OpenNetwork Technologies DirectorySmart 4.6 AuthMark Performance Details

By Bruce Weiner

(PDF version, 149 KB)

April 16, 2001

Contents

Acknowledgment

We thank Stefan Hinker, Benchmark Engineer at Sun's Benchmark Center in Langen, Germany, which is part of Worldwide Customer Benchmarking at Sun, who helped configure the servers and explained the E10000 architecture.

Test Methodology

Mindcraft® tested the performance of OpenNetwork Techonolgies DirectorySmart 4.6 using our iLOAD MVP™ tool to run the AuthMark ™ Benchmark Login and Extranet Scenarios. In this section, we describe these tools so that you will be able to understand the performance results discussed in the Result Analysis section below.

iLOAD MVP Overview

iLOAD MVP is a general-purpose, script-driven capacity planning, benchmarking, and regression testing tool. The major components of iLOAD MVP are:

- A Control Center that manages client systems, controls test script execution, and reports on test results.
- Multi-threaded client load generators that execute test scripts to simulate users accessing a server.
- Test script generation programs.
- Test data generation programs.

iLOAD MVP provides the capabilities needed to test high-performance servers with a small number of client systems. Its capabilities include:

- The ability to simulate a large number of simultaneous user sessions. The number of user sessions is limited only by the client OS, the amount of memory and the performance of the client systems.

- Support for HTTP 1.0 and 1.1 as well as LDAP V3.
- Support for authentication and authorization.
- Support for SSL.
- Custom test scripts.

The AuthMark Benchmark

The AuthMark Benchmark is designed to test the performance of products that provide authentication and authorization services in support of Web servers. *Authentication* is the process of verifying who a user is; it typically occurs when a user logs in. *Authorization* is the process of verifying that an authenticated user is allowed to see or to use a particular resource. In the case of a Web server such resources include HTML files, graphic files, and programs that generate Web pages dynamically.

AuthMark simulates a large number of users accessing Web servers via their browsers. This approach permits AuthMark to test authentication and authorization performance independent of the technology used to provide those services.

AuthMark consists of several test scenarios to determine various aspects of performance for authentication and authorization systems under different circumstances. For the DirectorySmart tests we used the AuthMark Login and Extranet Scenarios.

AuthMark Login Scenario

The AuthMark Login Scenario focuses on testing authentication. We call it the Login Scenario because authentication is done the first time a user accesses a protected part of a Web site, just like a login. It is important to understand what happens during a login in order to understand what the Login Scenario measurements mean.

Login Process

The following simplified sequence will walk you through the login process to show you how it works using the DirectorySmart login process (which differs from the HTTP 1.0 and 1.1 protocols in that a form is used to send the user name and password):

1. The iLOAD test client (a script-driven program that emulates a web browser) sends a request to the Web server for a protected resource.
2. The Web server returns the login form (in these tests, the login credentials are username and password) and an encrypted cookie from the DirectorySmart Web server plug-in.
3. Using an HTTP POST operation, the test client returns the login credentials and the DirectorySmart cookie to the Web server, which forwards them to the DirectorySmart Web server plug-in.
4. The DirectorySmart Web server plug-in checks the credentials against those in the LDAP directory to validate the user name and password. If authenticated, authorization is checked in the next step. Otherwise, an an authentication error is returned returned.
5. DirectorySmart checks if the user is authorized to access the requested resource. If so, the resource, which in this case is one of the 14 KB Web pages, is returned to the test client along with an encrypted session cookie.

Once it has been authenticated, the iLOAD test client automatically sends the encrypted session cookie in each header whenever it requests a URL in the same realm, just like a Web browser does.

Login Scenario Configuration

Table 1 shows the AuthMark Login Scenario configuration parameters we used.

Table 1: AuthMark Login Scenario Configuration Parameters

Parameter	Value
Number of users in the security database	1,000,000
Number of Organizational Units or security groups	10
Total number of user sessions per test	100,000

The number of user sessions active during a given test run is determined by the length of the test and the number of logins. Sessions are not logged out once created. Instead, each session remains quiescent after login.

Running the Login Scenario

The basic steps for running the Login Scenario are:

1. Generate the data to fill the security directory. iLOAD MVP provides a tool to generate realistic data for the LDAP V3 organizationalPerson object class and Netscape's inetOrgPerson object class. It also includes tools to load the same data into an LDAP directory, which were used for this test.
2. Load the security directory with the user data.
3. Generate the test scripts for the Login Scenario. iLOAD MVP provides a tool to do this. These scripts drive iLOAD MVP to simulate user interaction with the Web server(s).
4. Load Web pages on the Web server(s). There are 100 Web pages each of which is 14 KB in size for the Login Scenario.
5. Load and configure the authentication/authorization system.
6. Run the benchmark.

The Login Scenario test script selects users randomly from the user database (see Table 1 for the numbers we used for this test). The tester is free to select the number of client test systems and the number of iLOAD MVP client threads to use. These are called the *load generators*.

The tester selects the number of load generators to get the highest performance possible from the authentication/authorization system being tested. In order to obtain the peak performance from an authentication/authorization system, the tester may need to use multiple Web servers and database servers.

