Know Your Network

A New Administrator's Guide to Network Monitoring

Routers

A router is a specialized computer that connects one network to another, directing data packets from a source to the final destination.

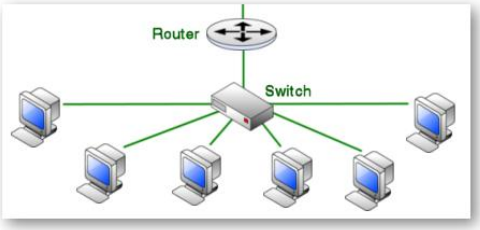
Data from individual computers flow to a switch and are then directed to the router. The router then decides which network to send that data to. That decision is based off of routing protocols stored on the router in a 'routing' or 'configuration table.' This table records the best way to get to and communicate with other routers on other networks.

On your network, there are few devices more important than your routers. When a router is down, your network is down. It cannot communicate to other networks within your organization, and it cannot communicate with the Internet. No email gets through, no instant messages, and no file transfer. If you do not monitor any other device on your network, you should certainly monitor your routers.

Communicating with a Router

Before you can effectively monitor your routers, you must first learn how to communicate with them. This is done by either directly connecting to the router (most routers have HTTP servers on them to aid in configuration) or by using SNMP to have a network monitoring application communicate with your router for you. SNMP (Simple Network Management Protocol) lets you manage and monitor network performance, troubleshoot problems with your network, and better prepare for future network growth.

The SNMP agent on your router can provide information about the device's network configuration and operations, such as the device's network interfaces, routing tables, IP packets sent and received, and IP packets lost. This information, called SNMP objects, is stored in a standard format defined in the Management Information Base (MIB).



Routers are different than switches, in that switches connect groups of computers to a LAN (Local Area Network,) and a router connects that LAN to another LAN, or to the Internet.

Each object in a MIB file has an OID (Object Identifier) associated with it. An OID is a series of numbers separated by dots that represent where on the MIB 'tree' the object is located. The MIB defines the SNMP objects that can be managed and the format for each object.

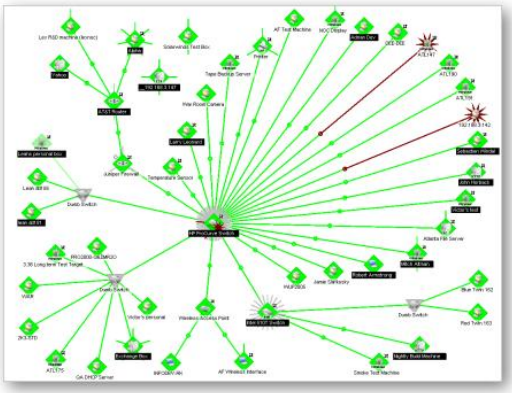
When you configure a router to use SNMP, you assign to it a Read and a Write community string. This acts as a password that allows an application to access the SNMP data on that device. The default community string is usually 'public.' One of the most important things you can do to ensure the security of your routers is to change this community string. It is a good idea to use terms that you will remember, or terms that are standard for that type of device on your network. For example, you may want to assign the string 'gatekeeper' to all of your routers.

For further security, SNMP agent software (on the device) usually lets you specify the IP addresses from which the agent will accept requests.

Monitoring a Router

When using WhatsUp Professional to monitor your network, you begin by discovering the devices or network resources connected to that network. Through WhatsUp Professional, you have the ability to do an SNMP discovery scan that uses the connectivity information stored on your router to find those devices.

To do an SNMP scan, you must configure WhatsUp Professional to use the proper community string to access the router used in the scan. Once your discovery is complete, you can then modify the default settings to better fit the devices you are monitoring. Since monitoring begins with your routers, that is a good place to begin configuring your network.



A network map in WhatsUp Professional

Types of Monitors

In WhatsUp Professional, there are three types of Monitors that you can assign to a device: Passive Monitors, Active Monitors, and Performance Monitors. The differences between these monitors come in the way they gather and report data.

- Active. Active Monitors query network services installed on a device then wait on the response.
- Passive. These monitors 'listen' for specific types of information on a device.
- Performance. These monitors gather data about specific properties on a device.

Generally, there are three things you need to be concerned with when deciding what types of monitors you want to configure for a router.

- Bandwidth Utilization. This Performance monitor collects statistics on the amount of traffic that passes through a given interface on the router. This data is displayed in the Interface Utilization report.
- Ping Availability. This Performance monitor records how often and quickly the device responds to a Ping check. This data is displayed in the Ping Latency and Availability report.
- Interface Health. This Active monitor queries the device for a specific SNMP value on an interface.

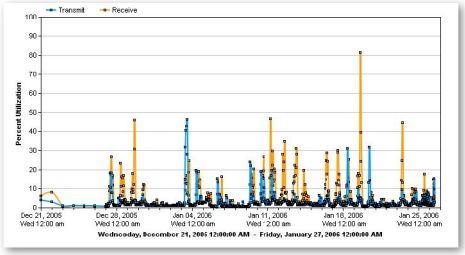
In WhatsUp, specific data connections are called interfaces. In the case of bandwidth monitoring and interface health, you are actually monitoring the traffic going through a specific connection on the router, either the pathway to the internet, or a pathway to another network.

For example: To create an Active monitor that checks on the up status of an interface, enter the following OID:

1.3.6.1.2.1.2.2.1.8 Followed by the instance identifier.

The data reported by these monitors is integral to the health and continued viability of your network. A spike in bandwidth or a drop in ping availability shows that your network is running slow.

When an interface is not responding on your network, then you could have an entire subnet without network connectivity.



Interface Utilization Report

For more information about how to use WhatsUp Professional, refer to the Getting Started Guide, and the application's online help. Both are great resources for configuration and solution information.

IPSWITCH WhatsUp™ Professional