平台，在一个集成的拓扑图环境下进行全部 IT 架构范围内的信息监测和管理控制。第二，告警信息知识库、告警信息以及告警阈值自定义，可以针对设备、链路、流量、应用系统运行性能、用户行为、网络安全等进行统一的告警，知识库自动生成易于理解的告警信息，可以直接提供领导决策层查询。第三，INTRAWARE 提供系统化的控制策略自定义并自动实施，控制范围包括交换机端口、用户流量、用户带宽、限制时段、网络服务（包括视频会议、QQ、P2P 等）。可以说，INTRAWARE 以立体化、系统化的视点，测控并重，提出了很好的 IT 运维管理方案。

2、网络拓扑管理

香农 INTRAWARE 支持 CISCO、华为等多个设备产商的私有拓扑发现算法，并可以和香农通用算法综合使用，特别适合众多网络品牌设备混用、IOS 操作系统

版本各异的大型网络。INTRAWARE 的拓扑发现准确而快速，并提供了拓扑图设备自动排列功能，近 300 台交换机约 1 万用户的拓扑，全部自动而准确的发现，只花费了近 20 分钟。

INTRAWARE 拓扑发现可以发现到用户 PC 机，以不同图标、颜色和声光报警的方式，提供了基于 J2EE 拓扑图交互操控模式的网络设备、机房环境、链路、用户 PC 机、服务器、流量协议监测和管理。由于校园网规模较大，INTRAWARE 分层视图的设计能够以全局或局部地展现拓扑视图，使得拓扑的操作清晰明了。

尤其值得一提的是，INTRAWARE 完全管控一体的交互式操作，完美地体现了图形化操控的能力。

3、网络主干性能的保证

网络主干性能的保证是校园网运维的重要工作内容，INTRAWARE 提供的性能保证可以从以下几个方面得到体现：

i) 网络主干链路的性能监测

INTRAWARE 以目录树的方式提供了设备及端口的性能监测，并且用户可以点选出若干主干（或重要）端口，在一个集中的窗口中进行主干链路的特别监测。在较大规模的校园网络里，这是一个很方便的功能。

i i) 决策数据的捕获

对于网络运维决策比较关键的一些数据包括：设备运行状态数据（包括设备 CPU、内存、电源、风扇等运行数据）；设备端口数据（包括端口状态、利用率、广播包、错包、丢包）；流量与协议数据（包括 VLAN 间流量、IP 流量、网络连接数、报文数、报文长、协议类型、流量查询统计等）。这些关键数据可以提供设备运行基本状态及用户流量基本状态，在决策过程中提供重要的依据。

iii) 异常流量的应对

校园网内存在大量异常流量，表现为：大量 P2P 连接、病毒时常暴发。INTRAWARE 对 P2P 连接进行限制后，上网速度明显改善，并能对大部分 ARP 病毒进行定位。

iv) 控制策略的实施

INTRAWARE 提供了一个控制策略定制器，按协议、端口、流量、网络连接数、目的 IP、源 IP 等可以自定制规则集，这个规则集可以方便地赋予若干个用户或若干个用户组（子网），更重要的是，INTRAWARE 的控制策略具备基于 SNMP 的自动实施能力，能够在校园网内复杂的设备环境中，把控制能力延伸到每一个设备端口。

4、用户管理与设备管理的统一

对于校园网主干性能保护来说，最根本的是管好用户，借助 IT 运维管理系统分析并规范用户的网络行为，是 IT 运维的重要目标之一。因此，用户管理统合设备的管理是 INTRAWARE 的一个重要优势。以流量和协议为线索，找出设备与用户的联系，快速定位用户的 PC 及设备端口物理对应位置，可以结合网管协议对其进行有效管理和控制。

5、设备管理配置的分发

校园网络配备设备数量巨大，经常要根据网络运行状况及应用分布状况调整网络规划和配置，INTRAWARE 提供了集中的设备管理配置分发功能，可以快速复制设备配置。

6、用户日志及上网行为控制

INTRAWARE 提供了详实的用户上网日志，由于校园网日志数据量巨大，我们在应用中仅保留每天最新时间的无重复数据，日志保留 15 日，每日产生 20G 的日志数据。对于上网行为控制，主要包括，对一些不健康网站的屏蔽以及利用 INTRAWARE 对一些 P2P 的连接进行限制，但对 P2P 的控制策略，我们采取的是适当限制，限而不止的思路。

