The Internet Outage and Attacks of October 2002

William F. Slater, III
President, Chicago Chapter of the Internet Society
ISOC-Chicago.org

Introduction

In October 2002, the Internet was hit with some unpleasant surprises that were unexpected, measurable, and had the potential to do greater damage than they did. This report will look at how these unpleasant surprises happened, what their impact was, why this happened, and the potential for future outages.

Interesting Times

An old Chinese curse says, "May you live in interesting times…" Certainly, we live in an interesting age. Despite the great Dot Com Bust of the early 21st Century, the growth of computers participating in the Internet has grown over six-fold since all that started to happen. We are in a recession, though some say the Information Technology field and the Telecommunications industry are both in a depression. Yet because the availability of the Internet has now become so commonplace, just like the electricity for lights in a room, it is now considered business critical in most of our day-to-day activities. We depend on our communications from the Internet and get quite upset when some technical glitch prevents the e-mail and the web pages from coming into our offices and homes. No small wonder then, that WorldCom, with its large share of Internet backbones that it owns and manages, was called to testify before a congressional sub-committee in July 2002, to guarantee the members of that sub-committee that their financial challenges of going through reorganization due to corporate bankruptcy would not threaten their ability to keep their share of the Internet backbones up and operational.

And as if all this was enough to make this age interesting enough, since September 11, 2001, we are all too aware that we live in an age where the threat of terrorist attacks is very real. And these attacks could come in any of several forms, targeted against people, buildings, businesses and infrastructures, hence our concern that terrorists could attack the Internet. It has already been proven that the Internet communication figured prominently in the planning and execution of the horrible attacks of September 11, 2001.

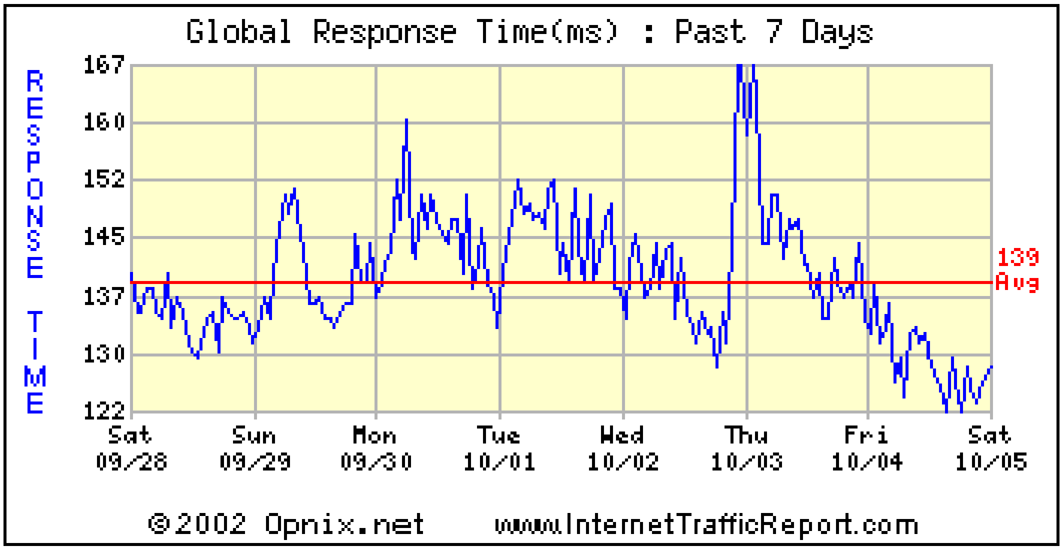
October 2002 proved to be an interesting month for the Internet.

