



# NEXUSTELECOM

WHITE PAPER

## NexusMETER

Challenges of VPN Performance Reporting

Issued Date	11 MAY 2007
Author	Mary-Lou Murphy
Issued by	Nexus Telecom, Switzerland
Document	T-12-00248



**NEXUSTELECOM**  
NETWORK AND SERVICE INVESTIGATION

# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>4</b>
<b>2</b>	<b>The challenges of VPN Performance Reporting.....</b>	<b>4</b>
2.1	VPN Metrics.....	6
2.2	How to measure the Metrics? .....	6
2.3	Service Level Verification .....	7
2.4	Customer v. Provider Viewpoints.....	8
2.5	Consequences of SNMP Protocol Weaknesses.....	9
<b>3</b>	<b>VPN Performance Reporting.....</b>	<b>10</b>
3.1	Similar Look and Feel.....	10
3.2	tatistics from Multiple Sources.....	11
3.3	Draft MIB Support.....	11
3.4	Reports for the NOC and the Customer.....	12
<b>4</b>	<b>Bringing it Together .....</b>	<b>12</b>
<b>5</b>	<b>VPN Reporting Summary within NexusMETER.....</b>	<b>13</b>
<b>6</b>	<b>Conclusion .....</b>	<b>14</b>
<b>7</b>	<b>About NexusMETER .....</b>	<b>14</b>
<b>8</b>	<b>About Nexus Telecom .....</b>	<b>16</b>

## Executive Summary

This paper examines some of the challenges involved in providing accurate statistics for VPNs and explains how the flexibility of the NexusMETER application permits VPN service providers to provide accurate and trustworthy reports to their customers, with relevant data in a customer-oriented manner.

One of the challenges for VPN providers is to ensure consistency across multiple offerings that appear to the customer to be similar, if not identical. NexusMETER is uniquely capable of working with VPNs of any type and from any vendor. No matter where the data originates, it is presented in a consistent manner with the same performance metrics provided in all cases.

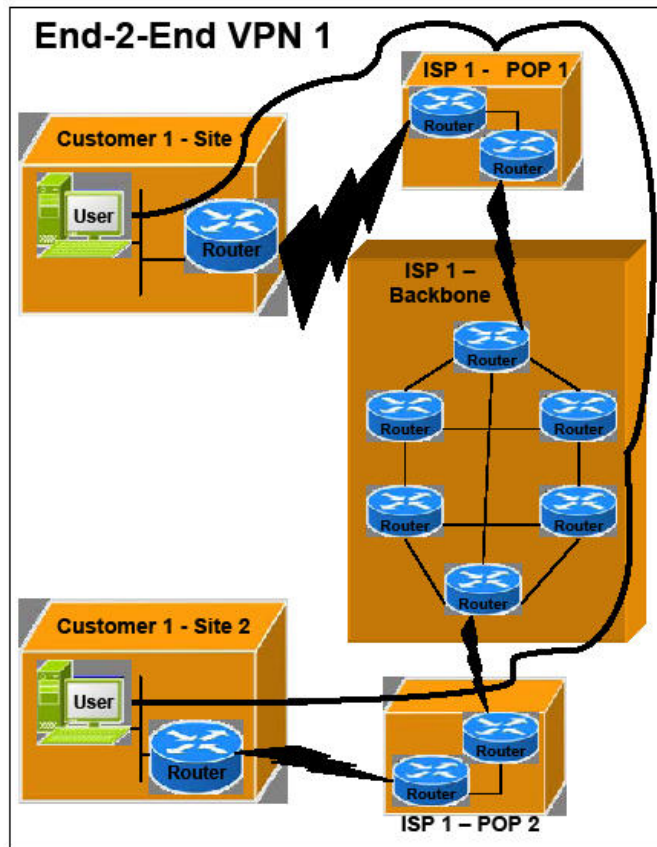
## 1 Introduction

Service offerings have had to adapt as the world migrates from traditional data services such as Frame-Relay and ATM to IP and VPN. VPNs provide a level of flexibility and ease of provisioning that is welcomed by customers and providers alike, but this does not mean that VPNs are in all ways simpler than the offerings they replace. Both the benefits and the challenges in VPNs are due to the first letter – the V – of the acronym. The Virtual nature of VPNs allows for great flexibility in deployment and speed of provisioning, as well as reducing the cost of such provisioning to the carrier; indeed it can even potentially permit a customer to provision his own network dynamically. However, that flexibility and speed comes at a cost of general lack of clarity about the service provided that can easily lead to severe customer dissatisfaction in the event of problems.

