Managing Central Monitoring in Distributed Systems

White Paper

Author: Daniel Zobel, Documentation and Support at Paessler AG

Contents

Introduction

Companies with multiple locations rely on a highly efficient IT infrastructure to ensure the smooth running of IT processes and reliable communication both internally (across company locations), as well as externally (with partners and customers). Ongoing monitoring is vital for multiple-location companies, as it enables them to keep a constant and close eye on the availability and bandwidth usage of locally distributed networks. This provides important information about the state of the networks and alerts IT staff when devices in the network are going to reach critical levels.

This White Paper shows how network monitoring can be extended to additional locations, using PRTG Network Monitor and its use of remote probes as an example.

The Probe Principle for Versatile Applications

PRTG Network Monitor provides network monitoring out-of-the-box. The first monitoring results are available immediately after installation and auto-discovery. Neither additional remote installations nor agents on the target systems are needed, because PRTG uses the standard protocols of the hardware manufacturers to retrieve information.

In addition to this standard scenario, there are a variety of application areas which require extended network monitoring. For these, a central installation of PRTG combined with additional remote probes can be set up. Remote probes can be thought of as small programs running on a computer anywhere in the network; they are in constant communication with the central PRTG installation, continually forwarding monitoring data. If the physical connection between remote probe and core server should be interrupted, the probe can buffer monitoring data and send it once the connection is reestablished.

Remote probes allow monitoring of multiple locations.

This configuration is relevant for all companies with a network spread over several locations, VPNs, or firewall separated network segments that target centralized network monitoring across different local or distributed networks (LANs/WANs). Remote probes are also a convenient and efficient solution for IT service providers that want to offer their customers a higher service level by monitoring networks directly within the customer's infrastructure.

The remote probe architecture is highly valuable for a number of special technical solutions:

• For simple load distribution of the monitoring tasks on several individual computers; this is recommended, for example, for extensive use of the slow WMI protocol in large networks.

• To establish a generally secure connection for transmitting monitoring data between two secured sites over the open Internet.

• For monitoring completely encapsulated services, such as mail or web server.

• The probe technology allows the administrator to measure the Quality of Service (QoS) of a network without any additional tools. The necessary test track is simply established between two PRTG probes.

Figure:
A standard installation of PRTG consists of core server and local probe

Local Probe

PRTG Core Server
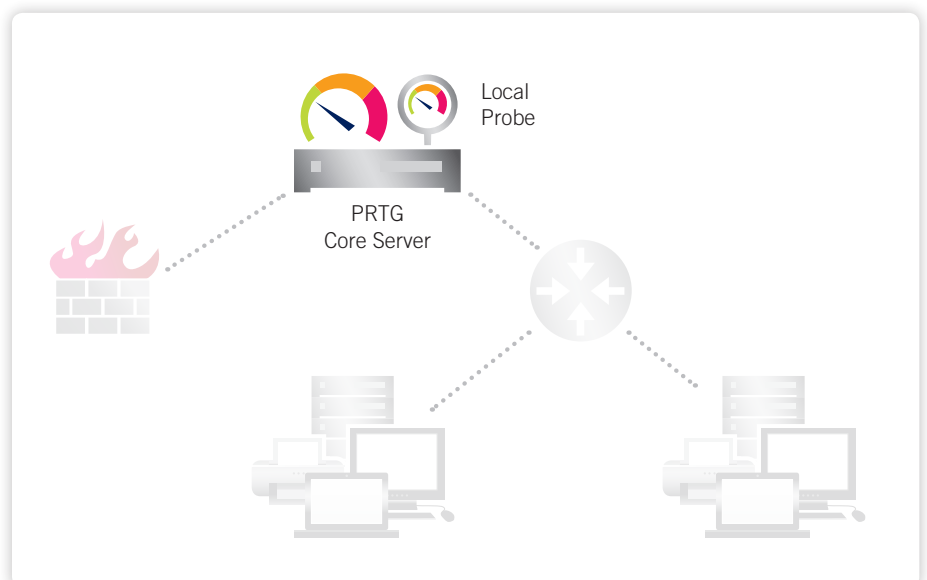
PRTG's Probe Architecture