The tester is permitted, but not required, to do a warm-up run of the test scenario in order to get the servers to a state that would more likely represent the state they would be in during normal operation. For this benchmark, we warmed-up the servers by running the test script in its entirety.

Extranet Scenario

The Extranet Scenario simulates an environment where users must login to a Web site and where all access requests require authorization. This scenario depicts a more complete and more realistic usage pattern than the Login Scenario.

The Extranet Scenario test execution starts with the same operation sequence as the Login Scenario (steps 1 - 5 above) and continues with the following operations:

6. The test client requests a resource, sending the encrypted session cookie along with the request.
7. The authorization services check the validity of the user and that the user is authorized to have access to the resource.
8. If the user is authorized, the resource is returned.
9. The test client then requests eight additional resources.

DirectorySmart checks the continuing validity of the authenticated user each time a resource access request is made to ensure that the user session has not been revoked. However, the user is not re-authenticated. As a result, the user does not see a new login request as long as the resources being accessed are in the Internet domain in which the user has been authenticated.

The Extranet Scenario operation sequence consists of one authentication followed by 10 authorizations yielding a total of 11 operations per user session. We call these 11 operations an Extranet Sequence. For the Extranet Scenario, we warmed-up the servers by running the test script in its entirety.

Result Analysis

This section analyzes the Login and Extranet Scenario performance characteristics of OpenNetwork Technologies DirectorySmart 4.6 including its performance scalability with different server configurations.

Login Performance - 1,000,000 User Directory

DirectorySmart, which is located on a Web server for the configurations we tested, is the control point for all authentication and authorization. Our tests were structured to push the Web server systems as closely as possible to 100% CPU utilization. Because DirectorySmart uses LDAP directory servers to store user authentication and authorization information without an intervening policy/authentication server, we were careful to be sure that the LDAP directory server CPUs were not 100% utilized, otherwise they would have limited DirectorySmart performance. That is why Table 2 summarizes the Login Scenario performance as a function of the Web and LDAP server configurations. The Scaling Factor in Table 2 shows how much faster a configuration is compared to the smallest configuration, Configuration 1.

Table 2: DirectorySmart Login Performance Scalability - 1,000,000 Users

Config.	Logins per minute	Scaling Factor	# LDAP Directory Servers & Total Directory CPUs	# Web Servers & Total Web CPUs	Logins/ minute/ Total CPUs	Web/LDAP Server CPU Utilization
1	**20,760**	-	Servers: 2 CPUs: 2	Servers: 2 CPUs: 4	**3,460**	Web: 100% LDAP: 60%

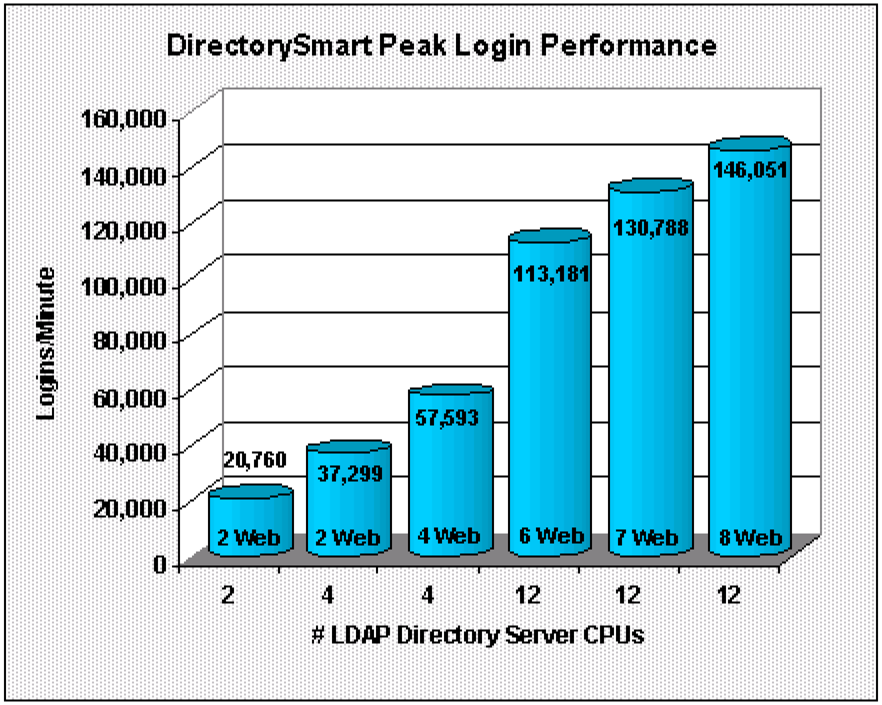
2	**37,299**	1.8	Servers: 2 CPUs: 4	Servers: 2 CPUs: 8	**3,108**	Web: 99% LDAP: 60%
3	**57,593**	2.8	Servers: 2 CPUs: 4	Servers: 4 CPUs: 12	**3,600**	Web: 90-95% LDAP: 85%
4	**113,181**	5.5	Servers: 3 CPUs: 12	Servers: 6 CPUs: 24	**3,144**	Web: 98% LDAP: 70%
5	**130,788**	6.3	Servers: 3 CPUs: 12	Servers: 7 CPUs: 28	**3,270**	Web: 92% LDAP: 82%
6	**146,051**	7.0	Servers: 3 CPUs: 12	Servers: 8 CPUs: 32	**3,319**	Web: 7@95%, 1@80% LDAP: 85%

The values in the "logins/minute/total CPUs" column are computed by dividing the "logins per minute" by the sum of the "#LDAP directory server CPUs" and "#Web servers & total Web CPUs" for each configuration.