One of the most troublesome areas of VPN operation is adherence to a Service Level Agreement (SLA). In many cases, VPN providers are unable to demonstrate their compliance with an SLA and have to accept the customer's word regarding the duration or severity of an outage when dealing with it. While clearly not an advantageous position to be in, frequently the only alternative is to place dedicated hardware probes on the affected VPN, a solution which is both costly and practically impossible to scale. As this white paper will demonstrate, NexusMETER, by virtue of its breadth of coverage, is able to obtain the correct metrics from any device in the path and thus provide a third alternative, one that is not only cost effective and scalable, but which precisely identifies the duration and extent of any SLA non-compliance.

## 2 The challenges of VPN Performance Reporting

Perhaps the greatest challenge is to provide meaningful statistics and reports about the VPN offered, to prove that it has met its associated Service Level Agreement (SLA). This is more complex than it was in previous network types, because there are a wide variety of underlying technologies that are used to provide a single service. Moreover, the service is virtual and usually uses just a fraction of the total bandwidth available; thus even basic statistics such as utilization or link quality are harder to quantify. For providers, one additional stumbling block is that, due to their origin as network management products, most generally available network reporting tools provide data in a format suitable for the provider, rather than in a format suitable for presentation to the customer. NexusMETER is unique in its ability to handle VPNs provisioned across heterogeneous networks, and makes it easy to provide reports in the form that customer IT staff or management desire.



**Figure 1: Example VPN**

Figure 1 shows a simple 2-point VPN for a customer. On each side the link leaving the customer building for the POP is the Customer Edge (CE). Where it enters the POP is the Provider Edge (PE). Between the two Provider Edges is the provider's network. It may well be that the provider subcontracts some of his long haul routes to a third party. It is important to note that the link between the two entities (CE and PE) is frequently provided by a carrier which is not the VPN provider. That link may, for example, be a DSL link offered by the incumbent operator, whereas either a separate section of the operator or an entirely different carrier may offer the VPN.

Details about who provides which service are irrelevant to most customers. Typically the customer just wants to know that the VPN is working and, if not, that there is a single point of contact to fix it. However, for the carrier it is rather more complex. The link between the PE and CE may be bad, necessitating a conversation with the link provider; the carrier may have problems in its own network; or the third party to whom it has subcontracted the bulk long distance data transfer may have problems. Moreover, the technologies and the network equipment at both ends may be different – a DSL link might be used to connect a branch office, while a leased fiber could be used for the main office. The provider may terminate one end in a Shasta or Redback-style Subscriber Management Device, and the other, for example, in a Juniper or Cisco router. However, this remains irrelevant to the customer; the customer wants a common set of reports that provide useful statistics on identical

relevant metrics at both ends, while large customers with multiple VPNs want the same statistics available for all of them, no matter that one is carried using MPLS, another using an RFC 2547 IP network, and so on.

This illustrates how flexibility in a provisioning method is both a curse and a blessing for VPNs. For the customer it should be a clear benefit, since he can use VPNs to provide connectivity between multiple locations connected to the Internet in different ways, and, in theory, the same flexibility benefits the provider. However, while this flexibility helps in the provisioning of the service, it hurts both provider and customer when it comes to monitoring, gathering statistics and providing status reports. Here, the very flexibility makes the job of gathering data more difficult, because the different devices may report either different statistics or the same statistics in different ways. What is needed is a way to collate and harmonize the various statistics produced and provide a report that gives information that is useful to customer and provider alike.

In order to do that, we have to work out what it is that should be reported and in what format the reports should be presented.

## 2.1 VPN Metrics

The basic metrics that need to be reported are:

- ▶ Availability
- ▶ Throughput/utilization
- ▶ Quality/packet loss
- ▶ Delay

These metrics may be provided at multiple points within the network. One could provide statistics from CE-CE, from PE-PE or from CE to PE. If the carrier has a third party providing backhaul, then for the carrier his network is also to some extent a VPN provided by this third party and, therefore, the same metrics need to be provided with regard to the subcontracted links and traffic.

