Computer Science and Application 计算机科学与应用, 2022, 12(4), 885-894
Published Online April 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.124090

Hans汉斯

基于多线程网络节点连通性探测技术的网络实时检查技术研究与系统开发应用

张　莉，崔凤娟

国家海洋局北海信息中心，山东 青岛

收稿日期：2022年3月7日；录用日期：2022年4月6日；发布日期：2022年4月13日

摘　要

研究利用ICMP协议和多线程技术实现多VPN网络的轮询监控方法，通过轮询信息发送、轮询信息采集、信息分析和后期处理、阈值设定和调整、报警与恢复功能开发，实现主要网络节点联通监测及模块化网络服务集成。本文方法在自然资源部北海区地面传输观测网环境内经实际应用，效果良好，证实了该方法的有效性。

关键词

ICMP协议，多线程，网络，系统

Research and Application of Network Real-Time Inspection Technology Based on Multi-Thread Network Node Connectivity Detection Technology

Li Zhang, Fengjuan Cui

North China Sea Data & Information Service of the State Oceanic Administration, Qingdao Shandong

Received: Mar. 7th, 2022; accepted: Apr. 6th, 2022; published: Apr. 13th, 2022

Abstract

The polling monitoring method of multi-VPN network based on ICMP protocol and multi-thread technology is studied. Through the development of polling information transmission, polling in-

文章引用: 张莉, 崔凤娟. 基于多线程网络节点连通性探测技术的网络实时检查技术研究与系统开发应用[J]. 计算机科学与应用, 2022, 12(4): 885-894. DOI: 10.12677/csa.2022.124090

formation collection, information analysis and post-processing, threshold setting and adjustment, alarm and recovery functions, the connection monitoring of main network nodes and the integration of modular network services are realized. This method has been applied in the environment of the ground transmission observation network in the North Sea area of the Ministry of Natural Resources.

Keywords

ICMP Protocol, Multithreading, Network, System

1. 引言

各单位及用户对网络管理的重视程度是随着网络应用的不断扩展而逐步提升的，这是在我国各地办公局域网网络发展过程中表现得非常明显的一个问题。在初期网络规划中往往只重视连接节点，而对网络监测与管理能力、网络故障发现与处理能力、网络安全与防范能力一般都没有考虑在内，因此利用有效技术手段实现网络监测与管理，实现网络故障发现与处理的需求也更加迫切。

2. 问题来源与思路

北海区网络约有 1200 个 VPN 网关，分布在 8 个 VPN 网段。此外还包含 300 个左右 24 小时在线的主要观监测数据采集设备和 120 余个关键服务器节点，网络节点的连通情况监控需要达到 10 秒以内报警的要求，原有的网络监控系统已经无法满足现在的网络管理的实际需要，迫切需要使用更完善和有效的技术手段实现对整合后网络的监控和管理。

从技术角度分析，网络管理技术是伴随着计算机、网络和通信技术的发展而发展的，二者相辅相成。从网络管理范畴来分类，可分为对网“路”的管理。即针对交换机、路由器等主干网络进行管理；对接入设备的管理，即对内部 PC、服务器、交换机等进行管理；对行为的管理。即针对用户的使用进行管理；对资产的管理，即统计 IT 软硬件的信息等。根据网管软件的发展历史，可以将网管软件划分为三代：

第一代网管软件就是最常用的命令行方式，并结合一些简单的网络监测工具，它不仅要求使用者精通网络的原理及概念，还要求使用者了解不同厂商的不同网络设备的配置方法，目前分局局域网基本处于这个运行阶段。

第二代网管软件有着良好的图形化界面。用户无须过多了解设备的配置方法，就能图形化地对多台设备同时进行配置和监控。大大提高了工作效率，但仍然存在由于人为因素造成的设备功能使用不全面或不正确的问题数增大，容易引发误操作。

第三代网管软件相对来说比较智能，是真正将网络和管理进行有机结合的软件系统，具有“自动配置”和“自动调整”功能。对网管人员来说，只要把用户情况、设备情况以及用户与网络资源之间的分配关系输入网管系统，系统就能自动地建立图形化的人员与网络的配置关系。

国内外技术人员已经在这方面进行了许多探索。在网络拓扑发现算法方面，赵玲分析了 SNMP 协议的功能、体系结构、协议框架及 MIB 库，研究并分析了 SNMP、ICMP、RIP、OSPF 和 ARP 等网络拓扑算法的特点[1]。吴君青介绍了一种可以在单个机器上实现物理拓扑发现的算法，并针对提供信息不足的

