Strategies in Network Capacity Planning and Network Optimization - AB Pound Co.
By Anthony Baron, MCS—United Kingdom

Editor's Note This article is excerpted from "Optimizing Network Traffic," which is part of the Microsoft Press Notes From the Field series that outlines the best system management practices and procedures. For more information on this and other Microsoft Press books, go to http://www.microsoft.com/mspress/.

Client-server applications need a reliable and available communication channel between systems, so it is critical that the network providing this link be correctly sized to meet capacity requirements. This chapter explores network capacity, offering strategies and best practices that show how to assess its current characteristics and potential, and how to look ahead to its changes and limitations as the network grows.

This chapter explains how to use the ideas and methods discussed in Chapters 1 and 2, to assess the state (current and projected) of your network.

On This Page

In Focus

Is this Really Necessary?
Network
AB Pound & Co.'s network consists of two subnets (one on each floor of the building) connected by a backbone.

Challenge
To gather information on network traffic, array it meaningfully, assess it, and use it to plan for a network that can handle normal capacity effectively.

Solution
Categorize traffic (background vs. transactional), discover its patterns as they relate to network use, and use an understanding of general and specific aspects to assess capacity requirements.

What You'll Find In This Chapter

• A discussion on understanding network capacity.
• Ways to assess the sorts of traffic that are moving through your network.
• Methods for gauging the relative predictability of different traffic types.
• An introduction of Network Monitor, a tool you can use for capacity planning.

Is this Really Necessary?
Network planning can be compared to designing a town's road system. In both tasks, you need to understand who is using which routes, how large batches of traffic are (and can be), where journeys start, where they stop, and how all of these things vary over time. If a road system doesn't have enough lanes, traffic jams up and people get delayed and testy; if each road has 20 lanes, you can stop worrying about traffic jams and start worrying about bankruptcy or about the possibility that the mere presence of all those extra lanes may encourage more traffic, ultimately causing problems for smaller roads connected to the big ones. If you under-size the
network, things slow down and eventually stop. People get delayed and unhappy. If you over-
size it, you waste money and invite problems further up the network.
Proper network capacity planning (like road planning) starts with careful capacity measurement.
You need to monitor and assess the number and type of vehicles (whether cars or packets)
using the system.

**Are There Risks of Doing It?**
It is part of the rich texture of life that even doing the right thing can have associated risks.
When you undertake network capacity planning you need to be confident that your results are
correct and reliable. If, for instance, you announce that a network has ten times the capacity it
will ever need, you invite users to load anything they want onto the wire.

Some key risks:

**Getting the figures wrong.** A simple thing such as inaccurately adding up a row of numbers
can be expensive if it impels you to upgrade unnecessarily from a 64-K line to a T1.

**Spending too much time trying to predict the unpredictable.** Sometimes the nature of
your business is simply unpredictable. If this is true, it can often cost you more to make
misguided attempts at scientific quantification than to guesstimate usage, monitor the network,
and tinker.

**Are There Risks of Not Doing It?**
Of course. The network is a critical conduit—if it stops working, the enterprise often stops
working as well. It is far better to anticipate problems than simply to encounter them.

Some key risks:

**Wasting Time.** Not all problems can be solved through capacity analysis. You don’t want to
waste time looking in the wrong place for a solution, and you may not even know when you
don’t understand which issues are relevant to which factors.

**Lost Productivity or Opportunity.** Many businesses, particularly in the securities industry,
rely on near instantaneous transaction completion. Delays can be expensive.

---

**Approach**
First off, you have to find and examine network traffic. There are two basic types:

**Background traffic.** This is a by-product of the infrastructure. For example: when you map a
drive to a network share, the keep-alive packets between PC and server are background traffic.

**Transactional/functional traffic.** This is generated when a task is performed. For example: a
bank teller enters a deposit for a customer.

There are several ways to categorize network traffic. As you discern types based on other
criteria, you need to know if they are background or transactional so that you can understand
their frequency and nature.

**The Daily Task List**
Another category of traffic contains high-level tasks that people perform daily as part of their
job. These vary from company to company of course, but to get a feel for the types here is an
example: a stock clerk in the Electronics department of the AB Pound & Co. The clerk’s high-
level objective is to ensure that the department holds enough stock to meet its sales objectives.
To accomplish this, he performs these tasks on a typical day:
• Logs on
• Reads e-mail
• Checks task list
• Reviews stock level
• Places stock orders
• Pays suppliers
• Produces standard letters to inform customers that orders are in.
• Reads e-mail
• Logs off

An analysis of this traffic would also look at when tasks are completed during a typical day.