## 2.2 How to measure the Metrics?

Throughput is quite simple, being just the number of bytes transmitted OUT of the VPN. Utilization represents this throughput over a particular time period compared with the SLA maximum over the same period. Thus from one metric the other is readily derivable.

Quality is the ratio of bytes received into the VPN to packets transmitted out at the other end. 100% quality means no data loss. If the VPN is being measured PE to PE, then the losses in CE-PE links are not included in the measure. However, it is important to note discards and errors on these links, as they do affect the perceived quality for the customer, who is typically unconcerned about where data loss occurs. The VPN provider must therefore provide these statistics even though he is probably unable to do anything to improve them.

Delay is generally measured in round trip terms (RTT). Not only does this solve the problem of time synchronization, it reflects the fact that most network traffic requires a response to each request. The key point is that the special delay-measuring packets must be almost identical to the regular traffic to ensure that they are routed the same way. It should be noted that some network equipment intentionally modifies its behavior with regard to classic RTT packets (ICMP pings), thus impacting the accuracy of the RTT statistics. This is particularly true for VPNs with multiple Classes of Service (delay measurements are required for each CoS), since the RTT packet must be classified identically to the CoS packets. As well as measuring delay, RTT packets can also be used to measure availability, because this can be calculated from the percentage of these packets that have no response or whose response is delayed above a certain threshold.

Availability is in many ways an overall metric that is provided by a combination of the others, since if the VPN is suffering from low quality or long delay, it is not available.

A VPN that offers multiple Classes of Service (CoS) represents, from a measurement perspective, multiple VPNs, each with its own set of metrics. In large and complex MPLS networks, for example, there is no guarantee that the various CoS levels for a VPN will follow the same path through the network. Unless the network is extremely under-utilized, it is certainly probable that the various levels will show radically different quality and delay figures, even if the levels follow the same route. As noted above, direct gauging of delay statistics for different CoS levels can be difficult to set up; though it is important to do so, as valid extrapolation of the statistics is otherwise impossible.

## 2.3 Service Level Verification

Typically, a VPN is negotiated as tied to a particular SLA. One of the big problems carriers face is proving to customers that they have indeed met the terms of the SLA or, in cases where the SLA has not been met, for how long it was breached. SLAs are generally measured in terms of the metrics above, thus carriers need to be able to report for each customer what the performance of their VPN(s) is with respect to these metrics. Indeed, a common complaint amongst both VPN providers and customers is that, apart from clear cases of total service unavailability over a protracted period, demonstrating that a VPN is in fact meeting its SLA can be exceedingly difficult.

Of course, SLAs are not just one-way, offered by the provider to the customer. In the other direction, customers frequently have some maximum total throughput for a particular time period (so many gigabytes per month, say, or utilization over 90% only for certain periods of the day), and the carrier also needs to be able to track how close the customer is to these upper limits in order to be able either to upgrade the customer or to terminate his services gracefully (i.e. with sufficient warning).

In both cases, the problem is not so crucial with a VPN provided to a large customer, since a provider is unlikely to have too many such customers, and can, therefore, devote the necessary resources to measuring. Likewise, the customer himself will probably have sufficiently competent technicians that can also quickly determine whether the VPN is meeting the SLA. The problem lies with VPNs to multiple small customers or, perhaps worst of all, with VPNs to a number of different partners. In these

instances, the customer is likely less able to perform network monitoring and, due to problems of scale (and cost), the provider is likely less able to dedicate sufficient resources to all these customers.

## 2.4 Customer v. Provider Viewpoints

As well as the issue of what should be measured and reported, there is the problem of taking data gathered from network elements and sorting it by customer. The customer doesn't want to get a report on, say, VPN KZ5NL between NYPOP05 and LONPOP13 and VPN KZ5PL between PAPOP03 and LONPOP13, since none of these names means anything to him. What he wants are reports on his VPN London-Paris and London-New York VPNs (as well as all the others). Typically, he wants to see overall summary reports, as well as various break downs, and only if there are problems does he want to see data on a particular VPN. Furthermore, he wants to have historical data so that he can see trends and make appropriate adjustments based on predicted growth; he will not be interested in the fact that 6 months ago his VPN was moved from router LONPOP07 to LONPOP13. As far as he is concerned, it is the same VPN and he expects statistical continuity.