实施效果:

网络风险已经不再反映为单一的危险，传统的网络管理工具往往在管理工具的选择上和管理工具使用的策略上顾此失彼，已经无力响应网管员的管理需求。一个统合高效的集成网络管理环境变得尤为重要，它必须具备综合分析处理网络内绝大多数不安全数据、并多方位多策略地自动实施应对方案的能力，最大程度地实现智能化管理、优化管理效能、提供集成管理方案。INTRAWARE 集成的 IT 运维管理操控环境，使得 IT 运维模式有了革命性的改变，特别是对用户管理及业务层管理的能力，把 IT 运维管理引申到了最根本的管理要素——人，从而得以控住面临越来越复杂的网络服务和网络应用。

Intraware 系统能及时收集并分析监控网络、设备、主机、数据库、应用服务器，预测并适当避免问题的发生；Intraware 系统还可以从不同的角度（网络链路层、网络层、应用层、系统资源、数据库及应用性能等）对统一 IT 架构实施全天候的（7X24 小时）性能管理和分析，从而保证客户 IT 架构的最大可用性。

Intraware 系统基于健壮的 Linux 平台，能在任何时刻自动实施控制策略，保障关键业务的健康运行。

INTRAWARE 从以下方面满足校园网 IT 运维的需求：

- 强化核心的 LINUX 操作系统作为运行平台，系统非常坚固，零客户端部署
- 基于 J2EE 的分布式计算环境，极大保护服务器性能
- WEB 界面，网络拓扑拖拽自如、基于图形的管控操作，管理随处可达
- 支持香农通用算法、CISCO CDP 算法、华为 NDP 算法，并能综合使用，以极高效率进行拓扑自动计算和自动绘制，拓扑自动排列
- 完备的故障管理、性能管理、配置管理、全计算环境分层式可视化管理、全息安全信息实时监察和历史数据
- 支持各厂家多种类的网络设备

- 面向计算机网络终端的管理甚至可以发现和控制非网管设备下的 PC
- 对跨地域的广域网络集中控制和管理
- 流量与协议分析
- 带宽与流量控制
- 强大的网络病毒预防与遏制能力，保证主干网络的健康运行，能对网络内染毒计算机的网络 DDOS 攻击、网络执法官、ARP 病毒、蠕虫病毒等异常流量及其变种自动采取应对策略。
- 优秀的上网行为控制，可按多种策略定制控制方法
- 控制策略预先设定与自动实施
- IP-MAC 全网自动扫描绑定
- 网络带宽分配和链路聚合、负载均衡
- 网络运行质量控制的有效工具
- 保证网络连续可靠安全可控制地工作
- 网络设备配置管理分发
- 支持广域网路由、Trunk 接入、NAT
- 可以直路部署，对主干流量与协议进行有效控制与整形，也可以旁路部署，对全网进行有效监测和管理

九、市级电网公司如何管好广域网络？

网络结构：

某市级电网公司下辖 10 余个县级分公司、50 个供电所、30 余个收费网点，各县公司分别通过电信运营商 2M 专线接入市公司；50 个供电所、30 余个收费网点均分别通过电信运营商 2M 专线接入市电信运营商，再由电信运营商汇总为一条 2M 专线汇接到市公司。