October 3, 2002 – Router Misconfiguration Causes a Large Internet Outage

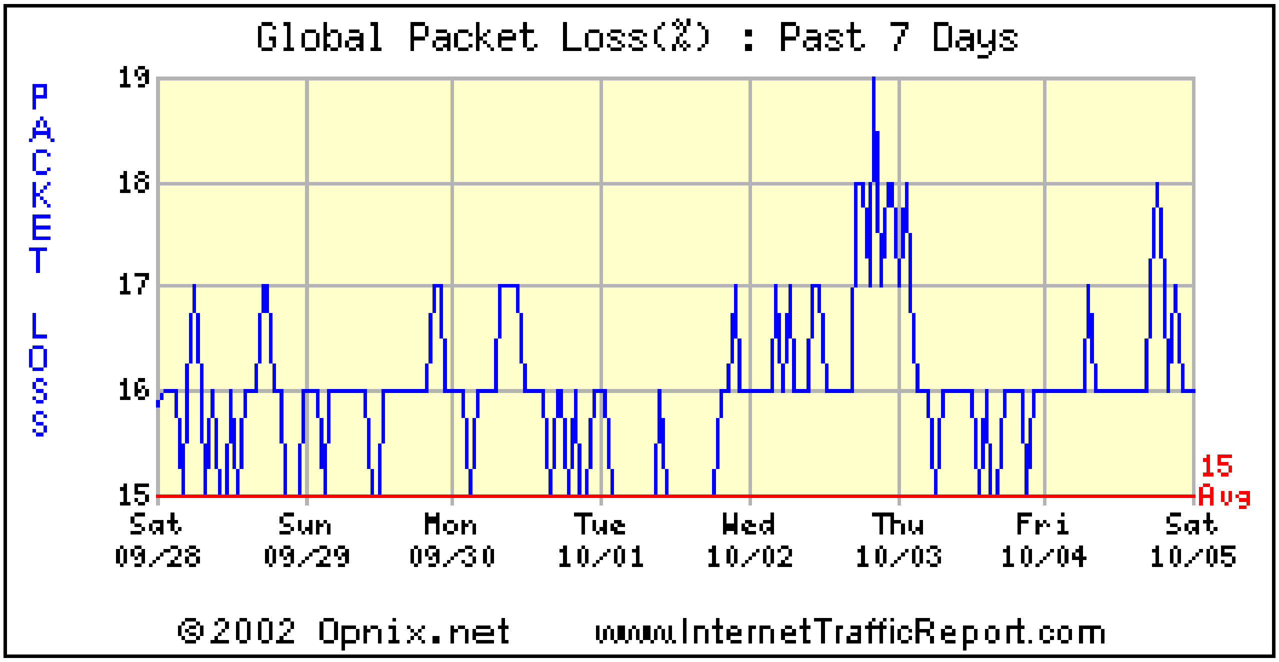
About between 8:30 am Central Time while at work we started noticing difficulties in getting our e-mail and web pages from the Internet. As you would expect, we immediately thought the problem was with our own internal infrastructure. Later, we would learn that it was a problem with a router table configuration linked to the UUNET segment of the WorldCom-managed portion of the Internet.

Pictures below show the impacts of this outage.