The Web server CPU utilizations for Configurations 3, 5, and 6 show that more performance could have been derived from DirectorySmart. The limiting factor in these cases was the performance of the load generator systems. The LDAP directory server CPU utilizations for all of the tests show that the directory servers could have supported more DirectorySmart-enabled Web servers.

Figure 1 shows DirectorySmart's Login performance from Table 2 by the number of LDAP directory server CPUs used. The number of Web servers used is shown in each column.

Figure 1: DirectorySmart Login Scalability for a 1,000,000-User Directory



Extranet Scenario

The Extranet Scenario measures the combination of one user authentication and 10 authorizations for access to resources (these 11 operations constitute one Extranet sequence). The Extranet Scenario, because it uses a more realistic mix of operations than the Login Scenario, provides a better basis for capacity planning purposes.

Table 3 shows the DirectorySmart Extranet Scenario performance for Configuration 6 in Table 2 - eight Web servers with four CPUs each and three LDAP directory servers with four CPUs each. The results demonstrate that DirectorySmart performs authorizations faster than it does authentications.

Table 3: DirectorySmart Extranet Performance - 1,000,000 User Directory

Measurement	Extranet Scenario	Web/LDAP Server CPU Utilization
Authentications/minute	25,428	Web: 86% LDAP: 20%
Authorizations/minute	254,280	
Total operations/minute	**279,708**	

The Web and LDAP directory server CPU utilizations shown in Table 3 indicate that DirectorySmart could have achieved higher performance. It was the load generator systems, running at 100% CPU utilization, that limited our ability to drive the Web servers with DirectorySmart to their maximum performance.

DirectorySmart uses the LDAP directory servers much less for authorizations than it does for logins, which is shown by the 20% CPU utilization for the Extranet Scenario test compared to the 60% to 85% CPU utilizations for the Login Scenario tests. This means that you can plan to deploy more Web servers per LDAP directory server than we used for the Extranet Scenario test. Of course with more DirectorySmart-enabled Web servers, you can expect to achieve higher authorization rates than we did, if your application load is comparable to the one we tested.

Conclusions

The benchmark results lead us to conclude that:

- OpenNetwork Technologies's DirectorySmart 4.6 has achieved the highest AuthMark Login and Extranet Scenario performance we've seen to date.
- DirectorySmart 4.6 delivers very consistent login performance per CPU, which makes it easy to plan configurations for the load you need to handle.
- DirectorySmart delivers outstanding performance scaling as CPUs are added to a configuration.

Hardware Configurations Tested

All of the Web server systems were partitioned from a single Sun Enterprise 10000 server into separate Dynamic System Domains, which function as separate systems. According to Stefan Hinker, Benchmark Engineer at Sun's Benchmark Center in Langen, Germany, which is part of Worldwide Customer Benchmarking at Sun and where we did the testing, "Memory performance per CPU is not higher in an Enterprise 10000 four-CPU Dynamic System Domain than in a four-CPU Enterprise 450." So, we conclude that OpenNetwork gained no performance advantage by using an Enterprise 10000 instead of a comparable number of Enterprise 450s configured with the same number of CPUs and the same amount of memory.

The LDAP directory servers were separate Sun Enterprise 3000, 3500, and 4500 systems. Table 4 shows the number of servers of each type and the number of CPUs per server for the configurations we tested. There were two different Web server configurations for Configuration 3, which is why there are two lines in the "Web Servers & CPUs/Server" column. Table 5 presents the configuration of each of the Web servers. Table 6 shows the configuration of the LDAP directory servers.

We used two switched networks for all of the tests. One network connected the load generators to the Web servers. The other network connected the Web servers to the directory servers.

Table 4: Servers and CPUs

Config.	LDAP Directory Servers & CPUs/Server	Web Servers & CPUs/Server	Lab Setup
1	Servers: 2 CPUs: 1	Servers: 2 CPUs: 2	Figure 2
2	Servers: 2 CPUs: 2	Servers: 2 CPUs: 4	Figure 3
3	Servers: 2 CPUs: 2	Servers: 2 CPUs: 4 Servers: 2 CPUs: 2	Figure 4
4	Servers: 3 CPUs: 4	Servers: 6 CPUs: 4	Figure 5

5	Servers: 3 CPUs: 4	Servers: 7 CPUs: 4	Figure 6
6	Servers: 3 CPUs: 4	Servers: 8 CPUs: 4	Figure 7

Table 5: Sun Enterprise 10000 Web Server Configuration

Feature	Configuration
CPU	4 x 400 MHz UltraSPARC II (we used the `psradm` command to enable/disable processors as specified in Table 4) Cache: L1: 16 KB I + 16 KB D; L2: 4 MB
RAM	4 GB ECC
Disk	1 x 18 GB SCSI
Networks	1 x Quad 100Base-TX NIC (4 ports, only 2 used) per Dynamic System Domain (Web server)