The software architecture of PRTG is unique and yet very simple. A default installation of PRTG initially consists of a central server and a local probe, each running as a service on any Windows computer on the network. The server stores the configuration and manages the monitoring data, reports, and notifications. It also provides a web server for the interface where the user can change settings and review monitoring data. The actual network monitoring is done by the local probe. It communicates via standard protocols with devices, as well as computers, and forwards received data to the PRTG core server. Monitoring can, for example, be conducted via SNMP, WMI, or WBEM; NetFlow protocols and packet sniffing are also used for traffic analysis. All data converges in a central monitoring solution, regardless of how it is received, and is then evaluated and analyzed. Various "triggers" prompt notifications or specific actions, for example, when certain thresholds are exceeded or when a device no longer reacts to a ping request. Even an automatic reboot of a monitored computer can be triggered in this way.

Solutions for Companies With a Distributed Infrastructure

Data from different protocols is managed centrally.

If necessary, remote probes can be added to the architecture with one single local probe. They are installed on another computer and run in the background. They communicate with the devices in their network and also send monitoring data to the PRTG core server. Unlike the local probe, a remote probe can be located in a completely different network and behind a firewall. It can monitor the network it is installed on "from the inside" and establish an encrypted connection to the PRTG core server outside. This way, network monitoring can easily be extended without exposing the network to the outside world. This maximizes security. These remote locations are seamlessly integrated into the monitoring solution, enabling the administrator to oversee all networks centrally.

Figure:
Paessler's probe in San Francisco in action (PRTG web interface)
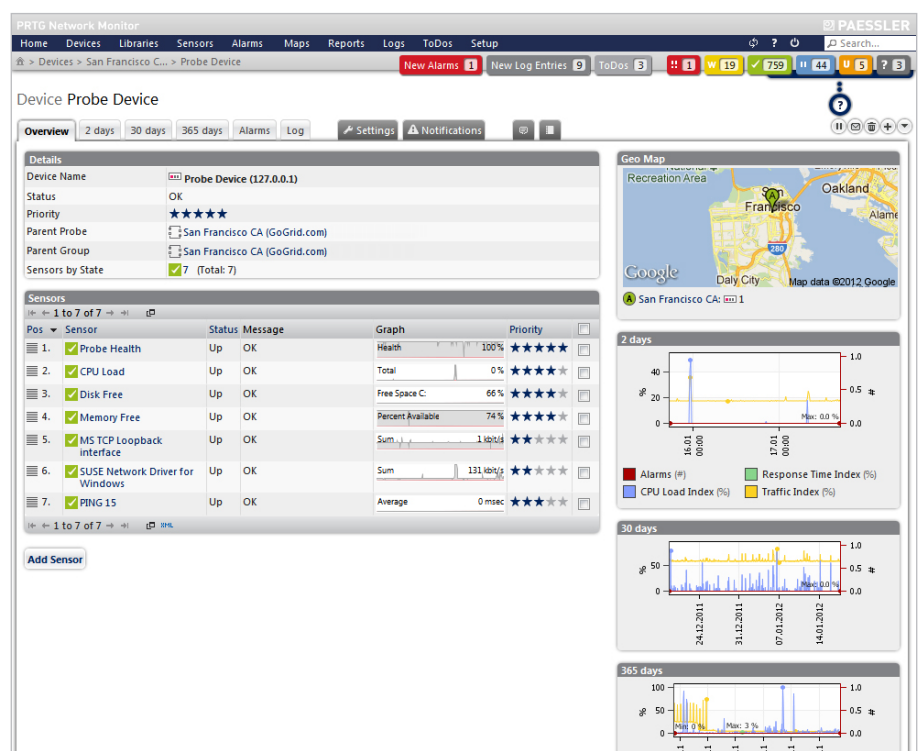
Multiple Locations

Using the probe functionality, a company with distributed infrastructure can integrate its own branch offices into central network monitoring even if they are behind firewalls in their own networks. This requires a one-time only installation of a central PRTG core server and several probes—one in each branch office. The company's available network connections are used for the connection between the branch offices and the headquarters, for example, this could be an existing VPN connection.

Minimize security risks using SSL: The server- probe-connection is encrypted by default.