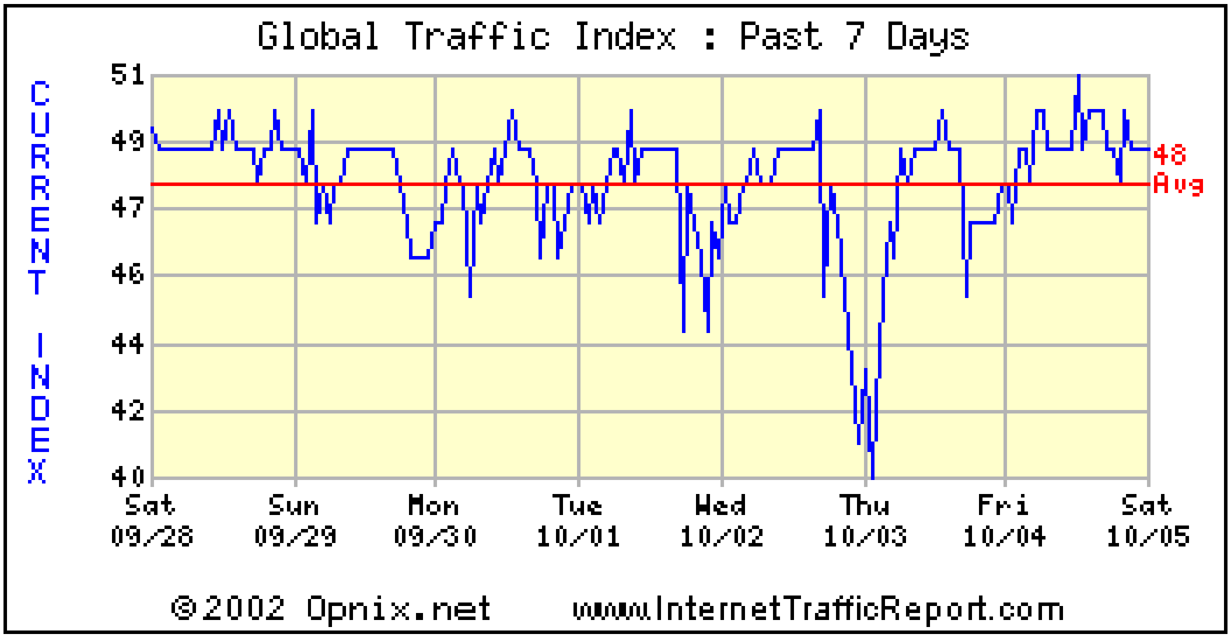
Response Times Were Increased:



Packet Losses Increased:



Traffic Was Down:



WorldCom's official statement on the incident is shown below:

> **WORLDCOM's INITIAL PRESS STATEMENT ON afternoon on 10/3:**
> **WORLDCOM IP NETWORK OPERATING NORMALLY**
> **CLINTON, Miss., October 3, 2002** - The following statement should be attributed to Jennifer Baker, WorldCom spokesperson: "Today WorldCom experienced an issue on its IP network, affecting approximately 20 percent of our U.S. IP customer base. Service to our customers has been restored. A preliminary investigation indicates there was a route table issue. We will continue to monitor the network, and we apologize to our customers who were affected."
>
> **WCOM STATEMENT to customers on Friday, 10/4 and Week of 10/7:**
> At 8:18 a.m. ET on October 3, 2002, certain routers in WorldCom's IP Network experienced a service interruption. WorldCom's Network Operations Center ("NOC") immediately initiated investigation and restoration procedures. The issue was escalated to the highest priority within WorldCom concurrent with escalation to the supporting vendors. WorldCom followed vendor directions to isolate the issue based on the vendors' review and integration of its equipment.
>
> WorldCom's investigation identified a particular router with a faulty configuration statement that propagated more route-broadcasts than the affected routers could handle. The suspected router was shut down and the network began to stabilize. The router configuration error was traced to an earlier repair activity. At 2:00 pm ET on October 3, 2002, the problem was resolved and the IP network returned to normal operation. WorldCom has taken steps to reinforce internal policies for implementing router configuration changes. WorldCom continues to work with equipment vendors to reduce the impact of service interruptions on network availability. WorldCom will review and refine its standard operating procedures to help minimize the possibility of a recurrence of this type of configuration error.
>
> **About WorldCom, Inc.**
> WorldCom, Inc. (NASDAQ: WCOEQ, MCWEQ) is a pre-eminent global communications provider for the digital generation, operating in more than 65 countries. With one of the most expansive, wholly-owned IP networks in the world, WorldCom provides innovative data and Internet services for businesses to communicate in today's market. In April 2002, WorldCom launched The Neighborhood built by MCI - the industry's first truly any-distance, all-inclusive local and long-distance offering to consumers. For more information, go to http://www.worldcom.com.