The major problem with current reports is that they tend to present things from the provider's perspective rather than the customer's. The provider looks at each VPN as just one of a whole collection of traffic passing through part of his network; thus VPNs are typically reported by PE router or by the aggregate using a particular interface or path. Thus, for the provider, it is hard to create a report summary consisting of data about VPNs on different paths. It may be easy to produce a report for a particular VPN (say KZ5NL or KZ5PL), but it is often difficult to combine the two (and any others that a particular customer may have) into a single report — especially when there may be hundreds of other customers who want similar collations.

The non-homogeneity of network equipment is another problem, in that the provider and the reporting systems he uses will tend to gather statistics best between like devices, and thus not necessarily provide the end-end statistics that a customer would like. Will a Juniper router (say) respond correctly to the RTT packets sent by a Shasta? Moreover, a customer who has multiple sites may find that the reports available for the VPN between Site 1 and Site 2 are different from those between Site 2 and Site 3, or Site 3 and Site 4, because the network equipment or VPN technology used between the different sites is different. This is, to put it mildly, far from ideal.

Finally, and just to make things even more interesting, there is the fact that the VPN may travel over networks provided by multiple carriers. In the example above, we have a customer with two VPNs, one from London to Paris and the other from London to New York. It is quite likely that a European regional carrier will only offer the latter VPN through some sort of reciprocal arrangement with a North American one, where the North American carrier permits the European one to collocate some VPN termination gear within (one of) his New York POPs. Depending on how things are arranged, the path between the London and New York POPs – to say nothing of the line between the POP and the customer premises – could pass through the fibers, switches and routers of two or three carriers. The customer doesn't care about this, but the carrier most certainly does, since he has to ensure that his subcontracted or outsourced transmission gear is behaving correctly, and thus he needs to achieve

similar statistics for his own network and match them against the SLAs he signed. In the event that there are multiple carriers in the path, it is important that the VPN provider be able to gather statistics on each carrier's portion. In our example, if the transatlantic portion uses one carrier's equipment, and the part within North America uses a second carrier, then the VPN provider needs details from the router(s) between the two in order that he can alert the correct carrier when a problem occurs.

## 2.5 Consequences of SNMP Protocol Weaknesses

Because of the aforementioned efficiency, reliability and scalability issues, many of the benefits of network monitoring and performance management are lost in large networks. Instead of getting a global picture and then drilling down into potential trouble spots using the same management database, users often find it better to move between various local management systems, because the global system is not updated frequently with information from the local management systems.

Likewise, there is the problem of erroneous statistics. Without accurate numbers it is impossible to make sensible predictions for future traffic growth or other similar network trends. However, not only do many SNMP elements report "inconsistent" numbers, they also frequently zero counts after reporting the latest numbers. If the reported number is lost, then it is impossible to retrieve it again, thus leading to numbers that are on average far too low. Needless to say, packet loss is most likely during periods of network congestion. If these numbers are being used to estimate utilization they will tend to be least accurate precisely when the greatest accuracy is required. Given that budgets for capital expenditure are highly dependent on traffic utilization trends, if the trends are underreported, CAPEX budgets are liable to be underestimated, leading to sudden extra-budgetary expenditure when actual traffic unexpectedly exceeds capacity. Such an event does not usually reflect well on those perceived to be responsible for it, typically the network managers and their superiors.

There is also a customer satisfaction problem associated with undercounting of statistics in a service provider environment. If the customer has an SLA and he is self-monitoring, he will be less than pleased if his reports are different from those produced by his carrier. This dissatisfaction may be particularly acute if the service provider maintains that the customer has met his SLA, when the customer believes this not to be the case.

Finally, there is the impact of the overhead of the monitoring traffic on the network itself, and the likely reduction in reliability that results from handling this overhead. Clearly, network monitoring is a compromise. At one extreme, no network monitoring will of course incur no overhead and thus no reduction in reliability. However, this is countered by the fact that no monitoring means that there is no gathering of warning signs that indicate that a network is about to fail. At the other extreme, querying each network element every second will provide a highly accurate picture of the network at the expense of a considerable overhead in network traffic and, perhaps worse, a considerable processing overhead in the network elements, impacting their ability to respond in a timely fashion to events such as link failure and route reconvergence. Striking a balance between the two extremes would of course be easier if SNMP had a lower overhead.

