Know Your Network

A New Administrator's Guide to Network Monitoring

Switches and Hubs

Switches and hubs are network devices that link the various nodes, or segments, on a subnetwork or LAN together.

Switches and hubs both allow data to pass from one device to another, but they are different in the way they direct data and how they handle network bandwidth.

Devices connected to a hub have to share the total bandwidth that is available, while devices connected through a switch can use the full bandwidth available on the network. Furthermore, data that passes through a hub is visible to all of the devices connected to the hub, while data that passes through a switch is sent to a specific device.

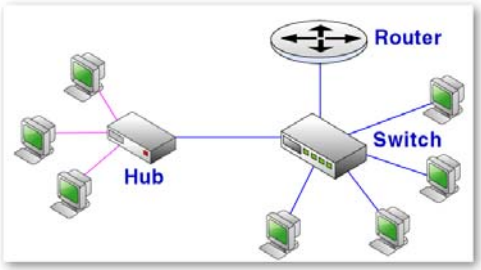
Think of your networks as a highway. A hub would be a four-way stop, where data has to wait until other data passes through before it can pass. A switch would be a series of intersections and on-ramps where all data passes through freely without worrying about what other data is doing.

In many networks, switches have replaced hubs entirely, but there are still occasions where a hub and a switch work together to connect devices with different needs. This is called a mixed network.

Communications

Most switches and many hubs are SNMP (Simple Network Messaging Protocol) enabled, meaning they use SNMP to communicate to other devices on your network. SNMP 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).



Devices connected to a hub share network bandwidth with other devices connected to the hub. Devices connected to the router have use of the full network bandwidth.

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 switch or a hub 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.

Connectivity

Switches and hubs are made up of physical interfaces that your network resources plug into. Each interface has a number assigned to it. It is a good idea to keep a resource map of your switches and hubs and which device is plugged into which interface. In an office environment, switches and hubs reside on server racks and connect to other computers through the office network infrastructure.

Monitoring a Switch/Hub

There are two things you should be concerned with monitoring on your switches and hubs. The first is the health and availability of the interfaces that make up the switch. The second is the amount of bandwidth used by each switch.

In WhatsUp Gold, these are handled by the following performance monitors and active monitors:

- 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. When setting up this monitor, use the following OID: 1.3.6.1.2.1.2.2.1.8 Followed by the instance identifier.

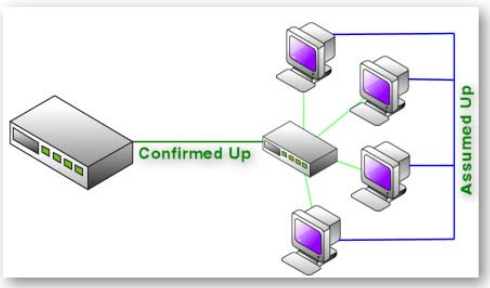
The data reported by these monitors is integral to the health and continued viability of your network. A spike in bandwidth or a drop in ping availability shows that your network is running slow.

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

Using Dependencies

When setting up how you monitor your network and how you are alerted when a device goes down, you should pay close attention to the WhatsUp Gold dependency feature.

This feature allows you to set conditions on your monitoring to only check downstream devices if the switch is up and running. This keeps you from wasting time troubleshooting the devices and lets you focus on the root of the problem. It also limits the number of 'false actions' that are executed.

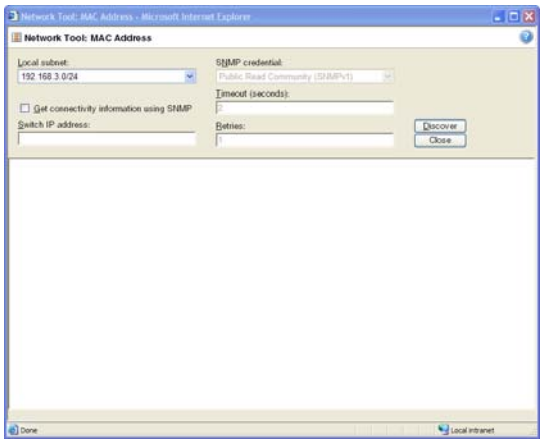


An illustration of up dependencies

You can also set down dependencies that only check upstream devices when a downstream switch or hub is down. This lets you limit the amount of polling traffic on devices that would not normally need to monitor (your connection to your ISP, for example.) So if your main router goes down, the down dependency would then check upstream to see if the problem is caused at the ISP level, or with the main router itself.

Mapping Devices to Interfaces

In WhatsUp Gold, the MAC address tool can tell you the MAC addresses that are present on your network.



The MAC Address tool is found in the web interface

If the switch is SNMP enabled, and you provide the correct read community string, you can get physical connectivity information for the devices on your network. Therefore, if you encounter an IP conflict, you can see which computer is connected to the port that the tool shows is using that IP address. If you have mapped out your interfaces to the offices they are connected to, you can find out exactly where the conflict is.

More Information

For more information about how to use WhatsUp Gold, refer to the User Guide, and the WhatsUp Gold online help. Both are great resources for configuration and solution information.

IPSWITCH WhatsUpGold Standard Edition v.11