# Troubleshooting Remote Site Networks – Best Practices

*Management and remote site employees expect the same level of network service as the headquarters site. However, when IT staff are faced with limited resources to support remote site networks, often the applications, services and performance at those sites is not as robust as the headquarters site.*

*See how to deliver a high level of network service at remote sites using the best practices outlined in this white paper.*

***Table of contents***



FLUKE networks

## Introduction

The need to establish a presence in strategic areas is forcing businesses to open new branch offices where remote employees expect the same network applications, services and performance as employees located at corporate headquarters. Unfortunately, IT organizations do not have unlimited budgets or headcounts. Therefore in most cases, there are no IT support personnel permanently available at remote locations.

Although server centralization, consolidation and the move towards web-enabled applications have business benefits, optimal productivity can still only be achieved when the same level of services are available in remote sites as in the corporate headquarters. Unfortunately, even the best-planned deployment can potentially leave remote offices and users vulnerable to performance degradation and availability issues. This creates additional challenges for the headquarters IT staff in maintaining remote site performance, availability, security and visibility.

Just as in the headquarters environment, when remote users complain about poor performance, IT staff must be able to determine the root cause of the problem and correct the situation. Remote office network outages and slowdowns are made far more difficult to solve because of the challenges presented by distance, travel time and the need for tools that may not necessarily be available at the remote location. Organizing the necessary tools and dispatching staff to remote locations to troubleshoot problems is both time consuming and expensive.

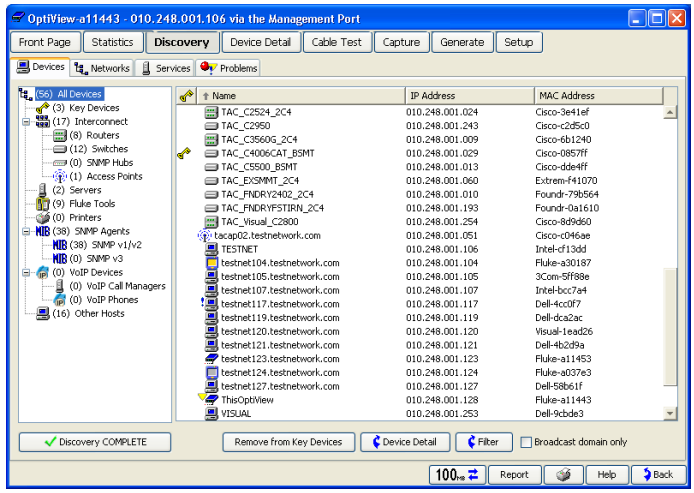
One method of solving these issues is to implement a strategy that spans both the remote site and the corporate headquarters site. With the right information and tools, IT staff are able to understand and resolve issues quickly and efficiently. Adding the appropriate level of visibility, IT staff could even identify remote network degradations before they become significant problems at that remote site. This strategy provides IT staff with the opportunity to take proactive action to eliminate congestion and other problems that could affect remote sites and interfere with operations. Additionally, the ability to enable staff to resolve problems from the headquarters site will avoid the need to dispatch staff and results in timesavings and increased network availability.

## Best practices for remote site troubleshooting

### Network Discovery

Before attempting to troubleshoot a problem at a remote site, IT staff must first know what they are dealing with. This is especially relevant when corporations have made acquisitions or mergers where the remote site equipment configuration and network design is disparate from the headquarters equipment and network design.

Discovery not only means what kind of equipment exists, but who are the users and how are they connected to the network? Discovery must include information on hardware inventory, switch and router configurations and network connectivity.




*Network discovery*

Today, inter switch trunks are widely deployed and now access trunks to the desktop are becoming more common, especially in VoIP deployments which support multiple broadcast domains together with both untagged and tagged traffic. It is therefore necessary to be able to detect all VLANs on a link and measure the traffic distribution across all those VLANs. In addition, traffic statistics on a specific VLAN to allow discovery, generate traffic and capture traffic only on that selected VLAN is essential to identify protocols, top hosts and conversations limited to that particular VLAN.