情况，对原有算法进行改进[2]。朱有产出了一种跨虚拟局域网(VLAN)的物理网络拓扑发现算法，算法基于以太网技术，被管理设备支持 SNMPv2。分别对实现了 Bridge MIB、部分或没有实现 Bridge MIB、服务器和路由器等节点提出了自动发现方法[3]。

在网络拓扑管理技术和应用方面，田云兵研究了基于 SNMP 网络管理的基本机构，在此基础上设计了一个网络管理系统。在设计出来的网络管理系统中，对传统的 SNMP 网络搜索设备的基础上进行了改进，并找出了唯一标识路由器的方法。孔令文等提出链路层网络拓扑发现算法，并对该算法进行了介绍，通过该算法，可以在单机上对当前网络的拓扑情况进行发现[4]。

在网络拓扑数据分析与表现方面，金培欣根据 EXCEL 工作表函数与数组公式的特点，提出了一种数据提取的方法。基于网络流量统计数据为例进行分析，构建了具有一定的通用性的数据提取公式，可提高网络管理的效率[5]。

3. 解决办法

在充分考虑北海区网络结构和特点的基础上，针对网络设备“管理网段”及“7 个 VPN 网段”共 8 个网段设计的网络结构特点，采用多线程技术和 ICMP 协议结合的方法，采用主动轮询的方式实现对北海区各关键网络节点通讯网关的连通性及响应时间的实时监控，并通过设定阈值及时对网络连通性问题和通讯质量故障进行报警，为提高整合后网络节点的管理能力，及早发现网络节点故障，加强对北海区海洋在线观测、监测和监视监控业务的支持能力提供保障。

3.1. 网络管理技术

网络监视技术一般可分为主动式和被动式两种，主动式一般是由管理主机向各个管理节点发送轮询指令，由各节点根据指定的协议，如 SNMP 协议返回相应的状态信息。同时 SNMP 协议也支持被动式的监视，如 SNMP TRAP，也就是在设定了一定的阈值后，在被监视节点本身发现超过阈值时主动向管理节点发送告警信息。主动式和被动式各有优点，在实际网络监视过程中都有一定的应用，而且经常是混合应用[6]。

“云计算”技术的发展相当大的程度上改变了许多企事业单位的网络结构，服务器、应用等重要节点纷纷“上云”，更进一步削弱了客户机网络的建设和运维管理的投入。这类网络一般没有复杂的 IMC 等管理系统，没有足够的网络监控监视工具，很难及时发现网络中存在的问题，如最简单的节点通断检测，往往是在应用系统发生故障时才会被发现。利用 ICMP (Internet Control Message Protocol)，Internet 控制报文协议)和多线程技术，结合数据库作为存储手段，开发应用于中小型网络的网络监视监视系统，可以在一定程度上解决中小型网络管理过程中的节点监控问题[7]。

3.2. ICMP 协议

ICMP 是 Internet 控制报文协议。它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用，ICMP 属于网络层的控制报文协议。

ICMP 协议是一种面向连接的协议，用于传输出错报告控制信息。它是一个非常重要的协议，它对于网络安全具有极其重要的意义。它是 TCP/IP 协议族的一个子协议，属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据无法访问目标、IP 路由器无法按当前的传输速率转发数据包等情况时，会自动发送 ICMP 消息。见图 1。

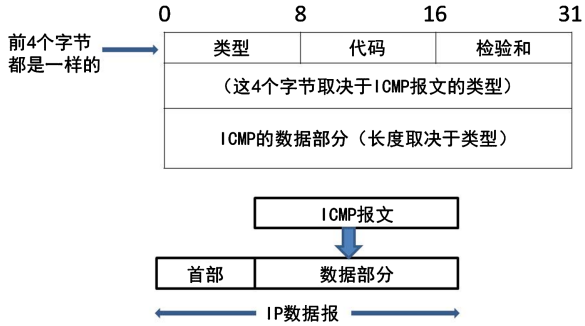

Figure 1. ICMP message format
图 1. ICMP 报文格式

ICMP 提供一致易懂的出错报告信息。发送的出错报文返回到发送原数据的设备，因为只有发送设备才是出错报文的逻辑接受者。发送设备随后可根据 ICMP 报文确定发生错误的类型，并确定如何才能更好地重发失败的数据包。但是 ICMP 唯一的功能是报告问题而不是纠正错误，纠正错误的任务由发送方完成。我们在网络中经常会使用到 ICMP 协议，比如我们经常使用的用于检查网络通不通的 Ping 命令，这个“Ping”的过程实际上就是 ICMP 协议工作的过程。还有其他的网络命令如跟踪路由的 Tracert 命令也是基于 ICMP 协议的。

