

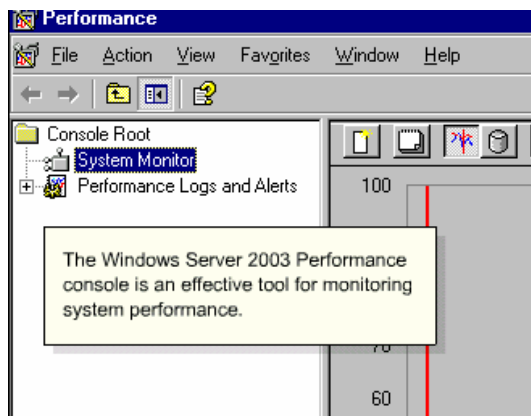
## Monitoring Network Traffic section two

This topic covers the following points:

1. Introducing the Performance console
2. Adding counters to System Monitor
3. Logging and viewing performance data
4. Creating a performance alert

Monitoring the performance of your network infrastructure is essential to ensuring that network resources are available and responsive to user requirements.

By establishing a performance baseline and regularly monitoring performance, you will quickly identify when network services are becoming overloaded or congested.



The Performance console is divided into two parts:

- System Monitor
- Performance Logs and Alerts

System Monitor allows you to view and analyze performance data from your local computer or remote computers on the network, both in real-time and from previously recorded log files.

You use System Monitor to choose specific objects and counters to be analyzed, and the parameters that will be used with these objects. You can also determine the format of the data that will be displayed – graph, histogram, or report view. And you can create HTML pages for viewing data.

Performance Logs and Alerts allow you to set up logging to record performance data in a log file and also set alerts to warn you when performance data goes above or below set limits.

It runs as a background service in Windows Server 2003, collecting data continuously.

### Question

Identify the component parts of the Windows Server 2003 Performance console.

Performance Logs and Alerts, and System Monitor are the components that make up the Windows Server 2003 Performance console.


## Monitoring Network Traffic section two

To use System Monitor to view data from either your local computer or other computers on the network you must have administrative permissions. Alternatively, you must be a member of the Performance Monitor Users or Performance Log Users group on the local computer or in the domain in which the computer is a member.

You can define the types of items you want System Monitor to collect:

- object
- counter
- instance


### object

In System Monitor, a performance object  is a collection of counters associated with a particular application, service, or hardware device. Every time an object performs a task, its corresponding counters are automatically updated.

Some of the most frequently monitored objects are

- Processor
- Memory
- Cache
- Physical Disk
- Server
- Network interface
- Paging File

### counter

A counter is a component within an object.  It signifies the information for a specific aspect of an application, service, or hardware device.

### instance


#### Question

Performance data can be obtained from many components in your computer, while these components are being used.

What type of item do you need to collect to view this data?

You use a performance object to obtain information about a particular application, service, or hardware device on your computer.

### instance

An instance is a single occurrence of multiple performance objects of the same type on a machine. 

If an object has many instances, adding a counter for each instance will allow you to track the statistics of each instance.

#### Question

Performance data can be obtained from many components in your computer, while these components are being used.

What type of item do you need to collect to view this data?

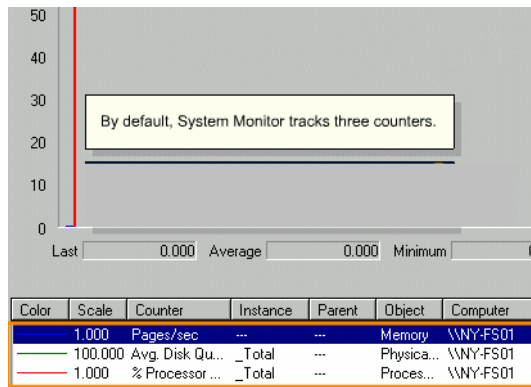
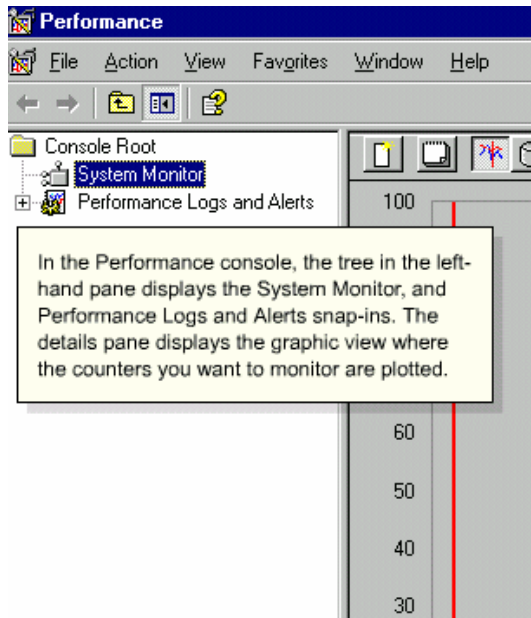
You use a performance object to obtain information about a particular application, service, or hardware device on your computer.

Suppose you are the systems administrator for a global haulage company called Interswift. The company has offices in New York, Seattle, and Chicago, with a European branch in London. You work in the Interswift headquarters in New York.

The company network has been experiencing network connectivity problems, and you are concerned that the network interface card on the New York domain server (NY-FS02) is being overloaded with network traffic. You decide to use System Monitor to investigate.

To open the System Monitor, select **Start - Administrative Tools - Performance**.

## Monitoring Network Traffic section two



The Pages/Sec counter indicates the rate at which pages are read from or written to disk.

This counter is a primary indicator of page faults that cause network delays.

The Avg Disk Queue Length counter is the average number of read and write requests that were queued for a particular disk during a sample interval.

The % Processor Time counter is the percentage of elapsed time that the processor spends to execute a working thread.

This counter will show processor activity by displaying the average percentage of busy time during a sample interval.

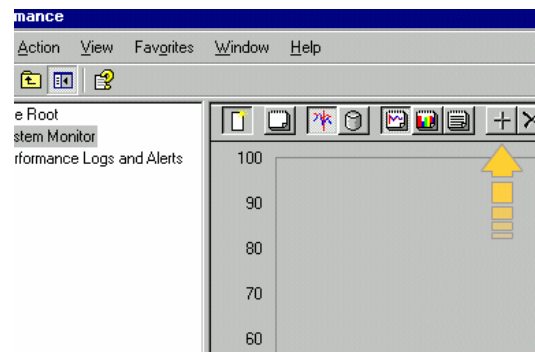
### Question

Suppose you want to use System Monitor to review the rate of page swapping between RAM and disk. Identify the counter you view for this information.

You use the Pages/Sec counter to review the rate of page swapping between RAM and disk.

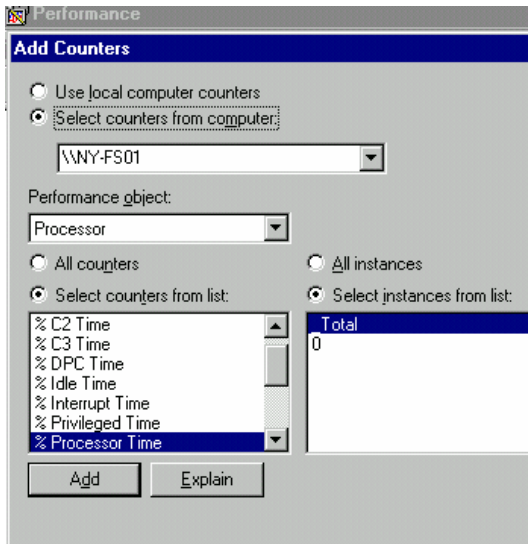
If necessary, you can remove the default counters, and add counters specific to monitoring network performance – namely Bytes Received/sec, Bytes Sent/sec, Bytes Total/sec, and Output Queue Length.