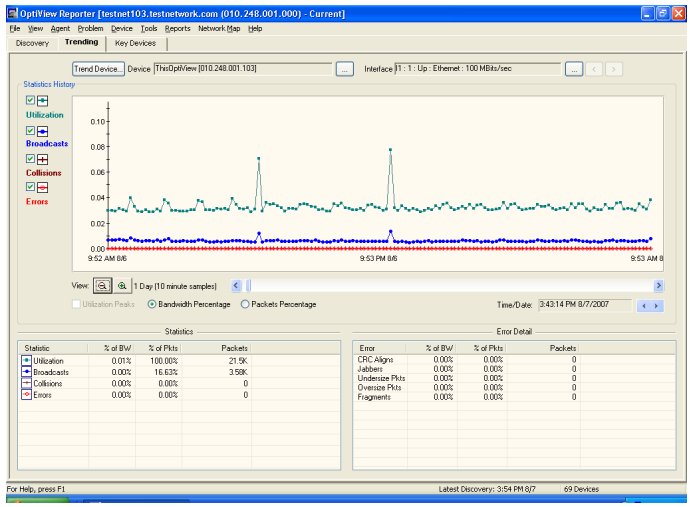
### Baselining

It is also necessary to baseline the existing remote network, not only to create documentation of the current network state but also to understand what "normal" traffic levels are at the remote site. This provides a reference to work from in order to determine abnormal activity and be able to measure against to validate potential problems.

IT staff must evaluate current network performance, including traffic patterns with protocol and application usage, bandwidth utilization, Internet connectivity, and last but not least, potential network vulnerabilities.

To provide this level of information it is necessary to deploy a network analyzer at the remote site, accessible from corporate headquarters to make the process outlined above easier, particularly if the device includes all of the following capabilities:

- Network discovery
- Mapping/documentation capabilities
- SNMP polling to baseline switch and router performance
- Wire speed, hardware packet capture and protocol analysis to measure application response times
- Traffic monitoring to determine which protocols are used on the network
- Host management utilities (telnet/ssh) to view and change infrastructure device configurations




*Device trending*

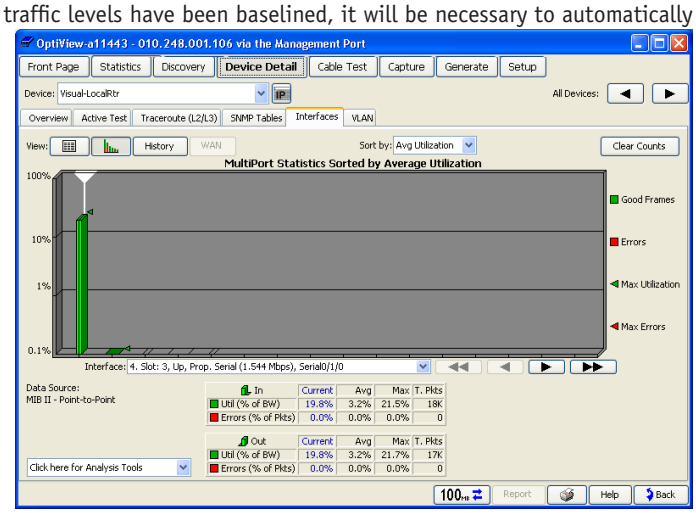
**Next steps**

Network professionals responsible for remote sites have to consider multiple tasks in order to support that site. These can generally be divided into the following:

- Proactive tasks
- Reactive tasks
- Maintenance window tasks

**Proactive Tasks**

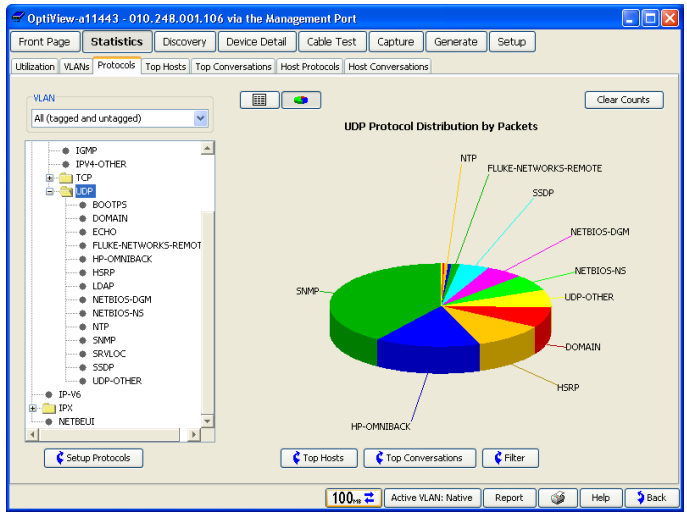
Once up-to-date network configuration diagrams are available and traffic levels have been baselined, it will be necessary to automatically alert headquarters staff when overall traffic levels or individual critical switch port traffic has exceeded what is considered to be 'normal' levels. In order to provide this level of detail, the analyzer deployed at the remote site must be capable of monitoring individual switch ports and WAN interface traffic and provide a method to determine when specific traffic thresholds have been exceeded on those interfaces, either by error rates or utilization rates. This will alert the IT staff to potential network degradations before they become significant problems at that remote site.