Sometimes sensitive monitoring data is collected and sent via the data stream between the probe and the core server. In addition, the probe receives the complete configuration through this connection with all necessary access rights to the monitored systems from the server. These are often passwords with administrator privileges to gain access to very machine-oriented information. So that sensitive information such as this doesn't fall into the wrong hands, the communication between the PRTG core server and the probes is always SSL-encrypted. Even a server-probe connection across the open Internet does not pose a security risk.

External mail servers hosted at a provider's can be integrated into the central monitoring setup using remote probes.

Company-owned mail servers running at a hosting provider's, and other components of the IT infrastructure that are not externally accessible via an HTTP connection, can easily be integrated into network monitoring using probes. Also, the IT department is informed of problems at all times and can gather workload statistics.

Figure:
Use of remote probes for integrating branch offices and for monitoring 'encapsulated' services. The probes monitor their respective sub-network and transmit the results to the central server.
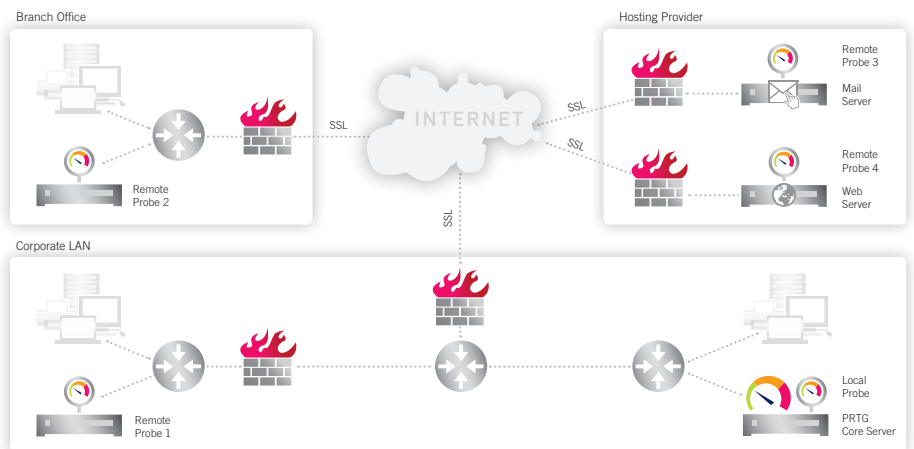
Simple Solutions for Managed Service Providers

Service providers in the IT industry, so-called "Managed Service Providers" (MSPs) are able to offer their customers intelligent monitoring directly at the customer's sites by setting up a central server in combination with many remote probes. This makes it easy for them to offer network monitoring as a service. The MSP simply needs one central system that is responsible for data analysis, failure notifications (to the MSP or to the customer directly), and even the production of extensive reports. Individual reports can be created for every customer, for example, reports about availability (uptime), workload of specific devices, or volume of Internet traffic. As such, the service provider does

not have to run and maintain an individual (virtual) server for every customer, and only needs to configure and maintain one central server installation. This saves both time and money.

On the customer's side, only a single remote probe is required. This monitors the customer's network "from the inside" and transmits the results to the MSP's server in an encrypted connection via the customer's pre-existing broadband connection.

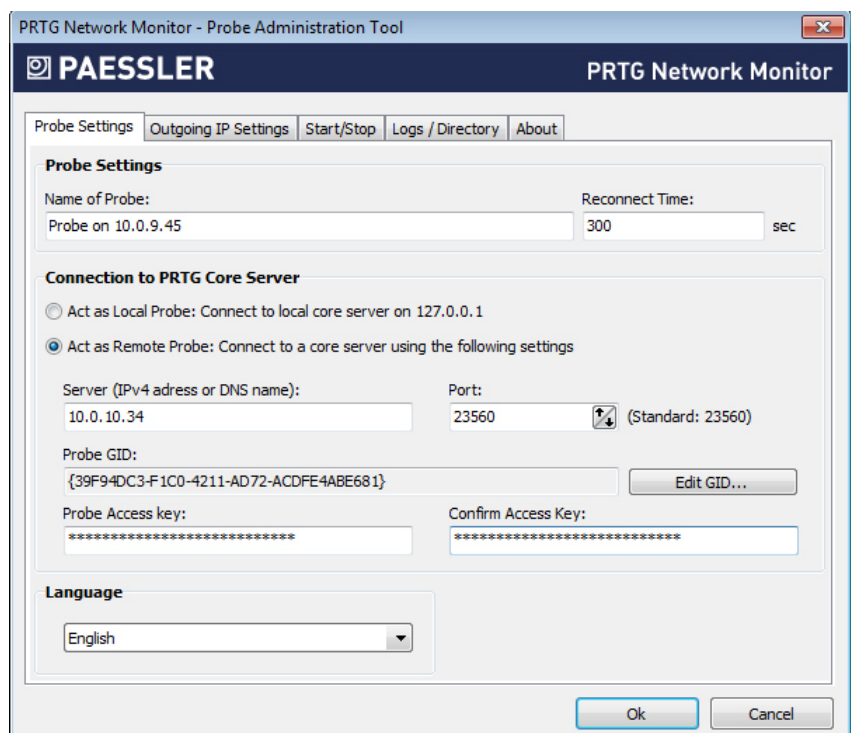**All an MSP requires in a customer's network is a remote probe.**