To delete all the counters currently being monitored, you click the **New Counter Set** button on the toolbar.



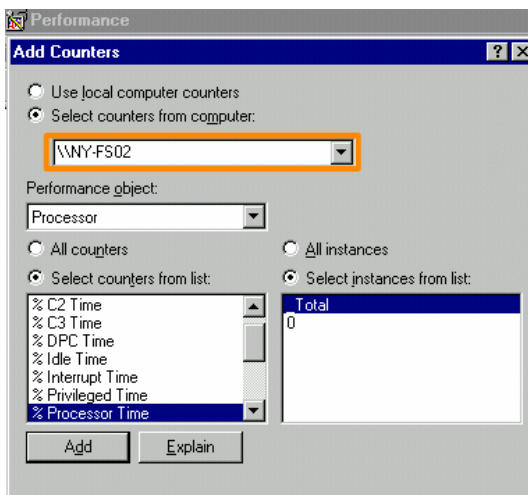
In the Add Counters dialog box, you can select to add counters from the local computer, or from another computer on the network.

## Monitoring Network Traffic section two



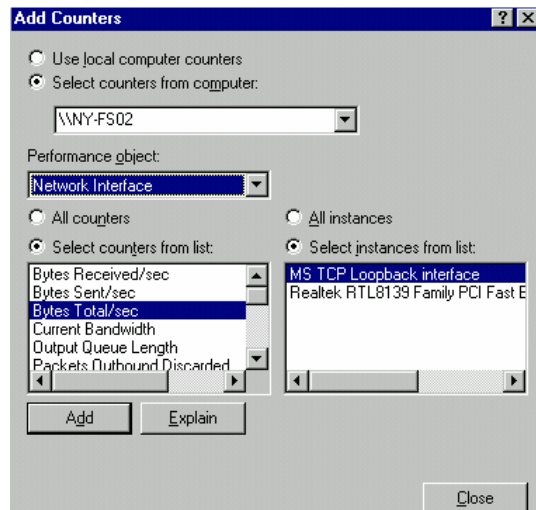
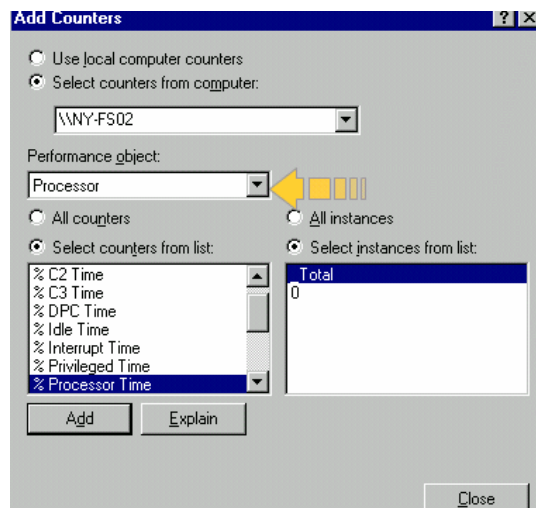
In this case, you want to monitor NY-FS02 on another server, so you ensure the **Select counters from computer** radio button is selected.

In this case you want to monitor NY-FS02, so you type `\\NY-FS02` in the drop-down list box.



You are concerned with monitoring counters from the NY-FS02 network interface card, so you must select the appropriate performance object.

To do this, click the down-pointing arrow in the Performance object drop-down box, and select **Network Interface**.

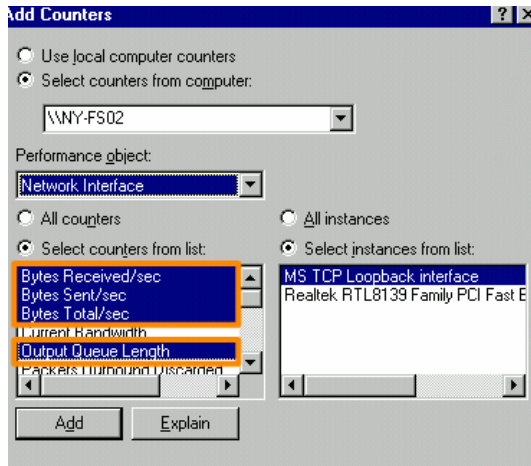


Once you have selected **Network Interface**, the associated counters are displayed in a list.

## Monitoring Network Traffic section two

Then, in the Select counters from list, you select the counters you want to track:

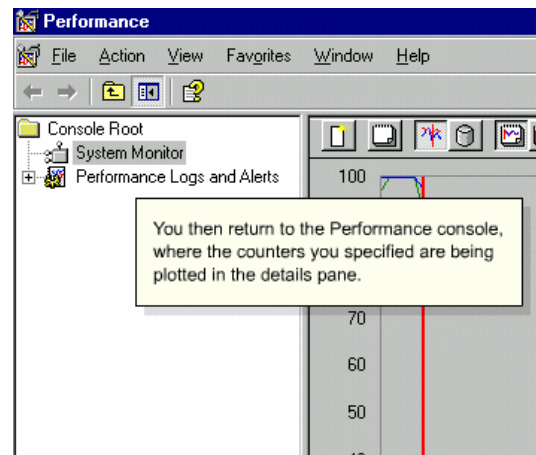
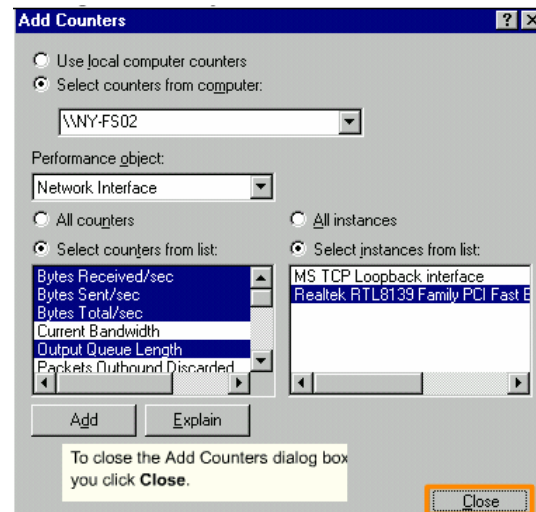
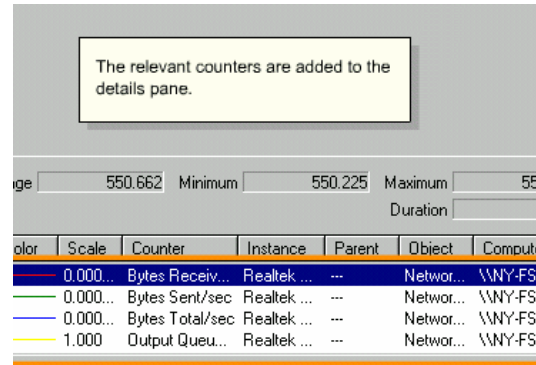
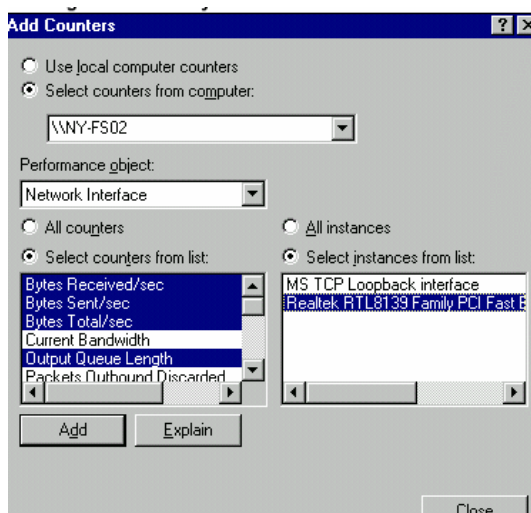
- Bytes Received/sec
- Bytes Sent/sec
- Bytes Total/sec
- Output Queue Length



Next, you need to select the instance to which the counters apply.