*Monitor switch ports*

It is also necessary to monitor the protocols in use, which is especially important for the traffic traversing the WAN link. Are users consuming valuable WAN bandwidth for non-business related applications? It is no longer enough for an analyzer to simply recognize HTTP as a protocol on the network because this could be a valid business application. But now, the analyzer must go deeper into the HTTP packet to determine the payload and identify for example streaming video or audio. Additionally, seemingly minor problems such as incorrect subnet masks, duplicate IP addresses etc. should also be reported.

Then, there is the security aspect that needs to be considered. Peer-to-peer applications such as Skype, BitTorrent, KaZaa, eDonkey and Gnutella, to name but a few, can pose a security threat for the remote site network. Therefore, the analyzer has to be capable of deep packet inspection in order to identify the potentially dangerous applications and also be able to identify the users of those applications.




*Monitor protocols*

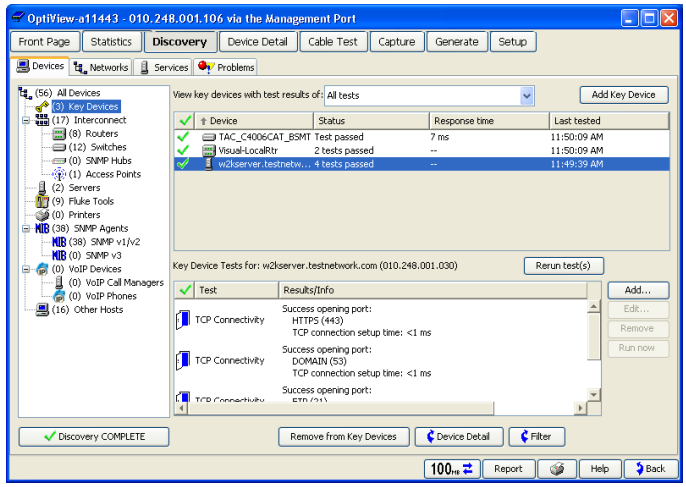
Unauthorized, unprotected rogue wireless access points – how are these discovered if there are no IT staff at the remote site to be able to walk around the site with a wireless network analyzer to find those rogues. Again, this is where in depth discovery from the wired side of the network becomes important – not only does the analyzer need to discover IP addresses but it also needs to discover the associated MAC addresses and decode the manufacturers prefix. Then by sorting the discovery database by MAC address, it is easy to scan the list and look for MAC prefixes that are not normally part of the network – if a suspicious MAC prefix is discovered, IT staff needs to know where that device is connected to the network and so they can shut down the switch port remotely.

**Reactive Tasks**

When remote users complain of a "slow network", the IT staff must have an analyzer at the remote site in order to perform a plethora of different tests. First, it is critical to identify the problem domain to prove who or what is at fault. Secondly, IT staff need to identify the most likely problem domain – is it the network, application, server, or client and subsequently be able to pass-on problems with confidence by providing enough data to avoid finger pointing and to confidently direct the problem to the responsible IT organization, but not necessarily solve an application issue.

To assist in identifying the problem domain, a network services test must be provided to ensure that vital network services are available and operating correctly. These services at a minimum would be DHCP, DNS and 802.1x authentication. The capability of adding additional DNS server addresses is necessary to perform both address to name or name to address resolution tests especially when applications are hosted on multiple servers at the headquarters site that use "round robin" DNS services for load balancing and look-ups.

To validate application connectivity, the analyzer needs to be capable of selecting specific TCP ports from a remote site to a server at the headquarters site and attempt to open those ports to provide details on the connection setup time to ensure that (1) application servers are available (2) there is a communication path and (3) there is an acceptable response time.