**Figure 3.1: Daily tasks that create network traffic-time distribution.**

![Figure 3.1](image)

Figure 3.1 profiles one type of user. Now all you have to do is repeat the process for each type of user so that you create a comprehensive set of profiles. AB Pound & Co., for example, has:

- Sales assistants
- Managers
- Stock clerks
- Secretaries
- Human resources workers
- Warehouse personnel
- Maintenance

Once you create a profile for each role, scale them up to the numbers of workers in each role.

### AB Pound & Co. user profiles and quantities— in general.

<table>
<thead>
<tr>
<th>Role</th>
<th>Average Net Traffic p/hour</th>
<th>Total Number of Users</th>
<th>Average Network per Hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales Assistants</td>
<td>700 K</td>
<td>420</td>
<td>294 Mb</td>
</tr>
<tr>
<td>Managers</td>
<td>60 K</td>
<td>40</td>
<td>2.4 Mb</td>
</tr>
<tr>
<td>Stock Clerks</td>
<td>6 Mb</td>
<td>26</td>
<td>156 Mb</td>
</tr>
<tr>
<td>Secretarial</td>
<td>2 Mb</td>
<td>8</td>
<td>16 Mb</td>
</tr>
<tr>
<td>Human Resources</td>
<td>4 Mb</td>
<td>6</td>
<td>24 Mb</td>
</tr>
<tr>
<td>Warehouse Personnel</td>
<td>400 K</td>
<td>30</td>
<td>12 Mb</td>
</tr>
<tr>
<td>Maintenance</td>
<td>20 K</td>
<td>20</td>
<td>400 K</td>
</tr>
</tbody>
</table>
This helps you see the average load on the network as a whole, which is important, but you also need to understand how potential traffic flow relates to the location of users, lines, and servers.

It so happens that AB Pound & Co. has two floors, each with a network, and a backbone that runs between them. Now the table can be rewritten this way:

**AB Pound & Co. user profiles and quantities—by floor.**

<table>
<thead>
<tr>
<th>Floor</th>
<th>Role</th>
<th>Average Net Traffic p/hour</th>
<th>Total Number of Users</th>
<th>Average Network per Hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>Sales Assistants</td>
<td>700 K</td>
<td>300</td>
<td>210 Mb</td>
</tr>
<tr>
<td></td>
<td>Managers</td>
<td>60 K</td>
<td>30</td>
<td>1.8 Mb</td>
</tr>
<tr>
<td></td>
<td>Stock Clerks</td>
<td>6 Mb</td>
<td>16</td>
<td>96 Mb</td>
</tr>
<tr>
<td></td>
<td>Secretarial</td>
<td>2 Mb</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Human Resources</td>
<td>4 Mb</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Warehouse Personnel</td>
<td>400 K</td>
<td>30</td>
<td>12 Mb</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td>20 K</td>
<td>20</td>
<td>400 K</td>
</tr>
<tr>
<td></td>
<td><strong>TOTAL Floor 1 Net</strong></td>
<td></td>
<td></td>
<td><strong>320.2 Mb/hour</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>89K/sec</strong></td>
</tr>
<tr>
<td>Two</td>
<td>Sales Assistants</td>
<td>700 K</td>
<td>120</td>
<td>84 Mb</td>
</tr>
<tr>
<td></td>
<td>Managers</td>
<td>60 K</td>
<td>10</td>
<td>600 K</td>
</tr>
<tr>
<td></td>
<td>Stock Clerks</td>
<td>6 Mb</td>
<td>10</td>
<td>60 Mb</td>
</tr>
<tr>
<td></td>
<td>Secretarial</td>
<td>2 Mb</td>
<td>8</td>
<td>16 Mb</td>
</tr>
<tr>
<td></td>
<td>Human Resources</td>
<td>4 Mb</td>
<td>6</td>
<td>24 Mb</td>
</tr>
<tr>
<td></td>
<td>Warehouse Personnel</td>
<td>400 K</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Maintenance</td>
<td>20 K</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td><strong>TOTAL Floor 2 Net</strong></td>
<td></td>
<td></td>
<td><strong>184.6 Mb/hour</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>52K/sec</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Backbone</strong></td>
<td></td>
<td></td>
<td><strong>504.8 Mb/hour</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Server Room</strong></td>
<td></td>
<td></td>
<td><strong>140 K/sec</strong></td>
</tr>
</tbody>
</table>

This gives a good idea of average network load an hour for each floor. The next question is: when does traffic flow throughout the day? Does it happen at the same time each day or does it vary throughout the day? Throughout the week?
To derive this information, you need to complete the above tables on an hourly basis each day of the week. This can be a huge undertaking and before you get started you should know that, unfortunately, your results may not reflect reality. Very few companies have consistent identifiable hourly traffic patterns that vary in any meaningful way. Not surprisingly, very few companies take the time to take a complete hourly-traffic profile.