1) Ping 命令

Ping 是 Windows/Linux 系列自带的一个可执行命令。利用它可以检查网络是否能够连通，可以很好地帮助我们分析判定网络故障。该命令只有在安装了 TCP/IP 协议后才可以使用。Ping 命令的主要作用是通过发送数据包并接收应答信息来检测两台计算机之间的网络是否连通。当网络出现故障的时候，可以用这个命令来预测故障和确定故障地点。Ping 命令成功只是说明当前主机与目的主机之间存在一条连通的路径。如果不成功，则考虑：网线是否连通、网卡设置是否正确、IP 地址是否可用等。

成功地与另一台主机进行一次或两次数据报交换并不表示 TCP/IP 配置就是正确的，必须执行大量的本地主机与远程主机的数据报交换，才能确信 TCP/IP 的正确性。按照缺省设置，Windows 上运行的 Ping 命令发送 4 个 ICMP (网间控制报文协议)回送请求，每个 32 字节数据，如果一切正常，系统应能得到 4 个回送应答。

Ping 能够以毫秒为单位显示发送回送请求到返回回送应答之间的时间量。如果应答时间短，表示数据报不必通过太多的路由器或网络连接速度比较快。Ping 还能显示 TTL (Time To Live 存在时间)值，可以通过 TTL 值推算一下数据包已经通过了多少个路由器：源地点 TTL 起始值 - 返回时 TTL 值。例如，返回 TTL 值为 119，那么可以推算数据报离开源地址的 TTL 起始值为 128，而源地点到目标地点要通过 9 个路由器网段(128~119)；如果返回 TTL 值为 246，TTL 起始值就是 256，源地点到目标地点要通过 9 个路由器网段。

2) TRACERT 命令

Tracert (跟踪路由)是路由跟踪实用程序，用于确定 IP 数据包访问目标所采取的路径。Tracert 命令用 IP 生存时间(TTL)字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

通过向目标发送不同 IP 生存时间(TTL)值的“Internet 控制消息协议(ICMP)”回应数据包，Tracert 诊断程序确定到目标所采取的路由。要求路径上的每个路由器在转发数据包之前至少将数据包上的 TTL 递减 1。数据包上的 TTL 减为 0 时，路由器应该将“ICMP 已超时”的消息发回源系统。

Tracert 先发送 TTL 为 1 的回应数据包，并在随后的每次发送过程将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。通过检查中间路由器发回的“ICMP 已超时”的消息确定路由。

3.3. 多线程技术

多线程(Multithreading)，是指从软件或者硬件上实现多个线程并发执行的技术。每个正在系统上运行的程序都是一个进程。每个进程包含一到多个线程。进程也可能是整个程序或者是部分程序的动态执行。线程是一组指令的集合，或者是程序的特殊段，它可以在程序里独立执行。也可以把它理解为代码运行的上下文。所以线程基本上是轻量级的进程，它负责在单个程序里执行多任务。通常由操作系统负责多个线程的调度和执行。线程是程序中一个单一的顺序控制流程。在单个程序中同时运行多个线程完成不同的工作，称为多线程。

具有多线程能力的计算机因有硬件支持而能够在同一时间执行多于一个线程，进而提升整体处理性能。具有这种能力的系统包括对称多处理机、多核心处理器以及芯片级多处理(Chip-level multithreading)或同时多线程(Simultaneous multithreading)处理器。在一个程序中，这些独立运行的程序片段叫做“线程”(Thread)，利用它编程的概念就叫做“多线程处理(Multithreading)”。具有多线程能力的计算机因有硬件支持而能够在同一时间执行多于一个线程，进而提升整体处理性能。多线程是为了同步完成多项任务，不是为了提高运行效率，而是为了提高资源使用效率来提高系统的效率。线程是在同一时间需要完成多项任务的时候实现的。

线程和进程的区别在于，子进程和父进程有不同的代码和数据空间，而多个线程则共享数据空间，每个线程有自己的执行堆栈和程序计数器为其执行上下文。多线程主要是为了节约 CPU 时间，发挥利用，根据具体情况而定。线程的运行中需要使用计算机的内存资源和 CPU。多线程技术的优点在于：