The cost for integration is minimal; if existing servers can be used, there is no need for hardware to be set up at the customer's. If, however, a separate PC is required, the probe software does not need high system resources, so that even very low-cost devices are sufficient for a small network, such as a thin client or a netbook. Alternatively, the probe can also be operated on a virtual machine (e.g.VMware, Hyper-V, or XEN).

If the customer network consists of several sub-networks, one probe is installed in each. They all establish a direct connection to the PRTG core server using the same port. So, the configuration work for the firewalls is manageable. The individual probe is recognized and authenticated by the PRTG core server via unique identifiers to ensure that only authorized probes may establish a connection.

Figure:
A unique key is used for probe authentication

The possible number of probes used is not technically limited by PRTG, so an MSP can serve a variety of customers and extend monitoring continuously.

An MSP customer can be migrated to a separate virtual server easily, if necessary.

Once a monitoring solution is established, the customer is often interested in additional monitoring data and scenarios. Requirements grow easily with advanced network monitoring. If the customer wants his/her own independent installation later on, the MSP can easily set up a virtual or real server. Still, the monitoring is done via remote probes. Existing probes in the customer's network can be used continuously without the need to integrate additional hardware. The MSP still provides the service and looks after the operation of the server.

Quick setup: The customer's setup effort is minimal.

The customer's firewall is not "perforated" because there is only one single port that needs to be opened for the probe connection. Such a connection is established by the probe from the inside of the network to the server outside; therefore, a change in the security settings on the customer's side is rarely necessary. This helps minimize the configuration effort.

Specific Solutions for Specific Scenarios

Special configurations often require special monitoring solutions. In this area, remote probes offer a number of applications that exceed simple central network monitoring of remote networks.

Load Balancing

If a very detailed monitoring is set up in a network, performance constraints can occur—depending on the number of sensors, the kind of monitoring technique and hardware used, and the topology of the network. For example, the use of packet sniffers typically uses more CPU power and RAM memory than simple SNMP monitoring; this is because with packet sniffing, there are much more data to analyze. Also, extensive use of the WMI protocol requires additional resources.

Spreading the load: Additional probes can relieve the local probe on the core server and take over parts of the monitoring.

If the administrator monitors the network relying heavily on these techniques, more powerful hardware is sometimes needed to process the volume of data in a reasonable time. Alternatively, network monitoring can be spread to several probes on the network, each of them taking over parts of the monitoring, so relieving the central core server. Each probe can be installed on its own system. The collected data converge at the central PRTG server, ready to be evaluated.

Ensuring an Encrypted Transmission

In the case of SNMP, the encrypted standard (version 3) is not well established. Many recent devices still only support SNMP v1, using a very simple authentication and insecure clear-text transmission of data. This is not a problem as long as, for example, information such as the printer toner level is transmitted. But when monitoring a router, more sensitive data may be transferred which could for example reveal information on the surfing habits of certain users.

Remote probes can compensate for the security risks of obsolete hardware.

Often there is no hardware alternative to SNMP v1. To ensure that sensitive data cannot be intercepted on its way to the central server, the administrator can install a remote probe in the network of these devices and monitor them from there. The collected data will then be transmitted via the SSL-encrypted server-probe-connection.