It may be useful, however, to take a look at the couple hours in the morning when most people arrive (if this is relevant) and to sample around to see if you can identify any other peaks or valleys in normal usage.

AB Pound & Co., for instance, found a surge on Monday mornings as people came in to shop after reading about sales in the Sunday newspaper. Although traffic often surges in networks on Mondays (particularly after extended weekends) the results in this case proved insignificant in the big picture. This is to say that the increases were neither frequent nor large enough to justify design changes or expensive implementation. The opening salvos on major sale days also showed measurably increased loading, but these figures, too, failed to warrant expansion. Once, a popular local mall experienced problems, and as a result many shoppers came to the more dependable venue of AB Pound & Co., but this, too, was (an unfortunate) anomaly warranting no design accommodation.

If you have a feel for the rhythms of your business you can make intelligent guesses about this kind of thing.

**Peak Workload Modeling**

An alternative approach is to identify the peak days for each role in each department, measure the traffic, and tabulate it. If you use these figures for capacity planning, the network should then be able to cope with peak traffic in all departments simultaneously. This may be too much capability, depending on the nature of the peaks you observe. Furthermore, actual figures may show that peaks seldom overlap so there is no need to plan for them doing so. AB Pound & Co, for instance, found that:

- Sales assistants are busiest on Saturdays, when they make the most sales and take the most orders.
- Stock clerks are busiest on Mondays, when they place orders with suppliers.
- The warehouse is busiest on Wednesdays, when they take the most deliveries from suppliers.
- Human Resources is busiest at the end of the month, when they pay employees.
- Other roles demonstrate no identifiable peaks.

**AB Pound & Co. user profiles and quantities—adjusted totals.**

<table>
<thead>
<tr>
<th>Floor</th>
<th>Role</th>
<th>Average Net Traffic p/hour</th>
<th>Total Number of Users</th>
<th>Average Network per Hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>One</td>
<td>Sales assistants (Saturday)</td>
<td>1Mb</td>
<td>300</td>
<td>300 Mb</td>
</tr>
<tr>
<td></td>
<td>Managers</td>
<td>60 K</td>
<td>30</td>
<td>1.8 Mb</td>
</tr>
<tr>
<td></td>
<td>Stock clerks (Monday)</td>
<td>10 Mb</td>
<td>16</td>
<td>160 Mb</td>
</tr>
<tr>
<td></td>
<td>Secretarial</td>
<td>2 Mb</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Human Resources (End of Month)</td>
<td>15 Mb</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Floor</td>
<td>Role</td>
<td>Average Net Traffic p/hour</td>
<td>Total Number of Users</td>
<td>Average Network per Hour</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------</td>
<td>----------------------------</td>
<td>-----------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Warehouse</td>
<td>(Wednesday)</td>
<td>800 K</td>
<td>30</td>
<td>24 Mb</td>
</tr>
<tr>
<td>Maintenance</td>
<td></td>
<td>20 K</td>
<td>20</td>
<td>400 K</td>
</tr>
<tr>
<td><strong>TOTAL Floor 1 Net</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>320.2Mb</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>p/hour</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>89k p/sec</strong></td>
</tr>
<tr>
<td><strong>Two</strong></td>
<td>Sales Assistants</td>
<td>1 Mb</td>
<td>120</td>
<td>120 Mb</td>
</tr>
<tr>
<td></td>
<td>Managers</td>
<td>60 K</td>
<td>10</td>
<td>600 K</td>
</tr>
<tr>
<td></td>
<td>Stock Clerks</td>
<td>10 Mb</td>
<td>10</td>
<td>100 Mb</td>
</tr>
<tr>
<td>Stock Clerks</td>
<td>(Monday)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secretarial</td>
<td>2 Mb</td>
<td>8</td>
<td>16 Mb</td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td>(End of month)</td>
<td>15 Mb</td>
<td>6</td>
<td>45 Mb</td>
</tr>
<tr>
<td>Warehouse</td>
<td>(Wednesday)</td>
<td>800 K</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Maintenance</td>
<td>20 K</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL Floor 2 Net</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>184.6 Mb/hour</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>52 K/sec</strong></td>
</tr>
<tr>
<td><strong>Backbone</strong></td>
<td>Server Room</td>
<td></td>
<td></td>
<td><strong>504.8 Mb/hour</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>140 K/sec</strong></td>
</tr>
</tbody>
</table>

**Map Tasks to Topology**

The next step is to look at the physical IT infrastructure, including the network topology, to get an understanding of where the servers are in relation to the clients that use them. In short: how the network is constructed.