各县公司网络均在三层交换机上配置 ACL，网络分为县公司办公网、营销网、供电所办公网。

各县公司统一配置一条 INTERNET 专线出口，出口处配置有防火墙、路由器等设备。

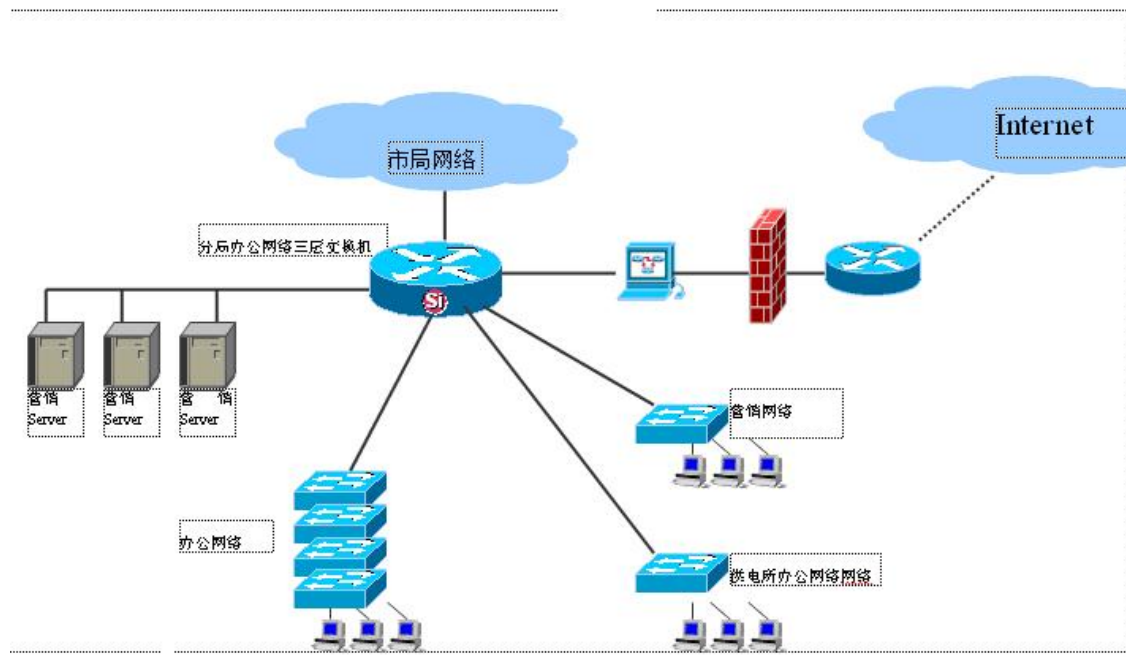
设备配备：

市公司配置三层交换机一台、各县公司分别配置三层交换机一台，各办公区、供电所、收费网点交换机均为不可网管交换机。

管理难点：

- 1、网络用户及设备分散，横跨地域广。
- 2、各县局的生产存在大量网络病毒，包括 ARP 病毒、DDOS 攻击。病毒攻击经常导致县局及市局生产网络堵塞，严重时常导致收费业务不能正常进行。
- 3、互联网出口路由器经常堵塞瘫痪，影响正常的办公应用。
- 4、大量的营业网点计算机网络是专线接入运营商，通过运营商汇聚后再专线接入县公司网络，由于这部分网络设备管理权在运营商，原来的管理手段以及通常的网管软件都管理不到这些网络及计算机。

香农网管解决方案拓扑：



方案优点:

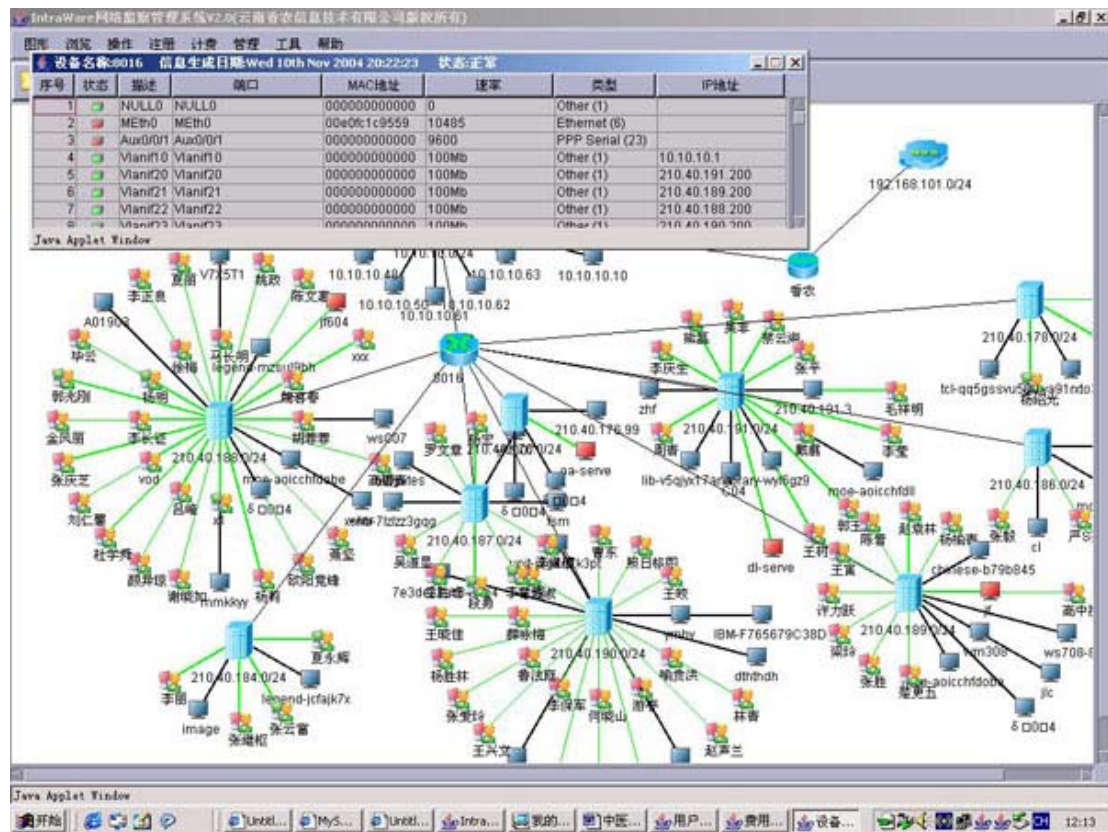
- 1、 每个县公司独立配置一套香农网管，市公司集中监控，县公司分布式管理与控制。
- 2、 部署于 Internet 出口防火墙之后，以香农网管卓越的出口吞吐性能，为低端路由器减轻大量 DDOS 攻击的负担。对网络用户 Internet 带宽进行控制与分配。
- 3、 零客户端部署，不增加任何网络运维管理成本。
- 4、 自动阻断各个子网 ARP 病毒，网管员高枕无忧。
- 5、 强大的物理、逻辑双模拓扑管理，渗透运营商汇聚设备，直达广域网络各供电所、收费点的不可网管 HUB 接入的计算机，对公司全部计算机（用户行为、访问日志、网络流量、协议）进行有效的监测、分析与控制。
- 6、 可视化的监测分析、交互图形界面的控制与查询。香农网管实现了智能化的管理、傻瓜式的操控，全面解决了困扰该局数年的网络管理老大难问题。