使用线程可以把占据时间长的程序中的任务放到后台去处理，用户界面可以更加吸引人，这样比如用户点击了一个按钮去触发某些事件的处理，可以弹出一个进度条来显示处理的进度，程序的运行速度可能加快。在一些等待的任务实现上如用户输入、文件读写和网络收发数据等，线程就比较有用了。在这种情况下可以释放一些珍贵的资源如内存占用等[8]。

3.4. 系统设计

利用 Microsoft .net 4.0 框架下的 C#进行开发，系统分为两个主要部分：“北海区网络状态探测监管系统.网络测试服务程序”和“北海分局网络状态探测监管系统.网络状态监视程序”。其中“网络测试服务程序”安装在一个距离核心交换机较近的服务器上，24 小时后台运行。“网络状态监视程序”可以安装在与网络连接的任意客户机上。此外还需要北海分局现有的虚拟化池和数据库服务器提供相应的支持，系统的部署如图 2 所示。

1) 网络通信测试

实现网络通信、网络联通的授权管理，联通状态的预测试和要检查的网络节点的读取，通过 Threading 组件采用多线程的方式发送 Ping 命令，并对 Ping 命令返回的信息进行解读，对网络通讯情况进行评价，并将评价结果(优、良、中、差、断)写入数据表。该系统采用有选择的双 Ping 技术，节约开销的同时也确保了系统的鲁棒性[9]。见图 3。

2) 实时数据采集

实现对每次扫描(全部节点 Ping 返回)后，对所有节点的通讯情况进行统计，形成小时、日、周、月、年统计结果，统计结果显示为优良比例、中差比例、断比例；采用容错技术，对故障节点(Ping 不通)的中断情况进行统计，当发现超过一定的阈值。(用户可以根据每个节点实际网络情况自定义每个节点阈值大小，系统也可在每个故障节点用户实际处理结果提示用户设置更合理阈值)时，向指定手机发送短信报警信息，当节点通信恢复正常后向指定手机发送恢复信息[10]。见图 4。

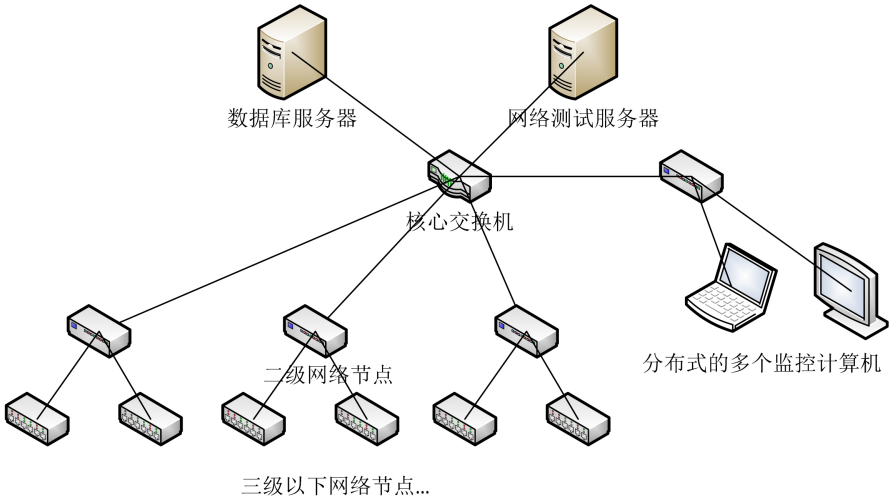

Figure 2. Network structure diagram of state detection supervision system of Beihai Branch
图 2. 北海分局网络状态探测监管系统网络结构示意图