## 3 VPN Performance Reporting

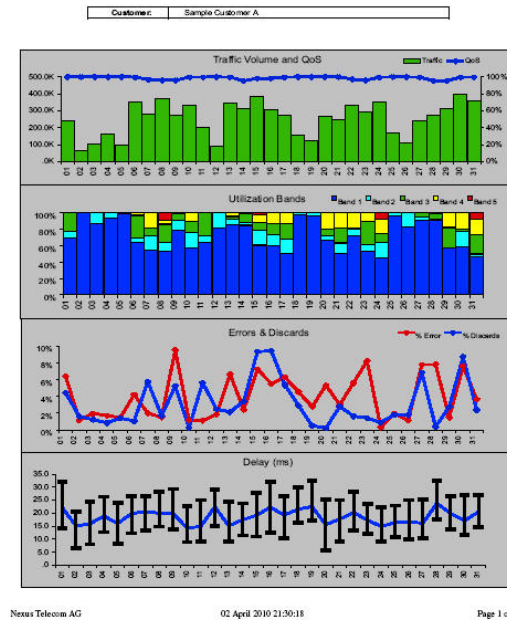
NexusMETER provides a series of reports explicitly tailored to providing a customer view of provider data. The reports can aggregate individual VPNs by site and by customer for suitable summary report generation. The reports can of course be customized with appropriate logos and other similar details. The reports can use data from a wide variety of devices, since the data is usually gathered using standard MIBs that are widely supported. In addition, equivalent data from Nortel's MSS products are also collected. These reports not only provide the relevant VPN data, they also provide them in a similar format to the reports produced for older technologies such as Frame Relay.

Since Nexus uses common standards for data gathering, it can provide the same reports no matter where in the network the data is gathered. No matter whether the VPN is measured CE-CE, PE-PE or some combination, the same data can be gathered and reported. Typically Nexus recommends that reports be gathered at the PE for a number of reasons. Firstly, this allows for sensible reporting of errors and discards on the CE-PE link, and thus eases troubleshooting – CE-CE VPN reporting combines these edge effects with packet loss within the provider network, which makes it harder to pinpoint a problem. Secondly, if the VPN is one with CoS then, since packets are usually classified only as they enter the PE device, CoS reports are not available (or hard to generate accurately) in other conformations.

However, the flexibility of the Nexus reports means that useful information can be gathered in non-PE/PE monitored VPNs. One common scenario in which this is important is a hub-and-spoke VPN service, where the hub has a single device located at the customer terminating multiple VPNs. In this case it makes more sense to monitor all the VPNs by querying this CE device than the upstream PE device at the provider's POP. Given the right permissions, ACLs and SNMP communities, a provider using NexusMETER is able to gather data from this CE device as well as the upstream PE one, and can combine that data with data gathered at the remote ends from the relevant PE device in the POP.

### 3.1 Similar Look and Feel

Related reports can be used within the provider to identify the most active VPNs or to group them by site or transport used. And, of course, with appropriate permissions, data can be gathered at any point within the provider's network. This means that the provider can use the same reports to resolve problems with his own service providers.



**Figure 2: Example Customer VPN Monthly Summary Report**

Although perhaps a minor point, the similar format to reports from previous technologies helps the customer compare his new VPN services to his older ones and feels more familiar. Likewise, since the data is presented in both graphical and tabular form, it is easy for trends to be identified. The reports have a common look and feel, whether the time period is daily or monthly and whether the report is a detail on one VPN or site, an aggregate of the total traffic, or a list of top 10 indicators.

### 3.2 statistics from Multiple Sources

NexusMETER can gather, in addition to data from Nortel's MSS (former Passport product line), SNMP data from any device capable of monitoring SNMP data. The SNMP MIBs used are generally standard ones with implementation across many diverse platforms, thus increasing the likelihood that devices at both ends of the VPN can provide identical statistics. The most complex statistic is the delay metric, provided using the RTT MON MIB, which may not be available in all devices but is available in the most common Layer 3 devices used as VPN termination equipment.

### 3.3 Draft MIB Support

Nexus can also support draft MIBs, as it did for the draft-ietf-ppvpn-mpls-vpn and the draft-ietf-l3vpn-rfc2547bis MIBs. These MIBs provide key information and performance metrics for MPLS VPNs which are not readily available from other MIBs that the network elements may also support.