十、网络管理，从用户管理开始(在特大国有企业的應用)

网络管理，从用户管理开始

----- 香农 Intraware 助力云南铜业股份有限公司网管

云南铜业股份有限公司年产高纯阴极铜达 36 万吨，销售收入超 280 亿元，是国家特大型国有企业。网络能否健康运行将直接影响到企业安全生产和经营。如何控制非法接入、访问权限、限制异常流量、预防和快速诊断网络故障变得至关重要。



云铜股份核心交换机采用 Cisco 6509，下接多种型号可网管或不可网管的交换机。通过 LAN 专线接入公网，企业内部网络规模较大，运行着 ERP、电子商务等重要应用系统。企业内部网络装备近 800 台计算机，按工作性质可分为小型机服务器、PC 服务器、工业工控机、行政办公机、财务办公机、市场销售办公机等类型，按网络物理区域可分为厂区、行政办公区、财务销售区等区域。企业网络以往都面临非法私自接入、访问权限无法控制、经

常有异常流量和网络病毒爆发等诸多问题。云铜股份采用香农 Intraware 实现了对企业网络简捷有效的管理。根据云铜股份的应用经验，把网内用户管好了，就管理好了企业网络所运行的网络服务，网络服务得到了控制，就能预防很多可能会出现的网络风险。我们来看看云铜股份是怎样利用 Intraware 实现对用户的有效管理的：

1、简单部署

由于企业网内用户数量较大，零客户端安装可以节省大量管理成本。

2、基于逻辑拓扑图管理

Intraware 可以对全网自动扫描绘制精确到计算机的拓扑图，同时以物理或者逻辑模式进行显示。因为企业的人力资源管理一般都是基于岗位或群组的管理的，因而，基于逻辑拓扑图的管理，可以更加准确地实现对计算机用户的管理，方便比对、方便管理策略的统一实施和部署。设备和用户的统合管理，把可能引发网络风险的设备因素、人为因素综合分析，从而提供全面防范和控制网络风险的基础数据。

3、接入权限管理

为企业网计算机用户分配固定的 IP 地址（也可以由 DHCP 分配固定的 IP 地址），然后利用 Intraware 的全网 IP-MAC 地址自动扫描绑定，把 IP 地址与网卡 MAC 一一对应起来，防止用户私自篡改 IP 地址（IP 地址混乱可能导致企业网大量 IP 地址冲突、外部入侵 IP 欺骗、网络事件及日志无从根究等等）。