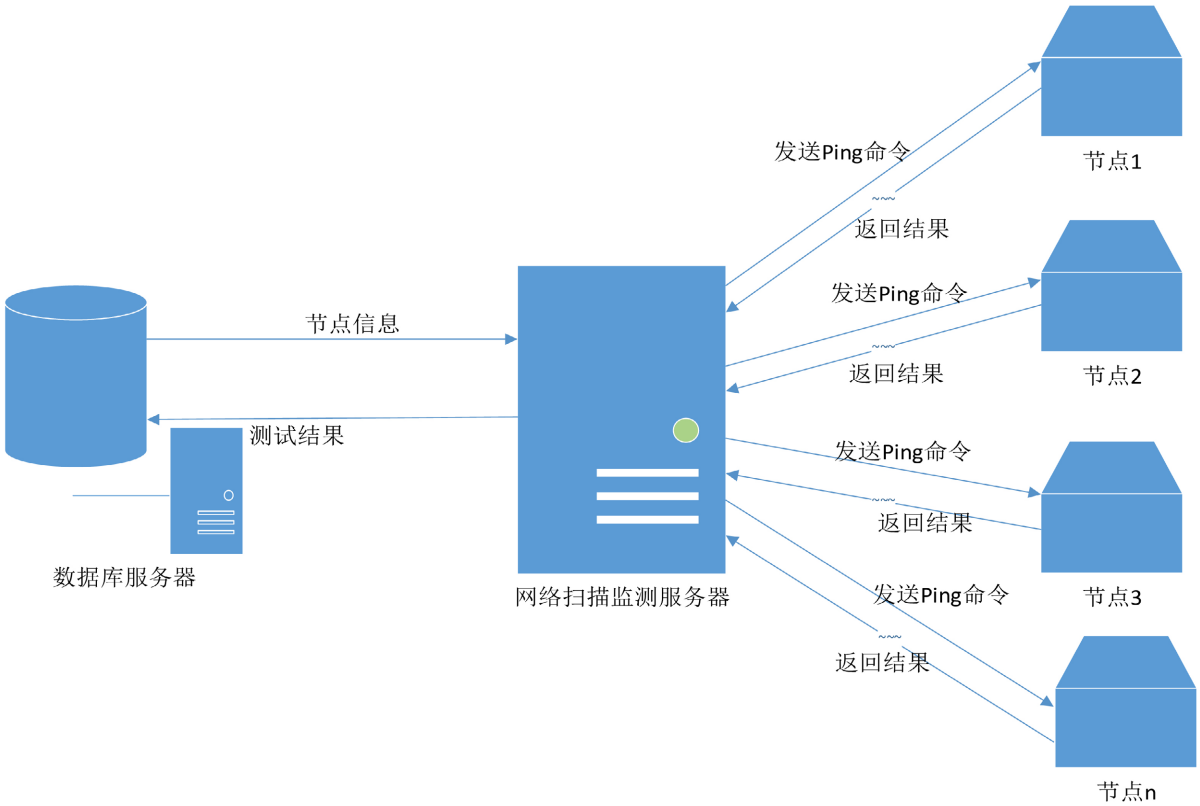

Figure 3. Network communication and testing
图 3. 网络通信与测试

3) 节点初始状态扫描统计分析输出

根据配置文件指定目录，输出节点统计网页，统计内容包括：当前全部节点通讯完好率、小时/日/月/年通讯完好率、系统总运行天数、总运行小时数、总扫描节点数；输出节点通讯统计堆叠图，堆叠内容包括网络优良比例、中差比例、断比例，时间为 24 小时滚动、31 天滚动、月统计和年统计。见图 5。