In an e-mail discussion about the incident, Dr. Vint Cerf, WorldCom's Senior VP of Internet Architecture and Technology, gave the following additional explanation:

> The outcome of the misconfiguration (which had a syntactically correct but semantically incorrect filter rule) caused the routes from the EBGP tables to be added to the internal tables of the intranet IS-IS. The overload of these routing tables triggered repeated route inserts and withdrawals and the latter, of course, resulted in a good deal of "disconnectedness" in our part of the Internet. It took a while to figure all this out. Especially when it turned out that the defect in the configuration was the misplacement of a single bracket in a complex route filter rule. It is actually more complex than I've suggested above because the tables were sorted with most-aggregated first and this also had an effect on the behavior of the routers when limits to the routing table were reached. The tables that were overloading were actually resident on line cards to increase efficiency.
>
> There are several lessons. One is that we have to work harder to make the software of routers even more robust - and in particular to deal with overloads and breaking of limits better. We need to double and triple check such things as router configurations - and apply some more automatic validation steps for operational transactions. The second is that no vendor's software is entirely free of bugs that trigger problems as threshholds are breached. In this case, two different vendor's equipment had different reactions to the problem that proved to be reinforcing in the worst sense. In a system as large as UUNET, we seem to routinely push the envelope of performance parameters.

DNS, Root Servers, and Name Resolution

Computers and users find their way to other networked computers across the Internet using networking software known as TCP/IP and by having names converted into IP addresses. For example, the name billslater.com resolves to 206.126.230.92. That resolution happens courtesy of a lookup request performed against a distributed database that is found in many locations around the Internet. This database known as the Domain Name System contains the IP addresses and names of computers that are registered to be on the Internet. This database is maintained and updated by the InterNIC (www.internic.net). This DNS database looks like an inverted tree, and the top parts of the database are stored on "Root Servers".

Each Root Server has a fully qualified domain name and IP address, but it also known by an alphabetic letter. The List DNS Root Servers is shown below:

Server	Operator	Cities
A	VeriSign Global Registry Services	Herndon VA, US
B	Information Sciences Institute	Merina Del Rey CA, US
C	Cogent Communications	Herndon VA, US
D	University of Maryland	College Park MD, US
E	NASA Ames Research Center	Mountain View CA, US
F	Internet Software Consortium	Palo Alto CA, US
G	U.S. DOD Network Information Center	Vienna VA, US
H	U.S. Army Research Lab	Aberdeen MD, US
I	Autonomica	Stockholm, SE
J	VeriSign Global Registry Services	Herndon VA, US
K	Reseaux IP Europeens - Network Coordination Centre	London, UK
L	Internet Corporation for Assigned Names and Numbers	Los Angeles CA, US
M	WIDE Project	Tokyo, JP

These Root Servers are critically important to the Internet and the Internet community, because they form the basis of the entire Domain Name System on which all the name resolution depends. Though there are other copies of it in other locations throughout the Internet, these Root Servers hold the main copies of the DNS database.

October 21, 2002 – DDoS Attacks Against the 13 Internet Root Servers

In the afternoon of this otherwise normal Monday, on October 21, 2002, a series of well-coordinated, simultaneous DDoS attacks were launched from various points around the world, against each of the 13 Root Servers that are used for the Internet's Domain Name System (DNS). The attack, which disabled nine of the 13 Root Servers, started at 4:45 pm EDT, lasted for about one hour.

The most affected Root Servers during this attack are listed below:

A	VeriSign Global Registry Services Herndon VA, US
G	U.S. DOD Network Information Center Vienna VA, US
H	U.S. Army Research Lab Aberdeen MD, US
I	Autonomica Stockholm, SE
J	VeriSign Global Registry Services Herndon VA, US
K	Reseaux IP Europeens - Network Coordination Centre London, UK
M	WIDE Project Tokyo, JP

In a DDoS attack, a server is repeatly hit with requests such as a ping (ICMP) request, or possibly even an SNMP (Simple Network Management Protocol) request by a program operated on another computer, often called a "zombie". The culprit will trigger the zombie computer(s) to begin their attacks at a time of his choosing, hoping to flood the target computer with so many requests that the operating system on the target computer finally gives up and freezes, or even in some cases, aborts its operation.

What was disturbing about these Root Server attacks is that it clearly done with the intent to cripple or shutdown the Internet. The person or persons who executed this attack had done their homework and knew exactly what they were doing, and how to accomplish it.

