THE PORT 80 BLACK HOLE

Jim Metzler
Ashton, Metzler & Associates
jim@ashtonmetzler.com

Introduction

In the June 2007 IT Impact Brief (*Does IT Provide Business Value?*), I presented the results of a survey that was given to the NetScout community in March 2007. As part of that survey we asked The Survey Respondents to rate the impact that a wide range of activities will have on their IT resources during the next 12 months. Based on the survey results, the area that will have the biggest impact on IT resources is improving the ability to ensure acceptable application performance.

The fact that improving the ability to ensure application performance will have such a significant impact on IT resources represents a change in the role of network managers. In particular, the traditional role of the network manager has been almost exclusively to guarantee the uptime of networks. Now that role has expanded and network managers also play a significant role in security and application performance.

Previous IT Impact Briefs have discussed many of the impediments to ensuring application performance. For example, the January 2007 IT Impact Brief highlighted a number of these impediments, including the:

- Deployment of chatty protocols
- Growing use of n-tier applications
- Movement to use Web services-based applications
- Webification of applications
- Data center consolidation
- Continued movement of employees out of headquarters facilities

In addition, the *August 2006 IT Impact Brief* discussed how widespread network misuse is. In that brief, network misuse referred to malicious applications such as spyware or recreational applications like YouTube or Internet radio. In that brief I made the statement that "Successful application delivery requires that IT organizations are able to identify the applications running on the network and are also able to ensure the acceptable performance of the applications relevant to the business while controlling or eliminating applications that are not relevant." I still believe that statement. In fact, I think it would be very difficult for anyone to argue against the validity of that statement.

Managing application performance in general - and identifying the applications that are running on a network in particular - are both very complex tasks. There are, however, some factors that make these tasks even more difficult. One of these factors will be discussed in this IT Impact Brief. That factor is that a lot of traffic runs undetected over port 80. This is sometimes referred to as the port 80 blind spot. However, given the volume of traffic that typically transits port 80 combined with the risk associated with not being able to manage this traffic, I feel justified in calling this the port 80 black hole.

Port Hopping

This section of the IT Impact Brief will discuss one of the causes of the port 80 black hole - applications that do port hopping and typically end up using port 80.

Instant Messaging

In TCP/IP and UDP networks, a port is an endpoint to a logical connection and is the way that a client program specifies a specific server program on a computer in a network. Port numbers range from 0 to 65535. As described in RFC 1700, the ports that are numbered from 0 to 1023 are reserved for privileged services and are designated as well-known ports. For example, port 80 is the port that the server listens to expecting to receive data from Web clients.

Some applications, however, have the ability to hop between ports. A good example of this is instant messaging (IM) software such as AOL's Instant Messenger (AIM). AOL has been assigned ports 5190 - 5193 for its Internet traffic and AIM is typically configured to use these ports. If these ports are blocked, however, AIM will use port 80. As a result, a network manager might well think that by blocking ports 5190 - 5193 they are blocking the use of AIM when in reality they are not.

The point of discussing AIM is not to state whether or not a company should block AIM traffic - that is a policy decision that needs to be made by the management of the company. There are, however, good reasons why a company might choose to block AIM. From a security perspective, viruses and worms are increasingly using IM as a means for their transmission. Hence, IM can present a security risk. In addition, there are regulatory reasons why companies may want to either block IM or at least monitor its usage. For example, the Securities and Exchange Commission requires that all stock brokers keep complete records of all communications with clients. This requires that phone calls are recorded and email is archived. It also means that IM needs to either be blocked or archived. However, if IM traffic is flowing through port 80 along with lots of other traffic, most network organizations will not even be aware of its existence.

Peer-to-Peer Networks and Skype

A peer-to-peer ('P2P') computer network leverages the connectivity between the participants in a network. This type of network differs from a client-server network where communication is typically to and from a central server. Peer-to-peer networks are typically used for connecting nodes via largely ad hoc connections. Such networks are useful for many purposes including file sharing and IP telephony.

Skype is a peer-to-peer based IP telephony and IP video service developed by Skype Technologies SA. The founders of Skype Technologies SA are the same people who developed the file sharing application Kazaa. Many IT organizations attempt to block peer-to-peer networks because they have been associated with distributing content in violation of copyright laws.

Many security experts have warned about other dangers associated with peer-to-peer networks. For example, Antonio Nucci wrote “In order to avoid detection, many peer-to-peer applications, including Skype, change the port that they use each time they start. Consequently, there is no standard 'Skype port' like there is a 'SIP port' or 'SMTP port'. In addition, Skype is particularly adept at port-hopping with the aim of traversing enterprise firewalls. Entering via UDP, TCP, or even TCP on port 80, Skype is usually very successful at passing typical firewalls. Once inside, it then intentionally connects to other Skype clients and remains connected, maintaining a 'virtual circuit'. If one of those clients happens to be infected, then the machines that connect to it can be infected with no protection from the firewall. Moreover, because Skype has the ability to port-hop, it is much harder to detect anomalous behavior or configure network security devices to block the spread of the infection.”

FIX-based Applications

This section of the IT Impact Brief will discuss another one of the causes of the port 80 black hole - applications that are designed to use port 80 but which require more careful management than the typical port 80 traffic. A good example of this is virtually any application that is based on the Financial Information eXchange ('FIX') protocol. The FIX protocol is a series of messaging specifications for the electronic communication of trade-related messages. Since its inception in 1992 as a bilateral communications framework for equity trading between Fidelity Investments and Salomon Brothers, FIX has become the de-facto messaging standard for pre-trade and trade communications globally within the Equity markets, and is now experiencing rapid expansion into the post-trade space, supporting Straight-Through-Processing (STP) from Indication-of-Interest (IOI) to Allocations and Confirmations. The use of the protocol is gathering increased momentum as it begins to be used across the Foreign Exchange, Fixed Income and Derivative markets.

In our industry we often overuse the phrase business-critical. However, the claim can easily be made that the applications that support the business functions described above are indeed business critical. Analogously, there is often a lot of subjectivity relative to whether or not an application is time sensitive. Again, that is not the case for the applications that support the business functions described above. For example, if a stock broker is placing an order for millions of dollars in stocks, a small delay in placing the order can significantly drive up the cost of the stock. That is a textbook definition of a time-sensitive application.

Summary and Call to Action

The NetScout community is increasingly involved in ensuring acceptable application performance. That is a classic bad news/good news situation. The bad news is that ensuring acceptable application performance is very difficult from both a technology and organizational perspective. The good news is that if done correctly, it is good for our careers. That follows because most senior business managers do not truly value the network - they just expect it to work all of the time. They do, however, value the small number of applications that they use to run their business units. This affords networking professionals the opportunity to show the business value they provide by demonstrating how they ensure the performance of those applications.

However, it is difficult to see how we can be successful with application delivery if we ignore the port 80 black hole. As describe in this brief, the port 80 black hole makes:

1. Organizations vulnerable to security breaches
2. It impossible for organizations to comply with government and industry regulations
3. Organizations vulnerable to being charged with breaking copyright laws
4. It impossible for organizations to manage the performance of key business-critical, time-sensitive applications

To do good things for our companies, and for our careers, we need to find ways to better manage the traffic that transits port 80. Some of the features to consider when evaluating performance management tools in support of this issue include verifying that it can:

- Identify all applications on the network - including range-of-port or port-hopping, peer-to-peer and instant messaging applications - and not just well-known applications
- Support URLs to help distinguish legitimate web-based business applications from recreational surfing
- Support pattern matching and alarming based on these patterns (particularly important with P2P)
- Capture the packets in question for additional analysis and decode.