Opnet IT Guru

Opnet IT Guru Network Planner enable planning and design of multi-technology, multi-vendor networks. Network Planner’s unique ability to model the behavior of the entire network and the supported applications:

• Delivers precise predictions in what-if scenarios to accurately plan for growth, change, technology migration, and new application deployment.
• Supports planning key initiatives such as data center migration, deployment of Unified Communications, VPN, and IPv6 migration.
• Automates capacity planning, survivability analysis, and traffic engineering.
• Provides a platform for validating network changes before deploying to the production network.

Delivering unparalleled value
What –If Analysis

Delivers precise predictions in what-if scenarios to accurately plan for growth, change, technology migration, and new application deployment.

Practical Examples:
- What is the performance of my WAN links if we loose the backup link or I restarted the backup Router?

- What would happen to my main WAN Routers links if we installed a new branch office?

- What is the utilization of my backbone links if I added some more switches? shall I upgrade to 10 G?

- I think we need to upgrade the connection speed link to allow VoIP? Well, I am not sure !!!!

- I think we don’t need 10G investment once we add the new application servers.. Maybe?

-We can safely migrate to IPv6.. I hope !!

NO MORE OF I THINK, I AM SURE !!
Network Capacity

Analyze network capacity usage to identify trends, threshold violations, inefficiencies, a typical behavior, and the timing of future upgrades.
Trend Reporting

Site-Based, Device Pair, and Application Trend Reporting help you quickly identify sites, devices, or even Applications with problematic links within and across the sites in your network.
Flow Analysis

- A primary task of network managers is to pinpoint actual and potential bottlenecks in their network. You need to answer these questions:
  - Is any part of the network currently overutilized?
  - Are there areas in danger of being overutilized?
- Flow Analysis can report the network’s behavior over the entire simulation, over an interval within that period, or it can give you a report based on the average or highest network load.
- The routes used by different traffic flows are calculated according to the modeled behavior of the configured routing protocols in the network.
Analyzing Services & Survivability

- Analyze services when there are no network failures. For example, there is no route between a service and one of its users.
- Analyze services under a particular failure scenario. Such as node or link failures on the services in the network.
- Analyze services under a variety of failure scenarios and determine which services and user groups are most susceptible to failures.

Our Disaster Recovery Plan Goes Something Like This...

HELP! HELP!

DILBERT
By Scott Adams
Survivability Reporting

- Ensures network survivability by predicting the impact of failures without impacting the production network, and proposes design recommendations to guarantee an optimal network.
Network Planner for Security

• IT Guru Network Planner includes security analysis features that let you create and analyze various security scenarios in a network

• A device in the network may have security policies configured that are designed to restrict access to all but authorized users.

• The security analysis feature analyzes the network and provides information to let you know if your security configuration will work correctly using security demands.

• A port scan analysis evaluates the network model and simulates security demands to find all TCP/UDP services permitted and denied between selected zones
Auditing Network with NetDoctor

- Using NetDoctor, you can audit your network periodically to do the following:
  - Locate network problems caused by misconfigurations
  - Identify hidden problems that may affect the network in the future
  - Validate the network configuration against the policies of your organization
  - Send notification of potential problems to other users
  - Customizable suite of 600+ rules of regulatory, organizational, and security policies, including FISMA, Sarbanes-Oxley, HIPAA, PCI, NIST, as well as best practice guidelines by Cisco, NSA, and others
Your organization is adding a new site networks, the IT staff need to test configuration changes in Opnet BEFORE deploying the actual configurations in the production to minimize any possible misconfigurations.

Several steps were taken in NetDoctor:

- Create a scenario of the proposed reconfiguration.
- Run NetDoctor to identify configuration errors related to the proposed network.
- Analyze the NetDoctor report to understand the errors and determine solutions.
- Correct the router configuration errors.
- Run NetDoctor again to test the correction.
Auditing Against Organizational Policies

- You can audit devices to make sure they follow organizational policies.
- The analysis engine compares organizational policy criteria against network device configuration files and reports on policy violations.
- The Organizational Policies rule suite has hundreds of rules for each vendor, a generic rule can be created and customized as well.

The rule detects a violation in organizational policy for the LA-Edge router. The command, “no ip http server” is not in the device configuration file.
NetMapper Module

- NetMapper publishes poster-size network diagrams in a Web Report or in Visio that you can view, download, share, or print.
- Accelerate network troubleshooting with “on demand” insight into network topology and configuration
- Meet regulatory compliance requirements for documenting network topology
- Improve network design by leveraging intelligent network topology and configuration diagrams

Delivering unparalleled value
NetMapper Module

- NetMapper can generate "Out of the Box" diagrams such as:
  - Layer 3
  - Layer 2 and 3
  - STP
  - MPLS
  - IS-IS
  - OSPF
  - VLANs
  - BGP
NetMapper – STP Diagram Example

- Accurate representation of your links, including port numbers
- Easily identify the STP blocked ports.
NetMapper – L2/L3 Diagram Example

- You can easily identify device IP addresses, connectivity, links, port numbers and many others.
Interested in Testing it?

• If you are interested in validating your configurations for example, we can do that in a variety of ways:
  • We can sign an NDA, and you can send us your device running configurations, and we will send you a report.
  • We can run the software on premises so your IT staff can evaluate it.
Questions?