This is unique to Nexus, as network management vendors are unwilling to add support for draft MIBs, except by allowing customers to make their own queries. By contrast, as Nexus realizes the critical importance of such MIBs, and felt that the current drafts had wide enough implementation, they were added to the standard reports and data sources for NexusMETER.

### 3.4 Reports for the NOC and the Customer

NexusMETER is able to provide both up-to-date statistics for a carrier's NOC, using its Raw Data Reporting Client, and customer-ready reports, using its Value-Added Reporting Client. Both systems query the same data and both can be used to identify problems or trends in VPN utilization.

## 4 Bringing it Together

The provision of performance statistics for managers of VPNs is a complex process made even more complex by the wide differences in VPN types and equipment. However, NexusMETER has by far the widest support for relevant network devices and MIBs, and is thus able to provide detailed reports of key VPN metrics. Thus carriers can clearly demonstrate the level of compliance with Service Level Agreements to their customers. Even more importantly, with NexusMETER's Raw Data Reporting Client it is possible for NOC personnel to identify harmful trends in advance and thus rectify situations that would otherwise lead to future SLA violation. The result is that the carrier can maintain revenue and satisfy his customers without the introduction of complex non-scalable probes throughout the network.

The Nexus reports provide information in a style which is familiar to managers who are used to monitoring the services that VPNs replace. This provides a significant benefit to the VPN provider since both his own personnel and those of his customer can quickly recognize the key information. In a similar vein, the ability to combine individual VPN services together to produce a summary report of overall levels makes the job of identifying problem areas simpler.

With Nexus Telecom, the promise of VPNs for richer statistics reported in a unified manner from a variety of different technologies is now a reality. Using NexusMETER, a carrier can be confident of offering VPN services with attractive SLAs without deploying complicated probes for each VPN to gather statistics, and without being tied to offering a single VPN type or a single vendor's equipment. Customers can now easily be provided with the exact reports they need, in a format that they want, from the same data that the provider uses himself to look at the network from his point of view. The result is increased revenue and increased customer satisfaction.

## 5 VPN Reporting Summary within NexusMETER

VPN Feature	IP Devices Support (Generic/Cisco etc.)		Nortel MSS Support (RFC 2764)		Nortel MSS Support (RFC 2547)	
	Raw Data	Value-Added	Raw Data	Value-Added	Raw Data	Value-Added
IP-VPN Policing	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>
	Value-Added	<input checked="" type="checkbox"/>	Value-Added	<input checked="" type="checkbox"/>	Value-Added	<input type="checkbox"/>
IP-VPN Delay	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>
	Value-Added	<input type="checkbox"/>	Value-Added	<input type="checkbox"/>	Value-Added	<input type="checkbox"/>
IP-VPN Utilization	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>
	Value-Added	<input checked="" type="checkbox"/>	Value-Added	<input checked="" type="checkbox"/>	Value-Added	<input type="checkbox"/>
IP-VPN Packet Loss	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>
	Value-Added	<input checked="" type="checkbox"/>	Value-Added	<input checked="" type="checkbox"/>	Value-Added	<input type="checkbox"/>
IP-VPN Throughput	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>
	Value-Added	<input checked="" type="checkbox"/>	Value-Added	<input checked="" type="checkbox"/>	Value-Added	<input type="checkbox"/>
IP-VPN CoS	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>	Raw Data	<input checked="" type="checkbox"/>
	Value-Added	<input checked="" type="checkbox"/>	Value-Added	<input type="checkbox"/>	Value-Added	<input type="checkbox"/>

**NOTE:** Boxes that are not checked indicate that the feature is not currently available.

## 6 Conclusion

The Virtual nature of VPNs allows for great flexibility in deployment and in the type of underlying network transport technology, which is highly attractive to both service providers and customers. However, although VPNs are deployed over networks consisting of a mixture of devices and technologies, customers want unified reports that cover the same metrics — and they want them presented in a way that makes sense to them. For providers, NexusMETER is the ideal way to meet this demand because of its ability to combine data from dissimilar sources into the same form and its ability to get the same meaningful statistics from all types of VPNs.

## 7 About NexusMETER

Nexus Telecom's performance reporting software, NexusMETER, provides a set of modular application tools with a common database that provides carrier-grade performance management functionality for wireless service providers. NexusMETER has two main applications:

### Raw Data Reporting Client

A workstation-based network analysis-reporting tool that provides detailed operational reports on all performance aspects of a wireless data network, saving time and resources for network data population for scheduled and on-demand reporting.