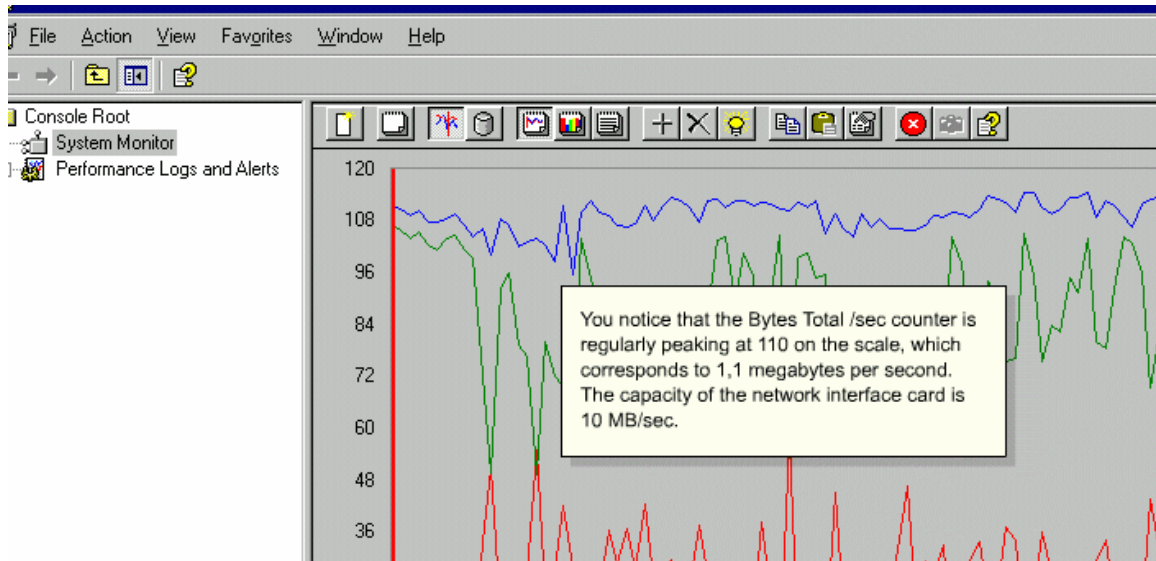
In this case it is the instance of the Realtek RTL8139 Family PCI Fast Ethernet NIC.

Select **Realtek RTL8139 Family PCI Fast Ethernet** in the Select instances from list, and click **Add**.





## Monitoring Network Traffic section two



This indicates that the NIC is working at nearly full capacity, so it would be worthwhile upgrading to a 100 MB card.

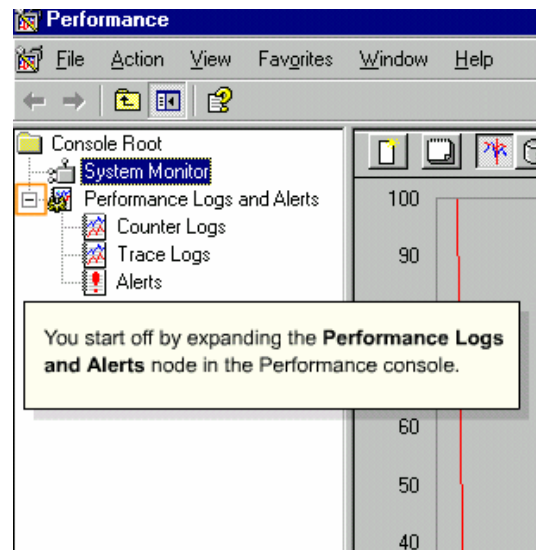
### SkillCheck

You want to investigate the performance of the NIC on NY-FS02 by reviewing the rate at which bytes are sent and received over the NIC. You have accessed the Performance console already.

To review the rate at which bytes are sent and received over the NY-FS02 NIC, you click the **Add** button on the toolbar. You ensure the **Select counters from computer** radio button is selected, and type **NY-FS02** in the drop-down box. You select **Network Interface** from the Performance object drop-down box. The Bytes Total/sec counter is selected, so you select **Realtek RTL8139 Family PCI Fast Ethernet** in the Select instances from list, and you click **Add**.

As the systems administrator for Interswift, you want to establish a baseline for the performance of the network interface card in an Interswift DC, which is NY-FS01.

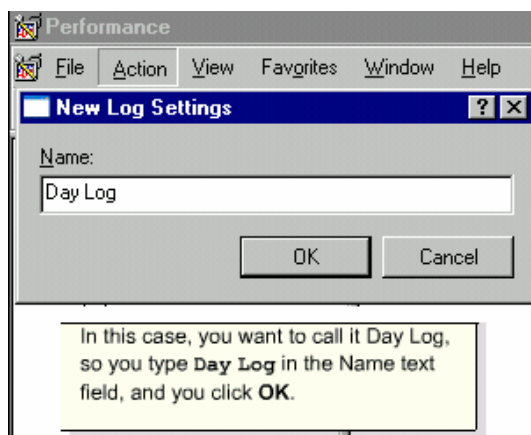
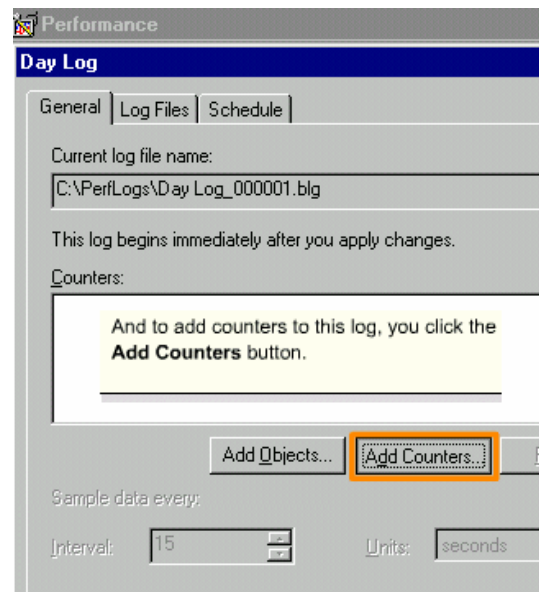
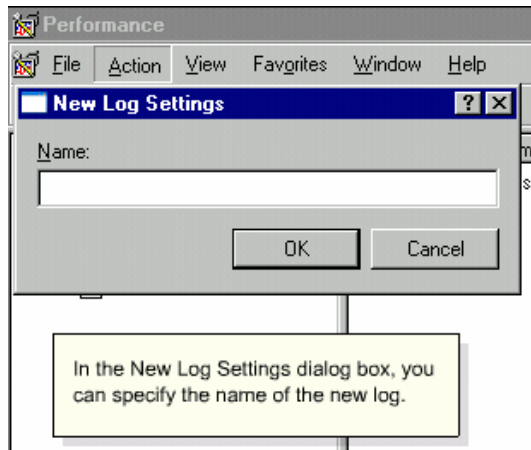
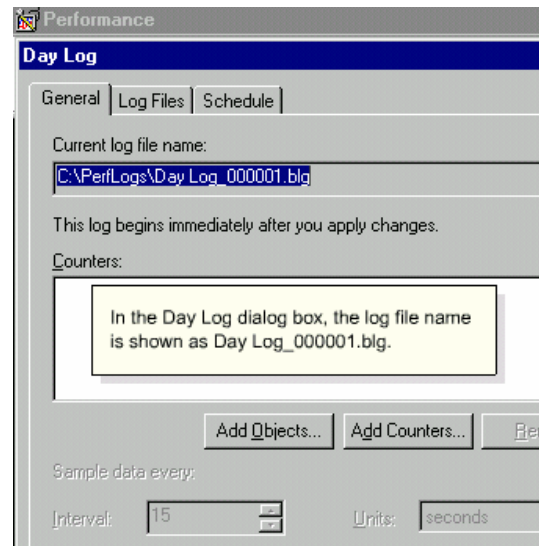
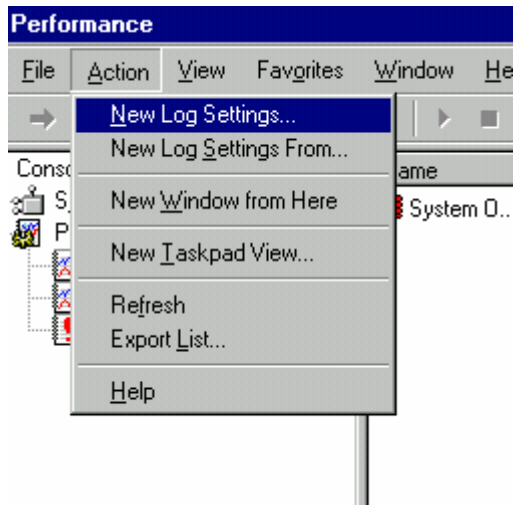
You wish to log the data during a normal day of operation for analysis later. To do this, you must set up a counter log.