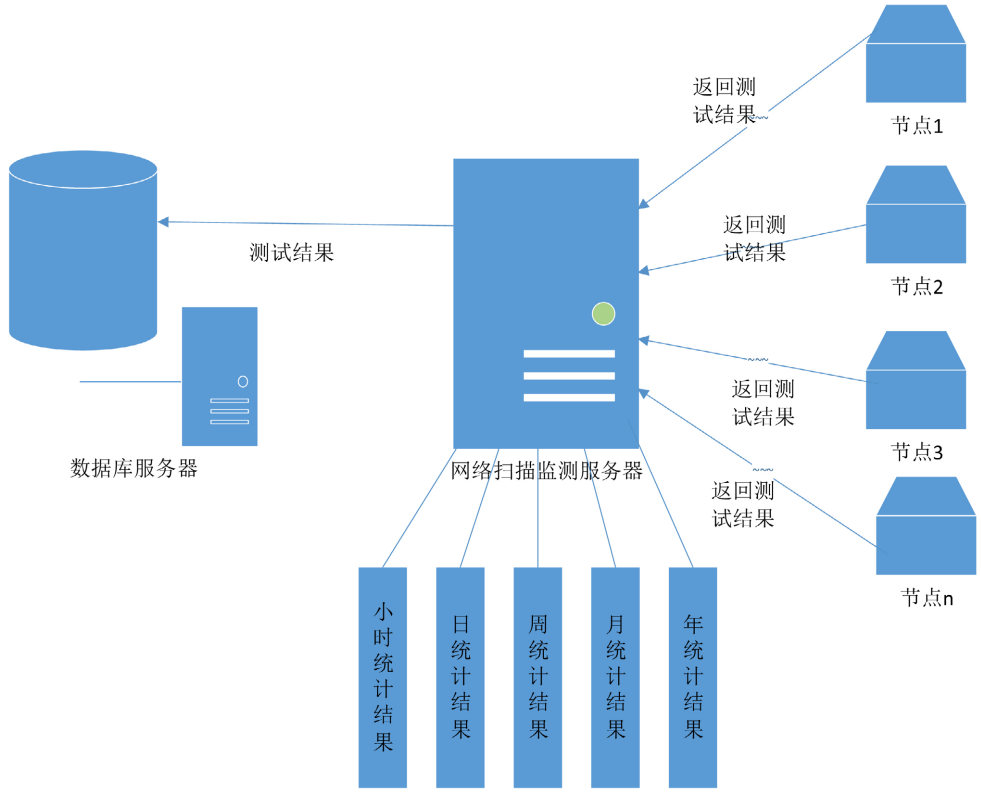

Figure 4. Network data collection
图 4. 网络数据采集

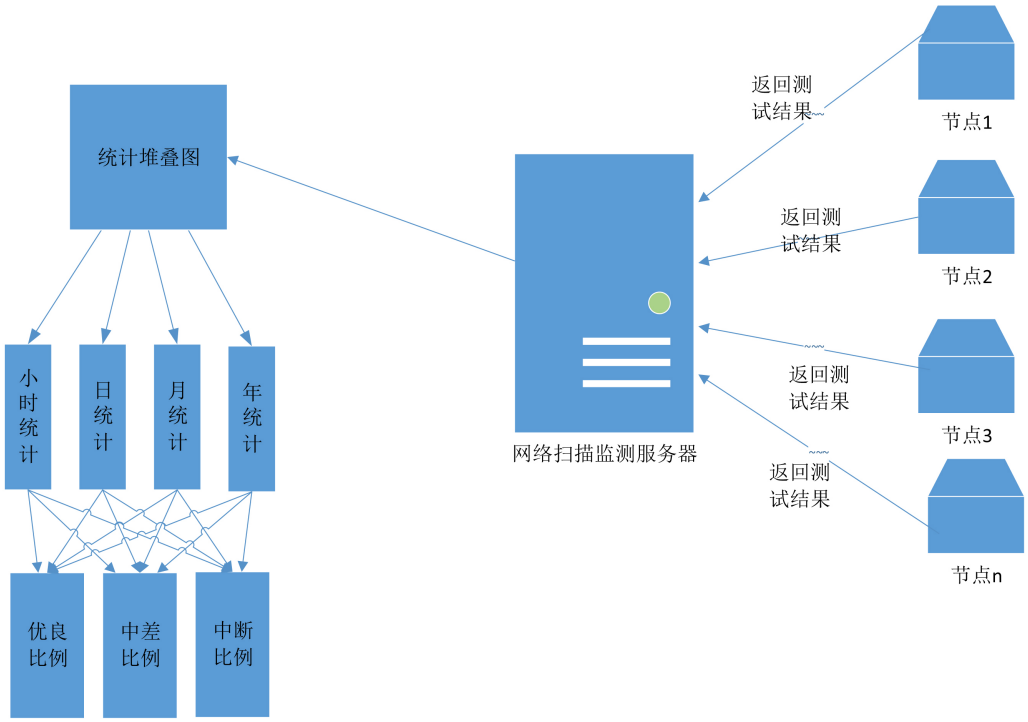

Figure 5. Statistical output of initial status scanning of nodes
图 5. 节点初始状态扫描统计输出图

4) 节点实时数据扫描统计分析输出

根据配置文件指定目录，输出网络节点通讯实时状况表，并输出节点通讯统计堆叠图，堆叠图的内容包括网络优良比例、中差比例、断比例，时间为 24 小时滚动、31 天滚动、月统计。系统扫描刷新时间可以由用户通过配置文件自行定制，Ping 命令的超时时间可以由用户通过配置文件自行定制；

根据配置文件指定目录，输出网络节点通讯故障一览表，包括：IP 地址、站点名称、节点类别、节点名称、中断时间、恢复时间、当前状态和中断原因。同时检查、统计和短信发送过程都将生成日志文件，并写入数据库。

同时为了保证系统运行效率，系统每天自动生成一个数据表，Ping 结果按日写入相应的数据表中，并可以设置自动删除时间过久的基础数据表，避免数据库过大，降低系统冗余性[11]。