Encapsulated Services

As previously mentioned, probes can also be used in systems which are generally inaccessible to the outside world. Windows web or mail servers are examples of such applications. If the administrator installs a probe on these servers, information about the systems can be queried from there—for example, using WMI sensors, processor load, memory and disk usage, or the current status of the mail queue. You do not require open ports for incoming connections for this, and the system's security is not compromised. However, current monitoring data is always available because, from the inside of its network, the probe establishes a connection to the central PRTG core server. If an irregularity occurs, PRTG's notification system immediately informs the administrator in charge.

Monitoring from Different Perspectives

A company's website, or even its own web shop, is key to its image and reputation and often generates a significant proportion of the company's revenue. Even short outages can negatively impact sales figures, which is why monitoring the company's online presence is essential. In particular companies that operate internationally, increasingly rely on a content distribution network (CDN) that mirrors the web content on different servers around the globe and delivers it to the visitors from the server "next" to them (in a topological view). This leads to shorter response times (ping) and faster page loading.

Global perspectives: Probes can monitor a website from every continent.

With PRTG, administrators can install one probe for server monitoring on each continent and monitor the Internet website from different perspectives.[1] This way, they can easily compare the loading times of websites in different countries, for example in Europe, Asia, or the U.S. Each probe checks the loading time via a separate network connection and transmits this data to the central server. The administrator can then check if the measurements match those requested by the Board, if the CDN network should be extended, or if systems need to be upgraded.

If a company pays an ISP for a certain service level, the administrator can also check if service level agreements are met. To do so, a probe with a QoS sensor is installed on a server hosted at the provider. This allows administrators to determine the quality of the network between the host server and the company's location.

Figure: QoS-Monitoring
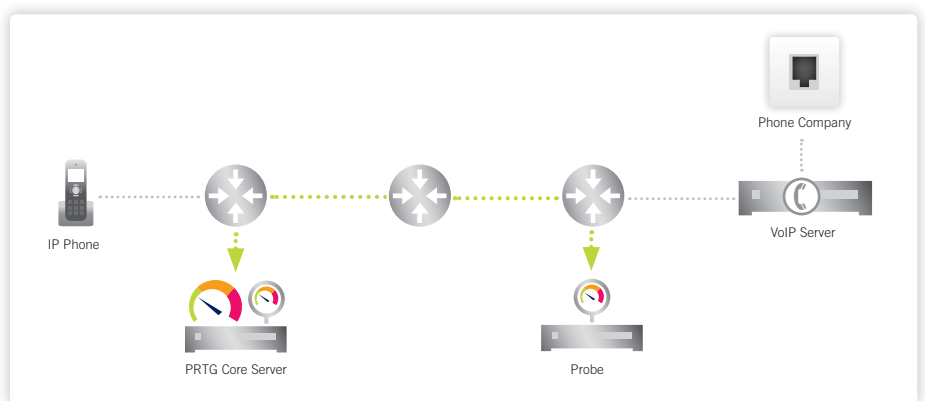
[1] An example of so-called „cloud" monitoring can be found at http://www.cloudclimate.com/
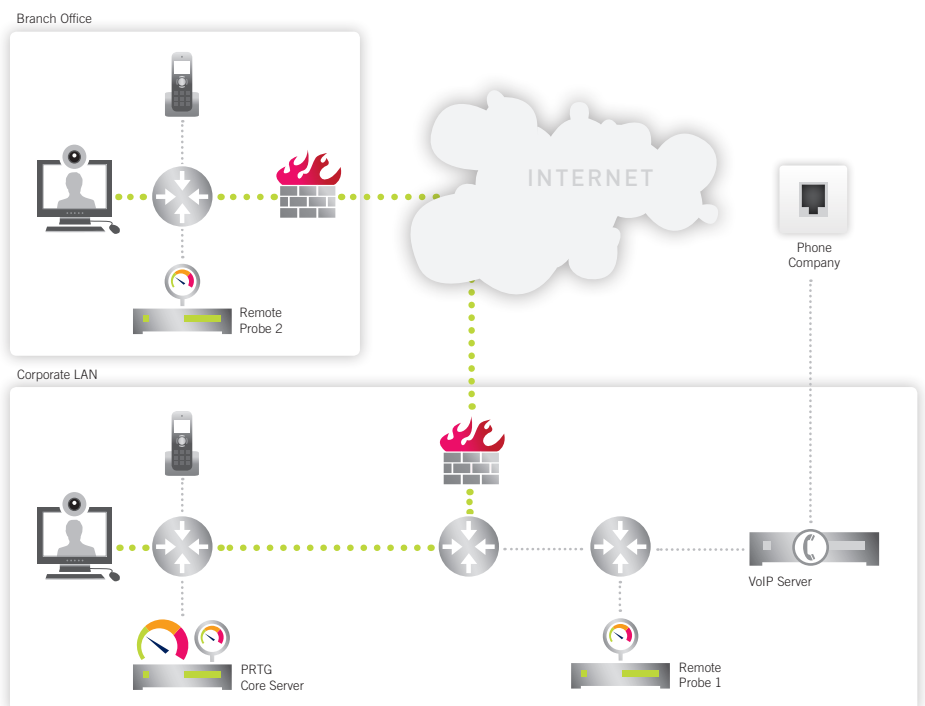
Quality of Service Measurements