Things begin to get difficult along about now. You know who works in the company, where they are, what they do, and when they do it. You need to map this information onto the network's physical topology so that you can work out which task causes which traffic and how much of the total is background traffic.

The only guarantee is that whatever you work out is at best an approximation and is at worst wrong, so you need to identify and allow for variables that can affect the accuracy of your calculation.

**Map Background Traffic**

You have to map background traffic (keep-alive packets, replication, etc.) to topology, too. First, identify all existing network services, list them, and identify the locations that use them. Cover at least:

**Background traffic types.**
<table>
<thead>
<tr>
<th>Traffic type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Traffic generated during IP address acquisition, renewal, and release.</td>
</tr>
<tr>
<td>WINS</td>
<td>Traffic generated during NetBIOS name registration, resolution, renewal, and release.</td>
</tr>
<tr>
<td>Logon validation</td>
<td>Traffic generated by a user logging on to the network and being validated by a domain controller.</td>
</tr>
<tr>
<td>Browser</td>
<td>Traffic generated by a client registering itself as a possible provider of network resources, retrieving a list of backup browsers, a list of servers on the network, and a list of resources on a server.</td>
</tr>
<tr>
<td>File session</td>
<td>Traffic generated when two computers set up a session.</td>
</tr>
<tr>
<td>Domain Name System</td>
<td>Traffic generated by Transmission Control Protocol/Internet Protocol (TCP/IP) hosts during TCP/IP host-name resolution. Usually generated by TCP/IP utilities such as Ping and Telnet, or applications such as Internet Explorer.</td>
</tr>
<tr>
<td>(DNS)</td>
<td></td>
</tr>
<tr>
<td>Internet browsing</td>
<td>Traffic generated by the Internet Explorer browser application to download pages from a Web site.</td>
</tr>
</tbody>
</table>

Some application traffic, too, runs in the background:

- Exchange
- Microsoft SQL Server
- Microsoft Systems Management Server
- Microsoft SNA Server

There are two basic types: server-to-server and client-to-server. If your configuration isolates servers in a computer room to reduce total cost of ownership (TCO), it is relatively easy to tell one type from the other when you look at the combined traffic.

**Example**

AB Pound & Co. put all of its servers in a computer room connected to the client systems over a backbone. All server-to-client traffic has to cross the backbone, so it is easy to identify and isolate it. The trick is to link it to a particular client. Here’s the method for completing the model:

- Size each application that runs on any client.
- Identify which network segment each client is on.
- Calculate the total amount of background traffic generated for each network segment.
- Combine the total of each segment to calculate the total potential load on the backbone.

Adding up the network segment loads to calculate the backbone load doesn't always give an accurate answer, because the true total depends on more than just packets: it also is influenced by network topology, particularly if network segments route onto the backbone and some degree of traffic filtering is applied. However adding segment volumes makes for a useful worst-case scenario. Any variance probably will represent an improvement.

Numerous technical sources supply information you can put to good use when sizing background traffic. Search Microsoft TechNet for the string *capacity planning network traffic*. 
To calculate server-to-server background traffic you have to model the applications that run and the amount of background traffic that each produces.

**Broadcast Traffic**

Broadcast traffic (Internet-Protocol (IP) datagrams sent to all hosts on the subnet) is often overlooked, but it can have a major effect on all client-server systems. Broadcast frames result in hardware interrupts, which result in CPU activity. At some critical CPU loading level, the system seizes up. Short of total breakdown, which is thankfully rare, broadcast traffic merely grinds things down.

When a computer system receives a datagram, hardware makes the first filtering decision. The network interface card discards all frames not carrying its system address, then passes all frames (including broadcasts) that do have this address to the NIC driver through a hardware interrupt. The NIC driver is software, so any frames that make it this far cost some CPU processing time.

Sometimes a network shows very low traffic levels and sufficient capacity to look healthy, but analysis of the broadcast traffic levels shows enough to seriously degrade system performance. A system's ability to cope with broadcast traffic depends on its configuration and what other sorts of traffic it is dealing with at the time.

It is easy to measure how excessive broadcast traffic affects a system. Connect two PCs to an isolated network. Put Microsoft Network Monitor (a tool explained below) on one of the systems to generate broadcast frames, and run Microsoft Performance Monitor on the other to monitor the processor time usage levels and interrupts/sec. You can watch these values climb if you gradually increase the number of broadcast frames. The system running Performance Monitor starts to act sluggish and eventually stops responding altogether.