4. 取得的效果

将网络拓扑协议分析方法引入到整合后的分局网络检查、监视、报警、运维与故障排除中，取代了原有人工进行协议分析和网络扫描的简单工作，极大的提高了整合后的网络管理能力和故障排除能力。

将 C#的多线程技术与 ICMP 协议分析结合起来，在减少网络扫描数据量的同时最大程度实现对网络拓扑结构和网络节点状态信息的获取，解决了分局网络整合后多 VPN 网关和多种设备共用产生的网络管理问题，提高了分局网络的智能化管理水平。

5. 应用实例

本研究成果已成功应用于自然资源部北海区地面传输观测网业务化应用。通过本研究成果的实际应用，在北海区网络设备“管理网段”及“7 个 VPN 网段”共 8 个网段中实现了对各关键网络节点通讯网关的连通性及响应时间的实时监控，并通过设定的合理阈值及时对网络连通性问题和通讯质量故障进行自动报警，提高了网络节点的管理能力，及时发现网络节点故障，加强了对北海区海洋在线观测、监测和监视监控业务支持能力。

图 6 和图 7 为应用效果图。

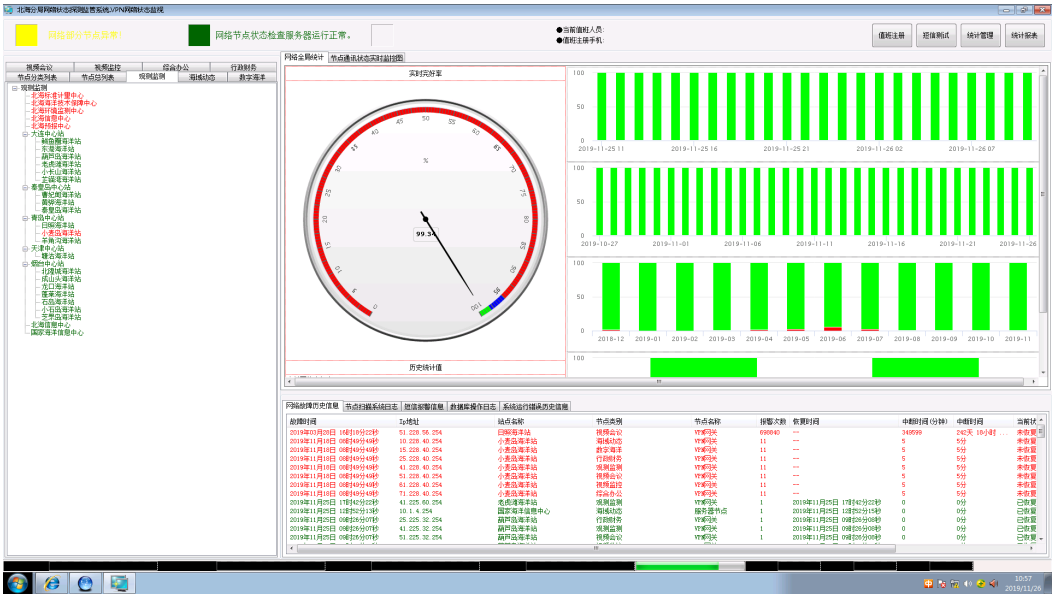

Figure 6. Application effect diagram
图 6. 应用效果图

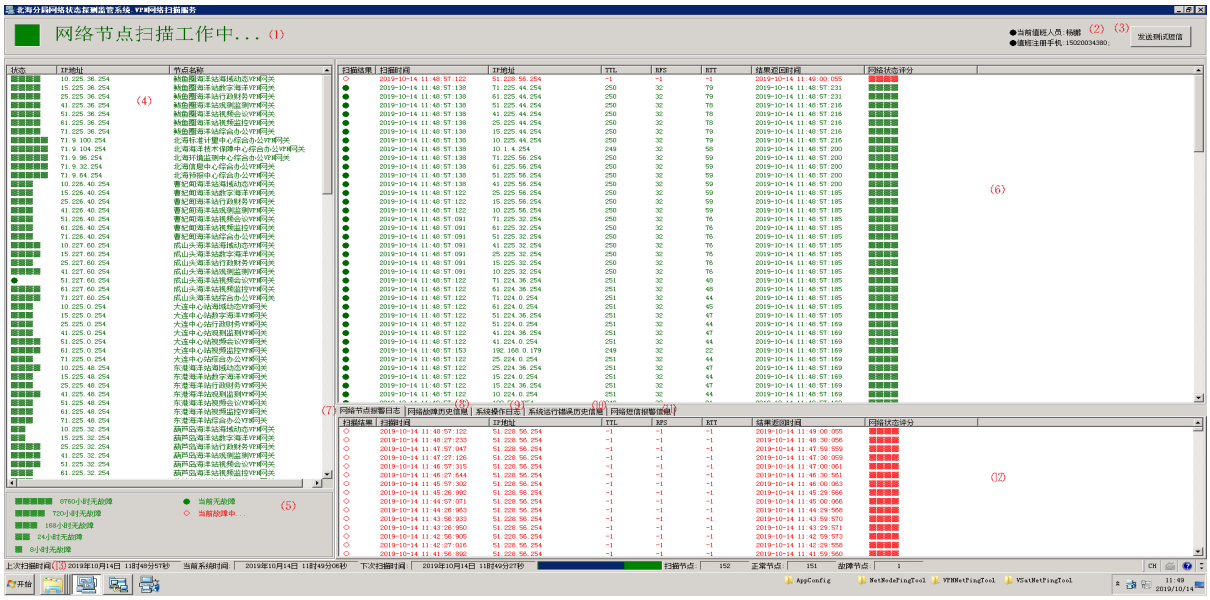

Figure 7. Application effect diagram
图 7. 应用效果图

6. 结论与创新

本研究将网络拓扑协议分析方法引入到整合后的分局网络检查、监视、报警、运维与故障排除中，取代了原有人工进行协议分析和网络扫描的简单工作，极大的提高了整合后的网络管理能力和故障排除能力。将 C#的多线程技术与 ICMP 协议分析结合起来，在减少网络扫描数据量的同时最大程度实现对网络拓扑结构和网络节点状态信息的获取，解决了分局网络整合后多 VPN 网关和多种设备共用产生的网络管理问题，提高了分局网络的智能化管理水平。随着系统的不断应用完善，结合更先进成熟的技术利用，未来可进一步完善网络监控算法及智能化程度，逐步实现更加智能、高效的网络智能化管理及安全态势研判能力。

基金支持

国家重点研发计划“海洋环境安全保障”重点专项“船载技术系统”课题 4“船载通信系统”(2017YFC***04)，自然资源部北海局海洋科技项目(201905)支持。