Now you can specify a new log.

To do this, select the **Counter Logs** node, and select **Action - New Log Settings**.

## Monitoring Network Traffic section two

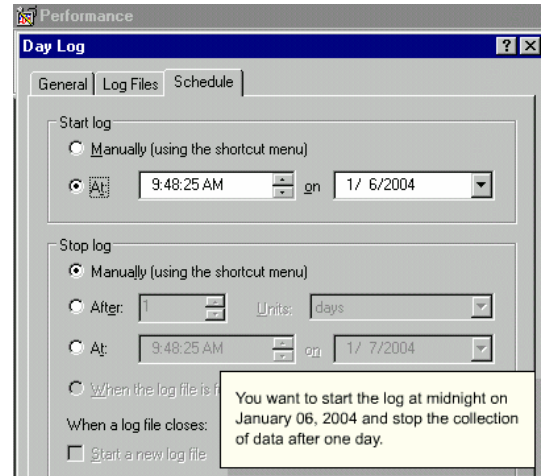
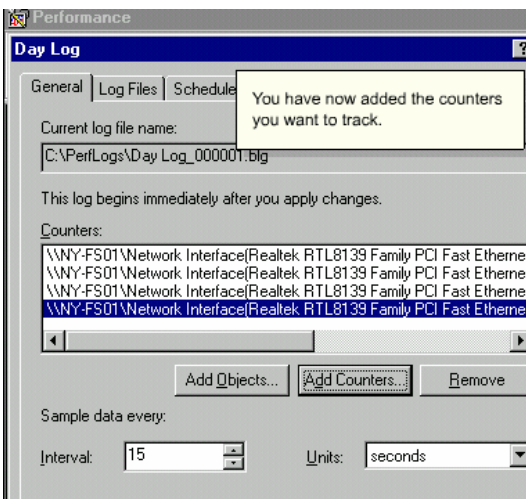
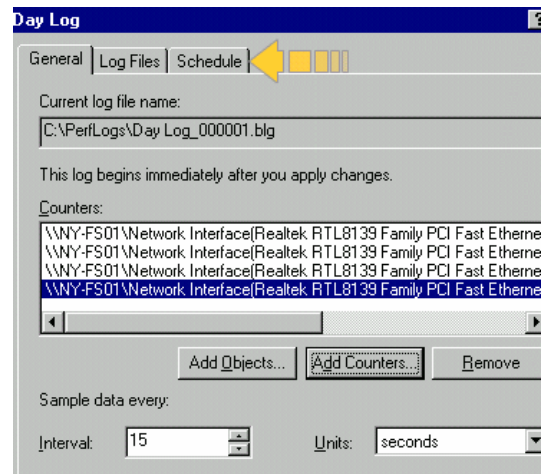
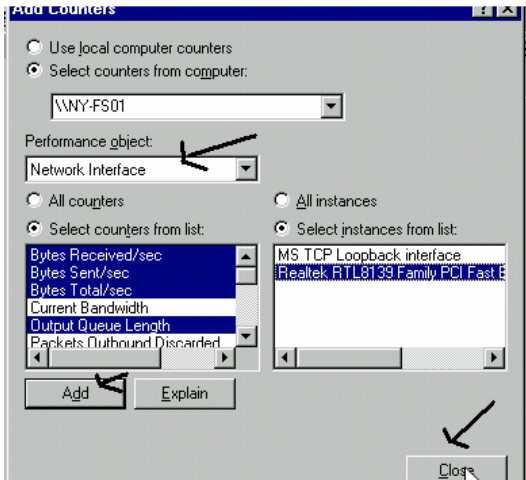


Now you can add the relevant performance object – Network Interface, and the appropriate counters – Bytes Received/sec, Bytes Sent/sec, Bytes Total/sec, and Output Queue Length.

To do this, you carry out the following steps:

- select the correct performance object
- select the correct counters and instance
- add the counters and instance, and confirm the selections

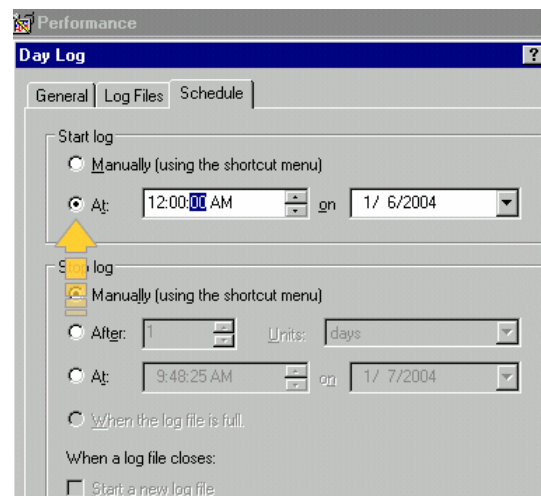
## Monitoring Network Traffic section two



Suppose you want to schedule the start and stop of log file entries.

To do this, you click the **Schedule** tab.

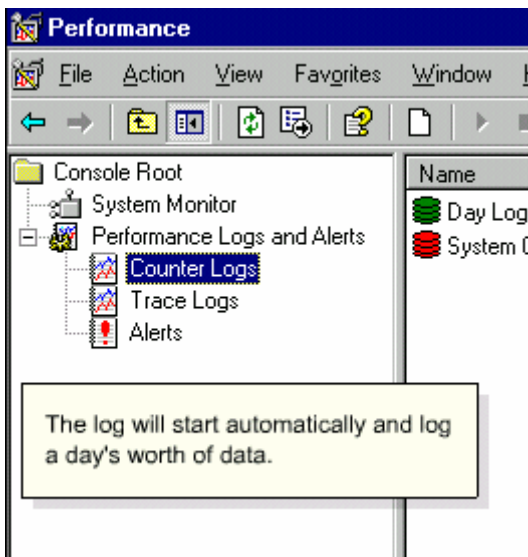
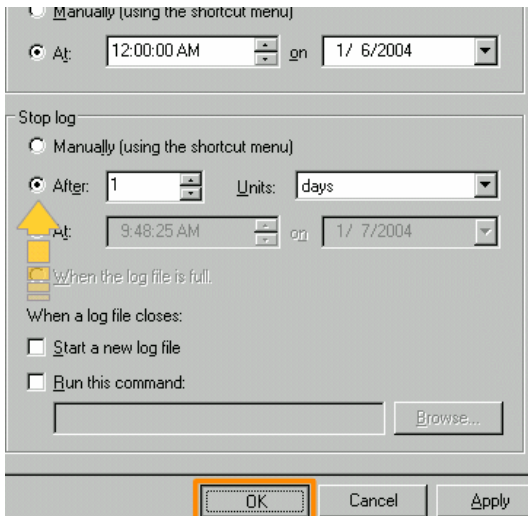
So, in the Start log section of the Schedule tabbed page, you ensure the **Start Log At** radio button is selected, and type 12 : 00 : 00 in the spin box.