**Bottlenecks**

Wouldn't it be nice if there were never any bottlenecks on your way to work? No traffic lights, fender benders, car problems, detours, people pulling out in front of you, four lane highways narrowing down to one lane presided over by a lethargic flagman. Stop wishing: it isn't going to happen. And it's not going to happen with your computer system either. Sooner or later the system will reach its limit and getting data onto the network or through a router will take longer...and longer...

As easy as they are to spot, bottlenecks are not easy to predict, but they generally occur where one network is connected to another network—at a router, hub, switch, or server.

There are two types: those that affect a single client and those that affect multiple clients or network segments. The first type is usually easily identified and solved, because it almost always is the result of a single capacity problem: an overloaded server, a wire so packed with bits that nothing can move, etc.

Multiple-effect bottlenecks are usually harder to find because they may be the result of one problem or many. Figuring one of these out usually requires a lot of investigation and carefully documented results. Part of the effort is required to isolate the problem so it can be predicted (maybe it is the result of a unique or anomalous event) and, if necessary solved. And part of the effort is required to help the network manager to justify the perhaps considerable expenditure needed to solve it.

There are a number of areas to examine when you look for bottlenecks. Are any components between a client and server running at 100% utilization? This is a clear warning of bottleneck potential but does not necessarily mean that there is a bottleneck. This usage may represent only a spike, and thus be temporary. And if the max-ed out device is not preventing any other resource from getting its work done—if nothing is waiting for it—then it is not a bottleneck and
Doubling bandwidth will cost money but will not affect the condition. On the other hand, you can have bottlenecks on devices utilized well below 100 percent.

Trace the paths through the network looking at the points of interconnection. Some examples may be:

- Suppose all the network segments connected to a given router are running well within their capacity but the router simply cannot forward the number of packets it receives. NetMon would not show you this. You would have to run the router management software.
- Look for unacceptable broadcast traffic levels. (See the "Broadcast Traffic" section above.)
- Network contention (more than one system attempting to transmit data onto a network at the same time) can cause problems in Ethernet cables. Look for high collision rates.

A good bottleneck strategy has to vary from network to network, but every one should include a certain degree of monitoring designed to find backups before they cripple the system.

**Scalability and Predicting the Future**

Capacity planning should, within certain practical limits, help you predict the future. Once you know how your network looks today you can experimentally change some values and work out how it might look in the future, and, more importantly, how well the network might cope with specific changes.

Suppose AB Pound & Co., for instance, expands its store by adding a third floor. This means 150 new client systems and a new server. To calculate how the network will cope, the analysts can try extending the current set of spreadsheets. Some enlightened guesswork can probably help them project network loading, predict traffic patterns, and adapt the infrastructure so as to reduce or avoid bottlenecks. At the very least they can get some idea of how network performance levels will change and how network access can be kept at acceptable levels.

Network Monitor

Capacity planning requires tools. Which tools you need is in part dictated by the approach you plan to take. If your network is business-critical you may need to buy additional packages of analytical tools, but Windows NT provides some very good tools for general analysis. Chief among these is Network Monitor. A scaled-down version of NetMon is packaged with Windows NT; a more robust version ships with Systems Management Server. The differences are discussed in Chapter 1. Complete instructions on using NetMon are in the Windows NT Server Concepts and Planning Manual, “Chapter 10: Monitoring Your Network,” and the Windows NT Server 4.0 Resource Kit, Supplement 1 "Chapter 7: Monitoring Bandwidth and Network Capacity."

You install the NetMon Agent driver onto a network card in a Windows NT system. This sets the card in promiscuous mode, which allows the monitor to watch all network packets that go through the system—even packets for other destination systems are copied and passed up to the NetMon Application.

How can seeing everything that crosses the wire help with capacity planning? Because to plan for capacity you need to understand what traffic the network handles on a continuing basis, and this requires that you analyze background and functional/transactional tasks completely, and NetMon provides the information you need for a full load analysis of each task.

For instance, AB Pound & Co., has approximately 25,850 silk ties on display, so of course a customer must have one that is available, he thinks, but not in one of the cases, he knows. It is a garish thing, but the customer is always right, so the clerk logs onto a PC, enters the stock description, uses it to find the stock code, calls up the online order form, fills it out, and
submits it. This transaction involves several activities, each of which can generate network traffic:

- a log on (plus authentication)
- a search for a stock item (matching fields from the form to the database)
- a response from the server (with information about the horrid tie in question)
- an order entry/submission (which involve a number of client/server transactions)
- a log-off (maybe)

NetMon can tell you how much traffic is generated at each step, and it can tell you in an extremely specific and accurate way if you perform each activity and trace it separately. From there it is a short extrapolation to calculate average numbers of tasks, at which point you are well on the way to establishing traffic levels and deriving a sense of required network capacity.