Table 6: Sun Enterprise 3000, 3500, and 4500 LDAP Directory Server Configuration

Feature	Configuration
CPU	4 x 400 MHz UltraSPARC II Cache: L1: 16 KB I + 16 KB D; L2: 4 MB
RAM	4 GB ECC
Disk	4 x 18 GB SCSI, no RAID
Networks	1 x 1000Base-SX Gigabit (fibre) Ethernet

Figure 2: Configuration #1 - 2 Directory (2 CPUs) and 2 Web Servers

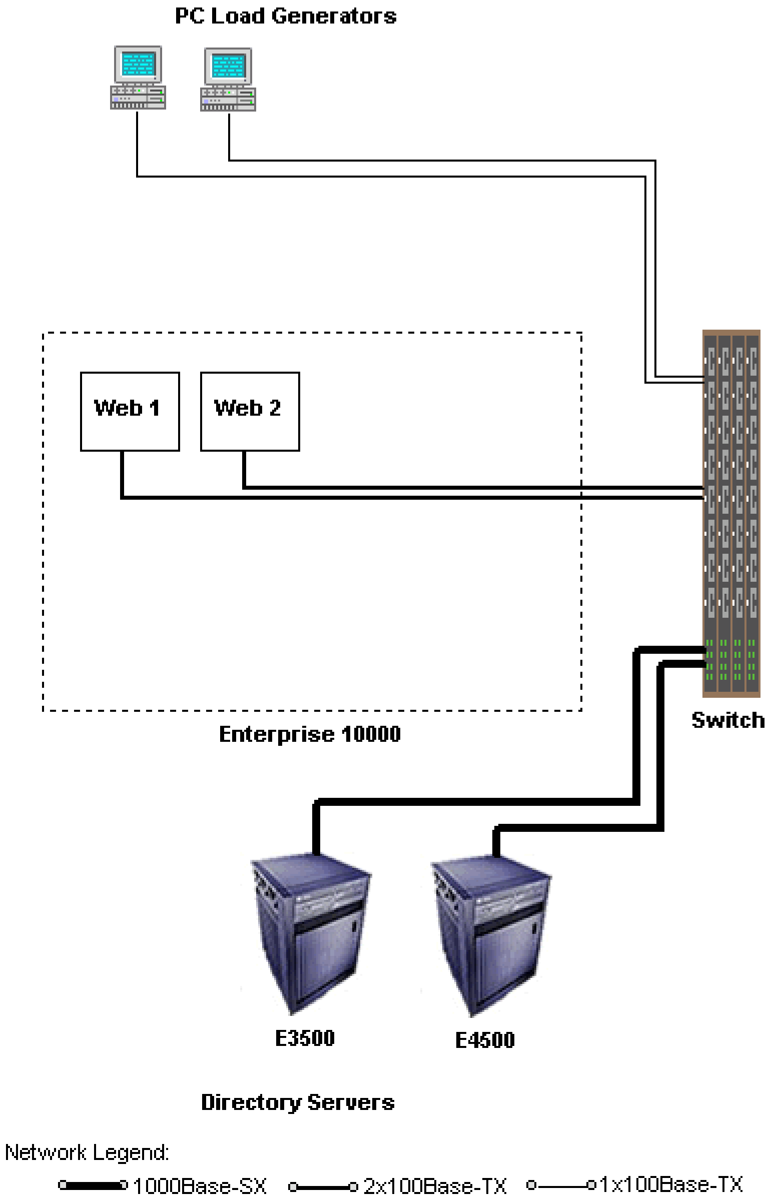


Figure 3: Configuration #2 - 2 Directory (4 CPUs) and 2 Web Servers