## Monitoring Network Traffic section two

In the Stop log section of the Schedule tabbed page, you select the **Stop log After** radio button, accept the default value of 1, and click **OK**.



### SkillCheck

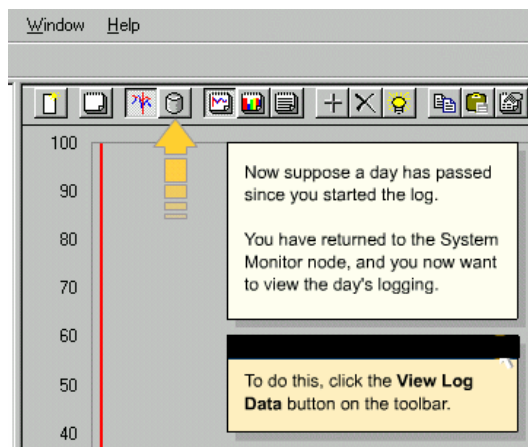
You want to investigate the performance of the NIC on NY-FS02. You wish to log the data during the normal operation on the NY-FS02 server, and have accessed the Performance console to do so.

To create a new log that will collect data from NY-FS02, you access the Performance console, expand the **Performance Logs and Alerts** node, and select the **Counter Logs** node. Then you select **Action - New Log Settings**.

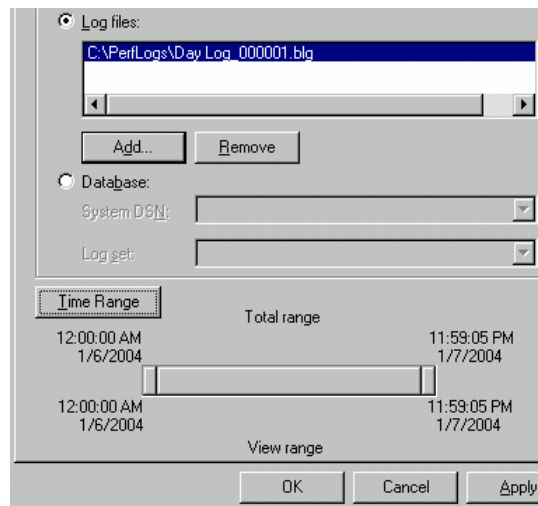
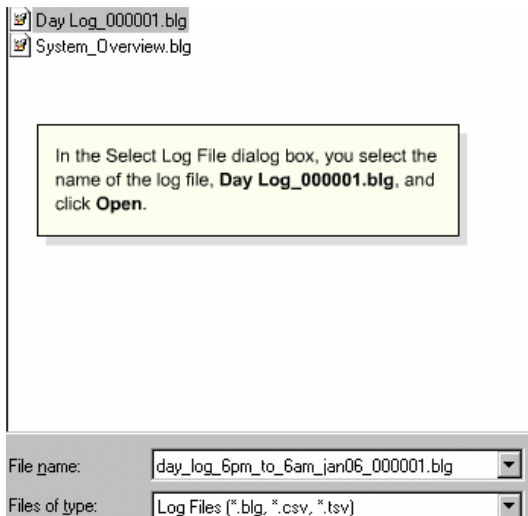
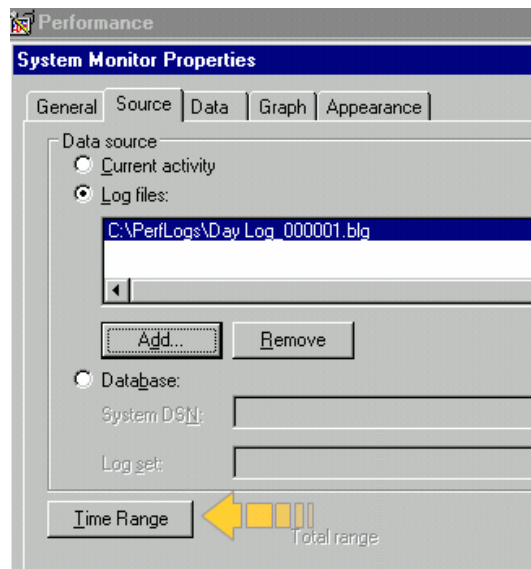
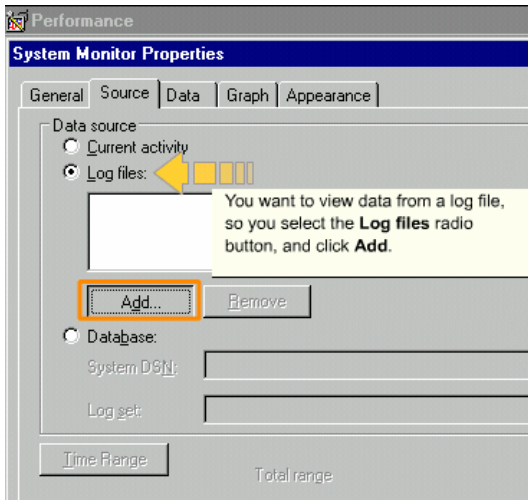
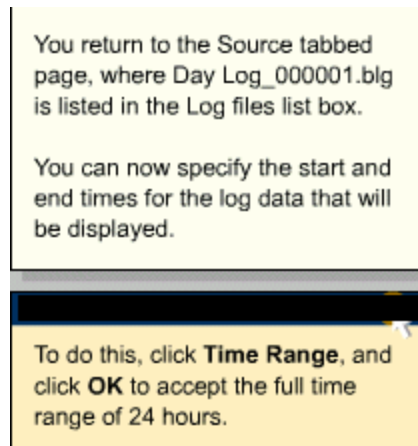
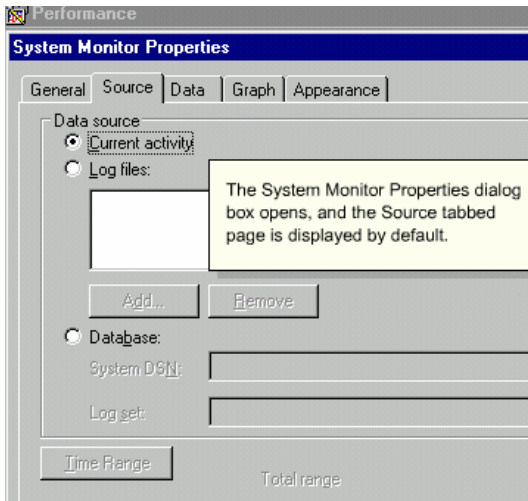
### SkillCheck

You want to investigate the performance of the NIC on NY-FS02. You wish to log the data during the busiest part of the Interswift working day – 08:00 to 13:00. You have created a new log, and added the counter. You have accessed the Schedule tabbed page to set the start and stop times.

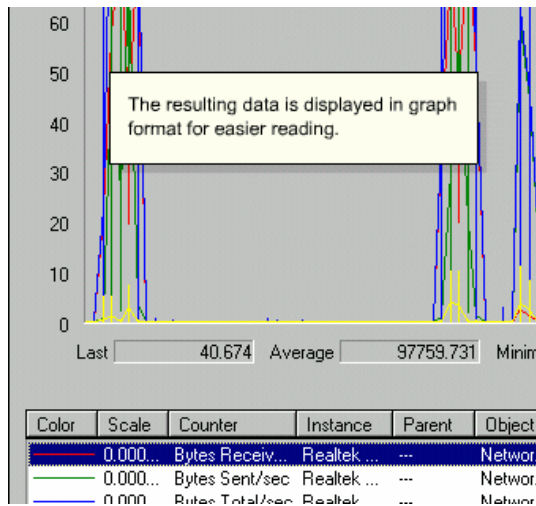
To set the start and stop times for the new log, you ensure the **Start log at** radio button is selected, and type 08:00:00 in the spinbox. You select the **Stop log at** radio button, type 13:00:00 in the spinbox, and then press **Enter**. Finally you click **OK**.