**Network Monitor Interface**

The first NetMon window to appear is the Capture window, which presents the UI menus and toolbar, and four panes of statistics you can use to analyze overall network performance:

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Graph</strong></td>
<td>Displays the current activity as a set of bar charts indicating</td>
</tr>
<tr>
<td></td>
<td>the % of network utilization, the frames per second, bytes per second,</td>
</tr>
<tr>
<td></td>
<td>broadcasts per second, and multicasts per second during the capture process.</td>
</tr>
<tr>
<td><strong>Session Statistics</strong></td>
<td>Displays the summary of the conversations between two hosts, and which host is initiating broadcasts and multicasts.</td>
</tr>
<tr>
<td><strong>Total Statistics</strong></td>
<td>Displays statistics for the traffic detected on the network as a whole, the statistics for the frames captured, per second utilization statistics, and network adapter card statistics.</td>
</tr>
<tr>
<td><strong>Station Statistics</strong></td>
<td>Displays a summary of the total number of frames initiated by a host, the number of frames and bytes sent and received, and the number of broadcast and multicast frames initiated.</td>
</tr>
</tbody>
</table>

**Capturing Data**

There are three methods:

- From the **Capture** menu, click **Start**.
- Click the **Start Capture** button on the toolbar.
- Press the F10 function key.

As data is captured, the four panes in the Capture window display current network statistics as well as statistics for the captured data.

- To stop the capture, use one of three methods:
  - From the **Capture** menu, click **Stop**.
  - Click the **Stop Capture** button on the toolbar.
  - Press the F11 function key.

You can set a capture filter that describes which frames are to be captured, buffered, displayed, and saved. Filters are commonly configured either for specific types of traffic (protocols), such as IP, IPX, VINES, and so on, or on source or destination addresses—media access control (hardware) addresses or protocol addresses (IP or IPX). You can see the value of being able to filter captures in this way. AB Pound & Co., for instance, wanted to measure server-to-client traffic over the backbone, but was confronted with the problem of figuring which portion of
pipeline traffic was for which client. Filtering by address can isolate this type of traffic so that you can observe it as a separate component of overall traffic flow.

If you don't want to analyze data as soon as it is captured, you can save it to a capture file (with suffix .CAP) for later analysis or to create a record of system performance.

**Configuring Capture Triggers**
When troubleshooting, you may want to configure a capture trigger, which directs NetMon to perform an action in response to a certain event or condition: a buffer being filled completely or to a specified amount, a pattern match, a pattern match then buffer space, or buffer space and then a pattern match. For example, suppose a client computer is having difficulty transferring a file from a server. You capture the session, and the results show that every time a specific data pattern is transferred during the session, the transfer stops. Once NetMon fills its buffers, it overwrites previously collected data, and if you can't find the frames leading up to the suspect data pattern because they have been overwritten (by data captured afterwards) you can set a trigger to stop the capture when it has recorded the event you are interested in. You can also set different responses to triggers: complete an action, capture data, perform a command, notify the administrator, etc.

**Displaying Data**
There are three methods:

- From the Capture menu, click **Display Captured Data**.
- Choose the **Display Captured Data** toolbar button.
- Press the F12 function key.

**Summary Pane (Top)**
This lists all frames included in the current view of the captured data. When a frame is highlighted in the Summary pane, NetMon displays its contents in the **Detail** and **Hex** panes. You can add colors to highlight specific frames.

You can use mouse clicks to sort, move, and resize the pane's nine columns:

- **Frame**. All frames captured during one session are numbered in the order of capture time. The frame number appears in this column.
- **Time**. The frame's capture time relative to the beginning of the capture process. It can be configured to display the time of day when the frame was captured, or time elapsed since the previous frame capture.
- **Src MAC Addr (Source media access control (MAC) Address)**. The hardware address of the computer that sent the frame.
- **Dst MAC Addr (Destination MAC Address)**. The hardware address of the target computer.
- **Protocol**. The protocol used to transmit the frame.
- **Description**. A summary of the frame's contents. This can show the first protocol used in that frame, the last protocol used, or an automatic selection.
- **Src Other Addr (Source Other Address)**. An additional identifying address for the originator of the frame, other than the MAC address. This might be an IP or IPX address.
- **Dst Other Addr (Destination Other Address)**. The frame's destination.
- **Type Other Addr (Type Other Address)**. The type of address displayed in the previous two columns IP or Internetwork Packet Exchange (IPX).

**Detail Pane (Middle)**
This pane displays protocol information for the frame currently highlighted in the Summary pane. When a frame contains several protocol layers, the Detail pane displays the outermost level first.