参考文献

[1] 赵玲. 网络拓扑发现算法的研究[D]: [硕士学位论文]. 吉林: 吉林大学, 2011.

[2] 吴君青, 陈卫卫, 胡谷雨. 物理网络拓扑发现算法的研究与改进[J]. 北京邮电大学学报, 2003, 26(z2): 139-144. https://doi.org/10.3969/j.issn.1007-5321.2003.z2.025

[3] 朱有产, 李春祥. 一种跨 VLAN 的网络拓扑发现算法[J]. 计算机工程, 2005, 31(3): 134-136+139.

[4] 田云兵. 基于 SNMP 网络管理的研究与应用[J]. 科技创新与应用, 2014(12): 51-52.

[5] 金培欣. 一种基于 EXCEL 工作表的网络管理数据的提取方法[J]. 大众科技, 2014(2): 27-28-32.

[6] 杨时茂. 基于 ICMP 和 UDP 的非合作网络拓扑发现技术研究与实现[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2014.

[7] 骆斌, 费翔林. 多线程技术的研究与应用[J]. 计算机研究与发展, 2000, 37(4): 407-412.

[8] 蔡雨辰, 赵保军, 邓宸伟, 等. 实时信息处理系统多线程框架的高效设计方法[J]. 高技术通讯, 2013, 23(1): 42-48.

https://doi.org/10.3772/j.issn.1002-0470.2013.01.007

[9] 张倩. 基于 ICMP 和 SNMP 的网络性能监测的分析和设计[D]: [硕士学位论文]. 镇江: 江苏大学, 2010. https://doi.org/10.7666/d.y2042720

[10] 史振华, 刘外喜, 杨家烨, 等. SDN 架构下基于 ICMP 流量的网络异常检测方法[J]. 计算机系统应用, 2016, 25(4): 135-142.

[11] 曹文斌, 陈国顺, 牛刚, 等. 基于 ICMP 和 SNMP 的网络设备监测技术[J]. 计算机工程与设计, 2014, 35(4): 1152-1155+1160. https://doi.org/10.3969/j.issn.1000-7024.2014.04.007