## Monitoring Network Traffic section two



## Monitoring Network Traffic section two



You can also display the data as a Histogram or a Report by clicking the appropriate buttons on the toolbar – **View Histogram**, and **View Report**.

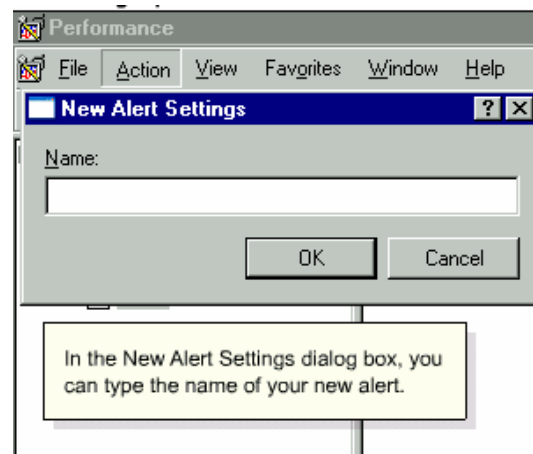
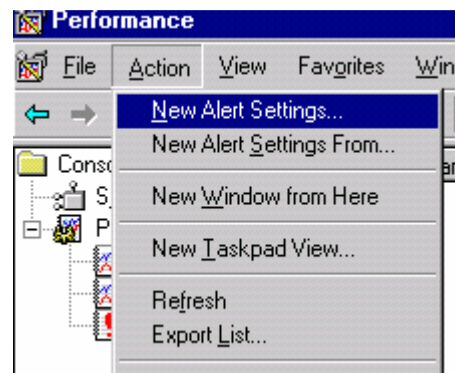
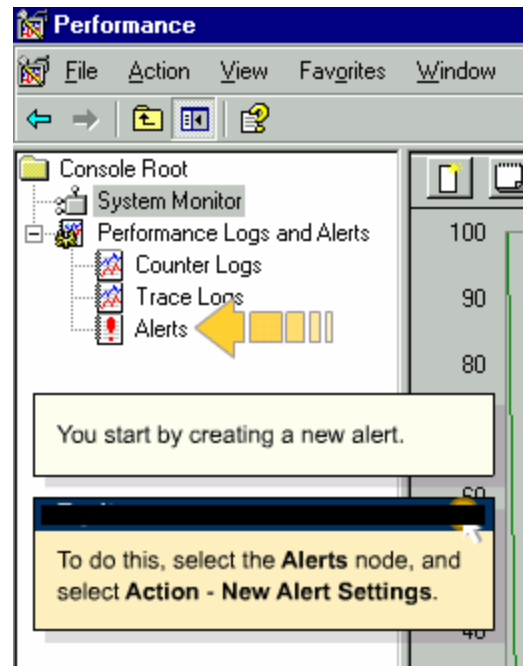
### SkillCheck

You want to investigate the performance of the NIC on NY-FS02 during the lunch time hours of 1:00 PM and 2:00 PM. You have already created a log to do this. It is called Lunchtime Log, and now you want to view this log's data.

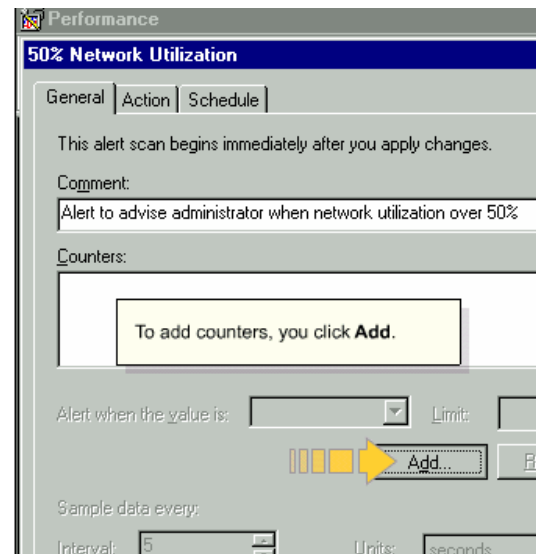
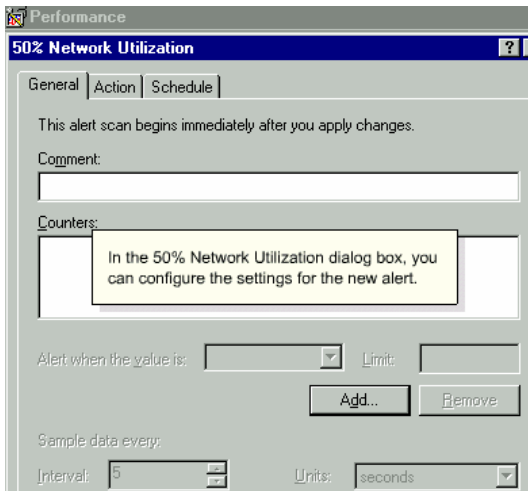
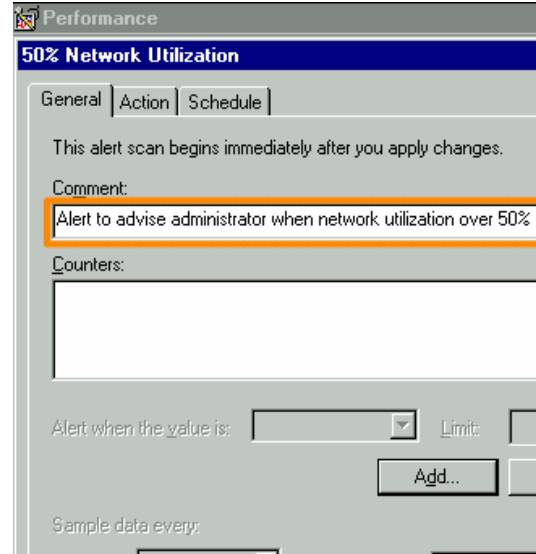
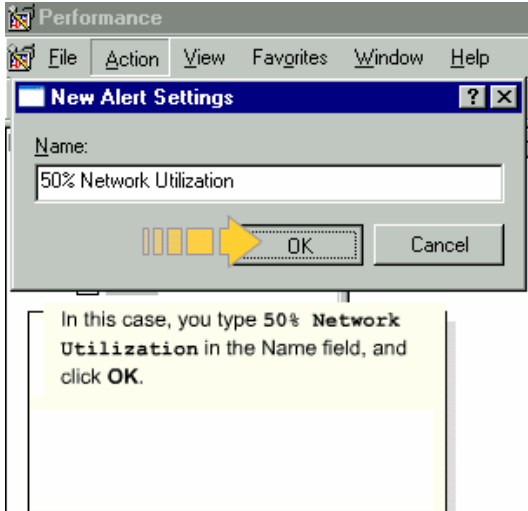
To view the Lunchtime Log file from System Monitor, you click the **View Log Data** button on the toolbar. In the Source tabbed page, you select the **Log files** radio button, and click **Add**. Next, you select **Lunchtime Log\_000001.blg** and click **Open**. Finally, you click **Time Range**, and then click **OK**.

As the systems administrator for Interswift, you are concerned about the performance of the network interface in the New York File and Print server and you want to be alerted when the utilization is over 50 percent.