When you select a protocol in the Detail pane, the frame's associated hexadecimal strings are highlighted (in the same color as that used for the protocol) in the Hex pane. If a protocol has a plus sign (+) beside it, you can display more information in the Detail pane by clicking on the +, by double-clicking the protocol, or by highlighting the protocol, and pressing ENTER. The expanded protocol information shows a line of data for each property associated with that frame.

Hexadecimal Pane (Bottom)
This pane displays in hexadecimal format the content of the selected frame. When information is highlighted in the Detail pane, the hexadecimal equivalent appears highlighted in the Hex pane. You may end up studying this data carefully, especially when you are attempting to determine the application programming interface (API) call used in a transaction.

Highlighting Displayed Data
The Capture Summary window displays a summary of all frames captured, and this sometimes is too much data, making the analysis difficult. There are several ways to highlight specific data.

Adding Color to Frames
You can color specific frames. For example, coloring all browser frames can provide a quick visual scan of how many frames were created by browser announcements. To color captured data:

- On the Display menu, click Colors.
- The Protocol Colors dialog box appears.
- Under Name, click the protocol(s) you want to color.
- Under Colors, set Foreground or Background to the color of choice.
- Click OK.

Implementing a Display Filter
A display separates out frames of interest, such as those from a particular host, or those using a particular protocol. You can configure display filters for protocols, for MAC or protocol addresses, or for unique frame properties (such as source or destination port). To configure:

1. On the Display menu, click Filter. The Display Filter dialog box appears.
2. Click either the Protocol == Any or ANY <-> ANY expression.
4. Click the Address, Protocol, or Property tab.
5. Configure the filter as appropriate for the address, protocol or property.
6. Click OK twice. The Capture Summary window displays only the data passed by the display filter.

To go back to displaying all captured data, either return the display filter to default (by loading DEFAULT.DF) or on the Display menu click Disable Filter.

Saving and Printing Captured Data
Network Monitor has built-in saving and printing capabilities. These are useful for any number of reasons. For example, the data does not have to be captured and analyzed by the same person. And when you are analyzing how a specific function affects network traffic, you probably will need the results of several captures to make an accurate assessment.

You can always print captures and save them, but data often is more useful (easier to manipulate, for instance) in soft copy, and NetMon gives you several options for saving captured data. If you configure a filter to display only data between a specific client and a specific server,
you can save the entire capture or just the data that passes the filter. Or you can save only a specific range of frames. Suppose you are analyzing a large data capture, and you are interested in a specific conversation that occurs in frames 17–21: NetMon allows you to save just those frames in a file that you can analyze later.

To save captured data:

1. On the File menu, click Save As. The Save Data As dialog box appears.
2. Under File Name, type a name that represents the data in the capture.
3. If a display filter has been implemented, click Filtered.
4. If a range of frames is to be saved, under Range, type the From and To values as appropriate.
5. Click OK.

Determining Network Resources
The full version of Network Monitor included with Systems Management Server 1.2 offers more sophisticated features to use when determining network usage:

Finding Top User
The Find Top Users option on the Capture Summary window’s Tools menu lists in order the computers that sent or received the highest number of frames in a capture. It also includes the bytes transmitted and received, as well as their percentages of the total.

Finding Top Protocol Distribution
The Protocol Distribution option on the Capture Summary window’s Tools menu displays the protocol that generated the most network traffic in the capture, by frames or bytes. This also includes their percentages of the total.

Finding Routers
The Find Routers option on the Capture Summary window’s Tools menu scans the capture and determines which network devices are routers, identifying them as Service Advertising Protocol (SAP), Browser, Routing Information Protocol over IPX (RIPX), IP, Open Shortest Path First (OSPF), or Raster Image Processor (RIP). You can invoke an interactive version of this function from the Network Monitor Capture window.

Finding MAC Address from Name
The Resolving Addresses From Name option on the Capture Summary window’s Tools menu queries the network using Domain Name System (DNS), NetBIOS name resolution, and the local NetMon database to display the MAC address associated with a name. You can also use it to query SAP and Systems Management Server databases. This function is also available on the Network Monitor Capture window’s Tool menu.

Remote Capturing
Normally, routers block traffic from moving between subnets unless destined for another network, so troubleshooting a problem on a remote network can be difficult. But NetMon has two components (application and agent) and by installing the agent on a remote computer, then attaching the application to it, you can see and analyze all traffic that appears on the remote network.

Installing the Agent
Separate NetMon agents allow either a Windows 9x or a Windows NT (3.5x and later) client to be the agent on a remote subnet.

To install the agent on Windows NT, in Control Panel click Network and Add Network Monitor Agent. This software is included with Windows NT 3.5x and later.