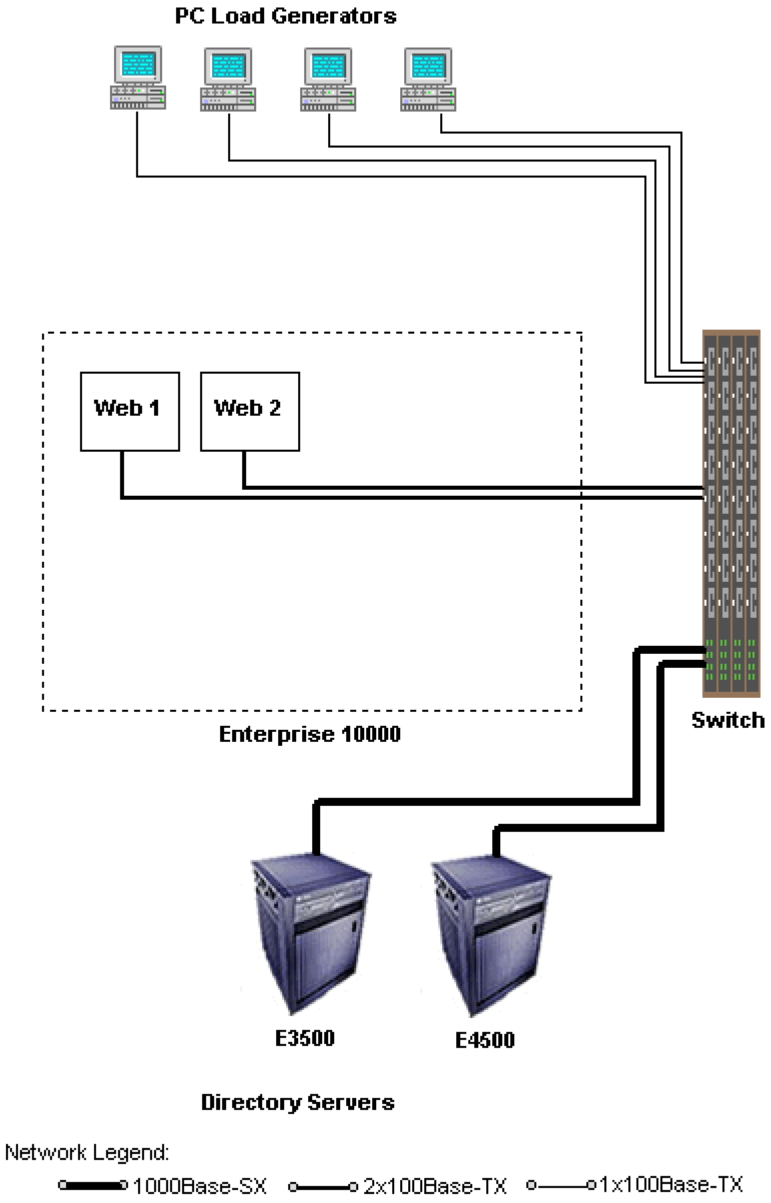


Figure 4: Configuration #3 - 2 Directory (4 CPUs) and 4 Web Servers

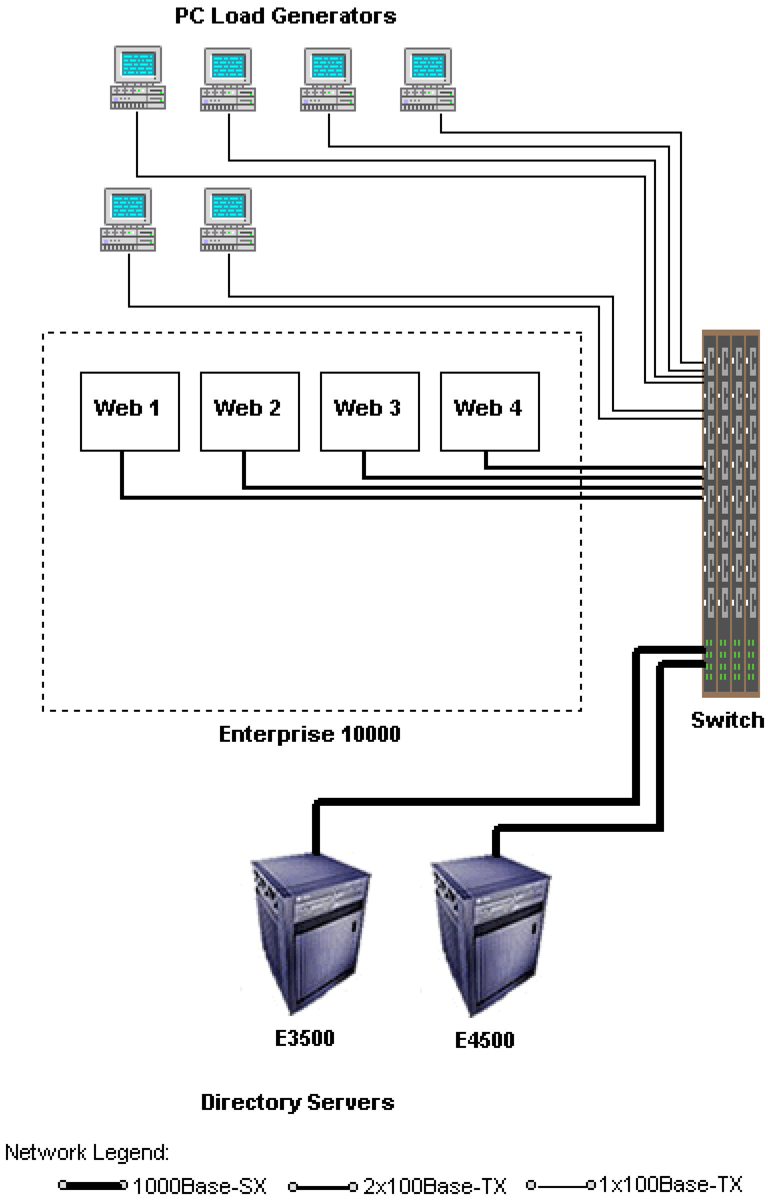


Figure 5: Configuration #4 - 3 Directory (12 CPUs) and 6 Web Servers

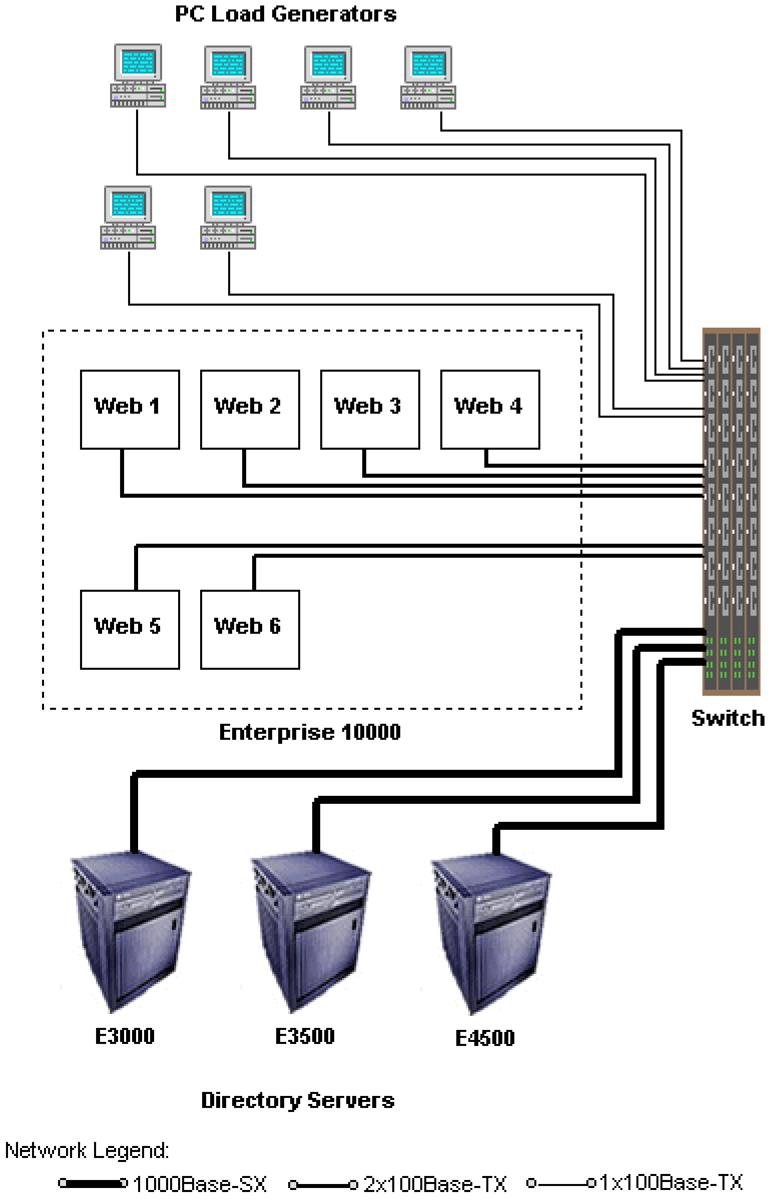


Figure 6: Configuration #5 - 3 Directory (12 CPUs) and 7 Web Servers

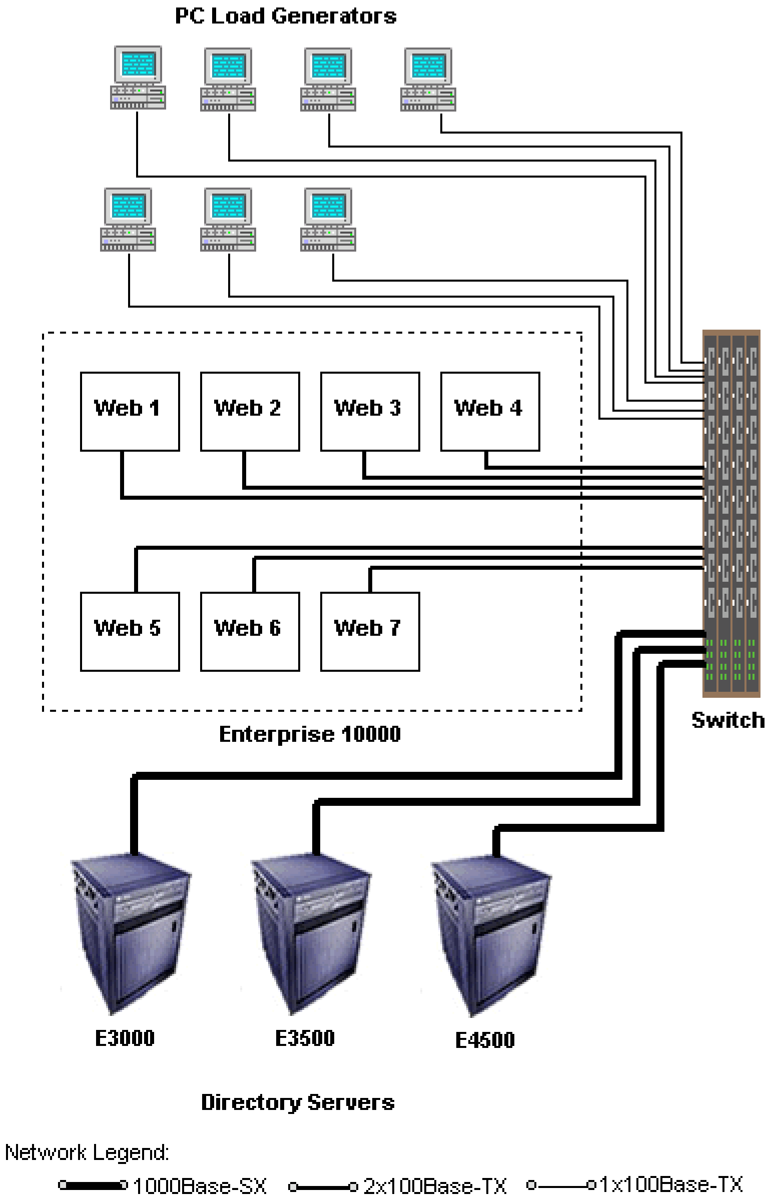
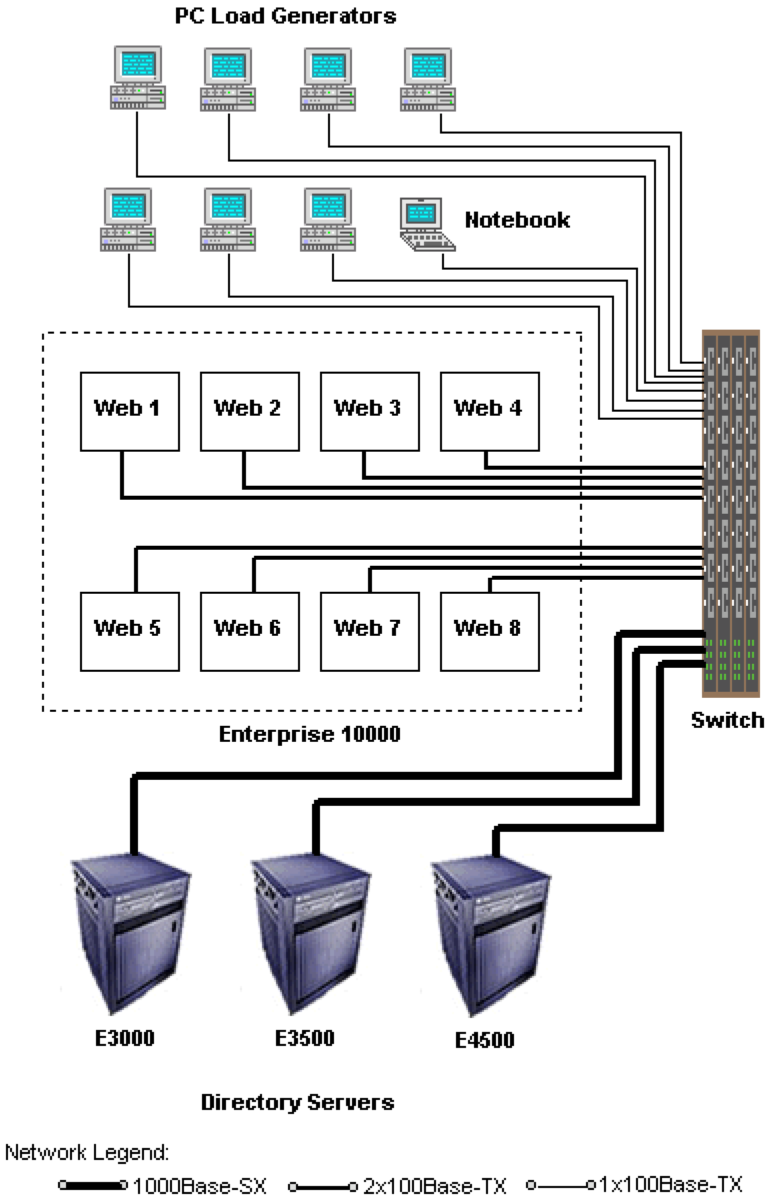


Figure 7: Configuration #6 - 3 Directory (12 CPUs) and 8 Web Servers


PC Load Generators
Notebook
Web 1
Web 2
Web 3
Web 4
Web 5
Web 6
Web 7
Web 8
Enterprise 10000
Switch
E3000
E3500
E4500
Directory Servers
Network Legend:
1000Base-SX
2x100Base-TX
1x100Base-TX

Server Software Configuration and Tuning

We used the following server software for these benchmark tests:

- Solaris 8 with all current recommended patches on all of the Sun systems
- Netscape Directory Server 4.12 (B00.193.0237)
- iPlanet Web Server, Enterprise Edition 4.1 Service Pack 3
- OpenNetwork Technologies DirectorySmart 4.6

All software ran with default settings except for the following:

- **For Netscape Directory Server**:

  Change in slapd.ldbm.conf:

  ```
  lookthroughlimit 10000
  allidsthreshold 5000
  cachesize 110000
  dbcachesize 1000000000
  db_home_directory /tmp/B2B

  index uid pres, eq, sub
  index ou eq, sub
  index o pres, eq
  ```