One source that worked at one of the organizations who maintains the Root Servers said this about the attacks: "This was the largest and most complex DDOS attack ever against the root server system."

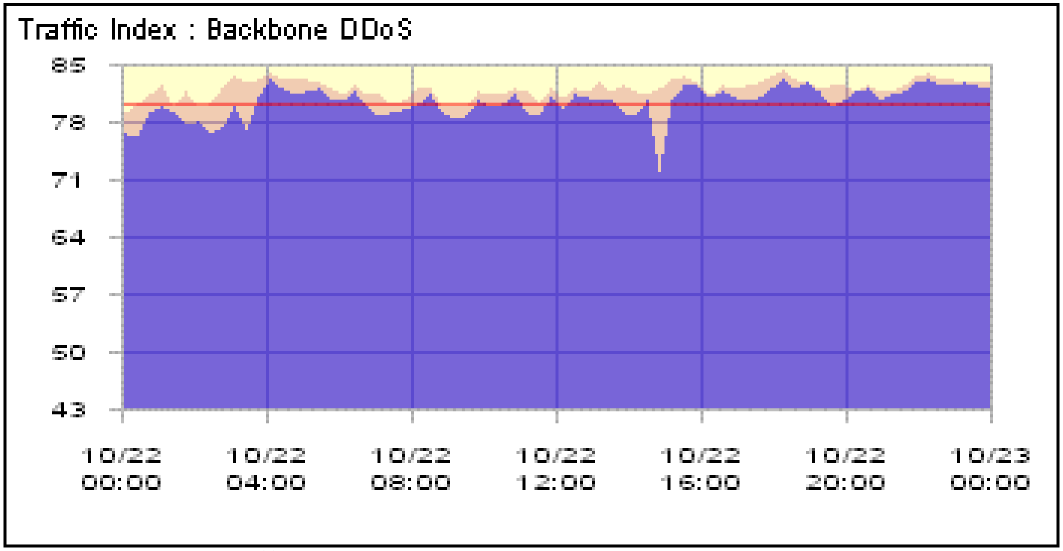
Result

In a news article by David McGuire and Brian Krebs, washingtonpost.com staff writers published at TechNews.com on October 22, 2002 has this analysis of the attacks:

> Ordinary Internet users experienced no slowdowns or outages because of safeguards built into the Internet's architecture. A longer, more extensive attack could have seriously damaged worldwide electronic communications, the source said.
>
> Internet Software Consortium Inc. Chairman Paul Vixie said that if more servers went down, and if the hackers sustained their hour-long strike a bit longer, Internet users around the world would have begun to see delays and failed connections.
>
> Chris Morrow, network security engineer for UUNET, said "This is probably the most concerted attack against the Internet infrastructure that we've seen." UUNET is the service provider for two of the world's 13 root servers. A unit of WorldCom Inc., it also handles approximately half of the world's Internet traffic.
>
> DDOS attacks are some of the most common and easiest to perpetrate, but the size and scope of Monday's strike set it apart.
>
> Vixie said only four or five of the 13 servers were able to withstand the attack and remain available to legitimate Internet traffic throughout the strike. "It was an attack against all 13 servers, which is a little more rare than an attack against any one of us," he said.