To install the agent on Windows 9x, start Control Panel and click Network. Click Add, and then click Service. Under Manufacturers click Microsoft, and then click Have Disk. In the Install
From Disk dialog box type the path Admin\Nettools\Netmon on the Windows 95 compact disc. Microsoft Network Monitor Agent will appear as the service name to install.

Starting the Agent
The agent must be started before it can be used to capture network traffic. On Windows NT, use the Services dialog box to start the agent. By default, it is configured for manual starting.

On Windows 9x, start System\NMAGENT.EXE whenever the agent is required.

Connecting to the Remote Agent
Once the remote agent has been started, connecting the application to it starts the data capture. The agent buffers the data locally then transmits it to the application when requested.

To connect to a remote agent:
1. On the Capture menu, click Networks. The Select Capture Network dialog box is displayed.
2. Click REMOTE, and then click Connect. The Connect To Network Monitoring Agent dialog box is displayed.
3. In the Agent Name box, type the remote computer name, and then click Connect. The Network Monitor Capture window displays the name of the remote agent computer.

Data is buffered and is not sent from the remote two agent to the local application until the capture is stopped, although (by default) the remote agent sends statistics to the application every two seconds. The updates generate some network activity, which you can decrease by decreasing the update frequency. To return to capturing on the local host, disconnect the remote connection and reconnect to the local network.

Comparing Network Protocols
Protocol can affect how much network traffic a function generates. Some protocols such as NWLink base much of their traffic on broadcasts, while others such as Transmission Control Protocol/Internet Protocol (TCP/IP) use more directed frames. Broadcast traffic can have an impact on a WAN, the severity of which depends on whether broadcasts are forwarded by the routers throughout the enterprise. If they are not, some functions will operate on the local network but not have complete functionality throughout the enterprise; if they are, complete functionality is available but WAN traffic is increased.

Microsoft recommends TCP/IP. Designed to avoid the disadvantages of protocols such as NetBEUI, it reduces traffic by delivering directed datagrams rather than broadcast packets.

Best Practices
How much effort (time and cost) should you invest in capacity planning? The answer to this is fairly straightforward although it takes some thinking: calculate how critical the network is to your organization and then calculate how severely network failure will affect your business. The closer this correlation, the more important capacity planning. If your network is less than critical, live monitoring may provide you with enough information and you can let it go at that.

Regardless of the depth of your analysis and planning effort, here are some practices derived in the field:

- Identify your business requirements and how critical the network is to their realization. Can the organization operate without its network? How long? To what degree will operation be curtailed or compromised?
- Identify the key user tasks. If possible, gather data to build a daily task timetable. With some tinkering, you can take into account hours of operation, days of the week, and other factors to get a fairly accurate look at regular network traffic. You may not
understand the network's enterprise role accurately until you look at what is done, by
whom, when, and how.

- Use Network Monitor to measure the amount of network activity that occurs for each of
  these tasks and record the results in a spreadsheet.
- Identify network topology and the location of clients and servers. Calculate the basic
  background traffic client-to-server and server-to-server, then map these onto a
  spreadsheet by segment (floors in a building, separate buildings, etc.—some
  segmentation scheme usually, but not necessarily, based on subnets).
- Multiply the total for each task by the number resources completing this task and add
  these to the spreadsheet.
- If the network is absolutely critical, use peak loading figures. Use average loading
  figures otherwise.
- Look for bottlenecks.
- Calculate how the network will scale and see if you can identify the point at which you
  will run out of capacity. Scenarios can help with this task. So can Performance Monitor,
  a tool you can use to observe network load over periods of time and under varying
  circumstances.


Read the TechNet article above and answer the following questions as you read through.

1. What are some risks associated with undertaking capacity planning?
2. What might you inadvertently encourage users to do if you brag about your network's
   bandwidth?
3. What are the risks of not undertaking capacity planning?
4. Describe the two types of network traffic that needs to be analysed?
5. Create a 'daily task list' for your busiest day at Swinburne.
6. Once you have created task lists for each user profile, summarised each profile's general use
   and mapped the usage to locations (e.g. floors) within the organisation, what should you do
   next? [Especially if you don't want to undertake the huge task of creating an hourly traffic
   profile]
7. What does it mean to 'map tasks to topology'?
8. How do you map background traffic?
9. Where do bottlenecks generally occur?
10. What types of bottlenecks may not be picked up using Network Monitor? How could you then
    monitor these bottlenecks?
11. What is the last stage in capacity planning?

Now read through the rest of the document and investigate each aspect of Network Monitor that is
raised in the document.

When you have finished try the Broadcast Traffic example in the last paragraph of the 'Broadcast Traffic'
section on page 8.