In a network, high quality service is key to smooth business operations. This is true not only for the "normal" operation of a network, but also, in particular for the integration of Voice over IP (VoIP). With VoIP an assured Quality of Service (QoS) is essential because UDP-packet based voice communication is particularly sensitive to disturbances such as packet loss, jitter or major delays in packet transmission. Professional devices, such as high-end Cisco routers, support Quality of Service measurements of the network route between two devices via the IP-SLA protocol. PRTG can read and analyze this data.

Probes allow QoS measurements without expensive hardware.

If this type of hardware is not available, the administrator can build his own test track using probes to measure the service quality via PRTG's built-in QoS sensors. A connection is either made between the PRTG server and a probe, or two probes are used that can be installed on any servers on the LAN or even on the Internet. So, there is a good deal of flexibility for setting up the "measuring stations." One of the probes in this setup handles the collection of data and sends the measured values to the server, which further evaluates them. Using this scenario, PRTG monitors the connection in real-time and alerts IT administrators when it reaches critical levels. Thus, the administrator in charge is consistently informed about whether the VoIP minimum quality is met.

Figure:
VoIP-Monitoring

A Simple Concept with Many Possibilities

The ability to set up distributed monitoring on the network through the use of remote probes opens up many different areas of application. Regardless of which kind of monitoring a probe is set up to do, at all times all data are stored in one central server. As a result, by analyzing the data, the administrator can quickly and easily get an overview of all locations monitored.

Companies using remote probes benefit from centralized monitoring of all branch offices, while IT service providers benefit from being able to provide monitoring directly at the customer site, with minimum network intervention and without having to set up a separate virtual server for every customer. Probes are also suitable for special technical solutions e.g. for load balancing in very large or CPU-intensive installations, as an additional security feature for monitoring, or for monitoring encapsulated services, such as mail or web server. In addition, thanks to their flexible setup, probes can be used for network monitoring from different perspectives (as, for example, in CDN networks), or for setting up a test track to assure a network's Quality of Service. The data moving between the different components of the PRTG software is always transmitted SSL-encrypted, which ensures optimal security at all times.

The administrator needs a single server installation with one license only. Several probes are already included in all PRTG licenses; they can be installed quickly and are configured in the server interface. On the server side, the company saves money from the lower cost of maintaining one central installation, because the hardware and operating system are only required once.

About Paessler AG

Founded in 1997 and headquartered in Nuremberg, Germany, Paessler AG builds cost effective software that is both powerful and easy to use. The product range is specialized on network monitoring and testing as well as website analysis. Its products are used by network administrators, website operators, Internet service providers, and other IT professionals worldwide. Freeware and Free Trial versions of all products can be downloaded from www.paessler.com.

Paessler AG
Bucher Str. 79a, 90419 Nuremberg, Germany
www.paessler.com, info@paessler.com

VAT-ID: DE 217564187
TAX-ID: FA Nuremberg 241/120/60894
Registration: Amtsgericht Nuremberg HRB 23757

CEO/COO: Dirk Paessler, Christian Twardawa
Chairman: Dr. Marc Roessel