4、身份识别

要求全网计算机在操作系统安装时，填写规范的“计算机名”，一般使用部门加使用者姓名来进行命名。利用 Intraware 对企业网全部计算机扫描其“计算机名”，并能被自动拓扑扫描引擎发现并绘制到拓扑图里。这样，就可以对计算机进行实名管理。

5、用户分组

对用户依据其部门、工作性质等等，对用户进行分组管理。这样可以对不同的用户组分配不同的权限和带宽占用级别，可以保证关键的岗位和关键的业务优先使用有限的网络资源。

6、监测网内计算机资源占用

监测并掌握全部计算机的 CPU、内存、硬盘等资源占用情况，监测各计算机软件安装配置状况及软件进程运行。全局的资源统计报表可以帮助判断网络是否真的被大流量阻塞或是计算机系统资源被异常占用。

7、定位网内计算机与设备端口的连接关系

定位网内计算机与设备端口的连接关系对快速判断流量异常、网络病毒或设备故障等都有很大的帮助。可以手动或自动关闭相关的一些交换机端口，控制异常流量的扩散。

8、设置条件阈值，对干扰网络运行的计算机停闭网络，并告警提示，可以在风险形成的最短时间内自动规避更大的风险。

9、带宽控制、大流量下载控制、BT 控制

对一些 BT 使用者及大流量下载用户，可以采用 Intraware 自动发现，进而自动适时降低其网络带宽，降低用户对下载的兴趣，也可以设定网络会话数阈值，一个用户启动的网络会话数超过阈值，则自动停闭该用户，这些管理策略的综合应用，可以有效遏止用户大流量及 BT 下载。

10、反 ARP 病毒、DDOS 病毒、蠕虫病毒

DDOS 病毒和蠕虫病毒都是大量地在网络中发包或建立巨量的网络连接会话数，占用路由设备负载能力资源阻塞网络，可以通过用户网络会话数的阈值限制并停闭这些用户交换机端口，达到控制的目的。ARP 病毒可复制并广播 LAN 内的 MAC 地址，造成网络冲突，Intraware 的 IP-MAC 双向绑定工具可有效侦测染毒计算机。

11、选择健壮的网管软件操作系统，云铜股份选择的 Intraware 是以 Linux 操作系统为运行平台的，管理端以 J2EE 的 B/S 模式进行操作，不但操作简单，而且无论多大的网络病毒和异常流量，Intraware 都能健康运行，对网络管理指挥若定。

按照以上原则进行管理，云铜企业网内一旦有网络故障发生的时候，管理员可以通过直观的拓扑图立即发现故障点，观察和故障点相关的硬件设备运行状况、端口状况、流量和协议占用情况，从而为正确排查故障提供快捷全面的支持信息。

十一、INTRAWARE ,护航国家重点工程“金质工程”

项目背景

国家“金质工程”是依托国家电子政务外网和现有信息化资源，通过“一网、一库、三系统”的建设，逐步实现行政审批网络化、监督管理信息化、决策支持智能化、业务处理规范化、信息交互发布自动化的信息化项目。“金质工程”一期工程项目总投资约为 2.5 亿元人民币。该工程将全面提升我国质检系统的行政执法水平，强化市场监管和质量安全监控的快速反应能力并改进质检行政管理的水平。据了解，“金质工程”一期工程项目建设将在现有资源的基础上完成。并将建立“金质工程”的相关技术标准和管理规范、制订相关指标体系；充分利用国家电子政务外网整合建设质检业务专网平台，形成连接国家质检总局和各试点局、分支局、办事处的局域网和广域网；建设国家标准信息数据库、企业质量信用信息数据库等基础质检数据库；建设包括全国执法打假快速反应、特种设备安全监管、计量业务监督管理、产品质量监督管理、进境货物检验检疫电子监管、国家强制性产品认证监管等内容的质检业务监督管理系统；建设进境货物备案审批等内容的质检业务申报审批系统；建设实施卫生与植物卫生措施协定(WTO/TBT-SPS)等国家通报、评议、咨询及风险预警快速反应等内容的质检信息服务系统；建设相关的安全保障和运行维护系统。

INTRAWARE 在金质工程中的应用

一、实施范围

云南省“金质工程一期”项目建设中，云南省质量技术监督局共采购了 17 套香农 INTRAWARE 综合网络管理系统，分别部署于省局、昆明市局、曲靖市局、玉溪市局、保山市局、临沧市局、普洱市局、昭通市局、大理州局、丽江市局、