*Monitor server connectivity and application response time*

Once basic services and application connectivity are validated, the analyzer must be capable of providing in-depth analysis at the remote site in order to identify the root cause of the problem.

Some problems encountered at remote sites can also be intermittent and recreating those problems is getting more complex and in some cases may be impossible – if you cannot reproduce the problem, would it be safe to say that no problem exists? Unfortunately, not – it is often difficult to determine what happens on the wire, at line rate, when application error messages are received. So, there is a need to provide a capability to capture traffic that is more relevant and analyze the data when time is available, not necessarily when problems occur. In order to solve these problems and to speed troubleshooting, triggers that stop or start capturing when an event is detected both save time and provide more flexibility through:

- Unattended monitoring – capture the traffic whenever the event occurs
- Minimizing number of captures required by ensuring the event is captured the first time and avoid doing random traffic captures that may not contain anything of interest
- Analyzing the captured traffic when time is available, not necessarily when the event occurred.
- Capturing traffic before, after or around the event, and only as much as needed by using capture filters to limit the amount of traffic captured and avoid having to review megabytes of traffic

**Maintenance Window**

During network maintenance times, ensure that the WAN links to the remote sites are capable of supporting the allocated bandwidth. In order to perform this task, an inter-network throughput test should be run between the analyzer at the remote site and a similar analyzer at the headquarters site. The test needs to be performed at various traffic rates and different frame sizes to determine if the WAN link is capable of handling the traffic, to determine packet loss and more importantly, in which direction the packets are being lost. If there are dropped packets, or the link will not support the advertised data rate, the analyzer needs to have features available to diagnose the source of the problem.

## How the OptiView™ Series III Workgroup analyzer makes managing remote sites easier

All the functionality of multiple tools is combined into one device, making remote site management and troubleshooting easier and faster when engineers no longer have to switch from tool to tool to conduct a full array of tests. In addition, network professionals can conduct all the necessary tests at the remote site without ever leaving the headquarters site. Just plug the OptiView analyzer into your network at the remote site and you'll get 24/7 visibility into the network – its like having a "virtual network engineer". And more then one person can view the data, with the OptiView analyzer, network professionals can also work together when some staff members are off-site because data can be shared by launching multiple user interfaces with the analyzer for assisted analysis and collaboration during implementation.


The OptiView analyzer then provides discovery information on network and device problems and identifies protocols in seconds. It also speeds reporting for complete infrastructure documentation. With the OptiView analyzer, network professionals can conduct a complete inventory of all network devices, where they're connected, and which services are running on them. It can do automated mapping, creating maps of the network in its current state. An engineer can plug the OptiView into the network, let it run the discovery, then go through a simple, multi-step process for

printing the map. The OptiView Reporter formats discovery data and exports that data to Microsoft® Visio®, so network professionals get the data in a familiar format which can easily be used when troubleshooting the remote site. Using the OptiView analyzer, network professionals can verify and prove network readiness for network expansions, mergers, consolidations, and upgrades. They can validate and document performance, and verify new configurations to ensure the stability of the network. And they can use the OptiView analyzer to identify VLAN configurations, validate network health, audit switch/router configurations and performance.

Contact Fluke Networks: Phone **800-283-5853** (US/Canada) or **425-446-4519** (other locations). **Email: info@flukenetworks.com**.

## The business case for an integrated network analyzer

The OptiView Series III Integrated Network Analyzer helps network professionals manage IT projects, solve network problems and support IT initiatives, resulting in reduced IT costs and improved user satisfaction. It gives you a clear view of your entire enterprise – providing visibility into every piece of hardware, every application, and every connection on your network.

*No other tool offers this much vision and all-in-one capability to help you:*

- Deploy new technologies and applications.
- Manage and validate infrastructure changes.
- Solve network and application performance issues.
- Secure the network from internal threats.

It shows you where your network stands today and helps you accurately assess its readiness for the changes you need to make now and in the future. Leverage the power of OptiView to give you vision and control of your network. To learn more, visit **www.flukenetworks.com/optiview**

NETWORKSUPERVISION

**Fluke Networks**
P.O. Box 777, Everett, WA USA 98206-0777

**Fluke Networks** operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.


Printed in U.S.A. 2/2008 3276477 A-EN-N Rev A