The server has a 10 Mb Ethernet card, which will have a capacity of 1.25 MB/sec.



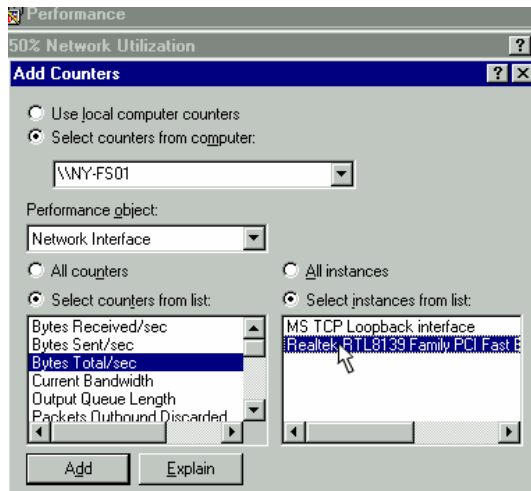
## Monitoring Network Traffic section two



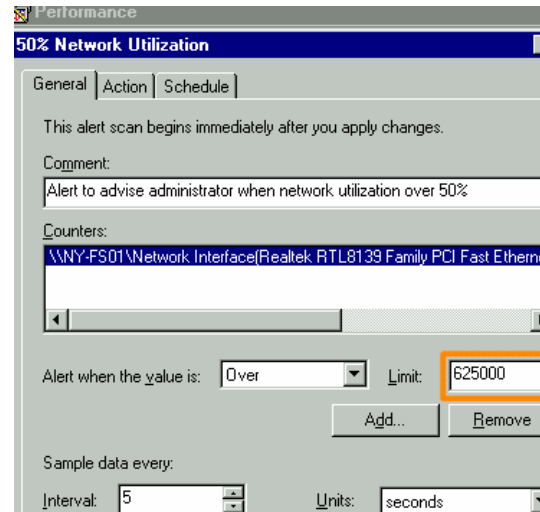
You first want to enter a comment in the Comment field to help you remember the alert. In this case, you type **Alert to advise administrator when network utilization over 50%**.

And in the Add Counters dialog box, you select the **Network Interface** performance object, ensure that the **Bytes Total /sec** counter is selected, and select **Realtek RTL8139 Family PCI Fast Ethernet** as the instance.

## Monitoring Network Traffic section two

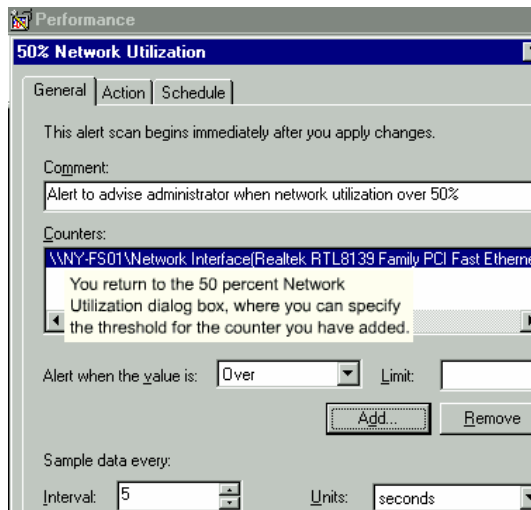


To confirm your selection, you click **Add**, and finally, you click **Close**.

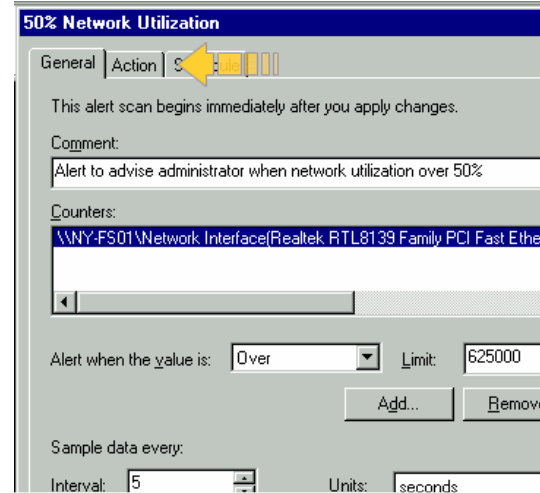


You can now specify the actions to take when the threshold is met.

To do this, select the **Action** tab.



The print server has a 10 MB Ethernet card, with a capacity of 1,25 million bytes per second. You want to be alerted when utilization is over 50 percent, so you type **625000** in the Limit field.

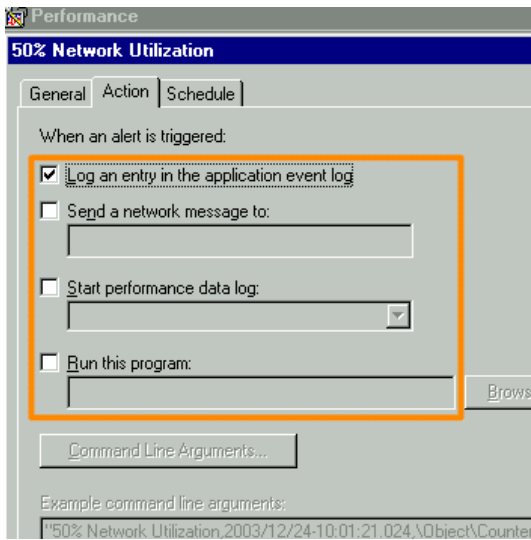


In the Action tabbed page, you can

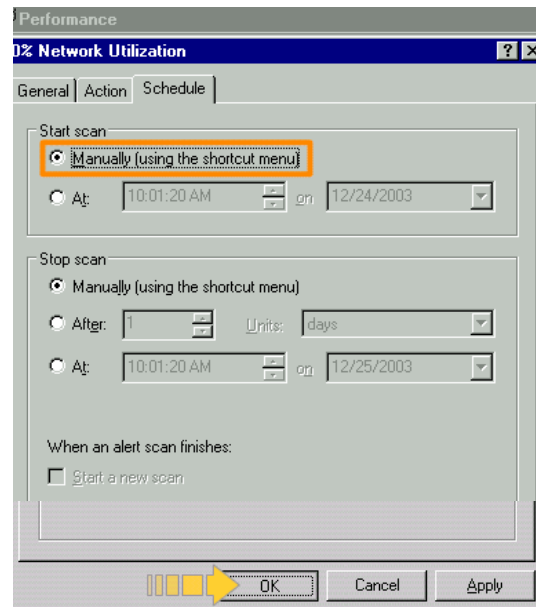
- create an event log entry
- send a network message
- start a performance data log
- run a specified program



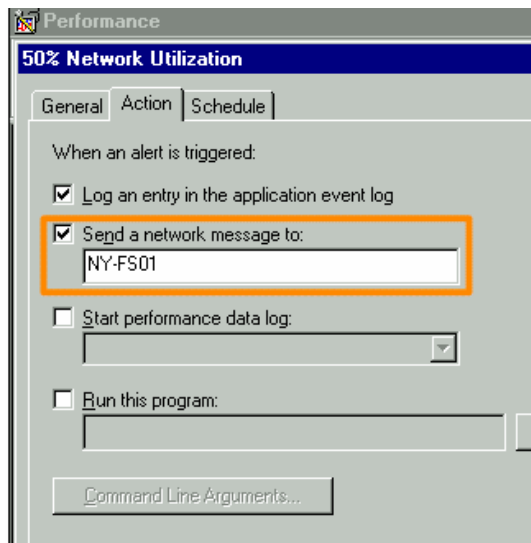
## Monitoring Network Traffic section two



In your case, you want to be alerted by a message when the utilization is over 50 percent, so you select the **Send a network message to** checkbox, and type **NY-FS01** in the text field.



And you click **OK** to close the 50% Network Utilization dialog box.