红河州局、西双版纳州局、楚雄州局、文山州局、德宏州局、迪庆州局、怒江州局。

二、运维管理模式

云南省“金质工程”网络架构于云南省电子政务专网平台，采用 VPN 组网方式，网络系统以三级架构的模式覆盖省局、州市局、县局。为达到网络运行维护管理、控制于一体的目标，本次采购的 17 套 INTRAWARE，以省、州市二级运维管理的模式进行部署。即省局 INTRAWARE 部署于核心交换机与路由器之间，对省局大楼的所有设备、流量协议、带宽、用户行为及应用系统进行管理，并能管理全省各州市、县的网络设备，对全省各州市的流量协议及用户行为进行监测。州市局部署网管系统于州市中心交换机与路由器之间，作为全省网管平台联动设计的一部分，独立配置州市级的网络管理权，可对本州市（包括县级局）的网络设备、流量协议、带宽、安全、用户行为等进行管理和控制。

三、INTRAWARE 管理优势

1、全局联动而权限分层的拓扑管理。云南省“金质工程”，作为全国重点的电子政务信息化建设项目，按照国家要求采取统一规划、统一建设、统一管理的建设方针，结合质检部门业务管理垂直化的特点，省级信息中心对全省的网络运行维护和业务应用系统承担完全的责任，而网络应用本身的复杂性，又对州市网络本地的运维能力提出了较高的要求。香农 INTRAWARE 中央控制台部署于省级信息中心，省级网管员可对全省三级组织架构的网络运维及应用系统性能了如指掌，各州市的分控台不仅可以为州市级网管人员提供一个监测管理平台，更能对州市县二级机构的设备及全部用户进行全面的控制。省级主控中心与各分控中心的联动管理，使得多层组织机构的大型网络运维游刃有余！

2、复杂网络环境的适应能力。INTRAWARE 可部署于大型广域网络的复杂环境之中，无论是基于 IP 专线、SDH、IP Over ATM 还是 FRAM RELAY 的广域网平台，以各种 VPN、LAN、ADSL 专线接入的网络，INTRAWARE 均可轻松部署。

3、按网络服务协议的首选流量控制。“金质工程”全省视频会议系统，借助于云南省电子政务专网广域网分配的 2M 带宽。由于带宽的限制和设备时延影响等诸多因素，视频会议系统（H. 323 协议的网络服务）很难获得完美效果。INTRAWARE 的按网络服务协议带宽控制技术，可以保证视频会议系统、某关键业务应用系统的优先带宽占用。

4、安全控制能力。云南省“金质工程”网络横跨 16 个州市，网络用户数量多达 3000 余人，涉及大量政务信息公开及行政审批业务，电子政务专网、外网应用交叉复杂，对网络运维提出了较高的要求。INTRAWARE 以其强健的 LINUX 操作系统运行平台，监测控制一体的运维管理能力，能有效地遏阻 DDOS 攻击、BT 下载、ARP 病毒等异常流量与异常网络连接。

5、多厂商设备管理能力。云南省“金质工程”网络整合了部分州市已建有的网络系统，INTRAWARE 特有的多种私有拓扑发现算法综合应用能力，实现了快速的拓扑发现与绘制以及精准的用户—设备端口定位功能，为面向用户与用户行为的管理控制提供了基本信息。

6、面向用户的管理。众所周知，网络的应用主体永远是人，除了设备自身的故障，其它全部 IT 运维风险的产生都和用户有直接或间接的关系，因此，INTRAWARE 独步的面向用户管理，可以提供集成化的、多维的、系统化的 IT 运维管理。

7、综合系统管理。“金质工程”建设有大量的应用系统，包括：政务信息公开系统、行政审批系统、12365 系统、邮件系统等外网系统；全国执法打假快速反应系统、特种设备安全监管系统、食品安全监管系统、计量业务监督管理、产品质量监督管理、国家强制性产品认证监管系统等内容的质检业务监督管理系统。大量的业务系统具有功能应用复杂、技术路线各异、数据分散而巨量、等特点，存在维护难度大、设备众多等监测管理难点，INTRAWARE 的综合系统管理提供了主机性能监测、操作系统监测、中间件性能监测、数据库性能监测、邮件监测、WEB 服务监测等功能，可对异种操作系统、异种数据库、异构技术架构的应用基础平台进行全面的监测。