  Changes in slapd.conf:

  ```
  timelimit 600
  sizelimit 10000
  ```

- **For Solaris**

  ```
  ndd -set /dev/tcp tcp_time_wait_interval 60000
  ndd -set /dev/tcp tcp_conn_req_max_q 1024
  ndd -set /dev/tcp tcp_conn_req_max_q0 4096
  ```

```
ndd -set /dev/tcp tcp_ip_abort_interval 60000
ndd -set /dev/tcp tcp_keepalive_interval 450000
ndd -set /dev/tcp tcp_rexmit_interval_initial 500
ndd -set /dev/tcp tcp_rexmit_interval_max 10000
ndd -set /dev/tcp tcp_rexmit_interval_min 3000
ndd -set /dev/tcp tcp_smallest_anon_port 1024
ndd -set /dev/tcp tcp_slow_start_initial 2
ndd -set /dev/tcp tcp_xmit_hiwat 32768
ndd -set /dev/tcp tcp_recv_hiwat 32768
ndd -set /dev/tcp tcp_deferred_ack_interval 5
```

- **For DirectorySmart**:

```
POST_TO_LOGIN="Y"
CONNECTION_POOL_SIZE="5"
CONNECTION_POOL_MAX_CHECKS="10"
WEB_SERVICE_CACHE_INITIAL_SIZE="20"
USER_CACHE_SIZE="100000"
USER_CACHE_REBALANCE_EVERY_N="10000"
```

Table 7 contains descriptions of how the LDAP directory server and Web server software was setup for each configuration.

Table 7: LDAP Directory Server and Web Server Software Setup

Config.	LDAP Directory Servers	Web Servers
1	Each of the two systems had two separate 1,000,000 -user directories installed with the same user information. Each directory server system had one Web server system (two Web server processes) pointing to it.	Each of the two systems had two separate Web server installations running and listening to ports 80 and 8081.
2	Each of the two systems had two separate 1,000,000 -user directories installed with the same user information. Each directory server system had one	Each of the two systems had four separate Web server installations running and listening to ports 80, 8081,

	Web server system (four Web server processes) pointing to it.	8082, and 8083.
3	Each of the two systems had two separate 1,000,000 -user directories installed with the same user information. Each directory server system had two Web server systems (a system with four Web server processes and another with two Web server processes) pointing to it.	Each of the two systems with four CPUs had four separate Web server installations running and listening to ports 80, 8081, 8082, and 8083. Each of the two systems with two CPUs had two separate Web server installations running and listening to ports 80 and 8081.
4	Each of the three systems had two separate 1,000,000 -user directories installed with the same user information. Each directory server system had two Web server systems (four Web server processes each) pointing to it.	Each of the six systems had four separate Web server installations running and listening to ports 80, 8081, 8082, and 8083.
5	Each of the three systems had two separate 1,000,000 -user directories installed with the same user information. Each directory server system had two Web server systems (four Web server processes each) pointing to it. The seventh Web server system pointed to all three directory server systems as follows: two Web server instances pointed to the first directory server system; another Web server instance pointed to the second directory server system; and the last Web server instance pointed to the third directory server system.	Each of the seven systems had four separate Web server installations running and listening to ports 80, 8081, 8082, and 8083.
	Each of the three systems had two separate 1,000,000 -user directories installed with the same user information. Each	

6	directory server system had two Web server systems (four Web server processes each) pointing to it. The seventh Web server systems pointed to all three directory server systems as follows: two Web server instances pointed to the first directory server system; another Web server instance pointed to the second directory server system; and the last Web server instance pointed to the third directory server system. The eighth Web server systems pointed to all three directory server systems as follows: one Web server instance pointed to the first directory server system; two Web server instances pointed to the second directory server system; and the last Web server instance pointed to the third directory server system.	Each of the eight systems had four separate Web server installations running and listening to ports 80, 8081, 8082, and 8083.

Client Test Systems

For all of the tests, we used personal computers for the load generator systems configured as shown in Table 8. For Configuration #6, we also used a notebook computer for a load generator. It was configured as shown in Table 9. The number of load generator systems we used for each test are shown in Figures 2 through 7.

Table 8: PC Load Generator System Configuration

Feature	Configuration

System	1 x 800EB MHz Pentium III CPU
RAM	512 MB SDRAM
Disk	1 x 10 GB ATA/66
Networks	1 x 100Base-TX (Intel Pro 100B)
Operating System	Microsoft Windows NT 4.0 Workstation, Service Pack 6a

Table 9: Notebook Load Generator System Configuration

Feature	Configuration
System	Toshiba Tecra 8100, 1 x 700 MHz Pentium III CPU
RAM	256 MB SDRAM
Disk	1 x 10 GB
Networks	1 x 100Base-TX (3Com 10/100)
Operating System	Microsoft Windows 2000 Professional, Service Pack 1

NOTICE:

The information in this publication is subject to change without notice.

MINDCRAFT, INC. SHALL NOT BE LIABLE FOR ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

This publication does not constitute an endorsement of the product or products that were tested. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state or local requirements.

Mindcraft is a registered trademark of Mindcraft, Inc.

Product and corporate names mentioned herein are trademarks and/or registered trademarks of their respective companies.

Mindcraft

Services Benchmarks Reports Price/Performance Company

Search Contact Us

For more information, contact us at: info@mindcraft.com
Phone: +1 (408) 395-2404
Fax: +1 (408) 395-6324