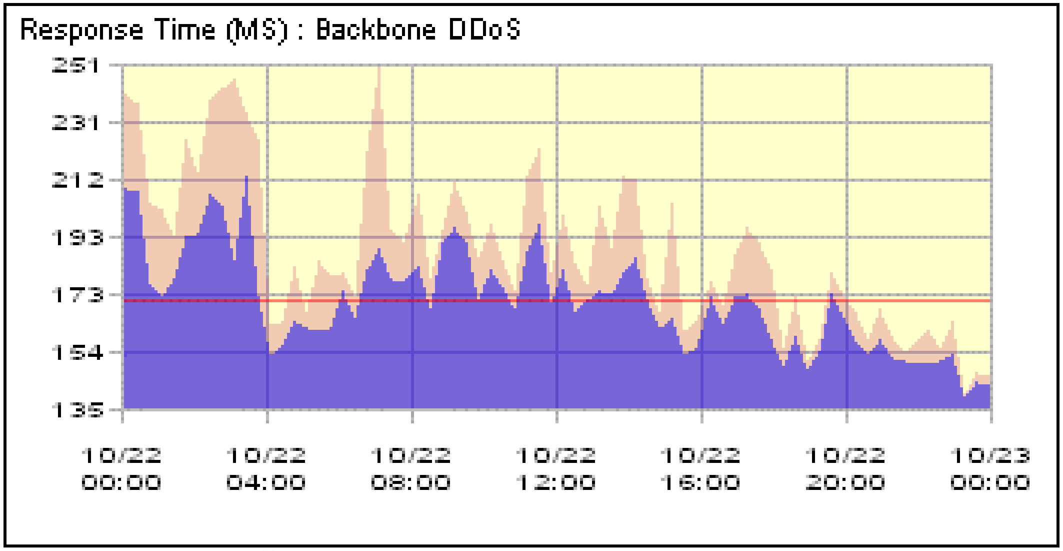
Pictures below show the impacts of this series of attacks.

A Drop in the Global Internet Traffic Index:



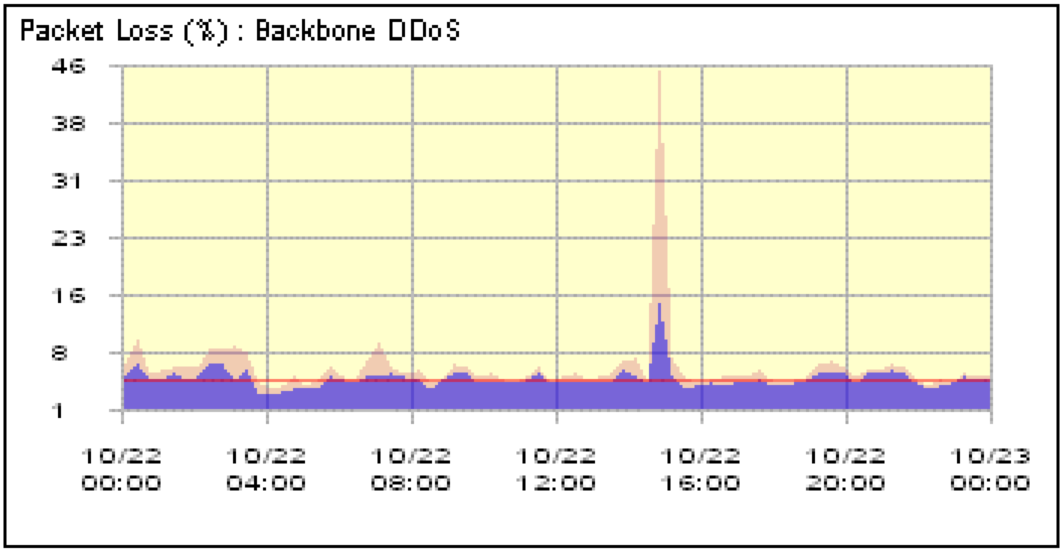
From the InternetTrafficReport.com website.
(Red indicates maximum, purple is average.)

An Increase in the Global Internet Response Time:



From the InternetTrafficReport.com website.
(Red indicates maximum, purple is average.)

An Increase in Packet Loss



From the InternetTrafficReport.com website.
(Red indicates maximum, purple is average.)

October 22, 2002 – DDoS Attacks Against Websites

Following the October 21, 2002 DDoS attacks, the very next day another series of DDoS attacks were launched against several websites worldwide.

Vint Cerf's Statement on the Internet's Robustness

> "We even tested these ideas by simulating the fragmentation of the ARPANET and re-binding it using flying packet radios on Strategic Air Command aircraft in the early 1980s," recalls Cerf, who is now senior vice president for Internet architecture and engineering at MCI Communications Corp. in Washington, D.C.
>
> That simulation, using special radios equipped with Internet technologies, proved that if a nuclear bomb dropped and the network was initially splintered, the remaining sections of the network would seek each other out and relink, continuing to transmit information across the surviving parts of the system.
>
> But Cerf is quick to say that there was no truth to the widespread belief that the Internet, or even its predecessor ARPANET, was impervious to nuclear attack. "That was not true, although its design did make use of the robustness of packet switching to route around failures and congestion."

