Chapter 14
A P2P-Based Strongly Distributed Network Polling Solution

Cristina Melchiors
Federal University of Rio Grande do Sul, Brazil

Dionatan Teixeira Mattjie
Federal University of Rio Grande do Sul, Brazil

Carlos Raniery Paula dos Santos
Federal University of Rio Grande do Sul, Brazil

André Panisson
Federal University of Rio Grande do Sul, Brazil

Lisandro Zambenedetti Granville
Federal University of Rio Grande do Sul, Brazil

Liane Margarida Rockenbach Tarouco
Federal University of Rio Grande do Sul, Brazil

ABSTRACT

Several activities are employed in network management to ensure correct network operation, including administration, monitoring, and provisioning of network devices. Among them, one of the most CPU- and bandwidth-intensive tasks is network polling. Although this task has to be performed in several real network management situations, it presents serious scalability and fault tolerance drawbacks if executed using traditional management architectures such as centralized or weakly distributed ones. It demonstrates the importance of investigating alternative architectures. This chapter presents a strongly distributed architecture for network polling. This architecture follows a P2P-based distributed management model, looking at P2P as an infrastructure that can be used to provide support for management operations to be accomplished in a highly distributed way. The chapter presents the polling architecture design, discusses the implemented prototype and the performance evaluation carried out to validate the approach, and provides a comparative analysis of the architecture with two other distributed polling approaches.

DOI: 10.4018/978-1-61350-110-8.ch014

INTRODUCTION

Several activities are employed in network management to ensure correct network operation, including activities for administration, maintenance, and provisioning of network devices (Commer, 2006; Clemm, 2007). Among these activities, one of the most CPU- and bandwidth-intensive tasks is network polling, used for network monitoring. This activity is performed by a network manager entity, which periodically requests status and performance information from a typically large set of network agent entities. The collected information enables, for example, the detection of critical conditions that require some reaction from the management system in order to lead the managed infrastructure back to a stable, safe state. It also can be used to collect periodic performance data for statistical and trending analyses.

When carried out using traditional management models, based on centralized and weakly distributed management paradigms (Martin-Flatin, Znaty & Hubaux, 1999; Martin-Flatin, 2003; Schönwälder, Quittek & Kappler, 2000), the employment of polling to monitor modern, high speed networks becomes a critical issue because the volume of generated traffic and the processing power required to deal with this management information is prohibitive. Given that, polling tends to be avoided as much as possible, or even replaced by other methods, such as instrumenting managed devices to automatically send a notification when anomalous situations are internally detected.

However, avoiding polling activity is not possible in many situations. It occurs, for example, when a management application must monitor the status of a device variable that does not generate events. It also happens when the notification itself is sent via an unreliable transport mechanism such as the User Datagram Protocol (UDP) as used by the Trap messages in the Simple Network Management Protocol (SNMP) (Harrington, Presuhn & Wijnen, 2002). In fact, it occurs frequently, as can be observed in recent investigations (Schönwälder, Pras, Harvan, Schippers & van de Meent, 2007) on the actual use of SNMP, in which SNMPv2 confirmed notifications (Inform messages) (Harrington, Presuhn & Wijnen, 2002) were rarely found in SNMP usage in actual production networks. In addition, such research work (Schönwälder, Pras, Harvan, Schippers & van de Meent, 2007) has confirmed that traditional, polling-based network monitoring responds for most of the SNMP traffic generated. This means that although alternatives for polling do exist, traditional polling is still extensively employed.

Nevertheless, polling architectures of traditional management models are not feasible to be used in modern networks. In such traditional architectures, the polling of all devices is executed by a single or few management stations. This causes serious scalability problems because there is a large overload of management traffic in the management stations as well as in the links close to them. Moreover, such architectures have fault tolerance problems because, if the communication between the managed device and the management stations is lost, the monitoring of all devices managed by this station is interrupted. This way, alternative approaches have to be investigated to execute polling-based network monitoring in current days.

A promising alternative for distributed management systems is peer-to-peer (P2P) technology (Lua, Crowcroft, Pias, Sharma & Lim, 2005; Androutsellis-Theotokis & Spinellis, 2004). P2P systems are largely used today in distributed systems, in a large range of application fields, including file sharing, communication, collaboration, distributed computing and distributed storage. Such systems operate based on virtual networks (called P2P overlay networks) composed of heterogeneous nodes (peers) and virtual links between such nodes. Because of its features, it can be analyzed as a technology that provides support for the distribution of network management operations to a large number of peers, bringing benefits