### Value-Added Reporting Client

A client-server performance management application tool used to measure and depict network availability, response times and utilization rates, producing a wide variety of detailed or summary reports on the traffic in your IP network, to prove that you meet or surpass your service level agreements. The SNMP (IP/OE) Base pack module is responsible for populating and processing performance statistics data collected by the SNMP data collectors within the IP network as shown in the diagrams earlier.

Designed for use in combination with the SNMP Base, NexusMETER SNMP Reports provide sophisticated, easy-to-read graphical performance reports for two key areas of Service/Network Management:

- ▶ Performance Management
- ▶ Service Quality

NexusMETER is a flexible, modular multi-domain, multi-vendor OSS performance reporting solution, offering support for FR/ATM networks, next generation IP services and Wireless GPRS/UMTS/GSM. It

assists enterprise and service provider managers to analyze problem areas at various levels of detail, while monitoring and evaluating network usage trends and traffic volumes. Many of the service-based reports are used for Service Level Verification of customer Service Level Agreements. NexusMETER's Raw Data Reporting Client provides support for multi-domain networks within carriers, service providers and large enterprises, thus enabling detailed and flexible network analysis to meet ever-changing business needs cost-effectively.

For detailed technical overviews, please visit our website, [www.nexustelecom.com](http://www.nexustelecom.com) or contact your nearest Nexus Telecom Office.

## 8 About Nexus Telecom

Founded in 1994, Nexus Telecom is a privately-held company with headquarters in Zurich, Switzerland and regional offices in Canada, Chile, South Africa and Pakistan. With over 200 employees, Nexus Telecom is a major OSS/BSS vendor delivering sophisticated state-of-the-art telecom management solutions to 2G, 3G, NGN and VoIP service providers and network operators worldwide.

### **Nexus Telecom - Network and Service Investigation**

Nexus Telecom provides investigation tools and techniques with which telecommunication service and network malfunctions and degradations can quickly be determined and successfully solved. Based on scientific analysis methods, these investigation, troubleshooting and monitoring tools help to unravel the hidden secrets behind often complex and mysterious service malfunctions.

### **Product Portfolio - Full range of investigation tools**

Nexus Telecom offers a wide range of such investigation tools used to effectively study problem cases, to collect and process transaction 'evidence' data, to correlate and combine events, to translate and decrypt transaction details and ultimately, to solve the case and fully restore the respective service quality. Clearly, such tools are indispensable to network operators and service providers who are committed to improving service quality to all their business and residential customers.



**Nexus Telecom  
Zurich**

### **Nexus Telecom - Partners and Customers**

With solutions deployed in over 100 countries, Nexus Telecom's installed customer base spans the globe, assuring service quality and revenue streams for many of the world's best-known telecom operators. For small and large service providers alike, including the world's largest GSM/UMTS network operated by T-Mobile, the highly scalable and modular end-to-end solutions from Nexus Telecom maximize the service provider's competitive edge through excellent ROI, quick and smooth launch of new services, and greatly increased end-customer satisfaction.

Nexus Telecom's fast time-to-market strategy is to gain early in-depth know-how about upcoming network technologies through strong development partnerships with leading network equipment manufacturers such as Nokia Siemens Networks, Nortel and Alcatel Lucent.

©Nexus Telecom, Zurich, Switzerland

This document and all the information contained herein is subject to change without notice and should not be construed as a commitment by Nexus Telecom. Although we believe the contents of this document to be accurate, Nexus Telecom assumes no responsibility for any errors that may occur in this document.

Nexus Telecom, and all Nexus Telecom Logos are trademarks of Nexus Telecom.

All other trademarks are acknowledged and are the property of their respective owners.

---

**Head Office**

**Europe**  
Zurich, Switzerland  
Tel: +41 44 355 6611

**Sales Offices**

**North America**  
Ottawa, Canada  
Tel: +1 613 224 2637

**Central and Latin America**  
Santiago, Chile  
Tel: +562 946 3102

**Africa**  
Centurion, South Africa  
Tel: +27 8 2773 5730

**Middle East**  
Islamabad, Pakistan  
Tel: +92 5 1285 4890

**South East Asia**  
Kuala Lumpur, Malaysia  
Tel: +603 7725 2099