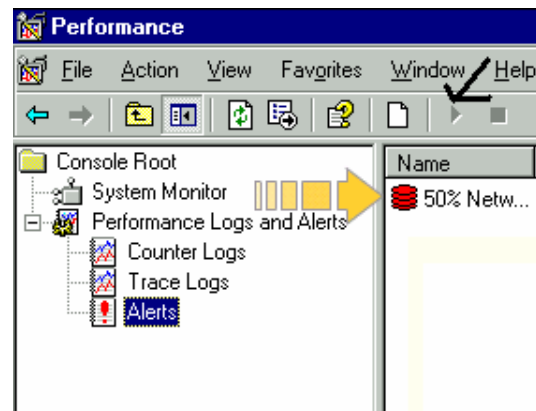


Lastly you can schedule a log scan manually. To do this you click the **Schedule** tab and select the **Manually (using the shortcut menu)** radio button in the Start scan section.

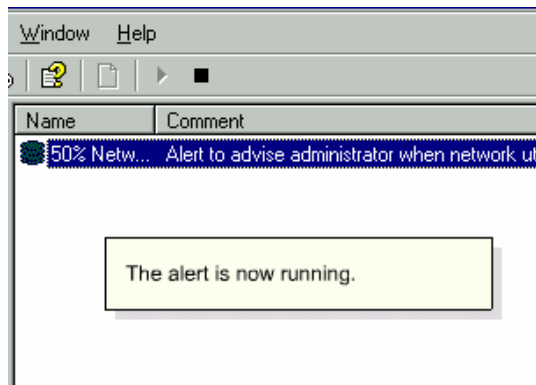
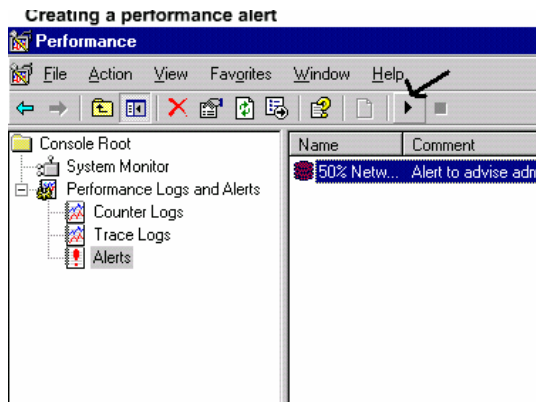
You return to the Performance console and the alert you created is displayed in the details pane.

And now you can start it.

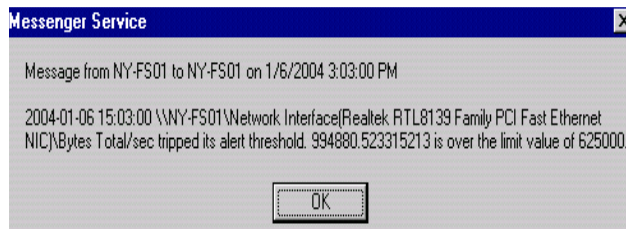
To do this, select **50% Network Utilization** and click the **Forward** icon.



## Monitoring Network Traffic section two



And when the utilization goes over 50 percent, an alert message appears.



To close the message you click OK

### SkillCheck

Perform the steps to begin creating an alert.

To begin creating an alert, you select the **Alerts** node, and select **Action - New Alert Settings**.

### SkillCheck

Suppose that the NY-FS03 server has a 10 MB Ethernet card, which will have a capacity of 1,250,000 bytes/sec. You want to create an alert to be sent to you when utilization runs over 10 percent (125,000).

To create an alert to be sent to you when utilization runs over 10 percent, you ensure that **Over** is selected in Alert when the value is drop-down list box, and type **125000** in the Limit field. Then you click the **Action** tab, select the **Send a Network message to** check box, and type **NY-FS03**. Finally, you click **OK**.

### Question

You are concerned that one of your servers is being overloaded with network traffic. How might you approach analyzing data from this overloaded server?

To analyze data from an overloaded server, you set System Monitor to analyze the relevant counters, and you set an alert to notify you if the capacity of the network interface passes a certain set threshold.

The Windows Server 2003 Performance console is an effective tool for monitoring system performance. It is composed of two parts – System Monitor, and Performance Logs and Alerts.

System Monitor allows you to view and analyze performance data from your local computer or other computers on the network. By default, it tracks three default counters – % Processor Time, Pages/Sec, and Avg Disk Queue Length. If necessary, you can remove these default counters, and add other counters.

## Monitoring Network Traffic section two

Performance Logs and Alerts allow you to monitor system stress and performance over a period of time. To do this, you can create new log files, which collect data over specified start and stop times. And once the log data has been collected, you can view it in one of three forms – graph, histogram, or report.

You can also use Performance Logs and Alerts to create alerts. These alerts can be sent to you when the thresholds you have set have been exceeded.

This topic covers the following points:

1. Exercise overview
2. Task 1: Adding counters to System Monitor
3. Task 2: Creating a performance alert

Exercise
In this exercise, you're required to monitor system performance and create a performance alert.
This involves the following tasks:
<ul style="list-style-type: none"><li>• adding counters to System Monitor</li><li>• creating a performance alert</li></ul>

The Interswift network has been experiencing connectivity problems, and you are concerned that the network interface card on the Interswift PDC (NY-FS01) is being overloaded with network traffic.

This topic covers the following points:

1. Exercise overview
2. Task 1: Adding counters to System Monitor
3. Task 2: Creating a performance alert

Exercise
In this exercise, you're required to monitor system performance and create a performance alert.
This involves the following tasks:
<ul style="list-style-type: none"><li>• adding counters to System Monitor</li><li>• creating a performance alert</li></ul>

The Interswift network has been experiencing connectivity problems, and you are concerned that the network interface card on the Interswift PDC (NY-FS01) is being overloaded with network traffic.

You have logged onto NY-FS01, and have decided to use System Monitor, with added counters, to investigate the problem.

Task 1 of 2
Open the Performance console and add the Bytes Received/sec and Bytes Sent/sec counters to System Monitor. Use the Realtek Fast Ethernet instance.

Steps
1. Select <b>Start - Administrative Tools - Performance</b>
2. Click the <b>New Counter Set</b> button, and click the <b>Add</b> button on the toolbar
3. Click the Performance object down-pointing arrow, and select <b>Network Interface</b>
4. Select <b>Realtek RTL8139 Family PCI Fast Ethernet</b> in the Select instances from list
5. Select <b>Bytes Received/sec</b> in the counters list, and click <b>Add</b>
6. Select <b>Bytes Sent/sec</b> in the counters list, and click <b>Add</b>
7. Click <b>Close</b>

You are concerned about the performance of the network interface card in an application server on your network. You would like to be alerted when the utilization is over 60 percent. The server has a 10 MB Ethernet card, which will have a capacity of 1,250,000 bytes/sec.

## Monitoring Network Traffic section two

### Task 2 of 2



Create an alert that will send a message to NY-FS01 when network utilization/interface capacity exceeds 60 percent (750000). First configure counters. Then set the alert threshold and configure action settings.

Name the alert "60% Network Utilization". The Network Interface instance is Realtek RTL8139 Family PCI Fast Ethernet.

### Steps

1. Expand the **Performance Logs and Alerts** node, select the **Alerts** node, and select **Action - New Alert Settings**
2. Type **60% Network Utilization**, and then click **OK**
3. Click **Add**
4. Click the Performance object down-pointing arrow and select **Network Interface**
5. Select **Realtek RTL8139 Family PCI Fast Ethernet** in the Select instances from list, then click **Add**, and click **Close**
6. Type **750000** in the Limit field
7. Click the **Action** tab
8. Select the **Send a Network message to** checkbox, type **NY-FS01**, and click **OK**