What Improvements Need to Be Done to Protect Against Future Similar Attacks?

Steve Crocker, a noted computer scientist and engineer who was one of the original developers of the ARPANET is working with ICANN to help assess Internet security problems and make improvements. During an interview, he gave his opinions on what needs to be done to improve security for the Root Servers:

> A: There are three areas for improvements. They range from relatively easy to relatively hard to do, and range from useful to more important.
>
> The first is improving the core protocols and service for DNS, and second, tightening up the Internet against DDoS attacks by having the Internet service providers impose some discipline and authentication on the hosts. In today's Internet, it's relatively easy for a host to lie about its address and send packets with misleading return addresses. It's possible to fix this.
>
> As part of tightening up the basic DNS system, we need to deploy the DNS security protocol [DNSSEC, a security protocol intended to improve data origin authentication] and create a wider set of implementations of BIND [the Internet Software Consortium's Berkeley Internet Name Domain server software used for DNS]. I hasten to add that lack of diversity is not actively causing any harm, and the main reason for wanting diverse implementations is general good practice. On the other hand, we do know that many people are running obsolete versions of BIND, and the older versions are known to have critical bugs.

Where to Go To Learn More

Obviously, one of the great things about the Internet and the World Wide Web is the abundance of knowledge about practically everything. The list below provides excellent sources for data about Internet performance, structure, and attacks.

Matrix Net Systems	www.matrix.net
Internet Traffic Report	www.internettrafficreport.com
Internet Weather Report	www.mids.org/weather
Cyber Geography Research	www.cybergeography.org
National Infrastructure Protection Center	www.nipc.gov
Computer Emergency Response Team	www.cert.org
The Internet Society	www.isoc.org

Conclusion

James Gleick in his 2000 book, ***Faster: The Acceleration of Just About Everything*** asserts that there is an efficiency paradox where the more complex and finely tuned a system is and the more it is depended upon to synchronize events in a process, then the greater the damage that results when the system breaks down or is halted. The WorldCom router problems of October 3, 2002 and the DDoS attacks of October 21 and 22, 2002, show us that while the Internet has its weak points that can succumb to an attack or human error, it is also so large, so distributed, and so resilient that continues to work as designed, even in the face of events like this. However, because the Internet is now so important to people, businesses, and governments around the world, it does need to be fortified against such problems as human error and DDoS attacks in the future. Fortunately for all us who enjoy and rely on the Internet, some of the best people are working on these problems right now.

Epilogue – November 6, 2002

The improvements to guard against Internet attacks have already started: On November 5, 2002, Verisign Inc., which operates two of the Root Servers, moved one Root Server to a different building in an unspecified location in northern Virginia and onto a different part of its network, company spokeswoman Cheryl Regan said on November 6, 2002.

Verisign said the change was designed to ensure that a hardware outage or focused attack targeting part of its network could not disrupt both servers.

Byline:

William F. Slater, III is a computer consultant who lives and works in the Chicago area. After obtaining a B.S. Eng. Tech. degree in Computer Systems Technology from Memphis State University in May 1977, he entered active duty in the U.S. Air Force as a computer systems staff officer supporting command control applications for the Strategic Air Command Battle Staff in Offutt Air Force Base, NE. After finishing his service in the U.S. Air Force, he began his civilian computer career, and continues working in software, networks, databases to this day. In the evenings, after work he teaches topics such as programming in Java, networks and databases. He lives in a home with his lovely Polish wife whom he met on the Internet and with 35-networked computers and over 3400 computer books. He is a co-founder and current president of the Chicago Chapter of the Internet Society. More on Mr. Slater can be found at billslater.com and at isoc-chicago.org .